代数学 I 第 1，2 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

1.1 導入

本講義のテーマは

『群論』

である．**群**とは “ある性質を満たす二項演算の定まった集合” である．正確な定義を後回しにして，大まかな説明を与えよう．“二項演算の定まった集合” というのは簡単に言えば “計算規則の定まった集合” というような意味である．良く知っている計算というと四則演算 $(+,-,\times,\div)$ であろう．このとき，どういう数達 (集合) の中でこれらの演算ができたかということを明確に意識してみる：

	集合	定義できる演算
自然数	$\mathbb{N} \coloneqq \{0,1,2,\dots\}$[*1]	$+,\times$
整数	$\mathbb{Z} \coloneqq \{\dots,-2,-1,0,1,2,\dots\}$	$+,-,\times$
有理数	$\mathbb{Q} \coloneqq \left\{\frac{b}{a} \middle\vert a \in \mathbb{Z}\setminus\{0\}, b \in \mathbb{Z}\right\}$	$+,-,\times,(0\text{ を除くと})\div$
実数	$\mathbb{R}$	$+,-,\times,(0\text{ を除くと})\div$
複素数	$\mathbb{C}$	$+,-,\times,(0\text{ を除くと})\div$

なおこの表の記号は今後も講義を通して用いられる．[*2]“自然数 $\mathbb{N}$ において，演算 $+$ が定義できる” というのは，$n_1, n_2 \in \mathbb{N}$ のとき $n_1+n_2 \in \mathbb{N}$ なので，“$+$ という演算が $\mathbb{N}$ 内で完結している ($\mathbb{N}$ は $+$ で**閉じている**という)” という意味である．一方例えば，$2,3 \in \mathbb{N}$ であるが，$2-3=-1 \notin \mathbb{N}$ なので，$\mathbb{N}$ は $-$ で閉じていない．考える範囲を $\mathbb{Z}$ にしておくと，引き算 $-$ でも閉じている．こういった調子で上の表は読めばよい．

もう少し数学的に書いてみよう．四則演算はどれも，“2 つの数から新しい数を得る” という操作である．例えば，$2+3=5$ は “2 と 3 から 5 を得ている” と考える．こう考えると，足し算は

$$\begin{array}{rccc} +\colon & \mathbb{N}\times\mathbb{N} & \longrightarrow & \mathbb{N} \\ & \cup & & \cup \\ & (n_1,n_2) & \longmapsto & n_1+n_2. \end{array}$$

という写像に他ならない．

復習

集合 X, Y に対し，

$$X \times Y \coloneqq \{(x,y) \mid x \in X, y \in Y\}$$

である．(この $\times$ は上で出てきた数の掛け算ではなくて集合の**直積**と呼ばれるものである．)

こうすると，四則演算 $\cdot$ が集合 G 上で定義できるとは，$\cdot$ が写像

$$\cdot\colon G \times G \to G \tag{1.1}$$

を定めるという意味である．[*3](1.1) の形の写像を**二項演算**という．

* *e-mail* : hoya@shibaura-it.ac.jp

[*2] $\mathbb{N}$ は Natural number の N，$\mathbb{Z}$ は Zahl(数，ドイツ語) の Z，$\mathbb{Q}$ は Quoziente(商，イタリア語) の Q，$\mathbb{R}$ は Real number の R，$\mathbb{C}$ は Complex number の C である．

[*3] 上の “閉じている” という概念とも整合していることに注意すること．

なお，写像という言葉で書こうとすると，割り算 $\div$ については少々注意が必要である．$\div\colon \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}, (a,b)\mapsto a\div b$ は，$(a,0)$ の形の元の行き先が $a\div 0$ となって定義できないため，写像としての定義ができていない．割り算をこの形で定義するためには，

$$\mathbb{Q}^\times \coloneqq \mathbb{Q}\setminus\{0\} \qquad \mathbb{R}^\times \coloneqq \mathbb{R}\setminus\{0\} \qquad \mathbb{C}^\times \coloneqq \mathbb{C}\setminus\{0\}. \tag{1.2}$$

としておいて，$\div\colon \mathbb{X}^\times\times\mathbb{X}^\times\to\mathbb{X}^\times, (a,b)\mapsto a\div b$ $(\mathbb{X}=\mathbb{Q},\mathbb{R},\mathbb{C})$ を考えるということになる．

