代数学 I 第 3 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

前回，群と部分群の抽象的な定義について学び，その中で $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ や $(\mathbb{Q}^\times,\times)$, $(\mathbb{R}^\times,\times)$, $(\mathbb{C}^\times,\times)$ といった慣れ親しんだ数の体系が群の例を与えることを見た．今回は新たな数の体系として整数の剰余類環 $\mathbb{Z}/n\mathbb{Z}$ と呼ばれるものを導入し，ここでの演算によって再び群の例が与えられることを見る[*1]．また，この数の体系を扱うにあたっては well-defined 性という考え方を習得することが重要である．well-defined 性は代数学 I の講義を通して非常に重要であるが，慣れるまでとっつきにくいものかもしれないので，ここの例で良く理解しておいてほしい．

2.1 整数の剰余類環 $\mathbb{Z}/n\mathbb{Z}$

定義 2.1

$n\in\mathbb{Z}_{>0}$ 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 $[b]_n$ を次のルールで同一視する：

$$\begin{aligned}[a]_n=[b]_n &\Leftrightarrow a-b \text{ が } n \text{ で割り切れる } (\Leftrightarrow a\equiv b \mod n)\\ &\Leftrightarrow \text{ある } k\in\mathbb{Z} \text{ が存在して，} a=b+kn.\end{aligned}\tag{2.1}$$

このとき，

$$\mathbb{Z}/n\mathbb{Z}\coloneqq\{[a]_n\mid a\in\mathbb{Z}\}=\{[0]_n,[1]_n,\dots,[n-1]_n\}\tag{2.2}$$

とする．これを n **を法とする整数の剰余類環 (the ring of integers modulo** n**)** という．ここで，同一視のルールにより，$[a]_n=[b]_n$ 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，(2.2) の 2 つめの等号は示される．

なお，「$\mathbb{Z}/n\mathbb{Z}$」という記号については $\mathbb{Z}$, $/$, $n\mathbb{Z}$ というように分解して意味を考えるのではなくて，「$\mathbb{Z}/n\mathbb{Z}$」で 1 つの記号として考えてほしい．この記号の “意味” は先の講義でわかることになる．

例 1. 同一視 (2.1) の例は以下のようなものである．

- $\mathbb{Z}/5\mathbb{Z}$ において，$[2]_5=[7]_5=[-3]_5=\cdots$
- $\mathbb{Z}/360\mathbb{Z}$ において，$[90]_{360}=[-270]_{360}=[450]_{360}=\cdots$

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 ($90^\circ=-270^\circ=450^\circ$)．

$\mathbb{Z}/n\mathbb{Z}$ は n 個の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：

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

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

*1 整数の剰余類環はその名の通り，数学においては**環**と呼ばれる対象として扱われるのが通常である．環とは簡単に言えば「加法と乗法が定まっているような数の体系」である．厳密な定義については代数学の基本的な参考書を参照すること．

例 2.

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

ここで重要なのがこれらの二項演算が“ちゃんと定義されている”かどうか (**well-defined 性**) の確認である.

重要 (well-defined 性について)

(2.1) 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[*2]．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：

$$\begin{array}{ccc}[1.5]_2\times[2]_2=[1.5\times2]_2=[3]_2\\ \quad\|\qquad\qquad\not\parallel\\ [1.5]_2\times[0]_2=[1.5\times0]_2=[0]_2.\end{array}$$

よって，この写像の定義は実は良くない (きちんと定義されていない) ということがわかる．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特定の表示 ($[r]_n$ や $[s]_n$ の r や s のこと) を用いてしまった』からである.

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**．定義として書いた対応が元の表示の仕方に依らずに確かにきちんと定まっているとき，その対応は **well-defined** であるという．well-defined 性への注意は慣れるまで見落としがちかもしれないが，今後の講義でも非常に重要になる.

上で定義した $\mathbb{Z}/n\mathbb{Z}$ における $+,-,\times$ は実は全て well-defined である．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．写像の定義域から選んで来た元について，どのような表示をとっても写像で送った結果が変わらないということを言えばよい.

