環論 NO.11 要約

今日のテーマ　PID ・素元分解環

単項イデアル環であるような整域を単項イデアル整域(principal ideal domain, 略して **PID**) とよぶ。

命題 10.7 の帰結として、次のことが成り立つことがわかる。

定理 11.1. PID R において、R の元 a, b をとる。$(a, b) = (d)$ を満たす d は a, b の最大公約元である。

補題 11.2. PID R の元 a, b, c が $\gcd(a, b) = 1$ かつ $a|bc$ を満たすならば、 $a|c$.

定義 11.3. R は可換環であるとする。R の元 x が**既約**であるとは、 x が 0 でも可逆元でもなく、なおかつ

$$\forall y \forall z (y, z \in R, yz = p \implies (y \in R^\times \text{ または } z \in R^\times))$$

をみたすときに言う。

命題 11.4. PID R においては、既約元は素元である。

定義 11.5. 整域 R が**素元分解環**であるとは、R の任意の元 x について、次のいずれかが成り立つときに言う。

(1) x=0
(2) $x \in R^\times$
(3) x は R の素元の積に分解される。

補題 11.6. R は整域であるとする。このとき、

(1) R の素元は、必ず既約である。
(2) R の既約元は、必ずしも素元とは限らない。
(3) R が素元分解環ならば、その既約元は必ず素元である。

- $\mathbb{Z}[\sqrt{-5}]$ では素因数分解は一意的でない。例えば

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3.$$

補題 11.7. 単項イデアル環 R のイデアルの増大列

$$I_1 \subset I_2 \subset I_3 \subset I_4 \subset \dots$$

は必ずどこかで止まる。すなわちある N があって、

$$I_N = I_{N+1} = I_{N+2} = \dots$$

がなりたつ。

上の補題はネータ環の一般論の特殊な場合である。ここで、R が**ネータ環**であるとは、R の任意のイデアルが有限個の元で生成される場合に言う。ネータ環のイデアルの増大列も、必ずどこかで止まることが証明できる。証明はほとんど同じなので進んで勉強したい人はやってみられると良い。(余談ながらネータ環は環論において大変重要な対象である。体上有限生成な環は全てネータ環である。(ヒルベルトの基定理))

《ベズーの等式》

命題 11.8. 可換環 R の元 a, b に対して、次は同値である。

(1)
$$(a, b) = (1)$$
(2) ある $l, m \in R$ が存在して、$la + mb = 1$ が成り立つ。

ユークリッド環については、最大公約数が 1 であるような a, b に対して、上の命題のような l, m は互除法により求まるのであった。例としてつぎのような定理、命題を考えることができる。(いくつかは既出である。)

定理 11.9. p が素数であれば、$\mathbb{Z}/p\mathbb{Z}$ は体である。

定理 11.10. 体 K 上の 既約多項式 $p \in K[X]$ にたいして、$K[X]/p(X)$ は体である。

命題 11.11. a, b は互いに素な正の整数とする。群 G の元 g が $g^a = e$, $g^b = e$ (e は G の単位元) を満足するならば、$g = e$ である。