p 進数入門

郡司泰生

目次

1 **はじめに** 2

2 **環論からの準備** 4

2.1 数と多項式の類似 4

2.2 環と整域と体 5

2.3 素元分解 8

2.4 商体 11

2.5 数と多項式の類似 part2 12

2.6 形式的ベキ級数環 13

3 **p 進数** 15

3.1 環 $\mathbb{Z}_p$, 体 $\mathbb{Q}_p$ の定義 15

3.2 $\mathbb{Z}_p$, $\mathbb{Q}_p$ の性質 18

3.3 Hensel の補題 23

3.4 Hensel の補題の応用 25

3.5 局所大域原理 26

4 **参考文献** 27

1　はじめに

皆さんこんにちは. 理学部数学科 3 年の郡司泰生と言います. 今回は, 今自分が大学のセミナーで勉強している p 進数という不思議な距離が入る数について紹介したいと思います. p 進数というのは, ” 環” という代数的な構造と” 距離” という位相的な構造をもった対象という意味では複雑に感じられるものかもしれませんが, どちらもまとめて勉強して, 大学でやる数学の雰囲気を掴む意味ではお得かなと思います. ただ時間の都合もあって距離の話をあまりちゃんと書けませんでした.

流れとしては, まずは 2 章では, 高校まででやった普通の数や多項式の類似について考え, 環という概念を導入して, p 進数を考えるモチベーションもまとめて書いています. そしてこの準備の後で p 進整数環 $\mathbb{Z}_p$ と p 進数体 $\mathbb{Q}_p$ を導入して, いくつかの環論的, 位相的な性質を見ます (ここが時間の都合で, 位相空間含め, かなりの前提知識を課してしまったので難しいかもしれません). そして最後に, Hensel の補題と局所大域原理のひとつとして, Hasse-Minkowski の定理の紹介だけします. このあたりは p 進数というものを考える嬉しさがわかりやすいと思います.

前提知識は一応高校までの数学 (特に整数) と思っていたんですが, ところどころいろんな知識を仮定してしまいました. 大学 1, 2 年生でやる集合論, 距離空間の初歩は最低限知っていてもらえると読みやすいと思いますし, 時間の都合で説明しきれてないところが多いので, わからないところは適当に読み飛ばして, 雰囲気を楽しんでもらえたらと思います (うまく読み飛ばしてもらえば, 最後の Hensel の補題あたりまで読み進められるはずです).

最後に, 自分もまだ勉強したばかりのこともあるので, わかっていないところは優しく指摘してもらえると嬉しいです.

よく使う記号のまとめ

特にことわりなく使う記号をまとめておきます.

- p：素数.
- n：正の整数.
- X：多項式の不定元 (小文字の x は数に使いたいです).
- $\mathbb{N} = \{n \mid n \text{ は正の整数}\}$.
- $\mathbb{Z} = \{n \mid n \text{ は整数}\}$.
- $\mathbb{Q} = \{r \mid r \text{ は有理数}\}$.
- $\mathbb{R} = \{x \mid x \text{ は実数}\}$.
- $\mathbb{C} = \{x \mid x \text{ は複素数}\}$.

2　環論からの準備

まずは, 数と多項式の類似について考えて p 進数というものを導入するモチベーションについて触れるとともに, 環論的な視点でこの類似についてみていきます. ただ p 進数を導入するための最低限のまとめ $(+\alpha)$ という感じなので, イデアルという基本的な対象についても書いてないですし, しっかり環論自体を勉強したい方は代数学の教科書をいろいろ見てみてください.

2.1　数と多項式の類似

まず, 高校までの数学ではいろんな計算をしてきたと思いますが, よくよく振り返ると, 大体は四則演算 (足し算, 引き算, 掛け算, 割り算) と, ベクトルであればスカラー倍という演算がありました. ここでは, 特に数と多項式の類似について考えてみたいと思います. まず, これらはどちらも足し算と掛け算が当たり前に出来ました (現代的には環になると言えます). そして, 整数では素因数分解が一意的にできるという性質がありましたが, 多項式でも, (細かいことを気にする方は係数は体と思ってください) 既約多項式の積には一意的に分解できるという意味では, このあたりに着目しても似た性質があると言えます (現代的にはどちらも一意分解整域であるということですね). 係数を複素数体 $\mathbb{C}$ とすれば, (代数学の基本定理というやつから) 任意の (定数でない) 多項式は 1 次式の積に分解できるので, $X-\alpha$ $(\alpha \in \mathbb{C})$ という多項式が" 素数" と思えるわけですね. 例えば,

$$X^2+1=(X+i)(X-i),\ X^3-1=(X-1)(X-\omega)(X-\omega^2)$$

(ただし $\omega=\dfrac{-1+\sqrt{3}}{2}$) というような感じです. 素因数分解っぽさがありますね.

そしてもう少し整数と多項式の似てるポイントとして, 整数も多項式も分数を考えられるというところがあります (わかる方向けにですが, つまり商体のことで, $\mathbb{Q}$ とか $\mathbb{C}[X]$ のことです). この類似点についても抽象代数学の言葉で記述できるわけですね. この先の節

では上で見た整数と多項式の類似を環論の言葉で書き換えていきます.

2.2 環と整域と体

上で見たように, 足し算と掛け算が大体普通にできることを要請するのが環という代数的な対象になります. 一応定義をしておきますが, 別にわかったと思えなくても抽象代数学をやるわけではないので, 気にせず先に進んでもらえたらと思います.
(わかっている方向けの注意として, ここでは環と言ったら乗法単位元 1_R を持つ可換環であるということです.)

定義 2.1: 環

空でない集合 R に対して, 演算 $+ : R \times R \to R$ と $\cdot : R \times R \to R$ があって, 次を満たすとき, 組 $(R, +, \cdot)$ を環という.

1. 任意の $a, b, c \in R$ に対して, $(a + b) + c = a + (b + c)$.
2. ある $0_R \in R$ があって, 任意の $a \in R$ に対して, $a + 0_R + 0_R + a = a$.
3. 任意の $a \in R$ に対して, ある $b \in R$ があって, $a + b = b + a = 0_R$.
4. 任意の $a, b \in R$ に対して, $a + b = b + a$.
5. 任意の $a, b, c \in R$ に対して, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
6. ある $1_R \in R$ があって, 任意の $a \in R$ に対して, $a \cdot 1_R = 1_R \cdot a = a$.
7. 任意の $a, b, c \in R$ に対して, $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$.
8. 任意の $a, b \in R$ に対して, $a \cdot b = b \cdot a$.

