非アーベル的相互法則

HIRAMATSU, Toyokazu / 斎藤, 正顕 / 平松, 豊一 / SAITO, Seiken

(出版者 / Publisher)
法政大学情報メディア教育研究センター
(雑誌名 / Journal or Publication Title)
Bulletin of Research Center for Computing and Multimedia Studies, Hosei University / 法政大学情報メディア教育研究センター研究報告
(巻 / Volume)
19
(開始ページ / Start Page)
55
(終了ページ / End Page)
66
(発行年 / Year)
2006-03-23
(URL)
https://doi.org/10.15002/00025062

非アーベル的相互法則

斎藤 正顕　　平松 豊一

法政大学大学院工学研究科システム工学専攻

21 世紀の数学は, 非アーベル的数学であるといわれている. アーベル群とかかわる数学をアーベル的数学といったのは ベェイユ である. アーベル群対非アーベル群の対比は, 自然現象や工学的現象での線形対非形の対比にたとえられる. 例えば, 非線形制御を扱うのにそれを線形制御で近似して議論する場合があるが, それは丁度可解群がアーベル群の有限ステップで得られることに対応している. しかし, 非線形をそれ自身で扱わなければならない場合があるように, アーベル群の範疇では扱えない群がある. その真に非アーベルな群を単純群というが, その最初の例が 5 次の交代群 A_5 である（単純群は, 決して単純な群ではない）. この論説では, S_5 をガロア群にもつ 5 次方程式

$$x^5 - x - 1 = 0$$

の非アーベル性を検討する.

1 はじめに

相互法則はガウスに始まり, クンマーの巾剰余の相互法則, そしてアーベル的数学の頂点ともいうべき高木・アルティンによる類体論, 更にはラングランズによる非アーベル的相互法則の予想へとつながる 200 年を越える壮大な数論の流れである. 非アーベル的相互法則についてみれば, ラングランズの視点は表現論的であり, それは枠組みを決めるには適しているが, 肉付けには適していないように我々は思う. そこで, この論説では原点に帰り, 真に非アーベルな最初の例である $f(X) = X^5 - X - 1$ の場合をとり上げ, その非アーベル性を検討する.　これが非アーベル的相互法則への突破口となることを期待したい.

2 高次相互法則

2.1 $\mathrm{Spl}(f)$

P を素数全体の集合とする. $f(X) \in \mathbb{Z}[X]$ を整係数でモニックな既約多項式とし, p を素数とする. この時 $f(X)$ の法 p による還元を $f_p(X)$ とかく. もし $f_p(X)$ が $\mathbb{F}_p[X]$ において異なる一次式に因数分解されるならば, $f(X)$ は法 p で完全分解するという. このとき集合 $\mathrm{Spl}(f)$ を次で定義する:

$$\mathrm{Spl}(f) := \{p \in P : f \text{ は法 } p \text{ で完全分解}\}.$$

f の $\mathbb{Q}$ 上の最小分解体を K_f とする. このとき集合 $\mathrm{Spl}(K_f)$ を次で定義する:

$$\mathrm{Spl}(K_f) := \{p \in P : (p) \text{ は} K_f \text{ で完全分解}\}.$$

次の定理により $\mathrm{Spl}(f) = \mathrm{Spl}(K_f)$ が従う:

Theorem 1 (Dedekind-Kummer [1]) θ を有理数体 $\mathbb{Q}$ 上の代数的整数とし, f を θ の $\mathbb{Q}$ 上の最小多項式とし, 数体 $K := \mathbb{Q}(\theta)$ の代数的整数環を $\mathfrak{O}_K$ とする. このとき $p \nmid [\mathfrak{O}_K : \mathbb{Z}[\theta]]$ なる素数に対し $f_p(X)$ が モニック既約多項式 $P_i(X) \in F_p[X]$ の積で

$$f_p(X) = \prod_{i=1}^{g} P_i(X)^{e_i},$$

のように分解されることと, (p) が K において次のように素イデアル分解されることが同値である:

$$p\mathfrak{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}.$$

ここに $\mathfrak{P}_i$ は p 上の K の素イデアルで, その形は $\mathfrak{P}_i = (p, P_i(\theta))$ であり, e_i は $\mathfrak{P}_i$ の $K/\mathbb{Q}$ に関する分岐指数である. さらに, $\mathfrak{P}_i$ の $K/\mathbb{Q}$ に関する相対次数 f_i は P_i の次数に等しい.

次の包含定理 (inclusion theorem) は集合族 $\{K_f\}_f$ と集合族 $\{\mathrm{Spl}(K_f)\}_f$ の間の一対一対応を示している.

Theorem 2 (Inclusion Theorem [2])
$f, g \in \mathbb{Z}[x]$ をモニック既約多項式とし, その最小分解体をそれぞれ K_f, K_g とする. このとき

$$K_f \supset K_g \Longleftrightarrow \mathrm{Spl}(K_f) \overset{*}{\subset} \mathrm{Spl}(K_g),$$

ここに $\overset{*}{\subset}$ は有限個の素数を除いて $\subset$ が成り立つことを意味する.

