Lois de réciprocité

Comprendre ce qu'est, au sens le plus général, une *loi de réciprocité*, est l'une des questions qui ont guidé et motivé tout le développement de la théorie algébrique des nombres, depuis les *Disquisitiones Arithmeticae* jusqu'aux recherches très actuelles qui s'incrivent dans le programme de Langlands. Nous nous proposons d'esquisser quelques éléments de réponses, au moins dans ce que l'on appellera le cas abélien, en faisant valoir de quelle façon certaines constructions abstraites du XX$^{\text{e}}$ siècle répondent aux questions du XVIII$^{\text{e}}$.

1 Les origines

Le terme de « loi de réciprocité » est dû à Legendre. Alors qu'il travaillait autour du petit théorème de Fermat, et de ce que l'on pourrait appeler la théorie des congruences, il énonce en 1785 le résultat suivant. [1]

Théorème 1 (Loi de réciprocité quadratique) *Si p et ℓ sont des nombres premiers impairs distincts, on a :*

$$\left(\frac{p}{\ell}\right) = (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} \left(\frac{\ell}{p}\right) \quad et \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

où le symbole de Legendre $\left(\frac{a}{p}\right)$, défini pour tout a non divisible par p, vaut $+1$ ou -1 selon que a est ou non un carré modulo p. [2]

Euler avait noté, bien plus tôt, un résultat équivalent dans son *Opusculum Analyticum*, mais s'avouait impuissant à le démontrer. Legendre en donne, quant à lui, une démonstration incomplète, et reposant sur un résultat qu'il ne parvient pas à montrer (une conséquence du théorème de la progression arithmétique de Dirichlet).

Les deux premières démonstrations complètes datent probablement de 1796. Elles sont l'œvre de Gauss, qui a alors dix-neuf ans ! Ils ne les publiera toutefois que cinq ans plus tard, dans ses *Disquisitiones*. Par la suite, les plus grands arithméticiens ont également donné des démonstrations de la loi de réciprocité quadratique, souvent pour tenter d'en trouver des généralisations : Eisenstein, Dedekind, Kronecker, puis Weil et Tate ont ainsi proposé leurs preuves.

Cet intérêt formidable pour un énoncé pour le moins mystérieux au premier abord est ce que nous aimerions comprendre. Donnons-en tout de suite une application.

Proposition 1 *Soit n un entier qui est un carré modulo p pour tout p sauf peut-être un nombre fini.* [3] *Alors n est un carré dans $\mathbf{Z}$.*

On aura besoin d'une forme un peu plus générale de la réciprocité quadratique, et qui en est une conséquence facile :

Théorème 2 (Loi de réciprocité de Gauss) *Pour tout entier impair $b = \pm p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, on définit le symbole de Jacobi $\left(\frac{a}{b}\right)$ par : $\left(\frac{a}{b}\right) = \prod_i \left(\frac{a}{p_i}\right)^{\alpha_i}$ pour tout a premier à b. Alors pour a et b impairs distincts, on a :*

$$\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} (-1)^{\frac{\operatorname{sgn} a-1}{2}\frac{\operatorname{sgn} b-1}{2}} \left(\frac{b}{a}\right) \quad et \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{2}}$$

Démonstration (de la proposition). On raisonne par l'absurde, en supposant n carré modulo p pour tout p différent de $p_1, \ldots, p_m$ (en particulier, $p_i \not| n$). Sans perte de généralité, on suppose n libre de carré et différent de ± 1 et ± 2. Il s'écrit donc $h\ell_1 \cdots \ell_k$, où $h \in \{\pm 1, \pm 2\}$ et où les ℓ_i sont premiers impairs distincts ($k \geq 1$). Il existe un entier naturel a tel que :

$$a \equiv 1 \pmod{8p_1 \cdots p_m \cdot \ell_1 \cdots \ell_{k-1}} \quad \text{et} \quad a \equiv r \pmod{\ell_k}$$

1. On en donne un peu plus loin une démonstration assez sophistiquée mais particulièrement courte. Pour plusieurs démonstrations dans l'esprit de Gauss, on renvoie à [IR82]. Les détails historiques sont développés dans [EE86].

