フロベニウス自己同型写像について

三宅　克哉（名古屋大　教養）

1．現在では「フロベニウス自己同型写像」といえば，例えば，有限体の上の万有体〈universal domain〉の場合にも用いられ，さらに代数幾何学的には，それから有限体上の多様体上に引き起こされる「フロベニウス写像」がしばしば用いられる．しかしここでは，ハセが高木-アルティンの類体論を詳細に解説した報文[H]で，彼が名付けた「フロベニウス記号」によって代数体のイデアルと対応させた代数体の自己同型写像の場合を見る．良く知られているように，また昨年のシムポジウムで触れたが（[M2,4] 参照），これはアルティンの相互法則（[A1]）に本質的に関わっており，さらにチェボタレフによる「フロベニウスの予想」（＝「チェボタレフの密度定理」）の証明（[Ts]）の方法がアルティンの相互法則の証明（[A2]）を産み出したのであった．ハセがフロベニウスの名を採ったのもまさにこれ（[Fr3]）による．それ以来「フロベニウス自己同型写像」と呼ばれることになる．しかし実は「フロベニウス自己同型写像」そのものは，円分体に関してはすでにクムマー [Ku1] が遥かに先んじてそれを取りだしており，デデキントは（絶対）ガロア拡大におけるイデアルの分解理論（[De4]）によってその正体を明かしていた．問題のフロベニウスの仕事 [Fr3] はこの分解理論に本質的に依拠している．

ここでは高木-アルティンの類体論との関わりから，「フロベニウスの予想」が提示されるまでの道筋のいくらかを辿ってみる．

２．フロベニウス自己同型写像といえば有限体の自己同型群の考察を欠くわけには行かないし，有限体といえばガロアを欠くことが出来ない．

もっともガウスはすでに彼の〈Disquisitiones Arithmeticae〉の草稿として有限素体の代数拡大の考察を用意していたが，出版に際してこれを割愛したようである．後に彼の全集のなかに出版される（[G2]）が，出版の時期からいえばこれはガロアに遅れることになる．もちろんガロアはこのガウスの仕事をまったく知ることはなかったろう．しかしさすがにガウスである；標数の素数を p とするとき有限素体 $GF(p)$ の有限次拡大にたいして，p 乗自己同型写像を導入して基本的なことをすべて押さえている．ただし彼の場合は抽象的な有限体の認識を表に出さずに，（有理）整数係数の多項式を $\bmod p$ のみならず，「素」多項式による合同関係によって考察している．

一方ガロア [Gal] はまったく現代風であって，旗色鮮明である；学術論文として練りあげたものでないだけに，彼がかかる対象をどのように認識していたかが直接に現われている．彼にとってはもとより $GF(p)$ の真の有限次拡大が問題であり，$GF(p)$ 上の高次既約多項式とその根が問題である．まず，ガウスの〈Disquisitiones Arithmeticae〉流の有理整数のあいだでの $\bmod p$ の合同関係について，混乱を避けてその記号「≡」を退けて，等号「＝」のみを用いる．そして与えられた $GF(p)$ 上の高次既約多項式 $Fx=0$ の「根」を，複素数の虚数単位の場合にならって「虚な記号の類として」〈comme des espéces de symboles imaginaires〉認識し，そのひとつを i と書き，それが $GF(p)$ 上に生成する拡大体を考察している．例えば既約多項式 Fx の次数を ν とするとき，この拡大体の要素が，有理整数の（$\bmod p$ の）代表系から $a, a_1, a_2, \ldots, a_{\nu-1}$ を取って

$$a + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1}$$

の形に一意的に表わされることを示している．当然p乗自己同型写像が本質的に利用されており，フェルマの小定理の拡張を与え，この拡大体の0でない要素がすべて1の$p^\nu-1$乗根であることを見ている；従って拡大体が次数νのみによることおよび各νにたいしてν次の拡大体GF(p^ν)が存在することが結論づけられる．

なお[M3]でもすでに名前をあげておいたが，シェネマン[S]が同じころに「高次合同関係」を考察している．しかしこれは（有理）整数環を素数の高い羃を法にして考察したものであって，一般の有限体の研究ではない；ベルヌーイ数についてのクムマーの一連の仕事ほどには直接の影響はなかったにしても，p-進数への先駆のひとつと見てもよかろう．

