3. Le théorème de densité

Le théorème de densité de Chebotarëv peut être vu comme la moindre généralisation du théorème de Dirichlet sur les nombres premiers dans les progressions arithmétiques (1837) et d'un théorème de Frobenius (1880 ; publié en 1896).

Le théorème de Dirichlet est facile à découvrir expérimentalement. Voici ci-dessous les nombres premiers inférieurs à 100, rangés par dernier chiffre :

$$\begin{array}{ll} 1 & : \ 11, 31, 41, 61, 71 \\ 2 & : \ 2 \\ 3 & : \ 3, 13, 23, 43, 53, 73, 83 \\ 5 & : \ 5 \\ 7 & : \ 7, 17, 37, 47, 67, 97 \\ 9 & : \ 19, 29, 59, 79, 89. \end{array}$$

Il n'est pas surprenant qu'il n'y ait pas de nombre premier se terminant par 0, 4, 6, ou 8, et que seuls deux nombres premiers se terminent par 2 ou 5. La table suggère qu'il y a une infinité de nombres premiers qui se terminent par 1, 3, 7, 9, et que, approximativement, ces classes se maintiennent à niveau. C'est en effet vrai ; c'est le cas particulier avec $m = 10$ du théorème suivant prouvé par Dirichlet (1805-1859) en 1837 (voir [14]). Désignons par $\varphi(m)$ le nombre d'entiers x avec $1 \leq x \leq m$ et $gcd(x, m) = 1$; on a $\varphi(10) = 4$.

Théorème de Dirichlet. *Soit m un entier positif. Alors pour tout entier a avec $gcd(a, m) = 1$, l'ensemble des nombres premiers p avec $p \equiv a \bmod m$ a pour densité $1/\varphi(m)$.*
Ici on dit qu'un ensemble S de nombres premiers a pour *densité* δ si

$$\left(\sum_{p \in S} \frac{1}{p^s}\right) \Big/ \left(\sum_{p \text{ premier}} \frac{1}{p^s}\right) \to \delta \quad \text{pour } s \downarrow 1.$$

Clairement, l'ensemble de tous les nombres premiers a pour densité 1. Des ensembles finis de nombres premiers ont pour densité 0, puisque $\sum_{p \text{ premier}} \frac{1}{p}$ diverge. Ainsi, pour $m = 10$, les nombres premiers "exceptionnels" 2, 5 ne comptent pas du point de vue de la densité, et les autres nombres premiers sont "équidistribués" sur les quatre classes résiduelles 1, 3, 7, 9 modulo 10 au sens où leurs quatre densités sont égales. La formulation initiale de son théorème par Dirichlet ne fait pas intervenir la notion de densité, mais ce qu'on a présenté ci-dessus, c'est ce que sa preuve fournit.

La notion de densité que nous venons de définir est parfois appelée *analytique* ou densité *de Dirichlet*. Il aurait été plus intuitif de dire qu'un ensemble S de nombres premiers a pour densité δ si

$$\frac{\#\{p \leq x \ : \ p \in S\}}{\#\{\{p \leq x \ : \ p \text{ premier}\}} \to \delta$$

Avec ce concept de densité, appelé densité *naturelle*, le théorème de Dirichlet est également valide, mais la preuve, qui est beaucoup plus difficile, a seulement été trouvée par De la Vallée-Poussin

Traduction des pages 9 et suivantes du texte téléchargeable ici https://www.math.leidenuniv.nl/ hwl/papers/cheb.pdf de P. Stevenhagen et H. W. Lenstra Jr. (exposé lors du centenaire de la naissance de Chebotarëv le 15 juin 1994 à Amsterdam).

en 1896 (voir [11]). Si un ensemble de nombres premiers a une densité naturelle alors il a une densité analytique, et les deux densités sont égales ; mais l'inverse est faux. Les résultats ci-dessous ont d'abord été démontrés pour la densité analytique, qui est plus facile à manipuler. Ils sont également valables pour la densité naturelle, mais dans ce cas, les preuves nécessitent des techniques supplémentaires, largement dues à Hecke [20].

Le théorème de Frobenius (1849-1917) que Chebotarëv a généralisé mérite d'être davantage connu qu'il ne l'est. Pour de nombreuses applications du théorème de Chebotarëv, il suffit d'avoir le théorème de Frobenius, qui est à la fois plus ancien (1880) et plus facile à démontrer que le théorème de Chebotarëv (1922).

À nouveau, le théorème de Frobenius peut être découvert empiriquement. Considérons un polynôme f à coefficients entiers, disons $f = X^4 + 3X^2 + 7X + 4$, et supposons qu'on souhaite décider si oui ou non, f est irréductible sur l'anneau $\mathbf{Z}$ des entiers. Une approche standard est de factoriser f modulo plusieurs nombres premiers p. Ainsi, on a

$$f \equiv X \cdot (X^3 + X + 1) \bmod 2,$$

où X et $X^3 + X + 1$ sont irréductibles sur le corps $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ à 2 éléments. On dit que le *type de décomposition* de f modulo 2 est 1, 3. Il découle de cela que si f est réductible sur $\mathbf{Z}$, alors son type de décomposition sera également 1, 3 : un produit d'un facteur linéaire et d'un facteur cubique irréductible. Pourtant, cette dernière alternative est incompatible avec le fait que le type de décomposition modulo 11 est 2, 2 :

$$f \equiv (X^2 + 5X - 1) \cdot (X^2 - 5X - 4) \bmod 11,$$

où les deux facteurs sont irréductibles sur $\mathbf{F}_{11}$. On conclut que f est irréductible sur $\mathbf{Z}$.

