Sur les corps résolubles de degré premier

Dedicated to Albrecht Fröhlich on his 70th birthday

Par *Soun-Hi Kwon* à Séoul et *Jacques Martinet* à Talence

---

§ 1. Généralités

Soit l un nombre premier et soit m un diviseur de $l-1$. A isomorphisme près, il existe un unique groupe G d'ordre ml qui est une extension d'un groupe d'ordre l par un groupe cyclique d'ordre m *opérant fidèlement*. L'extension est un produit semi-direct, et G est isomorphe à l'unique sous-groupe d'ordre lm du groupe affine d'une droite sur $\mathbb{F}_l$. Pour $m=l-1$, G est le groupe affine lui-même. Pour $m=1$ (resp. 2), G est cyclique (resp. diédral). On peut caractériser ces groupes comme étant les groupes résolubles transitifs de degré premier (théorème de Burnside). Le groupe G peut être défini par deux générateurs σ et τ, liés par les relations $\sigma^l=\tau^m=1$ et $\tau\sigma\tau^{-1}=\sigma^a$, où a est l'un des $\varphi(m)$ éléments d'ordre m de $(\mathbb{Z}/l\mathbb{Z})^*$. A isomorphisme près, G ne dépend pas de a. Toutefois, lorsque l'on cherche à plonger une extension cyclique k/k_0 de degré $m>2$ dans une extension galoisienne M/k_0 à groupe de Galois isomorphe à G, le choix de a n'est pas indifférent, puisque l'on a des procédés pour fixer un générateur du groupe de Galois de k/k_0. Nous reviendrons là-dessus aux paragraphes 3 et 5.

1. 1. Exemple. (i) Si k_0 est un corps de caractéristique différente de l, pour tout $\alpha \in k_0$ non puissance l-ième, l'extension $K=k_0(\sqrt[l]{\alpha})$ de k_0 a une clôture galoisienne de groupe de Galois isomorphe au groupe G pour lequel m est le degré sur k_0 du corps des racines l-ièmes de l'unité.

(ii) (cf. § 3.) Si k_0 est un corps de nombres, et si k est une extension cyclique de degré m de k_0 telle que toutes les sous-extensions strictes de k/k_0 aient un nombre de classes premier à l, les extensions non ramifiées de degré l de k sont engendrées par celles qui sont galoisiennes sur k_0 et ont un groupe de Galois isomorphe à un groupe G.

1. 2. Notations. On note k_0 un corps, $\bar{k}_0$ une clôture séparable de k_0, M une sous-extension galoisienne de $\bar{k}_0/k_0$ de groupe de Galois G d'ordre lm comme ci-dessus (l est premier et m divise $l-1$), k la sous-extension de degré m de M/k_0, et K une sous-extension de degré l de M (K possède l conjugués si $m>1$). On désigne par H (resp. g) le groupe de Galois de M/k (resp. de M/K), et l'on identifie g au groupe de Galois de k/k_0. On note en outre μ_l le groupe des racines l-ièmes de l'unité de $\bar{k}_0$, ζ un générateur de μ_l.

Lorsque L est un corps de nombres, $\mathbb{Z}_L$ (resp. E_L, resp. Cl_L) désigne l'anneau des entiers (resp. le groupe des unités, resp. le groupe des classes) de L, et l'on pose $h_L = \text{card}\, Cl_L$.

1. 3. Plan. On étudie dans le § 2 la structure des discriminants et, dans le § 3, on indique quelques résultats permettant de construire des extensions à l'aide de la théorie du corps de classes. Ces résultats sont ensuite utilisés dans le § 4 pour étudier les petits discriminants. Dans le § 5, on expose brièvement la théorie de Kummer, que l'on applique dans le § 6 à la construction des polynômes. Le § 7 contient quelques remarques concernant les petits discriminants.

§ 2. Décomposition et conducteurs d'Artin

On conserve les notations du § 1; on se donne en outre un anneau de Dedekind A de corps des fractions k_0, relativement à qui sont calculés les discriminants, et l'on suppose ses corps résiduels finis. On note en outre v_0 une place de k_0 et v une place de k au-dessus de v_0, et, si v_0 est finie, on suppose qu'elle correspond à un idéal premier non nul $\mathfrak{p}_0$ de A, et l'on note $\mathfrak{p}$ l'idéal correspondant à v et $\mathfrak{P}$ un idéal premier de M au-dessus de $\mathfrak{p}$. Les groupes de ramification de $\mathfrak{P}$ dans M/k_0, M/k et M/K sont alors notés G_i, H_i et g_i, $i \geqq -1$.

2. 1. Proposition. *Soit e (resp. f) l'indice de ramification (resp. le degré résiduel) de v_0 dans k/k_0.*

(i) *Si v est inerte (resp. ramifiée) dans M/k, v_0 est inerte (resp. totalement ramifiée) dans K/k_0;*

(ii) *Si v est décomposée dans M/k, K possède au-dessus de v_0 une place de degré local 1 et $\dfrac{l-1}{ef}$ places d'indice de ramification e et de degré résiduel f.*

Démonstration. Cela résulte tout de suite des relations $g_i = G_i \cap g$ et $G_i(\sigma\mathfrak{P}) = \sigma G_i(\mathfrak{P})\sigma^{-1}$.

2. 2. Corollaire. *Si v_0 est réelle, et si K n'est pas totalement réel au-dessus de v_0, alors m est pair, k et M sont totalement imaginaires au-dessus de v_0, et K possède une unique place réelle au-dessus de v_0.*

2. 3. Proposition. *Si l'indice de ramification de $\mathfrak{p}_0$ dans M/k_0 est $> l$, $\mathfrak{p}_0$ divise l; si cet indice divise m et est > 1, et si $\mathfrak{p}_0$ ne divise pas l, alors $\mathfrak{p}$ se décompose dans M/k.*

Démonstration. On utilise simplement le fait que G_1 (resp. G_0) est distingué dans G_0 (resp. G_{-1}).

