XII
Applications et versions effectives du théorème de Chebotarev

1. Caractérisation de corps de nombres par les critères locaux

Soit K un corps de nombres. Si E et F sont deux sous-ensembles de premiers non nuls de K, on pose $E\tilde{\subset}F$ si $F - E$ est fini (*presque inclusion*).

Soit $L|K$ une extension finie. Notons $\mathcal{P}(L/K)$ l'ensemble des premiers de K non ramifiés dans L qui sont au-dessous d'un premier de L de degré résiduel égal à 1. En particulier, si l'extension $L|K$ est galoisienne, $\mathcal{P}(L/K)$ est l'ensemble des premiers de K totalement décomposés dans L. Il est utile de garder à l'esprit le critère suivant.

Proposition 1. — *Soit $M|K$ une clôture galoisienne de l'extension $L|K$. Un premier de K non ramifié dans M est totalement décomposé dans L si et seulement si il est totalement décomposé dans M.*

Démonstration. — Il suffit de montrer qu'un idéal premier $\mathcal{Q}$ de K non ramifié est totalement décomposé dans L est totalement décomposé dans M. Dire que $M|K$ est une clôture galoisienne signifie que M est minimal parmi les extensions galoisiennes de M qui contiennent L, ou encore que le seul sous-groupe normal de G contenu dans H est trivial. Soit H' le sous-groupe de G engendré par les groupes de décomposition en les idéaux premiers de M au dessus de $\mathcal{Q}$. C'est un sous-groupe normal puisque l'ensemble des sous-groupes de décomposition est stable par conjugaison. On a donc $H' = 1$ et tout sous-groupe de décomposition de $\mathrm{Gal}(M/K)$ est trivial. Il en résulte que $\mathcal{Q}$ est totalement décomposé dans M.

En général, on peut décrire $\mathcal{P}(L/K)$ ainsi.

Proposition 2. — *Soit $M|K$ une extension galoisienne finie contenant L. Posons $G = \mathrm{Gal}(N/K)$ et $H = \mathrm{Gal}(N/L)$. On a la réunion disjointe*

$$\mathcal{P}(L/K) = \sqcup_{<\sigma>\cap H\neq\emptyset} P_{N/K}(\sigma),$$

où σ parcourt les élément de G et $< \sigma >$ est la classe de conjugaison de σ dans G.

Démonstration. — Un premier $\mathcal{Q}$ de K non ramifié dans L appartient à $\mathcal{P}(L/K)$ si et seulement si il existe $\mathcal{P}$ premier de L au dessus de $\mathcal{Q}$ tel que la substitution de Frobenius en $\mathcal{P}$ soit triviale dans le groupe de Galois résiduel en $\mathcal{P}$. C'est le cas si et seulement si il existe $\mathcal{R}$ premier de M au dessus de $\mathcal{Q}$ tel que la substitution de Frobenius en $\mathcal{R}$

soit dans H. Cela revient encore à dire que la classe de conjugaison de la substitution de Frobenius en $\mathcal{R}$ rencontre H ou encore que $\mathcal{P} \in P_{N/K}(\sigma)$ pour un élément σ de G tel que $< \sigma > \cap H \neq \emptyset$.

Proposition 3. — *Notons d le degré de l'extension $L|K$. Alors l'ensemble $\mathcal{P}(L/K)$ a densité $\geq 1/n$. Par ailleurs, on a $d(\mathcal{P}(L/K)) \geq 1/n$ si et seulement si l'extension $L|K$ est galoisienne.*

Démonstration. — Soit $M|K$ une extension galoisienne finie contenant L. Posons encore $G = \mathrm{Gal}(N/K)$ et $H = \mathrm{Gal}(N/L)$. D'après la proposition 2, l'ensemble $\mathcal{P}(L/K)$ s'écrit comme une réunion disjointe. On a donc, en reprenant les notations de la proposition 2,

$$d(\mathcal{P}(L/K)) = \sum_{<\sigma>\cap H\neq\emptyset} P_{N/K}(\sigma)\frac{|<\sigma|}{|G|} = \frac{|\sqcup_{<\sigma>\cap H\neq\emptyset} < \sigma > |}{|G|}.$$

On a l'inclusion tautologique $H \subset \sqcup_{<\sigma>\cap H\neq\emptyset} < \sigma >$. Il en résulte que $d(\mathcal{P}(L/K)) \geq |H|/|G| = 1/n$.