L'irréductibilité de f aurait-elle pu être prouvée avec un *unique* nombre premier ? Modulo un tel nombre premier, f devrait être irréductible, avec un type de décomposition égal à l'unique nombre 4. Les librairies actuelles de calcul algébrique informatique rendent faciles de telles expérimentations numériques. Il y a 168 nombres premiers inférieurs à 1000. Deux d'entre eux, $p = 7$ et $p = 19$, sont spéciaux, au sens où f acquiert des facteurs répétés modulo p :

$$f \equiv (X - 3)^2 \cdot (X + 3)^2 \bmod 7,$$
$$f \equiv (X - 3)^3 \cdot (X + 9) \bmod 19.$$

Cela n'arrive pour aucun autre nombre premier, et on trouve les types suivants :

$$\begin{aligned} \text{type } 1,3: &\quad 112 \text{ nombres premiers } (67.5\%). \\ \text{type } 2,2: &\quad 44 \text{ nombres premiers } (26.5\%), \\ \text{type } 1,1,1,1: &\quad 10 \text{ nombres premiers } (6.0\%). \end{aligned}$$

On suggère que les nombres premiers de type 1, 3 ont pour densité $\frac{2}{3}$; que les nombres premiers de 2, 2 ont pour densité $\frac{1}{4}$; qu'aucun nombre premier n'existe qui soit de type 4 ou de type 1, 1, 2 ; et, pour que la somme des densités vaille 1, que les nombres premiers de type 1, 1, 1, 1 ont pour densité $\frac{1}{12}$.

La table suivante montre les résultats d'expérimentations similaires réalisées sur plusieurs polynômes du quatrième degré. Pour chaque polynôme f dans la première colonne, la table donne la densité apparente des nombres premiers p pour lesquels f modulo p a un type de décomposition donné.

f	4	$1,3$	$2,2$	$1,1,2$	$1,1,1,1$
$X^4 - X - 1$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{24}$
$X^4 - X^2 + 1$	0	0	$\frac{3}{4}$	0	$\frac{1}{4}$
$X^4 + X^3 + X^2 + X + 1$	$\frac{1}{2}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$
$X^4 - X^2 - 1$	$\frac{1}{4}$	0	$\frac{3}{8}$	$\frac{1}{4}$	$\frac{1}{8}$
$X^4 + 3X^2 + 7X + 4$	0	$\frac{2}{3}$	$\frac{1}{4}$	0	$\frac{1}{12}$

Le théorème de Frobenius nous dit comment comprendre ces fractions par le *groupe de Galois* du polynôme.

Soit, généralement, f un polynôme à coefficients entiers et de coefficient dominant 1, et notons le degré de f par la lettre n. Supposons que le discriminant $\Delta(f)$ de f ne s'évanouisse pas, de telle façon que f a n zéros distincts $\alpha_1, \alpha_2, \ldots, \alpha_n$ dans une extension de corps adéquate du corps $\mathbf{Q}$ des nombres rationnels. Écrivons K pour le corps engendré par ces zéros : $K = \mathbf{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$. Le groupe de Galois G de f est le groupe des automorphismes de corps de K. Chaque $\sigma \in G$ permute les zéros $\alpha_1, \alpha_2, ..., \alpha_n$ de f, et est complètement déterminé par la façon dont il permute ces zéros. Par conséquent, on peut considérer G comme un sous-groupe du groupe S_n des permutations de n symboles. En écrivant un élément $\sigma \in G$ comme un produit de cycles disjoints (incluant les cycles de longueur 1), et en regardant les longueurs de ces cycles, on obtient le *schéma de cycle de* σ, qui est une partition $n_1, n_2, ..., n_t$ de n.

Si p est un nombre premier ne divisant pas $\Delta(f)$, alors on peut écrire f modulo p comme un produit de facteurs distincts irréductibles sur $\mathbf{F}_p$. Les degrés de ces facteurs irréductibles forment le type de décomposition de f modulo p ; c'est aussi une partition de n. Le théorème de Frobenius affirme, en l'énonçant grossièrement, que le "nombre" de nombres premiers avec un type de décomposition donné est proportionnel au nombre de $\sigma \in G$ avec le même schéma de cycle.