3．いよいよフロベニウス同型写像に移ろう．

有限次代数的数体のガロア拡大K/kが与えられたとし，そのガロア群をGとする；またKおよびkの全整数の環を$\mathfrak{O}$，$\mathfrak{o}$と表わす．体Kの素イデアル$\mathfrak{P}$にたいして$\mathfrak{p}=\mathfrak{P}\cap\mathfrak{o}$は$k$の素イデアルであり，剰余体$\mathfrak{K}=\mathfrak{O}/\mathfrak{P}$，$\mathfrak{k}=\mathfrak{o}/\mathfrak{p}$は有限体である；これら$\mathfrak{P}$，$\mathfrak{p}$の下にある（で割り切れる）有理素数を$p$とすれば，$\mathfrak{k}$の標数は$p$であり，位数$q=|\mathfrak{k}|$は$p$の羃である．さらに$f=[\mathfrak{K}:\mathfrak{k}]$を拡大次数とすれば，$\mathfrak{K}/\mathfrak{k}$のガロア群は$\mathfrak{K}$の$q$乗自己同型写像で生成される位数$f$の巡回群である．

もとのガロア拡大K/kに戻って，Gの部分群$Z(\mathfrak{P})=\{\sigma\in G \mid \mathfrak{P}^\sigma=\mathfrak{P}\}$を$\mathfrak{P}$の分解群という．部分群$Z(\mathfrak{P})$の各要素は明らかに$\mathfrak{K}/\mathfrak{k}$の同型写像を引き起こすが，この対応で$Z(\mathfrak{P})$からガロア群Gal$(\mathfrak{K}/\mathfrak{k})$への準同型写像が得られ，$K/k$の生成元を$\mathfrak{O}$から選べばわかるように，これは上への写像である．ここで特に$\mathfrak{K}$のq乗自己同型写像に写されるものを$\mathfrak{P}$のフロベニウス同型写像と呼ぶ．一般的にはこれは$\mathfrak{P}$にたいしてただ一つ定まるわけではない；この準同型写像の核を$V(\mathfrak{P})$とすれば，$Z(\mathfrak{P})$における$V(\mathfrak{P})$の剰余類として確定する．しかしK/kで分岐する有限個の$\mathfrak{P}$を除けば実は$V(\mathfrak{P})=1$となる．実際，拡大K/kにおいて素イデアル$\mathfrak{p}$は，$\mathfrak{p}$

$=(\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)^e$, $\mathfrak{P}_1=\mathfrak{P}$, $g=[G:Z(\mathfrak{P})]$, $e=|V(\mathfrak{P})|$, と分解され，$V(\mathfrak{P})$ の位数 e が $\mathfrak{p}$ の分岐指数である；また明らかに $\{\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_g\}=\{\mathfrak{P}^\sigma \mid \sigma\in G\}$.

これらのことは特に K と k が共に有理数体上のガロア拡大である場合にデデキント [De3, 4] に見られる；群論的なイデアルの分解法則に関する部分は [De4] として 1894 年に出版された；しかしその最後に付けられた日付は 1882 年 6 月 8 日である．序文には，1882 年 6 月 3 日のフロベニウスからの問い合わせにたいしてこの日付にこの内容をそのまま送付したものとある；もともとデデキントが 1877 年の論文 [De1] の § 27 Examples empruntés á la division du cercle で例示した事柄について，利用できそうな形の一般論をフロベニウスが求めたようである．またヒルベルトがこの内容を含む論文を 1894 年 7 月 7 日付けで発表するというので公表することにした旨が書かれている．フロベニウスもそのいきさつを，この我々の小論の焦点である [Fr3] の序文で証言している．デデキントの 1878 年の [De2] では，「フロベニウス自己同型写像」はまったく表にはあらわれていないが，有理素数が代数体でどのように分解・分岐するかが説明されてある；また理想数に関する「ゾロタレフの理論」についての 1874 年と 1877 年のゾロタレフの報告へのコメントが序文と二箇所の脚注にある．ただしゾロタレフがこの理論の全体像を公表したものは 1880 年の [Z 2] であるようである；彼のこの理論への動機は楕円積分の計算（[Z 1]）とその一般化を図るところから来ているとある．

4．もう少し数学に立ち入ってチェボタレフの密度定理を紹介する必要がある．これはフロベニウスが 1880 年に着想を得たあと 1896 年の論文 [Fr3] によってようやくその定式化を与え，特殊な場合を示して一般の場合を予想したものである．