証明. $[a]_n=[a']_n$, $[b]_n=[b']_n$ $(a,a',b,b'\in\mathbb{Z})$ であると仮定する．このとき, (2.1) から, ある $k_1,k_2\in\mathbb{Z}$ が存在して,

$$a'=a+k_1n \qquad b'=b+k_2n$$

と書ける．これより,

$$\begin{aligned}[a']_n\times[b']_n&=[(a+k_1n)(b+k_2n)]_n\\&=[ab+(ak_2+bk_1+k_1k_2n)n]_n\end{aligned}$$

となるが，いま$ak_2+bk_1+k_1k_2n$ は整数なので，結局 $[a']_n\times[b']_n=[ab]_n=[a]_n\times[b]_n$ となる．これより，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.

well-defined 性について慣れるために，well-defined である写像とそうでない写像の例をもう少し出しておこう.

[*2] 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.

例 3. 写像

$$f_1 \colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z},\ [a]_6 \mapsto [a]_3$$

は well-defined である．なぜなら，$[a]_6 = [a']_6$ $(a, a' \in \mathbb{Z})$ であるとき，(2.1) からある $k \in \mathbb{Z}$ が存在して，$a' = a + 6k$ と書け，このとき，

$$f_1([a']_6) = [a']_3 = [a + 6k]_3 = [a + 3 \cdot 2k]_3 = [a]_3 = f_1([a]_6)$$

となるためである．

一方，

$$f_2 \colon \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z},\ [a]_5 \mapsto [a]_3$$

は well-defined ではない (このような対応の写像は存在しない)．なぜなら，$[0]_5 = [5]_5$ であるにもかかわらず，

$$f_2([0]_5) = [0]_3 \neq [2]_3 = [5]_3 = f_2([5]_5)$$

となるためである．

2.2 $\mathbb{Z}/n\mathbb{Z}$ の群構造

話を $\mathbb{Z}/n\mathbb{Z}$ での二項演算に戻そう．正の整数 $n \in \mathbb{Z}_{>0}$ に対して，$(\mathbb{Z}/n\mathbb{Z}, +)$ は群である．これを n を法とする**整数の剰余類群**という．$\mathbb{Z}/n\mathbb{Z}$ の $+$ は $\mathbb{Z}$ の通常の加法 $+$ に由来しているので群の二項演算の 3 性質が成立することはほぼ明らかではあるが，一応確認してみよう．

(I) (結合法則) 任意の $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，

$$([a]_n + [b]_n) + [c]_n = [a + b + c]_n = [a]_n + ([b]_n + [c]_n).$$

(II) (単位元の存在) 単位元は $[0]_n \in \mathbb{Z}/n\mathbb{Z}$ である．実際，任意の $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，

$$[0]_n + [a]_n = [a]_n = [a]_n + [0]_n$$

が成立する．

(III) (逆元の存在) 任意の $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，$[-a]_n \in \mathbb{Z}/n\mathbb{Z}$ であって，

$$[-a]_n + [a]_n = [0]_n = [a]_n + [-a]_n$$

が成立する．($[a]_n$ の逆元 $[-a]_n$ は $[a]_n^{-1}$ ではなく $-[a]_n$ としばしば書かれる．)

さらに，$+$ は

(IV) 任意の $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，$[a]_n + [b]_n = [a + b]_n = [b]_n + [a]_n$

をみたすので，これは可換群である．また，$|\mathbb{Z}/n\mathbb{Z}| = n$ であったので，これは位数 n の有限群である．この例によって，全ての正の整数 $n \in \mathbb{Z}_{>0}$ に対し，位数 n の群が少なくとも 1 つ存在するということがわかったことになる．

なお，$(\mathbb{Z}/n\mathbb{Z}, +)$ はその部分群も全て完全に記述できる．証明はそんなに複雑ではないので，ぜひ各自で考えてみてもらいたい (講義では触れないので，別途補足プリントとして配布する)．

