虚数乗法論と RECIPROCITY LAW

上田勝 述 AND 土基善文・吉冨賢太郎 記

Contents

0. “ 虚数乗法論と Reciprocity Law” について

上田　勝　（奈良女子大理学部）

早いもので，あの楽しかった賢島の研究会からもう一年が経ってしまいました．企画者の京大の松沢氏から，去年の夏に講演を原稿にまとめるよう依頼されたのですが，生来の遅筆の上，大学を移った等の事情により，断らざるを得ませんでした．ところが京大の土基氏，吉冨氏の両氏が今回私の拙い講演をまとめて下さる事になり，まったく

1993 に上田勝先生が行われた講述のノート (1994 完成) の復刻です。.

すばらしい物に仕上がりました．ここに両氏に心からの感謝の意を表明させて頂きます．

また，元になった講演は確かに私が行った物ですが，ここにでき上がった文章の内容は私の講演の不備を補うのみならず，重要にもかかわらず講演では触れる事のできなかった数々の事柄についての完璧な解説も含まれております．土基氏は，この文章の著者として私の名前をあげておりますが，それは，土基，吉冨の両氏に改めさせてもらいたいと思います．

さて数学上の内容につきましては，土基氏達による本文を参照して頂くとして，ここでは，講演した時の状況とか，賢島のセミナー中の様子とかについて書いて見たいと思います．

講演の一番手は京大の梅田さんでした．梅田さんの講演の数学上の内容は私にはとても理解できない実に深遠な物でしたが，素人にも判ったのは，マンボウの重要性です．志摩マリンランドにいるというマンボウについて実に生き生きと梅田さんは解説して下さいました．その為でしょうか，志摩マリンランドにマンボウを見にいった人が多かったようです．

梅田さんの話によるとマンボウは脳の骨が退化していて固い物にぶつかると脳がつぶれて死んでしまうそうです．そのため飼育が難しく，ここ志摩マリンランドでは水槽の内側に透明のビニールシートを垂らし，脳が粉砕されるのを防いでいるのだそうです．

この話は実に身につまされる話ではないでしょうか？「頭を柔らかくしなさい！」「君はなんて頭が固いんだ！」「数学者は頭が柔軟でなければ」と師匠より言われ続けてきてやっとそれに成功した学生が師匠より与えられた困難な問題に脳を粉砕されている... よく見受けられる光景です．一部の大先生を除いた研究会の参加者が同類であるマンボウに同情の念を禁じ得なかったのは無理もない話でした．

この事についてはまた後に触れるとして，二つ目の講演が私の番でした．私は４日間で４回の講演をして欲しいという事でしたのでここで私は次のような予定表を書きました．

（１）“類体論”という言葉の意味

（２）局所 (local) －大域 (global) の話

（３）虚数乗法論の素朴な解説

（４）二日酔いの為中止

もちろん最後のは（３）と（４）の間に懇親会があった為に書いたJoke のつもりだったのですが（３）と（４）の順番が逆とはいえ，本当の事になってしまいました．ここで改めておわびします．とはいえこれは，東北大の某氏に責任があります．

私の講演の本来の目的は（３）にあったのですが，今回の研究会には数論の専門家が少ないという事で企画者より数論の初歩的な所を解説して欲しいという依頼があり（１）（２）に重点がかかってしまい，本論に入れなかったのは残念でした．しかし，今回講演を文章にまとめてくれた，土基，吉冨の両氏の尽力で私の当初の目論見以上の解説が完成しました．どうかそれをお読み下さい．両氏には重ね重ね感謝いたします．

さて，こんな文章をいつまでも続ける訳にも行かないので，幾つかコメントをかいて，終わりにします．

今回の研究会には数学のいろいろな分野の研究者が集まったのでそれぞれの行動の様式が変わっていて面白いものでした．特に齋藤恭司先生達の特異点のグループは夕食後いつも夜中過ぎまで数学の議論を続けていたのには参りました．このグループの方は朝食，昼食中も数学の話でした．

そういえば，あご湾めぐりの観光船のなかで立命のＮ先生に講演についての質問をされ，景色を見られなかった事もありました．（もっとも風が寒くて見る気もしなかったのですが）

あるいは，Ｈ現論の分野のように酒をのんでは他人の部屋に乱入する，というのもありました．

志摩マリンランドの事について．その後の休憩の時間にみんなでマンボウを見に行きました．マンボウはビニールシートを垂らした水槽の中で，ある者は壁に向かって直進しようともがき，ある者は縦と横を間違えながら泳いでいるといった状況でした．しかし我々の目をひいたのはマンボウだけではなく，隣の水槽に居た小判ザメでした．彼らは３匹並んで水槽の壁に張り付きひたすら水槽の上から落ちて来る

餌を待っているのです．いつ落ちて来るかも判らない餌を！我々は又も身につまされる状況を目撃してしまったのです．こうして暗い気持ちになりながら，我々は志摩マリンランドを後にしたのでした．

後日談

先日 1 年振りに女房と志摩マリンランドにいって参りました．マンボウはまだ同じ場所でもがいていました．一年もがいていたのでしょうか...。私は何ともいえぬ気持ちで隣の水槽に向かいました．

すると，小判ザメは喜ぶべき事に自立していたのです．彼らは何と，「太り過ぎの小判ザメ」なる芸を覚えました．もう壁にははりついていなくても良くなったのです！

研究会に参加した者にとり，これは何を暗示しているのでしょうか？

1994/2/21

1. 始めに（筆記者の一人の落書）

この講演の目的は、モデュラー関数達の成す体の自己同型群を SL_2 のアデール値点全体のなす群によって表現できるという、志村の相互律を紹介することで、そのためにまずそのお手本となるアルティンの相互律の説明、さらにそれらの説明に必要になるイデール、アデール、p-進数体といった基礎的な対象の復習がなされています。これらの話の出発点として、素朴な剰余類型の分解法則が選ばれていることがこの講演のいい所で、一見取り付きにくそうにみえる数論の話題をうまく切り出していると思います。上田先生の語り口は素人にも理解しやすように配慮されており、筆記者の一人 (土基) は (風邪をひいて死にそうであったけれど) とても感銘を受けました。そして、できればこの話を自分の頭の中でもっと整理しておきたいと思いました。そこで、この講演のノートを作る話を聞いたとき、私はすぐにそれに飛び付きました。「やった」と思いました。しかし、考えてみるとこのノートは実際には上田先生ご本人がお書きになるのが最もよろしかった訳で、それを時間の都合等のやむを得ない理由があったにせよ私にまわして来たからには、上田先生にはこのノートの書き方に関して余り大きく主張できないのではないかと睨みました。そこで、私はこのノートでかなり乱暴なことをしても良いのだろうと解釈して、それなら私なりのア

レンジを加えてみようと思いました。このノートの主語はすべて土基である、という体裁になっています。もちろん上田先生の言葉が中心にある訳ですから、このノートは上田先生の言葉を聞いた土基の感想ないし妄想の記録であるといった方が良いかもしれません。そういう訳で、このノートの悪い所は大抵私の妄想であって、読者はそれを気になさらず上田先生の名講義を思い浮かべてくれるようお願いいたします。

このノートを作ることは、私にとって非常に有意義で、面白い時間の一つとなりましたが、他方で数論の奥深さや、難しさもわかって来ました。正直に言うと、上田先生のおっしゃった内容を細部の証明まで理解することは、現在もできていません。ですから、このノートは専ら、類体論とは何をやっているものなのか？イデール、アデールというのは大体どういう物なのか、といった漠然としたことについての「素人」向けの荒い解説をすることが目的になっています。細部についてもっと詳しく知りたい人は、A. Weil の Basic Number Theory や、G. Shimura の Introduction to the arithmetic theory of automorphic functions 等をお読みください。この文章で読者の皆さんが数論気分を満喫できることが、私の目的であり、もっとも大きな喜びです。このノートは塚本千秋先生と長谷川浩司先生のそれぞれがが個人的にとられた二つのノートを下敷きにしました。また、作成にあたっては、このノートのもう一人の筆記者である吉冨賢太郎君に数論のいろいろな基本事項を教えてもらいました。何しろずぶのド素人に教えなければならなかったので彼も大変だったと思います。さらに池田保先生には数論の細かい部分について随分教えてもらいましたし、平賀郁先生には相互律写像のうまい説明を幾種類か考えていただきました。吉岡康太さんにはこの文章の原稿を読んでいただき、細部にわたって有用な意見をいただきました。庵原隆雄さん、久米貴浩さんとの深夜にわたる議論はこの文章を読みよくするのに役に立っていると思います。中村滋さんにはこの文章を TeX で作成する上でのコンピュータのいろいろな事について教えていただきました。このノートの原稿の校正をどうしようか考えていたとき、古田智徳さんと上松和弘さんが快くこれを引き受けてくれ大変助けられました。、しかもその精密な意見はとて

も参考になりました。その他、大勢の人にこの原稿に目をとおしていただき、ご意見やご声援をいただきました。これらの人々に感謝致します。なお、私の悪友座敷童氏 (仮名) にもいろいろな意見をもらって、そのせいでちょっと毛色の変わった所があります。彼に代わって御詫び致します。

土基善文

2. “類体論” という言葉の意味

一言でいうと、

類体 (論)= アーベル拡大 (の理論)

ということができます。もうちょっと詳しく言うなら、k を、$\mathbb{Q}$ 上の代数的数体、つまり $\mathbb{Q}$ の有限次拡大体であるとして、そのアーベル拡大 K/k、ないしそのガロア理論を調べるのが類体論である、とおおざっぱには言っていいでしょう。でもそれだけでは何が問題なのか判らないでしょうから、もっと具体的な話をしましょう。Table 1, 2 に、1 変数 X についてのいろいろな既約多項式の、X が小さい自然数の時の値の表をあげてみました。

TABLE 1. 多項式の値 I

x	x^2+1	$x^4+x^3+x^2+x+1$	x^2+x-1	x^3+x^2-2x-1
0	1	1	-1	-1
1	2	5	1	-1
2	5	31	5	7
3	$10=2\times 5$	$121=11^2$	11	29
4	17	$341=11\times 31$	19	71
5	$26=2\times 13$	$781=11\times 71$	29	139
6	37	$1555=5\times 311$	41	239
7	$50=2\times 5^2$	2801	$55=5\times 11$	$377=13\times 29$
8	$65=5\times 13$	$4681=31\times 151$	71	13×43
9	$82=2\times 41$	$7381=11^2\times 61$	89	$791=7\times 113$
10	101	$11111=41\times 271$	109	$1079=13\times 83$
11	$122=2\times 61$	$16105=5\times 3221$	131	1429
12	$145=5\times 29$	22621	5×31	1847

TABLE 2. 多項式の値 II

x	x^6+x^3+1	x^3-3x+1	$8x^3-6x-1$	$x^4-x^3-4x^2+4x+1$
0	1	1	-1	1
1	3	-1	1	1
2	73	3	$51=3\times17$	1
3	757	19	197	31
4	$4161=3\times19\times73$	53	487	$145=5\times29$
5	$15751=19\times829$	$111=3\times37$	$969=3\times17\times19$	421
6	$46873=19\times2467$	199	$1691=19\times89$	$961=31^2$
7	$117993=3\times37\times1063$	$323=17\times19$	$2701=37\times73$	$1891=31\times61$
8	262657	$489=3\times163$	$4047=3\times19\times71$	3361
9	$532171=19\times37\times757$	$703=19\times37$	$5777=53\times109$	$5545=5\times1109$
10	$1001001=3\times333667$	971	$7939=17\times467$	8641
11	1772893	$1299=3\times433$	$10581=3\times3527$	$12871=61\times211$
12	$2987713=37\times80749$	1693	13751	18481

これらの表を見てみると、いろいろとおもしろい事が判ります。例えば、Table 1 の一番初めの X^2+1 の場合を見てみましょう。X^2+1 の値を素因数分解して出てくる素数を列挙してみると、

$$2,5,13,17,29,37,41,61,101,\dots$$

となりますが、これを見ると、2 を例外として、あとの素因子はすべて 4 で割って 1 余る数になっています。これは、偶然でしょうか？

次の、$X^4+X^3+X^2+X+1$ の値の素因子も並べてみましょう。

$$5,11,31,41,61,71,151,271,311,2801,3221,22621,\dots$$

これらは、5 を例外として、すべて 10 で割って 1 余る数、つまり末尾が 1 である数になっています。同じ様にして見てやると、$X=0,1,2,3,\dots,12$ に対して、

- X^2+X-1 の素因子は 5 を除いてすべて $\pm1 \mod 10$。
- X^3+X^2-2X-1 の素因子は 7 を除いてすべて $\pm1 \mod 14$。
- X^6+X^3+1 の素因子は 3 を除いてすべて $\pm1 \mod 18$。
- X^3-3X+1 の素因子は 3 を除いてすべて $\pm1 \mod 18$。
- $8X^3-6X-1$ の素因子は 3 を除いてすべて $\pm1 \mod 18$。

- $X^4 - X^3 - 4X^2 + 4X + 1$ の素因子は 5 を除いてすべて $\pm 1 \bmod 30$。

である事が判ります。± 1 というのはなんかズルイ感じがするかもしれませんが、ディリクレの算術級数定理、

算術級数定理

「任意の正の整数 d と、d と互いに素な任意の自然数 r に対して、
$$\lim_{n\to\infty} \frac{\#\{n \text{ よりも大きい素数で、} d \text{ で割ると } r \text{ 余るもの}\}}{\#\{n \text{ よりも大きい素数}\}} = \frac{1}{\varphi(d)},$$
ここに $\varphi(d)$ はオイラーの関数 (d より小さく、d と互いに素な自然数の数)。すなわち、素数を d で割った数の余りの分布は、(もちろん d と余りとは互いに素であるという自明な条件を除いては、) 一様である。」

を見ると、もし上に述べたような事が一般の自然数 x に対して成り立つなら、上にあげたような多項式の値に、ある規則性が存在するということになります。

そこで、上にあげた事は本当に正しいのか、どうやってチェックすればいいのか？ということになるわけですが、例えば X^2+1 の時には、次のように考えれば処理できます。2 以上の素数 p に対して、

$$\begin{aligned}
& x^2 + 1 \equiv 0(p) \\
\Leftrightarrow\quad & x^2 \equiv -1(p) \\
\Leftrightarrow\quad & (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times \text{ の中で、} x \text{ の位数が } 4 \\
\Leftrightarrow\quad & 4|(p-1) \qquad (\because (\mathbb{Z}/p\mathbb{Z})^\times \text{ は位数が } p-1 \text{ の巡回群}) \\
\Leftrightarrow\quad & p \equiv 1(4).
\end{aligned}$$

