§1. 可換環

定義　空でない集合 R とその上の 2 つの二項演算 $+, \cdot$ が与えられ，次をみたすとき，$(R, +, \cdot)$ は**環**であるという（略して，R は環である，ということが多い）．

(R1) $(R, +)$ はアーベル群である．

(R2) R は $\cdot$ に関して結合的である，すなわち

$$\forall a, b, c \in R \text{ に対して，} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(R3) R は $+, \cdot$ に関して分配的である，すなわち

$$\forall a, b, c \in R \text{ に対して，} \quad (a+b) \cdot c = a \cdot c + b \cdot c \text{ かつ } a \cdot (b+c) = a \cdot b + a \cdot c.$$

演算 $+, \cdot$ はそれぞれ，**和**，**積**と呼ばれる．多くの場合，積の演算記号 $\cdot$ は明示せず，たとえば $a \cdot b$ は ab と書く．

定義　環 $(R, +, \cdot)$ がさらに次をみたすとき，R を**可換環**という．

(R4) 積 $\cdot$ に関して可換，すなわち，

$$\forall a, b \in R \text{ に対して，} \quad ab = ba$$

定義　環 $(R, +, \cdot)$ がさらに次をみたすとき，R は**単位的**であるという．

(R5) 積 $\cdot$ に関する**単位元**をもつ，すなわち，R は元 1 を持ち，

$$\forall a \in R \text{ に対して，} \quad a1 = 1a = a$$

定義　$(R, +, \cdot)$ を環とする．

(1) アーベル群 $(R, +)$ を，R の**加法群**といい，その単位元を**零元**という．
(2) R が単位的であるとき，積に関する単位元を R の**単位元**という．
(3) 零元を通常 0 で表す．
(4) 単位元は存在すれば一意的である．単位元を通常 1 で表す．
(5) $R = \{0\}$ のとき，これを**零環**という．

定義　R を単位的可換環とし，$a, b \in R$ とする． $ax = b$ をみたす $x \in R$ が存在するとき，a を b の**約元**といい，$a|b$ で表す． このとき，b を a の**倍元**，a は b を割り切る，b は a で割り切れる，ともいう．

定義　R を単位的可換環とする． 1 の約元を**単元**という． R の単元全体は積に関して群となるが，これを R の**単元群**といい $R^\times$ で表す．

定義　R を単位的可換環とし，$a \in R$ とする． $ax = 0$ をみたす 0 でない $x \in R$ が存在するとき，a を**零因子**という．

定義　0 のほかに零因子を持たない単位的可換環を**整域**という． すなわち，可換環 R が整域であるとは，任意の $a, b \in R$ に対して

$$ab = 0 \text{ ならば，} \quad a = 0 \text{ または } b = 0$$

が成り立つことをいう．

定義　0 でない元がすべて単元である単位的可換環を**体**という． すなわち，可換環 R が体であるとは，

$$\forall a \in R \ (a \neq 0) \text{ に対して，} \quad \exists b \in R \text{ s.t. } ab = 1$$

が成り立つことをいう．

注意　可換でない環について，整域や体に相当するものを考えることもできるが，この講義では扱わない．

定義　$(R, +, \cdot)$ を環とし，S を R の空でない部分集合とする． 演算 $+, \cdot$ を S に制限したものが S の二項演算になっていて，それらにより S が環であるとき，S を R の**部分環**という．

命題 1.1　R を環とし，S を R の部分環とする． $0, 1$ を R の零元，単位元とし，$0_S, 1_S$ を S の零元，単位元とする．

(1)　$0_S = 0$ が成り立つ．

(2)　R が整域ならば $1_S = 1$ が成り立つ．

命題 1.2　有限個の元からなる整域は体である.

定義　R, S を単位的環とする.　写像 $f : R \to S$ が**準同型写像**であるとは,

$\forall a, b \in S$ に対して,　$f(a+b) = f(a) + f(b)$,　$f(ab) = f(a)f(b)$

かつ　$f(1) = 1$

をみたすことである. $\mathrm{Im}\, f = \{\ f(a) \mid a \in R\ \}$, $\mathrm{Ker}\, f = \{\ a \in R \mid f(a) = 0\ \}$ をそれぞれ f の**像**, **核**という.

定義　R, S を単位的環とする.　準同型写像 $f : R \to S$ が全単射であるとき, f は**同型写像**であるという.

定義　R, S を単位的環とする.　R から S への同型写像が存在するとき, R と S は**同型**であるといい, $R \simeq S$ と表す.