さて，群の (ラフな) 定義をもう一度思い出そう．群とはある性質を満たす二項演算 $\cdot\colon G\times G\to G$ が定まった集合 $(G,\cdot)$ である．上に出てきたものの中では，実は $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+),(\mathbb{Q}^\times,\times),(\mathbb{R}^\times,\times),(\mathbb{C}^\times,\times)$ が群の例となる．(それ以外の上に出てきた集合と二項演算の組は残念ながら群の定義を満たす演算にはならない．) まずは，群とはこのような “計算ができる数” を一般化したようなものだと思えば良い．これは非常に重要な一般化で，キーワード的に書いておくと，

- 群は “対称性” を数学的に抽象化したものとなる．例えば，平面図形や空間図形の回転，ルービックキューブの変形等は群を用いて表すことができる．このようなことから，例えば物理においても基本的な言語として用いられるものとなる．
- “5 次以上の方程式には，その係数の四則演算と冪根で表される解の公式が存在しない” という有名な事実は，方程式から定まる**ガロア群**と呼ばれる群の性質を調べることから証明される．この講義の中では扱うことができないが，興味のある方は『ガロア理論』というキーワードで調べて勉強すると良いであろう．

ちなみに，“足し算と掛け算” の定まった $(\mathbb{Z},+,\times)$ のような集合の抽象化の話もある．これは**環論**と呼ばれ，『代数学 II』で学ぶこととなる．さらに，上で四則演算が全て定義できた $(\mathbb{Q},+,\times,\div)$(ただし割り算においては 0 を除く) のような集合を扱う話は**体論**と呼ばれる．演算が増えるごとに難しくなっていくというわけではなく，これらは独立に，しかしあるところでは関連しながら代数学の世界をなしている．例えば，上に書いた『ガロア理論』においては，これら全ての考え方が，本質的に表れてくる．

1.2 合同算術

群の定義をするのはもう少し先にして，1.1 章で見た例以外で，非自明な二項演算が定義される集合の例を学ぶ．

n を正の整数とする．各 $a\in\mathbb{Z}$ に対し，$[a]_n$ という記号を割り当てる．ただし，$a,b\in\mathbb{Z}$ に対し，$[a]_n$ と $[b]_n$ は次のルールで同一視されているとする：

$$[a]_n=[b]_n \quad\Leftrightarrow\quad a-b \text{ が } n \text{ で割り切れる } (\Leftrightarrow a\equiv b \mod n). \tag{1.3}$$

例 1. 同一視の例：

- $[2]_5=[7]_5=[-3]_5=\cdots$
- $[90]_{360}=[-270]_{360}=[450]_{360}=\cdots$

この計算は角度計算のように考えればこれまで十分慣れ親しんだものと言えるだろう $(90^\circ=-270^\circ=450^\circ)$．

このとき，

$$\mathbb{Z}/n\mathbb{Z}\coloneqq\{[a]_n\mid a\in\mathbb{Z}\}=\{[0]_n,[1]_n,\dots,[n-1]_n\} \tag{1.4}$$

とする．ここで，(1.3) により，$[a]_n=[b]_n$ となる必要十分条件は a と b を n で割った余りが等しいことであり，整数を n で割った余りは $0,1,\dots,n-1$ のいずれかであることから，2 つめの等号は示される．$\mathbb{Z}/n\mathbb{Z}$

は n 元からなる有限集合であるが，ここに以下の方法で二項演算を定義する：

$$+\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ ([a]_n, [b]_n) \mapsto [a+b]_n$$
$$-\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ ([a]_n, [b]_n) \mapsto [a-b]_n$$
$$\times\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ ([a]_n, [b]_n) \mapsto [ab]_n.$$

例 2.

$$[2]_7 + [5]_7 = [7]_7 = [0]_7 \qquad [2]_7 - [5]_7 = [-3]_7 = [4]_7 \qquad [2]_5 \times [3]_5 = [6]_5 = [1]_5.$$

重要 (これらはちゃんと定義されている (well-defined)?)

(1.3) において a, b を有理数と考えて，$[a]_n$ の定義を $a \in \mathbb{Q}$ に拡張してみよう[*4]．例えば，$[0.5]_2 = [2.5]_2 = [-1.5]_2$ 等である．正の整数 $n \in \mathbb{Z}$ に対して，$\mathbb{Q}/n\mathbb{Z} = \{[r]_n \mid r \in \mathbb{Q}\}$ とする．このとき，

$$\times\colon \mathbb{Q}/n\mathbb{Z} \times \mathbb{Q}/n\mathbb{Z} \to \mathbb{Q}/n\mathbb{Z},\ ([r]_n, [s]_n) \mapsto [rs]_n.$$

