Sur l'existence d'une preuve « euclidienne » du théorème de Dirichlet (d'après Ram Murty)

Bruno Martin
sous la direction de G. Hanrot et G. Tenenbaum
Université Henri Poincaré, Nancy

10 juillet 2002

Table des matières

Introduction

Aux alentours de 300 avant J.-C., Euclide fournit la preuve de l'infinitude des nombres premiers. Rappelons cette preuve : supposons *a contrario* qu'il n'existe qu'un nombre fini de nombres premiers, disons $\{p_1, ..., p_k\}$ (cet ensemble est non vide car 2 est premier) ; le nombre $p_1...p_k + 1$ est différent de 1, il possède donc un diviseur premier. Mais ce diviseur premier ne peut être l'un des p_i, d'où une contradiction. Il existe donc une infinité de nombres premiers.

On peut se demander dans quelle mesure une telle preuve peut être généralisée et s'appliquer à la démonstration de l'infinitude des nombres premiers appartenant à une progression arithmétique $\ell \pmod k$ où k et ℓ sont deux entiers premiers entre eux. Les preuves de ce théorème, énoncé et démontré par Dirichlet en 1837, sont assez élaborées. Toutefois, des cas particuliers ont été démontrés à la manière d'Euclide ; nous en verrons quelques-uns dans le chapitre 1.

L'objectif de ce mémoire est de présenter de façon détaillée un travail de Ram Murty [3] qui détermine les progressions pour lesquelles une preuve euclidienne, en un sens précis, est possible. Il s'agit avant tout de bien définir un concept de preuve euclidienne, en partant des exemples déjà connus, ce sera l'objet du chapitre 1. Ensuite nous démontrerons le théorème suivant :

Théorème 1 (Ram Murty) *Soient k et ℓ deux entiers non nuls premiers entre eux. Il existe une preuve euclidienne de l'infinitude des nombres premiers appartenant à la progression arithmétique $\ell \pmod k$ si et seulement si $\ell^2 \equiv 1 \pmod k$.*

En particulier, il est impossible de démontrer le théorème de Dirichlet dans le cas général à la manière d'Euclide. Montrer que la condition est suffisante est l'œuvre de Schur [6] en 1912, et la réciproque a été démontrée par Murty [3] en 1988.

Chapitre 1

Qu'est-ce qu'une preuve euclidienne ?

1.1 Premiers exemples

Nous allons démontrer le théorème de Dirichlet pour les progressions arithmétiques modulo 4 :

Proposition 1 *Il existe une infinité de nombres premiers dans la classe* $1 \pmod 4$ *et une infinité dans la classe* $3 \pmod 4$.

Démonstration. Étudions tout d'abord la progression $1 \pmod 4$: supposons par l'absurde que cette progression ne contienne qu'un nombre fini de nombres premiers, disons $\{p_1, ..., p_k\}$. On considère le polynôme $f(x) = x^2+1$ et l'entier $A = f(4Q) = 16Q^2+1$ où $Q = p_1...p_k$ (on pose $Q = 1$ si l'ensemble $\{p_1, ..., p_k\}$ est vide). Si q est un diviseur premier de A alors -1 est un carré modulo q donc $q \equiv 1 \pmod 4$. Si A n'est pas premier alors A est divisible par un entier $q \equiv 1 \pmod 4$ qui n'est pas dans $\{p_1, ..., p_k\}$. Ceci est absurde et il existe donc une infinité de nombres premiers dans cette progression.

Étudions à présent la progression $3 \pmod 4$: on suppose de même par l'absurde que cette progression ne contient qu'un nombre fini de nombres premiers, disons $\{p_1, ..., p_k\}$. On considère le polynôme $g(x) = x-1$ et l'entier $B = g(4Q) = 4Q - 1$ où Q est défini comme précédemment. L'entier B a un facteur congru à $3 \pmod 4$ puisqu'il est impair. Si tous ses facteurs premiers sont congrus à $1 \pmod 4$ alors $B \equiv 1 \pmod 4$, impossible. Donc il existe $q \equiv 3 \pmod 4$ tel que $q \mid B$ et il ne peut s'agir de l'un des p_k, d'où la conclusion. □

1.2 Diviseurs premiers d'un polynôme et autres exemples

Ces deux preuves reposent sur l'existence d'un polynôme dont les valeurs prises en des entiers sont divisibles par des nombres premiers dans la progression voulue. Dans le premier cas, $f(x) = x^2 + 1$, chaque valeur prise en un entier n'est divisible que par des nombres premiers congrus à $1 \pmod 4$. Dans le deuxième cas, $g(4x) = 4x - 1$, chaque valeur prise en un entier est divisible par au moins un nombre premier congru à $3 \pmod 4$. Cela nous conduit à étudier la notion suivante :

Définition 1 *Un premier p est un diviseur premier d'un polynôme f à coefficients dans $\mathbb{Z}$ s'il existe $n \in \mathbb{Z}$ tel que $p \mid f(n)$. On notera $p \mid f$. On notera également $P(f)$ l'ensemble des diviseurs premiers d'un polynôme f.*

Étudions par exemple le cas du k-ième polynôme cyclotomique que l'on note ϕ_k.

Proposition 2 *Supposons que $p \nmid k$. Alors*

$$p \mid \phi_k \quad \textit{si et seulement si} \quad p \equiv 1 \pmod k.$$

Démonstration. Soit p tel que $p|\phi_k(a)$ et $p \nmid k$. On a l'identité suivante bien connue :

$$X^k - 1 = \prod_{k|n} \phi_d(X). \tag{1.1}$$

On en déduit que $a^k \equiv 1 \pmod p$. Soit ℓ l'ordre de a modulo p et supposons que $\ell < k$. On a $a^\ell \equiv 1 \pmod p$; il existe donc d'après (1.1) d_0 tel que $\phi_{d_0}(a) \equiv 0 \pmod p$, donc a est racine double de $X^k - 1 \pmod p$. Mais cela implique que $p|\mathrm{Disc}(X^k - 1)$, donc que $p|k$ ce qui est exclu. Finalement a est d'ordre k modulo p et donc $k|(p-1)$.

Réciproquement si $k|(p-1)$, comme $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique, il existe a d'ordre k modulo p. Donc $\phi_d(a) \equiv 0 \pmod p$ pour un certain d qui divise k. Mais si $d < k$ l'ordre de a serait plus petit que k d'après $a^d - 1 \equiv 0 \pmod p$. Donc $p|\phi_k(a)$. □

Étudions à présent un dernier exemple de preuve euclidienne, un peu plus délicat que les deux précédents, qui nous guidera ultérieurement dans la preuve du cas général.

Proposition 3 *Il existe une infinité de nombres premiers dans la classe* $9 \pmod{20}$.

Démonstration. Considérons le polynôme f suivant :

$$f(x) = x^4 + 3x^2 + 1.$$

On a les deux identités suivantes :

$$f(x) = (x^2+1)^2 + x^2, \tag{1.2}$$

$$f(x) = (x^2-1)^2 + 5x^2. \tag{1.3}$$

Soit maintenant p un diviseur premier de f différent de 5. D'après l'identité (1.2), -1 est un carré modulo p. En effet, si $p|f(x)$ et $p|x$, alors $p|(x^2+1)$ donc $p|1$, impossible. Par suite x est premier avec p, et donc on a l'identité $-1 = ((x^2+1)/x)^2 \pmod{p}$, et $p \equiv 1 \pmod{4}$.