2. Le symbole de Legendre $\left(\frac{-}{p}\right)$ est donc, en langage moderne, le morphisme surjectif canonique $\mathbf{F}_p^\times \to \mathbf{F}_p^\times/(\mathbf{F}_p^\times)^2 \cong \{\pm 1\}$. On a $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

3. Par p et ℓ, on désignera toujours des nombres premiers impairs

Il vient, par la loi de réciprocité de Gauss (et éventuellement la loi supplémentaire si n est pair) :

$$\left(\frac{n}{a}\right) = \left(\frac{\ell_1 \cdots \ell_k}{a}\right) = \prod_i \left(\frac{a}{\ell_i}\right) = \left(\frac{1}{\ell_1}\right) \cdots \left(\frac{1}{\ell_{k-1}}\right) \left(\frac{r}{\ell_k}\right) = -1$$

a a donc un diviseur premier p différent des p_i tel que $\left(\frac{n}{p}\right) = -1$, ce qui est la contradiction recherchée. □

2 Une reformulation de la réciprocité quadratique

Gauss, Kummer et leurs successeurs ont rapidement souhaité obtenir des lois de réciprocités «supérieures», qui donneraient une condition pour que p soit une puissance n-ième modulo ℓ quand ℓ est une puissance n-ième modulo p. Il s'est avéré que le cadre naturel pour formuler ce problème et les problèmes de réciprocité en général est celui des corps de nombres (les extensions finies de $\mathbf{Q}$).

Pour faire de l'arithmétique dans un corps de nombre K, on a besoin d'un équivalent de $\mathbf{Z}$. Il est fourni par l'ensemble $\mathcal{O}_K$ des entiers de K, qui sont les $x \in K$ tels que le groupe abélien $\mathbf{Z}[x]$ soit de type fini. $\mathcal{O}_K$ est bien un sous-anneau de K : si x et y sont entiers, xy et $x \pm y$ sont dans $\mathbf{Z}[x, y]$ qui est de type fini. Toutefois, il manque en général à cet anneau une propriété essentielle du point de vue de la théorie des nombres : l'unicité de la décomposition en facteurs irréductibles. [4] Pour avoir une bonne théorie de la divisibilité dans K on est donc amené à considérer non plus les entiers eux-mêmes, mais des objets qui étendent la divisibilité des entiers algébriques et pour lesquels il y a bien unicité de la décomposition en facteurs premiers. Un des résultats fondateurs de la théorie algébrique des nombres, pressenti par Kummer et prouvé par Dedekind, est que les idéaux de $\mathcal{O}_K$ peuvent jouer ce rôle. [5] En particulier, les bons équivalents des nombres premiers dans K sont les idéaux premiers (non nuls) de $\mathcal{O}_K$.

Une question naturelle est alors de savoir comment l'arithmétique de $\mathbf{Q}$ se transporte dans celle d'un corps de nombre K, ou plus généralement, comment la divisibilité des idéaux se comporte dans une extension L/K de corps de nombres. La question a bien un sens, puisque $\mathcal{O}_K$ est alors un sous-anneau de $\mathcal{O}_L$, [6] et à tout idéal $\mathfrak{a}$ de $\mathcal{O}_K$ est donc naturellement associé l'idéal $\mathfrak{a}\mathcal{O}_L$ de $\mathcal{O}_L$. Par unicité de la décomposition des idéaux en facteurs premiers, il suffit de regarder comment les idéaux premiers de K se décomposent dans L. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. On peut écrire :

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

où les $\mathfrak{P}_i$ sont des idéaux premiers distincts non nuls de $\mathcal{O}_L$, et les e_i des entiers ≥ 1. On note en outre f_i, pour tout i, le degré de l'extension de corps [7] $\kappa(\mathfrak{P}_\mathrm{i})/\kappa(\mathfrak{p})$, où $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ désigne le corps résiduel en l'idéal $\mathfrak{p}$. On a alors la propriété classique :

$$\sum_{i=1}^{r} e_i f_i = [L : K] = n$$

En particulier, r peut prendre les valeurs de 1 à n. Quand $r = 1$, on dit que $\mathfrak{p}$ ne se décompose pas dans K, et quand à l'inverse $r = n$, on dit que $\mathfrak{p}$ se décompose complètement.

