I240 暗号理論 2019
数学的準備

2019/11/13,11/15 講師 藤崎

1 準備の準備

1.1 類別

定義 1（同値関係 (equivalence relation)） S を集合とする。任意の $a, b, c \in S$ に対して以下の条件を満たすとき、$\sim$ は集合 S 上の同値関係であるという。

- $a \sim a$.
- $a \sim b$ なら、$b \sim a$.
- $a \sim b, b \sim c$ なら、$a \sim c$.

定義 2（同値類 (equivalence class)） $(S, \sim)$ を集合とその上の同値関係とする。S の部分集合 C が以下の条件を満たすとき、$(S, \sim)$ における同値類という。

- $C \neq \emptyset$.
- $x \sim y$ なら、$x, y \in C$.
- $x \sim y$ かつ $x \in C$ なら、$y \in C$.

同値関係は同値類により集合 S を一意に分解する。

定義 3 $(S, \sim)$ が定義されているとする。$a \in S$ と同値なもの全体のなす集合を、$C(a)$ であらわし、a を含む同値類とよぶ。

命題 4

- $a \in C(a)$.
- $b \in C(a)$ なら、$C(b) = C(a)$.
- $C(a) \neq C(b)$ なら、$C(a) \bigcap C(b) = \emptyset$.

命題 5（分割） $(S, \sim)$ で定まる同値類の集合は、集合 S の分割になる。すなわちある S の部分集合 $A(\subset S)$ が存在し、

- $S = \bigcup_{a \in A} C(a)$ と表せ
- 全ての $a, b \in A$ にたいして、$C(a) \bigcap C(b) = \emptyset$.

同値関係は、S を同値類で一意に分割するから、A の選び方に寄らず S を分割する各同値類は一意に決まっている。

定義 6（商集合 (quotient set)） $(S, \sim)$ で定まる（S を分割する）同値類の集合 $\{C(a)\}_{a \in A}$ を、$S/\sim$ とかき、S の $\sim$ による商集合という。

1.2 写像

定義 7 S, S' を集合、$f : S \to S'$ を S から S' への写像とする。$\mathsf{Im}(f) := \{f(x) \,|\, x \in S\}$ を f による S の像 (image) と呼ぶ。

定義から $\mathsf{Im}(f) \subseteq S'$.

定義 8（全射） $\mathsf{Im}(f) = S'$ のとき、f は全射 (surjective) であるという

定義 9（単射） $x \neq x'$ となる全ての $x, x' \in S$ に対して、$f(x) \neq f(x')$ のとき、f は単射 (injective) であるいう

定義 10（全単射） f が全射かつ単射のとき、全単射 (bijective) であるという

2 環 $\mathbb{Z}/n\mathbb{Z}$

定義 11（整数の合同） $n \in \mathbb{N}$ に対して、二つの整数 a, b の差 $a - b$ が n の倍数であるとき（すなわち、$n|(a-b)$ であるとき）、a, b は n を法として合同であるといい、

$$a \equiv b \pmod{n}$$

と書く。

法 n での整数の合同は、集合 $\mathbb{Z}$ 上の同値関係 $\sim_n$ である。

$$a \equiv b \pmod{n} \iff a \sim_n b$$

$(\mathbb{Z}, \sim_n)$ で定まる（相異なる）同値類は、

$$n\mathbb{Z},\ 1 + n\mathbb{Z},\ \ldots,\ (n-1) + n\mathbb{Z}$$

であり、商集合 $\mathbb{Z}/\sim_n$ を、$\mathbb{Z}/n\mathbb{Z}$ と書く。すなわち、

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z},\ 1 + n\mathbb{Z},\ \ldots,\ (n-1) + n\mathbb{Z}\}$$

である。

■$\mathbb{Z}/n\mathbb{Z}$ で、二つの二項演算 $+$ と $\cdot$ を定義する

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z}$$
$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) := (a \cdot b) + n\mathbb{Z}$$

と演算を定義すると、これは well-defined になる。well-defined になるとは次のようなことである。

$a' \in (a + n\mathbb{Z})$, $b' \in (b + n\mathbb{Z})$ なら同値類の性質より、$a' + n\mathbb{Z} = a + n\mathbb{Z}$, $b' + n\mathbb{Z} = b + n\mathbb{Z}$。すなわち、$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a' + n\mathbb{Z}) + (b' + n\mathbb{Z})$ にならないと都合が悪いが、そのためには常に $(a' + b') + n\mathbb{Z} = (a' + b') + n\mathbb{Z}$ が成立する必要がある。同様に、$(a' \cdot b') + n\mathbb{Z} = (a \cdot b) + n\mathbb{Z}$ も常に成立する必要がある。これがちゃんと成立することを、演算が well-defined であるという。上記の演算はそれを満足する。後述するが、演算 $+$ が well-defined な理由は、$n\mathbb{Z}$ が $\mathbb{Z}$ の正規部分群だからであり、演算 $\cdot$ が well-defined な理由は、$n\mathbb{Z}$ が $\mathbb{Z}$ の（両側）イデアルだからである。

■$\mathbb{Z}/n\mathbb{Z}$ は環になる　$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ は上記演算で環になる（剰余類環とよぶ)。また、$n = p$（素数）のとき、$\mathbb{Z}/p\mathbb{Z}$ は体になる。

■オイラー関数

定義 12（Euler's Totient function）　$\phi(n)$ をオイラー関数 (Euler's totient function) といい、$0, \ldots, n-1$ のうち、n と互いに素なものの個数（ただし、$\phi(1) = 1$) と定義する。

$$\phi(n) := \#\{x \in \{0, 1, \ldots, n-1\} \mid \gcd(x, n) = 1\}$$

- $(m, n) = 1$（m と n の最大公約数が 1）なら、$\phi(mn) = \phi(m)\phi(n)$ が成り立つ
- 素数 p と、自然数 e に対して、$\phi(p^e) = p^{e-1}(p-1)$ であること

