p 進整数環を構成する

りす. @riss_gendarmery

最近一部界隈で p 進に対する需要が上がっているようなのでこの機会に p 進について説明をしてみようかなと思いました. しかしながら, ただ解説するだけでは僕がつまないので Witt 環による構成法を勉強して書こうと思ったのですが, 頭の悪いことに 2 日前にデレステをダウンロードしてしまい, 時間が無限に融けてしまいました. 何とか Witt 環を構成するところまで読んだのですが, Witt 環による構成よりそれで何が得られるかが大切だと思ってしまった上に時間がないので, 申し訳ないのですが今後勉強を続けて余裕があれば advent calendar の空いている日に投稿しようと思います (するとは言ってない). 申し訳ないのですが時間が足りなかったので後で 事実 6+α を書いて上げ直そうと思います. とりあえず間に合わせで申し訳ないですがあげておきます.

この pdf 全体を通して p を素数とする. まず $n \in \mathbb{N}$ に対して (p^n) を p^n の倍数全体と定義する. つまり, $(p^n) = \{p^n x; x \in \mathbb{Z}\}$ とする.

定義 1 (p 進絶対値).
$|\cdot|_p : \mathbb{Z} \to \mathbb{R}$ を次で定義する: $n \in \mathbb{Z} \setminus 0$ が $n \in (p^m) \setminus (p^{m+1})$ であるとき $|n|_p = p^{-m}$, また $|0|_p = 0$ と定める.

この p 進絶対値は $\mathbb{Z}$ だけでなく $\mathbb{Q}$ にまで伸ばすことができるが今回はその話をしない.

補題 2.
$n_1, n_2 \in \mathbb{Z}$ に対して $|n_1 + n_2|_p \leq \max\{|n_1|_p, |n_2|_p\}$ が成り立つ. 特に $|n_1|_p \neq |n_2|_p$ であるとき, 等号が成り立つ.

証明.
$n_i \in (p^{e_i}) \setminus (p^{e_i+1})$ $(i = 1, 2)$ とする. このとき, ある p の倍数でない定数 $c_i \in \mathbb{Z}$ があって, $n_i = p^{e_i} c_i$ となる $(i = 1, 2)$. このとき $e_1 \leq e_2$ としてよい. そうすると $|n_1+n_2|_p = |p^{e_1}(c_1+p^{e_2-e_1}c_2)|_p$ となり, $c_1 + p^{e_2-e_1}c_2$ は整数であるため $|n_1 + n_2|_p \leq |p^{e_1}|_p = \max\{|n_1|_p, |n_2|_p\}$ となる.
$|n_1|_p > |n_2|_p$ であるとき, つまり $e_2 > e_1$ であるとき, $c_1 + p^{e_2-e_1}c_1$ は p の倍数でないものと p の倍数の和になるので p の倍数でなくなる. したがって等号が成立する.□

ここで距離関数の定義を復習する.

定義 3.
X を集合とする. 写像 $d(\cdot,\cdot) : X \times X \to \mathbb{R}_{\geq 0}$ が X 上の距離関数であるとは以下を満たすときを

言う: 任意の $x,y,z \in X$ に対し

(1) $d(x,y)=0 \Leftrightarrow x=y$,
(2) $d(x,y)=d(y,x)$,
(3) $d(x,z) \leq d(x,y)+d(y,z)$.

ここで p 進距離を導入しよう.

定義 & 命題 4 (p 進距離).
$d_p(n_1,n_2)=|n_1-n_2|_p$ で定めるとき, d_p は距離関数になっている. この d_p を p 進距離という.

証明.
距離関数の定義を満たすことを示す.

(1) $d_p(n_1,n_2)=0$ であることはすなわち $|n_1-n_2|_p=0$ を意味する. 定義より $n_1-n_2=0$ なので $n_1=n_2$ と同値である.
(2) 符号を変えても素因数分解にあらわれる p の冪の数は変わらないため, $d_p(n_1,n_2)=|n_1-n_2|_p=|n_2-n_1|_p=d_p(n_2,n_1)$ となる.
(3) 補題 2 より, $d_p(n_1,n_3)=|n_1-n_3|_p=|(n_1-n_2)+(n_2-n_3)|_p \leq \max\{|n_1-n_2|_p,|n_2-n_3|\}=\max\{d_p(n_1,n_2),d_p(n_2,n_3)\} \leq d_p(n_1,n_2)+d_p(n_2,n_3)$ となる.□

ここで簡単に完備化を復習をしようと思う.

