Cher Jean-Pierre Serre, voici avec un peu de retard quelques explications sur les déterminants de dimension 2.

Soient k un anneau commutatif unitaire et R une k-algèbre associative unitaire. Un déterminant (de dimension 2) de R/k est la donnée d'une forme quadratique[1]

$$q : R \to k$$

telle que $q(1) = 1$ et $q(xy) = q(x)q(y)$ pour tout $x, y \in R$. Autrement dit, c'est une forme quadratique qui est multiplicative (mais ce terme est déjà utilisé sous un sens plus faible en théorie de Pfister). On ne fait pas d'hypothèse de finitude sur le k-module R.

L'exemple important est le suivant. Si $\rho : R \to \mathrm{M}_2(k)$ un homomorphisme de k-algèbres, alors $\det \circ \rho$ est un déterminant de R/k. On peut bien entendu remplacer l'arrivée par une k-algèbre d'Azumaya et det par sa norme réduite. Je me propose de démontrer la proposition suivante, qui est une variante d'un résultat de Procesi. [2]

Proposition 1. *Supposons que k est un corps algébriquement clos. Tout déterminant de R/k est de la forme* $\det \circ \rho$ *pour une unique k-représentation ρ semisimple de dimension 2 de R.*

L'assertion d'unicité est bien connue (Brauer-Nesbitt), je me contenterai donc de justifier l'existence.

Étape 0 : *Quelques identités remarquables.* Fixons q un déterminant de R/k, avec pour l'instant k un anneau quelconque. Je noterai en général $f : R \times R \to k$, $f(x, y) = q(x + y) - q(x) - q(y)$ sa forme polaire, et aussi $t : R \to k$ la forme k-linéaire définie par

$$t(x) = f(x, 1).$$

En particulier, $f(x, x) = 2q(x)$ pour tout $x \in R$, et donc $t(1) = 2$. L'axiome de multiplicativité de q entraîne que pour tout $x, y, z \in R$,

$$f(zx, zy) = q(z)f(x, y) \tag{1}$$

Fixant x, y et polarisant les formes quadratiques restantes en z on obtient

$$f(zx, wy) + f(wx, zy) = f(z, w)f(x, y) \tag{2}$$

pour tout w, x, y, z dans R. En particulier, si $w = y = 1$ on constate que

$$f(x, z) = t(z)t(x) - t(zx) \tag{3}$$

pour tout $x, z \in R$. Ainsi, $t(zx) = t(xz)$ pour tout $x, z \in R$ (t est "centrale").[3]

[1] Par là j'entends simplement que $q(\lambda x) = \lambda^2 q(x)$ pour tout $x \in R$, $\lambda \in k$, et que l'application "polaire" $R \times R \to k$, $(x, y) \mapsto q(x + y) - q(x) - q(y)$ est k-bilinéaire.

[2] C. Procesi, *Finite dimensional representations of Algebras*, Israël J. of math. (1974).

[3] Une autre identité intéressante, bien que nous ne l'utiliserons pas, est l'identité de Frobenius (prendre $w = 1$ dans (2)) : pour tout $x, y, z \in R$ on a $t(x)t(y)t(z) - t(x)t(yz) - t(y)t(xz) - t(z)t(xy) + t(xyz) + t(xzy) = 0$. Une forme linéaire centrale $t : R \to k$ satisfaisant cette identité et $t(1) = 2$ est appelée pseudocaractère (de dimension 2) de R/k (Taylor, Rouquier). Quand 2 est inversible dans k, on peut vérifier que $q \mapsto t$ est une bijection entre déterminants et pseudocaractères de R/k.

ÉTAPE 1 : *Réduction au cas non-dégénéré.* On conserve les hypothèses et notations de l'étape 0. Je note $\mathrm{Ker}(f)$ le noyau de la forme bilinéaire symétrique f. Les relations (3) et $t(x) = f(x, 1)$ entraînent que $\mathrm{Ker}(f) = \{x, t(xz) = 0\ \forall z \in R\}$. En particulier, c'est un idéal bilatère de R car t est centrale. Notons aussi

$$\mathrm{Ker}(q) = \{x \in \mathrm{Ker}(f), q(x) = 0\}.$$

Il est stable par addition par l'identité de polarisation, par multiplication à droite et à gauche par R car q est multiplicative : c'est encore un idéal bilatère de R. On dit que q est *non dégénéré* si $\mathrm{Ker}(q) = 0$. Si $J \subset \mathrm{Ker}(q)$ est un idéal bilatère, la formule $\overline{q}(x + J) = q(x)$ définit un déterminant de la k-algèbre quotient R/J. Si $J = \mathrm{Ker}(q)$ ce déterminant $\overline{q}$ est non dégénéré.