皆さんが高校くらいまででやってきた対象では大体こんな感じのことが当たり前にできたわけですが, その当たり前を要請するのが環と言えます. そして, 数や多項式ではなくて, 足し算や掛け算ができることから何が言えるかということを考えていきます. でも, 例えばベクトルでは” 掛け算” というのはできなかったはずで (内積や外積というものはありますが), これらの公理を満たしません. つまりここでは最低限できてほしい足し算と掛け算ができることに注目しているわけですね. 考えたい演算が違うだけで, もちろんベク

トルも大事な数学的な対象です.

そしていくつか注意として, 普通環と言ったら演算は明らかなケースが多いので, 単に R を環と呼ぶことがほとんどで, ここでもそのように言うことにします. また, 0_R や 1_R は一意的に存在します. こういうのは環論の授業の最初の方にやらされると思うんですが, そこまで細かいことがしたいわけでもないので, 具体例で納得してもらうくらいでいいと思います.

また, もう一つ" 当たり前" を要請します. 上の分数の話をするときや, 環の具体例を見るときに登場します. これも当たり前に成り立ってほしいし, そんなような気がするかもしれませんが...

定義 2.2: 整域

R を環とする. 任意の $a, b \in R$ に対して, $a \neq 0$ かつ $b \neq 0$ なら, $a \cdot b \neq 0_R$ が成り立つとき, R を整域という.

ではどんな集合が環になるかというと, 当然上で見た整数や多項式は環になります. また, 今回の主題である p 進整数というものも環 (もっというと整域) になります.

例 2.1: 環

1. 整数全体 $\mathbb{Z}$ は普通の足し算と掛け算に関して環になる.
2. 有理数の集合 $\mathbb{Q}$ や, 複素数の集合 $\mathbb{C}$ を係数とする多項式全体は, 多項式の和と積で環になる.

蛇足かもしれませんが多項式環について, たとえば係数を $\mathbb{Q}$ とすると,

$$(X^2 + X + 1) + (-X + 1) = X^2 + 2,\ (X + 1)(X - 1) = X^2 - 1$$

みたいな和と積を考えるということです.

次に, 何も説明してないんですが, p 進整数環も紹介だけしてみます.

例 2.2: p **進整数環**

$\mathbb{Z}_p \coloneqq \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \mid \forall m \leq n,\ x_n \bmod p^m = x_m\}$ は環.

ここで, 上で書いた $\mathbb{Z}/p^n\mathbb{Z}$ というやつが, 大体 $\mathrm{mod}p^n$ の世界を考えることになるんですが, これを正当化するのは長くなって面倒 (剰余環というやつです. 興味があれば調べてみてください) なので, $\mathbb{Z}/p^n\mathbb{Z}$ をただの記号と思って, 普通に足し算と掛け算を考えます. 一般に合同式の演算は p^n だけでなく正の整数でできたので, その形で紹介します.

例 2.3: $\mathbb{Z}/m\mathbb{Z}$

m を正の整数とする, このとき, $\mathbb{Z}/m\mathbb{Z}$ という集合を, $\overline{0}, \overline{1}, \cdots, \overline{m-1}$ という数からなるものとし, 各 $\overline{i}$ $(0 \leq i \leq m-1)$ は m で割った余りが同じものをひとまとまりにしている (同値類というやつです). このとき, 演算を

$$\overline{a} + \overline{b} \coloneqq \overline{a+b}$$

$$\overline{a} \cdot \overline{b} \coloneqq \overline{a \cdot b}$$

とすることで環になる.

まあ普通にできてほしい計算が普通にできたので環になることはまあいいでしょう. ここで, $\mathbb{Z}/m\mathbb{Z}$ は常に整域となることはないことに注意です. たとえば $m = 6$ のとき, $\overline{2} \cdot \overline{3} = \overline{0}$ というようなことが成り立ちます. 0 でないもの同士をかけて 0 になることはあるんですね. ($m = p^n$ でも, $n \geq 2$ なら整域ではないですが, $\mathbb{Z}_p$ は整域になります.)

そして, 環では足し算 (と引き算) と掛け算は普通にできたわけですが, 割り算は一般にはできません. というのも, たとえば $\mathbb{Z}$ では $1 \div 2 \notin \mathbb{Z}$ というように, 演算で" 閉じてない" わけです. ですが有理数など, 割り算 (よって四則演算) が普通にできる数もあるわけで, これを体と言います.

定義 2.3: 体

環 R の任意の 0 でない元 a に対して, ある $b \in R$ があって, $a \cdot b = b \cdot a = 1_R$ が成り立つとき, R を体という.

この b も a に対して一意的に存在することがわかるので a^{-1} とも書きます. また, 体は一般的には文字 K や L で表されることが多いです.

例 2.4: 体

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ などは体.
2. K を体として, $K(X) = \left\{ \dfrac{f(X)}{g(X)} \mid f(X), g(X) \in K[X],\ g(X) \neq 0 \right\}$ という集合も, 普通の演算で体になる (有理関数体と言います).
3. これも紹介だけになりますが, p 進数体 $\mathbb{Q}_p$ というものがあります.

2.3 素元分解

そして次に, 数と多項式の類似で見た, 素数っぽい数についての話をします. まず普通の素数がもってた性質について振り返って, 素元と既約元というものを定義して, 一意分解整域というものを定義します.

例えば, $a, b \in \mathbb{Z}$ として, ab が p の倍数であるなら a か b のどちらかが p の倍数です. また, $p = ab$ と書けているとすると, a か b は ± 1 になりますね. このあたりは大学入試の数学でもよく使うと思うんですが, 一般の環ではこれらは同値とは限りません. ただ $\mathbb{Z}$ や $K[X]$ (K は体) なんかだと同じものとなってしまうので一応定義はわけておきますが, 最初は同じものと思っていただいてもいいかもしれません.

定義 2.4: 素元

R を環, $p \in R$ とする. $a, b \in R$ に対して, $p \mid ab$ なら, $p \mid a$ または $p \mid b$ が成り立つとき, p を素元という.

$p \mid a$ とは, ある $q \in R$ があって, $a = pq$ が成り立つことを言います. このあたりから掛け算の $\cdot$ も省略していくと思います.

定義 2.5: 既約元

R を環, $p \in R$ とする. $a, b \in R$ に対して, $p = ab$ なら a または b が単元となるとき, p を既約元という.

単元というのは, $\mathbb{Z}$ での ± 1 みたいなやつで, ” 素因数分解” をしたいときに邪魔になるやつというイメージです. ちゃんとやるならその環の中で乗法逆元を持つもののことを言います. そして, R の単元全体の集合に $R^\times$ という記号を使います (Hensel の補題の証明とかで使ってます).

