

群論と代数的数論

名大教養 三宅克哉 (Katsuya Miyake)

1. 最も基本的な群の構造は数の世界に見られるが、そこにはもともと加法と乗法とがあり、群構造が認知される以前に、二の両者が複合した環ないし体の構造があった。従って数学史的な観点から群の構造の認知を問題にするときには、少し注意をはらう必要がある。加法と乗法との間にあるある程度の相似点の明確に意識されるようにならねばならない。

明確に群の構造に興味をひかれた例としては Fermat のあげられようか。

Fermat の小定理 素数 p に対し、これと素な整数 n について必ず $n^{p-1} \equiv 1 \pmod{p}$ が成り立つ。

二つの最も素朴な証明は加法的なもので、2 項係数を用いて

数学的帰納法により

$$\begin{aligned}(a+1)^p &= a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1 \\ &\equiv a^p + 1 \equiv a + 1 \pmod{p}\end{aligned}$$

とするもあてあろう。この方法は Euler が最初に (1736 年) 得た証明であった。Leibnitz も既に 1681 年頃、恐らくは Fermat とは独立にこの定理を再発見していたと思われる。彼の証明は、変数 $a, b, c, \dots$ についての合同式

$$(a+b+c+\cdots)^p \equiv a^p + b^p + c^p + \cdots \pmod{p}$$

を観察して、 $a=b=c=\cdots=1$ とするもあてあ、た。

Fermat 自身は証明を残してゐたが、しかし、Pascal と共に二項係数についての習知していたから、このような方法を知っていたとしてもよからうが、それ以上に、「乗法的証明」を有していたと思ふふいがある (Weil [43])。Euler は最晩年に至ってようやく、数論についてのほぼ Fermat の見ているものをそのまま (従って時代が下、命令だけは進んで) 見るに至ったと思ふふいだが、1758 年頃には「乗法的証明」を得、それを加法的なものに勝るとしてあり、更に Fermat の小定理を拡張して例の Euler の関数 φ を与えている (17

60年頃). この「乗法的証明」において有限アーベル群の構造に興味あるものとして認知されつつあるとしてよからう.

2. 代数的数については, やはり晩年の Euler と Lagrange によって 1770年頃の報告後に導入された. 2変数の2次形式の公式を導くために2次体が導入され, さらに3次体の数も用いられた. だがこの頃には代数的数自体が興味を持たれたわけがなく, 便法として導入されたであり, 「裏口から数論に登場した (Weil [43])」とされている.

このような公式は, 例之は

$$(u^2 + Av^2) \cdot (x^2 + Ay^2) = (ux \pm Avy)^2 + A(uy \mp vx)^2$$

であり, 2次体 $\mathbb{Q}(\sqrt{-A})$ 上では

$$\begin{cases} u^2 + Av^2 = (u + \sqrt{-A}v) \cdot (u - \sqrt{-A}v), \\ x^2 + Ay^2 = (x + \sqrt{-A}y) \cdot (x - \sqrt{-A}y), \end{cases}$$

と因数分解されることから直ちに得られる. この公式において $A=1$ の場合は, 古代に遡れる. 19世紀の半ばに至るまでは, 一般の2次体でも数論の対象としての実体とは見なされておらず, 2変数2次形式のほうに, 伝統的な実体であった.

二変数二次形式については1775年のLagrangeの記事が画期的である。彼は $GL_2(\mathbb{Z})$ の元による変換に基づく分類を行なった。数論から見ても群論と関連からしても、19世紀末の Gauss [20] の寄与は圧倒的である。彼は何故か

$$Ax^2 + 2Bxy + Cy^2 \quad (A, B, C \in \mathbb{Z})$$

なる形のものをとり (Lagrange は $2B$ ととり、単に B とした), しかも, 例之は) $= d$ と $Ay^2 + 2Bxy + Cx^2$ とを区別して $SL_2(\mathbb{Z})$ による分類を行なった。=d 故に Lagrange とは異なり, 2次体 $\mathbb{Q}(\sqrt{D})$, $D = B^2 - AC$, における order $\mathbb{Z} + \mathbb{Z} \cdot \sqrt{D}$ のイデアル類群と同等なものを得ることとなり, 其の genus 理論を通じて平方剰余の相互法則の分析にも適用し得た。さらに著しいのは, 一般的に「二次形式の composition」を導入し, 判別式を同じくする二次形式の類に可換群の構造を与え, 有限アーベル群の基本定理に相当する方法によって分類を明確にした。彼はしかも二群の演算を「+」という記号を用いて表し, 「ユークリッドの互除法」を駆使した。この点で Gauss が抽象有限アーベル群をとらせ, その群構造を巧みに用いた最初の人といふことが出来る。(Gauss [21] を参照のこと。)

