Loi de réciprocité quadratique (bis)

Mon développement

On rappelle deux propriétés du symbole de Legendre. Pour tous $x, y \in \mathbb{Z}$ et tout nombre premier impair p, on a :

(i)
$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) ,$$

(ii)
$$\left(\frac{x}{p}\right) \equiv x^{(p-1)/2}[p] .$$

Théorème. Soient p et q deux nombres premiers impairs distincts. On a
$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right) .$$

Pour tout entier impair n, on note
$$V_n(X) = \prod_{k=1}^{(n-1)/2}\left(X - 2\cos\left(\frac{2k\pi}{n}\right)\right)$$
et
$$K_n(X) = \prod_{k=1}^{(n-1)/2}\left(X + 4\sin^2\left(\frac{k\pi}{n}\right)\right) = V_n(X+2) .$$

Lemme. Ces polynômes ont les propriétés suivantes.
(a) K_n est unitaire de degré $\frac{n-1}{2}$.
(b) On a
$$X^{(n-1)/2}V_n(X + X^{-1}) = \sum_{k=0}^{n-1} X^k .$$
(c) On a $K_n(0) = n$.
(d) Si p est premier impair, alors $K_p(Y) = Y^{(p-1)/2}$ dans $\mathbb{F}_p[Y]$, où $Y = X - 2 + X^{-1}$.
(e) Si p est premier impair, alors K_p est à coefficients dans $\mathbb{Z}$.

Le point (a) est évident. Ensuite, on a
$$\begin{aligned} X^{(n-1)/2}V_n(X + X^{-1}) &= \prod_{k=1}^{(n-1)/2}\left(X^2 - 2\cos\left(\frac{2k\pi}{n}\right)X + 1\right) \\ &= \prod_{k=1}^{(n-1)/2}\left(X - e^{2ik\pi/n}\right)\left(X - e^{-2ik\pi/n}\right) \\ &= \frac{X^n - 1}{X - 1} \end{aligned}$$
ce qui permet d'obtenir (b). Puisque $K_n(0) = V_n(2)$, le point (c) en découle en appliquant cette relation en 1.

Enfin, soit p un nombre premier impair. En utilisant (b) et le morphisme de Frobenius, on a, dans $\mathbb{F}_p[X]$,

$$X^{(p-1)/2}V_p(X+X^{-1}) = \frac{X^p-1}{X-1} = (X-1)^{p-1}$$

donc

$$K_p(X-2+X^{-1}) = V_p(X+X^{-1}) = \left(X^{-1}(X-1)^2\right)^{(p-1)/2} = (X-2+X^{-1})^{(p-1)/2}$$

d'où, en posant $Y = X-2+X^{-1}$, $K_p(Y) = Y^{(p-1)/2}$ dans $\mathbb{F}_p[Y]$. Le point (d) est donc démontré et le point (e) en est une conséquence directe. □

On va maintenant démontrer la loi de réciprocité quadratique à l'aide de la loi de réciprocité des résultants. Soient p et q deux nombres premiers impairs distincts. D'après (e), le résultant $\mathrm{Res}(K_p(Y), K_q(Y))$ est un entier, et il est non nul car K_p et K_q sont scindés sans racine commune, donc premiers entre eux. On va montrer que ce résultant vaut -1 ou 1, puis qu'il est égal à $\left(\frac{q}{p}\right)$ modulo p.

D'une part, on suppose que le résultant $\mathrm{Res}(K_p(Y), K_q(Y))$ ne vaut ni -1, ni 1. Il existe alors un nombre premier r qui le divise, donc $K_p(Y)$ et $K_q(Y)$ ne sont pas premiers dans $\mathbb{F}_r[Y]$. Dans une extension de $\mathbb{F}_r$, $K_p(Y)$ et $K_q(Y)$ ont donc une racine commune y, donc, dans une extension de $\mathbb{F}_r$ (une extension de la précédente), l'équation $x-2+x^{-1} = y$ admet une solution x qui n'est pas égale à 1. D'après (b),

$$(X-1)X^{(p-1)/2}K_p(X-2+X^{-1}) = X^p-1$$

et

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

donc x est à la fois racine de X^p-1 et de X^q-1. Ceci contredit le fait que $x \neq 1$.
On a ainsi montré par l'absurde que $\mathrm{Res}(K_p(Y), K_q(Y))$ vaut -1 ou 1.

D'autre part, dans $\mathbb{F}_p$, on a

$$\begin{aligned}
\mathrm{Res}(K_p(Y), K_q(Y)) &= \mathrm{Res}(Y^{(p-1)/2}, K_q(Y)) \qquad \text{(d'après (e))} \\
&= (\mathrm{Res}(Y, K_q(Y)))^{(p-1)/2} \qquad \text{(multiplicativité du résultant)} \\
&= (K_q(0))^{(p-1)/2} \\
&= q^{(p-1)/2} \qquad \text{(d'après (c))} \\
&= \left(\frac{q}{p}\right) \qquad \text{(d'après (ii))}.
\end{aligned}$$

Finalement, on a montré que $\mathrm{Res}(K_p(Y), K_q(Y))$ vaut -1 ou 1 et qu'il est congru à $\left(\frac{q}{p}\right)$ modulo p. p étant impair, on en déduit que

$$\mathrm{Res}(K_p(Y), K_q(Y)) = \left(\frac{q}{p}\right) .$$

D'après la loi de réciprocité pour les résultants, on en conclut que

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\mathrm{Res}(K_q(Y), K_p(Y)) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)$$

□

Références

J'ai utilisé [Hin08, p. 70], [Mér06, p. 389].

Leçons correspondantes

J'utilise ce développement pour la leçon 146. On peut également l'utiliser pour les leçons 109, 110, 112.

Remarques

- Le polynôme V_p est noté Φ_p^+ dans [Hin08], c'est le p-ième polynôme cyclotomique réel.
- On peut montrer différemment que $\mathrm{Res}(K_p(Y), K_q(Y))$ vaut -1 ou 1, voir [Hin08, p. 70].
- Il existe d'autres preuves de la loi de réciprocité quadratique, dont l'une constitue d'ailleurs un autre de mes développements. Voir par exemple [Hin08, p. 14], [Ser77, p. 16], [Hin08, p. 26], [Ser77, p.18].
- Grâce à la loi de réciprocité quadratique et aux autres propriétés du symbole de Legendre, on peut calculer n'importe quel symbole de Legendre.

Questions possibles

1. Citer une application de la loi de réciprocité quadratique.
2. Citer une application des symboles de Legendre.
3. A-t-on $K_p(X) = X^{(p-1)/2}$ dans $\mathbb{F}_p[X]$?
4. Démontrer la loi de réciprocité des résultants.
5. Montrer que pour tout p premier impair,
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$
6. Montrer que pour tout p premier impair,
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$
7. Calculer $\left(\frac{29}{43}\right)$.

Références

[Hin08] Marc Hindry : *Arithmétique*. Calvage & Mounet, 2008.

[Mér06] Jean-Yves Mérindol : *Nombres et algèbre*. EDP Sciences, 2006.

[Ser77] Jean-Pierre Serre : *Cours d'arithmétique*. Presses Universitaires de France, 1977.