それゆえ

$$\begin{aligned} K_f = K_g \quad &\Longleftrightarrow \quad \mathrm{Spl}(K_f) \overset{*}{=} \mathrm{Spl}(K_g) \\ &\Longleftrightarrow \quad \mathrm{Spl}(f) \overset{*}{=} \mathrm{Spl}(g). \end{aligned}$$

ここで $\overset{*}{=}$ は $p \nmid D_f$ なる有限個の素数を除いて $=$ が成り立つことを示す. これは $\mathrm{Spl}(f)$ を明らかにすることの重要性を示している.

与えられた $f(X)$ に対し, $\mathrm{Spl}(f)$ に属する素数を決定する規則がもしあれば, その法則を高次相互法則と呼ぶことがある [9]. 特に, $K_f/\mathbb{Q}$ がアーベル拡大のとき f をアーベル多項式といい, このときは類体論より次の定理が成り立つ:

Theorem 3 (アーベル多項式定理 [9]) $\mathrm{Spl}(f)$ が $f(X)$ のみによって決まる法に関する合同条件のみで記述されるための必要十分条件は $f(X)$ がアーベル多項式であることである.

アーベル多項式の例として $\Phi_n(X)$ を n 位円分多項式とすると, $\mathrm{Spl}(\Phi_n)$ は次のように合同条件のみで記述される:

$$\mathrm{Spl}(\Phi_n) = \{p \in P : p \equiv 1 \pmod{n}\}.$$

しかし f がアーベル多項式でない場合は $\mathrm{Spl}(f)$ を記述するためには一般に p についての合同条件だけでなく他の条件が必要となる. 例えば,

$$\mathrm{Spl}(X^3-2) = \{p \in P : p \equiv 1\,(3),\, x^2+27y^2 = p\}.$$

このような非アーベルな場合で, 最も大切な

$$\mathrm{Spl}(x^5 - x - 1)$$

の場合はまだ解明されていない.

2.2 $\mathrm{Spl}(f)$ の計算

与えられた $f(X)$ に対し $\mathrm{Spl}(f)$ を計算するには, 次数別分解アルゴリズム (distinct degree factorization algorithm) を使う. このアルゴリズムは以下の定理から導かれる:

Theorem 4 ([1]) $g(x) \in \mathbb{F}_p[X]$ を次数 n の既約多項式とし, m を正整数とする. このとき

$$g(X) \mid (X^{p^m} - X) \text{ in } \mathbb{F}_p[X] \Longleftrightarrow n \mid m.$$

上の定理より次が従う:

$$\mathrm{Spl}(f) = \left\{ p \in P : \begin{array}{l} p \nmid D_f \text{ かつ} \\ f_p(X) \mid (X^p - X) \text{ in } \mathbb{F}_p[X] \end{array} \right\}.$$

ここで D_f は $f(X)$ の判別式とする.

3 $K_f/\mathbb{Q}$ が S_5-拡大のとき

3.1 5 次式の法 p における分解のタイプ

$\mathrm{Gal}(K_f/\mathbb{Q}) = S_5$ であるような 5 次式 $f(X)$ が与えられたとき, f の mod p での分解のタイプとして次の 8 通りがある:

Type	0 :	$p \mid D_f$	
Type	1 :	(5 つの 1 次式)	1/120
Type	23 :	(2 次式)(2 次式)(1 次式)	15/120
Type	24 :	(2 次式)(3 つの 1 次式)	10/120
Type	3 :	(3 次式)(1 次式)(1 次式)	20/120
Type	4 :	(4 次式)(1 次式)	30/120
Type	5 :	(5 次式)	24/120
Type	6 :	(2 次式)(3 次式)	20/120

上で分解のタイプが $d\nu$ のとき, d はフロベニウス写像の位数を表し, ν はその退化次数 (nullity) を表す. 簡単のために, 分解のタイプが $d0$ のときは d とかく. 第三列の分数はチェボタレフの密度定理より求まる各タイプの素数の密度である. $\mathrm{Spl}(f)$ の密度は 1/120 であることに注意する.

Theorem 5 (Stickelberger [1], [8]) K を $\mathbb{Q}$ 上 n 次の数体とする. 有理素数 p が K において不分岐で $p\mathfrak{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i$ と素イデアル分解するならば $\left(\frac{d(K)}{p}\right) = (-1)^{n-g}$. ただし, $d(K)$ を K の判別式とする.

$\left(\frac{d(K)}{p}\right) = \left(\frac{D_f}{p}\right)$ より, $\left(\frac{D_f}{p}\right) = (-1)^{5-g}$ である. 以上のことと定理 1 より次を得る:

Corollary 1

$\{p \in P:\ p \nmid D_f \text{ and } \left(\frac{D_f}{p}\right) = 1\}$
$= \{p \in P : p$ は Type 1, 23, 3 or 5$\} \supset \mathrm{Spl}(f)$.

