DIVISION ALGEBRAS AND THE HAUSDORFF-BANACH-TARSKI PARADOX

DIVISION ALGEBRAS AND THE HAUSDORFF-BANACH-TARSKI PARADOX

by Pierre Deligne and Dennis Sullivan

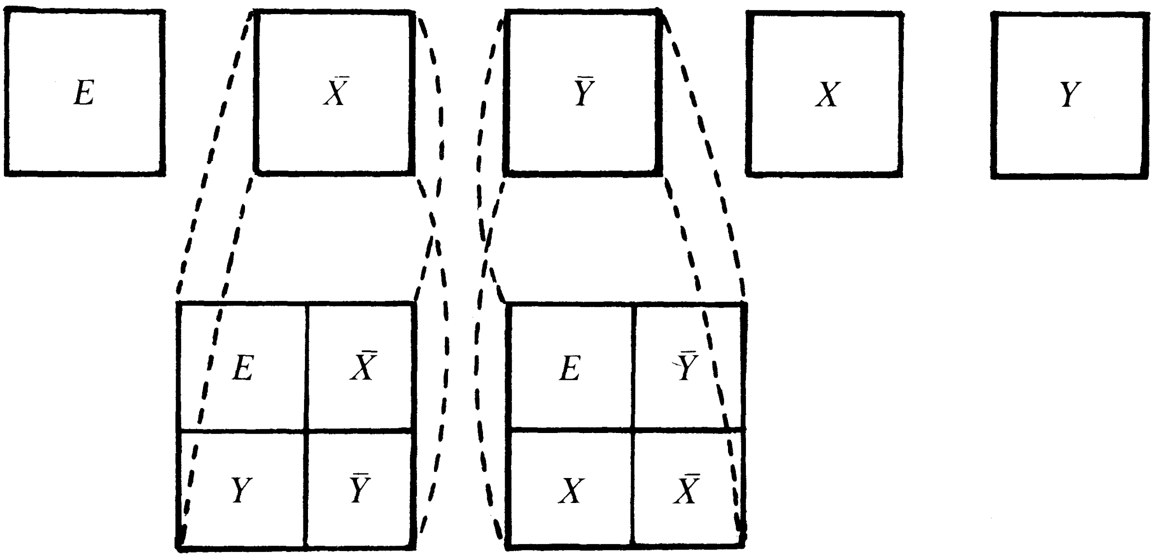
In this note we observe that a question raised by Dekker (1956) about rotations inspired by the Hausdorff-Banach-Tarski paradox can be answered using algebraic number theory. For motivation, we recall a form of the paradox.

Partition the free group in two generators F into the five sets E, X, $\bar{X}$, Y, $\bar{Y}$ consisting respectively of the identity and of the elements which, when written in reduced form, begin with x, x^{-1}, y or y^{-1}. If F acts freely on a sphere S, by rigid rotations, and if, using the axiom of choice, we choose a transversal T, i.e. a set with exactly one point in each orbit, the five subsets T, XT, $\bar{X}T$, YT, $\bar{Y}T$ form a partition of S. For economy of notation, we will write again E, X, $\bar{X}$, Y, $\bar{Y}$ for T, XT, $\bar{X}T$, YT, $\bar{Y}T$. The rotation by x moves $\bar{X}$ onto

$$S - X = E \cup \bar{X} \cup Y \cup \bar{Y}.$$

Similarly, y moves $\bar{Y}$ onto

$$S - Y = E \cup X \cup \bar{X} \cup \bar{Y}.$$



Thus we can reassemble from these 11 (actually 5) pieces 2 congruent spheres plus one congruent copy of the set E. This is a form of the Hausdorff-Banach-Tarski paradox which comes quickly from a free action of a free group on two generators (see Appendix A for the more precise form). Thus we have the question of Dekker (communicated by Jan Mycielski): do such actions really exist? The sphere must be odd-dimensional for topological reasons: a fixed point free map $f : S^d \to S^d$ must have vanishing Lefschetz number

$$L(f) = \sum(-1)^i \operatorname{Trace}(f\,;\, H_i(S^d)) = 1 + (-1)^d \deg(f)\,.$$

For a free action of a free group, the square of a non-trivial element will act by a map of degree $+1$ and this forces d odd. The dimension must be >1. These are the only conditions.

