暗号の数理要綱 #2

1 群と演算

1.1 2 項演算

定義 1.1 A を集合とする。積集合 $A \times A$ から A への写像を，A 上の **2 項演算** (*binary operation*) という。

例 1.2 (1) $A = \{ a \}$ のように一つの要素からなる集合の場合は，A 自身の積集合は $A \times A = \{ (a, a) \}$ となり，やはり一つの要素からなるので，2 項演算は，$(a, a) \longmapsto a$ というもの一つしかない。

(2) $A = \{ a, b \}$ のように，2 つの要素からなる集合の場合は，積集合は $A \times A = \{(a, a), (a, b), (b, a), (b, b)\}$ となり 4 個の要素からなる。2 項演算は，これらのそれぞれに a 又は b のどちらかを対応させることになるので，全部で $2^4 = 16$ 通りある。

$X = \{ 0, 1 \}$ とすると，X の演算は 16 通りある。

$$\varphi_0(0, 0) = 0, \quad \varphi_0(0, 1) = 1, \quad \varphi_0(1, 0) = 1, \quad \varphi_0(1, 1) = 0$$

と定義すると φ_0 は **bit 和**として知られている演算である。

$$\varphi_1(0, 0) = 0, \quad \varphi_1(0, 1) = 0, \quad \varphi_1(1, 0) = 0, \quad \varphi_1(1, 1) = 1$$

と定義すると φ_1 は **bit 積**として知られている演算である。

$$\max(0, 0) = 0, \quad \max(0, 1) = 1, \quad \max(1, 0) = 1, \quad \max(1, 1) = 1$$

と定義すると max は**論理和**として知られている演算である。

$$\min(0, 0) = 0, \quad \min(0, 1) = 0, \quad \min(1, 0) = 0, \quad \min(1, 1) = 1$$

と定義すると min は**論理積**として知られている演算である。

bit 積は論理積と同じものである。bit 和は論理和とは異なる。bit 和は**排他的論理和**と呼ばれる演算と同じものである。

演習問題 1.1 $A = \{ a, b, c \}$ とする。A の 2 項演算は全部で何個存在するか?

$\varphi : A \times A \to A$ をひとつの 2 項演算とする。任意の $a, b \in A$ に対して，$\varphi(a, b) \in A$ が定まる。これを略して，$\varphi(a, b) = a \cdot b \in A$ と書くことにしよう。

以下では，2 項演算は，主に $a \cdot b$ で表すことにする。(しかし，$a + b$ という記号を使うこともある。)

A 上の 2 項演算は単に $A \times A$ から A への写像のことだから，あらゆるものがあり得るわけだが，あまり一般的なものを考えても，役に立つ性質は期待できない。そこで，演算として，最低限の要求として，以下の条件を課すことにしよう。

結合律： 任意の $a, b, c \in A$ に対して，$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ が成り立つ。

ほとんどの代数的対象は結合律を満たす。群，環，体，加群，束 などが主な例だが，Lie 環，ケーリー代数のように結合律を満たさないものも存在する。

定義 1.3 結合律が成り立つような 2 項演算が定義された集合を**半群** (*semigroup*) という。

集合に適当に演算を定義しただけでは，結合律を満たすとは限らない。

例 1.4 例えば，$A = \{a, b\}$ において，

$$\begin{aligned} a \cdot a &= b \\ a \cdot b &= b \\ b \cdot a &= b \\ b \cdot b &= a \end{aligned}$$

という演算が定義されているとする。この時，

$$(b \cdot a) \cdot a = b \cdot a = b$$

だが，

$$b \cdot (a \cdot a) = b \cdot b = a$$

となり，$(b \cdot a) \cdot a \neq b \cdot (a \cdot a)$ であるので，結合律を満たさない。

演習問題 1.2　$A = \{\, a, b \,\}$ とする。A の演算で結合律を満たすようなものをすべて列挙せよ。

さてこの半群というのは，かなり一般的なものではあるが，半群として考えなければならないような数学的対象はいろいろあり，重要な概念である。

しかしこれだけでは概念としてちょっと広すぎるので，もう少し条件を付けて，議論をしやすくしてみよう。

演算と言えば，数の 0 や 1 のように，特別な性質を持つ元があるのが普通である。そこで，

定義 1.5 任意の $a \in A$ に対して $a \cdot e = e \cdot a = a$ となるような元 $e \in A$ が存在する時，それを**単位元** (*unit element*) と言う。

命題 1.6 単位元は，存在するならば，ただ一つである。

証明　e_1, e_2 を単位元とする。単位元の定義より，

$$e_1 = e_1 \cdot e_2 = e_2 \quad \blacksquare$$

定義 1.7 単位元 $e \in A$ が存在する時，$a \in A$ に対して $aa' = a'a = e$ となる元 a' を a の**逆元** (*inverse element*) と言う。

