La loi de réciprocité quadratique

Daniel PERRIN

1 L'énoncé du théorème

On renvoie à [1] ch. 3 pour des précisions sur les extensions de corps et les corps finis.

Soit p un nombre premier impair et $\mathbf{F}_p$ le corps fini $\mathbf{Z}/p\mathbf{Z}$. Rappelons que dans $\mathbf{F}_p^*$ il y a autant de carrés que de non carrés et qu'on a défini le symbole de Legendre $\left(\frac{x}{p}\right)$, pour $x \in \mathbf{F}_p^*$, égal à $+1$ si x est un carré et à -1 sinon. Le théorème principal sur le sujet est la fameuse loi de réciprocité quadratique :

1.1 Théorème. *Soient p, n deux nombres premiers impairs distincts. On a la formule :*

$$\left(\frac{p}{n}\right) = (-1)^{\frac{(n-1)(p-1)}{4}} \left(\frac{n}{p}\right).$$

On peut encore formuler ce théorème sous l'une des deux formes suivantes que l'on établit en distinguant [1] les congruences modulo 4 :

1.2 Théorème. *Soient p, n deux nombres premiers impairs distincts.*

1) Si p ou n est congru à 1 modulo 4 on a $\left(\frac{p}{n}\right) = \left(\frac{n}{p}\right)$. Si tous deux sont congrus à -1 on a $\left(\frac{p}{n}\right) = -\left(\frac{n}{p}\right)$.

2) Le nombre $(-1)^{(n-1)/2}\, n$ est un carré modulo p si et seulement si p est un carré modulo n.

Le but de ce qui suit est d'établir le théorème (sa variante 2) par une démonstration qui est celle que je trouve la plus simple. Elle ne fait pas appel explicitement à la théorie de Galois, mais le lecteur averti en détectera facilement la présence dans les idées qui sous-tendent cette preuve : si L est le corps de décomposition du polynôme $X^n - 1$ sur $\mathbf{F}_p$, on peut voir son groupe de Galois comme groupe de permutations des racines de l'unité, comme sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$, et comme groupe cyclique engendré par l'automorphisme de Frobenius F. Le point décisif est alors de traduire de deux manières le fait que F induit une permutation paire : en écrivant que le discriminant de $X^n - 1$, qui vaut, aux carrés près, $(-1)^{(n-1)/2}n$, est un carré modulo p, ou en identifiant le sous-groupe des permutations paires comme le groupe des carrés de $(\mathbf{Z}/n\mathbf{Z})^*$, ce qui assure que F, alias p, est un carré modulo n.

1. Pour la variante 2) il faut aussi savoir que -1 est un carré modulo p si et seulement si p est congru à 1 modulo 4.

2 Rappels sur le discriminant

2.1 Définition et propriété caractéristique

2.1 Notations. On désigne par K un corps de caractéristique différente de 2, par P un polynôme de degré $n > 0$ à coefficients dans K et par L son corps de décomposition $L = D_K(P)$. On suppose que le polynôme P admet n racines distinctes dans L, que l'on note $x_1, \ldots, x_n$.

2.2 Proposition-Définition. *On pose* $\delta(P) = \prod_{1\leq i<j\leq n} (x_i - x_j)$ *et* $\Delta(P) = \delta(P)^2 = \prod_{1\leq i<j\leq n} (x_i - x_j)^2$. *Le nombre* $\Delta(P)$ *est appelé* **discriminant** *du polynôme* P. *On a la formule* $\Delta(P) = (-1)^{n(n-1)/2} \prod_{i\neq j}(x_i - x_j)$.

Démonstration. Il suffit de compter les signes $-$, donc les couples (i, j) avec $i > j$, il y en a bien $n(n-1)/2$.

Le discriminant est lié aux permutations des racines :

2.3 Proposition. *Soit* $\sigma \in \mathfrak{S}_n$ *une permutation de l'ensemble* $\{1, 2, \ldots, n\}$. *On pose* $\sigma(\delta) = \prod_{1\leq i<j\leq n} (x_{\sigma(i)} - x_{\sigma(j)})$ *On a* $\sigma(\delta) = \epsilon(\sigma)\delta$ *où* $\epsilon(\sigma)$ *est la signature de la permutation* σ.

Démonstration. Cela résulte du comptage du nombre d'inversions [2] de σ.

2.2 Calcul du discriminant

2.4 Théorème. *On reprend les notations de 2.1, et on suppose* P *unitaire de degré* n *premier à la caractéristique de* K. *Soit* P' *son polynôme dérivé. On a la formule :*

$$\Delta(P) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} P'(x_i).$$

Démonstration. On part de la formule $P(X) = \prod_{i=1}^{n}(X - x_i)$ que l'on dérive :

$$P'(X) = \sum_{i=1}^{n}(X - x_1) \cdots \widehat{(X - x_i)} \cdots (X - x_n)$$

2. On peut d'ailleurs définir la signature par cette formule, vue dans l'anneau de polynômes $K[x_1, \ldots, x_n]$.

où le chapeau signifie que le terme correspondant est omis et on calcule $P'(x_i)$. Tous les termes de la somme sont nuls sauf celui où l'on a omis x_i et on a donc, pour i fixé, $P'(x_i) = \prod_{j,\, j\neq i} (x_i - x_j)$. On en déduit la valeur du produit $\prod_{i=1}^{n} P'(x_i) = \prod_{i,j,\, j\neq i} (x_i - x_j)$ et la formule s'ensuit.

