

代 数 学 1

April 24, 2017

はじめに

この講義の第 1 の目的は通常の整数環

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

と Gauss 整数環と呼ばれる

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

が類似してゐることを解説することにある。特に、 \mathbb{Z} における素数の概念は $\mathbb{Z}[i]$ においても有効であり、後者の素数がどの様なものであるかを詳述する。その上で、素因数分解の一意性が $\mathbb{Z}[i]$ でも成り立つことを証明する。

もう 1 つの目的は、この講義のあとに続く代数学の講義に登場する概念の具体例を与えることで、それらの講義を受講する際に助けとなる様な内容を盛り込むことである。その概念とは、群、部分群、巡回群、剰余類分解、環、体、剰余環、ideal などである。

André Weil の教科書 [W] はこの講義の内容に近い。[W] には多くの演習問題が収録されてゐるので、講義の進度に合はせて、それらの問題を解いていくことをお勧めする。

この講義 note は 2015 年度前期の代数学 1 の講義を進めながら執筆したものであるが、2016 年度の数学科受講生からは講義中に多くの指摘を受け、ほぼ完備なものになったと思ふ。ここに、その学生のみなさんに御礼申し上げる。

この note では、定理、命題、補題、例、例題、練習、演習問題等の すべてを通し番号 にしてゐる。

Contents

1	対称群	1
2	群	6
3	部分群	8
4	巡回群	10
5	Euler の函数 $n \mapsto \varphi(n)$	12
6	可換環と体	14
7	整数の性質	15
8	素因数分解の一意性	17
9	剰余類の演算	19
10	Fermat の小定理, Euler の定理	21
11	多項式の基本的性質	23
12	Lagrange の定理	24
13	原始根	26
14	平方剰余	28
15	平方剰余の相互法則	29
16	Gauss 整数	32
17	剰余類	36
18	正規部分群と剰余類群	37
19	中国の剰余定理	38

1 対称群

次節以降で群の抽象的な説明をするに先立ち、群のひとつの重要な例として対称群と呼ばれるものを学ぶ。自然数 n を固定する。 n 個の要素からなる集合をひとつ用意する。わかり易くするため $\{1, 2, \dots, n\}$ とする。このとき

$$S_n = \{ \sigma \mid \sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \text{ は全単射} \}$$

とおく。 $\sigma \in S_n$ について $\sigma(1) = k_1, \sigma(2) = k_2, \dots, \sigma(n) = k_n$ であることを

$$(1.1) \quad \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

と表す。さらに S_n の中に写像の合成により演算を考へる。 $\sigma, \tau \in S_n$ のときこれらの写像の合成 $\sigma \circ \tau$ を普通は $\sigma\tau$ と書いて σ と τ の積と呼ぶ。この積といふ演算については交換法則が成り立たない (確認せよ)。

例 1.2. 上の記号で $n = 5$ として、 $\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 5, \sigma(4) = 4, \sigma(5) = 1$ のとき

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

と書く。また $\tau(1) = 5, \tau(2) = 1, \tau(3) = 3, \tau(4) = 2, \tau(5) = 4$ のとき

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

である。このとき $\sigma\tau(1) = \sigma(\tau(1)) = \sigma(5) = 1$ であり、同様に $\sigma\tau(2) = 4, \sigma\tau(3) = 5, \sigma\tau(4) = 2, \sigma\tau(5) = 3$ であるから、

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 2 & 3 \end{pmatrix}.$$

まづ、 $\sigma \in S_n$ について (1.1) の記法において $\sigma(j) = j$ である様な列は省いて良いことにする。また、(1.1) において、第 1 列と数字のすぐ下にそれが写る数字がありさへすれば、左右の並び順は問はないものとする。

例 1.3. 例 1.2 の σ について

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 \\ 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 5 \\ 5 & 3 & 1 \end{pmatrix}.$$

集合 S_n の要素を n 次の置換と呼ぶ。 S_n の要素のうち、 $1, 2, \dots, n$ の全てをそれ自身に写す置換は、恒等置換と呼ばれ、通常 ε と表示される：

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

任意の $\sigma \in S_n$ に対し、 $\sigma\varepsilon = \varepsilon\sigma = \sigma$ が成り立つ。

また

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

に対して,

$$\sigma^{-1} = \begin{pmatrix} k_1 & k_2 & \cdots & k_n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

とおき, これを σ の 逆置換 と呼ぶ. ここで, 等式

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = \varepsilon$$

が成り立つ.

例 1.4. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$ ならば,

$$\sigma^{-1} = \begin{pmatrix} 4 & 5 & 1 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

定義 1.5. 上の集合 S_n を演算も考慮に入れた上で n 次対称群 と呼ぶ.

練習 1.6. S_n の要素の個数は $n!$ であることを示せ.

洗練された記号へ より使ひ易い記号を導入する. 定義域 $\{1, 2, \dots, n\}$ の m 個の要素からなる部分集合 $\{k_1, \dots, k_m\}$ について, 上の記法で

$$\rho = \begin{pmatrix} k_1 & k_2 & k_3 & \cdots & k_m \\ k_2 & k_3 & k_4 & \cdots & k_1 \end{pmatrix}$$

の様に隣に順繰りに写す写像 ρ は m 次の巡回置換 であると言はれて, 略記号で

$$(1.7) \quad \rho = \begin{pmatrix} k_1 & k_2 & k_3 & \cdots & k_m \\ k_2 & k_3 & k_4 & \cdots & k_1 \end{pmatrix} = (k_1 k_2 k_3 \cdots k_m)$$

と書かれる. 2 次の巡回置換は 互換 と呼ばれる.

例 1.8. これらの例として

$$\begin{pmatrix} 4 & 3 & 5 & 7 \\ 3 & 5 & 7 & 4 \end{pmatrix} = (4 \ 3 \ 5 \ 7), \quad \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} = (4 \ 3)$$

はどちらも巡回置換である. 特に, 後者の $(4 \ 3)$ は互換である.

いくつかの n 次置換 $\sigma_1 \sigma_2, \dots, \sigma_\ell$ について, 真 に動く数字 (自身に写る数字以外の数字) に共通なものがないとき, これらは 互ひに素な置換 であるといふ.