Par ailleurs de la même façon, d'après l'identité (1.3), -5 est un carré modulo p. La loi de réciprocité quadratique ajoutée au fait que $p \equiv 1 \pmod{4}$ montre que $p \equiv 1$ ou $9 \pmod{20}$. Nous pouvons maintenant remarquer que $29 \equiv 9 \pmod{20}$ est premier et que $f(2) = 29$. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers congrus à $9 \pmod{20}$, et notons Q le produit de tous ces nombres à l'exception de 29. Comme 29 et $5Q$ sont premiers entre eux, le théorème chinois assure l'existence d'un entier c tel que :

$$c \equiv 2 \pmod{29^2}$$

et

$$c \equiv 0 \pmod{5Q}$$

On a donc :

$$f(c) \equiv 29 \pmod{29^2} \tag{1.4}$$

et

$$f(c) \equiv 1 \pmod{5Q} \tag{1.5}$$

Soit maintenant p un diviseur premier de $f(c)$; p ne peut être égal ni à 5 ni à l'un des facteurs premiers de Q d'après (1.5). Tous ces diviseurs sont donc congrus à $1 \pmod{20}$ à l'exception de 29. Par suite, d'après (1.4), $f(c) \equiv 9 \pmod{20}$. Mais cela contredit $f(c) \equiv 1 \pmod{5}$, ce qui achève la preuve. □

1.3 Définition d'une preuve euclidienne

Suite à ces exemples et à la définition des diviseurs premiers d'un polynôme, la première nécessité pour une preuve euclidienne est l'existence d'un polynôme possédant une infinité de diviseurs premiers appartenant à la progression arithmétique voulue. Cela dit, il n'est pas *a priori* évident qu'un polynôme possède une infinité de diviseurs premiers. C'est l'objet du théorème suivant.

Théorème 2 (Schur) *Tout polynôme f non constant de $\mathbb{Z}[x]$ possède une infinité de diviseurs premiers.*

Démonstration. Si $f(0) = 0$, alors tous les nombres premiers divisent f. Supposons à présent que $f(0) = c \neq 0$. L'équation $f(x) = \pm 1$ n'a qu'un nombre fini de solutions, donc f admet au moins un diviseur premier. Supposons par l'absurde que l'ensemble des diviseurs de f soit fini. Notons $P(f) = \{p_1, ..., p_k\}$. Si $A = p_1...p_k$, alors on a

$$f(Acx) = \sum_{p=0}^{n} a_p(Acx)^p = c(1 + \sum_{p=1}^{n} a_p c^{p-1}(Ax)^p) = cg(x)$$

avec $g(x) = 1 + c_1x + ... + c_nx^n$. Le polynôme g est à coefficients entiers et $A \mid c_i$ pour tout $i > 0$. Si p est un diviseur premier de g alors c'est un diviseur premier de f donc p est l'un des p_i. Dès lors $p \mid A \mid c_i$ pour tout $i > 0$. Et comme p divise aussi $g(A)$ il vient $p \mid 1$, absurde.

□

On peut remarquer que l'on obtient ainsi, à la manière d'Euclide, un cas particulier du théorème de Dirichlet, grâce à la proposition 2 :

Corollaire 1 *Pour tout entier k, il existe une infinité de nombres premiers congrus à $1 \pmod{k}$.*

Nous allons maintenant envisager les diviseurs premiers d'un polynôme d'une autre manière, plus précisément en terme de factorisation d'un nombre premier dans l'anneau des entiers d'un corps de nombres. On rappelle le théorème suivant :

Théorème 3 *Soit $K = \mathbb{Q}(\alpha)$, f le polynôme minimal de α sur $\mathbb{Q}$ et $\mathbb{Z}_K$ son anneau des entiers. Soit p un nombre premier tel que $p \nmid [\mathbb{Z}_K : \mathbb{Z}[x]]$. Si la factorisation modulo p de f en produit de facteurs irréductibles s'écrit*

$$f(X) = \prod_{i=1}^{g} f_i(X)^{e_i},$$

alors

$$p\mathbb{Z}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

où les $\mathfrak{p}_i = p\mathbb{Z}_K + f_i(\alpha)\mathbb{Z}_K$ *sont des idéaux premiers deux à deux distincts de* $\mathbb{Z}_K$ *et où l'on a* $N(\mathfrak{p}_i) = p^{\deg f_i}$.

Par unicité de la factorisation dans un anneau de Dedekind, on peut en déduire immédiatement la proposition suivante :

Proposition 4 *Excepté pour un nombre fini de nombres premiers,* p *divise* f *si et seulement si* p *admet un facteur premier de degré résiduel égal à* 1 *(on dira désormais de degré 1) dans un corps de rupture de* f.

Remarque : les premiers que l'on exclut sont ceux qui divisent $[\mathbb{Z}_K : \mathbb{Z}[x]]$. En particulier ils divisent le discriminant de f car

$$\mathrm{Disc}(f) = [\mathbb{Z}_K : \mathbb{Z}[x]]^2 \,.\, \mathrm{Disc}(K).$$

Avant d'aborder le théorème suivant, nous donnons un lemme qui nous servira à plusieurs reprises.

Lemme 1 *Soit* $\mathbb{Q} \subseteq K \subseteq L$ *deux extensions de* $\mathbb{Q}$. *Si un nombre premier* p *possède un facteur premier de degré* 1 *dans* L, *alors il possède un facteur premier de degré* 1 *dans* K.

Démonstration. Soit $\mathfrak{P}$ un idéal de L tel que $\mathfrak{P} \mid p$ et $N_{K/\mathbb{Q}}(\mathfrak{P}) = p$. Posons $\mathfrak{p} = \mathfrak{P} \cap \mathbb{Z}_K$. Dès lors

$$\mathfrak{p} \cap \mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}_K \cap \mathbb{Z} = p\mathbb{Z} \cap \mathbb{Z}_K = p\mathbb{Z},$$

autrement dit $\mathfrak{p}|p$. Par ailleurs on a la suite d'inclusions (en fait d'injections) suivantes :

$$\mathbb{Z}/p\mathbb{Z} \subseteq \mathbb{Z}_K/\mathfrak{p} \subseteq \mathbb{Z}_L/\mathfrak{P} \subseteq \mathbb{Z}/p\mathbb{Z},$$

la dernière inclusion provenant de $\mathrm{card}\, \mathbb{Z}_L/\mathfrak{P} = N_{L/\mathbb{Q}}(\mathfrak{P}) = p$. On en déduit que $N_{K/\mathbb{Q}}(\mathfrak{p}) = \mathrm{card}\, \mathbb{Z}_K/\mathfrak{p} = p$. Donc $\mathfrak{p}$ est de degré 1 ce qui achève la preuve. □

Ce qui précède va nous permettre de démontrer aisément un théorème dû à Nagell.

Théorème 4 (Nagell) *Si* f *et* g *sont deux polynômes non constants de* $\mathbb{Z}[x]$, *alors* $P(f) \cap P(g)$ *est infini.*

Démonstration. Soit α une racine de f ; notons $K_f = \mathbb{Q}(\alpha)$. Notons K_g l'homologue pour g.

Considérons L le plus petit sous-corps de $\mathbb{C}$ contenant K_f et K_g. Ce corps est une extension de degré fini sur $\mathbb{Q}$, d'après le théorème de l'élément primitif il existe donc $\beta \in L$ tel que $L = \mathbb{Q}(\beta)$. Cet élément β possède un polynôme minimal à coefficients dans $\mathbb{Z}$. D'après le théorème de Schur et la proposition 4, l'ensemble des nombres premiers qui ont un facteur premier de degré 1 dans L est infini. D'après le lemme 1, ces nombres premiers ont donc un facteur de degré 1 dans K_f et dans K_g. Il existe donc une infinité de nombres premiers ayant un facteur de degré 1 à la fois dans K_f et dans K_g. En vertu de la proposition 4, on conclut que $P(f) \cap P(g)$ est infini. □

Une preuve plus élémentaire (et plus longue) de ce résultat existe mais celle-la nous permet de nous familiariser avec les outils fondamentaux utilisés par la suite.

Le théorème de Nagell nous permet de repréciser la définition d'une preuve euclidienne. On a vu que les diviseurs premiers du k-ième polynôme cyclotomique sont les diviseurs de k et les nombres premiers congrus à $1 \pmod k$. Le théorème de Nagell implique donc que tout polynôme possède une infinité de diviseurs premiers congrus à $1 \pmod k$ pour tout entier k, ce qui réduit à néant tout espoir de prouver le théorème de Dirichlet de la même manière que le cas particulier de la progression $1 \pmod k$ (corollaire 1).