に注意する。そのとき $n = \prod_{i=1}^{s} p_i^{e_i}$ とすると、

$$\phi(n) = n\prod_{i=1}^{s}(1 - \frac{1}{p_i})$$

とわかる。

3　群の話

3.1　部分群、巡回群

定義 13　群 G の部分集合 H が、G における演算 $\circ$ で群を作る時、H は G の**部分群**という。

定理 14　以下は、H が G の部分群になる必要十分条件である。

$$\forall a, b \in H \implies \quad a \circ b^{-1} \in H \tag{1}$$

(証明) H が部分群なら (1) をみたすの明らか。逆に (1) を満たすとすると、

$$a, a \in H \implies \quad e = a \circ a^{-1} \in H$$

より、$e \in H$. よって、

$$e, a \in H \implies \quad a^{-1} = e \circ a^{-1} \in H$$

なので、$a \in H \implies a^{-1} \in H$. さらに、

$$a, b \in H \implies a, b^{-1} \in H \implies a \circ b = a \circ (b^{-1})^{-1} \in H.$$

よって逆も成立。

定義 15　$a \in G$ とする。$a^n := \overbrace{a \circ \cdots \circ a}^{n}$ と定義し、$\ldots, a^{-1}, a^0, a^1, \ldots$ の集合を $\langle a \rangle$ とかく。すなわち

$$\langle a \rangle := \{a^n | n \in \mathbb{Z}\}$$

.

定理 16　$\langle a \rangle$ は G の部分群になる。

問題 17　定理 16 を示せ。

$\langle a \rangle$ を**巡回群**という。a を $\langle a \rangle$ の生成元という（$\langle a \rangle$ の生成元は a だけとは限らない)。G が可換・非可換によらず、$\langle a \rangle$ は可換群である。

定義 18　$a^n = 1$（1 は単位元）となる最小の正の整数を a の**位数**という（そのような正整数が無い場合は a の位数は無限という)。

a の位数は、部分群 $\langle a \rangle$ の位数（元の個数）と一致する。

3.2　剰余類と Lagrange の定理

定義 19（剰余類 (residue class)、傍系 (coset))　H を群 G の部分群とする。$a \in G$ に対して、

$$aH := \{a \circ h | h \in H\}$$
$$Ha := \{h \circ a | h \in H\}$$

と定義し、aH を左剰余類 (左傍系, left coset)、Ha を右剰余類 (右傍系, right coset) という（もし G が可換群なら、H も当然可換群で、$aH = Ha$)。

H を群 G の部分群、aH を左剰余類とする（$aH := \{a \circ h | h \in H\}$)。

定理 20　$a, b \in G$ に対して、

$$a \sim b \quad \Longleftrightarrow \quad aH = bH$$

と定義すると、$\sim$ は G 上の同値関係になる。

(証明)

- $aH = aH$.
- $aH = bH$ なら、$bH = aH$.
- $aH = bH$, $bH = cH$ なら、$aH = cH$.

同様に、右剰余類でも H により同値関係が定義できる。

群 G の部分群 H による左剰余類は、同値関係をつくるので、ある G の部分集合 A があって、左剰余類の集合 $\{aH\}_{a \in A}$ により、G を分割できる。

$$G = \bigcup_{a \in A} aH.$$

定義より、$\forall a, b \in A$ $(a \neq b)$ に対して、$aH \bigcap bH = \emptyset$.

定義 21　$G/H := \{aH\}_{a \in A}$.

同様に右剰余類により G を分割した右剰余類の集合を $G \backslash H$ とかく。後述の理由により、同じ A を用いて $G \backslash H = \{Ha^{-1}\}_{a \in A}$ と書ける。

定義 22（合同）　$a, b \in G$ が $a^{-1}b \in H$ のとき、a と b は、H を法として、左合同であるといい、$a, b \in G$ が $ab^{-1} \in H$ のとき、a と b は、H を法として、右合同であるという。G が可換の時は、単に**合同**といい、

$$a \equiv b \pmod{H} \quad \Longleftrightarrow \quad a^{-1}b \in H$$

と書く。

命題 23　$a, b \in G$ に対して、$aH = bH \iff a^{-1}b \in H$ が成り立つ。同様に、$a, b \in G$ に対して、$Ha = Hb \iff ab^{-1} \in H$ が成り立つ。

よって、左（または右）合同は同値関係 $\sim$ を定義している。G が加法群であれば、$a \equiv b \pmod{H} \iff a - b \in H$. これは、$n$ を法とする整数の合同の一般化になっている。

定理 24　$|G/H| = |G\backslash H|$ である。

(証明) $a \in G \mapsto a^{-1} \in G$ は全単射である。よって、$ah \mapsto (ah)^{-1} = h^{-1}a^{-1}$ も全単射のため、$aH = Ha^{-1}$. よって、$G = \bigcup_{a\in A} aH$ を H の左剰余類による分割とすると、$G = \bigcup_{a\in A} Ha^{-1}$ も H の右剰余類による分割になる。剰余類（同値類）の分類は A の選び方によらず一意だから結局 $|G/H| = |G\backslash H|$ を満たす。

定義 25　$[G : H] := |G/H| = |G\backslash H|$ を G における H の**指数 (index)** という。

定理 26（Lagrange **の定理**）　H を群 G の部分群とすると、$|G| = [G : H]|H|$.

(証明) $G = \bigcup_{a\in A} aH$ を H の左剰余類による分割とする。このとき $[G : H] = |A|$ である。さらに任意の $a \in A$ にたいして、$h(\in H) \mapsto ah \in aH$ は全単射。よって、

$$|G| = |\bigcup_{a\in A} aH| = \bigcup_{a\in A} |aH| = |A| \cdot |H|.$$

ゆえに $|G| = [G : H]|H|$。 ■

3.3　Fermat **の小定理、**Euler **の定理**

定理 27（Fermat **の小定理**）　$a \in \mathbb{Z}\backslash\{0\}$、$p$ は素数の時、

$$a^{p-1} = 1 \bmod p$$

が成り立つ

(証明) $(\mathbb{Z}/p\mathbb{Z})^\times$ は群で位数 $p-1$ である（$|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$）。$a$ は $(\mathbb{Z}/p\mathbb{Z})^\times$ の元とみなせる。よって、$\langle a\rangle$ は $(\mathbb{Z}/p\mathbb{Z})^\times$ の部分群であり、Lagrange の定理により a の位数（$\langle a\rangle$ の元の個数）は、$p-1$ の約数。よって、$a^{p-1} = 1 \in (\mathbb{Z}/p\mathbb{Z})^\times$.

