

長岡亮介数学勉強会

「A History of Abstract Algebra by I.Kleiner」

第 26 回 (p49)

3 History of Ring Theory

3.2 Commutative ring theory 可換環論

3.2.1 Algebraic Number Theory 代数的数論

(ii) Reciprocity laws 相互法則

代数学で代数方程式を解くことが重要であると全く同じようにして、数論では合同多項式、

$$a_0 + a_1x + \cdots + a_mx^m \equiv 0 \pmod{n}$$

を解くことが重要である。 m が任意の場合は面倒だけど、2 次の場合

$$a_0 + a_1x + a_2x^2 \equiv 0 \pmod{n}$$

は、Disquisitiones Arithmeticae (ディスキジティオネス・アリトメティカエ数論講義: 1801 年) 書の中でガウスにより扱われた。2 次の合同式の場合は奇素数 p と q に対して

$$x^2 \equiv q \pmod{p}$$

を考慮するだけで十分である (偶数の場合は別個に考慮される必要がある)。ガウスは名高い平方剰余の相互法則を証明した。すなわち

$$x^2 \equiv q \pmod{p}$$

が解を持つのは $x^2 \equiv p \pmod{q}$ が解を持つ場合であって且つその時に限る。ただし $p \equiv q \equiv 3 \pmod{4}$ の時、 $x^2 \equiv q \pmod{p}$ が解を持つのは $x^2 \equiv p \pmod{q}$ が解を持たない場合である。これを「平方剰余の相互法則」という。

より高次 (べき) の剰余相互法則はどうか? すなわち、 $m > 2$ に対して $x^m \equiv q \pmod{p}$ の可解性と $x^m \equiv p \pmod{q}$ の可解性の間に「相互的な関係」があるか? ガウスは、有利整数の範囲内でそのような法則が適切に推測することさえできないという見方を取った。

以前に容認されていた数論の法則では、[相互法則の] 一般理論の基礎に十分ではない。そのような理論は、数論の領域を高次に拡大していくことを果てしなく要求することになってしまう。

本当にまるで予言者のような言い回しだ。ガウスは代数的整数の数論の基礎づけを要求していたのである。事実、ガウス自身はガウス整数

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

として知られるようになったものを導入し、それらが UFD を形成することを示すことによって、数論の世界を拡大しはじめた。これは、1829 年と 1831 年の 2 つの論文において彼は成した。その論文の中で、4 次剰余の相互法則を定式化するために彼は $\mathbb{Z}[i]$ を使用した。

およそ同じ時間に、ヤコビおよびアイゼンシュタイン (ガウスと同じように、未発表の論文で) が、3 次相互法則を定式化した。ここでは、ドメイン

$$Z[\rho] = \{a + b\rho : a, b \in Z\}$$

ρ が 1 の原始立方根である (すなわち、 $\rho^3 = 1, \rho \neq 1$) を考慮する必要があった。これは、また、UFD であると明らかにされた。より高次の相互法則の研究が続いた。しかしフェルマーの最終定理の場合と同様に、ここでも最初のいくつかを越えて新しい方法が必要であった。そして $Z[i]$ と $Z[\rho]$ と違って、そのような法則を定式化するために必要な高次の代数的整数環が UFDs ではなかったのである。[4]、[13] を見なさい。