JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

ARTUR TRAVESA

Nombre d'extensions abéliennes sur Q

Journal de Théorie des Nombres de Bordeaux, tome 2, n° 2 (1990), p. 413-423

<http://www.numdam.org/item?id=JTNB_1990__2_2_413_0>

Séminaire de Théorie des Nombres,
Bordeaux **2** *(1990), 413–423*

Nombre d'extensions abéliennes sur $\mathbb{Q}$

par ARTUR TRAVESA*

Abstract. The aim of this paper is to give the numbers of abelian number fields with given degree and ramification indices. We describe, also, an algorithm to compute all these fields.

1. Introduction.

Un des problèmes dont la solution est devenue nécessaire en pratique est celui de "compter les extensions". En fait, I. R. Šafarevič proposa, en 1962, de déterminer si le groupe de Galois de l'extension maximale d'un corps de nombres non ramifiée en dehors d'un ensemble fini d'idéaux premiers de son anneau d'entiers est ou non topologiquement engendré par un nombre fini d'automorphismes et, dans le cas affirmatif, de donner des bornes supérieures pour le nombre de ces générateurs.

Le théorème de Hermite–Minkowski assure que, pour tout corps de nombres, il n'y a qu'un nombre fini d'extensions de degré donné qui sont non ramifiées en dehors d'un ensemble fini de premiers. La connaissance de bonnes bornes supérieures pour ces nombres jouerait un rôle important au moment de rendre effectifs les résultats de G. Faltings sur la conjecture de Mordell.

Le problème de compter les extensions a été étudié dans le cas local par M. Krasner et J.-P. Serre. D'un côté Krasner a calculé le nombre des extensions de degré donné d'un corps p-adique; pour cela, il a compté les extensions totalement ramifiées de degré et discriminant donnés d'un corps local arbitraire, non nécessairement p-adique. D'un autre côté, Serre a donné une intéressante formule de masse pour le nombre des extensions totalement ramifiées de degré donné d'un corps local à partir de laquelle obtient par une voie très commode et rapide les nombres calculés par Krasner.

J'ai repris ce problème, dans ma thèse, pour le cas abélien. Ce cas est si agréable que non seulement on peut donner le nombre des extensions

Avec le soutien partiel de CAICYT, PB85-0075.
*Je suis sincèrement l'obligé du Prof. Pilar Bayer; sans ses précieux conseils et sa constante attention cet article n'aurait pas pu être.
Manuscrit reçu le 2 août 1990.

mais aussi des algorithmes faciles pour calculer toutes ces extensions. La méthode peut s'appliquer aussi au cas des extensions abéliennes du corps des nombres rationnels. C'est ce que je vais faire dans ce qui suit

2 Énoncé des résultats.

Donnons nous un ensemble fini et non vide P de nombres premiers, un entier $n \geq 1$ et une famille $\{e_p\}_{p\in P}$ d'entiers $e_p \geq 1$ que j'écrirai partout sous la forme $e_p = p^{r_p} e'_p$, avec $r_p \geq 0$ et $p \nmid e'_p$. L'ensemble $\Sigma(n;P)$ des corps K extensions du corps $\mathbb{Q}$ des nombres rationnels qui sont dans une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ avec degré $[K:\mathbb{Q}] = n$, et non ramifiés en dehors de P est un ensemble fini. Donc, aussi l'ensemble $\Sigma_{ab}(n;P)$ des corps $K \in \Sigma(n;P)$ tels que $K/\mathbb{Q}$ soit abélienne et les ensembles $\Sigma_{ab}(n,\{e_p\}_p;P)$ des $K \in \Sigma_{ab}(n;P)$ tels que l'on ait :

(i) $K/\mathbb{Q}$ est non ramifiée au dessus de tout premier $p \in P$, et

(ii) l'indice de ramification $e_p(K/\mathbb{Q})$ est égal à e_p, pour tout $p \in P$.

Ces ensembles donc sont des ensembles finis, peut-être vides.

Le premier problème que j'ai en tête est celui de caractériser le cas où ces ensembles ne sont pas vides. Cette caractérisation est donnée par le théorème suivant:

THÉORÈME 1. *a) Pour que l'ensemble $\Sigma_{ab}(n,\{e_p\}_p;P)$ soit non vide, il faut et il suffit que les trois conditions suivantes soient réunies :*

(1) $\mu | n$,
(2) $n | e$, *et*
(3) $e'_p | p-1$, *pour tout* $p \in P$,

où $\mu := p.p.c.m.\{e_p : p \in P\}$ et $e := \prod_{p\in P} e_p$ désignent respectivement le plus petit multiple commun et le produit des e_p.

b) Pour que l'ensemble $\Sigma_{ab}(n;P)$ soit non vide, il faut et il suffit que pour tout nombre premier $\ell \notin P$ on ait :

$$\mathrm{v}_\ell(n) \leq \sum_{p\in P} \mathrm{v}_\ell(p-1),$$

où v_ℓ désigne la valuation ℓ-adique de l'anneau $\mathbb{Z}$ des nombres entiers.