は定義されるだろうか? 実は以下のような困ったことが起こってしまう：

$$\begin{array}{ccc} [1.5]_2 \times [2]_2 & = & [1.5 \times 2]_2 = [3]_2 \\ \| & & \not= \\ [1.5]_2 \times [0]_2 & = & [1.5 \times 0]_2 = [0]_2. \end{array}$$

よって，この写像の定義として良くないことがわかる．なぜ，このようなことが起こるかというと，『$\mathbb{Q}/n\mathbb{Z}$ の中では，1 つの元を表す方法が何通りもある ($[2]_2 = [0]_2$ 等) にもかかわらず，写像の定義においてこの表示を用いてしまった』からである．この結果，本当は同じ元なのに，表わし方が違ったがために結果が変わるということになってしまったのである．
このように，1 つの元の表し方が複数あるような集合からの写像を定義する際には細心の注意を払う必要がある．定義した写像が元の表示の仕方に依らないとき，その写像は *well-defined* であるという．この注意は慣れるまで難しいと思われるが，今後の講義でも非常に重要になる．
試しに，$\times\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ が well-defined であることを示そう．ある元に対して，どんな表示を持ってきても結果が変わらないことを言えばよい．

証明. $a, a', b, b' \in \mathbb{Z}$ に対し，$[a]_n = [a']_n$，$[b]_n = [b']_n$ であると仮定する．このとき，(1.3) から，ある $m_1, m_2 \in \mathbb{Z}$ が存在して，

$$a' = a + m_1 n \qquad b' = b + m_2 n$$

と書ける．これより，

$$\begin{aligned} [a']_n \times [b']_n &= [(a + m_1 n)(b + m_2 n)]_n \\ &= [ab + (am_2 + bm_1 + m_1 m_2 n)n]_n \end{aligned}$$

となるが，いま$am_2 + bm_1 + m_1 m_2 n$ は整数なので，結局 $[a']_n \times [b']_n = [ab]_n = [a]_n \times [b]_n$ となり，well-defined であることが示された． □

a, b が有理数の場合には下線部分が言えないので，well-defined ではなかったのである．この調子で，$\mathbb{Z}/n\mathbb{Z}$ 上の二項演算 $+, -$ が well-defined であることを確認してもらいたい．ちなみに，$+$ や $-$ に関しては $\mathbb{Q}/n\mathbb{Z}$ においても well-defined に拡張される．

応用例：フェルマーの小定理

$\mathbb{Z}/n\mathbb{Z}$ における計算の応用例として，フェルマーの小定理を証明しよう．まず以下の命題を準備する：

[*4] ちゃんと言うと，“$a - b$ が n で割り切れる” は “$a - b$ が n で割り切れる整数である” に修正する．

命題 1.1

p を素数とする．このとき，各 $a, b \in \mathbb{Z}$ に対し，

$$([a]_p + [b]_p)^p = ([a]_p)^p + ([b]_p)^p$$

ここで p 乗は，$\mathbb{Z}/p\mathbb{Z}$ における $\times$ を p 回繰り返し行うという意味である．

証明.

$$\begin{aligned}([a]_p + [b]_p)^p &= ([a+b]_p)^p \\ &= [(a+b)^p]_p \\ &= \left[a^p + {}_p\mathrm{C}_1 a^{p-1}b + {}_p\mathrm{C}_2 a^{p-1}b^2 + \cdots + {}_p\mathrm{C}_{p-1}ab^{p-1} + b^p\right]_p \quad \text{(二項定理)}.\end{aligned}$$

ここで，${}_p\mathrm{C}_k = \dfrac{p!}{k!(p-k)!}$ $(k = 1, \ldots, p-1)$ である．いま，p は素数なので，$k = 1, \ldots, p-1$ のとき，$k!(p-k)!$ は p では割り切れない．一方で，$p!$ は p で割り切れることに注意すると，${}_p\mathrm{C}_k$ は $k = 1, \ldots, p-1$ のとき p の倍数であることがわかる．これより，定義 (1.3) から，

$$\left[a^p + {}_p\mathrm{C}_1 a^{p-1}b + {}_p\mathrm{C}_2 a^{p-1}b^2 + \cdots + {}_p\mathrm{C}_{p-1}ab^{p-1} + b^p\right]_p = [a^p + b^p]_p.$$