ÉTAPE 2 : *Identité de Cayley-Hamilton.* Soit q un déterminant de R/k. Si $x \in R$ on pose

$$\chi(x) = x^2 - t(x)x + q(x) \in R.$$

(Ici $q(x)$ signifie $q(x).1$ bien entendu). On dit que q est de *Cayley-Hamilton* si $\chi(x) = 0$ pour tout $x \in R$.

Lemme 1. *Soit q un déterminant de R/k. Si $x \in R$ alors $\chi(x) \in \mathrm{Ker}(q)$. En particulier, si q est non dégénéré alors q est de Cayley-Hamilton.*

Preuve — Soient $x, z \in R$. On constate que

$$t(\chi(x)z) = t(x^2z) - t(x)t(xz) + q(x)t(z) = -f(x, xz) + q(x)t(z),$$

qui s'annule par (1). De plus, si $w = x^2 - t(x)x$ on constate que $f(w, 1) = -f(x, x) = -2q(x)$ et $q(w) = q(x)q(x - t(x)) = q(x)^2$ car $q(x - t(x)) = q(x) + t(x)^2 - t(x)^2 = q(x)$. Au final, $q(\chi(x)) = q(w) + q(x)^2 + q(x)f(w, 1) = 0$. □

Observons pour usage ci-dessous que la polarisation de l'identité de Cayley-Hamilton s'écrit $\chi(x + y) - \chi(x) - \chi(y) = xy + yx - t(x)y - t(y)x + f(x, y)\ \ \forall\ x, y \in R$.

ÉTAPE 3 : *Deux lemmes sur les éléments idempotents.*

Lemme 2. *Supposons que q est non dégénéré, que* $\mathrm{Spec}(k)$ *est connexe, et qu'il existe $e \in R$ un élément idempotent non trivial, i.e. différent de* 0 *et* 1*. Alors $t(e) = 1$, $q(e) = 0$ et le k-module eRe est libre de base e.*

Preuve — En effet, $q(e)^2 = q(e)$ et donc $q(e) = 0$ ou $q(e) = 1$ par hypothèse sur k. L'identité de Cayley-Hamilton entraîne que $e(1 - t(e)) = -q(e)$, et donc $q(e) = 0$ car e est non inversible dans R. Appliquant ceci à $1 - e$ il vient aussi que $0 = q(1 - e) = 1 + q(e) - t(e)$, donc $t(e) = 1$. Fixons maintenant $x \in eRe$. On observe que $f(x, 1 - e) = t(x)$, donc la polarisation de Cayley-Hamilton nous donne pour $(x, 1 - e)$

$$-t(x)(1 - e) - x + t(x) = 0$$

soit $x = t(x)e$, ce qui conclut. □

Lemme 3. *Supposons que k est un corps, que q est non dégénéré, que $e \in R$ est un idempotent non trivial et que $eR(1-e)$ est non nul. Alors $eR(1-e)$ et $(1-e)Re$ sont de k-dimension 1. De plus, il existe $u \in eR(1-e)$ et $v \in (1-e)Re$ tels que $uv = e$ et $vu = 1-e$.*

Preuve — Soit $u \in eR(1-e)$ non nul. On a $q(u) = q(eu) = q(e)q(u) = 0$. Par non dégénérescence de q il existe donc $v \in R$ tel que $f(u,v) = -1$. Comme t est centrale on a $t(u) = t(eu(1-e)) = 0$ donc $f(u,v) = -t(uv)$ et on peut aussi supposer que $v \in (1-e)Re$ quitte à le remplacer par $(1-e)ve$. On a alors $uv \in eRe$ et donc $uv = t(uv)e = e$ (lemme précédent). De même $vu = e$. Soit $x \in eR(1-e)$. Alors $x = xe = xvu = (xv)u = t(xv)u$ car $xv = t(xv)e$ (lemme précédent). Ainsi $eR(1-e) = ku$ et de même $(1-e)Re = kv$. □

Lemme 4. *Sous les hypothèses du dernier lemme, $(R,q) \simeq (\mathrm{M}_2(k), \det)$.*