Théorème de Frobenius. *La densité de l'ensemble des nombres premiers p pour lesquels f a un type de décomposition donné $n_1, n_2, ..., n_t$ existe, et elle est égale au produit de $1/\#G$ par le nombre de $\sigma \in G$ avec schéma de cycle $n_1, n_2, ..., n_t$.*

Considérons par exemple, la partition dans laquelle tous les n_i sont égaux à 1. Seule la permutation identité a ce schéma de cycle. Par conséquent, l'ensemble des nombres premiers p pour lesquels f modulo p se décompose complètement en facteurs linéaires a pour densité $1/\#G$. Ainsi, la dernière colonne de la table indique que les groupes de Galois des cinq polynômes dans la table ont pour ordres 24, 4, 4, 8, et 12, respectivement. En fait, ces groupes de Galois sont le groupe complet symétrique S_4, le groupe de Klein V_4, le groupe cyclique C_4, le groupe dihédral D_4 d'ordre 8, et

le groupe alterné A_4. Ceci est une liste complète des groupes transitifs de S_4, de telle façon que tout polynôme irréductible f de degré 4 se comporte comme l'un des cinq polynômes dans la table. Pour f réductible, il y a d'autres possibilités.

Le groupe alterné A_4 contient, en plus de l'élément identité, huit éléments de type 1, 3, et trois éléments de type 2, 2. Cela explique les fractions $\frac{8}{12} = \frac{2}{3}$ et $\frac{3}{12} = \frac{1}{4}$ qu'on a trouvées pour le polynôme $f = X^4 + 3X^2 + 7X + 4$.

Avec un peu de théorie des groupes, on peut déduire quelques jolies conséquences du théorème de Frobenius. Par exemple, si f modulo p a un zéro dans $\mathbf{F}_p$ pour tout nombre premier p, alors f est soit linéaire soit réductible. Aussi, le nombre de facteurs irréductibles de f sur $\mathbf{Z}$ est égal au nombre moyen de zéros de f modulo p dans $\mathbf{F}_p$, moyenné sur tous les p (de manière évidente). Historiquement, la logique allait dans la direction opposée : la dernière assertion a été démontrée par Kronecker en 1880 [23], et elle a formé la base de la preuve de Frobenius ; c'est Frobenius qui a utilisé la théorie des groupes dans son argument, et non Kronecker.

Pour voir une connexion entre les théorèmes de Dirichlet et Frobenius, on considère les polynômes de type $f = X^m - 1$, où m est un entier positif. On a $\Delta(X^m - 1) = (-1)^{m(m-1)/2} m^m$, donc on exclut les nombres premiers divisant m. Pour les nombres premiers restant p, on peut déterminer le type de décomposition de $X^m - 1$ modulo p en appliquant des propriétés élémentaires des corps finis (voir [25, Théorème 2.47]). Avec $m = 12$, on trouve de cette manière que le type de décomposition dépend seulement de la classe résiduelle de p modulo 12, comme suit :

$$\begin{aligned} p \equiv 1 \bmod 12 &: \quad 1,1,1,1,1,1,1,1,1,1,1,1 \\ p \equiv 5 \bmod 12 &: \quad 1,1,1,1,2,2,2,2 \\ p \equiv 7 \bmod 12 &: \quad 1,1,1,1,1,1,2,2,2 \\ p \equiv 11 \bmod 12 &: \quad 1,1,2,2,2,2,2. \end{aligned}$$

Notons que les quatre types de décomposition correspondant aux quatre classes résiduelles premières entre elles sont distincts deux à deux. Par conséquent, le théorème de Frobenius implique le cas particulier $m = 12$ du théorème de Dirichlet. Cela ne marche pas pour tout m. Par exemple, avec $m = 10$ on trouve de la même façon les types de décomposition suivants :

$$\begin{aligned} p \equiv 1 \bmod 10 &: \quad 1,1,1,1,1,1,1,1,1,11 \\ p \equiv 3 \text{ ou } 7 \bmod 10 &: \quad 1,1,4,4 \\ p \equiv 9 \bmod 10 &: \quad 1,1,2,2,2,2. \end{aligned}$$

Le type de décomposition dépend seulement de p modulo 10, mais le théorème de Frobenius ne fait pas de distinction entre les classes résiduelles 3 mod 10 et 7 mod 10. Généralement, le théorème de Frobenius pour $f = X^m - 1$ est impliqué par le théorème de Dirichlet pour le même m, mais non l'inverse.

On peut formuler une version plus étroite du théorème de Frobenius qui pour $f = X^m - 1$ revient au théorème de Dirichlet. Pour cela, on doit répondre à une question qui est suggérée par la connexion entre les types de décompositions et les schémas de cycle. Notamment, est-il possible d'associer d'une façon naturelle à chaque nombre premier p ne divisant pas $\Delta(f)$, un élément $\sigma_p \in G$ tel que le type de décomposition de f modulo p est le même que le type de cycle de σ_p ? La réponse est

presque affirmative : cela peut en effet se faire, excepté que σ_p, appelé traditionnellement la *substitution de Frobenius* de p, est seulement bien définie à conjugaison près dans G. (Les permutations conjuguées ont le même schéma de cycle, donc cela ne devrait pas trop nous ennuyer). Une fois que la substitution de Frobenius a été définie, on peut s'interroger à propos de la densité de l'ensemble des nombres premiers p pour lesquels σ_p est égal à un certain élément de G. Cela amène à la généralisation commune souhaitée des théorèmes de Dirichlet et Frobenius. Cette généralisation a été formulée comme une conjecture par Frobenius, et finalement démontrée par Chebotarëv.