命題 1.8 逆元は，存在するならば，ただ一つである。

証明　a_1, a_2 を a の逆元とする。逆元の定義より，

$$a_1 = a_1 \cdot e = a_1 \cdot (a \cdot a_2) = (a_1 \cdot a) \cdot a_2 = e \cdot a_2 = a_2 \quad \blacksquare$$

この命題より，逆元は存在すれば唯一つなので，a の逆元を a^{-1} という記号で表すことにする。

1.2 群

定義 1.9 G を 2 項演算が定義されている集合とする。次の 3 つの条件が満たされる時，G を**群** (*group*) という。
(1) この演算は結合法則を満たす。
(2) 単位元が存在する。
(3) G の任意の元に対して，その逆元が存在する。

例 1.10

(1) $\mathbb{Z}$ を整数全体の集合，$\mathbb{Q}$ を有理数全体の集合，$\mathbb{R}$ を実数全体の集合，$\mathbb{C}$ を複素数全体の集合とする。加法 $+$ という演算に関して，$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は群となる。

(2) $\mathbb{Q}^* = \mathbb{Q} - \{0\}, \mathbb{R}^* = \mathbb{R} - \{0\}, \mathbb{C}^* = \mathbb{C} - \{0\}$ をそれぞれ，有理数全体の集合から 0 を除いた集合，実数全体の集合から 0 を除いた集合，複素数全体の集合から 0 を除いた集合とする。これらは，積 $\cdot$ という演算に関して群となる。

(3) $M_n(\mathbb{R})$ を成分が実数である n 次行列全体の集合とし，$M_n(\mathbb{Q})$ 成分が有理数である n 次行列全体の集合とする。$GL(n;\mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid \det A \neq 0 \}$ とすると，$GL(n;\mathbb{R})$ は行列の積という演算に関して群をなす。$GL(n;\mathbb{Q}) = \{ A \in M_n(\mathbb{Q}) \mid \det A \neq 0 \}$ とすると，$GL(n;\mathbb{Q})$ は行列の積という演算に関して群をなす。

(4) $P_n = \{1, \cdots, n\}$ を 1 から n までの自然数全体の集合とする。これを並べ替える操作全体の集合を $\mathcal{S}_n$ と書き，n **次対称群** (*symmetric group*) という。

単位元は，全く動かさない操作であり，ある並べ替え $\sigma \in \mathcal{S}_n$ の逆元は，それをもとの標準の位置に戻すような並べ替え $\sigma^{-1} \in \mathcal{S}_n$ である。

$\mathcal{S}_n$ の元は P_n から P_n への一対一上への写像と考えることができる。この立場で見ると，積は合成写像と考えることができる[(1)]。単位元は恒等写像であり，σ の逆元は写像 σ の逆写像になっている。

$\mathcal{S}_n$ は $n!$ 個の元を持っている。

演習問題 1.3 $\mathbb{Z}$ が加法に関して群になることを示せ。$\mathbb{R}^*$ が乗法に関して群になることを示せ。

演習問題 1.4 次を示せ。ただし n 次行列 A, B, C に対し結合法則 [$(AB)C = A(BC)$] が成立することなど線型代数の知識は既知としてよい。
(1) $GL(2;\mathbb{R})$ および $GL(2;\mathbb{Q})$ が群になることを示せ。
(2) $M_n(\mathbb{Z})$ を成分が整数である n 次行列全体の集合とする。$GL(n;\mathbb{Z}) = \{ A \in M_n(\mathbb{Z}) \mid \det A \neq 0 \}$ とすると，行列の積という演算に関して $GL(2;\mathbb{Z})$ は群にならないことを示せ。

演習問題 1.5 S_n が群になることを証明せよ。

定義 1.11 (1) 集合 A 上の 2 項演算 $\cdot$ は，任意の $a, b \in A$ に対して $a \cdot b = b \cdot a$ が成り立つ時，元 a と元 b は**可換** (*abelian,commutative*) であると言う。

---

(1)ただし積の表記には注意が必要である。σ をほどこした後 τ をほどこしたものを前者の場合通常 $\sigma \cdot \tau$ と書くが，写像の場合 $\tau \circ \sigma$ と書くことが多い。議論するときはどちらの表記に従っているかに注意すること。

(2) 群 G の元どうしがすべて可換の時，その群を**可換群** (*commutative group*) 又は**アーベル群** (*abelian group*) と言う。G がアーベル群の時，G の演算を $+$ という記号で表し，G の元 g の逆元を $-g$ と表すことが多い。

