数式処理 *Bulletin of JSSAC(2013)*
Vol. 20, No. 1, pp. 3 - 12

奨励賞受賞論文

Magmaによる局所体高速生成アルゴリズムの実装

横山 俊一*

九州大学マス・フォア・インダストリ研究所 / JST CREST

概　要

We present an efficient algorithm for isomorphy of extensions of a local field. Using this, we give a database of local extension fields with higher degree. We also give an algorithm to compute the Galois group of a local extension field. This paper is a resume of the following two papers: [12] and [13].

1 序

代数学，とりわけ整数論においては，基礎体と拡大次数（及び必要に応じて拡大の種類）が与えられた時，そのような拡大体を全て調べ尽くす事は有益な営みである．データベースとして統一化されることにより，計算機の非専門家でもデータを利用する事が可能となるため，具体的な拡大体やそれに付随する代数的構造物（ray 類体や Galois 群など）を精密に調べる事が出来るからである．実際，Klüners-Malle による [7] や Jones-Roberts による [3], [4] などは知名度も高く，頻繁に用いられている．但し汎用アルゴリズムを用いた場合は，計算時間等を考慮すると次数 10 前後までしか計算出来ないという課題もあり，実用面での改良が望まれている．

本論文では，局所体上の拡大体生成 [4] に注目して，このデータベースが到達し得なかった高次の拡大体データベースを生成するための手法を提案する．そこでは 2 つの拡大が与えられた時，それらが同型か否かを効率的に判定するアルゴリズムが主軸を担っている．またこの応用として，特別な拡大に対しては高次であっても Galois 群を正確に決定出来ることを述べる．

論文の構成は次の通りである．まず 2 節で局所体に関する基礎事項を整理する．続いて 3 節で局所体の高速同型判定と拡大体データベース生成に関して論じ，4 節で Galois 群計算への応用例を述べる．そして 5 節で計算機実験結果を纏め，6 節で整数論的補足と今後の展望を述べる．なお 2 節と 3〜6 節は独立であるから，局所体に詳しい方は 2 節は読み飛ばして頂いて構わない．

最後に，本論文における研究内容は全て吉田学氏（九州産業大学付属九州産業高校・非会員）との共同研究であり，奨励賞受賞論文としての掲載という理由に基づき単著論文となっていることをここに明記しておく．

*s-yokoyama@imi.kyushu-u.ac.jp

© 2013 Japan Society for Symbolic and Algebraic Computation

2 局所体, 特に p 進体の基礎事項

体には大きく分けて，**大域体**（global field）と**局所体**（local field）の 2 種類が存在する．例えば有理数体 $\mathbb{Q}$ 及びその有限次拡大体（**代数体**と呼ぶことが多い），有限体 $\mathbb{F}_p$（p は素数）及びその一変数代数関数体 $\mathbb{F}_p(t)$ などは全て大域体である．一方局所体としてはこの後定義する p **進数体**（p-adic field）$\mathbb{Q}_p$ や，$\mathbb{F}_p(t)$ の有限次拡大体などが挙げられる．また状況に応じて，実数体 $\mathbb{R}$ や複素数体 $\mathbb{C}$ も局所体として扱うこともある[1)]が，ここでは特に深入りしない．本稿では以降，局所体として主に p 進数体とその有限次拡大体だけを考えることにする．

大域体 $\mathbb{Q}$ と局所体 $\mathbb{Q}_p$ との違いは，簡単に言えば入っている距離の違いだけである．例えば次のような無限和を考える．

$$\text{(A)}\ \sum_{n\geq 0} 2^n = 1 + 2 + 2^2 + 2^3 + \cdots \qquad \text{(B)}\ \sum_{n\geq 0} \frac{1}{2^n} = 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots$$

