なんでも p 乗してみる。

Contents

1. この稿全体の問題: $x^p \pmod p$ を求めよ 2
2. $x = n$ が整数のとき 2
2.1. 素数か否かの粗い判定法 2
2.2. Carmichael 数 3
2.3. 高速冪乗 4
2.4. 問題 4
2.5. 素数判定法 5
3. 剰余環と有限体 $\mathbb{F}_p$ 5
3.1. 剰余環 5
3.2. 体 $\mathbb{F}_p$ 6
4. p 乗の和 (可換な場合) 6
4.1. p 乗の和 (可換な場合) 6
4.2. 二項係数の話から 6
4.3. Fermat の小定理の証明 7
4.4. 系 7
5. α が代数的数のとき。 8
5.1. 代数的数、代数的整数 8
5.2. 8
6. 余談: 代数体の自己同型としての Frobenius 写像 etc 8
6.1. アナロジー: リーマン面の基本群、被覆群 9
6.2. 類体論というエエトコ取り 9
6.3. 局所類体論 9
6.4. 素数全体に渡るはなしと積公式 11
6.5. アバウトな話 11
6.6. 例 11
7. 行列 $A \in M_n(\mathbb{Q})$ にたいして 12
8. p 乗の和 (非可換の場合:Jacobson の公式) 12
8.1. 微分と積分 12
8.2. Jacobson の公式 13
8.3. 証明と variant 13
9. p-curvature 14
9.1. $r = 1$ のとき、 14
9.2. r: 一般, 可換な場合 15
9.3. r: 一般、可換とは限らない場合 15

10. Weyl 環の元 16
11. Hochshild-Serre の公式 17

1. この稿全体の問題: $x^p \pmod p$ を求めよ

この稿を通じて、p は素数であるとします。次のような問題を考えます。

この稿全体の問題

与えられた x に対して、x^p modulo p (x^p を p で割った余り) を計算せよ。

x としていろんなものをとるというのがミソで、さしあたって

- 数
- 行列
- 微分作用素
- 数列へのずらし

などが考えられるところです。

2. $x = n$ が整数のとき

はじめの例として、 x が整数の時を考えましょう。

定理 2.1. x が整数ならば、$x^p \mod p$ は x に等しい。*(つまり変わらない。)*

証明. Fermat の小定理により、

$$n^p \equiv n \mod p.$$

□

Fermat の小定理の証明はこの稿の 4.3 節でも一応証明してあります。

2.1. **素数か否かの粗い判定法.** 「変わらない」ことは意味をもたない気もするかもしれませんが、そうではありません。

p が素数なら、$2^p \mod p = 2$ でないといけないし、$3^p \mod p = 3$, $4^p \mod p = 4$, $5^p \mod p = 5$, ..., でないといけない。あとで少しだけ触れるように、べき乗は比較的短時間で計算できるので、このことは p が素数か否かの粗い判定法を与えます。たとえば、$2^p \mod p \neq 2$ であればただちに p が素数でないことがわかるというわけです。

2.2. **Carmichael 数.** 急いで付け加えておかなければなりません。整数 p が、$2^p \mod p = 2, 3^p \mod p = 3, 4^p \mod p = 4, 5^p \mod p = 5, \ldots,$ を満たすにもかかわらず p が素数でない場合があります。このような数は Carmichael 数と呼ばれます。より正確に定義を述べれば、次のような具合です:

定義 2.1. 正の整数 n が Carmichael 数であるとは、n は素数でないにもかかわらず、n と互いに素な任意の a に対して、$a^n \equiv a \mod n$ が成り立つときに言う。

2.2.1. *Carmichael* 数 の確率的判定法. 正の整数 n にたいして、つぎのような判定法が考えられます。

Carmichael 数 の判定

次のようなことを繰り返し行う。

(1) $(\mathbb{Z}/n\mathbb{Z})^\times$ の元 x をランダムにとる。
(2) $x^n = x$ か否かをチェックする。($x^n \neq x$ ならばもちろん n は Carmichael 数 ではない。)

これを例えば 100 回行って、いつもチェックが成功すれば、n が Carmichael 数でも素数でもないのにそんなことが起こる確率は $1/2^{100}$ 以下である。

証明. 群論を用いる。n がもし Carmichael 数 ではないならば、$(\mathbb{Z}/n\mathbb{Z})^\times$ の部分集合

$$H = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times; x^n = x\}$$

は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群であり、したがって n がもし Carmichael 数 ではないならば、$(\mathbb{Z}/n\mathbb{Z})^\times$ の部分集合

$$H = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times; x^n = x\}$$

は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群であり、したがって

$$\#(\mathbb{Z}/n\mathbb{Z}^\times)/\#H = \#((\mathbb{Z}/n\mathbb{Z}^\times)/H)$$