定理 28（Euler **の定理**）　$n \in \mathbb{N}$、$(a, n) = 1$ なる $a \in \mathbb{Z}$ に対して、

$$a^{\phi(n)} = 1 \bmod n$$

が成り立つ。

(証明) $(\mathbb{Z}/n\mathbb{Z})^\times$ の位数は $\phi(n)$ であるから。

3.4　**正規部分群** (Normal Subgroup) **と剰余類群** (residue class group)

H を群 $(G, \circ)$ の部分群。（左）剰余類の集合 G/H の元同士の演算を次のように定義してみる。

$$aH \circ bH := \{(a \circ h_i) \circ (b \circ h_j) | h_i, h_j \in H\}$$

これが、ある $cH \in G/H$ と一致して

$$cH = aH \circ bH$$

となって欲しいが通常はそううまくいかず、二項演算が定義できない。

定義 29（正規部分群 (Normal Subgroup)） H を群 $(G, \circ)$ の部分群。全ての $a \in G$ に対して

$$aH = Ha$$

が成立するとき、H を G の正規部分群とよび、$H \lhd G$ とかく。

G が可換群のとき、任意の部分群は正規部分群であることに注意。

H が正規部分群ならば、

$$aH \circ bH = (a \circ b)H$$

となるので、剰余類同士の二項演算が定義できることになる [*1]。

結果、剰余類の商集合 G/H は上記の演算により群になる。G/H を**剰余（類）群**とよぶ。

定理 30 H が G の正規部分群なら、G/H $(= G\backslash H)$ は、群になる。

問題 31 定理 30 を証明せよ。

定理 32 N を群 $(G, \circ)$ の部分群とする。以下の条件は全て等しい。

1. N は G の正規部分群。すなわち $N \lhd G$.
2. 全ての $a \in G$ に対して、$aN = Na$.
3. 全ての $a \in G$ に対して、$aN \subset Na$.
4. 全ての $a \in G$ に対して、$Na \subset aN$.
5. 全ての $a \in G$ に対して、$N = aNa^{-1}$.
6. 全ての $a \in G$ に対して、$N \subset aNa^{-1}$.
7. 全ての $a \in G$ に対して、$aNa^{-1} \subset N$.

3.5 （群）準同型写像

$(G, \circ)$, $(G', \cdot)$ を群とする。$f : G \to G'$ を G から G' への写像とする。e, e' をそれぞれ群 G, G' の単位元とする。

定義 33（像と核） $\mathsf{Im}(f) := \{f(x) \,|\, x \in G\}$ を f の像 (image)、$\mathsf{Ker}(f) := \{x \in G \,|\, f(x) = e' \in G'\}$ を f の核 (kernel) という。

定義 34（準同型写像） 全ての元 $x, y \in G$ に対して、$f(x \circ y) = f(x) \cdot f(y)$ をみたすとき、f は（群）準同型写像であるという。

命題 35 e, e' を G,G' の単位元とする。$f : G \to G'$ が群の準同型写像であれば、$f(e) = e'$ が成立。

命題 36 $f : G \to G'$ が群の準同型写像であれば、任意の元 $x \in G$ に対して、$f(x^{-1}) = f(x)^{-1}$ が成立。

命題 37 $f : G \to G'$ が群の準同型写像であれば、$\mathsf{Im}(f)$ は G' の部分群。

(証明) [命題 35 の証明] $e \circ e = e$ であるから、準同型性より、$f(e) = f(e \circ e) = f(e) \cdot f(e)$. 両辺に $f(e)^{-1}$

[*1] 逆に、$aH \circ bH := (a \circ b)H$ を二項演算の定義としても良い。このとき H が正規部分群であると、aH, bH の代表元 a', b' の取り方によらず、常に $a' \cdot b' \in (a \cdot b)H$ となるので、定義として意味がある (well-defined) ものとなる。

をかけると、$e' = f(e)$.

(証明) [命題 36 の証明] 任意の $x \in G$ に対して、$x \circ x^{-1} = e$ より、$f(x \circ x^{-1}) = f(x) \cdot f(x^{-1}) = f(e) = e'$. よって、$f(x)^{-1}$ を $f(x) \cdot f(x^{-1}) = e'$ の両辺に左からかけて、$f(x^{-1}) = f(x)^{-1}$ をえる。

(証明) [命題 37 の証明] 省略。証明してみよ。

定義 38（同型写像） 全単射な準同型写像 $f : G \to G'$ を同型写像とよび、G と G' は同型であるといい、$G \cong G'$ とかく。

命題 39 準同型写像 $f : G \to G'$ が同型写像である必要十分条件は、$\mathsf{Im}(f) = G'$ かつ、$\mathsf{Ker}(f) = \{e\}$.

(証明) [命題 39 の証明] 全射の必要十分条件が $\mathsf{Im}(f) = G'$ なのは明らか。単射の必要十分条件は、

$$\forall x_1, x_2 \in G : \quad f(x_1) = f(x_2) \quad \Longrightarrow \quad x_1 = x_2.$$

これは、準同型性と $f(x^{-1}) = f(x)^{-1}$ から、

$$\forall x_1, x_2 \in G : \quad f(x_1 \circ {x_2}^{-1}) = e' \quad \Longrightarrow \quad x_1 \circ {x_2}^{-1} = e.$$

と等しい。これは、

$$\forall x \in G : \quad f(x) = e' \quad \Longrightarrow \quad x = e.$$

と等しい。よって、$\mathsf{Ker}(f) = \{e\}$ と等しい。

3.6 群の準同型定理

定理 40（群準同型定理） $f : G \to G'$ を群 G から群 G' への準同型写像とする。 このとき、次が成り立つ。

1. $\mathsf{Im}(f)$ は G' の部分群
2. $\mathsf{Ker}(f)$ は正規部分群
3. $\bar{f} : x \circ \mathsf{Ker}(f) \in G/\ker(f) \mapsto f(x) \in G'$ という写像は準同型写像であり、

$$G/\mathsf{Ker}(f) \cong \mathsf{Im}(f)$$

特に $\mathsf{Im}(f) = G'$（全射）であれば、$G/\mathsf{Ker}(f) \cong G'$ が得られる。

(証明)

(1) $\mathsf{Im}(f)$ は G' の部分群の証明（省略）。

(2) $\mathsf{Ker}(f)$ は次のことから正規部分群である。全ての $a \in G$, 全ての $x \in \mathsf{Ker}(f)$ に対して、

$$f(a \circ x \circ a^{-1}) = f(a) \cdot f(x) \cdot f(a^{-1}) = f(a) \cdot e' \cdot f(a)^{-1} = e'.$$