二の「composition」は, 原理的には, 二次形式を2次体

において1次因子に分解し、2個の2次形式から、た1次因子の積を作り、得られる2個の primitive な $\mathbb{Z}$ 係数の2次式を新たな変数と見て $\mathbb{Q}$ 上への norm をとって新たな2次形式を作る操作と見てよく、上記の公式の一般化といつてよいが、Gauss は2次体を一切用いずにすべて $\mathbb{Z}$ 上で表現している。とはいえ、どう見ても α の「composition」は、数の加法「+」ではなく、数の乗法に根ざしているものがあることに注意すべきである。

α の Gauss [20] は 18 冊の著書をも含んでおり、彼に続く Abel, Jacobi, Dirichlet, Eisenstein, Kummer, Kronecker, Dedekind 等に決定的な影響を与えた。

3. Abel は、例之は $\sqrt{5} = 2\sqrt{5} - 1$ の等分点を用い、カハワ群が (n, n) 型アーベル群 $\frac{1}{n} \cdot \mathbb{Z}[\sqrt{n}]/\mathbb{Z}[\sqrt{n}]$ にあるアーベル多項式を与えており ([1])、さらに「アーベル多項式の特徴づけ」追々求めたカハワ理論に肉薄した ([2])。方程式論においても Lagrange の影響を失ふことは出来ない。彼は原理的には、例之は n 変数の有理関数体 $\mathbb{C}(x_1, \dots, x_n)$ の対称式の体 $\mathbb{C}(s_1, \dots, s_n)$ 上でのカハワ理論を与えたともいえる。これに加え、Gauss [19] による方程式論の整理と代

数学の基本定理の証明が与えた影響は大である。

4. 19世紀後半になるとガロワの理論が提示される([18]), Kummer [35] により、最終に本格的な代数的数論への第一歩が記されることになり、両者は Kronecker と Dedekind に強く影響を与える。この Kummer の仕事については、やはり 4 次剰余の相互法則についての Gauss [22] の影響も欠くことはできない。

Kronecker は Galois 以上の Abel の影響を受け、「アーベル多項式の特徴づけ」を強く意識するとともに([30]), 楕円関数の虚数乗法論を取りあげ、また Kummer の「理想数」により実体的な内実を与えようとし、結局は単項化定理を含む類体をつながる世界を夢想した([31, 32])。

Dedekind も 1850 年代後半には、群とガロワの理論についての講義を与えていた。Kronecker と競って一般的な代数的数論の基礎を整備し、特に Dedekind [6] により、体, module, 代数的整数となす maximal order とそれに基づくイデアル論等を、ほぼそのまま現在につながる形で与えた。

その頃になると C. Jordan [29] でもガロワの理論が完全に整備されたが、特筆すべきは、この著書ではまさに群が主人

公であり、Dedekind [6]に見られるものとは全く異った哲学と表現様式とを与えている。この点で C. Jordan はかなり本質的な影響を Dedekind と、彼に続く Frobenius に与えているといえよう。

Dedekind [8] において、代数的数体のガロワ拡大における素イデアルの分解様式が、ガロワ群を用いて完全に群論的に記述できることを示されている。この論文は 1882 年に書かれたが、発表は遅れて、Hilbert の「分解論」についての同内容の論文 [26] を発表するところまで 1894 年にまで公刊したもののようである。Dedekind は 1882 年には [7] において代数的数体の拡大におけるイデアルの分岐を定式化したため、ガロワ群による「分岐論」を得るにはいたらなかったように、結局これは Hilbert [27] の手になり、ヘルベルト理論と呼ばれる通りである。

この理論は、生命線の原因を Minkowsky [36] の依頼せざるを得ないといえ、1853 年の Kronecker が言明した

Kronecker-Weber の定理 有理数体上のアーベル多項式の根はすべて円分体に含まれる、

に対して、簡明な証明を見事に与えて驚異的であった。有名な

な報文[28]をまねて, Hilbert は代数的数論への必要不可欠な調和を強調している。Kronecker の「夢みたまへ」への、代数的数論の大飛躍が二の項にはいそる。

