# Discriminant et loi de réciprocité quadratique

Préparation à l'agrégation de mathématiques
Université de Nice - Sophia Antipolis
Antoine Ducros

9 novembre 2006

## 1 Le discriminant

### 1.1 À propos de la signature

Soit $n$ un entier et soit $\mathfrak{S}_n$ le groupe des permutations de $\{1,\dots,n\}$. Soit $D$ le polynôme en $n$ variables et à coefficients entiers

$$\prod_{i\neq j}(X_i - X_j).$$

Il est symétrique, c'est-à-dire invariant sous l'action de $\mathfrak{S}_n$. Par ailleurs on peut l'écrire

$$\prod_{i>j}(X_i - X_j)(X_j - X_i) = \prod_{i>j}(-1).(X_i - X_j)^2,$$

soit encore $(-1)^{n(n-1)/2}(\prod_{i>j}(X_i - X_j))^2$ puisqu'il y a exactement $n(n-1)/2$ paires d'entiers compris entre 1 et $n$. Soit $\Delta$ le polynôme $\prod_{i>j}(X_i - X_j)$. Comme $\Delta^2$ coïncide avec $D$ au signe près, il est symétrique. Soit $\sigma$ appartenant à $\mathfrak{S}_n$ ; on a $(\sigma(\Delta))^2 = \sigma(\Delta^2) = \Delta^2$. On en déduit qu'il existe un élément $\varepsilon(\sigma)$ de $\{-1,1\}$ tel que $\sigma(\Delta) = \varepsilon(\sigma)\Delta$. Il est immédiat que $\sigma \mapsto \varepsilon(\sigma)$ est un homomorphisme de groupes de $\mathfrak{S}_n$ dans $\{-1,1\}$ ; un calcul explicite montre qu'il prend la valeur $(-1)$ sur toute transposition, et on en conclut qu'il coïncide avec la signature (à moins qu'on ne le prenne pour *définition* de la signature).

### 1.2 Un calcul de déterminant

Soit $L$ un corps, soit $n$ un entier et soit $\mathsf{M}$ une matrice triangulaire supérieure de $M_n(L)$. Soient $\lambda_1,\dots,\lambda_n$ les coefficients diagonaux de $\mathsf{M}$ ; notez que les $\lambda_i$ ne sont pas forcément deux à deux distincts.

Soit $Q$ un polynôme à coefficients dans $L$. La matrice $Q(\mathsf{M})$ est triangulaire supérieure, et sa diagonale est $Q(\lambda_1),\dots,Q(\lambda_n)$. En conséquence,

$$\det Q(\mathsf{M}) = \prod_{i=1}^{n} Q(\lambda_i).$$

## 1.3 Définition du discriminant

Soit $k$ un corps, et soit $P$ un polynôme unitaire à coefficients dans $k$, dont on note $n$ le degré. Il est bien connu (ou il *devrait* être bien connu !!) que la $k$-algèbre $E := k[T]/(P)$ est, en tant que $k$-espace vectoriel, de dimension $n$ ; la famille $(\overline{1}, \overline{T}, \ldots, \overline{T}^{n-1})$ en constitue une base.

Soit $u$ l'application $k$-linéaire de $E$ dans $E$ égale à la multiplication par $\overline{T}$. On voit aussitôt par récurrence que pour tout entier $m$, l'endomorphisme $u^m$ de $E$ est la mutliplication par $\overline{T}^m$ ; on en déduit que pour tout polynôme $Q$ appartenant à $k[X]$, l'endomorphisme $Q(u)$ de $E$ est la multiplication par $Q(\overline{T})$.

