p-Adic Fields

Qiu Caiyong

December 22, 2022

The ring $\mathbf{Z}/p^n\mathbf{Z}$

Let p be a prime number, $n \in \mathbf{N}$ be a positive integer.
For any $x \in \mathbf{Z}$, we define

$$x + p^n\mathbf{Z} = \{x + p^n k : k \in \mathbf{Z}\}$$

This is the set of all integers with residue x modulo p^n

Example

$$2 + 3^2\mathbf{Z} = \{\dots, -16, -7, 2, 11, 20, 29, \dots\}$$

It is possible that $x_1 + p^n\mathbf{Z} = x_2 + p^n\mathbf{Z}$ while $x_1 \neq x_2$:

Theorem

We have $x_1 + p^n\mathbf{Z} = x_2 + p^n\mathbf{Z}$ if and only if $x_1 \equiv x_2 \bmod p^n$

The ring $\mathbf{Z}/p^n\mathbf{Z}$

We define the set $\mathbf{Z}/p^n\mathbf{Z}$ to be

$$\mathbf{Z}/p^n\mathbf{Z} = \{x + p^n\mathbf{Z} : x \in \mathbf{Z}\}$$

Notice that this set has exactly p^n elements.
It is possible to make this set into a ring by defining the addition and multiplication as the following:

$$(x_1 + p^n\mathbf{Z}) + (x_2 + p^n\mathbf{Z}) = (x_1 + x_2) + p^n\mathbf{Z}$$

$$(x_1 + p^n\mathbf{Z})(x_2 + p^n\mathbf{Z}) = (x_1x_2) + p^n\mathbf{Z}$$

So $\mathbf{Z}/p^n\mathbf{Z}$ is a finite ring, and it is a field if and only if $n = 1$.

Review of some important homomorphisms

We've defined some important ring homomorphisms:

$$\begin{aligned} \beta_n : \mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}, &\quad \beta_n(x) = x + p^n\mathbf{Z} \\ \beta_n^m : \mathbf{Z}/p^m\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}, &\quad \beta_n^m(x + p^m\mathbf{Z}) = x + p^n\mathbf{Z} \\ \phi_n : \mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}/p^{n-1}\mathbf{Z}, &\quad \phi_n(x + p^n\mathbf{Z}) = x + p^{n-1}\mathbf{Z} \end{aligned}$$

These ring homomorphisms barely do anything. And automatically we have

$$\left(\mathbf{Z} \xrightarrow{\beta_m} \mathbf{Z}/p^m\mathbf{Z} \xrightarrow{\beta_n^m} \mathbf{Z}/p^n\mathbf{Z}\right) = \left(\mathbf{Z} \xrightarrow{\beta_n} \mathbf{Z}/p^n\mathbf{Z}\right)$$

$$\left(\mathbf{Z}/p^l\mathbf{Z} \xrightarrow{\beta_m^l} \mathbf{Z}/p^m\mathbf{Z} \xrightarrow{\beta_n^m} \mathbf{Z}/p^n\mathbf{Z}\right) = \left(\mathbf{Z}/p^l\mathbf{Z} \xrightarrow{\beta_n^l} \mathbf{Z}/p^n\mathbf{Z}\right)$$

Definition of p-adic integers

$$\cdots \xrightarrow{\phi_5} \mathbf{Z}/p^4\mathbf{Z} \xrightarrow{\phi_4} \mathbf{Z}/p^3\mathbf{Z} \xrightarrow{\phi_3} \mathbf{Z}/p^2\mathbf{Z} \xrightarrow{\phi_2} \mathbf{Z}/p\mathbf{Z}$$

Definition (p-adic integer)

A p-adic integer is a infinite list

$$(x_1, x_2, x_3, \dots)$$

where each $x_n \in \mathbf{Z}/p^n\mathbf{Z}$, and satisfying $\phi_n(x_n) = x_{n-1}$ for all n.

