Chapitre II DÉCOMPOSITION, RAMIFICATION, DISCRIMINANT

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **18 (1972)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.05.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

D'autre part il est nécessaire que K_r soit réelle car: $(-1)^2 = 1 \in S_r$, implique, d'après le lemme I.1, $-1 \in S_i$ pour tout $i < r'$. Donc tous les sous-corps stricts de $K_{r'}$ sont réels.

Pour démontrer la réciproque, on peut remarquer que:

si $u_r = 0$, -1 se décompose dans les sous-groupes $T\left(n_r, \frac{n_r}{p_j}\right)$ de la façon suivante:

$$-1 = \prod_{1 \leq j \leq m_r} c_j^{\frac{p_j - 1}{2}}.$$

On déduit de la condition I.6.A *bis* que si $j \leq m_i$, alors $\frac{p_j - 1}{2} \equiv 0\ (2^{r-i+1})$ et compte tenu du lemme I.2 *bis*, $c_j^{\frac{p_j-1}{2}} \in S_r$. Donc $-1 \in S_r$ et K_r est réelle.

Donc si $u_r = 0$, I.6.B *bis* est une conséquence de I.6.A *bis* et on démontre l'existence de $K_{r'}$ comme précédemment.

Si maintenant $u_r \geq 2$, -1 se décompose dans $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$ et $T\left(n_r, \frac{n_r}{p_j}\right)$ sous la forme:

$$-1 = a_0 \prod_{1 \leq j \leq m_r} c_j^{\frac{p_j - 1}{2}}.$$

La condition I.6.A *bis* implique donc comme précédemment, que $c_j^{\frac{p_j-1}{2}} \in S_r$ d'où $-a_0 \in S_r$.

Si $u_r = 2$, $a_0 \notin S_r$ (lemme I.2 *bis*) donc les conditions I.6.A *bis* et I.6.B *bis* sont incompatibles.

Si $u_r \geq 3$, les conditions I.6.A *bis* et I.6.B *bis* impliquent donc $a_0 \in S_r$, d'où $\alpha_0 \equiv 0\ (2^r)$.

On termine la démonstration comme précédemment.

Chapitre II

DÉCOMPOSITION, RAMIFICATION, DISCRIMINANT

II.1. Rappels

Soient K et K' deux corps de nombres, K' étant abélien sur K. Soient A et A' leurs anneaux d'entiers respectifs et $\mathfrak{p}$ un idéal premier de A. $\mathfrak{p}A'$ se décompose en idéaux premiers de A' sous la forme: $\mathfrak{p}A' = (\prod_{1 \leq v \leq g} \mathfrak{p}_v)^e$

et pour tout v de 1 à g, $\frac{A'}{\mathfrak{p}_v}$ a pour dimension f sur $\frac{A}{\mathfrak{p}}$. f est le degré résiduel de $\mathfrak{p}_v$ sur K et e l'indice de ramification de $\mathfrak{p}_v$ sur K (ou de $\mathfrak{p}$ dans K'). On a les relations:

$$efg = [K':K] \quad \text{et} \quad N_{K'/K}(\mathfrak{p}_v) = \mathfrak{p}^f .$$

Les $\mathfrak{p}_v$, $1 \leq v \leq g$, sont exactement les idéaux premiers de A' contenant $\mathfrak{p}$.

Soit $G(K'/K)$ le groupe de Galois de K' sur K. L'ensemble des σ de $G(K'/K)$ tel que $\sigma(\mathfrak{p}_v) = \mathfrak{p}_v$ est un sous-groupe de $G(K'/K)$ ne dépendant pas de v et appelé groupe de décomposition de $\mathfrak{p}_v$ sur K (ou de $\mathfrak{p}$ dans K'). Son cardinal est égal à ef. S'il est égal à 1, on dit que $\mathfrak{p}$ se décompose complètement dans K'.

L'ensemble des σ de $G(K'/K)$ tel que $\sigma(x) - x$ appartienne à $\mathfrak{p}_v$ pour tout x de A', est un sous-groupe de $G(K'/K)$ ne dépendant pas de v et appelé groupe d'inertie de $\mathfrak{p}_v$ sur K (ou de $\mathfrak{p}$ dans K').