例 2.5: 素元, 既約元

1. $\mathbb{Z}$ では p を素数として, $\pm p$ が素元であり, 既約元でもある.
2. $\mathbb{C}[X]$ では, $\alpha \in \mathbb{C}$ として, $X - \alpha$ という多項式は素元であり既約元.
3. $\mathbb{R}[X]$ では, $\alpha \in \mathbb{R}$ として, $X - \alpha$ も, $X^2 + 1$ なんかも素元であり既約元.
4. $\mathbb{Q}[X]$ では n を 2 以上の整数として, $X^n - 2$ とかも素元であり既約元.

素元と既約元に関しては次のことが知られていて, 紹介だけします. 証明は一般的な代数学の教科書に書いてあると思うので, 興味がある方は探してみるか自力で証明してください.

命題 2.1

R を整域とすると, 任意の R の素元は既約元.

つまり, 素元であることの方が少し条件として強いということですね. 逆に既約元ならば素元であるかということも気になるわけですが, これは一般の環では No で, 一意分解整域という環であれば成り立ちます. $\mathbb{Z}$ も $K[X]$ (K は体) も一意分解整域なので問題なく同値性が従います.

定義 2.6: 一意分解整域

R を整域として, $x \in R$ は 0 でも単元でもないとする. このとき, ある素元 $p_1, \cdots p_r$ があって, $x = p_1 \cdots p_r$ と書けるとき, R は素元分解整域であるという. また, このような分解があれば” 一意的” なので一意分解整域ともいう.

つまり素因数分解っぽいことができる環ということです. ” 一意的” というのは, 整数でいうところの ± 1 倍みたいなものの差を無視して一意ということで, たとえば, $15 = 3 \cdot 5 = (-3) \cdot (-5)$ などというのは同じ分解とみなすということです.

つまり, 整数と多項式は素元分解整域という意味で同じなんですが, もっと強く, ” 割り算” のようなことができたはずで, Euclid 整域というやつにもなっています. たとえば, $15 \div 4 = 3$ 余り 3, つまり $15 = 4 \times 3 + 3$ というような計算だったり, $\mathbb{Q}[X]$ で, $(X^3 + X + 1) \div X = (X^2 + 1)$” 余り”1, つまり $X^3 + X + 1 = X(X^2 + 1) + 1$ というような計算のことです. 割り算ができるなら確かに結構似ている感じがしますね.

例 2.6: 素元分解整域

1. $\mathbb{Z}$ は当然素元分解整域.
2. K を体として, $K[X]$ も素元分解整域.
3. p 進整数環 $\mathbb{Z}_p$ も素元分解整域 (紹介だけ).

このあたりの話は p 進数とかはあまり関係ないんですが, 普通に環論をやるときには知っておくべきことという感じなので, ここらへんで難しいと感じるところがあっても雰囲気で読み進めていただけたらと思います.

2.4 商体

” 素因数分解” に関する話は一旦終わりにして, 次は $\mathbb{Z}$ と $\mathbb{Q}$ の関係や, 多項式環 $\mathbb{C}[X]$ と有理関数体 $\mathbb{C}(X)$ の関係性についてのお話をします.

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$$

$$\mathbb{C}(X) = \left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in \mathbb{C}[X], g(X) \neq 0 \right\}$$

という式を見るとめちゃくちゃ似てるのがわかりますね. こんな感じのものを一般化したいんですが, ちゃんとやるのは書くのが面倒なのと, そんなに紙面を割きたくないので必要最小限の形で定義します. しっかりやりたい方はこれまた代数学の教科書を見てみてください.

R を整域として, 考えたいのは分数っぽいものなので, $x, y \in R$ $(y \neq 0_R)$ として, $\frac{x}{y}$ を正当化できればいいわけですが, これはたとえば $\mathbb{Q}$ で $\frac{1}{2} = \frac{3}{6}$ であるように, 一般の整域でも $\frac{x}{y}$ と $\frac{x'}{y'}$ $(y, y' \neq 0_R)$ は $xy' = x'y$ が成り立つときに同じ元と思ってやれば, 特に問題はありません. つまり集合論を知っている方向けの説明ですが, この分数の形の元は同値類になっています (剰余環の話のときにも出てきたやつです). もっというっと, 分母は一般に積閉集合というやつであればなんでもよくて, 整域 R では $R \setminus \{0\}$ がとってこれるということです. そして, あとでまたちゃんとやりますが, p 進整数環 $\mathbb{Z}_p$ に対して, 同じような操作をすることで p 進数体 $\mathbb{Q}_p$ を作ります.

興味がある方向けにもう少し軽く触れます (興味なければ次の節に進んでもらった方がいいと思います). ただここだけは集合論の知識をいくらか仮定します. 集合論を知らない方も先に進んでもらった方がいいかもしれません.
まず, $S \subset R$ が積閉集合であるというのは $1_R \in S$ で, $a, b \in S$ なら $ab \in S$ であるようなもの (文字通り積で閉じてるもの) を言います. そして, $R \times S$ 上の同値関係 $\sim$ を上のよ

うに定め (ここでも R は整域としています), $S^{-1}R := R \times S/\sim$ と定義します. そして, 組 $(r,s) \in R \times S$ の同値類を $\frac{r}{s}$ と書けばいいわけです. そしてこの商集合に, 足し算は通分みたいな演算を, 掛け算は普通に分母分子の積で演算をいれると well-defined になって, 一般には整域になり, さらに, $S = R \setminus \{0\}$ のとき (これが積閉集合になっているのは R が整域だからです) は体になることがわかり, 商体と呼びます. 一般に $S^{-1}R$ は R を含む (単射があるという意味で) ので, このような操作で環 R からいい感じに大きな環が作れるということがわかります.

2.5 数と多項式の類似 part2

一旦抽象的な環論の話は終わりにして, また数と多項式の類似の話に戻ります. ここでは, 類似点もそうですが, やっぱり数と多項式というものは直感的には別物なわけで, そのあたりについても考えていきたいと思います. これでそろそろ p 進数が考えたくなってこれそうです.

例えば, 多項式 $P(X) \in \mathbb{C}[X]$ をとると, $P(X) = \sum_{i=0}^{n} a_i X^i$ $(a_i \in \mathbb{C})$ というような表示を持ち, 適当に" 平行移動" をすることで, $P(X) = \sum_{i=0}^{n} b_i (X-\alpha)^i$ $(b_i \in \mathbb{C})$ とできます. ここで, $X - \alpha \in \mathbb{C}[X]$ は素元になっています ($\mathbb{R}[X]$ や $\mathbb{Q}[X]$ などでも同様です). この表示について, 整数での類似を考えると, $n \in \mathbb{N}$ について, $n = \sum_{i=0}^{m} c_i p^i$ $(c_i \in \{0, 1, \cdots, p-1\})$ みたいなものであるべきですね. つまり, こう見ると普段の生活で当たり前に使う 10 進法の世界というのは少し変な感じがするわけです. そして p 進数という数は, 大体 $\sum_{i=0}^{\infty} a_i p^i$ というような数のことです. このままでは普通に考えれば無限大に発散してしまいますが, 適切に" 距離" を考えることで問題なく扱えます. 詳しくは 4 章でやります.

