Proyecciones
Vol. 19, N^o 1, pp. 53-63, May 2000
Universidad Católica del Norte
Antofagasta - Chile
DOI: 10.4067/S0716-09172000000100005

CORPS DE NOMBRES D'INDICE DIVISIBLE PAR UN ENTIER DONNÉ, DANS FACTEUR CARRÉ

DENIS HÉMARD
Univ. de Valenciennes et du Hainaut Cambrésis, France

Abstract

If K is a number field, $\mathcal{O}_K$ its ring of integers and $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$, the index of α is the index of abelian groups $ind\alpha = (\mathcal{O}_K : \mathbf{Z}[\alpha]) \in \mathbf{N}$ and the index $i(K)$ of K is the gcd of these $ind\alpha$. We show a way to construct via Hilbert class fields of quadratic number fields, for any integer n without square factor, an infinite family of number fields K with $i(K)$ divisible by n.

Introduction

Le paragraphe 1 présente une variante de l'interprétation habituelle de la notion d'indice, qui permet une démonstration simplifiée d'un théorème de Dedekind et d'un de ses corollaires (corollaire 2) (on pourra consulter [N] ou [H] pour une autre présentation).

Le paragraphe 2 se base sur ce corollaire pour construire des corps de nombres d'indice divisible par un entier donné sans facteur carré. On les obtient comme sous-corps (laissés fixes par certains sous-groupes de Galois) de corps de classes de Hilbert de certaines extensions quadratiques de $\mathbf{Q}$. Et un résultat de Yamamoto [Y] nous assure l'existence d'une infinité de telles extensions quadratiques.

Le fait qu'il y ait une infinité de corps de nombres d'indice divisible par un entier donné sans facteur carré était déjà connu de M. Bauer en 1907 ([B]). Sa méthode basée sur les polygones de Newton et le corollaire déjà cité, fournit des polynômes irréductibles définissant de telles extensions. Il nous a semblé utile d'en rappeler le principe dans un appendice. (Voir également, pour d'autres résultats sur l'indice, les références données dans [N] p198)

1. Le théorème de Dedekind

Soient K un corps de nombre de degré n sur $\mathbf{Q}$, $\mathcal{O}_K$ son anneau d'entiers et $\alpha \in \mathcal{O}_K$ tel que $K = \mathbf{Q}(\alpha)$ ($\simeq \frac{\mathbf{Q}[X]}{(P)}$ où $P = Irr(\alpha, \mathbf{Q}) \in \mathbf{Z}[X]$ est le polynôme minimal de α sur $\mathbf{Q}$). On sait que $\mathcal{O}_K$ est un $\mathbf{Z}$-module libre de rang n et $\mathbf{Z}[\alpha] \simeq \frac{\mathbf{Z}[X]}{(P)}$ un sous $\mathbf{Z}$-module libre de même rang ; d'où la notion d'indice :
$ind\alpha = |\frac{\mathcal{O}}{\mathbf{Z}[\alpha]}| = (\mathcal{O}_K : \mathbf{Z}[\alpha]) = \prod_{i=1}^{r} m_i$ où $m_r | m_{r-1} | \dots | m_1$ sont les facteurs invariants ($\neq 1$) du sous $\mathbf{Z}$-module $\mathbf{Z}$ de $\mathcal{O}_K$.

Définition :

On appelle indice de $K/\mathbf{Q}$ l'entier $i(K) = pgcd\{ind\alpha; \quad \alpha \in \mathcal{O}_K, \mathbf{Q}(\alpha) = K\}$.

Remarque :

En choisissant une $\mathbf{Z}$-base $(e_1, \ldots, e_n)$ de $\mathcal{O}_K$ de telle sorte que $(m_1 e_1, \ldots, m_n e_n)$ soit une $\mathbf{Z}$-base de $\mathbf{Z}[\alpha]$ (avec $m_{r+1} = \cdots = m_n = 1$) , on voit que les discriminants vérifient l'égalité :

$$(ind\alpha)^2 disc(\mathcal{O}_K/\mathbf{Z}) = disc(\mathbf{Z}[\alpha]/\mathbf{Z}).$$

D'où le fait que les diviseurs de l'indice $i(K)$ soient généralement désignés en allemand, par "außerwesentliche Diskriminantenteiler" et en anglais, par "(common) inessential discriminantal divisor" (ils divisent tous les $disc(\mathbf{Z}[\alpha]/\mathbf{Z})$ sans nécessairement diviser $disc(\mathcal{O}_K/\mathbf{Z})$).