上記 § 3 の記号にもどる．体 k の素イデアル $\mathfrak{p}$ から見る場合，もし最初に取った $\mathfrak{P}$ のかわりに他の $\mathfrak{P}_i=\mathfrak{P}^\sigma$, $\sigma\in G$，を取ったなら，$Z(\mathfrak{P})$ は $\sigma^{-1}Z(\mathfrak{P})\sigma$ で置き換えられる；従って K/k で分岐しない $\mathfrak{p}$ にたいしては，その上にある K の各素イ

デアルのフロベニウス自己同型写像全体が G のひとつの共役類となって確定し，それが対応する．（特に K/k がアーベル拡大，すなわち G がアーベル群であれば，これらのフロベニウス自己同型写像はすべて一致し，$\mathfrak{p}$ にたいしてただひとつ確定する．これら両者の対応がアルティンの相互法則の要であった．）このように，基礎の数体 k の数論的な要素である素イデアルがガロア群として与えられた有限群 G の代数的な構造のみで決まってしまう共役類と対応づけられる．ここではこれをフロベニウス対応と言うことにしよう．

数論的な要員をさらに整備しよう．体 k の素イデアルの集合 M にたいして次の極限値 $\Delta(M)$ が存在する場合にこれを M の（クロネッカー式）密度という：

$$\Delta(M) = \lim_{s \to 1+0} \frac{\sum_{\mathfrak{p} \in M} \frac{1}{N\mathfrak{p}^s}}{\log \frac{1}{s-1}}$$

もちろん一般の M について密度 $\Delta(M)$ が存在するはずもないが，特に k のすべての素イデアルの集合 $S(k)$ については $\Delta(S(k)) = 1$ となる．

定理（チェボタレフ）　有限次代数的数体のガロア拡大 K/k のガロア群を G とする．群 G の共役類 C にたいし，それにフロベニウス対応する k の素イデアル全体の集合を $M(C)$ とすると，その密度は必ず存在して $\Delta(M(C)) = |C| / |G|$ で与えられる．

すなわち数論的な密度 $\Delta(M(C))$ が完全に代数的に，いわば共役類 C の群 G 内での「密度」として確定する．

この定理は実に強力である；例えば G の要素 σ を与えたとき，G の巡回部分群 $\langle \sigma \rangle$ に対応する K の部分体を F とし，K/k に代えて K/F に定理を適用すれば，

σ そのものをフロベニウス同型写像にもつ K の素イデアルの存在ばかりか，それらの（K での）密度もわかる．

始めに触れたように，チェボタレフによるこの定理の証明法が，シュライヤー [Sc] による分析の助けをも得て，アルティンの相互法則の証明（[A2]）に大きく寄与した．しかし高木-アルティンの類体論は直接この定理には拠らずに証明でき，さらに類体論（によるアーベル拡大の存在とその特徴づけ）の簡単な応用としてこの定理を証明することができる．ただしこのとき，チェボタレフの方法から抽出されたものが形をかえて類体論の証明のなかに折り込みずみであるとも言える．

5．我々は上で素イデアルの集合の密度を，高木 [T] に倣って「（クロネッカー式）密度」と呼んだ．これは，上の形に定理を定式化したフロベニウスのそもそもの出発点に起因する．フロベニウスは 1880 年のクロネッカー [Kr4] の問題提起によって着想を得て以来，この定式化を 1896 年の [Fr3] によって公表するまでに 16 年を費やした．（チェボタレフ [Ts] によって証明が得られるまでになんとさらに 30 年が必要であった．）歴史を見る場合の常道ではあるが，これを理解するに当たって，我々は当時の数学界の状況を想像を逞しくして捉えておかなければなかろう．たとえガロアの理論がすでに当時十分の認知を得るに至っていたとしても，有限群論はまだまだ幼なかった；たとえば体論抜きでガロアの理論を書き上げたジョルダンの「置換論」（[J]）の出版は 1870 年のことであり，シローの定理（[Sy]）が出たのはようやく 1872 年であった．はたして当時の誰が，深い数学的現象を記述するに際して有限群が本質的に有効であると考え得たろう．ガロアの理論からさらに数論的な現象の深部にまで踏み込んだところにある事象が，ガロア群の代数的構造を用いればいとも簡明に記述されてしまうなどと誰が予期していたろう．

