martinetmath.u-bordeaux1.fr
Tél. +33 (0)5-40-00-60-96

Talence, le 2 septembre 1999

Jacques Martinet

Eva Bayer

Objet : Réseaux et Variétés Abéliennes

Chère Eva,

Je voudrais revenir sur ce que je t'ai dit à Rome en présence de Joseph Oesterlé.[1] Lorsque j'ai commencé cette lettre, à la fin du mois de juillet, je voulais simplement commenter la remarque suivante : *les géomètres algébristes, qui nous ont résolu tant de problèmes ces 20 dernières années, devraient bien être capables de construire* a priori *des variétés abéliennes correspondant via la théorie complexe à des réseaux célèbres comme $\mathbb{E}_8$ ou ceux de Coxeter-Todd, Barnes-Wall ou Leech. Encore faudrait-il qu'ils ne considèrent pas les variétés abéliennes seulement à isogénie près, ce qui est trop souvent le cas.*

En y pensant de temps à autres pendant les vacances, j'ai étoffé quelque peu mon projet. Toutefois, ce n'est pas une lettre sérieuse, dans le sens que je n'ai pas regardé soigneusement la littérature existante ni traité beaucoup d'exemples, ce qui empêche toute tentative de formuler des conjectures précises. Mais peut-être des gens plus compétents que moi dans le domaine des schémas pourront-ils apporter les compléments indispensables.

L'article qu'a écrit Anne-Marie Bergé pour ton colloque irlandais a été une source d'inspiration pour cette lettre, et permet en outre de préciser certaines de mes affirmations.

1. Soit V un espace vectoriel complexe, soit $\Lambda \subset V$ un réseau, et soit $T = V/\Lambda$ le tore quotient. C'est un groupe de Lie compact et connexe, et ces deux propriétés caractérisent du reste les tores complexes. On s'intéresse à ceux de ces tores qui possèdent un plongement projectif, que l'on appelle *variétés abéliennes*. Il revient au même de dire qu'ils sont des variétés algébriques (par le théorème de Chow), ou encore que le degré de transcendance sur $\mathbb{C}$ du corps $M(T)$ de leurs fonctions méromorphes est égal à leur dimension complexe $m = \dim_{\mathbb{C}} V$. (*A priori*, on n'a que la majoration $\operatorname{deg.tr.}(M) \leq m$).

Il n'y a pas de problème en dimension 1, qui est le cas des *courbes elliptiques* : la fonction $\wp$ de Weierstraß associée à Λ fournit une

[1] À quelques détails typographiques près, cette lettre est la copie de la lettre originale, augmentée de notes de bas de page issues de remarques de Joseph Oesterlé

fonction méromorphe non constante, et l'équation différentielle qu'elle vérifie définit à la fois un plongement projectif et une structure de variété algébrique ; ce genre de remarque s'applique du reste à toute surface de Riemann, quel que soit son genre.

2. La situation est radicalement différente à partir de la dimension complexe 2. Le degré de transendance de $M(T)$ est génériquement zéro, et il faut que le réseau vérifie certaines conditions de nature arithmétique pour qu'il existe ne serait-ce qu'une fonction méromorphe non constante. Je me souviens que Ramis m'a dit il y a un quart de siècle (alors que nous fréquentions tous deux la commission du C.N.R.S) qu'on ne savait presque rien des cas deg. tr. $(M) < m$. Je ne sais pas ce qu'il en est maintenant, mais, quoi qu'il en soit, nous nous limiterons au cas algébrique, qui est mieux connu. Encore un mot sur le cas général : on peut associer canoniquement à T un tore quotient T', qui est une variété abélienne à travers laquelle se factorisent tous les morphismes dans une variété abélienne ; les fonctions méromorphes sur T proviennent alors des fonctions méromorphes sur T'.