学部数学においては，ここに絶対値に関する距離が入っていると考えるため，(A) は発散し (B) は 2 に収束する，という結論に達する．しかしここで (A) を 2 進数体 $\mathbb{Q}_2$ の元の無限和と見なすと，これは -1 に収束する．この理由は，2 進数体に入っている距離が

$$\lim_{n\to\infty} 2^n = 0$$

という性質を満たすからである．このことをもう少し正確に述べてみる．

定義 1

p を素数とする．$x \in \mathbb{Q}^\times$ は以下の様に一意に表せる：

$$x = p^m \cdot \frac{a}{b}\ \ (a, b, m \in \mathbb{Z},\ b > 0,\ (a, p) = (b, p) = 1)$$

ここで $\nu_p(x) = m,\ \nu_p(0) = \infty$ とおけば ν_p は $\mathbb{Q}$ の正規付値となる．これを $\mathbb{Q}$ の p **進付値**と呼ぶ.

即ち，2 つの p 進数 x_1, x_2 が与えられた時，$\nu_p(x_1 - x_2)$ が非常に増大することと，x_1 と x_2 とが p 進的に「近くなる」ことは等価であると言える．この付値によって

$$\lim_{n\to\infty} p^n = 0,\ \ \sum_{n\geq 0} p^n = \frac{1}{1-p}$$

も成立する．先程の例は $p = 2$ を代入したものとなっている．

注意 2

$\mathbb{Q}$ の非自明な付値は，絶対値 $|\cdot|$ とこの ν_p で尽きている．前者を**アルキメデス的付値**，後者を**非アルキメデス的付値**と呼ぶ.

定義 3

$\mathbb{Q}$ の ν_p による完備化を p **進数体**といい，$\mathbb{Q}_p$ と書く．

[1)] $\mathbb{R}$ や $\mathbb{C}$ は代数体の完備化であるが，今回主に考える局所体を得るために行う完備化とは方法が異なる．より正確には完備化に使用する付値が**アルキメデス的**か**非アルキメデス的**かという違いである（cf. 注意 2）.

注意 4

有理数体 $\mathbb{Q}$ の整数環として $\mathbb{Z}$ が得られるのと同様に，$\mathbb{Q}_p$ の整数環も構成出来る．それを $\mathbb{Z}_p$ と書いて p **進整数環**と呼ぶ．これは ν_p の付値環（valuation ring）として構成出来るが，今回は $\mathbb{Z}_p$ を扱う事は特に無いので，詳しい定義は省略する．それよりも注意すべきは，$\mathbb{Z}_p$ を $\mathbb{Z}/p\mathbb{Z}$（有理整数の mod p 剰余環）と混同してはいけないという点である．符号理論や離散数学においては，$\mathbb{Z}/p\mathbb{Z} = \left\{\overline{0}, \overline{1}, \cdots, \overline{p-1}\right\}$ のことを $\mathbb{Z}_p$ と書く習慣があるが，整数論においては $\mathbb{Z}/p\mathbb{Z}$ と $\mathbb{Z}_p$ は厳密に区別して書かなければならない．

p 進数体 $\mathbb{Q}_p$ から出発して，体の拡大や Galois 理論が大域体と同様に展開出来る．これが p 進体の理論である．本稿のゴールは，局所体の枠組みにおける Galois 群の高速計算を実現することである．

さて，大域体のうちの一つである有限体上の数学は，近年暗号理論などで非常に重宝されているのは周知の通りである．その一方で，局所体の理論には何か応用があるのか？という疑問も生まれるであろう．答えは勿論 yes である．例えば局所体において，ある構造の幾何的性質を調べる場合，そのコホモロジーを考えることによって代数的に理解する事が出来る．Dwork による “p 進解析化” の理論（の拡張）を用いて得られる，標数 p の体上のスムースなアフィン代数多様体として Monsky-Washnitzer コホモロジーと呼ばれるものが存在するが，これを用いると，超楕円曲線の有理点の個数を計算するアルゴリズムが得られることが知られている（Kedlaya, [6]）．これは暗号理論への実用的な応用を与えるという意味で非常に注目されている．このように，大域体上の理論から一度局所体の枠組みに変換し，それを再度引き戻すというテクニックは，現代数論のトレンドとなりつつある．

