Une Introduction aux Formes Quadratiques : Algèbre, Géométrie et Arithmétique

Isar Stubbe

(Version du 10 janvier 2022 à 12h08)

Table des matières

Préface

Voici mon cours sur les formes quadratiques à l'Université du Littoral.

Dans les deux premiers chapitres, l'origine géométrique du groupe orthogonal du plan réel, et le rôle du produit scalaire usuel pour le décrire, sont expliqués. Les chapitres 3 et 4 contiennent les notions de base de la théorie des formes quadratiques : espaces quadratiques et isométries, et leurs incarnations matricielles et polynomiales. Dans le chapitre 5 on étudie la somme orthogonale d'espaces quadratiques, alors que le chapitre 6 contient le résultat important que tout espace quadratique est une somme orthogonale d'espaces de dimension 1. A l'aide de quelques invariants étudiés dans le chapitre 7, on donne la classification complète des espaces quadratiques complexes, réels et finis dans le chapitre 8 : on appréciera les résultats forts différents selon le corps de base. Le chapitre 9 est consacré à l'étude d'isotropie dans un espace quadratique, et on la termine avec la fameuse décomposition de Witt d'un espace quadratique. Dans le chapitre 10 on démontre les théorèmes classiques concernant la décomposition de Witt. Une des démonstrations du chapitre 10 utilise la notion géométrique de réflexion orthogonale, et dans le chapitre 11 on voit son importance pour l'étude du groupe orthogonal d'un espace quadratique quelconque. Le produit tensoriel d'espaces quadratiques est étudié dans le chapitre 12, et on observe comment les (classes d'isométrie des) espaces quadratiques anisotropes sur un corps donné forment un anneau. On calcule explicitement ce fameux anneau de Witt pour le corps des complexes, le corps des réels et les corps finis, dans le dernier chapitre de ce cours.

Cette introduction à la théorie des formes quadratiques est très limitée : l'ensemble de ces notes est prévu pour un cours de seulement 45h, exercices compris. Ainsi l'étude du groupe orthogonal n'est pas très détaillée, et les espaces hermitiens et simplectiques ne sont mentionnés que dans les exercices. Je regrette encore plus l'absence des formes quadratiques rationnelles (le théorème de Hasse-Minkowski étant un grand résultat de la théorie des nombres), des algèbres de Clifford (très élégante généralisation des quaternions) ou encore des formes quadratiques de Pfister (utilisées pour une étude approfondie de l'anneau de Witt). Cependant, j'espère que ce cours rend les références spécialisés accessibles à l'étudant·e intéressé·e.

I.S.

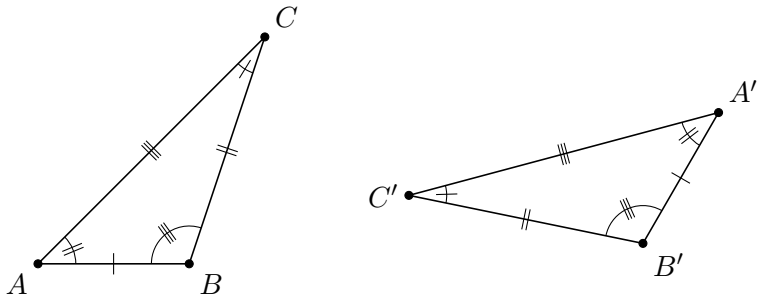
1. Isométries du plan d'Euclide

En -300, Euclide écrit ses *Eléments*, 13 livres dans lesquels il fait un état de la géométrie (plane et solide) connue à son époque, de manière axiomatique. Son sujet, au moins dans les premiers livres, est la *géométrie plane*, qu'il conçoit comme un *espace*—un ensemble de "points" façonné par la disposition de certains sous-ensembles (droites, cercles, triangles, etc.). Dans cette première section, nous rappelons et complétons quelques notions importantes de mon cours de Géométrie en L2 Mathématique [1].

1.1. Le groupe euclidien

Ci-dessous, nous travaillons dans le plan d'Euclide, que nous notons Π. Dans son premier livre, Euclide explique la théorie des triangles congruents :

Définition 1.1.1 *Dans le plan Π, deux triangles sont* congruents *s'il existe une bijection entre les sommets telle que les côtés et angles correspondants sont égaux.*



Un "grand classique" parmi les Propositions d'Euclide est alors :

Proposition 1.1.2 *On a la congruence de deux triangles s'ils ont trois côtés égaux.*

Ceci implique la propriété remarquable que toute transformation du plan préservant les distances (les longueurs de segments), préserve aussi les angles. Par ailleurs, une telle transformation préserve aussi la collinéarité de points, et envoit tout cercle sur un cercle de même rayon (exercice). Cela mérite d'être souligné par :

Définition 1.1.3 *Une* isométrie *du plan Π est une bijection $f : \Pi \to \Pi$ préservant les distances :*

$$\forall A, B \in \Pi : \mathrm{dist}(A, B) = \mathrm{dist}(f(A), f(B)).$$

1. Disponible ici : `http://www-lmpa.univ-littoral.fr/~stubbe/GM`

La composée de deux isométries est une isométrie ; et la fonction inverse $f^{-1}\colon \Pi \to \Pi$ d'une isométrie $f\colon \Pi \to \Pi$ préserve aussi les distances (exercice). Ainsi il suit facilement que :

Proposition 1.1.4 *Les isométries de* Π *forment un groupe (pour la composition usuelle de fonctions, le neutre étant donc la fonction "identité"* $\mathsf{id}\colon \Pi \to \Pi\colon P \mapsto P$*), noté* Iso*. (On l'appelle aussi parfois le* groupe euclidien *du plan.)*

Intuitivement il est clair que, parmi les isométries de Π, on a :

- les *translations* (de déplacement donné),
- les *rotations* (de centre et angle donnés),
- les *réflexions* (d'axe donné).

Dans le groupe Iso, on peut donc composer ces isométries particulières pour en obtenir d'autres.

On se donne maintenant pour but de mieux comprendre le groupe Iso. Pour cela, on va classifier les éléments de Iso, en faisant le lien avec les triangles congruents.

Proposition 1.1.5 *Toute isométrie du plan* $f\colon \Pi \to \Pi$ *envoit un triangle* ABC *sur un triangle congruent* $f(A)f(B)f(C)$*.*

Démonstration. Par le critère CCC de triangles congruents. □

Lemme 1.1.6 *Il n'existe pas deux points distincts ayant les mêmes distances aux trois sommets d'un triangle donné.*

Démonstration. Soit un triangle ABC. S'il existe deux points distincts, P et Q, tels que

$$\mathrm{dist}(P,A) = \mathrm{dist}(Q,A), \mathrm{dist}(P,B) = \mathrm{dist}(Q,B), \mathrm{dist}(P,C) = \mathrm{dist}(Q,C),$$

alors A, B et C sont des points de la médiatrice du segment PQ. Mais les sommets d'un triangle ne sont jamais collinéaires. On a donc $P = Q$. □

Proposition 1.1.7 *Pour toute paire de triangles congruents*[2] ABC *et* $A'B'C'$*, il existe au plus une isométrie* $f\colon \Pi \to \Pi$ *telle que* $f(A) = A'$*,* $f(B) = B'$*,* $f(C) = C'$*.*

Démonstration. Cette isométrie envoit un point $P \in \Pi$ nécessairement sur l'unique point P' tel que $\mathrm{dist}(A,P) = \mathrm{dist}(A',P')$, $\mathrm{dist}(B,P) = \mathrm{dist}(B',P')$, $\mathrm{dist}(C,P) = \mathrm{dist}(C',P')$. □

Proposition 1.1.8 *Pour toute congruence de triangles* ABC *et* $A'B'C'$*, il existe une composée* $f\colon \Pi \to \Pi$ *de au plus trois réflexions telle que* $f(A) = A'$*,* $f(B) = B'$*,* $f(C) = C'$*.*

Démonstration. On fait au plus trois réflexions comme suit (exercice : faire un dessin !) :

1. la réflexion r_1 par la médiatrice de AA' : on a $A' = r_1(A)$, et on note aussi $B_1 := r_1(B)$, $C_1 := f_1(C)$,

2. Lorsqu'on parle de triangles congruents ABC et $A'B'C'$, on sous-entend toujours que la congruence est donnée par la bijection entre les sommets $A \leftrightarrow A'$, $B \leftrightarrow B'$, $C \leftrightarrow C'$.

2. la réflexion r_2 par la médiatrice de B_1B' : on a $A' = r_2(A_1) = r_2(r_1(A))$ et $B' = r_2(B_1) = r_2(r_1(B))$, et on note aussi $C_2 := r_2(C_1) = r_2(r_1(C))$,
3. la réflexion r_3 par la médiatrice de C_2C' : on obtient finalement $A' = r_3(r_2(r_1(A))$, $B' = r_3(r_2(r_1(B)))$, $C' = r_3(r_2(r_1(C)))$.

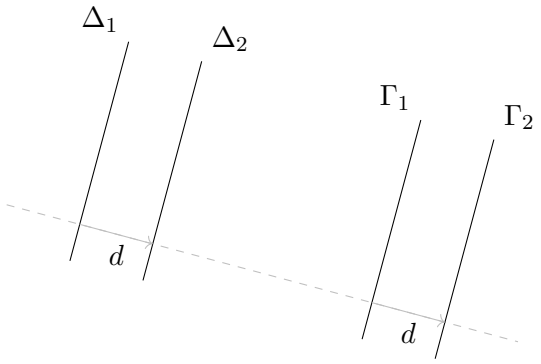
L'isométrie $f = r_3 \circ r_2 \circ r_1$ envoit ainsi ABC sur $A'B'C'$. □

On peut conclure :

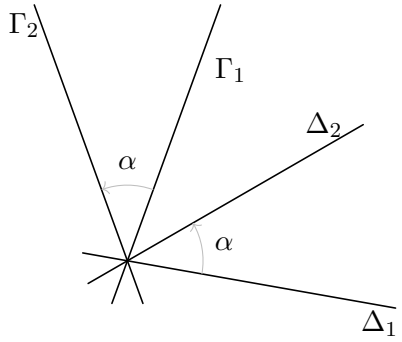
Théorème 1.1.9 *Toute isométrie $f\colon \Pi \to \Pi$ est la composée de au plus trois réflexions.*

Ce résultat nous permet de classifier les isométries :

1. Une réflexion $r_\Delta\colon \Pi \to \Pi$ (d'axe Δ, une droite dans le plan Π) fixe tous les points de la droite Δ, et change l'orientation des triangles. Toute réflexion est sa propre inverse : $(r_\Delta)^{-1} = r_\Delta$; autrement dit, $(r_\Delta)^2 = r_\Delta \circ r_\Delta$ est le neutre du groupe.
2. Une translation est la composée de deux réflexions d'axes parallèles : $r_{\Delta_2} \circ r_{\Delta_1}$ avec $\Delta_1 \parallel \Delta_2$. Elle n'a pas de points fixes (hormis le cas $\Delta_1 = \Delta_2$, auquel cas la translation est le neutre du groupe, et fixe donc tous les points du plan) et préserve l'orientation des triangles. La distance entre les droites est la moitié du déplacement de la translation, qui se fait orthogonalement aux deux droites, dans le sens de Δ_1 vers Δ_2. De plus, si Γ_1 et Γ_2 sont deux droites parallèles entre elles et parallèles à Δ_1 et Δ_2, et la distance entre Δ_1 et Δ_2 est égale à la distance entre Γ_1 et Γ_2 (et dans le même sens), alors $r_{\Gamma_2} \circ r_{\Gamma_1} = r_{\Delta_2} \circ r_{\Delta_1}$; autrement dit, les Γ_i's déterminent la même translation que les Δ_i's.



3. Une rotation est la composée de deux réflexions d'axes sécants : $r_{\Delta_2} \circ r_{\Delta_1}$ avec $\Delta_1 \nparallel \Delta_2$. Une rotation préserve l'orientation des triangles. Son seul point fixe est le point d'intersection des droites Δ_1 et Δ_2 (hormis le cas $\Delta_1 = \Delta_2$, auquel cas la rotation est le neutre du groupe, et fixe donc tous les points du plan), qui est donc le centre de la rotation ; l'angle de Δ_1 à Δ_2 est la moitié de l'angle de la rotation. De plus, si deux droites Γ_1 et Γ_2 sont sécantes au même point que les droites Δ_1 et Δ_2, et si l'angle entre les Γ_i's et le même que l'angle entre les Δ_i's, alors $r_{\Gamma_2} \circ r_{\Gamma_1} = r_{\Delta_2} \circ r_{\Delta_1}$; autrement dit, les Γ_i's déterminent la même rotation que les Δ_i's.



4. Une réflexion glissée est la composée de trois réflexions, $r_{\Delta_3} \circ r_{\Delta_2} \circ r_{\Delta_1}$, et on peut toujours faire en sorte que $\Delta_1 \parallel \Delta_2 \perp \Delta_3$; autrement dit, une réflexion glissée est toujours une translation suivie d'une réflexion. (Démonstration : exercice !) Elle n'a pas de points fixes (hormis le cas $\Delta_1 = \Delta_2$, auquel cas la réflexion glissée se réduit à une simple réflexion, et fixe donc tous les éléments de la droite Δ_3), et change l'orientation des triangles.

Remarque 1.1.10 Soulignons que le neutre du groupe Iso, $\mathsf{id} \colon \Pi \to \Pi \colon P \mapsto P$, est toujours égal à la composée d'une réflexion r_Δ avec elle-même : $\mathsf{id} = r_\Delta \circ r_\Delta$ (pour Δ quelconque). Ainsi, on peut conclure que id est une translation (déterminée par deux droites identiques) mais également une rotation (déterminé par deux droites identitiques) ; par contre, id est ni une réflexion ni une réflexion glissée.

1.2. Le groupe orthogonal

Observons d'abord :

Proposition 1.2.1 *Soit un point $P \in \Pi$, alors l'ensemble*

$$\mathsf{Iso}_P = \{f \in \mathsf{Iso} \mid f(P) = P\}$$

est un sous-groupe de Iso (qui ne contient aucune translation, hormis l'identité). Pour tout $Q \in \Pi$, soit $t \in \mathsf{Trans}$ l'unique translation telle que $t(P) = Q$. On a alors l'isomorphisme de groupes

$$\mathsf{Iso}_P \underset{\psi}{\overset{\phi}{\rightleftarrows}} \mathsf{Iso}_Q$$

par $\phi(f) = t \circ f \circ t^{-1}$ et $\psi(g) = t^{-1} \circ g \circ t$.

Démonstration. Exercice. □

Ce résultat confirme l'idée d'une "homogénéité" du plan : pour tout choix de point P, les "symétries" du plan fixant ce point P sont les mêmes. De plus, via des translations on peut passer d'un point à l'autre, et ce déplacement "ne déforme pas" les symétries qu'on y observe. Clairement, ce groupe Iso_P (ou mieux dit, cette classe de groupes isomorphes $\mathsf{Iso}_P \cong \mathsf{Iso}_Q \cong \mathsf{Iso}_R \cong$ ... autant de copies isomorphes du groupe qu'il y a des points dans Π !) mérite un nom :

Définition 1.2.2 *"Le" groupe orthogonal du plan* Π *est* $\mathsf{O} \cong \mathsf{Iso}_P$ *(pour* P *un point quelconque du plan).*

Pour insister une fois de plus, ce groupe est donc défini à isomorphisme près. Par ailleurs, voici une autre façon de le décrire :

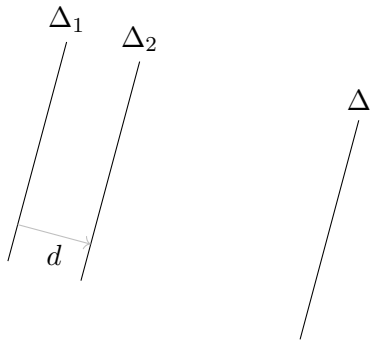
Proposition 1.2.3 *Les translations de* Π *forment un sous-groupe normal de* Iso*, noté* $\mathsf{Trans} \trianglelefteq \mathsf{Iso}$*.*

Démonstration. La composée de deux translations est une translation (exercice : donner les détails !), et le neutre de Iso est une translation ; ainsi Trans est un sous-groupe de Iso. Pour montrer qu'il s'agit d'un sous-groupe normal, on doit vérifier que, pour tout $f \in \mathsf{Iso}$ et tout $t \in \mathsf{Trans}$, on a $f \circ t \circ f^{-1} \in \mathsf{Trans}$. Mais puisque tout $f \in \mathsf{Iso}$ est la composée de (au plus trois) réflexions, il suffit de montrer que $r_\Delta \circ t \circ r_\Delta^{-1} \in \mathsf{Trans}$. De manière équivalente, on doit montrer qu'il existe $t' \in \mathsf{Trans}$ telle que $r_\Delta \circ t = t' \circ r_\Delta$. On sait qu'une translation s'écrit comme $t = r_{\Delta_2} \circ r_{\Delta_1}$, pour $\Delta_1 \parallel \Delta_2$. On distingue deux cas :

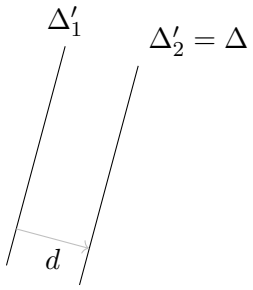
a) Si $\Delta \parallel \Delta_1$ (et donc $\Delta \parallel \Delta_2$), on fait le calcul suivant :

$$r_\Delta \circ t = r_\Delta \circ r_{\Delta_2} \circ r_{\Delta_1} = r_\Delta \circ r_{\Delta_2'} \circ r_{\Delta_1'} = \mathsf{id} \circ r_{\Delta_1'} = r_{\Delta_1'} = r_{\Delta_1'} \circ \mathsf{id} = r_{\Delta_1'} \circ r_\Delta \circ r_\Delta = t' \circ r_\Delta.$$

Ici, on démarre donc avec les trois droites parallèles :



puis on remplace les droites Δ_1 et Δ_2 par des droites parallèles Δ_1' et Δ_2' (définissant la même translation t) de telle sorte que $\Delta_2' = \Delta$:

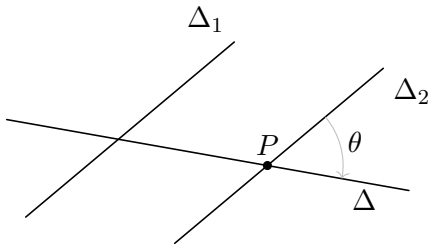


Ainsi on a $r_\Delta \circ r_{\Delta_2'} = \mathsf{id}$, et l'isométrie composée revient à faire tout simplement $r_{\Delta_1'}$. On introduit l'identité, écrite comme $\mathsf{id} = r_\Delta \circ r_\Delta$, et pour conclure on définit la translation $t' = r_{\Delta_1'} \circ r_\Delta$.

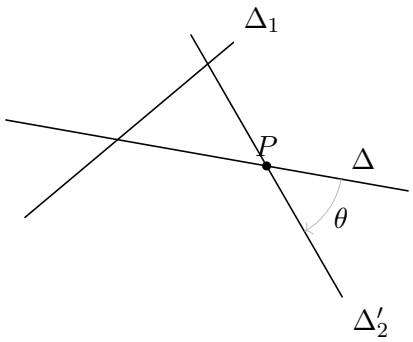
b) Si $\Delta \nparallel \Delta_1$ (et donc $\Delta \nparallel \Delta_2$), on fait le calcul suivant :

$$r_\Delta \circ r_{\Delta_2} \circ r_{\Delta_1} = r_{\Delta_2'} \circ r_\Delta \circ r_{\Delta_1} = r_{\Delta_2'} \circ r_{\Delta_1'} \circ r_\Delta.$$

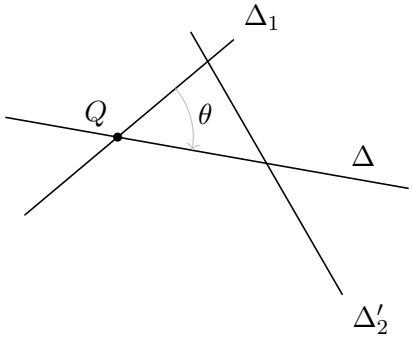
Maintenant on démarre donc avec deux droites parallèles et une sécante :



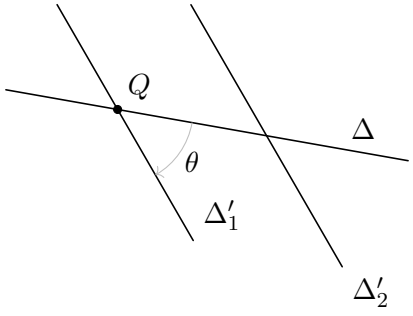
Les droites sécantes Δ_2 et Δ définissent une rotation ; on peut en modifier la disposition par rotation de centre P pour que $r_\Delta \circ r_{\Delta_2} = r_{\Delta_2'} \circ r_\Delta$:



Ensuite, on peut faire de même avec les droites sécantes Δ_1 et Δ :



En modifiant la position des droites (par rotation de centre Q) on a l'égalité $r_\Delta \circ r_{\Delta_1} = r_{\Delta_1'} \circ r_\Delta$:



Par la géométrie de la situation, on obtient deux droites parallèles $\Delta_1' \parallel \Delta_2'$, et donc on termine sur une translation $t' = r_{\Delta_2'} \circ r_{\Delta_1'}$ à effectuer après la réflexion r_Δ. □

On peut donc calculer le quotient du groupe Iso par son sous-groupe normal Trans, soit $\mathsf{Iso}/\mathsf{Trans}$.

Théorème 1.2.4 *Pour tout $P \in \Pi$ on a un isomorphisme de groupes $\mathsf{Iso}/\mathsf{Trans} \cong \mathsf{Iso}_P$; autrement dit, le groupe orthogonal du plan Π est également défini (à isomorphisme près) par $\mathsf{O} \cong \mathsf{Iso}/\mathsf{Trans}$.*

Démonstration. On montre facilement que $\mathsf{Trans} \cap \mathsf{Iso}_P = \{\mathsf{id}\}$; puis aussi que $\mathsf{Trans} \circ \mathsf{Iso}_P = \mathsf{Iso}$, c'est à dire, tout $f \in \mathsf{Iso}$ peut s'écrire comme une composée $f = t \circ g$ avec $t \in \mathsf{Trans}$ et $g \in \mathsf{Iso}_P$. (Exercice : compléter les détails.) □

Du point de vue théorique (et conceptuel), il est utile de savoir que le groupe orthogonal O est le quotient $\mathsf{Iso}/\mathsf{Trans}$; mais du point de vue pratique il est souvent plus facile de le penser (à isomorphisme près) comme Iso_P. Fixant $P \in \Pi$, on voit en effet facilement que les éléments de $\mathsf{O} \cong \mathsf{Iso}_P$ sont :

- soit des réflexions d'axe passant par P,
- soit des rotations de centre P (= composées de deux réflexions d'axes passant par P).

On résume :

Corollaire 1.2.5 *Tout élément du groupe orthogonal O est une composée de au plus deux réflexions.*

De façon similaire à ce que nous avons fait pour les translations, on peut démontrer pour les rotations que :

- les rotations de centre $P \in \Pi$ forment un sous-groupe normal de Iso_P, noté $\mathsf{Rot}_P \trianglelefteq \mathsf{Iso}_P$,
- l'isomorphisme $\mathsf{Iso}_P \cong \mathsf{Iso}_Q$ (induit par l'unique translation t telle que $t(P) = Q$) se restreint à un isomorphisme $\mathsf{Rot}_P \cong \mathsf{Rot}_Q$,
- on peut donc définir "le" groupe orthogonal spécial par $\mathsf{SO} \cong \mathsf{Rot}_P$ (pour un point $P \in \Pi$ quelconque),
- pour tout choix de réflexion $r_\Delta \in \mathsf{Iso}_P$, on a le sous-groupe $\{\mathsf{id}, r_\Delta\}$ de Iso_P, et on a un isomorphisme de groupes $\mathsf{Iso}_P/\mathsf{Rot}_P \cong \{\mathsf{id}, r_\Delta\}$,
- le groupe $\{\mathsf{id}, r_\Delta\}$ étant (à isomorphisme près) le groupe cyclique d'ordre 2, noté C_2, l'assertion précédente implique que $\mathsf{O}/\mathsf{SO} \cong \mathsf{C}_2$,
- autrement dit, il existe un homomorphisme surjectif $h\colon \mathsf{O} \to \mathsf{C}_2$ dont le noyau est SO.

On le laisse en exercice.

1.3. Exercices

1. Compléter tous les exercices indiqués dans le texte.

2. Montrer que le groupe Iso n'est pas commutatif. Qu'en est-il pour Trans ? Pour O ? Pour SO ?

3. Montrer qu'un sous-groupe N d'un groupe G est normal si et seulement si $N = \ker(f)$ pour un homomorphisme de groupes $f\colon G \to H$. Indication : étant donné $N \trianglelefteq G$, on peut considérer le quotient $q\colon G \to G/N$. (Que se passe-t-il pour un sous-groupe "non-normal" ?)

4. *Le produit direct de groupes.* Pour $H, K \leq G$ deux sous-groupes d'un groupe $G = (G, \cdot, 1)$, montrer que $f\colon H \times K \to G\colon (h,k) \mapsto hk$ est un isomorphisme de groupes (où on définit $(h,k)\cdot(h',k') = (hh', kk')$) si et seulement si $H, K \trianglelefteq G$ sont des sousgroupes normaux tels que $G = HK$ et $H \cap K = \{1\}$. Dans ce cas, on dit que G est le *produit direct* de H et K.
Solution. Partant de l'isomorphisme $f(h,k) = hk$, on sait que tout $g \in G$ s'écrit de manière unique comme $g = hk$ avec $h \in H$ et $k \in K$; ainsi $G = HK$. Aussi, si $g \in H \cap K$ alors $f(g, g^{-1}) = 1 = f(1,1)$ et donc $g = 1$. Finalement, pour tout $f(h,k) \in G$ et $f(h',1) \in H$, on a $f(h,k)\cdot f(h',1)\cdot f(h,k)^{-1} = f(h,k)\cdot f(h',1)\cdot f(h^{-1},k^{-1}) = f(hh'h^{-1}, kk^{-1}) = f(hh'h^{-1}, 1) \in H$ donc $H \trianglelefteq G$; et de la même manière on démontre la normalité de K. Réciproquement, la fonction $f\colon H \times K \to G\colon (h,k) \mapsto hk$ satisfait toujours à $f(1,1) = 1$. Par la supposée normalité de H et de K, on a pour $h \in H$ et $k \in K$ que $hkh^{-1}k^{-1} \in H \cap K$, donc si on suppose en plus que $H \cap K = \{1\}$ alors on trouve $hk = kh$. Par conséquent, la fonction f préserve la multiplication : $f((h,k)\cdot(h',k')) = f(hh', kk') = hh'kk' = hkh'k' = f(h,k)\cdot f(h',k)$. Le noyau de l'homomorphisme f est $\ker(f) = \{(h,k) \in H \times K \mid hk = 1\} = \{(h,k) \in H \times K \mid h = k^{-1}\} = \{(g, g^{-1}) \mid g \in H \cap K\}$; il est donc trivial – et f est injective – par l'hypothèse que $H \cap K = \{1\}$. Finalement, f est une surjection si on suppose que $G = HK$. Somme toute, f est un isomorphisme.

5. *Le produit semidirect de groupes.* Soit $N \trianglelefteq G$ un sous-groupe normal et $H \leq G$ un sous-groupe quelconque d'un groupe $G = (G, \cdot, 1)$. Montrer que (1) $N \cap H = \{1\}$ et $NH = G$ si et seulement si (2) la composée de l'inclusion $i\colon H \to G$ avec le quotient $q\colon G \to G/N$ est un isomorphisme, si et seulement si (3) il existe un homomorphisme $f\colon G \to H$ qui est l'identité sur H et dont N est le noyau. Dans ce cas, on dit que G est le *produit semidirect* de N et H, noté $G = N \rtimes H$.
Solution. Avec la donnée de $N \trianglelefteq G$ et $H \leq G$, on a toujours la composée $q \circ i\colon H \to G/N\colon h \mapsto [h]$. Son noyau est $\ker(q\circ i) = \{h \in H \mid [h] = [1]\} = N \cap H$ et son image est $\mathrm{im}(q\circ i) = \{[h] \mid h \in H\}$. Ainsi, $q\circ i$ est injectif si et seulement si $N \cap H = \{1\}$; et $q\circ i$ est surjectif si et seulement si pour tout $g \in G$ il existe un $h \in H$ tel que $[g] = [h]$, si et seulement si $G = NH$. Cela démontre $(1 \Leftrightarrow 2)$. Supposons maintenant la validité de (2). La composée $\varphi^{-1} \circ q\colon G \to H$ est un homomorphisme de noyau $\ker(\varphi^{-1}\circ q) = \{g \in G \mid \varphi^{-1}(q(g)) = 1\} = \varphi(1)\} = \{g \in G \mid [g] = [1]\} = G \cap N = N$. De même, pour $h \in H$ on peut calculer que $\varphi^{-1}(q(h)) = \varphi^{-1}([h]) = h$, donc $\varphi^{-1}\circ q$ est l'identité sur H. Ainsi on trouve que $f = \varphi^{-1}\circ q$ est l'homomorphisme demandé en (3). Réciproquement, un homomorphisme $f\colon G \to H$ de noyau $\ker(f) = N$ et tel que la composée $f \circ i\colon H \to H$ est l'identité, détermine un isomorphisme $\overline{f}\colon G/N \to \mathrm{im}(f) = H$ satisfaisant à $\overline{f}\circ q = f$ (par la propriété universelle du quotient). On peut calculer que $\overline{f}\circ q \circ i = f \circ i = \mathsf{id}_H$ donc $q \circ i = \overline{f}^{-1}$

est aussi un isomorphisme. Ainsi on obtient (2).

6. *Le produit semidirect de sous-groupes normaux est leur produit direct.* Si $N \trianglelefteq G$ et $H \trianglelefteq G$ et $G = N \rtimes H$, montrer que G est isomorphe à $N \times H$, le produit direct.
Solution. On sait que $G = N \rtimes H$ est équivalent à $G = NH$ et $N \cap H = \{1\}$. Puisqu'on ajoute ici que non-seulement $N \trianglelefteq G$ mais aussi $H \trianglelefteq G$, on obtient la commutation de tout $n \in N$ avec tout $h \in H$. En effet, le commutateur $nhn^{-1}h^{-1}$ est à la fois dans N (par normalité de N) et dans H (par normalité de H), et puisque $N \cap H = \{1\}$, on obtient bien $nh = hn$. Et c'est exactement ce qu'il faut pour avoir un isomorphisme $f\colon N \times H \to G\colon (n, h) \mapsto nh$.

7. Soit une action d'un groupe $G = (G, \cdot, 1)$ sur un ensemble X, notée $G \times X \to X\colon (g, x) \mapsto gx$. Notons $G_x = \{g \in G \mid gx = x\}$ le stabilisateur de $x \in X$, et $Gx = \{gx \in X \mid g \in G\}$ l'orbite de $x \in X$. On dit que l'action est *libre* lorsque $G_x = \{1\}$ pour tout $x \in X$; et l'action est *transitive* si $Gx = X$ pour tout $x \in X$.

(a) Montrer que G_x est un sous-groupe de G, et que $G_x \cong G_{gx}$ pour tout $g \in G$.

(b) Montrer que, si l'action de G sur X est transitive, alors tous les G_x sont isomorphes.

Supposons maintenant que $H \trianglelefteq G$ est un sous-groupe normal tel que l'action induite $H \times X \to X$ est libre et transitive.

(c) Montrer qu'aussi l'action $G \times X \to X$ est transitive (mais pas nécessairement libre).

(d) Montrer que G/H est isomorphe à (chaque) G_x. Indication : Soit $h_{x,y}$ l'unique élément de H tel que $h_{x,y}x = y$, alors l'application $G \to G_x\colon g \mapsto h_{gx,x} \circ g$ est un homomorphisme surjectif dont le noyau est H.

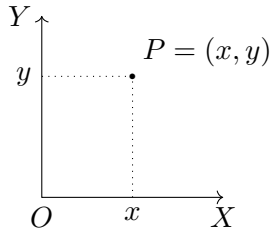
(e) Appliquer à l'action $\mathsf{Iso} \times \Pi \to \Pi\colon (f, P) \mapsto f(P)$ et le sous-groupe normal $\mathsf{Trans} \trianglelefteq \mathsf{Iso}$.

2. Isométries du plan cartésien

En 1637, René Descartes publie son *Discours de la méthode* "pour bien conduire la raison et chercher la vérité dans les sciences", dont un annexe sur *La Géométrie* mets en application cette méthode. Il y introduit ce que l'on appelle aujourd'hui la géométrie analytique : une présentation algébrique de la géométrie d'Euclide. Dans cette section nous donnons ainsi une description matricielle des groupes d'isométries de la section précédente, en rappelant et en complétant ici encore mon cours de Géométrie en L2 Mathématique.

2.1. Coordonées

On travaille toujours dans le plan, mais on y choisit désormais un *repère orthonormé* : on se donne ainsi la possibilité d'identifier le plan avec $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$.



On peut développer des "formules" – des expressions analytiques en x et y – pour les notions élémentaires de la géométrie plane, que nous avons rencontrées dans la section précédente :

(a) la distance (euclidienne) d'un point $P = (x_1, y_1)$ à un point $Q = (x_2, y_2)$ se calcule par la formule

$$\operatorname{dist}(P, Q) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

(b) une droite Δ est le lieu d'une équation linéaire en deux variables, soit

$$\Delta = \{(x, y) \mid ax + by + c = 0\},$$

ou simplement écrit comme $\Delta : ax + by + c = 0$,

(c) la translation [1] envoyant $O = (0, 0)$ sur $A = (a, b)$ est donnée par

$$f \colon \mathbb{R}^2 \to \mathbb{R}^2 \colon \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$$

1. On utilisera souvent la notation matricielle : on confondera le couple (x, y) avec la matrice colonne $\begin{pmatrix} x \\ y \end{pmatrix}$.

(d) la rotation de centre $O = (0, 0)$ et d'angle θ est donnée par

$$f\colon \mathbb{R}^2 \to \mathbb{R}^2\colon \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

(e) La réflexion d'axe $\Delta : ax + by + c = 0$ est donnée par

$$f\colon \mathbb{R}^2 \to \mathbb{R}^2\colon \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \ldots \qquad \text{(exercice)}$$

Maintenant on veut donner une description matricielle des groupes Iso, O et SO.

Proposition 2.1.1 *Toute isométrie du plan cartésien $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ peut s'écrire comme*

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^i \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$$

pour certains $\theta \in [0, 2\pi[$, $i \in \{0, 1\}$ et $(a, b) \in \mathbb{R}^2$.

Démonstration. Une isométrie du plan définit, et est définie par, deux traingles congruents, disons ABC et $A'B'C'$. (On peut choisir p.e. $A = (0, 0)$, $B = (1, 0)$ et $C = (0, 1)$; pour $A'B'C'$ on prend alors l'image par f de ABC.) Pour envoyer le triangle ABC sur le triangle $A'B'C'$, on peut faire la composée de :

1. d'abord, si nécessaire, une réflexion d'axe X, pour orienter ABC et $A'B'C'$ de la même façon,
2. puis, une rotation de centre O, pour obtenir le parallélisme des côtés des deux triangles,
3. et finalement, une translation, pour faire coïncider les deux triangles.

Cela donne la formule souhaitée. (Détails et dessin : exercice) □

Puisqu'une matrice [2] $M \in \mathbb{R}^{2\times 2}$ est de la forme

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^i$$

si et seulement si elle est orthogonale (exercice), on obtient :

Proposition 2.1.2 *Une fonction $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ est une isométrie du plan cartésien si et seulement si*

$$f\begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix} + V$$

avec $M \in \mathbb{R}^{2\times 2}$ tel que $M^t M = I$, et $V \in \mathbb{R}^{2\times 1}$.

2. On note $\mathbb{R}^{m\times n}$ l'ensemble des matrices réelles $m \times n$, et I_n est la matrice unité $n \times n$, mais on l'écrit tout simplement I si sa dimension est évidente.

Ensuite, le groupe orthogonal (du plan cartésien) O peut être identifié avec le groupe Iso_O des isométries ayant $O = (0,0)$ comme point fixe. Mais pour $f \in \mathsf{Iso}$ on a clairement

$$f \in \mathsf{Iso}_O \quad \Longleftrightarrow \quad f\begin{pmatrix}0\\0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix} \quad \Longleftrightarrow \quad f\begin{pmatrix}x\\y\end{pmatrix} = M\begin{pmatrix}x\\y\end{pmatrix}.$$

De plus, la composition de deux telles isométries $f, g \in \mathsf{Iso}_O$ correspond au produit matriciel :

$$\text{pour } f\begin{pmatrix}x\\y\end{pmatrix} = M\begin{pmatrix}x\\y\end{pmatrix} \text{ et } g\begin{pmatrix}x\\y\end{pmatrix} = N\begin{pmatrix}x\\y\end{pmatrix} \text{ on a } (g\circ f)\begin{pmatrix}x\\y\end{pmatrix} = NM\begin{pmatrix}x\\y\end{pmatrix}.$$

On obtient immédiatement que :

Théorème 2.1.3 *Le groupe orthogonal est (à isomorphisme près) le groupe des matrices orthogonales :* $\mathsf{O} \cong \{M \in \mathbb{R}^{2\times 2} \mid M^t M = I\}$.

Finalement, l'application

$$\det\colon \{M \in \mathbb{R}^{2\times 2} \mid M^t M = I\} \to \{-1,+1\}\colon M \mapsto \det(M)$$

est un homomorphisme surjectif de groupes pour la multiplication (exercice). Son noyau est le sous-groupe normal

$$\ker(\det) = \{M \in \mathbb{R}^{2\times 2} \mid M^t M = I \text{ et } \det(M) = 1\}.$$

On vérifie facilement qu'une matrice orthogonale $M \in \mathbb{R}^{2\times 2}$ est une matrice de rotation (de centre $O = (0,0)$, donc) si et seulement si $\det(M) = 1$ (exercice). Puisque le groupe multiplicatif $\{-1,+1\}$ est (à isomorphisme près) le groupe cyclique C_2 à deux éléments, il suit :

Théorème 2.1.4 *Le groupe orthogonal spécial est (à isomorphisme près) le groupe des matrices orthogonales spéciales :* $\mathsf{SO} \cong \{M \in \mathbb{R}^{2\times 2} \mid M^t M = I \text{ et } \det(M) = 1\}$. *On a un isomorphisme de groupes* $\mathsf{O}/\mathsf{SO} \cong \mathsf{C}_2$.

Démonstration. Le noyau d'un homomorphisme de groupes $h\colon G \to H$ est toujours un sous-groupe normal : $\ker(h) \trianglelefteq G$; si h est surjectif, on a toujours un isomorphisme $G/\ker(h) \cong H$. On applique ce résultat général de la théorie des groupes ici à l'homomorphisme surjectif $\det\colon \mathsf{O} \to \mathsf{C}_2$, dont le noyau est SO. □

2.2. Produit scalaire

Dans la suite nous allons peaufiner notre description analytique des isométries du plan cartésien en considérant le rôle du produit scalaire. Rappelons que $\mathbb{R}^2$ est bien évidemment un espace vectoriel réel ; désormais on note $\underline{x} = (x_1, x_2)$ pour un élément de $\mathbb{R}^2$ (et on utilisera au besoin aussi des notations matricielles). Cet espace est muni du produit scalaire :

$$\underline{x}\cdot\underline{y} = x_1y_1 + x_2y_2 = \begin{pmatrix}x_1 & x_2\end{pmatrix}\begin{pmatrix}y_1\\y_2\end{pmatrix}.$$

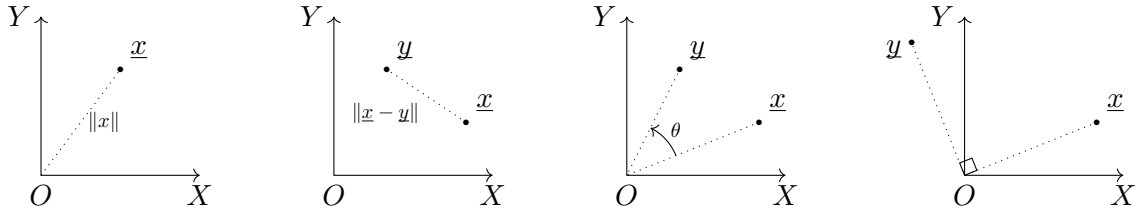
Ce produit scalaire sert notamment à :

– définir la norme d'un vecteur : $\|\underline{x}\| = \sqrt{\underline{x} \cdot \underline{x}}$,

– calculer la distance entre deux vecteurs : $\mathrm{dist}(\underline{x}, \underline{y}) = \|\underline{x} - \underline{y}\|$,

– calculer (le cosinus de) l'angle entre deux vecteurs : $\cos(\theta) = \frac{\underline{x} \cdot \underline{y}}{\|\underline{x}\|\|\underline{y}\|}$,

– détecter l'orthogonalité de deux vecteurs : $\underline{x} \perp \underline{y} \iff \underline{x} \cdot \underline{y} = 0$.