Après tensorisation par $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ (p premier $\in \mathbf{N}$), l'isomorphisme $\frac{\mathbf{Z}[X]}{(P)} \simeq \mathbf{Z}[\alpha]$ et l'injection canonique $\mathbf{Z}[\alpha] \hookrightarrow \mathcal{O}_K$ fournissent les morphismes

$$\frac{\mathbf{F}_p[X]}{(\overline{P})} \simeq \frac{\mathbf{Z}[\alpha]}{p\mathbf{Z}[\alpha]} \xrightarrow{\varphi_\alpha} \frac{\mathcal{O}_K}{p\mathcal{O}_K}$$

de $\mathbf{F}_p$-algèbres de même $\mathbf{F}_p$-dimension n (où $\overline{P}$ = image de P dans $\mathbf{F}_p[X]$).

Lemme :

a) $p \nmid ind\alpha \Leftrightarrow \varphi_\alpha$ est un isomorphisme.

b) $p \nmid i(K) \Leftrightarrow \frac{\mathcal{O}_K}{p\mathcal{O}_K}$ est une $\mathbf{F}_p$-algèbre monogène.

Démonstration :

a) $p \nmid ind\alpha \Leftrightarrow \frac{\mathcal{O}_K}{\mathbf{Z}[\alpha]} \otimes \mathbf{F}_p = 0 \Leftrightarrow \varphi_\alpha$ surjectif

$\Leftrightarrow \varphi_\alpha$ isomorphisme (par égalité des $\mathbf{F}_p$-dimensions)

b) $p \nmid i(K) \Leftrightarrow \exists \alpha \in \mathcal{O}_K,\ \mathbf{Q}(\alpha) = K$ et φ_α isomorphisme (par a))

$\Leftrightarrow \mathcal{O}_K/p\mathcal{O}_K$ $\mathbf{F}_p$-algèbre monogène (engendrée par $\alpha \, mod \, p\mathcal{O}_K$).

(Pour le sens $\Leftarrow$, on remarque que si les n premières puissances de α sont $\mathbf{F}_p$-linéairement indépendantes modulo $p\mathcal{O}_K$, on a $deg(Irr(\alpha, \mathbf{Q})) = n$ et donc $\mathbf{Q}(\alpha) = K$).

Corollaire 1 (Théorème de Dedekind) :

Si $p \nmid ind\alpha$, soit $\overline{P} = \prod_{i=1}^{s} \overline{Q}_i^{r_i}$ la décomposition en irréductibles unitaires de l'image $\overline{P}$ de $P = Irr(\alpha, \mathbf{Q})$ dans $\mathbf{F}_p[X]$ (et les Q_i unitaires, antécédents de $\overline{Q}_i$ dans $\mathbf{Z}[X]$) ; alors

a) les idéaux de $\mathcal{O}_K$, $p_i = (p, Q_i(\alpha))$, sont les idéaux premiers de $\mathcal{O}_K$ au dessus de p ; il y en a donc s.

b) $deg\, Q_i = f(p_i/p)$ (le degré résiduel)

c) $r_i = ep_i/p$ (l'indice de ramification) pour tout $i \in \{1, \ldots, s\}$.

(En particulier, si $p \nmid i(K)$, la décomposition de p dans $\mathcal{O}_K$ est complètement déterminée par la connaissance d'un α tel que $p \nmid ind\alpha$.)

Démonstration :

Par hypothèse, l'application

$$\begin{array}{c} \frac{\mathbf{F}_p[X]}{(\overline{P})} \longrightarrow \frac{\mathcal{O}_K}{p\mathcal{O}_K} \\ \overline{Q} mod\left(\overline{P}\right) \longmapsto Q(\alpha)\, mod p\mathcal{O}_K \end{array}$$

(indépendante du choix de l'antécedent $Q \in \mathbf{Z}[X]$, de $\overline{Q}$)

est un isomorphisme de $\mathbf{F}_p$-algèbres.

