XI
Le théorème de densité de Chebotarev

1. Densité d'idéaux premiers

Soit K un corps de nombres. Soit E un ensemble d'idéaux premiers de K. La limite, si elle existe, de quotients de séries de Dirichlet

$$\lim_{s\longrightarrow 1^+} \frac{\sum_{\mathcal{P}\in E} 1/|\mathcal{P}|^s}{\sum_{\mathcal{P}} 1/|\mathcal{P}|^s}$$

s'appelle la *densité de Dirichlet* de E. Un ensemble fini est de densité de Dirichlet nulle. Cette notion de densité de Dirichlet s'avère plus utile que (et en un certain sens généralise) la notion intuitive de *densité naturelle*, *i.e.* la limite, si elle existe,

$$\lim_{x\longrightarrow\infty} \frac{|\{\mathcal{P}\in E/|\mathcal{P}|\leq x\}|}{|\{\mathcal{P}/|\mathcal{P}|\leq x\}|}.$$

Proposition 1. — *La densité analytique de E, si elle existe, est donnée par la formule*

$$d(E) = \lim_{s\longrightarrow 1^+} \frac{\sum_{\mathcal{P}\in E} 1/|\mathcal{P}|^s}{\log(\frac{1}{s-1})}.$$

Démonstration. — On a, avec $\mathcal{P}$ parcourant les idéaux premiers de K,

$$\log(\zeta_K(s)) = \sum_{n=1}^{\infty}\sum_{\mathcal{P}} \frac{1}{n|\mathcal{P}|^{ns}} = \sum_{\mathcal{P}} \frac{1}{|\mathcal{P}|^s} + \sum_{n=2}^{\infty}\sum_{\mathcal{P}} \frac{1}{n|\mathcal{P}|^{ns}}.$$

Le deuxième terme du dernier membre est analytique en $s=1$; seul le premier terme compte pour définir les densités de Dirichlet.

Pour $\mathcal{P}$ idéal premier de K, notons $f_{\mathcal{P}}$ le degré résiduel absolu de K en $\mathcal{P}$. On a donc la formule asymptotique en $s=1^+$

$$\log(\zeta_K(s)) \simeq \sum_{\mathcal{P}} \frac{1}{|\mathcal{P}|^s} \simeq \sum_{\mathcal{P}, f_{\mathcal{P}}=1} \frac{1}{|\mathcal{P}|^s},$$

car la fonction

$$\sum_{\mathcal{P}, f_{\mathcal{P}} \geq 2} \frac{1}{|\mathcal{P}|^s}$$

est analytique, puisqu'on a $|\mathcal{P}| = p^{f_{\mathcal{P}}}$. Rappelons qu'on a en 1^+ (en considérant le logarithme de $\zeta(s)$)

$$\log(\frac{1}{s-1}) \simeq \sum_p \frac{1}{p^s}.$$

Cela prouve le résultat.

Soit F le sous-ensemble de E constitué par les idéaux premiers $\mathcal{P}$ de degré résiduel égal à 1 (*i.e.* résiduellement triviaux) dans l'extension $K|\mathbf{Q}$.

PROPOSITION 2. — *La densité de Dirichlet de E coïncide avec celle de F.*
Démonstration. — Notons d le degré de l'extension $K|\mathbf{Q}$. La série $\sum_{\mathcal{P} \in E-F} 1/|\mathcal{P}|^s$ est dominée par $d \sum_p 1/p^{2s}$ puisqu'il y a au plus d idéaux premiers de K dessus d'un nombre premier p, et que tout élément de $E - F$ est de degré résiduel ≥ 2. Or la série $d \sum_p 1/p^{2s}$ converge absolument pour s de partie réelle $> 1/2$.

Nous utiliserons souvent cette observation dans ce qui suit.

2. Énoncé du théorème de Chebotarev

Soit $L|K$ une extension galoisienne finie de corps de nombres. Soit $\mathcal{P}$ un idéal premier de L au-dessus d'un idéal premier $\mathcal{Q}$ de K non ramifié dans l'extension $L|K$. La substitution de Frobenius en $\mathcal{P}$ ne dépend que de $\mathcal{Q}$ à conjugaison près dans $\mathrm{Gal}(L/K)$.

Soit C une classe de conjugaison de $\mathrm{Gal}(L/K)$. Le théorème de Chebotarev affirme que les substitution de Frobenius sont également réparties dans les classes de conjugaisons. Notons P_C l'ensemble des idéaux premiers de K tels que la classe de conjugaison de la substitution de Frobenius en $\mathcal{P}$ soit égale à C.

THÉORÈME 1. — *La densité de Dirichlet de P_C existe et vaut*

$$d(P_C) = \frac{|C|}{|\mathrm{Gal}(L/K)|}.$$

En particulier, P_C est non-vide.

Remarque . — 0) Lorsque $K = \mathbf{Q}$ et $L = \mathbf{Q}(\zeta)$, où ζ est une racine primitive n-ème de l'unité, on identifie $\mathrm{Gal}(L/K)$ à $(\mathbf{Z}/n\mathbf{Z})^\times$ par l'inverse de $i \mapsto (\zeta \mapsto \zeta^i)$. L'image d'une substitution de Frobenius en un nombre premier p ne divisant pas n est la classe de p modulo n. Le théorème de Chebotarev dans ce cas n'est autre que le théorème de la progression arithmétique de Dirichlet.

1) On peut principalement trouver deux démonstration du théorème de Chebotarev dans la littérature. Énonçons d'abord ce qu'elles ont en commun. On se ramène facilement au cas d'une extension cyclique. Dans un cas comme dans l'autre, on généralise la notion de fonction L de Dirichlet aux fonctions L de caractères de groupes de classes de rayon d'idéaux. On utilise la formule du nombre de classes pour donner une formule asymptotique pour le nombre d'idéaux d'un corps de nombres K contenus dans une classes d'idéaux. Ainsi on peut montrer que la fonction ζ de K admet un pôle simple en $s = 1$, et que, par ailleurs, les fonctions L de Dirichlet de caractères ($\neq 1$) de groupes de classes de rayon d'idéaux n'ont ni pôles, ni zéro en $s = 1$. Cela est une extrapolation des arguments classiques qui permettent de démontrer le théorème de Dirichlet.