あとでまた詳しく述べますが、そのほかの例についても実は、一番初めにあげた主張が正しいことが証明できます。しかし、すべての多項式が上にあげたような性質を満たすわけではありません。その様な、だめな例として X^3-2 を考えてみましょう。先程と同様に考えてみると、p が x^3-2 の形の数の素因数になるのはちょうど 2 が $\mathbb{Z}/p\mathbb{Z}$ の中で三乗根を持つときです。$\mathbb{Z}/p\mathbb{Z}$ の乗法群の構造、

$$(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$$

から $p-1$ が 3 と互いに素であるとき (すなわち p が $3n+2$ の形の素数のとき) にはいつでも 2 (に限らず任意の数) は $\mathbb{Z}/p\mathbb{Z}$ の中で三乗根を持ち、したがってこのとき p は x^3-2 の形の数の素因数になる事がわかります。p が $3n+1$ の形の素数のときには、少し厄介ですが、$(\mathbb{Z}/p\mathbb{Z})^\times$ の元の中で三乗根を持つものは丁度その 1/3 ほどである事から、2 がその様な数になる可能性は、1/3 ぐらいである事は、大体想像できるでしょう。厳密にやろうとすると少々難しいですが、とにかく「与えられた素数が x^3-2 の素因数として現れるかどうか」は適当な数に関する剰余類だけでは判別できないことがわかります。X^4-2 なんかでも同様です。この違いはどこから生じるのでしょうか？

この問いの答を出す前に、もう一つのおもしろい現象を紹介しましょう。フィボナッチ数列

$$u_n = u_{n-1} + u_{n-2}, \quad u_1 = 1, u_0 = 0 \tag{2.1}$$

の、n が小さいときの表を Table 3 にあげておきました。

TABLE 3. フィボナッチ数列

n	1	2	3	4	5	6	7	8	9	10
u_n	1	1	2	3	5	8	13	21	34	55
	11	12	13	14	15	16	17	18	19	20
	89	144	233	377	610	987	1597	2584	4181	6765
	21	22	23	24	25	26	27	28	29	30
	10946	17711	28657	46368	75025	122393	196418	317811	514229	832040
	31	32								
	1346269	2178309								

この表を眺めてみると、やはりおもしろい事がたくさん目につきます。例えば u_n が偶数になるような n は、2 つ飛びに現れていますし、u_n が 3 の倍数になるような n は、3 つ飛びに現れています。(これらはの確認は簡単にできますから、やってみることをおすすめします。) この講演の視点からは、例えば各素数 p について 5 を法として現れる次

の規則性

$$u_5 \equiv 0 \pmod 5$$
$$u_{p+1} \equiv 0 \pmod p \quad (p \equiv 2,3 \quad (5) \text{ のとき})$$
$$u_{p-1} \equiv 0 \pmod p \quad (p \equiv 1,4 \quad (5) \text{ のとき})$$

を説明することができます。もちろん、この事は、漸化式 2.1 と深い関係にある方程式、

$$X^2 = X + 1$$

の解 $\alpha, \beta = (1 \pm \sqrt{5})/2$ を用いて、u_n が、

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \ (= \frac{1}{\sqrt{5}} \times \{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n\})$$

と表記されることと密接に関連しています。これはこの講演の理解度をチェックする宿題として残しておきましょう。今のような、「n の剰余類によって決まる性質」がもっとも端的に現れるのは、何といっても、

$$u_n = -(u_{n-1} + u_{n-2}) \quad u_0 = 0, u_1 = 1$$

で、これは $0, 1, -1$ がくり返し現れる単純な数列になります。これは余りにもつまらないという向きには、

$$u_n = 2(u_{n-1} + u_{n-2})$$

などはどうでしょう。これは modulo 12 で面白い性質を持ちます。

さて、いよいよここで問題の解答を与えましょう。問題の方を先に整理しておくと、次のようになります。まず、整数係数の既約多項式 $f \in \mathbb{Z}[X]$ について、「剰余類型の分解法則が成り立つ」という言葉で、

剰余類型の分解法則

《ある正の整数 d と、剰余類の族 $\{a_i\}_{i=1}^s \subset \mathbb{Z}/d\mathbb{Z}$ があって、
$\{p : \text{prime}; f(X) \equiv 0 \pmod p$ が $\mathbb{Z}$ に解を持つ。$\}$
$=\{a_i + \mathbb{Z}d$ の中に出てくる素数 $(1 \le i \le s)\}$
が (p について有限個の例外を除いて) 成り立つ》

ということを表すことにします。すると問題は単純に、

問題

どのような方程式 f が剰余類型の分解法則を持つか？

ということになります。答の方も簡単に表現することができて、

答

f の根の体 $\mathbb{Q}(X)/(f(X))$ が $\mathbb{Q}$ 上アーベル拡大のとき。

ということができます。数表の方に戻って確かめて見ますと、

$$f = X^2+1, X^4+X^3+X^2+X+1, X^6+X^3+1$$

はそれぞれ 1 の原始 $4, 5, 9$ 乗根の最少多項式ですから、これらの例については確かに $\mathbb{Q}(X)/(f(X))$ は $\mathbb{Q}$ の上のアーベル拡大です。そのほかの例についても拡大 $(\mathbb{Q}(X)/(f(X)))/\mathbb{Q}$ がアーベルであることを確認できます。

$\mathbb{Q}$ に、1 の巾根

$$\zeta_n = \exp\left(\frac{2\pi\sqrt{-1}}{n}\right)$$

を付け加えた体 $\mathbb{Q}(\zeta_n)$ を円分体 (cyclotomic field) といいますが、これはもちろん $\mathbb{Q}$ のアーベル拡大の重要な例になります。実際、同型

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

が、《$\mathbb{Z}/n\mathbb{Z}$ の可逆元 a に対して

$$\zeta_n \mapsto \zeta_n^a$$

によって決まるガロア群の元 σ_a を対応させる》ことにより与えられます。

このことと上の「答」からわかる、

わかる事実

円分体 は類体である。すなわち ζ_n の最少多項式（円分多項式）は剰余類型の分解法則を持つ。

という事実が、数論における一つの大きな発見であるといっても良いでしょう。下の体を $\mathbb{Q}$ に限らないで一般の数体としたときにも、

アーベル体=類体

という主張は正しく、類体論における基本的な定理の一つになっています。実は、下の体が $\mathbb{Q}$ の場合には次のようなうまい特殊事情があります。

Kronecker-Weber の定理

$\mathbb{Q}$ の任意のアーベル拡大はある円分体に含まれる。特に、

$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_n \mathbb{Q}(\zeta_n).$$

(代数体の最大アーベル拡大に関する似たような表示は、虚二次体のような限られた場合にしか良くわかっていません。) この事は、$\mathbb{Q}$ の上の類体論の説明を比較的易しくしてくれます。

3. 局所 (LOCAL)-大域 (GLOBAL) の話

まずゼータ関数から話をはじめましょう。

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (\Re(s) > 1)$$

この関数は次のような無限積展開を持ちます。

$$\begin{aligned}\zeta(s) =& (1 + 2^{-s} + 2^{-2s} + \dots)(1 + 3^{-s} + 3^{-2s} + \dots)(1 + 5^{-s} + 5^{-2s} + \dots)\dots \\ =& \prod_{p:\text{prime}} (1 - p^{-s})^{-1}\end{aligned}$$

この無限積展開は、素因数分解の一意性からきています。実際、無限積を展開すると、その展開の各項は p^{-s} を重複を許して有限個とったものの積であることがわかるでしょう。この事だけでも、ゼータ関数が素数と強く結び付いていることは十分予測できます。実際、ゼータ関数を用いて素数が無限個存在することを示すことができますし、もっと精密に、素数の分布の具合が、ゼータ関数に関する、リーマンのある重要な予想と結び付いていることは、皆さんもご存じでしょう。

ゼータ関数の値の中で、例えば、

$$\zeta(2) = \sum_{i=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

は良く知られているとおもいます。無限積展開を使えば、

$$\frac{\pi^2}{6} = \prod_p (1-p^{-2})^{-1}.$$

この両辺を良く眺めてみると、とてもおもしろいことがわかります。左辺は、$\mathbb{R}, \mathbb{C}$ に関係する量、もっといえば、$\exp, \sin, \cos$ の周期に関係するような量であるのにたいし、右辺は、素数に関する量になっています。これは、別に $\zeta(2)$ に限ったことではなく、一般に、

$$\zeta(2m) = \prod_p (1-p^{-2m})^{-1} = \pi^{2m} B_{2m} \qquad (B_{2m} \in \mathbb{Q} \text{ はベルヌーイ数})$$

という関係が成り立ちます。[ここに出てくる第三の役者、ベルヌーイ数もなかなか興味ある対象で、いろいろと興味深い性質を持っています。]

ここに見られるような、すべての素数に関する量と、実数や複素数に関する量とを結び付ける式を説明するうまい理論として、以下ではアデールによる定式化を見てみる事にしましょう。このアデールの理論は、各々の素数についての理論 (「局所的」な理論) をつなぎあわせて「大域的」に見る理論であるといえます。この理論によって、ガロア群

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

についても、$\mathbb{Q}(\zeta_n)$ についての二通りの見方 (アーベル拡大、分解法則の成り立つ体) をうまく統合したい、という目論見もあります。

3.1. **p-進数 (p-adic number).** この小節では、局所的な理論、つまり各々の素数についての詳しい様子を見る理論、特に、p-進数体の事について述べようとおもいます。p-進数体の研究は、ヘンゼルによって始められましたが、彼と同時代のヒルベルトは、彼の事をバカにしていた節があって、ヒルベルトの弟子であったハッセがヘンゼルに再入門した時ヒルベルトとハッセの仲が少し悪くなったというような事もあったようです。

さて、任意の正の整数 a は、

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n \quad (a_0, \ldots, a_n \in \{0, 1, \ldots, p-1\})$$

と一意的にあらわせます。これは、単に a を p-進法で、

$$a = (a_n a_{n-1} \dots a_2 a_1 a_0)_{(p)}$$

と表現できるということにすぎません。私達の１０進法は、１０が素数でないのでこれからの話にはむきませんが、例えばコンピュータをやる人なら２進法は良くご存じでしょう。一般に、正の実数は p-進小数を用いて、

$$a = (a_n a_{n-1} \dots a_2 a_1 a_0 . a_{-1} a_{-2} \dots)_{(p)}$$

と表記できます。ここでちょっといたずら心をおこして、この表記を小数点を境にひっくり返してしまうことを考えてみましょう。無限小数だと面倒なので、有限小数だけに限ると、

$$a = [a_{-n} a_{-n+1} \dots a_{-2} a_{-1} . a_0 a_1 a_2 \dots a_n]_{(p)} \tag{3.1}$$

とこういう具合になるはずです。別に何ら変わったところが無いようにもみえます。実際、足し算や掛け算も、普通の時と大体同じ調子で計算できます。普通と大きく異なるのは、繰り上がりの規則で、例えば

$$[0.1]_{(5)} + [0.4]_{(5)} = [0.01]_{(5)}$$

という具合になります。つまり普通とは逆に右側に繰り上がることになります。

さて、こうすると、すべての正整数は、

$$[0.531461632]_{(7)}$$

のように、0 コンマいくらと表記されることになります。なんとなく小さく感じるのではないですか？さらに、a が小数点以下 N 桁までゼロ、つまり、

$$a = [0 . a_0 a_1 a_2 \dots a_N \dots a_M]_{(p)}$$

とあらわした時、

$$a_i = 0 \quad (0 \le i < N)$$

だということと、a が p^N で割り切れること、つまり $a \equiv 0 \mod p^N$、は同値になります。こういうわけで、p の大きいべきで割れるほど、「小さい」とみなせるようなおもしろい体系を、今から少し考えてみましょ

う。有限小数 (3.1) の形であらわされるものの全体は、分母が p の巾からなるような正の有理数全体と一致します。当然、無限小数

$$a = [a_{-n}a_{-n+1}\dots a_{-2}a_{-1}.a_0a_1a_2\dots]_{(p)}$$

も考えられるはずです。実は、実数を考える時に見られた表記の不定性、

$$0.999999999\cdots = 1.00000\dots$$

は、この場合にはありません。その代わりに、もっと奇妙なこと、つまり、「プラス符号の」無限小数のマイナス元がまた「プラス符号の」無限小数であらわされる、ということが起こります。(そこで「プラス符号」「マイナス符号」はこの体系では意味がありません。)

$$[0.1]_{(2)} + [0.111111111\dots]_{(2)} = 0$$

これが例の繰り上がりの奇妙な規則のせいであるのは明白でしょう。割り算は、繰り下がりの規則にさえ気を付ければ、通常と同じ様にできます。つまり、こうして定義した無限小数の全体は、体をなします (これを p-進数体 $\mathbb{Q}_p$ と呼びます。)。このことは、特に、$\mathbb{Q}$ の元がすべて私達の無限小数で書けることを意味しています。

今見たことを、「小さい」という表現を明確にしてもう一度整理してみましょう。任意の有理数 x に対して、その位数 (オーダー) を、

$x/p^{\mathrm{ord}_p x}$ を既約分数で表現した時、分母分子は共に p と互いに素である。

がなりたつように定義します。(ただし 0 の位数は無限大と解釈しておきます。以下では 0 のこのようなやや例外的だが明らかな約束事に関しては、いちいち述べないことにします。) さらに、x の「ノルム」(p-進ノルム) を、

$$|x|_p = p^{-\mathrm{ord}_p(x)}$$

で定義します。もちろんこれは元の大きさを計るもので、期待通り $\mathbb{Z}$ の元にたいしてはそのノルムは小さい、1 以下である、ことがすぐにわかります。p-進ノルムは次の性質を満たします。

$$|xy|_p = |x|_p|y|_p \tag{3.2}$$

$$|x+y|_p \le |x|_p + |y|_p \tag{3.3}$$

実は下の不等式はさらに強く、

(3.4)

$$|x+y|_p \leq \max(|x|_p, |y|_p) \qquad (|x|_p \neq |y|_p \text{ ならば等号が成り立つ。})$$

とできます。

ちょっと確かめておきましょう。有理数 x, y を、

$$x = p^{\mathrm{ord}_p(x)}\tilde{x} \tag{3.5}$$

$$y = p^{\mathrm{ord}_p(y)}\tilde{y} \tag{3.6}$$

と書いてみれば、位数の定義とから、$\tilde{x}, \tilde{y}$ が共に分母分子とも p の倍数でないような既約分数であらわされます。x と y の立場を必要なら入れ替えれば、$\mathrm{ord}_p(x)$ の方が $\mathrm{ord}_p(y)$ より大きいとして十分でしょう。そうすると、

$$x+y = p^{\mathrm{ord}_p(y)}(p^{\mathrm{ord}_p(x)-\mathrm{ord}_p(y)}\tilde{x} + \tilde{y}) \tag{3.7}$$

