SOUS-GROUPES DISCRETS DE $\mathbb{R}^n$, RÉSEAUX

DIDIER AUROUX

1. Généralités sur les réseaux

1.1. Définitions, caractérisations.

Déf 1. *Soient* $e_1, \dots, e_m \in \mathbb{R}^n$ *indépendants, le sous-groupe additif de* $(\mathbb{R}^n, +)$ *engendré par les* e_i *est appelé* réseau de dimension m engendré par $e_1 \dots e_m$.

Cor 1. *Un réseau de dimension* m *est un groupe abélien libre (i.e. possédant une base) de rang* m.

Déf 2. *Une partie de* $\mathbb{R}^n$ *est* discrète *ssi son intersection avec toute boule de centre* 0 *est finie.*

Th 1. *Si* G *est un sous-groupe de* $\mathbb{R}^n$*, on a les équivalences suivantes :*
(i) G *est un réseau,*
(ii) G *est discret,*
(iii) G *est de type fini et admet une* $\mathbb{Z}$*-base* $\mathbb{R}$*-libre,*
(iv) G *est de type fini et* $\mathrm{rang}(G) = \dim_{\mathbb{R}}(\mathrm{Vect}_{\mathbb{R}}(G))$.
Si ces conditions sont vérifiées, toute famille $\mathbb{Z}$*-libre de* G *est* $\mathbb{R}$*-libre.*

Appl 1 (Approximation simultanée de Kronecker)**.** *Soit* $n \in \mathbb{N}^*$, $\theta = (\theta_1 \dots \theta_n) \in \mathbb{R}^n$. $\forall \varepsilon > 0$, $\exists q \in \mathbb{N}^*$, $\exists p_1 \dots p_n \in \mathbb{Z}$ *tels que* $\forall i$, $\|\theta_i - \frac{p_i}{q}\| \le \frac{\varepsilon}{q}$.

Remarques : - Quitte à se limiter au sous-espace engendré par un réseau, on peut toujours supposer qu'il est de dimension n.
- On notera simplement par la suite *réseau* un réseau R de dimension maximale, caractérisé en plus par le fait que $\mathbb{R}^n/R$ est compact.

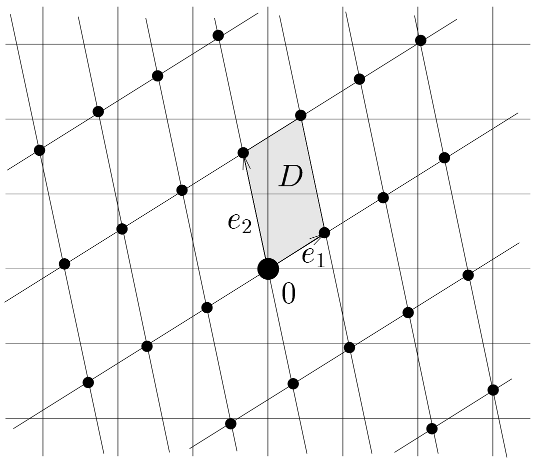

Fig. 1 Exemple de réseau dans $\mathbb{R}^2$.

Th 2. *Si* R *et* R' *sont deux réseaux de* $\mathbb{R}^n$*, sont équivalentes :*
(i) $\mathrm{Vect}_{\mathbb{Q}}(R) = \mathrm{Vect}_{\mathbb{Q}}(R')$,
(ii) $R + R'$ *est un réseau,*
(iii) $R \cap R'$ *est un réseau.*

1.2. Groupes abéliens de type fini.

Prop 1. *Si* G *est un sous-groupe de* $(\mathbb{Z}^n, +)$*, il existe une base* $(e_1 \dots e_n)$ *de* $\mathbb{Z}^n$ *et* $m_1 | \dots | m_n$ *des entiers tels que* $G = \bigoplus_{i=1}^n \mathbb{Z} m_i e_i$.

1 **Appl 2** (Théorème fondamental de structure)**.** *Tout groupe abélien de type fini est isomorphe à un produit direct* $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z} \times \mathbb{Z}^s$ *pour des entiers* r, s *et* n_i *tels que* $n_i | n_{i+1}, i = 1 \dots r-1$.

Date: 28 Janvier 2000.