Les lois de réciprocité permettent alors d'aborder le problème suivant : étant donnée une extension L/K de corps de nombres, comment caractériser simplement les idéaux $\mathfrak{p}$ de K se décomposant d'une certaine façon (avec une famille (e_i, f_i) donnée) dans L? En particulier, on voudrait pouvoir expliciter l'ensemble $\mathrm{Spl}(L/K)$ des idéaux de K qui se décomposent complètement dans L. Nous ne

4. Par exemple, pour $K = \mathbf{Q}(\sqrt{-5})$, on a $\mathcal{O}_K = \mathbf{Z}[\sqrt{-5}]$, et dans cet anneau, $(1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$. Or ces entiers algébriques ont respectivement pour norme sur $\mathbf{Q}$ 6, 6, 4 et 9, donc sont irréductibles, puisque $\mathbf{Z}[\sqrt{-5}]$ n'a pas d'élément de norme 2 ou 3.

5. Pour une démonstration de ce résultat ou des autres théorèmes de base de théorie algébrique des nombres utilisés ici, on renvoit à [Sam71] ou au premier chapitre de [Neu99].

6. Mieux : $\mathcal{O}_L$ est l'ensemble des éléments des éléments de L entiers sur $\mathcal{O}_K$, c'est-à-dire engendrant un $\mathcal{O}_K$-module de type fini.

7. Une des bonnes propriétés des anneaux d'entiers est qu'ils sont « de dimension 1 » : tout idéal premier non nul est maximal.

nous intéresserons qu'à la situation où tous les e_i sont égaux à 1 : on montre que c'est le cas pour tous les idéaux premiers de K sauf peut-être pour un nombre fini d'idéaux que l'on dit ramifiés.

Voyons de quelle façon la réciprocité quadratique répond presque complètement à la question pour les extensions quadratiques de $\mathbf{Q}$ (i.e. elle y répond pour tous les nombres premiers sauf un nombre fini).

Proposition 2 *Soit K un corps quadratique, et $a \in \mathbf{Z}$ un entier sans carré tel que $K = \mathbf{Q}(\sqrt{a})$. Alors pour tout nombre premier p ne divisant pas $2a$, (p) est non ramifié dans K. Si $\left(\frac{a}{p}\right) = 1$, alors (p) se décompose complètement dans K, et ne se décompose pas sinon.*

Démonstration. Il est classique que $\mathcal{O}_K = \mathbf{Z}[\omega]$ avec, suivant la valeur de a, $\omega = \sqrt{a}$ ou $\omega = (1+\sqrt{a})/2$. Or dans ce dernier cas, un élément $a + b\omega$ de $\mathcal{O}_K$ qui n'est pas dans $R = \mathbf{Z}[\sqrt{a}]$ est tel que b est impair, et est donc congru à $a + (b+p)\omega \in R$ modulo p. On a donc dans tous les cas :

$$\mathcal{O}_K/p\mathcal{O}_K \cong R/pR \cong \mathbf{Z}[X]/(X^2 - a, p) \cong \mathbf{F}_p[X]/(X^2 - a)$$

Or, si $p\mathcal{O}_K = \mathfrak{P}_1{}^{e_1} \cdots \mathfrak{P}_r{}^{e_r}$, on a, d'après le théorème Chinois :

$$\mathcal{O}_K/p\mathcal{O}_K \cong \bigoplus_{i=1}^{r} \mathcal{O}_K/\mathfrak{P}_i{}^{e_i}$$

L'algèbre $\mathbf{F}_p[X]/(X^2-a)$ étant sans élément nilpotent, (p) est donc non ramifié dans K, et $\mathcal{O}_K/p\mathcal{O}_K$ est la somme de $r = 1$ ou 2 corps qui sont des extensions de $\mathbf{F}_p$. Il en résulte alors que, selon que $X^2 - a$ est ou non irréductible sur $\mathbf{F}_p$, c'est-à-dire selon la valeur de $\left(\frac{a}{p}\right)$, (p) ne se décompose pas ou se décompose complètement dans K. □