は 1 より大きい整数である。もし、ランダムに $(\mathbb{Z}/n\mathbb{Z})^\times$ の元をとれば、それが H に入る確率は多く見積もっても $1/2$ 以下である。 □

上のことから、与えられた数が Carmichael 数であるか否かはすばやく判定できる確率アルゴリズムがありますが、Carmichael 数は数が少ないため、次のことは問題として残ります。

問題 2.1. 与えられた数 n に対して、n より大きな Carmichael 数のうち最小のものを ($\log n$ の多項式程度の時間で) 求める確率的アルゴリズムは存在するか?

オンライン整数列大辞典には、Carmichael 数の最初の数十個が書いてあります。それによれば、最初の Carmichael 数は 561 のようです。

2.3. **高速冪乗.** f, n, m が比較的大きい数であっても、$f^n \mod m$ を手早く計算できます。ruby のプログラムを置いておきましょう。

```
# a* f^n mod  m
def mypow1(a,f,n,m)
   while (1==1) do
       if (n==0)
          return(a % m)
       end
       if (n==1)
         return((a*f) % m)
       end
       n1 =n.div(2)
       r1 = n % 2
       if (r1 == 1)
           a=a * f
       end
       f=(f*f) % m
       n=n1
   end
end
#####################################################################
# mypow(f,n,m)
# returns
# f^n mod m
#####################################################################
def mypow (f, n,m)
return(mypow1(1,f,n,m))
end
```

2.4. **問題.** 問題、と言っても大して大事な問題というわけではありませんが、次のものを挙げておきます。

問題 2.2. p と互いに素な a に対して、$a^{(p-1)/2} \in \{\pm 1\}$ が常に成り立つならば、p は素数だろうか?

つちもとはこの問題に対する答を知りません。10 桁ぐらいまでの範囲なら正しいようです。

2.5. **素数判定法.** 素数判定について、よく知られて、正しい方向性としては、Miller-Rabin 判定法と Solovay-Strassen の判定法があります。

Solovay Strassen の判定法

n が与えられたとする。n と互いに素な a に対して、

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \text{(Jacobi 記号)} \mod n$$

が成り立てば、a についてのテストは合格。

ランダムな a ついて上記のようなテストを行い、不合格なら n は素数ではなく、合格なら n が素数である可能性が上がる。(テストを行うごとに誤判定の可能性を $1/2$ にできます。)

Jacobi 記号の知識/計算が必要なところが大変そうですが、次の Miller-Rabin 判定法ではそれが必要なくなります。

Miller-Rabin 判定法

n が与えられたとする。$n-1$ を 2 で割れるだけ割って、

$$n-1 = 2^s d \qquad (\gcd(d,2)=1)$$

と書く。このとき、

(1) $a^d = 1$ か
(2) $a^{2^r d} = -1 \qquad (\exists (r \in \{0,\dots,s-1\})$

が成り立てば、a についてのテストは合格。

ランダムな a ついて上記のようなテストを行い、不合格なら n は素数ではなく、合格なら n が素数である可能性が上がる。(テストを行うごとに誤判定の可能性を $1/4$ にできます。)

詳しくは wikipedia にもあるのでそちらをご参照ください。

3. 剰余環と有限体 $\mathbb{F}_p$

3.1. **剰余環.** 整数 m に対して、 剰余環 $\mathbb{Z}/m\mathbb{Z}$ とは、要するに

$$a \equiv b \mod m$$

を

$$a = b \qquad \text{in } \mathbb{Z}/m\mathbb{Z}$$

と書き換えて得られる世界です。ガウス整数論 (高瀬正仁訳) 第 1 章の注を見ると

> ルジャンドルは著作の中で合同式に対しても等号をそのまま使用した。しかし我々は曖昧さが発生するかも知らえないことを恐れて、それを模倣する気持ちにはなれなかったのである。

と書かれていて、少し驚きます。ガウスは剰余環 (と現代では言われるもの) についても十分理解していたでしょうが、それとともに同世代の無理解なひとたちのことも理解していたのでしょう。すくなくとも、ずっとあとの世代の環論の整備を待たねば、それらの人々には扱いが危なっかしいと感じられた面もあったのでしょう。