1.3. **Identification des réseaux.** $GL_n(\mathbb{R})$ agit transitivement sur les bases de $\mathbb{R}^n$, donc sur les réseaux :

$$\begin{array}{ccc} GL_n(\mathbb{R}) \times \mathcal{B} & \to & \mathcal{B} \\ (M, (e_i)) & \mapsto & M.(e_i) \end{array}$$

L'orbite du réseau $\mathbb{Z}^n$ est exactement l'ensemble des réseaux de $\mathbb{R}^n$ et son stabilisateur est $SL_n(\mathbb{Z})$. L'application $u \mapsto u(\mathbb{Z}^n)$, de $GL(\mathbb{R}^n)$ dans l'ensemble des réseaux induit donc une bijection de $GL_n(\mathbb{R})/SL_n(\mathbb{Z})$ sur l'ensemble des réseaux de $\mathbb{R}^n$.

2. Quotients et volumes

2.1. **Domaine fondamental.**

Déf 3. *Si R est un réseau engendré par $(e_1 \dots e_n)$, son* domaine fondamental *est $D = \{\sum_{i=1}^n a_i e_i, 0 \leq a_i < 1\}$.*

Prop 2. $\mathbb{R}^n = \bigsqcup_{x \in R} (D + x)$

2.2. **Tore quotient.** Notons $\mathbb{T}^n$ le tore de dimension n ($\mathbb{T}^n = S^1 \times \dots \times S^1$), et $\phi : \mathbb{R}^n \to \mathbb{T}^n, (a_1 e_1 + \dots + a_n e_n) \mapsto (\exp(2\pi i a_j))_j$.

Lemme 1. *ϕ induit une bijection $\phi_{|D}$ de D dans $\mathbb{T}^n$.*

Th 3. *Si R est un réseau de $\mathbb{R}^n$, $\mathbb{R}^n/R$ est isomorphe à $\mathbb{T}^n$.*

Th 4. *Si R est un réseau m-dimensionnel de $\mathbb{R}^n$, $\mathbb{R}^n/R$ est isomorphe à $\mathbb{T}^m \times \mathbb{R}^{n-m}$.*

2.3. **Volumes.**

Déf 4. *Si X est une partie de $\mathbb{T}^n$, son* volume *est $v(X) = V(\phi^{-1}(X))$ où ϕ est la bijection $D \to \mathbb{T}^n$ et V le volume usuel sur $\mathbb{R}^n$.*

Le morphisme $\phi : \mathbb{R}^n \to \mathbb{T}^n$ de noyau R conserve localement le volume. Est-ce encore vrai globalement ?

Appl 3. *Si X est une partie bornée de $\mathbb{R}^n$ dont le volume existe, si $v(\phi(X)) \neq V(X)$ alors $\phi_{|X}$ n'est pas injective.*

Th 5 (Minkowski)**.** *Soient R un réseau n-dimensionnel de $\mathbb{R}^n$, D son domaine fondamental, X un convexe symétrique borné de $\mathbb{R}^n$. Si $V(X) > 2^n V(D)$ alors X contient un élément non nul de R.*

2 **Th 6** (Deux carrés)**.** *Si p est un nombre premier de la forme $4k+1$, alors p est somme de deux carrés.*

Th 7 (Quatre carrés)**.** *Tout entier positif est somme de quatre carrés.*

2.4. **Invariant d'un couple de réseaux.**

Lemme 2. *Si $B = (f_1 \dots f_n)$ et $B' = (f'_1 \dots f'_n)$ sont deux $\mathbb{Z}$-bases d'un réseau R, les domaines fondamentaux associés $D_B = \{\sum_{i=1}^n a_i f_i, 0 \leq a_i < 1\}$ et $D_{B'} = \{\sum_{i=1}^n a_i f'_i, 0 \leq a_i < 1\}$ ont même volume.*

Déf 5. *Le* volume fondamental $\mathrm{Vol}(R)$ *du réseau R est le volume $V(D)$ du domaine fondamental.*

Appl 4. *L'indice d'un sous-groupe G de $\mathbb{Z}^n$ est $[\mathbb{Z}^n : G] = \mathrm{Vol}(G)$.*