Une fois obtenu un critère facile pour décider si les ensembles $\Sigma_{ab}(n,\{e_p\}_p;P)$ et $\Sigma_{ab}(n;P)$ sont vides ou non, nous pouvons nous interroger sur leurs cardinaux. A ce sujet, nous aurons besoin de quelques

notations pour désigner certains invariants attachés à l'ensemble P de façon naturelle pour ce problème, ainsi que d'introduire certaines fonctions pour compter les cardinaux.

Pour tout couple d'entiers N, $M \geq 0$ et tout nombre premier ℓ je vais considérer la fonction

$$\begin{bmatrix} N+M \\ M \end{bmatrix}_\ell := \prod_{j=1}^{M} \frac{\ell^{N+j}-1}{\ell^j - 1}.$$

Si l'on pense ℓ comme une indéterminée, cette fonction a des propriétés semblables à celles de la fonction donnée par les nombres combinatoires $\binom{N+M}{M}$; notamment, c'est une fonction entière, $\begin{bmatrix} N+M \\ M \end{bmatrix}_\ell \in \mathbb{Z}[\ell]$, symétrique, $\begin{bmatrix} N+M \\ M \end{bmatrix}_\ell = \begin{bmatrix} M+N \\ N \end{bmatrix}_\ell$, et l'on a $\begin{bmatrix} N \\ N \end{bmatrix}_\ell = \begin{bmatrix} N \\ 0 \end{bmatrix}_\ell = 1$, pour tout $N \geq 0$.

Par ailleurs, pour tout nombre premier ℓ et tout entier $j \geq 1$, j'écrirai

$$T_j(\ell) := \#\{p \in P : p = \ell \text{ ou } \ell^j | p-1\},$$

sauf dans le cas $\ell = 2$, $2 \in P$ et $j = 1$ où je poserai

$$T_1(2) := 1 + \#P.$$

Avec ces notations on peut déjà énoncer le théorème suivant:

THÉORÈME 2. *Le nombre d'extensions abéliennes de $\mathbb{Q}$ de degré n qui sont non ramifiées en dehors de P est donné par*

$$\#\Sigma_{ab}(n;P) = \prod_{\ell} \#\Sigma_{ab}(\ell^{v_\ell(n)};P)$$

et

$$\#\Sigma_{ab}(\ell^v;P) = \sum_{\mathbf{M}=v} \ell^{\sum_{i\geq 1} M_{i+1}(T_i(\ell)-M_i)} \prod_{i\geq 1} \begin{bmatrix} T_i(\ell)-M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_\ell$$

où l'on fait la somme sur toutes les partitions $\mathbf{M}$: $\sum_i M_i = v$ tels que l'on ait $M_i \geq M_{i+1} \geq 0$ et $M_i \leq T_i(\ell)$ pour tout indice i.

REMARQUE. *Les sommes et produits qui ont paru dans ces formules sont en fait finies, puisque $M_i = 0$ pour i assez grand.*

Il nous reste encore à donner les cardinaux des ensembles $\Sigma_{ab}(n, \{e_p\}_p; P)$. Pour tout entier $v \geq 0$, tout nombre premier ℓ, et toute

suite $\mathbf{N} := (N_1, \dots, N_s, 0, \dots)$ d'entiers $N_1 \geq N_2 \geq \cdots \geq N_s \geq 0$, posons

$$f_\ell(\mathbf{N}; v) :=$$
$$\sum_{\mathbf{M}=v} \prod_{i\geq 1} \sum_{k_i=0}^{N_i - N_{i+1}} (-1)^{k_i} \binom{N_i - N_{i+1}}{k_i} \ell^{M_{i+1}(N_i - k_i - M_i)} \begin{bmatrix} N_i - k_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_\ell,$$

où l'on fait la somme sur toutes les partitions de v, $\sum_{i\geq 1} M_i = v$, tels que l'on ait $M_i \geq M_{i+1} \geq 0$ et $M_i \leq N_i$ pour tout indice i. Comme dans le théorème qui précède, le produit est fini. Remarquons aussi que si $v \geq \sum_{i\geq 1} N_i$, alors on a $f_\ell(\mathbf{N}; v) = 0$.

