Lecture 24

Ｒｉｎｇ　環

[例]

$\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{C}$, F = field, $M_n(F)$

環のおおまかな定義：

- 演算　＋　についてアーベル群（単位元 0）
- × について可換とは限らない、単位元　１を持つ。 しかし、逆元はあるとは限らない。
- 分配法則が成り立つ　$a(b+c)=ab+ac$ ，$(a+b)c=ac+bc$

部分環　$R'\subset R$　（R'はそれ自身　環であり、R' における演算はR の演算をそのまま引き継ぐ。R'はRの部分環と呼ばれる）例：$\mathbb{Z}\subset\mathbb{Q}$

[例]　$R=\mathbb{C}$　（複素数の作る環）の部分環として、

$\mathbb{R},\mathbb{Q},\mathbb{Z}$,　$\mathbb{Z}+\mathbb{Z}i=\{a+bi:a,b\in\mathbb{Z}\}$　などなどたくさんある。

$\mathbb{Z}+\mathbb{Z}i$　は普通$\mathbb{Z}[i]$と書かれ「ガウスの整数」と呼ばれる。

[例]　$\mathbb{C}$　には含まれない大切な環として、$\mathbb{C}$を係数とする１変数X　の多項式から成る環　$\mathbb{C}[X]$ がある。

$= \{a_nX^n + \cdots + a_1X + a_0 : a_i \in \mathbb{C}\}$

denoted $\mathbb{C}[X]$

さらに、多変数多項式

$\mathbb{C}[X,Y] = \mathbb{C}[X][Y]$.

を考えることができる。もっと一般には、R　を可換環とするとき、Rの要素を係数とする多項式全体から作る$R[X]$　という可換環を作ることができる。

[例]　$R=\mathbb{Z}/2$ とするとき、$R[X]$においては、例えば

$$(X+1)(X+1)=X^2+2X+1=X^2+1$$

などという計算ができる。ここで、$\mathbb{Z}/2$ では$2=0(\mathrm{mod}\,2)$ を用いている。

極端な場合であるが、$R=\{0\}$ という１要素だけからなる環がある。これは最小なものであり$1=0$ というようなことが起きている。しかし、２つ以上の要素をもつR では$1=0$というようなことはない。

命題：$R\neq\{0\}$においては、$1\neq 0$である。

証明）$a\in R$ とし$1=0$ を仮定する。このとき、$a=1\cdot a=0\cdot a$　である。一方、分配法則により$0\cdot a=(0+0)\cdot a=0\cdot a+0\cdot a$ であるが、$0\cdot a=0$　加法の単位元の一意性より、$0\cdot a=0$がしたがう。つまり、$a=0$ となった。a は任意であった、つまり$R=\{0\}$となってしまい、仮定に矛盾する。■

任意の大きさの環が存在することは、大きさn の$\mathbb{Z}/n\mathbb{Z}$ を考えればよい。

アーベル群$(A,0,+)$から環を作る方法を示す。ある数学的対象からそれ自身への射（あるいは準同型）は自己準同型 Endomorphism とよばれる。いま、$f:A\to A$ なる自己準同型すなわち、$R\equiv End(A)=\{f:A\to A\text{準同型}\}$ とすると、このRは環である。ただし、Rにおける演算を次のようにする。任意の$a\in A$ に対して$f+g$ は$(f+g)(a)=f(a)+g(a)$　、$0_R(a)=0_A$、$-f$ は$(-f)(a)=-(f(a))$ 、$f\times g$ は写像の合成$(f\times g)(a)=f(g(a))$、$1_R(a)=a$。そして、掛け算についての逆元の存在は仮定しない。（f が可逆であるためには、isomorphic 同型であることが必要十分である）。

[例]　$R=End(\{e\})=\{0\}$ 自明なものであるが、数学ではしばしばこのようなものを考えておくことがある。また$\mathbb{Z}$ は$End(\mathbb{Z},+,0)$ であるが、$f\mapsto f(1)$ は

$End(\mathbb{Z},+,0)\to\mathbb{Z}$ なる bijection　であり、

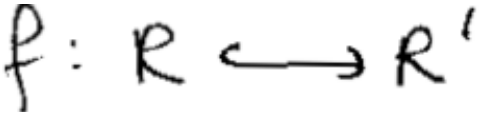
$f(k)=f(1+1+\cdots+1)=f(1)+f(1)+\cdots+f(1)=k\cdot f(1)$ より $f(k)=k\cdot f(1)$ が任意の $f\in End(\mathbb{Z})$ で成り立つから、$End(\mathbb{Z},+,0)$ は $f(1)$ を定めればすべてが決まってしまう。しかしこれは、$\mathbb{Z}$ における普通の加法と乗法という操作においては違いがあるわけではない。その意味で、$\mathbb{Z}=End(\mathbb{Z},+,0)$ である。

同様なことは、$\mathbb{Z}/n\mathbb{Z}=End(\mathbb{Z}/n\mathbb{Z},+,0)$ についても $f\mapsto f(1)$ と言う対応からわかる。そして、