THEOREM. *For $n \geqslant 2$, there is a free non-abelian group of rigid rotations acting freely on the odd dimensional sphere S^{2n-1}.*

Remark. The corresponding orthogonal matrices can be chosen to have algebraic entries, and the group of matrices corresponds to a subgroup of the non-zero elements in a division algebra over a number field.

Remark. The theorem was proved by Dekker for n even [D].

Remark. Let $u : O(p) \times O(q) \to O(p+q)$ be the natural embedding:

$$u(A, B) = \text{matrix} \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

If $A \in O(p)$ and $B \in O(q)$ don't have any nonzero fixed vector, neither has $u(A, B)$. If $\sigma_1 : F \to O(p)$ and $\sigma_2 : F \to O(q)$ define free actions on S^{p-1} and S^{q-1}, $u(\sigma_1, \sigma_2)$ hence defines a free action of F on S^{p+q-1}. Using this remark, one could reduce the theorem to the two particular cases $n = 2$ and $n = 3$.

Proof. Let $k \subset \mathbf{R}$ be a real algebraic number field, and $k' \subset \mathbf{C}$ be a quadratic extension of k. We assume that $k' \not\subset \mathbf{R}$, i.e. that $k' \otimes_k \mathbf{R} = \mathbf{C}$. Let D be a division algebra of dimension n^2 over its center k', equipped with an anti-involution $*$ inducing on k' the complex conjugation. The $\mathbf{R}$-algebra $D \otimes_k \mathbf{R}$ is a simple algebra over its center $k' \otimes_k \mathbf{R} = \mathbf{C}$, hence isomorphic to $M(n, \mathbf{C})$. We assume that, for a suitable isomorphism between $D \otimes_k \mathbf{R}$ and $M(n, \mathbf{C})$, $*$ becomes transpose conjugate.

In term of an isomorphism as above, the elements u of D satisfying $uu^* = 1$ become unitary matrices. They operate on the unit sphere in $\mathbf{C}^n$. Furthermore, if $u \neq 1$, $u - 1$ is invertible in D so that the corresponding matrix does not have 1 as an eigenvalue. It hence acts without fixed point on the sphere.

The group $\Gamma := \{u \in D \mid uu^* = 1\}$ is the group of k-rational points of a k-form of the real algebraic group $U(n)$. For $n > 1$, the perfect subgroup $SU(n)$

of $U(n)$ is not trivial, and $U(n)$ is not solvable. The group Γ is dense in $U(n)$: skew adjoints elements of D are dense in the skew adjoint matrices in $M(n, \mathbf{C})$, and the Cayley transform $t \mapsto \dfrac{t-1}{t+1}$ is an homeomorphism from the space of skew-adjoint matrices in $M(n, \mathbf{C})$ to an open dense subset of $U(n)$, carrying skew adjoint elements of D into Γ. From this density, it results that, if $n > 1$, the linear group Γ is not solvable. By [Tits], it contains a non abelian free subgroup.

It remains to construct pairs $(D, *)$. A division algebra D with center k' admits an anti-involution $*$ inducing on k' the non trivial element $\mathrm{Gal}(k'/k)$, if and only if its class $\mathrm{cl}(D)$ in the Brauer group $\mathrm{Br}(k')$ of k' has a trivial image by the norm map $N_{k'/k} : \mathrm{Br}(k') \to \mathrm{Br}(k)$—see Appendix B. Class field theory provides an explicit computation of $\mathrm{Br}(k)$, and of $N_{k'/k}$, and tells which elements of $\mathrm{Br}(k')$ come from division algebras. From the explicit description it provides, existence of such D follows. A direct construction is given in Appendix C. When we choose an isomorphism of $D \otimes_k \mathbf{R}$ with $M(n, \mathbf{C})$, the involution $*$ becomes adjunction with respect to some hermitian form ϕ on $\mathbf{C}^n$, not necessarily positive definite: $\phi(ax, y) = \phi(x, a^* y)$. If h is self adjoint in D, $\mathrm{int}(h^{-1}) \circ *$ is adjunction, with respect to the form $\phi_h(x, y) = \phi(hx, y)$. For suitable h, ϕ_h is positive definite and $(D, \mathrm{int}(h^{-1}) \circ *)$ is of the type sought.