On en déduit une correspondance bijective entre idéaux premiers de $\mathbf{F}_p[X]$ contenant $\overline{P}$ et idéaux premiers de $\mathcal{O}_K$ contenant p ; d'où a) puisque les idéaux premiers de $\mathbf{F}_p[X]$ contenant $\overline{P}$ sont les $(\overline{Q}_i)$, $i = 1, \ldots, s$. b) s'en déduit car

$$deg\, \overline{Q}_i = dim \frac{\mathbf{F}_p[X]/(\overline{P})}{(\overline{Q}_i)/(\overline{P})} = dim \frac{\mathcal{O}_K/p\mathcal{O}_K}{(Q_i(\alpha), p)/p\mathcal{O}_K} = f(p_i/p)$$

ainsi que c), car dans $\frac{\mathbf{F}_p[X]}{(\overline{P})}$, il y a exactement $r_i + 1$ puissances distinctes de l'idéal engendré par $\overline{Q}_i\ mod(\overline{P})$ (correspondant aux exposants $0, 1, \ldots, r_i$). ∎

Corollaire 2 :

Soit $p\mathcal{O}_K = p_1^{e_1} \ldots p_s^{e_s}$ la décomposition dans $\mathcal{O}_K$ d'un p premier $\in \mathbf{N}$ et $f_i = f(p_i/p)$, pour $i = 1, \ldots, s$; alors

$$p \nmid i(K) \Leftrightarrow \exists P_1, \ldots, P_s \in \mathbf{F}_p[X], \text{ irréductibles, unitaires, distincts, de degré } f_1, ..., f_s \text{ respectivement.}$$

Démostration :
$\Rightarrow$) : $\exists \alpha \in \mathcal{O}_K,\ p \dagger ind\alpha$; on applique alors le corollaire 1.
$\Leftarrow$) : Comme extensions (de corps) de même degré sur $\mathbf{F}_p$, on a des isomorphismes de $\mathbf{F}_p$-algèbres :

$$\frac{\mathcal{O}_K}{p_i} \simeq \frac{\mathbf{F}_p[X]}{(P_i)} \qquad \forall i = 1, \ldots, s.$$

Par un petit lemme (démontré ci-dessous), on en déduit des isomorphismes de $\mathbf{F}_p$-algèbres :

$$\frac{\mathcal{O}_K}{p_i^{e_i}} \simeq \frac{\mathbf{F}_p[X]}{(P_i^{e_i})} \qquad \forall i = 1, \ldots, s.$$

Par application du théorème chinois, il en résulte des isomorphismes de $\mathbf{F}_p$-algèbres :

$$\frac{\mathbf{F}_p[X]}{(P_1^{e_1} \ldots P_s^{e_s})} \simeq \prod_{i=1}^{s} \frac{\mathbf{F}_p[X]}{(P_i^{e_i})} \simeq \prod_{i=1}^{s} \frac{\mathcal{O}_K}{p_i^{e_i}} \simeq \frac{\mathcal{O}_K}{p\mathcal{O}_K}.$$

En particulier $\frac{\mathcal{O}_K}{p\mathcal{O}_K}$ est une $\mathbf{F}_p$-algèbre monogène et donc $p \dagger i(K)$. $\diamondsuit$ ∎

Démonstration du lemme utilisé :

$$\frac{\mathbf{F}_p[X]}{(P)} \simeq \frac{\mathcal{O}_K}{p} \Rightarrow \frac{\mathbf{F}_p[X]}{(P^r)} \simeq \frac{\mathcal{O}_K}{p^r} \quad \forall r = 1, \ldots, e$$

(on a omis les indices i).

Soit R un relèvement unitaire de P, dans $\mathbf{Z}[X]$; on peut choisir $\alpha \in \mathcal{O}_K$ tel que $R(\alpha) \in p \backslash p^2$. Alors $P^{r-1}(\alpha \, mod \, p^r) = R^{r-1}(\alpha) \, mod \, p^r \neq 0$. Par conséquent, l'homomorphisme de $\mathbf{F}_p[X]$ dans $\mathcal{O}_K/p^r$ qui envoie X sur $\alpha \, mod \, p^r$ est de noyau (P^r) et induit donc l'isomorphisme cherché, par égalité des $\mathbf{F}_p$-dimensions (égalité qu'on peut vérifier par une récurrence et un "dévissage" après avoir localisé $\mathcal{O}_K/p^r$ en p, ce qui ne change rien à ce quotient mais permet de supposer $\mathcal{O}_K$ principal).