3. Soit h une forme hermitienne sur V, dont nous notons h_1 la partie réelle et h_2 la partie imaginaire ; h_1 et h_2 sont des formes ($\mathbb{R}$-)bilinéaires sur l'espace vectoriel réel V_0 de dimension $n = 2m$ sous-jacent à V.
• La condition $h(y,x) = \overline{h(x,y)}$ montre que h_1 est symétrique et que h_2 est alternée.
• Les identités $h(ix,y) = ih(x,y)$ et $h(x,iy) = -ih(x,y)$ entraînent l'identité $h(ix,iy) = h(x,y)$, d'où l'invariance des trois formes h, h_1 et h_2 par l'isomorphisme $\mathbb{R}$-linéaire $x \mapsto ix$ de V_0.
• En explicitant les relations ci-dessus, on voit que l'une quelconque des formes h, h_1, h_2 détermine les deux autres : on trouve

$$h_2(x,y) = h_1(x,iy)\,,\ \ h_1(x,y) = h_2(ix,y)\,,\ \text{ et}$$
$$h(x,y) = h_1(x,y) + i\,h_1(x,iy) = h_2(ix,y) + i\,h_2(x,y)\,.$$

On en déduit que l'on a $\operatorname{rg} h_1 = \operatorname{rg} h_2 = 2\ \operatorname{rg}_{\mathbb{C}} h$.
• Comme $h_1(x,x) = h(x,x)$, la signature de h_1 est le double de celle de h ; en particulier, h est définie positive si et seulement si h_1 l'est.
• La donnée de h définie positive sur V fait du couple (V_0,h_1) un espace euclidien, que nous notons E, muni d'un automorphisme σ de carré $\sigma^2 = -\operatorname{Id}$, à savoir $x \mapsto ix$.
• Réciproquement, la donnée d'un couple (E,σ) comme ci-dessus permet de munir E d'une structure d'espace vectoriel complexe hermitien : il suffit de poser

$$i\,x = \sigma(x) \quad \text{ et } \quad h(x,y) = x.y + i\,(x.\sigma(y))\,.$$

4. Les variétés abéliennes sont caractérisées parmi les tores complexes par l'existence d'une forme hermitienne h définie positive à partie imaginaire entière sur le réseau (condition dite *condition de Riemann*, qui a découvert l'existence d'une telle forme dans le cas des jacobiennes de courbes). Cette “forme de Riemann” s'appelle une *polarisation*. Le couple $(V/\Lambda, h)$ s'appelle une *variété abélienne polarisée* ; c'est là une donnée plus précise que la simple donnée de V/Λ.

La relation $h_2(x, y) = h_1(x, iy)$ permet de traduire la condition de Riemann en termes purement euclidiens :

le réseau Λ *satisfait l'inclusion* $\sigma(\Lambda) \subset \Lambda^* \Leftrightarrow \Lambda \subset \sigma(\Lambda^*)$.

Finalement, la donnée d'une variété abélienne complexe polarisée équivaut à la donnée d'un triplet (E, σ, Λ) où E est un espace euclidien, σ un élément de son groupe orthogonal $\mathrm{O}(E)$ de carré $-\mathrm{Id}$, et Λ un réseau de E vérifiant la condition $\sigma(\Lambda) \subset \Lambda^*$, la polarisation correspondante ayant pour partie réelle le produit scalaire de E et pour partie imaginaire $x.\sigma(y) = -\sigma(x).y$. On note alors V l'espace E muni de la structure complexe définie par σ, et l'on note $n = 2m$ la dimension de E.

La structure du quotient $\Lambda^*/\sigma(\Lambda)$ est un invariant de la polarisation ; en particulier, l'ordre de ce quotient, i.e. l'indice $[\Lambda^* : \sigma(\Lambda)]$, est un invariant appelé le *degré de la polarisation*, et les polarisations de degré 1 sont appelées *polarisations principales*. Noter que le degré de la polarisation est le déterminant de Λ (qui est donc un entier) : cela résulte des égalités $\det(\sigma(\Lambda)) = \det(\sigma)^2 \det(\Lambda)$ et $\det(\Lambda)^{-1} = \det(\Lambda^*) = [\Lambda^* : \sigma(\Lambda)]^{-2} \det(\sigma(\Lambda))$.
[Dans les textes de variable complexe, le degré apparaît en considérant la dualité *pour la forme alternée*, partie imaginaire de la polarisation ; cela revient à considérer que le dual de Λ est $\sigma(\Lambda^*)$ au lieu de l'usuel Λ^* de la théorie euclidienne.]