Venons-en maintenant à la décomposition des discriminants. Le groupe G possède m caractères irréductibles de degré 1 (qui proviennent de G/H) et $\dfrac{l-1}{m}$ caractères irréductibles de degré m, qui sont induits par des caractères de degré 1 et d'ordre l de H, et qui sont conjugués sur le sous-corps de degré $\dfrac{l-1}{m}$ du corps des racines l-ièmes de l'unité. Notons ψ un caractère irréductible de degré m. On vérifie tout de suite que le

caractère de la représentation de permutation de G/g est somme des conjugués de ψ et du caractère unité. En utilisant [13], ch. VI, § 3, prop. 6, b et son cor. 1, on obtient:

2. 4. Proposition. *Soit $\mathfrak{F}$ le conducteur d'un caractère de degré 1 et d'ordre l de H. Les discriminants de K/k_0 et de M/k_0 sont donnés par les formules*

$$\mathfrak{d}_{K/k_0} = \mathfrak{d}_{k/k_0}^{\frac{l-1}{m}} \cdot \mathrm{N}_{k/k_0}(\mathfrak{F})^{\frac{l-1}{m}} \quad \text{et} \quad \mathfrak{d}_{M/k_0} = \mathfrak{d}_{k/k_0}^{l} \cdot \mathrm{N}_{k/k_0}(\mathfrak{F})^{l-1}.$$

Dans la pratique, on connaît le discriminant de k/k_0, et l'on doit préciser la norme de $\mathfrak{F}$. Voici deux résultats, dont le premier est relatif à la partie modérée du discriminant.

2. 5. Proposition. *La partie première à l de $\mathfrak{F}$ est un produit étendu à k d'idéaux premiers distincts de k_0 qui ont mêmes degrés résiduels dans k et dans $k_0(\mu_l)$.*

Démonstration. Seule la dernière assertion mérite une démonstration. Après complétion, on se trouve dans la situation de la théorie locale du corps de classes, k/k_0 étant non ramifiée. Le degré m de M/K est maintenant égal au degré résiduel de k/k_0; nous notons q le cardinal du corps résiduel. Nous allons montrer l'égalité $k = k_0(\mu_l)$. Comme M/k est totalement et modérément ramifiée de degré l, k contient μ_l, et l'on est ramené à prouver l'inégalité $[k_0(\mu_l) : k] \geqq m$. Quitte à changer de générateur pour g, on peut supposer que τ est le "Frobenius" dans k/k_0. Si x est une unité de k, $\tau x/x^q$ est alors une unité distinguée, si bien que τx et x^q ont même image dans H par l'application d'Artin. On a donc l'égalité $\tau\sigma\tau^{-1} = \sigma^q$, ce qui prouve l'inégalité cherchée, puisque q est d'ordre m modulo l.

[La démonstration ci-dessus donne en outre des indications sur la valeur possible de a modulo l.]

Pour énoncer la proposition suivante, on considère un idéal premier $\mathfrak{p}$ de k divisant l et ramifié dans M/k, et l'on note t son saut de ramification dans M/k (on a $H_t = H$ et $H_{t+1} = \{1\}$). On a $v_{\mathfrak{p}}(\mathfrak{d}_{M/k}) = (t+1)(l-1)$ ([13], ch. V, § 3, lemme 4), $t \geqq 1$ (puisque la ramification n'est pas modérée en $\mathfrak{p}$ dans M/k) et $t \leqq \frac{le_{\mathfrak{p}}}{l-1}$, $e_{\mathfrak{p}}$ désignant l'indice absolu de ramification de $\mathfrak{p}$ (cela se voit en majorant le discriminant d'un polynôme d'Eisenstein définissant M/k).

2. 6. Proposition. *L'entier t est premier à l'indice de ramification e de $\mathfrak{p}$ dans k/k_0.*

Démonstration. C'est clair si $e = 1$. Sinon, quitte à grossir k_0, on peut supposer que l'on a $m = e$ et que e est premier. On a $\sigma \in G_t$, $\sigma \notin G_{t+1}$, $\tau \in G_0$ et $\tau\sigma\tau^{-1}\sigma^{-1} = \sigma^{a-1} \notin G_{t+1}$. Donc ([13], ch. IV, § 2, cor. 1 à la prop. 9), $\tau^t \notin G_{t+1}$, i.e. e ne divise pas t.

2. 7. Remarque. Il résulte des propositions 2. 5 et 2. 6 que $\mathfrak{F}$ provient d'un idéal de k_0 si M/k est modérément ramifiée ou si $m \leqq 2$. Il n'en est pas de même en général, comme le montre l'exemple où $k_0 = \mathbb{Q}$ et $K = \mathbb{Q}(\sqrt[5]{2})$: le polynôme $X^5 - 2$ a pour discriminant $2^4 \cdot 5^5$, est d'Eisenstein en 2, et $(X+2)^5 - 2$ est d'Eisenstein en 5. Le discriminant de K est donc $2^4 \cdot 5^5 = 50000$, d'où $\mathfrak{F} = (2\sqrt{5})$.

§ 3. Théorie du corps de classes

On conserve les notations des paragraphes 1 et 2, et l'on suppose que k_0 est un corps local ou global de caractéristique zéro. Pour un tel corps E, on note C_E le groupe E^* ou le groupe des classes d'idèles de E. L'extension M/k est définie par un caractère χ tel que $(\tau \cdot \chi)(x) = \chi(\tau^{-1}x)$, et l'application d'Artin transforme la condition $\tau\sigma\tau^{-1} = \sigma^a$ en la condition $\tau \cdot \chi = \chi^{a^{-1}}$ (qui met en évidence le rôle du choix de a, déjà signalé au § 1). Le lien entre extensions K/k_0 de discriminant égal au discriminant de k/k_0 et extensions non ramifiées M/k de degré l est clair (cf. exemple 1. 1, (ii) et prop. 2).

