Gauss 和と平方剰余の相互法則

慶應義塾大学理工学部数理科学科 2 年 近田真治

2017 年 1 月 15 日

1 はじめに

p を奇素数, a を p の倍数でない整数とする. ある整数 x が存在して $x^2 \equiv a \pmod{p}$ が成立するとき, a は p を法として平方剰余, このような x が存在しないとき平方非剰余と言う.

p, q を相異なる奇素数としたとき, p が q を法として平方剰余かどうかと, q が p を法として平方剰余かどうかには平方剰余の相互法則と呼ばれる密接な関係がある. 平方剰余の相互法則は何通りも異なる証明が知られており, Gauss は生涯に 7 通りもの証明を与えた.

1 の原始 p 乗根たちに平方剰余記号で適切に符号をつけたものの和を Gauss 和という. 本講演は Gauss 和を利用して平方剰余の相互法則を示す方法を紹介する.

2 講演内容

まず, 有限巡回群の指標群について基本的なことを述べる. 次に Legendre 指標 (記号) を導入し, Euler 規準, 第一補充法則, 第二補充法則を示す. その後, Gauss 和を定義してその 2 乗の値を調べ, それを利用した平方剰余の相互法則の証明を紹介する. また, Gauss 和の 2 乗の値から Kronecker-Weber の定理の 2 次体の場合の証明が得られることも述べる.

予備知識として巡回群の定義を仮定する.

References

[1] 小野孝, 数論序説, 裳華房, 2001.
[2] 山崎隆雄, 初等整数論 数論幾何への誘い, 共立出版, 2015.
[3] 雪江明彦, 整数論 2 代数的整数論の基礎, 日本評論社, 2013.