Remarque :

On utilisera ce corollaire sous la forme contraposée équivalente (avec les notations supplémentaires $r(f_i) = \#\{p_i | p, f(p_i/p) = f_i\}$ et $g(f_i) = \#\{P \in \mathbf{F}_p[X]$, unitaires, irréductibles et de degré $f_i\}$):

$$p|i(K) \Leftrightarrow \exists i \in \{1, \ldots, s\} \qquad r(f_i) > g(f_i)$$

2. Corps de nombres d'indice divisible par un entier donné sans facteur carré

Soit k une extension galoisienne finie de $\mathbf{Q}$ et H l'extension abélienne de k partout non ramifiée, de degré impair, maximale (dans une clôture algébrique de $\mathbf{Q}$). On notera $\Gamma = Gal(H/k)$ d'ordre $|\Gamma| = m$ (impair) et $Cl'_k = Cl_k/Cl_k(2)$ le quotient du groupe des classes d'idéaux de k par sa partie 2-primaire.

Par maximalité $H/\mathbf{Q}$ est galoisienne et le corps de classes fournit un isomorphisme de $Gal(k/\mathbf{Q})$-modules $Cl'_k \simeq \Gamma$ (qui à la classe $\overline{p}$ d'un idéal premier p associe son Frobenius Frob p dans Γ).

Prenons pour k une extension quadratique de $\mathbf{Q}$. Alors les 2-Sylow de $Gal(H/\mathbf{Q})$ sont d'ordre 2 et n'importe quel élément σ d'ordre 2 dans $Gal(H/\mathbf{Q})$ est un relèvement du générateur τ de $Gal(k/\mathbf{Q})$. En particulier $Gal(H/\mathbf{Q}) = \Gamma \times Gal(k/\mathbf{Q})$. Soit $K = H^{<\sigma>}$ le corps laissé fixe ; alors :

Proposition :

Avec ces notations, pour p premier $\in \mathbf{N}$ et m la partie impaire du nombre de classes de k, on a $p|i(K)$ dans les cas suivants :

a) p ramifié dans $k/\mathbf{Q}$ et $m > 2p - 1$.

b) p inerte dans $k/\mathbf{Q}$ et $m > p^2 - p + 1$.

Démonstration :

Comme τ opère par inversion sur Cl_k et Cl'_k (en particulier toute sous-extension de H/k reste galoisienne sur $\mathbf{Q}$), on a

$$\gamma\sigma\gamma\sigma = \gamma\gamma^{-1} = 1 \qquad \forall \gamma \in \Gamma.$$

Par conséquent, il y a m éléments d'ordre 2 et donc m 2-Sylow dans $Gal(H/\mathbf{Q})$, lesquels sont conjugués par les théorèmes de Sylow ; ce sont donc les ${}^{\gamma}<\sigma>$, $\gamma \in \Gamma$ (où ${}^{\gamma}\sigma = \gamma\sigma\gamma^{-1}$).
Si p ramifié dans $k/\mathbf{Q}$: $p\mathcal{O}_k = p^2 \Rightarrow \overline{p} = 1$ dans $Cl'_k \Rightarrow$ Frob $p = 1$ dans $\Gamma \Rightarrow p\mathcal{O}_H = \mathcal{B}_1 \ldots \mathcal{B}_m = \prod_{\gamma\in\Gamma} \gamma(\mathcal{B})$ totalement décomposé.

Le groupe d'inertie sur $\mathbf{Q}$ de $\mathcal{B} = \mathcal{B}_1$ est de la forme $T_{\mathcal{B}} =< \sigma >$ d'ordre 2. Ses conjugués sont les ${}^{\gamma}T_{\mathcal{B}} = T_{\gamma(\mathcal{B})}$; ils sont tous distincts : ce sont les m 2-Sylow de $Gal(H/\mathbf{Q})$. Donc si $K = H^{<\sigma>}$ est le corps laissé fixe par σ, on a :

$$Gal(H/K) = T_{\mathcal{B}} \Rightarrow \mathcal{B}^2 = \wp_1\mathcal{O}_H \text{ pour un } \wp_1|p \text{ dans } \mathcal{O}_K$$

et pour $2 \leq i \leq m$,

$$T_{\mathcal{B}_i} \cap T_{\mathcal{B}} = \{1\} \Rightarrow \exists j \neq i \text{ et } \wp_i|p \text{ dans } \mathcal{O}_K,\ \mathcal{B}_{i\mathcal{B}j} = \wp_i\mathcal{O}_H$$