Le polynôme caractéristique de $u$ est égal (au signe près) à $P$. Pour le voir, on dispose de deux méthodes :

- On peut écrire la matrice de $u$ dans la base $(\overline{1}, \overline{T}, \ldots, \overline{T}^{n-1})$ ; on voit très facilement que ce n'est autre que la matrice compagnon associée à $P$ ; il n'y a plus qu'à calculer son polynôme caractéristique.
- On peut aussi remarquer que $P(u)$ est nul, puisque c'est la multiplication par $P(\overline{T})$ ; en conséquence, $P$ est un polynôme annulateur de $u$. Par ailleurs, soit $Q = \sum a_i T^i$ un polynôme de degré strictement inférieur à $n$. Supposons que $Q(u) = 0$ ; alors $Q(u)(\overline{1}) = (\sum a_i \overline{T}^i).\overline{1} = \sum a_i \overline{T}^i = 0$. Le polynôme $Q$ étant de degré strictement inférieur à $n$ et la famille $(\overline{1}, \overline{T}, \ldots, \overline{T}^{n-1})$ étant libre, on a $a_i = 0$ pour tout $i$ ; autrement dit, $Q$ est nul. On vient d'établir que $P$ est le polynôme minimal de $u$ ; comme son degré est égal à la dimension de $E$, c'est aussi (au signe près) son polynôme caractéristique.

Soit $\mathsf{M}$ la matrice de $u$ dans la base $(\overline{1}, \overline{T}, \ldots, \overline{T}^{n-1})$. Soit $L$ un corps contenant $k$ dans lequel $P$ est scindé (par exemple une clôture algébrique de $k$ ou, plus simplement, un corps de décomposition de $L$). Écrivons $P = \prod_{i=1}^{n} (T - \lambda_i)$ avec les $\lambda_i$ dans $L$. La matrice $\mathsf{M}$ est semblable, dans $M_n(L)$, à une matrice triangulaire supérieure dont la diagonale est $\lambda_1, \ldots, \lambda_n$. En conséquence, on déduit du calcul fait plus haut que pour tout polynôme $Q$ de $k[X]$ on a l'égalité

$$\det Q(u) = \prod_{i=1}^{n} Q(\lambda_i) \ ;$$

notez que le terme de droite appartient *a priori* à $L$, mais que cette égalité assure entre autres qu'il appartient à $k$.

Appliquons ceci lorsque $Q$ est égal à la dérivée $P'$ du polynôme $P$. Sur le corps $L$, on peut écrire

$$P' = \sum_{i=1}^{n} \prod_{j \neq i} (T - \lambda_j),$$

d'où découle pour tout $i$ l'égalité

$$P'(\lambda_i) = \prod_{j \neq i} (\lambda_i - \lambda_j).$$

De la formule vue ci-dessus on déduit donc que

$$\det P'(u) = \prod_{i \neq j} (\lambda_i - \lambda_j).$$

D'après le 1.1, le terme de droite peut se réécrire $(-1)^{n(n-1)/2}(\prod_{i>j}(\lambda_i - \lambda_j))^2$.

Le *discriminant de* $P$ est défini comme étant égal à $(-1)^{n(n-1)/2} \prod_{j \neq i}(\lambda_i - \lambda_j)$ ; on le note Disc $P$. Indiquons-en quelques propriétés :

- Disc $P$ est nul si et seulement si $P$ possède une racine multiple dans $L$.
- Disc $P$ coïncide au signe $(1)^{n(n-1)/2}$ près avec le déterminant de la multiplication par $P'(\overline{T})$ modulo $P(\overline{T})$. Il appartient donc à $k$, peut s'exprimer comme une fonction polynomiale (elle-même à coefficients entiers) des coefficients de $P$, et peut ainsi être calculé sans connaître les $\lambda_i$.
- Disc $P$ est égal à $(\prod_{i>j}(\lambda_i - \lambda_j))^2$. On en déduit que si $\prod_{i>j}(\lambda_i - \lambda_j)) \in k$, alors Disc $P$ est le carré d'un élément de $k$ ; réciproquement, si Disc $P$ est le carré d'un élément $x$ de $k$, alors $x = \pm \prod_{i>j}(\lambda_i - \lambda_j)$, et $\prod_{i>j}(\lambda_i - \lambda_j)$ appartient donc à $k$.