Le lemme suivant nous permet de définir ce que nous entendrons par preuve euclidienne pour la progression $\ell \pmod k$. Notons qu'il est nécessaire d'exhiber un nombre premier de la progression pour pouvoir conclure (condition c).

Lemme 2 *Supposons l'existence d'un polynôme f de $\mathbb{Z}[x]$ vérifiant les conditions suivantes :*
a) Les diviseurs premiers de f sont des diviseurs de $k\mathrm{Disc}(f)$, et tous les nombres premiers congrus à 1 ou $\ell \pmod k$.
b) Tous les diviseurs premiers de $f(0)$ sont congrus à $1 \pmod k$.
c) Il existe $p \equiv \ell \pmod k$ qui ne divise pas $\mathrm{Disc}(f)$.
Alors il existe une infinité de nombres premiers congrus à $\ell \pmod k$.

Démonstration. Soit $p \equiv \ell \pmod k$ un nombre premier qui ne divise pas $\mathrm{Disc}(f)$. D'après a) il existe $b \in \mathbb{Z}$ tel que $p \mid f(b)$. On peut en fait choisir b de manière à ce que $p^2 \nmid f(b)$. On part pour cela de l'identité :

$$f(b+p) \equiv f(b) + pf'(b) \pmod p^2. \tag{1.6}$$

Supposons à présent que $p^2 \mid f(b)$. Comme $p \nmid \mathrm{Disc}(f)$, $p \nmid f'(b)$. Donc $p^2 \nmid f(b+p)$ sinon la congruence (1.6) serait fausse ; et cependant $p|f(b+p)$. Un tel choix de b est donc possible.

Maintenant supposons *a contrario* qu'il n'existe qu'un nombre fini de nombres premiers congrus à $\ell \pmod{k}$. Soit Q le produit de ces nombres à l'exclusion de p (on pose $Q = 1$ si p est le seul premier de ce type). Si l'on note $D = \mathrm{Disc}(f)$, les entiers p^2 et DkQ sont premiers entre eux donc le théorème chinois garantit l'existence d'un entier naturel c tel que :

$$c \equiv b \pmod{p^2}$$

et

$$c \equiv 0 \pmod{DkQ}.$$

Dès lors

$$f(c) \equiv f(b) \pmod{p^2} \tag{1.7}$$

et

$$f(c) \equiv f(0) \pmod{DkQ} \tag{1.8}$$

D'après (1.7) et le choix de b, $p \mid f(c)$ et $p^2 \nmid f(c)$. Maintenant, étudions les éventuels diviseurs de $f(c)$:

- $f(c)$ est premier avec Q. En effet si q, un nombre premier congru à $\ell \pmod{k}$, divisait $f(c)$ alors il diviserait $f(0)$ d'après (1.8) ce qui est exclu d'après b).
- $f(c)$ est premier avec k. En effet si q est un nombre premier tel que $q|k$ et $q|f(c)$, encore exclu d'après b).
- Si un nombre premier divise $f(c)$ et D, il divise $f(0)$ d'après (1.8), il est donc congru à $1 \pmod{k}$ d'après b).

Donc, à l'exception de p, tous les diviseurs premiers de $f(c)$ sont congrus à $1 \pmod{k}$. Comme de plus $p^2 \nmid f(c)$, on a $f(c) \equiv \ell \pmod{k}$. Mais ceci contredit $f(c) \equiv f(0) \equiv 1 \pmod{k}$, d'où le résultat. □

Comme on peut le voir, la factorisation des nombres premiers dans un corps de nombres, et même dans une extension relative, joue un rôle central dans notre problème. Nous allons ainsi avoir besoin d'un théorème nous renseignant sur la proportion des nombres premiers présentant un certain type de factorisation dans une extension galoisienne. Ce théorème fera l'objet du chapitre 2. Dans le chapitre 3 nous nous intéresserons à la factorisation des nombres premiers dans des sous-extensions d'une extension galoisienne de $\mathbb{Q}$ et nous résoudrons en détail le cas cyclotomique. Enfin dans le dernier chapitre nous rédigerons la preuve de l'équivalence annoncée, à l'aide de tous les outils introduits.

Chapitre 2

Le théorème de Tchébotarev

En prévision de la suite, nous allons devoir traiter le cas général d'une extension relative.

Dans tout ce chapitre, K désigne un corps de nombres, $\mathbb{Z}_K$ son anneau des entiers (sur $\mathbb{Q}$ ou sur un autre corps de nombres), L une extension galoisienne de K, n son degré, G son groupe de Galois, et $\mathbb{Z}_L$ la fermeture intégrale de $\mathbb{Z}_K$ dans L.

2.1 Factorisation des nombres premiers dans une extension galoisienne

Nous rappelons le théorème important suivant, qui montre que la situation est très agréable dans le cas galoisien.

Théorème 5 *Si $\mathfrak{p}$ est un idéal premier de $\mathbb{Z}_K$, les idéaux premiers $\mathfrak{P}_i$ de $\mathbb{Z}_L$ figurant dans la factorisation de $\mathfrak{p}$ dans $\mathbb{Z}_L$ sont deux à deux conjugués, et donc ont le même degré résiduel f et le même indice de ramification e ; ainsi*

$$\mathfrak{p}\mathbb{Z}_L = \Big(\prod_{i=1}^{g} \mathfrak{P}_i\Big)^e$$

et,

$$n = efg.$$

Pour la preuve nous renvoyons à Samuel [5].

Cela a une conséquence évidente mais importante : dès que $\mathfrak{p}$ est un idéal premier non ramifié dans une extension galoisienne, il est équivalent de dire qu'il y admet un facteur de degré 1 ou qu'il y est totalement décomposé.

2.2 Groupe de décomposition et groupe d'inertie

On considère maintenant un idéal premier $\mathfrak{p}$ de $\mathbb{Z}_K$, et un idéal premier $\mathfrak{P}$ de $\mathbb{Z}_L$ qui divise $\mathfrak{p}$.

Définition 2 *Les $\sigma \in G$ tels que $\sigma(\mathfrak{P}) = \mathfrak{P}$ forment un sous-groupe noté $D_{\mathfrak{P}}$ de G, qu'on appelle le groupe de décomposition de $\mathfrak{P}$.*

Remarque : si g est le nombre de conjugués de $\mathfrak{P}$ on a, grâce à un théorème classique sur les actions de groupe,

$$g = \mathrm{card}\,(G).\,\mathrm{card}\,(D_{\mathfrak{P}})^{-1} \qquad \text{soit} \qquad \mathrm{card}\,(D_{\mathfrak{P}}) = \frac{n}{g} = ef.$$

Pour $\sigma \in D_{\mathfrak{P}}$, la relation $\sigma(\mathbb{Z}_L) = \mathbb{Z}_L$ montre que σ définit, par passage au quotient, un automorphisme $\overline{\sigma}$ de $\mathbb{Z}_L/\mathfrak{P}$. Il est clair que $\overline{\sigma}$ est un $\mathbb{Z}_K/\mathfrak{p}$-automorphisme.

Définition 3 *Le noyau $I_{\mathfrak{P}}$ de l' homomorphisme de groupes $\sigma \longrightarrow \overline{\sigma}$ est un sous-groupe de $D_{\mathfrak{P}}$ appelé le groupe d'inertie de $\mathfrak{P}$.*

On a maintenant le théorème suivant :

Théorème 6 *$\mathbb{Z}_L/\mathfrak{P}$ est une extension galoisienne de degré f de $\mathbb{Z}_K/\mathfrak{p}$, et $\sigma \longrightarrow \overline{\sigma}$ est un homomorphisme surjectif de $D_{\mathfrak{P}}$ sur son groupe de Galois. De plus,* $\mathrm{card}\,(I) = e$.

Démonstration. Dans toute cette démonstration on notera $D = D_{\mathfrak{P}}$ (de même pour $I_{\mathfrak{P}}$).

La première assertion est claire : il s'agit d'une extension de corps finis de degré fini.

