

## II.2. Nombres premiers ramifiés dans une extension abélienne de $\mathbb{Q}$

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.09.2024**

### **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.

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

Si  $e_v$  est l'indice de ramification de  $p_v$  sur  $K$  on a:  $h_v \geq e_v - 1$  et  $h_v = e_v - 1$  si et seulement si  $e_v$  est premier avec la caractéristique du corps  $\frac{A'}{p_v}$ . 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:  $p = (1 - \xi)^{\varphi(p^s)}$ ,  $\xi$  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  $\xi$  est une racine primitive  $n^{\text{eme}}$  de 1,  $\{1, \xi, \dots, \xi^{\varphi(n)-1}\}$  est une base de l'anneau des entiers de  $\Omega(n)$  sur  $Z$ . Le discriminant de  $\Omega(n)$  sur  $Q$  est:

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

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  $\pi$  l'application canonique de  $G(n)$  sur  $G(K/Q)$  qui à tout automorphisme de  $\Omega(n)$  fait correspondre sa restriction à  $K$ .  $\pi$  a pour noyau  $G(\Omega(n)/K)$  et comme  $\Omega(n)$  est le plus petit corps cyclotomique contenant  $K$ , on a donc :

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

$\pi(T(n, n'))$  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  $u_r \geq 2$ ,

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

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

— 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  $u_r \geq 3$ , 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

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