Déf 6. *L'*invariant affine *d'un couple de réseau (R, R') est $I(R, R') = \mathrm{Vol}(R)/\mathrm{Vol}(R')$, rapport invariant par changement de base utilisée pour le calcul des volumes.*

Appl 5. *Soient R et R' deux réseaux de $\mathbb{Z}$-bases respectives $\{e_i\}$ et $\{e'_i\}$. Pour tout réel $a > 0$, soit Q_a le pavé $\{\sum_{i=1}^n t_i e_i\}_{(t_1 \dots t_n) \in [-a,a]^n}$ et $\nu(a) = \mathrm{card}(R' \bigcap Q_a)$, alors $\lim_{a\to\infty} \frac{\nu(a)}{(2a)^n} = I(R, R')$.*

3. Réseaux unimodulaires

3.1. **Déterminants.** Soit q une forme quadratique, β_q sa forme polaire.

Lemme 3. *Le groupe $GL_{\mathbb{Z}}(R)$ des $\mathbb{Z}$-automorphismes de R est isomorphe à $GL_n(\mathbb{Z})$.*

Cor 2. *Le déterminant de q est le même dans toutes les $\mathbb{Z}$-bases de R.*

Déf 7. *Le R-*déterminant *de q est $\det_R(q) = \det([\beta_q(e_i, e_j)])$, $\forall (e_1 \dots e_n)$ $\mathbb{Z}$-base de R.*

Déf 8. *Le* déterminant *$\Delta(R)$ de R est le R-déterminant de la forme quadratique $x \mapsto \|x\|^2$.*

Prop 3. $\Delta(R) = (\mathrm{Vol}(R))^2$

Déf 9. *Un réseau R est* entier *si $\forall (x, y) \in R^2, (x|y) \in \mathbb{Z}$.*

Déf 10. *Un réseau R est* unimodulaire *ssi $\Delta(R) = 1$ et R est entier.*

Appl 6. *Si $n \leq 5$, tout réseau unimodulaire de $\mathbb{R}^n$ admet une $\mathbb{Z}$-base orthonormée.*

3.2. **Réseau dual.**

Déf 11. *Le réseau* dual *de R est $R^* = \{x \in \mathbb{R}^n ; \forall y \in R, (x|y) \in \mathbb{Z}\}$.*

Prop 4. *La base duale d'une base de R est une $\mathbb{Z}$-base de R^*.*

Prop 5. *Les déterminants d'un réseau et de son dual sont inverses l'un de l'autre.*

Prop 6. *Un réseau est entier ssi il est contenu dans son dual. Dans ce cas, l'indice $[R^* : R]$ est égal au déterminant de R. Un réseau est unimodulaire ssi il est égal à son dual.*

3.3. **Exemples.** Soit R_1 le réseau de $\mathbb{R}^2$ engendré par $(1, 0), (0, \sqrt{2})$. R_1 est clairement entier, mais $\Delta(R_1) = (\sqrt{2})^2 = 2 \neq 1$ donc R_1 n'est pas unimodulaire. Le réseau dual est $R_1^* = \mathbb{Z}(1, 0) \oplus \mathbb{Z}(0, \frac{\sqrt{2}}{2})$, qui est de déterminant $\frac{1}{2}$, et qui n'est pas égal à R_1 ce qui confirme que ce n'est pas un réseau unimodulaire.

Soit maintenant le réseau $R_2 = \mathbb{Z}(\sqrt{2}, 0) \oplus \mathbb{Z}(0, \frac{\sqrt{2}}{2})$, $\Delta(R_2) = 1$ mais R_2 n'est pas unimodulaire (non entier), et $R_2^* = \mathbb{Z}(\frac{\sqrt{2}}{2}, 0) \oplus \mathbb{Z}(0, \sqrt{2})$.

Références

[AB95] J.-M. Arnaudiès et J. Bertin, *Groupes, algèbres et géométrie*, Tome 2, Ellipses, 1995.

[BR74] A. Bouvier et D. Richard, *Groupes - observation, théorie, pratique*, 2ème édition (1979), Hermann, 1974.

[Mar96] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, Masson, 1996.

[ST87] I.N. Stewart et D.O. Tall, *Algebraic number theory*, second edition, Chapman & Hall, 1987.