Appendix A

Consider $\phi : S' \cup S'' \to S - E$ as in the introduction, with S' and S'' two copies of the sphere S, and $\psi : S \to S'$ the obvious bijection. Consider as in the Schröder-Bernstein theorem the set S_e of points p in S with an even number of ancestors, namely for which there exists an integer $n \geqq 0$ with $p \in \mathrm{Im}(\phi\circ\psi)^n$ and $p \notin \mathrm{Im}(\psi \circ (\phi\circ\psi)^n)$. Consider also the set S_0 of those p in S for which there exists $n \geqq 0$ with $p \in \mathrm{Im}(\psi \circ (\phi\circ\psi)^n)$ and $p \notin \mathrm{Im}(\phi\circ\psi)^{n+1}$, and finally the set S_∞ of those p such that $p \in \mathrm{Im}(\phi\circ\psi)^n$ for any $n \geqq 0$. Consider similarly

$$S' \cup S'' = (S' \cup S'')_e \cup (S' \cup S'')_0 \cup (S' \cup S'')_\infty .$$

Then ψ induces a bijection from $S_e \cup S_\infty$ onto $(S' \cup S'')_0 \cup (S' \cup S'')_\infty$ and ϕ^{-1} from S_0 onto $(S' \cup S'')_e$. Combining these two we have a bijection $\chi : S \to S' \cup S''$ and a partition of S into finitely many pieces, the restriction of χ to each of these being a rotation.

APPENDIX B

Let K be a separable quadratic extension of a field k. We denote $x \mapsto \bar{x}$ the non trivial element $\mathrm{Gal}(K/k)$. Let D be a simple algebra with dimension n^2 over its center K. We will check the criterion of the text, for the existence of an involution of the second kind on D, i.e. of an anti-involution * of D, inducing $x \mapsto \bar{x}$ on K. The criterion is that $N_{K/k}\,\mathrm{cl}(D) = 0$ in $\mathrm{Br}(k)$.

Let us localize, for the étale topology, over $\mathrm{Spec}(k)$. This means making large enough étale extensions of scalars $\otimes_k k'$, and keeping track of the functoriality in k'. The field K becomes the separable quadratic extension $K' = K \otimes_k k'$ of k'. The algebra D becomes $D' = D \otimes_k k'$, and is of the form $D' = \mathrm{End}_{K'}(V')$, for V' a free module K'. The module V' is not determined uniquely by D', only up to homotheties (the corresponding projective space is uniquely determined).

For any K-module M, let M^- be the module deduced from M by the extension of scalars $^- : K \to K$, i.e. the module, unique up to unique isomorphism, provided with an anti-linear isomorphism $x \mapsto \bar{x} : M \xrightarrow{\sim} M^-$. Similarly for K'-modules. If $D' = \mathrm{End}(V')$, then $D^{-\prime} = \mathrm{End}(V'^-)$, and

$$(D \otimes_K D^-)' = \mathrm{End}(V' \otimes V'^-)\,.$$

Let W' be the fixed subspace of the anti-linear automorphism of $V' \otimes V'^-$ defined by $v \otimes \bar{w} \mapsto w \otimes \bar{v}$. It is the space of Hermitian forms on the dual of V'. One has $W' \otimes_{k'} K' = V' \otimes V'^-$. If $D_1 \subset D \otimes_K D^-$ is the fixed subspace of the anti-linear automorphism of $D \otimes_K D^-$ defined by $x \otimes \bar{y} \mapsto y \otimes \bar{x}$, then D'_1 is the k'-form of the K'-algebra $(D \otimes_K D^-)' = \mathrm{End}(V' \otimes V'^-)$ deduced from the k'-form W' of the K'-module $V' \otimes V'^- : D'_1 = \mathrm{End}_{k'}(W')$.