Examinons la situation opposée dans laquelle le nombre de classes de k est premier à l. On se donne un idéal $\mathfrak{F}$ de k stable par g et vérifiant les conditions des propositions 2. 6 et 2. 7, et l'on cherche si $\mathfrak{F}$ est le conducteur d'une extension M/k galoisienne sur k_0 à groupe de Galois isomorphe à G. On est amené à chercher les caractères modulo $\mathfrak{F}$ stables par g, triviaux sur le groupe E_k des unités de k, qui ne sont pas définis modulo un diviseur strict de $\mathfrak{F}$ et qui ne proviennent pas de caractères définis sur un sous-corps de K. La présence des unités rend difficile l'énoncé de résultats généraux. Toutefois, on peut prévoir dans certains cas l'existence de corps du type cherché. L'exemple suivant est susceptible de diverses généralisations (cf. § 4):

3. 1. Proposition. *Soit k un corps cyclique totalement imaginaire dont le degré m divise $l-1$ et est une puissance de 2, et soit $p \neq l$ un nombre premier non ramifié dans $k/\mathbb{Q}$, ayant même degré résiduel f dans k et dans $\mathbb{Q}(\mu_l)$. Supposons que le nombre de classes de k est premier à l et que k n'est pas le corps $\mathbb{Q}(\mu_l)$, et notons k' le sous-corps réel maximal de k et d le nombre d'idéaux premiers au-dessus de p dans k' $\left(\frac{m}{d}\right.$ est l'ordre de p modulo l si $p \not\equiv 1$ modulo l et $d = \frac{m}{2}$ sinon — cf. prop. 2. 5$\left.\right)$. Alors, il existe exactement d extensions $M_1, \ldots, M_d$ cycliques de degré l sur k et galoisiennes sur $\mathbb{Q}$ dont les groupes de Galois G_i peuvent être définis par deux générateurs σ_i et un relèvement τ_i d'un générateur fixé τ de $k/\mathbb{Q}$, liés par les relations $\sigma_i^l = 1$, $\tau_i^m = 1$ et $\tau_i\sigma_i\tau_i^{-1} = \sigma_i^{a_i}$ avec a_i d'ordre m modulo l, et les a_i s'obtiennent à partir de l'un d'entre eux par multiplication par les racines d-ièmes de l'unité modulo l.*

Démonstration. L'ensemble des extensions cycliques de degré 1 ou l de k de conducteur divisant (p) est en bijection avec le $\mathbb{F}_l$-espace vectoriel X des caractères de $(\mathbb{Z}_k/(p))^*$ à valeurs dans $\mathbb{C}^*$ et d'ordre divisant l qui sont triviaux sur le groupe E_k des unités de k. Le groupe g opère sur X par $(\tau \cdot \chi)(x) = \chi(\tau^{-1}x)$, et les extensions qui sont galoisiennes sur $\mathbb{Q}$ sont associées aux droites de X qui sont stables.

Plaçons-nous d'abord dans le cas $p \not\equiv 1 \bmod l$. Le degré résiduel f de p dans k est alors >1 (prop. 2. 5), et p est de degré $\frac{f}{2}$ dans k'. L'ordre de $(\mathbb{Z}_k/(p))^*$ (resp. de $(\mathbb{Z}_{k'}/(p))^*$) est $u = (p^f - 1)^d$ (resp. $u' = (p^{\frac{f}{2}} - 1)^d$). Ecrivons $u = u_1 u_2$ où u_1 est une puissance de l et u_2 est premier à l. Pour tout $\varepsilon \in E_{k'}$ (groupe des unités de k'), on a $\varepsilon^{u'} \equiv 1 \bmod p$. Comme l'indice de $E_{k'}$ dans E_k est fini et premier à l et que u' n'est pas divisible par l, on a $\varepsilon^{u_2} \equiv 1 \bmod p$ pour tout $\varepsilon \in E_k$. Il en résulte que X est un espace vectoriel de dimension d sur $\mathbb{F}_l$ (dimension de la l-composante du groupe $(\mathbb{F}_{p^f}^*)^d$).

L'espace X définit une représentation de g sur $\mathbb{F}_l$, qui est rationnelle, car $\mathbb{F}_l$ contient les racines de l'unité d'ordre m. Comme g est transitif, X définit une représentation du quotient de g par le sous-groupe de décomposition g_{-1} isomorphe à la représentation régulière. Donc, X est somme directe de d droites qui sont des $\mathbb{F}_l[g/g_{-1}]$-modules deux à deux non isomorphes. Il y a donc exactement d droites stables, les exposants a_i de l'énoncé sont deux à deux distincts, et ils sont d'ordre m modulo l puisque les extensions $M_1, \ldots, M_d$ ne proviennent pas d'un sous-corps strict de k (un tel sous-corps serait contenu dans k'). Il reste à voir que les a_i^d coïncident modulo l. Cette propriété ne dépend pas du choix du générateur τ de g. Cela permet de ramener au cas où τ^d est le Frobenius dans l'extension complétée en un idéal de k au-dessus de p. Alors, on a $\tau^d \sigma \tau^{-d} = \sigma^p$ (voir la démonstration de la proposition 2. 5), donc $a_i^d \equiv p \bmod l$ pour tout i.

Si $p \equiv 1 \bmod l$, la l-composante de $(\mathbb{Z}_{k'}/(p))^*/\operatorname{Im} E_{k'}$ est facteur direct de la l-composante de $(\mathbb{Z}_k/(p))^*/\operatorname{Im} E_k$; cela montre l'existence de $d = \frac{m}{2}$ extensions du type cherché, et la démonstration s'achève comme précédemment; toutefois, il peut exister d'autres extensions galoisiennes de $\mathbb{Q}$ que $M_1, \ldots, M_d$, provenant d'extensions de k'.

3. 2. Remarque. On peut s'affranchir de l'hypothèse "m est une puissance de 2" à condition d'imposer des restrictions aux sous-corps stricts de k non contenus dans k'. On obtient également des résultats analogues en remplaçant (p) par $\mathfrak{P}^2$, $\mathfrak{P}$ désignant le produit des idéaux premiers de k au-dessus de l.