となりますが、実際には p の倍数でないような数を掛けることは p-進ノルムに影響しませんので、両辺にそういう数を掛けて、$\tilde{x}$ や $\tilde{y}$ は整数としてよろしい。するとどういうことになるかというと、もし x と y の位数が等しくないならば、$p^{\mathrm{ord}_p(x)-\mathrm{ord}_p(y)}\tilde{x} + \tilde{y}$ の部分は p で割り切れない整数であるし、よしんば等しくてもこの部分は整数なのだから、どの道 (3.7) の右辺の p-進ノルムは $p^{-\mathrm{ord}_p(y)}$ よりも小さいことになります。(整数のノルムは小さいことを忘れずに。)

これで (3.4) が証明できました。この不等式が成り立つことから、$\mathbb{Q}_p$ の幾何学は通常のものとは大分と異なることがわかります。例えば、

- すべての三角形は二等辺三角形である。
- 円内のすべての点はその円の中心である。

ということがわかります。(講演ではこのことの証明も簡単に解説されましたが、ここでは読者の楽しみにとっておきましょう。ここで数分考えてみることをおすすめします。)

さて、$\mathbb{Q}_p$ に話を戻しましょう。この体は、今のノルムの言葉を使うと、$\mathbb{Q}$ のこのノルムに関する完備化であるということができます。$\mathbb{Q}_p$ にもこの p-進ノルムは延長されて、(3.2)〜(3.4) を満たすことも、言う

までもないでしょう。結局、$\mathbb{Q}_p$ は「無限小数」

$$a = [a_{-n}a_{-n+1}\dots a_{-2}a_{-1}.a_0a_1a_2\dots]$$

あるいは、書き方を変えるなら、

$$a = \sum_{i\gg -\infty}^{\infty} a_i p^i$$

(これは $\mathbb{Q}_p$ の中の収束級数と考えることもできます。) の全体であって、それには p-進ノルム

$$|a|_p = p^{-\min\{i;a_i\neq 0\}}$$

が定義されていて、$\mathbb{Q}_p$ の位相は、0 の基本近傍系として、

$$O_n = \{x \in \mathbb{Q}_p; |x|_p \leq p^{-n}\}$$

を採ることにより得られる。ということになります。(こういう風に現代的な言葉で言ってみると、p-進数の定義も確固たるもののような気がしますが、始めに述べたような導入のしかたでは、何か胡散臭げな感じを受ける人があっても仕方が無いかもしれません。ヒルベルトがヘンゼルを評価しなかったのもひょっとしたらこういう所が気になったからかもしれません。) ここで、特に、 $n = 0$ の時、つまり O_0 は $\mathbb{Z}_p$ と書かれ、 これは $\mathbb{Q}_p$ の極大コンパクト部分環になります。この集合は、0 コンマいくらと表される元ばかりを集めた集合ですから、実数の $[0, 1]$ 区間と同様な感覚で、コンパクトなのは肯けると思いますが、これが環でもある、つまり掛け算や足し算についても閉じている、という所がすごいところです。開集合がコンパクトと言うのも、普通の感覚とずれる所です。もちろん、重要なことですが、$\mathbb{Z}$ は $\mathbb{Z}_p$ の部分集合であり、後者は前者の完備化になっています。

これらのことから、$(\mathbb{Q}_p, +)$ は、局所コンパクトアーベル群である。と結論することができます。一般論により、その様な群にはハール測度 (左不変測度) が存在します。$\mathbb{Q}_p$ のハール測度を $d\mu_p$ と書きましょう。(要するに、 $\mathbb{Q}_p$ の部分集合の測度 (体積) だとか、$\mathbb{Q}_p$ 上の関数の積分だとかを、通常と同じ様に考えることができて、それは加法と協調的である。つまり、部分集合や関数を平行移動したものの測度や積

分が、元のものと変わらない:

$$\mu_p(a+S)=\mu_p(S),\quad \int_{\mathbb{Q}_p} f(a+x)d\mu_p(x)=\int_{\mathbb{Q}_p} f(x)d\mu_p(x)$$

ということです。) 実際には、このような測度の存在を頭から認めてしまえば、幾つかの測度や積分は不変性だけから容易に計算することができます。まず、このような測度は定数倍の任意性がありますから、それをノーマライズするために、

$$\int_{\mathbb{Z}_p} 1 d\mu_p = 1$$

であるとしましょう。(これは $[0,1]$ 区間の測度が 1 であることと対比できるかもしれません。) そうすると、任意の整数 n に対して、

$$\mu_p(O_n)=\int_{O_n} 1\cdot d\mu_p = p^{-n}$$

が成り立つことがわかります。n が正であるとして、これを説明してみましょう。O_n というのは、小数点以下 n 桁目まで 0 であるような p-進数の全体ですから、$\mathbb{Z}_p$ の中には、小数点以下最初の n 桁目までの違いによって都合 p^n 個の O_n のコピー、平行移動が入っていることがわかります。つまり、

$$|\mathbb{Z}_p : O_n| = p^n.$$

体積が 1 の所に、p^n 個の同じ体積のものが入っているわけですから、結局一個一個の体積は p^{-n} ということになります。同じような考え方で、n が負の時も処理できるでしょう。

ハール測度のことが出てきたついでに、$\mathbb{Q}_p$ の乗法群 $\mathbb{Q}_p^\times$ のハール測度 $d\mu_p^\times$ もここで登場させておきましょう。これはもちろん不変性

$$\mu_p^\times(a\times S)=\mu_p^\times(S),\quad \int_{\mathbb{Q}_p^\times} f(a\times x)d\mu_p^\times=\int_{\mathbb{Q}_p^\times} f(x)d\mu_p^\times$$

を持つ測度のことです。ノーマリゼーションは、$\mathbb{Z}_p^\times$ の体積が丁度 1 になるようにとります。

$$\mu_p^\times(\mathbb{Z}_p^\times)=1$$

この $\mathbb{Z}_p^\times$ と言うのは、$\mathbb{Z}_p$ の乗法群で、言い方をかえれば、p-進ノルムが丁度 1 であるような $\mathbb{Q}_p$ の元の全体です。

3.2. **アデール (adele)・イデール (idele).** ここから、「大域」の方のお話をしましょう。先程の、ゼータ関数の話で出て来た等式

$$\frac{\pi^2}{6} = \prod_p (1-p^{-2})^{-1}$$

を再び思い起こしてみましょう。右辺の各因子は、先程の、$\mathbb{Q}_p$ のある部分集合の体積と関係付けられそうです。(π が何の体積 (面積、長さ) と関係付けられるかはいうまでもないでしょう。) 右辺は、すべての p についての積になっています。そこで、一つ一つの p について考えるのではなく、すべての $\mathbb{Q}_p$ を束にして考えることができるとよさそうです。そこで、次のようなものを考えてみましょう。

$$\mathbb{Q}_A = \prod_p{}' \mathbb{Q}_p \times \mathbb{R} \subset \prod_p \mathbb{Q}_p \times \mathbb{R}$$

ここに、《制限直積》 $\prod'$ の意味は、

$$\mathbb{Q}_A \ni (a_p, r) \Leftrightarrow (\text{有限個の } p \text{ を除き、 } a_p \in \mathbb{Z}_p)$$

ということです。$\mathbb{Q}_A$ を、アデール環と呼びます。もう少しキモチヨクというか、位相が良くわかるように、これを定義するには、次のようにすればよいでしょう。

$$\mathbb{Q}_A = \varinjlim_{\substack{S \subset P \\ S:\text{有限}}} \mathbb{Q}_A(S)$$

ここに、P は素数全体の集合で、$\mathbb{Q}_A(S)$ は、次で定義されます。

$$\mathbb{Q}_A(S) = \prod_{p \in S} \mathbb{Q}_p \times \prod_{p \notin S} \mathbb{Z}_p \times \mathbb{R}$$

これは (チコノフの定理により、) すぐわかるように、局所コンパクト群ですから、ハール測度が入り、その順極限として、$\mathbb{Q}_A$ にもハール測度が入ります。

あえていうなら、アデール環は、$P \cup \{\infty\}$ を時間パラメータと見た、経路の空間であるとみることもできるでしょう。ただし、各「時刻」 p における粒子の位置は、$\mathbb{R}$ ではなくて $\mathbb{Q}_p$ に入っている所が特異な所です。(∞ においては $\mathbb{R}$ のままで可。) 《制限直積》の意味は、例えて言うなら、経路が有限個の時刻の例外を除けば、$[0,1]$ 区間に閉じこめられているということで、これは確かに $\mathbb{R}$ の世界では気持ちの良く

ない条件であるけれども、$\mathbb{Q}_p$ の中では $\mathbb{Z}_p$ は標準的な、重要な存在であるので、アデール環も重要な対象になってくる。といえるでしょう。(もちろん P が飛び飛びの集合であるということも事をやさしくしている一つの原因です。)

アデール環の乗法群ともいうべき、イデール群もここで導入しておきましょう。定義は、

$$\mathbb{Q}_A^\times = \prod_p{}' \mathbb{Q}_p^\times \times \mathbb{R}^\times \subset \prod \mathbb{Q}_p^\times \times \mathbb{R}^\times,$$

で、ここに、制限直積 $\prod'$ の意味は先程とは少し異なって、

$$\mathbb{Q}_A^\times \ni (a_p, r) \Leftrightarrow (\text{有限個の } p \text{ を除いて、} a_p \in \mathbb{Z}_p^\times.)$$

とします。イデールという言葉はイデアルという言葉をもじっており、アデールとは additive idele のイミのようです。アデール環の場合と同様にイデール群にもハール測度 $d\mu_A^\times$ が入ります。(少し技術的な事になりますが、イデール群の位相はアデール環の位相からの誘導位相ではないという事に注意しておきます。イデール群の中で、ネット (点列とおもって差し支えありません) $\{a_i\}$ が収束するという事は、そのネット $\{a_i\}$ と、逆元を並べたネット $\{a_i^{-1}\}$ が共にアデール環の中で収束するというのと同値です。) もう一つ定義をしておきましょう。イデール群 $\mathbb{Q}_A^\times$ の元の 「イデールノルム」 を、

$$\mathbb{Q}_A^\times \ni a = (a_p, a_\infty) \mapsto |a|_A = \prod_p |a_p|_p |a_\infty|_\infty$$

で定めます。ほとんどすべての p について、$|a_p|_p = 1$ ですから、これは有限で、しかもゼロではありません。

さて、ゼータ関数をイデール群の上の関数の積分と解釈してみましょう。まず次のようなアデール環上の関数を導入します。

$$\Phi_A = \prod_p \Phi_p \times \Phi_\infty,$$

ここに、

$$\Phi_\infty : \mathbb{R} \ni x \mapsto \exp(-\pi x^2), \tag{3.8}$$

$$\Phi_p : \mathbb{Q}_p \ni x \mapsto \begin{cases} 1 & (x \in \mathbb{Z}_p \text{のとき}) \\ 0 & (x \notin \mathbb{Z}_p \text{のとき}) \end{cases}. \tag{3.9}$$

そこで、 複素数 $s \in \mathbb{C}, \Re s > 1$ に対して、積分

$$\int_{\mathbb{Q}_A^\times} \Phi_A(a)|a|_A^s d\mu_A^\times \tag{3.10}$$

を考えてみます。イデール群上の積分は、被積分関数が今の場合のように $\mathbb{Q}_p^\times$ 上の関数の積に分解できる時には、単にそれぞれの因子の積分の積と同じになります。(この事はイデール群の測度の決めかたを逐一見ていけばわかります。また、これは $\mu_p^\times$ のノーマリゼーションのしかたと無縁ではありません。1 はいくら掛けても 1 であるというのが効いています。)

$$\prod_p \int_{\mathbb{Q}_p^\times} \Phi_p(a_p)|a_p|_p^s d\mu_A^\times \\ \times \int_{\mathbb{R}^\times} \exp(-\pi x^2)|x|_\infty^s d\mu_\infty^\times$$

$\mathbb{R}^\times$ の不変測度 $d\mu_\infty^\times$ は、$dx/|x|$ と同じですから、「無限素点」での積分の方は、

$$\int_{\mathbb{R}^\times} \exp(-\pi x^2)|x|_\infty^s d\mu_\infty^\times = \int \exp(-\pi x^2)|x|^{s-1} dx = \pi^{-s/2}\Gamma(s/2)$$

となります。他方、有限素点での積分は、

$$\int_{\mathbb{Q}_p^\times} \Phi_p(a)|a_p|_p^s d\mu_p^\times \tag{3.11}$$

$$= \int_{\mathbb{Q}_p^\times \cap \mathbb{Z}_p} |a_p|_p^s d\mu_p^\times \tag{3.12}$$

という具合になりますが、ここで、被積分関数の値によって、積分領域 $\mathbb{Q}_p^\times \cap \mathbb{Z}_p$ を分けてみましょう。

$$\mathbb{Q}_p^\times \cap \mathbb{Z}_p \tag{3.13}$$

$$= \coprod_{n=0}^{\infty} \{x \in \mathbb{Q}_p; |x|_p = p^{-n}\} \tag{3.14}$$

$$= \coprod_{n=0}^{\infty} p^n \mathbb{Z}_p^\times \tag{3.15}$$

そこで、私達の積分は、定数の積分の可算和として書ける事になります。

$$\begin{aligned} &\sum_{n=0}^{\infty} \int_{p^n\mathbb{Z}_p^\times} p^{-ns} d\mu_p^\times \\ =&\sum_{n=0}^{\infty} p^{-ns} \mu_p^\times(p^n\mathbb{Z}_p^\times) \\ =&\frac{1}{1-p^{-s}} \end{aligned}$$

結局、

$$\begin{aligned} &\int_{\mathbb{Q}_A^\times} \Phi_A(a)|a|_A^s d\mu_A^\times \\ =&\pi^{-s/2}\Gamma(s/2)\prod_p (1-p^{-s})^{-1} \\ =&\pi^{-s/2}\Gamma(s/2)\zeta(s) \end{aligned}$$