とりあえず我々は現代に住んでいて、$\mathbb{Z}/m\mathbb{Z}$ というものを集合論、環論の土台の上に手に入れています。

3.2. **体 $\mathbb{F}_p$.** p が素数であるとき、$\mathbb{Z}/p\mathbb{Z}$ は体です。(つまり、0 以外の元により割り算ができます。) これはユークリッドの互除法によりわかります。

以後、$\mathbb{Z}/p\mathbb{Z}$ のことを $\mathbb{F}_p$ と書きます。

4. p 乗の和 (可換な場合)

a, b が可換ならば、バラバラと展開して、$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$ という式が成り立つのでした。もしこれが $\mathbb{F}_3$ 上の話なら、右辺の間の項は全て消えて、

$$(a+b)^3 = a^3 + b^3 \qquad (\mathbb{F}_3 \text{ 上の環の可換な元 } a, b \text{ について})$$

がなりたちます。この節の内容はその一般化です。

4.1. **p 乗の和 (可換な場合).**

定理 4.1. $\mathbb{F}_p$ 上の環の元 a, b が可換ならば

$$(a+b)^p = a^p + b^p$$

証明. 二項定理により、

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p$$

あとは次小節の内容からわかります。

□

4.2. **二項係数の話から.**

補題 4.2. p は素数であるとする。このとき、

$$p \mid \binom{p}{k} \qquad if\ 1 \le k \le p-1$$

[これは Pascal の 3 角形が p の段で両端を除いて p の倍数ばかりが現れることを意味している。]

証明.

$$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!}$$

は整数であり、分母は p を素因子にもたず、分子は p を素因子に持つ。ゆえに、(素因数分解の一意性により) $p \mid \binom{p}{k}$. □

4.3. **Fermat の小定理の証明.**

$$S = \{x \in \mathbb{F}_p; x^p = x\}$$

とおきます。

つぎのことがわかります。

(1) $1 \in S$.
(2) $a, b \in S \implies a + b \in S$.

実際、(1) は当たり前ですし、(2) は前小節の内容からすぐに従うことです。

このことから、$S = \mathbb{F}_p$. すなわち、任意の $x \in \mathbb{F}_p$ に対して、$x^p = x$ がわかります。

(ついでに $x \in \mathbb{F}_p$ が、$x \neq 0$ をみたすなら、$x^p = x$ の両辺を x で割って、 $x^{p-1} = 1$ が得られます。普通 Fermat の小定理として知られているのはこっちでしょう。)

4.4. **系.**

系 4.3. $\mathbb{F}_p$ 上の環の元 a, b が可換ならば、$\mathbb{F}_p$ 上で

$$(a-b)^{p-1} = \sum_{j=0}^{p-1} a^j b^{p-1-j}$$

証明. まず多項式環 $\mathbb{F}_p[T, U]$ 上で考えよう。T, U は不定元である。

$$T^p - U^p = (T-U)^p$$

ゆえに

$$(T-U)^{p-1} = \frac{T^p - U^p}{T-U} = \sum_{j=0}^{p-1} T^j U^{p-1-j}$$

一般の場合はこの特殊化として得られる。 □

この手の議論は代数ではよく行われます。まず零因子をもたない環 (多項式環などがその典型) で等式を証明し、手に入れた等式に一般の元を代入 (特殊化) することで一般の場合の証明ができるという寸法です。

5. α が代数的数のとき。

5.1. **代数的数、代数的整数.** 本稿では代数的数、代数的整数についていろいろなことを扱いますが、その基本事項についてはここでは割愛します。少なくとも下の事実は使います。

- 体 K とその部分環 R が存在するとき、K 内で R 上整なものの全体は環をなす。これを R の K 内での整閉包と呼ぶ。
- とくに、$K \subset \bar{\mathbb{Q}}$ のとき、$\mathbb{Z}$ の K 内での整閉包を $\mathcal{O}_K$ と書き、K の整環と呼ぶ。

5.2. α が代数的数、 すなわち、$\alpha \in \mathcal{O}[1/d]$ ($\mathcal{O}$ はある代数体 K の整数環, d は正の整数) のとき。$u(X)$ を α の $\mathbb{Q}$ 上の (モニック) 最小多項式にとります。$\alpha_1, \ldots, \alpha_n$ を u の根としましょう。

$$r_{(p)}(X) = \sum_j \frac{u(X)\alpha_j^p}{(X-\alpha_j)u'(X)}$$

(Lagrange の補間式) とおけば、

$$X^p \equiv r_{(p)}(X) \pmod{u(X), p}$$

であって、

$$\alpha^p = r_{(p)}(\alpha)$$

です ("Kuroiwa 理論")