Le cas particulier où $k = \mathbb{Q}(\mu_l)$ est facile à étudier directement: il correspond aux "corps purs", de la forme $K = \mathbb{Q}(\sqrt[l]{b})$, $b \in \mathbb{Z}$. On peut prendre $b > 1$ et non divisible par la puissance l-ième d'un nombre premier. Dans ces conditions, en notant b_0 le produit des diviseurs premiers de m, on montre facilement:

3. 3. Proposition. *Le discriminant du corps $\mathbb{Q}(\sqrt[l]{b})$ est égal à $l^l b_0^{l-1}$ si $b_0^{l-1} \not\equiv 1 \bmod l^2$, et $l^{l-2} b_0^{l-1}$ sinon. Pour $l \neq 11$, le plus petit discriminant d'un corps pur est atteint pour $b = 2$, et est égal à $2^{l-1} l^l$ si $l < 1093$. (Pour $l = 11$, le discriminant minimal est $3^{10} 11^9 = 139\,234\,453\,205\,859$, correspondant au corps $\mathbb{Q}(\sqrt[11]{3})$.)*

§ 4. Petits discriminants

Pour appliquer la théorie du corps de classes à la détermination des discriminants minimaux des corps de degré l à clôture galoisienne de degré lm (m divisant $l-1$), il faut disposer des nombres de classes et des unités des corps cycliques de degré m jusqu'à des bornes difficiles à préciser a priori, dépendant du nombre l choisi. On dispose de tables très étendues de corps quadratiques d'origines très diverses. Pour les corps imaginaires, on dispose des tables de classes relatives confectionnées par Hasse pour les conducteurs $\leqq 100$ ([6]), et prolongées jusqu'au conducteur 200 par Hirabayashi et Yoshino ([8]). Pour les corps réels, des tables dans les cas $m = 3$ et $m = 4$ ont été faites par Mme Gras ([4], [5]) et, dans les cas $m = 6$, par Mäki ([9]), prolongées par Mäki lui-même jusqu'au conducteur 4000. C'est à l'aide de ces tables qu'ont été obtenus les résultats de ce paragraphe.

Pour $m=1$, il s'agit de corps cycliques. Les discriminants minimaux sont bien connus. Pour mémoire, il s'agit de $7^2=49$ si $l=3$, $11^4=14641$ si $l=5$, $29^6=594823321$ si $l=7$ et $23^{10}=41426511213649$ si $l=11$.

Pour $m=2$, il s'agit de corps à clôture galoisienne diédrale. Dans le cas imaginaire, on lit sur les tables de corps quadratiques le plus petit discriminant correspondant à une extension non ramifiée, puis l'on cherche si la proposition 3.1 permet de faire mieux. On constate qu'il n'en est rien pour $l\leqq 11$ (et même bien au-delà). Les discriminants minimaux sont -23 si $l=3$, $+47^2=2209$ si $l=5$, $-71^3=-357911$ si $l=7$ et $-167^5=-129891985607$ si $l=11$.

Dans le cas réel, on doit déterminer l'ordre de l'image du groupe des unités modulo les conducteurs a priori possibles. Les discriminants minimaux sont $2^2\cdot 37=148$ pour $l=3$, $401^2=160801$ pour $l=5$, $577^3=192100033$ pour $l=7$ et $1297^5=3670285774226257$ pour $l=11$.

La proposition suivante achève l'étude du degré 5 en résolvant la question pour $m=4$.

4.1. Proposition. (i) *Pour $l=5$ et $m=4$, les trois premiers discriminants de corps ayant une place réelle sont $2^4\cdot 13^3=35132$, $3^2\cdot 17^3=44217$ et $2^4\cdot 5^5=50000$, et il y a un corps (à isomorphisme près) pour chacun de ces discriminants.*

(ii) *Pour $l=5$ et $m=4$, le plus petit discriminant pour un corps totalement réel est $2^4\cdot 53^3=2382032$. Il y a (à isomorphisme près) un unique corps ayant ce discriminant; il définit une extension non ramifiée du corps $\mathbb{Q}(\sqrt{53+2\sqrt{53}})$.*

Démonstration. (i) L'existence et l'unicité des corps résultent de la proposition 3.1 pour le premier, de la divisibilité par 5 du nombre de classes relatif d'un unique corps de degré 4 et de conducteur 53 ([5], p. 162) pour le second et de la remarque 2.7 pour le troisième. La proposition 3.3 montre que le seul corps associé au corps k de discriminant 125 est le corps $\mathbb{Q}(\sqrt[5]{2})$ de discriminant 50000. Si M/k est non ramifiée, on a, f et m désignant les conducteurs de k et de son sous-corps quadratique, $d_k=mf^2\leqq 5\cdot 10^4$, d'où $f\leqq 100$ puisque $m\geqq 5$ et les tables de Hasse permettent de conclure. Il reste à examiner les corps k avec $d_k>125$ et h_k premier à 5. On vérifie alors à l'aide des tables de Hasse que le corps k de conducteur 13 est le seul compatible avec la proposition 2.5 conduisant à un corps K de discriminant $\leqq 50000$.

(ii) L'examen des tables de M.-N. Gras ([5]) montre que le discriminant $2^4\cdot 53^3$ est le plus petit pour lequel M/k est non ramifiée (il faut examiner les conducteurs $\leqq 690$). Pour un corps K de discriminant $\leqq 2^4\cdot 53^3$, la minoration $d_k\geqq 3^2\cdot 5^3$ impose au conducteur de M/k d'être un idéal principal engendré par l'un des entiers 2, 3, 6, $\sqrt{5}$, $2\sqrt{5}$, $3\sqrt{5}$, et 5 de k. La proposition 2.5 permet d'écarter les possibilités $\mathfrak{F}=(6)$ et $\mathfrak{F}=(3\sqrt{5})$. Pour montrer l'impossibilité des autres cas, on examine l'image modulo $\mathfrak{F}$ des "unités χ-relatives" données par la table de M.-N. Gras. Des calculs un peu fastidieux, qui ne sont pas reproduits ici, permettent de conclure.