となり、思惑通りゼータ関数をイデール群上の積分として表すのに成功しました。これはなかなか有用なもので、例えばゼータ関数の関数等式

$$\zeta(s) \leftrightarrows \zeta(1-s)$$

をこのような枠組みのもとでフーリエ変換の理論 (特にポアソンの和公式等) を用いて証明することもできます。このような $\mathbb{Q}_A, \mathbb{Q}_A^\times$ 上の Fourier 解析学はヴェイユによって始められました。[1] この方法は、GL_1 を一般の代数群に置き換えることによりゼータ関数の理論を容易に拡

[1] ここは少し土基の筆が滑ってしまったようで、イデール、アデール上のフーリエ解析を始めたのはテイトと岩沢ではないかと梅田先生から御指摘を受けた。数学辞典には E. アルティンの名も見受けられる。そこで改めて上田先生の指示を仰いだ結果、非常におもしろいメールが返ってきたので、これはこの節の末尾に載せる事にします。

張できるという利点も持っています。(イデール群は GL_1 の $\mathbb{Q}_A$-値点であることに注意しましょう。)

ゼータ関数は数論的な諸性質を解析関数で表すことができる面白い存在で、ここではそれが上のような積分の理論に持つ事を、局所・大域の話との関連から説明をしてみました。数論に興味のある方はゼータ関数を一つの道しるべとして先に進む事も可能でしょう。しかしここではゼータ関数の話はこのぐらいにして次のセクションからまた類体論の話に戻ることにしましょう。

おまけ：誰がアデール、イデール上のフーリエ解析学を始めたか？

（上田先生の e-mail からの抜粋)

> Tate は S.Lang と共に E.Artin の弟子でした．彼の学位論文が Fourier Analysis on Idele についての論文でした．多分この考えについて最初に公表された論文ではないでしょうか．一方　岩沢先生はこれとは独立に全く同じアイディアを別な場所（Tate はヨーロッパ、岩沢先生はアメリカ）で講演等で発表していたはずです．しかしこれは論文の形にはなっていないのではないでしょうか？
>
> Tate はこの論文で Artin の後継者として認められ、更に Artin の娘も獲得しました．ライバルの S.Lang は傷心の思いを胸に、新大陸アメリカに渡り、A.Weil のところに入門したのです.（かなり脚色してあります (ˆ ˆ;)）
>
> A.Weil はこの Tate の学位論文のアイディアを教科書で紹介しました．それが Basic Number Theory です．もっとも、アデール群が重要だ、というアイディア、それと、位相群の上のフーリエ解析の理論の創設は A.Weil に拠るのですから、A.Weil の名前が出てくるのもおかしくはないのです.
>
> そこで、正解となると、やはり、Tate と Iwasawa でしょう.

4. アルティン写像

4.1. **ガロア群の幾何学的イメージ.** アルティン写像は、$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ についての完全な情報を与えてくれますが、その説明に入る前に、この節と次の節ではガロア群について少し復習しておくことにします。

この節はガロア群の幾何学的なイメージの確認を行います。 $\mathbb{C}$ 上の一変数有理関数体 $K = \mathbb{C}(Y)$ のガロワ拡大と、その拡大のガロワ群について考えてみましょう。 K の有限次代数拡大体になっているような体（一変数代数関数体）はあるリーマン面の関数体と見なせました。これについて復習してみましょう。K は非斉次座標 Y を持つ射影空間 $\mathbb{P}^1$ の上の有理関数全体のなす体と同型です。K の有限次代数拡大体 L をとってきてやると、代数拡大という言葉の定義によりこの体の任意の元 X は K 上の適当な代数的な関係式

$$F_Y(X) = \sum_{i=0}^{n} a_i(Y)X^i = 0 \quad (a_i(Y) \in K)$$

を満たすはずです。F_Y として最小のものをとってきましょう。K に X を付け加えた体 $K(X) = \mathbb{C}(X, Y)$ は、方程式 $F_Y = 0$ を $X - Y$-平面にプロットした《グラフ》の上の有理型関数の全体に一致します。この《グラフ》の上にはもともとの Y-座標の他に、X-座標（を制限したもの）があるという訳です。簡単な考察により、$L = K(X) = \mathbb{C}(X, Y)$ となる X が存在する事がわかります。つまり任意の一変数代数関数体はある方程式 $F_Y = 0$ の《グラフ》 Γ_{F_Y} の上の有理型函数全体のなす体と見なせる訳です。包含写像 $K \subset L$ は、P^1 上の有理型関数を Γ_{F_Y} 上に引き戻して Γ_{F_Y} 上の関数を作ることに対応しています。

《このように、体論において、体の「生成元」というのは、体に対応する代数多様体（この場合には《グラフ》）の埋めこまれた先（この場合には $\mathbb{P}^2$) の「座標」とみなせ、生成元達の代数的な関係式は、埋めこんだ先での定義方程式を与えていると考えて差し支えありません。もちろん、生成元の取り方がいろいろある事は、多様体の埋めこみ方、座標の取り方がいろいろあるのに対応しています。さらに関数体同士の準同型写像があるという事は行き先の座標がもとの座標からわかるという事を意味していますから、それは対応する代数多様体の写像（正

確には幾つかの穴の部分を除いた部分で定義された写像）とみなすことができます。このようにして、係数体上有限生成な体の理論は、代数多様体の幾何学で解釈しなおす事ができます。ただし、体ばっかりを考えているぶんには、関数がどこに極を持つかという事が余り考えられていませんから、このようなやり方では、代数多様体を考えるといっても実は「その多様体から有限個の有理型関数の極を除いて穴を開けたような領域」のみを相手にしている事になります。そして、穴がどれだけ開いたかについては余り問題にしません。このような幾何学は「双有理幾何学」と呼ばれます。例えば $\mathbb{P}^2$ と $\mathbb{P}^1 \times \mathbb{P}^1$ とはこの幾何学では 「おなじ」にみえます。（もともと同じにみえる人もいるかもしれません。このふたつは実は $\mathbb{C}^2$ の二つの異なるコンパクト化で、要するに無限遠方の様子が違うのですが、双有理幾何では無限遠方なんてあってもなくてもいいのです。）随分乱暴な幾何学のようですが、実際には面白いことがいろいろあります。》

さて、双有理幾何学では、無限遠点があってもなくても同じとい言いましたが、それはあくまでも理論的には、という話であって、どうせ同じならばコンパクトなものを選んで扱うのが良いに決まっています。上で考えた《グラフ》Γ_F 自体は特異点を持つかもしれないし、コンパクトでもないのですが、実は特異点や無限遠点を適当に修正してやる事により、L を関数体として持つようなコンパクトリーマン面 $\mathcal{R}_L$ を作ることができます。$\mathcal{R}_L$ は L の非特異モデルと呼ばれます。（非特異モデルは高次元でも同様に存在します。これは広中の特異点解消理論の主張する所です。）

代数多様体の関数体同士の準同型写像に対応するのは一般には（像が稠密な）有理写像

$$(\text{代数多様体 I}) \setminus (\text{穴}) \to (\text{代数多様体 II})$$

なのですが、(代数多様体 I) が一次元で特異点を持たず、(代数多様体 II) には穴が開いていない（つまりコンパクトである）ならば、除去可能性の定理によって、(穴) の部分にこの写像が一意に延長されます。この事から、話を一次元に限れば、関数体の写像と、リーマン面同士の定値写像でない正則写像とが一対一に対応することがわかります。と

くに、体の恒等写像にこの議論を適用すると、同じ体を関数体に持つようなリーマン面は互いに同型であるという事になります。まとめると、一対一の対応

$$\text{リーマン面 } \mathcal{R} = \mathcal{R}_K \underset{\text{非特異モデルをとる}}{\overset{\text{関数体をとる}}{\longleftrightarrow}} \text{一変数代数関数体 } K = K(\mathcal{R})$$

があって、この対応のもとで、《準同型 $K \to L$ は 非定値正則写像$\pi : \mathcal{R}_L \to \mathcal{R}_K$ と対応する。》となります。《体の準同型は必ず単射である事》、《リーマン面同士の非定値正則写像は分岐を許した被覆に対応している事》にも注意しておきましょう。

この状況のもとでは、ガロア群 $\mathrm{Gal}(L/K)$ の元 σ というのは、

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & L \\ {\scriptstyle \text{包含写像}}\uparrow & & {\scriptstyle \text{包含写像}}\uparrow \\ K & = & K \end{array}$$

を可換にするような L の自己同型ですから、これは丁度図式

$$\begin{array}{ccc} \mathcal{R}_L & \longleftarrow & \mathcal{R}_L \\ {\scriptstyle \pi}\downarrow & & {\scriptstyle \pi}\downarrow \\ \mathcal{R}_K & = & \mathcal{R}_K \end{array}$$

を可換にするような $\mathcal{R}_L$ の自己同型（被覆変換）に対応します。被覆変換は局所化して考えることができます。つまり、$\mathcal{R}_K$ の開集合 U を任意にとったとき、任意の大域的な被覆変換 σ は、U に《制限》

$$\begin{array}{ccc} \pi^{-1}(U) & \longleftarrow & \pi^{-1}(U) \\ \downarrow & & \downarrow \\ U & = & U \end{array}$$

して局所的な被覆変換を考えることができるし、逆に局所的な被覆変換がうまく貼り合っておれば大域的な被覆変換を構成できるというわけです。次の節で形式的巾級数体のガロア群について述べますが、これはリーマン面の被覆変換の局所理論を述べていると考えることができます。また、その様に考えるほうが次の節の理解も容易になるでしょう。この節は多少舌足らずになってしまいましたが、ここの内容についてはリーマン面の教科書の多くに良い解説がありますし、自分で遊んでみることができるところですから、この辺で止めておきます。

4.2. **いろいろな拡大体のガロア群.** この節ではいろいろな拡大のガロア群についてまとめておくことにしましょう。

(1) 有限体の場合。

任意の有限体 k は素体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 上の有限次分離代数拡大です。k ガロア群 $\mathrm{Gal}(k/\mathbb{F}_p)$ の元のひとつに、フロベニウス写像 ϕ

$$\phi : x \mapsto x^p \quad (x \in k)$$

があります。実はガロア群はこのフロベニウス写像 ϕ で生成される巡回群です。

(2) 形式的ローラン巾級数体 $\mathbb{C}((t))$ の代数的閉包は、ピュイズー級数体 $\varinjlim_N \mathbb{C}((t^{1/N}))$ です。ガロア群 $\mathrm{Gal}(\varinjlim_N \mathbb{C}((t^{1/N}))/\mathbb{C}((t)))$ ($\mathbb{C}((t))$ の絶対ガロワ群) の元は、変数 t の巾根 $t^{1/N}$ の行き先で決まります。

$$t^{1/N} \mapsto \alpha_N t^{1/N} \quad ((\alpha_N)^N = 1, \quad (\alpha_{kN})^k = \alpha_N \quad (\forall k, N \in \mathbb{N})).$$

結局、$\mathbb{C}((t))$ の絶対ガロア群は、

$$\hat{\mathbb{Z}} = \varprojlim_N \mathbb{Z}/N\mathbb{Z}$$

と同型になります。

ここで一つ言葉の復習をしておきましょう。上に述べたことから、$\mathbb{C}((t))$ の任意の有限次拡大体は、

$$\mathbb{C}((t^{1/N}))$$

の形になります。この N を、分岐指数といいます。拡大 $\mathbb{C}((t^{1/N}))/\mathbb{C}((t))$ は幾何学的には、

$$\mathbb{C} \ni z \mapsto t = z^N \in \mathbb{C}$$

という写像の原点での挙動を見ていることになっており、N が原点での分岐の数を表していることに注意しましょう。

(3) $\mathbb{Q}$ 上の形式的ローラン巾級数体 $\mathbb{Q}((t))$ の代数的閉包は、$\mathbb{Q}$ の代数的閉包 $\bar{\mathbb{Q}}$ の上のピュイズー級数体 $\varinjlim_N \bar{\mathbb{Q}}((t^{1/N}))$ です。これと $\mathbb{Q}((t))$ との間には中間体 $\bar{\mathbb{Q}}((t))$ があります。(2) と全く

同様の理由により、

$$\mathrm{Gal}(\varinjlim_N \bar{\mathbb{Q}}((t^{1/N}))/\bar{\mathbb{Q}}((t))) \cong \hat{\mathbb{Z}}$$

となります。他方で

$$\mathrm{Gal}(\bar{\mathbb{Q}}((t))/\mathbb{Q}((t))) \cong \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}),$$

(左辺のガロア群の元の作用は巾級数の係数を対応する右辺のガロワ群の元で動かすことにより得られる) が成り立ちますから、結局

$$1 \to \hat{\mathbb{Z}} \to \mathrm{Gal}(\varinjlim_N \bar{\mathbb{Q}}((t^{1/N}))/\mathbb{Q}((t))) \,\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to\!\!\to 1$$

なる完全系列があって、$\mathbb{Q}((t))$ の絶対ガロア群は、$\{t^{1/N}\}$ の行き先を変化させる分の $\hat{\mathbb{Z}}$ と、係数をいじる分の $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ によって生成されることがわかります。中間体 $\bar{\mathbb{Q}}((t))$ は、$\mathbb{Q}((t))$ の係数体を変えただけで、パラメータ t の方は $\bar{\mathbb{Q}}((t))$ でも巾根を持ちません。このような拡大を不分岐な拡大と呼びます。$\bar{\mathbb{Q}}((t))$ は $\mathbb{Q}((t))$ の最大不分岐拡大です。

(4) $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ p-進数体 $\mathbb{Q}_p$ と巾級数体との類似性については既にお気付きになったことと思います。これらの体は完備離散付値体 ($\mathbb{Z}$ に値を持つ「位数」というものが定義されていて、それによって誘導されるノルムによって完備な距離空間の位相を持つような位相体) の二つの重要な例になっています。完備離散付値体 K については、次のことを知っておくことが重要でしょう。

- K の元で位数が非負のもの全体 $\mathfrak{O}_K$ は K の部分環をなす。K は $\mathfrak{O}_K$ の商体である。
- K の元でさらに位数が正のもの全体 $\mathfrak{M}_K$ は $\mathfrak{O}_K$ の極大イデアルになる。$\mathfrak{M}_K$ は $\mathfrak{O}_K$ の唯一の極大イデアルであって、体 $\mathfrak{O}_K/\mathfrak{M}_K$ は K の剰余体と呼ばれる。
- $\mathfrak{M}_K$ は $\mathfrak{O}_K$ の単項イデアルである。その生成元 π は $\mathfrak{O}_K$ の単数による掛け算の任意度を除いて一意で、K の素元と呼ばれる。

- K の任意の有限次代数拡大 L はまた完備離散付値体である。$\mathfrak{O}_L, \mathfrak{M}_L$ はそれぞれ $\mathfrak{O}_K, \mathfrak{M}_K$ を含んでいる。