Pour montrer la surjectivité, on va d'abord montrer que l'on peut se ramener au cas où $K = L^D$, où L^D est la sous-extension de L fixée par D. Comme l'extension L/L^D est aussi galoisienne et que son groupe de Galois est D, d'après le théorème 5, $\mathfrak{P}$ est le seul facteur premier de $\mathfrak{p}_D = \mathfrak{P} \cap \mathbb{Z}_{L^D}$ dans $\mathbb{Z}_{L^D}$. On peut poser :

$$\mathfrak{p}_D \mathbb{Z}_{L^D} = \mathfrak{P}^{e'},$$

et

$$f' = [\mathbb{Z}_L/\mathfrak{P} \,:\, \mathbb{Z}_{L^D}/\mathfrak{p}_D],$$

le degré résiduel de $\mathfrak{P}$ sur $\mathbb{Z}_{L^D}$. D'après la remarque sur le cardinal d'un groupe de décomposition, on a

$$e^{'} f^{'} = [L : L^D] = \text{card}\,(D) = ef. \tag{2.1}$$

Comme $\mathbb{Z}_K/\mathfrak{p} \subseteq \mathbb{Z}_{L^D}/\mathfrak{p}_D \subseteq \mathbb{Z}_L/\mathfrak{P}$ on a $f^{'} \leq f$. Par ailleurs $\mathfrak{p}_D|\mathfrak{p}$ donc $e^{'} \leq e$. Combiné à (2.1), ces deux inégalités donnent : $e^{'} = e$ et $f^{'} = f$. On en déduit :

$$\mathbb{Z}_K/\mathfrak{p} \simeq \mathbb{Z}_{L^D}/\mathfrak{p}_D.$$

Soit à présent $\overline{a}$ un élément primitif de $\mathbb{Z}_L/\mathfrak{P}$ sur $\mathbb{Z}_{L^D}/\mathfrak{p}_D$ (qui existe par le théorème de l'élément primitif puisque l'extension est de degré fini sur un corps fini) et soit $\overline{h}$ son polynôme minimal sur $\mathbb{Z}_{L^D}/\mathfrak{p}_D$. On relève $\overline{a}$ en un élément a de $\mathbb{Z}_L$ et on note f le polynôme minimal de a sur L^D. Les coefficients de f sont en fait dans $\mathbb{Z}_{L^D}$ puisque $x \in \mathbb{Z}_{L^D}$. Comme l'extension L/L^D est galoisienne, tous les conjugués de x sont dans L et donc dans $\mathbb{Z}_L$ puisque $f \in \mathbb{Z}_{L^D}[X]$. Ainsi

$$f(X) = \prod_{\sigma \in D} (X - \sigma(a)).$$

L'image de ce polynôme par la surjection canonique $\mathbb{Z}_L \longrightarrow \mathbb{Z}_L/\mathfrak{P}$ est :

$$\overline{f} = \prod_{\sigma \in D} (X - \overline{\sigma}(\overline{a})).$$

L'élément $\overline{a}$ figure parmi les racines de $\overline{f}$. Donc $\overline{h}|\overline{f}$ et ainsi les conjugués de $\overline{a}$ sont parmi les $\sigma(\overline{a})$ pour $\sigma \in D$. Ainsi si $\tau \in \text{Gal}(\mathbb{Z}_L/\mathfrak{P}\,/\,\mathbb{Z}_{L^D}/\mathfrak{p}_D)$, $\tau(\overline{a}) = \sigma(\overline{a})$ pour un $\sigma \in D$ et donc τ et $\overline{\sigma}$ coïncident sur $\mathbb{Z}_L/\mathfrak{P}$ et la surjectivité est prouvée.

Finalement $\text{Gal}(\mathbb{Z}_L/\mathfrak{P}\,/\mathbb{Z}_K/\mathfrak{p}) \simeq D/I$. Mais l'ordre du premier groupe est $[\mathbb{Z}_L/\mathfrak{P} : \mathbb{Z}_K/\mathfrak{p}] = f$, on en déduit donc que $\text{card}\,(I) = e$. □

Corollaire 2 *Pour que $\mathfrak{p}$ ne se ramifie pas dans $\mathbb{Z}_L$, il faut et il suffit que le groupe d'inertie soit réduit à l'identité.*

Nous terminerons ce paragraphe par une proposition utile.

Proposition 5 *Si on note $D_{\mathfrak{P}}$ le groupe de décomposition de l'idéal premier $\mathfrak{P}$, celui du conjugué $\sigma(\mathfrak{P})$ est*

$$D_{\sigma(\mathfrak{P})} = \sigma D_{\mathfrak{P}} \sigma^{-1}.$$

Démonstration. Si $\tau \in D_{\mathfrak{P}}$, on a $\tau(\mathfrak{P}) = \mathfrak{P}$, d'où $\sigma\tau\sigma^{-1}(\sigma(\mathfrak{P})) = \sigma(\mathfrak{P})$, donc $\sigma D_{\mathfrak{P}} \sigma^{-1} \subseteq D_{\sigma(\mathfrak{P})}$. En appliquant cela à σ^{-1} et à $\sigma(\mathfrak{P})$, on obtient l'inclusion réciproque. □

Ainsi lorsque L est une extension abélienne de K, les groupes $D_{\mathfrak{P}}$ sont tous égaux, et ne dépendent que de l'idéal $\mathfrak{p}$ de $\mathbb{Z}_K$.

2.3 L'automorphisme de Frobenius

Soit maintenant $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_K$ qui ne se ramifie pas dans $\mathbb{Z}_L$, et soit $\mathfrak{P}$ un facteur premier de $\mathfrak{p}$. D'après le corollaire 2, le groupe d'inertie de $\mathfrak{P}$ est réduit à l'identité, et son groupe de décomposition D est donc canoniquement isomorphe au groupe $\mathrm{Gal}(\mathbb{Z}_L/\mathfrak{P}\,/\,\mathbb{Z}_K/\mathfrak{p})$ d'après le théorème 6. Mais ce dernier est cyclique, avec un générateur privilégié $\overline{\sigma}$: $\overline{x} \mapsto \overline{x}^q$ où $q = \mathrm{card}\,(\mathbb{Z}_K/\mathfrak{p})$. Par surjectivité, on en déduit la définition suivante :

Définition 4 *Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_K$ qui ne se ramifie pas dans $\mathbb{Z}_L$, et soit $\mathfrak{P}$ un facteur premier de $\mathfrak{p}$ dans $\mathbb{Z}_L$. On pose $q = N_{K/\mathbb{Q}}(\mathfrak{p})$. Alors $D_{\mathfrak{P}}$ est cyclique, avec un générateur privilégié σ tel que*

$$\sigma(x) \equiv x^q \pmod{\mathfrak{P}}$$

pour tout $x \in \mathbb{Z}_L$. On appelle ce générateur l'automorphisme de Frobenius de $\mathfrak{P}$, et on le note $(\mathfrak{P}, L/K)$.

Pour $\tau \in G$ on a, d'après la proposition 5,

$$(\tau(\mathfrak{P}), L/K) = \tau.\,(\mathfrak{P}, L/K).\,\tau^{-1}.$$

En particulier, si L est une extension abélienne, $(\mathfrak{P}, L/K)$ ne dépend que de l'idéal $\mathfrak{p}$ de $\mathbb{Z}_K$ et on notera $(\mathfrak{p}, L/K)$ cet élément. Si en revanche l'extension n'est pas abélienne, l'ensemble des $(\mathfrak{P}, L/K)$ où $\mathfrak{P}|\mathfrak{p}$ est une classe de conjugaison de G, que l'on notera également par abus, $(\mathfrak{p}, L/K)$. Nous pouvons résumer cela dans la définition suivante :

Définition 5 *Soit $\mathfrak{p}$ un idéal premier non ramifié de $\mathbb{Z}_K$. On appelle symbole d'Artin et on note $(\mathfrak{p}, L/K)$ la classe de conjugaison (éventuellement réduite à un élément) des automorphismes de Frobenius des idéaux premiers intervenant dans sa factorisation dans $\mathbb{Z}_L$.*