Maintenant, pour tout nombre premier ℓ et tout entier $j \geq 1$, il faut considérer les nombres

$$N_j(\ell) := \#\{p \in P : \mathrm{v}_\ell(e_p) \geq j\},$$

la suite

$$\mathbf{N}(\ell) := (N_1(\ell), \dots, N_j(\ell), \dots)$$

et, si $2 \in P$ et $r_2 \geq 1$, aussi les suites

$$\mathbf{N}'(2) := (N_1(2) + 1, N_2(2), \dots, N_{r_2}(2) - 1, \dots, N_j(2), \dots)$$

et

$$\mathbf{N}''(2) := (N_1(2), N_2(2), \dots, N_{r_2}(2) - 1, \dots, N_j(2), \dots).$$

Les cardinaux des ensembles $\Sigma_{ab}(n, \{e_p\}_p; P)$ sont donnés par le théorème suivant:

THÉORÈME 3. *Pourvu que la condition (3) du théorème 1, a) soit satisfaite on a les formules*

$$\#\Sigma_{ab}(n, \{e_p\}_p; P) = \prod_\ell \#\Sigma_{ab}(\ell^{\mathrm{v}_\ell(n)}, \{\ell^{\mathrm{v}_\ell(e_p)}\}_p; P)$$

et $\#\Sigma_{ab}(\ell^v, \{\ell^{\mathrm{v}_\ell(e_p)}\}_p; P) =$

$$\begin{cases} f_\ell(\mathbf{N}(\ell); v) & \text{si } \ell \neq 2 \text{ ou si } \ell = 2 \text{ et } 2 \notin P, \\ 3f_2(\mathbf{N}(2); v) & \text{si } \ell = 2,\ 2 \in P \text{ et } e_2 = 2, \\ 2f_2(\mathbf{N}(2); v) + f_2(\mathbf{N}'(2); v) - f_2(\mathbf{N}''(2); v) & \text{si } \ell = 2,\ 2 \in P \text{ et } e_2 > 2. \end{cases}$$

REMARQUE. *Il faut noter qu'il n'y a pas besoin des conditions (1) et (2) pour appliquer ces formules-ci car les facteurs* $f_\ell(\mathbf{N}(\ell); v)$ *détectent leur*

défaut. Mais il est nécessaire de s'assurer de la validité de la condition (3). Par exemple, si l'on prenait $P = \{3,5\}$, $n = 4$ *et* $\{e_3, e_5\} = \{2,4\}$, *les invariants* $N_j(\ell)$, *qui sont les seuls qui jouent un rôle important dans la formule, seraient les mêmes dans le cas* $e_3 = 2$, $e_5 = 4$, *où il existe le corps* $\mathbb{Q}(2\cos(2\pi/15)) = \mathbb{Q}(e^{2\pi i/15})^+$, *et dans le cas* $e_3 = 4$, $e_5 = 2$, *où il n'existe aucun corps .*

La démonstration qu'on va faire de ces théorèmes nous munira en plus d'un algorithme pour calculer effectivement toutes les extensions abéliennes de degré et ramification donnés. Bien sûr on peut dessiner un tel algorithme à partir de la "cyclotomicité" des extensions abéliennes de $\mathbb{Q}$: un corps $K \in \Sigma_{ab}(n, \{e_p\}_p; P)$ est un sous-corps de $\mathbb{Q}(\zeta)$ pour une racine de l'unité ζ que peut être bien déterminée à partir de P, n et des e_p. Avec un choix optimal de ζ, l'extension $\mathbb{Q}(\zeta)/K$ est modérément ramifiée au dessus de tous les idéaux premiers de l'anneau d'entiers de K; mais, en général, il y a effectivement des idéaux premiers qui y sont ramifiés.

La méthode que nous allons suivre consiste à construire certains corps facilement calculables L, attachés aux données P et $\{e_p\}_p$, et de sorte que l'on ait $K \subseteq L$ et que les extensions L/K soient non ramifiées au dessus de tous les idéaux premiers de l'anneau des entiers de K; de plus, la ramification aux places à l'infini y reste complètement contrôlée.

3. Démonstration du théorème 1.

Il faut commencer par le cas où P est un singleton $\{p\}$; c'est-à-dire, où il n'y a qu'un premier qui se ramifie ; en ce cas nous avons les données $\{p\}$, $e_p = p^{r_p} e'_p$ et n.