以上より，$([a]_p + [b]_p)^p = [a^p + b^p]_p = ([a]_p)^p + ([b]_p)^p$ となる． □

定理 1.2 (フェルマーの小定理)

p を素数する．このとき，$a \in \mathbb{N}$ に対し，a^p を p で割った余りと，a を p で割った余りは等しい．

証明. $[a^p]_p = [a]_p$ を示せばよい．命題 1.1 を繰り返し用いると，

$$\begin{aligned}[a^p]_p = ([a]_p)^p = ([1]_p + [a-1]_p)^p &= ([1]_p)^p + ([a-1]_p)^p \\ &= ([1]_p)^p + ([1]_p + [a-2]_p)^p = ([1]_p)^p + ([1]_p)^p + ([a-2]_p)^p \\ &\cdots \\ &= \underbrace{([1]_p)^p + ([1]_p)^p + \cdots + ([1]_p)^p}_{a\text{ 個}} = \underbrace{[1]_p + [1]_p + \cdots + [1]_p}_{a\text{ 個}} = [a]_p\end{aligned}$$

□

1.3 次回への準備：拡張ユークリッド互除法

次回，$\mathbb{Z}/n\mathbb{Z}$ における “割り算” について考察する．そのために必要な拡張ユークリッド互除法について思い出す．ここでは，具体例をもとにその方法を思い出すにとどめる．厳密な取り扱いについては，補足プリント “拡張ユークリッド互除法について” を参考にすること．

定義 1.3.

正の整数 a, b に対して，その最大公約数 (greatest common divisor) を $\gcd(a, b)$ と書く．さらに 0 以上の整数 a に対して，$\gcd(0, a) = \gcd(a, 0) = a$ とする．

正の整数 a, b が与えられたときに，$\gcd(a, b)$ を効率良く求める方法が**ユークリッド互除法**である．例として，2394 と 714 の最大公約数 $\gcd(2394, 714)$ を求めてみよう．

ユークリッド互除法を用いて $\gcd(2394, 714)$ を求める

(Step 1) 大きい方の数を小さい方の数で割る：

$$2394 = \underset{\text{商}}{\underline{3}} \times 714 + \underset{\text{余り}}{\underline{252}}. \tag{1.5}$$

このとき，以下のようにして $\gcd(2394, 714) = \gcd(714, 252)$ であることがわかる．

$m = \gcd(2394, 714)$ とすると，714 と 2394 は共に m の倍数であるから，$[252]_m = [252 + 3 \times 714]_m = [2394]_m = [0]_m$ なので，252 も m で割り切れる．よって，$\gcd(2394, 714) = m \leq \gcd(714, 252)$.

一方，$n = \gcd(714, 252)$ とすると，714 と 252 は共に n の倍数であるから，$[2394]_n = [3 \times 714 + 252]_n = [0]_n$ なので，2394 も n で割り切れる．よって，$\gcd(714, 252) = n \leq \gcd(2394, 714)$.

以上より，$\gcd(2394, 714) = \gcd(714, 252)$.

一般の状況での厳密な証明は補足プリント “拡張ユークリッド互除法について” の命題を参照のこと．(証明方法はこれと同じである．)

(Step 2) 元の問題は $\gcd(714, 252)$ を求める問題に変わったので，714 と 252 に対して，(Step1) を繰り返す．

$$714 = \underset{\text{商}}{\underline{2}} \times 252 + \underset{\text{余り}}{\underline{210}}. \tag{1.6}$$

このとき，上と同様に考えて，$\gcd(714, 252) = \gcd(252, 210)$.

(Step 3) 元の問題は $\gcd(252, 210)$ を求める問題に変わったので，252 と 210 に対して，(Step1) を繰り返す．

$$252 = \underset{\text{商}}{\underline{1}} \times 210 + \underset{\text{余り}}{\underline{42}}. \tag{1.7}$$

このとき，上と同様に考えて，$\gcd(252, 210) = \gcd(210, 42)$.

(Step 4) 元の問題は $\gcd(210, 42)$ を求める問題に変わったので，210 と 42 に対して，(Step1) を繰り返す．

$$210 = \underset{\text{商}}{\underline{5}} \times 42 + \underset{\text{余り}}{\underline{0}}. \tag{1.8}$$

ここで，割り切れたので，$\gcd(210, 42) = 42$ である．($\gcd(210, 42) = \gcd(42, 0) = 42$ と考えても良い．) 以上より，$\gcd(2394, 714) = 42$.

