代数学 IB NO.9 要約

今日のテーマ

《割り算の原理 (ユークリッド環)》前回は余りを許したわり算のできる環 (ユークリッド環) の定義をした。ユークリッド環においては、ユークリッドの互除法が実行できるのであった。

. . . . . .

今回は、前回積み残した命題の証明を行う。さらに、イデアルの包含関係と数の整除の関係、ユークリッドの互除法のイデアル論的な意義について解説する。

定義 9.1. 環 R が**ユークリッド環**であるとは、整列順序集合 W と 写像 $\rho : R \to W$ (「重さ」を調べる写像) があって、次の性質を満たすときに言う

(1) R の元 a の「重さ」 $\rho(a)$ が最小 $\Leftrightarrow a = 0$
(2) R の元 a, b $(a \neq 0)$ に対して、

$$b = aq + r, \quad q, r \in R, \quad \rho(r) < \rho(a)$$

となる q, r が存在する。

(「W が整列集合である」とは、W は順序集合であって、しかも「W の任意の部分集合 X は最小元を持つ」というときにいう。この定義が難しく感じられる諸君には $W = \mathbb{N}$ と思っても初級の段階には充分である。)

定義 9.2. 環 R のイデアル I が**単項イデアル**であるとは、ある $a \in R$ が存在して、 $I = (a)$ が成り立つときに言う。

R の全てのイデアルが単項イデアルであるとき、R は**単項イデアル環**であると言う。

定理 9.1. ユークリッド環は単項イデアル環である。

系 9.2. 整数 a, b が与えられているとし、その最大公約数を d とおく。このとき、

$$al + bm = d$$

をみたす整数 l, m が存在する。

系 9.3. k を体とする。k 上の多項式 a, b が与えられているとし、その最大公約数を d とおく。このとき、

$$a(X)l(X) + b(X)m(X) = d(X)$$

をみたす k 上の多項式 l, m が存在する。

定義 9.3. 環 R と $a, b \in R$ とにたいして、

(1) $a \in bR$ のとき、 a は b の**倍元**であるといい、$b|a$ で書き表す。b を主語として、b は a の**約元**であるともいう。
(2) ある $u \in R^\times$ があって、$a = bu$ をみたすとき、a と b とは**同伴**であるという。

命題 9.4. 整域 R の元 a, b にたいして、

(1) $(a) \subset (b) \Leftrightarrow b|a.$
(2) a と b が同伴 $\Leftrightarrow (a) = (b).$

一般に、単項イデアル環 R において、2 つの元 a, b で生成されるイデアル (a, b) は、単項であるから $(d) = (a, b)$ なる $d \in R$ が存在するはずである。この d は a, b の最大公約元 (gcd) である。

問題 9.1. 5 桁以上の 2 つの数 a, b を具体的に挙げ、その gcd d を互除法を用いて求め、その a, b, d について イデアルの等式 $(a, b) = (d)$ を一般論によらずに証明せよ。他の人と a, b が重ならないこと、簡単になりすぎないことに留意すること。