Il suit immédiatement de la formule matricielle du produit scalaire que :

Proposition 2.2.1 *Le produit scalaire est :*

1. *bilinéaire :* $(\alpha\underline{x} + \beta\underline{y}) \cdot \underline{z} = \alpha(\underline{x} \cdot \underline{z}) + \beta(\underline{y} \cdot \underline{z})$ *et* $\underline{x} \cdot (\alpha\underline{y} + \beta\underline{z}) = \alpha(\underline{x} \cdot \underline{y}) + \beta(\underline{x} \cdot \underline{z})$,
2. *symétrique :* $\underline{x} \cdot \underline{y} = \underline{y} \cdot \underline{x}$,
3. *définie positive :* $\underline{x} \cdot \underline{x} \geq 0$, *et* $\underline{x} \cdot \underline{x} = 0$ *si et seulement si* $\underline{x} = \underline{0}$.

Mais il y a encore une autre façon de manipuler le produit scalaire—via la "norme au carré" :

Proposition 2.2.2 *Pour l'application* $q\colon \mathbb{R}^2 \to \mathbb{R}\colon \underline{x} \mapsto \underline{x} \cdot \underline{x}$, *qu'on appelle la* forme quadratique *associée au produit scalaire* $\underline{x} \cdot \underline{y}$, *on a que*

$$\underline{x} \cdot \underline{y} = \frac{1}{2}(q(\underline{x} + \underline{y}) - q(\underline{x}) - q(\underline{y})).$$

Démonstration. Exercice. □

Maintenant nous pouvons reformuler la notion d'isométrie fixant $O = (0, 0)$ du plan $\mathbb{R}^2$:

Théorème 2.2.3 *Pour une application* $f\colon \mathbb{R}^2 \to \mathbb{R}^2\colon \underline{x} \mapsto f\underline{x}$, *on a l'équivalence des assertions suivantes :*

1. $f \in \mathsf{Iso}_O$,
2. f *est un automorphisme linéaire*[3] *tel que, pour tout* $\underline{x} \in \mathbb{R}^2$, $q(\underline{x}) = q(f\underline{x})$,
3. f *est un automorphisme linéaire tel que, pour tout* $\underline{x}, \underline{y} \in \mathbb{R}^2$, $\underline{x} \cdot \underline{y} = f\underline{x} \cdot f\underline{y}$.

Démonstration. (1⇒2) Soit une isométrie $f \in \mathsf{Iso}_O$. Par l'isomorphisme de groupes $\mathsf{Iso}_O \cong \{M \in \mathbb{R}^2 \mid M^t M = I\}$ on peut supposer que

$$f\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = M\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \text{ pour une matrice orthogonale } M,$$

3. Un automorphisme linéaire est une application linéaire bijective d'un espace à lui-même. C'est équivalent à une application linéaire inversible d'un espace à lui-même.

et f est donc un automorphisme linéaire. De plus, puisque f préserve les distances, on peut vérifier que

$$q(\underline{x}) = \underline{x} \cdot \underline{x} = \|\underline{x}\|^2 = \mathrm{dist}(\underline{x}, \underline{0})^2 = \mathrm{dist}(f\underline{x}, f\underline{0})^2 = \mathrm{dist}(f\underline{x}, \underline{0})^2 = \|f\underline{x}\|^2 = f\underline{x} \cdot f\underline{x} = q(f\underline{x}).$$

(2⇒1) Si $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ est un automorphisme linéaire tel que $q(\underline{x}) = q(f\underline{x})$ pour tout $\underline{x} \in \mathbb{R}^2$, alors f est certainement une bijection, et on peut calculer que

$$\mathrm{dist}(\underline{x}, \underline{y}) = \|\underline{x} - \underline{y}\| = \sqrt{q(\underline{x} - \underline{y})} = \sqrt{q(f(\underline{x} - \underline{y}))} = \sqrt{q(f\underline{x} - f\underline{y})} = \|f\underline{x} - f\underline{y}\| = \mathrm{dist}(f\underline{x}, f\underline{y}).$$

Ce f est donc une isométrie. (2⇔3) Suit de la correspondence donnée dans la Proposition ci-dessus (exercice). □

On peut conclure :

Théorème 2.2.4 *Le groupe orthogonal* O *est (à isomorphisme près) le groupe des automorphismes linéaires de* $\mathbb{R}^2$ *préservant la forme quadratique* $q(\underline{x}) = \|\underline{x}\|^2$*, et le groupe orthogonal spécial* SO *est (à isomorphisme près) son sous-groupe normal des éléments de déterminant égal à 1.*

2.3. Exercices

1. Compléter tous les “exercices” marqués dans le texte.

3. Espaces quadratiques

Dans les deux sections précédentes, nous avons vu quatre définitions équivalences du groupe orthogonal O du plan : c'est (à isomorphisme près)

- le quotient $\mathsf{Iso}/\mathsf{Trans}$ du groupe des isométries du plan par le sous-groupe normal des translations,
- le groupe Iso_P des isométries du plan ayant un même point fixe,
- le groupe des matrices réelles 2×2 orthogonales,
- le groupe des automorphismes de l'espace vectoriel réel $\mathbb{R}^2$ préservant la forme quadratique $q(\underline{x}) = \underline{x} \cdot \underline{x}$.

Les deux premières formulations sont plus conceptuelles—mais moins pratiques pour faire des calculs. La formulation avec les matrices est, en revanche, très concrète—mais a le désavantage qu'on a été obligé d'introduire un repère orthonormal du plan réel. La dernière formulation est indépendante de toute base, mais reste assez pratique pour faire des calculs—c'est le "juste milieu".

Dans la suite, nous allons nous intéresser à une large généralisation de cette dernière description du groupe orthogonal :

- on travaillera sur un corps F quelconque (mais, pour des raisons que l'on expliquera, de caractéristique différent de 2),
- on se donnera un espace vectoriel V sur F de dimension quelconque (mais finie),
- et on munira l'espace V d'une forme quadratique quelconque.

C'est cette dernière notion que nous devons tout d'abord préciser.

3.1. Espaces

On fixe un corps quelconque F. Pour V un espace vectoriel sur F, on note $\underline{x}, \underline{y}, \underline{z}, ... \in V$ les éléments de V. Pour l'instant, nous ne fixons aucune base dans V (et V peut être de dimension infinie).

Définition 3.1.1 *Une forme*[1] $b\colon V \times V \to F\colon (\underline{x}, \underline{y}) \mapsto b(\underline{x}, \underline{y})$ *est dite*

1. bilinéaire *si* $b(\underline{x}, -)\colon V \to V\colon y \mapsto b(\underline{x}, \underline{y})$ *et* $b(-, \underline{y})\colon V \to V\colon y \mapsto b(\underline{x}, \underline{y})$ *sont linéaires*
2. symétrique *si* $b(\underline{x}, \underline{y}) = b(\underline{y}, \underline{x})$

1. Le mot "forme" est utilisé ici dans le sens d'une application d'une puissance d'un espace vectoriel V vers le corps de base F ; donc typiquement $f\colon V^m \to F$ où $V^m = V \times ... \times V$ est le produit ("cartésien") à m facteurs.

(pour tout $\underline{x}$ et $\underline{y}$ dans V, bien sûr).

Exemple 3.1.2 On note $\mathbb{R}_{\leq n}[X]$ l'espace vectoriel réel des polynômes de degré au plus n à coefficients dans $\mathbb{R}$. Pour un polynôme $f(X) = a_nX^n + ... + a_1X + a_0$ on note $f'(X) = na_nX^{n-1} + ... + 2a_2X + a_1$ pour sa dérivée (formelle). L'application

$$b\colon \mathbb{R}_{\leq n}[X] \times \mathbb{R}_{\leq n}[X] \to \mathbb{R}\colon (f, g) \mapsto f'(1)g(0)$$

est une forme bilinéaire (non-symétrique).

Exemple 3.1.3 Soit $F^{k\times k}$ l'espace de matrices $k \times k$ à coefficients dans F ; on note typiquement $M = (m_{ij})_{i,j}$ pour les éléments d'une matrice. L'application

$$b\colon F^{k\times k} \times F^{k\times k} \to F\colon (M, N) \mapsto m_{11}n_{11} + m_{22}n_{22} + ... + m_{kk}n_{kk}$$

est une forme bilinéaire symétrique.

La source d'inspiration pour la définition ci-dessus est, lorsque $F = \mathbb{R}$ et $V = \mathbb{R}^2$, on prend pour $b(\underline{x}, \underline{y})$ le produit scalaire usuel. Comme dans la section précédente, nous voulons aussi parler de l'application "norme au carré" $q(\underline{x})$ associée. Cependant, le lien entre b et q est donné par une formule contentant la fraction $\frac{1}{2}$; on doit donc s'assurer que $2 \neq 0$ dans le corps F. Pour toute la suite du cours, on fixe donc :

Convention 3.1.4 *Tout corps sera de caractéristique différente de* 2.

Cela nous permet de poser :

Définition 3.1.5 *Une forme $q\colon V \to F\colon \underline{x} \mapsto q(\underline{x})$ est dite* quadratique *si*

1. *$q(a\underline{x}) = a^2q(\underline{x})$ pour tout $a \in F$ et $\underline{x} \in V$,*
2. *et la formule $b_q(\underline{x}, \underline{y}) = \frac{1}{2}(q(\underline{x} + \underline{y}) - q(\underline{x}) - q(\underline{y}))$ définit une forme bilinéaire.*

Exemple 3.1.6 L'application $q\colon F^{2\times 2} \to F\colon M \mapsto \det(M)$ est une forme quadratique [2].

L'observation suivante est cruciale :

Proposition 3.1.7

1. *Si $b\colon V \times V \to F$ est une forme bilinéaire (pas nécessairement symétrique), alors*
$$q_b\colon V \to F\colon \underline{x} \mapsto b(\underline{x}, \underline{x})$$
est une forme quadratique.
2. *Si $q\colon V \to F$ est une forme quadratique, alors*
$$b_q\colon V \times V \to F\colon (\underline{x}, \underline{y}) \mapsto \frac{1}{2}\Big(q(\underline{x} + \underline{y}) - q(\underline{x}) - q(\underline{y})\Big)$$
est une forme bilinéaire <u>symétrique</u>.

2. Attention : il est crucial de considérer des matrices 2×2 ; ce n'est pas vrai pour des matrices $k \times k$ si $k \neq 2$!

3. *La correspondence entre formes bilinéaires symétriques et formes quadratiques est bijective :*

$$\{\textit{formes bilinéaires symétriques sur } V\} \rightleftarrows \{\textit{formes quadratiques sur } V\}$$
$$b \longmapsto q_b$$
$$b_q \longmapsfrom q$$

Démonstration. Exercice. □

Exemple 3.1.8 Pour la forme bilinéaire symétrique

$$b\colon F^{k\times k} \times F^{k\times k} \to F\colon (M,N) \mapsto m_{11}n_{11} + m_{22}n_{22} + ... + m_{kk}n_{kk}$$

on trouve la forme quadratique $q_b\colon F^{k\times k} \to F\colon M \mapsto \sum_i m_{ii}^2$.

Exemple 3.1.9 Pour la forme quadratique $q\colon F^{2\times 2} \to F\colon M \mapsto \det(M) = m_{11}m_{22} - m_{12}m_{21}$ on trouve la forme bilinéaire symétrique

$$b_q\colon F^{2\times 2} \times F^{2\times 2} \to F\colon (M,N) \mapsto \frac{1}{2}\Big(m_{11}n_{22} + n_{11}m_{22} - m_{12}n_{21} - m_{21}n_{12}\Big).$$

Dans la suite on parlera d'un *espace quadratique* (V,q) pour un espace vectoriel V muni d'une forme quadratique $q\colon V \to F$. On peut également le penser comme un *espace bilinéaire symétrique* (V,b) via la correspondence de la Proposition précédente ; on confondra les deux notions si le contexte est sans ambiguïté.

Remarque 3.1.10 Nous ne demandons pas que le corps F soit $\mathbb{R}$, ou même un corps ordonné [3], et donc il n'a pas de sens de demander que "la forme quadratique soit positive", ou que "la forme bilinéaire soit définie positive", comme c'est le cas pour le produit scalaire usuel sur $\mathbb{R}^2$ (ou même $\mathbb{R}^n$). En effet, c'est exactement cette positivité (sur $\mathbb{R}$) qui distingue les produits scalaires parmi les formes bilinéaires symétriques. On peut donc bien faire appel à notre "intuition réelle", car $\mathbb{R}^n$ muni du produit scalaire usuel est bel et bien un *exemple* d'un espace quadratique—mais la théorie *générale* des espaces quadratiques réserve tout de même quelques surprises et subtilités !

Nous voulons maintenant définir le groupe orthogonal d'un espace quadratique quelconque. Avec un œil sur le Théorème 2.2.4, l'observation pertinente est :

Proposition 3.1.11 *Soient des espaces quadratiques (V,q) et (V',q') (avec b et b' les formes bilinéaires symétriques associées). Pour une application linéaire $f\colon V \to V'$ on a l'équivalence des conditions suivantes :*

1. $q(\underline{x}) = q'(f\underline{x})$, *(pour tout $\underline{x} \in V$),*
2. $b(\underline{x},\underline{y}) = b'(f\underline{x}, f\underline{y})$ *(pour tout $\underline{x},\underline{y} \in V$).*

On dit alors que f est une application linéaire isométrique *(pour q et q').*

3. Nous reviendrons sur la notion de 'corps ordonné' dans un chapitre ultérieur.

Démonstration. Exercice. □

Définition 3.1.12 *Une* isométrie $f\colon (V,q) \to (V',q')$ *d'espaces quadratiques est un isomorphisme isométrique.*

Remarque 3.1.13 Le sens du mot "isométrie" est quelque peu plus restreint ici par rapport à la notion du même nom dans la Définition 1.1.3 ; pour éviter toute confusion on pourrait parler ici d'*isométrie linéaire*. Mais puisque, dans la suite de ce cours, nous parlerons exclusivement d'isométries au sens de la Définition 3.1.12, nous laissons tomber cette précision.

Exemple 3.1.14 L'application linéaire $i\colon \mathbb{R}^2 \to \mathbb{R}^3\colon (x,y) \mapsto (x,y,0)$ est isométrique pour les produits scalaires usuels sur $\mathbb{R}^2$ et $\mathbb{R}^3$; par contre, l'application linéaire $p\colon \mathbb{R}^3 \to \mathbb{R}^2\colon (x,y,z) \mapsto (x,y)$ ne l'est pas.

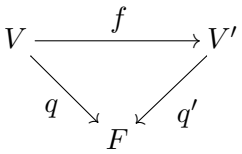
Exemple 3.1.15 L'application linéaire $f\colon \mathbb{R}^2 \to \mathbb{R}\colon (x,y) \mapsto x-y$ est isométrique pour les formes bilinéaires symétriques $b((x_1,x_2),(y_1,y_2)) = x_1y_1 - x_1y_2 - x_2y_1 + x_2y_2$ et $b'(s,t) = st$ (mais elle ne l'est pas pour les produits scalaires usuels).

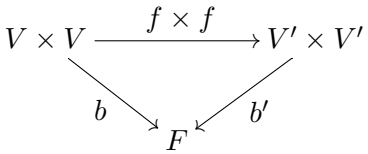
Exemple 3.1.16 L'espace vectoriel F^4 est isomorphe à $F^{2\times 2}$; explicitement on peut décrire cette isomorphisme par

$$f\colon F^4 \to F^{2\times 2}\colon (w,x,y,z) \mapsto \begin{pmatrix} w & x \\ y & z \end{pmatrix}.$$

Si on définit la forme quadratique $q(w,x,y,z) = wz - xy$ sur F^4, alors l'isomorphisme f est une isométrie de (F^4,q) à $(F^{2\times 2},\det)$.

Pour une application linéaire isométrique $f\colon (V,q) \to (V',q')$ on peut visualiser les conditions équivalentes de la Proposition ci-dessus : elles expriment la commutativité des diagrammes suivantes :





Il est alors évident que la composée de deux applications linéaires isométriques est encore une application linéaire isométrique, et que l'application "identité" $\mathsf{id}_V\colon V \to V\colon \underline{x} \mapsto \underline{x}$ est une application linéaire isométrique, quelque soit la forme quadratique que l'on met sur V. (On obtient ainsi la *categorie* Quad_K dont les *objets* sont les K-espaces quadratiques et les *morphismes* sont les applications linéaires isométriques.) Il n'est pas difficile non plus de vérifier (exercice !) que l'inverse d'une isométrie (en tant qu'isomorphisme entre espaces vectoriels) est une isométrie. (Les isométries sont donc exactement les morphismes inversibles dans la catégorie Quad_K.) Par conséquent, l'ensemble des isométries sur un espace quadratique (V,q) est un groupe :

Définition 3.1.17 *Le* groupe orthogonal *d'un espace quadratique* (V,q) *est*

$$\mathsf{O}(V,q) = \{f\colon (V,q) \to (V,q) \mid f \textit{ est une isométrie}\}.$$

Notons tout de suite une évidence : si $f\colon (V,q) \to (V',q')$ est une isométrie d'epaces quadratiques, alors $\mathsf{O}(V,q) \to \mathsf{O}(V',q')\colon g \mapsto f \circ g \circ f^{-1}$ est un isomorphisme de groupes (exercice). En mots : deux espaces quadratiques isométriques ont leurs groupes orthogonaux isomorphes.

Le *but principal* de la théorie des espaces quadratiques est de répondre aux deux questions suivantes :

- pour un corps F donné, classifier les espaces quadratiques (V,q) à isométrie près,
- pour un espace quadratique (V,q) donné, déterminer la structure du groupe $\mathsf{O}(V,q)$.

3.2. Matrices

Jusqu'à présent, notre approche aux espaces quadratiques (V,q) et leurs isométries était "canonique" : on ne faisait nullement référence à une éventuelle base de V. Si on *choisit* une base dans V, et on suppose que V est de dimension finie, alors on peut se servir du calcul matriciel. Pour la suite du cours on s'accorde donc sur :

Convention 3.2.1 *Tout espace vectoriel sera de dimension finie.*

Soit $(\underline{e}_1, ..., \underline{e}_n)$ une base d'un espace vectoriel V ; on peut donc écrire tout $\underline{x} \in V$ de façon unique comme $\underline{x} = \sum_i x_i \underline{e}_i$. Toute forme bilinéaire symétrique $b\colon V \times V \to F$ détermine une matrice symétrique

$$(b(\underline{e}_i, \underline{e}_j))_{i,j} = \begin{pmatrix} b(\underline{e}_1,\underline{e}_1) & \cdots & b(\underline{e}_1,\underline{e}_n) \\ \vdots & \ddots & \vdots \\ b(\underline{e}_n,\underline{e}_1) & \cdots & b(\underline{e}_n,\underline{e}_n) \end{pmatrix} \in F^{n\times n}.$$

Réciproquement, si $B \in F^{n\times n}$ est une matrice symétrique quelconque, alors la formule

$$b(\sum_i x_i\underline{e}_i, \sum_i y_i\underline{e}_i) = \begin{pmatrix} x_1 & ... & x_n \end{pmatrix} B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

définit une forme bilinéaire symétrique. Ainsi, pour V un espace vectoriel muni d'une base $(\underline{e}_1, ..., \underline{e}_n)$, la procédure décrite ci-dessus donne une correspondence bijective entre les formes bilinéaires symétriques $b\colon V \times V \to F$, et les matrices symétriques $B \in F^{n\times n}$. (Exercice : écrire les détails.)

Exemple 3.2.2 Soit la forme bilinéaire symétrique

$$b\colon \mathbb{R}_{\leq 3}[X] \times \mathbb{R}_{\leq 3}[X] \to \mathbb{R}\colon (f,g) \mapsto f'(1)g'(1).$$

La base "canonique" de $\mathbb{R}_{\leq 3}[X]$ est $(X^3, X^2, X, 1)$; pour cette base on peut calculer la matrice symétrique

$$B = \begin{pmatrix} 9 & 6 & 3 & 0 \\ 6 & 4 & 2 & 0 \\ 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Si l'espace V admet une autre base $(\underline{e}'_1, ..., \underline{e}'_n)$, la même forme bilinéaire (symétrique) b détermine une autre matrice (symétrique)

$$B' = (b(\underline{e}'_i, \underline{e}'_j))_{i,j}.$$

Quelle est alors la relation entre B et B' ? Voici le résultat général pertinent :

Proposition 3.2.3 *Soient deux espaces quadratiques (V, b) et (V', b'), avec des bases $(\underline{e}_1, ..., \underline{e}_n)$ et $(\underline{e}'_1, ..., \underline{e}'_m)$, et les matrices symétriques $B = (b(\underline{e}_i, \underline{e}_j))_{i,j} \in F^{n\times n}$ et $B' = (b'(\underline{e}'_i, \underline{e}'_j))_{i,j} \in F^{m\times m}$. Pour une application linéaire $f\colon V \to V'$ de matrice $C \in F^{m\times n}$ par rapport aux bases données, on a l'équivalence des assertions suivantes :*

1. *f est isométrique,*
2. *$B = C^t B' C$.*

En particulier, f est une isométrie si et seulement si C est inversible et $B = C^t B' C$; on dit alors que les matrices symétriques B et B' sont congruentes.

Démonstration. (1)⇒(2) Rappelons que la matrice $C = (c_{ij})_{i,j}$ est telle que $f(\underline{e}_i) = \sum_j c_{ij}\underline{e}'_j$. Autrement dit, pour tout $\underline{x} = \sum_i x_i \underline{e}_i$ dans V on a $f\underline{x} = \sum_i x'_i \underline{e}'_i$ dans V', où

$$\begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = C \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Puisque f est isométrique, on sait que $b(\underline{x}, \underline{y}) = b'(f\underline{x}, f\underline{y})$ pour tout $\underline{x}, \underline{y} \in V$, ce qui veut dire pour les matrices B et B' que

$$\begin{pmatrix} x_1 & ... & x_n \end{pmatrix} B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = b(\underline{x}, \underline{y}) = b'(f\underline{x}, f\underline{y}) = \begin{pmatrix} x'_1 & ... & x'_n \end{pmatrix} B' \begin{pmatrix} y'_1 \\ \vdots \\ y'_n \end{pmatrix}.$$

Mais on a également le calcul matriciel

$$\begin{pmatrix} x'_1 & ... & x'_n \end{pmatrix} B' \begin{pmatrix} y'_1 \\ \vdots \\ y'_n \end{pmatrix} = \left[C \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right]^t B' \left[C \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right] = \begin{pmatrix} x_1 & ... & x_n \end{pmatrix} C^t B' C \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Il suit ainsi que

$$\begin{pmatrix} x_1 & ... & x_n \end{pmatrix} B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 & ... & x_n \end{pmatrix} C^t B' C \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

pour tout $(x_1, ..., x_n), (y_1, ..., y_n) \in F^n$, d'où $B = C^t B' C$.
(2)⇒(1) Exercice. □

Exemple 3.2.4 Soit encore la forme bilinéaire symétrique

$$b\colon \mathbb{R}_{\leq 3}[X] \times \mathbb{R}_{\leq 3}[X] \to \mathbb{R}\colon (f,g) \mapsto f'(1)g'(1),$$

mais équipons l'espace $\mathbb{R}_{\leq 3}[X]$ de la base $(X^3+X^2+X+1, X^2+X+1, X+1, 1)$. Pour cette base aussi on peut calculer une matrice symétrique, soit :

$$B' = \begin{pmatrix} 36 & 18 & 6 & 0 \\ 18 & 9 & 3 & 0 \\ 6 & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

On peut donner explicitement la congruence $B = C^t B' C$ avec la matrice symétrique B calculée ci-dessus : la matrice C est la matrice du changement de base de $(X^3, X^2, X, 1)$ à $(X^3+X^2+X+1, X^2+X+1, X+1, 1)$:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

Ainsi, deux espaces quadratiques (V,b) et (V',b') sont isométriques si et seulement si les matrices symétriques B et B' (déterminées par des bases aux choix de V et de V') sont congruentes. Mais on peut aussi utiliser la Proposition pour donner une description matricielle du groupe orthogonal :

Théorème 3.2.5 *Soit (V,q) un espace quadratique. Si B est la matrice symétrique de (la forme bilinéaire symétrique b définie par) q pour une base $(\underline{e}_1, ..., \underline{e}_n)$ de V, alors on a un isomorphisme de groupes*

$$\mathsf{O}(V,q) \cong \{C \in F^{n\times n} \mid B = C^t B C \text{ et } C \text{ est inversible}\}.$$

Démonstration. L'isomorphisme envoit une isométrie $f\colon (V,q) \to (V,q)$ sur sa matrice par rapport à la base $(\underline{e}_1, ..., \underline{e}_n)$. □

Exemple 3.2.6 : Pour $\mathbb{R}^n$ muni du produit scalaire usuel et de la base canonique, on retrouve son groupe orthogonal comme étant le groupe des matrices orthogonales $n \times n$.

3.3. Polynômes

Il nous reste, pour terminer cette section, un dernier point de vue à expliquer : celui de l'arithmétique.

Si V est un espace vectoriel muni d'une base $(\underline{e}_1, ..., \underline{e}_n)$, alors toute forme quadratique $q\colon V \to F$ détermine un polynôme homogène de degré 2 en n variables $X_1, ..., X_n$ et à coefficients dans F :

$$f_q(X_1, ..., X_n) = \sum_{i,j} b(\underline{e}_i, \underline{e}_j) X_i X_j = \begin{pmatrix} X_1 & \dots & X_n \end{pmatrix} B \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \in F[X_1, ..., X_n].$$

(On retrouve ici la même matrice symétrique B que ci-dessus.) Réciproquement, si un polynôme $f \in F[X_1, ..., X_n]$ est homogène de degré 2, alors on a l'habitude de l'écrire comme

$$f(X_1, ..., X_n) = \sum_{i \leq j} a_{ij} X_i X_j.$$

Mais une simple manipulation des coefficients

$$b_{ij} := \frac{1}{2}(a_{ij} + a_{ji})$$

permet de l'écrire aussi comme

$$f(X_1, ..., X_n) = \sum_{i,j} b_{ij} X_i X_j.$$

Cette matrice symétrique $B = (b_{ij})_{i,j}$ définit alors la forme bilinéaire symétrique

$$b(\underline{x}, \underline{y}) = \begin{pmatrix} x_1 & ... & x_n \end{pmatrix} B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

sur l'espace V muni de la base $(\underline{e}_1, ..., \underline{e}_n)$, qui détermine à son tour l'espace quadratique (V, q) de départ. Autrement dit, si V est un espace vectoriel muni d'une base $(\underline{e}_1, ..., \underline{e}_n)$, alors la procédure décrite ci-dessus donne une correspondence bijective entre les formes quadratiques $q \colon V \times V \to F$, et les polynômes $f \in F[X_1, ..., X_n]$ homogènes de degré 2.

Exemple 3.3.1 Soit la forme quadratique $q \colon F^{2\times 2} \to F \colon M \mapsto \det(M) = m_{11}m_{22} - m_{12}m_{21}$ et mettons la base canonique sur $F^{2\times 2}$: c'est la suite de matrices

$$\left(E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, E_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, E_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right).$$

On peut alors calculer le polynôme

$$f_q(X_1, X_2, X_3, X_4) = X_1X_4 - X_2X_3.$$

Exemple 3.3.2 Soit le polynôme $3X_1X_2 + X_2^2 - X_1X_3 \in \mathbb{Q}[X_1, X_2, X_3]$. On peut le réécrire comme

$$0X_1^2 + \frac{3}{2}X_1X_2 - \frac{1}{2}X_1X_3 + \frac{3}{2}X_2X_1 + 1X_2^2 + 0X_2X_3 - \frac{1}{2}X_3X_1 + 0X_3X_2 + 0X_3^2$$

et on voit donc qu'il détermine la matrice symétrique

$$B = \begin{pmatrix} 0 & \frac{3}{2} & -\frac{1}{2} \\ \frac{3}{2} & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{pmatrix}.$$

Si on prend n'importe quel espace vectoriel V de dimension 3, muni d'une base quelconque $(\underline{e}_1, ..., \underline{e}_3)$, alors on peut "réaliser" le polynôme donné par l'espace quadratique (V, b) où

$$b(\sum_i x_i \underline{e}_i, \sum_i y_i \underline{e}_i) = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} B \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}.$$

Mais pourquoi ne pas faire simple ? On peut prendre l'espace $V = \mathbb{Q}^3$ muni de sa base canonique $((1,0,0),(0,1,0),(0,0,1))$, et le faire porter la forme bilinéaire symétrique

$$b((x_1,x_2,x_3),(y_1,y_2,y_3)) = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} B \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix},$$

qui par ailleurs correspond à la forme quadratique

$$q\colon \mathbb{Q}^3 \to \mathbb{Q}\colon (x_1,x_2,x_3) \mapsto 3x_1x_2 + x_2^2 - x_1x_3.$$

Autrement dit, le polynôme $3X_1X_2 + X_2^2 - X_1X_3 \in \mathbb{Q}[X_1,X_2,X_3]$ est réalisé, tout simplement, par la forme quadratique $q(x_1,x_2,x_3) = 3x_1x_2 + x_2^2 - x_1x_3$ sur $\mathbb{Q}^3$.

Mais si $(\underline{e}'_1,...,\underline{e}'_n)$ est une autre base de V, et on calcule un autre polynome $f'_q \in F[X_1,...,X_n]$ à l'aide de cette base, quelle est alors la relation entre f_q et f'_q ? Voici le résultat général pertinent :

Proposition 3.3.3 *Soient deux espaces quadratiques (V,q) et (V',q'), avec des bases $(\underline{e}_1,...,\underline{e}_n)$ et $(\underline{e}'_1,...,\underline{e}'_m)$, et notons les polynomes homogènes de degré 2 respectifs par $f \in F[X_1,...,X_n]$ et $f' \in F[X_1,...,X_m]$. Pour une application linéaire $g\colon V \to V'$ de matrice $C \in F^{m\times n}$ par rapport aux bases données, on a l'équivalence des assertions suivantes :*

1. *f est isométrique,*
2. *pour $Y_i = \sum_j c_{ij}X_j$ on a $f(X_1,...,X_n) = f'(Y_1,...,Y_n)$.*

En particulier, f est une isométrie si et seulement si C est inversible et pour $Y_i = \sum_j c_{ij}X_j$ on a $f(X_1,...,X_n) = f'(Y_1,...,Y_n)$; dans ce cas, on dit que f et f' sont equivalents*, noté $f \cong f'$.*

Démonstration. Ceci est une variante sur la démonstration de la Proposition 3.2.3. Pour vérifier facilement les détails, il est utile de penser les variables $X_1,...,X_n$ et $Y_1,...,Y_n$ commes des colonnes

$$X = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \quad \text{et} \quad Y = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix}$$

et de noter que le changement de variables $Y_i = \sum_j c_{ij}X_j$ n'est alors rien d'autre que le produit matriciel $Y = CX$. □

En mots, deux espaces quadratiques (V,q) et (V',q') sont isométriques si et seulement si les polynômes f et f' (déterminés par des bases aux choix de V et de V') sont "identiques à un changement linéaire et inversible de variables près".

Exemple 3.3.4 Sur tout corps F, le polynôme $f(X_1,X_2) = X_1^2 - X_2^2$ est équivalent à $g(Y_1,Y_2) = Y_1Y_2$, parce que l'on peut poser

$$\begin{cases} Y_1 = X_1 + X_2 \\ Y_2 = X_1 - X_2 \end{cases}$$

qui est effectivement un changement de variables linéaire et inversible (exercice !), et sous son effet on a $f(X_1, X_2) = g(X_1 + X_2, X_1 - X_2)$. Si on travaille sur le corps $F = \mathbb{C}$, on peut aussi montrer que $h(Z_1, Z_2) = Z_1^2 + Z_2^2$ est équivalent à f (et à g) : car maintenant le changement de variables

$$\begin{cases} Z_1 = X_1 \\ Z_2 = -iX_2 \end{cases}$$

est autorisé—mais ceci n'est clairement pas possible sur $F = \mathbb{R}$ par exemple. Autrement dit, la manipulation des polynômes à coefficients dans F depend – bien évidemment – du corps F. Ainsi, *l'étude des espaces quadratiques sur F est une façon d'étudier des propriétés du corps F.*

Pour résumer, nous avons maintenant

- l'outil géométrique : les espaces quadratiques de dimension n sur F, déterminés à isométrie près,
- l'outil algébrique : les matrices symétriques dans $F^{n\times n}$, déterminées à congruence près,
- l'outil arithmétique : les polynômes homogènes de degré 2 dans $F[X_1, ..., X_n]$, déterminés à équivalence près,

pour parler essentiellement de la même chose : la *théorie des formes quadratiques sur F*.

3.4. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Déterminer les formes quadratiques parmi les applications suivantes. Le cas échéant, donner la forme bilinéaire symétrique associée, ainsi qu'une matrice symétrique (pour une base au choix) et un polynôme honogène de degré 2 (pour une base au choix).

(a) $q\colon \mathbb{R}_{\leq n}[X] \to \mathbb{R}\colon f \mapsto f(1)^2$,

(b) $q\colon \mathbb{R}_{\leq n}[X] \to \mathbb{R}\colon f \mapsto \int_0^1 f(x)dx$,

(c) $q\colon \mathbb{C} \to \mathbb{R}\colon z \mapsto z\overline{z}$,

(d) $q\colon \mathbb{C} \to \mathbb{C}\colon z \mapsto z\overline{z}$.

3. Parmi les applications ci-dessous, déterminer les formes bilinéaires (pas nécessairement symétriques). Pour chaque forme bilinéaire, donner la forme quadratique associée, la forme bilinéaire *symétrique* associée à cette forme quadratique, une matrice symétrique de cette forme bilinéaire symétrique (pour une base au choix), et un polynôme homogène de degré 2 (pour une base au choix).

(a) $b\colon \mathbb{R}[X]_{\leq n} \times \mathbb{R}[X]_{\leq n} \to \mathbb{R}\colon (P, Q) \mapsto P(0) \cdot Q'(0)$

(b) $b\colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}\colon (z_1, z_2) \mapsto i \cdot |z_1| \cdot \overline{z_2}$

(c) $b\colon \mathbb{C} \times \mathbb{C} \to \mathbb{R}\colon (z_1, z_2) \mapsto \Re(z_1 + z_2)$

(d) $b\colon \mathbb{Q}^{3\times 3} \times \mathbb{Q}^{3\times 3} \to \mathbb{Q}\colon (A, B) \mapsto \mathrm{tr}(A^t \cdot B)$

(e) $b\colon \mathbb{R}[X]_{\leq 3} \times \mathbb{R}[X]_{\leq 3} \to \mathbb{R}\colon (P, Q) \mapsto \displaystyle\int_0^1 tP(t)Q'(t)dt$

(f) $b\colon \mathbb{R}[X]_{\leq 3} \times \mathbb{R}[X]_{\leq 3} \to \mathbb{R}\colon (P,Q) \mapsto \sum_{k=0}^{n} P(k)\cdot Q(k)$

(g) $b\colon \mathbb{R}^5 \times \mathbb{R}^5 \to \mathbb{R}\colon ((x_1,...,x_5),(y_1,...,y_5)) \mapsto x_1y_2 - (3x_3+x_2)y_5$

4. Pour les polynômes suivants, donner si possible un espace quadratique (V,q) les réalisant (ou expliquer pourquoi ce n'est pas possible) :

(a) $X_1 + 2X_2 + 3X_3^2 \in \mathbb{Q}[X_1,X_2,X_3]$

(b) $(X_1+X_2)(X_3+X_4) \in \mathbb{Q}[X_1,..,X_4]$

(c) $X_1^2 + 4X_1X_2 \in \mathbb{R}[X_1,X_2]$

(d) $X_1^2 + 4X_1X_2 \in \mathbb{C}[X_1,...,X_5]$

5. *Géométrie symplectique.* Une forme bilinéaire $b\colon V\times V \to F$ est *anti-symétrique* si $b(\underline{x},\underline{y}) = -b(\underline{y},\underline{x})$ pour tout $\underline{x},\underline{y} \in V$; l'espace (V,b) est alors un *espace symplectique*. La définition d'isométrie $f\colon (V,b)\to(V',b')$ entre espaces symplectiques est sans surprise, et on note $\mathrm{Sp}(V,b)$ le *groupe symplectique* des isométries sur (V,b).

(a) Montrer que $b\colon V\times V\to F$ est anti-symétrique si et seulement si [4] b est *alternée* : $b(\underline{x},\underline{x}) = 0$ pour tout $\underline{x}\in V$. La notion de "forme quadratique" n'a pas de sens dans ce contexte.

(b) Caractériser matriciellement les formes bilinéaires anti-symétriques.

(c) Soit une forme bilinéaire b sur V. Montrer que

$$b(\underline{x},\underline{y}) = 0 \iff b(\underline{y},\underline{x}) = 0$$

si et seulement si b est symétrique ou anti-symétrique. (On dit parfois qu'une telle forme est *réflexive*, mais cela n'a rien à voir avec la réflexivité d'une relation binaire !)
Solution. Une implication est immédiate. Pour l'autre, si on a $b(\underline{x},\underline{x}) = 0$ pour *tout* $\underline{x}\in V$ alors en développant $b(\underline{x}+\underline{y},\underline{x}+\underline{y})$ (et en utilisant l'hypothèse) on trouve que b est anti-symétrique. Si b n'est pas anti-symétrique, il existe au moins un $\underline{x}_0\in V$ tel que $b(\underline{x}_0,\underline{x}_0)\neq 0$. Pour tout $\underline{y}\in V$ on peut calculer que $b(\underline{x}_0, b(\underline{x}_0,\underline{y})\underline{x}_0 - b(\underline{x}_0,\underline{x}_0)\underline{y}) = 0$; par l'hypothèse on a aussi $b(b(\underline{x}_0,\underline{y})\underline{x}_0 - b(\underline{x}_0,\underline{x}_0)\underline{y},\underline{x}_0) = 0$, dont le développement donne déjà l'identité $b(\underline{x}_0,\underline{y}) = b(\underline{y},\underline{x}_0)$. Pour $\underline{x}\in V$ quelconque, si $b(\underline{x},\underline{x})\neq 0$ on reprend l'argument précédent (avec $\underline{x}$ à la place de $\underline{x}_0$) pour montrer que $b(\underline{x},\underline{y}) = b(\underline{y},\underline{x})$ pour tout $\underline{y}\in V$; supposons donc que $b(\underline{x},\underline{x}) = 0$. Il existe toujours un $\alpha\in F^\times$ tel que $b(\underline{x}_0+\alpha\underline{x},\underline{x}_0+\alpha\underline{x}) = b(\underline{x}_0,\underline{x}_0) + 2\alpha b(\underline{x}_0,\underline{x}) \neq 0$. Mais alors, pour tout $\underline{y}\in V$, on a par le raisonnement précédent que $b(\underline{x}_0+\alpha\underline{x},\underline{y}) = b(\underline{y},\underline{x}_0+\alpha\underline{x})$, dont le développement entraîne en effet $b(\underline{x},\underline{y}) = b(\underline{y},\underline{x})$.

6. *Géométrie hermitienne.* Soit $F=\mathbb{C}$ le corps des nombres complexes. Une application $b\colon V\times V\to\mathbb{C}$ est une *forme sesquilinéaire* si $b(\underline{x},-)$ est linéaire et $b(-,\underline{y})$ est semi-linéaire (par rapport à la conjugaison dans $\mathbb{C}$). Si $b(\underline{x},\underline{y}) = \overline{b(\underline{y},\underline{x})}$ alors on dit que (V,b) est un *espace hermitien*.