Notice that, if $(x_1, x_2, x_3, \dots)$ is a p-adic integer, then we have

$$\beta_n^m(x_m) = \phi_{n+1} \cdots \phi_{m-1}\phi_m(x_m) = x_n$$

$$\begin{tikzcd} \mathbf{Z}/p^m\mathbf{Z} \arrow[r, "\phi_m"] \arrow[rrr, bend left, "\beta_n^m"] & \mathbf{Z}/p^{m-1}\mathbf{Z} \arrow[r, "\phi_{m-1}"] & \cdots \arrow[r, "\phi_{n+1}"] & \mathbf{Z}/p^n\mathbf{Z} \end{tikzcd}$$

Definition of p-adic integers

The set of all p-adic integers is denoted by $\mathbf{Z}_p$, we will make the set $\mathbf{Z}_p$ into a ring by defining

$$(x_1, x_2, \dots) + (y_1, y_2, \dots) = (x_1 + y_1, x_2 + y_2, \dots)$$

$$(x_1, x_2, \dots)(y_1, y_2, \dots) = (x_1 y_1, x_2 y_2, \dots)$$

The zero element (additive identity) of $\mathbf{Z}_p$ is

$$(0 + p\mathbf{Z}, 0 + p^2\mathbf{Z}, 0 + p^3\mathbf{Z}, \dots)$$

which will be denoted simply by $[0]$.
The multiplicative identity of $\mathbf{Z}_p$ is

$$(1 + p\mathbf{Z}, 1 + p^2\mathbf{Z}, 1 + p^3\mathbf{Z}, \dots)$$

which will be denoted simply by $[1]$.

Structure of the ring $\mathbf{Z}_p$

We can consider the mapping $\mathbf{Z} \to \mathbf{Z}_p$

$$n \mapsto \begin{cases} \underbrace{[1] + \cdots + [1]}_{n}, & n > 0 \\ [0], & n = 0 \\ \underbrace{(-[1]) + \cdots + (-[1])}_{-n}, & n < 0 \end{cases}$$

This is an injective ring homomorphism, so from now on, we will think of $\mathbf{Z}$ as a subring of $\mathbf{Z}_p$. So if n is an integer, then we will simply write $[n]$ for the following p-adic integer

$$[n] = (n + p\mathbf{Z}, n + p^2\mathbf{Z}, n + p^3\mathbf{Z}, \dots) \in \mathbf{Z}_p$$

Later we will see that $\mathbf{Z}_p$ is strictly larger than $\mathbf{Z}$.

Structure of the ring $\mathbf{Z}_p$

Theorem

In $\mathbf{Z}_p$, the multiples of $[p^n]$ are exactly those elements whose n-th component is zero.

$$\{[p^n]x : x \in \mathbf{Z}_p\} = \{(x_1, x_2, \dots) \in \mathbf{Z}_p : x_n = 0\}$$

Theorem

Let $\mathbf{U}$ be the multiplicative group of invertible elements in $\mathbf{Z}_p$.
That is, $\mathbf{U} = \{x \in \mathbf{Z}_p : \exists y \in \mathbf{Z}_p, xy = [1]\}$.
Then we have $x \in \mathbf{U}$ if and only if $x_1 \neq 0 \in \mathbf{Z}/p\mathbf{Z}$

Theorem

Every non-zero element $x \in \mathbf{Z}_p$ can be written uniquely as

$$x = u(x)[p]^{v_p(x)}$$

where $u(x) \in \mathbf{U}$ and $v_p(x) \in \mathbf{N}$ are uniquely determined by x.

Structure of the ring $\mathbf{Z}_p$

Suppose $x \in \mathbf{Z}_p$ is a non-zero element. TFAE:

- $n \in \mathbf{N}$ is the largest integer such that $x_n = (0 + p^n\mathbf{Z})$
- $n \in \mathbf{N}$ is the largest integer such that $x_1, \ldots, x_n = 0$
- $n = v_p(x)$ is the p-adic valuation of the p-adic integer x
- x is the multiple of $[p^n]$ but not the multiple of $[p^{n+1}]$
- there exists $u \in \mathbf{U}$ such that $x = u[p^n]$

If $x = [0]$, we define $v_p(x) = \infty$. So we always have

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

In particular, if $x, y \in \mathbf{Z}_p$ such that $xy = [0]$, then at least one of x, y is the zero element $[0]$.