3 局所体の高速生成アルゴリズム

本稿では特に断らない限り，基礎体は $\mathbb{Q}_p$ で固定する．即ち次のような問題を考える．

問題 5

与えられた $n \in \mathbb{Z}_{\geq 2}$ に対して $\mathbb{Q}_p$ 上 n 次拡大の同型類を全て構成せよ．

$\overline{\mathbb{Q}}_p$ 内では n 次拡大体の同型類は有限個しかないことが知られているので，計算機的問題としては理論上有限回の処理で終了する問題である．実際 Pauli-Roblot による先行研究 [10] があり，計算代数システム Magma には汎用実装 `AllExtensions` が搭載されている．しかしながら，現実的な時間で終了するような (p, n) の値の上限は非常に小さく，n に至っては高々 10 程度である．これを受けて Pauli はアーベル拡大（Galois 群がアーベル群となるような拡大）に対しては最大馴分岐（部分）拡大体上の p 次巡回拡大の塔（cyclic tower）を用いた類体論的手法を [9] で提案しているが，それでも劇的な改善には至っていない．

この原因は，採用されている同型判定アルゴリズムにある．Pauli らによるアルゴリズムにおいては，Panayi の “root counting” アルゴリズム [8] が用いられている．これは多項式の根を近似的に求めることで同型判定を行う手法で，拡大次数や多項式の複雑さに計算負荷が大きく依存してしまう．そこで我々は，Panayi のアルゴリズムの使用を回避する戦略をとることにする．

定義 6

$E(n)$ を $\mathbb{Q}_p$ 係数の n 次 Eisenstein 多項式[2)]の集合とする．2 つの Eisenstein 多項式 $f = \sum_{0\le i\le n} a_i x^i$, $g = \sum_{0\le i\le n} b_i x^i$ に対して, その距離を

$$v_p(f,g) = \min_{0\le i\le n-1} \left\{ v_p(a_i - b_i) + \frac{i}{n} \right\}$$

と定義する．これは $E(n)$ の超距離（ultrametric）を定める．

この時，分岐理論を用いて同型判定の規準を得る事が出来る，$f \in E(n)$ に対して $L_f = \mathbb{Q}_p[x]/(f)$ と定義し，$u_f = u_{L_f/\mathbb{Q}_p}$ を拡大 $L_f/\mathbb{Q}_p$ の最大上付き分岐跳躍数とする．詳細な定義は複雑になるため省略するが，u_f は定義から直接計算するのではなく，Newton 多角形（Newton polygon）を用いて効率的に計算出来る事が知られている．一方，上で定義した距離は多項式の係数の情報しか使っていないため，Panayi のアルゴリズムのように根の探索をする必要がなく，次数が上がっても高速計算可能である．

$f, g \in E(n)$ に対して，$\mathbb{Q}_p$ 上の同型写像 $L_f \simeq L_g$ が存在する時 $f \sim g$ と書く．これは $E(n)$ 上の同値関係を定める．

命題 7 ([12], 命題 2.3)

$f, g \in E(n)$ に対して $v_p(f,g) > u_f$ ならば $f \sim g$ が成り立つ．

これを用いると，$\mathbb{Q}_p$ 上 p 次拡大（即ち $n = p$）の Galois 群の高速計算が可能となる．これについては 4 節で詳細に述べる．

一方で，次のような問題を考えてみる：

問題 8

$f, g \in E(n)$ が与えられた時に $f \nsim g$ となるような場合の（高速な）判定規準は存在するか？

これが得られると，拡大体のデータベース生成が可能となる．具体的には，サンプルとなる多項式を一つ用意し，そこから係数を変化させることによって，互いに同型でないような多項式たちを必要個数に達するまで生成する．その個数に関しても幾つかの公式が知られている．ここでは，整数論的に重要な**完全分岐アーベル拡大**（totally ramified abelian extension）という特別な拡大に対してその判定規準を与えてみる．以下 p は**奇素数**であると仮定する．

命題 9 (Travesa, [11])