2) La démonstration originale de Chebotarev utilise seulement le fait que la fonction ζ_K d'un corps de nombre K a un unique pôle, qui est simple, en $s = 1$ et une version étendue du théorème classique de la progression arithmétique. Ce dernier point utilise de la géométrie des nombres (équirépartition des idéaux dans une classe donnée) et est un énoncé sur la répartition des idéaux premiers de K qui sont résiduellement triviaux. Pour démontrer son théorème. Chebotarev bâtit sa démonstration sur ces notions et se ramène de façon astucieuse au cas d'une extension cyclotomique.

3) L'autre démonstration utilise la théorie, très élaborée, du corps de classe : toute fonction L associée au caractère d'un groupe de Galois de corps de nombres coïncide avec une fonction L de Dirichlet généralisée au sens de 1) (ou encore toute extension abélienne d'un corps de nombres est contenue dans un corps de classe de rayon approprié). Ainsi, il suffit de montrer le théorème de Chebotarev pour les extensions correspondant aux corps de classe de rayon. Dans un tel cas, la démonstration est directement modelée sur la démonstration du théorème de la progression artihmétique à l'aide de 1).

4) On ne sait pas démontrer que P_C est non-vide (un énoncé dénué d'analyse) sans utiliser de série de Dirichlet. De nombreuses applications du théorème de Chebotarev utilisent simplement le fait que P_C est non-vide.

5) Une des conséquences faibles du théorème de Chebotarev, qui peut être établie de façon algébrique, sans utiliser de fonction ζ, joue un rôle important pour établir la théorie du corps de classes par voie algébrique. C'est l'énoncé suivant. Soit S un ensemble fini d'idéaux premiers d'un corps de nombres K. Soit $L|K$ une extension abélienne finie. Son groupe de Galois est engendré par les substitutions de Frobenius associées aux nombres premiers en dehors de S.

6) L'énoncé ci-dessus du théorème de Chebotarev n'est pas effectif : il ne donne pas un majorant explicite pour le plus petit élément de P_C. Pour cela, il faut utiliser la seconde démonstration et la combiner avec une certaine version du théorème des nombres premiers.

3. Rappels sur les caractères d'un groupe abélien fini

Soit G un groupe abélien et fini d'ordre n. Un homomorphisme de groupes

$$G \longrightarrow \{z \in \mathbf{C}/|z| = 1\}$$

s'appelle un *caractère* de G.

On note G^* le groupe des caractères de G. Rappelons-en quelques propriétés.

PROPOSITION 3. — *L'ordre de G^* est égal à n. L'homomorphisme de groupes $G \longrightarrow G^{**}$ qui à g associe $\chi \mapsto \chi(g)$ est un isomorphisme.*
Démonstration. — On remarque d'abord que pour tout sous-groupe H de G un caractère χ de H se prolonge en un caractère de G. Cela se démontre par récurrence sur l'indice de H dans G. Si cet indice est égal à 1, c'est évident. Sinon, on fait l'hypothèse de récurrence. Soit $x \in G - H$. Notons H' le sous-groupe de G engendré par x et H. On va construire un caractère χ' sur H' qui prolonge χ ; cela suffira pour conclure par hypothèse de récurrence, puisque l'indice de H' dans G est $<$ à l'indice de H dans G. Soit n le plus petit entier > 1 tel que $x^n \in H$. Posons $t = \chi(x^n)$. Soit $w \in \mathbf{C}^*$ tel que $w^n = t$. Posons, pour $k \in \mathbf{Z}$ et $h \in H$,

$$\chi'(x^k h) = w^k \chi(h).$$

Cela définit un caractère de H' prolongeant χ.

On a une application $G^* \longrightarrow H^*$ induite par la restriction à H dont le noyau est formé par les caractères triviaux sur H. On vient de voir que cette application est surjective. On a donc une suite exacte de groupes abéliens

$$1 \longrightarrow (G/H)^* \longrightarrow G^* \longrightarrow H^* \longrightarrow 1.$$

L'ordre de G^* est donc égal au produit des ordres de H^* et $(G/H)^*$.

Démontrons par récurrence sur n que G et G^* ont même ordre n. Si G est cyclique, ses caractères sont de la forme $g \mapsto \zeta^g$, où ζ est une racine n-ième de l'unité. Comme il y a n racines n-ièmes de l'unité le résultat s'en suit. Si G est non cyclique, il possède un facteur cyclique H non trivial. Les ordres de H^* et $(G/H)^*$ sont égaux aux ordres de H et G/H par hypothèse de récurrence.

On a donc

$$|G| = |H||G/H| = |H^*|(|G/H)^*| = |G^*|.$$

Les groupes G, G^* et G^{**} ont donc même ordre. Pour démontrer que l'application $x \mapsto (\chi \mapsto \chi(x))$ est un isomorphisme, il suffit donc de prouver qu'elle est injective. C'est-à-dire prouver que pour tout $x \in G$ il existe $\chi \in G^*$ tel que $\chi(x) \neq 1$. Un tel caractère existe lorsque G est cyclique. Dans le cas général il suffit pour cela de considérer un prolongement à G d'un caractère χ' du sous-groupe cyclique H de G engendré par x tel que $\chi'(x) \neq 1$. Un tel caractère existe d'après ce qui précède.

On en déduit ce qui est essentiellement les relations d'orthogonalité des caractères de G.

COROLLAIRE . — *On a les deux relations suivantes, pour $\chi \neq 1$*

$$\sum_{g \in G} \chi(g) = 0$$

et pour $g \neq 1$

$$\sum_{\chi \in G^*} \chi(g) = 0.$$

De plus on a $\sum_{\chi\in G^*} 1 = g$ *et* $\sum_{g\in G} 1 = g$.
Démonstration. — Les deux dernières égalités sont évidentes compte-tenu de la proposition 3.

En raison de la dualité établie par la proposition 3, les deux premières égalités sont équivalentes. Démontrons la première. Soit $h \in G$ tel que $\chi(h) \neq 1$. On a

$$\chi(h)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(gh) = \sum_{g\in G}\chi(g).$$

La formule cherchée s'ensuit.

4. Fonctions L de Dirichlet généralisées

Soit K un corps de nombres de degré d sur $\mathbf{Q}$. Soit $\mathcal{M}$ un cycle arithmétique de K (ou encore diviseur d'Arakelov). Soit χ un caractère du groupe des classes de rayon $\mathcal{M}$. On dit dans ce cas que $\mathcal{M}$ est le *niveau* du caractère χ.

