整域・整数の剰余類の環

Joh @物理のかぎプロジェクト

2006-05-27

整数の全体が環になることは 環 の例で見ました．整数の環を **整数環** と呼ぶのでした．整数環の勉強には，素因数分解，合同など，整数ならではの知識がどうしても必要になってきます．

この記事の最後に整数の剰余類の環について勉強しますが，そこで，二つの整数 a, b とその最大公約数 d に対し，次の関係式を満たす整数 x, y が必ず一組存在することを使います．

$$d = ax + by \tag{1}$$

このような x, y を探す問題はディオファントス方程式と呼ばれ，必ず解が一意的に決まることが知られていますが，ここでは解の存在証明は省略します (ゴメンナサイ $(>\_<)$)．

二つの整数 a, b の最大公約数 d は，$d = (a, b)$ という記号で書くことにします．$(a, b) = 1$ となるとき a **と** b **は互いに素である** といい，自分より小さな全ての整数と互いに素になる整数を **素数** と呼びます．

整域

整数環に関係深い概念に **整域** があります．整域の定義は，『可換環で，単位元を持ち，零元以外に零因子を持たない環』です．

整域の例として重要なのは，**整数環** と **多項式環** です．

整数環

整数環とは，普通の整数全体のことです．さきほど見たように，普通の意味で整数の足し算・掛け算を考えることで整数全体は環となります．整数の掛け算は可換です．しかも単位元 1 を持ち，零因子はありません．

ですから，整数環は整域になるわけです．

多項式環

実数係数の多項式全体は，通常の加法と乗法に関して可換環になります．(これを R 上の多項式環と呼び，以後 $R[x]$ と書きます．R は，実数体の意味です．)

---

*1 整域という名前から分かるように，そもそも整域とは，整数の性質を念頭に置いて考え出された概念です．

次の二つの多項式に対し，加法と乗法がなりたつことを確認してみてください．

$$f_1(x) = a_0x^m + a_1x^{m-1} + ... + a_{m-1}x + a_m$$

$$f_2(x) = b_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$$

多項式環の単位元は 1 です．また 0 以外に零因子はありません．(もし多項式環に零因子があるならば，$(x-a)(x-b) = 0$ という形に因数分解して方程式を解くことが出来なくなります)．

多項式環は整域になります．

体

体では乗法の逆演算として除法が定義されていますので，乗法の零元以外には零因子を持ちません．また，体は単位元を持ち，体の乗法は可換と定義されていました．そこで，**体も整域だ** と考えることができます．

整数の剰余類

整数環 Z は加法に関しては群になります．この加法群 Z の整数 m による剰余群を考えます ($[k]$ は k の倍数を含む剰余類という意味です)．

$$Z/[m] = \{[0], [1], ..., [m-1]\}$$

整数 k は $[0], [1], ..., [m-1]$ のうちのどれかに属するはずですが，いま仮に k を含む剰余類を $\overline{k}$ と書くことにすると，すでに 体 の例 6 で見たように，剰余類の間に加法と乗法を定義できます．

$$\overline{k} + \overline{l} = \overline{k+l}$$

$$\overline{k}\overline{l} = \overline{kl}$$

ここで m を素数ではないとすると，m は $m = m_1m_2$ のように素因数分解できるはずです．このとき $\overline{m_1} \neq \overline{0}, \overline{m_2} \neq \overline{0}$ ですが，$\overline{m_1}\overline{m_2} = \overline{m_1m_2} = \overline{0}$ がなりたちますので $\overline{m_1}, \overline{m_2}$ はそれぞれ互いに零因子であり，$Z/[m]$ は整域ではなくなります．

逆に，m が素数のとき，$\overline{0}$ 以外の剰余類に属する元 a に対して常に $(m, a) = 1$ がなりたちます．そこで式 (1) より $1 = mx + ay$ を満たす整数 x, y が存在しているはずで，剰余を考えると次式が示されます．

$$\begin{aligned}\overline{1} &= \overline{mx + ay} \\ &= \overline{mx} + \overline{ay} \\ &= \overline{ay} \quad (\because\ \overline{mx} = \overline{0}) \\ &= \bar{a}\bar{y}\end{aligned}$$

なんとこれは，式中の $\overline{y}$ が $\overline{a}$ の逆元になっているという主張です．a は $\overline{0}$ 以外の剰余類に属する任意の元でしたので，結局，m が素数の場合は乗法に逆元も存在することになり，$Z/[m]$ は体になります．(もちろん $Z/[m]$ は整域にもなります．)

Important

整数の剰余類の環 $Z/[m]$ は，m が素数でない場合には零因子が存在し，整域にはならない．(単なる環)．m が素数の場合は，整域になり，乗法に逆元が入るので体になる．

整数の剰余環は，法とする整数が素数かどうかで，かなり構造が違ってくるんですね．