Passons maintenant aux corps de degré 7 avec $m>2$. Le cas $m=6$ et K totalement réel pourrait peut-être se résoudre à l'aide des tables de Mäki. Le premier conducteur rencontré pour lequel le nombre de classes relatives est divisible par 7 étant relativement

grand (819), les calculs à faire peuvent s'avérer très longs et l'étude n'a pas été entreprise. En revanche les deux autres cas ont été résolus (propositions 4. 2 et 4. 4).

4. 2. Proposition. *Les deux plus petits discriminants de corps de degré 7 avec* $m=3$ *sont* $2^6 \cdot 73^4 = 1817487424$ *et* $313^4 = 9597924961$, *et il y a, à isomorphisme près, un seul corps par discriminant.*

Démonstration. On vérifie tout de suite sur les tables de M.-N. Gras que la plus petite possibilité avec M/k non ramifiée apparaît pour k de conducteur 313. Si $\mathfrak{F} \neq (1)$, on écrit $N_{k/\mathbb{Q}}(\mathfrak{F}) = a^3\, 7^x$, et on doit étudier les possibilités $(x, a) = (3, 1)$, $(2, 1)$, $(0, 11)$ et $(0, 2)$ (les autres sont éliminées par la proposition 2. 5). Une étude des unités permet de se limiter au cas de $\mathfrak{F} = (2)$, qui se résoud sans peine à l'aide de la proposition suivante, dont la démonstration est laissée au lecteur.

4. 3. Proposition. *Soit* k *un corps cubique cyclique dont le nombre de classes est premier à* 7 *et dans lequel* 2 *est inerte. Alors, il existe une extension cyclique de* k *de degré* 7 *et de conducteur* 2 *si et seulement si l'on a, pour une unité fondamentale* ε (*i.e. engendrant avec ses conjuguées le groupe des unités de norme* 1) *les congruences* $\mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon) \equiv \mathrm{Tr}_{K/\mathbb{Q}}(\varepsilon^{-1}) \equiv 1$ *modulo* 2.

Dans le cas du corps K de discriminant $2^6 \cdot 73^4$, l'unité ε de k est définie par le polynôme $X^3 + 49X^2 + 119X - 1$.

4. 4. Proposition. *Parmi les corps de degré* 7 *à une place réelle correspondant à* $m=6$, *le discriminant minimum* (*en valeur absolue*) *provient d'une extension non ramifiée d'un corps de conducteur* 143, *et est égal à* $-11^3 \cdot 13^4 = -38014691$.

Démonstration. Les tables de Hasse et de Hirobayashi-Yoshino montrent que ce discriminant est minimum parmi ceux des corps provenant d'une extension M/k non ramifiée (il faut examiner les conducteurs $\leqq 168$). Sinon, la proposition 2. 4 montre que le conducteur $\mathfrak{F}$ doit être l'un des idéaux $\mathfrak{P}^2$, $\mathfrak{P}^3$, $2\mathfrak{P}^2$, (2) et (3), où $\mathfrak{P}$ désigne l'idéal de k au-dessus de 7, supposé totalement ramifié, et que, si $\mathfrak{F} \neq (2)$, k doit être le corps $\mathbb{Q}(\mu_7)$, cas exclu par la proposition 3. 3 (K serait un corps pur). Les cas où $\mathfrak{F} = (2)$ (qui concernent quelques corps k contenant un corps cubique de conducteur 7, 9 ou 13) sont exclus à l'aide de la proposition 2. 5.

Pour les degrés >7, on ne peut obtenir que des résultats très partiels. En voici un:

4. 5. Proposition. *Si* $l=13$ *et* $m=3$, *les deux premiers discriminants sont* $3^{12} \cdot 13^{16} = 3{,}536\ldots 10^{23}$ *et* $1063^8 = 1{,}630\ldots 10^{24}$, *et il y a, à isomorphisme près, un seul corps par discriminant.*

Démonstration. On utilise les tables de M.-N. Gras et une étude des unités modulo 2 analogue à la proposition 4. 3.

4. 6. Remarque. Trouver les discriminants minimaux dans les trois cas où l'on a $l=13$ et $m \leqq 2$ n'est pas difficile.

On pourrait également, pour $m \leqq 3$, aborder l'étude de cas avec $l>13$. En revanche, les tables existantes ne permettent pas de conclure pour $l=13$ et $m \geqq 4$. Par exemple, les tables de M.-N. Gras en degré 4 permettent de voir qu'il existe un unique corps de discriminant $17^6 \cdot 89^9$ pour $l=13$ et $m=4$ (il est associé à une extension non ramifiée du corps $\mathbb{Q}(\sqrt{17(89+8\sqrt{89})})$, et que ce discriminant est minimal parmi les

corps associés à un corps k de conducteur $\leqq 4000$; mais on ne peut pas exclure l'existence d'un corps de type non ramifiée et de conducteur dans l'intervalle [4000, 6383]. Curieusement, il n'y a pas, pour m pair $\geqq 4$, de tables étendues de classes relatives dans le cas imaginaire, bien que la complexité des calculs mis en jeu ne crée pas de difficulté insurmontable. Signalons toutefois la table de Schrutka von Rechtenstamm qui donne des indications pour les conducteurs f avec $\varphi(f) \leqq 256$, cela quel que soit m.

§ 5. Théorie de Kummer

On conserve les notations des paragraphes 2 et 3, en supposant que k_0 n'est pas de caractéristique l. Pour $E \subset \bar{k}_0$, E' désigne l'extension $E(\zeta)$ de E, ζ désignant une racine de l'unité d'ordre l. L'extension M'/k' peut être engendrée par la racine l-ième d'un élément de k'. En fait, on peut rechercher les radicaux dans un sous-corps de k'. Soit G' le groupe de Galois de M'/k_0; identifions à H celui de M'/k'. Le groupe G' opère sur le groupe des caractères de H (le groupe $H^* = \mathrm{Hom}(H, \mu_l)$) par $(s \cdot \chi)(t) = s\,\chi(s^{-1}ts)$, opération tenant compte de l'action galoisienne de G' sur μ_l et de son action sur H par automorphismes intérieurs. Le noyau de cette opération est un sous-groupe de G' contenant H, qui invarie une sous-extension de k'/k_0 que l'on note traditionnellement $\tilde{k}$ (cf. [3]). Les radicaux sont définis par les résolvantes de Lagrange $\langle \theta, \chi \rangle = \sum_{t \in H} \chi(t^{-1})t\theta$: on a $s\langle \theta, \chi \rangle = \langle s\theta, s \cdot \chi \rangle$, ce qui montre que $\langle \theta, \chi \rangle^l$ est un élément de k'. Si l'on prend pour θ un élément primitif de K/k_0 et pour χ un caractère d'ordre l, on voit tout de suite que $\langle \theta, \chi \rangle^l$ est un élément primitif de $\tilde{k}/k_0$.

