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》

まずは記法から。この記法は今日すぐ用いるというわけではないが、あとあとたびたび用いるので、ここで書いておく:

補題 5.1. 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が存在する。

定義 5.1. 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。

丸括弧は、区切りを表す以外には何の付加的な意味を持たないのが普通であるが、この用法は例外である。

補題 5.2. 可換環 R の有限部分集合 $T = \{a_1, a_2, \dots, a_n\}$ に対して、

$$(T) = Ra_1 + Ra_2 + Ra_3 + \cdots + Ra_n$$

が成り立つ。$(T) = (\{a_1, a_2, \dots, a_n\})$ のことを普通 $(a_1, a_2, \dots, a_n)$ と書く。

($Ra_1 + Ra_2 + Ra_3 + \cdots + Ra_n$ とは

$$\{\sum_{j=1}^{n} c_j a_j ; c_j \in R\}$$

の略記であることに注意しよう。)

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 5.3. 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					