代数学 IB NO.5 要約

$\boxed{\text{今日のテーマ}}$ 《剰余環、素イデアル、極大イデアル》

前回までに、環 R の、そのイデアル I による剰余環について解説した。

$$\bar{x} = \bar{y} \Leftrightarrow x - y \in I$$

なる判定法により R にクラス分けが入ること、R/I に加法、乗法が代表元のとり方によらずに定まることがポイントであった。たとえば $\mathbb{Z}/11\mathbb{Z}$ において、

$$\overline{153} \times \overline{493}$$

を計算するのに、$\overline{153 \times 493}$ を計算してもよいが、$\overline{153} = \overline{-1}, \overline{493} = \overline{-2}$ と代表元を取り換えてから $\overline{-1} \times \overline{-2}$ とやっても良いわけである。

……………………………………………………………………………

可換環 R と、R の部分集合 S について、S を含む R のイデアルのうち最小のものを、S で生成される R のイデアル といい、(S) と表すのであった。S が有限集合の場合には、$(\{a_1, a_2, \ldots, a_n\})$ のことを普通単に $(a_1, a_2, \ldots, a_n)$ と書く。

補題 5.1. 可換環 R の有限部分集合 $T = \{a_1, a_2, \ldots, a_n\}$ に対して、

$$(T) = Ra_1 + Ra_2 + Ra_3 + \cdots + Ra_n$$
$$(= \{\sum_{j=1}^{n} c_j a_j ; c_j \in R\})$$

が成り立つ。

定義 5.1. 可換環 R の元 x が R の**零因子**であるとは、$xy = 0$ かつ $y \neq 0$ をみたす R の元 y が存在するときに言う。

定義 5.2. 可換環 R があたえられたとする。

(1) R に 0 以外の零因子がないなら、 R は**整域**であるという。
(2) R の 0 以外の元が R で可逆であるとき、R は**体**であるという。

もちろん、体は必ず整域である。

定義 5.3. 可換環 R のイデアル I $(R \neq I)$ について、

(1) R/I が整域であるとき、I は R の素イデアルであるという。
(2) R/I が体であるとき、I は R の極大イデアルであるという。

これらの名前の由来はもっとあとのほうで述べる。さしあたっては、次の例が重要である。

例 5.1.

(1) $\mathbb{Z}$ のイデアル $\{0\}$ は $\mathbb{Z}$ の素イデアルであるが、極大イデアルではない。
(2) 素数 p があたえられたとき、 $\mathbb{Z}$ のイデアル $p\mathbb{Z}$ は $\mathbb{Z}$ の極大イデアルである。
(3) 正の整数 n が素数でないとき、$n\mathbb{Z}$ は $\mathbb{Z}$ のイデアルではあるが、素イデアルではない。

定義 5.4. 素数 p が与えられたとき、$\mathbb{Z}/p\mathbb{Z}$ は (上の例に述べたように) 元の数が p の体である。この体を $\mathbb{F}_p$ と書く。

整域でない環では、今までの「常識」が通用しないことがある:

補題 5.2. 環 R と、その上の一変数多項式 $f(X)$ が与えられているとする。$d = \deg(f)$ (f の次数) とおくとき、

(1) R が整域ならば、 $f(r) = 0$ をみたす R の元 r は d 個以下である。
(2) R が整域でなければ、$f(r) = 0$ をみたす R の元 r が d 個以上存在する場合もある。

(2) の例:

(1) $R = \mathbb{Z}/6\mathbb{Z}$, $f(X) = 3X$ は一次式だが、$0, 2, 4$ のどれを代入しても 0 である。
(2) $R = \mathbb{Z}/6\mathbb{Z}$, $f(X) = (X-1)(X-2)$ は二次式だが、$1, 2, 4, 5$ のどれを代入しても 0 である。

※レポート問題
(期限：次の講義の終了時まで。)

(I) $\mathbb{F}_{13} = \mathbb{Z}/13\mathbb{Z}$ の、0 以外の各元について、その逆元をもとめて、下の表を完成させなさい。

x	1	2	3	4	5	6	7	8	9	10	11	12
x^{-1}	1	7					2					