La construction de la substitution de Frobenius est moyennement technique, ce qui est la cause principale de la relative impopularité du théorème de Chebotarëv en dehors de la théorie algébrique des nombres. Dans notre exposé, on prendra pour acquis quelques faits faciles à établir.

Prenons d'abord un nombre premier p fixé, et dénotons par $\overline{\mathbf{F}}_p$ une fermeture algébrique du corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. L'outil fondamental dans la théorie des corps finis est l'*application de Frobenius* $\mathrm{Frob} : \overline{\mathbf{F}}_p \to \overline{\mathbf{F}}_p$, qui est définie par $\mathrm{Frob}(\alpha) = \alpha^p$. Elle respecte clairement la multiplication, et elle respecte, miraculeusement, l'addition également : c'est un *automorphisme de corps* de $\overline{\mathbf{F}}_p$. Il découle de cela que Frob permute les zéros de tout polynôme g qui a ses coefficients dans $\mathbf{F}_p$. La théorie de Galois pour les corps finis amène l'énoncé que le *schéma de cycle de* Frob, *vu comme une permutation des zéros de g est le même que le type de décomposition de g sur* $\mathbf{F}_p$. C'est vrai pour tout polynôme g avec des coefficients dans $\mathbf{F}_p$ qui n'a pas de facteur répété. La preuve se réduit essentiellement au cas où g est irréductible, auquel cas, on applique [25, Théorème 2.14]. Le cas qui nous intéresse est $g = (f \bmod p)$, avec f comme précédemment.

L'application de Frobenius est un automorphisme du corps $\overline{\mathbf{F}}_p$ de caractéristique p, et la substitution de Frobenius σ_p va être un automorphisme du corps K de caractéristique zéro. Pour relier les deux corps, on développe une manière de prendre les éléments de $K = \mathbf{Q}(\alpha_1, ..., \alpha_n)$ modulo p, de telle façon que les "zéros de $(f \bmod p)$" puissent être vus comme les "(zéros de f) mod p".

Par une *place* de K sur p, on désigne une application $\psi : K \to \overline{\mathbf{F}}_p \cup \{\infty\}$ pour laquelle

(i) $\psi^{-1}\overline{\mathbf{F}}_p$ est un sous-anneau de K, et $\psi : \psi^{-1}\overline{\mathbf{F}}_p \to \overline{\mathbf{F}}_p$ est un homomorphisme d'anneaux ;

(ii) $\psi x = \infty$ si et seulement si $\psi(x^{-1}) = 0$, pour tout $x \in K$ non nul.

Notons qu'un nouveau symbole comme ∞ nous est imposé si on tente de prendre des éléments de K modulo p : on veut de manière évidente que $p \bmod p$ soit nul, ce qui amène à $(1/p) \bmod p = 1/0 = \infty$.

Les faits élémentaires à propos des places sont les suivants :

(a) une place de K sur p existe, pour tout nombre premier p ;

(b) si ψ, ψ' sont deux places sur p, alors $\psi' = \psi \circ \tau$ pour un certain $\tau \in G$;

(c) si p ne divise pas $\Delta(f)$, alors l'élément $\tau \in G$ dans (b) est déterminé de manière unique par ψ et ψ'.

Dans la formulation que nous avons choisie, ces faits sont difficiles à trouver dans la littérature. Cela fournit un exercice attrayant pour le lecteur qui ne souhaite pas les prendre pour garantis.

Soit p n'importe quel nombre premier ne divisant pas $\Delta(f)$, et soit ψ une place de K sur p. On voit facilement que $\psi(\alpha_1), \psi(\alpha_2), ..., \psi(\alpha_n)$ sont les zéros de (f mod p) dans $\overline{\mathbf{F}}_p$. En appliquant (b) et (c) à $\psi' = \mathrm{Frob} \circ \psi$ - qui est également une place sur p, avec $\mathrm{Frob}(\infty)=\infty$ - on trouve qu'il y a un unique élément $\mathrm{Frob}_\psi \in G$ pour lequel

$$\psi \circ \mathrm{Frob}_\psi = \mathrm{Frob} \circ \psi$$

Ce sera notre substitution de Frobenius. Comme un élément de G, elle est caractérisée par

$$\psi(\mathrm{Frob}_\psi(x)) = \mathrm{Frob}(\psi(x)) \qquad \text{pour tout} x \in K.$$

Cela montre que Frob_ψ permute $\alpha_1, \alpha_2, ..., \alpha_n$ de la même manière que Frob permute les zéros $\psi(\alpha_1), \psi(\alpha_2)...\psi(\alpha_n)$ de (f mod p). Par conséquent, le schéma de cycle de Frob_ψ est en effet égal au type de décomposition de f modulo p.

