Dans les méandres de la pensée d'Emil Artin

(Kta)Phil Caldero

Séminaire de mathématiques Ktorphée

14/09/24

I. Réciprocité quadratique, ses interprétations

On commence par prendre un nombre premier impair p et on pose, pour tout entier d non divisible par p

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{si } d \text{ est un carré modulo } p \\ -1 & \text{sinon} \end{cases}$$

On montre que $\left(\frac{d}{p}\right) = d^{\frac{p-1}{2}}$ modulo p.

Ceci implique que la fonction $\left(\frac{?}{p}\right)$ de $(\mathbb{Z}/p\mathbb{Z})^*$ est multiplicative.

Scoop : le produit de deux non carrés est un carré ! Comme dans $\mathbb{R}$ finalement.

Théorème

Loi de réciprocité quadratique (LRQ)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

avec p, q premiers différent de 2.

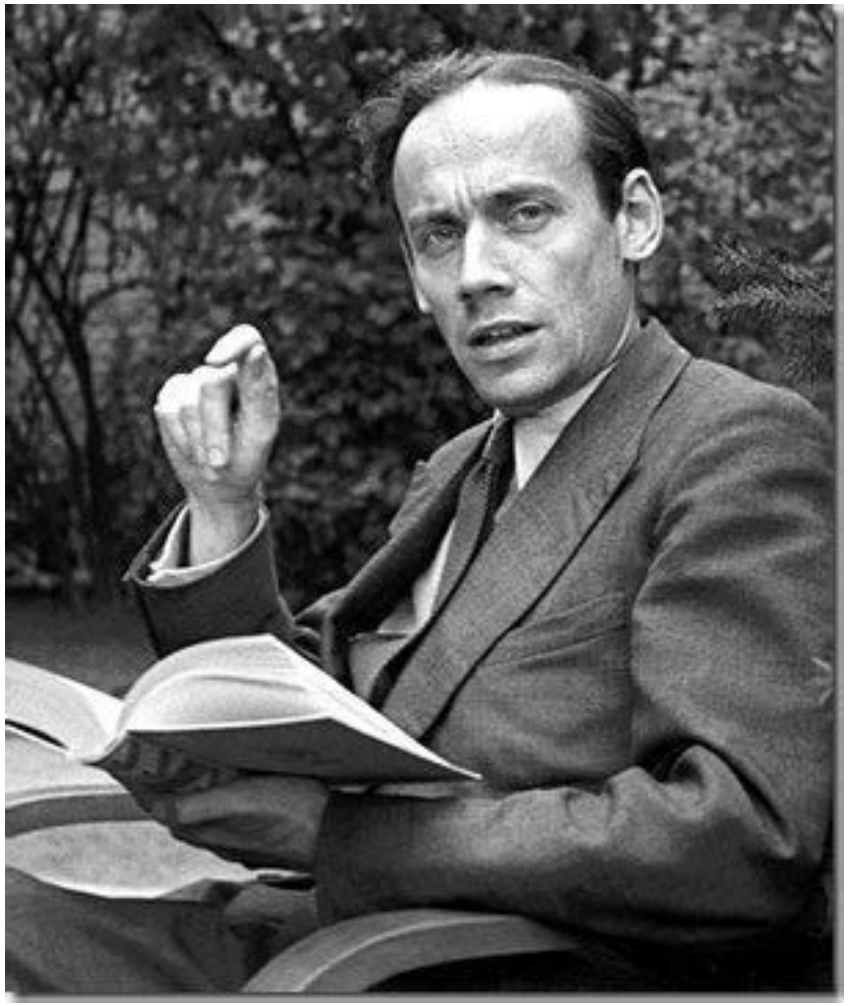
Cette réciprocité peut paraître déconcertante : on compare deux mondes qui ne se côtoient pas.