補題 1.9. どんな置換も, 互ひに素な巡回置換の積で表せる.

これは例で説明した方がわかり易い.

例 1.10. 置換

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix}$$

で写る数字を順次観察すると $1 \mapsto 3 \mapsto 5 \mapsto 7 \mapsto 1$, $2 \mapsto 4 \mapsto 6 \mapsto 2$ と写つてみて, これで

全ての数字を尽してゐるから

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix} = (1 \ 3 \ 5 \ 7)(2 \ 4 \ 6) = (2 \ 4 \ 6)(1 \ 3 \ 5 \ 7).$$

かう見てみると (1.7) の記法は返つて元の記号よりわかり易くなつたことに気付くであらう.

補題 1.11. いかなる巡回置換も互換のみの積で表せる.

これも例で説明した方がわかり易いが, 練習問題として取り上げる.

練習 1.12. (1) 次の等式を確かめよ:

$$(1 \ 2 \ 3 \ 4 \ 5 \ 6) = (1 \ 6)(1 \ 5)(1 \ 4)(1 \ 3)(1 \ 2).$$

(2) 一般に, 次の式が成り立つことを示せ:

$$(k_1 \ k_2 \ k_3 \ \cdots \ k_m) = (k_1 \ k_m)(k_1 \ k_{m-1}) \cdots (k_1 \ k_3)(k_1 \ k_2).$$

補題 1.9 と補題 1.11 より次がわかる.

命題 1.13. いかなる置換も互換のみの積として表せる.

練習 1.14. 次の置換を互換のみの積で表せ:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 4 & 5 & 8 & 1 & 6 & 2 & 7 \end{pmatrix}.$$

演習問題

1.15. ひとつの置換を互換の積で表す仕方は何通りもあり、その積に現れる互換の個数も様々であることを例をあげて示せ.

以下の問題 1.16 から 1.19 は一続きの問題である.

1.16. n 個の文字 x_1, x_2, \dots, x_n を用意する. これらの文字からなる (係数がすべて、例へば \mathbb{Q} に属する) 多項式 $f(x_1, x_2, \dots, x_n)$ と $\sigma \in S_n$ について、新たな多項式 σf を

$$(\sigma f)(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

で定める. このとき、以下のそれぞれについて σf を求めよ.

- (1) $f = x_1 x_3 + 2x_1^2 + x_3 + x_4$, $\sigma = (1\ 2\ 4)$.
- (2) $f = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$, $\sigma = (1\ 2)$.
- (3) $f = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$, $\sigma = (1\ 2\ 3)$.

1.17. 任意の $\tau, \sigma \in S_n$ と任意の多項式 f について $(\tau\sigma)f = \tau(\sigma f)$ が成り立つことを示せ.

1.18. いま、

$$\Delta = \Delta(x_1, x_2, \dots, x_n) = \prod_{i < j} (x_i - x_j)$$

とおく¹. このとき、任意の互換 σ について $\sigma\Delta = -\Delta$ となることを証明せよ.

1.19. 任意の置換 σ について、 σ を互換のみの積として、どう表しても使用する互換の個数の偶奇は σ のみで定まり、表し方に依らないことを証明せよ.

(ここでの方法以外にも非常に多くの証明が知られてゐるので、調べてみると良い.)

1.20. 問題 1.19 によつて、符号 と呼ばれる写像

$$\text{sgn} : S_n \rightarrow \{1, -1\}$$

を、置換 $\sigma \in S_n$ が m 個の互換で表されるとき $\text{sgn}(\sigma) = (-1)^m$ と定めることで定義できる (m の値に依存しないで σ だけで決まる). このとき $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$ となることを示せ. また、置換

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 4 & 5 & 8 & 1 & 6 & 2 & 7 \end{pmatrix}$$

を互換の積で表し、符号 $\text{sgn}(\sigma)$ を求めよ.

1.21. $\sigma \in S_n$ について、 $\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma)$ を示せ.

¹例へば $n = 4$ なら $\Delta(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \cdot (x_2 - x_3)(x_2 - x_4) \cdot (x_3 - x_4)$.

1.22. 1 から n までの自然数が与えられてゐる. これを並べた順列 k_1, k_2, \dots, k_n において, $i < j$ かつ $k_i > k_j$ となる (大小関係が逆転してゐる) 組 (k_i, k_j) を 転倒した組 といふ. 転倒した組の個数をこの順列の 転倒数 といふ. 例へば $n = 7$ で

$$5, 1, 2, 6, 7, 4, 3$$

の転倒した組は

$$(5, 1), (5, 2), (5, 4), (5, 3), (6, 4), (6, 3), (7, 4), (7, 3), (4, 3)$$

の 9 組なので, 転倒数は 9 である. 1 から 8 までの自然数の順列

$$8, 3, 7, 4, 5, 1, 6, 2$$

の転倒した組をすべて挙げ, 転倒数を求めよ.

1.23. n 次の置換 σ に対して, それの第 1 行の数を小さい順に並べた表示

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

の第 2 行 (k_1, k_2, \dots, k_n) を順列とみなし, それの転倒数を 置換 σ の転倒数 と呼んで, $r(\sigma)$ と書く. また $(a \ a+1)$ の形の互換を 隣接互換 と呼ぶ. 置換 σ と隣接互換との積 $\sigma(a \ a+1)$ の転倒数 $r(\sigma(a \ a+1))$ は $r(\sigma) + 1$ か $r(\sigma) - 1$ に等しいことを示せ.

1.24. 任意の置換

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

は隣接互換だけの積で表され, しかもその際に必要な隣接互換の最小数は, σ の転倒数に一致することを証明せよ. (Hint: $k_a < k_{a+1}$ なる a があれば, 積 $\sigma(a \ a+1)$ の転倒数が σ のそれと比較してどうなるかを考へよ.)

1.25. 問題 1.23 の記号を使い, 置換 σ について, $\overline{\text{sgn}}(\sigma) = (-1)^{r(\sigma)}$ と定める. 問題 1.20 で定めた符号について

$$\overline{\text{sgn}}(\sigma) = \text{sgn}(\sigma)$$

となることを示せ.