La substitution de Frobenius Frob_ψ dépend en général du choix de la place ψ sur p. Par (b), n'importe quelle autre place sur p est de la forme $\psi \circ \tau$, et on vérifie rapidement à partir de la définition que $\mathrm{Frob}_{\psi\circ\tau} = \tau^{-1} \circ \mathrm{Frob}_\psi \circ \tau$; c'est-à-dire, si ψ varie sur les places sur un nombre premier fixé p, alors Frob_ψ couvre une classe de conjugaison dans G. On dénotera un élément typique de cette classe de conjugaison par σ_p ; il est bien défini seulement à conjugaison près, et on l'appelle la *substitution de Frobenius de p.*

Pour illustrer ce qui vient d'être présenté ci-dessus, on considère à nouveau le polynôme $f = X^m - 1$. Dans ce cas, K est un corps *cyclotomique*, obtenu en adjoignant une racine primitive $m^{\text{ième}}$ de l'unité ζ à $\mathbf{Q}$. Le groupe de Galois G a pour ordre $\varphi(m)$, et il est naturellement isomorphe au groupe $(\mathbf{Z}/m\mathbf{Z})^*$ d'unités de l'anneau $\mathbf{Z}/m\mathbf{Z}$; ici, $\tau \in G$ correspond à (a mod m) $\in (\mathbf{Z}/m\mathbf{Z})^*$ si $\tau(\zeta) = \zeta^a$. Soit p un nombre premier ne divisant pas m. Puisque le groupe de Galois est abélien, la substitution de Frobenius σ_p est un élément bien défini de G, pas seulement à conjugaison près. Pour le calculer, soit ψ une place sur p. Alors $\eta = \psi(\zeta)$ est une racine primitive $m^{\text{ième}}$ de l'unité dans $\overline{\mathbf{F}}_p$. Par définition de σ_p, on a $\psi(\sigma_p(x)) = \psi(x)^p$ pour tout $x \in K$. En posant $x = \zeta$, et en faisant que a est tel que $\sigma_p(\zeta) = \zeta^a$, on trouve que $\eta^a = \eta^p$, de telle façon que $a \equiv p \bmod m$. En d'autres termes, *si p est un nombre premier ne divisant pas m, alors la substitution de Frobenius σ_p est l'élément de G qui selon l'isomorphisme $G \simeq (\boldsymbol{Z}/m\boldsymbol{Z})^*$ correspond à* (p mod m).
L'exemple qui vient d'être donné nous permet de reformuler le théorème de Dirichlet comme suit : *si $f = X^m - 1$ pour un certain entier positif m, alors l'ensemble des nombres premiers p pour lesquels σ_p est égal à un élément donné de G a une densité, et cette densité est égale à $1/\#G$;* ainsi la substitution de Frobenius est équidistribuée sur le groupe de Galois si p varie sur tous les nombres premiers ne divisant pas m. Le théorème de Chebotarëv étend cela à tous les f.

Théorème de densité de Chebotarëv. *Soit f un polynôme à coefficients entiers et avec coefficient dominant 1. Supposons que le discriminant $\Delta(f)$ de f ne s'évanouit pas. Soit C une classe de conjugaison du groupe de Galois G de f. Alors l'ensemble des nombres premiers p ne divisant pas $\Delta(f)$ pour lesquels σ_p appartient à C a une densité, et cette densité est égale à $\#C/\#G$.*

À la première inspection, on peut penser que le théorème de Chebotarëv n'est pas beaucoup plus fort que la version de Frobenius. En fait, pour appliquer ce dernier à un polynôme bien choisi (avec le même corps de décomposition que f), on trouve une variante du théorème de densité dans lequel il est nécessaire que C soit un *diviseur* de G plutôt qu'une classe de conjugaison ; ici, deux éléments de G appartiennent au même diviseur si les sous-groupes cycliques qu'ils engendrent sont conjugués dans G. Frobenius lui-même avait déjà reformulé son théorème de cette manière. La partition de G en diviseurs est en général moins facile que sa partition en classes de conjugaison, et le théorème de Frobenius est de façon correspondante plus faible que celui de Chebotarëv. Par exemple, (3 mod 10) et (7 mod 10) appartiennent au même diviseur du groupe $(\mathbf{Z}/10\mathbf{Z})^*$, et c'est pourquoi le théorème de Frobenius ne peut distinguer les nombres premiers appartenant à ces deux classes résiduelles.

On termine cette section avec trois applications élémentaires typiques du théorème de densité de Chebotarëv. Pour les démonstrations, il suffit d'appliquer le théorème aux corps adéquats, de la même façon qu'on obtient le théorème de Dirichlet en regardant les corps cyclotomiques.

La première application est un résultat de la théorie algébrique des nombres : les idéaux premiers de l'anneau des entiers d'un corps de nombres algébriques sont équidistribués sur les classes d'idéaux. La preuve nécessite d'utiliser la notion de *corps de classe de Hilbert*.

La seconde application concerne les formes quadratiques : l'ensemble des nombres premiers p qui peuvent être écrits comme $p = 3x^2 + xy + 4y^2$, avec $x, y \in \mathbf{Z}$, a une densité, qui est égale à $\frac{1}{5}$. Des résultats de cette sorte dépendent des *corps de classe anneau*.

