補 講3　倍数の集合について

3.0　はじめに

倍数の集合はちょっと面白い性質をもっています。かなり高度な内容ですが，紹介しておきます。ときどきこの性質に類するような内容の入試問題が出題されるので知っておくと役に立つでしょう。

最後の節に紹介する定理が目標です。
なお，この補講では，負の整数までこめて **整数** ということにします。

3.1　倍数の集合の性質

まず次の定理を証明しましょう。

定理 (倍数の集合の性質)　整数の集合 A がある整数 d の倍数全体からなるとき，

$$a,\ b \in A \ \Rightarrow\ a+b \in A$$
$$a \in A,\ m \in \mathbb{Z} \Rightarrow\ ma \in A$$

が成り立つ。

証明　$a,\ b \in A$ ならば，$a,\ b$ は d の倍数なので，$a = a'd,\ b = b'd$ と書ける。よって

$$a+b = a'd + b'd = (a'+b')d$$

ゆえに $a+b$ も d の倍数である。つまり $a+b \in A$。
次に，$a \in A,\ m \in \mathbb{Z}$ とすると，$a = a'd$ と表すことができ，

$$ma = m(a'd) = (ma')d$$

より ma も d の倍数。つまり $ma \in A$。　**(証明終)**

さて，本節の話題の中心は，この定理の逆が成り立つということです。つまり次の定理が成り立ちます。

定理 (単項イデアル)　整数の集合 A において　**単項イデアル**

$$a,\ b \in A \ \Rightarrow\ a+b \in A$$
$$a \in A,\ m \in \mathbb{Z} \Rightarrow\ ma \in A$$

が成り立つならば，どんな A の要素も，ある負でない整数 d の倍数である。

証明　$A = \{0\}$ なら $d = 0$ とすればよい。

$A \neq \{0\}$ とする。$k \in A$ とすると，二番目の性質から $-k \in A$ ($m = -1$ とすればよい)。よって A は自然数を含む。

A に含まれる最小の自然数を d としよう (「最小元の存在」定理からこれは保証される)。このとき，A は d のすべての倍数を含む。

逆に $a \in A$ とする。「除法の原理」から

$$a = qd + r, \quad 0 \leqq r < d$$

となる整数 $q,\ r$ が存在する[1]。よって $r = a - qd$ であるが，$a \in A,\ qd \in A$ より，一番目の性質から $r \in A$ となる。

いま d は A に属する最小の自然数であったので，$r = 0$ 以外にあり得ない。よって $a = qd$。つまり a は d の倍数。　**(証明終)**

3.2　整数論の基本定理

さて，以上の準備から次の定理が証明できます。

定理 (整数論の基本定理)　二つの整数 $a,\ b$ の最大公約数が d のとき，整数 $p,\ q$ で　**整数論の基本定理**

$$ap + bq = d$$

となるものが存在する。

特に a と b が互いに素なら，

$$ap + bq = 1$$

となる整数 $p,\ q$ が存在する。

証明

$$A = \{ax + by \mid x,\ y \in \mathbb{Z}\}$$

とおく。$ax_1 + by_1 \in A,\ ax_2 + by_2 \in A$ とすると，

$$(ax_1 + by_1) + (ax_2 + by_2) = a(x_1 + x_2) + b(y_1 + y_2)$$

[1]「除法の原理」は a, b ともに自然数として述べましたが，実は整数 a と自然数 b に対して成り立ちたちます。研究してみてください。

となり，$x_1 + x_2 \in \mathbb{Z},\ y_1 + y_2 \in \mathbb{Z}$ より，

$$(ax_1 + by_1) + (ax_2 + by_2) \in A$$

を得る。

また $m \in \mathbb{Z}$ とすると，

$$m(ax_1 + by_1) = a(mx_1) + b(my_1)$$

で，$mx_1 \in \mathbb{Z},\ my_2 \in \mathbb{Z}$。よって

$$m(ax_1 + by_1) \in A$$

以上から，先の節の二番目の定理「単項イデアル」の仮定が成り立つので，A の任意の要素は負でない整数 d の倍数になる。

$a = a \times 1 + b \times 0$ より $a \in A$ なので，d は a の約数。

同様にして，d は b の約数にもなっている。つまり d は a と b の公約数である。

次に d' を a と b の正の公約数とし，$a = a''d',\ b = b''d'$ とする。

d は A の正の最小元だったので $d \in A$。つまり $d = ax + by,\ x,\ y \in \mathbb{Z}$ と表すことができる。よって

$$d = ax + by = a''d'x + b''d'y = (a''x + b''y)d'$$

つまり d' は d の約数。ゆえに d は a と b の最大公約数である。　　**(証明終)**