5. 1. Remarque. La notation $\tilde{k}$ est justifiée par le fait que $\tilde{k}$ ne dépend effectivement pas de l'extension M/k. Toutefois, τ étant fixé, le choix de a tel que $\tau\sigma\tau^{-1} = \sigma^a$ n'est pas indifférent. Eventuellement, nous écrirons $\tilde{k}_a$ au lieu de $\tilde{k}$.

Les corps $\tilde{k}$ associés aux différentes extensions k/k_0 cycliques de degré m sont des extensions cycliques de k_0, de degré divisant $l-1$ et divisible par $\dfrac{l-1}{m}$, et de degré effectivement égal à $l-1$ lorsque k et k'_0 sont des extensions linéairement disjointes de k_0 et que $k_0(\zeta_l)$ est de degré $l-1$ sur k_0 (les extensions K/k_0 pures sont celles pour lesquelles on a $\tilde{k} = k_0$).

Dans la suite, on se limitera au cas où $\tilde{k}$ est de degré $l-1$ sur k_0, le seul cas qui nous sera utile en dehors du cas trivial des extensions pures, en supposant en outre k et $k_0(\zeta_l)$ linéairement disjointes sur k_0.

On trouvera des résultats supplémentaires lorsque m est premier dans la thèse de troisième cycle de Cougnard ([2]).

5. 2. Proposition. *Soit $\alpha \in \tilde{k}$ tel que $M' = k'(\sqrt[l]{\alpha})$ et soit s un générateur du groupe de Galois $\tilde{g}$ de $\tilde{k}/k_0$. Il existe $b \in \mathbb{Z}$ engendrant $(\mathbb{Z}/l\mathbb{Z})^*$ et $\beta \in \tilde{k}$ tels que $s\alpha = \alpha^b\beta^l$.*

Démonstration. Identifions le groupe $(\mathbb{Z}/l\mathbb{Z})^*$ au groupe de Galois de k'/k au moyen de l'application qui associe à $i \in \mathbb{Z}$ premier à l l'automorphisme s_i de k'/k tel que $s_i\zeta = \zeta^i$, et soient θ un élément primitif de K/k_0 et χ un caractère d'ordre l de H. Quitte à remplacer α par un élément de $\tilde{k}$ de la forme $\alpha^m\gamma^l$, $(m, l)=1$, on peut supposer que l'on a $\alpha = \langle\theta, \chi\rangle^l$. On a alors $s_i\langle\theta, \chi\rangle = \langle\theta, \chi^i\rangle$ pour tout i premier à l. Par restriction, le groupe de Galois de k'/k s'identifie à $\tilde{g}$. On peut donc trouver $b \in \mathbb{Z}$ tel que s et s_b aient même action sur $\tilde{k}$; alors, $(s_b\alpha)/s\alpha \in \tilde{k}^{*l}$.

Il est commode de définir α dans $\tilde{k}^*/\tilde{k}^{*l}$, qui est un $\mathbb{F}_l[\tilde{g}]$-module. La proposition précédente montre que le module engendré par α est annulé par $s-b$ pour un b convenable.

5. 3. Proposition. *Pour b primitif modulo l, soit $\omega_b = \prod_{i \not\equiv 0, b} (s-i) \in \mathbb{F}_l[g]$. Si $\alpha \in \tilde{k}^*/\tilde{k}^{*l}$ est annulé par $s-b$, il existe $u \in \tilde{k}^*/\tilde{k}^{*l}$ tel que $\alpha = u^{\omega_b}$. (Nous adoptons la notation exponentielle pour l'action des groupes de Galois.)*

Démonstration. Soit φ_i ($i \not\equiv 0 \bmod l$) le caractère de $\tilde{g}$ à valeurs dans $\mathbb{F}_l$ tel que $\varphi_i(s) = i$. On a ainsi tous les caractères irréductibles de $\tilde{g}$, si bien que l'intersection des noyaux des φ_i pour $i \not\equiv b \bmod l$ est une droite de $\mathbb{F}_l[\tilde{g}]$. Cette droite contient ω_b, et ω_b^2 n'est pas dans le noyau de φ_b. Par conséquent ω_b^2 est proportionnel à ω_b et est non nul, et $u = \alpha^{\omega_b}$ convient.

La connaissance d'un élément u vérifiant la proposition 5. 3 permet de trouver un élément primitif de K/k_0:

5. 4. Proposition. *Soit $u \in \tilde{k}$ tel que u^{ω_b} ne soit pas une puissance l-ième dans $\tilde{k}$, et soit x une racine l-ième de u dans M'. Alors $\mathrm{Tr}_{M'/M}(x)$ est un élément primitif de K/k_0, de trace sur k_0 nulle.*

Cela résulte facilement de la théorie de Galois.