(a) Pour b une forme sesquilinéaire sur V, montrer que l'application $q\colon V\to\mathbb{C}\colon \underline{x}\mapsto q(\underline{x}) = b(\underline{x},\underline{x})$ prend ses valeurs dans $\mathbb{R}$ si et seulement si b est hermitienne. Indication : pour le sens non-trivial, calculer $b(\underline{x}+\underline{y},\underline{y}+\underline{x})$ et $b(\underline{x}+i\underline{y},i\underline{y}+\underline{x})$ pour trouver que $b(\underline{x},\underline{y})+b(\underline{y},\underline{x})$

4. Comme toujours et partout, on suppose que $\mathrm{car}F \neq 2$. Si $\mathrm{car}(F) = 2$, on n'a pas l'équivalence de 'anti-symétrie' et 'alternance' d'une forme bilinéaire b !

ainsi que $i(b(\underline{x},\underline{y}) - b(\underline{y},\underline{x}))$ sont des nombres réels ; puis conclure.
Solution. Une direction est claire. Pour l'autre, par

$$b(\underline{x}+\underline{y},\underline{y}+\underline{x}) = b(\underline{x},\underline{y}) + b(\underline{x},\underline{x}) + b(\underline{y},\underline{y}) + b(\underline{y},\underline{x})$$

on a que $b(\underline{x},\underline{y}) + b(\underline{y},\underline{x})$ est réel ; et par un calcul similaire de

$$b(\underline{x}+i\underline{y},i\underline{y}+\underline{x}) = b(\underline{x},i\underline{y})+b(\underline{x},\underline{x})+b(i\underline{y},i\underline{y})+b(i\underline{y},\underline{x}) = ib(\underline{x},\underline{y})+b(\underline{x},\underline{x})+b(\underline{y},\underline{y})-ib(\underline{y},\underline{x})$$

on voit que $i(b(\underline{x},\underline{y}) - b(\underline{y},\underline{x}))$ est réel. Ainsi le résultat suit.

(b) Montrer que $f\colon (V,b) \to (V',b')$ est une isométrie (avec la définition habituelle) si et seulement si $f \circ q' = q$ (pour q et q' les *formes hermitiennes* déterminées par b et b'). Le groupe des isométries sur un espace hermitien (V,b) est noté $\mathrm{U}(V,b)$, et appelé *groupe unitaire*.

4. Régularité et orthogonalité

Dans cette section nous allons d'abord rappeler et compléter quelques notions classiques de l'algèbre linéaire – notamment concernant le dual d'un espace vectoriel – pour ensuite en tirer du profit dans le cadre des espaces quadratiques.

4.1. Espace dual

Rappelons-nous d'abord de :

Proposition 4.1.1 *Si V et W sont des F-espaces, alors*

$$\mathrm{Lin}(V,W) = \{f\colon V \to W \mid \ f \text{ est une application linéaire}\}$$

est un F-espace pour les opérations

$$\begin{cases} (f+g)(\underline{x}) = f\underline{x} + g\underline{x} \\ (\alpha f)(\underline{x}) = \alpha(f\underline{x}) \end{cases}$$

On a $\dim(\mathrm{Lin}(V,W)) = \dim(V)\dim(W)$.

Démonstration. Tout est évident (exercice). Pour la formule de dimension, on observera que, si $(\underline{e}_1, ..., \underline{e}_n)$ est une base V, et $(\underline{d}_1, ..., \underline{d}_m)$ est une base de W, alors les mn applications linéaires $(f_{ij}\colon V \to W)_{i,j}$ définies par

$$f_{ij}(\underline{e}_k) = \begin{cases} \underline{0} \text{ si } k \neq i \\ \underline{d}_j \text{ si } k = i \end{cases}$$

forment une base de $\mathrm{Lin}(V,W)$. Alternativement, on peut utiliser l'isomorphisme de F-espaces $\mathrm{Lin}(V,W) \cong F^{m\times n}$ donné par le calcul de la matrice d'une application linéaire $f \in \mathrm{Lin}(V,W)$ par rapport aux bases $(\underline{e}_1, ..., \underline{e}_n)$ et $(\underline{d}_1, ..., \underline{d}_m)$: les applications ci-dessus correspondent alors avec la base canonique de $F^{m\times n}$ (les mn matrices qui sont nulles partout sauf un élément qui vaut 1). □

En particulier, nous avons :

Définition 4.1.2 *L'*espace dual *d'un F-espace V est le F-espace $V^* = \mathrm{Lin}(V,F)$; les éléments de V^* sont donc les* formes linéaires *sur V.*

Par conséquent, V et V^* sont de même dimension, et donc isomorphe. Si $(\underline{e}_1, ..., \underline{e}_n)$ est une base de V, la *base duale* de V^* est donnée par les n applications linéaires notées $e_i^*\colon V \to F$ définies par

$$e_i^*(\underline{e}_j) = \begin{cases} 0 \text{ si } i \neq j \\ 1 \text{ si } i = j \end{cases}$$

(C'est exactement la formule donnée dans la démonstration ci-dessus, pour la base (1) de F en tant que F-espace.) Pour $\underline{x} \in V$, une telle application linéaire calcule donc

$$e_i^*(\underline{x}) = e_i^*(\sum_j x_j \underline{e}_j) = \sum_j x_j e_i^*(\underline{e}_j) = x_i = \text{ } i\text{-ième coordonnée de } \underline{x} \text{ dans la base } (\underline{e}_1, ..., \underline{e}_n).$$

Autrement dit, le n-uple des coordonnées de $\underline{x} \in V$ pour la base $(\underline{e}_1, ..., \underline{e}_n)$ est $(\underline{e}_i^*(\underline{x}), ..., \underline{e}_n^*(\underline{x}))$.

De l'autre côté, pour $f \in V^*$ et $\underline{x} \in V$ on peut calculer que

$$f(\underline{x}) = f(\sum_i x_i \underline{e}_i) = \sum_i x_i f(\underline{e}_i) = \sum_i f(\underline{e}_i) e_i^*(\underline{x}).$$

Ce $f \in V^*$ s'écrit donc (de manière unique) comme $f = \sum_i f(\underline{e}_i) e_i^*$; ainsi les coordonnés de $f \in V^*$ par rapport à la base duale $(\underline{e}_1^*, ..., \underline{e}_n^*)$ de V^* forment le n-uple $(f(\underline{e}_1), ..., f(\underline{e}_n))$.

Exemple 4.1.3 Si $f\colon V \to W$ est une application linéaire, et on a des bases $(\underline{e}_1, ..., \underline{e}_n)$ et $(\underline{d}_1, ..., \underline{d}_m)$ de V et W respectivement, alors la matrice de f par rapport à ces bases est $C = (\underline{d}_i^*(f(\underline{e}_j)))_{i,j}$. En effet, dans la j-ième colonne de C on trouve ainsi les coordonnées dans la base $(\underline{d}_1, ..., \underline{d}_m)$ de l'image par f du j-ième élément de la base $(\underline{e}_1, ..., \underline{e}_n)$.

Exemple 4.1.4 Une matrice $C \in F^{n \times n}$ est inversible si et seulement si ses colonnes forment une base de l'espace F^n (que nous allons identifier avec $F^{n \times 1}$, les colonnes à n éléments) ; notons cette base par $(\underline{c}_1, ..., \underline{c}_n)$. Les coordonnées d'un $\underline{x} \in F^n$ sont ces éléments $x_1, ..., x_n \in F$ pour lesquels on a $\underline{x} = \sum_i x_i \underline{c}_i$, et cela s'écrit matriciellement comme

$$\underline{x} = C \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \text{ ou de manière équivalente } \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = C^{-1} \underline{x}.$$

Si maintenant on note L_i pour la i-ième ligne de C^{-1}, alors les éléments de la base duale $(\underline{c}_1^*, ..., \underline{c}_n^*)$ sont les formes linéaires $\underline{c}_i^*\colon F^n \to F\colon \underline{x} \mapsto L_i \underline{x}$.

Par analogie avec $\mathrm{Lin}(V, W)$ on a aussi :

Proposition 4.1.5 *Si V, W et Z sont des F-espaces, alors*

$$\mathrm{Bilin}(V, W; Z) = \{f\colon V \times W \to Z \mid \text{ } f \text{ est une application bilinéaire}\}^{\,1}$$

est un F-espace pour les opérations

$$\begin{cases} (f+g)(\underline{x}, \underline{y}) = f(\underline{x}, \underline{y}) + g(\underline{x}, \underline{y}) \\ (\alpha f)(\underline{x}, \underline{y}) = \alpha(f(\underline{x}, \underline{y})) \end{cases}.$$

1. Ceci veut bien sûr dire que tous les $f(\underline{x}, -)\colon V \to Z$ et $f(-, \underline{y})\colon W \to Z$ sont linéaires.

On a un isomorphisme $\mathrm{Bilin}(V,W;Z)\cong\mathrm{Lin}(V,\mathrm{Lin}(W,Z))$ *de* F*-espaces donné par*

$$\mathrm{Bilin}(V,W;Z)\to\mathrm{Lin}(V,\mathrm{Lin}(W,Z))\colon f\mapsto\Big(\hat f\colon V\to\mathrm{Lin}(W,Z)\colon \underline{x}\mapsto f(\underline{x},-)\Big)$$

avec inverse

$$\mathrm{Lin}(V,\mathrm{Lin}(W,Z))\to\mathrm{Bilin}(V,W;Z)\colon g\mapsto\Big(\check g\colon V\times W\to Z\colon(\underline{x},\underline{y})\mapsto g(\underline{x})(\underline{y})\Big).$$

Démonstration. Exercice. □

Par conséquent – et c'est l'intérêt pour les espaces quadratiques ! – on obtient l'isomorphisme

$$\mathrm{Bilin}(V,V;F)\cong\mathrm{Lin}(V,\mathrm{Lin}(V,F))=\mathrm{Lin}(V,V^*).$$

Autrement dit, toute forme bilinéaire (pas nécessairement symétrique) $b\colon V\times V\to F$ détermine, et est déterminée par, une application linéaire $\hat b\colon V\to V^*$; explicitement, $\hat b(\underline{x})\in V^*$ est la forme linéaire $b(\underline{x},-)\colon V\to F\colon\underline{y}\mapsto b(\underline{x},\underline{y})$. Nous disposons donc de tous les outils de l'algèbre linéaire pour étudier les formes bilinéaires sur V—au détail près qu'on devra s'habituer à travailler avec l'espace dual V^*. Par exemple :

Proposition 4.1.6 *Soit une forme bilinéaire* $b\in\mathrm{Bilin}(V,V;F)$*. Si* $(\underline{e}_1,...,\underline{e}_n)$ *est une base de* V*, et* $(\underline{e}_1^*,...,\underline{e}_n^*)$ *la base duale de l'espace dual* V^**, alors la matrice de l'application linéaire* $\hat b\colon V\to V^*$ *par rapport à ces deux bases est* $B=(b(\underline{e}_i,\underline{e}_j))_{i,j}$*.*

Démonstration. Soit $M=(m_{ij})_{i,j}$ la matrice de $\hat b\colon V\to V^*$ par rapport aux bases $(\underline{e}_1,...,\underline{e}_n)$ et $(\underline{e}_1^*,...,\underline{e}_n^*)$. L'élément m_{ij} est donc la j-ième coordonnée par rapport à la base $(\underline{e}_1^*,...,\underline{e}_n^*)$ de l'image par $\hat b$ du i-ième vecteur de la base $(\underline{e}_1,...,\underline{e}_n)$, soit $m_{ij}=\hat b(\underline{e}_i)(\underline{e}_j)=b(\underline{e}_i,\underline{e}_j)$. □

Nous retrouvons donc la même matrice B (symétrique, si la forme b l'est) que nous avions calculée dans la section précédente pour un espace quadratique (V,b) muni d'une base $(\underline{e}_1,...,\underline{e}_n)$.

Pour étendre la notion d'espace dual aux applications linéaires, observons d'abord :

Proposition 4.1.7 *Si* $f\colon V\to W$ *est une application linéaire entre* F*-espaces, alors pour tout* F*-espace* Z *aussi*

$$\mathrm{Lin}(W,Z)\to\mathrm{Lin}(V,Z)\colon g\mapsto g\circ f$$

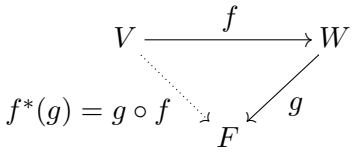
est une application linéaire.

Démonstration. Exercice. □

Par conséquent, toute application linéaire $f\colon V\to W$ détermine une *application linéaire duale* $f^*\colon W^*\to V^*$; explicitement on a

$$f^*\colon\mathrm{Lin}(W,F)\to\mathrm{Lin}(V,F)\colon g\mapsto f\circ g.$$

Le diagramme suivant montre bien ce qui se passe :



Il est alors évident d'observer que, si on note $\mathsf{id}_V : V \to V : \underline{x} \mapsto \underline{x}$ l'application "identité" sur un F-espace, alors $(\mathsf{id}_V)^* = \mathsf{id}_{V^*}$ (en mots : "l'application duale de l'identité sur V est l'application identité sur l'espace dual de V") ; et si on a deux applications linéaires $f : V \to W$ et $g : W \to Z$, alors $(g \circ f)^* = f^* \circ g^*$ (en mots : "l'application duale d'une composée est la composée renversée des applications duales").

Exemple 4.1.8 Soit $f : V \to W$ une application linéaire quelconque, et $(\underline{e}_1, ..., \underline{e}_n)$ et $(\underline{d}_1, ..., \underline{d}_m)$ des bases de V et de W. L'élément en position (i, j) de la matrice de f par rapport à ces bases est $\underline{d}_i^*(f(\underline{e}_j))$, la i-ième coordonnée de $f(\underline{e}_j)$ par rapport à la base $(\underline{d}_1, ..., \underline{d}_m)$. Pour l'application duale $f^* : W^* \to V^*$ on peut faire pareil : l'élément en position (i, j) de sa matrice par rapport aux bases duales $(\underline{d}_1^*, ..., \underline{d}_m^*)$ et $(\underline{e}_1^*, ..., \underline{e}_n^*)$ est la i-ième coordonnée de $f^*(\underline{d}_j^*)$ par rapport à la base $(\underline{e}_1^*, ..., \underline{e}_m^*)$. Mais si on évalue $f^*(\underline{d}_j^*) = \sum_i a_i \underline{e}_i^* \in V^*$ en $\underline{e}_i \in V$ on trouve d'un côté

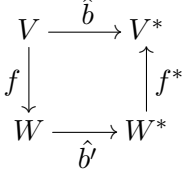
$$f^*(\underline{d}_j^*)(\underline{e}_i) = (\underline{d}_j^* \circ f)(\underline{e}_i) = \underline{d}_j^*(f(\underline{e}_i))$$

et de l'autre côté

$$(\sum_i a_i \underline{e}_i^*)(\underline{e}_j) = \sum_i a_i \underline{e}_i^*(\underline{e}_j) = a_j.$$

C'est à dire, la i-ième coordonnée de $f^*(\underline{d}_j)$ par rapport à la base $(\underline{e}_1^*, ..., \underline{e}_m^*)$ est $a_i = \underline{d}_j^*(f(\underline{e}_i))$. Conclusion : la matrice de f par rapport aux bases $(\underline{e}_1, ..., \underline{e}_n)$ et $(\underline{d}_1, ..., \underline{d}_m)$ est la *transposée* de la matrice de l'application duale f^* par rapport aux bases duales $(\underline{d}_1^*, ..., \underline{d}_m^*)$ et $(\underline{e}_1^*, ..., \underline{e}_n^*)$.

Exemple 4.1.9 Soit une application linéaire $f : V \to W$ entre deux espaces quadratiques (V, b) et (W, b'). "Par dualisation" on peut considérer les applications linéaires suivantes :



On a alors que f est isométrique si et seulement si le diagramme ci-dessus commute. En effet, pour des bases $(\underline{e}_1, ..., \underline{e}_n)$ de V et $(\underline{d}_1, ..., \underline{d}_m)$ de W, et les bases duales de V^* et W^*, on peut calculer les matrices de ces quatre applications linéaires ; soient ainsi les matrices B pour $\hat{b}$, B' pour $\hat{b'}$, C pour f et (donc) C^t pour f^*. Par Proposition 3.2.3, le résultat suit. En particulier, f est une isométrie si et seulement si f est un isomorphisme (d'espaces vectoriels) faisant commuter le diagramme ci-dessus.

4.2. Espace quadratique régulier

Revenons aux espaces quadratiques (V, b) ; on supposera donc que b est une forme bilinéaire *symétrique* sur V, mais on se permet de le traiter par l'application linéaire $\hat{b}\colon V \to V^*$.

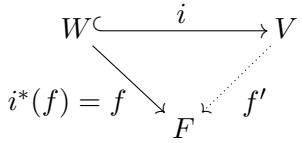
Si $W \subseteq V$ est un sous-espace vectoriel d'un F-espace V, alors l'inclusion $i\colon W \hookrightarrow V\colon \underline{x} \mapsto \underline{x}$ est une application linéaire (évidemment injective). L'application duale est

$$i^*\colon V^* \to W^*\colon f \mapsto f \circ i,$$

c'est à dire, $i^*(f) = f \circ i = f_{|W}$ est tout simplement la restriction de $f\colon V \to F$ au sous-espace W. Notons déjà pour plus tard que i^* est, en fait, surjective : D'abord, si on prend une base $(\underline{e}_1, ..., \underline{e}_k)$ de W, alors on peut l'étendre en une base $(\underline{e}_1, ..., \underline{e}_k, \underline{e}_{k+1}, ..., \underline{e}_n)$ de tout V. Maintenant, pour tout $f \in W^*$ on peut définir $f' \in V^*$ en posant (par exemple)

$$f'(\underline{e}_i) = \begin{cases} f(\underline{e}_i) \text{ si } i \leq k \\ \underline{0} \text{ sinon} \end{cases}$$

Ainsi on aura défini une application linéaire $f'\colon V \to F$ telle que $i^*(f') = f$:



Cet observation permet de définir élégamment :

Définition 4.2.1 *Soit* (V, b) *un espace quadratique. L'*orthocomplément *d'un sous-espace* $W \subseteq V$ *est*

$$W^\perp = \ker(\, V \xrightarrow{\hat{b}} V^* \xrightarrow{i^*} W^* \,).$$

Le radical *de* (V, b) *est* $\mathrm{rad}(V, b) = V^\perp$*, et* (V, b) *est un* espace régulier *(aussi appelé* espace non-dégénéré*) si* $\mathrm{rad}(V, b) = \{\underline{0}\}$ *("le radical est nul").*

Par sa définition comme le noyau d'une application linéaire, $W^\perp$ est un sous-espace de V. Explicitement, on peut calculer que

$$\begin{aligned} W^\perp &= \{\underline{x} \in V \mid i^*(\hat{b}(\underline{x})) = \underline{0}\} \\ &= \{\underline{x} \in V \mid \hat{b}(\underline{x}) \circ i = \underline{0}\} \\ &= \{\underline{x} \in V \mid b(\underline{x}, i-) = \underline{0}\} \\ &= \{\underline{x} \in V \mid \forall \underline{y} \in W : b(\underline{x}, \underline{y}) = 0\}. \end{aligned}$$

En effet, par l'application linéaire $\hat{b}\colon V \to V^*\colon \underline{x} \mapsto b(\underline{x}, -)$ on a, pour tout $\underline{x} \in V$, l'application linéaire $\hat{b}(\underline{x})\colon V \to F\colon \underline{y} \mapsto b(\underline{x}, \underline{y})$, que l'on précompose avec $i\colon W \hookrightarrow V$ pour obtenir $(i^* \circ \hat{b})(\underline{x})$.

Naturellement, on dira que $\underline{x}$ est *orthogonal* à $\underline{y}$ dans (V, b), noté $\underline{x} \perp \underline{y}$, si $\underline{x} \in \underline{y}^\perp$; ici, par $\underline{y}^\perp$ on veut dire l'orthocomplément du sous-espace de V engendré par $\underline{y} \in V$. On a que

$$\underline{x} \perp \underline{y} \iff b(\underline{x}, \underline{y}) = 0 \iff \underline{y} \perp \underline{x};$$

la relation d'orthogonalité est donc symétrique. En particulier, l'espace quadratique (V, b) est régulier si et seulement si, pour tout $\underline{x} \in V$:

$$\Big(\forall \underline{y} \in V : \underline{x} \perp \underline{y}\Big) \Longrightarrow \Big(\underline{x} = \underline{0}\Big).$$

Exemple 4.2.2 Pour le produit scalaire usuel sur $\mathbb{R}^2$, la notion d'orthogonalité est la notion usuelle : $(x, y) \perp (x', y')$ si et seulement si $xx' + yy' = 0$. L'espace quadratique $(\mathbb{R}^2, q(\underline{x}) = \|\underline{x}\|^2)$ ainsi obtenu est régulier : seul $(0, 0)$ est orthogonal à tous les (x, y). Par contre, si on met la forme bilinéaire symétrique $b((x, y), (x', y')) = xx'$ sur $\mathbb{R}^2$, alors on a l'"orthogonalité" de $(0, 1)$ à lui-même—l'espace quadratique $(\mathbb{R}^2, b)$ n'est donc pas régulier. En fait, on peut calculer facilement que $\mathrm{rad}(\mathbb{R}^2, b) = \{(x, y) \mid \forall (u, v) : b((x, y)(u, v)) = 0\}$ est le sous-espace engendré par $(0, 1)$.

Exemple 4.2.3 Soit l'espace $\mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3$ muni de la forme quadratique $q(x, y, z) = 2xy + z^2$; la forme bilinéaire symétrique associée est $b((x, y, z), (u, v, w)) = xv + yu + zw$. Soit par exemple le sous-espace $W = \{(x, y, z) \mid x + y = 0\} = \{(x, -x, z)\} = \{(x, 2x, z)\}$; son orthocomplément est

$$\begin{aligned} W^\perp &= \{(u, v, w) \mid \forall (x, 2x, z) : b((u, v, w,), (x, 2x, z)) = 0\} \\ &= \{(u, v, w) \mid \forall x, z : xv + 2xu + zw = 0\} \\ &= \{(u, v, w) \mid \forall x, z : x(v + 2u) + zw = 0\} \\ &= \{(u, u, 0)\} \end{aligned}$$

Il est, par ailleurs, facile de voir que cet espace n'est pas régulier.

Exemple 4.2.4 Toute application linéaire isométrique $f : (V, b) \to (V', b')$ partant d'un espace régulier est injective. En effet : si $f\underline{x} = \underline{0}$ alors, pour tout $\underline{y} \in V$ on a nécessairement $b(\underline{x}, \underline{y}) = b'(f\underline{x}, f\underline{y}) = b'(\underline{0}, f\underline{y}) = 0$ – c'est à dire que $\ker(f) \subseteq \mathrm{rad}(V, b)$ – et donc $\ker(f) = \{\underline{0}\}$ si (V, b) est régulier. (On vérifie facilement que l'application d'Exemple 3.1.15 est définie sur un espace non-régulier !)

Voici d'autres caractérisations de la régularité d'un espace quadratique :

Proposition 4.2.5 *Pour un espace quadratique (V, b) on a l'équivalence des assertions suivantes :*

1. *(V, b) est régulier,*
2. *$\hat{b} : V \to V^*$ est un isomorphisme,*
3. *pour toute base $(\underline{e}_1, ..., \underline{e}_n)$ de V, la matrice symétrique $B = (b(\underline{e}_i, \underline{e}_j))_{i,j}$ est inversible.*

Démonstration. (1) $\Longleftrightarrow$ (2) L'espace (V, b) est régulier si et seulement si son radical est nul. Mais le radical $V^\perp$ est le noyau de $\hat{b}$, donc le radical est nul si et seulement si $\hat{b}$ est injectif. Puisque $\dim(V) = \dim(V^*)$, $\hat{b}$ est injectif si et seulement si c'est un isomorphisme.
(2) $\Longleftrightarrow$ (3) L'application linéaire $\hat{b}$ est un isomorphisme si et seulement si sa matrice par rapport

à la base $(\underline{e}_1, ..., \underline{e}_n)$ de V et la base duale $(\underline{e}_1^*, ..., \underline{e}_n^*)$ de V^* est inversible ; et c'est exactement la matrice $B = (b(\underline{e}_i, \underline{e}_j))_{i,j}$ (par une Proposition ci-dessus). □

Exemple 4.2.6 L'*espace de Minkowski* est $\mathbb{R}^4$, dont on pense les éléments (x, y, z, t) comme des points dans l'espace-temps, muni de la forme quadratique $q(x, y, z, t) = x^2 + y^2 + z^2 - t^2$. Cet espace est crucial pour la théorie de la relativité restreinte de Einstein ; il est régulier, comme on voit facilement par considération d'une matrice symétrique associée (exercice).

La Proposition ci-dessus implique immédiatement :

Corollaire 4.2.7 *Si (V, b) et (V', b') sont des espaces isométriques, alors l'un est régulier si et seulement si l'autre l'est.*

En effet, pour chaque espace on peut calculer une matrice symétrique (par rapport à une base au choix), soient B et B' respectivement. Les espaces sont isométriques si et seulement si ces matrices sont congruentes : $B = C^t B' C$ pour C inversible. Il suit que B est inversible si et seulement si B' est inversible—autrement dit, (V, b) est régulier si et seulement si (V', b') l'est.

Pour les espaces quadratiques réguliers, on a un comportement particulièrement agréable des orthocompléments des sous-espaces :

Proposition 4.2.8 *Si (V, b) est un espace quadratique régulier, et $S \subseteq V$ est un sous-espace quelconque, alors*

(a) $\dim(S) + \dim(S^\perp) = \dim(V)$,

(b) $(S^\perp)^\perp = S$.

Démonstration. (a) Considérons l'application linéaire $\hat{b}\colon V \to V^*$, et l'application linéaire duale $i^*\colon V^* \to S^*$ de l'inclusion naturelle $i\colon S \hookrightarrow V$. On a par définition que $S^\perp = \ker(i^* \circ \hat{b})$ et donc, comme pour toute application linéaire,

$$\dim(V) = \dim(\ker(i^* \circ \hat{b})) + \dim(\mathrm{im}(i^* \circ \hat{b})) = \dim(S^\perp) + \dim(\mathrm{im}(i^* \circ \hat{b})).$$

Mais (V, b) est régulier par hypothèse, donc $\hat{b}$ est un isomorphisme ; et i^* est surjectif puisque i est injectif ; et donc $\mathrm{im}(i^* \circ \hat{b}) = S^*$. On peut conclure par $\dim(\mathrm{im}(i^* \circ \hat{b})) = \dim(S^*) = \dim(S)$. (b) Pour tout $\underline{x} \in S$ on a par définition de $S^\perp$ que

$$\forall \underline{y} \in S^\perp : \underline{x} \perp \underline{y}.$$

Ainsi on a toujours $S \subseteq (S^\perp)^\perp$. Sous l'hypothèse de régularité de (V, b), on utilise la partie (a) pour affirmer que

$$\dim(S^\perp) + \dim((S^\perp)^\perp) = \dim(V) = \dim(S) + \dim(S^\perp).$$

(On applique donc la partie (a) au sous-espace $S^\perp \subseteq V$ pour la première équation.) Il suit que $\dim(S) = \dim((S^\perp)^\perp)$, et l'inclusion $S \subseteq (S^\perp)^\perp$ est donc nécessairement une égalité. □

Exemple 4.2.9 On a déjà vu que, pour la forme bilinéaire symétrique $b((x, y), (x', y')) = xx'$, l'espace quadratique $(\mathbb{R}^2, b)$ n'est pas régulier. Pour $S = \{(0, a) \mid a \in \mathbb{R}\}$ on peut calculer que $S^\perp\{(x, y) \mid \forall (0, a) : b((0, a), (x, y)) = 0\} = \mathbb{R}^2$; on n'a donc pas $\dim(S) + \dim(S^\perp) = \dim(\mathbb{R}^2)$.

4.3. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Soit l'application $\phi\colon \mathrm{Bilin}(V,V;F) \to \mathrm{Bilin}(V,V;F)$ telle que $\phi(b)(\underline{x},\underline{y}) = b(\underline{y},\underline{x})$. Montrer qu'il s'agit d'un automorphisme et calculer ses valeurs et vecteurs propres.

3. Pour deux espaces vectoriels V et W, montrer que le produit ("cartésien") $V \times W$ est un espace vectoriel pour les opérations

$$\begin{cases} (\underline{x},\underline{y}) + (\underline{x}',\underline{y}') = (\underline{x}+\underline{x}', \underline{y}+\underline{y}') \\ \alpha(\underline{x},\underline{y}) = (\alpha\underline{x}, \alpha\underline{y}) \end{cases}$$

Calculer $\mathrm{Lin}(V \times W, F) \cap \mathrm{Bilin}(V,W;F)$.

4. Montrer que, si une application linéaire $f\colon V \to W$ est injective, alors l'application duale $f^*\colon W^* \to V^*$ est surjective. Indication : Soit une base $(\underline{e}_1, ..., \underline{e}_n)$ de V. Par injectivité de f on a une suite libre $f\underline{e}_1, ..., f\underline{e}_n$ dans W, que l'on peut compléter en une base. Pour une application linéaire $g\colon V \to F$ on peut définir une application $h\colon W \to F$ par son effet sur les éléments de cette base de W ; un choix judicieux permettra d'affirmer que $h \circ f = g$.

5. Montrer que $\varphi_V\colon V \to (V^*)^*\colon \underline{x} \mapsto (\mathrm{ev}_{\underline{x}}\colon f \mapsto f\underline{x})$ est un isomorphisme (pour un espace V de dimension finie). Indication : montrer que φ_V est injective, et conclure par l'égalité des dimensions de source et but.

6. Montrer que "dualiser" définit un foncteur contravariant $(-)^*\colon \mathsf{Vec}_F \to \mathsf{Vec}_F$ sur la catégorie des F-espaces et applications linéaires et que la famille $(\varphi_V\colon V \to V^{**})_{V \in \mathsf{Vec}_F}$ des isomorphismes de l'exercice précédent constitue une transformation naturelle

$$\mathsf{Vec}_F \underset{(-)^* \circ (-)^*}{\overset{\mathsf{id}_{\mathsf{Vec}_F}}{\Downarrow \varphi}} \mathsf{Vec}_F \ .$$

7. Dans les exercices de la section précédente, repérer les espaces quadratiques réguliers.

8. Réaliser le polynôme $X_1^2 + 2X_3X_4 \in \mathbb{R}[X_1, ..., X_4]$ par un espace quadratique (V,q) et montrer que cet espace n'est pas régulier. Trouver un sous-espace $S \subseteq V$ tel que $\dim(S) + \dim(S^\perp) \neq \dim(V)$. Trouver un sous-espace $S \subseteq V$ tel que $(S^\perp)^\perp \neq S$.

9. Soit un espace quadratique (V,b) et $(\mathrm{Sub}(V), \subseteq)$ l'ensemble ordonné de ses sous-espaces vectoriels. Montrer que $(-)^\perp\colon \mathrm{Sub}(V) \to \mathrm{Sub}(V)\colon S \to S^\perp$ est une application antitone et que $(-)^{\perp\perp}\colon \mathrm{Sub}(V) \to \mathrm{Sub}(V)\colon S \mapsto S^{\perp\perp}$ est une application monotone, croissante et idempotente sur $\mathrm{Sub}(V)$. Calculer $\{\underline{0}\}^{\perp\perp}$ et $V^{\perp\perp}$. Montrer que (V,b) est un espace régulier si et seulement si $S \mapsto S^{\perp\perp}$ est l'identité.

5. Somme orthogonale

Nous rappelons et complétons d'abord quelques notions de l'algèbre linéaire, cette fois-ci concernant la somme d'espaces vectoriels, pour ensuite les appliquer aux espaces quadratiques.

5.1. Somme interne

Si $W_1, W_2 \subseteq V$ sont des sous-espaces d'un F-espace V, alors

- l'intersection $W_1 \cap W_2 \subseteq V$ est le plus grand sous-espace contenu dans W_1 et W_2,
- la somme $W_1 + W_2 = \{\underline{x}_1 + \underline{x}_2 \mid \underline{x}_i \in W_i\} \subseteq V$ est le plus petit sous-espace contenant W_1 et W_2,
- si $W_1 \cap W_2 = \{\underline{0}\}$, alors on dit que $W_1 + W_2$ est une *somme directe*, et on la note $W_1 \oplus W_2$.

Dans une somme directe, on peut écrire tout élément $\underline{x} \in W_1 \oplus W_2$ *en exactement une manière* comme une somme $\underline{x} = \underline{x}_1 + \underline{x}_2$. Il suit que, si $(\underline{e}_1, ..., \underline{e}_k)$ est une base de W_1 et $(\underline{d}_1, ..., \underline{d}_l)$ est une base de W_2, alors $(\underline{e}_1, ..., \underline{e}_k, \underline{d}_1, ..., \underline{d}_l)$ est une base de $W_1 \oplus W_2$. Ainsi il suit évidemment que $\dim(W_1 \oplus W_2) = \dim(W_1) + \dim(W_2)$. (Exercice : démontrer ces assertions !)

Si maintenant (V, b) est un espace quadratique, il est possible que les éléments de W_1 et de W_2 soient mutuellement orthogonaux dans V ; on introduit :

Définition 5.1.1 *Soit un espace quadratique (V, b) et deux sous-espaces $W_1, W_2 \subseteq V$. Si*

$$W_1 \cap W_2 = \{\underline{0}\} \text{ et pour tout } \underline{x} \in W_1 \text{ et } \underline{y} \in W_2 : b(\underline{x}, \underline{y}) = 0$$

alors on dit que la somme directe $W_1 \oplus W_2$ est une somme orthogonale *; on le note $W_1 \perp W_2$.*

Exemple 5.1.2 Soit le polynôme $X_1^2 + 2X_2^2 + X_2X_3 \in \mathbb{F}_5[X_1, X_2, X_3]$. On peut le réaliser par l'espace $\mathbb{F}_5^3$ muni de la forme $b((x, y, z), (u, v, w)) = xu + 2yv + 3zv + 3yw$. Les sous-espaces $\{(x, 0, 0) \mid x \in \mathbb{F}_5\}$ et $\{(0, y, 0) \mid y \in \mathbb{F}_5\}$ sont orthogonaux ; $\{(0, y, 0) \mid y \in \mathbb{F}_5\}$ et $\{(0, 0, z) \mid z \in \mathbb{F}_5\}$ ne le sont pas.

Voici un exemple typique de cette situation. Si $W \subseteq V$ est un sous-espace vectoriel d'un espace quadratique (V, b), il est évident que la restriction de la forme bilinéaire symétrique $b\colon V \times V \to F$ à $W \times W \subseteq V \times V$ est aussi une forme bilinéaire symétrique ; on dit que (W, b) est un *sous-espace quadratique* de (V, b). (Autrement dit, la forme quadratique $q\colon V \to F$ est restreinte à $q_{|W}\colon W \to F$. Ou encore, l'inclusion $W \hookrightarrow V$ est une application linéaire isométrique.) En tant que "espace quadratique de son propre droit", (W, b) peut être régulier, même si (V, b) ne l'est pas ; et, par ailleurs, même si (V, b) est régulier, il est possible que (W, b)

ne le soit pas (cf. les exercices). D'où l'importance de l'énoncé suivant (qui ressemble à, mais est différent de, la Proposition 4.2.8) :

Proposition 5.1.3 *Soit un espace quadratique (V, b). Si $W \subseteq V$ détermine un sous-espace quadratique régulier, alors on a $V = W \perp W^\perp$.*

Démonstration. Pour être parfaitement clair, on note $i\colon W \hookrightarrow V$ l'inclusion de W dans V, et donc

$$W^\perp = \ker(\ V \xrightarrow{\hat{b}} V^* \xrightarrow{i^*} W^*\ )$$

On calcule que

$$\begin{aligned} W \cap W^\perp &= \{\underline{x} \in W \mid \forall \underline{y} \in W : b(\underline{x}, \underline{y}) = 0\} \\ &= \mathrm{rad}(W, b) \\ &= \{\underline{0}\} \end{aligned}$$

puisque, par hypothèse, (W, b) est un espace quadratique *régulier*. Ainsi on sait déjà que $W + W^\perp = W \oplus W^\perp$; pour avoir l'égalité $W \oplus W^\perp = V$ il suffit de montrer que $\dim(W \oplus W^\perp) = \dim(V)$. Or, on peut considérer les applications linéaires

$$\begin{array}{ccccc} V & \xrightarrow{\hat{b}} & V^* & \xrightarrow{i^*} & W^* \\ {\scriptstyle i}\uparrow & & & \nearrow_{i^* \circ \hat{b} \circ i} & \\ W & & & & \end{array}$$

La composée $i^* \circ \hat{b} \circ i\colon W \to W^*$ est exactement l'application linéaire déterminée par la restriction de la forme bilinéaire $b\colon W \times W \to F$ (exercice : donner les détails). Ainsi, $i^* \circ \hat{b} \circ i\colon W \to W^*$ est un isomorphisme (car (W, b) est régulier par hypothèse), et donc $i^* \circ \hat{b}$ est surjective [1] (même si $\hat{b}$ n'est pas un isomorphisme, i.e. même si (V, b) n'est pas régulier !). On peut alors calculer que

$$\begin{aligned} \dim(V) &= \dim(\ker(i^* \circ \hat{b})) + \dim(\mathrm{im}(i^* \circ \hat{b})) \\ &= \dim(W^\perp) + \dim(W^*) \\ &= \dim(W^\perp) + \dim(W) \\ &= \dim(W \oplus W^\perp) \end{aligned}$$

Pour conclure, on note qu'évidemment tout élément de W est orthogonal à tout élément de $W^\perp$; la somme directe est donc une somme orthogonale, et $V = W \perp W^\perp$. □

Exemple 5.1.4 Soit la matrice symétrique non-inversible

$$B = \begin{pmatrix} 6 & 1 & 0 \\ 1 & 0 & 6 \\ 0 & 6 & 1 \end{pmatrix} \in \mathbb{F}_7^{3\times 3}$$

1. Si une composée $g \circ f$ de deux fonctions est bijective, alors f est injective et g est surjective ; exercice.

L'espace quadratique $(\mathbb{F}_7^3, b)$ réalisé par

$$b((x,y,z),(u,v,w)) = \begin{pmatrix} x & y & z \end{pmatrix} B \begin{pmatrix} u \\ v \\ w \end{pmatrix} = 6xu + xv + yu + 6yw + 6zv + zw$$

est donc non-régulier. Le sous-plan d'équation cartésienne $z = 0$ est, par contre, régulier : la restriction de la forme b à ce sous-plan est

$$b((x,y,0),(u,v,0)) = 6xu + xv + yu$$

et, pour la base $((1,0,0),(0,1,0))$, sa matrice symétrique est inversible. L'orthocomplément de ce plan étant

$$\{(x,y,0)\}^\perp = \{(u,v,w) \mid \forall (x,y,0) : 6xu + xv + yu + 6yw = 0\} = \{(u,u,u) \mid u \in \mathbb{F}_7\},$$

on sait donc que $\mathbb{F}_7^3 = \{(x,y,0)\} \perp \{(z,z,z)\}$.

Exemple 5.1.5 Nous avons déjà remarqué (Exemple 4.2.4) que, lorsque (V,b) est un espace quadratique régulier, toute application linéaire isométrique $f\colon (V,b) \to (V',b')$ est injective. Bien évidemment, f détermine alors une isométrie entre (V,b) et $\mathrm{im}(f) \subseteq (V',b')$, et ce dernier est donc aussi régulier. Il suit de Proposition 5.1.3 que $(V',b') = im(f) \perp im(f)^\perp$. Autrement dit, toute application linéaire isométrique partant d'un espace régulier est, essentiellement, une isométrie sur un facteur direct orthogonal de l'espace but.

Voici un autre exemple important de somme de sous-espaces :

Proposition 5.1.6 *Soit un espace quadratique (V,b). Il existe $W \subseteq V$ tel que $V = \mathrm{rad}(V,b) \perp W$, et (W,b) est régulier.*

Démonstration. On sait déjà que $\mathrm{rad}(V,b) = \{\underline{x} \in V \mid \forall \underline{y} \in V : b(\underline{x},\underline{y}) = 0\}$ est un sous-espace de V. On peut toujours trouver un sous-espace $W \subseteq V$ tel que $\mathrm{rad}(V,b) \oplus W = V$. (Par exemple, on peut prendre une base $(\underline{e}_1, ..., \underline{e}_k)$ de $\mathrm{rad}(V,b)$, la compléter en une base $(\underline{e}_1 ..., \underline{e}_k, \underline{e}_{k+1}, ..., \underline{e}_n)$ de V, puis définir $W \subseteq V$ comme le sous-espace de base $(\underline{e}_{k+1}, ..., \underline{e}_n)$.) Par définition de $\mathrm{rad}(V,b)$ on a l'orthogonalité de tout élément de $\mathrm{rad}(V,b)$ à tout élément de W. Autrement dit, on sait que $V = \mathrm{rad}(V,b) \perp W$. Reste à montrer que la restriction de la forme b au sous-espace W est régulière : mais

$$\mathrm{rad}(W,b) = \{\underline{x} \in W \mid \forall \underline{y} \in W : b(\underline{x},\underline{y}) = 0\} \subseteq \{\underline{x} \in W \mid \forall \underline{y} \in V : b(\underline{x},\underline{y}) = 0\} = W \cap \mathrm{rad}(V,b)$$

et, par construction, cette intersection est $\{\underline{0}\}$; ainsi (W,b) est régulier. □

La restriction à $\mathrm{rad}(V,b)$ de la forme b sur V est trivialement nulle. Le résultat ci-dessus dit donc comment on peut "décomposer" tout espace quadratique en une partie triviale (son radical) et une partie régulière. Soulignons que, pour la partie régulière (W,b), on peut choisir n'importe quel complément (pour la somme directe) de $\mathrm{rad}(V,b)$ dans V.