2 群

たとへば、整数の全体 \mathbb{Z} の加法といふ演算は、 $(a, b) \mapsto a + b$ で定められた写像 $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ のことに他ならない。一般に、集合 G に関して、ある写像 $G \times G \rightarrow G$ が定義されておるとき、 G に 演算が定義されておる といふ。

定義 2.1. 1 つの演算 $G \times G \rightarrow G$, $(a, b) \mapsto ab$ が定義された集合 G が群であるとは、次の 3 つが全て成り立つときをいふ：(但し a, b, c は G の任意の元を表す。)

G1 結合法則： $(ab)c = a(bc)$ 。

G2 単位元の存在：ある元 $1 \in G$ が存在して任意の $a \in G$ について $1a = a1 = a$ が成り立つ。 1 は 単位元 と呼ばれる。(特に $G \neq \emptyset$ である。)

G3 逆元の存在：任意の元 $a \in G$ に対し、 $ax = xa = 1$ を満たす元 $x \in G$ が存在する。その様な x を a の 逆元 と呼ぶ。一般的な状況では、その様な x を a^{-1} と記す。

また、 G が群であつて (つまり **G1**, **G2**, **G3** を満たし) しかも

G4 交換法則： $ab = ba$

も満たすならば、 G は Abel 群 または 可換群 であると言われる。可換群でない群を 非可換群 と呼ぶ。 G が群のとき、各 $a \in G$ ごとにその逆元は唯 1 つだけ存在する。実際、もし x と y がともに a の逆元であれば、 $xa = ax = 1$, $ya = ay = 1$ であるから

$$y = y1 = y(ax) = (ya)x = 1x = x$$

となるからである。群 G に対して、その要素の個数を G の 位数 といふ。要素の個数が無限個の場合は、位数は無限大であるといふ。

例 2.2. 群に近いが、群ではない例をいくつか挙げる。

(1) 自然数の集合 $\mathbb{N} = \{1, 2, 3, \dots\}$ について加法をその演算と見たとき、演算は定義されて **G1** は成り立つが、**G2** と **G3** は成立しない。(**G4** も成立してゐる)

(2) 自然数の集合 \mathbb{N} について乗法をその演算と見たとき、演算は定義されて **G1** と **G2** は成り立つが、**G3** は成立しない。(**G4** も成立してゐる)

例 2.3. 群の例をいくつか挙げる。

(1) 加法を演算として、整数の全体 \mathbb{Z} は群をなす。単位元は 0 で a の逆元は $-a$ 。

(2) 加法を演算として、有理数の全体 \mathbb{Q} 。

(3) 乗法を演算として、 0 以外の有理数の全体 \mathbb{Q}^\times 。

(4) 前節で述べた対称群 S_n 。

(5) 行列の乗法を演算として、成分がすべて整数で行列式が 1 である様な 2 次正方行列全体 $SL(2, \mathbb{Z})$ 。これは \mathbb{Z} 上の 2 次特殊線形群 (the special linear group of degree 2 over \mathbb{Z}) と呼ばれる。

(6) 行列の乗法を演算として、行列式が 0 でなく、成分がすべて有理数で、行列式が 0 でない 2 次正方行列全体 $GL(2, \mathbb{Q})$ 。これは \mathbb{Q} 上の 2 次一般線形群 (the general linear group of degree 2 over \mathbb{Q}) と呼ばれる。また、実数を成分とする同様な集合 $GL(2, \mathbb{R})$ 。

(7) 後述する対象であるが、正の整数 n に対し、法 n による剰余系 $\mathbb{Z}/n\mathbb{Z}$ は加法を演算として、位数 n の Abel 群である。

演習問題

2.4. すべての成分が整数であり行列式が 0 でない 2 次正方行列のすべてからなる集合 M に演算として行列の積を込めて考へる. このとき, $\mathbf{G1}$, $\mathbf{G2}$ は成り立つが $\mathbf{G3}$ と $\mathbf{G4}$ が成り立たないことを示せ.

2.5. G を群とする. $a \in G$ を固定する. 次の写像は全単射であることを証明せよ.

- (1) $\iota: G \rightarrow G, x \mapsto x^{-1}$.
- (2) $\lambda_a: G \rightarrow G, x \mapsto ax$.
- (3) $\rho_a: G \rightarrow G, x \mapsto xa$.

2.6. 群 G の 4 つの要素 a_1, a_2, a_3, a_4 について

$$((a_1 a_2) a_3) a_4, (a_1 (a_2 a_3)) a_4, a_1 ((a_2 a_3) a_4), a_1 (a_2 (a_3 a_4)), (a_1 a_2) (a_3 a_4)$$

はすべて相等しい. このことを示せ.

上のことは 5 つ以上の要素の演算についても同様であつて, どこから計算しても同一の結果を得る. これより, いくつかの要素の演算を $a_1 a_2 a_3 \cdots a_n$ と書いても誤解は生じない.

2.7. 群 G の任意の元 a, b について $(ab)^{-1} = b^{-1} a^{-1}$ であることを示せ. 一般に G の n 個の元 $a_i \in G$ ($i = 1, \dots, n$) について, $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$ となることを示せ.

2.8. 群 G の任意の要素 a は $a^2 = 1$ を満たすとする. このとき, G は Abel 群であることを示せ.

2.9. 対称群 S_n における逆元について, 次を示せ.

- (1) $\begin{pmatrix} 1 & 2 & \cdots & \ell \\ k_1 & k_2 & \cdots & k_\ell \end{pmatrix}^{-1} = \begin{pmatrix} k_1 & k_2 & \cdots & k_\ell \\ 1 & 2 & \cdots & \ell \end{pmatrix}$
- (2) $((j_1 \ j_2)(j_3 \ j_4) \cdots (j_{m-1} \ j_m))^{-1} = (j_{m-1} \ j_m) \cdots (j_3 \ j_4)(j_1 \ j_2)$

2.10. $n \geq 3$ のとき S_n は Abel 群ではない. これを示せ. (Hint: まづは S_3 が Abel 群でないことを確認せよ.)