Par abus de notation on note $\chi(I)$ pour l'image par χ de la classe d'un idéal I. De plus on pose $\chi(I) = 0$ lorsque I et $\mathcal{M}$ ne sont pas premiers entre eux. La fonction $I \mapsto \chi(I)$ est donc multiplicative.

La *fonction L de Dirichlet* associée à χ est la série de Dirichlet

$$L(\chi, s) = \sum_I \frac{\chi(I)}{|I|^s},$$

où I parcourt les idéaux entiers de K. On peut récrire cette série sous forme de produit eulérien :

$$L(\chi, s) = \prod_{\mathcal{P}} \frac{1}{1 - \chi(\mathcal{P})|\mathcal{P}|^{-s}},$$

en utilisant la multiplicativité de χ et toujours le théorème de factorisation des idéaux. Il est facile de voir que cette série de Dirichlet converge sur D_1 (lemme X-2), puisque ses coefficients sont des nombres complexes de valeur absolue égale à 1.

Proposition 4. — *Si χ est un caractère différent de 1, la fonction $L(\chi, s)$ se prolonge en une fonction holomorphe sur $D_{1-1/d}$.*
Démonstration. — Pour $R \in \mathcal{C}\ell(K)^{\mathcal{M}}$, on considère la fonction

$$\zeta(s, R) = \sum_{I\in R} \frac{1}{|I|^s},$$

où I parcourt les idéaux entiers K. Cette fonction est méromorphe sur $D_{1-1/d}$ (voir la démonstration du théorème X-1). On a

$$L(\chi, s) = \sum_{R\in\mathcal{C}\ell(K)^{\mathcal{M}}} \chi(R)\zeta(s, R).$$

Comme les fonctions $\zeta(s,R)$ n'ont des pôles qu'en 1 et comme les résidus correspondants sont tous égaux (démonstration du théorème X-1), la fonction $L(\chi,s)$ n'a pas de pôle en 1 en raison de la formule $\sum_R \chi(R)=0$.

5. Le théorème de Chebotarev dans le cas des extensions cyclotomiques

Soit K un corps de nombres. Soit m un entier ≥ 1. Notons $K(\zeta)$ l'extension cyclotomique engendrée par une racine m-ème primitive de l'unité ζ. L'extension $K(\zeta)|K$ est abélienne.

PROPOSITION 5. — *Le théorème de Chebotarev est vérifé pour l'extension $K(\zeta)|K$.*
Démonstration. — Le groupe de Galois de $K(\zeta)|K$ s'identifie à un sous-groupe de $(\mathbf{Z}/m\mathbf{Z})^*$ par l'application $\sigma \mapsto i(\sigma)$, avec $\sigma(\zeta)=\zeta^{i(\sigma)}$. Notons H l'image ainsi obtenue de $\mathrm{Gal}(K(\zeta)/K)$ dans $(\mathbf{Z}/m\mathbf{Z})^*$. Notons $\hat{H}$ le groupe des caractères de H. Soit $\chi\in\hat{H}$. Pour $\mathcal{P}$ idéal premier de K, la classe modulo m de $|\mathcal{P}|$ est dans H. Ainsi, $\chi(|\mathcal{P}|)$ est bien défini.

On pose

$$L(\chi,s)=\prod_{\mathcal{P}}(1-\chi(|\mathcal{P}|)|\mathcal{P}|^{-s})$$

où $\mathcal{P}$ parcourt les nombres premiers non ramifiés dans l'extension $K(\zeta)|K$. Lorsque $\chi=1$, on retrouve la fonction ζ_K de Dedekind à un nombre fini de facteurs près.

La fonction $s\mapsto L(\chi,s)$ est une fonction L de Dirichlet généralisée. En effet, considérons l'idéal $m\mathcal{O}_K$ de $\mathcal{O}_K$ et le groupe des classes de rayon $\mathcal{M}=\infty.m\mathcal{O}_K$. On a un morphisme de groupes $\mathcal{C}\ell(K)^{\mathcal{M}}\to(\mathbf{Z}/m\mathbf{Z})^*$ qui à la classe d'un idéal premier $\mathcal{P}$ qui n'est pas dans le support de $\mathcal{M}$ associe la classe de $|\mathcal{P}|$ modulo m.

De plus, on a

$$\zeta^{(m)}_{K(\zeta)}(s)=\prod_{\chi\in\hat{H}}L(\chi,s),$$

où $\zeta^{(m)}_{K(\zeta)}$ est la fonction ζ de K privée des facteurs eulériens en les idéaux premier divisant m. En effet, il suffit de le vérifier pour chaque facteur au dessus d'un idéal premier $\mathcal{P}$ de $\mathcal{O}_K$ qui n'est pas dans le support de $\mathcal{M}$. Il suffit donc de vérifier que

$$\prod_{\mathcal{Q}|\mathcal{P}}(1-|\mathcal{Q}|^{-s})=\prod_{\chi\in\hat{H}}(1-\chi(|\mathcal{P}|)|\mathcal{P}|^{-s}).$$

Le terme de gauche est égal à

$$(1-|\mathcal{P}|^{-fs})^{|H|/f}$$

où f est le degré résiduel en tout $\mathcal{Q}$ divisant $\mathcal{P}$. De plus, la classe de $|\mathcal{P}|$ dans H est d'ordre f. Il reste à montrer que, pour tout élément $h\in H$ d'ordre f, on a l'identité de polynômes :

$$(1-X^f)^{|H|/f}=\prod_{\chi\in\hat{H}}(1-\chi(h)X).$$

C'est le cas, puisque $\chi(h)$ parcourt les racines f-èmes de l'unité avec multiplicité $|H|/f$ lorsque χ parcourt $\hat{H}$.