Son cardinal est égal à e. $\mathfrak{p}$ est dit ramifié dans K' si $e \geq 2$ ([1] chapitre 5; [2] chapitre 5).

Soit K'' un corps de nombres, contenant K' et abélien sur K, et soit A'' son anneau d'entiers. Si $\mathfrak{p}_v A''$ se décompose en idéaux premiers de A'' sous la forme: $\mathfrak{p}_v A'' = (\prod_{1 \leq v' \leq g'} \mathfrak{p}_{vv'})^{e'}$ et si f' désigne le degré résiduel de $\mathfrak{p}_{vv'}$ sur K', les quantités e', g', f' sont les mêmes pour tout v entre 1 et g. L'indice de ramification de $\mathfrak{p}$ dans K'' est ee' et son degré résiduel ff'. Si D est le groupe de décomposition de $\mathfrak{p}_{vv'}$ sur K et π l'application de $G(K''/K)$ sur $G(K'/K)$ qui à tout automorphisme de K'' fait correspondre sa restriction à K', alors $D \cap G(K''/K')$ est le groupe de décomposition de $\mathfrak{p}_{vv'}$ sur K' et $\pi(D)$ est le groupe de décomposition de $\mathfrak{p}_v$ sur K. On a un résultat analogue avec les groupes d'inertie ([3] chapitre 1).

On appelle corps de décomposition de $\mathfrak{p}$ dans K' le sous-corps de K' laissé invariant par les éléments du groupe de décomposition de $\mathfrak{p}$ dans K'. C'est le plus grand corps, compris entre K et K', dans lequel $\mathfrak{p}$ se décompose complètement. De même le corps d'inertie de $\mathfrak{p}$ dans K' est le sous-corps de K' laissé invariant par les éléments du groupe d'inertie de $\mathfrak{p}$ dans K'. C'est le plus grand corps compris entre K et K', dans lequel $\mathfrak{p}$ ne se ramifie pas ([4] chapitre 2).

Différente : L'ensemble des x de K' tels que $Tr_{K'/K}(xA') \subseteq A$, est un idéal fractionnaire de K' dont l'inverse est la différente de K' sur K notée $\delta_{K'/K}$. Elle est engendrée par les $F'(x)$, où x parcourt A' et F désigne le polynome minimal de x sur K. Si $\mathfrak{p}_1 \ldots \mathfrak{p}_m$ sont les idéaux de A' ramifiés sur K, alors:

$$\delta_{K'/K} = \prod_{1 \leq v \leq m} \mathfrak{p}_v^{h_v}.$$

Si e_v est l'indice de ramification de $\mathfrak{p}_v$ sur K on a: $h_v \geqq e_v - 1$ et $h_v = e_v - 1$ si et seulement si e_v est premier avec la caractéristique du corps $\frac{A'}{\mathfrak{p}_v}$. Le discriminant de K' sur K est $N_{K'/K}(\delta_{K'/K})$ et on a la formule de transitivité: $\delta_{K''/K} = \delta_{K''/K'}\, \delta_{K'/K}$ ([2] chapitre 4, [5] chapitre 3).

Corps cyclotomiques: Dans un corps cyclotomique $\Omega(p^s)$, (p premier) p est leur seul nombre premier ramifié et: $p = (1-\xi)^{\varphi(p^s)}$, ξ désignant une racine primitive $(p^s)^{\text{eme}}$ de 1, est la décomposition de p en idéaux premiers de $\Omega(p^s)$.

p est ramifié dans un corps cyclotomique $\Omega(n)$ si et seulement si p divise n. Si n s'écrit: $n = p^s n'$ avec n' premier avec p, alors le corps d'inertie de p dans $\Omega(n)$ est $\Omega(n')$ et l'indice de ramification de p dans $\Omega(n)$ est $\varphi(p^s)$. Si q est premier avec n, la classe de q modulo n est l'automorphisme de Frœbenius, et elle engendre dans $G(n)$ le groupe de décomposition de q dans $\Omega(n)$. Le degré résiduel de q dans $\Omega(n)$ est donc le plus petit entier f tel que: $q^f \equiv 1\ (n)$.

