代数学 II 要約 NO.2

今日のテーマ:

環の標数、9 去法、「11 去法」

$\mathbb{Z}/9\mathbb{Z}$ での計算は、九去法 (あるいは、ナントカ占い) の名で知られているものの簡単な説明を与える。

例題 2.1. 3457 を 9 で割ったあまりを求めよ。

(解答)

$$\begin{aligned}
&[3457]_9\\
=&[3\times 10^3+4\times 10^2+5\times 10+7]_9\\
=&[3]_9\times[10]_9^3+[4]_9\times[10]_9^2+[5]_9\times[10]_9+[7]_9\\
=&[3]_9+[4]_9+[5]_9+[7]_9\\
=&[1]_9
\end{aligned}$$

つまり $[10]_9=[1]_9$ であることが最大のポイントなわけだ。同様にして、10 進法で書いた数を 11 で割ったあまりも簡単に求めることができる。($[10]_{11}=[-1]_{11}$) に注意)

環 R に対して、その単位元を 1_R, と書き、 1_R+1_R を 2_R とかく。$3_R, 4_R$ 等も同様。(この $?_R$ の R は「石井浩郎」と「石井琢郎」を区別するのに 石井$_{浩}$ とか 石井$_{琢}$ とかくのと同様で、言わなくても分かるときには省略する。)

定義 2.1 (環の標数)**.** ある正の整数 n があって、

$$n_R=0$$

が成り立つとき、このような n のなかで正で最小のものを R の標数と呼ぶ。そのような n がないときには、R の標数は 0 であると定義する。R の標数のことを、以下では $\mathrm{char}(R)$ と書く。

例 . $\mathbb{Z}/n\mathbb{Z}$ の標数は n である。

上で、「余り」というものがでたついでに、整数同士の「余りを許した割り算」について復習しておこう。この講義では特に断らない限りは次の意味の割り算をする。

定義 2.2. $m,n\in\mathbb{Z}$ とし、$n\neq 0$ であるとする。このとき、m を n で割った商 q と、余り r とは、次の関係式を満たす唯一のものとして定義される。

$$m=nq+r\qquad 0\le r\le |n|-1$$

この定義では、 m や n が負の数でも構わないということに注意しておく。余りだけについて言えば、次のような言い換えも可能である。

m を n で割った余りが r $\Leftrightarrow$ $([m]_{|n|}=[r]_{|n|}$ かつ $0\le r\le |n|-1)$

割り算を用いて次の結果を証明できる

補題 2.1. $\mathbb{Z}$ のイデアルは 0 か、または $n\mathbb{Z}$ *(n は正の整数)* の形のものに限る。

補題 2.2. 正の整数 n について、

- n が素数ならば環 $\mathbb{Z}/n\mathbb{Z}$ は体である。
- n が素数でなければ環 $\mathbb{Z}/n\mathbb{Z}$ は体ではない。

先週述べたこの補題の証明はもう少し一般化できる。
まず次の言葉を用意しておこう。

定義 2.3.

(1) 環 R の元 x が零因子であるとは、ある R の元 $y \neq 0$ があって、$xy = 0$ が成り立つときに言う。
(2) 環 R が 0 以外に零因子を持たないとき、R は整域であると言う。

補題 2.3. (1) 元の個数が有限の環の非零因子は必ず可逆である。
(2) 元の個数が有限の環 R が整域ならば、R は体である。

レポート問題が複数ある場合には、一つを選んで解くこと。保険のために二つ選んでもよい。その場合には評価はよい方のものを与える。(和にはならない。)

問題 2.1. 10 進法で書いた整数 n (例: $n = 1234567890$) を 13 で割った余りを求めるのは、9 や 11 のときほど簡単ではないが、つぎのようにできる。

(1) n を三桁毎に区切る。($n = |1|234|567|890|$)
(2) 区切ったものをそれぞれ符号をつけて加える。

$$890 - 567 + 234 - 1 = 556$$

(3) 加えた答えを 13 で割った余りを求める。(556 を 13 で割った余りは 10)

この最後の答えが n を 13 で割った答えである。これはなぜか説明せよ。

問題 2.2. 上と同様な考察により、10 進法で書いた整数を 17 で割った余りを「一定の桁数毎に区切って」求める方法はないか？

問題 2.3. 一般に、素数 p に対して、10 進法で書いた整数を p で割った余りを「一定の桁数毎に区切って」求める方法はいつでも存在するだろうか？(但しもちろん $p = 2$ と $p = 5$ の場合は例外とする。)