Preuve — Les deux lemmes ci-dessus montrent que $e, 1-e, u, v$ est une k-base de R. De plus $Re = eRe + (1-e)Re$ est un idéal à gauche de R de k-dimension 2, ce qui fournit une représentation $\rho : R \to \mathrm{M}_2(k)$ dans la base (e,v). Pour $a,b,c,d \in k$, on constate que

$$\rho(ae + bu + cv + d(1-e)) = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

donc ρ est un isomorphisme. Si $x = ae + bu + cv + d(1-e)$, on constate aussi que $q(x) = ad - bc = \det \circ \rho(x)$. □

Étape 4 : *Existence d'éléments idempotents non triviaux.*

Lemme 5. *On suppose q non dégénéré, k quadratiquement clos*[4] *et $\dim_k R > 1$. Alors R possède un idempotent non trivial.*

Preuve — En effet, la restriction de la forme quadratique q à n'importe quel sous-espace de dimension 2 de R admet par hypothèse sur k un zéro non trivial. On peut donc trouver $a \in R$ non nul tel que $q(a) = 0$. Comme q est non dégénéré on peut trouver $b \in R$ tel que la forme q est hyperbolique au sens quadratique dans la base a, b, i.e. $q(a) = q(b) = 0$ et $f(a,b) = 1$. Observons que si $x \in R$ satisfait $q(x) = 0$ la relation de Cayley-Hamilton montre que $x^2 = t(x)x$, donc si de plus $t(x) \neq 0$ alors $x/t(x)$ est un idempotent de trace 1 donc non trivial. On peut donc supposer $t(a) = t(b) = 0$, mais alors $f(a,b) = -t(ab) = 1$ et $q(ab) = 0$ et donc l'élément $-ab$ est un idempotent non trivial. □

Étape 5 : *Démonstration de la proposition.* On peut supposer que q est non dégénéré par l'étape 1. Si $R = k$ alors $q(\lambda) = \lambda^2$ et on peut prendre pour ρ la représentation de k sur k^2 par homothéties. Sinon on peut trouver un idempotent non trivial $e \in R$ (étape 4). Si $eR(1-e)$ est non nul, on conclut par le dernier lemme de l'étape 3. Sinon $eR(1-e) = 0$, et les deux premiers lemmes de l'étape 3 assurent que $(1-e)Re = 0$, $eRe = ke$, $(1-e)R(1-e) = k(1-e)$. Ainsi, l'application $k \times k \to R$, $(x,y) \mapsto xe + y(1-e)$

[4] I.e. n'admet pas d'extension de corps de degré 2.

est un isomorphisme de k-algèbres (celle de gauche étant la k-algèbre diagonale). On conclut car si $a, b \in k$, alors $q(ae + b(1-e)) = ab$.

Cela achève la démonstration. Elle démontre d'ailleurs que l'énoncé de la proposition vaut plus généralement si k est quadratiquement clos.

Digressions :

(a) Quand on suppose simplement que k n'a pas d'extension quadratique étale, il y a un cas supplémentaire dans l'étape 4, à savoir $\mathrm{char}(k) = 2$ et $t(R) = 0$ (car $X^2 - t(x)X + q(x)$ est séparable sur k si $t(x) \neq 0$). Dans ce cas, $x^2 = q(x) \in k^*$ pour tout $x \in R$ non nul : R est une algèbre à division, elle est même commutative par le théorème de Jacobson-Noether ("existence d'éléments séparables sur le centre"). Dans cette exception tout à fait éventuelle, ρ n'existe pas si $[R : k] > 2$.

(b) Ceci étant fait il n'est pas difficile de déterminer les couples $(R/k, q)$ où q est un déterminant non dégénéré et k un corps quelconque par descente galoisienne. Un premier sorite nécessaire est la notion d'extension des scalaires pour les déterminants. Le point est que si R est un k-module (k un anneau commutatif quelconque), si $q : R \to k$ est une forme quadratique de polaire f, et si k' est une k-algèbre commutative, alors il existe une unique forme quadratique $q \otimes_k k'$ sur $R \otimes_k k'$ qui vaut $q(x)$ sur les $x \otimes 1$ et de forme polaire $f \otimes_k k'$. Si R est une k-algèbre associative et q est un déterminant alors $q \otimes_k k'$ est encore un déterminant (cela se déduit par exemple du lemme 6). On constate par descente galoisienne que si k'/k est une extension galoisienne de corps, $\mathrm{Ker}(q \otimes_k k') = \mathrm{Ker}(q) \otimes_k k'$. En particulier, dans ce cas si q est non dégénéré il en va de même de $q \otimes_k k'$. Ainsi, si k est un corps quelconque et si $q : R \to k$ est un déterminant non dégénéré, on en déduit par extension des scalaires à une clôture séparable de k que : soit $R = k$ et $q(x) = x^2$, soit R/k est une extension quadratique étale et q est sa norme, soit R/k est une algèbre de quaternions et q sa norme réduite, soit k est de caractéristique 2, R/k est une extension purement inséparable d'exposant 2 et q est le Frobenius $x \mapsto x^2$.