3.2 5 次式と付随する楕円曲線の 5 等分体

$t \neq 0, \frac{1}{1728}$ なる $t \in \mathbb{Q}\left(\sqrt{5D_f}\right)$ に対し, 次の 5 次式

$$f_t(x) = x^5 - 10tx^3 + 45t^2x - t^2$$

を考える. この形の 5 次式は Brioschi quintic とよばれる. 任意の $\mathbb{Q}$ 係数 5 次式は代数的に Brioschi quintic へ変換することができる. 楕円曲線

$$E_t : y^2 + xy = x^3 + 36tx + t$$

の 5 等分点の x 座標を $\mathbb{Q}$ に添加した体を L_5^+ とすると $K_{f_t} \subset L_5^+$ が成り立つ. E_t を f_t に付随する楕円曲線とよぶ. このとき,

$$\mathrm{Gal}(K_{f_t}/\mathbb{Q}(\sqrt{5D_f})) \simeq \mathrm{Gal}(K_f/\mathbb{Q})$$

が成立する. ゆえに $f \pmod p$ の分解の型は $f_t \pmod p$ の分解の型に等しく, それは拡大 $L_5^+/\mathbb{Q}(\sqrt{5D_f}))$ に関する (p) の素イデアル分解の型に等しい. E_t に関する Frobenius trace を a_p とする. E_t の $\mathrm{mod}\, p$ における Deuring lift により, Frobenius automorphism ϕ_p をある虚二次体の元 $\mathbb{Q}(\sqrt{\Delta_p})$ $(\Delta_p < 0)$ と同一視したとき, $a_p^2 - 4p = b_p^2\Delta_p$ によって正整数 b_p を決める. このとき, (p) の分解 すなわち $f \pmod p$ の分解は表 1 のように決定される ([3]).

分解の型	$\left(\frac{a_p^2-4p}{5}\right)$	$\left(\frac{p}{5}\right)$	
23	1	1	
4	1	-1	
3	-1	1	
24	-1	-1	$5 \mid a_p$
6	-1	-1	$5 \nmid a_p$
5	0		$5 \nmid b_p$
1	0		$5 \mid b_p$

表 1: 分解の型の判別条件 ([3])

Lemma 1 $b \neq 0$ かつ $t \neq 0, \frac{1}{1728}$ のとき Bring quintic

$$f(X) = X^5 + 5bX + c$$

を Briosichi quintic

$$f_t(Y) = Y^5 - 10tY^3 + 45t^2Y - t^2$$

に変換すると t は次式で与えられる:

$$t = \frac{d\left(-c^2 \pm \sqrt{d}\right)}{64c^2\left(8c^2 \mp 9\sqrt{d}\right)^2}. \quad \text{(複号同順)}$$

ただし, $d = c^4 + 256b^5 = 5^{-5}D_f$ とする. 特に, $f(x) = x^5 - x - 1$ すなわち $b = -1/5$, $c = -1$ のときは, $D_f = 2869$ で,

$$t = \frac{1}{64} \cdot \frac{D_f(821 \mp 5^2\sqrt{5D_f})}{7^4 \cdot 661^2}. \quad \text{(複号同順)}$$

Proof 簡単のために文献 [6] の記号に合わせて $j = V$, $t = Z$ と置き直して議論する. すなわち

$$z^5 + 5az^2 + 5bz + c = 0 \qquad (1)$$

で $a = 0$ のとき, これを次の Brioschi quintic に変換する:

$$y^5 - 10Zy^3 + 45Z^2y - Z^2 = 0$$

式 (1) から決まる量 V, Z, λ, μ があって次の関係式をみたす ([6]):

$$\frac{1}{Z} + V = 1728, \qquad (2)$$

$$Va = 8\lambda^3 + \lambda^2\mu + (72\lambda\mu^2 + \mu^3)Z, \qquad (3)$$

$$Vb = -\lambda^4 + 18\lambda^2\mu^2Z + \lambda\mu^3Z + 27\mu^4Z^2, \qquad (4)$$

$$Vc = \lambda^5 - 10\lambda^3\mu^2Z + 45\lambda\mu^4Z^2 + \mu^5Z^2. \qquad (5)$$

$(4) \times \lambda + (5)$ と (3) より $V \neq 0$ のとき

$$\mu^2Za = \lambda b + c$$

ゆえ, 特に $a = 0$, $b \neq 0$ のとき,

$$\lambda = -\frac{c}{b}.$$

(3) に上を代入して次を得る:

$$b^3Z\mu^3 - 72b^2cZ\mu^2 + bc^2\mu - 8c^3 = 0. \qquad (6)$$

$(4)\times\mu^2 Z-(5)\times\lambda$ より:

$$V=\frac{(\lambda^2-3\mu^2 Z)^3}{\lambda c-\mu^2 Zb}. \tag{7}$$

上式は $a=0$ のときも成り立つ. $(3)\times\lambda/\mu-(4)\times 8/\mu$ より:

$$V\cdot\frac{\lambda a+8b}{\mu}=\lambda^3+216\lambda^2\mu Z+9\lambda\mu^2 Z+216\mu^3 Z^2. \tag{8}$$