Cette proposition donne une description de la décomposition des idéaux qui, prise telle quelle, semble peu satisfaisante : pour déterminer le comportement de chaque nombre premier p, il faudrait évaluer une infinité de symboles de Legendre. Mais c'est là que la réciprocité quadratique intervient. En effet, il s'en déduit immédiatement que $\left(\frac{a}{p}\right)$ ne dépend que de la classe de congruence de p modulo $4a$. En particulier, on peut déterminer $\mathrm{Spl}(K/\mathbf{Q})$ par un nombre fini de calculs :

Proposition 3 $\mathrm{Spl}(\mathbf{Q}(\sqrt{a})/\mathbf{Q})$ *est l'ensemble de tous les nombres premiers contenus dans une certaine réunion de classes non nulles modulo $4a$, auquel il faut éventuellement ajouter des diviseurs premiers de $2a$.*

Une telle description de la décomposition des idéaux premiers est précisément ce que l'on entendra, à la suite de [Wym72], par « loi de réciprocité ».

3 La réciprocité cyclotomique

On a encore une description simple (en termes de « congruences ») de la décomposition des nombres premiers dans les corps cyclotomiques, de la forme $\mathbf{Q}(\zeta_n)$ où ζ_n est une racine primitive n-ième de l'unité. On aura besoin du résultat important suivant :

Proposition 4 *Le polynôme minimal de ζ_n est $\Phi_n = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^\times} (X - \zeta_n^k)$.*

La très belle démonstration suivante est due à Van der Waerden ([CF67] ch. III).

Démonstration. Notons tout d'abord que :

$$\prod_{k|n} \Phi_k = \prod_{r \in \mathbf{Z}/n\mathbf{Z}} (X - \zeta_n^r) = X^n - 1$$

Il en résulte par récurrence sur n que Φ_n est à la fois dans $\mathbf{C}[X]$ et dans $\mathbf{Z}[[X]]$, ce qui montre que c'est un polynôme à coefficients entiers. Il s'agit de montrer qu'il est irréductible. Soit P un facteur irréductible de Φ_n sur $\mathbf{Q}$, unitaire et différent de 1. On veut montrer que $P = \Phi_n$, c'est-à-dire que toutes les racines primitives n-ièmes de l'unité sont racines de P. Pour cela, il suffit de vérifier que si ζ est une racine de P et p un nombre premier ne divisant pas n, alors $P(\zeta^p) = 0$. Supposons le contraire : soit ζ une racine de P et $p \nmid n$ tels que que $P(\zeta^p) \neq 0$. Écrivons alors $\Phi_n = PQ$. ζ^p est racine de Q, donc ζ est racine de $R = Q(X^p)$. Notons que P et Q, et donc R, sont à coefficients entiers. P et R ont une racine commune, donc un pgcd (unitaire, à coefficients entiers) différent

de 1. En particulier, les polynômes $\bar{P}$ et $\bar{R}$ obtenu à partir de P et R par réduction modulo p ne sont pas premiers entre eux. Or $\bar{R} = \bar{Q}(X^p) = \bar{Q}^p$, donc $\bar{P}$ et $\bar{Q}$ ne sont pas premiers entre eux. Il en résulte que $\bar{\Phi}_n = \bar{P}\bar{Q}$ a des racines multiples dans $\mathbf{F}_p[X]$, et il en est donc a fortiori de même pour $X^n - 1$. Or le polynôme dérivé nX^{n-1} n'a certainement aucune racine de $X^n - 1$, d'où la contradiction recherchée. □

Observons alors comment Φ_n se décompose modulo $p \not| n$:

Proposition 5 *Soit p un nombre premier ne divisant pas n, et f l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$. Alors Φ_n est, dans $\mathbf{F}_p[X]$, le produit de polynômes irréductibles distincts $P_1, \ldots, P_r$ tous de degré f.*