(on numérotera les $\mathcal{B}_i$, $2 \leq i \leq m$, de sorte que les $\frac{m-1}{2}$ premiers s'associent aux $\frac{m-1}{2}$ derniers).

D'où

$$p\mathcal{O}_K = \wp_1\wp_2^2 \ldots \wp_{\frac{m+1}{2}}^2.$$

Il y a donc $\frac{m+1}{2}$ idéaux premiers de $\mathcal{O}_K$ au-dessus de p, dont les degrés résiduels sont tous égaux à 1.

Il suffit donc que $\frac{m+1}{2} > p$ c'est à dire $m > 2p-1$ pour que $p|i(K)$ par le corollaire 2 de §1.
Si p inerte dans $k/\mathbf{Q}$: $p\mathcal{O}_k = p$; on a comme précédemment

$$p\mathcal{O}_H = \mathcal{B}_1 \ldots \mathcal{B}_m = \prod_{\gamma\in\Gamma} \gamma(\mathcal{B}).$$

Le groupe de décomposition sur $\mathbf{Q}$ de $\mathcal{B} = \mathcal{B}_1$ est de la forme $D_{\mathcal{B}} =< \sigma >$ d'ordre 2, distincts des autres $D_{\mathcal{B}_i}$ qui lui sont conjugués.

$$K = H^{<\sigma>} \Rightarrow Gal(H/K) = D_{\mathcal{B}} \Rightarrow \exists \wp_1|p \text{ dans } \mathcal{O}_K \quad \wp_1\mathcal{O}_K = \mathcal{B}$$

et pour $2 \leq i \leq m$,

$$D_{\mathcal{B}_i} \cap D_{\mathcal{B}} = \{1\} \Longrightarrow \exists\ j \neq i \text{ et } \wp_1|p \text{ dans } \mathcal{O}_K,\ \mathcal{B}_{i\mathcal{B}j} = \wp_1\mathcal{O}_H.$$

D'où

$$p\mathcal{O}_K = \wp_1\wp_2 \ldots \wp_{\frac{m+1}{2}}$$

avec $f(\wp_1/p) = 1$, $f(\wp_1/p) = 2 \quad \forall\ i = 2, \ldots \frac{m+1}{2}$.

Comme le nombre de polynômes irréductibles unitaires et de degré 2 sur $\mathbf{F}_p$ est $\frac{p^2-p}{2}$, il suffit donc que $\frac{m-1}{2} > \frac{p^2-p}{2}$ c'est à dire $m > p^2-p+1$ pour que $p|i(K)$ par le corollaire 2 de §1. ∎

Remarque :

H est la clôture galoisienne de K et k est l'unique extension quadratique de $\mathbf{Q}$, contenue dans H (car $4 \dagger |Gal(H/\mathbf{Q})|$). Deux extensions quadratiques distinctes de $\mathbf{Q}$ ne peuvent donc fournir la même extension K.

Corollaire :

Pour un entier $n = p_1 \dots p_r$ sans facteur carré, il y a une infinité de corps de nombres d'indice divisible par n.

Démonstration :

Par un résultat de Yamamoto ([Y], théorèmes 1 et 2), pour des entiers premiers $q_1, \dots, q_u$ et $q'_1, \dots, q'_v$ et un entier t, fixés, il existe une infinité d'extensions quadratiques $k/\mathbf{Q}$ dans lesquelles les q_i sont ramifiés, les q'_i inertes et telles que $t|\ |Cl_k|$. Ceci s'applique de plusieurs façons ici : il suffit de décomposer $\{p_1, \dots, p_r\} = S_1 \cup S_2$ en deux sous-ensembles disjoints (l'un d'entre eux pouvant être vide), et de choisir t impair $> sup(2s_1 - 1, s_2^2 - s_2 + 1)$ où $s_1 = supS_1$ et $s_2 = supS_2$. Il y a alors une infinité de $k/\mathbf{Q}$ quadratiques dans lesquelles les p de S_1 se ramifient et ceux de S_2 restent inertes et telles que $t|m = |Cl'_k|$. D'où par la proposition, une infinité de K avec $p_1, \dots, p_r$ divisant $i(K)$, c'est à dire $n|i(K)$.