一方, $(3)^2\times 27-(8)^2/Z$ と (2) より

$$27a^2 V-\frac{V(\lambda a+8b)^2}{\mu^2 Z}=(\lambda^2-3\mu^2 Z)^3. \tag{9}$$

(9) の V に (7) を代入すると

$$27a^2-\frac{(\lambda a+8b)^2}{\mu^2 Z}=\lambda c-\mu^2 Zb. \tag{10}$$

$a=0, b\neq 0$ のとき, $\lambda=-\frac{c}{b}$ より式 (10) は

$$b^2(\mu^2 Z)^2+c^2(\mu^2 Z)-64b^3=0$$

よって

$$\mu^2 Z=\frac{1}{b^2}\left\{-c^2\pm\sqrt{c^4+256b^5}\right\}. \tag{11}$$

$d=c^4+256b^5$ とおくと (6) と (11) より

$$\mu=\frac{-8c(8c^2\mp 9\sqrt{d})}{\pm b\sqrt{d}}.\quad \text{(複号同順)}$$

よって

$$Z=\frac{d\left(-c^2\pm\sqrt{d}\right)}{64c^2\left(8c^2\mp 9\sqrt{d}\right)^2}.\quad \text{(複号同順)}$$

■

3.3 K が類数 1 のとき

Proposition 1 $K=\mathbb{Q}(\theta)$ を $\mathbb{Q}$ 上の n 次の数体とし, θ の $\mathbb{Q}$ 上の最小多項式を f とする. K の整数環を $\mathfrak{O}_K$ とし整基底を $\{\omega_1,\omega_2,\cdots,\omega_n\}$ とする. $\alpha=\sum_{i=1}^n x_i\omega_i\in\mathfrak{O}_K$ とするとき n 元 n 次形式 F を

$$F(x_1,x_2,\cdots,x_n)=N_{K/\mathbb{Q}}(\alpha)$$

で定める. このとき K の類数が 1 ならば, $f_p\in\mathbb{F}_p[X]$ が一次の因子をもつための必要十分条件は不定方程式

$$F(x_1,x_2,\cdots,x_n)=p$$

または

$$F(x_1,x_2,\cdots,x_n)=-p$$

が整数解をもつことである.

Proof 元のノルムと単項イデアルのノルムの関係

$$|N_{K/\mathbb{Q}}(\alpha)|=\mathcal{N}_{K/\mathbb{Q}}((\alpha))$$

より定理 1 から $f_p\in\mathbb{F}_p[X]$ が一次の因子 $X-A\in\mathbb{F}_p[X]$ を持つならば, $k\in\mathbb{Z}$ が存在して $pk=N_{K/\mathbb{Q}}(\theta-A)$ と表される. このとき, 定理 1 から $p=\mathcal{N}_{K/\mathbb{Q}}((p,\theta-A))$ である. もし, 整数環 $\mathfrak{O}_K$ の類数が 1 ならば $\pi\in\mathfrak{O}_K$ が存在して $(p,\theta-A)=(\pi)$ となるので $p=\pm N_{K/\mathbb{Q}}(\pi)$ が従う.

逆に, $F(x_1,x_2,\cdots,x_n)=\pm p$ の整数解がなければ, K の類数は 1 であることから, (p) の上の素イデアル $\mathfrak{p}$ の剰余次数は 1 より大きい. ゆえに定理 1 から f_p は $\mathbb{F}_p[X]$ において一次の因子をもたない.■

特に K が 2 次体のときは p を $F(x_1,x_2)=p$ の整数解 (a_1,a_2) を持つような素数とすると $\pi=a_1\omega_1+a_2\omega_2\in\mathfrak{O}_K$ に対して $p=\mathcal{N}((\pi))$ ゆえ (π) は p 上の剰余次数 1 の素イデアルであり $K/\mathbb{Q}$ は Galois 拡大より $2=efg$ である. $p\nmid d(K)$ なら $e=1$ で $\mathfrak{P}_1=(\pi)$ の p 上の分岐指数は 1 なので $f=1$ で $2=1\cdot 1\cdot g$ より $g=2$ となるので $p\in\mathrm{Spl}(f)$ となるから次が成り立つ.

Proposition 2 $D\in\mathbb{Z}$ を非平方数とし, $f(X)=X^2-D$ のとき 2 次体 $\mathbb{Q}(\sqrt{D})$ の類数が 1 ならば, $\left(\frac{D}{p}\right)=1$ と $F(x_1,x_2)=p$ が整数解をもつことは同値である.

Corollary 2 D を *square-free* な整数とし $D\equiv 1 \pmod 4$ とする. $K=\mathbb{Q}(\sqrt{D})$ の類数が 1 ならば, $\left(\frac{D}{p}\right)=1$ と $x^2+xy+\frac{1-D}{4}y^2=\pm p$ が整数解をもつことは同値である.

4 $\mathrm{Spl}(X^5-X-1)$

4.1 X^5-X-1 についての基本事項

$f(X)=X^5-X-1$ とし f の任意の根 $\theta\in\mathbb{C}$ をとって固定する. 以下は周知である：

1. $D_f=2869=19\cdot 151$.
2. $\mathfrak{O}_K$ の $\mathbb{Z}$-基底は $(1,\theta,\theta^2,\theta^3,\theta^4)$ である.