(見かけ上少しだけ) 別の計算法もあります。$|t| >> 0$ に対する展開

$$\frac{1}{u(t)}\frac{(u(x)-u(t)}{x-t} = \sum_{n=0}^{\infty} r_n(x)t^{-n-1}$$

を考えます。このとき、素数 p にたいして $r_p(x) \pmod p$ はうえの $r_{(p)}(x)$ と一致します。

6. 余談: 代数体の自己同型としての Frobenius 写像 etc

本稿では殆どは標数 p、$\mathbb{F}_p$ 上の話をするのですが、ちょっとだけ $\mathbb{Q}$ とその代数閉包 $\bar{\mathbb{Q}}$ の話を書いておきましょう。本格的には「類体論」ということになるわけですが、類体論の書物は良いものがたくさん出ているのでここではアバウトなことのみ書いておきます。(この節は特に書きかけの度合いが高くなっています。)

L を $\mathbb{Q}$ の有限次ガロア拡大、$\mathcal{O}_L$ をその整数環とします。L は $\mathbb{Q}$ 上単純拡大です。すなわち $L = K(\alpha)$ となる $\alpha \in L$ が存在します。(標数ゼロの有限次代数拡大に関するガロア理論). α の $\mathbb{Q}$ 上の最小多項式を u と書くと、u は $\mathbb{Z}[1/d]$ 上定義される一変数多項式です。

さて、$\mathfrak{p}$ を $\mathcal{O}_L$ の 0 でない素イデアルとします。$\mathcal{O}_L/\mathfrak{p}$ の標数を p とおきます。d の約数ではない p に対して、 u modulo p が考えられて、その分解のしかたが p にどう依存するかが大事になります。

u の判別式が p の倍数の場合は u が modulo p で重根を持つことになり、特別の注意が必要になります。このような場合を「分岐する場合」それ以外の場合を「不分岐の場合」と呼びます。

本稿ではおもに p が u などに比べて十分大きい場合を考えたいので、不分岐な場合を考えることが多くなることになります。が、「類体論」の精緻な世界では分岐する場合も合わせて考えないとうまく説明できないことも多いので、この節ではほんのちょっとだけ分岐の場合も述べることにします。

6.1. **アナロジー: リーマン面の基本群、被覆群.** 数体の Galois 群はリーマン面の基本群とたいへん似た性質があります。

画用紙に見立てたリーマン面に画鋲でプスプス穴を開けて、残りの部分をアリンコより小さい妖精さんが歩き回っている様子を思い浮かべるといいかもしれません。

6.2. **類体論というエエトコ取り.** 類体論は、Galois 群の可換な部分のみをとります。これには、2 つのとらえ方が考えられるでしょう。

- $\mathbb{Q}$ のアーベル拡大のみを考える理論。
- $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ の可換化 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}}$ を調べる理論

手順前後はしばしば重大な結果を生むのですが、そこを無視して、エエトコをとったのが類体論、というわけです。ちなみに、そのへんを無視せずに、全部の寄与を考えようというのが非可換類体論、ということになるのでしょう。

6.3. **局所類体論.** 画用紙に画鋲であなをひとつだけ開けて、その穴のごくごく周辺で妖精さんが歩き回る、その様子が局所類体論、ということになります。

6.3.1. 不分岐の場合. 基本的には、穴のまわりを「何回まわるか」、が大事になります。

L を $\mathbb{Q}$ のガロア拡大、$\mathcal{O}_L$ をその整数環、$\mathfrak{p}$ を $\mathcal{O}_L$ の 0 でない素イデアルとします。$\mathcal{O}_L/\mathfrak{p}$ の標数を p とおきます。

(1) $F : \mathcal{O}_L/\mathfrak{p} \ni x \mapsto x^p \in \mathcal{O}_L/\mathfrak{p}$ は体の同型である。
(2) F は $\mathcal{O}_L$ の $\mathfrak{p}$-進完備化 $\widehat{(\mathcal{O}_L)_{\mathfrak{p}}}$ の同型を誘導する。これを以下仮に $\hat{F}$ と書くことにする。
(3) $\mathcal{O}_L$ は $\widehat{(\mathcal{O}_L)_{\mathfrak{p}}}$ の中の $\mathbb{Z}$ の整閉包であるから、$\hat{F}$ で保たれる。すなわち $\hat{F}$ は $\mathcal{O}_L$ の同型を誘導する。これを以下仮に $F_{\mathcal{O}_L}$ と書くことにする。
(4) 不分岐の場合、$F_{\mathcal{O}_L}$ は $\mathcal{O}_L$ の商体 L の自己同型を誘導する。これを以下仮に F と書くことにする。