On peut décrire complètement le cas $p = 2$ par la proposition suivante, dont la preuve, facile, est laissée comme exercice :

PROPOSITION 1. *Soient* n *et* e_2 *des nombres entiers positifs.*

a) Pour que l'ensemble $\Sigma_{ab}(n, e_2; \{2\})$ *soit non vide il faut et il suffit que l'on ait* $n = e_2 = 2^{r_2}$ *pour quelque* $r_2 \geq 0$, *c'est-à-dire,* $e'_2 = 1$.

b) On a $\Sigma_{ab}(2^{r_2}, 2^{r_2}; \{2\}) = \{\mathbb{Q}(\zeta^2), \mathbb{Q}(\zeta + \zeta^{-1}), \mathbb{Q}(\zeta - \zeta^{-1})\}$, *où* ζ *est une racine primitive* 2^{r_2+2}*-ième de l'unité. Les trois corps sont différents si* $r_2 \neq 0$ *et les extensions* $\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q}$ *et* $\mathbb{Q}(\zeta - \zeta^{-1})/\mathbb{Q}$ *sont cycliques; par contre, on a* $\mathrm{Gal}(\mathbb{Q}(\zeta^2)/\mathbb{Q}) \simeq C_2 \times C_{2^{r_2-1}}$, *où* C_m *dnote un groupe cyclique d'ordre* m.

Pour décrire le cas où p est un premier impair il faut généraliser les périodes des équations cyclotomiques de Gauss (cf. [vdW: §8.4]) au cas

où q est une puissance d'un nombre premier et non seulement un nombre premier lui même. Pour commencer, il est facile de voir que si l'ensemble $\Sigma_{ab}(n, e_p; \{p\})$ est non vide, il vient : $e'_p | p-1$; nous allons donc supposer, et, que la condition $e'_p | p-1$ est vérifiée.

Soit ζ une racine primitive p^{r_p+1}-ime de l'unité et soit g une racine primitive modulo p^{r_p+1}; c'est-à-dire, un générateur du groupe multiplicatif des unités de $\mathbb{Z}/p^{r_p+1}\mathbb{Z}$. Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est cyclique engendré par l'automorphisme σ de $\mathbb{Q}(\zeta)$ tel que $\sigma(\zeta) = \zeta^g$. Pour tout entier i nous pouvons considérer le i-ième e_p-période de ζ relative à g

$$\eta_i := \sum_{j=0}^{d-1} \sigma^{je_p}(\zeta^{g^i})$$

où $d := p^{r_p}(p-1)/e_p = (p-1)/e'_p$. On a l'égalité $\eta_i = \eta_j$ si $i \equiv j \pmod{e_p}$. L'ensemble $\{\eta_0, \ldots, \eta_{e_p-1}\}$ ne dépend pas de ζ ni de g, bien que η_0 dépende de ζ mais non de g, et les autres périodes dépendent de ζ et de g. Avec ces notations, il n'est pas difficile de prouver la proposition suivante:

PROPOSITION 2. *Soient p un nombre premier, $n \geq 0$ un entier et $e_p = p^r e'_p$, avec $r \geq 0$ et $p \nmid e'_p$, un autre entier.*

a) Pour que l'ensemble $\Sigma_{ab}(n, e_p; \{p\})$ soit non vide il faut et il suffit que l'on ait $n = e_p$ et $e'_p | p-1$.

b) Si e'_p divise $p-1$, alors il vient $\mathbb{Q}(\eta_0) = \mathbb{Q}(\eta_1) = \cdots = \mathbb{Q}(\eta_{e_p-1})$.

c) Si on a $n = e_p$ et $e'_p | p-1$, il suit $\Sigma_{ab}(n, e_p; \{p\}) = \{\mathbb{Q}(\eta_0)\}$.

Maintenant, nous allons démontrer le théorème 1 dans le cas général. Pour faire cela, nous allons construire quelques corps L attachés aux données P et $\{e_p\}_p$.