Exemple : étudions le cas d'une extension cyclotomique, soit $K = \mathbb{Q}$ et $L = \mathbb{Q}(\zeta_k)$ où ζ_k est une racine k-ème de l' unité. Soit p un nombre premier non ramifié, autrement dit qui ne divise pas k. L'automorphisme $\sigma = (p, \mathbb{Q}(\zeta_k)/\mathbb{Q})$ est l'unique élément de $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ tel que

$$\sigma(x) \equiv x^p \pmod{\mathfrak{p}}, \text{ pour tout } x \in \mathbb{Z}[\zeta_k],$$

pour un idéal premier $\mathfrak{p}$ divisant p. L'élément σ est alors l'automorphisme $\zeta_k \mapsto \zeta_k^p$. En effet si $\mathfrak{p}$ est un idéal premier divisant p, on a

$$\sigma\left(\sum a_i\zeta_k^i\right) = \sum a_i\zeta_k^{ip} \equiv \sum a_i^p\zeta_k^{ip} \equiv \left(\sum a_i\zeta_k^i\right)^p \pmod{\mathfrak{p}},$$

où les a_i sont dans $\mathbb{Z}$. En particulier le symbole d'Artin d'un premier dans $\mathbb{Q}(\zeta_k)$ ne dépend que de sa classe résiduelle dans $(\mathbb{Z}/k\mathbb{Z})^*$.

Nous terminons ce paragraphe par une proposition permettant de travailler avec les automorphismes de Frobenius dans une tour d'extensions.

Proposition 6 *Avec les hypothèses précédentes on se donne une extension intermédiaire K'. On note f le degré résiduel de $\mathfrak{P} \cap K'$ sur K. Alors*
i) on a $(\mathfrak{P}, L/K') = (\mathfrak{P}, L/K)^f$
ii) si l'extension K' est galoisienne sur K, la restriction de $(\mathfrak{P}, L/K)$ à K' est égale à $(\mathfrak{P} \cap K', K'/K)$.

Démonstration. Posons $\sigma = (\mathfrak{P}, L/K)$ et $q = \text{card}\,(\mathbb{Z}_K/\mathfrak{p})$. Par définition de f, q^f est le cardinal du corps résiduel $(\mathbb{Z}_L \cap K')/(\mathfrak{P} \cap K')$. De plus le groupe de décomposition de $\mathfrak{P}$ sur K' est clairement un sous-groupe de $D_{\mathfrak{P}}$ et il est d'ordre

$$\left[\mathbb{Z}_L/\mathfrak{P} \,:\, (\mathbb{Z}_L \cap K')/(\mathfrak{P} \cap K')\right] = f^{-1}\,[\mathbb{Z}_L/\mathfrak{P} \,:\, \mathbb{Z}_K/\mathfrak{p}] = f^{-1}.\,\text{card}\,(D_{\mathfrak{P}})$$

d'après la première remarque sur le cardinal d'un groupe de décomposition et la multiplicativité des degrés. Comme $D_{\mathfrak{P}}$ est cyclique et engendré par σ il admet un unique sous-groupe d'ordre $f^{-1}.\,\text{card}\,(D)$ et ce dernier est engendré par σ^f. Enfin les relations $\sigma^f(\mathfrak{P}) = \mathfrak{P}$ et $\sigma^f(x) \equiv x^{q^f} \pmod{\mathfrak{P}}$ se déduisent immédiatement de celles vérifiées par σ, ce qui prouve i).

Supposons maintenant que K' est galoisienne sur K, et notons $\tilde{\sigma}$ la restriction de σ à K'. Comme $\sigma(\mathfrak{P}) = \mathfrak{P}$ et $\sigma(K') = K'$, on a $\tilde{\sigma}(\mathfrak{P} \cap K') = \mathfrak{P} \cap K'$ et donc $\tilde{\sigma}$ appartient au groupe de décomposition de $\mathfrak{P} \cap K'$ sur K. De plus on a évidemment

$$\tilde{\sigma}(x) \equiv x^q \pmod{\mathfrak{P} \cap K'} \quad \text{pour tout } x \in \mathbb{Z}_L \cap K'.$$

Cela démontre ii). □

2.4 Le théorème de Tchébotarev

Nous allons enfin récolter les fruits de toute cette construction et énoncer un théorème de densité comme annoncé à la fin du chapitre 1. Définissons tout d'abord la notion de densité naturelle d'un ensemble de nombres premiers.

Définition 6 *Soit S un ensemble de nombres premiers. On dit que S admet une densité naturelle δ si la limite du rapport*

$$\frac{\text{card}\,\{p \in S \text{ tel que } p \leq n\}}{\text{card}\,\{p \text{ premier tel que } p \leq n\}}$$

tend vers δ lorsque n tend vers $+\infty$.

On peut remarquer qu'un ensemble S fini est de densité nulle. Ainsi un ensemble S de nombres premiers admettant une densité non nulle est infini.

Nous pouvons maintenant énoncer, sans démonstration, le théorème de Tchébotarev.

Théorème 7 *Soit K une extension galoisienne finie de $\mathbb{Q}$ de groupe de Galois G ; soit C une classe de conjugaison de G et S un ensemble de nombres premiers dont le symbole d'Artin est égal à C. Alors S admet une densité égale à* $\dfrac{\text{card}\,(S)}{\text{card}\,(G)}$.

Ce théorème est très fort et nous allons tout de suite nous en rendre compte en l'appliquant au cas cyclotomique : soit ℓ un entier premier avec k ; tout nombre premier p congru à $\ell \pmod{k}$ admet pour symbole d'Artin l'automorphisme $\zeta_k \mapsto \zeta_k^\ell$ (voir l'exemple plus haut) dont la classe de conjugaison est réduite à lui-même puisque $\text{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$ est abélien. Ce dernier est de cardinal $\varphi(k)$. Le théorème de Tchébotarev redonne ainsi le théorème des nombres premiers en progression arithmétique (sans terme d'erreur) à savoir :

$$\pi(x, \ell, k) \sim \frac{\pi(x)}{\varphi(k)} \qquad \text{quand } x \to +\infty.$$

On peut donc voir le théorème de Tchébotarev comme une généralisation du théorème de Dirichlet. La démonstration de ce théorème utilise d'ailleurs les fonctions L de Hecke, qui généralisent les fonctions L de Dirichlet à des corps de nombres.

Permettons-nous à ce stade, une petite disgression historique. Frobenius s'est intéressé à la factorisation d'un polynôme modulo des nombres premiers et est parvenu à faire correspondre la proportion des nombres premiers qui réalise un type de décomposition et la proportion des éléments du groupe de Galois qui se décomposent de la même manière en produits de cycles.

Précisément on considère un polynôme f de degré n à coefficients entiers de discriminant non nul. On dira que f a une décomposition de type $(n_1, ..., n_t)$ modulo p si f se factorise modulo p en un produit de t facteurs irréductibles distincts de degrés respectifs n_i (on écarte d'emblée les cas exceptionnels où les facteurs ne sont pas distincts, c'est-à-dire lorsque p est ramifié).

On note K un corps de décomposition de f. Le groupe de Galois G de $K/\mathbb{Q}$ peut-être vu comme un sous-groupe du groupe symétrique d'ordre n. Tout élément σ de G se factorise en un produit de cycles disjoints et si on note n_i la longueur de chacun de ces cycles, on dit que σ est de type $(n_1, ..., n_t)$. On peut alors énoncer le théorème de Frobenius :

Théorème 8 *La densité naturelle de l'ensemble des nombres premiers p pour lesquels f a une factorisation de type $(n_1, ..., n_t)$ modulo p existe et vaut $\dfrac{\text{card}\,(T)}{\text{card}\,(G)}$ où T est l'ensemble des éléments de G de type $(n_1, ..., n_t)$.*

Nous pouvons ainsi retrouver le théorème de Dirichlet pour les progressions modulo 12. En effet la factorisation modulo p du polynôme $X^{12}-1$ pour $p \equiv 1 \pmod{12}$ (resp. 5,7,11 $\pmod{12}$) est de type $(1,1,1,1,1,1,1,1,1,1,1,1)$ (resp. $(1,1,1,1,2,2,2,2)$, $(1,1,1,1,1,1,2,2,2)$, $(1,1,2,2,2,2,2)$).