定理 2.2

$n \in \mathbb{Z}_{>0}$ とする．k を n の約数としたとき，

$$H_k \coloneqq \{[ka]_n \mid a \in \mathbb{Z}\} \subset \mathbb{Z}/n\mathbb{Z}$$

は $(\mathbb{Z}/n\mathbb{Z}, +)$ の位数 n/k の部分群である．さらに，$(\mathbb{Z}/n\mathbb{Z}, +)$ の部分群はこの形のもので尽くされる．

例 4. $(\mathbb{Z}/12\mathbb{Z}, +)$ の部分群は以下で全てである．

$$H_{12} = \{[0]_{12}\}, \quad H_6 = \{[0]_{12}, [6]_{12}\}, \quad H_4 = \{[0]_{12}, [4]_{12}, [8]_{12}\}, \quad H_3 = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\},$$
$$H_2 = \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}, \quad H_1 = \mathbb{Z}/12\mathbb{Z}.$$

注意 1. $k \in \mathbb{Z}$ が n の約数でなくても，

$$H_k \coloneqq \{[ka]_n \mid a \in \mathbb{Z}\}$$

は $\mathbb{Z}/n\mathbb{Z}$ の部分群である．定理 2.2 が主張しているのは，「k が n の約数である」という条件を付ければ $\mathbb{Z}/n\mathbb{Z}$ **の部分群が過不足なく得られる**ということである (つまり，k が n の約数である場合を考えるだけで部分群は全て見つかり，しかも k と k' が n の異なる約数であるとき，$H_k \neq H_{k'}$)．例えば，$\mathbb{Z}/8\mathbb{Z}$ においては，

$$H_6 = \{[6a]_8 \mid a \in \mathbb{Z}\} = \{[-2a + 8a]_8 \mid a \in \mathbb{Z}\} = \{[-2a]_8 \mid a \in \mathbb{Z}\} = \{[2a]_8 \mid a \in \mathbb{Z}\} = H_2$$

となる．6 は 8 の約数ではないが，結局 H_6 は H_2 と一致するので，部分群を列挙するに当たっては考える必要はないのである．

なお，k と k' が n の異なる約数であるとき $H_k \neq H_{k'}$ となることは，位数が異なることから直ちにわかる．

2.3 復習：ユークリッド互除法

※本節は講義内で時間をかけて扱うことはしないため，不安がある場合は各自で事前に予習すること．質問があれば講義前後の時間にお願いします．

次の節で $\mathbb{Z}/n\mathbb{Z}$ における $\times$ を二項演算として実現される群を扱う．先に少し述べておくと，$(\mathbb{Z} \setminus \{0\}, \times)$ が群にならなかった (第 1,2 回講義資料例 3) のと同様に $((\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]_n\}, \times)$ も群になるとは限らない．一方で，$\mathbb{Z} \setminus \{0\}$ の部分集合で $\times$ に関して群をなすものは $\{1\}$ と $\{1, -1\}$ のみであったのに対し，$(\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]_n\}$ の場合は必ずしも $\{[1]_n\}$ と $\{[1]_n, [-1]_n\}$ のみではない．状況はもう少し複雑で，それを調べるためには，**ユークリッド互除法**について思い出す必要がある．ここでは，具体例をもとにその方法を思い出そう．厳密な原理については，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 2.3

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：

$$2394 = \underset{\text{商}}{\underline{3}} \times 714 + \underset{\text{余り}}{\underline{252}}. \tag{2.3}$$

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．(証明方法はこの議論を一般的に書くだけである．)

(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．

$$714 = \underset{\text{商}}{\underline{2}} \times 252 + \underset{\text{余り}}{\underline{210}}. \tag{2.4}$$

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．

$$252 = \underset{\text{商}}{\underline{1}} \times 210 + \underset{\text{余り}}{\underline{42}}. \tag{2.5}$$

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．

$$210 = \underset{\text{商}}{\underline{5}} \times 42 + \underset{\text{余り}}{\underline{0}}. \tag{2.6}$$

