Réciprocité quadratique par le résultant

Leçons

142 Algèbre des polynômes à plusieurs indéterminées.

143 Résultant. Applications

Source Mérindol [Mer06, page 389]. Attention aux quelques petites coquilles, il y a plusieurs échanges entre R et S notamment.

Pré-requis

1. La formule du résultant à partir des racines
2. Le théorème des polynômes symétriques
3. Les propriétés élémentaires du symbole de Legendre

Théorème 1. *Soient p et ℓ deux nombres premiers impairs distincts. Alors*

$$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}. \tag{1}$$

(a) Un lemme sur les polynômes palindromiques

Définition 0.1. Soient A un anneau, $P = a_d X^d + \cdots + a_0$ un polynôme de degré d dans $A[X]$. On lui associe son homogénéisé $\tilde{P} \in A[X, Y]$ par

$$\tilde{P}(X, Y) = a_d X^d + a_{d-1} X^{d-1} Y + \cdots + a_1 X Y^{d-1} + a_0 Y^d$$

On dit que P est palindromique si $\tilde{P} \in A[X, Y]^{\mathfrak{S}_{\{X,Y\}}}$. Cela revient à $a_0 = a_d$, $a_1 = a_{d-1}$ etc.

Lemme 2. *Si $P \in \mathbb{Z}[X]$ est palindromique de degré d pair, alors il existe $S \in \mathbb{Z}[T]$ de degré $d/2$ tel que*

$$P(X) = X^{d/2} S(X + 1/X).$$

Démonstration. D'après le théorème des polynômes symétriques, l'homogénéisé s'écrit sous la forme

$$\tilde{P}(X,Y) = U(X+Y, XY),$$

où U est de degré $d/2$. Puisque $\tilde{P}$ est homogène de degré pair, et comme les puissances de XY sont de degré pair, il ne peut pas y avoir de puissance impaire de la première variable dans U ; ainsi, il existe V puis W homogènes de degré $d/2$ tels que

$$\tilde{P}(X,Y) = V\left((X+Y)^2, XY\right) = W\left(X^2+Y^2, XY\right).$$

Posons alors $S(X) = W(X,1)$. Dans $\mathbb{Q}(X)$, il vient

$$\begin{aligned} P(X) = \tilde{P}(X,1) = W\left(X^2+1, X\right) &= X^{d/2} W(X+1/X, 1) \\ &= X^{d/2} S(X+1/X). \quad \square \end{aligned}$$

(b) Les polynômes K_p

Proposition 3. *Soit p un nombre premier impair. Le polynôme*

$$P(X) = X^{p-1} + \cdots + X + 1$$

est palindromique. On lui associe V_p tel que $P(X) = X^{(p-1)/2} V_p(X+1/X)$, unitaire de degré $(n-1)/2$, puis $K_p(Y) = V_p(Y+2)$. Alors

$$\begin{aligned} K_p(0) &= p && (2) \\ K_p(Y) &\equiv Y^{(p-1)/2}(p). && (3) \end{aligned}$$

Démonstration. Pour (2) on calcule directement :

$$K_p(0) = V_p(2) = V_p(1+1/1) = p.$$

Pour (3) remarquons que modulo p, d'après le petit théorème de Fermat

$$X^{p-1} + \cdots + 1 \equiv \frac{X^p - 1}{X-1} \equiv \frac{(X-1)^p}{X-1} \equiv (X-1)^{p-1},$$

d'où $V_p(X+1/X) \equiv X^{-\frac{p-1}{2}}(X-1)^{p-1} \equiv \left[\frac{(X-1)^2}{X}\right]^{\frac{p-1}{2}} \equiv \left(X-2+X^{-1}\right)^{\frac{p-1}{2}}$, puis $K_p(Y) \equiv Y^{\frac{p-1}{2}}$. $\square$

(c) Loi de réciprocité quadratique

Proposition 4. *Soient p et ℓ premiers, impairs, distincts. Alors*

$$\left(\frac{\ell}{p}\right) = \operatorname{Res}(K_p, K_\ell). \quad (4)$$

Démonstration. Déjà, $\operatorname{Res}(K_p, K_\ell)$ est dans $\mathbb{Z}$. Soit r un nombre premier qui le divise. Alors les réductions $\overline{K_p}$ et $\overline{K_\ell}$ modulo r ont une racine commune ρ dans une extension K de $\mathbb{F}_r$. Si L est un corps de décomposition de $T^2 - 2T + 1 - \rho$ sur K, et x une racine de ce polynôme, alors $x + x^{-1} - 2 = \rho$. Etant données les définitions de K_p et K_ℓ, x est racine de $X^p - 1$ et $X^\ell - 1$, ce qui est absurde. Donc $\operatorname{Res}(K_p, K_\ell)$ est dans $\{\pm 1\}$.

Ensuite, on utilise (3) puis (2) de la proposition précédente pour obtenir modulo p

$$\begin{aligned}\operatorname{Res}(K_p, K_\ell) \equiv \operatorname{Res}\left(Y^{\frac{p-1}{2}}, K_q\right) &\equiv \operatorname{Res}(Y, K_q)^{\frac{p-1}{2}} \\ &\equiv K_\ell(0)^{\frac{p-1}{2}} \\ &\equiv \ell^{\frac{p-1}{2}}.\end{aligned}$$

Puisque $\operatorname{Res}(K_p, K_\ell) = \pm 1$, ceci conclut. □

Finalement,

$$\begin{aligned}\left(\frac{\ell}{p}\right) = \operatorname{Res}(K_p, K_\ell) &= (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} \operatorname{Res}(K_\ell, K_p) \\ &= (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} \left(\frac{\ell}{p}\right).\end{aligned}$$

Remarque 5. Une grande-aïlleule de cette preuve a été publiée (en français) par Gotthold Eisenstein en 1845 au journal de Crelle [Eis45, p.179] et elle est reprise dans le cours de Serre [Ser70, I, Appendice]. Un calcul montre que le polynôme K_p se scinde sur $\mathbb{R}$ et

$$K_p(Y) = \prod_{k=1}^{(p-1)/2} \left(Y + 4\sin^2 \frac{\pi k}{p}\right),$$

d'où l'on déduit

$$\left(\frac{\ell}{p}\right) = 4^{\frac{\ell-1}{2}\frac{p-1}{2}} \prod_{j=1}^{(p-1)/2} \prod_{k=1}^{(\ell-1)/2} \left(\sin^2 \frac{\pi k}{\ell} - \sin^2 \frac{\pi k}{p}\right).$$

La loi de réciprocité quadratique est alors visible sur le produit de droite. Eisenstein décrit sa méthode comme une élimination, opération d'ordre algébrique, ce qui explique le titre « Application de l'Algèbre à l'Arithmétique transcendante ». Il l'applique aux résidus biquadratiques et laisse les résidus cubiques au lecteur...

Références

[Eis45] G. Eisenstein. Applications de l'Algèbre à l'Arithmétique transcendante. *J. Reine Angew. Math.*, 29 :177–184, 1845.

[Mer06] Jean-Yves Merindol. *Nombres et algèbres*. Collection Grenoble Sciences. EDP Sciences, 2006.

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique : par Jean-Pierre Serre*. SUP. Le mathématicien. Presses universitaires de France, 1970.