5. Frobenius は Dedekind に強く影響を受けたことは、彼の論文のいくつかに自身から書き残していることとみあせて Dedekind [9] から見えてくる。「予言者」Kronecker の「1 次の素イデアルの『密度』によって代数的数体を分類する」という「夢想」([33]) を具体化しようとして、彼はガロワ群の共役類の分析へと誘われ([11])、二つの重大な進展([12])を与えて、Hasse の命名により「Frobenius 置換」の名を残すこととなった。Dirichlet による2次形式の(従って自然に読みかえて2次体の)類数を与え、 L -関数を用いた解析的方法([10])を、Dedekind は、一般に、 $\mathbb{Q}$ 上のガロワ拡大の拡張する構想をみちめていたが、Frobenius はそれに強く影響されたが([9])、hypercomplex Größen, Gruppencharaktere および Gruppendeterminante の理論を展開し([13, 14])、有限群の線型表現にまで及ぼした([15])。二つは Artin の L -関数の結実することになるわけにある。

6. 今世紀に入ると, Schur が, 後に我々の関係に来る群の transfer を導入してより ([39]), また, 表現論の成熟に寄与して指標の理論が明快になり, さらに E. Noether-Artin から van der Waerden の *Moderne Algebra* への流れが生み出される.

代数的数論のほうでは, Weber が Kronecker の最愛の青春の夢の対して着実な歩を進める ([42]) とともに, Furtwängler が終に Hilbert の類体の存在を証明する ([16]). 更に 1920 年になると, 突然, Takagi が合同類体の理論を建てる ([40]), 一気に Hilbert-Weber-Furtwängler の流れを統合し, 完成させ, 同時に Kronecker の最愛の青春の夢を決した. Artin は直ちに Takagi 類体論の非アーベル化を志向し, 1924 年には一般相互法則を予想するとともに, アーティン-エル関数を導入する ([3]). 二つの群の指標の理論が完全に代数的数論へと入り込まれ, Kronecker-Dedekind-Frobenius の流れが定式化されると, 1926 年には Tschebotareff が終に密度定理を完成する ([41]). 二つの影響さした, 本人自身の予想にさえはるかに先んいて, 翌年には Artin が一般相互法則の証明を与えた ([4]).

同時に彼は, Kronecker の基本問題たる ([34]) 単項化定理を, その相互法則により群論化し, 数論固有の素因子論から

答したひとつの基本的な問題を, Γ マタペリアン群における transfers に関する問題に帰着せしめた ([5]). そのとき知られた老(?) Furtwängler はたまたま (1 年ほど) のうちにこれを決いてしまう ([17]).

この頃 Schreier, Magnus, Grün, Witt, Zassenhaus, Fitting, Brauer 等の群論畑の人々が巣立って行く.

一方では, このドイツにおける高揚の影響という, Weil や Chevalley に関し, N. Bourbaki の「成人として」誕生する.

なお, 群の transfers については, 上記のように, まずはじめに Schur [39] により導入されたが, transfer との命名は Hasse [25] による. (Hannink [24] 参照のこと.) また Zassenhaus の教科書 [45] により, transfers に関する基本的な結果として紹介されたこととなった Grün の定理については, Grün の原論文 [23] の脚註がどれなりに興味深い. 当初彼は transfers などを用いた結果を得たが, Hasse や Witt による助言により, transfers を用いて簡易化したとある.

以上では, 例えば, 群論に欠くべからざる Mathieu, Sylow, Burnside, Dickson, P. Hall 等をあげたが, 群論の創りか

ら見た 二つの時代の描写が望まれ...

④. さて上記のごとく、代数的数論と群論に関し、あいに注目して現代代数学の誕生期に至るたが、その後両者は互に固有の方向へと進展する。代数的数論においては、類体論の非アーベル化という方向を内包しながら、より深い方向とより広い方向へ歩を進めることになる。

上述の、群の transfers に帰した現象は、その後 Scholz, Taniyama, Iyanaga 等のもと、Tannaka, Terada による、いくらか孤立的な、しかし、重大な進展を見た。

ようやく最近になって、筆者は数論からの問題に誘われて特に群の transfers について中零性に関する箇處に一展開を求めた ([37])。代数的数論にとりては、二の他αにいくつかの徴候から見ても、「中零拡大」の研究がひとつの基本的な方向を与えてくると見られる。二の点、アーベル拡大αの場合に比べて、群論面での發育不良が実感されている。特に数論から見て現に興味深い問題αひとつを予稿集のまけであいたが、一応再記しておく。

問題 χ タベリアン p -群 G とそのアーベル部分群 A 2

G を交換子群 $[G, G]$ を含むものとして, G を A への移送 (transfer) $V_{G \rightarrow A}: G \rightarrow A$ とするとき, 指数 $[G: A]$ は $[\text{Ker } V_{G \rightarrow A}: [G, G]]$ と割り切れるか?