Exemple. Soit Λ un réseau entier muni d'un automorphisme σ de carré $-\mathrm{Id}$. Alors, Λ^* contient $\sigma(\Lambda)$, et l'on attache canoniquement une variété abélienne au couple (Λ, σ) (qui ne dépend du reste que de la classe de conjugaison de σ dans $\mathrm{Aut}(\Lambda)$).

On a une notion naturelle de rationnalité pour les réseaux : Λ est *rationnel sur un corps* K s'il est proportionnel à un réseau possédant une matrice de Gram définie sur K ; cela ne dépend que de la classe de similitude de Λ. On a de même une notion de corps de définition pour les variétés abéliennes complexes.
Question 1. Soit Λ un réseau rationnel sur un corps K, et vérifiant l'inclusion $\sigma(\Lambda) \subset \Lambda^*$. Est-il possible de réaliser sur une extension de K

de petit degré, voire sur K lui-même, une variété abélienne isomorphe sur $\mathbb{C}$ à E/Λ ?[2]

En fait, du côté réseaux – tores, la notion naturelle est celle de similitude complexe. i.e. de similitude euclidienne commutant avec σ. Toutefois, si l'on s'impose la contrainte $\sigma(\Lambda) \subset \Lambda^*$, le rapport de similitude ne peut prendre que des valeurs discrètes. On peut normaliser Λ de façon que le degré de la polarisation soit minimal. Les autres choix sont alors les $\sqrt{\lambda}\,\Lambda$ pour $\lambda \in \mathbb{N}$.

5. Les jacobiennes constituent l'une des principales sources de variétés abéliennes. On peut voir la question d'un point de vue plus général, en séparant les cas complexes et algébriques.

• Soit X une variété anytique compacte et connexe. On peut lui associer son *tore d'Albanese* $T(X)$, en fait un couple $(q, T(X))$ où q est une application analytique de X dans $T(X)$, qui est universel pour la propriété suivante : toute application analytique de X dans un tore se factorise à travers $T(X)$ en le composé d'un homomorphisme analytique et d'une translation.[3]

[Il paraît que c'est Blanchard qui a construit le tore d'Albanese en toute généralité.]

• Soit X une variété algébrique complète et connexe définie sur un corps K algébriquement clos. On peut lui associer sa *variété d'Albanese* $A(X)$ ...

[Lors de mes lectures de jeunesse de Weil et de Lang, on ne savait construire en toute généralité cette variété que sur un corps algébriquement clos. J'ignore ce qu'il en est trente ans après.]

• Lorsque X est algébrique sur $\mathbb{C}$, le passage de $T(X)$ à $A(X)$ se fait via un plus grand quotient que j'ai déjà mentionné, lequel s'obtient en considérant l'ensemble des formes hermitiennes positives (mais non nécessairement définies) à partie imaginaire entière sur le réseau.

• Lorsque X est une courbe (projective non singulière) sur $\mathbb{C}$, autrement dit une surface de Riemann compacte et connexe, il y a identité entre $T(X)$ et $A(X)$. Qui plus est :

(1) La construction de $A(X)$ est possible sur le corps de définition de X quel que soit ce corps ;

(2) La polarisation donnée par la construction est principale.
[Il existe une notion de polarisation sur un corps arbitraire.]

C'est la variété jacobienne $\mathrm{Jac}(X)$ de X, de dimension égale au genre de X.

[2] modulo quelques restrictions sur le réseau

[3] Peut-être faudrait-il aussi choisir un point base ; idem dans le cas de $\mathrm{Jac}(X)$ considéré plus loin.

[Bavard m'a signalé qu'il existe aussi des "variétés d'Albanese" dans le cadre Riemannien, qui sont des tores réels, construits en considérant des formes harmoniques au lieu de formes holomorphes. Je ne crois pas qu'il y ait des constructions explicites utiles pour la théorie des réseaux.]