En faisant usage du théorème de Kronecker–Weber on voit aisément que les conditions (1) et (3) du théorème 1, a) sont nécessaires pour que l'ensemble $\Sigma_{ab}(n, \{e_p\}_p; P)$ soit non vide ; nous pouvons, donc, supposer ces conditions satisfaites. Cela étant, pour tout $p \in P$ nous pouvons considérer le corps $L_p := \mathbb{Q}(\eta_0)$ attaché au couple (e_p, p) par la proposition 2, si $p \neq 2$, et les trois corps $L_2 \in \{\mathbb{Q}(\zeta^2), \mathbb{Q}(\zeta + \zeta^{-1}), \mathbb{Q}(\zeta - \zeta^{-1})\}$ attachés $(e_2, 2)$ par la proposition 1, si $p = 2$. Nous désignerons par L n'importe lequel des corps composés $L := \prod_{p \in P} L_p$; ces corps seront appelés les corps $(P; \{e_p\}_p)$-universels; il n'y en a qu'un si $2 \notin P$ ou si $2 \in P$ et $e_2 = 1$, et il y en a trois si $2 \in P$ et $e_2 > 1$. En regardant les indices de ramification, on voit facilement que les extensions $L_p/\mathbb{Q}$ sont linéairement disjointes et l'on peut écrire l'énoncé suivant:

LEMME 3. *Les extensions $(P;\{e_p\}_p)$-universelles $L/\mathbb{Q}$ sont abéliennes, non ramifiées en dehors de P, d'indices de ramification $e_p(L/\mathbb{Q}) = e_p$ pour tout $p \in P$ et de degré $e := \prod_{p\in P} e_p$. Autrement dit, on a $L \in \Sigma_{ab}(e,\{e_p\}_p;P)$.*

En plus, les corps L peuvent être donnés explicitement. En effet, si $\mathbb{Q}(\beta_1)/\mathbb{Q}$ et $\mathbb{Q}(\beta_2)/\mathbb{Q}$ sont des extensions galoisiennes linéairement disjointes dont l'une au moins est de degré impair, alors on a $\mathbb{Q}(\beta_1,\beta_2) = \mathbb{Q}(\beta_1\beta_2)$. Si l'on applique convenablement ce fait aux corps L_p, on trouve que L est donné par un produit explicite de périodes.

En jouant avec les groupes de Galois des extensions $L/\mathbb{Q}$ on obtient la vraie clé de cette théorie :

PROPOSITION 4. *Supposons que les données P, $\{e_p\}_p$ et n satisfassent les conditions (1) et (3) du théorème 1, a). Si $K \in \Sigma_{ab}(n,\{e_p\}_p;P)$, alors il existe une extension $(P;\{e_p\}_p)$-universelle $L/\mathbb{Q}$ et une seule telle que $K \subseteq L$.*

Ce résultat donne la condition (2) du théorème 1, a) ainsi que le corollaire suivant:

COROLLAIRE 5. *L'ensemble $\Sigma_{ab}(n,\{e_p\}_p;P)$ est la réunion, sur tous les corps $(P;\{e_p\}_p)$-universels L, des ensembles*

$$\Sigma_{ab}^{L}(n,\{e_p\}_p;P) := \{K \in \Sigma_{ab}(n,\{e_p\}_p;P) : K \subseteq L\}.$$

Cette réunion est disjointe.

Si l'on ne cherchait qu'une démonstration du théorème 1, on pourrait finir par un argument bien simple : si l'on suppose satisfaites les conditions (1), (2) et (3) du théorème, on a $\Sigma_{ab}(e,\{e_p\}_p;P) \ni L$ pour les corps $(P;\{e_p\}_p)$-universels L; en outre, si $K_0 \in \Sigma_{ab}(\mu,\{e_p\}_p;P)$, alors L/K est une extension abélienne et non ramifiée partout; donc, si K/K_0 est une sous-extension de degré n/μ de L/K_0, alors $K \in \Sigma_{ab}(n,\{e_p\}_p;P)$. Ainsi, il reste prouver que $\Sigma_{ab}(\mu,\{e_p\}_p;P)$ est non vide. Si nous prenons L tel que chacun des sous-corps L_p soit cyclique sur $\mathbb{Q}$, ce qui est possible, alors on peut prendre K_0 comme le corps fixé par un sous-groupe H du groupe des caractères de $L/\mathbb{Q}$

$$\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Gal}(L/\mathbb{Q}),\mathbb{C}^*) \simeq \prod_{p\in P} \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Gal}(L_p/\mathbb{Q}),\mathbb{C}^*)$$

engendré par un élément $(\chi_p)_{p\in P}$ tel que χ_p engendre $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Gal}(L_p/\mathbb{Q}),\mathbb{C}^*) \simeq \mathbb{Z}/e_p\mathbb{Z}$ (cf. [Wa: Thm. 3.5]). Ainsi, on obtient une preuve du théorème 1, a) et le corollaire suivant:

COROLLAIRE 6. *Pourvu que les conditions du théorème 1, a) soient satisfaites on a*

$$\#\Sigma_{ab}(\mu, \{e_p\}_p; P) \geq \varphi(\mu)^{-1} \prod_{p \in P} \varphi(e_p)$$

où φ dénote la fonction d'Euler.