Exemple 5.1.7 Soit $(\mathbb{R}^3, q)$ avec $q(x,y,z) = x^2 + xy$; le radical de cet espace non-régulier est $\{(0,0,z) \mid z \in \mathbb{R}\}$. Puisque $\mathbb{R}^3 = \{(x,y,0)\} \oplus \{(0,0,z)\}$, il suit que $(W,b) = (\{(x,y,0)\}, b)$ est régulier et on a une somme orthogonale $\mathbb{R}^3 = \{(x,y,0)\} \perp \{(0,0,z)\}$. Mais on a par exemple aussi $\mathbb{R}^3 = \{(x,y,y)\} \oplus \{(0,0,z)\}$, et donc aussi $(W',b) = (\{(x,y,y)\}, b)$ est régulier, et on a aussi la somme orthogonale $\mathbb{R}^3 = \{(x,y,y)\} \perp \{(0,0,z)\}$.

5.2. Somme externe

Ci-dessus nous avons étudié la somme directe (orthogonale) de deux *sous-espaces* W_1 et W_2 d'un espace (quadratique) V ; on l'appelle parfois la *somme directe (orthogonale) interne*. Il est aussi possible de faire ces constructions pour deux espaces (quadratiques) quelconques, même si – a priori – ils ne sont pas des sous-espaces d'un même "espace enveloppant" ; on parle alors de la *somme directe (orthogonale) externe*.

En effet, si V_1 et V_2 sont deux F-espaces, alors nous avons déjà rappelé que le produit ("cartesien") $V_1 \times V_2$ est aussi un F-espace pour les opérations

$$\begin{cases} (\underline{x},\underline{y}) + (\underline{x}',\underline{y}') = (\underline{x}+\underline{x}', \underline{y}+\underline{y}') \\ \alpha(\underline{x},\underline{y}) = (\alpha\underline{x}, \alpha\underline{y}) \end{cases}$$

De plus, les applications linéaires

$$i_1 \colon V_1 \to V_1 \times V_2 \colon \underline{x} \mapsto (\underline{x},\underline{0}) \quad \text{et} \quad i_2 \colon V_2 \to V_1 \times V_2 \colon \underline{y} \mapsto (\underline{0},\underline{y})$$

sont injectives, donc la restriction aux images respectives donne des isomorphismes

$$V_1 \cong \{(\underline{x},\underline{0}) \in V_1 \times V_2\} \quad \text{et} \quad V_2 \cong \{(\underline{0},\underline{y}) \in V_1 \times V_2\}.$$

A cette identification près, on peut considérer que V_1 et V_2 sont des sous-espaces de $V_1 \times V_2$; et plus en est, $V_1 \times V_2$ est exactement la somme directe de ses "sous-espaces" V_1 et V_2 :

$$V_1 \times V_2 = \{(\underline{x},\underline{0}) \in V_1 \times V_2\} \oplus \{(\underline{0},\underline{y}) \in V_1 \times V_2\} \cong V_1 \oplus V_2.$$

Pour faciliter l'écriture, on a l'habitude de "oublier" les isomorphismes

$$i_1 \colon V_1 \xrightarrow{\sim} \{(\underline{x},\underline{0}) \in V_1 \times V_2\} \quad \text{et} \quad i_2 \colon V_2 \xrightarrow{\sim} \{(\underline{0},\underline{y}) \in V_1 \times V_2\}$$

et d'identifier ainsi formellement

$$V_1 \oplus V_2 = \{\underline{x} + \underline{y} \mid \underline{x} \in V_1, \underline{y} \in V_2\},$$

en se souvenant que tout élément de $V_1 \oplus V_2$ s'écrit *de manière unique* comme une somme $\underline{x}+\underline{y}$, et que les opérations sont alors données par

$$\begin{cases} (\underline{x}+\underline{y}) + (\underline{x}'+\underline{y}') = (\underline{x}+\underline{x}') + (\underline{y}+\underline{y}') \\ \alpha(\underline{x}+\underline{y}) = (\alpha\underline{x} + \alpha\underline{y}) \end{cases}$$

Ainsi il est particulièrement clair que V_1 et V_2 sont des sous-espaces de $V_1 \oplus V_2$: les inclusions s'écrivent tout simplement

$$i_{V_1} \colon V_1 \hookrightarrow V_1 \oplus V_2 \colon \underline{x} \mapsto \underline{x} \quad \text{et} \quad i_{V_2} \colon V_2 \hookrightarrow V_1 \oplus V_2 \colon \underline{y} \mapsto \underline{y}.$$

Nous adopterons ces notations dans la suite du cours.

Supposons maintenant que (V_1, b_1) et (V_2, b_2) sont deux espaces quadratiques. On vérifie facilement que

$$b\colon (V_1 \oplus V_2) \times (V_1 \oplus V_2) \to F\colon (\underline{x}_1 + \underline{x}_2, \underline{y}_1 + \underline{y}_2) \mapsto b_1(\underline{x}_1, \underline{y}_1) + b_2(\underline{x}_2, \underline{y}_2)$$

est une forme bilinéaire symétrique (exercice) ; et clairement la restriction de cette forme aux sous-espaces V_1, resp. V_2, donne la forme b_1, resp. b_2. Autrement dit, (V_1, b_1) et (V_2, b_2) sont des sous-espaces quadratiques de $(V_1 \oplus V_2, b)$. Mieux encore, pour $\underline{x}_1 \in V_1$ et $\underline{x}_2 \in V_2$ on a

$$b(\underline{x}_1, \underline{x}_2) = b(\underline{x}_1 + \underline{0}_{V_2}, \underline{0}_{V_1} + \underline{x}_2) = b_1(\underline{x}_1, \underline{0}_{V_1}) + b_2(\underline{0}_{V_2}, \underline{x}_2) = 0 + 0 = 0$$

dans $V_1 \oplus V_2$. C'est à dire, V_1 et V_2 sont mutuellement orthogonaux dans $(V_1 \oplus V_2, b)$. Pour résumer tout cela, on définit :

Définition 5.2.1 *La* somme orthogonale *de deux F-espaces quadratiques (V_1, b_1) et (V_2, b_2) est la somme directe $V_1 \oplus V_2$ muni de la forme $b(\underline{x}_1 + \underline{x}_2, \underline{y}_1 + \underline{y}_2) = b_1(\underline{x}_1, \underline{y}_1) + b_2(\underline{x}_2, \underline{y}_2)$; on le note $(V_1, b_1) \perp (V_2, b_2)$.*

Remarquons tout de suite que les deux définitions – de somme orthogonale interne et somme orthogonale externe – ne sont pas contradictoires :

Proposition 5.2.2 *Soit un espace quadratique (V, b) et deux sous-espaces vectoriels $W, W' \subseteq V$. Si on considère les sous-espaces quadratiques (W, b) et (W', b) (pour la restriction de la forme b sur V, donc), alors $V = W \perp W'$ (au sens de la Définition 5.1.1) si et seulement si $(V, b) = (W, b) \perp (W', b)$ (au sens de la Définition 5.2.1).*

Démonstration. Il suffit d'écrire les détails des définitions. □

Pour poursuivre, donnons les différentes "incarnations" (forme bilinéaire symétrique, forme quadratique, matrice symétrique, polynôme homogène de degré 2) de la somme orthogonale de deux espaces quadratiques :

Proposition 5.2.3 *Soient deux espaces quadratiques (V_1, b_1) et (V_2, b_2).*

1. *La forme quadratique q déterminé par $(V_1, b_1) \perp (V_2, b_2)$ est*

$$q(\underline{x}_1 + \underline{x}_2) = q_1(\underline{x}_1) + q_2(\underline{x}_2),$$

   où q_k est la forme définie par (V_k, b_k).

2. *La matrice symétrique B déterminée par $(V_1, b_1) \perp (V_2, b_2)$ est (à congruence près)*

$$B = \begin{pmatrix} B_1 & O \\ O & B_2 \end{pmatrix}$$

   où B_k est la matrice symétrique définie par (V_k, b_k).

3. *Le polynôme (homogène de degré 2) f déterminé par $(V_1, b_1) \perp (V_2, b_2)$ est (à équivalence près)*
$$f(X_1, ..., X_n, X_{n+1}, ..., X_{n+m}) = f_1(X_1, ..., X_n) + f_2(X_{n+1}, ..., X_{n+m})$$
où f_k est le polynôme déterminé par (V_k, b_k).

Démonstration. (1) Un simple calcul montre que

$$q(\underline{x}_1 + \underline{x}_2) = b(\underline{x}_1 + \underline{x}_2, \underline{x}_1 + \underline{x}_2) = b_1(\underline{x}_1 + \underline{x}_1) + b_2(\underline{x}_2 + \underline{x}_2) = q_1(\underline{x}_1) + q_2(\underline{x}_2).$$

(2) Si l'on choisit une base $(\underline{e}_1, ..., \underline{e}_n)$ de V_1 et une base $(\underline{d}_1, ..., \underline{d}_m)$ de V_2, alors on peut calculer les matrices respectives

$$B_1 = (b_1(\underline{e}_i, \underline{e}_j))_{i,j} \quad \text{et} \quad B_2 = (b_2(\underline{d}_k, \underline{d}_l))_{k,l}.$$

De l'autre côté, pour la base $(\underline{e}_1, ..., \underline{e}_n, \underline{d}_1, ..., \underline{d}_m)$ de la somme directe $V_1 \oplus V_2$ on peut calculer (pour tout $1 \leq i, j \leq n$ et $1 \leq k, l \leq m$) que

$$b(\underline{e}_i, \underline{e}_j) = b_1(\underline{e}_i, \underline{e}_j) \quad , \quad b(\underline{e}_i, \underline{d}_k) = 0 = b(\underline{d}_k, \underline{e}_i) \quad , \quad b(\underline{d}_k, \underline{d}_l) = b_2(\underline{d}_k, \underline{d}_l).$$

Ainsi on obtient la matrice

$$B = \begin{pmatrix} b(\underline{e}_1, \underline{e}_1) & \cdots & b(\underline{e}_1, \underline{e}_n) & b(\underline{e}_1, \underline{d}_1) & \cdots & b(\underline{e}_1, \underline{d}_m) \\ \vdots & & \vdots & \vdots & & \vdots \\ b(\underline{e}_n, \underline{e}_1) & \cdots & b(\underline{e}_n, \underline{e}_n) & b(\underline{e}_n, \underline{d}_1) & \cdots & b(\underline{e}_n, \underline{d}_m) \\ b(\underline{d}_1, \underline{e}_1) & \cdots & b(\underline{d}_1, \underline{e}_n) & b(\underline{d}_1, \underline{d}_1) & \cdots & b(\underline{d}_1, \underline{d}_m) \\ \vdots & & \vdots & \vdots & & \vdots \\ b(\underline{d}_m, \underline{e}_1) & \cdots & b(\underline{d}_m, \underline{e}_n) & b(\underline{d}_m, \underline{d}_1) & \cdots & b(\underline{d}_m, \underline{d}_m) \end{pmatrix} = \begin{pmatrix} B_1 & O \\ O & B_2 \end{pmatrix}$$

(3) Même genre de raisonnement (exercice). □

Exemple 5.2.4 La somme orthogonale de $(\mathbb{R}^2, q_1(x, y) = x^2 + xy)$ avec $(\mathbb{R}^3, q_2(x, y, z) = xy + y^2 + xz)$ est l'espace $(\mathbb{R}^5, q(x_1, x_2, x_3, x_4, x_5) = x_1^2 + x_1x_2 + x_3x_4 + x_4^2 + x_3x_5)$.

Exemple 5.2.5 Lorsqu'on calcule la somme orthogonale $(V_1, q_1) \perp (V_1, q_2)$, on équipe l'espace $V_1 \oplus V_2$ de la "somme" $q(\underline{x}_1 + \underline{x}_2) = q_1(\underline{x}_1) + q_2(\underline{x}_2)$; mais réciproquement on peut donc aussi "décomposer" une forme quadratique donnée par "séparation des variables". Par exemple, la forme quadratique $q\colon F^6 \to F\colon (x_1, ..., x_6) \mapsto x_1^2 + 3x_1x_5 - x_3^6 + x_4x_6 + x_6^2$ peut être considérée comme la somme des formes $q_1\colon F^2 \to F\colon (x_1, x_5) \mapsto x_1^2 + 3x_1x_5$, $q_2\colon F^2 \to F\colon (x_2, x_3) \mapsto -x_3^2$ et $q_3\colon F^3 \to F\colon (x_4, x_6) \mapsto x_4x_6 + x_6^2$.

Maintenant on peut donner un argument matriciel pour les assertions suivantes :

Proposition 5.2.6 *1. Une somme orthogonale $(V_1, b_1) \perp (V_2, b_2)$ est un espace quadratique régulier si et seulement si les termes (V_1, b_1) et (V_2, b_2) sont des espaces quadratiques réguliers.*

2. *Si on a des isométries* $(V_1, b_1) \cong (V_1', b_1')$ *et* $(V_2, b_2) \cong (V_2', b_2')$ *alors on a aussi une isométrie* $(V_1, b_1) \perp (V_2, b_2) \cong (V_1', b_1') \perp (V_2', b_2')$.
3. *On a une isométrie* $(V_1, b_1) \perp (V_2, b_2) \cong (V_2, b_2) \perp (V_1, b_1)$.
4. *On a une isométrie* $((V_1, b_1) \perp (V_2, b_2)) \perp (V_3, b_3) \cong (V_1, b_1) \perp ((V_2, b_2) \perp (V_3, b_3))$.
5. *Si on note* $(\{\underline{0}\}, 0)$ *l'(unique) espace quadratique de dimension* 0*, alors on a une isométrie* $(V_1, b_1) \perp (\{\underline{0}\}, 0) \cong (V_1, b_1)$.

Démonstration. (1) La matrice symétrique

$$B = \begin{pmatrix} B_1 & O \\ O & B_2 \end{pmatrix}$$

de $(V_1, b_1) \perp (V_2, b_2)$ est inversible si et seulement si les matrices B_1 et B_2 de (V_1, b_1) et (V_2, b_2) le sont.
(2) L'isométrie $(V_1, b_1) \cong (V_1', b_1')$ implique qu'au niveau matriciel les matrices symétriques respectives B_1 et B_1' sont congruentes ; de même, l'isométrie $(V_2, b_2) \cong (V_2', b_2')$ implique une congruence de matrices symétriques B_2 et B_2'. Il suit (par "assemblage" de matrices) qu'aussi

$$B = \begin{pmatrix} B_1 & O \\ O & B_2 \end{pmatrix} \quad \text{et} \quad B' = \begin{pmatrix} B_1' & O \\ O & B_2' \end{pmatrix}$$

sont congruentes ; et cela atteste de l'isométrie $(V_1, b_1) \perp (V_2, b_2) \cong (V_1', b_1') \perp (V_2', b_2')$.
(3, 4, 5) Même genre de raisonnement (exercice). □

Remarque 5.2.7 La Proposition ci-dessus indique en particulier que, pour trois espaces quadratiques (V_1, b_1), (V_2, b_2) et (V_3, b_3), les deux façons de calculer leur somme orthogonale donnent des résultats isométriques ; par abus de langage, on parle donc de "la" somme orthogonale $(V_1, b_1) \perp (V_2, b_2) \perp (V_3, b_3)$ (sans expliciter les parenthèses). De manière évidente, on généralise tout cela à la somme orthogonale de k espaces, $(V_1, b_1) \perp ... \perp (V_k, b_k)$.

Remarque 5.2.8 Encore dans la Proposition ci-dessus, on parle – pour la première fois explicitement – de l'(unique) espace vectoriel nul $\{\underline{0}\}$, qui est effectivement de dimenion 0 (donc finie). L'unique forme quadratique sur cet espace est la forme nulle, $q(\underline{0}) = 0$. L'unique base de cet espace est la base vide, et donc la matrice symétrique de cet espace est la "matrice vide". Bien sûr, cet espace nul semble sans aucun intérêt—si ce n'est qu'il est le "neutre" pour la somme orthogonale d'espaces quadratiques. En effet, les assertions (3, 4, 5) de la Proposition ci-dessus disent que "la somme orthogonale d'espaces quadratiques est commutative, associative et admet un neutre" (à isométrie près). Ce point de vue sera important vers la fin du cours...

5.3. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Montrer que $(\mathbb{R}^2, q(x,y) = x^2)$ est un espace quadratique non-régulier et que la droite engendrée par $(1,0)$ en est un sous-espace régulier. Montrer que $(\mathbb{R}^2, q(x,y) = xy)$ est un espace quadratique régulier et que la droite engendrée par $(1,0)$ en est un sous-espace non-régulier. Montrer que le plan cartésien $(\mathbb{R}^2, q(x,y) = x^2 + y^2)$ est un espace quadratique régulier dont tout sous-espace est régulier. Montrer que $(\mathbb{R}^2, q(x,y) = 0)$ est un espace quadratique non-régulier dont tout sous-espace non-nul est non-régulier.

6. Diagonalisation

Soit V un F-espace ; nous allons noter $F\underline{x} = \{\alpha\underline{x} \mid \alpha \in F\}$ pour le sous-espace engendré par un vecteur $\underline{x} \in V$. Ainsi, une suite $(\underline{e}_1, ..., \underline{e}_n)$ de vecteurs de V est une base si et seulement si $V \cong F\underline{e}_1 \oplus ... \oplus F\underline{e}_n$. Autrement dit, pour trouver une base de V, on *décompose* cet espace en une somme directe de sous-espaces de dimension 1. On veut faire "la même chose" avec les espaces quadratiques : on veut *décomposer* un espace quadratique (V, q) en une somme orthogonale de sous-espaces quadratiques de dimension 1.

6.1. Représentation

Introduisons d'abord la notation :

Définition 6.1.1 *Pour $d \in F$ on note $\langle d\rangle$ l'espace quadratique $(F, q\colon F \to F\colon x \mapsto dx^2)$.*

La forme bilinéaire symétrique de $\langle d\rangle$ est donc

$$b\colon F \times F \to F\colon (x, y) \mapsto dxy,$$

la matrice symétrique est (à congruence près)

$$B = (d) \in F^{1\times 1},$$

et le polynôme f est (à équivalence près)

$$f(X) = dX^2 \in F[X].$$

Clairement, $\langle d\rangle$ est régulier si et seulement si d est un élément inversible de F.

Plus généralement, pour $d_1, ..., d_n \in F$ nous allons noter

$$\langle d_1, ..., d_n\rangle = \langle d_1\rangle \perp ... \perp \langle d_n\rangle.$$

Explicitement, c'est l'espace $F \oplus ... \oplus F = F^n$ muni de la forme quadratique

$$q\colon F^n \to F\colon (x_1, ..., x_n) \mapsto d_1x_1^2 + ... + d_nx_n^2;$$

sa matrice symétrique est (à congruence près) la matrice diagonale

$$\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$$

et son polynôme est (à équivalence près) la somme pondérée de carrés,

$$f(X_1, ..., X_n) = d_1X_1^2 + ... + d_nX_n^2.$$

Ainsi, étant donné un espace quadratique quelconque (V, b), nous voulons établir une isométrie

$$(V, b) \cong \langle d_1 \rangle \perp ... \perp \langle d_n \rangle = \langle d_1, ..., d_n \rangle$$

pour des nombres $d_1, ..., d_n \in F$ qui sont donc à déterminer. De manière équivalente, au niveau matriciel, cela veut dire que nous voulons trouver, pour toute matrice symétrique B, une congruence avec une matrice diagonale :

$$B = C^t \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} C \quad \text{pour } C \text{ inversible.}$$

Ou encore de manière équivalente, au niveau des polynômes, nous voulons transformer tout polynôme f homogène de degré 2 en une somme pondérée de carrés par un changement linéaire et inversible de variables :

$$f(X_1, ..., X_n) = d_1Y_1^2 + ... + d_nY_n^2 \quad \text{pour } \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = C \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \text{ et } C \text{ inversible.}$$

Ce problème s'appelle la *diagonalisation* de l'espace quadratique (V, b).

Pour mener à bien cette tâche, nous introduisons d'abord [1] :

Définition 6.1.2 *On appelle* $D(V, q) = \{d \in F^\times \mid \exists \underline{x} \in V : q(\underline{x}) = d\}$ *l'ensemble des* valeurs représentées *par un espace quadratique* (V, q).

Exemple 6.1.3 Soit $X_2^2 + 3X_2X_3 \in \mathbb{F}_5[X_1, ..., X_4]$, alors on peut réaliser l'espace quadratique $(\mathbb{F}_5^4, q)$ par la forme quadratique $q(x, y, z, t) = y^2 + 3yt$. L'espace $\mathbb{F}_5^4$ compte 625 éléments ; en calculant la valeur de q en chacun de ces 625 points, on trouve les valeurs (non-nulles !) représentées par q, d'où l'ensemble $D(\mathbb{F}_5^4, q)$ (exercice).

Proposition 6.1.4 *1. Si* $(V, q) \cong (V', q')$ *alors* $D(V, q) = D(V', q')$.

2. $D((V, q) \perp (V', q')) = \{d \in F^\times \mid \exists \underline{x}_1 + \underline{x}_2 \in V \oplus V' : d = q(\underline{x}) + q'(\underline{x}')\}$.

3. Pour tout espace (V, q) *il existe un sous-espace* régulier (W, q) *tel que* $D(V, q) = D(W, q)$.

Démonstration. (1, 2) Exercice.
(3) Par Proposition 5.1.6 on sait que $(V, b) \cong (\mathrm{rad}(V, b), b) \perp (W, b)$ avec (W, b) régulier. La forme b est nulle sur $\mathrm{rad}(V, b)$, donc $D(V, b) = D((\mathrm{rad}(V, b), b) \perp (W, b)) = D(W, b)$ suit par (2). □

1. On note $F^\times$ pour l'ensemble des éléments inversibles de F ; puisque F est un corps, on a $F^\times = F \setminus \{0\}$.

Théorème 6.1.5 (Critère de représentation) *Soit un espace quadratique (V,b) et $d \in F^\times$. On a $d \in D(V,b)$ si et seulement s'il existe une décomposition $(V,b) \cong \langle d\rangle \perp (V',b')$.*

Démonstration. ($\Leftarrow$) Supposons que $(V,b) \cong \langle d\rangle \perp (V',b')$. On a $D(V,b) = D(\langle d\rangle \perp (V',b'))$, et $d \in D(\langle d\rangle)$ étant évident, on a aussi $d \in D(V,b)$ (par exemple comme valeur en $(1,\underline{0}) \in F \oplus V'$). ($\Rightarrow$) Supposons d'abord que (V,b) est régulier. Pour $d \in D(V,b)$ on peut trouver un $\underline{v} \in V$ tel que $d = q(\underline{v}) = b(\underline{v},\underline{v})$. Le sous-espace $F\underline{v}$ de V est un espace quadratique pour la restriction de la forme b, et on a une isométrie $(F\underline{v},b) \cong \langle d\rangle$: en effet, la matrice symétrique de $F\underline{v}$ pour la base $(\underline{v})$ est identique à la matrice symétrique que pour $\langle d\rangle$; a fortiori les deux matrices sont congruentes, et donc les espaces sont isométriques. L'espace $(F\underline{v},b)$ est régulier (car isométrique à $\langle d\rangle$ pour $d \neq 0$!), et donc

$$F\underline{v} \cap (F\underline{v})^\perp = \mathrm{rad}(F\underline{v},b) = \{\underline{0}\}.$$

Ainsi on sait que $F\underline{v} + (F\underline{v})^\perp = F\underline{v} \oplus (F\underline{v})^\perp$. Par la Proposition 4.2.8 (et donc par la supposée régularité de (V,b)) on a aussi

$$\dim(F\underline{v}) + \dim((F\underline{v})^\perp) = \dim(V),$$

et donc $F\underline{v} \oplus (F\underline{v})^\perp = V$. L'évidente orthogonalité de $F\underline{v}$ à $(F\underline{v})^\perp$ permet de conclure que

$$(V,b) = (F\underline{v},b) \perp ((F\underline{v})^\perp,b) \cong \langle d\rangle \perp ((F\underline{v})^\perp,b).$$

Si l'espace quadratique (V,b) n'est pas régulier, on peut appliquer la Proposition 5.1.6 pour d'abord décomposer $(V,b) = (\mathrm{rad}(V,b),b) \perp (W,b)$ avec (W,b) régulier ; et par la Propostion 6.1.4 on sait que $D(V,b) = D(W,b)$. Ainsi, par hypothèse on a $d \in D(V,b) = D(W,b)$, et on peut faire le raisonnement précédent pour l'espace régulier (W,b) ; on trouve $(W,b) \cong \langle d\rangle \perp (W',b')$, et donc aussi

$$(V,b) = (\mathrm{rad}(V,b),b) \perp (W,b) \cong (\mathrm{rad}(V,b),b) \perp \langle d\rangle \perp (W',b') \cong \langle d\rangle \perp (V',b')$$

si on pose $(V',b') = (\mathrm{rad}(V,b),b) \perp (W',b')$. □

Remarquons que cette démonstration donne un algorithme pour calculer concrètement la décomposition $(V,b) \cong \langle d\rangle \perp (V',b') \cong (F\underline{v},b) \perp ((F\underline{v}^\perp,b)$, où $d = q(\underline{v})$.

Exemple 6.1.6 Soit le polynôme $2X_1X_2 + X_2^2 + X_2X_3$ sur $\mathbb{F}_3$. On peut le penser comme espace quadratique en posant $V = \mathbb{F}_3^3$ et $q(x,y,z) = 2xy + y^2 + yz$, la forme bilinéare symétrique étant donc

$$b((x,y,z),(u,v,w)) = xv + yu + yv + 2yw + 2zv.$$

On "voit" ici que $q(1,2,0) = 2 \in \mathbb{F}_3^\times$—avec les notations du Théorème, $q(\underline{v}) = d$ pour $\underline{v} = (1,2,0)$ et $d = 2$. Pour décomposer l'espace en $(\mathbb{F}_2^3,q) \cong \langle 2\rangle \perp (W,b)$ on calcule $W = (\mathbb{F}_3 \cdot (1,2,0))^\perp = (1,2,0)^\perp$ dans $(\mathbb{F}^3,b)$:

$$(\mathbb{F}_3 \cdot (1,2,0))^\perp \quad = \quad (1,2,0)^\perp$$

$$\begin{aligned} &= \{(x,y,z) \in \mathbb{F}_3^3 \mid b((x,y,z),(1,2,0)) = 0\} \\ &= \{(x,y,z) \mid 2x + z = 0\} \\ &= \{(x,y,z) \mid x = z\} \\ &= \{(x,y,x)\} \end{aligned}$$

C'est à dire, W est le sous-plan d'équation $x = z$ de $\mathbb{F}_3^3$. La restriction de la forme quadratique $q(x,y,z) = 2xy + y^2 + yz$ sur $\mathbb{F}_3^3$ à $W \subseteq \mathbb{F}_3^3$ est $q_{|W}(x,y,x) = y^2$; la restriction de la forme bilinéaire symétrique b est $b_{|W}((x,y,x),(u,v,u)) = yv$. On obtient la décomposition $(\mathbb{F}_3^3, q) \cong \langle 2 \rangle \perp (W, q_{|W})$.

6.2. Diagonalisation

Le corollaire principal du Théorème 6.1.5 est enfin :

Théorème 6.2.1 (Diagonalisation) *Pour tout espace quadratique (V,b) il existe des scalaires $d_1, ..., d_n \in F$ tels que $(V,b) \cong \langle d_1, ..., d_n \rangle$.*

Démonstration. Si $D(V,b) = \emptyset$, alors nécessairement $b(\underline{x}, \underline{y}) = 0$ pour tout $\underline{x}, \underline{y} \in V$, et donc $(V,b) \cong \langle 0, ..., 0 \rangle$. Si $D(V,b) \neq \emptyset$ alors il existe $d \in D(V,b)$ et par le Critère de Représentation on trouve une décomposition $(V,b) \cong \langle d \rangle \perp (V', b')$; et dans ce cas on a $\dim(V') = \dim(V) - 1$. On répète la procédure sur (V', b') ; et (par induction sur la dimension de V) on arrive au résultat. □

Cette démonstration donne une méthode pour calculer une décomposition $(V,b) \cong \langle d_1, ..., d_n \rangle$. Concrètement, on construit une suite $\underline{v}_1, ..., \underline{v}_n$ dans V telle que

$$b(\underline{v}_i, \underline{v}_j) = \begin{cases} d_i \text{ si } i = j \\ 0 \text{ si } i \neq j \end{cases}$$

de façon que $V \cong F\underline{v}_1 \oplus ... \oplus F\underline{v}_n$, et donc $(V,b) \cong \langle d_1 \rangle \perp ... \perp \langle d_n \rangle$. Autrement dit, $(\underline{v}_1, ..., \underline{v}_n)$ est une *base orthogonale* de V. (On pourrait avoir envie de définir des vecteurs $\underline{w}_i = \frac{1}{\sqrt{d_i}} \underline{v}_i$, pour constituer une base ortho*normale* $(\underline{w}_1, ..., \underline{w}_n)$ de V... mais cela dépend de la possibilité de calculer des racines carrés dans le corps F ! On y reviendra.)

Exemple 6.2.2 Reprenons l'exemple ci-dessus : l'espace quadratique $(\mathbb{F}_3^3, q(x,y,z) = 2xy + y^2 + yz)$ se décompose en $(\mathbb{F}_3^3, q) = \langle 2 \rangle \perp (W, q_{|W})$ pour $W = \{(x,y,x) \mid x, y \in \mathbb{F}_3\}$ et $q_{|W}(x,y,x) = y^2$; la forme bilinéaire sur W est $b_{|W}((x,y,x),(u,v,u)) = yv$. On refait l'argument du Théorème 6.1.5 avec l'espace $(W, q_{|W})$: on "voit" que $q_{|W}(1,1,1) = 1$, et on sait donc que $(W, q_{|W}) \cong \langle 1 \rangle \perp (Z, q_{|Z})$ pour $Z = (\mathbb{F}_3 \cdot (1,1,1))^\perp$... mais attention, c'est l'orthocomplément de $\mathbb{F}_3 \cdot (1,1,1)$ dans $(W, q_{|W})$:

$$\begin{aligned} (\mathbb{F}_3 \cdot (1,1,1))^\perp &= \{(x,y,x) \in W \mid b_W((x,y,x),(1,1,1)) = 0\} \\ &= \{(x,y,x) \mid y = 0\} \\ &= \{(x,0,x)\} \end{aligned}$$

Posons donc $Z = \{x, 0, x\} \subseteq W$ (et notons que $(1, 0, 1)$ est une base de Z : Z est de dimension 1) ; nous avons une décomposition $(W, q_W) \cong \langle 1\rangle \perp (Z, q_{|Z})$. La restriction de la forme $q_{|W}$ à Z est $q_{|Z}(x, 0, x) = 0$ (et aussi la forme bilinéaire sur Z est donc nulle) ; puisque Z est de dimension 1, il suit que $(Z, q_{|Z}) \cong \langle 0\rangle$. Au final, nous avons ainsi calculé que

$$(\mathbb{F}_3^3, q) \cong \langle 2\rangle \perp (W, q_{|W}) \cong \langle 2\rangle \perp \langle 1\rangle \perp (Z, q_{|Z}) \cong \langle 2\rangle \perp \langle 1\rangle \perp \langle 0\rangle \cong \langle 2, 1, 0\rangle.$$

Cette décomposition est réalisée par la base orthogonale $((1, 2, 0), (1, 1, 1), (1, 0, 1))$ de $\mathbb{F}_3^3$ pour la forme bilinéaire b.

Par ailleurs, ce résultat peut aussi être compris au niveau matriciel. En effet, si on équipe l'espace $\mathbb{F}_3^3$ de sa base canonique, alors la matrice symétrique de la forme quadratique $q(x, y, z) = 2xy + y^2 + yz)$ est

$$B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{pmatrix} \in \mathbb{F}_3^{3\times 3}.$$

L'isométrie $(\mathbb{F}_3^3, q) \cong \langle 2, 1, 0\rangle$ dit exactement que B est congruente à la matrice diagonale

$$D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix};$$

la matrice inversible C telle que $B = C^t DC$ est précisément la matrice de changement de base de la base orthogonale $((1, 2, 0), (1, 1, 1), (1, 0, 1))$ à la base canonique $((1, 0, 0), (0, 1, 0), (0, 0, 1))$:

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Finalement, nos calculs attestent du fait que le polynôme $2X_1X_2+X_2^2+X_2X_3 \in \mathbb{F}_3[X_1, ..., X_3]$ est équivalent au polynôme $2X_1^2+X_2^2 \in \mathbb{F}_3[X_1, X_2, X_3]$. En effet, si on note cette dernière somme pondérée de carrés pour un instant par $2Y_1^2 + Y_2^2$ (pour ne pas confondre les variables), alors le changement (linéaire et inversible !) de variables donné par la matrice C ci-dessus, soit

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} \iff \begin{cases} X_1 = Y_1 + Y_2 + Y_3 \\ X_2 = 2Y_1 + Y_2 \\ X_3 = Y_2 + Y_3 \end{cases}$$

montre bien que

$$2X_1X_2 + x_2^2 + X_2X_3 = 2(Y_1 + Y_2 + Y_3)(2Y_1 + Y_2) + (2Y_1 + Y_2)^2 + (2Y_1 + Y_2)(Y_2 + Y_3) = 2Y_1^2 + Y_2^2.$$

Remarque 6.2.3 Si on "oublie" pour un instant les espaces quadratiques et les matrices symétriques, on peut dire que le Théorème de Diagonalisation atteste tout simplement du fait que tout polynôme $f \in F[X_1, ..., X_n]$ homogène de degré 2 peut être écrit comme une somme

pondérée de carrés à un changement linéaire inversible de variables près. Autrement dit, pour un tel f il existe une matrice inversible $C \in F^{n\times n}$ telle que, si on pose

$$\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = C \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix},$$

alors on a $f(X_1, ..., X_n) = \sum_i d_i Y_i^2$. La *méthode de réduction de Gauss* est un algorithme pour calculer la somme pondérée $\sum_i d_i Y_i^2$ directement—sans passer par l'espace quadratique déterminé par f.

D'abord, supposons que $f(X_1, ..., X_n)$ a un terme $a_i X_i^2$ non-nul ; on peut supposer (à permutation des variables près) que c'est aX_1^2. On peut alors réécrire (puisque $2 \neq 0$ dans F !)

$$\begin{aligned} f(X_1, ..., X_n) &= aX_1^2 + X_1 g(X_2, ..., X_n) + h(X_2, ..., X_n) \\ &= a\Big(X_1 + \frac{1}{2a} g(X_2, ..., X_n)\Big)^2 - a\Big(\frac{1}{2a} g(X_2, ..., X_n)\Big)^2 + h(X_2, ..., X_n) \end{aligned}$$

et par le changement linéaire et inversible de variables

$$\begin{cases} Y_1 = X_1 + \dfrac{1}{2a} g(X_2, ..., X_n) \\ Y_2 = X_2 \\ \vdots \\ Y_n = X_n \end{cases}$$

on voit que

$$f(X_1, ..., X_n) = aY_1^2 + k(Y_2, ..., Y_n)$$

où $k(Y_2, ..., Y_n)$ est homogène de degré 2, et ne contient pas de Y_1.

Supposons, par contre, que $f(X_1, ..., X_n)$ n'a aucun terme en X_i^2 ; si f n'est pas nul (au quel cas sa diagonalisation est triviale !), il y a donc un terme $a_{ij} X_i X_j$ de coefficient non-nul et (à permutation des variables près) on peut supposer que c'est aX_1X_2. On peut réécrire f comme

$$\begin{aligned} f(X_1, ..., X_n) &= aX_1X_2 + X_1 g(X_3, ..., X_n) + X_2 h(X_3, ..., X_n) + k(X_3, ..., X_n) \\ &= a\Big(X_1 + \frac{1}{a} h(X_3, ..., X_n)\Big)\Big(X_2 + \frac{1}{a} g(X_3, ..., X_n)\Big) + l(X_3, ..., X_n) \\ &= \frac{a}{4}\Big(X_1 + X_2 + \frac{g(X_3, ..., X_n) + h(X_3, ..., X_n)}{a}\Big)^2 \\ &\qquad -\frac{a}{4}\Big(X_1 - X_2 + \frac{-g(X_3, ..., X_n) + h(X_3, ..., X_n)}{a}\Big)^2 + l(X_3, ..., X_n) \end{aligned}$$

Par le changement linéaire et inversible de variables

$$\begin{cases} Y_1 = X_1 + X_2 + \dfrac{g(X_3, ..., X_n) + h(X_3, ..., X_n)}{a} \\ Y_2 = X_1 - X_2 + \dfrac{-g(X_3, ..., X_n) + h(X_3, ..., X_n)}{a} \\ Y_3 = X_3 \\ \vdots \\ Y_n = X_n \end{cases}$$

le polynôme devient

$$f(X_1, ..., X_n) = \frac{a}{4}Y_1^2 - \frac{a}{4}Y_2^2 + l(Y_3, ..., Y_n)$$

où $l(Y_3, ..., Y_n)$ est homogène de degré 2, et ne contient pas de Y_1 ou de Y_2.

Ainsi, par itération de la procédure – par induction sur le nombre de variables – on peut écrire le polynôme $f(X_1, ..., X_n)$ comme une somme pondérée de carées des Y_i's, et ce en ne faisant que des changements linéaires et inversibles des variables.

Voici une application concrète : soit $f(X_1, X_2, X_3) = 3X_1^2 + 4X_1X_2 - 5X_2^2 - X_1X_3$ sur $\mathbb{F}_{11}$. Alors on peut calculer (dans $\mathbb{F}_{11}$ bien sûr !) à changement linéaire et inversible de variables près :

$$\begin{aligned}
3X_1^2 + 4X_1X_2 - 5X_2^2 - X_1X_3 &= 3X_1^2 + X_1(4X_2 - X_3) - 5X_2^2 \\
&= 3\Big(X_1^2 + 4X_1(4X_2 - X_3)\Big) - 5X_2^2 \\
&= 3\left[\Big(X_1 + 2(4X_2 - X_3)\Big)^2 - \Big(2(4X_2 - X_3)\Big)^2\right] - 5X_2^2 \\
&= 3\Big(X_1 + 2(4X_2 - X_3)\Big)^2 - 3\Big(2(4X_2 - X_3)\Big)^2 - 5X_2^2 \\
&= 3\Big(X_1 + 2(4X_2 - X_3)\Big)^2 - (4X_2 - X_3)^2 + 6X_2^2 \\
&= 3\Big(X_1 + 2(4X_2 - X_3)\Big)^2 - (16X_2^2 - 8X_2X_3 + X_3^2) + 6X_2^2 \\
&= 3\Big(X_1 + 8X_2 + 9X_3)\Big)^2 + X_2^2 + 8X_2X_3 - X_3^2 \\
&\cong 3Y_1^2 + Y_2^2 + 8Y_2Y_3 - Y_3^2 \\
&= 3Y_1^2 + \Big((Y_2 + 4Y_3)^2 - (4Y_3)^2\Big) - Y_3^2 \\
&= 3Y_1^2 + (Y_2 + 4Y_3)^2 - 16Y_3^2 - Y_3^2 \\
&= 3Y_1^2 + (Y_2 + 4Y_3)^2 + 5Y_3^2 \\
&\cong 3Z_1^2 + Z_2^2 + 5Z_3^3
\end{aligned}$$

Les changements de variables à faire sont donc

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = \begin{pmatrix} 1 & 8 & 9 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} \text{ et } \begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix}$$

Si on les compose on a

$$\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 8 & 9 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} = \begin{pmatrix} 1 & 8 & 9 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix}$$

et on peut inverser cette matrice pour obtenir C :

$$C = \begin{pmatrix} 1 & 8 & 9 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 3 & 1 \\ 0 & 1 & 7 \\ 0 & 0 & 1 \end{pmatrix}.$$

6.3. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Pour $d \in F$, montrer que l'espace quadratique $\langle d \rangle$ est régulier si et seulement si $d \neq 0$. Quand a-t-on une isométrie $\langle d \rangle \cong \langle d' \rangle$? Quand a-t-on la régularité de l'espace $\langle d_1, ..., d_n \rangle$?