## 1.4 Exemples

**Le cas où** $n = 2$. On écrit $P = T^2 + bT + c$. Le polynôme $P'$ est égal à $2T + b$. Écrivons la matrice, dans la base $(\overline{1}, \overline{T})$, de la multiplication par $P'(\overline{T})$ dans $k[T]/(P)$. L'image de $\overline{1}$ par cette multiplication est $b + 2\overline{T}$ ; celle de $\overline{T}$ est

$$b\overline{T} + 2\overline{T}^2 = b\overline{T} - 2b\overline{T} - 2c = -b\overline{T} - 2c.$$

La matrice cherchée est de ce fait

$$\begin{pmatrix} b & -2c \\ 2 & -b \end{pmatrix}$$

et son déterminant est égal à $4c - b^2$. En conséquence, le discriminant de $P$ est égal à $(-1)^{2(2-1)/2}(4c - b^2)$, soit à $b^2 - 4c$ ; on retrouve la formule bien connue.

**Le cas où** $n = 3$. On suppose pour simplifier que $P$ est de la forme $T^3 + pT + q$. Le polynôme $P'$ est égal à $3T^2 + p$. Écrivons la matrice, dans la base $(\overline{1}, \overline{T}, \overline{T^2})$, de la multiplication par $P'(\overline{T})$ dans $k[T]/(P)$. L'image de $\overline{1}$ par cette multiplication est $p + 3\overline{T}^2$ ; celle de $\overline{T}$ est

$$p\overline{T} + 3\overline{T}^3 = p\overline{T} - 3p\overline{T} - 3q = -2p\overline{T} - 3q\ ;$$

celle de $\overline{T}^2$ est

$$p\overline{T}^2 + 3\overline{T}^4 = p\overline{T}^2 - 3p\overline{T}^2 - 3q\overline{T} = -2p\overline{T}^2 - 3q\overline{T}.$$

La matrice cherchée est de ce fait

$$\begin{pmatrix} p & -3q & 0 \\ 0 & -2p & -3q \\ 3 & 0 & -2p \end{pmatrix}$$

et son déterminant est égal à $4p^3 + 27q^2$. En conséquence, le discriminant de $P$ est égal à $(-1)^{3(3-1)/2}(4p^3 + 27q^2)$, soit à $-4p^3 - 27q^2$.

**Discriminant de $T^q - 1$, où $q$ est un entier non nul.** La dérivée de $T^q - 1$ est $qT^{q-1}$. Dans $k[T]/(T^q - 1)$ on a évidemment $\overline{T}^q = 1$. En conséquence, la multiplication par $q\overline{T}^{q-1}$ envoie $\overline{1}$ sur $q\overline{T}^{q-1}$ et $\overline{T}^i$ sur $q\overline{T}^{i-1}$ pour tout $i$ compris entre 2 et $q$. La matrice de cette application linéaire a donc tous ses coefficients nuls, à l'exception de celui en bas à gauche et de ceux de la surdiagonale qui sont tous égaux à $q$ ; en faisant un développement par rapport à la première colonne, on voit que son déterminant est égal à $(-1)^{q-1}q^q$. On en déduit que le discriminant de $T^q - 1$ vaut

$$(-1)^{q-1+q(q-1)/2}q^q = (-1)^{(q-1)(q+2)/2}q^q.$$

**Attention : l'expression $q^q$ est un abus de notation pour $(q.1_k)^q$, où $1_k$ est l'élément unité de $k$.**

# 2 La loi de réciprocité quadratique

## 2.1 Le symbole de Legendre

Soit $q$ un nombre premier différent de 2. Si $x$ appartient à $\mathbb{F}_q^*$, alors $x^{(q-1)/2}$ a pour carré 1, puisque $x^{q-1} = 1$ ; en conséquence $x^{(q-1)/2}$ vaut 1 ou $-1$. On démontre qu'il vaut 1 si et seulement si $x$ est le carré d'un élément de $\mathbb{F}_q$. L'élément $x^{(q-1)/2}$ de $\{-1, 1\}$ est noté $\left(\frac{x}{q}\right)$. Si $y$ est un entier premier à $q$, on écrira $\left(\frac{y}{q}\right)$ au lieu de $\left(\frac{\overline{y}}{q}\right)$. Par contruction, $x \mapsto \left(\frac{x}{q}\right)$ est un morphisme de groupes de $\mathbb{F}_q^*$ vers $\{-1, 1\}$.