L'extension $L|K$ est galoisienne si et seulement si H est un sous-groupe normal de G. Cela se traduit par le fait $< \sigma > \subset H$ si et seulement si $< \sigma > \cap H \neq \emptyset$. C'est le cas si et seulement si on a l'égalité $H \sqcup_{<\sigma>\cap H\neq\emptyset} < \sigma >$. Cette dernière égalité équivaut au fait que $d(\mathcal{P}(L/K)) = |H|/|G|$.

Corollaire 1. — *Si presque tous les premiers de K sont totalement décomposés dans l'extension $L|K$, on a $L = K$.*

Démonstration. — On considère une clôture galoisienne M de $L|K$. On utilise la proposition 1 si bien que

$$1 = d(\mathcal{P}(M/K)) = d(\mathcal{P}(L/K)) = 1/m,$$

où m est le degré de l'extension $M|K$, si bien que $m = 1$ et qu'on a l'égalité $M = L = K$.

Corollaire 2. — *L'extension $L|K$ est galoisienne si et seulement si tout idéal de $\mathcal{P}(L/K)$ est totalement décomposé dans L.*

Démonstration. — Il suffit de montrer que si tout idéal de $\mathcal{P}(L/K)$ est totalement décomposé dans L, l'extension $L|K$ est galoisienne. Considérons une clôture galoisienne $M|K$ de l'extension $L|K$. Notons m son degré. L'ensemble $\mathcal{P}(M/K)$ coïncide avec les premiers de K totalement décomposés dans L d'après la proposition 1. On a donc $\mathcal{P}(M/K) = \mathcal{P}(L/K)$ et donc

$$1/m = d(\mathcal{P}(M/K)) = d(\mathcal{P}(L/K)) \geq 1/d.$$

Comme $d \leq m$ on a $d = m$ et donc $M = L$.

Proposition 4. — *Supposons $L|K$ galoisienne. Soit $L'|K$ une extension finie telle qu'il existe un corps M contenant L et L'. On a $\mathcal{P}(L'/K)\tilde{\subset}\mathcal{P}(L/K)$ si et seulement si on a $L \subset L'$.*

Démonstration. — Il suffit de montrer que si on a $\mathcal{P}(L'/K)\tilde{\subset}\mathcal{P}(L/K)$, alors on a $L \subset L'$. On peut supposer que l'extension $M|K$ est galoisienne. Posons $G = \mathrm{Gal}(M/K)$, $H = \mathrm{Gal}(M/L)$ et $H' = \mathrm{Gal}(M/L')$. Il suffit de montrer que H' est contenu dans H. Utilisons l'hypothèse et la proposition 2. On a

$$\mathcal{P}(L'/K) = \sqcup_{<\sigma>\cap H' \neq \emptyset} P_{N/K}(\sigma) \tilde{\subset} \mathcal{P}(L/K) = \sqcup_{<\sigma>\cap H \neq \emptyset} P_{N/K}(\sigma).$$

Soit $\sigma \in H'$. D'après le théorème de Chebotarev, il existe un premier $\mathcal{R}$ de M tel que $\mathcal{R} \in P_{M/K}(\eta)$ où $\eta \in G$ est tel que $\eta \cap H \neq \emptyset$. Dans ce cas σ et η sont conjugués dans G. Comme H est un sous-groupe normal de G, la classe de conjugaison de σ est contenue dans H. Ainsi on a $\sigma \in H$ et $H' \subset H$.