REMARQUE. *L'égalité est satisfaite si $2 \notin P$ ou si $e_2 = 1$.*

La seconde partie du théorème 1 est un corollaire immédiat de la première.

4. Les nombres d'extensions.

Nous nous sommes proposés non seulement de savoir s'il y a des corps dans $\Sigma_{ab}(n; P)$ et dans $\Sigma_{ab}(n, \{e_p\}_p; P)$, mais de savoir exactement combien il y a de tels corps ; autrement dit, nous voulons démontrer les théorèmes 2 et 3.

Supposons donc que les conditions (1), (2) et (3) soient satisfaites et posons $G_p := \mathrm{Gal}(L_p/\mathbb{Q})$ pout tout $p \in P$. Le groupe G_p est un groupe cyclique d'ordre e_p engendré par l'automorphisme σ_p puissance $(p-1)/e'_p$-ième de l'automorphisme σ défini après la proposition 1, sauf dans le cas $L_2 = \mathbb{Q}(\zeta^2)$, ζ une racine primitive 2^{r_2+2}-ième de l'unité, $r_2 > 1$; dans ce dernier cas, en effet $G_2 = \langle c \rangle \oplus \langle \sigma_0 \rangle$ où c dénote la conjugaison complexe et σ_0 l'automorphisme de $\mathbb{Q}(\zeta^2)$ défini par $\sigma_0(\zeta^2) := (\zeta^2)^5$. Le calcul des indices de ramification des sous-corps du corps $(P; \{e_p\}_p)$-universel L fournit le résultat suivant:

PROPOSITION 7. *Il existe une correspondance biunivoque entre l'ensemble $\Sigma^{L}_{ab}(n, \{e_p\}_p; P)$ et l'ensemble des sous-groupes $X \subseteq G := \bigoplus_{p \in P} G_p$ tels que l'on ait*

(1) *l'égalité indicative $(G : X) = n$; et*
(2) *$X \cap G_p = \{id\}$, pour tout $p \in P$.*

REMARQUE. *Puisque tous ces sous-groupes sont effectivement calculables, cette proposition nous fournit un algorithme effectif pour obtenir tous les corps $K \in \Sigma_{ab}(n, \{e_p\}_p; P)$; en fait, ces corps sont les sous-corps de L fixes par les sous-groupes X. Comme L est donné par un élément primitif explicite θ, et comme X peut être donné par générateurs effectivement calculables, il est facile de calculer le polynôme irréductible $\mathrm{Irr}(\theta, K) = \prod_{\sigma \in X}(X - \sigma(\theta))$; alors, les coefficients de ce polynôme engendrent le corps K sur $\mathbb{Q}$; ces coefficients ne sont que certaines sommes de racines de l'unité convenables.*

Il s'agit donc de calculer le nombre des sous-groupes X sous les conditions (1) et (2) de la proposition 7; mais la condition sur l'intersection est très désagréable à imposer. Il convient donc d'exprimer cette proposition sous une forme équivalente plus aisément maniable.

Si $\{H_i\}_{i\in I}$ est une famille arbitraire de groupes et $\pi_i : \prod_{i\in I} H_i \to H_i$ les projections usuelles, on notera $\Pi(\{H_i\}_{i\in I})$ l'ensemble de tous les sous-groupes $X \subseteq \prod_{i\in I} H_i$ tels que l'on ait $\pi_i(X) = H_i$ pour tout $i \in I$; de manière analogue, $\Pi(\{H_i\}_{i\in I}; n)$ désignera le sous-ensemble de $\Pi(\{H_i\}_{i\in I})$ constitué par les sous-groupes X d'ordre n. Avec ces notations, on peut écrire la proposition 7 sous la forme équivalente suivante:

PROPOSITION 7'. *Il existe une correspondance biunivoque entre l'ensemble* $\Sigma^I_{ab}(n, \{e_p\}_p; P)$ *et l'ensemble* $\Pi(\{\widehat{G}_p\}_{p\in P}; n)$, *où* $\widehat{G}_p := \mathrm{Hom}_{\mathbb{Z}}(G_p, \mathbb{C}^*)$ *est le groupe des caractères du groupe abélien* G_p.

