II.1. Rappels

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **29.03.2024**

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.