

## 環論 NO.4 要約

### 今日のテーマ 剰余環

**補題 4.1.**  $R$  が単位元をもつ環であるとし、 $I$  をそのイデアルとする。このとき、

- (1)  $R$  に同値関係  $\sim$  が、次のようにして決まる。

$$a \sim b \Leftrightarrow a - b \in I.$$

- (2)  $R/\sim$  に、足し算を次のようにして入れる。

$$\bar{a} + \bar{b} = \overline{a + b} \quad (\bar{?} \text{ は } ? \text{ の } \sim \text{ に関するクラスを表す。})$$

この足し算はうまく定義されていて、 $R/\sim$  はこの足し算について可換群になる。

- (3)  $R/\sim$  に、かけ算を次のようにして入れる。

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

このかけ算はうまく定義されていて、 $R/\sim$  はこのかけ算について半群になる。

- (4)  $R/\sim$  は上で定義された足し算、かけざんに関し環をなす。しかも、この環は単位元  $\bar{1}$  を持つ。

**定義 4.1.** 上の補題の仮定のもとで、 $R/\sim$  に上のような足し算、かけ算を入れて環にしたものを  $R/I$  と書き、 $R$  の  $I$  による**剰余環**と呼ぶ。

**例題 4.1.** 17770430 を 9 で割った余りを求めよ。

(解答) 整数  $n$  の  $\mathbb{Z}/9\mathbb{Z}$  におけるクラス (剰余類) を  $\bar{n}$  と書くことにする。一般に、 $\overline{10} = \bar{1}$  であることに注意すると、

$$\overline{10^k} = \bar{1} \quad (k \in \mathbb{Z}_{>0})$$

という等式が成り立つことがわかる。これを用いると、

$$\begin{aligned} \overline{17770430} &= \overline{1 \times 10^7 + 7 \times 10^6 + 7 \times 10^5 + 7 \times 10^4} \\ &\quad + \overline{0 \times 10^3 + 4 \times 10^2 + 3 \times 10^1 + 0} \\ &= \bar{1} \times \overline{10^7} + \bar{7} \times \overline{10^6} + \bar{7} \times \overline{10^5} + \bar{7} \times \overline{10^4} \\ &\quad + \bar{0} \times \overline{10^3} + \bar{4} \times \overline{10^2} + \bar{3} \times \overline{10^1} + \bar{0} \\ &= \bar{1} + \bar{7} + \bar{7} + \bar{7} + \bar{0} + \bar{4} + \bar{3} + \bar{0} \\ &= \overline{1 + 7 + 7 + 7 + 0 + 4 + 3 + 0} \\ &= \overline{29} = \overline{2 \times 10 + 9} = \overline{2 + 9} = \bar{2} \end{aligned}$$

を得る。

(答え) 2

(注意) 九去算は計算機のない時代に、計算の確かめの目的で使われた。現在でも、占い(カバラ占い)等で名残を見かけることがある。

問題:

あなたの思い付いた8桁以上の数(簡単すぎないもの)を  $x$  とします。このとき、 $x \times 314159265 + 1234567$  を 9 で割ったあまりを(計算機やコンピュータを使わずに)求めなさい。 $x$  自身と、求め方も書くこと。なお、検算にコンピュータ等を使用するのは構わないし、むしろ推奨する。