Du fait que nous sommes en train d'étudier les extensions abéliennes dont les ses groupes de Galois se décomposent en produit de leurs sous-groupes de Sylow, nous pouvons supposer que le degré n est une puissance ℓ^s d'un nombre premier ℓ. En ce cas, nous avons les données P, ℓ^s et une famille $\{\ell^{r_p}\}_{p\in P}$, de sorte que les conditions du théorème 1 se traduisent par les suivantes:

(1) $\max\{r_p : p \in P\} \leq s$;
(2) $s \leq \sum_{p\in P} r_p$; et
(3) $\ell^{r_p} | p-1$ pour tout $p \in P$, $p \neq \ell$.

Si l'on pose $n_j(\ell) := N_j(\ell) - N_{j+1}$, pour tout $j \geq 1$, on trouve que le groupe $\widehat{G}$ peut s'écrire sous la forme

$$\widehat{G} \simeq (\mathbb{Z}/\ell\mathbb{Z})^{n_1(\ell)} \times \cdots \times \left(\mathbb{Z}/\ell^{s-1}\mathbb{Z}\right)^{n_{s-1}(\ell)} \times (\mathbb{Z}/\ell^s\mathbb{Z})^{N_s(\ell)}$$

sauf dans le cas où L_2 n'est pas cyclique, cas dans lequel on a

$$\widehat{G} \simeq (\mathbb{Z}/2\mathbb{Z})^{n_1(2)+1} \times \cdots \times (\mathbb{Z}/2^{r_2}\mathbb{Z})^{n_{r_2}(2)-1} \times \cdots \times (\mathbb{Z}/2^s\mathbb{Z})^{N_s(2)}.$$

Dans ce cas, si l'on pose $\widehat{G}_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r_2-1}\mathbb{Z}$, $\widehat{G}'_2 = \mathbb{Z}/2^{r_2-1}\mathbb{Z}$ et H_2 le sous-groupe cyclique de $\widehat{G}_2$ d'ordre 2^{r_2-1} engendré par l'élément $(1,1)$, il n'est pas difficile de prouver que l'ensemble $\Pi(\{\mathbb{Z}/2\mathbb{Z}, \widehat{G}'_2, \widehat{G}_p\}_{p\in P, p\neq 2})$ est la réunion des ensembles $\Pi(\{\widehat{G}_p\}_{p\in P})$ et $\Pi(\{H_2, \widehat{G}_p\}_{p\in P, p\neq 2})$. Maintenant, nous avons l'avantage d'avoir tous les groupes H_2, $\widehat{G}'_2$ et $\widehat{G}_p$, $p \neq 2$, cycliques comme dans le cas général.

La démonstration du théorème 3 découle du résultat suivant:

PROPOSITION 8. *Soit Γ_ℓ un groupe abélien isomorphe au groupe*

$$(\mathbb{Z}/\ell\mathbb{Z})^{n_1} \times \cdots \times (\mathbb{Z}/\ell^{s-1}\mathbb{Z})^{n_{s-1}} \times (\mathbb{Z}/\ell^s\mathbb{Z})^{n_s}$$

et posons $N_s := n_s$, $N_i := N_{i+1} + n_i$, pour $1 \leq i \leq s-1$, et $\mathbf{N} := (N_1, \ldots, N_s, 0, \ldots)$. Le nombre des sous-groupes de Γ_ℓ d'ordre ℓ^v qui se projettent surjectivement sur chacun des facteurs est donné par $f_\ell(\mathbf{N}; v)$.

DÉMONSTRATION: Nous définissons le type du ℓ-groupe abélien fini Γ_ℓ comme la suite $\mathbf{N} := (N_1, \ldots, N_s, 0, \ldots)$. Avec cette définition, le type est une suite décroissante d'entiers non negatifs qui est nulle à partir d'un certain rang et qui détermine le groupe à isomorphisme près. La valeur de s est déterminée par l'exposant ℓ^s du groupe, l'ordre est $\ell^{N_1+\cdots+N_s}$ et N_1 est la dimension du $\mathbb{F}_\ell$-espace vectoriel $\Gamma_\ell/\ell\Gamma_\ell$. Si $\mathbf{N}$ et $\mathbf{M}$ sont des types de ℓ-groupes abéliens finis, nous disons que $\mathbf{M} \leq \mathbf{N}$ si $M_i \leq N_i$ pour tout $i \geq 1$. Ainsi, pour qu'un groupe de type $\mathbf{N}$ contienne un sous-groupe de type $\mathbf{M}$ il faut et il suffit qu'on ait $\mathbf{M} \leq \mathbf{N}$; et le type d'un produit de groupes de types $\mathbf{N}$ et $\mathbf{M}$ est un groupe de type $\mathbf{N}+\mathbf{M} := (N_1+M_1, \ldots, N_s+M_s, \ldots, 0, \ldots)$.