定義 1.12 G を群とする。G の部分集合 H が，G 上で定義された演算によって群となる時，H を G の**部分群** (*subgroup*) という。このとき

$$H < G$$

と表す。G 自身と，単位元のみの集合 $\{e\}$ は，明らかに G の部分群となる。これらを自明な部分群という。

例 1.13 (1) 加法に関して，$\mathbb{R}$ は $\mathbb{C}$ の部分群であり，$\mathbb{Q}$ は $\mathbb{R}, \mathbb{C}$ の部分群であり，$\mathbb{Z}$ は $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ の部分群である。m を整数とする。$m\mathbb{Z} = \{\, k \in \mathbb{Z} \mid k \text{ は } m \text{ で割り切れる} \,\}$ とすると，$m\mathbb{Z}$ は $\mathbb{Z}$ の部分群である。即ち

$$m\mathbb{Z} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$$

が成立する。

(2) 積に関して，$\mathbb{R}^*$ は $\mathbb{C}^*$ の部分群であり，$\mathbb{Q}^*$ は $\mathbb{R}^*, \mathbb{C}^*$ の部分群である。即ち

$$\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$$

が成立する。

(3)

$$SL(n;\mathbb{R}) = \{\, A \in M_n(\mathbb{R}) \mid \det A = 1 \,\}$$
$$SL(n;\mathbb{Q}) = \{\, A \in M_n(\mathbb{Q}) \mid \det A = 1 \,\}$$
$$SL(n;\mathbb{Z}) = \{\, A \in M_n(\mathbb{Z}) \mid \det A = 1 \,\}$$

とする。即ち行列式が 1 となるような n 次正方行列全体の集合とする。このとき

$$SL(n;\mathbb{Z}) < SL(n;\mathbb{Q}) < SL(n;\mathbb{R}) < GL(n;\mathbb{R})$$
$$SL(n;\mathbb{Q}) < GL(n;\mathbb{Q}) < GL(n;\mathbb{R})$$

が成立する。

演習問題 1.6 $m\mathbb{Z}$ が群になることを示せ。

演習問題 1.7 $SL(2;\mathbb{Z})$ が群になることを示せ。

次は星印付きの演習問題である。星印の付いた演習問題は理解を深めることに役立つが，全員が解くことを要求するものではない。意欲のある人はチャレンジして下さい。

演習問題 *1.8 $SL(n;\mathbb{Z})$ が群になることを示せ。

命題 1.14 [**部分群の判定条件**] G を群とし，H を G の空でない部分集合とする。H が部分群であるための必要十分条件は，次の (1), (2) が成り立つことである。

(1) 任意の $a, b \in H$ に対して $a \cdot b \in H$

(2) 任意の $a \in H$ に対して $a^{-1} \in H$

証明　H が部分群ならば (1), (2) が成立する。(1), (2) が成立するならば部分群になることを示せば良い。そのためには，H が群であることを言えば良い。まず，H 上の演算は G 上のものと同じなので，結合律は成り立っている。(2) より，任意の元には逆元が存在している。また (1) より，$a \cdot a^{-1} = e \in H$ より，単位元も存在している。故に，H は群となっている。 ∎

部分群であることの必要十分条件としては，次のような言い方もある。

命題 1.15 [**部分群の判定条件**] G を群とし，H を G の空でない部分集合とする。H が部分群であるための必要十分条件は，次の条件 $(*)$ が成り立つことである。

(∗) 任意の $a, b \in H$ に対して $a \cdot b^{-1} \in H$

演習問題 1.9　命題 1.15 を証明せよ。

1.3　2 項関係

定義 1.16 A を集合とする。$A \times A$ の部分集合 R が与えられた時，これを A 上の **2 項関係** (*binary relation*) と言う。

R が 2 項関係である時，(a, b) が R の元であるとき，即ち $(a, b) \in R \subseteq A \times A$ が成立することを $a \sim b$ と書くことがある。同様に元 (a, b) が R の元でないとき，即ち $(a, b) \notin R \subseteq A \times A$ が成立することを $a \not\sim b$ と書くことがある。

A 上の 2 項関係は，$A \times A$ の部分集合を指定すると定まるので，(A, R) と書くべきだが，関係を表す記号 $\sim$ を使って，$(A, \sim)$ と書くことが多い。

例 1.17 $A = \{1, 2, 3\}$ とする。

(1) $R = \{(1, 2), (1, 3), (2, 3)\}$ とする。この関係「$\sim$」は $a \sim b$ のとき通常 $a < b$ と表記される。

(2) $R = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$ とする。この関係「$\sim$」は $a \sim b$ のとき通常 $a \leq b$ または $a \leqq b$ と表記される。

定義 1.18 $(A, \sim)$ を A 上の 2 項関係とする。

(1) 「任意の $a \in A$ に対して $a \sim a$」が成り立つ時，この 2 項関係は**反射律** (*reflexive law*) を満たすと言う。