Notons H' l'image du morphisme $\mathcal{C}\ell(K)^{\mathcal{M}} \to H$. Considérons K' le sous-corps de $K(\zeta)$ fixé par H'. Tout caractère χ de H, trivial sur H', vérifie $L(\chi, s) = \zeta_K(s)$. Comme $\zeta_{K'}(s) = \prod_{\chi\in\hat{H},\chi(H')=1} L(\chi, s)$, on a $\zeta_{K'} = \zeta_K(s)^{|H/H'|}$, cela entraîne $|H/H'| = 1$ et donc $H' = H$, si bien que l'application $\mathcal{C}\ell(K)^{\mathcal{M}} \to H$ est surjective. Pour $\chi \neq 1$, il résulte de la formule du nombre de classes que chaque facteur $L(\chi, s)$ est sans pôle en $s = 1$. Comme $\zeta_{K(\zeta)}$ et ζ_K ont toutes deux des pôles simples en $s = 1$, on a $L(\chi, 1) \neq 0$ pour $\chi \in \hat{H}$, $\chi \neq 1$. Il en résulte que $s \mapsto \log(L(\chi, s))$ admet un prolongement sur demi-plan contenant $s = 1$ et donc que $s \mapsto \sum_{\mathcal{P}} \chi(|\mathcal{P}|)|\mathcal{P}|^{-s}$ converge en $s = 1$.

Pour $h \in H$, et $s \in D_1$, posons $\phi_h(s) = (\sum_{\chi\in\hat{H}} \chi^{-1}(h) \sum_{\mathcal{P}} \chi(|\mathcal{P}|)|\mathcal{P}|^{-s})/|H|$. On a

$$|H|\phi_h(s) = \sum_{\mathcal{P}} |\mathcal{P}|^{-s} + \sum_{\chi\in\hat{H},\chi\neq 1} \chi^{-1}(h) \sum_{\mathcal{P}} \chi(|\mathcal{P}|)|\mathcal{P}|^{-s}),$$

dont le premier terme est équivalent à $-\log(s-1)$ lorsque s tend vers 1 et le second terme est borné. Donc $\phi_h(s)$ est équivalent à $-\log(s-1)/|H|$ lorsque s tend vers 1.

Par ailleurs, on a

$$\phi_h(s) = \frac{1}{|H|} \sum_{\mathcal{P}} \sum_{\chi\in\hat{H}} \chi(|\mathcal{P}|h^{-1})|\mathcal{P}|^{-s} = \frac{1}{|H|} \sum_{\mathcal{P},|\mathcal{P}|\equiv h \pmod m} |\mathcal{P}|^{-s}.$$

On a donc montré que la densité analytique de l'ensemble des idéaux premiers $\mathcal{P}$ de K tel que la substitution de Frobenius en $\mathcal{P}$ est égale à h est $1/|H|$. C'est-à-dire le théorème de Chebotarev pour l'extension $K(\zeta)/K$.

Il en résulte le théorème de la progression arithmétique lorsque $K = \mathbf{Q}$. À l'inverse, le groupe de Galois de $K(\zeta)|K$ s'identifie à un sous-groupe de $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$; pourtant, le théorème précédent ne résulte pas facilement du théorème de la progression arithmétique.

6. La première démonstration du théorème de Chebotarev

Soit E un ensemble d'idéaux premiers de K. On pose

$$d_K^-(E) = \liminf_{s\to 1^+} \frac{\sum_{\mathcal{P}\in E} 1/|\mathcal{P}|^s}{\sum_{\mathcal{P}} 1/|\mathcal{P}|^s}$$

et

$$d_K^+(E) = \limsup_{s\to 1^+} \frac{\sum_{\mathcal{P}\in E} 1/|\mathcal{P}|^s}{\sum_{\mathcal{P}} 1/|\mathcal{P}|^s}.$$

Si ces nombres sont égaux, la densité analytique de E existe et vaut leur valeur commune.

Abordons maintenant le théorème dans le cas des extensions cycliques.

Proposition 6. — *Soit $L|K$ une extension cyclique de corps de nombres. Le théorème de Chebotarev est valide pour $L|K$.*

Démonstration. — Notons G le groupe de Galois de l'extension $L|K$. Notons n son cardinal. Pour tout entier $k \geq 1$, il existe une infinité de nombres premiers congrus à 1 modulo n^k, et donc une infinité de tels nombres premiers ne divisant pas le discriminant absolu de L. Soit q un tel nombre premier (il dépend de k).

Soit ζ une racine primitive q-ème de l'unité. Comme on a q est non ramifié dans L, et est le seul nombre premier ramifié dans l'extension $\mathbf{Q}(\zeta)$, l'extension $L \cap \mathbf{Q}(\zeta)$ est partout non ramifiée. Donc $L \cap \mathbf{Q}(\zeta) = \mathbf{Q}$. Donc l'extension $L(\zeta)|L$ est abélienne et son groupe de Galois s'identifie à $(\mathbf{Z}/q\mathbf{Z})^*$.

Par conséquent, on a un isomorphisme de groupes $\mathrm{Gal}(L(\zeta)/K) \simeq \mathrm{Gal(L/K)} \times \mathrm{Gal}(K(\zeta)/K)$. On identifiera donc $\mathrm{Gal}(L(\zeta)/K)$ à $G \times H$.

Soit $\sigma \in G$. Notons S l'ensemble des idéaux premiers $\mathcal{P}$ de K tels que le Frobenius en $\mathcal{P}$ dans G soit égal à σ. Pour $\tau \in H$, notons S_τ l'ensemble des idéaux premiers $\mathcal{P}$ de K tels que le Frobenius en $\mathcal{P}$ dans $G \times H$ soit égal à (σ, τ). On a $S = \cup_{\tau \in H} S_\tau$ (réunion disjointe) et donc

$$d_K^-(S) \geq \sum_{\tau \in H} d_K^-(S_\tau).$$

Supposons $\tau \in H$ d'ordre divisible par n. Déterminons $d_K(S_\tau)$. Notons $< (\sigma, \tau) >$ le sous-groupe de $G \times H$ engendré par (σ, τ). Posons $F = L(\zeta)^{<(\sigma,\tau)>}$. On a

$$F(\zeta) = F.K(\zeta) = L(\zeta)^{<(\sigma,\tau)>}.L(\zeta)^{G\times 1} = L(\zeta)^{<(\sigma,\tau)> \cap G \times \{1\}}.$$

Comme τ est d'ordre divisible par n, on a $< (\sigma, \tau) > \cap G \times \{1\} = \{(1, 1)\}$. Donc on a $F(\zeta) = L(\zeta)$. L'extension $L(\zeta)|F$ est donc cyclotomique. Considérons l'ensemble des idéaux premiers $\mathcal{P}$ de F tels que Frobenius en $\mathcal{P}$ dans l'extension $L(\zeta)/F$ est égal à (σ, τ). D'après la proposition 5, la densité de ce dernier ensemble est $1/[L(\zeta) : F]$.