Connaissant maintenant un élément primitif de K/k_0, on peut au moins théoriquement calculer son polynôme caractéristique. Le calcul est évident pour $l=3$: on trouve $X^3 - 3u^{1+s}X - u^{1+s}\,\mathrm{Tr}(u)$ (Tr est la trace de K sur k_0). Le calcul pour $l=5$ est plus difficile. Or, il se trouve que la calcul fait par G. Gras ([3]) dans le cas particulier où $m=2$ s'applique à toutes les valeurs de m. Cela permet d'énoncer:

5. 5. Proposition. *Relevons ω_{-2} dans $\mathbb{Z}[G]$ en l'élément s^3+2s^2-s+3, et soit $X^5 + a_1X^4 + a_2X^3 + a_3X^2 + a_4X + a_5$ le polynôme caractéristique de la trace sur K d'une racine l-ième de $u^{\omega-2}$. On a:*

$$a_1 = 0, \qquad a_2 = -\frac{5}{2}\,\mathrm{Tr}(u^{1+s^2}),$$

$$a_3 = -5\,\mathrm{Tr}(u^{1+s+s^2}), \qquad a_4 = -5\left(\mathrm{Tr}(u^{2+s^2+s^3}) - \frac{1}{2}\,\mathrm{Tr}(u^{2+2s^2}) + \mathrm{N}\right)$$

et

$$a_5 = -\mathrm{N}\left(\mathrm{Tr}(u^{2-2s+s^2}) + 20\,\mathrm{Tr}(u^{1-s+s^2}) + 30\,\mathrm{Tr}(u) - \frac{25}{2}\,\mathrm{Tr}(u^{-1})\,\mathrm{Tr}(u^{1+s^2})\right).$$

(Tr *et* N *désignent la trace et la norme dans* $\tilde{k}/k_0$; *on a posé* $\mathrm{N} = \mathrm{N}(u)$.)

On montre (cf. [3], § 3) que le polynôme ci-dessus, lorsque l'on prend pour u une puissance 5-ième dans $\tilde{k}$, possède une racine rationnelle.

Pour achever ce paragraphe, nous allons indiquer une condition de ramification dans M/k des facteurs des idéaux premiers de k_0 qui ne divisent pas l.

5. 6. Proposition. *Pour que les facteurs d'un idéal premier $\mathfrak{p}_0$ de k_0 soient ramifiés dans M/k, il faut que $\mathfrak{p}_0$ soit totalement décomposé dans $\tilde{k}/k_0$ et qu'il existe un idéal premier de $\tilde{k}$ au-dessus de $\mathfrak{p}_0$ ayant un exposant dans u non divisible par l.*

Démonstration. En effet, si les idéaux premiers de k au-dessus de $\mathfrak{p}_0$ se ramifient dans M/k, les idéaux premiers de k' au-dessus de $\mathfrak{p}_0$ se ramifient dans M'/k', donc ont un exposant non nul dans α, donc dans u. En outre, si $\mathfrak{p}_0$ n'est pas totalement décomposé dans $\tilde{k}$, pour tout idéal $\tilde{\mathfrak{p}}$ de $\tilde{k}$ au-dessus de $\mathfrak{p}_0$, $\tilde{\mathfrak{p}}^{\omega_b}$ a un exposant dans α divisible par l.

5. 7. Remarque. Le fait que $\mathfrak{p}_0$ soit totalement décomposé dans $\tilde{k}_a$ pour au-moins une valeur de a est équivalent à la proposition 2. 5. Lorsque $\mathfrak{p}_0$ divise l, la non ramification en $\mathfrak{p}_0$ équivaut au fait que α est congru à une puissance l-ième modulo une puissance assez élevée d'un idéal de $\tilde{k}$ au-dessus de $\mathfrak{p}_0$ (cf. [7], § 39).

§ 6. Polynômes

Un certain nombre de polynômes correspondant aux corps décrits au § 4 sont bien connus pour $m \leqq 2$ et l petit. Les corps abéliens de degrés 3, 5, 7 et de discriminants 7^2, 11^4 et 29^6 sont définis par les polynômes X^3+X^2-2X-1, $X^5+X^4-4X^3-3X^2+3X+1$ et $X^7+X^6-12X^5-7X^4+28X^3+14X^2-9X+1$ de discriminants respectifs 7^2, 11^4 et $29^6 \cdot 17^2$. Les corps cubiques de discriminants -23 et $+148$ peuvent être définis par les polynômes X^3-X-1 et X^3+X^2-3X-1 de mêmes discriminants. Pour $m=2$, k imaginaire et $l=5$ et 7, Weber ([15], Band 3, p. 723) a donné les polynômes $X^5-X^3-2X^2-2X-1$ et $X^7-2X^6-X^5+X^4+X^3+X^2-X-1$ dont les discriminants ($+47^2$ et -71^3 respectivement) sont égaux à ceux des corps qu'ils définissent. Les procédés de Mestre, utilisant des courbes elliptiques ([11]), permettent de définir de nombreuses extensions cycliques non ramifiées de corps quadratiques de degrés $\leqq 7$ à l'aide de polynômes. En particulier, pour $m=2$, k réel et $l=5$, [11] fournit le polynôme $X^5-8X^4+15X^3-6X^2-2X+1$ de discriminant 401^2.

Nous allons maintenant nous occuper des corps décrits dans la proposition 4. 1. Pour le discriminant $2^4 \cdot 13^3$, le corps $\tilde{k}$ est de conducteur $5 \cdot 13$, et 2 y est totalement décomposé. Donc, $\tilde{k}=\mathbb{Q}(\sqrt{65+8\sqrt{65}})$. Une unité fondamentale "χ-relative" (cf. [5]) est

$$\eta = 18+2\sqrt{65}+3\sqrt{65+8\sqrt{65}}.$$

Soit $\omega = \dfrac{1+\sqrt{65+8\sqrt{65}}}{2}$. Alors, $u_0 = 1+\dfrac{(\omega-1)(7-\sqrt{65})}{2}$ engendre le carré d'un idéal au-dessus de 2. On doit prendre $u=\eta^x u_0$, $x \bmod 5$. La congruence à une puissance 5-ième modulo le carré d'un idéal au-dessus de 5 a lieu pour $x \equiv -1 \bmod 5$. En prenant