4. Développement 1

Prop. *Si G est un sous-groupe de $(\mathbb{Z}^n,+)$, il existe une base $(e_1 \dots e_n)$ de $\mathbb{Z}^n$ et $m_1|\dots|m_n$ des entiers tels que $G = \bigoplus_{i=1}^n \mathbb{Z} m_i e_i$.*

Déf 12. *Si $x = (x_1 \dots x_n) \in \mathbb{Z}^n$, le* contenu *de x est* $\mathrm{cont}(x) = \mathrm{pgcd}(x_i)$.

Lemme 4. *Si $x_0 \in \mathbb{Z}^n$ est de contenu 1, $\exists H; \mathbb{Z}^n = H \oplus \mathbb{Z}x_0$.*

Démonstration. Soit (ε_i) la base canonique de $\mathbb{Z}^n$, $\mathbb{Z}^n = \bigoplus_{i=1}^n \mathbb{Z}\varepsilon_i$. x_0 s'écrit $\sum_{i=1}^n x_i\varepsilon_i$ et $\mathrm{cont}(x_0) = 1$ donc $\exists (u_i) \in \mathbb{Z}; \sum_{i=1}^n x_i u_i = 1$. Soit p le morphisme défini par

$$\begin{array}{ccc} \mathbb{Z}^n & \to & \mathbb{Z}x_0 \\ \sum_{i=1}^n \alpha_i\varepsilon_i & \mapsto & (\sum_{i=1}^n \alpha_i u_i)x_0, \end{array}$$

p est un projecteur : $p((\sum \alpha_i u_i)x_0) = (\sum \alpha_i u_i)(\sum x_i u_i)x_0 = (\sum \alpha_i u_i)x_0$. De plus $\mathrm{Im}\ p = \mathbb{Z}x_0$ donc p est surjectif. On a donc $\mathbb{Z}^n = \mathrm{Ker}\ p \oplus \mathbb{Z}x_0$. □

Démonstration. Soit $E = \{\mathrm{cont}(g); g \in G\}$, $E \neq \{0\}$ et E est une partie de $\mathbb{N}$ donc elle admet un plus petit élément non nul m_1. Soit $g_1 \in G; \mathrm{cont}(g_1) = m_1$, soit $e_1 = \frac{g_1}{m_1}$. On a $\mathrm{cont}(e_1) = 1$ et $m_1 e_1 \in G$. En appliquant le lemme précédent, on a $\mathbb{Z}^n = \mathbb{Z}e_1 \oplus \mathrm{Ker}\ p$.

Lemme 5. *$G = \mathbb{Z}m_1e_1 \oplus (\mathrm{Ker}\ p \cap G)$.*

Démonstration. On a donc $G = \mathrm{Ker}\ p_{|G} \oplus p_{|G}(G) = (\mathrm{Ker}\ p \cap G) \oplus \mathbb{Z}me_1$ pour un certain entier m.

- $p_{|G}(g_1) = p_{|G}(m_1e_1) = m_1e_1$ car p est un projecteur et donc $m_1e_1 \in \mathbb{Z}me_1$ donc $m|m_1$.
- Soit $g = me_1 + y$, $y \in (\mathrm{Ker}\ p \cap G)$. y s'écrit $\sum y_i\varepsilon_i$ et $e_1 = \sum \alpha_i\varepsilon_i$. $y \in \mathrm{Ker}\ p$ donc $\sum u_i y_i = 0$ et par définition du contenu, $\mathrm{cont}(g)\mathbb{Z} = (m\alpha_1 + y_1)\mathbb{Z} + \dots + (m\alpha_n + y_n)\mathbb{Z}$ donc $\sum (m\alpha_i + y_i)u_i \in \mathrm{cont}(g)\mathbb{Z}$ (i.e.) $m\sum \alpha_i u_i + 0 \in \mathrm{cont}(g)\mathbb{Z}$ (i.e.) $m \in \mathrm{cont}(g)\mathbb{Z}$ (i.e.) $\mathrm{cont}(g)|m$. Ceci implique que $\mathrm{cont}(g)|m_1$ et par construction de m_1, $\mathrm{cont}(g) = m_1$ et donc $m_1|m$.