よって、全ての $a \in G$ に対して、$a \circ \mathsf{Ker}(f) \circ a^{-1} \subset \mathsf{Ker}(f)$. よって、$\mathsf{Ker}(f)$ は正規部分群。

(3) まず、$\bar{f}$ が well-defined な写像であることを確認する。以下、$N := \mathsf{Ker}(f)$ と書く。

$$\bar{f} : xN \in G/N \mapsto f(x) \in G'$$

類別の定義から任意の $y \in xN$ に対して、$xN = yN$ よって、$\bar{f} : G/N \to G'$ が矛盾なく（well-defined に）定義される条件は、$\bar{f}(xN) = \bar{f}(yN)$ であり、これは $f(x) = f(y)$ と同じことである。さらに f の準同型性より、$f(x) = f(y) \Leftrightarrow f(x)f(y)^{-1} = f(xy^{-1}) = e'$.

$y \in xN$ より、ある $n \in N$ があって $y = xn$ を満足することに注意すると、$xy^{-1} = x(xn)^{-1} = xn^{-1}x^{-1}$。これから

$$f(xy^{-1}) = f(xn^{-1}x^{-1}) = f(x)f(n)^{-1}f(x)^{-1} = f(x)e'^{-1}f(x)^{-1} = f(x)e'f(x)^{-1} = f(x)f(x)^{-1} = e'.$$

(すなわち、$xy^{-1} \in N$)。よって、$xN = yN$ なる全ての x, y に対して、$\bar{f}(xN) = \bar{f}(yN)$ を示せたので、写像 $\bar{f}$ は well-defined に定義されている。

次に、N が正規部分群なので、$xN \circ yN = (x \circ y)N$ が言え、

$$\bar{f}((xN) \circ (yN)) = \bar{f}((x \circ y)N) = f(x \circ y) = f(x) \cdot f(y) = \bar{f}(xN)\bar{f}(yN).$$

よって、準同型写像であることも示せた。後は単射を言えば良い。単射の必要十分条件は、

$$\bar{f}(xN) = \bar{f}(yN) \Longrightarrow xN = yN$$

となること。$\bar{f}(xN) = \bar{f}(yN) \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x \circ y^{-1}) = e' \Leftrightarrow x \circ y^{-1} \in N(:= \mathsf{Ker}(f)) \Leftrightarrow x \in yN \Leftrightarrow xN = yN$. よって、$\bar{f}$ は単射。

$\mathsf{Im}(f) = G'$ であれば、全射であるので、$G/\mathsf{Ker}(f) \cong G'$ が得られる。 ■

二つの群が同型であることを示すのは簡単でないことが多く、準同型定理が威力を発揮する。

- G を群、$a \in G$ とする。$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ は有限巡回群で位数を q とすると、写像 $f : x \in \mathbb{Z} \mapsto a^x \in G$ は準同型写像だから、準同型定理から
$$\mathbb{Z}/q\mathbb{Z} \cong \langle a \rangle.$$
ここで $\mathbb{Z}/q\mathbb{Z}$ は加法群。
- 群 $(\mathbb{Z}, +)$ から 群 $(\mathbb{Z}/p\mathbb{Z}, +)$ への写像を
$$f_p : x \mapsto (x \bmod p) + p\mathbb{Z}$$
で定義する。$n = p_1 \cdot p_2 \cdots p_\ell$ ($p_1, \ldots, p_k$ は互いに素の整数) とし、群 $\mathbb{Z}$ から 直積群 $\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell\mathbb{Z}$ への写像を
$$f_n : x \mapsto (f_{p_1}(x), \ldots, f_{p_\ell}(x))$$
と定義すると、これは全射準同型写像。よって、準同型定理から
$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell\mathbb{Z}.$$
- 写像 $x \in \mathbb{Z} \mapsto i^x \in \mathbb{C}^\times (= \mathbb{C} - \{0\})$ から、
$$\mathbb{Z}/4\mathbb{Z} \cong \langle i \rangle.$$
ここで $\mathbb{Z}/4\mathbb{Z}$ は加法群。
- 群 $(\mathbb{R}, +)$ から 群 $(\mathbb{C}^\times, \cdot)$ への写像を $x \mapsto e^{2\pi\imath x}$ で定義すると、
$$\mathbb{R}/\mathbb{Z} \cong T := \{z \in \mathbb{C}^\times \mid |z| = 1\}.$$
- $M_n(\mathbb{R})$ を実数をエントリーに持つ n 次正方行列。一般線形群 $GL_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$、特殊線形群 $SL_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) \mid \det(A) = 1\}$ とすると、(全射) 準同型写像 $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ により、
$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times.$$

4 環の話

ここからは環に関する話。

4.1 部分環

定義 41（部分環） 環 $(R,+,\cdot)$ の部分集合 S が、環 R の演算に関して環をつくるとき、S を R の**部分環**という。

定理 42 S が R の部分環になる必要十分条件は、

$$\forall a,b\in S:\quad a-b\in S,\quad ab\in S$$

が成立することである。

4.2 イデアル (ideal)

定義 43（イデアル） 環 $(R,+,\cdot)$ の部分集合 I が、(1), (2) を満たす時、左イデアル、(1), (3) を満たす時、右イデアル、(1), (2), (3) を満たす時、両側イデアル、または単に**イデアル**という。

1. I は加法群 $(R,+)$ の部分群
2. $r\in R, x\in I \implies r\cdot x\in I.$
3. $r\in R, x\in I \implies x\cdot r\in I.$

- R が可換環なら、常に左（右）イデアルは両側イデアル。
- $n\mathbb{Z}$ は、整数環 $(\mathbb{Z},+,\cdot)$ のイデアル。$(n\mathbb{Z},+)$ は加法群で、任意の $a\in\mathbb{Z}, x\in n\mathbb{Z}$ に対して、$ax, xa\in n\mathbb{Z}.$
- $\{0\}$, R は、常に（可換とは限らない）環 R の両側イデアル。