Si ξ est une racine primitive n^{eme} de 1, $\{1, \xi, \ldots \xi^{\varphi(n)-1}\}$ est une base de l'anneau des entiers de $\Omega(n)$ sur Z. Le discriminant de $\Omega(n)$ sur Q est:

$$\frac{n^{\varphi(n)}}{\prod p^{\frac{\varphi(n)}{p-1}}}$$

ce dernier produit étant étendu à tous les nombres premiers p divisant n ([5] chapitre 4).

II.2. Nombres premiers ramifiés dans une extension abélienne de Q

Lemme II.1.

> Soient K une extension abélienne de Q et $\Omega(n)$ le plus petit corps cyclotomique contenant K. Alors un nombre premier p se ramifie dans K si et seulement s'il divise n.

Si p est ramifié dans K, alors il est ramifié dans tout surcorps de K, donc dans $\Omega(n)$ et il divise n.

Réciproquement, si p divise n, posons $n = p^s n'$, avec n' premier avec p.

Alors le corps d'inertie de p dans $\Omega(n)$ est $\Omega(n')$ et son groupe d'inertie $T(n, n')$.
Soit π l'application canonique de $G(n)$ sur $G({}^{K}/_{Q})$ qui à tout automorphisme de $\Omega(n)$ fait correspondre sa restriction à K. π a pour noyau $G({}^{\Omega(n)}/_{K})$ et comme $\Omega(n)$ est le plus petit corps cyclotomique contenant K, on a donc:

$$\Omega(n') \not\supseteq K \quad \text{c'est-à-dire} \quad T(n, n') \not\subseteq G({}^{\Omega(n)}/_{K}) .$$

$\pi(T(n, n'))$ qui est le groupe d'inertie de p dans K, n'est donc pas réduit à l'identité et p se ramifie dans K.

II.3. Décomposition d'un nombre q premier, non ramifié dans K_r

K_r désigne une extension cyclique de degré p^r sur Q (p premier) et $(\Omega(n_i))_{1 \leq i \leq r}$ la suite de corps cyclotomiques associée. Les notations restent les mêmes qu'au premier chapitre. q est un nombre premier non ramifié dans K_r, c'est-à-dire d'après le lemme précédent, premier avec n_r.

Si p est impair et suivant que $u_r = 0$ ou $u_r \geqq 2$,

soit
$$q \equiv c_1^{\beta_1} c_2^{\beta_2} \dots c_{m_r}^{\beta_{m_r}} (n_r)$$

ou
$$q \equiv b_0^{\beta_0} c_1^{\beta_1} \dots c_{m_r}^{\beta_{m_r}} (n_r) ,$$

la décomposition de q dans $G(n_r)$.

On posera alors:

— Si
$$2 \leqq u_r \leqq r : V(q) = \alpha_0 \beta_0 + \sum_{2 \leq j \leq m_r} \alpha_j \beta_j - \beta_1$$

— Si
$$u_r = r + 1 : V(q) = \sum_{1 \leq j \leq m_r} \alpha_j \beta_j - \beta_0$$

— Si
$$u_r = 0 : V(q) = \sum_{2 \leq j \leq m_r} \alpha_j \beta_j - \beta_1$$

De même si $p = 2$ et suivant que $u_r = 0$, ou $u_r = 2$, ou $u_r \geqq 3$, soit

$$q \equiv c_1^{\beta_1} c_2^{\beta_2} \dots c_{m_r}^{\beta_{m_r}} (n_r) \quad \text{ou} \quad q \equiv a_0^{\beta_0} c_1^{\beta_1} \dots c_{m_r}^{\beta_{m_r}} (n_r)$$

ou

$$q \equiv a_0^{\beta_0} a_0'^{\beta'_0} c_1^{\beta_1} \dots c_{m_r}^{\beta_{m_r}} (n_r)$$

la décomposition de q dans $G(n_r)$. On posera alors:

— Si

$$3 \leqq u_r \leqq r+1 : V(q) = \alpha_0\beta_0 + \alpha'_0\beta'_0 + \sum_{2 \leq j \leq m_r} \alpha_j\beta_j - \beta_1$$

— Si

$$u_r = r+2 \qquad : V(q) = \sum_{0 \leq j \leq m_r} \alpha_j\beta_j - \beta'_0$$

— Si

$$u_r = 2 \qquad : V(q) = 2^{r-1}\beta_0 + \sum_{2 \leq j \leq m_r} \alpha_j\beta_j - \beta_1$$

— Si

$$u_r = 0 \qquad : V(q) = \sum_{2 \leq j \leq m_r} \alpha_j\beta_j - \beta_1$$

PROPOSITION II.1.