3. $\mathrm{Gal}(K_f/\mathbb{Q}) \simeq S_5$ (5 次の対称群).
4. K_f は $\mathbb{Q}(\sqrt{D_f}) = \mathbb{Q}(\sqrt{19\cdot 151})$ 上の不分岐拡大で, $\mathrm{Gal}(K_f/\mathbb{Q}(\sqrt{D_f})) \simeq A_5$ (5 次の交代群).
5. K の類数は 1 である ([4, 例 8.5]).
6. ２次体 $\mathbb{Q}(\sqrt{D_f})$ の類数は 1 である ([7]).

$\mathfrak{O}_K$ の任意の元を $\alpha = a + b\theta + c\theta^2 + d\theta^3 + e\theta^4$ $(a, b, c, d, e \in \mathbb{Z})$ とする. このときノルム $N_{K/\mathbb{Q}}(\alpha)$ は以下の形になる:

$$\begin{aligned}
&N_{K/\mathbb{Q}}(\alpha)\\
&= a^5 - ab^4 + b^5 + 4a^2b^2c - 5ab^3c\\
&- 2a^3c^2 + 5a^2bc^2 + ac^4 - bc^4 + c^5 - 4a^3bd\\
&+ 5a^2b^2d - 5a^3cd - 4abc^2d + 4b^2c^2d + ac^3d\\
&- 5bc^3d + 2ab^2d^2 - 2b^3d^2 + 4a^2cd^2 - 7abcd^2\\
&+ 5b^2cd^2 + 5ac^2d^2 + 3a^2d^3 - 5abd^3 - ad^4\\
&+ bd^4 - cd^4 + d^5 + 4a^4e - 5a^3be + 4ab^2ce\\
&- 4b^3ce - 4a^2c^2e + 3abc^2e + 5b^2c^2e - 5ac^3e\\
&- 8a^2bde + 13ab^2de - 5b^3de - 2a^2cde - 5abcde\\
&+ 5a^2d^2e + 4acd^2e - 4bcd^2e + 4c^2d^2e - ad^3e\\
&+ bd^3e - 5cd^3e + 6a^3e^2 - 11a^2be^2 + 5ab^2e^2\\
&+ 5a^2ce^2 - 2ac^2e^2 + 2bc^2e^2 - 2c^3e^2 - 4abde^2\\
&+ 4b^2de^2 + 3acde^2 - 7bcde^2 + 5c^2de^2 - ad^2e^2\\
&+ 5bd^2e^2 + 4a^2e^3 - 7abe^3 + 3b^2e^3 + 6ace^3\\
&- 5bce^3 - 5ade^3 + ae^4 - be^4 + ce^4 - de^4 + e^5.
\end{aligned}$$

上式右辺の 5 元 5 次形式を $F_K(a, b, c, d, e)$ とおく.

4.2 主結果

Theorem 6 (主定理) $p \neq 19, 151$ のとき, $p \in \mathrm{Spl}(X^5 - X - 1)$ となるための必要十分条件は $\left(\frac{19\cdot 151}{p}\right) = 1$ かつ $5 \mid (a_p^2 - 4p)$ かつ次をみたす有理整数の組 (a, b, c, d, e) が存在することである:

$$F_K(a, b, c, d, e) = p.$$

ここに, a_p は楕円曲線 E_t の Frobenius trace で,

$$t = \frac{1}{64} \cdot \frac{19\cdot 151(821 \mp 5^2\sqrt{5\cdot 19\cdot 151})}{7^4 \cdot 661^2}. \qquad (12)$$

Proof 定理 5 より, $\left(\frac{D_f}{p}\right) = 1$ であるためには p が type 1, type 23, type 3, または type 5 のいずれかであることが必要十分である.

また, 補題 1 より $X^5 - X - 1$ に付随する楕円曲線 E_t は (12) の t で与えられる. 表 1 より $\left(\frac{a_p^2-4p}{5}\right)$ の値が 0, 1, -1 のいずれをとるかに従って type 1 または 5, type 23, type 3 を区別することができる.

最後に type 1 と type 5 を区別しなければならない. そこで K の類数は 1 であることと 命題 1 より $f_p(X)$ が少なくとも一つの一次の因子 $X - a \in \mathbb{F}_p[X]$ をもつための必要十分条件は不定方程式

$$F_K(a, b, c, d, e) = p$$

の解 $(a, b, c, d, e) \in \mathbb{Z}^5$ が存在することである (K の $\mathbb{Q}$ 上の次数が奇数なので, $\pm p$ ととる必要はない). よって主張が従う. ■

Remark 1 3.2 節の表 1 より, type 1 と type 5 は b_p で区別できるが, b_p は複雑な量であり, ここではより具体的な条件で両者を区別した. 今後の一般化に際しては, b_p の解析が必要になるだろう.

5 数表

今回, PARI を使って $\mathrm{Spl}(X^5 - X - 1)$ に属する素数 p を $p < 1,000,000$（即ち素数 999983 まで）の範囲でもとめた結果, 650 個の完全分解する素数を得た（ $1,000,000$ 未満の素数の個数は $78,498$ である）. 表において $\pi(p)$ は p を越えない素数の個数を表す. $1,000,000$ 未満の素数で $\mathrm{Spl}(X^5 - X - 1)$ に含まれるものの個数の割合は $\frac{650}{78498} \approx 0.00828$ であり, $\frac{1}{120} - \frac{650}{78498} \approx 5.286 \times 10^{-5}$ なのでこれはチェボタレフの密度定理に従っている (図 1 参照).