高校でもやったと思いますが, $x \in \mathbb{R}$ くらいとして, こんな式

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i$$

について考えると, $|x| < 1$ なら収束し, $|x| > 1$ なら発散してしまうというような問題がありました. 有理関数でも同様に,

$$\frac{1}{1-X} = 1 + X + X^2 + \cdots$$

という式は細かいことを気にしなければ成り立ってほしいわけですが, その細かいこととというのは主に収束するかどうかという話で, このような表示を正当化するのがべき級数で, この例では, $\mathbb{C}(X)$ を $\mathbb{C}((X))$ (Laurant 級数環というやつです) に埋め込んでいると言えます.

2.6 形式的ベキ級数環

というわけで, 形式的ベキ級数というものを導入します. これは適当な演算を考えることでまた環になります.

定義 2.7: 形式的ベキ級数環

R を環として, 形式的な無限和 $f(X) = \sum_{i=0}^{\infty} a_i X^i$ $(a_i \in R)$ 全体を $R[\![X]\!]$ と書く.

さらに, $f(X) = \sum_{i=0}^{\infty} a_i X^i$, $g(X) = \sum_{i=0}^{\infty} b_i X^i$ $(a_i, b_i \in R)$ に対して, 和と積を,

$$f(X) + g(X) := \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

$$f(X) \cdot g(X) := \sum_{i=0}^{\infty} (\sum_{j=0}^{i} a_j b_{i-j}) X^i$$

と定めることで環になり, これを形式的ベキ級数環という.

掛け算の定義がちょっとややこしいかもしれませんが, 普通の多項式と同じように, 次数を見て計算すれば自然であるとわかります. ちゃんと書くと少し仰々しい見た目になってしまいますね. べき級数環の p 進類似ともいうべきものが p 進数で, $\sum_{n=1}^{\infty} a_n p^n$ というよ

うな数を p 進数と思いたくて, これも直感的にはベキ級数環に似ているんですが, p 進数はこの表示がちゃんと収束するように意味を持たせるという意味でも厳密にはちょっと違うことに注意です. これが p 進展開というものによる p 進数の定義につながるんですが, これは演算で繰り上がりを考えたり面倒なことが多くて, 次章ではこのあたり不便がないように射影極限というものを使って p 進数を定義します.

3　p 進数

これでようやっと p 進数が導入できます．長くなってしまってすみません．p 進数は同値な定義がいろいろあって，p 進展開や，p 進距離で $\mathbb{Z}$ や $\mathbb{Q}$ を完備化したり，自分がセミナーで読んでいる本 ([1]) では，射影極限というもので $\mathbb{Z}_p$ を定義して，その商体として $\mathbb{Q}_p$ を定義していました．p 進展開は直感的にはわかりやすいかもしれませんが，ちゃんと数学的にやるのは面倒なので，射影極限としての定義を紹介します．距離空間の完備化としての定義もあるんですが，この記事の公開までに時間がないのと，演算が同値類を考えるという意味でまあまあ面倒なのでカットさせていただきます．[4] なんかではこのあたりの話が書いてあったので興味があれば読んでみてください．

3.1　環 $\mathbb{Z}_p$，体 $\mathbb{Q}_p$ の定義

射影極限は最初は慣れないかもしれませんが，演算を考えるときはこれがわかりやすく記述できます．まずは射影系というものを定義して，射影系に対して射影極限というものが定義されます．$\mathbb{Z}/p^n\mathbb{Z}$ の射影極限として $\mathbb{Z}_p$ を定義して，その商体として $\mathbb{Q}_p$ を定義します．

定義 3.1: 射影系

$\{X_n\}_{n\in\mathbb{N}}$ を環の族とする．$m, n \in \mathbb{N}$ は $n \leq m$ を満たすとき，環の準同型写像 $\varphi_{nm} : X_m \to X_n$ があるとする．このとき，以下を満たす組 $(X_n, \varphi_{nm})_{n\leq m}$ を射影系という．

1. 任意の $n \in \mathbb{N}$ に対して，$\varphi_{nn} = \mathrm{id}_{X_n}$.
2. 任意の $k \leq l \leq m \in \mathbb{N}$ に対して，$\varphi_{km} = \varphi_{kl} \circ \varphi_{lm}$.

そういえば，環論の準備を本当に必要最低限くらいでしたのでまだ説明をしてないんですが，環の準同型写像というのは，R と S を環として，$f : R \to S$ であって，任意の $x, y \in R$ に対して $f(x + y) = f(x) + f(y)$, $f(x \cdot y) = f(x) \cdot f(y)$, $f(1_R) = 1_S$ が成り立

つようなもので, よく言われるのは演算を保つような写像というところで, 基本的には環の間の写像といったら準同型写像しか考えないです.

少し最初は難しく感じると思われることが続きますが, なんとか読み進めてもらいたいです. 射影極限も抽象的な形で定義しておきます.

定義 3.2: 射影極限

射影系 $(X_n, \varphi_{nm})_{n\leq m}$ が与えられたとき, その射影極限を,

$$\varprojlim(X_n, \varphi_{nm}) \coloneqq \{(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} X_n \mid \forall n \leq m,\ \varphi_{nm}(x_m) = x_n\}$$

と定義し, 射影系 $(X_n, \varphi_{nm})_{n\leq m}$ の射影極限といい, これは成分ごとの和と積で再び環になる.

ここで, $X_n = \mathbb{Z}/p^n\mathbb{Z}$ として, $\varphi_{nm} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ を, $x \mod p^m \mapsto x \mod p^n$ という写像であるとしたとき, これは射影系になり, この射影系の射影極限を $\mathbb{Z}_p$ と書いて, p 進整数環といいます. ただ別にこの場合, となりあう番号で mod をとればいいだけなので, 単に φ_n と書いたら, $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$; $x \mod p^{n+1} \mapsto x \mod p^n$ とすることにすると,

$$\cdots \to \mathbb{Z}/p^{n+1}\mathbb{Z} \xrightarrow{\varphi_n} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_2} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\varphi_1} \mathbb{Z}/p\mathbb{Z}$$

が射影系をなすと言えます. ただ単に mod の p ベキでで落ちてくるだけという感じですが, 無限大の側から降りてくる感じが最初は慣れないかもしれません.