Par conséquent, $m = m_1$, ce qui achève la démonstration du lemme. □

De plus, on vient de montrer que si $y \in \mathrm{Ker}\ p \cap G$, $\exists g \in G; y = g - m_1e_1$. D'après ce qui précède, $\mathrm{cont}(g) = m_1$ et donc $m_1|\mathrm{cont}(y)$. Nous allons achever la démonstration par récurrence en se basant sur le fait que si $r = \mathrm{rang}(G)$, $\mathrm{rang}(\mathrm{Ker}\ p \cap G) = r - 1$.

- $r = 1$: $G = \mathbb{Z}g_1$ avec g_1 de contenu minimal, notons $e_1 = \frac{g_1}{\mathrm{cont}(g_1)}$, alors $G = \mathbb{Z}m_1e_1$ et $\mathbb{Z}^n = \mathbb{Z}e_1 \oplus \mathrm{Ker}\ p$.
- Soit $r = \mathrm{rang}(G) > 1$. D'après l'étude précédente, on a $\mathbb{Z}^n = \mathbb{Z}e_1 \oplus \mathrm{Ker}\ p$ et $G = \mathbb{Z}m_1e_1 \oplus (\mathrm{Ker}\ p \cap G)$ et $\mathrm{rang}(\mathrm{Ker}\ p \cap G) = r - 1$ donc pas hypothèse de récurrence, $\mathrm{Ker}\ p = \mathbb{Z}e_2 \oplus \dots \oplus \mathbb{Z}e_n$, $\mathrm{Ker}\ p \cap G = \mathbb{Z}m_2e_2 \oplus \dots \oplus \mathbb{Z}m_ne_n$ avec $m_2|\dots|m_n$. Il suffit de montrer que $m_1|m_2$ pour achever la preuve : $\mathrm{cont}(m_2e_2) = m_2$ et $m_2e_2 \in \mathrm{Ker}\ p \cap G$ donc d'après la remarque suivant la preuve du dernier lemme, $m_1|\mathrm{cont}(m_2e_2) = m_2$.

□

Prop. *Si G est un groupe abélien libre de type fini, H un sous-groupe non nul, alors il existe une base $\{e'_1 \dots e'_n\}$ de G et $\{m_1 \dots m_n\}$ des entiers vérifiant $H = \bigoplus_{i=1}^n \mathbb{Z}m_ie'_i$ et $m_{i-1}|m_i$.*

Démonstration. Analogue à la démonstration de la proposition précédente en utilisant le lemme suivant :

Lemme 6. *Tout groupe abélien libre de type fini est isomorphe à* $\mathbb{Z}^n$.

□

Th (Théorème fondamental de structure)**.** *Tout groupe abélien de type fini est isomorphe à un produit direct* $\prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \times \mathbb{Z}^s$ *pour des entiers* r, s *et* n_i *tels que* $n_i | n_{i+1}, i = 1 \ldots r-1$.

Démonstration. **Lemme 7.** *Soit* x *un élément sans torsion (i.e. d'ordre infini) d'un groupe* G *abélien, alors* $\mathbb{Z}x/\mathbb{Z}nx = \mathbb{Z}/n\mathbb{Z}$.

Soit G un groupe abélien de type fini, possédant une partie génératrice $\{g_1 \ldots g_n\}$. On peut alors définir le morphisme surjectif $f : \mathbb{Z}^n \to G$ qui à $(z_1 \ldots z_n)$ associe $\sum_{i=1}^{n} z_i g_i$. On a donc $G \simeq \mathbb{Z}^n/\mathrm{Ker}\ f$, qui est un quotient de deux groupes libres (Ker f est un sous-groupe du groupe libre $\mathbb{Z}^n$). En utilisant la proposition précédente, on a $G \simeq (\bigoplus_{i=1}^{n} \mathbb{Z}e_i)/(\bigoplus_{i=1}^{n} \mathbb{Z}m_i e_i) \simeq \prod_{i=1}^{n} \mathbb{Z}e_i/\mathbb{Z}m_i e_i \simeq \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$ (d'après le lemme 7), avec $m_i | m_{i+1}$. A partir d'un certain rang, $m_i = 0$ et donc $\mathbb{Z}/m_i\mathbb{Z} = \mathbb{Z}$, ce qui achève la démonstration. □