Soient K_r une extension cyclique de degré p^r sur Q et q un nombre premier, ne divisant pas n_r. Alors la décomposition de q en idéaux premiers de K_r est de la forme:

$$q = \prod_{1 \leq v \leq g_q} \mathfrak{q}_v$$

et g_q est le $PGCD$ de p^r et de $V(q)$.

Le groupe de décomposition de q dans $\Omega(n_r)$ est le sous-groupe de $G(n_r)$ engendré par la classe de q modulo n_r et la restriction de q, considéré comme automorphisme de $\Omega(n_r)$, à K_r engendre le groupe de décomposition de q dans K_r.

Le degré résiduel f_q de q dans K_r est donc l'ordre de $q\,S_r$ dans $\dfrac{G(n_r)}{S_r}$. Supposons par exemple p impair et $2 \leqq u_r \leqq r$ et considérons alors:

$$\begin{aligned} s &= (c_1^{\alpha_0} b_0)^{\beta_0} (c_1^{\alpha_2} c_2)^{\beta_2} \dots (c_1^{\alpha_{m_r}} c_{m_r})^{\beta_{m_r}} \\ &= b_0^{\beta_0} c_1^{V(q)+\beta_1} c_2^{\beta_2} \dots c_{m_r}^{\beta_{m_r}} \end{aligned}$$

D'après la proposition I.3, $s \in S_r$ et l'on a modulo n_r:

$$sq^{-1} = c_1^{V(q)}.$$

f_q est donc égal à l'ordre de $c_1^{V(q)}\,S_r$ dans $\dfrac{G(n_r)}{S_r}$ et comme l'ordre de $c_1 S_r$

est p^r (lemme I.2), on a donc:

$$f_q = \frac{p^r}{PGCD\left(p^r, V(q)\right)}$$

et

$$g_q = PGCD\left(p^r, V(q)\right).$$

II.4. Indice de ramification dans une extension K_r

Proposition II.2.

> Soient K_r une extension cyclique de degré p^r sur Q et $\left(\Omega\,(n_i)\right)_{1 \leq i \leq r}$ la suite de corps cyclotomiques associée à K_r. Pour tout i de 1 à r et tout j tel que $m_{i-1} < j \leq m_i$, l'indice de ramification de p_j dans K_r est p^{r-i+1}.
> Si $u_r \neq 0$, l'indice de ramification de p dans K_r est p^{r-l+1}.

Soit j tel que $m_{i-1} < j \leq m_i$. p_j divise donc n_i et ne divise pas n_{i-1}. C'est-à-dire que p_j se ramifie dans $\Omega\,(n_i)$ et ne se ramifie pas dans $\Omega\,(n_{i-1})$. D'après le lemme II.1, ceci implique que p_j se ramifie dans K_i et ne se ramifie pas dans K_{i-1}. K_{i-1} est donc le corps d'inertie de p_j dans K_r et l'indice de ramification de p_j dans K_r est égal à: $[K_r : K_{i-1}]$.

De même si $u_r \neq 0$, K_{l-1} est le corps d'inertie de p dans K_r.

II.5. Discriminant de K_r

Proposition II.3.