Appendice :

La méthode de M. Bauer par le polygone de Newton.

On se donne un entier premier p et un polynôme unitaire

$$P = X^n + c_1 X^{n-1} + \dots + c_{n-1} X + c_n \in \mathbf{Z}[X]$$

de racines $\omega = \omega_1, \omega_2, \dots, \omega_n$ (non nécessairement distinctes) dans une clôture algébrique de $\mathbf{Q}$. D'où l'extension de corps

$$K = \mathbf{Q}(\omega_1, \dots, \omega_n) \supset k = \mathbf{Q}(\omega) \supset \mathbf{Q}.$$

On choisit $\mathcal{B}|p$ dans $\mathcal{O}_K$ et l'on pose $p = \mathcal{B} \cap \mathcal{O}_k$; on a donc des décompositions de la forme

$$p\mathcal{O}_k = p^{ep} \dots \quad \text{et} \quad p\mathcal{O}_K = \mathcal{B}^{e_\mathcal{B}} \dots$$

Comme $K/\mathbf{Q}$ est galoisienne, $e = e_\mathcal{B}$ ne dépend pas de $\mathcal{B}$ mais seulement de p. Soit $w = w_\mathcal{B}$ la valuation associée à $\mathcal{B}$ et $v = v_p$ la valuation p-adique de $\mathbf{Z}$; on suppose les racines ordonnées par ordre croissant de valuation dans $\mathcal{O}_K$:

$$w(\cdot) : \underbrace{\omega_1, \dots, \omega_{k_1}}_{a_1} \underset{<}{,} \underbrace{\omega_{k+1}, \dots, \omega_{k_1+k_2}}_{a_2} \underset{<}{,} \begin{matrix} \cdots \\ \cdots \end{matrix}$$

Comme les coefficients c_j vérifient

$$c_j = \pm \sum_{i \le i_1 < \cdots < i_j \le n} w_{i_1} \dots w_{i_j}$$

on en déduit

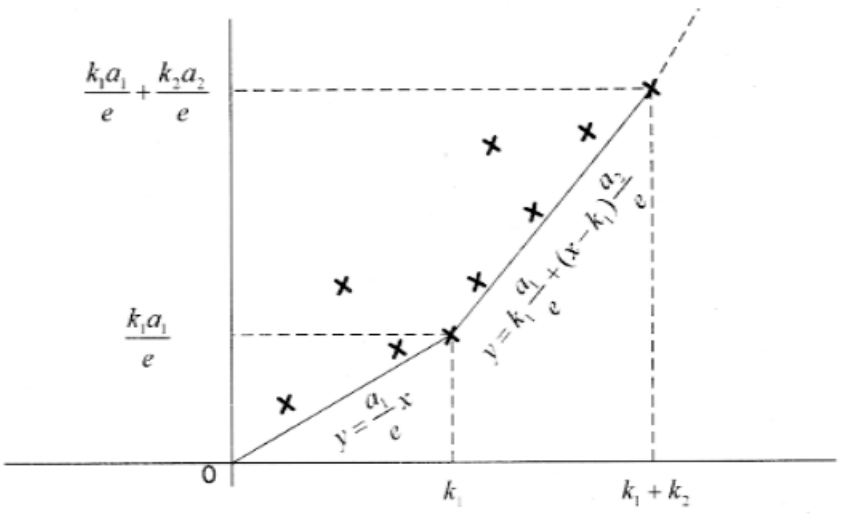
$$\begin{gathered} 1 \le j \le k_1 \Longrightarrow w(c_j) \ge ja_1 \Longrightarrow v(c_j) \ge \tfrac{ja_1}{e} \\ w(ck_1) = k_1 a_1 \Longrightarrow v(c_{k_1}) = \tfrac{k_1 a_1}{e} \quad (\Longrightarrow e \mid k_1 a_1) \end{gathered}$$

de mème

$$\begin{gathered} k_1 + 1 \le j \le k_1 + k_2 \Longrightarrow v(c_j) \ge (k_1 a_1 + (j - k_1) a_2)/e \\ v(c_{k_1+k_2}) = \tfrac{k_1 a_1}{e} + \tfrac{k_2 a_2}{e} \quad (\Longrightarrow e \mid k_2 a_2) \end{gathered}$$

etc...