フロベニウスの出発点に立ってみよう．

クロネッカーの論文 [Kr4] のなかで特にフロベニウスが群論へと引き込れていく契機になったと思われる件（[Fr3]）は，次のようである：まずフロベニウスは [Fr3] の冒頭でその主定理を引用している．

定理（クロネッカー）　整数係数の多項式 $F(x)$ にたいして，素数 p を法にする合同式 $F(x) \equiv 0 \mod p$ の（重複度をこめた）根の個数を ν_p とするとき，すべての素数 p にわたる級数

$$\sum \nu_p \cdot p^{-1-w}$$

の和の w の値が正で無限に小さくなるときの極限値は $log\,(1/w)$ の値と比例し，ちょうど $log\,(1/w)$ に $F(x)$ の既約因子の個数を掛けたものと一致する．

さて各整数 k，$0 \le k \le n = \deg F$, にたいして $F(x) \equiv 0 \mod p$ がちょうど k 個の根を持つ素数を p_k と表わすことにすれば，上の級数は

$$\sum k \cdot \sum {p_k}^{-1-w}$$

となる．そこで次の極限が存在すると仮定する：

$$D_k = \lim_{w \to 0+} \frac{\sum {p_k}^{-1-w}}{log\,(1/w)} = \lim_{w \to 0+} \frac{\sum {p_k}^{-1-w}}{\sum p^{-1-w}}$$

ここで最後の項の分母はすべての素数にわたる和である．このとき，もし定理を認めるとすれば，等式

$$\sum k \cdot D_k = 1$$

が得られる．この等式こそがフロベニウスを捉えてしまったものであった．

現代の学生，あるいは数学者でさえ，果たして何人がここに群論に踏み込む着想を得るだろうか？

またクロネッカーはD_kの「存在を仮定したにすぎなかったが，ここでも『ヤマ』が当たって，」D_k「の存在はFrobeniusの部分的成功の後を継いでTschebotareffに至って確定したのである」（高木[T]）．

フロベニウスはこのあと，上で述べたように1882年にデデキントからイデアルの分解法則に関しての群論的な分析のノウト（[De4]）を得たあと，1887年には，副産物（?!）シローの定理の別証明[Fr1]とともに，まず群論的な部分[Fr2]を公表する．これについても，さらにフロベニウスが群指標の理論を独創するに至った背景にあるディリクレ[Di1, 2, 3]に発する数論的な問題意識についても，すでに[M1]で述べた；群指標の理論の独創に関してのデデキントの影響についてはホウキンス[Hk1, 2]が興味深い．

補記．すぐ上でクロネッカーの仕事についての高木のコメントを引いた．誤解があるやも知れないので，少し言葉を補っておく．数学における「定理」は厳密な証明が付けられて始めて「定理」であり，そこで始めて「数学的な言明」，あるいは端的に，「数学」になる，とする観点から見れば，このコメントは，まさに見事に，的確にクロネッカーの仕事の本質を衝いている．高木は，必ずしもガウス流を唯一尊んだ訳ではないだろうが，数学者としての自分自身をこの意味で非常に厳密に律していたものと思われる．しかも，例の彼の「高木節」とでも言うような語り口の背景に，今日の並の「数学者」には想像もつかないほどの深く広い数学的教養を身に付けていた．すなわち，常識が我々とまったく異なっているのだ．そう単純に「ヤマ」などという言葉づかいに乗ってしまうわけには行かない．

また数学史からの観点からすれば，そのように端的に切り捨てるわけには行かな

い．例えば「厳密な証明」にしても，それは当然その時点での数学界のレヴェルと相対的でしかありえない．高木も「この予言者の名を冠して『クロネッケル』式密度の称呼を用いたのである」．クロネッカーは彼にとっても単に「数学」の観点からアッサリと切り捨てられる者ではない．

とはいえ，クロネッカーの論文の多くは，特に彼がその構築をライフワークとした代数的数論に関するものについては，「数学的」に書かれていると言えるものではない；恐らく当時の常識からしても．しかし，例えば現代の物理学者達の論文と対比して見れば，わかりやすい．クロネッカーは，いまだ定義も，概念すらはっきりとはしない，しかし彼にとって現代の物理学者達の見るものよりも遥かに厳然，確固として存在する「数学的な事実」を発見し，それを報告しようとした．彼が見たもの自身は，例えば「一般的な関数」，「一般的な無限級数」と言ったあやふやな，捉え所のない新参者とは異なり，新しいとはいえどこから見ても伝統的で歴とした数学であった．彼はそこに新しく驚嘆すべきものを発見し，それを，書き方としては「数学的」ではなっかたにせよ，なんとか報告したのであった．そこに自身の数学者としての全身を賭けて．