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．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．

問題

$2394x + 714y = 42$ 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”.

$$\begin{aligned}
42 &= 252 - 1 \times 210 \quad (\text{(2.5) より}) \\
&= 252 - 1 \times (714 - 2 \times 252) \quad (\text{(2.4) より}) \\
&= (-1) \times 714 + 3 \times 252 \\
&= (-1) \times 714 + 3 \times (2394 - 3 \times 714) \quad (\text{(2.3) より}) \\
&= 3 \times 2394 + (-10) \times 714
\end{aligned}$$

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． □

さらに，$2394x + 714y = 42$ を満たす整数の組 (x, y) を 1 つ見つければ，全ての整数解も次のように求められる．つまり，以下の問題に答えることができる．

問題

$2394x + 714y = 42$ を満たす整数の組 (x, y) を全て求めよ．

解. $2394x + 714y = 42$ を満たす整数の組 (x, y) の 1 つとして，$(x, y) = (3, -10)$ が存在する (上の手順)．これより，

$$\begin{aligned} & 2394x + 714y = 42 \\ \Leftrightarrow\ & 2394(x-3) + 714(y-(-10)) = 0 \\ \Leftrightarrow\ & 57(x-3) + 17(y+10) = 0 \quad (\text{両辺を } 42 = \gcd(2394, 714) \text{ で割る．}) \end{aligned}$$

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． □

以上の手法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) は次のようにして全て求められる．

(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って $ax + by = \gcd(a, b)$ 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．

注意 2 (やや発展：拡張ユークリッド互除法)．$\gcd(2394, 714)$ を求めるユークリッド互除法の途中経過は以下

のように行列を用いて表すことができる (一般的な式は補足プリントを参照のこと)：

$$\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}2394\\ 714\end{pmatrix}=\begin{pmatrix}714\\ 2394-3\times 714\end{pmatrix}=\begin{pmatrix}714\\ 252\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}714\\ 252\end{pmatrix}=\begin{pmatrix}252\\ 714-2\times 252\end{pmatrix}=\begin{pmatrix}252\\ 210\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}252\\ 210\end{pmatrix}=\begin{pmatrix}210\\ 252-1\times 210\end{pmatrix}=\begin{pmatrix}210\\ 42\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}210\\ 42\end{pmatrix}=\begin{pmatrix}42\\ 210-5\times 42\end{pmatrix}=\begin{pmatrix}42\\ 0\end{pmatrix}.$$

これより，

$$\begin{aligned}\begin{pmatrix}42\\ 0\end{pmatrix}&=\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}210\\ 42\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}252\\ 210\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}714\\ 252\end{pmatrix}\\ &=\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}2394\\ 714\end{pmatrix}.\end{aligned}$$

ここで，

$$\begin{pmatrix}x_0 & y_0\\ z_0 & w_0\end{pmatrix}:=\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}$$

とすると，

$$\begin{pmatrix}42\\ 0\end{pmatrix}=\begin{pmatrix}x_0 & y_0\\ z_0 & w_0\end{pmatrix}\begin{pmatrix}2394\\ 714\end{pmatrix}=\begin{pmatrix}2394x_0+714y_0\\ 2394z_0+714w_0\end{pmatrix}.$$

なので，(x_0, y_0) が $2394x+714y=42$ を満たす整数の組 (x, y) の 1 つである．これを踏まえると，$2394x+714y=42$ を満たす整数の組 (x, y) の 1 つは以下のようにも求められることがわかる．

(Step 1) $2394=\underset{\text{商}}{3}\times 714+\underset{\text{余り}}{252}$ なので，行列

$$\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}$$

を準備する．

(Step 2) $714=\underset{\text{商}}{2}\times 252+\underset{\text{余り}}{210}$ なので，Step1 で準備した行列に左から $\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}$ を掛けて，

$$\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}=\begin{pmatrix}1 & -3\\ -2 & 7\end{pmatrix}$$