Cette densité ne change pas si on se limite aux idéaux premiers de F qui sont résiduellement triviaux sur K. Soit $\mathcal{P}$ un idéal premier premier de F résiduellement trivlal tel que le Frobenius en $\mathcal{P}$ est égal à (σ, τ) dans l'extension $L(\zeta)/F$. Il est au dessus de $\mathcal{Q}$, idéal premier de K qui est dans S_τ. Un idéal premier de K dans S_τ est au-dessous de $[F : K]$ idéaux premiers de F, qui sont nécessairement résiduellement triviaux.

La densité de S_τ est donc $1/([F : K][L(\zeta) : F]) = 1/[L(\zeta) : K] = 1/(|G|.|H|)$. Notons H_n l'ensemble des éléments de H d'ordre divisible par n.

On a alors

$$d_K^-(S) \geq \sum_{\tau \in H_n} d_K^-(S_\tau) = \sum_{\tau \in H_n} d_K(S_\tau) = \frac{|H_n|}{|G|.|H|}.$$

Le groupe H est cyclique d'ordre $q - 1$. Factorisons $q - 1$ et n : $q - 1 = \prod_p p^{a_p}$ et $n = \prod_p p^{b_p}$. Un élément h de H est d'ordre divisible par n si et seulement si il est d'ordre divisible par p^{b_p} pour tout nombre premier p divisant n, ou encore si et seulement si il n'est pas dans $p^{a_p - b_p + 1}H$ pour tout nombre premier p divisant n. Si on décompose H en produit de composantes p-primaires sous la forme $H \simeq \prod_p H_p$, et $h = \prod_p h_p$ (avec $h_p \in H_p$) cela revient à dire que $h_p \in H_p - p^{a_p - b_p + 1}H_p$, pour tout nombre premier p divisant n. Ainsi h

est d'ordre divisible par n si et seulement si $h \in \prod_{p|n}(H_p - p^{a_p - b_p + 1}H_p) \prod_{(p,n)=1} H_p$. Il y a donc $\prod_{p|n}(p^{a_p} - p^{b_p - 1}) = |H| \prod_{p|n}(1 - p^{-1+b_p-a_p})$ éléments dans H_n.

On a donc

$$d_K^-(S) \geq \frac{1}{|G|} \prod_{p|n}(1 - p^{-1-a_p+b_p}),$$

pour tout entier $k \geq 1$ et donc $d_K^-(S) \geq 1/|G|$ en faisant tendre k vers l'infini. En effet, b_p est indpendant de k et a_p tend vers l'infini lorsque k tend vers l'infini (pour p premier divisant n). Pour tout sous-ensemble T de l'ensemble des nombres premiers de K, notons T' le complémentaire de T. On a alors

$$d_K^+(T) \leq 1 - d_K^-(T').$$

Pour chaque $\sigma' \in G$, notons S' l'ensemble des idéaux premiers (non ramifiés dans $L|K$) $\mathcal{P}$ de K tels que le Frobenius en $\mathcal{P}$ dans G soit égal à σ'. Le complémentaire de S dans l'ensemble des idéaux premiers (non ramifés dans $L|K$) de K est $\cup_{\sigma' \neq \sigma} S'$. Ainsi on a

$$d_K^+(S) \leq 1 - \sum_{\sigma' \in G, \sigma' \neq \sigma} d_K^-(S') \leq 1 - (|G| - 1)/|G| = 1/|G| \leq d_K^-(S).$$

On a bien montré $d_K^-(S) = d_K^+(S) = d_K(S) = 1/|G|$.

Cela achève la démonstration de la proposition 6. Passons maintenant à la preuve du théorème 1.

Démonstration. — Soit $\sigma \in C$. Notons E le sous-corps de L fixé par σ. L'extension $L|E$ est cyclique. Notons $P(\sigma)$ l'ensemble des idéaux premier $\mathcal{P}$ de L tels que la substitution de Frobenius en $\mathcal{P}$ de $\mathrm{Gal}(L/K)$ coïncide avec σ.

L'application qui à $\mathcal{P}$ associe $\mathcal{P} \cap E$ définit une bijection entre $P(\sigma)$ et l'ensemble $P'(\sigma)$ formé par les idéaux premiers $\mathcal{Q}'$ de E tels que l'extension $E|K$ soit résiduellement triviale en $\mathcal{Q}'$ et tels que la substitution de Frobenius en tout idéal de L au-dessus de $\mathcal{Q}'$ soit égale à σ. L'extension $E|K$ est résiduellement triviale, si et seulement si on a, pour $\mathcal{Q}' \in P'(\sigma)$,

$$|\mathcal{Q}| = |\mathcal{Q}'|,$$

où $\mathcal{Q} = \mathcal{P} \cap K$.

Par ailleurs, l'application qui à $\mathcal{P}$ associe associe $\mathcal{Q} = \mathcal{P} \cap K$ définit une application surjective de $P(\sigma)$ vers P_C (la surjectivité résulte du fait que les élements de C sont tous conjugués).

Le nombre T d'éléments de $P(\sigma)$ au dessus de $\mathcal{Q}$ est donné par la formule

$$T = |\{\tau \in \mathrm{Gal}(L/K)/\tau\sigma = \sigma\tau\}|/|D_{\mathcal{P}}|,$$

où $D_{\mathcal{P}}$ est le sous groupe de décomposition en $\mathcal{P}$ de $\mathrm{Gal}(L/K)$. Or on a par un argument direct de théorie des groupes

$$|\{\tau \in \mathrm{Gal}(L/K)/\tau\sigma = \sigma\tau\}| = |\mathrm{Gal}(L/K)|/|C|.$$

Par ailleurs on a, puisque σ engendre le sous-groupe de décomposition en $\mathcal{P}$, $D_{\mathcal{P}} = \mathrm{Gal}(L/E)$. On a donc

$$T = \frac{|\mathrm{Gal}(L/K)|}{|C|.|\mathrm{Gal}(L/E)|}.$$

Passons au calcul de la densité de Dirichlet de P_C. On a

$$d(P_C) = \lim_{s \longrightarrow 1^+} \frac{\sum_{\mathcal{Q} \in P_C} \frac{1}{|\mathcal{Q}|^s}}{\log(\frac{1}{s-1})}.$$