Exemple d'utilisation : $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = 1.$

On note que la fonction sur les nombres premiers $\left(\frac{13}{?}\right)$ est de "période 13". Par exemple, $\left(\frac{13}{29}\right) = \left(\frac{13}{3}\right) = 1$

But : On va généraliser dans un premier temps le symbole de Legendre en remplaçant d par le polynôme $X^2 - d$, puis $X^2 - d$ par un polynôme unitaire $f \in \mathbb{Z}[X]$. La condition p impair ne divise pas d devient p ne divise pas $\Delta(f)$. On veut donner un sens à $\left(\frac{f}{p}\right)$, puis, dans ce contexte, à la loi de réciprocité (qui n'est plus quadratique, et n'est plus réciproque !). On peut se demander pourquoi faire cela. Déjà afin de comprendre le comportement de f modulo p à partir du comportement de f modulo q. On va tomber sur la loi de réciprocité d'Artin, qui est la pierre angulaire de la théorie des corps de classe.

Bref, on est parti pour un grand voyage en Arithmétique.



Idée : On va tout d'abord interpréter la LRQ par une périodicité de la fonction $\left(\frac{d}{?}\right)$.

(Formulation d'Euler de la LRQ)

Soit p, q premiers ne divisant pas $2d$.

$$p \equiv q\,[4d] \Longrightarrow \left(\frac{d}{p}\right) = \left(\frac{d}{q}\right)$$

$$p \equiv -q\,[4d] \Longrightarrow \left(\frac{d}{p}\right) = \operatorname{sgn}(d)\left(\frac{d}{q}\right)$$

(Formulation de Legendre de la LRQ)

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

avec p, q premiers différent de 2.

C'est Legendre qui fait le lien entre cette formulation, et la formulation devenue classique de "réciprocité".
Montrons que les deux formulations sont équivalentes.

Montrons que "Legendre $\Longrightarrow$ Euler".
On se ramène aux cas : $d = -1$ et d premier (positif) (avec $d = 2$ et $d \neq 2$).

Pour $d = 2$, on fait la vérification à la main grâce à la loi complémentaire.

On va en fait juste montrer la seconde implication, la première étant analogue en plus simple.

On suppose $p \equiv -q\,[4d]$. On va montrer $\left(\frac{d}{p}\right) = \mathrm{sgn}(d)\left(\frac{d}{q}\right)$ pour $d = r$ premier positif et $d = -1$.

$$\left(\frac{r}{p}\right) = (-1)^{\frac{p-1}{2}\frac{r-1}{2}}\left(\frac{p}{r}\right) = (-1)^{\frac{p-1}{2}\frac{r-1}{2}}\left(\frac{-q+4kr}{r}\right)$$
$$=(\text{-}1)^{\frac{p-1}{2}\frac{r-1}{2}}\left(\frac{-q}{r}\right) = (-1)^{\frac{p-1}{2}\frac{r-1}{2}+\frac{r-1}{2}}\left(\frac{q}{r}\right)$$
$$=(\text{-}1)^{t}\left(\frac{r}{q}\right),$$

avec $t := \frac{p-1}{2}\frac{r-1}{2} + \frac{r-1}{2} + \frac{q-1}{2}\frac{r-1}{2}$ qui est pair. Donc, $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right)$.

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

$$=(\text{-}1)^{\frac{q+1}{2}} = -(-1)^{\frac{q-1}{2}} = \operatorname{sgn}(-1)\left(\frac{-1}{q}\right).$$

Réciproquement, montrons que "Euler $\Longrightarrow$ Legendre".
Si p et q sont deux nombres premiers impairs, on a soit $p - q \equiv 0$, [4], soit $p + q \equiv 0$, [4]. On va juste faire le second cas.
On pose $p = -q + 4k$, $k > 0$.

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4k}{q}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{q-4k}{q}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{-4k}{q}\right)$$
$$= \left(\frac{k}{q}\right) = \operatorname{sgn}(k)\left(\frac{k}{q}\right) = \left(\frac{k}{p}\right) = \left(\frac{q}{p}\right),$$

Or, dans cette situation, $\frac{p-1}{2}\frac{q-1}{2}$ est pair. On a donc $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$.

