Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 18 (1972)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉTUDE ARITHMÉTIQUE DES CORPS CYCLIQUES DE DEGRE p' SUR LE CORPS DES NOMBRES RATIONNELS

Autor: Oriat, Bernard

Kapitel: INTRODUCTION

DOI: https://doi.org/10.5169/seals-45361

INTRODUCTION

Ce travail a pour objet l'étude arithmétique des extensions cycliques de degré une puissance d'un nombre premier sur le corps des rationnels, considérées comme sous-corps d'un corps cyclotomique. Le théorème de Kronecker (dont on pourra trouver une démonstration dans *Algebraic Number Theory*, J. W. S. Cassels et A. Fröhlich; chapitre VII, J. T. Tate; Academic Press) montre en effet que toute extension abélienne du corps des nombres rationnels est incluse dans un corps cyclotomique.

L'étude des extensions abéliennes du corps des nombres rationnels a déjà été traitée par plusieurs auteurs, en particulier H. W. Leopoldt, Zur Arithmetic in abelschen Zahlkörpern; *Jour. reine angew. Math.* 209, pp. 54-71 (1962).

Le présent travail n'a pas pour but de démontrer des résultats essentiellement originaux, mais de donner un exposé aussi élémentaire que possible des propriétés les plus importantes.

J'ai supposé connu et j'ai utilisé sans les citer explicitement des résultats concernant les propriétés élémentaires des groupes abéliens finis et la théorie de Galois dans les extensions abéliennes finies. Dans le premier chapitre, j'ai rappelé et employé la décomposition de $\left(\frac{Z}{n}\right)^*$ en produit direct de groupes cycliques (théorème chinois). Les propriétés des corps cyclotomiques utilisées ont été mentionnées au début de chaque chapitre.

Dans le premier chapitre, j'ai associé à toute extension K_r cyclique de degré p^r sur Q, la suite des plus petits corps cyclotomiques contenant respectivement chaque sous-corps de K_r. J'ai établi les conditions que doit vérifier une telle suite et réciproquement, j'ai obtenu toutes les extensions K_r dont cette suite est la suite associée.

Dans le deuxième chapitre, j'ai montré que la donnée d'une suite de corps cyclotomiques associée à une extension K_r est équivalente à la donnée du discriminant de K_r sur Q et j'ai calculé la valeur de ce discriminant.

Dans le troisième chapitre, j'ai énoncé des conditions équivalentes d'existence de bases d'entiers normales dans les extensions abéliennes sur

Q. J'ai montré que si une extension K_r ne vérifie pas ces conditions, on peut toujours obtenir une base d'entiers de K_r en complétant une base des entiers de K_{r-1}, sous-corps de K_r de degré p^{r-1}, avec $\varphi(p^r)$ conjugués d'un même entier.

Je tiens à exprimer ma profonde reconnaissance à M. le professeur Châtelet pour l'attention constante qu'il a manifestée à cette étude et pour les nombreux conseils qu'il m'a donnés.

Je remercie vivement M. le professeur Parizet qui a bien voulu examiner ce travail et faire partie du jury.

Je remercie également M. le professeur Bantegnie pour ses encouragements et M. le professeur Hellegouarch pour les entretiens qu'il a bien voulu m'accorder lors du commencement de ce travail.

Chapitre Premier

SUITE DE CORPS CYCLOTOMIQUES ASSOCIÉE A UNE EXTENSION CYCLIQUE DE DEGRÉ p^r SUR Q

I.1. Rappels et notations

Le corps des rationnels sera noté Q. Si n est un entier positif et ξ une racine primitive n^{eme} de 1, $Q(\xi)$ est le n^{eme} corps cyclotomique et sera noté $\Omega(n)$. Le degré, $[\Omega(n): Q]$, de $\Omega(n)$ sur Q est $\varphi(n)$, φ est l'indicateur d'Euler. Si n est impair, on a $\Omega(n) = \Omega(2n)$; c'est le seul cas où $\Omega(n) = \Omega(n')$ avec $n \neq n'$.

$\dfrac{Z}{n}$ désigne l'anneau des classes résiduelles modulo n et $\left(\dfrac{Z}{n}\right)^*$ est l'ensemble des classes résiduelles modulo n, premières avec n. C'est aussi le groupe multiplicatif des éléments inversibles de $\dfrac{Z}{n}$.

$\Omega(n)$ est une extension abélienne de Q. On notera $G(n)$ son groupe de Galois. A tout automorphisme σ de $\Omega(n)$ correspond un élément de $\left(\dfrac{Z}{n}\right)^*$,