$u=\eta^{-1}u_0$, en effectuant un calcul numérique précisé par des congruences, et en définissant s par $s\omega=\dfrac{1+\sqrt{65-8\sqrt{65}}}{2}$, on aboutit au polynôme

$$X^5-35X^3-1595X^2-16840X-\frac{282991}{4},$$

qui, par la transformation $X\mapsto\dfrac{5(X-1)}{2}$, se transforme en

$$X^5-2X^4-4X^3-96X^2-352X-568,$$

de discriminant $(2^4\cdot 13^3)\cdot(2^4\cdot 10429)^2$ (modulo 10429, la racine double est 8069). Pour le discriminant $3^2\cdot 17^3$, on a le choix pour $\tilde{k}$ entre les deux corps de conducteur $3\cdot 5\cdot 17$ qui contiennent $\mathbb{Q}(\sqrt{85})$. A l'aide des unités données dans [5] et en essayant chaque fois ω_2 et ω_{-2}, on trouve les quatre polynômes

$$P_1(X)=X^5-10X^3-105X^2+2110X+14004,$$
$$P_2(X)=X^5-10X^3-105X^2+2110X-5121,$$
$$P_3(X)=X^5-10X^3-105X^2-440X-531,$$
$$P_4(X)=X^5-10X^3-105X^2-440X-1296,$$

dont les discriminants s'écrivent $(3^2\cdot 17^3)\cdot f_i^2$ avec

$$f_1=2\cdot 5^7\cdot 353,\quad f_2=5^{10},\quad f_3=5^4\cdot 59\quad\text{et}\quad f_4=2^7\cdot 5^5.$$

La transformation $X\mapsto 5(X+1)$ permet de trouver à partir de P_2 le polynôme $X^5+X^4-X^2+3X-1$ de discriminant $3^2\cdot 17^3$. En résumé, on a:

6. 1. Proposition. *Les corps de discriminants* $2^4\cdot 13^3$, $3^2\cdot 17^3$ *et* $2^4\cdot 5^5$ *décrits dans la proposition* 4. 1 *peuvent être définis par les polynômes respectifs* $X^5-2X^4-4X^3-96X^2-352X-568$, $X^5+X^4-X^2+3X-1$ *et* X^5-2.

La construction d'un polynôme définissant le corps de la proposition 4. 1, (ii) nécessite la détermination d'une classe d'ordre 5 dans un corps de discriminant 297754000 que nous n'avons pas entreprise.

§ 7. Remarques finales

Les résultats de cet article, joints aux commentaires de [10], § 7, permettent de trouver le discriminant minimal pour chaque type de permutation et chaque signature jusqu'au degré 5, à l'exception du cas A_5 totalement réel. (Les corps à groupe A_5 ayant une place réelle ont été étudiés par Buhler dans [1].)

L'étude analogue des corps résolubles de degrés 6 et 7 peut sans doute être faite au prix de quelques calculs, à condition d'utiliser des méthodes géométriques pour étudier les extensions cubiques des corps quadratiques, car les tables de corps de degré 4 dont on dispose ne sont pas assez étendues pour permettre l'utilisation de la théorie du corps de classes. Il est aussi sans doute possible de résoudre le cas des groupes S_6 et S_7 à l'aide de calculs d'une longueur modérée; du reste seuls deux cas sont en suspens (le degré 6 avec deux places réelles et le degré 7 avec cinq places réelles; cf. [10]). En revanche la recherche des discriminants minimaux pour les groupes A_6, A_7 et $PSL(3, 2)$, que l'on ne peut faire que par une détermination de polynômes, dépasse sans doute les possibilités actuelles.

Signalons pour terminer la thèse de Soicher ([14]), qui contient un exemple de chacun des types de permutation jusqu'au degré 7 (mais pas de chaque signature).

Bibliographie

[1] *J.-P. Buhler*, Icosahedral Galois Representations, Lecture Notes in Math. **654**, Berlin 1978.

[2] *J. Cougnard*, Sur les extensions galoisiennes, non abéliennes de degré pq du corps des rationnels (p et q premiers), Thèse de troisième cycle, Bordeaux, 1972 et C. R. Acad. Sc. Paris A, **274** (1972), 236—239.

[3] *G. Gras*, Extensions abéliennes non ramifiées de degré premier d'un corps quadratique, Bull. Soc. Math. France **100** (1972), 177—193.

[4] *M.-N. Gras*, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$, J. reine angew. Math. **277** (1975), 89—116.

[5] *M.-N. Gras*, Classes et unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$, Publ. Math. Besançon 1977—1978, fasc. 2 et Ann. Inst. Fourier **29** (1979), 107—124.

[6] *H. Hasse*, Über die Klassenzahl abelscher Zahlkörper, Berlin 1952.

[7] *E. Hecke*, Vorlesungen über die Theorie der algebraischen Zahlen, New York 1948.

[8] *M. Hirabayashi, K. Yoshino*, On the relative Class Number of the Imaginary Abelian Number Field. I, II, Memoirs of the College of Liberal Arts, Kanazawa Medical University, **9** (1981), 5—53 et **10** (1982), 33—81.

[9] *S. Mäki*, The Determination of Units in Real Cyclic Sextic Fields, Lecture Notes in Math. **797**, Berlin 1980.

[10] *J. Martinet*, Méthodes géométriques dans la recherche des petits discriminants, Sém. Théorie des Nombres de Paris, octobre 1983, Boston 1985.

[11] *J.-F. Mestre*, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, J. reine angew. Math. **343** (1983), 45—57.

[12] *G. Schrutka von Rechtenstamm*, Tabelle der (Relativ)-Klassenzahlen der Kreiskörper, Abh. Deutsche Akad. Berlin, Berlin 1954.

[13] *J.-P. Serre*, Corps locaux, Paris 1962.

[14] *L. Soicher*, The Computation of Galois groups, Thèse, Montréal 1981.

[15] *H. Weber*, Lehrbuch der Algebra. 3, deuxième éd., Braunschweig 1908.

College of Education, Korea University, 1. 5-Ka, Anam-Dong, Sungbuk-Ku, Séoul, Corée

L. A. associé au C.N.R.S. n° 226, U.E.R. de Math. et d'Informatique, Université de Bordeaux I, 351, cours de la Libération, F-33405 Talence Cedex

Eingegangen 15. April 1986