特に G/A が巡回群であるとき, $A = [G, G]$ であるとき, ある $\varphi \in \text{End}(G)$ に対し

$$A = G[\varphi] = \langle g^{-1} \cdot \varphi(g) \mid g \in G \rangle \cdot [G, G]$$

となるときは, 答は肯定的であることが知られている.
(最新のレビュー [38] に詳述している.)

もうひとつ数論から見た興味ある問題をあげよう.

問題 G を class 2 の p -群とすると, その Schur multiplier $H^2(G, \mathbb{Q}/\mathbb{Z})$ の構造を, G がアーベル群である場合に近しい程度に詳しく分析せよ.

ここでいうアーベル群である場合というのは, 例えは K. Yamazaki [44] の §2 を念頭に置いている.

文献

- [1] N.H. Abel, Recherches sur les fonctions elliptique, J.reine angew. Math., 2(1827); 3(1828) = Oeuvres I, 263-398.
- [2] ———, Memoire sur une classe particulière d'équations resolubles algébriquement, J.reine angew. Math., 4(1829) = Oeuvres I, 478-507.
- [3] E. Artin, Über eine neue Art von L-Reihen, Abh. Math. Sem. Univ. Hamburg, 3(1924), 89-108 = Coll. Papers, 105-124.
- [4] ———, Beweis des allgemeinen Reziprozitätsgesetzes, Abh. Math. Sem. Univ. Hamburg, 5(1927) = Coll. Papers, 131-141.
- [5] ———, Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, Abh. Math. Sem. Univ. Hamburg, 7(1930), 46-51 = Coll. Papers, 159-164.
- [6] R. Dedekind, Supplement X. Über die Komposition der binären quadratischen Formen, to Vorlesungen über Zahlentheorie von P.G. Lejeune Dirichlet (2. Auflage), 423-462(1871) = Werke III, 223-261.
- [7] ———, Über die Discriminanten endlicher Körper, Abh. König. Gesell. Wiss. Göttingen, 29(1882), 1-56 = Werke I, 351-396.
- [8] ———, Zur Theorie der Ideale, Nachr. König. Gesell. Wiss. Göttingen, Math.-Phys. (1894), 272-277 = Werke II, 43-48.
- [9] ———, Aus Briefen an Frobenius, Werke II, 414-442.
- [10] P.G. Lejeune Dirichlet, Recherches sur les formes quadratiques a coefficients et a indéterminées complexes, J.reine angew. Math., 24(1842), 291-371 = Werke I, 533-618.
- [11] G. Frobenius, Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul, J.reine angew. Math., 101(1887), 273-299 = Gesam. Abh. II, 304-330.
- [12] ———, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, Sitzungsab. König. Preuss. Akad. Wiss. Berlin(1896), 689-703 = Gesam. Abh. II, 719-733.
- [13] ———, Über Gruppencharaktere, Sitzungsab. König. Preuss. Akad. Wiss. Berlin(1896), 985-1021 = Gesam. Abh. III, 1-37.
- [14] ———, Über die Primfactoren der Gruppendeterminante, Sitzungsab. König. Preuss. Akad. Wiss. Berlin(1896), 1343-1382 = Gesam. Abh. III, 38-77.
- [15] ———, Über die Darstellung der endlichen Gruppen durch