例えば，有理数体上のアーベル多項式の根が1の羃乗根の有理整数係数の有理式として表わされることを「発見」して，躊躇わずにそれを「定理」〈Satz〉として報告した（[Kr1]）．有限体の扱い方を例にとれば，彼は決してガロア流を採らず，あくまでもガウス流にこだわり続けたろう．それは，彼の代数体における因子論（[Kr5]；高木 [T]，附録（3）も参照）からも想像がつく．例えば彼は，師でもあったクムマーの理想数の与え方（[Ku2, 3]）に満足せず，そのように本質的なものは「明確な数学的なもの」によって表示すべきであるとした；（そしてその嗅覚は確かであった）；まず虚二次体について，それを虚数乗法として持つ楕円関数の特異モデュライが本物の数として虚二次体の理想数を具現すること，および，そ

れらの数による虚二次体の拡大が不分岐であること，を発見した（[Kr2, 3]）；さらに「単項化定理」に基づく「類体」の存在を信じて彼の代数的数論構築ひとつの大きな指針とし，一般の代数的数体にたいして「単項化定理」を彼の流儀で定式化した（[Kr5]）．ヒルベルトがそこから出発して彼の類体論の構想へと進んだことは明らかである（[M2]）．また，例えばフライは，彼の数学史の論文 [F] で，虚二次体の絶対類体を「クロネッカーの類体」と呼んでいる．

文　献

[A1] E. Artin. Über eine neue Art von L-Reihen, Abh. Math. Sem. Univ. Hamburg 3 (1924), 89-108 = Collected Papers, 105-124.

[A2] _____. Beweis des allgemeinen Reziprozitätsgesetzes, Abh. Math. Sem. Univ. Hamburg 5 (1927), 353-363 = Collected Papers, 131-141.

[De1] R. Dedekind. Sur la Théorie des Nombres entiers algébriques, Paris, Gauthier-Villars, 1877, 1-121, Bulletin des Sci. math. astron., 1er série, t. XI, 2e série, t. I, 1876, 1877 (= Werke III, 262-296).

[De2] _____. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Abh. kgl. Ges. Wiss. Göttingen, Bd.23 (1878), 1-23 = Werke I, 202-230.

[De3] _____. Über die Discriminanten endlicher Körper, Abh. kgl. Ges. Wiss. Göttingen Bd. 29 (1882), 1-56 = Werke I, 351-396.

[De4] _____. Zur Theorie der Ideal, Nachr. kgl. Ges. Wiss. Göttingen, Math.-phys. Klasse, 1894, 272- 277 = Werke II, 43-48.

[Di1] P.G. Lejeune Dirichlet. Sur l'usage des séries infinies dans la théorie des nombres, Jour. reine angew. Math. Bd.18 (1838), 259-274 = Werke I, 357- 374.

[Di2] _____. Recherches sur diverses applications de l'analyse infinitésimale á la théorie des nombres, Jour. reine angew. Math. Bd.19 (1839), 324-369, Bd.21 (1840), 1-12 und 134-155 = Werke I, 411-196.

[Di3] _____. Recherches sur les formes quadratiques á coefficients et indeté rminées complexes, Jour. reine angew. Math. Bd. 24 (1842), 291-371 = Werke I, 533 -618.

[F] G. Frei. Heinrich Weber and the Emergence of Class Field Theory, in The History of Modern Mathematics, ed. by D.E. Rowe and J. McCleary, Academic Press, 1989.

[Fr1] G. Frobenius. Neuer Beweis des Sylowschen Satzes, Jour. reine angew. Math. Bd. 100 (1887), 179-181 = Ges. Abh. II, 301-303.

[Fr2] _____. Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul, Jour. reine angew. Math. Bd.101 (1887), 273-299 = Ges. Abh. II, 304-330.

[Fr3] _____. Über Beziehungen zwischen Primzahlen eines algebraischen Körpers und den Substitutionen seiner Gruppe, Sitzungsb. kgl. preuss. Akad. Wiss. Berlin (1896), 689-703 = Ges. Abh. II, 719-733.