Théorème 1. — *Une extension galoisienne $L|K$ est déterminée à isomorphisme près par l'ensemble $\mathcal{P}(L/K)$ des premiers de K totalement décomposés dans L.*
Démonstration. — En effet, soit $L'|K$ une extension galoisienne telle que $\mathcal{P}(L/K) = \mathcal{P}(L'/K)$. On peut plonger L et L' dans un corps commun M. On applique alors la proposition 4, qui entraîne que les images de L et L' dans M sont égales. Ainsi, L et L' sont isomorphes.

Corollaire 1. — *Soient L_1 et L_2 deux extensions finies de K telles que $\mathcal{P}(L_1/K)$ et $\mathcal{P}(L_2/K)$ ne diffèrent que par un nombre fini d'éléments. Alors les clôtures galoisiennes de L_1 et L_2 sont isomorphes.*
Démonstration. — Soient M_1 et M_2 les clôtures galoisiennes de L_1 et L_2. Les ensembles $\mathcal{P}(M_1/K) = \mathcal{P}(L_1/K)$ et $\mathcal{P}(M_2/K) = \mathcal{P}(L_2/K)$ ne diffèrent que par un nombre fini d'éléments. Donc M_1 et M_2 sont isomorphes.

Remarque . — 1) Un tel énoncé est faux si on remplace la notion de totalement décomposé par inerte. Il existe des extensions $L|K$ sans premiers de K inerte dans L. Le théorème de Chebotarev, qui repose sur la notion de densité de Dirichlet, s'intéresse en premier lieu aux premiers qui sont décomposés.

2) Le théorème 1 soulève la question de caractériser les ensembles $\mathcal{P}(L/K)$ en termes purement de K. La théorie du corps de classe fournit une réponse lorsque l'extension $L|K$ est abélienne. Par exemple, lorsque $K = \mathbf{Q}$, le corps L est contenu dans un corps cyclotomique, engendré, disons, par les racines m-èmes de l'unité. L'ensemble $\mathcal{P}(L/K)$ est alors l'ensemble des nombres premiers satisfaisant certaines congruences modulo m. En particulier si L est le corps cyclotomique engendré par les racines m-èmes de l'unité, $\mathcal{P}(L/K)$ est constitué des nombres premiers congrus à 1 modulo m.

Théorème 2. — *Notons H le corps de classe de Hilbert de K. La densité de l'ensemble des premiers de K totalement décomposés dans H est égale à $1/h_K$, où h_K est le nombre de classe de K.*
Démonstration. — On sait que cette densité est l'inverse du degré de $H|K$. Mais ce degré est égal à h_K par la théorie du corps de classe.

Remarque . — Il existe des versions du théorème 2 pour toute extension abélienne en terme de groupe de classe de rayon.

2. Versions effectives du théorème de Chebotarev

Il n'y aura pas de démonstration dans cette section. Pour x nombre réel ≥ 2, on pose

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}.$$

Cette fonction intervient dans le théorème des nombres premiers, puisqu'elle constitue un équivalent au nombre de nombre premier $\leq x$. Il en existe une généralisation au corps de nombres K. C'est le *théorème des idéaux premiers* de Landau.

THÉORÈME 3. — *Soit x un nombre réels > 0. Le nombre d'idéaux premiers de $\mathcal{O}_K$ de norme absolue $< x$ est égal à*

$$\mathrm{Li}(x) + \rho(x),$$

où $\rho(x)$ est tel qu'il existe des nombres réels A_K et B_K ne dépendant que de K avec