2.11. S_4 の真の部分集合で可換な群になつてゐるものと非可換な群になつてゐるもの (次節で学ぶ部分群) をそれぞれ 2 つずつ挙げよ.

3 部分群

群 G の部分集合 H が G の演算で群になつてゐるとき, H は G の 部分群 であるといはれ, $H < G$ あるいは $G > H$ と記す. 特に部分群は空集合ではない.

例 3.1. 加法に関する群 \mathbb{Z} と 1 つの $m \in \mathbb{Z}$ について, m の倍数の全体 $m\mathbb{Z}$ は部分群である.

例 3.2. 0 以外の有理数全体のなす乗法に関する群 \mathbb{Q}^\times と, $m \in \mathbb{Q}^\times$ について,

$$m^{\mathbb{Z}} = \{m^k \mid k \in \mathbb{Z}\}$$

は \mathbb{Q}^\times の部分群である: $m^{\mathbb{Z}} < \mathbb{Q}^\times$

例 3.3. 4 次対称群 S_4 のすべての元を書けば

$$\begin{aligned} S_4 = \{ & \varepsilon, (12), (13), (14), (23), (24), (34), \\ & (123), (132), (124), (142), (134), (143), (234), (243), \\ & (1234), (1243), (1324), (1342), (1423), (1432), \\ & (12)(34), (13)(24), (14)(23) \} \end{aligned}$$

この中で

$$S_3 = \{ \varepsilon, (12), (13), (23), (123), (132) \},$$

$$V = \{ \varepsilon, (12)(34), (13)(24), (14)(23) \}$$

はどちらも S_4 の部分群である. V は Klein の 4 元群 とよばれる.

練習 3.4. 上記, 例 3.3 で $V < S_4$ であることを確かめよ.

例 3.5. $SL(2, \mathbb{Z})$ は $GL(2, \mathbb{R})$ の部分群である. 他に,

$$\begin{aligned} T &= \left\{ \begin{bmatrix} a & \\ & a \end{bmatrix} \mid a \in \mathbb{R}^\times \right\}, & A &= \left\{ \begin{bmatrix} a & \\ & c \end{bmatrix} \mid a, c \in \mathbb{R}^\times \right\}, \\ B &= \left\{ \begin{bmatrix} a & b \\ & c \end{bmatrix} \mid a, c \in \mathbb{R}^\times, b \in \mathbb{R} \right\}, & C &= \left\{ \begin{bmatrix} 1 & b \\ & 1 \end{bmatrix} \mid b \in \mathbb{R} \right\} \end{aligned}$$

なども $GL(2, \mathbb{R})$ の部分群である². 但し, 成分が 0 である場合は空欄としてゐる.

例 3.6. $SL(2, \mathbb{Z})$ は多種多様な部分群を多く含む. (一例が演習問題 3.15 にある.)

練習 3.7. 例 3.5 の言明をすべて確認せよ.

例 3.8. 次が成り立つ:

$$\left. \begin{array}{l} \{1, -1\} \\ \{z \mid z \in \mathbb{C}, z^3=1\} \end{array} \right\} < \{z \mid z \in \mathbb{C}, z^6=1\} < \{z \mid z \in \mathbb{C}, z^{12}=1\} < \{z \mid |z|=1\} < \mathbb{C}^\times$$

練習 3.9. G が群で $H < G, K < G$ のとき, $H \cap K < G$ であることを示せ.

² \mathbb{R}^\times は 0 を除いた実数全体を表す.

演習問題

3.10. G を群とする.

$$Z(G) = \{g \in G \mid gx = xg \ (\forall x \in G)\}$$

とおくとき, $Z(G) < G$ を示せ. $Z(G)$ は G の 中心 と呼ばれる.

3.11. G を群とし, $H < G$ とする. また $c \in G$ を取り固定する. このとき

$$c^{-1}Hc = \{c^{-1}hc \mid h \in H\} < G$$

であることを示せ. これを H の (1つの) 共役部分群 と呼ぶ.

3.12. 対称群 S_n の部分集合 $A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\}$ は S_n の部分群であることを示せ. さらに, その位数は $n!/2$ であることを示せ. A_n は n 次 交代群 と呼ばれる. また $\{\sigma \in S_n \mid \text{sgn}(\sigma) = -1\}$ は部分群でないことを示せ.

3.13. 3次対称群 S_3 の部分群を全て挙げよ. (ちなみに S_4 の全ての部分群を 12.13 で求める.)

3.14. 4次対称群 S_4 の部分集合 $H = \{\varepsilon, (12)\}$, $K = \{\varepsilon, (124), (142)\}$ は S_4 の部分群であることを確認せよ. また $H \cup K$ および $HK = \{hk \mid h \in H, k \in K\}$ は S_4 の部分群ではないことを示せ.

3.15. 自然数 N に対し,

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}(2, \mathbb{Z}) \mid a-1, d-1, b, c \text{ は } N \text{ の倍数} \right\}$$

とおく. $\Gamma(N) < \text{SL}(2, \mathbb{Z})$ であることを示せ.

4 巡回群

群 G の元 a に対して, $aa = a^2$, $(aa)a = a(aa) = a^3$ 等と記す. また a の逆元 a^{-1} に対して $a^{-1}a^{-1} = a^{-2}$, $a^{-1}a^{-1}a^{-1} = a^{-3}$ などと記す. これにより, “指数法則”

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn} \quad (m, n \in \mathbb{Z})$$

が成り立つ.

定義 4.1. 群 G が, その中の 1 つの元 a によつて

$$G = \{a^k \mid k \in \mathbb{Z}\}$$

と表せるとする. 実際この様に表される集合は群である (確かめよ). この様な群 G を 巡回群 と呼ぶ. この場合 a を G の 生成元 と呼び, G は a で 生成される といふ. この状況を $G = \langle a \rangle$ と表す.

一般に, 群 G と $a \in G$ について, $a^k = 1$ となる最小の正の整数 k を a の 位数 といひ $\text{ord } a$ と書く. $\langle a \rangle = G$ のとき G の位数は a の位数と一致する. なぜなら, 元 a の位数が n (つまり $\text{ord } a = n$) のとき

$$1, a, a^2, \dots, a^{n-1}$$

は互いに異なる元である (*****) からである. 位数が有限な巡回群は 有限巡回群 と呼ばれる.