[Gal] E. Galois. Sur la théorie des nombres, Journ. Math. pures appl. 11 (1846), 398-407 = Écrite et Mémoires Mathématiques d'Évariste Galois, par R. Bourgne et J.-P. Azra, Gauthier-Villars, Paris, 1962, pp.113-127.

[G1] C.F. Gauss. Disquisitiones Arithmeticae, 1801.

[G2] _____. Disquisitiones Generales de Congruentiis. Analysis Residuorum Caput Octavum, Gauss Werke II, Göttingen, 1863, 212-242.

[H] H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper II, Jahresber. dt. Math.-Ver. Erg. Bd. 6 (1930), 1-204.

[Hk1] Th. Hawkins. The origins of the theory of group characters, Arch. history exact sci. 7 (1970/71), 142-170.

[Hk2] _____. New light on Frobenius' creation of the theory of group characters, Arch. history exact sci. 12 (1974), 217-243.

[J] C. Jordan. Traité des substitutions et des équations algébriques, Gauthier-Villars, Paris, 1870.

[Kr1] L. Kronecker. Über die algebraisch auflösbaren Gleichungen, Monatsber. König. Preuss. Acad. Wiss. Berlin (1853), 365-374 = Werke IV, 1-11.

[Kr2] _____. Über die elliptische Functionen, für welche complex Multiplication stattfindet, Monatsb. König. Preuss. Acad. Wiss. Berlin (1857), 455-460 = Werke IV, 177-183.

[Kr3] _____. Über die complex Multiplication der elliptischen Functionen, Monatsb. König. Preuss. Acad. Wiss. Berlin (1862), 363-372 = Werke IV, 207-217.

[Kr4] _____. Über die Irreductibilität von Gleichungen, Monatsb. König. Preuss. Acad. Wiss. Berlin (1880), 155-162 = Werke II, 85-93.

[Kr5] _____. Grundzüge einer arithmetschen Theorie der algebraischen Grössen, Jour. reine angew. Math. 92 (1882), 1-122 = Werke II, 237-388.

[Ku1] E. Kummer. Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen, Jour. reine angew. Math. Bd. 30 (1846), 107-116 = Collected Papers I, 193-202.

[Ku2] _____. Zur Theorie der complexen Zahlen, Monatber. kgl. preuss. Wiss. Berlin (1845), 87-96 = Jour. reine angew. Math. Bd.35 (1847), 319-326 = Collected Papers I, 203-210.

[Ku3] _____. Über die Zerlegung der aus Wurzeln der Einheit gebildeten complex Zahlen in ihre Primfactoren, Jour. reine angew. Math. Bd.35 (1847), 327-367 = Collected Papers I, 211-251.

[M1] K. Miyake. A note on the arithmetic background to Frobenius' theory of group characters, Expo. Math. 7 (1989), 347-358.

[M2] _____. The Establishment of the Takagi-Artin Class Field Theory, Preprint series 1990, No.12, Coll. Gen. Educ., Nagoya Univ. Submitted to Proceedings of The Tokyo History of Mathematics Symposium 1990.

[M3] _____. デデキントの数論について，津田塾大学　数学・計算機科学研究所報 1 (1991), 22-31.

[M4] _____. アルティンの相互法則ついて，津田塾大学　数学・計算機科学研究所報 4 (1992), 44-53.

[S] Schönemann. Gründzuge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist, Jour. reine angew. Math. Bd.31 (1846), 269-325; Von denjenigen Moduln, welche Potenzen von Primzahlen sind, Jour. reine angew. Math. Bd.32 (1846), 93-105.

[Sc] O. Schreier. Über eine Arbeit von Herrn Tschebotareff, Abh. Math. Sem. Univ. Hamburg 5 (1927), 1-6.

[Sy] L. Sylow. Théorèmes sur les groups de substitutions, Math. Ann. 5 (1872), 584-594.

[T] 高木貞治. 代數的整數論，岩波書店，1948；第2版，1971.

[Ts] N. Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, Math. Ann. 95 (1926), 191-228.

[Z1] M.G. Zolotareff. Sur la Méthode d'intégration de M. Tchebichef, Journ. de Math. pures appl. 2e série, 16 (1874), 161-188.

[Z2] _____. Sur la théorie des nombres complexes, Journ. de Math. pures appl. 3e série, 6 (1880), 51-84, 129-166.