**Un calcul de signature.** Soit $x$ un élément de $\mathbb{F}_q^*$. La multiplication par $x$ induit une bijection $\sigma_x$ de $\mathbb{F}_q$ sur lui-même. Elle possède un unique point fixe, à savoir 0, et tout cycle non trivial de la décomposition de $\sigma_x$ est de la forme

$$(\lambda, x\lambda, x^2\lambda, \ldots, x^{d-1}\lambda)$$

où $\lambda$ appartient à $\mathbb{F}_q^*$ et où $d$ est l'ordre de $x$ dans $\mathbb{F}_q^*$. La longueur d'un tel cycle est $d$, et il y en a donc exactement $(q-1)/d$. La signature de $\sigma_x$ vaut dès lors $(-1)^{(d-1)(q-1)/d}$. *On va montrer qu'elle est égale à $\left(\frac{x}{q}\right)$ ; comme $\left(\frac{x}{q}\right)$ et $\varepsilon(\sigma_x)$ sont deux éléments de $\{-1, 1\}$, il suffit d'établir l'équivalence*

$$\left(\frac{x}{q}\right) = 1 \iff \varepsilon(\sigma_x) = 1.$$

- Si $\left(\frac{x}{q}\right) = 1$ alors $x^{(q-1)/2} = 1$, donc $d$ divise $(q-1)/2$ ; ceci signifie que $(q-1)/2$ s'écrit $dm$ avec $m$ dans $\mathbb{N}$. Dans ce cas $(d-1)(q-1)/d = (d-1)2m$ qui est pair, et $\varepsilon(\sigma_x) = 1$.

- Si $\varepsilon(\sigma_x) = 1$ alors $(d-1)(q-1)/d$ est pair. On est donc dans l'un des deux cas suivants :

  - Premier cas : $d-1$ est pair. Ceci entraîne que $d$ est impair ; or il divise $q-1$, c'est-à-dire $2.(q-1)/2$ ; par le lemme de Gauß, il divise $(q-1)/2$ et $\left(\frac{x}{q}\right) = 1$.
  - Second cas : $(q-1)/d$ est pair. Cela signifie que $(q-1)$ est de la forme $2dm$ pour un certain entier $m$ ; dès lors $(q-1)/2$ est égal à $dm$ et est donc multiple de $d$. En conséquence, $\left(\frac{x}{q}\right) = 1$.

**Remarque.** Soit $G$ un groupe cyclique de cardinal $q$ noté *multiplicativement* et soit $x$ un entier premier à $q$. Soit $\varphi$ l'appplication $g \mapsto g^x$ de $G$ dans lui-même. Par hypothèse, il existe un isomorphisme de groupes entre $(G, \times)$ et $(\mathbb{Z}/q\mathbb{Z}, +)$ ; et $\varphi$ s'identifie *via* cet isomorphisme à la *multiplication* par $x$ de $\mathbb{Z}/q\mathbb{Z}$ dans lui-même ; on déduit de ce qui précède que $\varphi$ induit une permutation de $G$ de signature $\left(\frac{x}{q}\right)$.

