Introduction

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **16 (1970)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **18.09.2024**

SUR UNE GÉNÉRALISATION DES SYMBOLES DE LEGENDRE-JACOBI

par P. Cartier (Strasbourg)

Introduction

Un théorème assez peu connu (Zolotareff, Frobenius) donne une interprétation des symboles de Legendre-Jacobi au moyen de la signature de permutations convenables. Cette interprétation suggère une généralisation de ces symboles, à laquelle nous consacrons dans ces pages une étude élémentaire. Les propriétés des symboles généralisés redonnent facilement les principaux résultats classiques de Legendre, Gauss et Jacobi et nous permettront d'étendre le théorème de Zolotareff-Frobenius au cas des corps de nombres algébriques. On peut utiliser les résultats de cette Note pour donner un exposé rapide des propriétés des symboles de Legendre-Jacobi, exposé qui différerait très peu de celui de Frobenius dans [2].

Première partie
La loi de réciprocité quadratique et le lemme de Gauss-Schering

1. *Résumé des résultats classiques* (Legendre, Gauss, Jacobi).

Soient a et b deux entiers, avec $b > 0$. On dit que a est *reste quadratique modulo* b s'il existe deux entiers x et y tels que $x^2 = a + by$, autrement dit, si la classe de a est un carré dans l'anneau des entiers modulo b. Gauss note $a\,R\,b$ cette relation et $a\,N\,b$ sa négation. Soient p et q deux nombres premiers, distincts de 2 et distincts entre eux. La loi de réciprocité quadratique, conjecturée par Euler, démontrée partiellement par Legendre, et établie par Gauss en 1796, affirme qu'il n'y a que les quatre possibilités suivantes:

$$\left.\begin{array}{l} p\,R\,q \text{ et } q\,R\,p \\ p\,N\,q \text{ et } q\,N\,p \end{array}\right\} \text{si } p \text{ ou } q \text{ est congru à 1 modulo 4,}$$

$$\left.\begin{array}{l} p\,R\,q \text{ et } q\,N\,p \\ p\,N\,q \text{ et } q\,R\,p \end{array}\right\} \text{si } p \text{ et } q \text{ sont congrus à 3 modulo 4.}$$

Le symbole de Legendre $\left(\frac{a}{p}\right)$ est défini pour un nombre premier $p \neq 2$ et un entier a non divisible par p; il vaut 1 ou -1 selon que a est reste