Cependant ce résultat ne nous permet pas par exemple de conclure pour les progressions modulo 10 : si l'on considère le polynôme $X^{10}-1$ on peut observer que la factorisation modulo des nombres premiers congrus à 3 ou à 7 $\pmod{10}$ est de même type, à savoir $(1,1,4,4)$.

D'où l'idée de Tchébotarev de préciser cette correspondance entre la factorisation modulo un nombre premier d'un polynôme et son groupe de Galois : conformément à l'idée de Frobenius, on considère les éléments du groupe de Galois qui préservent un facteur irréductible de f et donc permutent ses racines : ils constituent le groupe de décomposition. On construit alors un générateur canonique de ce groupe, l'automorphisme de Frobenius, qui nous permet de différencier dans le cas cyclotomique des nombres premiers appartenant à des classes de congruence différentes. En revanche le théorème de Frobenius ne fait pas à ce stade de distinction entre des factorisations de même type.

Chapitre 3

Les premiers totalement décomposés

3.1 Sous-extensions et factorisation des nombres premiers

Dans le chapitre 2, nous avons vu que les groupes de décomposition des idéaux premiers au-dessus d'un nombre premier p nous permettent de contrôler le type de factorisation d'un nombre premier totalement décomposé. Nous allons voir qu'ils permettent aussi de contrôler la factorisation dans une extension intermédiaire.

Proposition 7 *Soit $\mathbb{Q} \subseteq K \subseteq L$ des extensions de $\mathbb{Q}$, $L/\mathbb{Q}$ étant galoisienne de groupe de Galois G. On note H le groupe de Galois de L/K. Si p est un nombre premier non ramifié dans L, les deux conditions suivantes sont équivalentes :*
i) p est totalement décomposé dans K.
ii) p a dans L un facteur premier $\mathfrak{P}$ tel que

$$D_{\mathfrak{P}} \subseteq \bigcap_{\sigma \in G} \sigma H \sigma^{-1}.$$

Démonstration. Soit p premier non ramifié dans L, $\mathfrak{P}$ un idéal premier de L divisant p. Son groupe de décomposition $D_{\mathfrak{P}}$ est de cardinal $f = f(\mathfrak{P}/p)$. Soit également $\mathfrak{p}$ un idéal premier de K tel que $\mathfrak{P} \mid \mathfrak{p} \mid p$. Le groupe de décomposition de $\mathfrak{P}$ sur K est :

$$D_K(\mathfrak{P}) = \{\sigma \in H | \, \sigma(\mathfrak{P}) = \mathfrak{P}\} = H \cap D_{\mathfrak{P}}.$$

Disons que $d := \text{card } D_K(\mathfrak{P})$. On a alors :

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^d.$$

De plus $N_{L/\mathbb{Q}}(\mathfrak{P}) = p^f$. On en déduit que

$$f(\mathfrak{p}/p) = \frac{f}{d}.$$

Supposons maintenant que p est totalement décomposé dans K. Soit $\mathfrak{P} \mid p$ dans L et $\sigma \in G$; on pose $\mathfrak{Q} = \sigma(\mathfrak{P})$. Si $\mathfrak{p} = \mathfrak{Q} \cap K$, alors d'après ce qui précède $f(\mathfrak{p}/p) = \frac{f}{d} = 1$ avec $f = \text{card } D_\mathfrak{Q}$ et $d = \text{card } D_\mathfrak{Q} \cap H$. Ainsi $D_\mathfrak{Q} \subseteq H$ et par suite,

$$D_\mathfrak{P} = \sigma^{-1} D_\mathfrak{Q} \sigma \subseteq \sigma^{-1} H \sigma.$$

Réciproquement supposons qu'il existe un idéal premier $\mathfrak{P}$ qui divise p dans L et dont le groupe de décomposition est inclus dans $\cap_{\sigma \in G} \sigma H \sigma^{-1}$. Comme l'extension L est galoisienne, les groupes de décomposition des facteurs premiers de p sont conjugués deux à deux (proposition 5). Donc tous les facteurs de p dans L ont leur groupe de décomposition inclus dans $\sigma H \sigma^{-1}$ pour tout $\sigma \in G$. Maintenant si $\mathfrak{p}|p$ dans K et $\mathfrak{P}|\mathfrak{p}$ dans L alors $f(\mathfrak{p}/p) = \frac{f}{d}$ et l'hypothèse implique avec $\sigma = \text{id}_L$ que $f = d$, soit $f(\mathfrak{p}/p) = 1$ et donc p est totalement décomposé dans K.

□

On peut démontrer de la même manière la proposition suivante :

Proposition 8 *Sous les mêmes hypothèses que celles de la proposition précédente, si p est un nombre premier non ramifié dans L, les deux conditions suivantes sont équivalentes :*
i) p admet un facteur premier de degré 1 dans K.
ii) p a dans L un facteur premier $\mathfrak{P}$ pour lequel il existe $\sigma \in G$ tel que $D_\mathfrak{P} \subseteq \sigma H \sigma^{-1}$.

On va déduire de ces propositions un résultat dû à Bauer [1] permettant de comparer deux extensions en y étudiant la factorisation des nombres premiers.

Théorème 9 (Bauer) *Soit $L/\mathbb{Q}$ une extension galoisienne de groupe de Galois G. On considère deux sous-extensions K_1 et K_2 et on suppose que $K_2/\mathbb{Q}$ est galoisienne. Les deux assertions suivantes sont équivalentes :*
i) à un nombre fini d'exceptions près, tout nombre premier ayant un facteur premier de degré 1 dans K_1 est totalement décomposé dans K_2.
ii) $K_2 \subseteq K_1$.

Démonstration. On remarque d'abord que H_2 est distingué dans G puisque $K_2/\mathbb{Q}$ est galoisienne. Notons $H_i = \mathrm{Gal}(L/K_i)$. Par correspondance de Galois, on a

$$K_2 \subseteq K_1 \Leftrightarrow H_1 \subseteq H_2 \Leftrightarrow \sigma H_1 \sigma^{-1} \subseteq \sigma H_2 \sigma^{-1} = H_2, \forall \sigma \in G.$$

Supposons que $K_2 \subseteq K_1$. Soit p un premier possédant un facteur de degré 1 dans K_1. Il existe donc $\mathfrak{P}$ qui divise p dans K_1 et $\sigma \in G$ tel que $D(\mathfrak{P}) \subseteq \sigma H_1 \sigma^{-1}$ d'après la proposition 8. On a alors :

$$D(\mathfrak{P}) \subseteq \sigma H_1 \sigma^{-1} \subseteq H_2 = \bigcap_{\tau \in G} \tau H_2 \tau^{-1}.$$

Et donc d'après la proposition 7, p est totalement décomposé dans K_2.

Supposons réciproquement que l'assertion i) soit vraie. Soit $\mathbb{G}$ un sous-groupe cyclique de H_1. En vertu du théorème de Tchébotarev, il existe (une infinité de) p premier ayant un facteur $\mathfrak{P}$ de p dans K_1 tel que $D(\mathfrak{P}) = \mathbb{G} \subseteq H_1$. Donc p admet un facteur de degré 1 (proposition 8), il est donc totalement décomposé dans K_2, donc il existe (proposition 7) $\sigma \in G$ tel que $\mathbb{G} \subseteq \sigma H_2 \sigma^{-1} = H_2$. Maintenant si $\tau \in H_1$ alors $< \tau > \subseteq H_2$ et donc $\tau \in H_2$. □

3.2 Le cas des sous extensions cyclotomiques

Dans toute cette partie, les lettres ℓ et k désignent des entiers premiers entre eux tels que $\ell^2 \equiv 1 \pmod{k}$. On désignera par ζ_k (et parfois ζ lorsqu'il n'y aura pas d'ambiguïté) une racine primitive k-ème de l'unité. On rappelle que l'extension $\mathbb{Q}(\zeta_k)$ est galoisienne sur $\mathbb{Q}$ et que son groupe de Galois est isomorphe à $(\mathbb{Z}/k\mathbb{Z})^*$. Le théorème 10 généralise la proposition 2.