Une $\mathbf{M}$-base dans Γ_ℓ est un ensemble minimal d'éléments de Γ_ℓ qui engendrent un sous-groupe de type $\mathbf{M}$. Notons $\mathrm{B}(\Gamma_\ell; \mathbf{M})$ l'ensemble de toutes les $\mathbf{M}$-bases dans Γ_ℓ; alors, $\#\,\mathrm{B}(\Gamma_\ell; \mathbf{M}) = \#\,\mathrm{S}(\Gamma_\ell; \mathbf{M}) \#\,\mathrm{Aut}(X_0)$, o $\mathrm{S}(\Gamma_\ell; \mathbf{M})$ est l'ensemble de tous les sous-groupes de Γ_ℓ de type $\mathbf{M}$ et X_0 un de ces sous-groupes.

Pour calculer $\#\,\mathrm{B}(\Gamma_\ell; \mathbf{M})$, on définit une application de cet ensemble sur celui des éléments de Γ_ℓ d'ordre égal au maximum des ordres des éléments de X_0; les fibres de cette application sont toutes équipotentes à l'ensemble $\mathrm{B}(\Gamma'_\ell; \mathbf{M}') \times X'_0$, où les primes signifient qu'on a enlevé la dernière composante de Γ_ℓ et de X_0, et $\mathbf{M}'$ est le type de X'_0.

Ce procédé nous donne une méthode récursive pour calculer $\#\,\mathrm{B}(\Gamma_\ell; \mathbf{M})$, puisque le cardinal de X'_0 ainsi que le nombre d'éléments de Γ_ℓ d'ordre donné sont facilement calculables. D'une manière analogue, nous évaluons $\#\,\mathrm{Aut}(X_0)$. Ainsi, nous trouvons que

$$(*) \qquad \#\,\mathrm{S}(\Gamma_\ell; \mathbf{M}) = \ell^{\sum_{i\geq 1} M_{i+1}(N_i - M_i)} \prod_{i\geq 1} \begin{bmatrix} N_i - M_{i+1} \\ M_i - M_{i+1} \end{bmatrix}_\ell .$$

Pour finir, nous obtenons $f_\ell(\mathbf{N}; v)$ en faisant la somme de ces nombres pour tous les types $\mathbf{M} \leq \mathbf{N}$ tels que l'on ait $\sum_{i\geq 1} M_i = v$, une fois sélectionnés les sous-groupes s'envoyant surjectivement sur les facteurs de Γ_ℓ par un argument usuel en théorie des ensembles ; cela introduit dans $f_\ell(\mathbf{N}; v)$ les facteurs $(-1)^{k_i}\binom{N_i - N_{i+1}}{k_i}$. ∎

Bibliographie

[**Fa**] Faltings, G., Wüstholz, G., et al., "Rational points," Seminar Bonn–Wuppertal 1983/84, Friedr. Vieweg & Sohn, 1984.

[**Kr**] Krasner, M., *Nombre des extensions d'un degré donné d'un corps p-adique*, C. R. Acad. Sc. Paris **254**, **255** (1962), 3470–3472, 224–226, 1682–1684, 2342–2344, 3095–3097. Voir aussi "Les Tendances Géométriques en Algèbre et Théorie des Nombres" dans *Colloques Internationaux du C.N.R.S.*, **143** (1966), pp. 143–169.

[**Sa**] Šafarevič, I. R., *Algebraic Number Fields*, Amer. Math. Soc. Trans. **31** (1963), 25–39.

[**Se**] Serre, J.-P., *Une formule de masse pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sc. Paris **286** (1978), 1031–1036.

[**Tr 1**] Travesa, A., "Nombres d'extensions abelianes i les seves funcions generatrius," Thse, Universitat de Barcelona, 1987.

[**Tr 2**] Travesa, A., *Generating functions for the numbers of abelian extensions of a local field*, Proc. Amer. Math. Soc. **108** (1990), 331–339.

[**vdW**] van der Waerden, B.L., "Algebra," vol. 1, Frederick Ungar Pub. Co., New York, 1970.

[**Wa**] Washington, L.C., "Introduction to Cyclotomic Fields," GTM 83 Springer-Verlag, New-York, 1982.

Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007 Barcelona, Catalunya, Espagne.