$n = ep^m > 1$（e と p は互いに素）を整数とする．この時 $\mathbb{Q}_p$ 上 n 次完全分岐アーベル拡大の同型類の個数は，$e \mid (p-1)$ の時 n 個，そうでなければ 0 個である．

これにより，n 個の互いに同型でない多項式を生成した時点でデータベースが完成した事が分かる．互いに同型でないような多項式を探索するには，次の命題が役に立つ．

[2)] $\sum_{0\le i\le n} a_i x^i \in \mathbb{Q}_p[x]$ で $a_n = 1$，$v_p(a_0) = 1$，$v_p(a_i) \ge 1$（$1 \le i \le n-1$）を満たすもの．

命題 10

$f, g \in E(n) = E(ep^m)$ とし，f, g は共に n 次完全分岐アーベル拡大を与えているとする．この時 $v_p(f, g) \in \{1, 2, \cdots, m+1\}$（但し $e = 1$ の時に限り $v_p(f, g) \in \{2, 3, \cdots, m+1\}$）ならば $f \nsim g$ が成り立つ．

この規準を基にして，明示的なアルゴリズムを構成する．

- 次を満たす整数 r をとる：$1 \le r \le p-1$ で $r \bmod p$ が $\mathbb{F}_p$ における 1 の原始 $p-1$ 乗根となる．
- 集合 $U = \left\{ r^i \left(1 + u_1 p + u_2 p^2 + \cdots + u_m p^m\right) \mid 0 \le i \le e-1,\ 0 \le u_j \le p-1 \right\}$ を作る[3)]．
- 各 $u \in U$ に対して, 次のようにして多項式を生成する：
  1. 多項式 $e(x)$ を $e(x) = x^p + upx$ で定義する．
  2. 多項式 $e^{m+1}(x)/e^m(x)$ を計算する（ここで $e^i(x)$ とは e を i 回作用させたもの）．この多項式の次数は $(p-1)p^m$ であり，$(p-1)i$ 次（$0 \le i \le p^m$）の項以外の係数は 0 となる．そこでこの多項式の $(p-1)i$ 次の係数を a_i と書く．
  3. 多項式 $f(x) = x^{ep^m} + a_{p^m-1} x^{e(p^m-1)} + \cdots + a_1 x^e + up$ を生成する．
- このようにして得られた多項式 $f(x)$ をデータベースに追加する．

この生成アルゴリズムは一見テクニカルに見えるが，前に定義した多項式の距離が命題 10 を満たすように（＝生成される拡大体が互いに同型でない n 次完全分岐アーベル拡大となるように）試行錯誤の上設計されたものである．本質的には係数をうまくずらして走らせているだけなので，高速生成が可能になるというわけである．

注意 11

この結果の背後にある定理は $p = 2$ の時には成り立たない．先程 p を奇素数と仮定したのはこのためである．

4 応用例：Galois 群の高速計算

ここでは，命題 7 を用いて $\mathbb{Q}_p$ の p 次拡大の Galois 群を高速判定する方法を述べる．鍵となるのは次の結果である．

定理 12 (Amano, [1])

p を奇素数とする．この時 $E(p)/\sim$（同型類別）の完全代表系は以下の 3 パターンで尽きている．

- **パターン 1：$x^p + apx^\lambda + p$ 型．**
  但し $1 \le a, \lambda \le p-1, (a, \lambda) \ne (p-1, p-1)$ ．全 $p^2 - 2p$ 通り．
- **パターン 2：$x^p - px^{p-1} + (1+ap)p$ 型．**
  但し $0 \le a \le p-1$ ．全 p 通り．
- **パターン 3：$x^p + (1+ap)p$ 型．**
  但し $0 \le a \le p-1$ ．全 p 通り．

[3)] $\#U = ep^m = n$ であることに注意.