4.3 剰余類環

環 $(R,+,\cdot)$ の左（右）イデアル I は $+$ に関して、可換群（加法群）であるから、群 $(R,+)$ の正規部分群。よって、群の時同様、剰余類群 R/I が定義され、各元（剰余類）は、$r+I:=\{r+i\,|\,i\in I\}$ $(r\in R)$。ここで、剰余類の乗法の意味ある定義をしたい。。

$$(r+I)\cdot(s+I):=(r\cdot s)+I$$

と乗法の二項演算を定義してみる。I が両側イデアルであると、

$$\{(r+i)\cdot(s+i')\,|\,i,i'\in I\}\subseteq(r\cdot s)+I$$

となるので、$(r+I)$, $(s+I)$ の各代表元 r',s' の選び方によらず、$r'\cdot s'\in(r\cdot s)+I$ が成り立つので、両側イデアルの場合は意味ある well-defined な二項演算を定義することができる。

定理 44 I を（両側）イデアルとする。上記のように定義された乗算により R/I は環になる。

定義 45（剰余類環） I を、環 $(R,+,\cdot)$ の両側イデアルとする。加法群 $(R,+)$ を（正規）部分群 $(I,+)$ を法として作った剰余類群 R/I に乗法の演算を、

$$(r+I)\cdot(s+I):=(r\cdot s)+I$$

で定義する。これにより定義された R/I を両側イデアル I を法とした剰余類環 (residue ring) という。

R が可換環であれば、R/I も可換環。

I を環 R の（両側）イデアルとする。$r' \in r+I$, $s' \in s+I$ とすると、合同の定義より $r' \equiv r \pmod{I}$, $s' \equiv s \pmod{I}$. さらに、$r's' - rs = r'(s'-s) + (r'-r)s \in I$ より、$r's' \equiv rs \pmod{I}$ となる。

4.4 環の準同型

R, R' を環とする。$f : R \to R'$ を R から R' への写像とする。

定義 46（環準同型写像） 全ての元 $x, y \in R$ に対して、

$$f(x+y) = f(x) + f(y)$$
$$f(x \cdot y) = f(x) \cdot f(y)$$

を満たす時、f を（環）準同型写像であるという。特に、f が全単射の時、（環）同型写像という。R, R' が環同型のとき、$R \cong R'$ とかく。

R の零元を 0, R' の零元を $0'$ とすると、$f(0) = 0'$ が常に成り立つが、両方に単位元が存在したとしても $f(1) = 1'$ は常に成り立つ訳では無い。

定理 47（環準同型定理） $f : R \to R'$ を環 R から環 R' への環準同型写像とする。 このとき、次が成り立つ。

1. $\mathsf{Im}(f) := \{f(x) \,|\, x \in R\}$ は R' の部分環
2. $\mathsf{Ker}(f) := \{x \in R \,|\, f(x) = 0' \in R'\}$ は R の両側イデアル
3. $\bar{f} : x + \mathsf{Ker}(f) \in R/\ker(f) \mapsto f(x) \in R'$ という写像は環準同型写像であり、

$$R/\mathsf{Ker}(f) \cong \mathsf{Im}(f).$$

特に $\mathsf{Im}(f) = R'$（全射）であれば、$G/\mathsf{Ker}(f) \cong R'$ が得られる。

実数係数の一変数多項式環 $\mathbb{R}[X]$ から、複素数体 $\mathbb{C}$ への写像 $\phi : \mathbb{R}[X] \to \mathbb{C}$

$$\phi : f(X) \mapsto f(i)$$

を考える。ϕ は全射準同型写像で、i は、$X^2+1=0$ の $\mathbb{C}$ での解であるから、$\mathsf{Ker}(\phi) = (X^2+1)$ であり、環準同型定理から、

$$R(X)/(X^2+1) \cong \mathbb{C}$$

が成り立つ。

4.5 環の直積

R_1, R_2 を環とする。R_1 と R_2 の直積集合

$$R_1 \times R_2 := \{(x_1, x_2) \,|\, x_1 \in R_1,\, x_2 \in R_2\}$$

は、自然な二項演算

$$(x_1, x_2) + (x_1', x_2') := (x_1 + x_1',\, x_2 + x_2')$$
$$(x_1, x_2) \cdot (x_1', x_2') := (x_1 \cdot x_1',\, x_2 \cdot x_2')$$

で環になる。群の時同様、n 個の直積も同様に環になる。

環の直積 $R_1 \times \cdots \times R_n$ の零元は $(0_{R_1}, \ldots, 0_{R_n})$. 全ての環が単位的であれば、直積も単位的で、$(1_{R_1}, \ldots, 1_{R_n})$ が（乗法の）単位元。

命題 48 $(R_1 \times \cdots \times R_n)^\times = R_1^\times \times \cdots \times R_n^\times$.

一般に、モノイド $G_1, \ldots, G_n$ に対して、$(G_1 \times \cdots \times G_n)^\times = G_1^\times \times \cdots \times G_n^\times$ が成り立つ。

命題 49 $R \cong R_1 \times \cdots \times R_n$ なら、$R^\times = R_1^\times \times \cdots \times R_n^\times$.

$R^\times \cong (R_1 \times \cdots \times R_n)^\times$ を示せば、命題 (48) より成り立つ。

命題 50 $(0_{R_1}, \ldots, R_i, \ldots, 0_{R_n})$ は、直積環 $(R_1 \times \cdots \times R_n)$ のイデアル

$R_1, \cdots, R_n$ が可換でなくとも、$(0_{R_1}, \ldots, R_i, \ldots, 0_{R_n})$ は（両側）イデアルになる。

4.6 剰余類環 $\mathbb{Z}/n\mathbb{Z}$ の分解

$n = p_1 \cdots p_\ell$（$p_1 \ldots p_\ell$ は互いに素）とする。
環 $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/p_1\mathbb{Z}$, …, $\mathbb{Z}/p_\ell\mathbb{Z}$ に対して、環準同型定理および、命題 (49) から、

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell\mathbb{Z} \\ (\mathbb{Z}/n\mathbb{Z})^\times &\cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_\ell\mathbb{Z})^\times \end{aligned}$$

が成り立つ。よって、

$$x \in (\mathbb{Z}/n\mathbb{Z})^\times \leftrightarrow (x_1, \ldots, x_\ell) \in (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_\ell\mathbb{Z})^\times$$

と

$$y \in (\mathbb{Z}/n\mathbb{Z})^\times \leftrightarrow (y_1, \ldots, y_\ell) \in (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_\ell\mathbb{Z})^\times$$