Je vais maintenant discuter du cas particulier où $R = k[G]$ est l'algèbre d'un groupe G. Il ne coutera pas plus cher de supposer encore que k est un anneau quelconque. Je note $D(G/k)$ l'ensemble des couples (d, t) où $d : G \to k^*$ est un homomorphisme de groupes et $t : G \to k$ est une fonction centrale, tels que $t(1) = 2$ et

$$\forall g, h \in G, \quad d(g)t(g^{-1}h) - t(g)t(h) + t(gh) = 0. \tag{4}$$

Soit q un déterminant de $k[G]/k$ de forme polaire f. On lui associe une paire (d, t) en posant $d(g) = q(g)$ et $t(g) = f(g, 1)$ pour $g \in G$, ce qui est compatible avec la définition précédente de t. On a bien $t(1) = 2$ et d est un homomorphisme par définition. Les identités (1) et (3) de l'étape 0 montrent que t et d satisfont (4). Si q est le déterminant d'une représentation $\rho : k[G] \to \mathrm{M}_2(k)$, il est clair que $d = \det \circ \rho_{|G}$ et $t = \mathrm{trace}\rho_{|G}$.

Proposition 2. *L'application ci-dessus $q \mapsto (d, t)$ est une bijection de l'ensemble des déterminants de $k[G]/k$ sur $D(G/k)$.*

Preuve — Un déterminant $q : k[G] \to k$ de forme polaire f est uniquement déterminé par $d = q_{|G}$ et $f_{|G\times G}$. La relation $f(g,h) = t(g)t(h) - t(gh)$ assure que t détermine f : l'application de l'énoncé est injective. Pour la surjectivité on part de (d,t) et on définit une forme bilinéaire sur $k[G]$ par $f(g,h) = t(g)t(h) - t(gh)$ pour tout $(g,h) \in G^2$. Elle est symétrique car t est centrale. De plus,

$$f(g,h) = d(g)t(g^{-1}h) \tag{5}$$

par la propriété (4). En particulier, $f(g,g) = 2d(g)$ car $t(1) = 2$, de sorte que la fonction

$$q(\sum_g a_g g) = \sum_g a_g^2 d(g) + \sum_{\{g,g'\}} a_g a_{g'} f(g,g')$$

(la seconde somme portant sur les parties à deux éléments de G) définit bien une forme quadratique sur $k[G]$ de forme polaire f. Reste à vérifier la multiplicativité de q. On applique le lemme qui suit à la famille $\mathcal{B} = G$. On a déjà $q(1) = d(1) = 1$ ainsi que (i) car d est un homomorphisme. La relation (ii) suit de (5) et du fait que t est centrale. La relation (iii) se vérifie après multiplication par $q(wy)^{-1} = q(w)^{-1}q(y)^{-1}$ auquel cas elle s'écrit compte tenu de (ii) :

$$t(w^{-1}zxy^{-1}) + f(xy^{-1}, w^{-1}z) = t(w^{-1}z)t(y^{-1}x),$$

qui est évidente car t est centrale. □

Le lemme qui suit est un exercice sans difficulté de polarisation.

Lemme 6. *Soit R une k-algèbre, soit $\mathcal{B}$ une famille génératrice de R comme k-module, et soit $q : R \to k$ une forme quadratique telle que $q(1) = 1$. Alors q est un déterminant de R/k si et seulement si pour tout $w,x,y,z \in \mathcal{B}$:*

(i) $q(x)q(y) = q(xy)$,
(ii) $q(x)f(y,z) = f(xy,xz) = f(yx,zx)$,
(iii) $f(zx,wy) + f(wx,zy) = f(z,w)f(x,y)$.