また どの a^k ($k \neq 0$) も単位元 1 と異なるとき, a は 位数無限 の元であるといはれ $\text{ord } a = \infty$ と書かれる. 下の例 4.3 (1) における元 1 と例 (2) における元 3 は位数無限である. 位数が無限の巡回群は 無限巡回群 と呼ばれる. 無限巡回群においては, $a^k = a^{k'} \iff k = k'$ が成り立つ (******).

練習 4.2. 上記の波線部 (*****) と (******) を証明せよ.

例 4.3. 巡回群の例を挙げる.

- (1) 加法に関して \mathbb{Z} は 1 で生成される巡回群である.
- (2) 乗法に関して $3^{\mathbb{Z}} = \{3^k \mid k \in \mathbb{Z}\}$ は 3 で生成される巡回群である.
- (3) 複素数体の中で 1 の 3 乗根の全体 $\{z \mid z^3 = 1\}$ は乗法に関して巡回群である.
- (4) 同じく, 1 の 4 乗根の全体 $\{z \mid z^4 = 1\} = \{1, i, -1, -i\}$ は巡回群である.
- (5) 同じく, 1 の 5 乗根の全体 $\{z \mid z^5 = 1\} = \{\cos \frac{2\pi k}{5} + i \sin \frac{2\pi k}{5} \mid k = 0, 1, 2, 3, 4\}$ は巡回群.

(6) $A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ とおく. このとき, 集合 $\{I, A, A^2, A^3\}$ は行列の積に関して A で生成される巡回群である. ただし I は単位行列. ($A^4 = I$ となることを確かめよ.)

練習 4.4. 巡回群は Abel 群である. これを示せ.

例題 4.5. 次のことを証明せよ.

- (1) 巡回群の部分群はどれも巡回群である.
- (2) 有限位数 n の巡回群 $\langle a \rangle$ の部分群はどれも, n の約数 m により $\langle a^m \rangle$ と書かれる.
- (3) 無限位数の巡回群 $\langle a \rangle$ の部分群は, どれも, 自然数 m により $\langle a^m \rangle$ と書いて, m が異なればその部分群も異なる. これらもすべて無限位数の巡回群である.

解答 (1) H を $\langle a \rangle$ の任意の部分群とせよ. もちろん H の元はどれも a^k の形に書ける. もしも $H = \{1\}$ ならば, 証明は済んでゐるから, $H \neq \{1\}$ とし, $a^k \in H$ となる k の中で正で最小なものを m とおく. その様な m は存在する. なぜなら $a^k \in H$ となる整数 $k (\neq 0)$ があるが, $a^k \in H$ ならば $a^{-k} \in H$ であるから. さて, 任意に $a^k \in H$ を取る. このとき $k = mq + r$ ($0 \leq r < m$) となる整数 q と r が存在する. しかるに $a^r = a^{k-mq} = a^k(a^m)^{-q}$ であり H は部分群であるから, $a^r \in H$ が導かれる. m の選び方から $r = 0$ でなければならない. つまり $k = mq$. よつて H の任意の元は $a^{mq} = (a^m)^q$ の形に書かれる. つまり $H = \langle a^m \rangle$.

(2) (1) より $\langle a \rangle$ の任意の部分群は, ともかく正で最小な m により $\langle a^m \rangle$ と書かれる. いま, $n = ml + s$ ($0 \leq s < m$) となる整数 l と s を取れば, $a^s = a^n a^{-ml} \in H$ なので $s = 0$ を得る. つまり m は n の約数である.

(3) 上の (1) の証明から, 無限巡回群 $\langle a \rangle$ の部分群 H について, それを $H = \langle a^m \rangle$ ($m > 0$) と表せば, m は必然的に H に含まれる元 a^k の中での最小の k に一致する. 従つて, m と m' が異なれば $\langle a^m \rangle$ と $\langle a^{m'} \rangle$ も異なる.

練習 4.6. (1) 成分がすべて整数である 5 次の正方行列を使つて, 行列の積を演算とする位数 5 の巡回群を構成せよ. また, その生成元も述べよ.

(2) 前問と同じく, 成分がすべて整数である 5 次の正方行列を使つて, 位数 6の巡回群を構成し, その生成元を述べよ.

(3) さらに, 成分がすべて整数である 2 次の正方行列で, 積に関して, 位数 6の巡回群を構成し, その生成元を述べよ.

演習問題

4.7. 例 3.2 で登場した群 \mathbb{Q}^\times は巡回群でない. これを証明せよ.

4.8. 4 つの 2 次正方行列の集合 $\left\{ \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, \begin{bmatrix} -1 & \\ & -1 \end{bmatrix}, \begin{bmatrix} & -1 \\ -1 & \end{bmatrix} \right\}$ は行列の積に関して群になることを確かめよ. さらに, この群が巡回群でないことを説明せよ.

4.9. n を自然数とする. 成分が全て実数である 2 次の正方行列を要素からなり, 演算を行列の積とする位数 n の巡回群を構成せよ. (Hint: 三角関数を使ふ.)

5 Euler の函数 $n \mapsto \varphi(n)$

まづ, 次の問題から始める.

練習 5.1. 位数 30 の元 a を生成元とする巡回群 $\langle a \rangle$ の生成元を全て書き上げよ.

自然数 n に対して, 集合 $\{1, 2, \dots, n\}$ の中で n と素なもの個数を $\varphi(n)$ で表し, 函数

$$n \mapsto \varphi(n)$$

を Euler の φ 函数³⁾ といふ. $\varphi(1) = 1$ に注意せよ. 例へば, 素数 p に対しては $\varphi(p) = p - 1$ であり, また, 素数 p の累乗について

$$(5.2) \quad \varphi(p^r) = p^r - p^{r-1}$$

であることは容易にわかる. さらに, 自然数 m と n に対して, その正の最大公約数を $\gcd(m, n)$ と表せば³⁾,

$$(5.3) \quad \gcd(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$$

が成り立つことをあとで (定理 9.7) で証明する.

練習 5.4. (1) 上記の (5.2) が成り立つ理由を述べよ.