Exemple 5.1. . Les courbes $y^2 = x^3 + \lambda x$ ($\lambda \in \mathbb{C}$) fournissent des réseaux semblables à $\mathbb{Z}[i] \subset \mathbb{C}$ (du point de vue euclidien, on doit prendre $E = \mathbb{R}^2$, $\sigma(x, y) = (\pm y, \mp x)$ et $\Lambda = \mathbb{Z}^2$). Mais "semblable" ne signifie pas "isométrique", car les périodes de la fonction $\wp$ sont sauf erreur[4] transcendantes lorsque λ est algébrique. Exemples voisins : $y^2 = x^3 + \lambda$ avec $\mathbb{A}_2$ au lieu de $\mathbb{Z}^2$, et plus généralement les idéaux inversibles des ordres des corps quadratiques imaginaires. Ces exemples montrent que l'on a intérêt à considérer les diverses données à similitude ou isomorphisme près.
Exemple 5.2. Les voisinages-Kneser permettent de transformer une variété abélienne polarisée en une autre munie d'une polarisation de même degré.

L'utilisation des jacobiennes pour construire des réseaux ne va pas très loin, et cela pour trois raisons :

(1) À partir du genre 4, l'ensemble des jacobiennes est de codimension positive dans l'espace des modules de variétés abéliennes principalement polarisées ;
(2) D'après les théorèmes de Hurwitz et de Torelli, on a pour une courbe X de genre $g \geq 2$ la majoration $|\operatorname{Aut}(X)| \leq 84(g-1)$ et l'une des égalités $|\operatorname{Aut}(\operatorname{Jac}(X))| = 2|\operatorname{Aut}(X)|$ ou $\operatorname{Aut}(\operatorname{Jac}(X)) = \operatorname{Aut}(X)$; l'odre du commutant de σ dans $\operatorname{Aut}(\Lambda)$ ne doit donc pas dépasser $168(g-1)$, majoration rarement satisfaite dans le cas des "beaux" réseaux de dimension réelle $n \geq 8$.
(3) Buser et Sarnak ont montré dans les *Inventiones* que les jacobiennes se terrent dans un coin de l'espace des réseaux ayant un petit invariant d'Hermite.

Question 2. Que peut-on dire des réseaux attachés aux variétés d'Albanese de diverses variétés complètes définies sur $\mathbb{C}$, et en particulier, *quid* des surfaces compactes ?

Dans ce dernier cas, j'ai cru comprendre qu'il y a des résultats de classification assez précis. On devrait donc pouvoir dire quelque chose. J'ignore s'il y a des obstructions du type Hurwitz-Torelli.

6. La notion de voisinage-Kneser permet souvent de passer d'une variété abélienne polarisée à une autre en conservant le degré. Voici

[4] Supprimer "sauf erreur"

un exemple fabriqué à partir de l'exemple 5.1. On attache à $\mathbb{Z}^{2m}$ une variété abélienne de dimension m isomorphe au produit de m copies de la courbe $C : y^2 = x^3 - x$. Soit $\mathbb{D}_{2m} = \{x \in \mathbb{Z}^{2m} \mid \sum x_i \equiv 0 \mod 2\}$. C'est un sous-réseau d'indice 2 de $\mathbb{Z}^{2m}$ stable par σ, et définissant une variété abélienne $\mathcal{D}_m$ munie d'une polarisation de type $(2, 2)$. On considère ensuite $\mathbb{D}_{2m}^+ = \mathbb{D}_{2m} \cup (\mathbb{D}_{2m} + \frac{1}{2}(\varepsilon_1 + \cdots + \varepsilon_{2m}))$ ((ε_i) désigne la base canonique de $\mathbb{R}^{2m}$). Pour $m \equiv 0 \mod 4$, on obtient un réseau unimodulaire (et de toute façon stable par σ), donc de nouveau une variété abélienne principalement polarisée. Pour $m = 4$, elle est associée au réseau $\mathbb{E}_8$. Bien entendu, on est passé deux fois par une isogénie de degré 2, ne conservant pas la polarisation. C'est la raison d'être de ma remarque en tête de la lettre sur les isogénies. On évite les constructions triviales en travaillant avec des variétés abéliennes polarisées.

De la même façon, on passe de $\mathbb{Z}^{24}$ à Λ_{24} (le réseau de Leech) par une suite de voisinage-Kneser. (Parmi les réseaux pairs, l'unique voisin est le réseau unimodulaire pair de système de racines $24\,\boldsymbol{A}_1$.)