$A=(\mathbb{Z}/p\mathbb{Z})^2=\{(a_1,a_2):a_i\in\mathbb{Z}/p\mathbb{Z},i=1,2\}$ にたいして、$End(A)=M_2(\mathbb{Z}/p\mathbb{Z})$ が成り立つ。すなわち、$\mathbb{Z}/p\mathbb{Z}$ を要素とする 2×2 行列となる。これは非可換な環である。もっと一般には、$A=(\mathbb{Z}/p\mathbb{Z})^n$ に対して $End(A)=M_n(\mathbb{Z}/p\mathbb{Z})$ となる。これは、$n\times n$ 行列からなる非可換環である。

ここからは断りがない限り、可換な環のみを扱うことにする。

２つの環 R,R' に対して、<u>環準同型</u>とは $f:R\to R'$ で、加法＋に関しては群準同型が成り立っており、さらに $f:1_R\to 1_{R'}$ および、$f(a\times_R b)=f(a)\times_{R'}f(b)$ となる対応を言う。



[例] $R\subset R'$ の場合は、inclusion map が環準同型を与える。

つぎに、環におけるカーネルは　$\ker(f)=\{a\in R:f(a)=0_{R'}\}$ で定義される。

この時 $\ker(f)$ は次の性質をもつ。

性質　１）$\ker(f)$ は＋に関して R の部分群である。

２） $a \in R$ ， $b \in \ker(f)$ とするとき、 $a \cdot b \in \ker(f)$

である。

２）は $f(a \times b) = f(a) \times f(b) = f(a) \times 0 = 0$ からわかる。

２）はもっと一般にイデアルという部分環の性質になる。

定義： $I \subset R$ なる部分集合で、 $+$ 演算で R の部分群になっており、× という演算で、任意 $a \in R$ との演算で閉じている（ $ai \in I$ ， $\forall$ $i \in I$ ）とする。この時、 I は R のイデアルと呼ばれる。

[イデアルの例]

1） f を R の環準同型とするとき、 $\ker(f)$

２） $\{0\}$ ： $f = id : R \to R$ とおけば、 $\ker(f) = \{0\}$

３） R ： $f = 0 : R \to \{0\}$ とおけば、 $\ker(f) = R$

４）ある $r \in R$ にたいして、 $I = \{ar : a \in R\}$

とくに、例における４）の形をしたイデアルは、 r により生成される principal イデアルと呼ばれる。

実は、任意のイデアル I は次の自然な環準同型の kernel になっている。

$R \to R/I$ ， $a \to a + I$ ．

ここで、群についてと全く同様にして、 R/I についての環の構造は、

$$(a+I)+(b+I)=(a+b)+I$$

$$(a+I)\times(b+I)=(a\times b)+I$$

となるが、これらは I がイデアルであることから導かれる。このことは後で詳しくのべる。

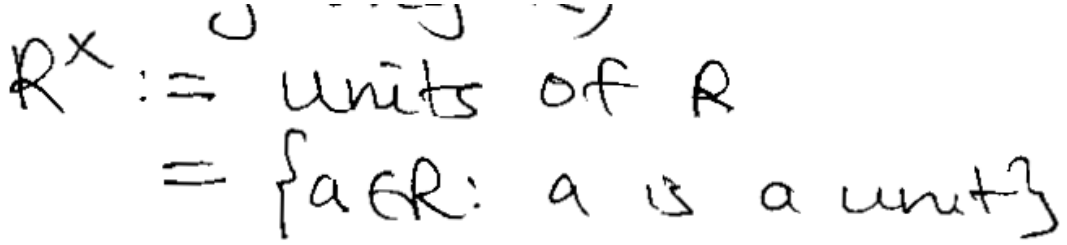
事実） $\mathbb{Z}$ におけるイデアルは、 $I = (n) = n\mathbb{Z}$ で　商環 $\mathbb{Z}/I$ は $\mathbb{Z}/n\mathbb{Z}$ に他ならない。

重要な事実） principal でないイデアルをもつ環がある。

重要なる概念：

R の単位元：$a \in R$ で$\exists b \in R$に対して$ab = 1$ を満たすもの。すなわち掛け算での逆元a^{-1}をもつようなa のこと。

R を任意の環とするとき、$R^{\times}$ は　R の単位元全体をあらわす。



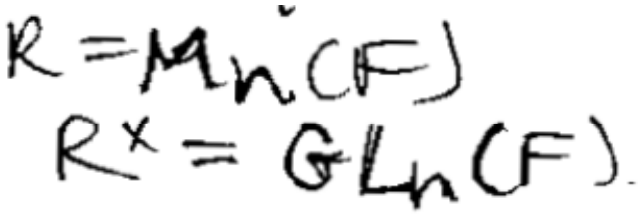
$R^{\times}$はRの単位群（unit group）　と呼ばれる（積演算での群）

[例]$R = F$　つまり体のとき、０以外逆元が存在するので$R^{\times} = R \setminus \{0\}$

[例]　$R = \mathbb{Z}$　のとき、$R^{\times} = \{\pm 1\}$

[例]　$R = \mathbb{Z}/n\mathbb{Z}$　のとき$R^{\times} = \{a + n\mathbb{Z}; \gcd(a,n) = 1\}$。つまり、$a$　はn　と互いに素な整数。

[例]$R = M_n(F)$　F　を要素とする$n \times n$　行列。



$GL_n(F)$ は逆行列をもつ$n \times n$　行列。$F = \mathbb{R}$　なら行列式がゼロでないもの。