Involutions of the second kind on D' correspond one to one to non degenerate Hermitian forms on V', taken up to a factor (in k'^*). Those, in turn, by the "dual form" construction, correspond to "non degenerate" elements of W'. Again, one has to take them up to a factor. The projective space $\mathbf{P}(W')$ over k' is determined up to unique isomorphism by D'. It is hence (this is the point of localisation) defined over $k : \mathbf{P}(W') = P \otimes_k k'$, functorially in k'. The k-points of P (rather, the non degenerate points) parametrize the involutions of the second kind on D.

The functorial isomorphism $D'_1 = \mathrm{End}_{k'}(W')$ shows that P is the form of projective space (Severi-Brauer variety) attached to D_1. It has a rational point, and is then the ordinary projective space, if and only if D_1 is a matrix algebra.

This shows that D has involutions of the second kind if and only if the class of D_1 in $\mathrm{Br}(k)$ is trivial. This class is the required norm $N_{K/k}(\mathrm{cl}(D))$. In the localization spirit, this can be deduced from the fact that the homothety by $\lambda \in K'^*$ of V' induces on W' the homothety by $N_{K'/k'}(\lambda) \in k'^*$.

Appendix C

For $n \geqslant 3$, examples can be obtained as follows: take $k' = \mathbf{Q}[\zeta]$, with $\zeta = \exp(2\pi i/n)$, and $k = k' \cap \mathbf{R}$. Fix $a, b \in k^*$ and let D be the k'-algebra generated by X, Y, subject to

$$X^n = a\,, \qquad Y^n = b$$
$$XY = \zeta YX\,.$$

It admits the anti-involution $*$, inducing complex conjugation on k', defined by $\zeta^* = \zeta^{-1}$, $X^* = X$, $Y^* = Y$. The algebra D is of the type we require, provided it is a division algebra. This happens already with $a, b \in \mathbf{Z}$: take for a a prime congruent to 1 mod n, and for b an integer whose residue mod a has in the cyclic group of order n $(\mathbf{Z}/(a))^*/(\mathbf{Z}/(a))^{*n}$ an image of exact order n. For instance $n = 3$, $a = 7$, $b = 2$. For $n = 2$, one proceeds similarly with $k' = \mathbf{Q}[i]$, $\zeta = -1$, a congruent to 1 mod 4 and b not a square mod a. For instance, $a = 5$, and $b = 2$. In each case, the assumption on a ensures that k' embed in the a-adic completion $\mathbf{Q}_a$ of $\mathbf{Q}$, and the fact that D is a division algebra can be seen locally at a : $D \otimes_{k'} \mathbf{Q}_a$ is a division algebra with center $\mathbf{Q}_a$.

BIBLIOGRAPHY

[A] ALBERT, A. *Structure of algebras.* A.M.S. Colloquium Publ. 24 (1939).

[Sch] SCHARLAU, W. Zur Existenz von Involutionen auf einfachen Algebren. *Math. Zeitschr. 145* (1975), 29-32.

[Myc] MYCIELKSKI, Jan. Can one solve equations in groups? *Amer. Math. Monthly 84* (1977), 723-726.

[Tits] TITS, J. Free subgroups in linear groups. *Journal of Algebra 20* (1972), 250-270.

[D] DEKKER, Th. J. Decomposition of sets and spaces I, II. *Indig. Math. 18* (1956), 581-595, and *19* (1957), 104-107.

(Reçu le 8 mars 1982)

Pierre Deligne
Dennis Sullivan

Institut des Hautes Etudes Scientifiques
35, route de Chartres
91440 Bures-sur-Yvette
France