Regardons de plus près l'implication

$$p \equiv q\,[4d] \Longrightarrow \left(\frac{d}{p}\right) = \left(\frac{d}{q}\right)$$

On peut la voir comme une périodicité de la fonction $\left(\frac{d}{?}\right)$, pour les p premiers avec $2d$.

Mieux ! On montre comme ci-dessus que si p, q, s sont premiers avec $2d$.

$$p \equiv qs\,[4d] \Longrightarrow \left(\frac{d}{p}\right) = \left(\frac{d}{q}\right)\left(\frac{d}{s}\right)$$

On le montre pour $d = r$ premier (par commutativité !) et pour $d = -1$. Dans les deux cas, on va devoir montrer que

$$\frac{qs-1}{2} - \frac{q-1}{2} - \frac{s-1}{2} \text{ est pair}$$

Or, il est égal à $\frac{(1-q)(1-s)}{2}$... De même , on montre que si $p_1 \dots p_k \equiv q_1 \cdots q_\ell \bmod 4d$, alors $\prod_{i=1}^{k} \left(\frac{d}{p_i}\right) = \prod_{j=1}^{\ell} \left(\frac{d}{q_j}\right)$.

Comme le groupe multiplicatif $(\mathbb{Z}/4d\mathbb{Z})^*$ est engendré par les classes de nombres premiers premiers avec $2d$, on obtient, grâce à 1) la périodicité, et 2) la multiplicativité

Théorème (Loi de réciprocité quadratique d'Artin)

On a un morphisme de groupes

$$(\mathbb{Z}/4d\mathbb{Z})^* \to \{1,-1\},\ p \mapsto \left(\frac{d}{p}\right).$$

A la classe de $n = \prod_i p_i$, on associe donc $\prod_{i=1}^{k} \left(\frac{d}{p_i}\right)$. On vérifie que l'application est bien définie et que c'est un morphisme.

En aparté, voir en video pourquoi y a-t-il "autant" de nombres premiers congrus à 1 et à 3 modulo 4? et aussi
Réciprocité quadratique: l'approche de Zolotarev

II. La loi de réciprocité d'Artin sur $\mathbb{Z}$

On voit maintenant comment généraliser une loi de réciprocité en degré supérieur : On fixe $f \in \mathbb{Z}[X]$ unitaire, et on voudrait un morphisme de groupes $p \mapsto \left(\frac{f}{p}\right)$.

De quoi vers quoi ?

Le groupe de départ devrait être $(\mathbb{Z}/\Delta(f)\mathbb{Z})^*$.

On peut aussi se douter que ce qui va remplacer le groupe $\{1, -1\}$: le groupe de Galois de f sur $\mathbb{Q}$.
En effet, dans le cas quadratique, si d est un carré de $\mathbb{Z}$, alors le groupe de Galois G de $X^2 - d$ est trivial, et en même temps, $\left(\frac{d}{p}\right)$ vaut toujours 1. Si d n'est pas un carré, alors $G :\simeq \{1, -1\}$. Les deux automorphismes de $\mathbb{Q}[\sqrt{d}]$ étant ceux définis par $\sqrt{d} \mapsto \pm\sqrt{d}$. Par exemple, si $d = -1$, on retrouve le morphisme bar de $\mathbb{Q}[i]$.

Dans les deux cas, l'image du morphisme est le groupe de Galois de $X^2 - d$.

Afin d'unifier le cas quadratique et de degré supérieur, on pose $\alpha = \sqrt{d}$.

Par abus de notation, on notera toujours α une racine de $X^2 - d$ quelque soit le corps.

$$\alpha := \overline{X} \in \mathbb{K}[X]/(X^2 - d).$$

On rappelle que $x \mapsto x^p$ définit un automorphisme du corps $\mathbb{F}_p[\alpha]$, appelé morphisme de Frobenius.