> K_r est une extension cyclique de degré p^r sur Q et $\left(\Omega\,(n_i)\right)_{1 \leq i \leq r}$ la suite de corps cyclotomiques associée. Le discriminant de K_r sur Q est:
>
> — *Dans le cas où* $u_r = 0$:
>
> $$\prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{p^{i-1}(p^{r-i+1}-1)}$$
>
> — *Dans le cas où* p est impair et $u_r \geq 2$:
>
> $$p^{p^{l-1}\left((r-l+2)p^{r-l+1} - \frac{p^{r-l+1}-1}{p-1} - 1\right)} \prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{p^{i-1}(p^{r-i+1}-1)}$$

— *Dans le cas où* $p = 2$ et $u_r = 2$:

$$2^{2^r} \prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{2^{i-1}(2^{r-i+1}-1)}$$

— *Dans le cas où* $p = 2$ et $u_r \geqq 3$:

$$2^{2^{l-1}((r-l+2)2^{r-l+1}-1)} \prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{2^{i-1}(2^{r-i+1}-1)}$$

Supposons tout d'abord $u_r = 0$. Désignons par A l'anneau des entiers de K_r. Pour tout j de 1 à m_r soit $p_j A = \prod_{1 \leq v \leq g_j} \mathfrak{p}_{jv}^{e_j}$ la décomposition de $p_j A$ dans K_r et soit f_j le degré résiduel de p_j dans K_r. Les p_j étant les seuls nombres premiers ramifiés dans K_r et leurs indices de ramification e_j étant premiers à p_j, la différente δ de K_r sur Q est:

$$\delta = \prod_{1 \leq j \leq m_r} \prod_{1 \leq v \leq g_j} \mathfrak{p}_{jv}^{e_j - 1}$$

Le déterminant D_f, de K_r sur Q, est donc $D = N_{K_r/Q}(\delta)$ et comme $N_{K_r/Q}(\mathfrak{p}_{jv}) = p_j^f$ on obtient:

$$D = \prod_{1 \leq j \leq m_r} p_j^{f_j g_j (e_j - 1)}$$

qui s'écrit également:

$$D = \prod_{1 \leq i \leq r} \prod_{m_{i-1} < j \leq m_i} p_j^{f_j g_j (e_j - 1)}.$$

Si $m_{i-1} < j \leqq m_i$, alors $e_j = p^{r-i+1}$ d'après la proposition II.2 et comme $e_j f_j g_j = p^r$, on obtient le résultat annoncé.

Supposons maintenant p impair et $u_r \geqq 2$.
Dans ce cas u_r et l sont liés par la relation $u_r = r - l + 2$. On notera toujours D le discriminant de K_r sur Q et on introduit la décomposition $\delta = \delta_0 \delta_1 \ldots \delta_{m_r}$ de la différente de K_r sur Q, en idéaux: $\delta_0, \delta_1, \ldots \delta_{m_r}$, tels que $D_0 = N_{K_r/Q}(\delta_0)$ soit une puissance de p et tels que $D_j = N_{K_r/Q}(\delta_j)$ soit une puissance de p_j. D s'écrira alors $D = D_0 D_1 \ldots D_{m_r}$. Le calcul de $D_1 D_2 \ldots D_{m_r}$ s'effectue comme dans la démonstration précédente. Pour calculer D_0, on introduit la différente δ' de $\Omega(n_r)$ sur K_r décomposée de la même façon en $\delta' = \delta_0' \delta_1' \ldots \delta_{m_r}'$ et $D'' = D_0'' D_1'' \ldots D_{m_r}''$ le discriminant de $\Omega(n_r)$ sur Q.
La formule de transitivité sur les différentes donne:

$$D_0'' = N_{\Omega(n_r)/Q}(\delta_0 \delta_0') = N_{\Omega(n_r)/Q}(\delta_0') N_{K_r/Q}(\delta_0^{[\Omega(n_r):K_r]})$$

d'où
$$D_0'' = N_{\Omega(n_r)/Q}(\delta_0') D_0^{\frac{\varphi(n_r)}{pr}}$$

Calcul de $N_{\Omega(n_r)/Q}(\delta_0')$:

Soient A et A_Ω les anneaux d'entiers respectifs de K_r et $\Omega(n_r)$ et soit $pA = \prod_{1 \leq v \leq g} \mathfrak{p}_v^e$ la décomposition de pA dans K_r et f le degré résiduel de p dans K_r. Soient:

$\mathfrak{p}_v A_\Omega = \prod_{1 \leq v' \leq g'} \mathfrak{p}_{vv'}^{e'}$ la décomposition de $\mathfrak{p}_v A_\Omega$ dans $\Omega(n_r)$ et f' le degré résiduel de $\mathfrak{p}_v$ dans $\Omega(n_r)$. L'indice de ramification e de p dans K_r est p^{r-l+1} (proposition II.2) et puisque l'indice de ramification ee' de p dans $\Omega(n_r)$ est $\varphi(p^{u_r}) = (p-1)p^{r-l+1}$, on a donc $e' = p-1$ et e' est premier à p. On en déduit que:

$$\delta_0' = \prod_{\substack{1 \leq v \leq g \\ 1 \leq v' \leq g'}} \mathfrak{p}_{vv'}^{p-2}$$

et comme $N_{\Omega(n_r)/Q}(\mathfrak{p}_{vv'}) = p^{ff'}$, on aura donc:

$$N_{\Omega(n_r)/Q}(\delta_0') = p^{ff'gg'(p-2)} = p^{\frac{(p-2)\varphi(n_r)}{(p-1)p^{r-l+1}}}$$

D'autre part on a $D_0'' = p^{\varphi(n_r)\left(r-l+2-\frac{1}{p-1}\right)}$ d'où l'égalité:

$$p^{\varphi(n_r)\left(r-l+2-\frac{1}{p-1}\right)} = p^{\frac{(p-2)\varphi(n_r)}{(p-1)p^{r-l+1}}} D_0^{\frac{\varphi(n_r)}{pr}}$$

dont on extrait la valeur de D_0.

Dans le cas $p = 2$ et $u_r = 2$; gardant les mêmes notations on a $e' = 1$ et $\delta_0' = 1$. On utilise alors comme précédemment la valeur $D_0'' = 2^{\varphi(n_r)}$.

Supposons maintenant $p = 2$ et $u_r \geq 3$:

On garde les mêmes notations que précédemment. On a cette fois: $u_r = r - l + 3$ et l'indice de ramification ee' de 2 dans $\Omega(n_r)$ est maintenant 2^{r-l+2} d'où $e' = 2$. δ_0' ne peut donc être obtenue comme précédemment. On introduit un corps E compris entre K_r et $\Omega(n_r)$ de la façon suivante: reprenant les notations introduites dans la proposition I.3 *bis* posons:

$$h = a_0'^{\frac{\alpha_0}{2^{l-1}}} a_0 \quad \text{et} \quad S = \{h, 1\}.$$

h est d'ordre 2, S est donc un sous-groupe de $G(n_r)$. Dans le cas où $l = 1$, c'est-à-dire $u_r = r + 2$, il apparaît immédiatement que S est inclus dans S_r. Si $l \geq 2$, c'est-à-dire si $3 \leq u_r \leq r + 1$ on constate que:

$\left(\frac{\alpha_0'}{2^{l-1}}+1\right)\alpha_0 \equiv 0\,(2^r)$ et qu'il existe donc un entier β tel que:

$$\left(\frac{\alpha_0'}{2^{l-1}}+1\right)\alpha_0 + 2^r\beta = p_1 - 1\,.$$

D'où

$$h = (c_1^{\alpha_0'} a_0')^{\frac{\alpha_0}{2^{l-1}}}\; c_1^{\alpha_0} a_0\, c_1^{2^r\beta}$$

qui montre que S est inclus dans S_r. E désigne le corps fixe de S, E contient donc K_r.

Le groupe d'inertie de 2 dans $\Omega(n_r)$ est $T\left(n_r, \frac{n_r}{2^{u_r}}\right)$, le groupe d'inertie de $\mathfrak{p}_{vv}$, sur E sera donc $T\left(n_r, \frac{n_r}{2^{u_r}}\right) \cap S = S$. $\mathfrak{p}_v$ n'est donc pas ramifié dans E et la différente de E sur K_r est première avec 2.