La dernière application concerne la base 10, comme le résultat par lequel nous avons commencé : la densité de l'ensemble des nombres premiers p pour lesquels $\frac{1}{p}$, quand on la développe dans le système décimal, a une longueur de période impaire, existe et est égale à $\frac{1}{3}$ (voir [31]). Cet exemple dépend, de façon assez intéressante, de polynômes en nombre infini, notamment ceux de la forme $f = X^{2^k} - 100$ pour tout $k \geq 2$.

4. Théorie des corps de classes et théorème de Chebotarëv

L'article dans lequel Frobenius a démontré son théorème, et formulé la conjecture qui devait devenir le théorème de densité de Chebotarëv, avait déjà été écrit en 1880. Chebotarëv communiqua les résultats de son article à Stickelberger et Dedekind, mais il différa la publication jusqu'à ce que la théorie des idéaux de Dedekind ait été imprimée. Cela eut lieu en 1894, et l'article de Frobenius sortit en 1896.

La conjecture de Frobenius avait 42 ans lorsque Chebotarëv la prouva en 1922. Durant ces 42 années, la théorie algébrique des nombres s'était développée de plusieurs manières : Dedekind et Kronecker posèrent les fondements de la théorie, Hilbert écrivit son *Zahlbericht*, Weber et Hilbert conçurent les principaux théorèmes de la *théorie des corps de classes*, et, peu de temps après la première guerre mondiale, le mathématicien japonais Takagi fournit les preuves de ces théorèmes (voir [18]).

La théorie des corps de classes décrit toutes les extensions abéliennes d'un corps de nombres algébriques donné. Elle est toujours considérée, plus de 70 ans après, comme une théorie difficile. Ses principaux résultats sont assez naturels, mais les preuves sont longues et fastidieuses ; elles ont un caractère de vérification plutôt qu'elles n'offrent une explication satisfaisante de la raison pour laquelle les résultats sont vrais.

On peut penser que la théorie des corps de classes a fourni à Chebotarëv un outil puissant pour sa preuve. En effet, les traitements dans les livres modernes du théorème de densité de Chebotarëv dépendent invariablement de la théorie des corps de classes (voir par exemple [24, Chapitre VIII, Section 4; 30, Chapitre V, Section 6]). Remarquablement, la preuve originale ne s'en servait pas. En fait, Chebotarëv n'était pas encore familier de la théorie des corps de classes ; il a prouvé son théorème essentiellement à mains nues. Comme on le verra, sa preuve a été plus importante pour la théorie des corps de classes que la théorie des corps de classes ne l'a été pour sa preuve.

L'argument de Chebotarëv était basé sur une nouvelle technique de sa propre invention, qui consistait à "croiser" des extensions abéliennes arbitraires de corps de nombres avec des extensions *cyclotomiques* obtenues en adjoignant une racine de l'unité. En n'utilisant rien de plus que la théorie de Galois de base, Chebotarëv a montré que cette procédure réduisait le cas général de son théorème au cas des extensions cyclotomiques (relatives). Il a traité ce cas au moyen d'un argument assez standard similaire à celui que Dirichlet avait utilisé. Davantage de détails peuvent être trouvés dans le compte-rendu contemporain très clair de Schreier [33] et dans l'appendice au présent article.

Chebotarëv a publié son théorème de densité d'abord en russe en 1923 [4], et ensuite en allemand en 1925 [5]. En 1923 également, Emil Artin publia sa loi de réciprocité [1, phrase 2]. Cette loi est maintenant considérée comme étant le résultat principal de la théorie des corps de classes, même si elle est manquante dans la conception originale de Weber et Hilbert. Artin formula audacieusement sa loi comme un théorème, mais il admit qu'il n'avait pas de démonstration. Il fit remarquer que sa loi de réciprocité impliquait la conjecture de Frobenius [1, section 7]. Le 10 février 1925, Artin écrivit à Hasse [16, p. 23] :

> [Avez-vous lu l'article de Chebotarëv dans les Annalen, vol. 95 ? Je n'ai pas compris l'article et le manque de temps m'a empêché jusque-là de me concentrer suffisamment dessus. S'il est correct, alors on a sûrement les lois de réciprocité générales abéliennes dans la poche. Ici nous différons l'étude de l'article jusqu'au prochain semestre. Peut-être l'avez-vous déjà lu et savez-vous s'il est juste ou faux ?]

L'intuition d'Artin était correcte. Chebotarëv lui-même écrit [7, vol. 3, pp. 155-156] :

> [L'été 1927, quand j'étudiais la théorie des corps de classes, je devins convaincu qu'il était possible de démontrer la loi de réciprocité d'Artin par ma technique consistant à prendre les compositions avec des extensions cyclotomiques. Quand je commençai à voir l'esquisse d'une démonstration, bien qu'encore assez faiblement, nous retournâmes de notre maison de campagne à la ville [Odessa], et là, je vis dans la vitrine de la librairie les Hamburger Abhandlungen avec l'article d'Artin [2]. Mon ennui fut immédiatement tempéré quand je vis qu'Artin mentionnait au début de son article que l'idée basique de sa démonstration, celle de prendre les compositions avec les extensions cyclotomiques était empruntée à mon article [5]. J'ai été très touché de la méticulosité d'Artin en terme d'attribution, dans la mesure où il n'y a qu'une analogie incomplète entre les manières dont la méthode consistant à prendre les compositions avec les extensions cyclotomiques est utilisée dans les deux articles.]