一旦次の主張を認めて, p 進付値というものを定義して, $\mathbb{Z}_p$ の商体 $\mathbb{Q}_p$ を定義します. 群とかなんとかいってるのは別にわからなくても大丈夫ですが, 一般に環の単元全体は乗法に関して群になります.

命題 3.1

1. $\mathbb{Z}_p$ の元 x が可逆であるための必要十分条件は, x が p の倍数とは異なること.
2. $\mathbb{Z}_p$ の単元全体からなる群を U と表すと, 任意の $0 \neq x \in \mathbb{Z}_p$ に対して, $x = p^n u$ となる $n \geq 0$ と $u \in U$ が存在する.

1 番の主張については, $x = (x_n)_{n\in\mathbb{N}}$ としてときに, $x_1 \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ ということです.

そしてこの命題の 2 番の n のことを p 進付値といいます.

定義 3.3: p 進付値

$0 \neq x \in \mathbb{Z}_p$ に対して, ある $n \in \mathbb{Z}_{\geq 0}$ と $u \in U$ を用いて, $x = p^n u$ と書けて, この n のことを x の p 進付値といい, $v_p(x)$ と書く.

任意の $\mathbb{Z}_p$ に対して付値を定義するため, $v_p(0) \coloneqq +\infty$ とします. まとめると, $v_p : \mathbb{Z}_p \to \mathbb{Z}_{\geq 0} \cup \{+\infty\}$ ということです.) また, 詳しくは省きますが, 定義より

$$v_p(xy) = v_p(x) + v_p(y),$$

$$v_p(x+y) \geq \inf(v_p(x), v_p(y))$$

がわかります. ここから, $\mathbb{Z}_p$ が整域であることがわかるので商体が定義できます.

定義 3.4: p 進数体

p 進整数環 $\mathbb{Z}_p$ の商体を $\mathbb{Q}_p$ と書いて p 進数体という.

普通に元を書き下すと,

$$\mathbb{Q}_p = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}_p,\ b \neq 0 \right\}$$

となってよくわからない気がするんですが, $0 \neq x \in \mathbb{Q}_p$ は $x = \dfrac{a}{b}$ とすると, $a, b \in \mathbb{Z}_p \setminus \{0\}$ だから, $a = p^n u$, $b = p^{n'} u'$ $(n, n' \in \mathbb{Z}_{\geq 0}, u, u' \in U)$ と表せるので, $x = p^{n''} u''$ $(n'' \coloneqq n - n' \in \mathbb{Z}, u'' \coloneqq u \cdot (u')^{-1} \in U)$ と表せます (正確には $\mathbb{Q}_p$ の元は同値類なんで

すが, このあたりの話が同値類の取り方に依らないことも普通にわかります). そして再びこの n'' を x の p 進付値といい, $\tilde{v}_p(x)$ と書きます.
(細かいですがこのとき, $\mathbb{Z}_p \hookrightarrow \mathbb{Q}_p$; $x \mapsto \dfrac{x}{1}$ で $\mathbb{Z}_p$ は $\mathbb{Q}_p$ の部分環と見て, $\tilde{v}_p|_{\mathbb{Z}_p} = v_p$ がわかります.)

3.2 $\mathbb{Z}_p$, $\mathbb{Q}_p$ の性質

駆け足になってしまったところもありますが, とりあえず $\mathbb{Z}_p$ と $\mathbb{Q}_p$ が定義できたので, これらに関していくつかの性質を見ていきます. 環論的な性質から位相的な性質まで様々です.

その前に, まずはこの後よく使うであろう記号をまとめます.

Notation:

1. $x, y \in \mathbb{Z}_p$ に対して, $x - y \in p^n\mathbb{Z}_p$ のとき, $x \equiv y \pmod{p^n}$ と書く.
2. $A_n \coloneqq \mathbb{Z}/p^n\mathbb{Z}$ と書く.

そしてここからは公開まで時間がないのでセミナー発表用に用意した資料を結構そのまま貼り付けます. 知らない知識等もあるかもしれないんですが, あくまで読み物として楽しく読んでもらえたらと思います. よくわかんない証明は主張だけ認めて適当に読み飛ばすことを推奨します. 最悪全部飛ばして Hensel の補題の方に進んでもらってもいいかもしれません. あと時間がないのでそんなに順番は意識できてないですが, 最初の方に環論的な性質を, 後半の方に位相的な性質をまとめました.

まず, $a \in \mathbb{Z}$ と, $(\cdots, \pi_n(a), \cdots, \pi_1(a))$ ($\pi_n : \prod_{n\in\mathbb{N}} A_n \to A_n$ は射影) を同一視できて, $\mathbb{Z}$ を $\mathbb{Z}_p$ の部分環とみなせる.

次に, $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ を主張する命題から. 写像 $p^n : \mathbb{Z}_p \to \mathbb{Z}_p$ を, 元 $x = (\cdots, x_{n+1}, x_n, \cdots, x_1)$ に $p^n x = (\cdots, p^n x_{n+1}, 0, \cdots 0)$ を対応させる写像 (つまり各成

分 p^n 倍) とすると, これは加法群の準同型になっている. $\varepsilon_n : \mathbb{Z}_p \to A_n$ を, $\mathbb{Z}_p$ の元 $x = (\cdots, x_n, \cdots, x_1)$ に, 第 n 成分 $x_n \in A_n$ を対応させる写像とすると, 次が成り立つ.

命題 3.2

以下は abel 群の完全系列 :

$$0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0.$$

Remark: この命題より, $\mathbb{Z}_p/p^n\mathbb{Z}_p$ と $A_n = \mathbb{Z}/p^n\mathbb{Z}$ を同一視できる. これは一般に群の完全系列

$$0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$$

があったとき, g: 全射, f: 単射と, $\ker(g) = \mathrm{Im}(f)$ と準同型定理より, $G/\ker(g) = G/\mathrm{Im}(f) \cong G/G' \cong G''$ が言えるので, $G = G' = \mathbb{Z}_p$, $G'' = A_n$ とすればわかる. あくまで加法群としての同型しか言えてないことに注意.

再掲

命題 3.3

1. $\mathbb{Z}_p$ の元 x が可逆であるための必要十分条件は, x が p の倍数とは異なること.
2. $\mathbb{Z}_p$ の単元全体からなる群を U と表すと, 任意の $0 \neq x \in \mathbb{Z}_p$ に対して, $x = p^n u$ となる $n \geq 0$ と $u \in U$ が存在する.