En comptant les idéaux de $P'(\sigma)$ on obtient

$$d(P_C) = \frac{1}{T} \lim_{s \longrightarrow 1^+} \frac{\sum_{\mathcal{Q}' \in P(\sigma)} \frac{1}{|\mathcal{Q}'|^s}}{\log(\frac{1}{s-1})}.$$

On peut ajouter dans cette dernière somme des termes correspondant à des idéaux résiduellement non-triviaux. On a

$$\lim_{s \longrightarrow 1^+} \frac{\sum_{\mathcal{Q}' \notin P(\sigma)} \frac{1}{|\mathcal{Q}'|^s}}{\log(\frac{1}{s-1})} = 0,$$

puisque la série $\sum_{\mathcal{Q}' \notin P(\sigma)} \frac{1}{|\mathcal{Q}'|^s}$ converge en $s = 1$ (cela résulte du fait que $|\mathcal{Q}'|$ est une puissance ≥ 2 de $|\mathcal{Q}|$). On a donc, en notant $P_{\{\sigma\}}$ l'ensemble des idéaux premiers $\mathcal{Q}'$ de E tels que la substitution de Frobenius en $\mathcal{P}|\mathcal{Q}'$ soit égale à σ,

$$d(P_C) = \frac{1}{T} \lim_{s \longrightarrow 1^+} \frac{\sum_{\mathcal{Q}' \in P(\sigma)} \frac{1}{|\mathcal{Q}'|^s}}{\log(\frac{1}{s-1})} + \frac{\sum_{\mathcal{Q}' \in P_{\{\sigma\}} - P(\sigma)} \frac{1}{|\mathcal{Q}'|^s}}{\log(\frac{1}{s-1})} = \frac{1}{T} d(P_{\{\sigma\}}),$$

où la dernière densité est relative aux idéaux premiers de E. Puisque l'extension $L|E$ est cyclique, on connaît cette densité, d'après le premier cas. On obtient alors

$$d(P_C) = \frac{|\mathrm{Gal}(L/E)|.|C|}{|\mathrm{Gal}(L/K)|}.\frac{1}{|\mathrm{Gal}(L/E)|} = \frac{|C|}{|\mathrm{Gal}(L/K)|}.$$

7. Les corps de classe de rayon

Soit K un corps de nombres. Soit $\mathcal{M}$ un cycle arithmétique. La théorie du corps de classe établit l'existence d'un corps de classe de rayon $\mathcal{M}$. On le note $H^{\mathcal{M}}$ et il est caractérisé par les propriétés suivante.

1) C'est une extension abélienne finie de K et le groupe Galois de l'extension $H^{\mathcal{M}}|K$ est isomorphe à $C_K/C_K^{\mathcal{M}} \simeq \mathcal{C}\ell(K)^{\mathcal{M}}$.

2) L'extension $H^{\mathcal{M}}|K$ est non ramifiée en dehors de $\mathcal{M}$.

3) Cet isomorphisme associe à une substitution de Frobenius en un idéal premier $\mathcal{P}$ (premier à $\mathcal{M}$) la classe de l'idéal $\mathcal{P}$ dans $\mathcal{C}\ell(K)^{\mathcal{M}}$.

4) Toute extension abélienne de K est contenue dans un corps de classes de rayon.

La deuxième démonstration du théorème de Chebotarev utilise ces propriétés en général. La première démonstration l'utilise dans des cas si particuliers qu'on n'a pas besoin de la théorie générale.

Soit $L|K$ une extension abélienne de corps de nombres. Comme tout sous-groupe d'indice fini de C_K contient un sous-groupe de congruence $C_K^{\mathcal{M}}$, pour $\mathcal{M}$ cycle arithmétique approprié, le corps L est un sous-corps du corps de classe de rayon $\mathcal{M}$.

Considérons l'isomorphisme de groupes

$$C_K/C_K^{\mathcal{M}} \simeq \mathcal{C}\ell(K)^{\mathcal{M}}$$

Le fait que L soit contenu dans le corps de classe de rayon $\mathcal{M}$ s'exprime dans le diagramme suivant

$$1 \longrightarrow \mathrm{Gal}(H^{\mathcal{M}}/L) \longrightarrow \mathrm{Gal}(H^{\mathcal{M}}/K) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1,$$

ce diagramme s'identifiant terme à terme à

$$1 \longrightarrow H/\mathcal{P}(K)^{\mathcal{M}} \longrightarrow \mathcal{C}\ell(K)^{\mathcal{M}} \longrightarrow \mathcal{I}(K)^{\mathcal{M}}/H \longrightarrow 1,$$

où H est un sous-groupe de $\mathcal{I}(K)^{\mathcal{M}}$ contenant $\mathcal{P}(K)^{\mathcal{M}}$.

La compatibilité locale-globale dans la théorie du corps de classe nous indique que l'extension $H^{\mathcal{M}}|K$ est non ramifiée en tout idéal premier à $\mathcal{M}$. C'est donc aussi le cas de l'extension $L|K$.

Puisque l'extension $L|K$ est abélienne, la substitution de Frobenius associée à un idéal premier $\mathcal{P}$ de L au-dessus de $\mathcal{Q}$ idéal premier de K ne dépend que de $\mathcal{Q}$. On peut donc la noter $\mathrm{Frob}_{\mathcal{Q}}$.

De plus dans l'isomorphisme de groupes

$$\mathrm{Gal}(L/K) \simeq \mathcal{I}(K)^{\mathcal{M}}/H$$

l'image de la substitution de Frobenius en $\mathcal{P}$ est la classe de l'idéal $\mathcal{P}$. Cela résulte du fait que l'isomorphisme de groupes construit par la proposition IX-2

$$C_K/C_K^{\mathcal{M}} \simeq \mathcal{C}\ell(K)^{\mathcal{M}}$$

associe à la classe d'une uniformisante en $\mathcal{P}$ (via l'homomorphisme canonique $K_{\mathcal{P}}^* \longrightarrow C_K$) la classe de $\mathcal{P}$ dans le corps de classe de rayon $\mathcal{M}$.

Il résulte de cela que l'ordre d'un idéal premier $\mathcal{P}$ ne divisant pas $\mathcal{M}$ dans $\mathcal{C}\ell(K)^{\mathcal{M}}$ est égal l'ordre de la substitution de Frobenius dans $\mathrm{Gal}(H^{\mathcal{M}}/K)$ c'est-à-dire le degré résiduel en $\mathcal{P}$ de l'extension $H^{\mathcal{M}}|K$. On en déduit encore que l'ordre de $\mathcal{P}$ dans $\mathcal{I}(K)^{\mathcal{M}}/H$ est égal au degré résiduel de l'extension $L|K$.