Artin trouva sa démonstration en juillet 1927 (voir [16, pp. 31-32]). Chebotarëv n'était pas loin derrière.

La technique de Chebotarëv est encore un ingrédient crucial de toutes les preuves connues de la loi de réciprocité d'Artin (e. g. [24, Chapitre X, Section 2]). On pense en général que ça marche mais pas pour les bonnes raisons, et que c'est juste aussi contre-intuitif que la plupart des preuves en théorie des corps de classes. À ces reproches, le fantôme de Chebotarëv pourrait répliquer que c'est notre intuition et notre psychologie humaine qui devraient plutôt être remplacées, et non pas son argument parfait et effectif. En effet, Neukirch [30] tisse le stratagème de Chebotarëv si profondément à travers sa présentation de la théorie qu'on peut croire qu'un jour, elle fera partie de notre façon de penser à la loi de réciprocité.

D'un autre côté, la ruse de Chebotarëv a disparu des traitements actuels de son théorème de densité : une fois que la loi de réciprocité est disponible, on peut travailler directement avec les extensions abéliennes, sans le détour par les extensions cyclotomiques. Le lecteur de l'appendice sera d'accord pour penser que cette approche, due à Deuring [12], est très naturelle ; mais elle fait apparaître le théorème de Chebotarëv comme plus difficile qu'il n'est en réalité.

Appendice

On donne une preuve du théorème de Chebotarëv qui suit sa stratégie originale, si ce n'est sa tactique. La référence est [24]. On suppose une familiarité avec les bases de la théorie algébrique des nombres, incluant les propriétés élémentaires des fonctions zeta [VIII.1-3], mais n'incluant pas la théorie des corps de classes.

On démontre une version plus générale du théorème, dans laquelle le corps de base peut être n'importe quel corps de nombres algébriques F plutôt que juste $\mathbf{Q}$. Comme dans le cas $F = \mathbf{Q}$, un ensemble de nombres premiers de F peut avoir une *densité* [VIII.4]. Soit K une extension de Galois finie de F, avec G comme groupe de Galois. Il y a à nouveau, pour tous les nombres premiers $\mathfrak{p}$ de F, sauf un nombre fini d'entre eux, une *substitution de Frobenius* $\sigma_{\mathfrak{p}}$, qui est un élément de G qui est bien définie à conjugaison près.

Théorème de Chebotarëv. *Pour toute classe de conjugaison C de G, la densité $d(K/F, C)$ de*

l'ensemble des nombres premiers $\mathfrak{p}$ *de* F *pour lesquels* $\sigma_{\mathfrak{p}} \in C$ *existe et est égale à* $\#C/\#G$.

La preuve commence avec une réduction au cas abélien. Soit $\sigma \in C$, et appelons $E = \{x \in K : \sigma x = x\}$. Alors K est une extension de Galois de E de groupe $\langle\sigma\rangle$. Un simple argument de comptage, mené dans [VIII.4, preuve du théorème 10], montre que
(*) la conclusion du théorème est vérifiée pour K, F, C si et seulement si elle est vérifiée pour $K, E, \{\sigma\}$.

Notons que le groupe de Galois $\langle\sigma\rangle$ de K sur E est abélien.

Ensuite, on considère le cas où K est cyclotomique sur F, i.e., $K = F(\sigma)$ pour une certaine racine de l'unité ζ. C'est le cas lorsque $F = \mathbf{Q}$ selon le théorème de Dirichlet, et c'est la preuve de ce dernier théorème qu'on imite. En utilisant le fait que la substitution de Frobenius d'un nombre premier $\mathfrak{p}$ dépend seulement de la norme de $\mathfrak{p}$ modulo l'ordre de ζ (cf. [VII.4, Exemple]), on exprime la fonction zeta $\zeta_K(s)$ de K comme un produit adéquat de L-fonctions de F. Alors on regarde l'ordre du pôle en $s = 1$, et on termine la preuve avec un argument traditionnel comme dans [VIII.4, Corollaire du théorème 8].

Une approche pour gérer les extensions abéliennes générales consiste à montrer qu'elles partagent les propriétés essentielles des extensions cyclotomiques qui sont utilisées. Ce n'est pas facile, c'est le sujet de la théorie des corps de classes. Cela amène à la preuve de Deuring du théorème de Chebotarëv [VIII.4, Théorème 10].