これらの体の拡大体のガロア群についても類似性はあります。まず巾級数体の場合の、「係数体の拡大」にあたることが p-進数体の場合にどうなるか考えてみましょう。この場合には係数体というのは意味が無いですから、剰余体の方を考えることになります。(もちろん巾級数体のときには係数体と剰余体は同じものでした。) 完備離散付値体についての上の注意により、$\mathbb{Q}_p$ の任意の有限次代数拡大体 L に対して、その剰余体 $\mathfrak{O}_L/\mathfrak{M}_L$ は $\mathbb{Q}_p$ の剰余体 $\mathbb{F}_p$ を含むことがわかりますが、逆に、$\mathbb{F}_p$ の任意の有限次代数拡大体 $\mathfrak{l}$ に対して、それを剰余体に持つような $\mathbb{Q}_p$ の不分岐代数拡大体 $L_\mathfrak{l}$ が存在して、それは同型を除いて一意であることが知られています。かなり荒っぽい言い方をすると、$\mathbb{Q}_p$ は、形式的ローラン巾級数体 $\mathbb{F}_p((t))$ に、「繰り上がりの規則」を導入して演算を定義しなおしたものといえますが、その言い方に沿うなら、$L_\mathfrak{l}$ は $\mathfrak{l}((t))$ に適当な繰り上がりの規則を導入して演算を定義しなおしたものであるということもできるでしょう。ガロア群に関しても、巾級数体のときのアナログ

$$\mathrm{Gal}(L_\mathfrak{l}/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathfrak{l}/\mathbb{F}_p),$$

が成り立ちます。極限をとって、次の結論が出ます。

$\mathbb{Q}_p^{\mathrm{ur}}$

$\mathbb{Q}_p$ の最大不分岐拡大 $\mathbb{Q}_p^{\mathrm{ur}}$ が存在する。拡大 $\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p$ のガロア群の元を剰余体に落とすことにより得られる自然な写像

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \to \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)(\cong \hat{\mathbb{Z}}) \tag{4.1}$$

は同型である。特に、$\mathbb{Q}_p^{\mathrm{ur}}$ は $\mathbb{Q}_p$ のアーベル拡大である。

$\mathbb{Q}_p^{\mathrm{ur}}$ の構造については、もっと詳しくわかっていて、

$$\mathbb{Q}_p^{\mathrm{ur}} = \bigcup_{(N,p)=1} \mathbb{Q}_p(\zeta_N)$$

であることが知られています。なお、(4.1) で右辺の位相的生成元がフロベニウス写像で与えられたことも思い出しておきま

しょう。これに対応する左辺のガロア群の元もフロベニウス写像と呼ばれます。

さて、$\mathbb{Q}_p$ 上の最大アーベル拡大について調べる番です。結果から言うと次のようになります。

$\mathbb{Q}_p^{\mathrm{ab}}$

$$\mathbb{Q}_p^{\mathrm{ab}} = \bigcup_k \mathbb{Q}_p(\zeta_k) = \bigcup_n \mathbb{Q}_p^{\mathrm{ur}}(\zeta_{p^n}).$$

この結果は、もちろん、$\mathbb{Q}$ 上の最大アーベル拡大が $\mathbb{Q}$ に 1 の巾根を付け加えることにより得られたことと関連しています。等式

$$x^{p^n} - 1 \equiv (x-1)^{p^n} \pmod{p}$$

により、$x^{p^n} - 1 = 0$ は $\mathbb{F}_p$ で p^n-重根 1 を持ち、ζ_{p^n} を加えることが剰余体の拡大に寄与しないことに注意しておきましょう。

さて、ガロア群 $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ はどういう構造になっているでしょうか？それについては次の小節で改めて考えてみましょう。

4.3. **局所アルティン写像の定義.** 前の小節で復習した所によれば、$\mathbb{Q}_p$ の最大アーベル拡大 $\mathbb{Q}_p^{\mathrm{ab}}$ の中には $\mathbb{Q}_p$ の最大不分岐拡大 $\mathbb{Q}_p^{\mathrm{ur}}$ が含まれていて、

$$\mathbb{Q}_p^{\mathrm{ur}} = \bigcup_{(N,p)=1} \mathbb{Q}_p(\zeta_N), \tag{4.2}$$

$$\mathbb{Q}_p^{\mathrm{ab}} = \bigcup_k \mathbb{Q}_p(\zeta_k) = \bigcup_n \mathbb{Q}_p^{\mathrm{ur}}(\zeta_{p^n}). \tag{4.3}$$

であるということでした。ガロア群については、

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$$

が成り立ち、これらの群の位相的生成元としてフロベニウス写像が取れることも述べました。次に ガロア群 $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{ur}})$ について調べてみましょう。(4.3) を見ますと、このガロワ群の元を与えるには ζ_{p^n} 達の行き先を指定すれば良いことがわかります。これらはもちろん互いに両立するように決めなければなりませんから、少し考えるとわかるように、

$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{ur}})$ の元 σ に対して、ある $\mathbb{Z}_p^\times$ の元 $\alpha = a_0 + a_1 p + a_2 p^2 + \ldots$ が存在して、σ の ζ_{p^m} への作用は、

$$\zeta_{p^m}^{\sigma} = \zeta_{p^m}^{\alpha}(\zeta_{p^m} \text{ の } \alpha \text{ 乗}) = \zeta_{p^m}^{a_0 + a_1 p + \ldots a_{m-1} p^{m-1}} \tag{4.4}$$

により定まるということがわかります。つまり、(4.4) から決まる対応により同型

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{ur}}) \cong \mathbb{Z}_p^\times$$

が与えられることがわかります。

さて、$\mathbb{Q}_p^{\mathrm{ab}}$ は、$\mathbb{Q}_p^{\mathrm{ur}}$ と、$\mathbb{Q}_p$ に 1 の p-巾乗根をすべて付け加えた体との合成ですから、$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ は、二つの群 $(\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{ur}})$ と $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p))$ の直和になります。結局、このガロア群の構造は

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \cong \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times$$

と書けることになります。ところで、この式と、

$$\mathbb{Z} \times \mathbb{Z}_p^\times \ni (k, x) \mapsto (p^k x) \in \mathbb{Q}_p^\times$$

により定まる同型

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$$

とを見比べてみると、興味深いことがわかります。$\mathbb{Q}_p^\times$ は $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ にすっぽり dense に入るのです。

$$\mathbb{Q}_p^\times \hookrightarrow \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$$

この写像を、アルティン写像 (あるいは resiprocity map) といいます。今紹介した定義では一見偶然的にみえますが、実はこの写像は自然に定義されるもので、類体論において基本的な役割を果たします。

4.4. **大域的アルティン写像の定義.** 前節で各素数毎に定義されたアルティン写像をつなげて $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ の表現を得ることを考えてみましょう。p-進展開によって $\mathbb{Q}$ が $\mathbb{Q}_p$ の部分体と考えられたのと同様の理由によって、$\mathbb{Q}$ の任意の有限次アーベル拡大は $\mathbb{Q}_p^{\mathrm{ab}}$ の幾つかの直和の部分体と考えることができます。これによって制限による自然な写像

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$$

を得ることができますから、局所アルティン写像とこの写像とをつなげることにより、

$$\mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$$

なる写像があります。今考えているガロア群等はすべて可換ですから、いろんな p に関して定義される上の写像をすべてまとめて、

$$\prod_p{}' \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$$

なる連続準同型写像が定義されます。(トポロジカルな議論が少し必要ですが、ここでは余りうるさく言わないでおきましょう。) イデール群の定義には $\mathbb{Q}_p^\times$ の制限直積にさらに $\mathbb{R}^\times$ を掛けておく必要がありました。$\mathbb{R}_+$ の元はすべてガロア群の単位元に写像されることにすると、これで待望の

$$\mathbb{Q}_A^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$$

が定義できました。($\mathbb{R}$ の -1 はどうなったんだという声が出そうです。これはイデール群の元 $(-1,-1,\ldots,-1)$ が上の写像で単位元に写るように定義されます。具体的には $\mathbb{R}$ の -1 に対応するのは「複素共役をとる」という元です。) この写像を大域的アルティン写像といいます。まずやるべきことはこの写像の核と余核を調べることです。実は次の完全系列があります。

$$1 \to \overline{\mathbb{Q}^\times \mathbb{R}_+^\times} \to \mathbb{Q}_A^\times \overset{\text{Artin map}}{\to} \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \to 1$$

つまり、アルティン写像は全射であって、その核は $\mathbb{Q}^\times \mathbb{R}_+^\times$ の閉包に等しいということが知られています。アルティン写像が全射であるというのも非常に大切ですが、その核に $\mathbb{Q}^\times$ が入っているということは、まったくもって自明でない事実で、この一つを見てもアルティン写像というものが決して人工的なものではないということがわかると思います。

4.5. **イデール群とイデアル (類) 群との関係.** ここで少しだけイデール群とイデアル類群との関係について述べておきましょう。イデール群の各元に対して、イデアル (分数イデアル) を次のように対応させるこ

とができます。

$$\mathbb{Q}_A^\times \ni a = (a_l, a_\infty) \mapsto (\prod_l |a_l|^{-1})\mathbb{Z} \tag{4.5}$$

言い換えれば、$\mathbb{Q}_A^\times$ の元 $(1, \ldots, p, \ldots, 1)$ に対して、$\mathbb{Z}$ の素イデアル $p\mathbb{Z}$ を対応させる写像を群準同型に拡張することができます。(リーマン面の理論をご存じの方なら、この群準同型がリーマン面 R のディバイザーからラインバンドルを与える写像

$$\mathrm{Div}_R \ni \sum_P a_P \mapsto \mathcal{O}_R(\sum_P a_P) \in \mathrm{Pic}_R$$

と良く似ていることに気がつかれると思います。) 準同型 (4.5) の存在により、イデアル群はイデール群の構造を反映することになります。アルティン写像の核が $\mathbb{Q}^\times$ を含むことから、類体論においてはイデアル群を $\mathbb{Q}^\times$ で割った群 (イデアル類群) が重要な役割を果たします。実際にイデアル類群によって類体論を進めたのが高木式類体論で、これは有限次のアーベル拡大には有効です。イデール群で話を進めるメリットは、無限次代数拡大まで扱えることで、実際にそこまでいって始めてアルティン写像のようなきれいな写像が自然にみえてくるのです。有限次ではかえってこういう構造が明らかにならずに、ガロア群の生成元を指定するようなことをせねばならなくなったりして、かえって面倒になります。

5. 剰余類型の分解法則の証明

前節で、アルティン写像が定義され、それが全射であって、その核が $\overline{\mathbb{Q}^\times \mathbb{R}_+}$ であることが示されました。この節では、その応用として、一番始めに述べた剰余型の分解法則を証明してみましょう。講義では、この証明はなく、代わりにフィボナッチ数列の宿題の方が解かれましたが、このノートではやはり宿題は残しておいて、こっちの証明の方をやってみようという訳です。この証明について考えるのは、アルティン写像を理解する上で非常によい問題になりますから、腕試しをしたい方はこの節を飛ばして自分で考えてみることをおすすめします。もっとも、この節ではこれまで以上に説明が雑になってしまうので、結局自分で考えていただくことになるかもしれません。

さて、$\mathbb{Z}$ 上の既約でモニックな多項式 f について、体 K を $K = \mathbb{Q}(X)/(f(X))$ で定義します。ここで証明したいことは、拡大 $K/\mathbb{Q}$ がアーベルであるならば、f について剰余類型の分解法則が成り立つということです。まずこのことを今のアルティン写像の言葉で書き換えてやる必要があります。(既に述べたようにリーマン面の分岐被覆の話 (関数体の拡大の話) と数体の拡大の話の間に著しい類似性があります。以下の話でもこのアナロジーを思い浮かべながらやると楽になる所が少しあります。$\mathbb{Q}$ の代わりに一変数有理関数体 (つまりリーマン球面の関数体)　$\mathbb{Q}(Y)$、K の代わりにリーマン球面上の分岐したアーベル被覆面の関数体 $\mathbb{Q}(X,Y)/(F(X,Y))$ を考えるのが良いでしょう。) 始めにすべきことは、拡大 $K/\mathbb{Q}$ を、局所的に (つまり各素数ごとに) 見てやることです。$\mathbb{Q}$ の各々の素数 p に対して、その上に乗っている K の素元 π が有限個あります。K の π による完備化 K_π は、$\mathbb{Q}_p$ のアーベル拡大であって、これは前の節で復習しましたように、分岐するか、しないかが問題になります。この判定には、関数体のときと同様に f の微分を考えるのが便利です。分岐しているのは f の根の一つを α として、

$$f'(\alpha) \equiv 0 \pmod{\pi}$$

のとき、あるいは同じことですが、

$$(f'(\alpha) \text{ のノルム}) \stackrel{\text{def}}{=} (f'(\alpha) \text{ の } \mathbb{Q}\text{-上のすべての共役の積}) \equiv 0 \pmod{p}$$

のときであることがわかります。この事から、分岐の起こるような p は有限個であることがわかります。(これらの p は一般に剰余類型の分解法則に現れる「有限個の例外」になります。)

そこで、$K_\pi/\mathbb{Q}$ が不分岐であるような p について考えてみますと、f が $\mathrm{mod}p$ で解を持つことと、《K_π の剰余体が $\mathbb{Q}_p$ の剰余体 $\mathbb{F}_p$ と等しい》ことが同値になる事がわかります。このことは、《K_π の剰余体の上でフロベニウス写像がトリビアルである》ということと同値で、さらにこれは、同型 (4.1) によって、《K_π のフロベニウス写像 ϕ_p がトリビアルである》ということと同値になります。アルティン写像の定義を逆にたどると、ϕ_p は $(1,\ldots,1,p,1,\ldots,1)$ ($\mathbb{Q}_p$ のところの成分のみ

が p) のアルティン写像による像によって引き起こされるということになります。従って問題は、

$$\rho_K : \mathbb{Q}_A^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$$
$$(\text{アルティン写像とガロア群の制限との合成})$$

なる写像の核に $(1,\ldots,1,p,1,\ldots,1)$ が入るのはいつか？ある数に関する p の剰余類で判定できるのか？

ということに帰着されることがわかります。既にこれは学部生程度の位相群論の演習問題ですが、念のためにやってみましょう。まず、直積 $\prod_p \mathbb{Z}_p^\times$ からイデール群への包含写像から決まる写像

$$\prod_p \mathbb{Z}_p^\times \to \mathbb{Q}_A^\times / \overline{\mathbb{Q}^\times \mathbb{R}_+^\times}$$