3. On considère la forme quadratique $q(x, y) = x^2 + 2xy$ sur $V = \mathbb{F}_5^2$. Vérifier que $d = 1 \in \mathbb{F}_5$ est représenté par cette forme quadratique, et (suivant la démonstration du Critère de Représentation) écrire (V, q) comme une somme orthogonale $\langle 1 \rangle \perp (W, q')$.

4. Appliquer le Théorème de Diagonalisation à :

   (a) $q(x, y, z) = y^2 + 4xy - z^2 + xz$ sur $\mathbb{R}$

   (b) $q(x, y, z) = y^2 + 4xy - z^2 + xz$ sur $\mathbb{F}_7$

5. Pour les formes ci-dessous, donner une diagonalisation par la méthode de réduction de Gauss :

   (a) $f(X_1, X_2, X_3) = 3X_1^2 + 4X_1X_2 - 5X_2^2 - X_1X_3$ sur $\mathbb{R}$,

   (b) $f(X_1, X_2, X_3) = 3X_1^2 + 4X_1X_2 - 5X_2^2 - X_1X_3$ sur $\mathbb{F}_7$,

   (c) $f(X, Y, Z) = XY + XZ + YZ$ sur $\mathbb{R}$,

   (d) $f(X, Y, Z) = XY + XZ + YZ$ sur $\mathbb{F}_3$.

7. Rang et déterminant

Dans cette section, nous introduisons deux *invariants* de classes d'isométrie d'espaces quadratiques, et nous voyons comment on peut *simplifier* la forme diagonale d'une forme quadratique donnée.

7.1. Compter les nuls

Rappelons la Proposition 5.1.6 : pour tout espace quadratique (V, b) on a une décomposition

$$(V, b) \cong \mathrm{rad}(V, b) \perp W$$

où $(\mathrm{rad}(V, b), b)$ est la "partie nulle" de (V, b), et (W, b) est sa "partie régulière". Cette décomposition est, en fait, unique à isométrie près :

Proposition 7.1.1 *Soit une isométrie $(V, b) \cong (V', b')$ et des décompositions $V \cong \mathrm{rad}(V, b) \perp W$ et $V' \cong \mathrm{rad}(V', b') \perp W'$. Alors on a des isométries*

1. $(\mathrm{rad}(V, b), b) \cong (\mathrm{rad}(V', b'), b')$,
2. $(W, b) \cong (W', b')$.

Démonstration. Soit une isométrie $f\colon (V, b) \to (V', b')$.
(1) Cette isométrie est un isomorphisme $f\colon V \to V'$ faisant commuter le carré suivant :

$$\begin{array}{ccc} V & \xrightarrow{\hat{b}} & V^* \\ {\scriptstyle f}\downarrow & & \uparrow{\scriptstyle f^*} \\ V' & \xrightarrow[\hat{b'}]{} & V'^* \end{array}$$

Mais aussi l'application duale $f^*\colon V'^* \to V^*$ est un isomorphisme d'espaces vectoriels (exercice), et on peut raisonner par injectivité de f^* que

$$\underline{x} \in \ker(\hat{b}) \iff \hat{b}(\underline{x}) = \underline{0} \iff (f^* \circ \hat{b'} \circ f)(\underline{x}) = \underline{0} \iff (\hat{b'} \circ f)(\underline{x}) = \underline{0} \iff f(\underline{x}) \in \ker(\hat{b'}).$$

Par surjectivité de f cela implique $f(\mathrm{rad}(V, b)) = f(\ker(\hat{b})) = \ker(\hat{b'}) = \mathrm{rad}(V', b')$, ce qui veut dire que la restriction $f\colon \mathrm{rad}(V, b) \to \mathrm{rad}(V', b')$ est bien définie, et c'est un isomorphisme. Puisque la forme b est nulle sur $\mathrm{rad}(V, b)$, et la forme b' est nulle sur $\mathrm{rad}(V', b')$, l'isométrie des radicaux est immédiat.

(2) Pour $\underline{w} \in W$, considérons l'unique décomposition $f(\underline{w}) = \underline{r}' + \underline{w}'$ avec $\underline{r}' \in \mathrm{rad}(V', b')$ et $\underline{w}' \in W'$; l'application

$$f' \colon W \to W' \colon \underline{w} \mapsto \underline{w}'$$

ainsi définie est linéaire (exercice). De plus, on a

$$f'(\underline{w}) = \underline{0} \iff f(\underline{w}) = \underline{r}' + \underline{0} \iff f(\underline{w}) \in \mathrm{rad}(V', b') \iff \underline{w} \in \mathrm{rad}(V, b)$$

(on utilise (1) pour la dernière équivalence). Puisque $W \cap \mathrm{rad}(V, b) = \{\underline{0}\}$ on trouve $\ker(f') = \{\underline{0}\}$, et f' est injective. Mais – encore par (1) – on sait aussi que

$$\dim(W) = \dim(V) - \dim(\mathrm{rad}(V, b)) = \dim(V') - \dim(\mathrm{rad}(V', b')) = \dim(W')$$

et donc f' est un isomorphisme. Reste à montrer que c'est une isométrie. Pour cela, pour $\underline{w}_i \in W$ on écrit $f(\underline{w}_i) = \underline{r}'_i + f'(\underline{w}_i)$ avec $\underline{r}'_i \in \mathrm{rad}(V', b')$ et on calcule :

$$\begin{aligned} b(\underline{w}_1, \underline{w}_2) &= b'(f(\underline{w}_1), f(\underline{w}_2)) \\ &= b'(\underline{r}'_1 + f'(\underline{w}_1), \underline{r}'_2 + f'(\underline{w}_2)) \\ &= b'(\underline{r}'_1, \underline{r}'_2) + b'(\underline{r}'_1, f'(\underline{w}_2)) + b'(f'(\underline{w}_1), \underline{r}'_2) + b'(f'(\underline{w}_1), f'(\underline{w}_2)) \\ &= 0 + 0 + 0 + b'(f'(\underline{w}_1), f'(\underline{w}_2)) \\ &= b'(f'(\underline{w}_1), f'(\underline{w}_2)). \end{aligned}$$

On a utilisé que tout élément de $\mathrm{rad}(V', b')$ est orthogonal à tout élément de V' pour l'avant-dernière équation. □

Cette Proposition implique que la dimension du radical et la dimension de la partie régulière d'un espace quadratique (V, b) sont des invariants de sa classe d'isométrie. Cela justifie :

Définition 7.1.2 *Le* rang *d'un espace quadratique (V, b) est la dimension de sa partie régulière ; autrement dit,* $\mathrm{rang}(V, b) = \dim(V) - \dim(\mathrm{rad}(V, b))$.

Exemple 7.1.3 Soit la forme $q(x, y, z) = xy + yz$ sur le corps $\mathbb{R}$. La forme bilinéaire symétrique associée est $b((x, y, z), (u, v, w)) = \frac{1}{2}(xv + yu + yw + zv)$ et le radical est la droite $\{(x, 0, -x) \mid x \in \mathbb{R}\}$. Le rang de $(\mathbb{R}^3, q)$ est donc 2.

Lorsqu'on diagonalise un espace quadratique $(V, b) \cong (\mathrm{rad}(V, b), b) \perp (W, b)$, on peut diagonaliser "à part" son radical et sa partie régulière. La restriction de b à $\mathrm{rad}(V, b)$ étant la forme nulle, la diagonalisation de $(\mathrm{rad}(V, b), b)$ est

$$(\mathrm{rad}(V), b) \cong \langle 0, ..., 0 \rangle.$$

La diagonalisation de l'espace régulier (W, b) se fait nécessairement par des valeurs non-nulles (exercice !) :

$$(W, b) \cong \langle d_1, ..., d_k \rangle \text{ pour } d_i \in F^\times.$$

Il suit ainsi que

$$(V, b) \cong \langle 0, ..., 0, d_1, ..., d_k \rangle \text{ pour } d_i \in F^\times.$$

Le nombre d'éléments non-nuls dans cette diagonalisation est le rang de (V, b) ; ce nombre est donc constant. Aussi le nombre de nuls est constant—c'est la dimension de son radical.

7.2. Eliminer les carrés

Pour apporter une deuxième simplification à la diagonalisation

$$(V, b) \cong \langle 0, ..., 0, d_1, ..., d_k \rangle,$$

rappelons que les d_i's sont des éléments de l'ensemble des valeurs représentées par (V, q),

$$D(V, q) = \{d \in F^\times \mid \exists \underline{x} \in V : q(\underline{x}) = d\}.$$

Par *quadraticité* de q, on peut calculer pour $d = q(\underline{x}) \in D(V, q)$ et $a \in F^\times$ que l'on a aussi $q(a\underline{x}) = a^2 q(\underline{x}) = a^2 d \in D(V, q)$. Par ailleurs, on a une isométrie évidente $\langle d \rangle \cong \langle a^2 d \rangle$, donnée par

$$\begin{array}{ccc} (F, q(x) = dx^2) & \rightleftarrows & (F, q'(x) = a^2 dx^2) \\ x & \longmapsto & a^{-1}x \\ ax & \longmapsfrom & x \end{array}$$

Par "assemblage" de tels isométries on obtient :

Proposition 7.2.1 *Pour tout $a_1, ..., a_n \in F^\times$, $d_1, ..., d_n \in F$, on a $\langle d_1, ..., d_n \rangle \cong \langle a_1^2 d_1, ..., a_n^2 d_n \rangle$.*

En mots, toute diagonalisation est déterminée "à carrés près" : on peut toujours "éliminer les carrés" dans (la partie régulière de) la forme diagonale. Ainsi, la disponibilité de carrés (ou, inversement, de racines carrées) dans le corps F permet une simplification considérable des formes diagonales.

Exemple 7.2.2 Sur $\mathbb{R}$, l'espace quadratique $\langle 3, 2, 1 \rangle$ est isométrique à $\langle 1, 1, 1 \rangle$, parce que 3 et 2 sont des carrés dans $\mathbb{R}$. Par contre, sur $\mathbb{Q}$ on ne peut pas utiliser cet argument ! (Et on verra qu'en effet ces espaces ne sont pas isométriques sur $\mathbb{Q}$.)

Exemple 7.2.3 Sur $\mathbb{F}_7$, les carrés non-nuls sont $1^2 = 6^2 = 1$, $3^2 = 4^2 = 2$ et $2^2 = 5^2 = 4$. On peut remplacer dans la diagonalisation $\langle 0, 0, 2, 4, 6, 1, 5 \rangle$ toute occurence d'un carré par 1, pour obtenir son isométrie avec $\langle 0, 0, 1, 1, 6, 1, 5 \rangle$. Mais on peut aussi remarquer que $6 = 4 \cdot 5 = 2^2 \cdot 5$, et donc on a encore l'isométrie avec $\langle 0, 0, 1, 1, 5, 1, 5 \rangle$. On obtient ainsi une forme diagonale avec des 0's, des 1's et des occurences d'un seul non-carré. Nous allons exploiter cette idée dans la section suivante...

7.3. Un invariant à carré près

Soit un espace quadratique (V, b) quelconque, alors par un choix de base $(\underline{e}_1, ..., \underline{e}_n)$ on peut calculer une matrice symétrique $B = (b(\underline{e}_i, \underline{e}_j))_{i,j} \in F^{n \times n}$; et cette matrice a un déterminant $\det(B) \in F$. Cependant, pour un autre choix de base on trouvera une autre matrice symétrique B', liée à la première par la relation

$$B' = C^t B C \quad \text{pour } C \text{ inversible,}$$

et donc $\det(B') = \det(C)^2 \det(B)$. Autrement dit, le déterminant d'une matrice symétrique associée à un espace quadratique n'en est qu'un *invariant à carré près.*

Pour formaliser cela, remarquons d'abord que $(F^\times, \cdot, 1)$, le groupe multiplicatif du corps F, contient l'ensemble des carrés non-nuls de F, soit $F^{\times 2} = \{a^2 \mid a \in F^\times\}$, qui en est un sous-groupe (exercice). Ces groupes étant commutatifs, on peut bien considérer le groupe quotient $F^\times/F^{\times 2}$; on y identifie donc deux nombres non-nuls de F si et seulement si leur quotient est un carré. D'où maintenant la définition suivante :

Définition 7.3.1 *Le* déterminant *d'un espace régulier* (V, b) *est*

$$\mathrm{d}(V, b) = [\det(B)] \in F^\times/F^{\times 2}$$

pour une (et donc toute) matrice symétrique B *déterminée par* (V, b).

La régularité de (V, b) assure que $\det(B) \neq 0$, et que donc $\mathrm{d}(V, b)$ est bien définie. Si (V, b) n'est pas régulier, on pourrait définir "$\mathrm{d}(V, b) = 0$", mais ceci est sans grand intérêt : nous savons déjà décomposer

$$(V, b) \cong \mathrm{rad}(V, b) \perp (W, b)$$

avec (W, b) régulier, et c'est le déterminant de (W, b) qui est alors intéressant.

Exemple 7.3.2 Pour (V, b) et (V', b') des espaces réguliers, on sait déjà que $(V, b) \perp (V', b')$ est aussi régulier ; et (par exemple par un argument matriciel ; exercice !) on obtient

$$\mathrm{d}\Big((V, b) \perp (V', b')\Big) = \mathrm{d}(V, b) \cdot \mathrm{d}(V', b') \in F^\times/F^{\times 2}.$$

En particulier, pour des $d_i \in F^\times$, on a $\mathrm{d}\langle d_1, ..., d_k\rangle = [d_1 \cdot ... \cdot d_k] \in F^\times/F^{\times 2}$.

Exemple 7.3.3 Pour les espaces (réguliers !) $\langle 3, 2, 1\rangle$ et $\langle 1, 1, 1\rangle$ sur $\mathbb{Q}$, on a

$$\mathrm{d}\langle 3, 2, 1\rangle = [6] \neq [1] = \mathrm{d}\langle 1, 1, 1\rangle \text{ dans } \mathbb{Q}^\times/\mathbb{Q}^{\times 2}.$$

Ces espaces sont donc non-isométriques.

7.4. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Montrer : si une application linéaire $f\colon V \to W$ est surjective, alors $f^*\colon W^* \to V^*$ est injective.

3. Donner le rang et le déterminant de tous les espaces quadratiques rencontrés jusqu'à présent.

4. Montrer que $\langle d\rangle \cong \langle d'\rangle$ si et seulement si $d = a^2 d'$ pour $a \in F^\times$.

5. Donner une démonstration "matricielle" pour la Proposition 7.2.1.

8. Classification des espaces quadratiques complexes, réels et finis

Pour résumer les sections précédentes, lorsqu'on calcule une diagonalisation $(V, b) \cong \langle d_1, ..., d_n \rangle$ d'un espace quadratique donné, on sait que :

- le nombre de zéros parmi les d_i's est toujours le même—la partie nulle correspond au radical de l'espace,
- le nombre de non-zéros parmi les d_i's est aussi toujours le même—la partie non-nulle correspond à la partie régulière de l'espace,
- on peut toujours remplacer un d_i par $a^2 d_i$ (ou $a^{-2} d_i$) pour $a \neq 0$,
- le produit des d_i's non-nuls est toujours le même à carré près.

Cela nous permettra de décrire *tous les espaces quadratiques complexes, réelles et finis*—comme suit.

8.1. Espaces quadratiques complexes

Soit un espace quadratique complexe (V, b) et une diagonalisation

$$(V, b) \cong \langle 0, ..., 0, d_1, ..., d_k \rangle \quad \text{avec } d_i \in \mathbb{C}^\times.$$

Puisqu'on a $d_i = (\sqrt{d_i})^2 \cdot 1$, on peut *simplifier* cette expression (à isométrie près, bien évidemment) :

$$\begin{aligned} (V, b) &\cong \langle 0, ..., 0, d_1, ..., d_k \rangle \\ &\cong \langle 0, ..., 0, (\sqrt{d_1})^2 \cdot 1, ..., (\sqrt{d_k})^2 \cdot 1 \rangle \\ &\cong \langle 0, ..., 0, 1, ..., 1 \rangle \end{aligned}$$

On peut résumer ainsi :

Théorème 8.1.1 *Tout espace quadratique sur $\mathbb{C}$ s'écrit – à isométrie près – comme*

$$\langle 0, ..., 0, 1, ..., 1 \rangle$$

et est ainsi entièrement déterminé par sa dimension et son rang.

En dimension n, il y a donc $n + 1$ classes d'isométrie distinctes d'espaces quadratiques. Par ailleurs, il y a un unique (à isométrie près) espace régulier de dimension n, à savoir $\langle 1, ..., 1 \rangle$.

Remarque 8.1.2 Un corps F est *quadratiquement clos* si tout élément de F est un carré ; c'est bien le cas pour $F = \mathbb{C}$ (mais pas, par exemple, pour $\mathbb{R}$: aucun nombre strictement négatif est un carré !). Le Théorème 8.1.1 est clairement valable pour tout corps quadratiquement clos. Mieux encore, cet énoncé *caractérise* les corps quadratiquement clos ; pour cela, il suffit de noter que $\langle d\rangle \cong \langle 1\rangle$ si et seulement s'il existe $a \in F$ tel que $d = a^2$.

Exemple 8.1.3 Soit la matrice symétrique

$$B = \begin{pmatrix} 1 & i & 1+i \\ i & 2i & 0 \\ 1+i & 0 & 1-i \end{pmatrix} \in \mathbb{C}^{3\times 3}$$

et (V, b) un espace quadratique complexe correspondant. On peut considerer l'application linéaire $\hat{b}\colon V \to V^*$ dont la matrice (pour des bases bien choisies, voir Proposition 4.2.5) est B ; son noyau est le radical de (V, b). Mais cette matrice est de rang 3, son noyau est de dimension 0, et on en déduit que $(V, b) \cong \langle 1, 1, 1\rangle$.

8.2. Espaces quadratiques réelles

Soit un espace quadratique réel (V, b) et une diagonalisation

$$(V, b) \cong \langle 0, ..., 0, d_1, ..., d_k\rangle \quad \text{avec } d_i \in \mathbb{R}^\times.$$

Puisque $\mathbb{R}$ n'est pas quadratiquement clos, on ne peut pas faire le même raisonnement que ci-dessus ; mais il est tout de même vrai que

$$d_i = \begin{cases} (\sqrt{d_i})^2 \cdot 1 & \text{si } d_i \geq 0 \\ (\sqrt{-d_i})^2 \cdot (-1) & \text{si } d_i \leq 0 \end{cases}$$

et donc on peut *simplifier* cette expression (à isométrie près, bien évidemment) :

$$\begin{aligned} (V, b) &\cong \langle 0, ..., 0, d_1, ..., d_k\rangle \\ &\cong \langle 0, ..., 0, (\sqrt{d_1})^2 \cdot (\pm 1), ..., (\sqrt{d_k})^2 \cdot (\pm 1)\rangle \\ &\cong \langle 0, ..., 0, \pm 1, ..., \pm 1\rangle \\ &\cong \langle 0, ..., 0, +1, ..., +1, -1, ..., -1\rangle \end{aligned}$$

Pour passer à la dernière ligne, on a permuté les éléments pour placer d'abord les $+1$'s puis les -1's ; cela est permis puisqu'une telle permutation est isométrique (exercice). Dans cette expression, le nombre de nuls et de non-nuls est invariant—mais qu'en est-il pour le nombre de $+1$'s et le nombre de -1's ?

1. James Joseph Sylvester (1814–1897) a démontré ce résultat en 1852 dans le cadre des polynômes. Il a par ailleurs aussi introduit le mot *matrix* (matrice) en algèbre linéaire.

Proposition 8.2.1 (Loi d'inertie de Sylvester [1]) *Sur le corps $\mathbb{R}$ on a une isométrie de deux espaces*

$$\langle \underbrace{1,...,1}_{r}, \underbrace{-1,...,-1}_{s} \rangle \cong \langle \underbrace{1,...,1}_{r'}, \underbrace{-1,...,-1}_{s'} \rangle$$

si et seulement si $r = r'$ et $s = s'$.

Démonstration. Une implication est évidente. Pour l'autre, on suppose avoir un espace (régulier) (V, b), et deux bases orthogonales $(\underline{e}_1, ..., \underline{e}_n)$ et $(\underline{e}'_1, ..., \underline{e}'_n)$, correspondant aux diagonalisations données ; on a donc

$$b(\underline{e}_i, \underline{e}_i) = \begin{cases} +1 \text{ si } i \leq r \\ -1 \text{ si } i > r \end{cases} \qquad \text{et} \qquad b(\underline{e}'_i, \underline{e}'_i) = \begin{cases} +1 \text{ si } i \leq r' \\ -1 \text{ si } i > r' \end{cases}$$
$$b(\underline{e}_i, \underline{e}_j) = 0 \text{ si } i \neq j \qquad\qquad b'(\underline{e}'_i, \underline{e}'_j) = 0 \text{ si } i \neq j$$

Observons d'abord que la suite $\underline{e}_1, ..., \underline{e}_r, \underline{e}'_{r'+1}, ..., \underline{e}'_n$ est libre. Pour cela, supposons qu'on ait une combinaison linéaire nulle,

$$\sum_{i=1}^{r} x_i \underline{e}_i + \sum_{j=r'+1}^{n} y_i \underline{e}'_j = \underline{0},$$

alors on doit montrer que tous les x_i's et tous les y_i's sont nuls. On peut réécrire cette combinaison linéaire comme

$$\sum_{i=1}^{r} x_i \underline{e}_i = - \sum_{j=r'+1}^{n} y_i \underline{e}'_j$$

puis calculer avec la forme bilinéaire b comme suit :

$$b(\sum_{i=1}^{r} x_i \underline{e}_i, \sum_{i=1}^{r} x_i \underline{e}_i) = \sum_{i,k=1}^{r} x_i x_k b(\underline{e}_i, \underline{e}_k) = \sum_{i=1}^{r} x_i^2 (+1) = \sum_{i=1}^{r} x_i^2$$

$$b(- \sum_{j=r'+1}^{n} y_i \underline{e}'_j, - \sum_{j=r'+1}^{n} y_i \underline{e}'_j) = (-1)(-1) \sum_{j,l=r'+1}^{n} y_j y_l b(\underline{e}'_j, \underline{e}'_l) = \sum_{j=r'+1}^{n} y_j^2 (-1) = - \sum_{j=r'+1}^{n} y_j^2$$

Dans le corps $\mathbb{R}$, tout carré est positif, donc toute somme de carrés est positive, donc l'égalité

$$\sum_{i=1}^{r} x_i^2 = - \sum_{j=r'+1}^{n} y_j^2$$

implique bel et bien $x_1 = ... = x_r = y_{r'+1} = ... = y_n = 0$, comme voulu. Il suit maintenant que $r + (n - r') \leq n$, donc $r \leq r'$; par un même argument on trouve aussi $r \geq r'$; et finalement on a bien sûr aussi $s = n - r = n - r' = s'$. □

Remarque 8.2.2 Le point crucial dans cette démonstration est l'assertion que, dans $F = \mathbb{R}$, "toute somme de carrés est positive". Ceci n'est pas possible dans un corps quelconque—par exemple, il n'y a pas de "nombres positifs" et de "nombres négatifs" dans le corps $\mathbb{C}$, ou dans un corps fini $\mathbb{F}_q$.

Bref, on peut conclure :

Théorème 8.2.3 *Tout espace quadratique sur* $\mathbb{R}$ *s'écrit – à isométrie près – comme*

$$\langle 0, ..., 0, +1, ..., +1, -1, ..., -1 \rangle$$

et est ainsi entièrement déterminé par sa dimension et sa signature *(= le nombre de* $+1$*'s et le nombre de* -1*'s).*

En dimension n, il existe donc $\frac{(n+1)(n+2)}{2}$ classes d'équivalence d'espaces quadratiques réels ; si on se limite aux espaces réguliers, alors il y en a $n+1$ (exercice).

Exemple 8.2.4 Une forme bilinéaire symétrique sur $\mathbb{R}^n$ est un produit scalaire si et seulement si l'espace quadratique (V, b) ainsi obtenu est isométrique à $\langle 1, ..., 1 \rangle$. Dans ce cas, le groupe orthogonal $\mathsf{O}(V, b)$ est isomorphe au groupe orthogonal $\mathsf{O}\langle 1, ..., 1 \rangle$, qui n'est autre que le groupe des matrices réelles orthogonales $n \times n$.

8.3. Espaces quadratiques finis

Notons $\mathbb{F}_p$ le corps à p éléments, pour p un nombre premier ; habituellement on réalise ce corps comme le quotient de l'anneau $\mathbb{Z}$ par l'idéal premier (p). Pour tout $m \in \mathbb{N}_0$ on peut trouver [2] un polynôme irréductible $f \in \mathbb{F}_p[X]$ de degré m, et il suit (par des arguments classiques de l'arithmétique) que

$$\mathbb{F}_q = \mathbb{F}_p[X]/(f)$$

est un corps à $q = p^m$ éléments. Concrètement, les éléments de $\mathbb{F}_q$ sont "les restes après division euclidienne par f dans $\mathbb{F}_p[X]$" : ce sont donc exactement les polynômes de degré strictement inférieur à m, avec la somme habituelle mais avec le produit modulo f. Rappelons enfin que, pour la théorie des formes quadratiques, puisqu'on veut des corps de caractéristique différent de 2, on prendra pour p un nombre premier impair.

Exemple 8.3.1 Le corps $\mathbb{F}_9$ à $9 = 3^2$ éléments peut être réalisé par le quotient de $\mathbb{F}_3[X]$ par un polynôme irréductible $f \in \mathbb{F}_3[X]$ de degré 2. On vérifie que, par exemple, $f(X) = X^2 + 1$ n'a aucune racine sur $\mathbb{F}_3$, et est donc irréductible. On peut ensuite identifier les éléments de $\mathbb{F}_9$ avec les polynômes

$$\begin{aligned} a_0 &= 0X + 0, \quad a_1 = 0X + 1, \quad a_2 = 0X + 2, \\ a_3 &= 1X + 0, \quad a_4 = 1X + 1, \quad a_5 = 1X + 2, \\ a_6 &= 2X + 0, \quad a_7 = 2X + 1, \quad a_8 = 2X + 2. \end{aligned}$$

La somme des éléments dans $\mathbb{F}_9$ correspond alors à la somme des polynômes (mais pour les coefficients on travaille dans $\mathbb{F}_3$ bien sûr) ; donc par exemple $a_3 + a_5 = a_8$, ou encore $a_2 + a_7 = a_6$, etc. Le produit des éléments dans $\mathbb{F}_9$ correspond au produit des polynômes modulo $f = X^2 + 1$; par exemple, $a_4 \cdot a_7 \equiv (X+1)(2X+1) \equiv 2X^2 + 3X + 1 \equiv 2X^2 + 1 \equiv 2 \equiv a_2$.

2. Malheureusement, il n'y a pas de "formule magique" pour produire un tel polynôme—c'est souvent une question de *trial and error* à l'aide d'un ordinateur.

Soit maintenant un espace quadratique fini [3] (V, b) et une diagonalisation

$$(V, b) \cong \langle 0, ..., 0, d_1, ..., d_k \rangle \quad \text{avec } d_i \in \mathbb{F}_q^\times.$$

Pour simplifier la partie régulière de cet espace, on va devoir s'intéresser aux carrés dans $\mathbb{F}_q$—ou mieux dit, à l'égalité des éléments de $\mathbb{F}_q^\times$ à carré près. Pour le corps $\mathbb{C}$, tout élément est un carré ; pour le corps $\mathbb{R}$, tout élément est un carré "à signe près" ; pour les corps finis, on a le résultat suivant :

Proposition 8.3.2 *On peut écrire tout $x \in \mathbb{F}_q^\times$ comme*

$$\begin{cases} \text{soit } x = y^2 \cdot 1 \\ \text{soit } x = y^2 \cdot \varepsilon \end{cases}$$

où $\varepsilon \in \mathbb{F}_q^\times$ n'est pas un carré.

Démonstration. Soit un corps quelconque F ; le groupe multiplicatif $(F^\times, \cdot, 1)$ contient le sous-groupe $F^{\times 2}$ des carrés, et $\gamma \colon F^\times \to F^{\times 2} \colon x \mapsto x^2$ est un homomorphisme surjectif de groupes (exercice). Si $\mathrm{car}(F) \neq 2$, on a $\ker(\gamma) = \{x \in F^\times \mid x^2 = 1\} = \{+1, -1\}$, et donc

$$F^{\times 2} \cong F^\times / \ker(\gamma) = F^\times / \{+1, -1\}.$$

Supposons pour la suite que $F = \mathbb{F}_q$ et q est impair ; alors on peut compter les éléments dans ces groupes (exercice) :

$$\left|\mathbb{F}_q^{\times 2}\right| = \frac{\left|\mathbb{F}_q^\times\right|}{|\{+1, -1\}|} = \frac{q-1}{2}.$$

Autrement dit, parmi les $q-1$ éléments de $\mathbb{F}_q^\times$, il y a $\frac{q-1}{2}$ carrés. Mais on a donc aussi

$$\left|\mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}\right| = \frac{\left|\mathbb{F}_q^\times\right|}{\left|\mathbb{F}_q^{\times 2}\right|} = \frac{q-1}{\frac{q-1}{2}} = 2.$$

Ainsi, "modulo carrés", il y a exactement deux éléments dans $\mathbb{F}_q^\times$. Sûrement $1 \in \mathbb{F}_q^\times$ est toujours un carré ; et on peut donc toujours trouver (au moins) un non-carré $\varepsilon \in \mathbb{F}_q^\times$. Ainsi, tout $x \in \mathbb{F}_q^\times$ est soit dans la classe $[1] \in \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}$, soit dans la classe $[\varepsilon] \in \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}$, et c'est le résultat annoncé. □

Maintenant on peut *simplifier* (à isométrie près, bien évidemment) la diagonalisation d'un espace quadratique sur $\mathbb{F}_q$:

$$\begin{aligned} (V, b) &\cong \langle 0, ..., 0, d_1, ..., d_k \rangle \\ &\cong \langle 0, ..., 0, (1 \text{ ou } \varepsilon), ..., (1 \text{ ou } \varepsilon) \rangle \\ &\cong \langle 0, ..., 0, 1, ..., 1, \varepsilon, ..., \varepsilon \rangle \end{aligned}$$

3. Soulignons qu'un espace vectoriel V est fini si et seulement si V est un espace de dimension finie sur un corps fini.

où on a d'abord remplacé chaque d_i par 1 (si d_i est un carré) ou ε (si d_i n'est pas un carré), puis on a permuté pour écrire les 1's avant les ε's. Notons que, par la Proposition ci-dessus, tout non-carré $\varepsilon \in \mathbb{F}_q^\times$ est, à carré près, égal à tout autre non-carré $\delta \in \mathbb{F}_q^\times$; la forme ci-dessus est donc aussi isométrique à $\langle 0, ..., 0, 1, ..., 1, \delta, ..., \delta\rangle$, le *choix* du non-carré est ainsi sans importance. Dans cette expression, le nombre de nuls est invariant ; mais qu'en est-il pour le nombre de 1's et de ε's ? On s'est déjà posé la question pour les espaces quadratiques réels, et dans la démonstration on a utilisé un argument basé sur "une somme de carrés". Aussi dans le cas fini on doit s'y intéresser :

Proposition 8.3.3 *Tout élément de $\mathbb{F}_q$ est une somme de deux carrés.*

Démonstration. Soit $x \in \mathbb{F}_q$, et notons

$$(\mathbb{F}_q)^2 = \{a^2 \mid a \in \mathbb{F}_q\} = \mathbb{F}_q^{\times 2} \cup \{0\} \quad \text{et} \quad x - (\mathbb{F}_q)^2 = \{x - a^2 \mid a \in \mathbb{F}_q\}.$$

Il suit par la Proposition 8.3.2 que $|\mathbb{F}_q| = q$ et $\left|(\mathbb{F}_q)^2\right| = \left|\mathbb{F}_q^{\times 2}\right| + 1 = \frac{q-1}{2} + 1 = \frac{q+1}{2}$, et par la bijection évidente

$$\begin{array}{ccc} x - (\mathbb{F}_q)^2 & \overrightarrow{\longleftarrow} & (\mathbb{F}_q)^2 \\ s & \longmapsto & -(s-x) \\ x - t & \longleftarrow\!\shortmid & t \end{array}$$

on a également que $\left|x - (\mathbb{F}_q)^2\right| = \left|(\mathbb{F}_q)^2\right| = \frac{q+1}{2}$. Par conséquent, l'intersection des sous-ensembles $x - (\mathbb{F}_q)^2$ et $(\mathbb{F}_q)^2$ de $\mathbb{F}_q$ est non-vide. Soit donc $y \in \left(x - (\mathbb{F}_q)^2\right) \cap \left((\mathbb{F}_q)^2\right)$, alors $y = x - a^2$ et $y = b^2$ pour certains $a, b \in \mathbb{F}_q$, d'où le résultat : $x = a^2 + b^2$. □

Voici une conséquence de cette Proposition :

Proposition 8.3.4 *Pour tout non-carré $\varepsilon \in \mathbb{F}_q$ on a $\langle 1, 1\rangle \cong \langle \varepsilon, \varepsilon\rangle$.*

Démonstration. Par la Proposition 8.3.3, le non-carré $\varepsilon \in \mathbb{F}_q$ est une somme de carrés, et donc ε est une valeur représentée par (l'espace quadratique réalisant) la forme quadratique régulière $q(x, y) = x^2 + y^2$ (sur le corps $\mathbb{F}_q$) : $\varepsilon \in D\langle 1, 1\rangle$. Par la Proposition 6.1.5 on sait qu'il existe une diagonalisation $\langle \varepsilon, d\rangle \cong \langle 1, 1\rangle$, pour un certain $d \in \mathbb{F}_q^\times$. Pour ce nombre non-nul on a soit $[d] = [1] \in \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$ (si d est un carré), soit $[d] = [\varepsilon] \in \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$ (si d n'est pas un carré) ; la forme $\langle \varepsilon, d\rangle$ est donc (à isométrie près) soit $\langle \varepsilon, \varepsilon\rangle$, soit $\langle \varepsilon, 1\rangle$. Mais l'isométrie $\langle \varepsilon, 1\rangle \cong \langle 1, 1\rangle$ est impossible : ces deux espaces n'ont pas le même déterminant (à carré près !). On a donc $\langle \varepsilon, \varepsilon\rangle = \langle 1, 1\rangle$, comme annoncé. □

Ainsi, dans la diagonalisation

$$(V, b) \cong \langle 0, ..., 0, 1, ..., 1, \varepsilon, ..., \varepsilon\rangle$$

on peut remplacer chaque occurrence *paire* de ε's par des 1's ; et donc la diagonalisation se simplifie de la manière suivante :

$$(V, b) \cong \begin{cases} \langle 0, ..., 0, 1, ..., 1\rangle & \text{si il y avait un nombre paire de } \varepsilon\text{'s} \\ \langle 0, ..., 0, 1, ..., 1, \varepsilon\rangle & \text{si il y avait un nombre impaire de } \varepsilon\text{'s} \end{cases}$$

Remarquons finalement que les espaces réguliers $\langle 1, ..., 1\rangle$ et $\langle 1, ..., 1, \varepsilon\rangle$ (de même dimension) ne sont pas isométriques : leurs déterminants respectifs ne sont bien évidemment pas égaux ! Résumons donc ainsi :

Théorème 8.3.5 *Tout espace quadratique sur $\mathbb{F}_q$ s'écrit – à isométrie près – comme*

$$\textit{soit } \langle 0, ..., 0, 1, ..., 1\rangle, \quad \textit{soit } \langle 0, ..., 0, 1, ..., 1, \varepsilon\rangle$$

(où $\varepsilon \in \mathbb{F}_q^\times$ est un non-carré au choix), et est donc entièrement déterminé par sa dimension, son rang et le déterminant de sa partie régulière.

En dimension n il y a ainsi $2n + 1$ classes d'isométrie d'espaces quadratiques sur $\mathbb{F}_q$, dont il y a seulement 2 classes d'espaces quadratiques réguliers (exercice). Il est remarquable que la caractéristique p du corps $\mathbb{F}_q = \mathbb{F}_{p^m}$ est sans importance pour cette classification !

Exemple 8.3.6 On reprend le corps $\mathbb{F}_9$ avec les notations de l'Exemple 8.3.1. Les quatre carrés non-nuls dans ce corps sont $\mathbb{F}_9^{\times 2} = \{a_1 = a_1^2 = a_2^2, a_2 = a_3^2 = a_6^2, a_3 = a_5^2 = a_7^2, a_6 = a_4^2 = a_8^2\}$; ainsi on peut prendre $\varepsilon = a_4$ comme non-carré non-nul (ce choix étant totalement arbitraire). Les espaces quadratiques réguliers de dimension 5 sur $\mathbb{F}_9$ sont $\langle 1, 1, 1, 1, 1\rangle$ et $\langle 1, 1, 1, 1, a_4\rangle$ (à isométrie près, évidemment).

8.4. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Soit un groupe $G = (G, \cdot, 1)$ et un sous-groupe normal $N \trianglelefteq G$. Montrer que $|G| = |G/N| \cdot |N|$. *Solution.* Les éléments de G/N sont les classes d'équivalence pour la relation d'équivalence $g_1 \sim g_2 \iff g_1 g_2^{-1} \in N$; on les note souvent gN (et on les appelle les "classes latérales de N dans G"). Comme pour toute relation d'équivalence, ces classes forment une partition de G. Par la bijection $N \to gN : n \mapsto gn$ on voit que toute classe latérale gN (donc tout élément de G/N) a la même cardinalité que N. Ainsi il suit que $|G| = |\uplus_{\mathcal{X} \in G/N} \mathcal{X}| = |G/N| \cdot |N|$. (Bien sûr, si G est fini, aussi N et G/N sont finis, et ceci est une égalité de nombres naturels.)

3. Pour F un corps quelconque,
   (a) montrer que $q : F^{n\times n} \to F : M \to \mathrm{tr}(M^2)$ est une forme quadratique,
   (b) calculer la forme bilinéaire symétrique associée, soit $b : F^{n\times n} \times F^{n\times n} \to F$,
   (c) monter que l'espace quadratique $(F^{n\times n}, b)$ est la somme orthogonale du sous-espace des matrices symétriques avec le sous-espace des matrices anti-symétriques,
   (d) montrer que, sur le sous-espace $W \subseteq F^{3\times 3}$ des matrices de trace nulle, l'espace quadratique (W, b) est isométrique à $\langle -1, -1, -1, 1, 1, 1, 2, 6\rangle$,
   (e) donner la "forme diagonale simplifiée" de (W, b) si $F = \mathbb{C}$, si $F = \mathbb{R}$ et si $F = \mathbb{F}_{13}$.

4. Déterminer si les formes quadratiques suivantes sont isométriques :
   (a) $q(x, y, z) = \frac{1}{2}x^2 + 3xy - yz$ et $\langle 1, 2, 3\rangle$ sur $\mathbb{Q}$.

(b) $\langle 1, 2, 3\rangle$ et $\langle 8, 13, 5\rangle$ sur $\mathbb{R}$,

(c) $\langle 1, 2, 3\rangle$ et $\langle 8, 13, 5\rangle$ sur $\mathbb{Q}$,

(d) $\langle 1, 2, 3\rangle$ et $\langle -1, 2, 3\rangle$ sur $\mathbb{R}$,

(e) $\langle 1, 2, 3\rangle$ et $\langle -1, -2, 3\rangle$ sur $\mathbb{R}$,

(f) $\langle 1, 1\rangle$ et $\langle 1, -1\rangle$ sur $\mathbb{F}_{11}$,

(g) $\langle 1, 1\rangle$ et $\langle 1, -1\rangle$ sur $\mathbb{F}_{13}$.

5. Soient (V, b) et (V', b') deux espaces quadratiques réguliers de dimension 2 sur un corps F quelconque. Montrer l'équivalence des assertions suivantes :

(a) $(V, b) \cong (V', b')$,

(b) $\mathrm{d}(V, b) = \mathrm{d}(V', b')$ et $D(V, b) = D(V', b')$,

(c) $\mathrm{d}(V, b) = \mathrm{d}(V', b')$ et $D(V, b) \cap D(V', b') \neq \emptyset$.

Qu'en est-il pour des espaces réguliers de dimension plus grand que 2 (p.e. sur le corps $F = \mathbb{R}$) ?

6. Donner la "forme diagonale simplifiée" pour les espaces quadratiques complexes, réels ou finis rencontrés lors des exercices précédents.

9. Isotropie et plans hyperboliques

9.1. Espaces hyperboliques

Le produit scalaire usuel sur $\mathbb{R}^n$ (ou tout autre produit scalaire—cela donnera le "même" espace quadratique, cf. Exemple 8.2.4) se distingue d'une forme bilinéaire symétrique générale par sa *stricte positivité* :

(a) le produit scalaire d'un vecteur avec lui-même est toujours positif [1],

(b) le seul vecteur de norme nulle est le vecteur nul.