Il n'y a pas de raison de se limiter aux voisinages pour le nombre premier 2, ni même de rester dans $\mathbb{Z}$: des voisinages sur les anneaux d'Eisenstein (resp. de Hurwitz) permettent en effet de construire K_{12} (resp. Λ_{16}).

7. Considérons un réseau Λ rationnel sur un corps de nombres K tel que la classe d'isomorphisme de V/Λ contienne un modèle rationnel sur K. Pour fixer les idées, nous nous limiterons au cas $K = \mathbb{Q}$, bien qu'une telle restriction soit gênante dans les applications. (Par exemple, parmi les VAPP de dimension 3 (i.e. en dimension réelle 6), le réseau conjecturalement de plus grande densité, découvert par Conway et Sloane, n'est défini que sur un corps quadratique.)

On a des données résiduelles des deux côtés.

Pour tout p premier, $\Lambda/p\Lambda$ est un espace quadratique sur $\mathbb{F}_p$, avec bonne réduction (c'est-à-dire non dégénérescence) presque partout, précisément en-dehors des diviseurs de $\det(\Lambda)$.

De même, pour tout p premier, on a une notion de réduction en p pour les variétés abéliennes, également liée à une divisibilité.

On aimerait pouvoir comparer les ensembles de places à mauvaise réduction, mais il n'y a rien d'évident. En effet, cet ensemble est vide dans le cas des réseaux unimodulaires alors que, d'après Fontaine, il n'y a pas de variété abélienne non triviale sur $\mathbb{Z}$. Il faut sans doute faire intervenir d'autres invariants des réseaux que le déterminant, mais je n'ai rien à proposer. Le nombre premier 2, et plus généralement les nombres premiers $p \leq 2m + 1 = n + 1$ pour lesquels la réduction des variétés abéliennes peut être plus sauvage, pourraient jouer un rôle particulier. En tout cas, dans les exemples (tous unimodulaires) $\mathbb{Z}^2$, $\mathbb{E}_8$, Λ_{24} que nous avons examinés, il y a bonne réduction en-dehors de 2 (puisque, sauf erreur, une isogénie respecte le type de réduction aux places qui ne divisent pas son degré[5]).

Voici *un* exemple (particulièrement intéressant) mettant en jeu une jacobienne : la courbe K de Klein $x^3y+y^3z+z^3x = 0$ possède un groupe d'automorphismes d'ordre $168 = 84(g-1)$, ce qui permet de conclure que sa jacobienne correspond au réseau P_6 de Barnes, maintenant le réseau $\mathbb{A}_6^{(2)}$ de Craig (il semble que Serre soit pour beaucoup dans cette histoire) ; ici, K est irréductible modulo les p différents de 7, le réseau est entier de déterminant 7^3 et tout se passe bien en-dehors de $p = 7$.

Question 3. La parité des réseaux a-t-elle une interprétation en termes de variétés abéliennes ?

8. Je termine par un mot à propos des représentations des groupes finis. On a l'habitude d'utiliser les réseaux via leurs groupes d'automorphismes pour construire des groupes finis munis d'une représentation rationnelle fidèle. À l'envers, on peut dans certains cas dire des choses assez précises sur l'existence de réseaux associés à une représentation donnée. L'exemple de base est le théorème de Thompson, qui prédit l'existence d'un réseau unimodulaire pair attaché à une représentation irréductible sur $\mathbb{R}$ dont toutes les réductions sont irréductibles. C'est un sujet à l'ordre du jour, après le (peu lisible) livre de Kostrikin et Tiep et divers travaux (Tiep, Gow, Scharlau-Tiep, ...).

Ainsi, partant d'une représentation, on arrive à un réseau (peut-être pas toujours unique), et ensuite à une variété abélienne lorsque le groupe contient un élément d'image de carré $-\mathrm{Id}$.

Question 4. Peut-on sous certaines conditions passer directement d'une représentation à une variété abélienne ?

Voilà. Tout est bien vaseux, mais je ne suis pas capable d'être plus précis (ni même de garantir l'absence d'incorrections).

Bien à toi, Jacques MARTINET

---

[5] et même à toutes les places.