この方法は，考える整数がどんどん小さくなっていくので，どんな 2 つの数から始めても必ずいつか割り切れて終わるということが容易に想像できるだろう．(厳密な取り扱いについては，補足プリント “拡張ユークリッド互除法について” を参考にすること．) これがユークリッド互除法である．

さて，ユークリッド互除法の各 Step を覚えておくことで，次のような問題に答えることができる．

$2394x + 714y = 42$ を満たす整数の組 (x, y) を 1 つ求めよ．

解. ユークリッド互除法での計算を “逆にたどる”.

$$\begin{aligned}
42 &= 252 - 1 \times 210 \quad (((1.7) \text{ より}) \\
&= 252 - 1 \times (714 - 2 \times 252) \quad (((1.6) \text{ より}) \\
&= (-1) \times 714 + 3 \times 252 \\
&= (-1) \times 714 + 3 \times (2394 - 3 \times 714) \quad (((1.5) \text{ より}) \\
&= 3 \times 2394 + (-10) \times 714
\end{aligned}$$

これより，$2394x + 714y = 42$ を満たす整数の組 (x, y) の例として，$(x, y) = (3, -10)$ が取れる． □

この解で行ったような，ユークリッド互除法を逆にたどるアルゴリズムは**拡張ユークリッド互除法**と呼ばれる．

ちなみに，$2394x + 714y = 42$ を満たす整数の組 (x, y) はこれだけではない．しかし，1 つ解を見つければ，一般に次のようにして全ての整数解が見つけられる．

$$\begin{aligned}
&2394x + 714y = 42 \\
&\Leftrightarrow 2394(x-3) + 714(y-(-10)) = 0 \quad (\text{ここで，さっき見つけた解を用いる}) \\
&\Leftrightarrow 57(x-3) + 17(y+10) = 0 \quad (\text{両辺を } 42 = \gcd(2394, 714) \text{ で割る．})
\end{aligned}$$

このとき，最大公約数で割ったので，57 と 17 は互いに素であることに注意すると，最後の等式が成立するためには，

$$(x-3, y+10) = (17m, -57m),\ m \in \mathbb{Z}$$

という形であることが必要十分である．よって，$2394x + 714y = 42$ を満たす整数の組 (x, y) は

$$(x, y) = (3 + 17m, -10 - 57m),\ m \in \mathbb{Z}$$

が全てである．以上の事実を一般的な言葉を使ってまとめておこう．

正の整数 a, b, 整数 k に対して，

$$ax + by = k\gcd(a, b)$$

を満たす整数の組 (x, y) は次のようにして求められる．

(Step 1) ユークリッド互除法で $\gcd(a, b)$ を求める．この際，途中計算を記録しておく．

(Step 2) ユークリッド互除法の計算を逆にたどる拡張ユークリッド互除法を用いて $ax + by = \gcd(a, b)$ を満たす整数の組 (x_0', y_0') を1 つ求める．

(Step 3) $x_0 \coloneqq kx_0', y_0 \coloneqq ky_0'$ とすれば，(x_0, y_0) は $ax_0 + by_0 = k\gcd(a, b)$ を満たす整数の組である．

(Step 4) $a' \coloneqq a/\gcd(a, b), b' \coloneqq b/\gcd(a, b)$ とすると，a' と b' は互いに素で，

$$ax + by = k\gcd(a, b) \Leftrightarrow a'(x - x_0) + b'(y - y_0) = 0$$

であるので，これを満たすためには，

$$(x - x_0, y - y_0) = (b'm, -a'm),\ m \in \mathbb{Z}$$

が必要十分である．

(Step 5) $ax + by = k\gcd(a, b)$ を満たす整数の組 (x, y) は

$$(x, y) = (x_0 + b'm, y_0 - a'm),\ m \in \mathbb{Z}$$

が全てである．

また，以下の定理の形も重要である：

定理 1.4

正の整数 a, b に対して，以下の (1) と (2) は同値である：

(1) $ax + by = d$ を満たす整数の組 (x, y) が存在する．

(2) $[d]_{\gcd(a,b)} = [0]_{\gcd(a,b)}$.

証明. (1) ⇒ (2)：a, b は $\gcd(a, b)$ の倍数なので，$ax + by = d$ を満たす整数の組 (x_0, y_0) が存在するとき，

$$[d]_{\gcd(a,b)} = [ax_0 + by_0]_{\gcd(a,b)} = [0]_{\gcd(a,b)}.$$

(1) ⇐ (2)：$[d]_{\gcd(a,b)} = [0]_{\gcd(a,b)}$ のとき，ある $k \in \mathbb{Z}$ を用いて，$d = k\gcd(a, b)$ と書ける．$ax + by = k\gcd(a, b)$ を満たす整数の組 (x, y) が存在することは上でまとめた通りである． □

系 1.5

正の整数 a, b に対して，以下の (1) と (2) は同値である：

(1) $ax + by = 1$ を満たす整数の組 (x, y) が存在する．
(2) a と b は互いに素．(つまり，$\gcd(a, b) = 1$．)