は全射であることに注意します。イデール群の元というのは有限個 $\mathbb{Z}_p$ からはみ出す成分を持っていますが、それらはみな $\mathbb{Q}^\times$ の元を掛けることによりはみ出さないようにできるということです。ρ_K の核は $\overline{\mathbb{Q}^\times \mathbb{R}_+^\times}$ を含みましたから、ρ_K を $\prod_q \mathbb{Z}_q^\times$ に制限したものも全射であるということになります。

元 $(1,\ldots,1,p,1,\ldots,1)$ は、$\prod_q \mathbb{Z}_q^\times$ には入りませんが、

$$p \times (1,\ldots,1,p,1,\ldots,1)^{-1} = (p,\ldots,p,1,p,\ldots,p)$$

は入ります。この元が ρ_K の核 N に入るか否かが f が $\mathrm{mod}p$ で解を持つかどうかと同値なわけです。ρ_K は連続で、行き先は離散群ですから、N は $\prod_q \mathbb{Z}_q^\times$ の開部分群になります。直積位相の定義により、有限個の素数の集合 S とある大きな整数 M があって、

$$N \supset \prod_{q\in S} \left(1 + q^M \mathbb{Z}_q\right) \times \prod_{q \notin S} \mathbb{Z}_q^\times$$

が成り立つことになります。剰余群

$$\left(\prod_q \mathbb{Z}_q\right) \Big/ \left(\prod_{q\in S} \left(1 + q^M \mathbb{Z}_q\right) \times \prod_{q \notin S} \mathbb{Z}_q^\times\right)$$

は既に有限群で、その代表系として $\mathbb{Z}$ の元ばかりをとってくることができます。とくに、この群に N を射影した群 $\tilde{N}$ の元をすべて並べて $\mathbb{Z}$ に代表元を選んだものを、

$$a_1, \ldots, a_m$$

とすれば、p が S の元でないとき、

$$(p, \ldots, p, 1, p, \ldots, p) \in N \Leftrightarrow \exists i \text{ があって、} p \equiv a_i \pmod{\prod_{q \in S} q^M}$$

これで証明が終わりました。

6. 虚数乗法論の素朴な解説

虚数乗法論 (complex multiplication law,CM) は、おそらくガウスがレムニスケート

$$r^2 = \cos(2\theta) \quad ((r, \theta):\text{極座標})$$

の n 等分方程式を、円分方程式 (=円を n 等分する方程式) のアナログとして考えたことから始まります。(ガウスは主に $n = 5$ の時について調べました。) レムニスケートの弧長を r で表現してみると、

$$u = \int_0^r \sqrt{(\frac{dx}{dr})^2 + (\frac{dy}{dr})^2}\ dr = \int_0^r \frac{dr}{\sqrt{1 - r^4}}$$

と、楕円積分で書かれるのがわかります。円の場合には、弧長によって逆に座標を書き下すと三角関数という美しい解析関数を得ることができました。今の場合にも、上の楕円積分の逆関数をとって、r を u の関数とみなすことが有効です。この関数は普通

$$r = \mathrm{sn}(u; \sqrt{-1})$$

と書かれます。この関数を用いると、レムニスケートの 5 等分問題は、方程式

$$\mathrm{sn}(5u; \sqrt{-1}) = 0$$

を解くのと同値になります。この方程式は超越的に見えますが、三角関数の場合と同様に楕円関数にも加法公式があって、$\mathrm{sn}(5u; \sqrt{-1})$ は

$\mathrm{sn}(u;\sqrt{-1})$ の有理式で表現できます。具体的には、$x=\mathrm{sn}(u;\sqrt{-1})$ と書くと、

$$\mathrm{sn}(5u;\sqrt{-1})=\frac{x^{25}+50x^{21}-125x^{17}+300x^{13}-105x^9-62x^5+5x}{1+50x^4-125x^8+300x^{12}-105x^{16}-62x^{20}+5x^{24}}$$

となります。[2] 結局、レムニスケートの 5 等分問題というのは、この有理式が 0 という方程式を解くことに帰着されます。これは、分子が 0 ということということと同じですから、我々は 25 次方程式を解くことになります。この方程式には、期待通りの 5 個の実根のほかに、20 個の虚数根を持ちます。この虚数根をどう考えるべきか、ということがガウスが関数論をやるきっかけになったようです。先走って現代的な言葉で言ってしまうと、これは実は複素トーラス $\mathbb{C}/\mathbb{Z}[\sqrt{-1}]$ の位数 5 の元 (それは丁度２５個ある) を求めているのであって、その中で、「実」のものが 5 個あるということになります。

さて、アーベルは、ガウスの考察よりも一般的な、

$$u=\int_0^r\frac{dr}{\sqrt{1-r^2}\sqrt{1-k^2r^2}}$$

の形の楕円積分を考えました。(ガウスの考えたのは $k=\sqrt{-1}$ の場合にあたります。) この場合にも、n-等分問題、すなわち上の楕円積分の逆関数を $f(u)=r$ と書いた時に、$f(u)$ を用いて $f(nu)=0$ を解くという問題を考えることができます。以後 n が奇数であるとして話を進めましょう。f にもやはり加法公式があって、

$$f(nu)=\frac{xS(x^2)}{T(x^2)}\quad(x=f(u),\ \ S,T\ \text{は}\ \frac{n^2-1}{2}\ \text{次の多項式})$$

と、この場合にも $f(nu)$ は $f(u)$ の有理式で書けることを示すことができます。問題は、$S(X)=0$ という方程式が解けるかということですが、アーベルは次のことを見抜きました。

(1) $S(X)$ は $\mathbb{Q}(k)$ 上既約な多項式である。$\mathbb{Q}(k)$ 上の S の最少分解体を K とおくと、K と $\mathbb{Q}(k)$ のあいだの特別な中間体 F

$$K\supset F\supset\mathbb{Q}(k),\quad [K:F]=\frac{n-1}{2},[F:\mathbb{Q}(k)]=n+1$$

が存在する。

[2] ここの「分母が昇巾で、分子が降巾」という書き方は、変かもしれませんが、校正者の意見を採用して、係数の対称性がよく見えるように敢えてこうしてみました。

(2) K/F はアーベル拡大である。
(3) 一般の k では、 $F/\mathbb{Q}(k)$ は可解ではないであろう。
(4) $\tau :=$ ($\mathrm{sn}(u;k)$ の周期の比) が虚二次体に入る時には、$F/\mathbb{Q}(k)$ が可解になる。

最後の τ に関する条件は、τ が、

$$a\tau^2 + b\tau + c = 0 \quad (a, b, c \in \mathbb{Z}, b^2 - 4ac < 0)$$

の形の二次方程式を満たすということと同値です。これが CM 理論の始まりであって、結論からいえば、$F/\mathbb{Q}(k)$ は、周期 τ の楕円曲線が CM を持つ時のみ可解になることがいえます。

こういう訳で、楕円の等分点と数論とは面白い結び付きを持っています。これより少しあとの、有名な Kronecker 青春の夢というのは、

Kronecker 青春の夢

$k = \mathbb{Q}(\sqrt{-m}), m \in \mathbb{Z}, m > 0$ 上の最大アーベル拡大は、k に、j-function と $\wp$-function (w.r.t. lattice $\mathbb{Z} + \mathbb{Z}\sqrt{-m}$) の special value を付け加えて得られる。

を主張するものですが、ここで言う “special value” というのは実際には楕円の等分点における値で、この問題もやはり楕円の等分点と数論との接点に現れた問題であるといえるでしょう。これから説明しようとする志村の相互律も、まさにこのような接点に視点を置くものと考える事ができます。但し今度は一個の楕円曲線について考えるのではなく、上半平面をパラメータ空間とする楕円曲線の普遍族について考えるのがポイントになります。それに呼応して等分点は上半平面から普遍曲線へのセクション、等分点での “special value” は上半平面上の関数とみなす事になります。この関数が実は保形函数になっていて、保形函数が楕円曲線の理論と関係付けられるという事が以下の話の内容です。話を進める前にまず少し楕円曲線のおさらいをしておきましょう。楕円曲線 (elliptic curve) というのは種数 (genus) が 1 のコンパクトリーマン面 $\mathcal{R}$ のことでした。$\mathcal{R}$ の関数体を $F(\mathcal{R})$ と書きますと、

$$F(\mathcal{R}) = \mathbb{C}(X, Y), \quad Y^2 = 4X^3 - g_2X - g_3 \quad (g_2, g_3 \in \mathbb{C}, g_2^3 - 27g_3^2 \neq 0)$$

と具体的に表現できました。さらに、このとき

$$J(\mathcal{R}) = 2^6 3^3 \frac{g_2^3}{g_2^3 - 27g_3^2}$$

は $\mathcal{R}$ によって一意に決まる (関数体の生成元 X, Y の選びかたによらない) 数で、つまり $\mathcal{R}$ の不変量となります。

次の事実は重要です。

- $J(\mathcal{R}_1) = J(\mathcal{R}_2) \Leftrightarrow \mathcal{R}_1 \cong \mathcal{R}_2 \Leftrightarrow F(\mathcal{R}_1) \cong F(\mathcal{R}_2)$.
- $\forall c \in \mathbb{C} \quad \exists \mathcal{R}; J(\mathcal{R}) = c$.

つまり、J という関数は楕円曲線を分類できる、$\{J \in \mathbb{C}\}$ は楕円曲線のモデュライ空間であるといえます。

他方、楕円曲線は次のように周期を用いて複素トーラスとして表現することもできます。

$$\mathcal{R} \cong \mathbb{C}/L, \exists L : \text{lattice} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \quad \tau := \omega_2/\omega_1 \in \mathfrak{H} = \{\tau | \Im\tau > 0\}$$

このように表現したとき、τ はホモトピー群の生成元を決めた $\mathcal{R}$ のモデュライ空間 (タイヒミュラー空間) の座標を与えている ($\mathfrak{H}$ が丁度タイヒミュラー空間と同型である) ことも良く知られています。

このように周期で書かれた複素トーラスの関数体はワイエルシュトラスの $\wp$-関数によって具体的に書き下すことができます。

$$\begin{aligned}
&\wp(z; \omega_1, \omega_2) = \wp(z; L) \\
&\quad = \frac{1}{z^2} + \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \left(\frac{1}{(z - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right), \\
&F(\mathbb{C}/L) = \mathbb{C}(\wp(z; L), \wp'(z; L))
\end{aligned}$$

さて、L としてイデアルを持ってきたらどうなるでしょうか。この問題を考えるために、いよいよ表題の虚数乗法を導入しましょう。

Definition 6.1.

$\mathbb{C}/L$ が虚数乗法を持つ

$\Leftrightarrow \exists \lambda \in \mathbb{C} \setminus \mathbb{R}$ で、$\lambda L \subset L$ を満たすものが存在する。

$$\Leftrightarrow \begin{bmatrix} \lambda\omega_1 \\ \lambda\omega_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} \quad (\exists \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}))$$

この時、λ, τ は、共に二次の代数的数になります。じっさい、

$$\tau = \frac{\lambda\omega_2}{\lambda\omega_1} = \frac{c\omega_1 + d\omega_2}{a\omega_1 + b\omega_2} = \frac{c + d\tau}{a + b\tau}$$

ですから、τ は次の方程式を満たします。

$$b\tau^2 + (a-d)\tau - c = 0, \quad a, b, c, d \in \mathbb{Z}, \Im\tau > 0, \tau \in \mathbb{C}/\mathbb{R}$$

そこで、先程述べたように、$\mathbb{Q}(\tau)$ は虚二次体になります。ところで、

$$\lambda = a + b\tau = \frac{1}{\tau}c + d$$

という関係式から、$\mathbb{Q}(\lambda) = \mathbb{Q}(\tau)$ でもあります。つまり、楕円関数から虚二次体 $\mathbb{Q}(\tau)$ を得るためには、上のような λ をとって来てそれを $\mathbb{Q}$ に付け加えればよいということになります。じつは、任意の虚二次体はこのように書けます。ちょっとやってみましょう。虚二次体 $k = \mathbb{Q}(\tau)$ に対し、その整数環を $\mathfrak{O}_k$ とし、さらにそのイデアルを、$\mathfrak{A} = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$ とあらわすと、$\mathfrak{O}_k$ による掛け算によって $\mathfrak{A}$ が不変であるということから、

$$\tau.\mathfrak{A} \subset \mathfrak{A}$$

となって、$\mathbb{C}/\mathfrak{A}$ は CM 型の楕円曲線になることがわかります。τ は、上でいう所の λ の役割を果たしていますから、$\mathbb{C}/\mathfrak{A}$ に上の意味で対応する虚二次体は期待通り $\mathbb{Q}(\tau)$ になっています。まとめると、次のような全射対応があります。

(虚二次体 k とそのイデアル $\mathfrak{A}$) $\mapsto$ CM を持つ楕円曲線 $\mathbb{C}/\mathfrak{A}$

ところで、この対応で同型な楕円曲線に対応するための $k, \mathfrak{A}$ の条件は何でしょうか。先程述べたように、体 $\mathbb{Q}(\tau)$ は、楕円曲線から一意に定まってしまいますから、問題はイデアル $\mathfrak{A}$ を変えたときにどうなるかです。これについては、

$$\begin{aligned}
&\mathbb{C}/\mathfrak{A}_1 \cong \mathbb{C}/\mathfrak{A}_2 \\
\Leftrightarrow &\exists\lambda \in k^\times, \quad \mathfrak{A}_1 = \lambda\mathfrak{A}_2 \\
(\overset{\text{Def}}{\Leftrightarrow} &\mathfrak{A}_1 \text{ と } \mathfrak{A}_2 \text{ は同じイデアル類に属する。}) \\
\Leftrightarrow &J(\alpha_2^{(1)}/\alpha_1^{(1)}) = J(\alpha_2^{(2)}/\alpha_1^{(2)})
\end{aligned}$$

ということになります。ここで、イデアル類という言葉が出て来ました。これについてもう少し詳しく話してみましょう。イデアルの全体 I は可換群をなし、その中で、単項イデアル全体を集めたもの P は部分群をなします。そこで、商群

$$I/P$$

を考えることができますが、これは有限群になることが知られています。この群をイデアル類群、その位数を類数と呼びます。

虚二次体 k に対して、それに付随する楕円曲線が、有限個定まることになります

$$\mathbb{C}/\mathfrak{A}_1, \mathbb{C}/\mathfrak{A}_2, \ldots, \mathbb{C}/\mathfrak{A}_h$$