La méthode de Chebotarëv n'a pas besoin de la théorie des corps de classes. C'est la suivante. Soit K abélien sur F, de groupe G et de degré n. Soit m n'importe quel nombre premier ne divisant pas le discriminant Δ de K sur $\mathbf{Q}$, et dénotons par ζ une racine primitive $m^{\text{ième}}$ de l'unité. Alors le groupe de Galois H de $F(\zeta)$ sur F est isomorphe à $(\mathbf{Z}/m\mathbf{Z})^*$, et le groupe de Galois de $K(\zeta)$ sur F peut être identifié avec $G \times H$. Si un nombre premier $\mathfrak{p}$ de F a comme substitution de Frobenius (σ, τ) dans $G \times H$, alors il a comme substitution de Frobenius $\sigma \in G$. Par conséquent, en écrivant $d_{\inf}$ pour *une plus faible* densité - définie comme la densité, mais avec lim remplacé par lim inf - on a $d_{\inf}(K/F, \{\sigma\}) \geq \sum_{\tau \in H} d_{\inf}(K(\zeta)/F, \{(\sigma, \tau)\})$. Maintenant fixons $\sigma \in G$ et $\tau \in H$, et supposons que n divise l'ordre de τ. Alors les sous-groupes $\langle(\sigma, \tau)\rangle$ et $G \times \{1\}$ de $G \times H$ ont une intersection triviale. Par conséquent le corps L des invariants de $\langle(\sigma, \tau)\rangle$ satisfait $L(\zeta) = K(\zeta)$, de telle façon que l'extension $L \subset K(\zeta)$ est cyclotomique. Par quoi l'on démontre que dans le cas cyclotomique, la densité $d(K(\zeta)/L, \{(\sigma, \tau)\})$ existe et a la valeur correcte. Ceci est, par (*), alors également vrai pour $d(K(\zeta)/F, \{(\sigma, \tau)\})$, qui par conséquent est égal à $1/(\#G \cdot \#H)$. En sommant sur τ, on obtient $d_{\inf}(K/F, \{\sigma\}) \geq \#H_n/(\#G \cdot \#H)$, où H_n est l'ensemble des $\tau \in H$ d'ordre divisible par n. Maintenant, il est facile de voir que lorsque m parcourt tous les nombres premiers ne divisant pas Δ, la fraction $\#H_n/\#H$ devient arbitrairement proche de 1 (utiliser, par exemple, le théorème de Dirichlet pour choisir $m \equiv 1 \bmod n^k$ pour les grandes valeurs de k). Ainsi, il découle que $d_{\inf}(K/F, \{\sigma\}) \geq 1/\#G$. En appliquant ceci à tous les *autres* éléments du groupe, on trouve que la densité supérieure $d_{\sup}(K/F, \{\sigma\})$ est au plus $1/\#G$. Par conséquent, la densité supérieure et la densité inférieure coïncident, et la densité est égale à $1/\#G$. Ceci complète la preuve du théorème.

Références

1. E. Artin, *Über eine neue Art von L-Reihen*, Abh. Math. Sem. Univ. Hamburg **3** (1923), 89-108 ; Collected papers, 105-124.

2. E. Artin, *Beweis des allgemeinen Reziproziätsgesetzes*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 353-363 ; Collected papers, 131-141.

4. N. G. Chebotaëev, *Opredelenie plotnosti sovokupnosti prostykh chisel, prinadlezhashchikh zadannomu klassu podstanovok (Determination of the density of the set of prime numbers, belonging to a given substitution class)*, Izv. Ross. Akad. Nauk (1923), 205-250 ; Sobranye Sochineni I, 27-65.

5. N. Tschebotareff (= N. G. Chebotarëv), *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehöoren*, Math. Ann. 95 (1925), 191-228.

7. N. G. Chebotarëv, *Sobranye Sochineni (Collected works)*, 3 volumes, Moskva-Leningrad, 1949-1950.

11. Ch. de la Vallée-Poussin, *Recherches analytiques sur la théorie des nombres premiers. Deuxième partie: Les fonctions de Dirichlet et les nombres premiers de la forme linéaire* $Mx + N$, Ann. Soc. Sci. Bruxelles **20** (1896), 281-362.

12. M. Deuring, *Über den Tschebotareffschen Dichtigkeitssatz*, Math. Ann. **110** (1935), 414-415.

14. G. Lejeune Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abhandlungen der Königlichen Akademie der Wissenschaften zu Berlin, mathematische Abhandlungen (1837), 45-71 ; Werke I, 313-342.

16. G. Frei, *Die Briefe von E. Artin an H. Hasse (1923-1953)*, Collection Mathématique, Département de Mathématiques, Université Laval, Québec, 1981.

18. H. Hasse, *History of class field theory*, pp. 266-279 in: J. W. S. Cassels, A. Fröhlich (eds), *Algebraic number theory, Proceedings of an instructional conference*, Academic Press, London, 1967.

20. E. Hecke, *Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. (1917), 299-318 ; Mathematische Werke, 178-197.

23. L. Kronecker, *Über die Irreductibilität von Gleichungen*, Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin (1880), 155-162 ; Werke II, 83-93.

24. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.

25. R. Lidl, H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, Mass., 1983.

30. J. Neukirch, *Class field theory*, Springer-Verlag, Berlin, 1986.

31. R. W. K. Odoni, *A conjecture of Krishnamurthy on decimal periods and some allied problems*, J. Number Theory 13 (1981), 303-319.

33. O. Schreier, *Über eine Arbeit von Herrn Tschebotareff*, Abh. Math. Semin. Univ. Hamburg **5** (1927), 1-6.