(2) $\varphi(9)$, $\varphi(5)$, $\varphi(45)$ を別々に計算し, この場合に (5.3) が成立してゐることを確認せよ.

巡回群の生成元について

命題 5.5. G を巡回群とする.

(1) G の位数 n が有限のときは, 生成元の個数は $\varphi(n)$ 個であり, 1 つの生成元を a とすれば, 生成元の全体は $\{a^m \mid \gcd(m, n) = 1\}$ である.

(2) G の位数が無限大のときは, 生成元は 2 つしかなく, その 1 方を a とすれば, 他方は a^{-1} である.

証明 (1) もし $\langle a \rangle = \langle a^m \rangle$ であれば, ある j について $a^{mj} = a$ だから $mj - 1$ は n の倍数である (これを $mj \equiv 1 \pmod{n}$ と書く). ゆゑに $\gcd(m, n) = 1$. 逆に, $\gcd(m, n) = 1$ とすると, $cm + dn = 1$ となる整数 c, d が存在する. このとき, $(a^m)^c = a^{cm} = a^{cm}(a^n)^d = a^{cm+dn} = a$ なので, $\langle a \rangle = \langle a^m \rangle$ を得る.

(2) については, すでに例題 4.5(3) で示されてゐる. □

³⁾最大公約数 (greatest common divisor)

注意 5.6. (Euclid の互除法) 2つの整数 a, b の (正の) 最大公約数を $\gcd(a, b)$ と書く. このとき $ax + by = \gcd(a, b)$ となる整数 x, y が存在することは Euclid の互除法を使つて証明できる. そのことを命題 5.5 (1) の証明で使つた. 例へば $a = 893, b = 237$ ならば

$$\begin{array}{l} 893 = 237 \times 3 + 182, \quad (711) \\ 237 = 182 \times 1 + 55, \quad (182) \\ 182 = 55 \times 3 + 17, \quad (165) \\ 55 = 17 \times 3 + 4, \quad (51) \\ 17 = 4 \times 4 + 1, \quad (16) \\ 4 = 1 \times 4 + 0, \quad (4) \end{array} \quad \begin{array}{c|c|c|c} 3 & 893 & 237 & 1 \\ & 711 & 182 & \\ \hline 3 & 182 & 55 & 3 \\ & 165 & 51 & \\ \hline 4 & 17 & 4 & 4 \\ & 16 & 4 & \\ \hline & 1 & 0 & \end{array}$$

この計算を下から順に使つて,

$$\begin{aligned} 1 &= 17 - 4 \times 4 \\ &= 17 - 4 \times (55 - 17 \times 3) \\ &= 13 \times 17 - 4 \times 55 \\ &= 13 \times (182 - 55 \times 3) - 4 \times 55 \\ &= 13 \times 182 - 43 \times 55 \\ &= 13 \times 182 - 43 \times (237 - 182 \times 1) \\ &= 56 \times 182 - 43 \times 237 \\ &= 56 \times (893 - 237 \times 3) - 43 \times 237 \\ &= 56 \times 893 - 211 \times 237 \end{aligned}$$

で $x = 56, y = -211$ が見付かるといふ具合である.

練習 5.7. $a = 9841, b = 1234$ とする. $\gcd(a, b) = 1$ を確かめよ. $ax + by = 1$ となる整数 x と y を 1 組求めよ.

練習 5.8. 位数 9841 の元 a から生成される巡回群 G がある. このとき, a^{1234} は G の生成元であるか. もし, さうならば $(a^{1234})^m = a$ となる整数 m が存在する筈である. その様な m で $0 \leq m < 9841$ なるものを求めよ.

演習問題

5.9. $13x + 7y + 11z = 1$ を満たす整数の組 (x, y, z) のすべてを求めよ (つまり, 解のすべてを簡明な仕方で記述せよ).

6 可換環と体

群はただ 1 つの演算を有するのであつたが、四則演算を備へた整数、有理数、実数などの集合を包摂する概念として、環といふものがある。

定義 6.1. 加法と呼ばれる演算 $(a, b) \rightarrow a + b$ と乗法と呼ばれる演算 $(a, b) \rightarrow ab$ の定義された集合 R が可換環であるとは、 R が次の 5 つの条件を満たすことである：(ただし a, b, c は R の任意の元を表す)

R1 R は加法に関して可換群である。(単位元は通常 0 で表す)

R2 乗法の結合法則： $(ab)c = a(bc)$.

R3 左右の分配法則⁴： $a(b + c) = ab + ac$, $(b + c)a = ba + ca$.

R4 単位元の存在：加法の単位元 0 とは異なるある元 $1 \in R$ が存在して、 R の任意の元 x に対して $1x = x1 = x$ が満たされる。

R5 乗法の交換法則： $ab = ba$

例 6.2. \mathbb{Z} , \mathbb{Q} , $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ はどれも可換環である。

定義 6.3. 可換環 R で、0 以外のどの元も乗法に関する逆元を持つならば、 R は体^{たい}であるといはれる。

例 6.4. \mathbb{Q} , \mathbb{R} , \mathbb{C} , p を素数としたとき、後述する $\mathbb{Z}/p\mathbb{Z}$ (証明は練習 9.4), $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$, $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ はすべて体である。

練習 6.5. 上記の $\mathbb{Q}[i]$ と $\mathbb{Q}[\sqrt{2}]$ が体であることを示せ。

注意 6.6. 上記の定義 6.1 において、5 つの条件のうちの最後の条件 **R5** を課さない場合は R は単に環であるといわれる。さらに、環 R の加法の単位元以外の元がどれも乗法に関して逆元を持つとき、 R は斜体^{しゃたい}であるといはれる。

例へば、 $\text{Mat}(2, \mathbb{C}) =$ “成分が複素数の 2 次正方行列の全体” は環である。また、

$$\mathbb{H} = \left\{ \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\} \subset \text{Mat}(2, \mathbb{C}) \quad (\text{もちろん } i \text{ は虚数単位})$$