Considérons le corps de classe $H^{\mathcal{M}}$ de rayon $\mathcal{M}$. Notons $h_{\mathcal{M}}$ le nombre de classes de rayon $\mathcal{M}$.

Proposition 7. — *On a*

$$\zeta_{H^{\mathcal{M}}}(s) = \prod_{\mathcal{P}|\mathcal{M}} \frac{1}{1-|\mathcal{P}|^{-s}} \prod_{\chi} L(\chi, s),$$

où χ parcourt les caractères du groupes des classes de rayon $\mathcal{M}$, et où $\mathcal{P}$ parcourt les idéaux premiers de $H^{\mathcal{M}}$ divisant $\mathcal{M}$.

Démonstration. — C'est un calcul direct. Dans ce qui suit, les sommes portant sur les caractères portent toutes sur tous les caractères du groupe des classes de rayon $\mathcal{M}$. Transformons les produits en sommes et utilisons le développement du logarithme :

$$\log(\prod_{\chi} L(\chi, s)) = \sum_{k=1}^{\infty} \sum_{\mathcal{Q}} \sum_{\chi} \frac{\chi(\mathcal{Q})^k}{k|\mathcal{Q}|^{ks}},$$

où $\mathcal{Q}$ parcourt les idéaux premiers de $\mathcal{O}_K$ ne divisant pas $\mathcal{M}$. En utilisant que χ est un homomorphisme de groupes, on obtient

$$\log(\prod_{\chi} L(\chi, s)) = \sum_{k=1}^{\infty} \sum_{\mathcal{Q}} (\sum_{\chi} \frac{\chi(\mathcal{Q}^k)}{k|\mathcal{Q}|^{ks}}).$$

En utilisant la formule $\sum_{\chi} \chi(R) = h_{\mathcal{M}}$ ou 0 suivant que R est nul ou non dans le groupe des classes de rayon $\mathcal{M}$, notre égalité devient

$$\log(\prod_{\chi} L(\chi, s)) = \sum_{k=1}^{\infty} \sum_{\mathcal{Q}, \mathcal{Q}^k \in \mathcal{P}(K)^{\mathcal{M}}} \frac{h_{\mathcal{M}}}{k|\mathcal{Q}|^{ks}}.$$

Par ailleurs $\mathcal{Q}^k$ est nul dans ce groupe des classes si et seulement si k est un multiple du degré résiduel $f_{\mathcal{Q}}$ de $\mathcal{Q}$ dans l'extension $H^{\mathcal{M}}|K$. Posons dans ce cas $k = f_{\mathcal{Q}} n$. Soit $\mathcal{P}$ l'idéal de $\mathcal{O}_K$ au-dessus de $\mathcal{Q}$. On a $|\mathcal{Q}|^{f_{\mathcal{P}}} = |\mathcal{P}|$.

On obtient

$$\log(\prod_{\chi} L(\chi, s)) = \sum_{\mathcal{Q}} \sum_{n=1}^{\infty} \frac{h_{\mathcal{M}}}{f_{\mathcal{P}} n |\mathcal{P}|^{f_{\mathcal{Q}} n s}}.$$

En utilisant la formule (et au passage le fait que $H^{\mathcal{M}}|K$ est non ramifié en $\mathcal{Q}$ par la théorie de corps de classe)

$$[H^{\mathcal{M}} : K] = h_{\mathcal{M}} = f_{\mathcal{P}} \sum_{\mathcal{P}|\mathcal{Q}} 1,$$

on obtient

$$\log(\prod_{\chi} L(\chi, s)) = \sum_{\mathcal{P}|\mathcal{M}} \sum_{n=1}^{\infty} \frac{1}{n|\mathcal{P}|^{ns}},$$

où $\mathcal{P}$ parcourt les idéaux premier de $H^{\mathcal{M}}$ ne divisant pas $\mathcal{M}$. Ajoutons à cette quantité

$$\log(\prod_{\mathcal{P}|\mathcal{M}} \frac{1}{1-|\mathcal{P}|^{-s}}) = \sum_{\mathcal{P}|\mathcal{M}} \sum_{n=1}^{\infty} \frac{1}{n|\mathcal{P}|^{ns}}.$$

On obtient le logarithme de la fonction $\zeta_{H^{\mathcal{M}}}$.

Corollaire 1. — *On a, pour χ caractère du groupe des classes de rayon $\mathcal{M}$ différent de 1,*

$$L(\chi, 1) \neq 0.$$

Démonstration. — Pour $\chi = 1$, on a

$$L(\chi, s) = \zeta_K(s) \prod_{\mathcal{P}|\mathcal{M}} (1 - |\mathcal{P}|^{-s}).$$

Le facteur de droite de la dernière égalité est non nul en $s = 1$. On a d'après le théorème 2,

$$\zeta_{H^{\mathcal{M}}}(s) = \zeta_K(s) \prod_{\chi \neq 1} L(\chi, s) \prod_{\mathcal{P}|\mathcal{M}} (1 - |\mathcal{P}|^{-s}).$$

Les fonctions $\zeta_{H^{\mathcal{M}}}$ et ζ_K ont des pôles simples en $s = 1$. On en déduit le corollaire.

Soit $\mathcal{M}'$ un cycle arithmétique divisant $\mathcal{M}$. Les fonctions L de Dirichlet associées aux caractères triviaux sur les groupes de classes de rayon $\mathcal{M}$ et $\mathcal{M}'$ ne sont pas égales : leurs produits euleriens diffèrent en les idéaux premiers divisant $\mathcal{M}$ sans diviser $\mathcal{M}'$. Cela nous amène aux considérations suivantes.