1 については, 前の命題の結果から, $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ で, 特に $n = 1$ とすると, $p\mathbb{Z}_p$ は $\mathbb{Z}_p$ の極大イデアルとわかる. そしてこの命題より, $\mathbb{Z}_p$ は極大イデアルが $p\mathbb{Z}_p$ の局所環とわかる.

Proof. 1 は, まず, $x \in A_n$ については普通に A_n が $(p) = pA_n$ を唯一の極大イデアルとする局所環であることから従うので, そこから $\mathbb{Z}_p$ についても同様のことが言えることを示す.
($\Rightarrow$) の方は簡単で, $x \in \mathbb{Z}_p$ が可逆元とすると, ある $y \in \mathbb{Z}_p$ があって, $xy = 1 =$

$(\cdots, 1, \cdots, 1)$ が成り立ち, 特に $x_1 y_1 = 1$ in $A_1 = \mathbb{F}_p$ だから $x_1 \neq 0$ で, $x \notin p\mathbb{Z}_p$.
$(\Leftarrow)$ の方は, $x = (x_n) \in \mathbb{Z}_p$ として, $x_1 \neq 0$ なら $x_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ で, 任意の $n \in \mathbb{N}$ について, $x_n \equiv x_1 \pmod{p}$ が成り立つ. $x_n \notin p\mathbb{Z}/p^n\mathbb{Z}$ なので, $x_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. したがって, $x_n y_n = 1$ in A_n となる y_n が存在. 任意の $n \in \mathbb{N}$ に対して, $\varphi_{n+1}(y_{n+1}) = \varphi_{n+1}({x_{n+1}}^{-1}) = (\varphi_{n+1}(x_{n+1}))^{-1} = (x_n)^{-1} = y_n$ なので, $y = (y_n) \in \mathbb{Z}_p$.

2 を示す. まず, $\mathbb{Z}_p$ の可逆元全体が群をなすのは簡単に確認できる (一般に環 A の単元全体は乗法に関して群になる). $0 \neq \forall x \in \mathbb{Z}_p$ をとると, $\varepsilon_m(x) = x_m = 0$ となる m のうち最大のもの (n とする) がある. このとき, $x = (\cdots, x_{n+1}, 0, \cdots, 0) = p^n u$ $(u \in \mathbb{Z}_p^\times = U)$ と書けて, u は p の倍数ではないから, 1 より $u \in U$. この分解が一意であることは, $p^n u = p^{n'} u'$ $(n, n' \in \mathbb{Z}_{\geq 0},\ u, u' \in U)$ とすると, $n < n'$ なら, $p^n u = p^n (p^{n'-n} u')$ となるが, p^n は単射だったので $u = p^{n'-n} u'$ で, 両辺に $(u')^{-1}$ をかけると, $(\mathbb{Z}_p)^\times \ni (u')^{-1} u = p^{n'-n}$ となり矛盾. よって $n = n'$ で, $p^n u = p^n u'$ だが, 再び Prop.1 より, p^n は単射なので $u = u'$. □

次に位相的な性質を見る. $\mathbb{Z}_p$ に入る位相について, 各 A_n に離散位相をいれると, $\prod_{n\in\mathbb{N}} A_n$ には, 直積位相が入る. $\mathbb{Z}_p$ には直積 $\prod_{n\in\mathbb{N}} A_n$ に相対位相をいれることで, 直積空間の部分空間と思える. この位相空間を $(\mathbb{Z}_p, \mathcal{O}_p)$ とする.

命題 3.4: $\mathbb{Z}_p$ の位相的性質

$\mathbb{Z}_p$ は Hausdorff かつコンパクトな位相空間.

Proof. まず, $\mathbb{Z}_p$ が Hausdorff なのは, 各 A_n が Hausdorff で, その直積 $\prod_{n\in\mathbb{N}} A_n$ も Hausdorff, さらにその部分空間も Hausdorff なのでよい.
次にコンパクト性について, 一般の位相空間の射影系 $(X_i, \varphi_{ij})_{i\in I}$ (ただし, 各 X_i は有限集合としておく) で考えて, 以下の流れで示す:

1. 各 X_i がコンパクトなら $\prod_{n\in\mathbb{N}} X_i$ はコンパクト.

2. $X_{ij} \coloneqq \{x \in \prod X_i \mid p_i(x) = \varphi_{ij} \circ p_j(x)\}$ (ただし, $p_i : \prod X_i \to X_i$ は自然な射影) とすると, これは閉集合.
3. $\varprojlim X_i = \bigcap_{i \leq j} X_{ij}$ だからこれは $\prod_{i \in I}$ の閉集合で, コンパクト空間の部分空間なのでコンパクト.

1. 各 X_i がコンパクトなら, Tychonoff の定理よりコンパクト空間の直積はコンパクトなので, $\prod_{i \in I} X_i$ はコンパクト.
2. まず, 射影 p_i, p_j は連続, φ_{ij} は射影系の定義より連続で, 合成 $\varphi_{ij} \circ p_j$ も連続. 一般に, $f, g : X \to Y$ は位相空間の連続写像で, Y が Hausdorff のとき, $Z \coloneqq \{x \in X \mid f(x) = g(x)\}$ は X の閉集合であることがわかる. これより X_{ij} は閉集合がわかる.
3. ここは先に書いた通り. □

また, $\mathbb{Z}_p$ に入る位相として, $x, y \in \mathbb{Z}_p$ に対して, $d(x, y) = p^{-v_p(x-y)}$ と置けば, d は $\mathbb{Z}_p$ の距離となる. この距離から誘導される位相空間 $(\mathbb{Z}_p, \mathcal{O}_d)$ というものも考えられて, $\mathcal{O}_p$ と $\mathcal{O}_d$ は同じ位相を定めることがわかる (点 0 の基本近傍系として同じものがとってこれて, あとは平行移動).

命題 3.5

$x, y \in \mathbb{Z}_p$ に対して,

$$d(x, y) = p^{-v_p(x-y)}$$

と置けば, d は $\mathbb{Z}_p$ の距離となる. この距離から誘導される位相空間 $(\mathbb{Z}_p, \mathcal{O}_d)$ は直積の相対位相として定義した位相空間 $(\mathbb{Z}_p, \mathcal{O}_p)$ と同じ位相を定める.

Remark: あまり強調できてないかもしれませんが, これがまさに p 進数の遠近感を表していて, 二つの数の差がたくさん p で割り切れるほど近いというのが p 進数です.

Proof. まず d が距離になるのは, $d(x, y) \geq 0$ は定義からよくて, $v_p(0) = \infty$ から, $d(x, y) = 0 \Leftrightarrow x = y$ もよい. $d(x, y) = d(y, x)$ は付値に影響がないので OK. 三角不等式は, 付値の性質から, $v_p(x - z) = v_p((x - y) + (y - z)) \geq \inf(v_p(x - y), v_p(y - z))$ から

わかる.