Nous allons voir que, dans le cas quadratique, le morphisme de Frobenius se relève en un $\mathbb{Q}$-automorphisme du corps $\mathbb{Q}[\sqrt{d}]$.

Pour cela, on effectue la division euclidienne de X^p par $X^2 - d$ dans $\mathbb{Z}$.

$$X^p = Q \cdot (X^2 - d) + aX + b$$

$$\alpha^p = a\alpha + b$$

$$-\alpha^p = -a\alpha + b$$

$$X^p = Q \cdot (X^2 - d) + \alpha^{p-1}X = Q \cdot (X^2 - d) + d^{\frac{p-1}{2}}X.$$

Attention, $d^{\frac{p-1}{2}} = \pm 1$ modulo p, c'est-à-dire que, dans $\mathbb{Z}$, $d^{\frac{p-1}{2}} = \pm 1 + pk$, $k \in \mathbb{Z}$.

Il vient

$$\alpha^p = \left(\frac{d}{p}\right)\alpha + pk\alpha, \ k \in \mathbb{Z}$$

.

On n'est pas loin de définir le symbole d'Artin φ_p (que l'on peut penser comme $\left(\frac{f}{p}\right)$). Mais il reste à faire sur f une

(Hypothèse drastique)

Il existe un groupe abélien G d'automorphismes de $\mathbb{Q}[\alpha] = \mathbb{Q}[X]/(f)$ tel que

$$f = \prod_{\sigma \in G} (X - \sigma(\alpha)).$$

Si f est irréductible, cela revient à dire que le groupe de Galois de f est abélien, ce qui est toujours assuré en degré 2, mais pas pour $n \geq 3$.

Exemple pour $n = 3$

Soit ω_7 une racine primitive 7-ième de l'unité (dans $\mathbb{C}$). On pose $\alpha := \omega_7 + \omega_7^{-1}$. On sait que le polynôme minimal sur $\mathbb{Q}$ de ω_7 est le polynôme cyclotomique

$$\phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

La théorie de Galois assure que le polynôme minimal f de α sur $\mathbb{Q}$ est de degré 3, mais on peut le trouver à la main.

On pose
$\alpha := \omega_7 + \omega_7^{-1}$, $\beta := \omega_7^2 + \omega_7^{-2} = \alpha^2 - 2$,

$\gamma := \omega_7^3 + \omega_7^{-3} = \alpha^3 - 3\alpha$.

En écrivant

$$\omega_7^3 + \omega_7^2 + \omega_7 + \omega_7^{-1} + \omega_7^{-2} + \omega_7^{-3} = -1,$$

on obtient

$$\alpha^3 + \alpha^2 - 2\alpha - 1 = 0,$$

et on vérifie que $f := X^3 + X^2 - 2X - 1$ est le polynôme minimal de α sur $\mathbb{Q}$.

Comme on n'a pas fait de choix de racine primitive de l'unité, β et γ sont les deux autres racines de f.

Décrivons le groupe G. Comme f est à coefficients dans $\mathbb{Q}$, un $\mathbb{Q}$-automorphisme de $\mathbb{Q}[\alpha]$ envoie α sur une racine de f, c'est-à-dire α, β, ou γ (qui sont bien tous dans $\mathbb{Q}[\alpha]$). Tout automorphisme est entièrement déterminé par l'image de α.

On a donc $G = \{\mathrm{id}, \sigma, \tau\}$, où $\sigma(P(\alpha)) = P(\beta)$, et $\tau(P(\alpha)) = P(\gamma)$, pour tout $P \in \mathbb{Q}[X]$.

Pour p premier, on va relever le Frobenius sur $\mathbb{F}_p[\alpha]$ sur $\mathbb{Q}[\alpha]$, par analogie avec le cas quadratique.

- $p = 2$.

$\alpha^2 \equiv \sigma(\alpha)$ [2]. On écrira $\varphi_2 = \sigma$.

- $p = 3$.

$\alpha^3 \equiv \tau(\alpha)$ [3]. $\varphi_3 = \tau$.