を得る．

(Step 3) $252=\underset{\text{商}}{1}\times 210+\underset{\text{余り}}{42}$ なので，Step2 で得られた行列に左から $\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}$ を掛けて，

$$\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & -3\\ -2 & 7\end{pmatrix}=\begin{pmatrix}-2 & 7\\ 3 & -10\end{pmatrix}$$

を得る．

(Step 4) $210=\underset{\text{商}}{5}\times 42+\underset{\text{余り}}{0}$ なので，Step3 で得られた行列に左から $\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}$ を掛けて，

$$\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}-2 & 7\\ 3 & -10\end{pmatrix}=\begin{pmatrix}3 & -10\\ -17 & 57\end{pmatrix}$$

を得る．ここで余りが 0 となったのでストップし，ここで最終的に得られている行列の 1 行目の $(3, -10)$ が $2394x+714y=42$ を満たす整数の組 (x, y) の 1 つである．

このように「行列を更新していく」方法だと，ユークリッドの互除法が終了した時点で $2394x + 714y = 42$ を満たす整数の組 (x, y) も得られているので，ユークリッドの互除法の途中経過を記録しておく必要がない．この方法を**拡張ユークリッド互除法**という[*3]．とりあえずはユークリッドの互除法の計算を逆にたどって $ax + by = d$ 型の方程式の整数解 (x, y) が求められれば十分であるが，慣れてきて「逆にたどるのが面倒である」というくらいこの原理に慣れた方は拡張ユークリッド互除法を用いると良い．

また，以下の定理も重要である．

定理 2.4

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. $\underline{(1) \Rightarrow (2)}$：$a, b$ は $\gcd(a, b)$ の倍数なので，$ax_0 + by_0 = d$ を満たす整数の組 (x_0, y_0) が存在するとき，

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

$\underline{(2) \Rightarrow (1)}$：$[d]_{\gcd(a,b)} = [0]_{\gcd(a,b)}$ 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 2.5

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，$\gcd(a, b) = 1$．)

証明. $[1]_{\gcd(a,b)} = [0]_{\gcd(a,b)}$ が成立するのは $\gcd(a, b) = 1$ のときのみなので，定理 2.4 より主張は成立する． □

2.4 $\mathbb{Z}/n\mathbb{Z}$ の乗法群

2.2 節では $(\mathbb{Z}/n\mathbb{Z}, +)$ が群となることを確かめ，その部分群が全て決定されることを述べた．この節では，$\mathbb{Z}/n\mathbb{Z}$ における $\times$ を二項演算として実現される群を扱う．ポイントは「$\mathbb{Z}/n\mathbb{Z}$ において $\times$ に関する逆元を持つのはいつか?」ということである．

まず，$\times$ は

$$\times : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ ([a]_n, [b]_n) \mapsto [a]_n[b]_n \coloneqq [ab]_n$$

というように $\mathbb{Z}$ の積をそのまま用いて定義されていたので，結合法則は

$$([a]_n[b]_n)[c]_n = [abc]_n = [a]_n([b]_n[c]_n)\ (a, b, c \in \mathbb{Z})$$

となって成立する．また，$[1]_n \in \mathbb{Z}/n\mathbb{Z}$ は

$$[1]_n[a]_n = [a]_n = [a]_n[1]_n\ (a \in \mathbb{Z})$$

を満たすので，単位元の性質を満たしている．

それでは，逆元を持つ $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ はどのようなものだろうか．$[1]_n$ を単位元としているので，逆元は以下のように定義される．

[*3] 本講義資料における拡張ユークリッド互除法の解説は，大阪大学の有木進先生の重要なご指摘を受け，昨年度以前のものから改良を加えております．有木進先生にこの場で御礼申し上げます．

定義 2.6

$[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対して，$[a]_n^{-1}$ を

$$[a]_n[a]_n^{-1} = [1]_n$$

を満たす $\mathbb{Z}/n\mathbb{Z}$ の元とする．この元を $[a]_n$ の $\times$ **に関する逆元**という．[*4]