この時，各パターンに対して拡大体の Galois 群が計算出来ることが知られている（cf. [5]）．具体的には，パターン 1 の場合は $C_p \ltimes C_d$（半直積），パターン 2 の場合は C_p，パターン 3 の場合は $C_p \ltimes C_{p-1}$ となる．ここで C_n は位数 n の巡回群，$d = (p-1)/\gcd((p-1)/m, \gcd(p-1, \lambda))$（$m$ は $a\lambda$ の $\mathbb{F}_p^\times$ における位数）である．よって，命題 7 を用いて全 3 パターン・p^2 個の多項式に片っ端から同型判定をかけて，唯一存在する同型な体を与える多項式を見つけ出せば良い．

注意 13

p は奇素数であるという仮定が付いているが，$p = 2$ の時，即ち $\mathbb{Q}_2$ の 2 次拡大は 7 つしかなく，次数も高くないため高速化は不要である．つまり，従来の汎用アルゴリズムで十分である．

5 計算機実験

以下全ての実験結果は，計算機代数システム Magma [2] version 2.17-9 を用いて，Windows 7 64bit 版，Intel® Core™ i7-2630QM CPU @ 3.30GHz の環境で得られたものである．まずは $\mathbb{Q}_p$ の p 次拡大の Galois 群の高速計算を行う．サンプル多項式は次の通り．

(A) $x^{97} + 194x^2 + 28324 \sim x^{97} + 194x^2 + 97$

(B) $x^{257} + 2056x^{256} + 366996 \sim x^{257} + 9252x^{256} + 257$

(C) $x^{1177207} + 1385816320849x + 20012519 \sim x^{1177207} + 188482106167207999$

上の（1 回の）同型判定に要する時間を Panayi の root counting アルゴリズムと比較して計測する．なお (A)〜(C) はそれぞれパターン 1〜3 に対応しており，Galois 群はそれぞれ $C_{97} \ltimes C_{48}$，C_{257}，$C_{1177207} \ltimes C_{1177206}$ となる．

Case	RC Alg. (sec)	Our Alg. (sec)
(A)	343.73	≤ 0.01
(B)	18329.05	≤ 0.01
(C)	failed*	4.64

タイミングデータから分かる通り，多項式の距離を用いた同型判定によって数百万倍の高速化が実現されている．なお (C) の failed はメモリが溢れて処理が停止したことを意味する．

注意 14

今回の高速化により，100 万次程の非常に高次な拡大に対しても同型判定が可能となったが，データベース生成や実際の Galois 群の判定アルゴリズムとしては，この規模では全く実用的ではないことに注意しなければならない．例えば (B) の例では，$\mathbb{Q}_{257}$ の 257 次拡大は全部で $257^2 = 66049$ 個存在するため，Galois 群の決定には worst case で 66048 回の同型判定が必要となる（1 個目から 66048 番目までが全て No と判定されれば最後の 66049 番目の多項式が同型な拡大を与えるため，総判定回数は 1 回減る）．しかしこの場合，一回あたり 0.01 秒以下しかかからないため，約 11 分以下で終了する．一方で (C) の例では，一回の判定が 5 秒程度で終了するとしても，worst case の場合の計算回数が $1177207^2 - 1 = 1385816320848$ = 約 1 兆 3858 億回という莫大な計算量を要求するため，判定終了までにかかる時間は約 20 万 3900 年もかかる計算となる．例

えアルゴリズムを高速化して一回あたりの判定時間を 0.01 秒まで高速化出来たとしても 440 年近くかかるため，並列処理という方法も考えられるが，現時点では世界最先端レベルのスーパーコンピュータ程度の性能（スレッド数）が無ければ不可能である．

続いて n 次完全分岐アーベル拡大のデータベース生成に要する時間を計測する．ここでは次の 2 つのケースに関して実験を行う．

(D) $n = p$ for $3 \leq p \leq 100$

p	$\#\mathcal{AT}(n)_{\mathbb{Q}_p}$	Time (sec)	p	$\#\mathcal{AT}(n)_{\mathbb{Q}_p}$	Time (sec)
3	3	≤ 0.01	43	43	0.46
5	5	≤ 0.01	47	47	0.75
7	7	≤ 0.01	53	53	1.72
11	11	≤ 0.01	59	59	2.12
13	13	≤ 0.01	61	61	2.19
17	17	0.02	67	67	6.98
19	19	0.02	71	71	5.43
23	23	0.04	73	73	10.90
29	29	0.09	79	79	11.27
31	31	0.11	83	83	13.60
37	37	0.29	89	89	14.76
41	41	0.40	97	97	54.57