$$|\rho(x)| \leq A_K x e^{-B_K\sqrt{\log(x)}}.$$

La question du terme d'erreur dans cette estimation est cruciale. Rappelons que la *bande critique* pour la fonction ζ_K est $\{s \in \mathbf{C}/0 < \Re(s) < 1\}$ et que la droite critique est $\{s \in \mathbf{C}/\Re(s) = 1/2\}$. L'*hypothèse de Riemann généralisée* (ou *hypothèse de Riemann étendue*, selon les auteurs) pour la fonction ζ de Dedekind ζ_K affirme que les seuls zéros de ζ_K dans la bande critique sont sur la droite critique. Admettre l'hypothèse de Riemann généralisée permet d'améliorer le théorème de Landau avec l'estimation, pour tout réel $\epsilon > 0$,

$$|\rho(x)| \leq C_{K,\epsilon} x^{1/2+\epsilon},$$

où $C_{K,\epsilon}$ est une constante qui ne dépend que de K et ϵ.

Soit $L|K$ une extension galoisienne de corps de nombres. Soit $\sigma \in \mathrm{Gal}(L/K)$. Soit X un nombre réel > 0. Les versions effectives du théorème de Chebotarev visent à répondre à la question suivante.

Existe-t-il un premier $\mathcal{P}$ de L au dessus d'un premier $\mathcal{Q}$ de K tel que la classe de conjugaison d'une substitution de Frobenius en $\mathcal{P}$ soit égale à σ avec $|\mathcal{Q}| < X$?

On dispose de réponses à cette question qui dépendent de l'hypothèse de Riemann généralisée. Une réponse typique est due à Oesterlé.

THÉORÈME 4. — *Supposons l'hypothèse de Riemann généralisée pour ζ_L. Soit C une classe de conjugaison de $G = \mathrm{Gal}(L/K)$. Notons $\pi_C(x)$ le nombre d'idéaux de K non ramifiés dans L, de norme absolue $\leq x$ et pour lesquels la classe de conjugaison du Frobenius dans G est égale à C. On a alors, pour tout réel $x \geq 2$,*

$$|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)| \leq \frac{|C|}{|G|}\sqrt{x}[(\log(|\mathcal{D}_L|)(1/\pi + 5,3/\log(x)) + [L:\mathbf{Q}](\log(x)^2/(2\pi) + 2)].$$

On en déduit que, si $L \neq \mathbf{Q}$ et si $x \geq 70 \log(|\mathcal{D}_L|)^2$, on a $\pi_C(x) \geq 1$.

Il existe des versions effectives du théorème de Chebotarev sans admettre l'hypothèse de Riemann généralisée. Toutefois les évaluations obtenues sont considérablement moins précises, si bien que les bornes sur x pour $\pi_C(x) \neq \emptyset$ sont d'un intérêt quantitatif moindre. C'est par exemple le cas pour le problème suivant.

3. La conjecture d'Artin sur les racines primitives

Soit a un entier qui n'est ni nul, ni une unité, ni un carré parfait. Notons $P(a)$ l'ensemble formé par les nombres premiers p tels que a engendre $(\mathbf{Z}/p\mathbf{Z})^\times$ (on dit alors que a est une *racine primitive modulo* p). La conjecture d'Artin (sur les racines primitives) affirme que l'ensemble $P(a)$ est infini. (Attention : il existe d'autres conjectures portant le nom d'Artin.)

Ce n'est connu pour aucun entier a. Toutefois Gupta et R. Murty ont montré que $P(a)$ est infini pour une infinité de a. Mieux, Heath-Brown a montré que l'ensemble des nombres premiers q tels que $P(q)$ est fini contient au plus deux éléments, et que l'ensemble des nombres entier $m > 1$ sans facteur carré tels que $P(m)$ est fini contient au plus trois éléments. Mais notre propos est ici d'indiquer le lien entre le problème d'Artin et le théorème de Chebotarev.

Proposition 5. — *L'entier a est une racine primitive modulo p si et seulement si $a^{(p-1)/k} \not\equiv 1 \pmod p$ pour tout nombre premier k divisant $p-1$.*
Démonstration. — Cela résulte du fait que le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $p-1$.