とおくとき、行列の通常の加法と乗法に関して \mathbb{H} は斜体になる(♠)。 \mathbb{H} は Hamilton の四元数体 と呼ばれる。

練習 6.7. 上の ♠ を証明せよ。

⁴R5 を使へば、一方の分配法則から他方のそれがでる。

7 整数の性質

代数学で後に、約数、倍数の概念の一般化を学ぶ。そのために、^{イデア}ideal の概念に触れておく。

定義 7.1. 可換環 R の空でない部分集合 $M \subset R$ は

I1 $a \in M, b \in M$ ならば $a + b \in M$,

I2 $a \in M, x \in R$ ならば $xa \in M$

が成り立つとき、 R の ideal と呼ばれる。

例 7.2. (1) $\{0\}$ は \mathbb{Z} の ideal である。 (2) $m\mathbb{Z}$ は \mathbb{Z} の ideal である。

(3) $m, n \in \mathbb{Z}$ を固定する。 $\{ms + nt \mid s, t \in \mathbb{Z}\}$ は \mathbb{Z} の ideal である。

(4) $m_1, m_2, \dots, m_r \in \mathbb{Z}$ を固定する。 $\{m_1s_1 + m_2s_2 + \dots + m_rs_r \mid s_1, s_2, \dots, s_r \in \mathbb{Z}\}$ は \mathbb{Z} の ideal である。

(5) 可換環 $\mathbb{Z}[\sqrt{-5}] = \{s + \sqrt{-5}t \mid s, t \in \mathbb{Z}\}$ を考える。このとき

$$M = \{2x + (1 + \sqrt{-5})y \mid x, y \in \mathbb{Z}\}$$

は $\mathbb{Z}[\sqrt{-5}]$ の ideal であり、 M は $\{2\xi + (1 + \sqrt{-5})\eta \mid \xi, \eta \in \mathbb{Z}[\sqrt{-5}]\}$ と一致する。これは通常 $(2, 1 + \sqrt{-5})$ と略記される。

練習 7.3. 次の集合は $\mathbb{Z}[i]$ を加法に関する群とみたとき、部分群であるか。また $\mathbb{Z}[i]$ を環とみたとき、この中で ideal であるか否か、理由を付けて答へよ。

(1) \mathbb{Z} . (2) $\{a + bi \mid a \text{ と } b \text{ はともに偶数かともに奇数}\}$. (3) $\{a + 2bi \mid a, b \in \mathbb{Z}\}$.

練習 7.4. 例 7.2 (4) において、 $M = \{2\xi + (1 + \sqrt{-5})\eta \mid \xi, \eta \in \mathbb{Z}[\sqrt{-5}]\}$ を証明せよ。さらに、 M が $\mathbb{Z}[\sqrt{-5}]$ の ideal であることを示せ。

練習 7.5. 可換環 $R = \mathbb{Z}[\sqrt{-5}]$ において $1 + \sqrt{-5}$ と 5 をともに含む ideal I は R と一致することを示せ。

定理 7.6. $M \subset \mathbb{Z}$ を \mathbb{Z} の ideal であるとする。このときある $d \in \mathbb{Z}$ が存在して、

$$M = d\mathbb{Z}$$

となる。ここで、さらに $d \geq 0$ といふ条件を付ければ、その様な d の存在は一意的である。

証明 $M = \{0\}$ であれば主張は明かなので、以下では $M \neq \{0\}$ とする。 M の正の要素で最小なものを d とすると、これが求めるものである。実際、任意の $k \in M$ に対して、それを d で割った余りを r とし、 $k = dq + r$, $0 \leq r < d$, と書くと、ideal の定義から $r = k - dq \in M$ となるが、 d の最小性から $r = 0$ でなくてはならない。つまり $k = dq \in d\mathbb{Z}$ がわかり、 $M \subset d\mathbb{Z}$ である。逆の包含関係は明かである。□

注意 7.7. 定理 7.6 の \mathbb{Z} を例 6.2 にある $\mathbb{Z}[i]$ や $\mathbb{Z}[\sqrt{2}]$ で置き換へても、同様なことが成り立つ (あとで、定理 16.12 として述べる)。しかし $\mathbb{Z}[\sqrt{-5}]$ などにおいては、さうでない場合が生じる。例へば、例 7.2 (3) の $M = (2, 1 + \sqrt{-5})$ は $d\mathbb{Z}[\sqrt{-5}]$ (但し $d \in \mathbb{Z}[\sqrt{-5}]$) の形には書けない。(複素数平面上での M の配置を考へればわかる)。

以下では, 整数 a と b について, a が b の約数であることを

$$a|b$$

で表す.

練習 7.8. 例 7.2 (3) の $M = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid x_1, x_2, \dots, x_n \in \mathbb{Z}\}$ について $M = d\mathbb{Z}$ となる $d \in \mathbb{Z}$ ($d \geq 0$) は a_1, a_2, \dots, a_n のすべてを割り切る非負整数の中で最大のものであることを示せ. (最大公約数の存在性の証明) (Hint : d' が a_1, \dots, a_n の任意の公約数であるとき $d'|d$ となることと, d 自身は a_1, \dots, a_n の公約数であることを示せばよい.)

定義 7.9. (最大公約数) 演習 7.8 の d を

$$\gcd(a_1, a_2, \dots, a_n)$$

と書く. この記法は注意 5.6 の記法と矛盾しない.

命題 7.10. (1) $\gcd(a, b) = 1$ かつ $a|bc$ ならば $a|c$.

(2) $\gcd(a, x) = \gcd(a, y) = 1$ のとき, $\gcd(a, xy) = 1$.

(3) $\gcd(a, x_1) = \gcd(a, x_2) = \cdots = \gcd(a, x_n) = 1$ のとき, $\gcd(a, x_1x_2 \cdots x_n) = 1$.

証明 (1) $\gcd(a, b) = 1$ ならば $ax + by = 1$ となる整数 x, y が存在する. これを c 倍すると $c = acx + bcy$ なので, 仮定 $a|bc$ より, $a|c$ がわかる.

(2) 仮定から $ap + xq = 1, ar + ys = 1$ となる整数 p, q, r, s が存在する. この 2 式の辺々を掛けて $a(apr + pqs + rxq) + xy(qs) = 1$ を得るから, $\gcd(a, xy) = 1$ である.