定義 5.
X を集合とし, d を X 上の距離とする.

- X の点列 $(x_n)_{n=1,2,\cdots}$ が Cauchy 列であるとは, 任意の $\epsilon>0$ に対してある $N \in \mathbb{N}$ があり $n,m>N$ に対して $d(x_n,x_m)<\epsilon$ となるときを言う.
- X の Cauchy 列 $(x_n)_{n=1,2,\cdots},(y_n)_{n=1,2,\cdots}$ が同値であるとは, 任意の $\epsilon>0$ に対してある $N \in \mathbb{N}$ があり $n>N$ に対して $d(x_n,y_n)<\epsilon$ が成り立つとき言う. $(x_n)_{n=1,2,\cdots},(y_n)_{n=1,2,\cdots}$ が同値であることを $(x_n)_{n=1,2,\cdots} \sim (y_n)_{n=1,2,\cdots}$ と書く.
- X の d による完備化を $\tilde{X} := \{(x_n)_{n=1,2,\cdots};(x_n)_{n=1,2,\cdots}$は X 上の Cauchy 列である.$\}/\sim$ と定義する.

これに従って, $\mathbb{Z}$ を d_p で完備化をしたものを $\mathbb{Z}_p$ と書くことにする. この $\mathbb{Z}_p$ を p 進整数環という. 環というからには和 $+$ と $\times$ が定義されている.

事実 6.
$\mathbb{Z}_p$ の和と積を $a,b \in \mathbb{Z}_p$ と, その値を代表する Cauchy 列 $(a_n)_{n=1,2,\cdots},(b_n)_{n=1,2,\cdots}$ に対して $a+b=\lim_{n\to\infty}(a_n+b_n), ab=\lim_{n\to\infty}(a_nb_n)$ で定める. この演算に関して $\mathbb{Z}_p$ は環になっている.

p 進整数環について次が成り立つ.

命題 7.
$\mathbb{Z}_p$ の元は $\sum_{n=0}^{\infty} a_n p^n,\ (a_n = 0, 1, \cdots, p-1)$ で表される.

証明.
任意の $\mathbb{Z}$ の元は $\sum_{n=0}^{k} a_n p^n\ (a_n = 0, 1, \cdots, p-1)$ と一意に書けることに注意する. $x \in \mathbb{Z}_p$ に対して, x に収束する $\mathbb{Z}_p$ の列 $(x_n)_{n=0,1,\cdots}$ に対し, 任意の $k \in \mathbb{N}$ に対して十分大きい $N_k \in \mathbb{N}$ があって $l, m \geq N_k$ に対して

$$|x_l - x_m|_p < p^{-k} \text{ かつ } |x - x_l| < p^{-k} \tag{1}$$

となる. 始めの注意より各 k に対し $a_{N_k} = \sum_{n=0}^{s} a_{k,n} p^n$ とかける. このとき $n \leq k$ に対し $a_n = a_{k,n}$ と定める. これは (1) の前半により k の取り方によらず定まる. $A_k := \sum_{n=0}^{k} a_n p^n$ とする. $|x - A_k|_p \leq \max\{|x - x_{N_k}|_p, |x_{N_k} - A_k|_p\} < p^{-k}$ となるため, $(A_k)_{k=0,1,\cdots}$ は x に収束する. したがって $x = \sum_{n=0}^{\infty} a_n p^n\ (a_n = 0, 1, \cdots, p-1)$ と書ける.□

参考文献

[1] J. ノイキルヒ 著, 梅垣 敦紀 翻訳, 「代数的整数論」, シュプリンガー・フェアラーク東京
[2] 松坂 和夫 著, 「集合・位相入門」, 岩波書店