Soit k un entier ≥ 1 sans facteur carré. Soit K un corps de décomposition du polynôme $X^k - a$. Il est égal à $\mathbf{Q}(\zeta, b)$ où ζ est une racine primitive k-ème de l'unité et b une racine k-ème de a. Si a n'est pas une puissance parfaite d'ordre premier à p, l'extension $K|\mathbf{Q}$ est galoisienne de degré $\phi(k)k$, en particulier de degré $k(k-1)$ si k est premier.

Proposition 6. — *Soit p un nombre premier. Il est totalement décomposé dans K si et seulement si on a simultanément $p \equiv 1 \pmod k$ et $a^{(p-1)/k} \equiv 1 \pmod p$.*
Démonstration. — Si p est totalement décomposé dans K, le polynôme $X^k - a$ est scindé sur le corps fini $\mathbf{F}_p$ si bien que 1 et a admettent des racines k-èmes dans $\mathbf{F}_p$, ce qui revient à dire que $p \equiv 1 \pmod k$ et $a^{(p-1)/k} \equiv 1 \pmod p$. Réciproquement, si $p \equiv 1 \pmod k$ et $a^{(p-1)/k} \equiv 1 \pmod p$, le polynôme $X^k - a$ est scindé sur le corps fini $\mathbf{F}_p$ si bien que p est totalement décomposé dans K.

Corollaire 1. — *Soit $P_k(a)$ l'ensemble des nombres premiers p tels que $p \equiv 1 \pmod k$ et $a^{(p-1)/k} \equiv 1 \pmod p$. Cet ensemble a pour densité de Dirichlet $1/[K : \mathbf{Q}]$, et est donc infini.*
Démonstration. — On applique le théorème de Chebotarev au corps K.

Rappelons que la fonction de Moebius $\mu : \mathbf{N} \to \{-1, 0, 1\}$ est donnée par $\mu(x) = 0$ si x a des facteurs carrés et, si x n'a pas de facteur carré, $\mu(x) = (-1)^{\sigma(x)}$, où $\sigma(x)$ est le nombre de diviseurs premiers de x. À partir de ces considérations, Hooley a démontré le résultat suivant, qui indique quel devrait être la forme quantitative de la conjecture d'Artin.

THÉORÈME 5. — *Supposons que l'hypothèse de Riemann généralisée pour ζ_K soit valide. L'ensemble $P(a)$ a pour densité naturelle $d(a)$ (et donc de Dirichlet)*

$$d(a) = \sum_{k=1}^{\infty} \frac{\mu(k)}{[K : \mathbf{Q}]},$$

et est donc infini. La densité $d(a)$ est donnée ainsi. Notons $|\mathcal{D}_a|$ le discriminant absolu du corps quadratique $\mathbf{Q}(\sqrt{a})$. Soit h l'entier ≥ 1 maximal tel qu'il existe $a_0 \in \mathbf{N}$ avec $a = a_0^h$. Posons

$$A(h) = \prod_{q \nmid h}(1 - \frac{1}{q(q-1)}) \prod_{q|h}(1 - \frac{1}{q-1}),$$

où q parcourt les nombres premiers ne divisant pas h dans le premier facteur, et les nombres premiers divisant h dans le deuxième facteur. On a alors

$$d(a) = A(h)$$

si $|\mathcal{D}_a| \equiv 0 \pmod 4$ et

$$d(a) = A(h)(1 - \mu(|\mathcal{D}_a|)) \prod_{q | |\mathcal{D}_a|, q|h} \frac{1}{q-2} \prod_{q | |\mathcal{D}_a|, q \nmid h} \frac{1}{q^2 - q - 1},$$

où q parcourt les nombres premiers, si $|\mathcal{D}_a| \equiv 1 \pmod 4$.

Comme $h = 1$ dans de nombreux cas, par exemple si a est sans facteur carré, notons la quantité

$$A(1) = \prod_{q}(1 - \frac{1}{q(q-1)}) = 0,37...,$$

où q parcourt les nombres premiers. C'est la *constante d'Artin.*