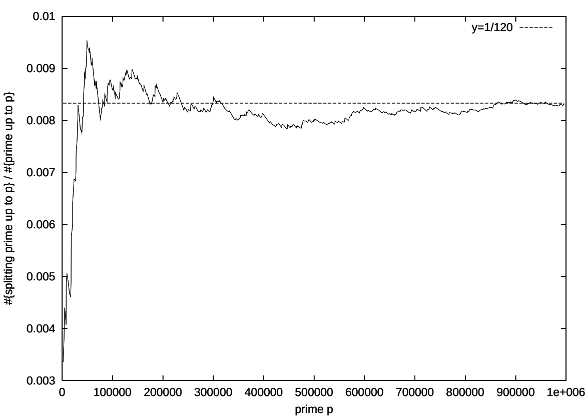

図 1: p 未満の完全分解素数の割合

The table of $p \in \mathrm{Spl}(X^5 - X - 1)$ for $p < 10^6$

p	$\pi(p)$	p	$\pi(p)$
1973	298	44221	4603
3769	525	45959	4758
5101	682	46229	4782
7727	981	47309	4879
8161	1024	47969	4944
9631	1190	48541	4995
11903	1426	48847	5023
14629	1713	48947	5031
16903	1950	50989	5221
17737	2036	52177	5334
17921	2054	53699	5473
18097	2074	54367	5530
19477	2210	57697	5844
20747	2336	58913	5955
20759	2339	59093	5975
21727	2437	64403	6446
22717	2538	65203	6516
23567	2622	67579	6734
25037	2766	67607	6737
26681	2924	75821	7470
27397	2994	76543	7531
27529	3007	77563	7622
28279	3079	77951	7658
29207	3175	79193	7762
29959	3243	80317	7865
30497	3293	80407	7872
31091	3350	82307	8049
31319	3375	84239	8213
33289	3564	84391	8225
36097	3834	84463	8234
37463	3965	86629	8423
39161	4123	88997	8619
39671	4171	89107	8632
40151	4217	89513	8667
41491	4339	89657	8683
42139	4405	90617	8770
42487	4445	91387	8837
42689	4462	93047	8986
43331	4522	93637	9042
44171	4597	94531	9116

p	$\pi(p)$	p	$\pi(p)$
95737	9228	148949	13753
99259	9530	149287	13786
100957	9670	153337	14134
101377	9709	154579	14237
105509	10066	156371	14387
105613	10076	160231	14705
107699	10248	161771	14832
109391	10400	162007	14853
111521	10578	162269	14869
112807	10686	167381	15290
113891	10778	168937	15407
114073	10796	174481	15875
114661	10844	175493	15949
114689	10847	177239	16104
115019	10874	177889	16149
117511	11088	178889	16237
118081	11142	178951	16246
120293	11326	180137	16352
120473	11339	180563	16390
120539	11342	181787	16475
122489	11521	184057	16669
123427	11598	184199	16681
124121	11657	184321	16691
125003	11735	184511	16704
125539	11780	184859	16734
127247	11919	186871	16909
127717	11964	187091	16925
128549	12036	191827	17314
132241	12345	194087	17507
134153	12508	199343	17929
134839	12563	200713	18039
136319	12692	200869	18050
137873	12831	203207	18237
138139	12852	204301	18324
138323	12869	205151	18395
138889	12918	208139	18647
141241	13117	210631	18863
144511	13383	213539	19092
146239	13529	214189	19146
147293	13616	214723	19189

p	$\pi(p)$	p	$\pi(p)$
215953	19284	280207	24449
217909	19438	280997	24519
218287	19466	285517	24880
219953	19613	286477	24951
220169	19630	287341	25023
221489	19735	288413	25093
221717	19754	291007	25309
224449	19976	293339	25488
225821	20090	293681	25511
227113	20188	294317	25562
227393	20211	294991	25615
227581	20231	295861	25677
228233	20278	295901	25682
231923	20595	297113	25782
241561	21350	298513	25885
242069	21396	299063	25926
242729	21449	299281	25940
244589	21599	300073	26002
248509	21921	300191	26011
249541	22010	300439	26032
249833	22030	306253	26509
252391	22234	306419	26522
254003	22363	308081	26650
254927	22430	309271	26745
255043	22442	311561	26919
255209	22461	312229	26969
255473	22480	315449	27228
257489	22637	317903	27432
261917	22982	322513	27808
262897	23060	325027	28011
263303	23094	327823	28234
265093	23237	329947	28398
269281	23589	331519	28525
271043	23731	332309	28592
272719	23865	340687	29238
274489	23998	343393	29454
274723	24013	344213	29517
276277	24146	345601	29622
278891	24353	348433	29852
279679	24411	349291	29915