(E) $n = p^k$ $(k \geq 1)$ for $3 \leq p \leq 10$

(p, k)	$\#\mathcal{AT}(n)_{\mathbb{Q}_p}$	Time (sec)
$(3, 1)$	3	≤ 0.01
$(3, 2)$	9	≤ 0.01
$(3, 3)$	27	0.04
$(3, 4)$	81	0.59
$(3, 5)$	243	14.67
$(3, 6)$	729	Out of memory
$(5, 1)$	5	≤ 0.01
$(5, 2)$	25	0.03
$(5, 3)$	125	2.23
$(5, 4)$	625	Approx. 5 hrs.
$(5, 5)$	3125	Out of memory
$(7, 1)$	7	≤ 0.01
$(7, 2)$	49	0.16
$(7, 3)$	343	84.87
$(7, 4)$	2401	Out of memory

(D) は 100 以下の奇素数 p に対し，$\mathbb{Q}_p$ の $n = p$ 次完全分岐アーベル拡大の同型類（それぞれ個数は p 個），(E) は $p = 3, 5, 7$ に対して，$n = p^k$ 次（k は自然数）完全分岐アーベル拡大の同型類（それぞれ個数は p^k 個）を全て決定するまでに要した時間を表す．なお (E) の p と n の組み合わせが最も計算困難である[4]．ここで $\#\mathcal{AT}(n)_{\mathbb{Q}_p}$ は $\mathbb{Q}_p$ の n 次完全分岐アーベル拡大の同型類の個数を表す．タイミングデータを見ると，実用的な計算時間に収まる次数の上限はおおよそ 700 くらいであると考えられる．

6 整数論的補足と今後の展望

まず命題 9 のような結果を拡張することを考える．即ち $\mathbb{Q}_p$ の有限次拡大体 K に対し，K 上の n 次拡大の同型類の個数はどれくらいかという問題を考える．これについては Monge が既に公式を得ているが，このアルゴリズムでは巡回拡大 $K(\zeta_{p^i})/K$（ζ_{p^i} は 1 の p^i 乗根で，i は $p^i | n$ を満たすものを走る）の**分岐指数**（ramification index）と**惰性次数**（inertia degree）の計算を要求する．この公式を利用可能とするため，我々はより一般に次の命題を示した．

命題 15 (Yokoyama-Yoshida, [13])
K を $\mathbb{Q}_p$ の有限次拡大体とし $\alpha \in \overline{K}$ とする．この時，単拡大 $K(\alpha)/K$ の分岐次数 e と惰性次数 f を求めるアルゴリズムは以下のように構成出来る：

1. K 上既約かつ $h(\alpha) = 0$ を満たすような多項式 $h(x) \in K[x]$ を選ぶ．h の次数を d とおく．
2. K 上 d 次不分岐拡大（unramified extension）M を構成する．
3. $h(x) \in M[x]$ として h を分解する．その個数が惰性次数 f となる．
4. 分岐指数は $e = d/f$ となる．

公式への適用には巡回拡大の場合だけで十分であるが，これに対してはより高速な実装を実現している．具体的なアルゴリズムは [13] に詳しく記載している，また，上記アルゴリズムにおける不分岐拡大の構成については，効率的な実装が既に Magma にも組み込まれており `UnramifiedExtension` 等の関数を使えば計算可能である．

続いて今回の拡大体データベース生成法の限界を述べる．現時点では，一般の拡大体については計算可能な公式が得られたのみであって，具体的にどのように構成するかという問題は未解決である．そこで問題を緩めてアーベル拡大の場合のみを考えると，不分岐拡大と完全分岐アーベル拡大の高速生成を組み合わせることで次を得ることが出来る．より正確には，不分岐拡大上で（Eisenstein 多項式の）定数項をうまく走らせることで高速生成を実現している．