元の虚二次体 k に、これらの楕円曲線の J 関数を加えたもの

$$k(J(\mathbb{C}/\mathfrak{A}_1)), k(J(\mathbb{C}/\mathfrak{A}_2)), \ldots, k(J(\mathbb{C}/\mathfrak{A}_h))$$

はすべて等しくなることが知られています。これが k 上のヒルベルト類体と呼ばれるものです。

ここで、$\mathrm{SL}_2(\mathbb{Z})$ に話をつなげましょう。

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}); \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

をレベル N の主合同群とするとき、上半平面 $\mathfrak{H} = \{\tau \in \mathbb{C}; \Im\tau > 0\}$ 上の関数 f がレベル N のモデュラー関数であるというのは、f が、

(1) f は $\mathfrak{H}$ 上の正則関数である。

(2)

$$f(\frac{a\tau + b}{c\tau + d}) = f(\tau) \quad (\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N))$$

(3) f は尖点 (cusp) で 高々極しか持たない。

という三つの条件を満たすことをいうのでした。これは要するに、《リーマン面 $\mathfrak{H}/\Gamma(N)$ の上の正則関数で、$\mathfrak{H}/\Gamma$ のコンパクト化まで有理型関数に伸びるもの》を、$\mathfrak{H}$ に引き戻したものです。レベル N のモデュラー関数全体のなす環の商体を $\mathcal{F}_N$ と書きましょう。$\mathcal{F}_N$ は $\mathfrak{H}/\Gamma(N)$ の関数体と同型です。

$$\mathcal{F}_N \cong F(\mathfrak{H}/\Gamma(N))$$

さらに、

$$\mathcal{F}_\infty = \bigcup_{N\geq 0} \mathcal{F}_N$$

と書きましょう。志村の相互律は、拡大 $\mathcal{F}_\infty/\mathbb{C}$ のガロア群、つまり体 $\mathcal{F}_\infty$ の $\mathbb{C}$ 上の自己同型を記述するもので、具体的には次の完全系列の存在を主張します。

$$1 \to \mathrm{GL}_2^+(\mathbb{R}) \to \mathrm{GL}_2(\mathbb{Q}_A) \to \mathrm{Gal}(\mathcal{F}_\infty/\mathbb{C}) \to 1$$

ここで GL_2 のアデール値点のなす群 $\mathrm{GL}_2(\mathbb{Q}_A)$ というのが出て来ました。これは、

(1) アデールを成分に持つ行列のなす環

$$M_2(\mathbb{Q}_A) = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix}; x, y, z, w \in \mathbb{Q}_A \right\}$$

の中の可逆な元のなす群、と思ってもいいし、

(2) 適当な意味の制限直積

$$\prod{}' \mathrm{GL}_2(\mathbb{Q}_p) \times \mathrm{GL}_2(\mathbb{R})$$

と思ってもかまいません。

不安な読者は適当な文献を参考にしながらこの二つの定義を確認していただきたい。

実はもうひとつこの完全系列について断っておく必要があって、それは $\mathcal{F}_\infty$ が上の定義では $\mathbb{C}$-係数であるけれども、実際には係数を $\mathbb{Q}$ まで還元して、その $\mathbb{Q}$ 上のガロア群を考えないと上の完全系列が成り立たないということです。この係数の還元のためにはもちろん $\mathcal{F}_\infty$ の元のうちどれが有理係数であるか述べないといけない訳ですが、これについてはここでは省略することにします。なぜそうする必要があるかについてはあとで少し述べましょう。

さて、この講義では相互律の写像

$$\mathrm{GL}_2(\mathbb{Q}_A) \to \mathrm{Gal}(\mathcal{F}_\infty/\mathbb{C})$$

をどう定義するかのあらましを述べることにして、残りは読者の研究に任せることにしましょう。まず次の小節で $\mathcal{F}_\infty$ がどういう元で生成されているかを調べることにします。

6.1. $\mathcal{F}_\infty$ **の生成元.** まずわかっていることは、リーマン面

$$\mathfrak{H}/\Gamma(1) = \mathfrak{H}/\operatorname{SL}_2(\mathbb{Z})$$

は $\mathbb{C}$ と同型であって、その座標関数として J が取れるということです。従って、

$$\mathcal{F}_1 = \mathbb{C}(J).$$

一般の $\mathcal{F}_N$ の生成元を考えるためには、$\mathfrak{H}/\Gamma(N)$ を次のような対応によって《原点 O を指定された楕円曲線 T と、その N-等分点 $\{P_{m,n}; m, n \in \mathbb{Z}/N\mathbb{Z}\}$ のモデュライ空間》として理解するのが便利です。

$$\mathfrak{H}/\Gamma(N) \ni \tau \mapsto \left(T = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau, \quad O = 0, \quad P_{m,n} = \frac{m + n\tau}{N} \quad (m, n \in \mathbb{Z}/N\mathbb{Z})\right)$$

$\mathcal{F}_N$ の元を与えることは、データ $(T, O, \{P_{m,n}\})$ を分類するための不変量を与えることにほかなりません。既に J が $\mathcal{F}_1$ の元であることがわかっていて、J によって楕円曲線 T の同型類 が決まってしまいますから、$\mathcal{F}_N$ の $\mathcal{F}_1$ 上の体としての生成元を考えるには、楕円曲線の N-等分点をどのように指定すれば良いかを考えれば良いことになります。点を指定するには座標を用いるのが簡明ですが、平坦な座標 z は $\mathbb{Z} + \mathbb{Z}\tau$ の分だけの不定性が残るので具合が良くありません。そこで、ワイエルシュトラスの $\wp$-関数を用いることにしましょう。各 $m, n \in \mathbb{Z}/N\mathbb{Z}$ に対して、$\mathfrak{H}$ 上の関数

$$\wp\left(\frac{m + n\tau}{N}; \tau\right), \quad \wp'\left(\frac{m + n\tau}{N}; \tau\right) \tag{6.1}$$

を考えようという訳です。気を付けておかなければならないことは、ワイエルシュトラスの $\wp$-関数は与えられたデータからでは一意に決まらないということです。$\wp$-関数は次のような性質で特徴づけられていました。

- $\wp$ は O 以外で正則である。
- $\wp$ は 平坦な座標 z で書いた時に O での挙動が、

  $$z^{-2} + O(z)$$

  と書かれる。

二番目の条件は平坦な座標の取り方 (それには定数倍の違いがある。) によって定数倍だけ変わってきます。従って、$\Gamma(N)$ の元によって τ を

動かすと、一般には (6.1) の関数はおのおの定数倍だけ変わってくることがわかります。言い換えれば、これらの関数はモデュラー形式であるということになります。モデュラー形式ではなくてモデュラー関数を得るためには、これらの形式の比をとればよろしい。すなわち、

$$\frac{\wp(\frac{m+n\tau}{N};\tau)}{\wp(\frac{m'+n'\tau}{N};\tau)},\quad \frac{\wp'(\frac{m+n\tau}{N};\tau)}{\wp'(\frac{m'+n'\tau}{N};\tau)},\quad \frac{(\wp'(\frac{m+n\tau}{N};\tau))^2}{(\wp(\frac{m'+n'\tau}{N};\tau))^3} \tag{6.2}$$

等が、$\mathcal{F}_N$ の元であることがわかります。今までの説明から実はこれらによって $\mathcal{F}_N$ は体として $\mathcal{F}_1$ 上生成されることも納得できるでしょう。

6.2. **相互律の写像の作り方.** 拡大 $\mathcal{F}_\infty/\mathbb{Q}$ のガロア群がどうなるか考えてみましょう。この場合も中間体 $\mathcal{F}_1$ をはさんで考えることが有効です。

$$\mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F}_1) \to \mathrm{Gal}(\mathcal{F}_\infty/\mathbb{C}) \to \mathrm{Gal}(\mathcal{F}_1/\mathbb{C}).$$

そこで問題は $\mathrm{Gal}(\mathcal{F}_1/\mathbb{C})$ と $\mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F}_1)$ の二つのガロア群を求めることです。順々にやってみましょう。

[1] ガロア群 $\mathrm{Gal}(\mathcal{F}_1/\mathbb{C})$。$\mathcal{F}_1$ は $\mathbb{C}$ 上の一変数有理関数体と同型でした。

$$\mathcal{F}_1 = \mathbb{C}(J).$$

この事から、$\mathcal{F}_1$ の $\mathbb{C}$ 上のガロア群は $\mathbb{P}^1(\mathbb{C})$ の自己同型群と同型であって、

$$\mathrm{Gal}(\mathcal{F}_1/\mathbb{C}) \cong \mathrm{PSL}_2(\mathbb{C})$$

であることがわかります。実はここで先に述べた係数の有理数への還元が問題になるのであって、相互律の写像を全射にするには $\mathbb{C}(J)$ の代わりに $\mathbb{Q}(J)$ をとる必要があります。こうしておけばガロア群は

$$\mathrm{Gal}(\mathbb{Q}(J)/\mathbb{Q}) \cong \mathrm{PSL}_2(\mathbb{Q})$$

という具合になります。

[2] ガロア群 $\mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F}_1)$。$\mathcal{F}_N$ は $\mathcal{F}_1$ の上に楕円曲線の N-等分点のデータを与える関数を付け加えて得られるのでした。従って、拡大 $\mathcal{F}_N/\mathcal{F}_1$ のガロア群の元は、N-等分点を置換することに対応していることがわかります。ただし、置換された後の点におけるワイエルシュトラスの $\wp$-関数がもとの関数関係を満たすためには、その置換が N-等分点のなす群の準同型であることが必要になります。楕円曲線の N-等

分点の全体のなす群は $((1/N)\mathbb{Z}/\mathbb{Z})^2$ と同型ですから、次の同型があります。

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong \mathrm{Aut}((\frac{1}{N}\mathbb{Z}/\mathbb{Z})^2)$$

N について極限をとると、$\mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F}_1)$ の元は丁度《楕円曲線の位数有限の元の全体のなす群》の自己同型群と同型になる事がわかります。

$$\mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F}_1) \cong \mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^2).$$

右辺に現れる群を解析するには、やはり素数ごとに分けるのが有効です。

$$\mathbb{Z}_{(p)} = \{p^{-k}n; k \in \mathbb{Z}, n \in \mathbb{Z}\}$$

と書くことにすると、任意の分数を素数巾を分母とする分数の和に書くことに対応する

$$\mathbb{Q}/\mathbb{Z} \cong \bigoplus_p (\mathbb{Z}_{(p)}/\mathbb{Z})$$

なる同形があります。従って、

$$(\mathbb{Q}/\mathbb{Z})^2 \cong \bigoplus_p (\mathbb{Z}_{(p)}/\mathbb{Z})^2$$

右辺の各直和因子は左辺の元のうち位数が p の巾であるものの全体と一致しますから、それらは自己同型で保たれます。ゆえに、

$$\mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^2) \cong \prod \mathrm{Aut}((\mathbb{Z}_{(p)}/\mathbb{Z})^2).$$

右辺に現れる群が $\prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ と同型であることはここまで読んできた読者には容易に証明できるはずです。

以上で $\mathrm{Gal}(\mathcal{F}_\infty/\mathbb{C})$ が $\mathrm{PSL}_2(\mathbb{Q})$ と $\prod GL_2(\mathbb{Z}_p)$ との合成で得られることが明らかになりました。アルティン写像の定義のときにやったのと同様の、分母をすべて $\mathrm{GL}_2(\mathbb{Q})$ に押し付ける方法により、

$$\mathrm{GL}_2(\mathbb{Q}_A) = \mathrm{GL}_2(\mathbb{Q}) \prod_p \mathrm{GL}_2(\mathbb{Z}_p)\mathrm{GL}_2(\mathbb{R})$$

という等式が成り立ちますから、$\prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ と $\mathrm{GL}_2(\mathbb{Q})$ の合成のされ方が $\mathrm{GL}_2(\mathbb{Q}_A)$ と $\mathrm{Gal}(\mathcal{F}_\infty/\mathbb{C})$ とで同様であることがわかれば、これで相互律の写像を定義することができたことになります。このあとの展開は読者の研究にお任せします。

7. 付録：平方剰余の相互法則

吉冨 賢太郎

この付録では, 参考として平方剰余の相互法則について補足します。

方程式 $X^2-1=0$ を　mod 3 で考えると解があります. 一方 方程式 $X^2+1=0$ を　mod 3 で考えるとこれは解がありません. 後者は何を意味するかといいますと, 二次体 $\mathbb{Q}(\sqrt{-1})$ において 3 が素数であると言う事になります。$X^2-m=0$ を mod p で考えること, つまり‘平方剰余’は, 素数の分岐などを考える上で意味があるわけです。この解があるかないか (= 平方剰余であるかどうか) が知りたいわけです。

まず, $X^2-1=0$ を考えましょう. これはどんな mod p で考えたって, 解があります.

つまり, 一般に p が奇素数のとき, 方程式 $X^2-m=0 \pmod p$ の解がある (resp. ない) を $\left(\frac{m}{p}\right)=1(resp.-1)$ で表すことにすると $\left(\frac{1}{p}\right)=1$ ということになります.

では $\left(\frac{-1}{p}\right)$ はどうなるでしょうか. 上で 3 の場合を調べましたから $\left(\frac{-1}{3}\right)$ は -1 ということになります. $\left(\frac{-1}{5}\right)$ はどうでしょうか. $X^2+1=0 \pmod 5$ の解があるかどうかを調べればよいのですから $1^2\equiv 1 \pmod 5, 2^2\equiv 4 \pmod 5, 3^2\equiv 4 \pmod 5, 4^2\equiv 1 \pmod 5$ を考えると $X=2,3$ が解になることが解りますから, $\left(\frac{-1}{5}\right)=1$ ということになります. こうやって $p=3,5,7,11,13,17,19,\ldots$ についてやってみますと,

$$\left(\frac{-1}{3}\right)=\left(\frac{-1}{7}\right)=\left(\frac{-1}{11}\right)=\left(\frac{-1}{19}\right)=-1$$

$$\left(\frac{-1}{5}\right)=\left(\frac{-1}{13}\right)=\left(\frac{-1}{17}\right)=1$$

となることがわかります. これをみるとどうやら

$$\begin{cases}\left(\frac{-1}{p}\right)=1 & (p \text{ が mod } 4 \text{ で } 1 \text{ と合同のとき})\\ \left(\frac{-1}{p}\right)=-1 & (p \text{ が mod } 4 \text{ で } 3 \text{ と合同のとき})\end{cases}$$

となりそうです.