## 2.2 Parité de l'automorphisme de Frobenius et symbole de Legendre du discriminant

Soit $p$ un nombre premier impair et soit $P$ un polynôme unitaire à coefficients dans $\mathbb{F}_p$. Soit $L$ un corps de décomposition de $P$ sur $\mathbb{F}_p$ ; écrivons $P = \prod_{i=1}^{n} (T - \lambda_i)$ avec les $\lambda_i$ dans $L$ ; *supposons-les deux à deux distincts.* On a établi à la fin du 1.3 l'équivalence

$$\text{« Disc } P \text{ est le carré d'un élément de } \mathbb{F}_p \text{ »} \iff \prod_{i>j} (\lambda_i - \lambda_j) \in k.$$

On peut la réécrire

$$\left(\frac{\text{Disc } P}{p}\right) = 1 \iff \prod_{i>j} (\lambda_i - \lambda_j) \in k.$$

Par ailleurs, soit $\sigma$ l'automorphisme de Frobenius $x \mapsto x^p$ de $L$. Comme $P$ est à coefficients dans $\mathbb{F}_p$, si $\lambda$ est une racine de $P$ alors $\sigma(\lambda)$ l'est aussi ; on en déduit que $\sigma$ induit une permutation de l'ensemble des $\lambda_i$, que l'on va noter $\sigma_P$.

Un élément $x$ de $L$ appartient à $k$ si et seulement si il est égal à $\sigma(x)$. Par ailleurs,

$$\sigma(\prod_{i>j} (\lambda_i - \lambda_j)) = \varepsilon(\sigma_P)(\prod_{i>j} (\lambda_i - \lambda_j))$$

d'après le 1.1. En conséquence, comme $1 \neq (-1)$ dans $k$ (puisque $p$ est différent de 2) et comme

$$\prod_{i>j} (\lambda_i - \lambda_j) \neq 0$$

(puisque les $\lambda_i$ sont par hypothèse deux à deux distincts),

$$\sigma(\prod_{i>j}(\lambda_i - \lambda_j)) \in k \iff \varepsilon(\sigma_P) = 1,$$

ce que l'on peut traduire, en vertu de ce qui précède, par l'égalité

$$\left(\frac{\text{Disc } P}{p}\right) = \varepsilon(\sigma_P).$$

## 2.3 Preuve de la loi de réciprocité quadratique

On garde les notations introduites ci-dessus, en supposant de plus que $P$ est égal à $T^q - 1$, où $q$ est un nombre premier impair distinct de $p$. Pour appliquer ce qui précède, il faut vérifier que les racines de $P$ dans $L$ sont simples. Or la dérivée de P est $qT^{q-1}$, dont la seule racine dans $L$ est 0, *puisque $q$ est premier à $p$*; comme 0 n'est pas racine de $P$, aucune racine de $P$ dans $L$ n'annule $P'$; les racines de $P$ dans $L$ sont donc simples.

L'ensemble des racines de $P$ dans $L$ a de ce fait exactement $q$ éléments. Par ailleurs, c'est l'ensemble des racines $q$-ièmes de l'unité dans $L$, et c'est donc un sous-groupe de $L^*$; il est en conséquence isomorphe à $\mathbb{Z}/q\mathbb{Z}$ (parce que $q$ est premier, ou bien parce que de toutes façons tous les sous-groupes de $L^*$ sont cycliques). La permutation $\sigma_P$ de ce groupe est induite par l'élévation à la puissance $p$. Par la remarque qui clôt le paragraphe 2.1, la signature de $\sigma_P$ est égale à $\left(\frac{p}{q}\right)$.

D'autre part elle s'identifie, comme on vient de le voir, à $\left(\frac{\text{Disc } P}{p}\right)$; or Disc $P$ été calculé, à la fin du 1.4; il vaut $(-1)^{(q-1)(q+2)/2}(q.1_{\mathbb{F}_p})^q$. On en déduit l'égalité

$$\left(\frac{\text{Disc } P}{p}\right) = \left(\frac{-1}{p}\right)^{(q-1)(q+2)/2} \left(\frac{q}{p}\right)^q.$$

Comme $q$ est impair, $\left(\frac{q}{p}\right)^q = \left(\frac{q}{p}\right)$. Comme $q+2$ est impair,

$$\left(\frac{-1}{p}\right)^{(q-1)(q+2)/2} = \left(\frac{-1}{p}\right)^{(q-1)/2} = (-1)^{(p-1)(q-1)/4}.$$

On a finalement démontré que

$$(-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

et c'est ce qu'on voulait.