まとめると、$L, \mathfrak{p}$ が与えられると、L の自己同型が与えられることになります。この自己同型を

$$\left(\frac{L/\mathbb{Q}}{\mathfrak{p}}\right)$$

と書くことにします。(Artin 記号)

6.3.2. 分岐の場合も込めての状況. p で「中途半端にまわる」のも込めてまわる様子を記述するのが局所類体論です。まわる様子を記述するのが Artin map

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

で、「何回まわるか」と「中途半端さの度合いは」という問いに対して $\mathbb{Q}_p^\times$ の元で答えます。以下、岩沢健吉「局所類体論」に沿っています。(記号を無理やり合わせようとしているため、他のところと整合性がとれていません。)

k を、標数 0、剰余体の標数が $p > 0$ であるような局所体であるとする。

k の素元 π ($\mathcal{O}_k$ の素元) に対して、次のような $\psi = \psi_\pi \in \mathrm{Gal}(k_{\mathrm{ab}}/k)$ が一意的に存在する。

ψ_π の定義

- $\psi|_{k_{\mathrm{ur}}} = \mathrm{Frob}$.
- $\pi \in N(F_\psi/k)$. $N(F_\pi/k)$ はノルム群というやつで、

$$N(F/k) = \bigcap_{F \supset k' \supset k} N_{k'/k}(k'^\times).$$

(F の部分体で k の有限次拡大 t 体であるような k' に関する共通部分。)

補題 6.1. 群準同型 $\alpha : k^\times \to \mathrm{Gal}(k_{\mathrm{ab}}/k)$ で、任意の素元 $\pi \in k$ に対して $\alpha(\pi) = \psi_\pi$ を満たすものが一意に存在する。α を *(local) Artin map* と呼ぶ。

$k^\times$ の元 x は $x = u\pi^l$ $(\exists l \in \mathbb{Z}, \exists u \in \mathcal{O}_K^\times)$ と書かれることに注意します。u を一つの π におっつけて $x = u\pi^l = (u\pi)\pi^{l-1}$ と書きますと、$\pi' = u\pi$ も素元であって、

$$\alpha(x) = \psi_{\pi'}\psi_\pi^{l-1}$$

と表されます。$\psi_{\pi'}$ や ψ_π は k_{ur} に制限すると「一回まわる」(Frobenius 写像) に相当しますから、$\alpha(x)$ は「l 回まわる」のに「イロ (尾ひれ) を付けた」ようなものだとわかります。

6.4. **素数全体に渡るはなしと積公式.** L を $\mathbb{Q}$ の有限次ガロア拡大体とします。

素数 p ごとに、$p\mathcal{O}_L$ の素因子 $\mathfrak{p}$ を考えることができます。$\mathfrak{p}$ は複数あるのですが、それらは $\mathrm{Gal}(L/\mathbb{Q})$ で共役で (中級環論)、以下で述べる議論には効いてこないので一つとって固定します。$\mathfrak{p}$ のことを 書くのが面倒なのでとりあえず p と同じ記号で書きます。

素数だけではなく無限遠点をひとつだけ加えたところを考えねばならないのです。$(\alpha_2, \alpha_3, \dots, \alpha_p, \dots)$ というイデール群の元に対して各素数での寄与の積を取ります。

$$(\alpha_2, \alpha_3, \dots, \alpha_p, \dots, \alpha_\infty)$$
$$\mapsto$$
$$((\alpha_2, L_2/\mathbb{Q}_2) \cdot (\alpha_3, L_3/\mathbb{Q}_3) \cdot \dots \cdot (\alpha_p, L_p/\mathbb{Q}_p) \cdot \dots \cdot (\alpha_\infty), L_\infty/\mathbb{Q}_\infty) \in \mathrm{Gal}(L/\mathbb{Q})$$

これは Artin 写像とよばれます。Artin 写像で $\mathbb{Q}^\times$ を送ると 1 になる、というのが積公式で、

次の定理は Artin の相互法則と呼ばれます。

定理 6.2 (Artin)**.** *(statement はノイキルヒ (*代数的整数論*)* 定理 *5.5)* から引用*)* 任意の有限次代数体の *Galois* 拡大 L/K に対して、標準的同型

$$G(L/K)^{\mathrm{ab}} \cong C_K/N_{L/K}C_L$$

が存在する。

6.5. **アバウトな話.** $L/\mathbb{Q}$ をアーベル拡大とします。ここに書いておきたいのは、次のような話です。($\mathbb{Q}$ 上でなく、一般の代数体上の話ても、あんまり変わらないが、とりあえずこうする。)