- linear Substitutionen, Sitzungs. König. Preuss. Akad. Wiss. Berlin(1897), 944-1015 = Gesam. Abh. III, 82-103; II, *ibid.*(1899), 482-500 = Gesam. Abh. III, 129-147.
- [16] Ph. Furtwängler, Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers, Math. Ann. 63(1907), 1-37.
- [17] ———, Beweis des Hauptidealsatzes für Klassenkörper algebraischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, 7(1930), 14-36.
- [18] E. Galois, Oeuvres mathématiques d'Evariste Galois(Liouville ed.), J. math.pure appl., 11(1846), 381-444.
- [19] C. Gauss, Demonstratis Nova Theorematis Omnen Functionem Algebraicam Rationalem Integram(1799), Werke III, 1-31.
- [20] ———, Disquisitiones Arithmeticae, Lipsiae(1801) = Werke I.
- [21] ———, Démonstration de Quelques Théorèmes concernant les Périodes des Classes binaires du second Degré(1801), Werke II, 266-268.
- [22] ———, Theoria Residuorum Biquadraticorum I(1828), II(1832), Werke II, 65-92, 93-148.
- [23] O. Grün, Beiträge zur Gruppentheorie I, J.reine angew. Math. 174(1936), 1-14.
- [24] G. Hannink, Verlagerung und Nichteinfachheit von Gruppen, Monatsh. Math. Phys., 50(1942), 207-233.
- [25] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper I, Ia, II, Jahresb. Deutsch. Math.-Ver., 35(1926), 1-55; 36(1927), 233-311; Ergänzungsband 6(1930), 1-204.
- [26] D. Hilbert, Über die Zerlegung der Ideale eines Zahlkörpers in Primideale, Math. Ann., 44(1894), 1-8 = Gesam. Abh. I, 6-12.
- [27] ———, Grundzüge einer Theorie des Galoisschen Zahlkörpers, Nachr. Gesell. Wiss. Göttingen(1894), 224-238 = Gesam. Abh. I, 13-23.
- [28] ———, Die Theorie der algebraischen Zahlkörper, Jahresb. Deutsch. Math.-Ver., 4(1897), 175-546 = Gesam. Abh. I, 63-363.
- [29] C. Jordan, Traité des Substitutions et des Équations algébriques, Gauthier-Villars, Paris(1870).

- [30] L. Kronecker, Über die algebraisch auflösbaren Gleichungen, Monatsb. König. Preuss. Akad. Wiss. Berlin(1853), 365-374 = Werke IV, 1-11.
- [31] ———, Über die elliptische Functionen, für welche complex Multiplication stattfindet, Monatsb. König. Preuss. Akad. Wiss. Berlin(1857), 455-460 = Werke IV, 179-183.
- [32] ———, Brief an G.L. Dirichlet vom 17 Mai 1857, Nachr. Gesell. Wiss. Göttingen(1885), Werke V, 418-421.
- [33] ———, Über die Irreductibilität von Gleichungen, Monatsb. König. Preuss. Akad. Wiss. Berlin(1880), 155-162 = Werke II, 85-93.
- [34] ———, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, J.reine angew. Math., 92(1882), 1-122 = Werke II, 237-388.
- [35] E. Kummer, Zur Theorie der complexen Zahlen, Monatsb. König. Preuss. Akad. Wiss. Berlin(1845), 87-96 = J.reine angew. Math. 35(1847), 319-326 = Coll. Papers I, 203-210.
- [36] H. Minkowski, Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen, J.reine angew. Math. 107(1891), 278-297 = Gesam. Abh. I, 243-260.
- [37] K. Miyake, The Application of the Principal Ideal Theorem to p -Groups, Nagoya Math. J., 99(1985), 73-88.
- [38] ———, Algebraic Investigations of Hilbert's Theorem 94, the Principal Ideal Theorem and Capitulation Problem, Preprint series 1986, No.1, Dept. Math., Coll. Gen. Education, Nagoya Univ.(1986).
- [39] I. Schur, Neuer Beweis eines Satzes über endliche Gruppen, Sitzungsab. Preuss. Akad. Wiss.(1902), 1013-1019 = Gesam. Abh. I, 79-85.
- [40] T. Takagi, Über eine Theorie des relativ Abel'schen Zahlkörpers, J. Coll. Sci. imp. Univ. Tokyo, 41(1920), 1-133 = Coll. Papers, 73-166.
- [41] N. Tschebotareff, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, Math. Ann., 95(1926), 191-228.
- [42] H. Weber, Lehrbuch der Algebra III, Braunschweig(1908).
- [43] A. Weil, Number Theory. An approach through history from Hammurapi to Legendre, Birkhäuser, Boston·Basel·Stuttgart (1983).

- [44] K. Yamazaki, On projective representations and ring extensions of finite groups, J. Fac. Sci. Univ. Tokyo, Sect. IA Math., 10 (1964), 147-195.
- [45] H. Zassenhaus, Lehrbuch der Gruppentheorie I, Leipzig und Berlin (1937).