D'où le polygone de Newton pour P et p (= bord inférieur de l'enveloppe convexe des points $(i, v(c_i))$, avec $c_0 = 1$) :



On pose $\alpha_i = \frac{k_i a_i}{e} (\in \mathbf{N})$.

Les pentes du polygone de Newton, $\frac{\alpha_i}{k_i} = \frac{a_i}{e}$ s'appellent les nombres de Puiseux (de P et p). Notons que $\omega = \omega_1$ se décompose sous la forme $\omega\mathcal{O}_K = \mathcal{B}^{a_\mathcal{B}} \ldots$ (où $a_\mathcal{B} = a_1$) et $\omega\mathcal{O}_k = p^{ap} \ldots$ et alors

$$\frac{a_p}{e_p} = \frac{a_\mathcal{B}}{e} \qquad \forall \mathcal{B}|p|p.$$

Applications

* Si les nombres de Puiseux sont $\frac{\alpha_1}{1}, \ldots, \frac{\alpha_n}{1}$, on en déduit que toutes les racines sont de valuation w distincte, donc que le groupe de décomposition $D_\mathcal{B}$ laisse chaque ω_i fixe et est donc trivial ; par conséquent p se décompose totalement dans $\mathcal{O}_k$ et $\mathcal{O}_K$.

En particulier, si $p < n$, alors $p|i(k)$ (par le corollaire 2).

** S'il n'y a qu'un nombre de Puiseux $\frac{\alpha}{n}$ avec $(\alpha, n) = 1$, alors toutes les racines ω_i ont même valuation $w(\omega) = a$ et

$$\frac{a_p}{e_p} = \frac{\alpha}{n} \Rightarrow n|e_p\alpha \Rightarrow n|e_p \Rightarrow n = e_p \quad (\text{car } e_p \leq [k : \mathbf{Q}] \leq n).$$

$\Rightarrow$ P irréductible (c'est le polynôme minimal de ω sur $\mathbf{Q}$) et $p\mathcal{O}_k = p^n$ est totalement ramifié dans $\mathcal{O}_k$; donc $p \dagger i(K)$.

*** On suppose P irréductible (en lui imposant par exemple la condition ** avec q à la place de p, pour un q premier $\neq p$).

Si les nombres de Puiseux pour p (et P) sont $\frac{\alpha_1}{2}, \frac{\alpha_2}{1}, \ldots, \frac{\alpha_{n-1}}{1}$ avec α_1 impair, alors $\frac{\alpha_1}{2} = \frac{a_1}{e} \Rightarrow 2|e$

et $p\mathcal{O}_k = p_1^2 p_2 \ldots p_{n-1}$ est la forme de la décomposition de p dans $\mathcal{O}_k$.

(Car seules ω_1 et ω_2 peuvent être racines dans $K_{\mathcal{B}}$ d'un même polynôme irréductible $\in \mathbf{Q}_p[X]$ et elles le sont effectivement car sinon p serait non ramifié dans K et ceci contredirait $2|e$).

En particulier, si $p < n-1$, alors $p|i(k)$ (et aussi $\mathrm{disc}(k/\mathbf{Q})$).

Pour d'autres exemples, on pourra consulter [B].

References

[B] M. BAUER Über die außerwesentlichen Diskriminantenteiler einer Gattung Math. Ann. 64, pp. 572 − 576, (1907).

[H] H. HASSE Number theory, Grundlehren der math. wiss., Nº 29, Springer-Verlag (1980).

[N] W. NARKIEWICZ "Elementary and analytic theory of algebraic numbers" 2nd edition, Springer Verlag (1990).

[Y] Y. YAMAMOTO *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7**, pp. 57 − 76, (1970).

Received by : December 20, 1999

Denis Hémard
Université de Valenciennes et du Hainaut Cambrésis
Laboratoire LAMATH B.P. 311
59304 Valenciennes Cedex
France