Démonstration. On a vu que $X^n - 1$ n'avait pas de racine multiples sur $\mathbf{F}_p$. Par conséquent, Φ_n s'écrit comme un produit de polynômes irréductibles distincts $P_1, \ldots, P_r$ dans $\mathbf{F}_p[X]$, et les racines d'un des P_i dans une extension de $\mathbf{F}_p$ où il est scindé sont des racines primitives n-ième de l'unité. Comme le groupe multiplicatif d'une extension $\mathbf{F}_{p^\nu}$ de $\mathbf{F}_p$ est cyclique d'ordre $p^\nu - 1$, $\mathbf{F}_{p^\nu}$ contient les racines primitives n-ième de l'unité si et seulement si $p^\nu \equiv 1 \pmod{n}$. Les P_i sont donc les polynômes minimaux d'éléments algébriques de $\mathbf{F}_p$ de degré f, d'où le résultat. □

Si l'on admet le résultat selon lequel pour $K = \mathbf{Q}(\zeta_n)$, on a $\mathcal{O}_K = \mathbf{Z}[\zeta_n]$, d'où $\mathcal{O}_K \cong \mathbf{Z}[X]/(\Phi_n)$, on en déduit comme dans le cas des corps quadratiques le corollaire suivant :

Proposition 6 (Réciprocité cyclotomique) *Soit $K = \mathbf{Q}(\zeta_n)$. Pour tout p ne divisant pas n, (p) est non ramifié dans K, et se décompose en idéaux premiers de même degré résiduel f, qui est l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$. En particulier,* $\mathrm{Spl}(K/\mathbf{Q})$ *est l'ensemble des nombres premiers congrus à 1 modulo n.*

4 L'action du groupe de Galois

Dans les deux cas que l'on vient de considérer, on étudiait des extensions galoisiennnes, et leurs groupes de Galois respectifs, $\{\pm 1\}$ et $(\mathbf{Z}/n\mathbf{Z})^*$, sont intervenus dans la loi de réciprocité. On va voir que cette observation est à la base d'une vaste généralisation des résultats précédents. Tout d'abord, voyons de quelle façon, pour une extension galoisienne L/K, le groupe de Galois G opère sur les idéaux. Si A est une partie de L et $\sigma \in G$, on définit σA élément par élément. Alors G laisse stable $\mathcal{O}_L$, et envoie les idéaux premiers sur des idéaux premiers.

Soit $\mathfrak{p}$ un idéal premier non nul de K. Alors tous les idéaux premiers $\mathfrak{P}_i$ de L au-dessus de $\mathfrak{p}$ ont même degré résiduel f et même indice de ramification e. De plus, G opère transitivement sur l'ensemble des $\mathfrak{P}_i$. En particulier, l'ordre du stabilisateur $G_{\mathfrak{P}_i}$ d'un des $\mathfrak{P}_i$ est égal à ef : dans le cas où $\mathfrak{p}$ est non-ramifié, ce groupe caractérise donc la décomposition de $\mathfrak{p}$. Or il se décrit naturellement ([Sam71] 6.2), dans le cas non ramifié, comme le groupe de Galois de l'extension de corps finis $\kappa(\mathfrak{P}_i)/\kappa(\mathfrak{p})$. En particulier, c'est un groupe cyclique, engendré par l'élément $\varphi_{\mathfrak{P}_i}$ de G associé, dans cette identification, à l'automorphisme $x \mapsto x^q$ de $\kappa(\mathfrak{P}_i)$, avec $q = |\kappa(\mathfrak{p})|$.

On aimerait alors pouvoir associer un tel élément φ à $\mathfrak{p}$ plutôt qu'à un idéal premier arbitraire au-dessus de lui. Or, pour $\sigma \in G$, on a $\varphi_{\sigma\mathfrak{P}_i} = \sigma\varphi_{\mathfrak{P}_i}\sigma^{-1}$. Par conséquent, dans le cas particulier où G est *abélien*, cet automorphisme ne dépend pas du choix de $\mathfrak{P}_i$: c'est le *symbole d'Artin* associé à $\mathfrak{p}$. On le note parfois $\left(\frac{L/K}{\mathfrak{p}}\right)$, ou simplement $\sigma_{\mathfrak{p}}$. D'après les observations précédentes, un idéal premier non ramifié $\mathfrak{p}$ se décompose complètement si et seulement si $\sigma_{\mathfrak{p}}$ est l'identité.