まず注意しないといけないのは，$a \in \mathbb{Z}$ が ± 1 でないとき，$[a]_n^{-1}$ は$[1/a]_n$ ではないということである．この場合 $1/a$ は整数ではないので，$[1/a]_n$ という元は $\mathbb{Z}/n\mathbb{Z}$ に存在しないのである．それにもかかわらず，$\mathbb{Z}/n\mathbb{Z}$ において $\times$ に関する逆元を持つ元は ($\mathbb{Z}$ の場合とは違って)$[\pm 1]_n$ だけではない．例えば，以下のような例がある．

例 5. $\mathbb{Z}/7\mathbb{Z}$ において，

$$[4]_7[2]_7 = [8]_7 = [1]_7$$

となるので，$[4]_7^{-1} = [2]_7$.

$\mathbb{Z}/12\mathbb{Z}$ において，

$$[5]_{12}[5]_{12} = [25]_{12} = [1]_{12}$$

となるので，$[5]_{12}^{-1} = [5]_{12}$.

一方で，$\times$ に関する逆元は常に存在するわけではない．

例 6. $\mathbb{Z}/n\mathbb{Z}$ において，任意の $a \in \mathbb{Z}$ に対し，

$$[0]_n[a]_n = [0]_n$$

となるので，$[0]_n$ は $\times$ に関する逆元を持たない．

$\mathbb{Z}/6\mathbb{Z}$ において，

$$[2]_6[0]_6 = [0]_6 \qquad [2]_6[1]_6 = [2]_6 \qquad [2]_6[2]_6 = [4]_6$$
$$[2]_6[3]_6 = [6]_6 = [0]_6 \qquad [2]_6[4]_6 = [8]_6 = [2]_6 \qquad [2]_6[5]_6 = [10]_6 = [4]_6$$

となるので，$[2]_6$ は $\times$ に関する逆元を持たない．

そこで，逆元を持つ元からなる $\mathbb{Z}/n\mathbb{Z}$ の部分集合を定義しておく．

定義 2.7

$(\mathbb{Z}/n\mathbb{Z})^\times := \{[a]_n \mid [a]_n^{-1}\text{が存在 }\} = \{[a]_n \mid \text{ある } b \in \mathbb{Z} \text{ が存在して，} [a]_n[b]_n = [1]_n\}$.[*5]

このとき，以下が成立する．

命題 2.8

(1) $(\mathbb{Z}/n\mathbb{Z})^\times$ は演算 $\times$ で閉じている．すなわち，任意の $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，

$$[a]_n[b]_n = [ab]_n \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

(2) $(\mathbb{Z}/n\mathbb{Z})^\times$ は逆元を取る操作で閉じている．すなわち，任意の $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，

$$[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

証明. (1) 任意の $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，$[a]_n[b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ であること，つまり $[a]_n[b]_n$ に $\times$ に関する逆元が存在することを示せばよい．$[a]_n^{-1}, [b]_n^{-1}$ が存在することより，

$$([a]_n[b]_n)([b]_n^{-1}[a]_n^{-1}) = [a]_n([b]_n[b]_n^{-1})[a]_n^{-1} = [a]_n[1]_n[a]_n^{-1} = [a]_n[a]_n^{-1} = [1]_n.$$

[*4] $\mathbb{Z}/n\mathbb{Z}$ においては $[a]_n[b]_n = [ab]_n = [b]_n[a]_n$ が成立するので，$[a]_n[a]_n^{-1} = [1]_n$ のとき，$[a]_n^{-1}[a]_n = [1]_n$ も成立することに注意．

[*5] $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ に対し，$\mathbb{K}^\times := \mathbb{K} \setminus \{0\}$ も $\mathbb{K}$ の中で $\times$ に関する逆元を持つものの集まりとなっていたことに注意しよう，