に対して、

$$x \cdot y \leftrightarrow (x_1 \cdot y_1, \ldots, x_\ell \cdot y_\ell)$$

が成立。

4.7 中国人の剰余定理 (Chinese Remainder Theorem)

「孫子算経」(Sunzi Suanjing) に記された問題：「3 で割れば 2 が余り、5 で割れば 3 が余り、7 で割れば 2 が余るような数は何か？」

$$\begin{aligned} x &= 2 \bmod 3 \\ x &= 3 \bmod 5 \\ x &= 2 \bmod 7 \end{aligned}$$

この解法は、$n = p_1 p_2 \cdots p_k$（$p_1, \ldots, p_k$ は互いに素の整数）のとき、

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z}$$

の環同型写像とその逆写像の計算方法を与えている。

準同型定理より、

$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

が次のように示せる。

- $f : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ を、

$$f(x) := \Big([x]_3,\, [x]_5,\, [x]_7\Big)$$

と定義したとき、これは準同型写像である。ここで、$[x]_n$ は、x を含む同値類（剰余類）$x + n\mathbb{Z}$ とする。すなわち

$$[x]_n := x + n\mathbb{Z}.$$

- $\mathsf{Ker}(f) = 105\mathbb{Z}$ であることが示せる（$105 = 3 \cdot 5 \cdot 7$）。
- よって、上記同型が示せる。

■CRT の一般解法　一般に、$n = p_1 \cdot p_2 \cdots p_\ell$（$p_i$ らは互いに素）の時、$\chi_1, \ldots, \chi_\ell \in \mathbb{Z}$ を

$$\frac{n}{p_1}\chi_1 + \frac{n}{p_2}\chi_2 + \cdots + \frac{n}{p_\ell}\chi_\ell = 1 \tag{2}$$

なる整数とする。$a_1, \ldots, a_n \in \mathbb{Z}$ の最大公約数が 1 のとき、（整数係数）一次不定方程式

$$a_1 X_1 + \cdots + a_n X_n = 1$$

は整数解を持つ。式 (2) は、p_i らが互いに素なので $(\frac{n}{p_1}, \ldots, \frac{n}{p_\ell}) = 1$ で、$\chi_1, \ldots, \chi_\ell \in \mathbb{Z}$ は整数解をもつ。このとき、f の逆写像の同型写像 $f^{-1} : \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_\ell\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ は

$$f^{-1}(x_1, \ldots, x_\ell) := x_1\frac{n}{p_1}\chi_1 + x_2\frac{n}{p_2}\chi_2 + \cdots + x_n\frac{n}{p_\ell}\chi_\ell$$

である。f^{-1} は f の逆写像である。すなわち、

$$x \in \mathbb{Z}/n\mathbb{Z} \quad \underset{\xleftarrow{f^{-1}}}{\xrightarrow{f}} \quad (x_1, \ldots, x_\ell) \in \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell\mathbb{Z}$$

f の逆写像であることは、次のことから確認できる。

$$\frac{n}{p_i}\chi_i = 1 \pmod{p_i}, \qquad \frac{n}{p_j}\chi_j = 0 \pmod{p_i} \quad (j \neq i)$$

であることに注意すると、

$$x_i \equiv x_1\frac{n}{p_1}\chi_1 + \cdots + x_i\frac{n}{p_i}\chi_i + \cdots + x_n\frac{n}{p_\ell}\chi_\ell \pmod{p_i}$$

である。よって、$x = x_1\frac{n}{p_1}\chi_1 + x_2\frac{n}{p_2}\chi_2 + \cdots + x_i\frac{n}{p_i}\chi_i + \cdots + x_n\frac{n}{p_\ell}\chi_\ell$ は、$f(x) = ([x_1]_{p_1}, \ldots, [x_\ell]_{p_\ell})$ である。

■孫子算経の回答　同型写像 $f : \mathbb{Z}/105\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ の逆写像 f^{-1} は、

$$f^{-1}(x_3, x_5, x_7) := \Big[-35x_3 + 21x_5 + 15x_7\Big]_{105}.$$

ここで、$35 \cdot (-1) + 21 \cdot 1 + 15 \cdot 1 = 1$ を使っている。今回のケース、$x_3 = 2$, $x_5 = 3$, $x_7 = 2$ なので、

$$f^{-1}(2, 3, 2) = [23]_{105} = 23 + 105\mathbb{Z}.$$

である。

問題 51 「3で割れば2が余り、5で割れば3が余り、7で割れば2が余るような数と、3で割れば1が余り、5で割れば2が余り、7で割れば5が余るような数を掛け合わせたとき、105 で割ると幾つあまりがでるか？」

$$\begin{aligned}&(2\cdot 1 \bmod 3)\cdot(-35)+(3\cdot 2 \bmod 5)\cdot 21+(2\cdot 5 \bmod 7)\cdot 15\\ =&2\cdot(-35)+1\cdot 21+3\cdot 15=-4.\end{aligned}$$

答えは、$[-4]_{105}=[101]_{105}$.

4.8 整域、約元、倍元、素元、既約元

定義 52（零因子） R を単位的可換環（1 を持つ可換環）とする。$a,b\in R$ に対して、$a\cdot b=0$ だが、$a\neq 0$ かつ、$b\neq 0$ のとき、a,b を R の零因子 (zero-divisor) とよぶ。

定義 53（整域） 単位的可換環 R において、零因子が存在しないとき、R を整域 (integral domain) とよぶ。

すなわち、R が整域なら、$ab=0$ なら、$a=0$ または $b=0$ が成り立つ。

- 体は、必ず整域。
- 整数環 $\mathbb{Z}$ は整域。
- 環 $\mathbb{Z}/15\mathbb{Z}$ は整域ではない。$3,5$ は、$\mathbb{Z}/15\mathbb{Z}$ の零因子。
- 環 $\supset$ 可換環 $\supset$ 単位的可換環（単位元を持つ） $\supset$ 整域（零因子持たない）

定義 54（約元、倍元） R を整域とする。$a,b\in R$ に対して、ある $x\in R$ が存在して、$a\cdot x=b$ のとき、$a|b$ とかき、a を b の約元 (divisor)、b を a の倍元 (multiple) とよぶ

- $\mathbb{Z}$: 約数、倍数　vs　整域 R: 約元、倍元
- $x\in R^\times \iff x|1$.