p	$\pi(p)$	p	$\pi(p)$
350941	30045	423587	35669
351343	30081	424243	35721
352813	30198	425609	35827
353603	30257	425813	35837
353629	30261	428137	36012
354751	30357	428429	36034
356927	30514	429791	36140
358069	30606	435637	36618
359599	30735	435893	36640
361903	30895	435947	36644
362221	30923	436853	36711
364961	31138	439441	36894
365423	31175	445307	37370
365489	31182	446759	37467
366031	31223	446827	37471
368111	31392	447053	37487
368803	31445	447427	37514
369143	31467	452497	37904
370883	31588	452689	37920
374639	31868	454501	38046
377831	32132	456167	38178
380657	32349	457001	38239
381749	32432	457669	38294
382519	32482	458531	38349
385291	32707	464557	38801
388211	32926	464587	38803
389099	32993	466649	38962
389579	33032	467147	38995
393611	33368	470299	39249
394967	33471	473101	39466
395897	33542	474619	39589
396637	33600	474911	39610
396679	33603	475271	39637
397811	33686	475429	39655
402859	34069	476519	39746
411197	34706	477011	39781
412081	34779	477469	39809
413141	34856	477823	39837
418391	35266	478321	39873
419999	35390	480427	40041

p	$\pi(p)$	p	$\pi(p)$
482231	40178	548239	45184
483577	40285	552047	45481
487307	40550	554837	45691
487843	40596	555337	45728
488711	40666	555361	45730
488981	40687	557861	45914
490283	40791	559781	46056
495701	41210	560171	46089
495959	41233	560543	46123
498163	41395	560837	46146
498977	41456	560977	46158
499117	41465	561373	46185
500693	41591	566939	46590
501187	41634	568627	46713
503213	41771	569083	46749
506083	41996	569237	46761
509123	42224	569903	46815
512167	42455	570403	46851
514093	42603	571397	46933
516563	42787	571811	46963
517711	42886	573451	47089
518129	42917	574283	47153
521869	43207	574373	47160
524947	43434	575087	47210
525871	43510	575369	47231
527291	43627	576551	47325
527897	43669	577757	47416
529957	43819	578251	47451
530599	43873	581377	47693
531901	43967	582983	47813
533837	44112	583859	47881
534059	44134	585071	47972
538249	44443	586309	48066
540803	44635	590327	48378
541237	44662	590537	48389
541361	44671	591053	48424
541417	44676	591443	48453
544627	44920	593141	48580
546739	45077	594137	48654
547871	45161	595363	48761

p	$\pi(p)$	p	$\pi(p)$
482231	40178	548239	45184
483577	40285	552047	45481
487307	40550	554837	45691
487843	40596	555337	45728
488711	40666	555361	45730
488981	40687	557861	45914
490283	40791	559781	46056
495701	41210	560171	46089
495959	41233	560543	46123
498163	41395	560837	46146
498977	41456	560977	46158
499117	41465	561373	46185
500693	41591	566939	46590
501187	41634	568627	46713
503213	41771	569083	46749
506083	41996	569237	46761
509123	42224	569903	46815
512167	42455	570403	46851
514093	42603	571397	46933
516563	42787	571811	46963
517711	42886	573451	47089
518129	42917	574283	47153
521869	43207	574373	47160
524947	43434	575087	47210
525871	43510	575369	47231
527291	43627	576551	47325
527897	43669	577757	47416
529957	43819	578251	47451
530599	43873	581377	47693
531901	43967	582983	47813
533837	44112	583859	47881
534059	44134	585071	47972
538249	44443	586309	48066
540803	44635	590327	48378
541237	44662	590537	48389
541361	44671	591053	48424
541417	44676	591443	48453
544627	44920	593141	48580
546739	45077	594137	48654
547871	45161	595363	48761

p	$\pi(p)$	p	$\pi(p)$
596279	48826	665591	53995
596851	48866	666821	54083
597769	48938	667367	54120
598141	48963	670051	54315
605533	49519	671081	54391
606413	49582	671159	54397
607249	49650	672377	54494
610559	49895	673669	54596
612223	50027	676279	54783
614617	50200	677717	54884
615137	50240	679229	54998
615313	50251	680299	55087
617039	50394	682277	55235
617273	50415	688097	55671
619027	50543	690929	55873
621289	50709	691297	55897
621611	50730	692401	55987
621721	50741	692663	56008
625199	51001	693157	56043
628499	51233	693571	56071
634187	51651	698171	56418
635707	51771	698821	56462
636739	51849	701383	56643
637243	51884	702349	56719
641051	52152	703231	56787
641239	52167	703709	56821
644869	52437	704029	56847
648391	52711	706481	57036
648803	52733	710791	57363
652039	52969	711299	57405
653893	53110	711539	57422
654023	53124	711751	57440
657617	53390	711793	57442
659999	53564	711923	57453
660061	53570	714443	57627
661931	53711	714677	57645
662681	53767	724021	58346
663587	53835	724093	58348
663853	53853	724723	58396
664597	53914	725317	58438