2.3 Le cas cyclotomique

2.5 Proposition. *Soit n un entier impair premier à la caractéristique de K. On a $\Delta(X^n - 1) = (-1)^{(n-1)/2}\, n^n$. Modulo les carrés de K, on a $\Delta = (-1)^{(n-1)/2}\, n$.*

Démonstration. On pose $P(X) = X^n - 1$ d'où $P'(X) = nX^{n-1}$. Soit ζ une racine primitive n-ième de l'unité. Comme n est impair on a $(-1)^{(n-1)/2}\Delta(P) = \prod_{i=1}^{n} P'(\zeta^i) = n^n \prod_{i=1}^{n} \zeta^{i(n-1)} = n^n \prod_{i=1}^{n} \zeta^{-i} = n^n \prod_{k=0}^{n-1} \zeta^k$ (en posant $k = n - i$). On reconnaît le produit des racines de P et on a le résultat.

3 La preuve du théorème

3.1 Notations. Dans ce qui suit p et n désignent des nombres premiers impairs et distincts. On considère le corps $\mathbf{F}_p$ et on note $L = D_{\mathbf{F}_p}(X^n - 1)$ le corps de décomposition de $X^n - 1$ c'est–dire le corps engendré par les racines n-ièmes de l'unité (voir [1]). Soit ζ une racine primitive n-ième, de sorte que les autres racines sont les ζ^i avec $i = 0, 1, \ldots, n-1$. On rappelle que l'application $F : L \to L$ définie par $F(x) = x^p$ est un automorphisme de L (dit de Frobenius) et qu'on a $F(x) = x$ si et seulement si $x \in \mathbf{F}_p$.

3.1 Frobenius

L'automorphisme de Frobenius F agit sur les racines[3] de l'unité par $F(\zeta^i) = \zeta^{ip}$. Il définit une permutation des exposants $0, 1, \ldots, n-1$, donc un élément de $\mathfrak{S}_n$, noté σ_F, par la formule $\sigma_F(i) = ip$ (modulo n). On a alors le résultat suivant :

3.2 Proposition. *La permutation σ_F est paire si et seulement si $(-1)^{(n-1)/2} n$ est un carré de $\mathbf{F}_p$.*

3. Une variante de la preuve consiste à regarder l'action sur les seules racines primitives.

Démonstration. On considère $\delta(X^n-1) = \prod_{0\leq i<j\leq n-1}(\zeta^i-\zeta^j)$. En vertu de 2.3, σ_F est paire si et seulement si $\sigma_F(\delta) = \prod_{0\leq i<j\leq n-1}(\zeta^{\sigma_F(i)}-\zeta^{\sigma_F(j)}) = \delta$. Mais, comme F est un homomorphisme, on a $F(\delta) = \prod_{0\leq i<j\leq n-1}(\zeta^{ip}-\zeta^{jp}) = \sigma_F(\delta)$. La permutation σ_F est donc paire si et seulement si l'on a $F(\delta) = \delta$, ce qui signifie que δ est dans $\mathbf{F}_p$ ou encore que $\Delta(X^n-1)$ est un carré de $\mathbf{F}_p$ et c'est exactement la conclusion en vertu de 2.5.

3.2 L'action de $(\mathbf{Z}/n\mathbf{Z})^*$ sur les racines de l'unité

Le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ opère sur les racines n-ièmes de l'unité ζ^i par la formule $a.\zeta^i = \zeta^{ai}$ $(i = 0, 1, \ldots, n-1)$. Cette action définit un homomorphisme injectif $\psi : (\mathbf{Z}/n\mathbf{Z})^* \to \mathfrak{S}_n$ et on a le résultat suivant :

3.3 Lemme. *Un élément $a \in (\mathbf{Z}/n\mathbf{Z})^*$ est un carré si et seulement si $\psi(a)$ est une permutation paire.*

Démonstration. Si a est un carré, $\psi(a)$ aussi, donc c'est une permutation paire comme on le voit en appliquant la signature. L'image réciproque $\psi^{-1}(\mathfrak{A}_n)$ est un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$, qui contient le sous-groupe d'indice 2 des carrés, et il suffit de montrer que ce n'est pas $(\mathbf{Z}/n\mathbf{Z})^*$ tout entier. Mais on sait que ce groupe est cyclique d'ordre $n-1$ et si a en est un générateur $\psi(a)$ est [4] le $n-1$-cycle $(0)(1, a, \ldots, a^{n-2})$ qui est impair puisque $n-1$ est pair.

3.4 *Remarque.* Parmi les éléments de $(\mathbf{Z}/n\mathbf{Z})^*$ il y a l'élément p et l'action de p sur les racines de l'unité n'est autre que celle donnée par le Frobenius F. On obtient donc :

3.5 Corollaire. *L'homomorphisme de Frobenius induit une permutation paire des racines n-ièmes de l'unité si et seulement si p est un carré modulo n.*

En mettant ensemble 3.2 et 3.5 on obtient le théorème 1.2.

Références

[1] Perrin Daniel, *Cours d'algèbre*, Ellipses, 1996.

4. Attention, $\psi(a)$ est une permutation des racines de l'unité, mais pas nécessairement un élément du groupe de Galois de L sur $\mathbf{F}_p$.