定義 55（素元、既約元） R を整域とする。

- p が素元とは、$p\notin R^\times$ であり、

$$\forall a,b\in R:\quad p|ab \quad\Longrightarrow\quad p|a \text{ or } p|b$$

  を満たすときをいう。
- q が既約元とは、$q\notin R^\times$ であり、次をみたすとき。

$$\forall x,y\in R:\quad q=xy \quad\Longrightarrow\quad x\in R^\times \text{ or } y\in R^\times$$

  を満たすときをいう。

- 「素元 $\Longrightarrow$ 既約元」は常に成立。一般には「既約元 $\not\Longrightarrow$ 素元」
- 整域 $\mathbb{Z}$ の素元は、$\pm$ 素数 。$\mathbb{Z}^\times=\{\pm 1\}$ より、整域 $\mathbb{Z}$ の既約元は、$\pm$ 素数。よって、整域 $\mathbb{Z}$ では、素元 = 既約元.

4.9 ユークリッド整域

定義 56（ユークリッド整域） R を整域とする。R が、ユークリッド整域 (Euclidean domain) とは、ある写像 $\lambda : R \to \mathbb{Z}^{\geq 0}$ が存在して次をみたすときである。

- 全ての $x \neq 0$ なる $x \in R$ に対して、$\lambda(0) < \lambda(x)$.
- 全ての $x \neq 0$ なる $x \in R$ と $d \in R$ に対して、ある $q, r \in R$ が存在して、$x = q \cdot d + r$ かつ $\lambda(r) < \lambda(d)$.

- 「余りつき割り算」ができるものをユークリッド整域という
- $\mathbb{Z}$ はユークリッド整域。$\lambda(x) := |x|$ とせよ。
- K を体とすると、一変数多項式環 $K[X]$ もユークリッド整域。$f \in K[X]$ に対して、$\lambda(f) := \deg(f)$ とせよ。

4.10 単項イデアル、素イデアル、極大イデアル、単項イデアル整域

定義 57（単項イデアル） R を単位的可換環とする（単位元 1 をもつ可換環）。$a \in R$ に対して、

$$(a) := \{r \cdot a \,|\, r \in R\}$$

と定義し、(a) を R の単項イデアルとよぶ。

定義 58（素イデアル） R を環、I を R のイデアルとする（ただし、$I \neq R$）。

$$I \neq R,\, a \cdot b \in I \quad \Longrightarrow \quad a \in I \text{ or } b \in I.$$

をみたすとき、I を素イデアルとよぶ。

命題 59 R を単位的可換環とすると、$a \in R$ が素元 $\Longleftrightarrow$ (a) が素イデアル。

定義 60（極大イデアル） R を環、I を R のイデアルとする（ただし、$I \neq R$）。$I \subset \tilde{I} \subset R$ なるイデアル $\tilde{I}$ は、$\tilde{I} = I$、または $\tilde{I} = R$ しか存在しないとき、I を極大イデアル (maximal ideal) という。

定義 61（単項イデアル整域） R を整域とする。R の全てのイデアルが単項イデアルになるとき、R を単項イデアル整域 (principal ideal domain (PID)) とよぶ。

定理 62 単項イデアル整域 R では次のことが成り立つ。

- $a \in R$ が既約元 $\Leftrightarrow$ a が素元 $\Leftrightarrow$ (a) が素イデアル.
- I が R の素イデアル $\Leftrightarrow$ I が極大イデアル.

よって、R が単項イデアル整域の時、

$$p \text{ が既約元} \;\Leftrightarrow\; p \text{ が素元} \;\Leftrightarrow\; (p) \text{ が素イデアル} \quad \Leftrightarrow\; (p) \text{ が極大イデアル}$$

が成り立つ。

ユークリッド整域 $\subset$ 単項イデアル整域である。さらに、一意分解整域というのがあって、

$$\text{ユークリッド整域} \;\subset\; \text{単項イデアル整域} \;\subset\; \text{一意分解整域.}$$

一意分解整域であれば、各元が素元の積に一意に分解できる（素因数分解の一般化）。

R を可換環とすると、

$$(a_1, \ldots, a_n) := \{r_1 \cdot a_1 + \cdots + r_n \cdot a_n \,|\, r_1, \ldots, r_n \in R\}$$

はイデアルである。R を単項イデアル整域とすると、ある $a \in R$ が存在して

$$(a_1, \ldots, a_n) = (a).$$

a を、$a_1, \ldots, a_n$ の**最大公約元**という。$R = (1)$ であることに注意。$(a_1, \ldots, a_n) = (1)$ であれば、ある $r_1, \ldots, r_n \in R$ が存在して、

$$r_1 \cdot a_1 + \cdots + r_n \cdot a_n = 1.$$

$\mathbb{Z}$ はユークリッド整域なので単項イデアル整域。よって、$\gcd(a_1, \ldots, a_n) = 1$ であれば、1 は、$a_1, \ldots, a_n$ の最大公約元であるので、ある $r_1, \ldots, r_n \in \mathbb{Z}$ が存在して $r_1 \cdot a_1 + \cdots + r_n \cdot a_n = 1$ を満たす。さらに、$\mathbb{Z}$ の全てのイデアルは単項イデアル $(n) = n\mathbb{Z}$ であり、p が素数の時 $p\mathbb{Z}$ は素イデアル。逆に I が素イデアルの時、ある素数 p があって $I = p\mathbb{Z}$ を満足する。

5 体の話

定義 63（体の定義） 二つの二項演算 $(+, \cdot)$ が定義された集合 K が体 (field) とは、$(K, +, \cdot)$ が次の条件を満たすときである。

- $(K, +, \cdot)$ が単位的可換環（零元 0 と単位元 1 をもち、演算 $\cdot$ に関して可換)。
- K の単元群（乗法群）$K^\times$ が、$K^\times = K - \{0\}$ を満たす。

定義 64（体の標数）

体 K の単位元 1 の n 個の和 $1 + \cdots + 1$ が零元になるとき、すなわち

$$1 + \cdots + 1 = 0$$

となる整数があるとき、その最小の正の整数を体 K の標数 (characteristic) といい、$\mathsf{chr}(K)$ と表す。そのような整数が存在しない時、$\mathsf{chr}(K) = 0$ と定義する

- p を素数とすると、$\mathbb{Z}/p\mathbb{Z}$ は体。その時 $\mathsf{chr}(\mathbb{Z}/p\mathbb{Z}) = p$.
- 体 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ の標数は 0.