よって，$[b]_n^{-1}[a]_n^{-1}$ が $[a]_n[b]_n$ の $\times$ に関する逆元となり，逆元の存在が示された． □

(2) $[a]_n[a]_n^{-1} = [a]_n^{-1}[a]_n = [1]_n$ は $[a]_n^{-1}$ の $\times$ に関する逆元が $[a]_n$ であるという式でもある．よって，$[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ であるとき，$[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ である． □

命題 2.8 (1) より，集合 $(\mathbb{Z}/n\mathbb{Z})^\times$ に二項演算

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

が定義される．これにより，$((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ は群をなす．実際，結合法則の成立，単位元の存在については本節の冒頭で述べた通り ($[1]_n^{-1} = [1]_n$ なので，$[1]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$)，逆元の存在については命題 2.8 (2) よりわかる．この群を $\mathbb{Z}/n\mathbb{Z}$ **の乗法群**という．

2.5 $\times$ に関する逆元の計算方法

本節では，乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ の構造についてより具体的に見ていくことにする．まずは $(\mathbb{Z}/n\mathbb{Z})^\times$ に具体的にどのような元が含まれるかについて調べよう．

命題 2.9

$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \gcd(a, n) = 1\}$.[*6]

証明. 次の同値関係をたどっていけばよい．

$$\begin{aligned}[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times &\Leftrightarrow \text{ある } x \in \mathbb{Z} \text{ が存在して，} [ax]_n (= [a]_n[x]_n) = [1]_n \\ &\Leftrightarrow \text{ある } x, y \in \mathbb{Z} \text{ が存在して，} ax + ny = 1 \\ &\Leftrightarrow \gcd(a, n) = 1. \text{ (系 2.5より)}\end{aligned}$$

□

例 7.

$$(\mathbb{Z}/12\mathbb{Z})^\times = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\} \qquad (\mathbb{Z}/7\mathbb{Z})^\times = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$

命題 2.9 の証明を見ると，各 $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ の $\times$ に関する逆元 $[a]_n^{-1}$ は，整数の組 (x, y) が

$$ax + ny = 1 \tag{2.7}$$

を満たすとき，

$$[a]_n^{-1} = [x]_n$$

として求められるということがわかる．(2.7) を満たす整数の組 (x, y) は 2.3 節で解説したように，ユークリッドの互除法の計算を逆にたどる，あるいは拡張ユークリッド互除法で見つけることができる．例題でこれを確かめてみよう．

例題

$\mathbb{Z}/60\mathbb{Z}$ において，$[17]_{60}$ の $\times$ に関する逆元を求めよ．

解答. まず，$\gcd(17, 60) = 1$ なので，命題 2.9 より，$[17]_{60}$ は確かに $(\mathbb{Z}/60\mathbb{Z})^\times$ の元である．

$$17x + 60y = 1$$

を満たす整数の組 (x, y) をユークリッド互除法の計算を逆にたどって求める．

$$\begin{aligned}60 &= 3 \times 17 + 9 & \qquad 17 &= 1 \times 9 + 8 \\ 9 &= 1 \times 8 + 1 & \qquad 8 &= 8 \times 1 + 0\end{aligned}$$

[*6] 負の数に対応する gcd 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」を参照のこと．

であるので,

$$\begin{aligned}1 &= 9 - 1 \times 8 \\ &= 9 + (-1) \times (17 - 1 \times 9) \\ &= (-1) \times 17 + 2 \times 9 \\ &= (-1) \times 17 + 2 \times (60 - 3 \times 17) \\ &= (-7) \times 17 + 2 \times 60\end{aligned}$$

より，$(x, y) = (-7, 2)$ が $17x + 60y = 1$ を満たす整数の組の例である．よって，求める逆元は

$$[17]_{60}^{-1} = [-7]_{60} = [53]_{60}.$$

□

検算してみると，確かに $[17]_{60}[-7]_{60} = [-119]_{60} = [1]_{60}$ となっている．

さて，$(\mathbb{Z}/n\mathbb{Z})^\times$ の元の個数を表す有名な関数をここで導入しておこう．

定義 2.10

正の整数 n に対し，n と互いに素な 1 以上 n 以下の自然数の個数を $\varphi(n)$ と書く．つまり，

$$\varphi(n) \coloneqq \#\{m \in \mathbb{N} \mid 1 \leq m \leq n, \gcd(m, n) = 1\}^{*7}$$