On dit qu'un caractère de Dirichlet de niveau $\mathcal{M}$ est *primitif* s'il n'existe pas de caractère de Dirichlet χ' de niveau $\mathcal{M}'$ divisant strictement $\mathcal{M}$ tel que χ et χ' coïncident sur presque tout les idéaux premiers. En particulier le caractère trivial de niveau $\mathcal{M}$ n'est pas primitif, sauf si $\mathcal{M} = 1$. À tout caractère de Dirichlet χ de niveau $\mathcal{M}$ on peut associer un unique caractère de Dirichlet primitif de niveau $\mathcal{M}'$ qui coïncide avec χ en tout idéal premier ne divisant pas $\mathcal{M}$ ou divisant $\mathcal{M}'$. À tout caractère de Dirichlet χ' de niveau $\mathcal{M}'$ on peut associer un unique caractère de Dirichlet χ de niveau $\mathcal{M}$ (avec $\mathcal{M}'|\mathcal{M}$) qui coïncide avec χ en les idéaux premiers $\mathcal{P}$ ne divisant pas $\mathcal{M}$ et valant 0 en les autres idéaux premiers.

Proposition 8. — *On a*

$$\zeta_{H^{\mathcal{M}}}(s) = \prod_{\chi} L(\chi', s),$$

où χ' parcourt les caractères primitifs de niveau divisant $\mathcal{M}$.

Démonstration. — En effet, considérons la correspondance bijective $\chi' \mapsto \chi$ entre les caractère primitifs de niveau divisant $\mathcal{M}$ et les caractères de niveau $\mathcal{M}$. Les facteurs des produits eulériens de $L(\chi', s)$ et $L(\chi, s)$ sont égaux sauf ceux correspondant à $\mathcal{P}|\mathcal{M}$ et tel que $\mathcal{P}$ ne divise pas le niveau de χ'. Ces facteurs sont respectivement $1/(1 - \chi'(\mathcal{P})|\mathcal{P}|^{-s})$ et 1. On retrouve ainsi les facteurs manquant de la fonction $\zeta_{H^{\mathcal{M}}}$ dans l'énoncé de la proposition 7.

Remarque . — À tout caractère ϵ de $\mathrm{Gal}(\bar{K}/K)$ d'image finie correspond donc un caractère de Dirichlet en le sens suivant. Un caractère de $\mathrm{Gal}(\bar{K}/K)$ se factorise par $\mathrm{Gal}(L/K)$ où

$L|K$ est une extension abélienne. Le groupe $\mathrm{Gal}(L/K)$ est un quotient de de $\mathrm{Gal}(H^{\mathcal{M}}/K)$ pour un certain rayon $\mathcal{M}$. On a donc un caractère de Dirichlet χ du corps de classe de rayon $\mathcal{M}$ tel que $\chi(\mathcal{P})$ soit égal à l'image par ϵ d'une substitution de Frobenius en $\mathcal{P}$ dans $\mathrm{Gal}(\bar{K}/K)$ (pour tout $\mathcal{P}$ idéal premier de K ne divisant pas $\mathcal{M}$). On peut donc associer une série L de Dirichlet à tout caractère d'image finie de $\mathrm{Gal}(\bar{K}/K)$. C'est

$$\prod_{\mathcal{P}} \frac{1}{1-\chi(\mathrm{Frob}_{\mathcal{P}})|\mathcal{P}|^{-s}}.$$

8. Deuxième démonstration du théorème de Chebotarev

Le théorème de la progression arithmétique de Dirichlet admet la généralisation suivante.

THÉORÈME 2. — *Soit $\mathcal{M}$ un cycle arithmétique de K. Soit H un sous-groupe de $\mathcal{I}(K)^{\mathcal{M}}$ d'indice h_0 contenant $\mathcal{P}(K)^{\mathcal{M}}$. Soit $R_0 \in \mathcal{I}(K)^{\mathcal{M}}/H$. Alors on a*

$$d(R_0) = \frac{1}{h_0}.$$

Démonstration. — On a (où $\mathcal{P}$ parcourt les idéaux premiers de K)

$$h_0 \sum_{\mathcal{P}\in R_0} \frac{1}{|\mathcal{P}|^s} = \sum_{\mathcal{P}} (\sum_{\chi} \chi(\mathcal{P})\chi(R_0^{-1})) \frac{1}{|\mathcal{P}|^s} = \sum_{\chi} \chi(R_0^{-1}) \sum_{\mathcal{P}} \frac{\chi(\mathcal{P})}{|\mathcal{P}|^s}.$$

En isolant les termes correspondant à $\chi = 1$, cette dernière expression est équivalente en 1^+ à

$$\sum_{\mathcal{P}} \frac{1}{|\mathcal{P}|^s} + \sum_{\chi\neq 1} \chi(R_0^{-1}) \log(L(\chi, s)).$$

Le deuxième terme de cette dernière expression est analytique en $s = 1$ d'après le corollaire de la proposition 7. Le premier terme étant équivalent à $\log(\frac{1}{s-1})$ on en déduit le théorème.

Remarque . — Le théorème de densité de Dirichlet donne dans un cas particulier le théorème de la progression arithmétique.

Donnons maintenant la démonstration du théorème 1 qui utilise la théorie du corps de classe.

On s'est ramené au cas où l'extension l'extension $L|K$ est cyclique. Elle est donc abélienne. On peut alors appliquer la théorie du corps de classe. Le corps L est contenu dans un corps de classe de rayon $H^{\mathcal{M}}$. Il existe un sous-groupe H de $\mathcal{I}(K)^{\mathcal{M}}$ et contenant $\mathcal{P}(K)^{\mathcal{M}}$ tel qu'on ait une suite exacte de groupes

$$1 \longrightarrow H/\mathcal{P}(K)^{\mathcal{M}} \longrightarrow \mathcal{I}(K)^{\mathcal{M}}/\mathcal{P}(K)^{\mathcal{M}} \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1.$$

Soit $\sigma \in \mathrm{Gal}(L/K)$. Puisque $\mathrm{Gal}(L/K)$ est abélien, la classe de conjugaison de σ est un singleton. Soit $R \in \mathcal{I}(K)^{\mathcal{M}}/H$ la classe associée à σ via l'isomorphisme de groupes $\mathcal{I}(K)^{\mathcal{M}}/H \simeq \mathrm{Gal}(L/K)$. On a

$$P_{\{\sigma\}} = \{\mathcal{P} \not| \mathcal{M}, \mathcal{P} \in R\}.$$

On a donc, d'après le théorème de Dirichlet,

$$d(P_{\{\sigma\}}) = \frac{1}{|\mathcal{I}(K)^{\mathcal{M}}/H|} = \frac{1}{|\mathrm{Gal}(L/K)|}.$$

Cela achève de traiter le cas cyclique.