Théorème 10 *Soit H un sous groupe de $(\mathbb{Z}/k\mathbb{Z})^*$. Soit p un nombre premier qui ne divise pas k ; alors les deux conditions suivantes sont équivalentes :*
i) p est totalement décomposé dans l'extension $\mathbb{Q}(\zeta_k)^H$ invariante sous l'action de H,
ii) p appartient à une classe résiduelle de H.

Démonstration. Soit p un nombre premier ne divisant pas k ; il est donc non ramifié dans $\mathbb{Q}(\zeta_k)$. On a alors la suite d'équivalences suivante :

$$\begin{array}{ccc} p \text{ est totalement} & & \text{il existe } \mathfrak{P} \text{ qui divise } p \\ \text{décomposé dans } \mathbb{Q}(\zeta_k)^H & \Leftrightarrow & \text{dans } \mathbb{Q}(\zeta_k) \text{ tel que } D_{\mathfrak{P}} \subseteq H \\ & \Leftrightarrow & (p, \mathbb{Q}(\zeta_k)/\mathbb{Q}) \in H \\ & \Leftrightarrow & p \text{ appartient à une classe de } H \end{array}$$

La première équivalence découle de la proposition 7 et du fait que $(\mathbb{Z}/k\mathbb{Z})^*$ est un groupe abélien ; la deuxième du fait que $D_{\mathfrak{P}}$ est engendré par l'automorphisme de Frobenius qui est ici le symbole d'Artin de p puisque que l'on est dans une extension abélienne ; enfin la troisième se déduit du calcul du symbole d'Artin dans une extension cyclotomique effectué dans le chapitre précédent. □

En vue de la construction d'une preuve euclidienne, nous pouvons expliciter un polynôme de $\mathbb{Z}[x]$ dont un corps de rupture est la sous-extension cyclotomique fixée par H.

Théorème 11 *Soit H un sous-groupe de $(\mathbb{Z}/k\mathbb{Z})^*$; il existe un polynôme f dont les diviseurs premiers sont, à un nombre fini d'exceptions près, les premiers dont la classe appartient à H. Les éventuels diviseurs premiers exceptionnels sont les diviseurs premiers de k et de $Disc(f)$.*

Démonstration. Pour construire ce polynôme, nous allons construire un élément primitif de l'extension $\mathbb{Q}(\zeta_k)^H/\mathbb{Q}$, en gardant un degré de liberté afin de pouvoir contrôler ultérieurement $f(0)$.

On sait que, si $s = \varphi(k)/\operatorname{card} H$,

$$\operatorname{Gal}(\mathbb{Q}(\eta)/\mathbb{Q}) \simeq (\mathbb{Z}/k\mathbb{Z})^*/H = \{m_1H, ..., m_sH\}$$

où les m_i sont des représentants adéquats. Si pour un entier u quelconque, on pose

$$g(u, \zeta_k) = \prod_{h\in H}(u - \zeta_k^h).$$

Pour tout entier u et tout $\sigma \in H$, on a $\sigma(g(u, \zeta_k)) = g(u, \zeta_k)$. Par suite, $\mathbb{Q}(g(u, \zeta_k)) \subset \mathbb{Q}(\zeta_k)^H$. Il s'ensuit que $g(u)$ est un élément primitif pour $\mathbb{Q}(\zeta_k)$ à condition qu'il possède s conjugués dans $\mathbb{Q}(\zeta_k)$. Pour cela il suffit de montrer que les $\eta_i = g(u, \zeta_k^{m_i})$ pour $1 \leq i \leq s$ sont des conjugués distincts de $g(u, \zeta_k)$. Supposons par exemple que

$$\prod_{h\in H}(u - \zeta_k^{m_1h}) = \prod_{h\in H}(u - \zeta_k^{m_2h}) \tag{3.1}$$

Le polynôme $\prod_{h\in H}(u-\zeta_k^{m_1h})-\prod_{h\in H}(u-\zeta_k^{m_2h})$ de $\mathbb{C}[u]$ est nul si et seulement si $m_1m_2^{-1} \in H$ ce qui est exclu d'après le choix des représentants des classes distinctes. L'équation (3.1) n'admet donc qu'un nombre fini de solutions, il suffit donc d'écarter un nombre fini de valeurs de u pour assurer que

$$\mathbb{Q}(\zeta_k)^H = \mathbb{Q}(g(\zeta_k)).$$

On pose à présent :

$$f(x) = \prod_{i=1}^{s} (x - \eta_i).$$

Le polynôme f est invariant sous l'action de $\mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$ donc $f \in \mathbb{Q}[x]$. De plus les coefficients de f sont des entiers de $\mathbb{Q}(\eta)$ et donc finalement $f \in \mathbb{Z}[x]$. La conclusion provient alors du théorème 10 et de la proposition 4. $\square$

Chapitre 4

Fin de la démonstration

4.1 Construction d'une preuve euclidienne dans le cas où $\ell^2 \equiv 1 \pmod{k}$

Le théorème 11 va nous permettre de conclure très rapidement.

Proposition 9 *Si $\ell^2 \equiv 1 \pmod{k}$, alors il existe un polynôme vérifiant les conditions a) et b) du lemme 2.*

Démonstration. D'après le théorème 11 appliqué au sous-groupe $H = \{1, \ell\}$, il existe un polynôme f de $\mathbb{Z}[x]$ vérifiant la condition a) du lemme 2 ; il s'écrit :

$$f(x) = \prod_{i=1}^{s} (x - (u - \zeta^{m_i})(u - \zeta^{\ell m_i})),$$

où u est un paramètre entier pour lequel il n'y a qu'un nombre fini de valeurs à éviter.

Vu que $\varphi(k)$ est pair, $f(0) = \phi_k(u)$. On peut choisir u de manière à ce qu'il soit un multiple de k. Dès lors :

$$f(0) = \phi_k(u) \equiv \phi_k(0) = 1 \pmod{k}$$

dès que $k \geq 2$. La proposition 2 nous indique que tous les diviseurs premiers de $\phi_k(u)$ donc de $f(0)$ divisent k ou sont congrus à 1 (mod k). Mais la première possibilité est exclue puisque $f(0) \equiv 1 \pmod{k}$. Cela nous donne donc bien la condition b) du lemme 2. □

Pour conclure il suffit alors d'exhiber un premier congru à $\ell \pmod{k}$ qui ne divise pas le discriminant du polynôme construit à l'instant.

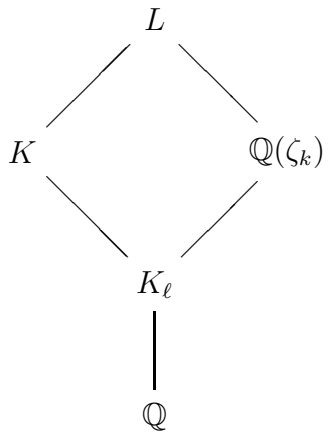
4.2 La réciproque

Théorème 12 *Soit f un polynôme irréductible de $\mathbb{Z}[x]$ dont tous les diviseurs premiers (à l'exception d'un nombre fini) sont congrus à 1 ou à ℓ* (mod k). *Alors $\ell^2 \equiv 1 \pmod{k}$.*

Démonstration. On considère K un corps de rupture de f. Nous allons étudier les diviseurs premiers de f *via* leur factorisation dans une extension de $\mathbb{Q}$: la factorisation d'un premier p dans K permet de contrôler s'il est ou non un diviseur premier de f, et sa factorisation dans une sous-extension cyclotomique permet de contrôler sa classe de congruence modulo k. Plus précisément, on va chercher à montrer que, comme dans le cas cyclotomique, à un ensemble fini d'exceptions près, les classes modulo k des diviseurs de f forment un sous-groupe de $(\mathbb{Z}/k\mathbb{Z})^*$. En particulier, s'il existe une infinité de diviseurs premiers congrus à 1 ou $\ell \pmod{k}$, il existe aussi une infinité congrus à $\ell^2 \pmod{k}$, ce qui nous permettra de conclure.

