「A History of Abstract Algebra」勉強会…第 10 回
(p19-20)
2 History of Group Theory
2.1.2 Number Theory　数論

1801 年の Disquisitiones Arithmeticae（数論講義）で、ガウスは先行する数論の多くを要約し、統一した。 この研究は数学者たちを丸 1 世紀全体にわたって支配続けた新しい方向を示すものであった。群論への影響に関して言えば、Disquisitiones Arithmeticae が有限アーベル群の理論を開始したきっかけとなったと言えよう。 実際、ガウスは群論の専門用語を一切使用せずに、これらの群の多くの重要な性質を述べた。

群は 4 つの異なる形態で登場しました。m を法とする(mod.m)整数加法群、m と互いに素な整数の乗法群、2 元 2 次形式の同値類の群、および 1 の n 乗根全体の群。そして、これらの例は数論的文脈で現れたが、ガウスはそれらを、現代代数の証明の明確な原型であることを用いて、アーベル群として扱った。

たとえば、ゼロを含まない整数モジュローp（p は素数）を考えて、彼は、それらはすべて単一の要素の全てのベキ（累乗）であることを示した。つまり、そのような整数の作る群 Z∗p（ゼットピースター）は巡回的である。

Zp は、p で割った時の剰余類、Z∗ は 0 を除いて作られる乗法群。

p を素数 7 として整数 5 の場合を考える。5 mod.7=5、5 2 mod.7=4、5 3 mod.7=6、5 4 mod.7=2、5 5 mod.7=3、 5 6 mod.7=1、 5 7 mod.7=5、 〜ー>p 乗で巡回する！

さらに、彼はこの群の生成元の数を決定し、それが φ（p − 1）に等しいことを示した。ここで、φ はオイラーの φ 関数。

オイラーの φ 関数とは、互いに素な自然数の個数。

φ(n)=n[] (1−1/pi)　 i=1〜k ただし，pi は n の素因数

12 と互いに素な 12 以下の自然数の個数は，12=2 ^2·3 より，12(1−1/2)(1−1/3)=4 個。

実際に全列挙すれば，1,5,7,11 の 4 つで正しいことが確認できる。

Z∗p の任意の要素が与えられて、彼は要素の order（この用語は使わなかったけれども）というものを定義し、要素の order(群の要素の個数/位数)が p − 1 の約数であることを示した。フェルマーの「小定理」、つまり p が a の倍数でない時、$a_{p-1} \equiv 1 \pmod{p}$ となるという「小定理」を証明するために、この結果を使用した。かくして群論的概念を用いて数論的な定理を証明したのであった。次に、t が p − 1 を割り切る正の整数であるならば、Z∗p の中に位数が t であるような要素（t 乗したら単位元になる）が少なくとも一つ存在しなければならない、本質的にラグランジュの巡回群の定理の逆である。

ラグランジュの定理とは、群 G の部分群の位数（要素の個数）は， G の位数の約数になる。

円分方程式と関連して彼が考えている 1 の n 乗根に関しては、彼はそれらも巡回群を形成することを示した。彼は、Z∗p について問いを立てて答えたのと全く同じように、この 1 の n 乗根を作る巡回群についても問いを立てて、答えた。

2 項 2 次形式を用いて整数を表現する問題は、17 世紀初頭のフェルマーにさかのぼる。（4n + 1 の形式の任意の素数は、$x^2 + y^2$ の 2 つの平方数の和として表すことができる、という彼の定理を思い出せ。）ガウスは Disquisitiones の大部分を 2 項 2 次形式の徹底した研究と、整数をそのような形式に表現すること（2 次形式論；エレガントな理論）に専念した。

2 項 2 次形式は、$ax^2 + bxy + cy^2$ ；a,b,c 整数 という形式の表わされる。ガウスはそのような形式に対する合成を定義し、K1 および K2 がそのような 2 つの形式ならば、1 つは K1 + K2 でその合成を表すことができるかもと気づいた。それから彼は、この合成は結合的で可換的であり、そこに単位元が存在すること、そして、各形式には逆形式があり、だからアーベル群のすべての性質を確認することを示した。

これらの驚くべき洞察にもかかわらず、ガウスが抽象群、または有限アーベル群の概念を持っていたと推論すべきではない。Disquisitiones での議論は非常に一般的であったけれども、彼が考えたさまざまなタイプの「群」のそれぞれが個別に取り扱われたのだった。　ーすべてのケースに適用される一体化した群論的な方法はなかった。
詳細については、[5]、[9]、[25]、[30]、[33]を参照してください。