- 不分岐な素数 p に対して 「p で一回まわる」 Frob_p が定義される。
- 分岐する素数 p では 「中途半端にまわる」ことがある。これらを全部記述できるのが局所類体論。
- $\mathrm{Gal}(L/K)$ の元は どの p で何回まわるか (中途半端にまわる場合も含む) で記述できる。それを記述するのがイデール群の元である。
- $\mathrm{Gal}(L/\mathbb{Q})$ はアーベル群なので、回った順序は気にしなくて良い。
- 積公式は「回った様子」から Galois 群を得るときの関係式を与える。
- 全部ひっくるめて、$\mathrm{Gal}(L/\mathbb{Q})$ の様子を記述するのが、Artin の相互法則。

6.6. **例.** $L = \mathbb{Q}(\sqrt{-1})$ のとき、$\mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id}, \sigma_1\}$. $\mathbb{Q}^\times$ の元をイデール群の元と見て $\mathrm{Gal}(L/\mathbb{Q})$ に送ると id になるはずである。$\mathbb{Q}^\times$ は素数と -1 とでで生成される (素因数分解の一意性) から、それらがどのように振る舞うかを見れば良い。

p :$4k-1$ 型のとき
2 と p とで一回づつまわる。
p :$4k+1$ 型のとき
どの点でも回らない。
$p=2$ のとき
どの点でも回らない。
$p=-1$ のとき
2 と ∞ で一回づつまわる。
なお、$4k+1$ 型の点 p は、$p=a^2+b^2=N(a+b\sqrt{-1})$ となる $a,b\in\mathbb{Z}$ が存在するので、p でまわる分は $\mathrm{Gal}(L/\mathbb{Q})$ には効いてこない。

7. 行列 $A\in M_n(\mathbb{Q})$ にたいして

A の固有多項式を u とおけば、$u(A)=0$ であり、前節とおなじことができる。
◎対角化する方法も考えられる。

8. p 乗の和 (非可換の場合:Jacobson の公式)

8.1. **微分と積分.** 環上の一変数多項式環 $A[T]$ の元

$$f(T)=\sum_j a_jT^j$$

にたいして、その T に関する微分 $(d/dT)f(T)$ を

$$(d/dT)f(T)=\sum_j ja_jT^{j-1}$$

で定義する。

$$f(T)=\sum_j a_jT^j$$

のうち、次の条件を満たすものを考える。

(I_0) $\qquad\qquad \forall j(a_j\neq 0 \implies j+1 \text{ は } A \text{ で 可逆})$

このとき、

$$\int f(T)dT=\sum_j \frac{1}{j+1}a_jT^{j+1}$$

と定義する。定積分なども同様に、定義される範囲で実数体上の積分とおなじ式で定義する。

8.2. **Jacobson の公式.**

定理 8.1. $\mathbb{F}_p$ 上の環の元 a, b にたいし、

$$(a+b)^p = a^p + b^p + \sum_{j=1}^{p-1} s_j(a,b)$$

ただし、

$$s_j(a,b) = \frac{1}{j}\operatorname{coef}((\operatorname{ad}(Ta+b)))^{p-1}a, T^{j-1})$$

$$\sum_{j=1}^{p-1} s_j(a,b) = \int_0^1 (\operatorname{ad}(Ta+b)))^{p-1}a)dT$$

8.3. **証明と variant.** a, b のいずれとも可換な変数 T を考え、$(Ta+b)^p$ を T のべきで展開して

$$(Ta+b)^p = T^p a^p + \sum_{j=1}^{p-1} T^j s_j(a,b) + b^p$$

と書く。両辺を T について微分すると

$$\sum_{i=0}^{p-1} (Ta+b)^i a (Ta+b)^{p-1-i} = \sum_{j=1}^{p-1} jT^{j-1} s_j(a,b).$$

左作用 λ, 右作用 ρ を用いて書くと

$$(\sum_{i=0}^{p-1} \lambda(Ta+b)^i \rho(Ta+b)^{p-1-i}).a = \sum_{j=1}^{p-1} jT^{j-1} s_j(a,b).$$