Fraction field

Definition (Domain)

A ring R is called a domain, if whenever $xy = 0$ we have at least on of x and y is 0.

Example

Suppose $n \geq 2$, then $\mathbf{Z}/p^n\mathbf{Z}$ is not a domain.

Theorem

Every subring of a field is a domain. Every domain D is a subring of some field, the smallest being the fraction field

$$Frac(D) = \left\{ \frac{x}{y} : x \in D, 0 \neq y \in D \right\}$$

Since $\mathbf{Z}_p$ is a domain, we can construct its fraction field, $\mathbf{Q}_p$, called the field of p-adic numbers.

Construction of p-adic numbers

By definition, the field of p-adic numbers is

$$\mathbf{Q}_p = \left\{ \frac{x}{y} : x \in \mathbf{Z}_p, 0 \neq y \in \mathbf{Z}_p \right\}$$

But we can write

$$x = u(x)[p]^{v_p(x)}, y = u(y)[p]^{v_p(y)}$$

where $u(x), u(y) \in \mathbf{U}$. So the element $u(y)$ is invertible in $\mathbf{Z}_p$, meaning that

$$u(\frac{x}{y}) = \frac{u(x)}{u(y)} \in \mathbf{Z}_p$$

So we have $\frac{x}{y} = u[p]^{v_p(x)-v_p(y)}$ where $u \in \mathbf{U}$.
So every p-adic number is of the form $x = u[p]^{v_p(x)}$ where $v_p(x)$ is still called the p-adic valuation of x.

The full-picture of p-adic numbers

Since $\mathbf{Z}$ is a subring of $\mathbf{Z}_p$, we have $\mathbf{Q}$ is a subfield of $\mathbf{Q}_p$. Given a rational number, we can think it as a p-adic number and compute its p-adic valuation by the following procedure.

1. write the rational number q as $q = p^v \frac{a}{b}$, where $v \in \mathbf{Z}$ and a, b not divisible by p.
2. v is the p-adic valuation of the rational number q.

Notice that if p does not divide n, then the p-adic valuation of $\frac{1}{n}$ is zero, which is non-negative. This means that $\frac{1}{n}$ is a p-adic integer. (a p-adic number is a p-adic integer if and only if the valuation is non-negative)
This shows that $\mathbf{Z}_p$ is strictly larger than $\mathbf{Z}$. Actually we have

$$\mathbf{Z}_p \cap \mathbf{Q} = \mathbf{Z}_{(p)} = \{q \in \mathbf{Q} : v_p(q) \geq 0\}$$

This ring is called the localization of $\mathbf{Z}$ at p.

Multiplicative structure of $\mathbf{Z}_p$ and $\mathbf{Q}_p$

The multiplicative structure of $\mathbf{Z}$ and $\mathbf{Q}$ can be described as:

- the unit group is $\mathbf{U}(\mathbf{Z}) = \{\pm 1\}$, it's simple
- for each prime number p, we have an integer v_p
- the number x is an integer if and only if $v_p \geq 0$ for all p
- $v_p(x+y) = v_p(x) + v_p(y)$

The multiplicative structure of $\mathbf{Z}_p$ and $\mathbf{Q}_p$ can be described as:

- the unit group is $\mathbf{U}$.
- we only need to consider one prime, namely p
- the number x is a p-adic integer if and only if $v_p \geq 0$
- $v_p(x+y) = v_p(x) + v_p(y)$

Later we will study the multiplicative group $\mathbf{U}$. And it turns out that $(\mathbf{U}, \times)$ is almost equal to $(\mathbf{Z}_p, +)$.
Notice that $(\mathbf{R}^\times, \times)$ is almost equal to $(\mathbf{R}, +)$

Equation theory