Pour un F-espace quadratique (V, q) quelconque, l'assertion (a) n'a aucun sense, puisqu'elle dépend de l'existence d'un ordre sur F, ce qui n'est pas le cas en général. C'est bien différent pour l'assertion (b) : il est parfaitement légitime d'étudier les $\underline{x} \in V$ pour lesquels $q(\underline{x}) = 0$. On pose les définitions suivantes :

Définition 9.1.1 *Soit (V, q) un espace quadratique. On dit que :*

1. *un vecteur $\underline{x} \in V \setminus \{\underline{0}\}$ est* isotrope *si $q(\underline{x}) = 0$ (et sinon $\underline{x}$ est* anisotrope*),*
2. *l'espace (V, q) est* isotrope *s'il contient un vecteur isotrope (et sinon (V, q) est* anisotrope*),*
3. *un sous-espace vectoriel $W \subseteq V$ est* totalement isotrope *si tout $\underline{x} \in W \setminus \{\underline{0}\}$ est isotrope.*

Clairement, un sous-espace vectoriel $W \subseteq V$ est totalement isotrope si et seulement si la restriction de la forme quadratique $q\colon V \to F$ à W est la forme nulle. Autrement dit, en tant que sous-espace quadratique, $(W, q_{|W})$ est équipé de la forme nulle.

Un vecteur non-nul $\underline{x}$ est isotrope dans (V, b) si et seulement si le sous-espace $F\underline{x} \subseteq V$ est totalement isotrope (exercice). Mais il est *faux* qu'un sous-espace $W \subseteq V$ ayant une base de vecteurs isotropes est nécessairement totalement isotrope !

Exemple 9.1.2 Soit la matrice symétrique

$$B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in \mathbb{R}^{3\times 3},$$

alors on peut réaliser, par le choix d'une base $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ de $\mathbb{R}^3$, un espace quadratique $(\mathbb{R}^3, b)$ ayant B pour matrice associée. Chaque vecteur de cette base est alors isotrope, mais l'espace $(\mathbb{R}^3, b)$ n'est pas totalement isotrope (car la forme n'est pas nulle).

1. On utilise ce terme pour "plus grand ou égal à zéro".

La restriction de la forme quadratique $q\colon V \to F$ au radical de l'espace (V,q) est toujours la forme nulle ; si le radical est non-nul, il contient donc des vecteurs isotropes. Ainsi, un espace non-régulier est toujours isotrope, et un espace anisotrope est toujours régulier. *Le sujet intéressant est donc celui des espaces réguliers isotropes !* Par ailleurs, tout espace quadratique (V,q) peut être décomposé en une partie nulle et une partie régulière :

$$(V,q) \cong (\mathrm{rad}(V,q),q) \perp (W,q).$$

Le radical est totalement isotrope ; et le but est maintenant d'étudier l'isotropie de la partie régulière (W,q). Pour cela, certains espaces de dimension 2 vont jouer un rôle crucial.

Théorème 9.1.3 *Pour un espace quadratique (V,b) de dimension 2, on a l'équivalence des assertions suivantes :*

1. *(V,b) est régulier et isotrope,*
2. *(V,b) est (régulier et) de déterminant $[-1] \in F^\times/F^{\times 2}$,*
3. *$(V,b) \cong \langle d,-d\rangle$ pour tout $d \in F^\times$,*
4. *$(V,b) \cong \langle 1,-1\rangle$,*
5. *$(V,b) \cong (F^2, q(x,y)=xy)$.*

Démonstration. (1⇒2) Soit une diagonalisation $(V,b) \cong \langle d_1,d_2\rangle$ par une base orthogonale $(\underline{e}_1,\underline{e}_2)$ de V, alors $d_1,d_2 \in F^\times$ par régularité de (V,b). Soit un vecteur isotrope $\underline{x}$ dans V ; on peut l'écrire comme $\underline{x} = x_1\underline{e}_1 + x_2\underline{e}_2$ et calculer alors que

$$0 = q(\underline{x}) = b(x_1\underline{e}_1 + x_2\underline{e}_2, x_1\underline{e}_1 + x_2\underline{e}_2) = \sum_{i,j} x_i x_j b(\underline{e}_i,\underline{e}_j) = d_1x_1^2 + d_2x_2^2.$$

Puisque (comme tout vecteur isotrope) $\underline{x} \neq \underline{0}$ on a $(x_1,x_2) \neq (0,0)$; supposons que $x_1 \neq 0$ (sinon on échange les vecteurs de la base). Il suit alors que

$$d_1 = -\frac{x_2^2}{x_1^2}d_2$$

et donc $(V,b) \cong \langle d_1,d_2\rangle \cong \langle -d_2,d_2\rangle$ dont le déterminant est $[-d_2d_2] = [-d_2^2] = [-1] \in F^\times/F^{\times 2}$. (2)⇒(3) Soit une diagonalisation $(V,b) \cong \langle d_1,d_2\rangle$, alors $d_1,d_2 \in F^\times$ par régularité de (V,b). On peut raisonner comme suit :

$$\begin{aligned}
\mathrm{d}(V,b) = [-1] &\iff [d_1d_2] = [-1] \\
&\iff d_1d_2 = -a^2 \text{ (pour } a \in F^\times) \\
&\iff d_2 = -\frac{a^2}{d_1^2}d_1 \\
&\implies [d_2] = [-d_1]
\end{aligned}$$

et donc $\langle d_1,d_2\rangle = \langle d_1,-d_1\rangle$. On veut encore montrer que l'on peut prendre $d_1 = d$ pour n'importe quel $d \in F^\times$; pour cela il suffit de montrer que tout $d \in F^\times$ est une valeur représentée par $(V,b) \cong \langle d_1,-d_1\rangle$: car si $d \in D(V,b)$ alors il vient par le Critère de Représentation que $(V,b) \cong$

$\langle d, d'\rangle$ (pour un certain $d' \in F^\times$) et l'argument ci-dessus implique alors $(V,b) \cong \langle d, -d\rangle$. Mais remarquons que le polynôme $f(X_1, X_2) = d_1X_1^2 - d_1X_2^2$ associé à l'espace $\langle d_1, -d_1\rangle$ est équivalent, par le changement linéaire inversible de variables

$$\begin{cases} Y_1 = X_1 + X_2 \\ Y_2 = X_1 - X_2 \end{cases}$$

au polynôme $g(Y_1, Y_2) = d_1Y_1Y_2$. Ce polynôme g peut, à son tour, être réalisé par l'espace quadratique $(F^2, q'(y_1, y_2) = d_1y_1y_2)$, nécessairement isométrique à $\langle d_1, -d_1\rangle$. Se souvenant que $d_1 \in F^\times$, on a

$$D\langle d_1, -d_1\rangle = D(F^2, q') = \{a \in F^\times \mid \exists (y_1, y_2) \in F^2 : d_1y_1y_2 = a\} = F^\times$$

et donc tout $d \in F^\times$ est une valeur représentée par $\langle d_1, -d_1\rangle$.
(3)⇒(4) Trivial.
(4)⇒(1) La régularité de $\langle 1, -1\rangle = (F^2, q(x,y) = x^2 - y^2)$ est évident par considération de la matrice diagonale associée ; et clairement le vecteur $(1,1) \in F^2$ est isotrope.
(4)⇔(5) L'isométrie $\langle 1, -1\rangle = (F^2, q(x,y) = x^2 - y^2) \cong (F^2, q'(x,y) = xy)$ suit par l'équivalence des polynômes $f(X,Y) = X^2 - Y^2$ et $g(X,Y) = XY$ (comme ci-dessus). □

Ces propriétés équivalentes remarquables méritent d'être soulignées par :

Définition 9.1.4 *Un espace quadratique (V,b) est un* plan hyperbolique[2] *si $(V,b) \cong \langle 1, -1\rangle$, et plus généralement un* espace hyperbolique *si (V,b) est une somme orthogonale de plans hyperboliques.*

Exemple 9.1.5 Reprenons les notations de l'Exercice 8.3.1. Le déterminant de la matrice symétrique

$$B = \begin{pmatrix} a_4 & a_5 \\ a_5 & a_3 \end{pmatrix} \in \mathbb{F}_9^{2\times 2}.$$

est $a_4a_3 - a_5a_5 \equiv (X+1)X - (X+2)^2 \equiv 2$ dans $\mathbb{F}_9$; tout espace quadratique (V,b) realisant cette matrice est donc régulier. Mais alors $\mathrm{d}(V,b) = [2] = [-1]$ dans $\mathbb{F}_9^\times/\mathbb{F}_9^{\times 2}$, donc cet espace (de dimension 2, évidemment) est un plan hyperbolique.

Revenons un instant sur une conséquence du Théorème 9.1.3. Par un argument donné dans sa démonstration on sait que, si (V,b) est un plan hyperbolique, alors $D(V,b) = D\langle 1, -1\rangle = F^\times$. Formulons de manière générale :

Définition 9.1.6 *Un espace quadratique (V,b) est* universel *si $D(V,b) = F^\times$.*

Exemple 9.1.7 Pour tout espace hyperbolique (V,b) on a

$$D(V,b) = D(\langle 1, -1\rangle \perp ... \perp \langle 1, -1\rangle) \supseteq D\langle 1, -1\rangle = F^\times,$$

ce qui dit donc que tout espace hyperbolique est universel—mais la réciproque n'est pas vraie : l'espace $\langle 1\rangle$ sur $\mathbb{C}$ est (régulier et) universel mais pas hyperbolique.

2. Cette terminologie est inspirée par le polynôme $f(X,Y) = XY$ dont les courbes de niveau sont des hyperboles.

9.2. Décomposition de Witt

Le Théorème 9.1.3 dit en particulier que tout plan hyperbolique est isotrope ; a fortiori, tout espace hyperbolique est isotrope (exercice). En fait, le lien entre isotropie et plans hyperboliques est extrêmement fort :

Proposition 9.2.1 *Un espace quadratique régulier (V, b) est isotrope si et seulement s'il existe une décomposition $(V, b) \cong \langle 1, -1\rangle \perp (V', b')$.*

Démonstration. Supposons d'abord que (V, b) est régulier et $(V, b) \cong \langle 1, -1\rangle \perp (V', b')$. Ainsi, $V \cong F^2 \oplus V'$ et le vecteur $\underline{x} \in V$ qui correspond avec $(1, 1) + \underline{0} \in F^2 \oplus V'$ est isotrope. Réciproquement, supposons que (V, b) est régulier et que $\underline{x}$ en est un vecteur isotrope ; on sait donc que $\underline{x} \neq \underline{0}$ et $q(\underline{x}) = b(\underline{x}, \underline{x}) = 0$. L'espace V contient certainement un $\underline{y} \neq \underline{0}$ tel que $b(\underline{x}, \underline{y}) \neq 0$; car sinon la forme b serait nulle partout sur V est donc (V, b) ne serait pas régulier. Les vecteurs $\underline{x}$ et $\underline{y}$ sont linéairement indépendants : si $\alpha\underline{x} + \beta\underline{y} = \underline{0}$ dans V alors on a d'un côté

$$b(\underline{x}, \alpha\underline{x} + \beta\underline{y}) = \alpha b(\underline{x}, \underline{x}) + \beta b(\underline{x}, \underline{y}) = \beta b(\underline{x}, \underline{y})$$

mais de l'autre côté aussi

$$b(\underline{x}, \alpha\underline{x} + \beta\underline{y}) = b(\underline{x}, \underline{0}) = 0,$$

et puisque $b(\underline{x}, \underline{y}) \neq 0$ on a nécessairement $\beta = 0$; et donc aussi $\alpha\underline{x} = \underline{0}$ ce qui implique $\alpha = 0$. Ainsi, on peut engendrer le sous-espace $W = F\underline{x} \oplus F\underline{y}$ de dimension 2 de V. Ce sous-espace $W \subseteq V$ est, en fait, régulier : en effet, pour la matrice symétrique de la restriction de b à W pour la base $(\underline{x}, \underline{y})$ on a

$$\det \begin{pmatrix} 0 & b(\underline{x}, \underline{y}) \\ b(\underline{y}, \underline{x}) & b(\underline{y}, \underline{y}) \end{pmatrix} = -b(\underline{x}, \underline{y})^2 \neq 0$$

Ainsi $W = F\underline{x} \oplus F\underline{y}$ est un espace régulier de dimension 2 contenant un vecteur isotrope— et par le Théorème 9.1.3 on sait que $W \cong \langle 1, -1\rangle$. Finalement, le sous-espace (W, b) étant régulier, on peut utiliser la Proposition 5.1.3 pour conclure que $V = W \perp W^{\perp}$, ou encore $(V, b) \cong \langle 1, -1\rangle \perp (V', b')$ si on pose $(V', b') = (W^{\perp}, b)$. □

Exemple 9.2.2 Sur le corps $\mathbb{R}$, les espaces quadratiques réguliers sont – à isométrie près – donnés par $\langle 1, ..., 1, -1, ..., -1\rangle$; les seuls espaces réguliers isotropes sont donc ceux qui ont au moins un $+1$ et un -1. Autrement dit, les seuls espaces régulieres anisotropes sont isométriques à $\langle 1, ..., 1\rangle$ ou à $\langle -1, ..., -1\rangle$ (les produits scalaires et leurs opposés).

Exemple 9.2.3 Si on pose

$$b((x_1, ..., x_4), (y_1, ..., y_4)) = \begin{pmatrix} x_1 & \cdots & x_4 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_4 \end{pmatrix}$$

alors $(\mathbb{R}^4, b)$ est un espace quadratique réel dont la matrice par rapport à la base canonique est B. On peut vérifier que $\underline{x} = (1-\sqrt{3}, \sqrt{3}-1, 0, 1)$ est un vecteur isotrope, et que $\underline{y} = (1, 1, 1, 1)$ est

un vecteur tel que $b(\underline{x},\underline{y}) = 7 - 3\sqrt{3} \neq 0$ (et, par ailleurs, $b(\underline{y},\underline{y}) = 12$). On voit clairement que $\underline{x}$ et $\underline{y}$ sont linéairement indépendants ; ils engendrent donc un plan $W = \{\alpha\underline{x} + \beta\underline{y} \mid \alpha, \beta \in \mathbb{R}\}$ dans $\mathbb{R}^4$, et la restriction de b à ce plan W est

$$b(\alpha_1\underline{x} + \beta_1\underline{y}, \alpha_2\underline{x} + \beta_2\underline{y}) = (7 - 3\sqrt{3})(\alpha_1\beta_2 + \beta_2\alpha_2) + 12\beta_1\beta_2.$$

Prenons $(\underline{x},\underline{y})$ comme base pour W ; la matrice symétrique de la restriction de b à W est alors

$$\begin{pmatrix} 0 & \frac{7-3\sqrt{3}}{2} \\ \frac{7-3\sqrt{3}}{2} & 12 \end{pmatrix}$$

dont le déterminant est strictement négatif dans $\mathbb{R}$, donc dans la classe $[-1]$ dans $\mathbb{R}^\times/\mathbb{R}^{\times 2}$. L'espace (W, b) est donc bel et bien un plan hyperbolique, donc isométrique à $\langle 1, -1\rangle$; et on peut décomposer $(\mathbb{R}^4, b) \cong \langle 1, -1\rangle \perp W^\perp$. (Il faut du courage pour calculer explicitement cet orthocomplément—mais en théorie c'est parfaitement possible !)

Si $(V, b) \cong \langle 1, -1\rangle \perp (V', b')$ est un espace régulier, alors bien évidemment (V', b') est un espace régulier de dimension $\dim(V') = \dim(V) - 2$. Si (V', b') est toujours isotrope, alors on peut à nouveau le décomposer : $(V', b') \cong \langle 1, -1\rangle \perp (V'', b'')$; sinon, (V', b') est anisotrope. Par induction sur la dimension de (V, b) on obtient ainsi :

Proposition 9.2.4 *Pour tout espace quadratique régulier (V, b) on a une décomposition*

$$(V, b) \cong \langle 1, -1\rangle \perp ... \perp \langle 1, -1\rangle \perp (V', b')$$

en $k \geq 0$ plans hyperboliques et un espace anisotrope (V', b').

Mais nous savons déjà que tout espace (V, b) admet une décomposition

$$(V, b) \cong (\mathrm{rad}(V, b), b) \perp (V', b')$$

en une partie nulle et une partie régulière ; avec la proposition précédente on peut conclure :

Théorème 9.2.5 (Décomposition de Witt) *Pour tout espace quadratique (V, b) on a une décomposition*[3]

$$(V, b) \cong (\mathrm{rad}(V, b), b) \perp \langle 1, -1\rangle \perp ... \perp \langle 1, -1\rangle \perp (V', b')$$

en une partie totalement isotrope, une partie hyperbolique, et une partie anisotrope : c'est la décomposition de Witt *de l'espace (V, b).*

Nous savons déjà que la partie totalement isotrope (le radical) est invariant sous isométrie (par la Proposition 5.1.6)—mais qu'en est-il pour la partie hyperbolique et pour la partie anistrope ? On consacrera l'entière section suivante à cette question.

3. Bien entendu, chacune de ces parties peut être nul !

9.3. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Montrer que $W \subseteq V$ est un sous-espace totalement isotrope d'un espace quadratique (V, b) si et seulement si $W \subseteq W^{\perp}$. Montrer que $\mathrm{rad}(V, b)$ est un sous-espace totalement isotrope. Donner un exemple d'un sous-espace totalement isotrope non-trivial d'un espace régulier.

3. *Paire hyperbolique.* Pour un espace régulier (V, b), montrer l'équivalence de :

   (a) (V, b) est isotrope,

   (b) il existe des vecteurs isotropes (nécessairement indépendants) $\underline{x}, \underline{y} \in V$ tel que $b(\underline{x}, \underline{y}) = 1$; c'est une *paire hyperbolique* dans V,

Montrer que, dans ce cas, le sous-espace $F\underline{x} \oplus F\underline{y}$ est un plan hyperbolique. Quelle est la matrice symétrique de la restriction de b à ce sous-espace pour la base $(\underline{x}, \underline{y})$? Quelle est le polynôme homogène de degré 2 (toujours pour cette base) ?
Indication : Une implication est triviale. Pour l'autre soit $\underline{x}$ un vecteur isotrope ; par régularité de (V, b) il existe un $\underline{y_0} \neq \underline{0}$ tel que $b(\underline{x}, \underline{y_0}) \neq 0$, et il suit que $\underline{x}$ et $\underline{y_0}$ sont indépendants. Soit alors $\underline{y} = \alpha\underline{x} + \beta\underline{y_0}$; on déterminera α et β par les conditions que $b(\underline{x}, \underline{y}) = 1$ et $b(\underline{y}, \underline{y}) = 0$.

4. Soit (V, b) un espace quadratique régulier isotrope de dimension 2 (et donc un plan hyperbolique). Montrer que les seuls vecteurs isotropes de (V, b) sont les multiples non-nuls de $\underline{x}$ et de $\underline{y}$, une paire hyperbolique.

5. *Base de vecteurs isotropes.* Pour un espace régulier (V, b), montrer l'équivalence de :

   (a) (V, b) est isotrope,

   (b) il existe une base de vecteurs isotropes.

Indication : si (V, b) est régulier et isotrope, alors $(V, b) = \langle 1, -1\rangle \perp (V', b')$. Soit $\underline{x}, \underline{y}$ une paire hyperbolique pour $\langle 1, -1\rangle$ (cf. un exercice précédent), et $\underline{e_1}, ..., \underline{e_n}$ une base (quelconque) de (V', b'). Par l'universalité de $\langle 1, -1\rangle$ on peut "adjuster" les vecteurs $\underline{e_i}$ pour en faire des vecteurs isotropes $\underline{e_i'}$ tout en s'assurant que la suite $\underline{x}, \underline{y}, \underline{e_1'}, ..., \underline{e_n'}$ soit toujours libre.

6. Utiliser la décomposition de Witt pour montrer que tout espace régulier isotrope est universel. Montrer que la réciproque n'est pas vraie.

7. Soit $r, s \in F^{\times}$ et $q\colon V \to F$ une forme quadratique régulière. Montrer que :

   (a) $r \in D(V, q)$ si et seulement si $(V, q) \perp \langle -r\rangle$ est isotrope.

   (b) $r \in D((V, q) \perp \langle -s\rangle)$ si et seulement si $s \in D((V, q) \perp \langle -r\rangle)$.

8. Sur le corps $\mathbb{F}_5$, soit V l'espace des matrices 2×2 muni de la forme bilinéaire symétrique $b(M, N) = \mathrm{tr}(MN)$.

   (a) Pour $X = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, construire une paire hyperbolique X, Y dans (V, b).

   (b) Calculer l'orthocomplément dans (V, b) du sous-espace engendré par X et Y.

   (c) Calculer la forme diagonale simplifiée de (V, b).

   (d) En déduire la décomposition de Witt de (V, b).

10. Simplification et décomposition de Witt

10.1. Les théorèmes de Witt

Pour répondre à la question posée en fin de la section précédente, nous allons démontrer le résultat suivant :

Théorème 10.1.1 (Simplification de Witt) *Pour des espaces quadratiques (V, b), (V_1, b_1) et (V_2, b_2) quelconques, si $(V, b) \perp (V_1, b_1) \cong (V, b) \perp (V_2, b_2)$ alors $(V_1, b_1) \cong (V_2, b_2)$.*

Dans la Proposition 5.2.6 nous avons vu que la somme orthogonale d'espaces quadratiques est une opération associative, commutative et admet un neutre "à isométrie près" ; le Théorème ci-dessus (démontré par E. Witt [1] en 1937) affirme que la somme orthogonale est aussi simplifiable. On note tout de suite la conséquence suivante (également démontré par Witt en 1937) :

Théorème 10.1.2 (Décomposition de Witt) *Tout espace quadratique (V, b) se décompose en une partie totalement isotrope, une partie hyperbolique, et une partie anisotrope,*

$$(V, b) \cong (V_t, b_t) \perp (V_h, b_h) \perp (V_a, b_a),$$

et les termes de cette somme orthogonale sont uniques à isométrie près.

Démonstration. On sait déjà que $(V_t, b_t) \cong (\mathrm{rad}(V, b), b)$ est la partie totalement isotrope de (V, b), et qu'elle est unique à isométrie près (Proposition 7.1.1). Reste la partie régulière de (V, b), notons-la par (W, b), que l'on peut toujours écrire comme

$$(W, b) \cong k\langle 1, -1\rangle \perp (W_1, b_1)$$

avec la notation $k\langle 1, -1\rangle$ pour la somme de k copies du plan hyperbolique, et (W_1, b_1) un espace anisotrope (Proposition 9.2.4). Supposons qu'aussi

$$(W, b) \cong l\langle 1, -1\rangle \perp (W_2, b_2)$$

est une telle décomposition. Par le Théorème 10.1.1 on peut simplifier, un par un, les plans hyperboliques dans l'isométrie

$$k\langle 1, -1\rangle \perp (W_1, b_1) \cong l\langle 1, -1\rangle \perp (W_2, b_2).$$

1. Ernst Witt, 1911–1991, étudiant de Emmy Noether à Göttingen.

Si $k > l$ alors on trouve après l simplifications que

$$(k-l)\langle 1,-1\rangle \perp (W_1,b_1) \cong (W_2,b_2),$$

mais il est impossible qu'un espace isotrope soit isométrique à un espace anisotrope ! Si $k < l$ on a un argument similaire ; et donc nécessairement $k = l$. Ainsi on a effectivement un espace hyperbolique $(V_h,b_h) \cong k\langle 1,-1\rangle$ et un espace anisotrope $(V_a,b_a) \cong (W_1,b_1)$, uniques à isométrie près. □

Dans la décomposition de Witt d'un espace quadratique, soit

$$(V,b) \cong (V_t,b_t) \perp (V_h,b_h) \perp (V_a,b_a) \cong \mathrm{rad}((V,b),b) \perp k\langle 1,-1\rangle \perp (V_a,b_a),$$

le nombre k de plans hyperboliques est unique ; cela mérite d'être souligné par :

Définition 10.1.3 *Pour un espace quadratique (V,b), son* indice de Witt *est le nombre de plans hyperboliques figurant dans sa décomposition de Witt ; autrement dit, l'indice vaut $\frac{1}{2}\dim(V_h,b_h)$.*

On peut montrer que, pour un espace régulier (V,b), cet indice est encore égal à la dimension de tout sous-espace totalement isotrope *maximal* de V ; on le détaillera en exercice.

Exemple 10.1.4 Puisque $[1] = [-1] \in \mathbb{C}^\times/\mathbb{C}^{\times 2}$, la décomposition de Witt de l'espace quadratique complexe $\langle 0,...,0,1,...,1\rangle = \langle 0\rangle \perp ... \perp \langle 0\rangle \perp \langle 1\rangle \perp ... \perp \langle 1\rangle = r\langle 0\rangle \perp s\langle 1\rangle$ est

$$r\langle 0\rangle + \left\lfloor \frac{s}{2} \right\rfloor \langle 1,-1\rangle + (\left\lceil \frac{s}{2} \right\rceil - \left\lfloor \frac{s}{2} \right\rfloor)\langle 1\rangle,$$

son indice de Witt est donc $\lfloor \frac{s}{2} \rfloor$. Par un même raisonnement on trouve que l'indice de Witt d'un espace quadratique réel de signature (r,s) est $\min\{r,s\}$. On laisse le cas d'un espace quadratique fini comme exercice.

Reste à faire : la démonstration du Théorème de Simplification de Witt !

10.2. La démonstration de la simplification

Par diagonalisation de (V,b) on peut supposer que cet espace est la somme orthogonale d'espaces de dimension 1 ; ainsi pour démontrer le Théorème 10.1.1 il est suffisant de montrer que

$$\text{pour tout } d \in F^\times : \text{ si } \langle d\rangle \perp (V_1,b_1) \cong \langle d\rangle \perp (V_2,b_2) \text{ alors } (V_1,b_1) \cong (V_2,b_2). \tag{10.1}$$

Pour cela, décomposons les espaces (V_i,b_i) en partie nulle et partie régulière, puis diagonalisons ces parties : on peut alors écrire

$$\begin{cases} (V_1,b_1) \cong (\mathrm{rad}(V_1,b_1),b_1) \perp (W_1,b_1) \cong r\langle 0\rangle \perp \langle d_1,..,d_k\rangle \\ (V_2,b_2) \cong (\mathrm{rad}(V_2,b_2),b_2) \perp (W_2,b_2) \cong s\langle 0\rangle \perp \langle d'_1,..,d'_l\rangle \end{cases}$$

avec $d_i, d'_i \in F^\times$, et où $r\langle 0\rangle$ désigne la somme orthogonale de r copies de $\langle 0\rangle$ (et de même pour $s\langle 0\rangle$).

Si $d = 0$ alors l'assertion (10.1) devient l'isométrie

$$\langle 0\rangle \perp r\langle 0\rangle \perp \langle d_1, .., d_k\rangle \cong \langle 0\rangle \perp s\langle 0\rangle \perp \langle d'_1, .., d'_l\rangle,$$

qui implique, par la Proposition 7.1.1, que $\langle 0\rangle \perp r\langle 0\rangle \cong \langle 0\rangle \perp s\langle 0\rangle$ et $\langle d_1, .., d_k\rangle \cong \langle d'_1, .., d'_l\rangle$. Il suit bien évidemment que $r = s$ et $k = l$, et donc on obtient l'isométrie

$$r\langle 0\rangle \perp \langle d_1, .., d_k\rangle \cong s\langle 0\rangle \perp \langle d'_1, .., d'_l\rangle$$

comme souhaité.

Si $d \neq 0$ alors l'assertion (10.1) devient l'isométrie

$$\langle d\rangle \perp r\langle 0\rangle \perp \langle d_1, .., d_k\rangle \cong \langle d\rangle \perp s\langle 0\rangle \perp \langle d'_1, .., d'_l\rangle$$

qui implique, par la même Proposition 7.1.1, que $r\langle 0\rangle \cong s\langle 0\rangle$ et $\langle d\rangle \perp \langle d_1, .., d_k\rangle \cong \langle d\rangle \perp \langle d'_1, .., d'_l\rangle$; et il suit bien que $r = s$ et $k = l$... mais il reste à démontrer que $\langle d_1, .., d_k\rangle \cong \langle d'_1, .., d'_l\rangle$! Autrement dit, il nous faut encore un argument pour démontrer que :

$$\text{pour tout } d, d_i, d'_i \in F^\times : \text{ si } \langle d, d_1, ..., d_k\rangle \cong \langle d, d'_1, ..., d'_k\rangle \text{ alors } \langle d_1, ..., d_k\rangle \cong \langle d'_1, ..., d'_k\rangle. \quad (10.2)$$

On peut considérer que $\langle d, d_1, ..., d_k\rangle$ et $\langle d, d'_1, ..., d'_k\rangle$ sont les diagonalisations de deux espaces réguliers (Z_1, b_1) et (Z_2, b_2), par des bases orthogonales respectives $(\underline{x}_0, \underline{x}_1, ..., \underline{x}_k)$ et $(\underline{y}_0, \underline{y}_1, ..., \underline{y}_k)$. L'assertion (10.2) devient alors :

$$\begin{array}{l} \text{pour toute isométrie } f\colon \Big(\bigoplus_{i=0}^k F\underline{x}_i, b_1\Big) \to \Big(\bigoplus_{i=0}^k F\underline{y}_i, b_2\Big) \\ \text{il y a une isométrie } f'\colon \Big(\bigoplus_{i=1}^k F\underline{x}_i, b_1\Big) \to \Big(\bigoplus_{i=1}^k F\underline{y}_i, b_2\Big), \end{array} \quad (10.3)$$

où l'on sait que

$$b_1(\underline{x}_0, \underline{x}_0) = d = b_2(\underline{y}_0, \underline{y}_0) \quad \text{et} \quad b_1(\underline{x}_i, \underline{x}_i) = d_i \ , \ b_2(\underline{y}_i, \underline{y}_i) = d'_i \quad \text{si } i \neq 0$$

pour $d, d_i, d'_i \in F^\times$.

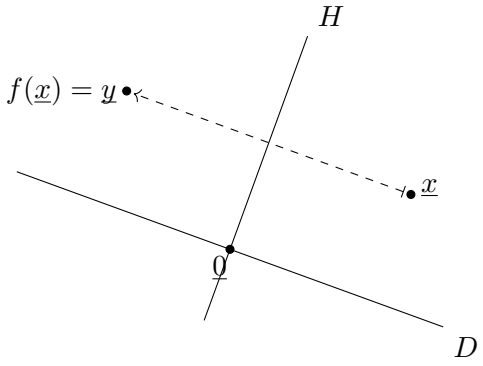
Si l'isométrie $f\colon (\bigoplus_{i=0}^k F\underline{x}_i, b_1) \to (\bigoplus_{i=0}^k F\underline{y}_i, b_2)$ envoit $\underline{x}_0$ sur $\underline{y}_0$, alors l'image par f de la suite libre $\underline{x}_1, ..., \underline{x}_k$ est une suite libre $f(\underline{x}_1), ..., f(\underline{x}_k)$ dans $\bigoplus_{i=1}^k F\underline{y}_i$. Ainsi la simple restriction de f à $\bigoplus_{i=1}^k F\underline{x}_i$ définit bien l'isométrie $f'\colon (\bigoplus_{i=1}^k F\underline{x}_i, b_1) \to (\bigoplus_{i=1}^k F\underline{y}_i, b_2)$ souhaitée.

Supposons, au contraire, que l'isométrie $f\colon (\bigoplus_{i=0}^k F\underline{x}_i, b_1) \to (\bigoplus_{i=0}^k F\underline{y}_i, b_2)$ envoit $\underline{x}_0$ sur $\underline{y}'_0 \neq \underline{y}_0$ dans $\bigoplus_{i=0}^k F\underline{y}_i$. *Si on trouve une isométrie* $g\colon (\bigoplus_{i=0}^k F\underline{y}_i, b_2) \to (\bigoplus_{i=0}^k F\underline{y}_i, b_2)$ *telle que* $g(\underline{y}'_0) = \underline{y}_0$, alors la composée $g \circ f\colon (\bigoplus_{i=0}^k F\underline{x}_i, b_1) \to (\bigoplus_{i=0}^k F\underline{y}_i, b_2)$ est une isométrie telle que $(g \circ f)(\underline{x}_0) = \underline{y}_0$, et on peut conclure par l'argument précédent. Mais une telle isométrie g, existe-t-elle ?

Voici donc le *crux* de notre démonstration—le cœur de la question :

Proposition 10.2.1 *Soit un espace quadratique* (V, b) *et* $\underline{x}, \underline{y} \in V$ *tels que* $b(\underline{x}, \underline{x}) = b(\underline{y}, \underline{y}) \neq 0$. *Il existe une isométrie* $f\colon (V, b) \to (V, b)$ *telle que* $f(\underline{x}) = \underline{y}$.

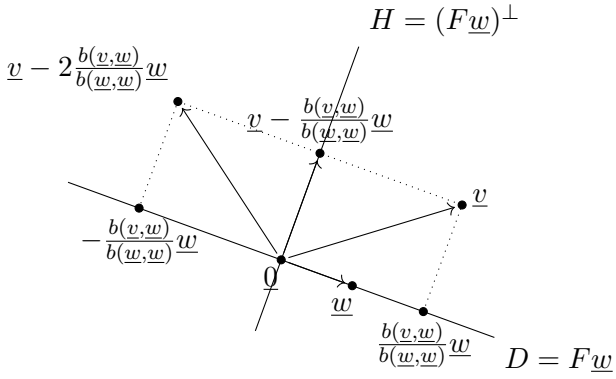
Démonstration. Nous cherchons un élément f du groupe orthogonal $\mathsf{O}(V,b)$ envoyant $\underline{x}$ sur $\underline{y}$; l'*idée géométrique* est d'utiliser une réflexion : on veut déterminer une décomposition $V = H \perp D$ en un hyperplan H et une droite D, telle que $f\colon V \to V\colon \underline{v}_H + \underline{v}_D \mapsto \underline{v}_H - \underline{v}_D$ soit une isométrie envoyant $\underline{x}$ sur $\underline{y}$.



En toute généralité, si $\underline{w} \in V$ est anisotrope, alors $D = F\underline{w}$ est une droite régulière dans V (le sous-espace quadratique $(F\underline{w}, b)$ est isométrique à $\langle b(\underline{w},\underline{w})\rangle$ et $b(\underline{w},\underline{w}) \neq 0$). Par Proposition 5.1.3, l'hyperplan $H = D^\perp$ permet la décomposition $V = H \perp D$. L'application linéaire

$$f_{\underline{w}}\colon V \to V\colon \underline{v} \mapsto \underline{v} - 2\frac{b(\underline{v},\underline{w})}{b(\underline{w},\underline{w})}\underline{w}$$

est alors une isométrie qui fixe les éléments de H et qui "change le signe" des éléments de D (exercice) ; c'est donc bien la *réflexion orthogonal* par rapport à l'hyperplan orthogonal à $\underline{w}$.



Finalement, pour $b(\underline{x},\underline{x}) = b(\underline{y},\underline{y}) \neq 0$ dans V on vérifie d'abord que

$$b(\underline{x}+\underline{y},\underline{x}+\underline{y}) + b(\underline{x}-\underline{y},\underline{x}-\underline{y}) = 2b(\underline{x},\underline{x}) + 2b(\underline{y},\underline{y}) = 4b(\underline{x},\underline{x}) \neq 0$$

et donc au moins un des deux vecteurs $\underline{x}+\underline{y}$ et $\underline{x}-\underline{y}$ est anisotrope. Si $\underline{x}-\underline{y}$ est anisotrope, alors on applique ce qui précède pour $\underline{w} = \underline{x}-\underline{y}$ et on trouve en particulier que

$$f_{\underline{x}-\underline{y}}(\underline{x}) = \underline{x} - 2\frac{b(\underline{x},\underline{x}-\underline{y})}{b(\underline{x}-\underline{y},\underline{x}-\underline{y})}(\underline{x}-\underline{y}) = \underline{y}$$

et donc $f_{\underline{x}-\underline{y}}$ est l'isométrie recherchée. Si $\underline{x}-\underline{y}$ est isotrope, alors $\underline{x}+\underline{y}$ est anisotrope, et on peut calculer que $f_{\underline{x}+\underline{y}}(\underline{x}) = -\underline{y}$. Ainsi l'isométrie $-f_{\underline{x}+\underline{y}}$ fera l'affaire. □

Un vecteur $\underline{x}$ étant anisotrope dans (V,b) si et seulement si la droite $F\underline{x} \subseteq V$ est un sous-espace régulier, la Proposition précédente est la version "en dimension 1" du résultat disant que "toute isométrie entre sous-espaces réguliers s'étend à une isométrie de l'espace entier" :

Corollaire 10.2.2 *Soit un espace quadratique (V,b) et $f\colon (W_1,b) \to (W_2,b)$ une isométrie entre deux sous-espaces réguliers de V. Il existe une isométrie $\overline{f}\colon (V,b) \to (V,b)$ dont la restriction à W_1 est f.*

Démonstration. Par régularité de W_1 on sait que $V = W_1 \perp W_1^\perp$, et l'isométrie $(W_1,b) \cong (W_2,b)$ implique que $V \cong W_2 \perp W_1^\perp$. Par régularité de W_2 on a aussi $V = W_2 \perp W_2^\perp$, et le Théorème 10.1.1 permet de dire qu'il existe une isométrie $g\colon (W_1^\perp,b) \to (W_2^\perp,b)$. L'assemblage des isométries f et g (comme on a fait dans la Propostion 5.2.6) est une isométrie $\overline{f}\colon (V,b) \to (V,b)$, dont la restriction à W_1 est bien évidemment f. □

Dans les exercices nous montrerons le resultat précédent pour des sous-espaces *quelconques* d'un espace *régulier*—ce résultat est connu comme le *Théorème de Witt*.

10.3. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Donner un élément de $\mathsf{O}(\mathbb{R}^4, q(x,y,z,t) = x^2+y^2+z^2-t^2)$ envoyant $(-1,0,0,2)$ sur $(1,2,1,3)$.

3. *Classification des plans quadratiques selon leurs droites isotropes.* Montrer que, si (V,b) est un plan quadratique, alors il y a soit aucune droite isotrope, soit une droite isotrope, soit deux droites isotropes, soit toutes les droites sont isotropes. Indication : décomposer (V,b).

4. Montrer que, si $\underline{x}$ et $\underline{y}$ sont deux vecteurs isotropes dans un espace régulier (V,b), alors il existe une isométrie $f \in O(V,b)$ telle que $f(\underline{x}) = \underline{y}$. Pourquoi n'est-ce pas le cas dans un espace non-régulier ? Indication : construire une paire hyperbolique $\underline{x},\underline{x}'$ ainsi qu'une paire hyperbolique $\underline{y},\underline{y}'$, puis étendre l'isométrie $F\underline{x} \oplus F\underline{x}' \cong F\underline{y} \oplus F\underline{y}'$ à tout (V,b).

5. *Tout sous-espace totalement isotrope est "la moitié" d'un sous-espace hyperbolique.* Montrer que, si $W = F\underline{w}_1 \oplus ... \oplus F\underline{w}_k$ est un sous-espace totalement isotrope d'un espace régulier (V,b), alors il existe un deuxième sous-espace totalement isotrope $W' = F\underline{w}'_1 \oplus ... \oplus F\underline{w}'_k$ tel que les sous-espaces $F\underline{w}_i \oplus F\underline{w}'_i$ sont des plans hyperboliques orthogonaux deux-à-deux (et W est ainsi un sous-espace d'un espace hyperbolique de deux fois la dimension de W). Indication : pour $W_1 = F\underline{w}_2 \oplus ... \oplus F\underline{w}_k$, montrer que l'on peut prendre $\underline{w}'_1$ dans $W_1^\perp \setminus F\underline{w}_1^\perp$; on obtient ainsi un plan hyperbolique $F\underline{w}_1 \oplus F\underline{w}'_1$ qui est orthogonal à W_1, puis considérer $F\underline{w}_1 \oplus F\underline{w}'_1 \perp W_1$ et faire une récurrence sur la dimension de W_1.

6. *Indice de Witt.* Montrer que, si W est un *sous-espace totalement isotrope maximal* d'un espace régulier (V,b) (c'est à dire, W n'est pas strictement inclu dans un sous-espace totalement isotrope), alors sa dimension est égale à l'indice de Witt de (V,b) (que nous avons défini comme le nombre de plans hyperboliques dans la décomposition de Witt).