すでに得た (よく知られた公式) 系 4.3 と、λ,ρ の可換性により、

$$(\lambda(Ta+b) - \rho(Ta+b))^{p-1}.a = \sum_j jT^{j-1} s_j(a,t).$$

すなわち

$$\operatorname{ad}(Ta+b)^{p-1}a = \sum_{j=1}^{p-1} jT^{j-1} s_j(a,t).$$

つまり、

パラメータ付き Jacobson の公式

$$(Ta+b)^p = T^p a^p + b^p + \int_0^T \operatorname{ad}(ta+b)^{p-1} a dt$$

9. p-CURVATURE

この節の問題

$[\eta, t] = 1$ をみたす η, t に対して、

$$A(t) \in M_r(\mathbb{Q}(t))$$

を考える。A の分母の最高次の係数の絶対値よりも大きな素数 p に対して $(\eta + A(t))^p$ (modulo p) を計算したい。

$\eta+A(t)$ はconnection と呼ばれます。$(\eta+A(t))^p = \eta^p+P_A(t)$ ($\exists P_A(t) \in \mathbb{Q}(t)$) となるので、実際には P_A を求めるのが問題になります。P_A のことを connection $\eta + A$ の p-curvature と呼びます。

p-curvature については Grothendieck-Katz 予想と呼ばれる有名な予想があります。詳しくは wikipedia などをご参照ください。(この稿はこれが多いな。)

9.1. $r = 1$ **のとき、.** Jacobson の公式により、

$$(\eta+A(t))^p = \eta^p+A(t)^p+\int_{s=0}^{1} \mathrm{ad}(s\eta+A(t))^{p-1}A(t)ds = \eta^p+A(t)^p-A^{(p-1)}(t)$$

つまり、

$$P_A = A(t)^p - A^{(p-1)}(t).$$

p-curvature を計算するのには、$\mathbb{F}_p$ の代数的閉包 $\bar{\mathbb{F}}_p$ を考えて、部分分数展開を利用すると便利でしょう。

$c \in \bar{\mathbb{F}}_p$, $e \in \{1, 2, \ldots, p-1\}$ にたいして、

$$f_{c,e}(t) \stackrel{\text{def}}{=} \frac{1}{(t-c)^e}$$

とおくと、$\forall a \in \bar{F}_p$ にたいして、

$$-(af_{c,e})^{(p-1)}(t) + (af_{c,e}(t))^p = \begin{cases} \frac{a^p}{(t-c)^{ep}} & \text{if } e > 1 \\ \frac{a^p-a}{(t-c)^p} & \text{if } e = 1 \end{cases}$$

ついでに、

$$f_{\infty,e}(t) \stackrel{\text{def}}{=} t^e$$

にたいして、

$$-(af_{\infty,e})^{(p-1)}(t) + (af_{\infty,e}(t))^p = a^p t^{ep}$$

$$P_A(t) = 0 \iff A(t) = \sum_j \frac{a_j}{t - c_j} \qquad (\exists\{a_j\} \subset \mathbb{F}_p, \quad \exists\{c_j\} \subset \bar{\mathbb{F}}_p)$$

命題 9.1. ほとんどすべての p にたいして、$P_A = 0$ となるための必要十分条件は、A が一位の *pole* しかもたず、なおかつそれぞれの *pole* での *residue* が有理数であることである。さらに、このとき、

$$\frac{d}{dt}f(t) = A(t)f(t)$$

は代数的な解

$$f(t) = \prod_i (t - c_i)^{a_i}$$

をもつ。

9.2. r**: 一般, 可換な場合.** $\{A(t)\}$ が可換な場合、すなわち、

$$[A(t), A(s)] = 0 \qquad (t, s \text{ の有理式として})$$

の場合を考えましょう。両辺を微分することにより、$A(t)$ の微分たちもそれぞれ可換であることがわかります。

この場合の話は、本質的には $r = 1$ の話の繰り返しになります。

Jacobson の公式により、

$$(\eta^p + A(t))^p = \eta^p + A(t)^p - A^{(p-1)}(t)$$

で、p-curvature は $P_A = A(t)^p - A^{(p-1)}(t)$ です。$c \in \bar{\mathbb{F}}_p$ にたいして、c での pole の位数を考えると、A は c で pole を持ったとしてもたかだか 1 位であるということがわかります。さらに、c において

$$A(t) = \frac{A_c}{t - c} + (c \text{ で正則な部分}) \qquad (A_c \in M_r(\bar{\mathbb{F}}_p))$$