À cet effet, nous introduisons K_ℓ, la sous-extension de $\mathbb{Q}(\zeta_k)$ fixée par $< \ell >$. À ce stade on peut remarquer que $K_\ell \subseteq K$. En effet, si p admet un facteur premier de degré 1 dans K alors c'est un diviseur de f donc $p \equiv 1$ ou $\ell \pmod{k}$. Or, d'après le théorème 10, les premiers totalement décomposés dans H_ℓ sont les premiers congrus à une classe de $< \ell >$ modulo k (tout cela à un nombre fini d'exceptions près). Le théorème 9 permet alors de conclure.

Il est plus commode d'étudier les facteurs premiers de K dans une extension galoisienne, situation où l'on peut utiliser le théorème de Tchébotarev. On introduit donc le corps $L = K(\zeta_k)$ et ainsi l'extension L/K est galoisienne. Nous avons donc le diagrammme suivant :



Nous allons maintenant comparer les deux extensions L/K et $\mathbb{Q}(\zeta_k)/K_\ell$ *via* leur groupe de Galois. Pour cela on considère l'application :

$$\begin{array}{rccc} T: & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_k)/K_\ell) \\ & \sigma & \longmapsto & \sigma_{|\mathbb{Q}(\zeta_k)} \end{array}$$

L'application T est bien définie car :
- Si $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\zeta_k)^k = 1$ donc $\sigma(\zeta_k) = \zeta_k^t$ où t est un entier naturel. Ainsi $\sigma(\mathbb{Q}(\zeta_k)) \subseteq \mathbb{Q}(\zeta_k)$;
- Si l'automorphisme σ est trivial sur K, il l'est aussi sur K_ℓ.

L'application T est clairement injective : si σ est trivial sur K et sur $\mathbb{Q}(\zeta_k)$ il l'est aussi sur L.

Montrons maintenant que T est surjective. Comme $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/K_\ell)$ est cyclique engendré par σ_ℓ, où σ_ℓ est défini par $\zeta_k \mapsto \zeta_k^\ell$, il suffit de montrer que σ_ℓ admet un antécédent par T. Par hypothèse, f a une infinité de diviseurs premiers dans la classe $\ell \pmod k$, et ceux-là, excepté un nombre fini d'entre eux, admettent un facteur premier de degré 1 dans K (proposition 4).

Soit $p \equiv \ell \pmod k$ un diviseur de f admettant un facteur premier $\mathfrak{P}$ de degré 1 dans K. Par le lemme 1, il admet un facteur premier $\mathfrak{p}$ de degré 1 dans K_ℓ. Soit $\mathfrak{Q}$ un facteur premier de $\mathfrak{P}$ dans L, et posons $\mathfrak{q} = \mathfrak{Q} \cap \mathbb{Q}(\zeta_k)$ idéal premier de $\mathbb{Q}(\zeta_k)$ qui divise $\mathfrak{p}$.

Tout d'abord on a vu que :

$$\sigma_\ell = (\mathfrak{q}, \mathbb{Q}(\zeta_k)/\mathbb{Q}).$$

Mais d'après le i) de la proposition 6 ,

$$(\mathfrak{q}, \mathbb{Q}(\zeta_k)/K_\ell) = (\mathfrak{q}, \mathbb{Q}(\zeta_k)/\mathbb{Q}) = \sigma_\ell,$$

car $\mathfrak{p}$ est de degré 1.

Par ailleurs

$$(\mathfrak{Q}, L/K) = (\mathfrak{Q}, L/K_\ell)$$

toujours d'après le i) de la proposition 6, car $f(\mathfrak{P}/\mathfrak{p}) = \frac{f(\mathfrak{P}/p)}{f(\mathfrak{p}/p)} = 1$. De plus d'après le ii) de la proposition 6,

$$(\mathfrak{Q}, L/K_\ell)_{|\mathbb{Q}(\zeta_k)} = (\mathfrak{q}, \mathbb{Q}(\zeta_k)/K_\ell).$$

Ainsi

$$(\mathfrak{Q}, L/K)_{|\mathbb{Q}(\zeta_k)} = \sigma_\ell$$

et la surjectivité est prouvée. Ainsi $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_k)/K_\ell)$.

Nous allons maintenant appliquer le théorème de Tchébotarev pour évaluer la proportion de diviseurs premiers de f suivant leur classe de congruence.

Soit $\sigma \in \mathrm{Gal}(L/K)$ et soit E une clôture galoisienne de L dans $\mathbb{Q}$; on prolonge arbitrairement σ à un élément $\tilde{\sigma}$ de $\mathrm{Gal}(E/\mathbb{Q})$. Par le théorème de Tchébotarev, il existe une infinité de nombres premiers p dont le symbole d'Artin $(p, E/\mathbb{Q})$ est la classe de conjugaison de $\tilde{\sigma}$ dans $\mathrm{Gal}(E/\mathbb{Q})$. Si p est un tel premier, d'après le théorème 5 il existe un facteur premier $\mathfrak{Q}$ de p dans E tel que $(\mathfrak{Q}, E/\mathbb{Q}) = \tilde{\sigma}$. On en déduit alors que :

$$D_{\mathfrak{Q}} =< \tilde{\sigma} > \subseteq \mathrm{Gal}(E/K),$$

puisque $D_{\mathfrak{Q}}$ est cyclique et engendré par $(\mathfrak{Q}, E/\mathbb{Q})$. Donc d'après la proposition 8, l'idéal premier $\mathfrak{p} = K \cap \mathfrak{Q}$ est de degré 1 sur K (la preuve de la proposition 8 montrerait que le facteur de degré 1 en question est effectivement $K \cap \mathfrak{Q}$). D'après le i) de la proposition 6, on a donc :

$$(\mathfrak{P}, E/K) = (\mathfrak{Q}, E/\mathbb{Q}).$$

Il ne reste plus qu'à considérer l'idéal premier $\mathfrak{P} = \mathfrak{Q} \cap L$ et à appliquer le ii) de la proposition 6 pour obtenir :

$$(\mathfrak{P}, L/K) = (\mathfrak{Q}, E/K)_{|L} = \tilde{\sigma}_{|L} = \sigma.$$

Il existe donc une infinité d'idéaux premiers de K de degré 1 dont le symbole d'Artin est un élémemt quelconque de $\mathrm{Gal}(L/K)$. Par surjectivité de T, il existe une infinité d'idéaux premiers de K de degré 1 dont le symbole d'Artin se restreint à un élément quelconque de $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/K_\ell) =< \ell >$. En particulier il existe une infinité de diviseurs premiers de f congrus à $\ell^2 \pmod{k}$. Cela implique que $\ell^2 \equiv 1 \pmod{k}$ ou $\ell^2 \equiv \ell \pmod{k}$, mais la deuxième possibilité est exclue puisque ℓ et k sont premiers entre eux, ce qui achève la preuve.

□

Bibliographie

[1] M. Bauer – « Zur Theorie der algebraischen Zahlkörper », *Math. Ann.* **77** (1916), no. 3, p. 353–356.

[2] I. Gerst et J. Brillhart – « On the prime divisors of polynomials », *Amer. Math. Monthly* **78** (1971), p. 250–266.

[3] R. Murty – « Primes in certain arithmetic progression », *Journal of Madras University* **51** (1988), p. 161–169.

[4] P. Ribenboim – *Classical theory of algebraic numbers*, Universitext, Springer-Verlag, New York, 2001.

[5] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[6] I. Schur – « Über die existenz unendlich vieler primzahlen in einiger arithmetischen progressionen », *S-B Berlin Math. Ges.* **11** (1912), p. 40–50.

[7] P. Stevenhagen et H. W. Lenstra, Jr. – « Chebotarëv and his density theorem », *Math. Intelligencer* **18** (1996), no. 2, p. 26–37.

[8] B. F. Wyman – « What is a reciprocity law ? », *Amer. Math. Monthly* **79** (1972), p. 571–586 ; correction, ibid. 80 (1973), 281.