命題 16
$\mathbb{Q}_p$ 上 n 次アーベル拡大の高速生成アルゴリズムは実装可能．**但し $v_p(n) \leq 2$ を仮定する．**

最後の仮定は，我々のアルゴリズムで本質的に用いている類体論的事情から除去不可である．この仮定を取り除くことが一つの改良の方向として挙げられる．また別の改良としては，$p = 2$ の場合にも適用可能なアルゴリズムを見出すという方向も考えられる．現在得られている低次の拡

[4] 整数論的な理由によるが，本稿では詳細な説明は省く．

大体データベースのうち，例えば $\mathbb{Q}_2$ の 8 次拡大などはかなりの力技で計算されているため，高速化が期待されている．

最後に正標数の場合について補足する．今回改良対象となっていた Pauli-Roblot の拡大体生成アルゴリズムの標数 p 版を考えた時，これが標数 0 の場合に帰着可能であることを論文 [13] の appendix で示した．これは標数 0 の拡大と標数 p の拡大とがある意味で「同値」となるように特別な条件を付加し，既存の拡大体生成アルゴリズムに落とし込むというアイデアを用いている．これにより汎用実装 `AllExtension` をそのまま採用する事が出来るという仕組みである．この理論については若干高度な整数論を用いるため，別の機会に改めて解説を書く予定である．

謝辞

まずはこの度，奨励賞という非常に名誉ある賞を授与頂いた事に対して，日本数式処理学会の関係者の方々に感謝御礼申し上げる．並びに元著論文に対する数多くのアドバイスを下さった田口雄一郎氏（九大数理）と，発表会場にて有益なご質問やコメントを下さった織田孝幸氏（東大数理），照井章氏（筑波大），藤本光史氏（福岡教育大），そして山村健氏（防衛大）に御礼申し上げたい．そして何より，本研究は共同研究者の吉田学氏（九産大付属九産高）の尽力による所が大きく，氏の協力無しでは成果を得る事は不可能であった．心より感謝の意を述べたい．

参 考 文 献

[1] S. Amano: Eisenstein equations of degree p in a p-adic field, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **18**, 1971, pp.1-21.

[2] W. Bosma, J. Cannon and C. Playoust: The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24**, 1997, pp.235-265.

[3] J. Jones and D. Roberts: Number fields of small degree, available at `http://hobbes.la.asu.edu/NFDB/`.

[4] J. Jones and D. Roberts: Local fields of small degree, available at `http://math.la.asu.edu/~jj/localfields/`.

[5] J. Jones and D. Roberts: A database of local fields, *J. Symbolic Comput.*, **41**, 2006, pp.80-97.

[6] K. Kedlaya: Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, *Journal of the Ramanujan Mathematical Society*, **16**, 2001, pp.323-338.

[7] J. Klüners and G. Malle: A database for number fields, available at `http://www.math.uni-duesseldorf.de/~klueners/minimum/`.

[8] P. Panayi: Computation of Leopoldt's p-adic regulator, PhD thesis, University of East Anglia, 1995.

[9] S. Pauli: Constructing class fields over local fields, *J. Théor. Nombres Bordeaux*, **18**, no. 3, 2006, pp.627-652.

[10] S. Pauli and X.-F. Roblot: On the computation of all extensions of a p-adic field of a given degree, *Math. Comp.*, **70**, no. 236, 2001, pp.1641-1660.

[11] A. Travesa: Generating functions for the number of abelian extensions of a local field, *Proc.*

Amer. Math. Soc., **108**, 1990, pp.331-339.

[12] S. Yokoyama and M. Yoshida: High-speed calculation for isomorphy of extension of a p-adic field with Magma, *Transactions of the Japan Society for Industrial and Applied Mathematics*, **22**(4), 2012, pp.277-286.

[13] S. Yokoyama and M. Yoshida: A note on the extension of a p-adic field, 2013, preprint.