と書くと、

$$P_A = \frac{A_c^p - A_c}{(t - c)^p} + (c \text{ で正則な部分})$$

となって、結局 $A_c^p = A_c$ でなければならないことがわかります。これは A_c の最小多項式が $\lambda^p - \lambda$ の約数でなければならないことを意味しますから、A_c の固有値は $\mathbb{F}_p$ の元で、なおかつ A_c は対角か可能であることがわかります。

$\{A_c\}_c \in \bar{F}_p$ は全て可換ですから、これらを同時対角化することができます。けっきょく、最初に述べたとおり、これは $r = 1$ の場合の直和と同型であるという結論が出るわけです。

9.3. r**: 一般、可換とは限らない場合.** 一般の場合も、各点 $c \in \bar{\mathbb{F}}_p$ で考えて得られる結論は変わりません。ただし詳細はわずかに異なるので、念のためここに書いてみます。$c \in \bar{\mathbb{F}}_p$ にたいして、

$$A(t) = \frac{A_c}{(t - c)^e} + B_c(t)$$

と分解してみます。$B_c(t)$ の部分がなければ話は可換の場合になるので、$e > 1$ なら、

$$(\eta + \frac{A_c}{(t-c)^e})^p - \eta^p = (\frac{A_c}{(t-c)^e})^p$$

「$e = 1$」 ならば、

$$(\eta + \frac{A_c}{(t-c)})^p - \eta^p = (\frac{A_c^p - A_c}{(t-c)^p})$$

なのでした。Jacobson の公式により、

$$\begin{aligned}&(\eta + \frac{A_c}{(t-c)^e} + B_c(t))^p \\ =&(\eta + \frac{A_c}{(t-c)^e})^p + \int_0^1 \left(\mathrm{ad}(T(\eta + \frac{A_c}{(t-c)^e}) + B_c(t))\right)^{p-1} B_c(t)dT\end{aligned}$$

積分の掛かる項はすべて $e(p-1)$ 位以下の pole ですから、結局、$P_A = 0$ になるためには $e = 1$ で、$A_c^p = A_c$ でなければならないことがわかります。これは A_c の最小多項式が $\lambda^p - \lambda$ の約数でなければならないことを意味しますから、A_c の固有値は $\mathbb{F}_p$ の元で、なおかつ A_c は対角か可能であることがわかります。まとめると:

命題 9.2. ほとんどすべての p にたいして、$P_A = 0$ となると仮定すると、A は一位の *pole* しかもたず、なおかつそれぞれの *pole* での *residue* は有理数である。

10. Weyl 環の元

命題 10.1. $[\eta, \xi] = 1$ なる元 ξ, η を考える。

$$(\eta(a\xi\eta + b))^p = \eta^p(a^p\xi^p\eta^p + b^p - ba^{p-1})$$

$\theta = \xi\eta$ に対して、

$$(\eta(a\theta + b))^p = \eta^p(a\theta + b)(a(\theta + 1) + b)\dots(a(\theta + (p-1)) + b)$$

であり、

$$\begin{aligned}&(a\theta + b)(a(\theta + 1) + b)(a(\theta + 2) + b)\dots(a(\theta + (p-1)) + b) \\ =&a^p \cdot \theta_1(\theta_1 + 1)(\theta_1 + 2)\dots(\theta_1 + (p-1)) \qquad (\theta_1 \stackrel{\mathrm{def}}{=} \theta + b/a) \\ =&a^p(\theta_1^p - \theta_1) \qquad (\mathbb{F}_p \text{ の数学}) \\ =&a^p(\theta_1^p + b^p/a^p - b/a) \\ =&a^p(\theta^p - \theta) + b^p - ba^{p-1} \\ =&a^p(\xi^p\eta^p) + b^p - ba^{p-1}\end{aligned}$$

11. Hochshild-Serre の公式

命題 11.1. *A :標数 p の可換環, $D \in \mathrm{Der}(A), a \in A$ ならば、*

$$(aD)^p = a^p D^p + (aD)^{p-1}(a) \cdot D$$

証明は松村英之著「可換環論」(共立出版) の「導分と微分」の章 (section 25, 定理 25.5) を参照のこと。
注意: 上の命題は A が非可換では無条件で正しくはない。
例えば $p = 3$ なら、

$$\begin{aligned}
(aD)^3 &= aDaDaD \\
&= a(aD + a')(aD + a')D \\
&= a(aDaD + aDa' + a'aD + a'^2)D \\
&= a(a(aD + a')D + aa'D + aa'' + a'aD + a'^2)D \\
&= a(a^2D^2 + aa'D + aa'D + aa'' + a'aD + aa'a')D.
\end{aligned}$$