- $p = 5$.

$$X^5 = (X^2 - X + 3)(X^3 + X^2 - 2X - 1) - 4X^2 + 5X + 3$$

$\alpha^5 = -4\alpha^2 + 5\alpha + 3 \equiv \alpha^2 - 2 = \sigma(\alpha)$ [5]. $\varphi_5 = \sigma$.

- $p = 7$.

$$X^7 = (X^4 - X^3 + 3X^2 - 4X + 9)(X^3 + X^2 - 2X - 1) - 14X^2 + 14X + 9$$

$\alpha^7 = 2$ [7]. $\varphi_7 =$???.

Pourquoi le petit miracle ne se reproduit plus ?

On va calculer le discriminant de f. En posant $X = Y - \frac{1}{3}$, il vient

$$f = X^3 + X^2 - 2X - 1 = Y^3 - \frac{7}{3}Y - \frac{7}{27}$$

$$\Delta(f) = -4 \cdot \Big(-\frac{7}{3}\Big)^3 - 27\Big(-\frac{7}{27}\Big)^2 = 49 = 7^2.$$

Il faut respecter la condition que p ne divise pas $\Delta(f)$.

On trouve, par multiplicativité, juste à l'aide de φ_2 et φ_3

$$\varphi_2 = \sigma,\ \varphi_3 = \tau,\ \varphi_5 = \sigma,$$

$$\varphi_{11} = \tau,\ \varphi_{13} = \mathrm{id},\ \varphi_{17} = \tau,$$

$$\varphi_{19} = \sigma,\ \varphi_{23} = \sigma,\ \varphi_{29} = \mathrm{id}$$

On peut énoncer la définition/proposition

Proposition (Symbole d'Artin)

Dans l'hypothèse "abélienne" faite sur le polynôme f de degré n, il existe, pour tout p premier *ne divisant pas* $\Delta(f)$, un unique automorphisme φ_p de $\mathbb{Q}[\alpha]$ qui relève le Frobenius de $\mathbb{F}_p[\alpha]$

$$\alpha^p = \varphi_p(\alpha) + p(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}),$$

où les a_i sont des rationnels dont les dénominateurs ne sont pas multiples de p.

La loi de réciprocité d'Artin (sur $\mathbb{Q}$) s'énonce alors ainsi :

Théorème (Loi de réciprocité d'Artin sur $\mathbb{Q}$)

Avec les hypothèses précédentes, il existe un (unique) morphisme de $(\mathbb{Z}/\Delta(f)\mathbb{Z})^*$ dans G qui envoie tout nombre premier p ne divisant pas $\Delta(f)$ sur φ_p.

On voit alors deux façons d'aller d'un nombre premier à l'autre :
1) la périodicité,

2) la multiplicativité.

Revenons à l'exemple qui précède. On a une période de 49, mais on peut faire mieux, car G est d'ordre 3.
La surjection canonique $\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ fournit un morphisme d'anneaux $\mathbb{Z}/49\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$, puis un morphisme de groupes $A := (\mathbb{Z}/49\mathbb{Z})^* \to (\mathbb{Z}/7\mathbb{Z})^*$, qui reste surjectif. Son noyau K est un groupe abélien d'ordre $\varphi(49)/\varphi(7) = 42/6 = 7$ et $A/K \simeq (\mathbb{Z}/7\mathbb{Z})^*$. Or, K s'envoie trivialement sur G, car G est d'ordre 3 premier avec 7. Donc, le morphisme d'Artin passe au quotient en $(\mathbb{Z}/7\mathbb{Z})^* \to G$, et on a une période de 7, que l'on peut constater...

En aparté, voir en vidéo Un fractal de Pascal

III. Prolongements de la théorie

On peut prolonger cette théorie sur d'autres corps que $\mathbb{Q}$, comme les corps de nombres : $K = \mathbb{Q}[\sqrt{7}]$, $K = \mathbb{Q}[i]$, $K = \mathbb{Q}[\sqrt[3]{2}]$...