p	$\pi(p)$	p	$\pi(p)$
727949	58636	796307	63681
727997	58638	798781	63870
728489	58668	801709	64087
728873	58701	803963	64238
728929	58708	804337	64268
735571	59205	804613	64290
736657	59278	807193	64480
737017	59303	807299	64489
738313	59400	808019	64537
739631	59506	808369	64561
739957	59529	809779	64666
741409	59629	812183	64846
747889	60083	812297	64855
752569	60433	815653	65098
753959	60533	817331	65224
757993	60821	819317	65359
759287	60921	820609	65461
759929	60973	825997	65877
766321	61462	826667	65926
767747	61565	827311	65974
767867	61577	828637	66062
767951	61581	829349	66118
770183	61750	830383	66190
771481	61847	831547	66275
775267	62123	832721	66375
775273	62124	834143	66475
778187	62332	835607	66573
778439	62352	835979	66603
780343	62489	838769	66800
786053	62921	839303	66836
787333	63008	839809	66875
788087	63066	843307	67133
788971	63136	844187	67198
790567	63250	845197	67273
790781	63267	846161	67336
791201	63299	847393	67431
791569	63326	848101	67478
792383	63389	850439	67658
794389	63541	851821	67754
796193	63674	854881	67964

p	$\pi(p)$	p	$\pi(p)$
854897	67965	905917	71700
855079	67980	908603	71912
855373	68001	912061	72175
856153	68061	920651	72779
856547	68091	921157	72819
857201	68142	922807	72942
857249	68145	923449	72986
860513	68382	923551	72995
861191	68437	925901	73178
861571	68459	926203	73204
862669	68554	928001	73325
862913	68568	928231	73341
865091	68725	929507	73437
865231	68735	933479	73720
865979	68795	933943	73751
872747	69296	936319	73927
873461	69339	938879	74109
875239	69463	940127	74196
877187	69616	943841	74479
878651	69720	944039	74492
879863	69815	944857	74551
880559	69868	945787	74609
881197	69920	947197	74708
881357	69932	948551	74807
883229	70060	949037	74837
886469	70299	952687	75105
886517	70303	954263	75217
888809	70473	957413	75434
889247	70503	957701	75451
891427	70653	957821	75460
893111	70783	958883	75540
894193	70860	966013	76065
894391	70877	967459	76164
894947	70916	969863	76340
895333	70946	971653	76479
896531	71033	976093	76802
898129	71147	976933	76859
899183	71225	979327	77028
904573	71595	980687	77112
905213	71654	981919	77203

p	$\pi(p)$	p	$\pi(p)$
905917	71700	985181	77433
908603	71912	986047	77497
912061	72175	986801	77555
920651	72779	987061	77577
921157	72819	987997	77634
922807	72942	989279	77720
923449	72986	993827	78047
923551	72995	993943	78056
925901	73178	994837	78125
926203	73204	996329	78234
928001	73325		
928231	73341		
929507	73437		
933479	73720		
933943	73751		
936319	73927		
938879	74109		
940127	74196		
943841	74479		
944039	74492		
944857	74551		
945787	74609		
947197	74708		
948551	74807		
949037	74837		
952687	75105		
954263	75217		
957413	75434		
957701	75451		
957821	75460		
958883	75540		
966013	76065		
967459	76164		
969863	76340		
971653	76479		
976093	76802		
976933	76859		
979327	77028		
980687	77112		
981919	77203		

参考文献

[1] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Math. **138**, Springer-Verlag, Third Corrected Printing 1996.

[2] J. W. S. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press, 1967.

[3] W. Duke and Á. Tóth, *The Splitting of Primes in Division Fields of Elliptic Curves*, Experimental Mathematics **11**, No. **4** (2002), pp.555-565.

[4] 藤崎源二郎,『代数的整数論入門（上)』, 基礎数学選書 **13A**, 裳華房, 第三版, 2002.

[5] T. Hiramatsu, *Theory of Automorphic Forms of Weight 1*, Adv. Stud. Pure Math.**13** (1988), 503-584.

[6] R.B. King, Beyond the Quartic Equation. Birkhuser Boston, Inc., Boston, MA, 1996.

[7] K. Matthews, Some BCMath/PHP number theory programs, `http://www.numbertheory org.org/php/php.html`

[8] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress (1897), Zürich, 182-193.

[9] B. F. Wyman, *What is a Reciprocity Law ?*, Amer. Math. Monthly, **79** (1972), 571-586.

キーワード.

非アーベル的相互法則, ラングランズ予想, 5 次方程式.

Summary

Non-abelian reciprocity laws

Seiken Saito　　Toyokazu Hiramatsu

Graduate School of Engineering, Hosei University

One of the main issues of mathematics in 21st century is a development of "non-abelian mathematics" in contrast to abelian mathematics which is first named by A. Weil. This contrast between abel and non-abel may be considered in engineering to the contrast between linear and non-linear. For instance the approximation of non-linear control by linear control is corresponded to the structure of the solvable groups consisting of finite abelian steps. We remark that any problems cannnot be solved by such linearlization or abelianization. In this article we study non-abelian properties of the quintic equation

$$x^5 - x - 1 = 0$$

of which Galois group over $\mathbb{Q}$ is the symmetric group S_5. Towards a non-abelian reciprocity law, we describe a necessary and sufficient condition when a prime splits completely in $\mathbb{Q}(\theta)$ with a root θ of $x^5 - x - 1$, and show a table of the splitting primes $p < 10^6$.

Keywords.

Non-abelian reciprocity laws, the Langlands conjecture, quintic equations.