Des deux propositions de ce texte résulte le corollaire qui semblait vous intéresser :

Corollaire 1. *Soit k un corps algébriquement clos et soit G un groupe. L'application $\rho \mapsto \mathrm{trace}\circ\rho$ induit une bijection entre l'ensemble des classes d'isomorphie de représentations semisimples $G \to \mathrm{SL}_2(k)$ et l'ensemble des fonctions centrales $t : G \to k$ telles que $\forall g,h \in G$, $t(g^{-1}h) + t(gh) = t(g)t(h)$ et $t(1) = 2$.*

Pour terminer je vais tenter de donner un bref aperçu de quelques autres propriétés des déterminants. Je fixe G un groupe et je considère le foncteur covariant évident $k \mapsto D(G/k)$, des anneaux commutatifs vers les ensembles. Il est visiblement représentable, disons par l'anneau $A(G)$. Il est raisonnable d'appeler $X(G) = \mathrm{Spec}(A(G))$ la *variété des caractères de dimension* 2 du groupe G. L'avantage de cette construction "explicite" de la variété des caractères $X(G)$ par rapport à celle que l'on aurait pu obtenir par la théorie géométrique des invariants comme quotient de la variété des représentations

$G \to \mathrm{GL}(2)$ par $\mathrm{PGL}(2)$ est que l'on dispose par définition d'une description explicite de son foncteur des points, ce qui est agréable. Si $x \in X(G)$, disons de corps résiduel $k(x)$, nous avons vérifié dans cette lettre qu'il existe une unique $k(x)$-représentation semisimple $\rho_x : k(x)[G] \to M_2(\overline{k(x)})$ de déterminant le déterminant associé à x (et toute telle représentation s'obtient ainsi). Pour aller plus loin il est intéressant de considérer le déterminant tautologique

$$q^{\mathrm{univ}} : A(G)[G] \to A(G).$$

Notons R^{univ} le quotient de $A(G)[G]$ par son idéal bilatère engendré par les $\chi(x)$ avec $x \in A(G)[G]$. Le lemme de l'étape 2 plus haut montre que q^{univ} se factorise par R^{univ}. On dispose d'un morphisme de groupes tautologique $G \to (R^{\mathrm{univ}})^*$. Alors :

(i) Il n'est pas difficile de voir que le sous-ensemble des $x \in X(G)$ tels que ρ_x est irréductible est un ouvert Zariski de $X(G)$. Sur cet ouvert l'algèbre R^{univ} est une algèbre d'Azumaya de norme réduite q^{univ} (Procesi, au langage près).

(ii) Soit $x \in X(G)$ tel que ρ_x est réductible, et soit $\mathcal{O}_x$ le hensélisé strict de $A(G)_x$. Si ρ_x est somme de deux caractères distincts, la $\mathcal{O}_x$-algèbre $R_x = R^{\mathrm{univ}} \otimes_{A(G)} \mathcal{O}_x$ est encore assez sympathique : c'est une algèbre de matrices généralisée au sens de mon livre avec Bellaïche (chapitre 1). Sa structure, ainsi que celle de $\mathcal{O}_x$, est intimement liée aux groupes d'extensions entre les deux constituents de ρ_x (cf. loc. cit. ainsi que l'article de Bellaïche sur les pseudodéformations).

(iii) (suite) Si ρ_x est la somme de deux caractères égaux, par exemple ρ_x trivial, l'anneau R_x est local de corps résiduel $k(x)$. Je renvoie au dernier chapitre de mon article sur les déterminants (cas $2 = 0$ dans $k(x)$), ainsi qu'aux § 2 et § 5 de mon article "*Sur la variété des caractères p-adiques du groupe de Galois absolu de* $\mathbb{Q}_p$" (cas $2 \in k(x)^*$) pour quelques résultats sur la détermination de R_x et $\mathcal{O}_x$.

S'il vous convient que 2 soit inversible, et d'adopter le langage des pseudocaractères, vous trouverez plus de détails sur ces questions dans le chapitre 2 de mon livre avec Bellaïche, ou encore dans les notes de mon cours à l'IHP disponibles à l'adresse `http://www.math.polytechnique.fr/~chenevier/coursihp.html` (cf. cours 3 §4 et cours 4 § 1 et § 2, la présentation est y proche de celle de cette lettre). En général (caractéristique et dimension quelconques) je renvoie à mon article sur les déterminants. Un déterminant de dimension n est simplement une loi polynomiale $q : R \to k$ homogène de degré n (au sens de N. Roby) telle que $q(1) = 1$ et $q(xy) = q(x)q(y)$ pour tout $x, y \in R$. La proposition 1 s'étend à ce cadre, ainsi que la plupart des choses discutées ci-dessus. Je renvoie à l'introduction loc. cit. pour une tentative d'historique de ce sujet (dont je suis loin cependant d'être un spécialiste, donc c'est à prendre avec des pincettes...).

Cordialement,

Gaëtan Chenevier.