この距離から誘導される位相空間 $(\mathbb{Z}_p, \mathcal{O}_d)$ について, $p^n\mathbb{Z}_p$ $(n \geq 0)$ は点 0 の基本近傍系であることがわかる. この位相が先ほど定義した位相空間 $(\mathbb{Z}_p, \mathcal{O}_p)$ と一致することを示す. $(\mathbb{Z}_p, \mathcal{O}_p)$ について, 点 0 の基本近傍系として, $p^n\mathbb{Z}_p$ $(n \geq 0)$ がとってこれることを言えばよい.

$$p^n\mathbb{Z}_p = \mathbb{Z}_p \bigcap \prod_{m>n} A_m \times \prod_{m\leq n} \{0\}$$

であり, $U_n \coloneqq \prod_{m>n} A_m \times \prod_{m\leq n} \{0\}$ と置くと, 示すべきは,

$$0 \in \forall V \in \mathcal{O}_p,\ \exists n\ s.t.\ U_n \cap \mathbb{Z}_p \subset V.$$

まず, $\prod_{n\in\mathbb{N}} A_n$ の開集合 O を用いて, $V = O \cap \mathbb{Z}_p$ と書ける. そして, $O \in \mathcal{O}_p$ より, $\prod_{n\in\mathbb{N}} A_n$ のある開基 B があって, $0 \in B \subset O$ となる. このとき,

$$B = \prod_{m>l} A_m \times \prod_{m\leq l} W_m\ (0 \in W_m \subset A_m)$$

であるから, $U_l = \prod_{m>l} A_m \times \prod_{m\leq l} \{0\} \subset \prod_{m>l} A_m \times \prod_{m\leq l} W_m$. すなわち

$$p^l\mathbb{Z}_p = U_l \cap \mathbb{Z}_p \subset B \cap \mathbb{Z}_p \subset O \cap \mathbb{Z}_p = V.$$

$\mathbb{Z}_p$ は位相群になるのであとは平行移動して, 点 $x \in \mathbb{Z}_p$ の基本近傍系は $x + p^n\mathbb{Z}_p$ であることがわかる. □

命題 3.6

$\mathbb{Z}_p$ は, p 進距離に関して完備で, $\mathbb{Z}$ を稠密な部分空間として含む

Proof. 上の命題より, これらの位相は等しく, 特に距離空間としてコンパクトなので完備. コンパクト距離空間が完備なのは, 任意の Cauchy 列と, その中の収束部分列がとれて (距離空間ではコンパクトと点列コンパクトが同値), 収束部分列の極限が全体の極限に一致することが示せる.

最後に, $\mathbb{Z}$ が $\mathbb{Z}_p$ で稠密であることを示す. 任意の $x \in \mathbb{Z}_p$ に対して, x に収束する $\mathbb{Z}$ の点列がとってこれればよいが, $x = (x_n)$ とすると, $y_n \in \mathbb{Z}$ として, $x_n \equiv y_n \pmod{p}$ となるようにとると, $d(x, y_n) \leq e^{-n} \to 0$. よって, x に収束する整数列 $\{y_n\}$ がとれたので, $\mathbb{Z}$ は $\mathbb{Z}_p$ で稠密. □

命題 3.7

$\mathbb{Q}_p$ は距離 $\tilde{d}(x, y) \coloneqq e^{-\tilde{v}_p(x-y)}$ を持つ局所コンパクト距離空間であり, $\mathbb{Z}_p$ はその開部分環, $\mathbb{Q}$ は $\mathbb{Q}_p$ の中で稠密.

Remark: $\mathbb{Q}_p$ がコンパクトでないのは 感覚的には負ベキが大きくなっていくとコンパクト感がなくなる. ただ局所的に見ればコンパクトっぽい.

Proof. $\mathbb{Q}_p$ が距離空間になるのは先ほどと同様.
局所コンパクトであるのは, まず, 0 のコンパクトな近傍として $\mathbb{Z}_p$ がとれるので, 0 まわりは OK. あとは $\mathbb{Z}_p$ が位相群なので平行移動すればよい.
$\mathbb{Z}_p$ が $\mathbb{Q}_p$ の開部分環になることは, $B(x, 1) \coloneqq \{y \in \mathbb{Q}_p \mid \tilde{d}(x, y) < 1\}$ とすると, $B(x, 1) \subset \mathbb{Z}_p$ となることからよい. 環になることは商体として定義したから OK(一般に環 R とその商体 K があったとき, 包含写像 $\iota : R \hookrightarrow K \ ; \ r \mapsto \dfrac{r}{1}$ は環準同型で, R と $\mathrm{Im}(\iota)$ を同一視できて, $\mathrm{Im}(\iota)$ は K の部分環).
$\mathbb{Q}$ が dense は, 任意の $x \in \mathbb{Q}_p$ に収束する $\mathbb{Q}$ の点列 $\{y_n\}$ がとってこれることを示せばよい. $x = 0$ は $y_n = 0$ とすればよく, $x \neq 0$ のとき, $x = p^n u$ $(n \in \mathbb{Z}, u \in (\mathbb{Z}_p)^\times)$ と書けて, $u \in \mathbb{Z}_p$ に収束する整数列 $\{v_n\}$ はとってこれることがわかってて, $y_m = p^n v_m$ とすれば, $d(x, y_m) \leq e^{m+n} \to 0$. □

3.3 Hensel の補題

前の節ではかなり多くの知識を仮定してしまいましたが, ここではそんなに難しいことはやりません. Hensel の補題という強力な定理 (補題という名前ですが...) を紹介します. これは, 方程式の解を考えるときには大体 mod$p$ だけを見ればいいと言っているようなも

ので, 局所環の嬉しさの一端が見れるという感じでしょうか.

定理 3.1: Hensel の補題

$F(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}_p[X]$ に対して, ある $\alpha_1 \in \mathbb{Z}_p$ があって, $F(\alpha_1) \equiv 0 \pmod{p}$, $F'(\alpha_1) \not\equiv 0 \pmod{p}$ が成り立つとする. このとき, ある $\alpha \in \mathbb{Z}_p$ があって, $\alpha \equiv \alpha_1 \pmod{p}$, $F(\alpha) = 0$ が成り立つ.

つまり, mod p で解があれば, 任意の p^n まで解を持ちあげることができるという主張です. $F'(X) \equiv 0$ という条件がよくわからない気もするんですが, 例えば $X^p = p$ という方程式の解は mod$p$ では存在しますが, $F(X) = X^p - p$ に対して, $F'(X) \equiv 0 \pmod{p}$ で持ち上げられない例になっています. Newton 法の類似であることを考えると, 確かに" 接線" が引けなくなるのでまずそうです. (Newton 法を知らなかったら無視してください.)