(2) 「$a \sim b$ ならば $b \sim a$」が成り立つ時，この 2 項関係は**対称律** (*symmetric law*) を満たすと言う。

(3) 「$a \sim b, b \sim c$ ならば $a \sim c$」が成り立つ時，この 2 項関係は**推移律** (*transitive law*) を満たすと言う。

(4) 「$a \sim b$ かつ $b \sim a$ ならば $a = b$」が成り立つ時，この 2 項関係は**反対称律** (*antisymmetric law*) を満たすと言う。

(5) 反射律，反対称律，推移律 が成立している時，この 2 項関係を**順序関係** (*order relation*) と言う。順序関係の場合は，$a \sim b$ と書く代わりに，$a \leq b$ あるいは $a \leqq b$ という記号を使うことが普通である。

(6) 反射律，対称律，推移律 が成立している時，この 2 項関係を**同値関係** (*equivalence relation*) と言う。

(7) $(A, \sim)$ を集合 A 上の同値関係とする。$a \in A$ に対して，a と同値な元全体の集合を

$$E(a) = \{\ x \in A \mid x \sim a\ \}$$

とする。これを a の**同値類** (*equivalence class*) と言う。

命題 1.19 定義 1.18 (7) の場合，A の任意の 2 つの元 a, b に対して，$E(a) = E(b)$ であるか又は $E(a) \cap E(b) = \emptyset$ である。

証明　$E(a) \cap E(b) = \emptyset$ ではないとすると，ある $c \in A$ が存在して $c \in E(a) \cap E(b)$ となっている。このとき $c \sim a$ および $c \sim b$ が成立している。対称律より $a \sim c$ が成立する。$a \sim c, c \sim b$ と推移律より $a \sim b$ が成立する。また対称律より $b \sim a$ も成立している。

x を $E(a)$ の任意の元とすると，$x \sim a$, $a \sim b$ であるから $x \sim b$ となり，$E(a) \subseteq E(b)$ である。y を $E(b)$ の任意の元とすると，$y \sim b$, $b \sim a$ であるから $y \sim a$ となり，$E(b) \subseteq E(a)$ である。$E(a) \subseteq E(b)$ でありかつ $E(b) \subseteq E(a)$ であるから，$E(a) = E(b)$ である。∎

A の全ての元に対してその同値類を考えると，それぞれの同値類は，この命題より，完全に一致しているか又は共通部分を持たないかのどちらかである。A の互いに異なる同値類全体を $\{E_i\}$ とすると，$A = \bigcup_i E_i$ であり，$i \neq j$ ならば $E_i \cap E_j = \emptyset$ となる。すなわち集合 A は，互いに共通部分を持たない部分集合の集まりに分割される。これを A の**同値類分割** (*equivalence class patition*) と言う。

逆に集合 A に対して，互いに共通部分を持たない部分集合への分割 $\{E_i\}$ が与えられたとしよう。$a, b \in A$ に対して，a, b が同じ分割集合 E_i に入っている時 $a \sim b$ と定義することにより，A 上の同値関係が定義される。

つまり，集合に同値関係を与えるということと，互いに共通部分を持たない部分集合に分割するということは，実は同じことなのである。

定義 1.20 (1)　E_i をある同値関係の一つの同値類とする。E_i から一つの元 $a_i \in E_i$ を取り出した時，a_i を E_i の**代表元** (*representative*) という。

(2) 集合 A の部分集合 $\{a_i\}$ は，全ての元が異なる同値類に属し，さらに任意の同値類に対して，その同値類に属するある元がこの部分集合の中に存在する時，**完全代表系** (*complete system of representatives*) という。言い換えると，完全代表系 $\{a_i\}$ とは，全ての同値類から代表元を 1 個の選び出し，それらを集めたものである。

演習問題 1.10

(1) $A = \{\, a, b, c \,\}$ とする。A 上の 2 項関係は何種類存在するか答えよ。

(2) $A = \{\, a, b, c \,\}$ 上の 2 項関係で同値関係になるものをすべて列挙せよ。またそれぞれに対し完全代表系を 1 つ選べ。

演習問題 1.11　整数 $\mathbb{Z}$ 上の関係 R が同値関係になるかどうか調べよ。同値関係になるときは証明し，そうでないときは反例をあげよ。また同値関係になるときは完全代表系を 1 つ選べ。

(1) $R = \{\, (m,n) \in \mathbb{Z} \times \mathbb{Z} \mid m+n \text{ は } 5 \text{ で割り切れる} \,\}$

(2) $R = \{\, (m,n) \in \mathbb{Z} \times \mathbb{Z} \mid m-n \text{ は } 5 \text{ で割り切れる} \,\}$

(3) $R = \{\, (m,n) \in \mathbb{Z} \times \mathbb{Z} \mid mn \text{ は } 5 \text{ で割り切れる} \,\}$