On calcule facilement le symbole d'Artin dans les cas déjà évoqués, avec $K = \mathbf{Q}$. Pour $L = \mathbf{Q}(\zeta_n)$ et p un nombre premier non ramifié, on a simplement $\sigma_p : \zeta_n \mapsto \zeta_n^p$. Pour $L = \mathbf{Q}(\sqrt{m})$, on a $\sigma_p = \left(\frac{m}{p}\right)$, en identifiant $\mathrm{Gal}(L/K)$ à $\{\pm 1\}$. On retrouve ainsi des résultats déjà énoncés. On a également une démonstration de la réciprocité quadratique. En effet, soit $L = \mathbf{Q}(\zeta_\ell)$. $\mathrm{Gal}(L/\mathbf{Q}) \cong \mathbf{F}_\ell^*$ a un unique sous-groupe d'indice 2, $H = (F_\ell^*)^2$, donc L a un unique sous-corps quadratique $M = L^H$. Un calcul classique à base de sommes de Gauss montre que $M = \mathbf{Q}(\sqrt{\ell^*})$ avec $\ell^* = (-1)^{(\ell-1)/2}$. Un nombre premier impair $p \neq \ell$ est non ramifié dans L et M, et la restriction à M du Frobenius $\left(\frac{L/\mathbf{Q}}{p}\right)$ est $\left(\frac{M/\mathbf{Q}}{p}\right)$. $\left(\frac{M/\mathbf{Q}}{p}\right)$ est donc l'identité si et seulement s'il est dans H, d'où $\left(\frac{M/\mathbf{Q}}{p}\right) = \left(\frac{p}{\ell}\right)$. Or on vient de voir que $\left(\frac{M/\mathbf{Q}}{p}\right) = \left(\frac{\ell^*}{p}\right)$. D'où le résultat.

5 La réciprocité d'Artin

Les considérations précédentes ont permis à E. Artin de résoudre finalement pour toutes les extensions abéliennes le problème de la décomposition des idéaux premiers. Voyons de quelle façon. Soit $\mathfrak{m}$ un idéal de K. On note $J_K^{\mathfrak{m}}$ le groupe des idéaux fractionnaires premiers à $\mathfrak{m}$, et $P_K^{\mathfrak{m}}$ le sous-groupe des idéaux principaux engendré par les $\alpha \equiv 1 \pmod{\mathfrak{m}}$, qui est d'indice fini. Notons que $J_K^{\mathfrak{m}}$ est le groupe abélien libre engendré par les idéaux premiers ne divisant pas $\mathfrak{m}$, donc si $\mathfrak{m}$ est divisible par les idéaux premiers ramifiés, le symbole d'Artin s'étend à $J_K^{\mathfrak{m}}$ par linéarité. Artin a conjecturé en 1923, et démontré en 1927, le résultat essentiel suivant ([Neu99] VI.7), qui est au centre de la théorie du corps de classe abélien.

Théorème 3 (loi de réciprocité d'Artin) *Soit L/K une extension finie abélienne. Pour un certain idéal $\mathfrak{m}$ de K (un produit des idéaux ramifiés) le morphisme :*

$$\left(\frac{L/K}{}\right) : J_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

est surjectif et son noyau $H^{\mathfrak{m}}$ contient $P_K^{\mathfrak{m}}$ (et on peut l'exprimer explicitement grâce au morphisme norme $N_{L/K}$).

Ce théorème donne, pour toutes les extensions abéliennes, une description en termes de congruences de la décomposition des idéaux premiers non ramifiés. Ainsi, pour $K = \mathbf{Q}$, soit m un générateur de l'idéal $\mathfrak{m}$. On a $J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \cong (\mathbf{Z}/m\mathbf{Z})^*$, donc le groupe $H^{\mathfrak{m}}$, qui est, aux premiers ramifiés près, $\mathrm{Spl}(L/K)$, est donc une réunion de classes de congruences modulo m.

