今日のテーマ **《剰余環、素イデアル、極大イデアル》**

定義 5.1. 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 5.2. 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 5.3. 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。

補題 5.1. 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

つぎのうち一問を選択して解きなさい。(期限:次の講義の終了時まで。)

(I) 正の数 $n, d \geq 2$ と、$R = \mathbb{Z}/n\mathbb{Z}$ 上の d 次多項式 $f(X)$ で、$f(x) = 0$ をみたす $x \in R$ の数が d 個より多いものの例を挙げ、実際にそのような $x \in R$ を $d+1$ 個以上書きなさい。