Si D' est le discriminant de E sur Q, et D_0' la plus grande puissance de 2 divisant D', on aura alors:

$$D_0' = N_{E/Q}(\delta_0) = N_{E/K_r}(D_0) = D_0^{\frac{\varphi(n_r)}{2^{r+1}}}$$

Il reste à calculer D_0'. Pour cela introduisons A_E l'anneau des entiers de E et ξ une racine primitive $(n_r)^{\text{eme}}$ de 1. A partir de l'égalité: $\xi^2 = -\xi^{h+1} + (\xi+\xi^h)\,\xi$, on constate par récurrence sur t que ξ^t peut toujours se mettre sous la forme $a + b\xi$, avec a et b dans A_E. Comme $\{1, \xi, \ldots \xi^{\varphi(n_r)-1}\}$ est une base des entiers de $\Omega(n_r)$ sur Z, on en déduit que $\{1, \xi\}$ est une base des entiers de $\Omega(n_r)$ sur A_E. Le polynome $X^2 - (\xi+\xi^h)\,X + \xi^{h+1}$ est le polynome minimal de ξ sur E et la différente δ'' de $\Omega(n_r)$ sur E sera donc l'idéal engendré par $\xi - \xi^h$.

La formule de transitivité sur les différentes appliquée entre Q, E et $\Omega(n_r)$ va donner:

$$D'' = D'^{[\Omega(n_r):E]}\, N_{\Omega(n_r)/Q}(\delta'') = D'^2\, N_{\Omega(n_r)/Q}(\delta'')$$

Pour obtenir la valeur de $N_{\Omega(n_r)/Q}(\delta'')$, montrons que ξ^{h-1} est une racine primitive $(2^{r-l+2})^{\text{eme}}$ de 1. En effet:

$h \in T\left(n_r, \frac{n_r}{2^{u_r}}\right)$ donc $h - 1 \equiv 0\left(\frac{n_r}{2^{u_r}}\right)$ et d'autre part, h étant premier à 2, on a $h - 1 \equiv 0\,(2)$.

Mais $h - 1 \not\equiv 0\,(4)$, sinon h appartiendrait à $T\left(n_r, \dfrac{n_r}{2^{u_r-2}}\right)$ et ce sous-groupe est engendré par a_0'.

On a donc finalement

$$h - 1 \equiv 0\left(\frac{n_r}{2^{r-l+2}}\right) \quad \text{et} \quad h - 1 \not\equiv 0\left(\frac{n_r}{2^{r-l+1}}\right)$$

On en déduit que

$$N_{\Omega(2^{r-l+2})/Q}(1 - \xi^{h-1}) = 2$$

et

$$N_{\Omega(n_r)/Q}(\delta'') = 2^{2^{\frac{\varphi(n_r)}{r-l+1}}}.$$

Comme D_0'' est égal à $2^{\varphi(n_r)(r-l+2)}$, on en déduit les égalités:

$$2^{\varphi(n_r)(r-l+2)} = D'^2 \,.\, 2^{2^{\frac{\varphi(n_r)}{r-l+1}}} = D_0^{\frac{\varphi(n_r)}{2^r}} \,.\, 2^{2^{\frac{\varphi(n_r)}{r-l+1}}}$$

D'où l'on déduit la valeur de D_0.

PROPOSITION II.4.

> Le discriminant de K_r, extension cyclique de degré p^r sur Q, ne dépend que de la suite de corps cyclotomiques associée à K_r. Réciproquement, si deux extensions cycliques de degré p_r sur Q, ont même discriminant sur Q, alors leurs suites de corps cyclotomiques sont égales.

C'est une conséquence de la proposition II.3.

Précisons pour la réciproque, que si K_r est une extension cyclique de degré p^r sur Q (p premier, par exemple) et si l'on connaît son discriminant D sur Q, alors les nombres premiers divisant n_r sont exactement ceux qui divisent D. L'exposant de p_j dans la décomposition de D en facteurs premiers n'est pas divisible par p^i si et seulement si $j \leq m_i$ c'est-à-dire si et seulement si p_j divise n_i. Ceci permet de préciser quels sont les diviseurs de n_i distincts de p. Si p ne divise pas D, on a $u_r = 0$ et alors tous les u_i sont nuls. Si p divise D, et comme $(r-l+2)\,p^{r-l+1} - \dfrac{p^{r-l+1} - 1}{p - 1} - 1$ est premier à p, on obtient, à partir de la valeur de l'exposant de p dans la décomposition de D, la valeur de l, donc la suite $(u_i)_{1 \leq i \leq r}$.