今日のテーマ イデアルとそれによる剰余環、環 $\mathbb{Z}/n\mathbb{Z}$

環をイデアルで割ることにより、新しい環を作ることが出来る。これは、群を正規部分群で割る操作に似ている。
とくに、$\mathbb{Z}$ を $n\mathbb{Z}$ で割った環は重要である。

定義 3.1. R は単位元をもつ環であるとし、I はその部分集合であるとする。I が R のイデアルであるとは、次の条件が成り立つときにいう。

(1) I は $(R,+)$ の部分群である。すなわち、I は R の加・減法について閉じている。
(2) I の元に R の元を右から掛けても左から掛けてもやっぱり I の元になる。すなわち、任意の $x \in I$ と任意の $r \in R$ について、

$$rx \in I, xr \in I$$

が成り立つ。

例 3.1 (イデアルの例).

(1) $10\mathbb{Z}$ は $\mathbb{Z}$ のイデアルである。
(2) もっと一般に、$n > 0$ にたいして、$n\mathbb{Z}$ は $\mathbb{Z}$ のイデアルである。
(3) 更に一般に、任意の可換環 R と 任意の $a \in R$ にたいして、aR は R のイデアルである。
(4) 任意の環 R に対して、$\{0\}$ は R のイデアルである。

補題 3.1. 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 3.2. 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 3.1 (剰余環の例).

(1) 任意の環 R に対して、剰余環 $R/0$ は R と同型 (環として同じもの) である。
(2) $\mathbb{C}[X]/X\mathbb{C}[X]$ は $\mathbb{C}$ と同型である。

$\mathbb{Z}/n\mathbb{Z}$ は、$\mathbb{Z}, \mathbb{C}[X]$ の次に重要な環の例である。環についての議論が正しいかどうかはこれらの環についてまずチェックしてみるのがよい。

補題 3.2. $\mathbb{Z}/10\mathbb{Z}$ において、

(1) $10 = 1 + 1 + \cdots + 1 \quad (10 \text{ 回 } 1 \text{ を足す}) = 0$ である。

(2) $2 \times 5 = 0$ である。(しかし、2 も 5 も 0 ではない。)

注意

$\mathbb{Z}/?\mathbb{Z}$ においては、単に $10, 2, 5$ と書く代わりに、$\overline{10}, \overline{2}, \overline{5}$ あるいは $[10], [2], [5]$ 等の記号を使って通常の数と区別することが多い。上の補題では、通常の感覚との違いを浮き出させるために、わざと $10, 2, 5$ 等と書いた。上のような例があるので、一般の環 R の元として例えば 300_R (または略して 単に 300) を考える時には、これが 0 かも知れないということを常に意識しておく必要がある。

$\mathbb{Z}/n\mathbb{Z}$ の性質は n が素数かどうかによって少し違って来る。それを説明するために、まず言葉を二つ用意する。

定義 3.3. R が環であるとする。R の元 x が R の零因子であるとは、次の二つのうちどちらかが成り立つ時に言う。

(1) $xy = 0, y \neq 0$ をみたす R の元 y が存在する。
(2) $yx = 0, y \neq 0$ をみたす R の元 y が存在する。

(もちろん、R が可換の時は上の二つの条件は同じことになる。) R が単位元を持つ可換環で、しかも 0 以外の零因子を持たない時、R を整域と言う。

補題 3.3. 正の整数 n を一つとって来る。このとき、

(1) n が素数でなければ、$\mathbb{Z}/n\mathbb{Z}$ は 0 以外に零因子を持つ。
(2) n が素数ならば、$\mathbb{Z}/n\mathbb{Z}$ は整域である。

実は、p が素数ならば、$\mathbb{Z}/p\mathbb{Z}$ は体であることがわかる。それには次の補題を使えばよい。

補題 3.4. R が整域で、かつ R の元の数 $\#R$ は有限であるとする。このとき、R は体である。とくに、$\mathbb{Z}/p\mathbb{Z}$ は体である。

系 3.1. 素数 p と、p で割り切れない整数 a とに対し、$ax + py = 1$ となる整数 x, y が存在する。

※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) (i) $\mathbb{Z}$ の元 x で、$\mathbb{Z}/100\mathbb{Z}$ の中で考えると $\bar{x} = \bar{1}$ が成り立つ例を 5 つあげなさい。(オリジナルであること:数はたくさんあるんだからケチケチしないで大きな数字をあげれば他の人と重ならないでしょう。) (ii) $\mathbb{Z}/12\mathbb{Z}$ の零因子をすべてあげ、それらが零因子であることを実際に示しなさい。

(II) $R = \mathbb{Z}[X]/(2, X^2 + X + 1)$ の元 (4 つある) をすべて書き、実際にそれらで R の元がつきていることを示しなさい。

(III) (II) の環 R は体であることを示しなさい。