証明する前に $\left(\frac{2}{p}\right)$ はどうなるかも考えてみましょう. $X^2-2=0 \pmod 3$ や $X^2-2=0 \pmod 5$ は上の合同式から解はありません. 他方 $X^2-2=0 \pmod 7$ には解 $X=3$ があります. こうやって $p=3,5,7,11,13,17,19,\ldots$ について調べてみると,

$$\left(\frac{2}{3}\right)=\left(\frac{2}{5}\right)=\left(\frac{2}{11}\right)=\left(\frac{2}{13}\right)=\left(\frac{2}{19}\right)=-1$$

$$\left(\frac{2}{7}\right)=\left(\frac{2}{17}\right)=1$$

です. どうやら

$$\begin{cases}\left(\frac{2}{p}\right)=1 & (p \text{ が } \bmod 8 \text{ で } 1,7 \text{ と合同のとき})\\ \left(\frac{2}{p}\right)=-1 & (p \text{ が } \bmod 8 \text{ で } 3,5 \text{ と合同のとき})\end{cases}$$

となりそうです。

さてそれでは上記のことを証明してみましょう. その前にオイラーの規準というのを説明しておきます。p 奇素数に対して,

$$X^2\equiv a \pmod p \text{が解をもつ} \iff a^{\frac{p-1}{2}}\equiv 1 \pmod p$$

というものです.

これを証明してみましょう. $\mathbb{Z}/p\mathbb{Z}^\times$ は位数が $p-1$ の巡回群であることはよく知られています. その生成元を一つ取って来てそれを γ とします.

$$\gamma^{\frac{p-1}{2}}\equiv -1 \pmod p$$

です。なぜならば $\gamma^{\frac{p-1}{2}}$ は 2 乗して 1 でそれ自身は 1 ではないからです。

$a\equiv\gamma^m \pmod p$ とすると, 明らかに

$$m\text{が偶数} \iff X^2\equiv a \pmod p \text{に解がある}$$

ですから

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv \gamma^{m\,\frac{p-1}{2}} \pmod{p} \\ &\equiv (-1)^m \pmod{p} \end{aligned}$$

よりオイラーの規準は証明されます。

さて, いわゆる平方剰余の第 1 補充法則, 第 2 補充法則の証明をしましょう.

Proposition 7.1. *(補充法則)*

(1) $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(2) $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Proof. (1) はオイラーの規準から明らかです. (2) については $\overline{\mathbb{F}_p}$ を $\mathbb{F}_p$ の代数的閉包とし, $\zeta \in \overline{\mathbb{F}_p}$ を -1 の 4 乗根とし, $y = \zeta + \zeta^{-1}$ とおきます。容易に $y^2 = 2, y^p = \zeta^p + \zeta^{-p}$ がわかります。y が 2 の平方根ですから結局 $y \in \mathbb{F}_p$ か $y \notin \mathbb{F}_p$ にしたがって, $\left(\dfrac{2}{p}\right) = 1$ か $\left(\dfrac{2}{p}\right) = -1$ となります。y が $\mathbb{F}_p$ に入っているかどうかはフロベニウス写像でどうなるかをみればいいわけです。

$p \equiv \pm 1 \pmod 8$ ならば $\zeta^p = \zeta^{\pm 1}$ だから $y^p = y$ つまり, $y \in \mathbb{F}_p$ であり

$p \equiv \pm 5 \pmod 8$ ならば $\zeta^4 = -1$ により

$$y^p = \zeta^5 + \zeta^{-5} = -(\zeta + \zeta^{-1}) = -y$$

すなわち $y \notin \mathbb{F}_p$ です。よって証明されました。 □

さて平方剰余の相互法則とは次の命題です。

Theorem 7.2. *p, q を 異なる奇素数とする時*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

が成り立つ。

これを使うと例えば,

$$\begin{aligned}\left(\frac{3}{5}\right) &= \left(\frac{5}{3}\right) \times (-1)^{2\times 1} \\ &= \left(\frac{2}{3}\right) \\ &= -1\end{aligned}$$

等として第一補充法則, 第二補充法則と合わせることにより $\left(\frac{q}{p}\right)$ を計算することができます。

証明はいろいろありますが本文の応用としてここではアルティンの写像をを使って証明することにします。

まず, 局所相互律写像がどうなるか考えて見ましょう。K を $\mathbb{Q}$ 上の二次体とし $\mathbb{Q}$ の (有限または無限) 素点 l に対して $\mathbb{Q}_l$, $K_\mathfrak{l}$ をそれぞれ l および l の上の素点に関する局所化とすると局所相互律写像

$$\phi_l : \mathbb{Q}_l^\times \quad \longrightarrow \quad \mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_l)$$

は,

$$\mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_l) \cong \{1, -1\}$$

ですから $\phi_l(a) = \pm 1$ とかけます。ここで本文に触れていないので恐縮ですが局所相互律写像が $\mathbb{Q}_l^\times / \mathrm{N}_{K_\mathfrak{l}/\mathbb{Q}_l} K_\mathfrak{l}^\times$ と $\mathrm{Gal}(K_\mathfrak{l}/\mathbb{Q}_l)$ の同型を誘導する事を使います。すると,

$$\phi_l(a) = 1 \ \text{ or } \ -1 \Longleftrightarrow a \in \ \text{ or } \ \notin \mathrm{N}_{K_\mathfrak{l}/\mathbb{Q}_l} K^\times$$

となります。

以下では k を一般に局所体 $\mathbb{R}$ または $\mathbb{Q}_p$ を表すとします。まずヒルベルト記号を定義します。

Definition 7.1. $k^\times$ の元 a, b に対して, $z^2 - a\,x^2 - b\,y^2 = 0$ を満たす k の元 z, x , y (ただし $x = y = z = 0$ は除く) が存在する時 $(a, b)_k = 1$, そうでない時 $(a, b)_k = -1$ とおく。

この $(a,b)_k$ がヒルベルト記号と呼ばれるもので定義から明らかに

$$(,)_k : k^\times/k^{\times 2} \times k^\times/k^{\times 2} \longrightarrow \{\pm 1\}$$

を定めます。さてここでヒルベルト記号の値とノルム群に入るという条件との関係を述べておきましょう。また, ヒルベルト記号の簡単な性質についても述べておきましょう。

Lemma 7.3. $p,q \in k^\times$, $K = k(\sqrt{q})$ とする。このとき, $(p,q)_k = 1$ となるためには, p が $N_{K/k}K^\times$ *(ノルム群と呼ぶ)* に含まれることが必要十分である。

Proof. q が $q = r^2$ $(r \in k^\times)$ ならば, $z^2 - px^2 - qy^2 = 0$ は解 $(z,x,y) = (r,0,1)$ がとれますから $(p,q)_k = 1$ です。一方, $K = k$ ですから $\mathrm{N}_{K/k}K^\times = k^\times$ で p はつねに $\mathrm{N}_{K/k}K^\times$ の元です。次に, q が平方数でない時は, K は k の 2 次拡大となりますから K の元 a は $a = z + y\sqrt{q}$ と書けて, $\mathrm{N}_{K/k}a = z^2 - qy^2$ です。したがって, $p \in \mathrm{N}_{K/k}K^\times$ ならば ある $z,y \in k^\times$ があって $p = z^2 - qy^2$ となり, 方程式 $z^2 - px^2 - qy^2 = 0$ は $(z,1,y)$ を解に持ちます。つまり,

$$p \in \mathrm{N}_{K/k}K^\times \quad \Longrightarrow \quad (p,q)_k = 1$$

が成り立ちます。逆に, $(p,q)_k = 1$ のときは定義により $z,x,y \in k^\times$ で方程式 $z^2 - px^2 - qy^2 = 0$ を満たすものが取れます。$x = 0$ とすると $q = (z/y)^2$ となって q が平方数ではないという仮定に反しますから, $x \neq 0$ です。このとき, $p = (\frac{z}{x})^2 - q(\frac{y}{x})^2$ ですから, $p \in \mathrm{N}_{K/k}K^\times$ が成り立ち, すなわち逆が成り立ちます。 □

Lemma 7.4. ヒルベルト記号は以下の公式を満たす*:*

(1) $(a,b) = (b,a)$, $(a,c^2) = 1$
(2) $(a,-a) = 1$, $(a,1-a) = 1$
(3) $(a,b) = 1 \to (aa',b) = (a',b)$
(4) $(a,b) = (a,-ab) = (a,(1-a)\,b)$
(5) $(aa',b) = (a,b)\,(a',b)$

Proof. (1) は明らかです。また, (2) は 方程式 $z^2 - ax^2 + ay^2 = 0$ と $z^2 - ax^2 - (1-a)y^2 = 0$ はそれぞれ解 $(0,1,1)$ と $(1,1,1)$ を持ちますから成り立ちます。(3) は $(a,b)_k = 1$ のとき, 前の Lemma でノルム群を N と書くと $a \in \mathrm{N}$ ですから

$$a' \in \mathrm{N} \Longleftrightarrow aa' \in \mathrm{N}$$

したがって (3) が成り立ちます。(4) は (1),(2),(3) から容易に従います。

(5) は次の定理から直ちに証明されます。(逆に (5) がわかれば (3) は自明です。) □

では (a,b) を計算しましょう。結果からいいますと:

Theorem 7.5. (1) k が $\mathbb{R}$ のとき:

$$\begin{cases} (a,b) = 1 & a,b \text{ の何れかが正のとき} \\ (a,b) = -1 & a,b \text{ がともに負のとき} \end{cases}$$

(2) k が $\mathbb{Q}_p$ のとき: $a = p^\alpha u, b = p^\beta v$ (ただし, u,v は p-進単数) とするとき

$$\begin{cases} (a,b) = (-1)^{\alpha\beta\epsilon(p)} \left(\dfrac{u}{p}\right)^\beta \left(\dfrac{v}{p}\right)^\alpha & p \neq 2 \\ (a,b) = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} & p = 2 \end{cases}$$

ただし, $\epsilon(x) = \dfrac{x-1}{2}$, $\omega(x) = \dfrac{x^2-1}{8}$ (何れも $mod\ 2$) を意味する。また $\left(\dfrac{u}{p}\right)$ は u を $\mathbb{Z}/p\mathbb{Z}$ のなかで考えた時の値である。

Proof. k が $\mathbb{R}$ のときは自明です。

k が $\mathbb{Q}_p$ とします。明らかに α , β を mod 2 で考えればいいので $(\alpha,\beta) = (0,0)$, $(0,1)$, $(1,1)$ の場合に考えれば十分です。ここでは, $p \neq 2$ の場合だけ証明を与えておきましょう。$p = 2$ の場合は [セール] を参照してください。

(1) $\alpha = 0, \beta = 0$ この場合は $(u,v) = 1$ を示せばよい。

[セール] 第 1 章 2.2 系 2 :

[K(有限体) 上の二次形式は 3 個以上の変数を持てば自明でない 0 を持つ]

によって, 有限体 $\mathbb{F}_p$ 上 $z^2 - ux^2 - vy^2 = 0$ は解をもつ。さらにこれは 逐次近似することで (具体的には [セール] 第 2 章 2.2 系 2 :

[$p \neq 2$, $f(X) = \sum_{1\leq i,j\leq m} a_{ij}X_iX_j$, $a_{ij} = a_{ji} \in \mathbb{Z}_p$ とし, $\det(a_{ij})$ が可逆であるとする. $a \in \mathbb{Z}_p$ に対し, $f(X) \equiv a \pmod p$ が原始的な解を持てばその解は $\mathbb{Z}_p$ 係数の $f(X) = a$ の解に持ち上げられる]

によって $\mathbb{Q}_p$ の解に持ち上げられるので $(u, v) = 1$ となります。

(2) $\alpha = 1, \beta = 0$ この場合は $(pu, v) = \left(\frac{v}{p}\right)$ を示せばよい。Lemma 7.4 (3) により, $(pu, v) = (p, v)$ ですから $(p, v) = \left(\frac{v}{p}\right)$ を示せばよいわけです。v が平方数でないとしてよい。 このとき, $\left(\frac{v}{p}\right) = -1$ 。いまもし, $z^2 - px^2 - vy^2 = 0$ が自明でない解を持つとします。原始解を z, x, y とすると $z^2 \equiv v\, y^2 \pmod p$ で, v が平方数でないのですからこれは $z \equiv y \equiv 0 \pmod p$ でなければならない。すると $p\ x^2 \equiv 0 \pmod{p^2}$ となり, $x^2 \equiv 0 \pmod p$ で原始解であることに反します。よって自明でない解はないわけです。つまり, $(p, v) = -1$。

(3) $\alpha = 1, \beta = 1$ のとき, $(pu, pv) = (-1)^{\frac{p-1}{2}}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$ を示せばよい。Lemma 7.4 により, $(pu, pv) = (pu, -p^2uv) = (pu, -uv)$。上のことから $(pu, -uv) = \left(\frac{-uv}{p}\right)$ ですから $(pu, pv) = \left(\frac{-uv}{p}\right)$。よって第 1 補充法則 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ より従います。

□

このヒルベルト記号から局所相互律写像を計算して見ましょう。

$k=\mathbb{Q}_l$ のときに $(a,b)_k$ を $(a,b)_l$ と書くことにします。$K=\mathbb{Q}(\sqrt{q})$ とすると, l を (有限または無限の) 素点として　$\phi_l(p)=(p,q)_l$ です。今, $l=p,q$ に対しては

$$(p,q)_p=(-1)^0\left(\frac{1}{p}\right)^0\left(\frac{q}{p}\right)^1=\left(\frac{q}{p}\right)$$

および

$$(p,q)_q=(-1)^0\left(\frac{p}{q}\right)^1\left(\frac{1}{q}\right)^0=\left(\frac{p}{q}\right)$$

となります。また $l=2$ のときは

$$(p,q)_2=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

です。$l\neq 2,p,q$ に対しては p,q は正の数ですから $l=\infty$ のときは

$$(p,q)_\infty=1$$

$l\neq\infty$ なら

$$(p,q)_l=(-1)^0\left(\frac{p}{l}\right)^0\left(\frac{q}{l}\right)^0=1$$

ですべて 1 です。

ここでヒルベルト記号の積公式：

Theorem 7.6.

$$\prod_{l\leqq\infty}(a,b)_l=1$$

これは, 本文中の大域相互律写像が $\mathbb{Q}^\times$ で 1 になることから容易に従います。これと上の $(p,q)_l$ の値とから

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

すなわち平方剰余の相互法則が得られます。以上でアルティンの相互律写像を使った平方剰余の相互法則の証明は終わりです。他の証明方法等については [セール] の数論講義の他, 平方剰余の相互法則 – ガウスの全証明 – (倉田令二朗：日本評論社) にあります。