証明は"p 進 Newton 法" なる証明もありますが, ここでは具体的な問題を解く上でもわかりやすいと個人的に思っている構成的な証明を与えます.

Proof. $\mathbb{Z}_p$ の数列 $\{\alpha_n\}$ であって, 任意の自然数 n に対して, 以下を満たすものを構成する.

1. $F(\alpha_n) \equiv 0 \pmod{p^n}$,
2. $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$.

このような $\{\alpha_n\}$ が構成できれば, これは Cauchy 列になり, 特に $\mathbb{Z}_p$ の完備性から収束し, その極限値を α とすると, 構成法から $\alpha \equiv \alpha_1 \pmod{p}$ で, さらに $F(\alpha) = 0$ も成り立つ.
このような $\{\alpha_n\}$ は, 以下のように帰納的に構成すればよい.
まず, α_2 は, mod p で α_1 と合同であってほしいので, $\alpha_2 = \alpha_1 + b_1p$ $(b_1 \in \mathbb{Z}_p)$ という形で 1 を満たす b_1 をうまくとってこれればよい. 普通に多項式を展開しても, Taylor 展

開のようなことができることを認めてもいいが,

$$\begin{aligned} F(\alpha_2) &= F(\alpha_1 + b_1 p) \\ &\equiv F(\alpha_1) + F'(\alpha_1) b_1 p \pmod{p^2} \end{aligned}$$

が成り立つ. ここで, 仮定より $F(\alpha_1) \equiv 0 \pmod{p}$ より, ある $x \in \mathbb{Z}_p$ があって, $\alpha_1 = px$ と書ける. よって

$$F(\alpha_1) + F'(\alpha_1) b_1 p = p(x + F'(\alpha_1) b_1) \pmod{p^2}.$$

すなわち, $x + F'(\alpha_1) b_1 \equiv 0 \pmod{p}$. $F'(\alpha_1) \not\equiv 0 \pmod{p}$ だったので, $F'(\alpha_1) \in (\mathbb{Z}_p)^\times$ であり, $b_1 \equiv -x \cdot (F'(\alpha_1))^{-1}$ とすればよい.
以下, 同様に α_{n+1} を, $\alpha_n + b_n p^n$ として, 1 を満たすものがとれる. □

3.4 Hensel の補題の応用

(書ける時間がないので) そんなに多くはできないんですが, Hensel の補題を使うとこんなことが言えるんですよという話をします. 例は少ないですが Hensel の補題の威力を実感できると思います. ここでは

1. いつ $a \in \mathbb{Z}_p$ の平方根がある?
2. 1 の $(p-1)$ 乗根は常に存在する.

ということを考えます (2 つ目は証明するといった方が適切かもしれないですが). 完備化としての定義の方がここは納得しやすいかもしれませんが, このあたりの例からも $\mathbb{Z}_p$ は真に $\mathbb{Z}$ を含んでいることがわかります.

例 3.1: $\sqrt{a}$ の存在

$p > 2$, $a = (a_n) \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ とする. このとき, $x \in \mathbb{Z}_p$ であって, $x^2 = a$ を満たすものが存在するための必要十分条件は, $\left(\frac{a_1}{p}\right) = 1$ となること. ここで $\left(\frac{\cdot}{p}\right)$ は Legendre 記号である.

Proof. $F(X) = X^2 - a$ とおくと, $F'(X) = 2X$ であり, Hensel の補題の仮定を満たす $\alpha_1 \in \mathbb{Z}_p$ が存在するかを考える. 存在するとすれば, $\alpha_1 \not\equiv 0 \pmod{p}$ なので, $F'(\alpha_1) \not\equiv 0 \pmod{p}$ で, $F(\alpha_1) \equiv 0 \pmod{p}$ を満たすかどうかを考えればよいが, $\alpha_1 = (\beta_n)$ とすると, $\beta_1^2 = a_1$ が A_1 で成り立てばよく, このような β_1 が存在するのは, $\left(\dfrac{a_1}{p}\right) = 1$ のときに限る. □

例 3.2: 1 の $(p-1)$ 乗根

1 の $(p-1)$ 乗根は, 常に $\mathbb{Z}_p$ の元となる.

Proof. $F(X) = X^{p-1} - 1$ とすると大体上と同じで, Fermat の小定理を使えばこの主張は従う. □

3.5 局所大域原理

局所大域原理というのはちゃんとした定義がある言葉があるものなのかは知りませんが, たとえば方程式の $\mathbb{Q}$ での解を知りたいときに, これは一般には難しいわけですが, $\mathbb{Q}_p$ と $\mathbb{Q}_\infty := \mathbb{R}$ での方程式と思ったときに解があるかどうかを見ればいいというような主張です. 具体例で少し見て終わります.

例 3.3

$a, b \in \mathbb{Q}$ として, 方程式 $ax^2 + by^2 = 1$ に有理数解があるための必要十分条件はすべての $p \in \{2, 3, 5, \cdots, \infty\}$ に対して $\mathbb{Q}_p$ で解を持つこと.

一般には二次形式というやつで同じことが言えるみたいですが, このあたりはまだまだ自分でも勉強が足りないので紹介くらいしかできずすみません.

4　参考文献

基本的にはセミナーでは [1] を読んでいて, とにかく難しいです. あとはこの資料で, 数と多項式の類似から入ったのは [2] を読んでいたからで, この本は完備化で $\mathbb{Q}_p$, $\mathbb{Z}_p$ を定義しているはずですが, かなりわかりやすいと思います. 完備化といての定義については, [3] にも [4] にも書いてあって, どっちもわかりやすいと思います. [3] の方がちょっと読み物っぽさがあったり, 他の代数的整数論の内容も載っています. [4] は p 進解析の話が勉強できる和書という意味ではかなり貴重だと思いますし, これも結構丁寧に書いてくれている印象です. また, 射影極限については圏論の本に書いてあることが多いんですが, [5] には p 進数の話ものっていたのでおすすめです.

[1] ジャン＝ピエール・セール,『数論講義』, 彌永健一 訳, 岩波書店, 2017.

[2] Fernando Q. Gouvêa, *p-adic Numbers: An Introduction*, Springer, Universitext, 3nd edition, 2020.

[3] 加藤和也, 黒川伸重, 斎藤毅『数論 Ⅰ』, 岩波書店, 2016.

[4] ニール・コブリッツ（著）, 長岡昇勇（訳）,『p 進解析入門』, 丸善出版, 2025.

[5] 松田茂樹,『加群とホモロジー代数入門』, 森北出版, 2024