Il faut alors trouver de bonnes généralisations. Tout d'abord $\mathbb{Z}$ sera remplacé par l'anneau $\mathbb{Z}_K$ des éléments de K entiers sur $\mathbb{Z}$ (racines d'un polynôme unitaire de $\mathbb{Z}[X]$).

• Les nombres premiers seront remplacés par les idéaux premiers $\mathfrak{p}$ de $\mathbb{Z}_K$, pour obtenir un corps fini $\mathbb{Z}_K/\mathfrak{p}$ et son Frobenius.
• Le polynôme f sera un polynôme unitaire de $\mathbb{Z}_K[X]$ de groupe de Galois abélien G et de discriminant $\Delta(f) \in \mathbb{Z}_K$.
• Un théorème d'Artin assure alors que l'on peut relever le Frobenius en un élément $\varphi_{\mathfrak{p}}$ de G.
• Le groupe $(\mathbb{Z}/\Delta(f)\mathbb{Z})^*$ ne peut pas être remplacé par le groupe $(\mathbb{Z}_K/\Delta(f)\mathbb{Z}_K)^*$, mais par le groupe $\mathrm{Cl}_{\Delta(f)}$ fourni par générateurs et relations : les générateurs sont les $[\mathfrak{p}]$, où $\mathfrak{p}$ parcourt les idéaux premiers de $\mathbb{Z}_K$ premiers avec l'idéal $\Delta(f)\mathbb{Z}_K$. Les relations sont données par $[\mathfrak{p}_1]\cdots[\mathfrak{p}_k] = 1$ dès que $\mathfrak{p}_1 \cdots \mathfrak{p}_k = \nu\mathbb{Z}_K$, avec $\nu = 1$ mod $\Delta(f)\mathbb{Z}_K$.
En effet, on vérifie que si $K = \mathbb{Q}$ (et donc $\mathbb{Z}_K = \mathbb{Z}$), on a un isomorphisme de groupes

$$\mathrm{Cl}_{\Delta(f)} \simeq (\mathbb{Z}/\Delta(f)\mathbb{Z})^*$$

Notez que cette définition de $\mathrm{Cl}_{\Delta(f)}$ nous vient de Chevalley.
Le théorème de réciprocité d'Artin s'énonce alors

Théorème (Théorème de réciprocité d'Artin)

On définit un morphisme $\mathrm{Cl}_{\Delta(f)} \to G$ par $[\mathfrak{p}] \mapsto \varphi_{\mathfrak{p}}$.

Une autre façon d'exprimer le résultat d'Artin est de dire

Théorème

Soit K un corps de nombre et L une extension abélienne de K. Soit $\mathfrak{p}$ un idéal premier de l'anneau des entiers de K et $\mathfrak{q}$ premier au-dessus de $\mathfrak{p}$. Alors, il existe un unique $\left(\frac{L/K}{\mathfrak{q}}\right) \in \mathrm{Gal}(L/K)$ tel que pour tout α de L, $\left(\frac{L/K}{\mathfrak{q}}\right)(\alpha) = \alpha^{N(\mathfrak{p})} \bmod \mathfrak{q}$, où N désigne la norme de l'idéal.

En aparté, voir en vidéo Groupe de Galois et réduction modulo p

Merci aux organisateurs pour avoir su créer cette ambiance unique et en même temps si bien adaptée au cadre d'un séminaire de mathématiques.

Et bien sûr merci à tous les participants Antoine, Corentin, Garance, Guillaume, Laura, Lucas, Maugan, Mona, Olivier, Quentin, et Sélène ! J'ai eu l'impression d'avoir passé une soirée avec des anges... mais sous terre, et ouais, maintenant c'est là qu'ils habitent !

Pour Garance et Guillaume, une spéciale dédicace CVA ! ! ! :-)

Et bonne soutenance à toi, Antoine ! En attendant que tu m'éclaires un peu sur les modules de Drinfel'd...