とする．n に対して $\varphi(n)$ を与える関数 $\varphi\colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}, n \mapsto \varphi(n)$ を**オイラー (Euler) の φ 関数**という．

例 8. $\varphi(n)$ の計算は定義通り考えると以下のように行うことができる．

- $\gcd(1, 1) = 1$ より，$\varphi(1) = 1$.
- $\gcd(1, 2) = 1, \gcd(2, 2) = 2$ なので，1 以上 2 以下の自然数 m で，$\gcd(m, 2) = 1$ を満たすものは 1 つであるから，$\varphi(2) = 1$.
- $\gcd(1, 3) = 1, \gcd(2, 3) = 1, \gcd(3, 3) = 3$ なので，1 以上 3 以下の自然数 m で，$\gcd(m, 3) = 1$ を満たすものは 2 つであるから，$\varphi(3) = 2$.
- $\gcd(1, 4) = 1, \gcd(2, 4) = 2, \gcd(3, 4) = 1, \gcd(4, 4) = 4$ なので，1 以上 4 以下の自然数 m で，$\gcd(m, 4) = 1$ を満たすものは 2 つであるから，$\varphi(4) = 2$.
- $\gcd(1, 5) = 1, \gcd(2, 5) = 1, \gcd(3, 5) = 1, \gcd(4, 5) = 1, \gcd(5, 5) = 5$ なので，1 以上 5 以下の自然数 m で，$\gcd(m, 5) = 1$ を満たすものは 4 つであるから，$\varphi(5) = 4$.

この調子で進めて行くと以下のようになる．

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

ここで，2 以上の自然数 n について，

$$n \text{ が素数} \quad \Leftrightarrow \quad 1, \ldots, n-1 \text{ は全て } n \text{ と互いに素} \quad \Leftrightarrow \quad \varphi(n) = n - 1 \tag{2.8}$$

となることに注意する．

命題 2.9 とオイラーの φ 関数の定義より，以下のことは直ちにわかる．

命題 2.11

$\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$．つまり，乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ の位数は $\varphi(n)$ である．

*7 $\#\{\ldots\}$ は集合 $\{\ldots\}$ の元の個数を表す記号である．

命題 2.11 と (2.8) での考察から，

$$\#(\mathbb{Z}/n\mathbb{Z})^\times = n-1 \quad \Leftrightarrow \quad n \text{ は素数}$$

であることがわかる．ここで例 6 で見たように，$[0]_n$ は $\times$ に関する逆元を持たないので，$\#(\mathbb{Z}/n\mathbb{Z})^\times = n-1$ であるとき，

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]_n\}$$

である．つまり，

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]_n\} \quad \Leftrightarrow \quad n \text{ が素数.} \tag{2.9}$$

となる．これより，p が素数のとき，$\mathbb{Z}/p\mathbb{Z}$ は「和 $+$ と積 $\times$ が定まっていて，$[0]_n$ 以外のすべての元が $\times$ に関する逆元を持つ」という性質を持つことがわかる．これは，$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ と似た性質である．こういった加減乗除のできる代数系の抽象化が第 1, 2 回講義資料でも現れた**体**と呼ばれるものであった．この言葉を用いれば，以下のように言うこともできる．

$$\mathbb{Z}/n\mathbb{Z} \text{ が体である} \quad \Leftrightarrow \quad n \text{ が素数.}$$

$\mathbb{Z}/p\mathbb{Z}$ (p は素数) という形の体は，有限個の元からなる体ということで，**有限体**と呼ばれるものの例となり，$\mathbb{F}_p$ とも書かれる．有限体は符号理論，暗号理論等でも用いられる応用上も重要な代数系である．