On peut, au passage, se demander dans quel mesure un énoncé aussi abstrait peut se relier aux considérations initiales de Gauss sur les lois de réciprocité supérieures. En fait, le lien existe bien : on peut énoncer une loi de réciprocité analogue à la réciprocité quadratique pour le symbole de Jacobi $\left(\frac{a}{b}\right)_m$ de m-ième puissance. C'est le symbole d'Artin d'une extension de la forme $K(\sqrt[m]{a})/K$, où $K = \mathbf{Q}(\zeta_m)$, et a et b des entiers impairs (b étant assimilé à l'idéal principal qu'il engendre). On renvoit aux exercices 1 et 2 de [CF67] pour les détails.

6 L'horizon non-abélien

Que peut-on dire, en revanche, dans le cas non-abélien ? On peut montrer ([Wym72] §4 pour le cas élémentaire) qu'une description de $\mathrm{Spl}(L/K)$ en termes de congruences est en fait *impossible*. On peut néanmoins formuler certains résultats, comme la forme assez faible suivante du théorème de densité de Čebotarev ([Neu99] VII.13) :

Théorème 4 *Soit L/K une extension finie galoisienne de degré n quelconque. Alors la* densité *de* $\mathrm{Spl}(L/K)$ *est égale à* $1/n$.

En revanche, l'obtention d'une description précise de $\mathrm{Spl}(L/K)$ reste encore aujourd'hui un problème ouvert : on n'a pas démontré, dans le cas général, de « loi de réciprocité non-abélienne ». À quoi une telle loi pourrait-elle ressembler ?

L'expression naturelle de la réciprocité d'Artin est qu'il existe un groupe abélien C_K naturellement associé à K (semblable au groupe des classes $J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ mais bien plus gros) et pour toute extension galoisienne L de K, un morphisme $N_{L/K} : C_L \to C_K$, tel que l'on ait un isomorphisme canonique $\mathrm{Gal}(L/K)^{\mathrm{ab}} \cong C_K/N_{L/K}C_L$. Un analogue non-abélien pourrait être un groupe $\mathfrak{G}_K$ et une famille de morphismes $\mathcal{N}_{L/K}$ tels que l'on ait des isomorphismes $\mathrm{Gal}(L/K) \cong \mathfrak{G}_K/\mathcal{N}_{L/K}\mathfrak{G}_L$. On ne connaît rien de tel.

En revanche, on sait associer certaines fonctions analytiques à des représentations des groupes de Galois des extensions de K, et d'autres fonctions analytiques à des représentations des groupes linéaires $\mathrm{GL}_n(\mathbf{A}_K)$ d'un certain anneau important $\mathbf{A}_K$ associé à K (C_K est par exemple un quotient de $\mathbf{A}_K^\times$). R. P. Langlands, dans les années 60 et 70, a formulé un important faisceau de conjectures concernant ces fonctions analytiques, qui établiraient un lien entre les représentation galoisiennes et les représentations des groupes linéaires. Ce lien fournirait précisément une « loi de réciprocité non-abélienne » (l'introduction du chapitre V de [Koc92] décrit de quelle façon).

On est ainsi toujours en quête, à ce jour, de ce que Gauss et plus tard Hilbert avaient recherché sans peut-être en saisir tout à fait l'ampleur : la loi de réciprocité la plus générale possible.

Références

[CF67] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic Number Theory*. Academic Press, 1967.

[EE86] W. J. Ellison and F. Ellison. Théorie des nombres. In J. Dieudonné, editor, *Abrégé d'histoire des mathématiques, 1700–1900*. Hermann, 1986.

[IR82] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, 1982.

[Koc92] H. Koch. *Algebraic number theory*, volume 62 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, 1992.

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenchaften*. Springer-Verlag, 1999.

[Sam71] P. Samuel. *Théorie algébrique des nombres*. Méthodes. Hermann, 1971.

[Wym72] B. F. Wyman. What is a reciprocity law? *Amer. Math. Monthly*, 79, 1972.