定理 65 R を単位的可換環、I を R のイデアルとする。このとき、

$$I \text{ が極大イデアル} \quad \Longleftrightarrow \quad R/I \text{ が体}$$

定理 66 任意の体 K の乗法群 $K^\times = K - \{0\}$ の有限部分群は必ず巡回群である。

系 67 有限体 $\mathbb{F}_q$ の乗法群 $\mathbb{F}_q^\times$ は、巡回群である。

5.1 一変数多項式環

Proposition 68 K を体とすると、一変数多項式環 $K[X]$ は、ユークリッド整域（$\lambda(f) := \deg(f)$）である。

- ユークリッド整域は、単項イデアル整域であるから、

  $f(X)$ が K 上の既約多項式 $\Leftrightarrow$ $f(X)$ が素元 $\Leftrightarrow$ $(f(X))$ が素イデアル $\Leftrightarrow$ $(f(X))$ が極大イデアル.

- K が体であるので、$f(X)$ が K 上の既約多項式なら、$K[X]/(f(X))$ は体。

5.2 有限体 $\mathbb{F}_q$

有限体は位数（元の個数）q のみで構造が決まる。位数 q の有限体を $\mathbb{F}_q$ と書く。そのとき、必ず $q = p^r$（p は素数）の形をしており、p は、$\mathbb{F}_q$ の標数になる $\mathsf{chr}(\mathbb{F}_q) = p$. 分野によっては $GF(p^r)$ と書いたりもする。q が素数の時、$\mathbb{F}_q$ を素体という。

$q = p^r$ とすると、任意のモニックで（最高次係数が 1 の）$\mathbb{F}_p$ 上既約な r 次多項式 $f(X) \in \mathbb{F}_p[X]$ $(\deg(f) = r)$ を法とする剰余環と同型になる。

$$\mathbb{F}_q \cong \mathbb{F}_p[X]/f(X)$$

上の結果により、$\mathbb{F}_q$ の元は、剰余類環 $\mathbb{F}_p[X]/f(X)$ の元で表すことができ、代表元を $\mathbb{F}_p[X]$ 上の $(r-1)$ 次多項式で表現できる。そのとき演算は

$$a(X) + b(X) := a(X) + b(X) \bmod f(X)$$
$$a(X) \cdot b(X) := a(X) \cdot b(X) \bmod f(X)$$

で定義できる（$\deg(a(X)), \deg(b(X)) \leq (r-1)$）。

付録 A　定義

定義 69（群の定義） 集合 G が二項演算 $\circ$ に対して以下を満たすとき、$(G, \circ)$ を群 (group) と言う。

- G_0（二項演算）二項演算 $\circ : G \times G \to G$ が定義されている.
- G_1（結合法則） $\forall a, b, c \in G :\quad (a \circ b) \circ c = a \circ (b \circ c)$.
- G_2（単位元の存在） $\exists e \in G, \forall a \in G :\quad a \circ e = e \circ a = a$.
- G_3（逆元の存在） $\forall a \in G, \exists a^{-1} \in G :\quad a \circ a^{-1} = a^{-1} \circ a = e$.

G_0 を満たすものをマグマ。G_0, G_1 を満たすものを**半群**。G_0, G_1, G_2 を満たすものを**モノイド（単位的半群）**とよぶ。

$\forall a, b \in G : a \circ b = b \circ a$ なら、G を**可換群、またはアーベル群**と呼ぶ。しばしば、可換群の演算を $+$ で書き、その時は特に**加法群**と呼ぶ。元の個数が有限個の群を**有限群**と呼ぶ。群（環、体）の元の個数を**位数**と呼ぶ。

注釈 70（群の直積） G_1, G_2 を群とする。G_1 と G_2 の直積集合

$$G_1 \times G_2 := \{(x_1, x_2) \,|\, x_1 \in G_1,\, x_2 \in G_2\}$$

は、自然な二項演算

$$(x_1, x_2) \circ (x_1', x_2') := (x_1 \circ x_1',\, x_2 \circ x_2') \in G_1 \times G_2$$

で群になる。n 個の直積も同様に群になる。

定義 71（環の定義） 二つの二項演算 $(+, \cdot)$ が定義された集合 R が環 (ring) とは、$(R, +, \cdot)$ が次の条件を満たすときである。

- R_1: $(R, +)$ が加法群（＝可換群＝アーベル群）である。
- R_2: $(R, \cdot)$ は半群。
- R_3: 分配法則が成り立つ。

  $$\forall a, b, c \in R :\qquad (a + b) \cdot c = (a \cdot c) + (b \cdot c),\quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

  が成立する。

特に、$(R,\cdot)$ が可換律をみたすとき、**可換環**という。

注釈 72　$R^\times := \{a \in R \,|\, \exists a^{-1} \in R\}$ は群になる。$R^\times$ を（R の）**乗法群**と呼ぶ。

注釈 73　慣例として、

- $(+,\cdot)$ を加法、乗法といってしまうことが多い。
- $+$ に関する単位元を 0 と書くことが多い。
- $\cdot$ に関する単位元（があれば）1 と書いてしまうことが多い。

付録 B　モノイドの性質

モノイド（単位的半群）で結構多くのことがいえる。モノイドで成り立つことは、群でも成り立つことに注意。$(G,\circ)$ をモノイドとする。

命題 74（単位元の一意性）　G の単位元 e は、一意である（単位元 e, e' が存在するならば、$e = e'$ である）。

命題 75（逆元の一意性）　$a \in G$ の逆元 $a^{-1} \in G$ が存在する場合、それは一意である（a の逆元 x, y が存在するならば、$x = y$ である）。

結合法則を満たさないマグマの場合、逆元が存在しても一意とは限らない。

命題 76（可逆元は移行可）　$a \in G$ が可逆ならば、方程式 $a \circ x = b$ の解は一意であり、$x = a^{-1} \circ b$.

命題 77　単位元 e の逆元は、e 自身である。

命題 78　$a, b \in G$ が両方とも可逆のとき、$a \circ b$ も可逆で、その逆元は

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

命題 79　$a \in G$ が可逆であるとき、a^{-1} も可逆で、$(a^{-1})^{-1} = a$ である。

命題 80　G の可逆元の集合 $G^\times$ は群である。