5. Développement 2

Th (Minkowski). *Soient R un réseau n-dimensionnel de $\mathbb{R}^n$, D son domaine fondamental, X un convexe symétrique borné de $\mathbb{R}^n$. Si $V(X) > 2^n V(D)$ alors X contient un élément non nul de R.*

Démonstration. Considérons le réseau R' double du réseau R, de domaine fondamental $2D$, de volume $2^n V(D)$. Soit le tore $\mathbb{T}^n = \mathbb{R}^n/2R$, de volume $V(2D) = 2^n V(D)$. En reprenant les notations de l'application 3, $v(\phi(X)) \leq v(\mathbb{T}^n) = 2^n V(D) < V(X)$. Donc $\phi_{|X}$ n'est pas injective et il existe $x_1 \neq x_2$ deux points de X tels que $\phi(x_1) = \phi(x_2)$, c'est-à-dire $x_1 - x_2 \in 2R$. X est symétrique donc $-x_2 \in X$ et donc par convexité, $\frac{1}{2}(x_1 - x_2) \in X$, mais par construction $\frac{1}{2}(x_1 - x_2) \in R$, donc on vient d'exhiber un élément non nul de R dans X. □

Th (Deux carrés). *Si p est un nombre premier de la forme $4k+1$, alors p est somme de deux carrés.*

Démonstration. Soit p un nombre premier, $G = (\mathbb{Z}/p\mathbb{Z})^*$ est un groupe cyclique d'ordre $p-1 = 4k$. G contient donc un élément u d'ordre 4. Comme -1 est le seul élément d'ordre 2 de G, $u^2 \equiv -1[p]$. Soit R le réseau de $\mathbb{R}^2$ constitué des points (a,b), $a, b \in \mathbb{Z}$, vérifiant $b \equiv ua[p]$. C'est un sous-groupe de $\mathbb{Z}^2$ d'indice p et donc le volume du domaine fondamental est p.
D'après le théorème de Minkowski, le cercle de centre 0 et de rayon r contient un point non nul de R dès que $\pi r^2 > 4p$. Choisissons un tel rayon, avec la condition supplémentaire $r^2 < 2p$ ($r^2 = \frac{3p}{2}$ convient par exemple). Soit (a,b) le point non nul du réseau contenu dans le disque considéré. On a $0 \neq a^2 + b^2 \leq r^2 < 2p$. Modulo p, $a^2 + b^2 \equiv a^2 + u^2 a^2 \equiv 0$, donc $a^2 + b^2 = p$. □

Th (Quatre carrés). *Tout entier positif est somme de quatre carrés.*

Démonstration. Soit p un nombre premier. Si p est pair, on a $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$. Supposons maintenant que p soit impair. Si $u, v \in \mathbb{Z}$, u^2 et $-1 - v^2$ prennent chacun $\frac{p+1}{2}$ valeurs distinctes modulo p. Il existe donc $u, v \in \mathbb{Z}$ tels que $u^2 + v^2 + 1 \equiv 0[p]$.
Considérons alors le réseau R constitué des points (a,b,c,d) tels que $c \equiv ua + vb[p]$ et $d \equiv ub - va[p]$. R est alors d'indice p^2 dans $\mathbb{Z}^4$, donc le volume de son domaine fondamental est p^2. Une sphère 4-dimensionnelle centrée en l'origine, de rayon r, a un volume $\frac{\pi^2 r^4}{2}$ et on choisit r pour rendre ce volume supérieur à $16p^2$, et $r^2 < 2p$ ($r^2 = 1.9p$ par exemple). D'après le théorème de Minkowski, il existe donc un élément (a,b,c,d) non nul du réseau R dans cette sphère, et donc $0 \neq a^2 + b^2 + c^2 + d^2 \leq r^2 < 2p$. Modulo p, par définition de a, b, c, d, on a $a^2 + b^2 + c^2 + d^2 \equiv 0$ et donc $a^2 + b^2 + c^2 + d^2 = p$. Le théorème est donc prouvé pour tous les nombre premiers.
La fin de la preuve repose sur la stabilité de cette propriété par produit : $(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 + (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2$. □