7. Donner l'indice de Witt des espaces quadratiques finis rencontrés auparavant.
Solution. Un espace quadratique sur $\mathbb{F}_q$ s'écrit comme soit $\langle 0, ..., 0, 1, ..., 1\rangle$, soit $\langle 0, ..., 0, 1, ..., 1, \varepsilon\rangle$, avec ε un non-carré au choix dans $\mathbb{F}_q$. On fait une analyse de la situation selon la quadraticité de -1. Si -1 est un carré dans $\mathbb{F}_q$ alors on utilise $\langle 1, 1\rangle \cong \langle 1, -1\rangle$ pour trouver le nombre de sous-plans hyperboliques de l'espace donné. Si -1 n'est pas un carré dans $\mathbb{F}_q$ alors on combine $\langle 1, 1\rangle = \langle \varepsilon, \varepsilon\rangle$ avec $\langle \varepsilon\rangle = \langle -1\rangle$ pour voir que $\langle 1, 1, 1, 1\rangle \cong \langle 1, -1, 1, -1\rangle$, et cela aide à trouver le nombre de sous-plans hyperboliques de l'espace donné. (Voir aussi la Proposition 13.3.1.)

8. *Généralisation d'un exercice précédent.* Soit (V, b) un espace régulier et W un sous-espace quelconque avec décomposition $(W, b) = \mathrm{rad}(W, b) \perp (W', b)$. Soit $\mathrm{rad}(W, b) = F\underline{w}_1 \oplus ... \oplus F\underline{w}_k$, alors il existe un sous-espace $F\underline{w}'_1 \oplus ... \oplus F\underline{w}'_k$ tel que les sous-espaces $F\underline{w}_i \oplus F\underline{w}'_i$ sont des plans hyperboliques orthogonaux deux-à-deux et aussi orthogonaux à W'.
Solution. Si $k = 1$, on a $W \cong F\underline{w} \perp W'$ avec $\underline{w}$ isotrope et W' régulier. On a toujours que $W^\perp \subseteq (W')^\perp$, et cette inclusion est stricte car sinon on aurait (par régularité de (V, b), cf. un exercice précédent) que $W' = (W')^{\perp\perp} = W^{\perp\perp} = W$, ce qui est absurde. Il existe donc un $\underline{w}' \in (W')^\perp \setminus W^\perp$, c'est à dire que $\underline{w}'$ est orthogonal à W' mais pas à $\underline{w}$, et donc $F\underline{w} \oplus F\underline{w}'$ est un plan hyperbolique orthogonal à W'. Pour $k \geq 2$, on a $W \cong (F\underline{w}_1 \oplus ... \oplus F\underline{w}_k) \perp W'$ et on peut poser $U = (F\underline{w}_2 \oplus ... \oplus F\underline{w}_k)$. On raisonne comme avant pour trouver $\underline{w}'_1 \in (U \perp W')^\perp \setminus W^\perp$, et on montre que $F\underline{w}_1 \oplus F\underline{w}'_1$ est un plan hyperbolique orthogonal à $U \perp W'$. Ainsi on construit $(F\underline{w}_1 \oplus F\underline{w}'_1) \perp U \perp W'$, et on peut faire une récurrence sur U (puisque $(F\underline{w}_1 \oplus F\underline{w}'_1) \perp W'$ est régulier).

9. *Encore un Théorème de E. Witt.* Montrer que, pour tout espace régulier (V, b) et toute isométrie $f\colon (W_1, b) \to (W_2, b)$ de sous-espaces (quelconques), il existe une isométrie $\overline{f} \in O(V, b)$ dont la restriction à W_1 est f.
Solution. Ayant démontré ce résultat pour des sous-espaces réguliers, on va s'y ramener comme suit. On peut décomposer $W_i = \mathrm{rad}(W_i) \perp W'_i$, et l'isométrie $f\colon W_1 \to W_2$ se décompose en une isométrie $\mathrm{rad}(W_1) \to \mathrm{rad}(W_2)$ et une isométrie : $W'_1 \to W'_2$. Si $\underline{w}_1, ..., \underline{w}_k$ est une base de $\mathrm{rad}(W_1)$, par isométrie on aura une base $f(\underline{w}_1), ..., f(\underline{w}_k)$ de $\mathrm{rad}(W_2)$; avec ces bases, on inclut les $\mathrm{rad}(W_i)$ dans des espaces hyperboliques H_i (comme dans un exercice précédent), et on étend de manière évidente l'isométrie des radicaux à leurs extensions hyperboliques. Maintenant l'isométrie $H_1 \perp W'_1 \to H_2 \perp W'_2$ (entre sous-espaces réguliers !) s'étend à tout (V, b).

11. Etude du groupe orthogonal

11.1. Réflexions

De manière générale, nous avons défini le *groupe orthogonal* d'un espace quadratique (V, b) par

$$\mathsf{O}(V, b) = \{f \colon (V, b) \to (V, b) \mid f \text{ est une isométrie}\}.$$

Rappelons une notion importante déjà utilisée dans la démonstration de la Proposition 10.2.1 :

Définition 11.1.1 *Soit $\underline{w}$ un vecteur anisotrope dans un espace quelconque (V, b), alors*

$$f_{\underline{w}} \colon (V, b) \to (V, b) \colon \underline{v} \mapsto \underline{v} - 2\frac{b(\underline{v}, \underline{w})}{b(\underline{w}, \underline{w})}\underline{w}$$

est une isométrie : c'est la réflexion (orthogonale) *par rapport à l'hyperplan $H = (F\underline{w})^{\perp}$, laissant fixe les éléments de H et envoyant les éléments de $F\underline{w}$ sur leurs opposés.*

Rappelons également que, si $q(\underline{x}) = q(\underline{y}) \neq 0$ dans un espace quelconque (V, b), alors on a toujours (au moins) un parmi $\underline{x} + \underline{y}$ et $\underline{x} - \underline{y}$ qui est anisotrope ; et

- si $q(\underline{x} - \underline{y}) \neq 0$ alors $f_{\underline{x}-\underline{y}}(\underline{x}) = \underline{y}$,
- si $q(\underline{x} + \underline{y}) \neq 0$ alors $-f_{\underline{x}+\underline{y}}(\underline{x}) = \underline{y}$.

Par ailleurs, on vérifie facilement que

$$f_{\underline{w}}(\underline{w}) = -\underline{w}$$

et donc, en particulier,

$$\underline{y} = -f_{\underline{x}+\underline{y}}(\underline{x}) = f_{\underline{x}+\underline{y}}(-\underline{x}) = f_{\underline{x}+\underline{y}}(f_{\underline{x}}(\underline{x})) = (f_{\underline{x}+\underline{y}} \circ f_{\underline{x}})(\underline{x}).$$

Ainsi, à moindres frais, nous pouvons quelque peu peaufiner la Proposition 10.2.1 :

Proposition 11.1.2 *Soit un espace quadratique (V, b) et deux vecteurs anisotropes $\underline{x}, \underline{y} \in V$ tels que $q(\underline{x}) = q(\underline{y})$. Il existe une composée de au plus deux réflexions $f \colon (V, b) \to (V, b)$ telle que $f(\underline{x}) = \underline{y}$.*

La conséquence suivante est à comparer avec le Corollaire 1.2.5 :

Corollaire 11.1.3 *Soit (V, b) un espace quadratique régulier de dimension n. Tout $f \in \mathsf{O}(V, b)$ est la composée de au plus $2n$ réflexions.*

Démonstration. On fait une démonstration par induction sur la dimension de V.
Pour $\dim(V) = 0$ tout est trivial.
Si $\dim(V) = 1$ alors on sait que $(V, b) \cong \langle d \rangle = (F, q(x) = dx^2)$ pour un $d \in F^\times$. Les isomorphismes $f\colon V \to V$ sont donnés par $f(x) = ax$ pour $a \in F^\times$; et un tel isomorphisme est une isométrie si et seulement si $a \in \{1, -1\}$. Ainsi $\mathsf{O}(V, b) \cong \{1, -1\}$, où -1 correspond à l'unique réflexion, et bien sûr $1 = (-1)(-1)$ exprime l'identité du groupe comme la composée de la réflexion avec elle-même. Ainsi l'énoncé est vraie.
Soit maintenant $\dim(V) = n \geq 2$, et $f \in \mathsf{O}(V, b)$ quelconque. Par régularité de (V, b) il existe un vecteur anisotrope $\underline{x} \in V$. On a bien sûr $q(f(\underline{x})) = q(\underline{x}) \neq 0$, et par la Proposition précédente on peut trouver (au plus) deux réflexions, disons $\sigma, \tau \in \mathsf{O}(V, b)$, telle que $(\sigma \circ \tau)(f(\underline{x})) = \underline{x}$. C'est à dire, quitte à composer avec (au plus) deux réflexions, on peut remplacer f par $f' = \sigma \circ \tau \circ f \in \mathsf{O}(V, b)$ et supposer que f' fixe un vecteur anisotrope $\underline{x}$. Par régularité du sous-espace $F\underline{x} \subseteq V$ on a alors la décomposition

$$(V, b) \cong (F\underline{x}, b) \perp (F\underline{x}, b)^\perp$$

en un espace de dimension 1 et un espace de dimension $n - 1$. Puisque

- pour $\underline{v} \in F\underline{x}$ on a $f'(\underline{v}) = f'(\alpha\underline{x}) = \alpha f'(\underline{x}) = \alpha\underline{x} = \underline{v}$,
- pour $\underline{v} \in (F\underline{x})^\perp$ on a $b(f'(\underline{v}), \underline{x}) = b(f'(\underline{v}), f'(\underline{x})) = b(\underline{v}, \underline{x}) = 0$ et donc $f'(\underline{v}) \in (F\underline{x}, b)^\perp$,

nous trouvons que la restriction de f' à $F\underline{x}$ est l'identité, et la restriction de f' à $(F\underline{x})^\perp$ est une isométrie ; notons-les par

$$f'_{F\underline{x}} = \mathsf{id}_{F\underline{x}}\colon F\underline{x} \to F\underline{x} \quad \text{et} \quad f'_{(F\underline{x})^\perp}\colon (F\underline{x})^\perp \to (F\underline{x})^\perp.$$

Par hypothèse d'induction on peut maintenant supposer que cette deuxième isométrie est une composée de (au plus) $2(n-1)$ réflexions de $(F\underline{x})^\perp$, soit

$$f'_{(F\underline{x})^\perp} = \sigma_r \circ \ldots \circ \sigma_1 \quad \text{avec } r \leq 2(n-1),$$

chaque réflexion σ_i étant déterminée par un hyperplan $H_i \subseteq (F\underline{x})^\perp$. Mais alors, par somme orthogonale

$$\mathsf{id}_{F\underline{x}} \perp \sigma_i\colon F\underline{x} \perp (F\underline{x})^\perp \to F\underline{x} \perp (F\underline{x})^\perp\colon \underline{v} + \underline{w} \mapsto \underline{v} + \sigma_i(\underline{w}),$$

on obtient autant de réflexions de (V, b) (par rapport aux hyperplans $\overline{H}_i = F\underline{x} \oplus H_i$) ; et la composée est bien

$$(\mathsf{id}_{F\underline{x}} \perp \sigma_r) \circ \ldots \circ (\mathsf{id}_{F\underline{x}} \perp \sigma_1) = \mathsf{id}_{F\underline{x}} \perp (\sigma_r \circ \ldots \circ \sigma_1) = f'_{F\underline{x}} \perp f'_{(F\underline{x})^\perp} = f'.$$

Par la construction de f' par composée de (au plus) deux réflexions avec f, on obtient le résultat annoncé. □

La borne donnée dans le Corollaire ci-dessus n'est pas optimale. Par exemple, pour l'espace $(\mathbb{R}^2, q(x, y) = x^2 + y^2)$ nous avons déjà montré que tout élément de son groupe orthogonal est une composée de au plus 2 (et non pas 4) réflexions. De manière générale on a en effet :

Théorème 11.1.4 (Théorème de Cartan-Dieudonné) *Si (V,b) est un espace quadratique régulier de dimension n, alors tout élément de $\mathsf{O}(V,b)$ est la composée de au plus n réflexions.*

La démonstration de ce résultat n'est pas très difficile mais un peu trop longue pour l'inclure ici ; pour les détails, consulter les références. La borne donnée dans le Théorème de Cartan-Dieudonné est, par contre, optimale :

Proposition 11.1.5 *Soit (V,b) un espace quadratique régulier et $f = \sigma_r \circ ... \circ \sigma_1$ une composée de r réflexions, alors les points fixes de f forment un sous-espace de dimension au moins $n-r$.*

Démonstration. Notons H_i l'hyperplan (de dimension $n-1$ donc) des points fixes de la réflexion σ_i. Alors l'intersection $\cap_i H_i \subseteq V$ contient des points fixes de $f = \sigma_r \circ ... \circ \sigma_1$; sa dimension est au moins $n-r$. □

Corollaire 11.1.6 *Pour tout espace quadratique régulier (V,b), le seul point fixe de l'isométrie $f\colon (V,b) \to (V,b)\colon \underline{x} \mapsto -\underline{x}$ est $\underline{0}$, et donc ce f n'est pas la composée de strictement moins que n réflexions.*

Rappelons que toute isométrie $f \in \mathsf{O}(V,b)$ a son déterminant $\det(f) \in F^\times$ (au sens de l'algèbre linéaire). On a ainsi un homomorphisme de groupes $\det\colon \mathsf{O}(V,b) \to F^\times\colon f \mapsto \det(f)$ (exercice : donner les détails), dont le noyau mérite notre attention :

Définition 11.1.7 *Le* groupe orthogonal spécial *de l'espace quadratique (V,b) est le noyau de $\det\colon \mathsf{O}(V,b) \to F^\times$, soit :*

$$\mathsf{SO}(V,b) = \{f \in \mathsf{O}(V,b) \mid \det(f) = 1\}.$$

Si l'espace quadratique (V,b) est régulier, alors pour tout $f \in \mathsf{O}(V,b)$ on a $\det(f) = \pm 1$ (exercice). Si en plus V est non-nul, l'homomorphisme det se restreint à un *surjection* $\det\colon \mathsf{O}(V,b) \to \{1,-1\}$. En effet, si $\dim(V) = n \neq 0$, considérons une réflexion $\sigma \in \mathsf{O}(V,b)$ avec son hyperplan H de points fixes et une droite D orthogonale à H ; on peut alors écrire

$$\sigma\colon H \perp D \to H \perp D\colon \underline{v} + \underline{w} \mapsto \underline{v} - \underline{w}$$

et, pour un "bon choix de base" de $V = H \perp D$ (à savoir, une base de H complété par une base de D), la matrice de σ sera la matrice diagonale

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$$

Le déterminant d'une réflexion est donc -1. Ainsi on a $\mathsf{O}(V,b)/\mathsf{SO}(V,b) \cong \{1,-1\}$. Autrement dit, le groupe orthogonal d'un espace régulier est le produit semidirect du groupe orthogonal spécial avec le groupe cyclique d'ordre 2 : $\mathsf{O}(V,b) \cong \mathsf{SO}(V,b) \rtimes \mathsf{C}_2$. Mais par le Théorème 11.1.4 on a aussi, par composition de réflexions, pour tout $f \in \mathsf{O}(V,b)$,

$$\text{si } f = \sigma_r \circ ... \circ \sigma_1 \text{ alors } \det(f) = (-1)^r.$$

Il suit ainsi que :

Corollaire 11.1.8 *Soit (V, b) un espace quadratique régulier. Le groupe $\mathsf{SO}(V, b)$ contient exactement les composées d'un nombre paire de réflexions.*

Terminons ici avec un résumé de quelques résultats que nous avons démontrés auparavant. D'abord, dans le Corollaire 10.2.2 nous avons expliqué que toute isométrie de sous-espaces *réguliers* d'un espace quadratique *quelconque* (V, b) s'étend à une isométrie de tout l'espace (V, b). Autrement dit :

Corollaire 11.1.9 *Pour tout espace quadratique (V, b), le groupe $\mathsf{O}(V, b)$ est transitif sur tout ensemble de sous-espaces réguliers isométriques.*

Par exemple, le groupe $\mathsf{O}(V, b)$ est transitif sur l'ensemble des sous-plans hyperboliques de (V, b).

Ensuite, en exercice nous avons démontré le Théorème de Witt disant que, pour tout espace *régulier* (V, b), toute isométrie de sous-espaces *quelconques* s'étend à une isométrie de tout l'espace (V, b). Ainsi :

Corollaire 11.1.10 *Pour tout espace quadratique régulier (V, b), le groupe $\mathsf{O}(V, b)$ est transitif sur tout ensemble de sous-espaces isométriques.*

Par exemple, le groupe $\mathsf{O}(V, b)$ est transitif sur l'ensemble des sous-droites isotropes d'un espace régulier (V, b).

11.2. Exemples

On peut démontrer bien d'autres résultats intéressants à propos de $\mathsf{O}(V, b)$ et son sous-groupe normal $\mathsf{SO}(V, b)$. Pour en donner une idée, citons ici deux résultats classiques à propos du centre [1] de ces groupes :

Proposition 11.2.1 *Soit (V, b) un espace régulier, alors $\mathcal{Z}(\mathsf{O}(V, b)) \cong \mathsf{C}_2$ si (V, b) n'est pas un plan hyperbolique sur $\mathbb{F}_3$, et $\mathcal{Z}(\mathsf{O}(\langle 1, -1\rangle_{\mathbb{F}_3})) = \mathsf{O}(\langle 1, -1\rangle_{\mathbb{F}_3}) \cong \mathsf{C}_2 \times \mathsf{C}_2$.*

Proposition 11.2.2 *Soit (V, b) un espace régulier de dimension $n = 2$, alors $\mathcal{Z}(\mathsf{SO}(V, b)) = \mathsf{SO}(V, b)$. Soit (V, b) un espace régulier de dimension $n \geq 3$, alors $\mathcal{Z}(\mathsf{SO}(V, b)) \cong \{1\}$ si n est impair et $\mathcal{Z}(\mathsf{SO}(V, b)) \cong \mathsf{C}_2$ si n est pair.*

Nous ne donnons pas les démonstrations ici—mais regardons tout de même quelques exemples de plus près. La notation suivante est justifiée par la Proposition 8.2.1 et le Théorème 8.2.3 :

Définition 11.2.3 *Pour $r, s \in \mathbb{N}$ on note $\mathsf{O}(r, s)$ le groupe orthogonal de l'espace quadratique réel régulier de signature (r, s) ; et on pose $\mathsf{O}(n) = \mathsf{O}(n, 0)$. On fait de même pour les sous-groupes normaux $\mathsf{SO}(r, s)$ et $\mathsf{SO}(n)$.*

1. Le centre d'un groupe $G = (G, \cdot, 1)$ est le sous-groupe (normal et commutatif) $\mathcal{Z}(G) = \{g \in G \mid \forall h \in G : gh = hg\}$; le groupe G est commutatif si et seulement si $G = \mathcal{Z}(G)$.

Exemple 11.2.4 Le groupe $\mathsf{O}(2)$ est le groupe orthogonal du plan $\mathbb{R}^2$ muni du produit scalaire usuel. Nous avons déjà vu que

$$\mathsf{O}(2) \cong \{M \in \mathbb{R}^{2\times 2} \mid M^t M = I\} = \left\{ \begin{pmatrix} \cos(t) & -\sin(t) \\ \pm\sin(t) & \pm\cos(t) \end{pmatrix} \mid t \in \mathbb{R} \right\}$$

$$\mathsf{SO}(2) \cong \{M \in \mathbb{R}^{2\times 2} \mid M^t M = I \text{ et } \det(M) = 1\} = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mid t \in \mathbb{R} \right\}$$

Le groupe $\mathsf{SO}(2)$ (des rotations) est commutatif, et donc

$$\mathcal{Z}(\mathsf{SO}(2)) = \mathsf{SO}(2).$$

On sait que tout élément du groupe orthogonal $\mathsf{O}(2)$ est soit une rotation, soit la composée d'une rotation avec une réflexion fixe ; au niveau matricielle, si on note

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{et} \quad J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

alors les éléments de $\mathsf{O}(2)$ sont les R_θ's et les $R_\theta J$'s. Mais il est facile de voir que $JR_\theta = R_\theta J$ si et seulement si $R_\theta = \pm I$, et ceci implique immédiatement que le centre de ce groupe ne peut contenir que $\pm I$; de l'autre côté, il est aussi facile de voir que I et $-I$ commutent effectivement avec tous les éléments du groupe. On conclut que

$$\mathcal{Z}(\mathsf{O}(2)) = \{\pm I\} \cong \mathsf{C}_2.$$

Exemple 11.2.5 Pour décrire matriciellement le groupe orthogonal d'un plan hyperbolique réel, soit $\mathsf{O}(1,1)$, notons la matrice de cette forme quadratique diagonale par

$$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

alors on a l'isomorphisme de groupes $\mathsf{O}(1,1) \cong \{M \in \mathbb{R}^{2\times 2} \mid M^t B M = B\}$; nous souhaitons expliciter ces matrices M. Si on pose

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

alors l'équation $M^t B M = B$ dit que

$$\begin{cases} a^2 - c^2 = 1 \\ b^2 - d^2 = -1 \\ ab = cd \end{cases}$$

Clairement, $a = 0$ est impossible, et aussi $d = 0$ est impossible. On sait ainsi que $c = abd^{-1}$ et donc $a^2 - (abd^{-1})^2 = 1$; mais puisque $b^2 - d^2 = -1$ ceci implique $a^2 = d^2$, ce qui à son tour implique $b^2 = c^2$. Mais l'équation $ab = cd$ implique tout de même que $ad^{-1} = b^{-1}c$ et donc si a

et d sont de signes identiques (resp. opposées), alors aussi b et c sont de signes identiques (resp. opposées). Bref, on a exactement les matrices de la forme

$$M_1 = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \quad \text{ou} \quad M_2 = \begin{pmatrix} a & b \\ -b & -a \end{pmatrix} \quad \text{avec } a^2 - b^2 = 1,$$

et on peut déjà écrire que

$$\mathsf{O}(1,1) \cong \left\{ \begin{pmatrix} a & b \\ \pm b & \pm a \end{pmatrix} \mid a^2 - b^2 = 1 \right\}.$$

La solution générale à l'équation de l'hyperbole $x^2 - y^2 = 1$ dans $\mathbb{R}^2$ est donnée par (exercice)

$$\begin{cases} x = \pm\cosh(t) = \pm\dfrac{e^t + e^{-t}}{2} \\ y = \pm\sinh(t) = \pm\dfrac{e^t - e^{-t}}{2} \end{cases} \qquad \text{pour } t \in \mathbb{R}$$

Les fonctions $\cosh, \sinh \colon \mathbb{R} \to \mathbb{R}$ sont le *cosinus hyperbolique* et le *sinus hyperbolique*. Ainsi tout élément de $\mathsf{O}(1,1)$ appartient à une des "quatre familles"

$$\begin{pmatrix} \cosh(t) & \sinh(t) \\ \sinh(t) & \cosh(t) \end{pmatrix}, \begin{pmatrix} \cosh(t) & \sinh(t) \\ -\sinh(t) & -\cosh(t) \end{pmatrix}, \begin{pmatrix} -\cosh(t) & -\sinh(t) \\ \sinh(t) & \cosh(t) \end{pmatrix}, \begin{pmatrix} -\cosh(t) & -\sinh(t) \\ -\sinh(t) & -\cosh(t) \end{pmatrix}.$$

Si on note

$$R_t = \begin{pmatrix} \cosh(t) & \sinh(t) \\ \sinh(t) & \cosh(t) \end{pmatrix} \quad \text{et} \quad J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

alors on peut écrire cela comme

$$\mathsf{O}(1,1) \cong \left\{ \pm J^i R_t \mid t \in \mathbb{R}, i \in \{0,1\} \right\}.$$

En sélectionnant les matrices de déterminant 1, on trouve également que

$$\mathsf{SO}(1,1) \cong \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a^2 - b^2 = 1 \right\} = \{ \pm R_t \mid t \in \mathbb{R} \}.$$

Le groupe $\mathsf{SO}(1,1)$ est commutatif, et donc il est égal à son centre :

$$\mathcal{Z}(\mathsf{SO}(1,1)) = \mathsf{SO}(1,1).$$

Pour le calcul du centre de $\mathsf{O}(1,1)$, on peut procéder par analogie avec l'Exemple précédent pour voir que

$$\mathcal{Z}\mathsf{O}(1,1) \cong \{I, -I\} \cong \mathsf{C}_2.$$

Exemple 11.2.6 (Groupe de Lorentz) On appelle le groupe $\mathsf{O}(3,1)$ des isométries de l'espace de Minkowski (voir Exemple 4.2.6) le *groupe de Lorentz*[2], et ses éléments les *transformations de Lorentz*. Pour avoir une description matricielle de ce groupe, notons

$$B = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$$

2. D'après Hendrik A. Lortentz (1853–1928), prix Nobel de physique en 1902.

la matrice de la forme quadratique (pour la base canonique), alors

$$\mathsf{O}(3,1) \cong \{L \in \mathbb{R}^{4\times 4} \mid L^t B L = B\}.$$

Si on écrit une telle matrice L "par blocs" séparant les 3 premières lignes et colonnes, comme

$$L = \left(\begin{array}{c|c} M & N \\ \hline P & c \end{array}\right)$$

alors il suit de $L^t B L = B$ que $N^t N - c^2 = -1$, et donc $c^2 \geq 1$; autrement dit, pour $L = (l_{ij})_{i,j} \in \mathsf{O}(3,1)$ on a soit $l_{44} \geq 1$, et on dit que L est *orthochrone* ("préserve la direction du temps"), soit $l_{44} \leq -1$, et L est *antichrone*. Montrons que l'application

$$\gamma\colon \mathsf{O}(3,1) \to \{+1,-1\}\colon L \mapsto \operatorname{sgn}(l_{44})$$

est un homomorphisme surjectif de groupes. Pour cela, on remarque d'abord que $B = L^t B L$ (et $BB = I$) implique $L^{-1} = B L^t B$; ainsi, avec les notations "en blocs" de ci-dessus,

$$\left(\begin{array}{c|c} M & N \\ \hline P & c \end{array}\right)^{-1} = \left(\begin{array}{c|c} M^t & -P^t \\ \hline -N^t & c \end{array}\right)$$

Il suit qu'aussi $(-P^t)^t(-P^t) - c^2 = -1$, c'est à dire, $PP^t = N^t N = c^2 - 1$ pour tout tel élément de $\mathsf{O}(3,1)$. Maintenant, soit une autre matrice

$$L' = \left(\begin{array}{c|c} M' & N' \\ \hline P' & c' \end{array}\right) \text{ telle que } B = L'^t B L',$$

et notons également

$$L'' = \left(\begin{array}{c|c} M'' & N'' \\ \hline P'' & c'' \end{array}\right) = \left(\begin{array}{c|c} M & N \\ \hline P & c \end{array}\right)\left(\begin{array}{c|c} M' & N' \\ \hline P' & c' \end{array}\right) = LL'.$$

On a alors que [3]

$$c'' = PN' + cc' \geq -|PN'| + cc' \geq -\|P\|\|N'\| + cc' = -\sqrt{c^2-1}\sqrt{c'^2-1} + cc'.$$

3. Ici on écrit $\|\cdot\|$ pour la norme usuelle dans $\mathbb{R}^3$, définie par le produit scalaire usuel, et donc on sait que $|\underline{x}\cdot\underline{y}| \leq \|\underline{x}\|\|\underline{y}\|$ pour tout $\underline{x},\underline{y} \in \mathbb{R}^3$. On identifie $\underline{x}$ avec la ligne P, et $\underline{y}$ avec la colonne N' ; le produit matriciel PN' est donc exactement le produit scalaire usuel $\underline{x}\cdot\underline{y}$.

Si c et c' ont le même signe, alors ceci implique que $c'' \geq 0$, et donc (puisque LL' est une transformation de Lortenz) $c'' \geq 1$; si c et c' sont de signes opposés, alors $c'' \leq 0$ et donc $c'' \leq -1$. Bref, nous avons montré que $\gamma(L)\gamma(L') = \gamma(LL')$. Clairement, $\gamma(I) = 1$, et il est facile de trouver une matrice L dans $\mathsf{O}(3,1)$ telle que $\gamma(L) = -1$. Ainsi on peut conclure que les transformations orthochrones forment un sous-groupe normal $\mathsf{O}^+(3,1) \trianglelefteq \mathsf{O}(3,1)$. De l'autre côté, nous savons déjà que $\det(L) = \pm 1$ pour tout $L \in \mathsf{O}(3,1)$; une transformation de Lorentz est *propre* si son déterminant vaut 1 (elle "préserve l'orientation de l'espace"), et *impropre* sinon. Le sous-groupe normal $\mathsf{SO}(3,1) \trianglelefteq \mathsf{O}(3,1)$ contient donc exactement les transformations *propres* de Lorentz. L'intersection de ces deux sous-groupes normaux est le sous-groupe normal noté $\mathsf{SO}^+(3,1) \trianglelefteq \mathsf{O}(3,1)$. Ce groupe est important en physique—car "physiquement" on peut ni changer l'orientation, ni changer la direction du temps, de l'espace de Minkowski. Quel est le quotient $\mathsf{O}(3,1)/\mathsf{SO}^+(3,1)$? On peut raisonner que – puisque tout $L \in \mathsf{O}(3,1)$ est soit propre, soit impropre ; et tout L est soit orthochrone, soit antichrone – on a une réunion disjointe

$$\begin{aligned}\mathsf{O}(3,1) \;=\; & \{\text{propre, orthochrone}\} \cup \{\text{propre, antichrone}\} \\ & \cup \{\text{impropre, orthochrone}\} \cup \{\text{impropre, antichrone}\}.\end{aligned}$$

Si on note

$$I = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \quad J = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} \quad K = \begin{pmatrix} -1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{pmatrix}$$

alors $\{I, J, K, -I\} \subseteq \mathsf{O}(3,1)$ est (à isomorphisme près) le groupe de Klein $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$. Mais la réunion disjointe ci-dessus correspond avec

$$\mathsf{O}(3,1) = \Big(\mathsf{SO}^+(3,1) \cdot I\Big) \cup \Big(\mathsf{SO}^+(3,1) \cdot J\Big) \cup \Big(\mathsf{SO}^+(3,1) \cdot K\Big) \cup \Big(\mathsf{SO}^+(3,1) \cdot (-I)\Big).$$

Ainsi le quotient $\mathsf{O}(3,1)/\mathsf{SO}^+(3,1)$ est effectivement isomorphe au groupe de Klein.

11.3. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Calculer $\mathsf{O}(V,b)$ et $\mathsf{SO}(V,b)$ si V est de dimension 1 (distinguer le cas où (V,b) est régulier du cas où (V,b) n'est pas régulier).

3. Soit (V,b) un espace quadratique quelconque, et $V = \mathrm{rad}(V,b) \perp V'$ sa décomposition en partie nulle et partie régulière (voir Proposition 5.1.6). Montrer à l'aide de la Proposition 7.1.1 que $\mathsf{O}(V,b) \cong \mathsf{O}(\mathrm{rad}(V,b),b) \times \mathsf{O}(V',b)$, et expliciter le premier facteur de ce produit de groupes. La plupart des résultats donnés dans cette section à propos du groupe $\mathsf{O}(V,b)$ suppose que (V,b) soit un espace quadratique régulier ; pourquoi est-ce une hypothèse raisonable dans ce contexte ?

4. Avec les notations de la Definition 11.2.3, montrer que $\mathsf{O}(r,s) \cong \mathsf{O}(s,r)$. Conclure qu'il peut y avoir deux espaces quadratiques non-isométriques ayant le même groupe orthogonal.

5. Plus généralement, sur un corps quelconque F, on dit que deux formes quadratiques q et q' sur un espace V sont *similaires* s'il existe un $a \in F^\times$ tel que $q'(\underline{x}) = a \cdot q(\underline{x})$. Montrer que, dans ce cas, $\mathsf{O}(V,q) \cong \mathsf{O}(V,q')$, mais que (V,q) et (V,q') ne sont pas nécessairement isométriques.

6. Sur le corps $\mathbb{C}$ on note $\mathsf{O}(n,\mathbb{C})$ pour le groupe orthogonal de l'unique (à isométrie près) espace régulier de dimension n, et $\mathsf{SO}(n,\mathbb{C})$ pour son sous-groupe d'isométries de déterminant 1. Donner leurs descriptions matricielles.

7. Décrire matriciellement le groupe orthogonal et le groupe orthogonal spécial de $\langle 1,1\rangle$ et de $\langle 1,-1\rangle$, et leurs centres, sur $\mathbb{F}_3$.

12. Anneau de Witt : définition

12.1. Un double monoïde

Rappelons la Definition 5.2.1 : si (V_1, b_1) et (V_2, b_2) sont des espaces quadratiques sur un corps F, alors aussi leur somme orthogonale $(V_1, b_1) \perp (V_2, b_2)$ est un tel espace quadratique : c'est la somme directe $V_1 \oplus V_2$ muni de la forme bilinéaire

$$b(\underline{v}_1 + \underline{v}_2, \underline{v}'_1 + \underline{v}'_2) = b_1(\underline{v}_1, \underline{v}'_1) + b_2(\underline{v}_2, \underline{v}'_2).$$

L'égalité évidente

$$\dim(V_1 \oplus V_2) = \dim(V_1) + \dim(V_2)$$

souligne le caractère *additif* de cette opération.

Lorsqu'on travaille "à isométrie près", nous avons par ailleurs déjà montré que

0. $(V_1, b_1) \perp (V_2, b_2)$ est régulier si et seulement si (V_1, b_1) et (V_2, b_2) sont réguliers,
1. $(V_1, b_1) \perp (V_2, b_2) \cong (V_2, b_2) \perp (V_1, b_1)$,
2. $((V_1, b_1) \perp (V_2, b_2)) \perp (V_3, b_3) \cong (V_1, b_1) \perp ((V_2, b_2) \perp (V_3, b_3))$,
3. $(V_1, b_1) \perp (\{\underline{0}\}, 0) \cong (V_1, b_1)$

dans la Propostion 5.2.6 ; et le Théorème 10.1.1 y ajoute que

4. si $(V, b) \perp (V_1, b_1) \cong (V, b) \perp (V_2, b_2)$ alors $(V_1, b_1) \cong (V_2, b_2)$.

Dans la suite nous allons noter $[(V, b)]$ pour la classe d'isométrie de l'espace quadratique (V, b). On peut alors résumer ces résultats comme :

Proposition 12.1.1 *L'ensemble des classes d'isométrie des espaces quadratiques réguliers sur un corps F est un monoïde commutatif simplifiable pour la somme orthogonale, noté $\mathcal{M}(F)$.*

Démonstration. Tout est évident—sauf peut-être le fait que $\mathcal{M}(F)$ est un *ensemble*. En effet, la collection de tous les espaces quadratiques sur F est une classe propre. Mais nous savons que, pour toute dimension n, toute classe $[(V, b)]$ contient (au moins) une forme diagonale $\langle d_1, ..., d_n \rangle$: ainsi le "nombre" de classes d'isométrie en dimension n est

$$\#\{[(V, b)] \mid \dim(V) = n\} \leq \#\{\langle d_1, ...d_n \rangle \mid d_i \in F\} \leq \#F^n.$$

Si on fait la réunion sur toutes les dimensions, on a donc

$$\#\mathcal{M}(F) \leq \# \cup_{n \in \mathbb{N}} F^n$$

ce qui est bien un ensemble (et non pas une classe propre). □

La régularité demandée des éléments de $\mathcal{M}(F)$ n'est pas vraiment essentiel pour ce résultat. Mais tout espace (V, b) se décompose en une partie nulle et une partie régulière,

$$(V, b) \cong (\mathrm{rad}(V, b), b) \perp (W, b) \cong \langle 0, ..., 0\rangle \perp (W, b),$$

et clairement l'espace $\langle 0, ..., 0\rangle$ est sans aucun intérêt pour l'étude du corps F ; c'est pourquoi on écarte les espaces non-réguliers dans la définition ci-dessus.

On peut non-seulement "additionner" deux espaces quadratiques—mais aussi les "multiplier". L'outil de l'algèbre linéaire dont on aura besoin pour cela, est :

Définition 12.1.2 *Le* produit tensoriel *de deux F-espaces vectoriels V_1 et V_2 est un F-espace $V_1 \otimes V_2$ muni d'une application bilinéaire* universelle $\tau\colon V_1 \times V_2 \to V_1 \otimes V_2$.

Cela veut dire que, pour tout F-espace V et toute application bilinéaire $t\colon V_1 \times V_2 \to V$, il existe une unique application linéaire $\hat{t}\colon V_1 \otimes V_2 \to V$ telle que $\hat{t} \circ \tau = t$; autrement dit, le diagramme suivant commute :

$$\begin{array}{ccc} V_1 \times V_2 & \xrightarrow{\ \tau\ } & V_1 \otimes V_2 \\ & {\scriptstyle \forall t} \searrow \quad \swarrow {\scriptstyle \exists ! \hat{t}} & \\ & V & \end{array}$$

Comme toute définition mathématique donnée par universalité, le produit tensoriel de V_1 et V_2 est défini "à unique isomorphisme près" ; c'est à dire, si on a deux applications bilinéaires universelles,

$$\tau\colon V_1 \times V_2 \to V \quad \text{et} \quad \tau'\colon V_1 \times V_2 \to V',$$

alors on peut montrer qu'il existe un unique isomorphisme $f\colon V \to V'$ tel que $f \circ \tau = \tau'$ (exercice). Rappelons une construction explicite du produit tensoriel d'espaces vectoriels :

Proposition 12.1.3 *Pour des espaces vectoriels V_1 et V_2, on peut construire une application bilinéaire universelle $\tau\colon V_1 \times V_2 \to V_1 \otimes V_2$ comme suit :*

- *d'abord on note*

$$W = \left\{ \sum_{i=1}^{r} a_i(\underline{v}_1^i, \underline{v}_2^i) \mid r \in \mathbb{N}, a_i \in F, (\underline{v}_1^i, \underline{v}_2^i) \in V_1 \times V_2 \right\}$$

  pour l'espace de toutes les combinaisons linéaires formelles de tous les éléments de $V_1 \times V_2$,

- *puis on note le sous-espace $S \subseteq W$ engendré par les éléments*

$$\begin{cases} (\underline{v}_1 + \underline{v}_1', \underline{v}_2) - (\underline{v}_1, \underline{v}_2) - (\underline{v}_1', \underline{v}_2) \\ (a\underline{v}_1, \underline{v}_2) - a(\underline{v}_1, \underline{v}_2) \\ (\underline{v}_1, \underline{v}_2 + \underline{v}_2') - (\underline{v}_1, \underline{v}_2) - (\underline{v}_1, \underline{v}_2') \\ (\underline{v}_1, a\underline{v}_2) - a(\underline{v}_1, \underline{v}_2) \end{cases}$$

  pour tout $\underline{v}_1, \underline{v}_1' \in V_1$ et $\underline{v}_2, \underline{v}_2' \in V_2$,

- *et finalement on pose $V_1 \otimes V_2 = W/S$ et $\tau\colon V_1 \times V_2 \to V_1 \otimes V_2\colon (\underline{v}_1, \underline{v}_2) \mapsto \underline{v}_1 \otimes \underline{v}_2$, où $\underline{v}_1 \otimes \underline{v}_2$ est la classe d'équivalence de $(\underline{v}_1, \underline{v}_2)$ dans le quotient.*

Dans la pratique, cela veut dire que l'on a

$$V_1 \otimes V_2 = \left\{ \sum_{i=1}^{r} \underline{v}_1^i \otimes \underline{v}_2^i \mid (\underline{v}_1^i, \underline{v}_2^i) \in V_1 \times V_2 \right\}$$

avec les opérations données par (extension par linéarité de)

$$\begin{cases} (\underline{v}_1 \otimes \underline{v}_2) + (\underline{v}_1' \otimes \underline{v}_2') = (\underline{v}_1 + \underline{v}_1') \otimes (\underline{v}_2 + \underline{v}_2') \\ a(\underline{v}_1 \otimes \underline{v}_2) = a\underline{v}_1 \otimes \underline{v}_2 = \underline{v}_1 \otimes a\underline{v}_2 \end{cases}$$

On appelle un élément $v_1 \otimes v_2 \in V_1 \otimes V_2$ un *tenseur pur* ; un élément quelconque de $V_1 \otimes V_2$ est donc une combinaison linéaire de tenseurs purs.

Si on a des bases $(\underline{e}_1, ..., \underline{e}_n)$ de V_1 et $(\underline{e}_1', ..., \underline{e}_m')$ de V_2, alors

$$(a_1\underline{e}_1 + ... + a_n\underline{e}_n) \otimes (b_1\underline{e}_1' + ... + b_m\underline{e}_m') = \sum_{i,j} a_i b_j (\underline{e}_i \otimes \underline{e}_j')$$

et donc plus généralement

$$\begin{aligned} \sum_i \underline{v}_1^i \otimes \underline{v}_2^i &= \sum_i \left(a_1^i\underline{e}_1 + ... + a_n^i\underline{e}_n \right) \otimes \left(b_1^i\underline{e}_1' + ... + b_m^i\underline{e}_m' \right) \\ &= \sum_i \sum_{k,l} a_k^i b_l^i (\underline{e}_k \otimes \underline{e}_l') \\ &= \sum_{k,l} (\sum_i a_k^i b_l^i)(\underline{e}_k \otimes \underline{e}_l') \end{aligned}$$

Ceci montre que la suite

$$(\underline{e}_1 \otimes \underline{e}_1', ..., \underline{e}_1 \otimes \underline{e}_m', \underline{e}_2 \otimes \underline{e}_1', ..., \underline{e}_2 \otimes \underline{e}_m', ..., \underline{e}_n \otimes \underline{e}_1', ..., \underline{e}_n \otimes \underline{e}_m')$$

des tenseurs purs des vecteurs de base (avec l'ordre lexicographique) est génératrice pour $V_1 \otimes V_2$. On peut aussi montrer que cette suite est libre (exercice), et donc c'est une base du produit tensoriel. On a donc

$$\dim(V_1 \otimes V_2) = \dim(V_1) \cdot \dim(V_2)$$

ce qui souligne le caractère *multiplicatif* du produit tensoriel.

Exemple 12.1.4 Le produit tensoriel de F^n et F^m peut être réalisé comme suit :

- on identifie $F^n \cong F^{n\times 1}$ et $F^m \cong F^{1\times m}$,
- un tenseur pur est alors donné par le produit matriciel

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} b_1 & \cdots & b_m \end{pmatrix} = \begin{pmatrix} a_1b_1 & \cdots & a_1b_m \\ \vdots & & \vdots \\ a_nb_1 & \cdots & a_nb_m \end{pmatrix}$$

- une somme de telles matrices est une matrice quelconque de taille $n \times m$, et on a donc $F^n \otimes F^m \cong F^{n\times m}$.

Par ailleurs, les bases canoniques de $F^{n\times 1}$ et $F^{1\times m}$ produisent par tenseurs purs la base canonique de $F^{n\times m}$.

On peut démontrer un tas de propriétés du produit tensoriel d'espaces vectoriels, mais on ne le fera pas ici—on pourra les retrouver dans toute bonne référence d'algèbre (multi-)linéaire.

Ce qui est important pour la théorie des espaces quadratiques, c'est l'observation que, pour deux espaces quadratiques (V_1, b_1) et (V_1, b_2), aussi le produit tensoriel $V_1 \otimes V_2$ porte une forme bilinéaire symétrique :

Définition 12.1.5 *Si (V_1, b_1) et (V_1, b_2) sont deux espaces quadratiques, alors leur* produit tensoriel *(aussi appelé* produit de Kronecker*) est l'espace quadratique $(V_1 \otimes V_2, b)$ défini sur les tenseurs purs par*

$$b(\underline{v}_1 \otimes \underline{v}_2, \underline{v}'_1 \otimes \underline{v}'_2) = b_1(\underline{v}_1, \underline{v}'_1) \cdot b_2(\underline{v}_2, \underline{v}'_2)$$

(et on étend par bilinéarité à tout $(V_1 \otimes V_2) \times (V_1 \otimes V_2)$).

Si on note q_1 et q_2 les formes quadratiques de (V_1, b_1) et (V_2, b_2), alors la forme quadratique q du produit tensoriel $(V_1 \otimes V_2, b)$ satisfait à

$$q(\underline{v}_1 \otimes \underline{v}_2) = q_1(\underline{v}_1) \cdot q_2(\underline{v}_2)$$

pour les tenseurs purs ; la formule pour un élément général de $V_1 \otimes V_2$ est bien plus compliquée. Par ailleurs, si on a des bases $(\underline{e}_1, ..., \underline{e}_n)$ et $(\underline{e}'_1, ..., \underline{e}'_m)$ pour (V_1, b_1) et (V_2, b_2), et donc des matrices symétriques $B_1 \in F^{n\times n}$ et $B_2 \in F^{m\times m}$, alors pour la base de $V_1 \otimes V_2$ des tenseurs purs $\underline{e}_i \otimes \underline{e}'_j$ (avec ordre lexicographique), on trouve pour $(V_1 \otimes V_2, b)$ la matrice symétrique

$$\begin{pmatrix} \beta_{11}B_2 & \cdots & \beta_{1n}B_2 \\ \vdots & & \vdots \\ \beta_{n1}B_2 & \cdots & \beta_{nn}B_2 \end{pmatrix} \in F^{nm\times nm}$$

où on a écrit $B_1 = (\beta_{ij})_{i,j}$ (et ceci est ce qu'on appelle plus généralement le *produit de Kronecker* de deux matrices).

Exemple 12.1.6 Si $a, b \in F$ alors le produit tensoriel des espaces $\langle a\rangle = (F, q_1(x) = ax^2)$ et $\langle b\rangle = (F, q_2(x) = bx^2)$ est l'espace $F \otimes F \cong F$ muni de la forme $q(x) = abx^2$. Pour s'en convaincre, il suffit de noter que le produit de Kronecker des "matrices" de $\langle a\rangle$ et de $\langle b\rangle$ est bel et bien (ab).

On peut démontrer que :

Proposition 12.1.7 *Pour des espaces quadratiques (V_1, b_1), (V_2, b_2) et (V_3, b_3) quelconques,*

1. *si (V_1, b_1) et (V_2, b_2) sont réguliers, alors $(V_1, b_1) \otimes (V_2, b_2)$ l'est aussi,*
2. *$(V_1, b_1) \otimes (V_2, b_2) \cong (V_2, b_2) \otimes (V_1, b_1)$,*
3. *$((V_1, b_1) \otimes (V_2, b_2)) \otimes (V_3, b_3) \cong (V_1, b_1) \otimes ((V_2, b_2) \otimes (V_3, b_3))$,*
4. *$(V_1, b_1) \otimes \langle 1\rangle \cong (V_1, b_1)$,*
5. *$(V_1, b_1) \otimes ((V_2, b_2) \perp (V_3, b_3)) \cong ((V_1, b_1) \perp (V_2, b_2)) \otimes ((V_1, b_1) \perp (V_3, b_3))$*

Démonstration. Exercice. □

Exemple 12.1.8 Le produit tensoriel de $\langle a_1, ..., a_n\rangle$ avec $\langle b_1, ..., b_m\rangle$ est (à isométrie près) l'espace $\langle a_1b_1, ..., a_1b_m, a_2b_1, ..., a_2b_m, ..., a_nb_1, ..., a_nb_m\rangle$. En effet, il suffit d'écrire $\langle a_1, ..., a_n\rangle = \langle a_1\rangle \perp ... \perp \langle a_n\rangle$ et $\langle b_1, ..., b_m\rangle = \langle b_1\rangle \perp ... \perp \langle b_m\rangle$, puis d'exploiter les règles de calcul de la Proposition 12.1.7.

Bien sûr, si on passe aux classes d'isométries d'espaces quadratiques réguliers, on peut compléter la Proposition 12.1.1 par :

Proposition 12.1.9 *L'ensemble $\mathcal{M}(F)$ des classes d'isométrie des espaces quadratiques réguliers sur un corps F est un monoïde commutatif pour le produit tensoriel ; le produit tensoriel est distributif par rapport à la somme orthogonal.*

La combinaison des Propositions 12.1.1 et 12.1.9 peut être résumée joliment par :

Théorème 12.1.10 *L'ensemble $\mathcal{M}(F)$ des classes d'isométrie des espaces quadratiques réguliers sur un corps F est un* rig [1] *commutatif, simplifiable pour la somme.*

12.2. Groupe de Grothendieck et anneau de Witt

Le rig $\mathcal{M}(F)$ n'est pas un anneau : il manque des "négatifs" ! On va y remédier, comme suit.

De façon générale, si $M = (M, +, 0)$ est un monoïde commutatif et simplifiable, alors

$$(m, n) \sim (m', n') \iff m + n' = m' + n$$

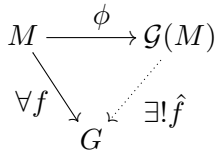
est une relation d'équivalence [2] sur $M \times M$; on va noter $(\!(m, n)\!)$ la classe d'équivalence d'un couple (m, n). Le quotient $\mathcal{G}(M) = M \times M/\!\sim$ est un groupe commutatif pour

$$(\!(m, n)\!) + (\!(m', n')\!) = (\!(m + m', n + n')\!) \quad , \quad 0 = (\!(0, 0)\!) \quad \text{et} \quad -(\!(m, n)\!) = (\!(n, m)\!).$$

De plus, l'application

$$\phi\colon M \to \mathcal{G}(M)\colon m \mapsto (\!(m, 0)\!)$$

est un homomorphisme injectif de monoïdes, qui est universel : pour tout groupe commutatif $(G, +, 0)$ et tout homomorphisme de monoïdes $f\colon M \to G$ il existe un unique homomorphisme de groupes $\hat{f}\colon \mathcal{G}(M) \to G$ tel que $\hat{f} \circ \phi = f$:



En mots, le groupe $\mathcal{G}(M)$ est le "plus petit" groupe contenant le monoïde M. (Exercice : détailler les arguments.) Cette construction porte un nom :

1. En anglais on dit *ring* pour un anneau ; un *rig* est un *ring without n(egatives)*—un "anneau sans négatifs". Formellement : un rig est un double monoïde $(M, +, 0, \cdot, 1)$ où $(M, +, 0)$ est commutatif et on a les distributivités $x(y + z) = xy + xz$ et $(x + y)z = xz + yz$, et l'annulation $0x = 0 = x0$. Un rig est commutatif si $xy = yx$. Un rig est un anneau si et seulement si $(M, +, 0)$ est un groupe.

2. Intuitivement, la relation d'équivalence $(m, n) \sim (m', n')$ exprime que "$m - n = m' - n'$"... sauf que cette soustraction n'existe pas nécessairement dans M !

Définition 12.2.1 *Si $(M,+,0)$ est un monoïde commutatif simplifiable, alors le groupe commutatif $(\mathcal{G}(M),+,0)$ est le* groupe de Grothendieck [3] *de M.*

L'exemple le plus simple – et le plus connu – est le groupe de Grothendieck du monoïde $(\mathbb{N},+,0)$ (qui est commutatif et simplifiable) : c'est $(\mathbb{Z},+,0)$. Mais bien sûr $\mathbb{Z}$ est un anneau, et on comprend bien que la multiplication dans $\mathbb{Z}$ est aussi définie par la multiplication dans $\mathbb{N}$. Aussi dans le cas général, si $(M,+,0,\cdot,1)$ est un rig commutatif qui est simplifiable pour $+$, alors on vérifie sans difficulté (exercice !) que son groupe de Grothendieck $(\mathcal{G}(M),+,0)$ est un anneau commutatif pour

$$(\!(m,n)\!)\cdot(\!(m',n')\!) = (\!(mm'+nn', mn'+nm')\!) \quad \text{et} \quad 1 = (\!(1,0)\!).$$

Pour simplifier nos notations dans la suite, observons que, dans $\mathcal{G}(M)$, on a

$$(\!(m,n)\!) = (\!(m,0)\!) + (\!(0,n)\!) = (\!(m,0)\!) - (\!(n,0)\!) = \phi(m) - \phi(n)$$

pour l'inclusion $\phi\colon M \to \mathcal{G}(M)$ qui identifie m avec $(\!(m,0)\!)$; ainsi il est tout à fait sensé de noter

$$(\!(m,n)\!) = m - n,$$

tout en se rappelant que ceci n'est pas nécessairement une soustraction dans M, mais une expression formelle dans $\mathcal{G}(M)$, qui néanmoins se *comporte* comme une soustraction !

Par conséquent, on peut définir :

Définition 12.2.2 *L'*anneau de Grothendieck-Witt *d'un corps F est $\mathcal{G}(\mathcal{M}(F))$.*

Les éléments de l'anneau $\mathcal{G}(\mathcal{M}(F))$ sont donc les "différences formelles" de classes d'isométrie d'espaces quadratiques réguliers sur F : des expressions comme $[(V_1,b_2)]-[(V_2,b_2)]$ pour (V_1,b_2) et (V_2,b_2) des espaces quadratiques réguliers sur F.

Aussi élégante qu'elle soit, cette construction s'avère quelque peu problématique pour l'étude d'un corps F :

Exemple 12.2.3 Pour tout corps fini $\mathbb{F}_q$, les espaces réguliers sont $\langle 1,...,1\rangle$ et $\langle 1,...,1,\varepsilon\rangle$; ainsi l'ensemble $\mathcal{M}(\mathbb{F}_q)$ est le même, quelque soit q. De plus, les opérations de somme et produit sur $\mathcal{M}(\mathbb{F}_q)$ sont les mêmes, quelque soit q, donc aussi l'anneau $\mathcal{G}(\mathcal{M}(\mathbb{F}_q))$ est le même pour tout q. Cet anneau semble donc sans intérêt pour l'étude de $\mathbb{F}_q$.

Exemple 12.2.4 Sur un corps quelconque F, on peut calculer dans l'anneau $\mathcal{G}(\mathcal{M}(F))$ que

$$[\langle d_1\rangle] + [\langle d_1\rangle] = [\langle d_1\rangle \perp \langle d_2\rangle] = [\langle d_1, d_2\rangle]$$

et en particulier, pour $d \in F^\times$,

$$[\langle d\rangle] + [\langle -d\rangle] = [\langle d, -d\rangle] = [\langle 1,-1\rangle].$$

Notons que cette dernière expression n'est pas nécessairement zéro dans $\mathcal{G}(\mathcal{M}(F))$—autrement dit, l'élément $[\langle -d\rangle]$ n'est pas l'opposé de $[\langle d\rangle]$!

3. D'après Alexander Grothendieck (1928–2014), médaille Fields en 1966.

Les exemples indiquent que l'anneau $\mathcal{G}(\mathcal{M}(F))$ est quelque peu "trop grand". L'idée brillante de E. Witt a été que, non pas toutes les formes quadratiques *régulières* sur F, mais plutôt les formes quadratiques *anisotropes* sont importantes pour l'étude de F. Heureusement, on a démontré que toute forme régulière se décompose en une partie hyperbolique et une partie anisotrope—voir la Proposition 9.2.4 ainsi que le Théorème 10.1.2. On veut donc "annihiler" la partie hyperbolique des éléments de $\mathcal{G}(\mathcal{W}(F))$; et tel un vrai seigneur des anneaux, on le fera en quotientant par un idéal :

Proposition 12.2.5 *Dans l'anneau $\mathcal{G}(\mathcal{M}(F))$, l'idéal engendré par le plan hyperbolique est l'ensemble des espaces hyperboliques et leurs opposés, $\mathcal{I} = \{m[\langle 1, -1\rangle] \mid m \in \mathbb{Z}\}$.*

Démonstration. Un espace hyperbolique est (par définition) isométrique à $m\langle 1, -1\rangle$ (pour $m \in \mathbb{N}_0$), et $m[\langle 1, -1\rangle] = [m\langle 1, -1\rangle]$; ainsi $\mathcal{I} = \{m[\langle 1, -1\rangle] \mid m \in \mathbb{Z}\}$ est effectivement l'ensemble des espaces hyperboliques et leurs opposés. Pour tout espace régulier $(V, b) \cong \langle d_1, ..., d_n\rangle$ (avec $d_i \neq 0$) on peut calculer que

$$(V, b) \otimes m\langle 1, -1\rangle \cong \langle d_1, ..., d_n\rangle \otimes m\langle 1, -1\rangle \cong m\langle d_1, -d_1, ..., d_n, -d_n\rangle \cong mn\langle 1, -1\rangle,$$

et il suit que $\mathcal{I}$ est un idéal de $\mathcal{G}(\mathcal{M}(F))$. □

Définition 12.2.6 *L'*anneau de Witt *d'un corps F est le quotient $\mathcal{W}(F) = \mathcal{G}(\mathcal{M}(F))/\mathcal{I}$*

Ecrivons $[\![(V, b)]\!]$ pour l'élément de $\mathcal{W}(F)$ déterminé par un espace quadratique régulier (V, b) ; alors on a $[\![(V, b)]\!] = [\![(V', b')]\!]$ si et seulement si $[(V, b)] - [(V', b')] \in \mathcal{I}$. Par la Décomposition de Witt (Théorème 10.1.2), on sait que tout espace régulier se décompose en une partie hyperbolique et une partie anisotrope :

$$(V, b) \cong (V_h, b_h) \perp (V_a, b_a).$$

Ainsi on a en particulier que $[\![(V, b)]\!] = [\![(V_a, b_a)]\!]$. C'est à dire, dans l'anneau de Witt on identifie deux formes quadratiques régulières lorsqu'elles ont la même partie anisotrope. Mieux encore :

Proposition 12.2.7 *Les éléments de $\mathcal{W}(F)$ sont en bijection avec les classes d'isométrie de formes quadratiques anisotropes sur F.*

Démonstration. Soit $d \in F^\times$, alors on peut calculer dans $\mathcal{W}(F)$ que

$$[\![\langle d\rangle]\!] + [\![\langle -d\rangle]\!] = [\![\langle d, -d\rangle]\!] = [\![\langle 1, -1\rangle]\!] = [\![0]\!]$$

et donc $-[\![\langle d\rangle]\!] = [\![\langle -d\rangle]\!]$. Ainsi, pour tout espace régulier $(V, b) \cong \langle d_1, ..., d_n\rangle$ on trouve (par induction sur n) que

$$-[\![\langle d_1, ..., d_n\rangle]\!] = [\![\langle -d_1, ..., -d_n\rangle]\!];$$

autrement dit, l'espace quadratique régulier $(V', b') = \langle -d_1, ..., -d_n\rangle$ "est" l'opposé de (V, b) dans $\mathcal{W}(F)$. Se limitant aux parties anisotropes de (V, b) et (V', b'), on obtient ainsi une surjection

$$\pi \colon \{F\text{-espaces quadratiques anisotropes}\} \to \mathcal{W}(F) \colon (V, b) \mapsto [\![(V, b)]\!].$$

Pour deux espaces anisotropes (V,b) et (V',b'), on a

$$\begin{aligned}
&[\![(V,b)]\!] = [\![(V',b')]\!] \quad \text{dans } \mathcal{W}(F)\\
\iff &[(V,b)] - [(V',b')] \in \mathcal{I} \quad \text{dans } \mathcal{G}(\mathcal{M}(F))\\
\iff &[(V,b)] - [(V',b')] = m[\langle 1,-1\rangle] \quad \text{dans } \mathcal{G}(\mathcal{M}(F))\\
\iff &[(V,b)] = [(V',b')] + m[\langle 1,-1\rangle] \quad \text{dans } \mathcal{G}(\mathcal{M}(F))
\end{aligned}$$

Quitte à échanger (V,b) et (V',b') on peut supposer que $m \in \mathbb{N}$, et donc le précédent est encore équivalent à $(V,b) \cong (V',b') \perp m\langle 1,-1\rangle$, mais puisque (V,b) est anisotrope par hypothèse, on doit avoir $m = 0$ et donc $(V,b) \cong (V',b')$. Ainsi, la surjection π se restreint à une bijection

$$\pi' \colon \left\{ \begin{array}{c} \text{classes d'isométrie de } F\text{-espaces} \\ \text{quadratiques anisotropes} \end{array} \right\} \to \mathcal{W}(F) \colon (V,b) \mapsto [\![(V,b)]\!]$$

comme voulu. □

Ainsi on retrouve la définition que E. Witt avait initialement donné de l'anneau qui porte aujourd'hui son nom :

Théorème 12.2.8 *L'anneau de Witt $\mathcal{W}(F)$ d'un corps F est aussi donné par l'ensemble des classes d'isométrie des espaces quadratiques anisotropes sur F, muni des opérations*

$$\left\{ \begin{array}{l} [(V_1,b_1)] + [(V_2,b_2)] = [\textit{partie anisotrope de } (V_1,b_1) \perp (V_2,b_2)] \\ [(V_1,b_1)] \cdot [(V_2,b_2)] = [\textit{partie anisotrope de } (V_1,b_1) \otimes (V_2,b_2)] \end{array} \right.$$

12.3. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Révision. Montrer que, étant défini par sa propriété universelle, le produit tensoriel $V_1 \otimes V_2$ est "unique à isomorphisme près". Reformuler la propriété universelle pour montrer un isomorphisme (canonique) de $\mathrm{Lin}(V_1 \otimes V_2, Z)$ avec $\mathrm{Lin}(V_1, \mathrm{Lin}(V_2, Z))$, quelque soit l'espace vectoriel Z. (Les *foncteurs* $V_1 \otimes -$ et $\mathrm{Lin}(V_1, -)$ sont *adjoints*.) Prendre $Z = F$ pour en déduire que $\dim(V_1 \otimes V_2) = \dim(V_1)\dim(V_2)$.

3. Révision. Montrer les isomorphismes (canoniques) pour le produit tensoriel d'espaces vectoriels :

(a) $V_1 \otimes (V_2 \otimes V_3) \cong (V_1 \otimes V_2) \otimes V_3$,

(b) $V_1 \otimes V_2 \cong V_2 \otimes V_1$,

(c) $F \otimes V \cong V$.

4. Révision. Montrer que $V_1^* \otimes V_2 \to \mathrm{Lin}(V_1, V_2) \colon (\varphi, \underline{v}) \mapsto \varphi(-)\underline{v}$ est un isomorphisme d'espaces vectoriels, son inverse étant donné par $f \mapsto \sum_i \underline{e}_i^* \otimes f(\underline{e}_i)$, où $\underline{e}_1, ..., \underline{e}_n$ est une base de V_2. En déduire que $\dim(V_1 \otimes V_2) = \dim(V_1)\dim(V_2)$.

5. Révision. Si $\underline{e}_1^1, ..., \underline{e}_n^1$ est une base de V_1 et $\underline{e}_1^2, ..., \underline{e}_m^2$ est une base de V_2, montrer que la suite $(\underline{e}_i^1 \otimes \underline{e}_j^2)_{i,j}$ (écrite dans l'ordre lexicographique, disons) est une base de $V_1 \otimes V_2$.

6. Révision. Montrer comment deux applications linéaires $f\colon V_1 \to W_1$ et $g\colon V_2 \to W_2$ définissent une application linéaire $f \otimes g\colon V_1 \otimes V_2 \to W_1 \otimes W_2$. Si on connaît des matrices pour f et g, comment peut-on calculer une matrice pour $f \otimes g$?

7. Montrer que le produit tensoriel (tout comme la somme orthogonale) de deux espaces quadratiques réguliers est un espace quadratique régulier. Montrer que le produit tensoriel (contrairement à la somme orthogonale) d'un espace régulier avec un espace hyperbolique est un espace hyperbolique. Indication : considérer des formes diagonales.

13. Anneau de Witt : exemples

En théorie algébrique des nombres, l'anneau de Witt est une des premières constructions pour la considération des formes quadratiques sur un corps F. Le but est de s'en servir pour étudier le corps F. C'est le sujet d'un cours spécialisé (voir les références) ; ici nous nous limitons à calculer quelques exemples.

13.1. Sur le corps des nombres complexes

Sur le corps $\mathbb{C}$ des nombres complexes, on sait par le Théorème 8.1.1 que tous les espaces quadratiques réguliers de dimension n sont isométriques à $\langle 1, ..., 1\rangle = n\langle 1\rangle$; en particulier, le plan hyperbolique sur $\mathbb{C}$ est $\langle 1, -1\rangle \cong \langle 1, 1\rangle$. Dans $\mathcal{W}(\mathbb{C})$ on "calcule à plan hyperbolique près", et donc

$$[\![n\langle 1\rangle]\!] = [\![\langle 1, 1, 1, ..., 1\rangle]\!] = \begin{cases} [\![\langle 1, -1, 1, -1..., 1\rangle]\!] = [\![\langle 1\rangle]\!] & \text{si } n \text{ est impair} \\ [\![\langle 1, -1, 1, -1..., -1\rangle]\!] = [\![0]\!] & \text{si } n \text{ est pair} \end{cases}$$

Ainsi l'anneau $\mathcal{W}(\mathbb{C})$ a exactement deux éléments—il est donc isomorphe à $\mathbb{Z}_2$, l'isomorphisme étant donné par la parité de la dimension :

$$\sigma\colon \mathcal{W}(\mathbb{C}) \to \mathbb{Z}_2\colon [\![(V, b)]\!] \mapsto \begin{cases} 1 & \text{si } \dim(V) \text{ est impaire} \\ 0 & \text{si } \dim(V) \text{ est paire} \end{cases}$$

De manière générale, comme déjà indiqué dans la Remarque 8.1.2, on peut montrer :

Théorème 13.1.1 *Un corps F est quadratiquement clos si et seulement si $\mathcal{W}(F) \cong \mathbb{Z}_2$.*

Démonstration. Si F est quadratiquement clos, alors on peut remplacer $\mathbb{C}$ par F dans l'argument ci-dessus pour montrer que $\mathcal{W}(F) \cong \mathbb{Z}_2$. Réciproquement, supposons que $\mathcal{W}(F) \cong \mathbb{Z}_2$; cela veut dire que tout espace quadratique régulier sur F, que l'on peut toujours décomposer comme

$$(V, b) \cong (V_h, b_h) \perp (V_a, b_a) \cong n\langle 1, -1\rangle \perp (V_a, b_a),$$

a pour sa partie anisotrope soit $[\![(V_a, b_a)]\!] = [\![\langle 1\rangle]\!]$, soit $[\![(V_a, b_a)]\!] = [\![0]\!]$. En particulier, pour $d \in F^\times$ on a $[\![\langle d\rangle]\!] = [\![\langle 1\rangle]\!]$, c'est à dire $\langle d\rangle \cong \langle 1\rangle$, et donc d est un carré. □

13.2. Sur le corps des nombres réels

Par le Théorème 8.2.3 on sait que les espaces quadratiques réguliers réels sont isométriques à $\langle 1, ..., 1, -1, ..., -1\rangle = r\langle 1\rangle \perp s\langle -1\rangle$; le couple (r, s) est la *signature* de l'espace. Par la décomposition de Witt on peut calculer dans l'anneau $\mathcal{W}(\mathbb{R})$ que

$$[\![r\langle 1\rangle \perp s\langle -1\rangle]\!] = r[\![\langle 1\rangle]\!] + s[\![\langle -1\rangle]\!] = r[\![\langle 1\rangle]\!] - s[\![\langle 1\rangle]\!] = (r-s)[\![\langle 1\rangle]\!].$$

En fait, l'application

$$\sigma\colon \mathcal{W}(R) \to \mathbb{Z}\colon [\![(V,b)]\!] \mapsto (r-s) \quad (\text{où } (V,b) \cong r\langle 1\rangle \perp s\langle -1\rangle)$$

ainsi obtenue est un isomorphisme d'anneaux (exercice). De manière générale, on peut même montrer :

Théorème 13.2.1 *Un corps F est ordonné par ses carrés*[1] *si et seulement si $\mathcal{W}(F) \cong \mathbb{Z}$.*

Pour une démonstration de ce résultat, on pourra consulter les références.

13.3. Sur un corps fini

Sur un corps fini $\mathbb{F}_q$, comme démontré dans le Théorème 8.3.5, les espaces quadratiques réguliers sont isométriques à soit $\langle 1, ..., 1\rangle = n\langle 1\rangle$, soit $\langle 1, ..., 1, \varepsilon\rangle = n\langle 1\rangle \perp \langle \varepsilon\rangle$, où ε est un non-carré au choix dans $\mathbb{F}_q$. Nous avons aussi déjà démontré que $\langle 1, 1\rangle \cong \langle \varepsilon, \varepsilon\rangle$ dans tout $\mathbb{F}_q$, dans la Proposition 8.3.4. Concernant le plan hyperbolique $\langle 1, -1\rangle$, nous devons distinguer deux possibilités :

– Soit -1 est un non-carré dans $\mathbb{F}_q$. On a alors que $\langle 1, -1\rangle \cong \langle 1, \varepsilon\rangle$ et on peut dresser la liste des éléments de $\mathcal{W}(\mathbb{F}_q)$ comme suit :

$[\![0]\!]$

$[\![\langle 1\rangle]\!]$

$[\![\langle \varepsilon\rangle]\!]$

$[\![\langle 1, 1\rangle]\!] = [\![\langle \varepsilon, \varepsilon\rangle]\!]$

$[\![\langle 1, \varepsilon\rangle]\!] = [\![0]\!]$

$[\![\langle 1, 1, 1\rangle]\!] = [\![\langle 1, \varepsilon, \varepsilon\rangle]\!] = [\![\langle 1, \varepsilon\rangle]\!] + [\![\langle \varepsilon\rangle]\!] = [\![0]\!] + [\![\langle \varepsilon\rangle]\!] = [\![\langle \varepsilon\rangle]\!]$

$[\![\langle \varepsilon, \varepsilon, \varepsilon\rangle]\!] = [\![\langle 1, 1, \varepsilon\rangle]\!] = [\![\langle 1\rangle]\!] + [\![\langle 1, \varepsilon\rangle]\!] = [\![\langle 1\rangle]\!] + [\![0]\!] = [\![\langle 1\rangle]\!]$

$$[\![n\langle 1\rangle]\!] = [\![\langle 1, ..., 1, 1\rangle]\!] = \begin{cases} [\![\langle 1, ..., 1, \varepsilon, ..., \varepsilon\rangle]\!] = [\![0]\!] & \text{si } n = 4m \\ [\![\langle 1, ..., 1, \varepsilon, ..., \varepsilon, 1\rangle]\!] = [\![\langle 1\rangle]\!] & \text{si } n = 1 + 4m \\ [\![\langle 1, ..., 1, \varepsilon, ..., \varepsilon, 1, 1\rangle]\!] = [\![\langle 1, 1\rangle]\!] & \text{si } n = 2 + 4m \\ [\![\langle 1, ..., 1, \varepsilon, ..., \varepsilon, 1, 1, 1\rangle]\!] = [\![\langle 1, 1, 1\rangle]\!] = [\![\langle \varepsilon\rangle]\!] & \text{si } n = 3 + 4m \end{cases}$$

1. Cela veut dire que la clause

$$x \leq y \iff y - x \text{ est un carré}$$

définit un ordre (compatible avec les operations du corps) sur F.

$$[\![n\langle 1\rangle \perp \langle\varepsilon\rangle]\!] = [\![n\langle 1\rangle]\!] + [\![\langle\varepsilon\rangle]\!] = \begin{cases} [\![0]\!] + [\![\langle\varepsilon\rangle]\!] = [\![\langle\varepsilon\rangle]\!] & \text{si } n = 4m \\ [\![\langle 1\rangle]\!] + [\![\langle\varepsilon\rangle]\!] = [\![\langle 1,\varepsilon\rangle]\!] = [\![0]\!] & \text{si } n = 1+4m \\ [\![\langle 1,1\rangle]\!] + [\![\langle\varepsilon\rangle]\!] = [\![\langle 1,1,\varepsilon\rangle]\!] = [\![\langle 1\rangle]\!] & \text{si } n = 2+4m \\ [\![\langle\varepsilon\rangle]\!] + [\![\langle\varepsilon\rangle]\!] = [\![\langle\varepsilon,\varepsilon\rangle]\!] = [\![\langle 1,1\rangle]\!] & \text{si } n = 3+4m \end{cases}$$

Autrement dit, on voit ici que

$$\mathcal{W}(\mathbb{F}_q) = \Big\{[\![0]\!], [\![\langle 1\rangle]\!], [\![\langle\varepsilon\rangle]\!], [\![\langle 1,1\rangle]\!]\Big\}$$

est un anneau à 4 éléments [2]. Lorsqu'on dresse les tables d'addition et de multiplication de cet anneau, on observe que $\mathcal{W}(\mathbb{F}_q) \cong \mathbb{Z}_4$.

– Soit -1 est un carré dans $\mathbb{F}_q$. Dans ce cas on a $\langle 1,-1\rangle \cong \langle 1,1\rangle$ et un calcul semblable à celui ci-dessus montre que

$$\mathcal{W}(\mathbb{F}_q) = \Big\{[\![0]\!], [\![\langle 1\rangle]\!], [\![\varepsilon]\!], [\![\langle 1,\varepsilon\rangle]\!]\Big\};$$

c'est donc aussi un anneau à 4 éléments. Par inspection de l'addition et de la multiplication, on obtient $\mathcal{W}(\mathbb{F}_q) \cong \mathbb{F}_2[\mathbb{Z}_2]$.

On peut élégamment formuler ce résultat graçe à :

Proposition 13.3.1 *Dans $\mathbb{F}_q$ (avec q impair),*

$$\begin{cases} -1 \text{ est un carré si et seulement si } q \equiv 1 \bmod 4 \\ -1 \text{ est un non-carré si et seulement si } q \equiv 3 \bmod 4 \end{cases}$$

Démonstration. Puisque q est impair, on n'a jamais $q \equiv 0 \bmod 4$ ou $q \equiv 2 \bmod 4$; la deuxième assertion ci-dessus est donc la négation de la première, et il suffit de démonter la première.

Si $-1 = a^2$ dans $\mathbb{F}_q$, alors $a^4 = 1$ et donc -1 est un élément d'ordre 4 dans le groupe multiplicatif $(\mathbb{F}_q^\times, \cdot, 1)$, et donc 4 divise l'ordre du groupe, soit $q-1$. On a donc $q-1 \equiv 0 \bmod 4$, ce qui est la même chose que $q \equiv 1 \bmod 4$.

Réciproquement, si $q \equiv 1 \bmod 4$ alors 4 divise $q-1$ et il existe donc un élément d'ordre 4 dans $(\mathbb{F}_q^\times, \cdot, 1)$, soit $x \in \mathbb{F}_q^\times$. Mais alors x^2 est d'ordre 2, donc nécessairement égal à -1 ; et -1 est ainsi un carré. □

Pour conclure en beauté, voici :

Théorème 13.3.2 *Pour q impair on a*

$$\begin{cases} \mathcal{W}(\mathbb{F}_q) \cong \mathbb{F}_2[\mathbb{Z}_2] \text{ si et seulement si } q \equiv 1 \bmod 4 \\ \mathcal{W}(\mathbb{F}_q) \cong \mathbb{Z}_4 \text{ si et seulement si } q \equiv 3 \bmod 4 \end{cases}$$

2. Il existe exactement 4 anneaux (unitaires) à 4 éléments : $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{F}_4$ et l'*anneau de groupe* $\mathbb{F}_2[\mathbb{Z}_2]$. En exercice on dressera les tables de somme et de produit de ces anneaux.

13.4. Exercices

1. Compléter tous les "exercices" marqués dans le texte.

2. Montrer que F est quadratiquement clos si et seulement si tout F-espace quadratique régulier de dimension 2 est un plan hyperbolique, si et seulement si tout F-espace quadratique régulier de dimension paire est un espace hyperbolique. Indication : Si, pour $d \in F^\times$, l'espace régulier $\langle 1, -d\rangle$ est isotrope, alors il existe $x, y \in F$ tels que $x^2 - dy^2 = 0$.

3. *Anneau d'un groupe G sur un corps F.* Soit un groupe $(G, \cdot, 1)$ et un corps F. Vérifier que l'ensemble

$$F[G] = \{f\colon G \to F \mid f \text{ est de support fini}\}$$

est un anneau pour les opérations

$$\begin{cases} f+g\colon G \to F\colon a \mapsto f(a)+g(a) \\ fg\colon G \to F\colon a \mapsto \sum\limits_{a=bc} f(b)g(c) \end{cases}$$

Si $|G| = n$, alors une fonction $f\colon A \to F$ est un n-uple $(f(a))_{a\in G} \in F^n$, que l'on note souvent par $\sum_{a\in G} f_a \underline{e}_a$ "comme si" les $\underline{e}_a$'s sont une base de F^n et les f_a's sont les coordonnées de f. Avec ses notations, les opérations de l'anneau $F[G]$ sont

$$\begin{cases} (\sum\limits_{a\in G} f_a\underline{e}_a) + (\sum\limits_{a\in G} g_a\underline{e}_a) = \sum\limits_{a\in G}(f_a+g_a)\underline{e}_a \\ (\sum\limits_{a\in G} f_a\underline{e}_a)(\sum\limits_{a\in G} g_a\underline{e}_a) = \sum\limits_{a\in G}(\sum\limits_{a=bc} f_b g_c)\underline{e}_a \end{cases}$$

Si le corps est aussi fini, disons $F = \mathbb{F}_q$, alors l'anneau $\mathbb{F}_q[G]$ compte q^n éléments.

4. Donner les 4 anneaux à 4 éléments : $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{F}_4$ et $\mathbb{F}_2[\mathbb{Z}_2]$ (donner leurs tables de somme et de produit). Dresser les tables de somme et de produit dans $\mathcal{W}(\mathbb{F}_q)$ (distinguer les cas où -1 est un carré ou non), et en déduire l'isomorphisme avec un des anneaux à 4 éléments.

5. Montrer que, pour tout corps fini $\mathbb{F}_q$, le groupe multiplicatif $(\mathbb{F}_q^\times, \cdot, 1)$ est cyclique. Indication : Sinon, il existe $n < q-1$ tel que $x^n = 1$ pour tous les $q-1$ éléments $x \in \mathbb{F}_q^\times$. Ainsi, tous les éléments de $\mathbb{F}_q^\times$ seraient racine du polynôme $X^n - 1 \in \mathbb{F}_q[X]$, qui ne peut avoir que n racines—contradiction.

6. Calculer les éléments inversibles dans $W(\mathbb{F}_q)$ (distinguer $q = 1+4k$ et $q = 3+4k$).

7. *Isotropie de formes quadratiques sur $\mathbb{Q}$.* On va s'intéresser aux formes quadratiques régulières $f \in \mathbb{Q}[X_1, ..., X_n]$; on supposera toujours que les formes sont diagonales : $f \cong \langle a_1, ..., a_n\rangle$ avec les $a_i \in \mathbb{Q}^\times$. On veut établir un critère pour l'isotropie de f, autrement dit, pour l'existence d'une solution rationnelle non-triviale à l'équation $f(X_1, ..., X_n) = 0$.

   (a) Montrer qu'il suffit de considérer des $f \cong \langle a_1, ..., a_n\rangle$ avec les $a_i \in \mathbb{Z}^\times$; on le fera désormais.

   (b) Montrer que, pour tout nombre premier $p \geq 2$, on peut écrire

$$\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_k\rangle \perp \langle p\rangle \otimes \langle b_{k+1}, ..., b_n\rangle$$

   avec tous les b_i non-divisibles par p ; on écrira cette décomposition comme $f \cong f_1^p \perp \langle p\rangle \otimes f_2^p$.

Un célèbre théorème de Hasse-Minkowksi implique que f est isotrope sur $\mathbb{Q}$ si et seulement si f est isotrope sur $\mathbb{R}$ et sur tous les $\mathbb{Q}_p$. Un tout aussi célèbre théorème de Springer implique que, pour tout nombre premier $p \geq 3$, $f \cong f_1^p \perp \langle p \rangle \otimes f_2^p$ est anisotrope sur $\mathbb{Q}_p$ si et seulement si f_1 et f_2 sont anisotropes sur $\mathbb{F}_p$.

(c) Montrer que tout f de dimension $n \geq 3$ sur $\mathbb{F}_p$ avec $p \geq 3$ est isotrope.

(d) En déduire que tout f de dimension $n \geq 5$ sur $\mathbb{Q}$ est isotrope si et seulement si elle est isotrope sur $\mathbb{R}$ et sur $\mathbb{Q}_2$.

Un résultat de Hilbert implique que, si f est de dimension 3 et f est isotrope sur tous les $\mathbb{Q}_p$ avec $p \geq 3$, alors f est aussi isotrope sur $\mathbb{Q}_2$. Les équations suivantes ont-elles des solutions non triviales dans $\mathbb{Q}$?

(e) $17x^2 + 26y^2 = z^2$

(f) $3x^2 + 15y^2 - 7z^2 = 0$

(g) $13x^2 + 26xy + 21y^2 - 11z^2 = 0$

Références

E. Artin, Geometric Algebra, Interscience Publishers Inc., New York-London, 1957.

J. W. S. Cassels, Rational quadratic forms, Academic Press Inc., London-New York, 1978.

B. Kahn, Formes quadratiques sur un corps, Soc. Math. France, Paris, 2008.

T.Y. Lam, Introduction to Quadratic Forms over Fields, Amer. Math. Soc., Providence, 2005.

D. Perrin, Cours d'Algèbre, Ellipses, Paris, 1996.

W. Scharlau, Quadratic and Hermitian forms, Springer-Verlag, Berlin, Heidelberg, New York and Tokyo, 1985.

J.-P. Serre, A Course in Arithmetic, Springer-Verlag, New York, 1973.