(3) これは (2) を繰り返し使えば示される. □

8 素因数分解の一意性

ここで、すでにお馴染みの素因数分解の一意性について述べる。

定理 8.1. (素因数分解とその一意性) 任意に整数 $n \neq 0$ が与へられたとせよ. このとき n は, 相異なる有限個の (正の) 素数 p_1, p_2, \dots, p_g により,

$$n = \pm \prod_{j=1}^g p_j^{e_j} \quad (e_j \text{ は自然数})$$

の形に素因数分解される. またその様な分解は一意的である. ここに, 先頭の符号は n の正負による.

注意 8.2. 読者は, 上記の定理をよくご存知だと思ふ. それをわざわざ定理として述べるのは, これが成り立たない可換環の例が身近にあつて (下の注意 8.7), そのことが近代の整数論の研究の動機の一部になつたからである.

証明 $n > 0$ のときに示せば十分であらう. n に関する帰納法で示す. $n = 1$ に対して定理の主張は明らかに正しい. いま p を n の 1 つの素因数とせよ. このとき, $n = p$ であれば証明は済んでゐる. でなければ, $\frac{n}{p} > 1$ は整数であるが, n より小さいので, 帰納法の仮定により $\frac{n}{p}$ は (一意的に) 素因数分解される. よつて n 自身も素因数分解される. 次に一意性を示す. いま $p_1, p_2, \dots, q_1, q_2 \dots$ を (正の) 素数 (同じものもいくつも含んでゐるかも知れない) として, n が

$$n = p_1 p_2 \cdots = q_1 q_2 \cdots$$

と 2 通りに素因数分解されてゐたとする. このとき, 左辺は p_1 で割れるから右辺の素因数のどれかが p_1 でなくてはならない. そこで, 両辺から p_1 を落して, 同じ議論を p_2, \dots に対して行つていく. 最後に $1 = 1$ なる等式に至る. よつて, 両辺に現れる素因数 p_1, p_2, \dots と $q_1, q_2 \dots$ は順序を無視すれば同一である. \square

定義 8.3. 可換環 R の 2 つの元 a, b について, ある $c \in R$ により, $b = ac$ と書けるとき, a は b の 約元 であるといひ, b は a の 倍元 であるといふ. また a は b を 割り切る, b は a で 割り切れる, などといふ. これも記号で $a|b$ と表す. これの否定を $a \nmid b$ と書く.

定義 8.4. 可換環 R と $q \nmid 1$ なる元 $q \in R$ について, 「任意の $a \in R, b \in R$ に対し, $q|ab$ ならば $q|a$ または $q|b$ である」が成り立つとき, q は R の 素元 であるといふ.

また, $q = ab$ ($a, b \in R$ で $a \nmid 1, b \nmid 1$) と書けないとき, q を R の 既約元 と呼ぶ.

注意 8.5. \mathbb{Z} においては素元と既約元の内容は一致する. 一般に, 零因子⁵ を含まない可換環では, 素元は既約元である. 実際, q が可換環 R の素元で, $q = ab$ ($a \nmid 1, b \nmid 1$) と書けたなら, $q|a$ または $q|b$ となるが, もし $q|a$ ならば, $q = a' b q$ と書けるので $1 = a'/b$, 即ち $b|1$ となつて矛盾である. $q|b$ の場合も同様. しかし, 既約元は素元とは限らない (次の例 8.6).

⁵ $ab = 0, a \neq 0, b \neq 0$ のとき, a, b は零因子と呼ばれる.

例 8.6. $R = \mathbb{Z}[\sqrt{-5}]$ において, $3 \mid (2+\sqrt{-5})(2-\sqrt{-5}) = 9$ であるが, $3 \nmid (2+\sqrt{-5})$ かつ $3 \nmid (2-\sqrt{-5})$ なので (絶対値を考察すればわかる), 3 は素元ではない. ちなみに 3 はこの R の既約元である.

注意 8.7. $R = \mathbb{Z}[\sqrt{-5}]$ においては,

$$21 = 3 \cdot 7 = (4+\sqrt{-5})(4-\sqrt{-5})$$

と 2 通りの既約元による分解が存在する.

練習 8.8. 例 8.6 と例 8.7 に関して, 3, 7, $4+\sqrt{-5}$, $4-\sqrt{-5}$ のいずれも $\mathbb{Z}[\sqrt{-5}]$ の既約元であることを示せ.

演習問題

8.9. n を自然数, p を素数とせよ. このとき, p^N が $n!$ を割り切るやうな最大の整数 N は

$$N = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

で与えられることを示せ. (この和は実質的には有限の和である.)

8.10. a, m, n はすべて自然数で, $m \neq n$ とする. このとき $a^{2^m} + 1$ と $a^{2^n} + 1$ の最大公約数は a の偶奇に応じて, 1 または 2 であることを示せ. (Hint: $n > m$ のとき $(a^{2^m} + 1) \mid (a^{2^n} - 1)$ であることを示して利用する.) このことから, 無限に多く素数が存在することを証明せよ.

8.11. $\gcd(a, b) = 1$ で $a^2 - b^2$ が完全平方数であるとき $\gcd(a - b, a + b)$ は 1 か 2 であることを示せ. さらにこのとき $a + b, a - b$ はともに完全平方数であるかどうかどちらも完全平方数の 2 倍であることを示せ.

8.12.* 自然数 $n \geq 2$ について, $\sum_{k=1}^n \frac{1}{k}$ は整数ではないことを証明せよ.

8.13.* n を p 進法で表示したときに, すべての桁の数の和を $S_p(n)$ とする.⁶ このとき, 問題 8.9 の N について,

$$N = \frac{n - S_p(n)}{p - 1}$$

であることを証明せよ.

⁶例へば 516 を 5 進法表示すると $4031_{(5)}$ なので $S_5(516) = 4 + 0 + 3 + 1 = 8$.

9 剰余類の演算

整数 x, y, n について $n|(x-y)$ となることを

$$x \equiv y \pmod{n}$$

とも表す. この式は, x と y を n で割ったときの余りが相等しいといふことを意味でもある.

命題 9.1. 整数 x_1, x_2, y_1, y_2 について, $x_1 \equiv y_1 \pmod{m}$, $x_2 \equiv y_2 \pmod{m}$ ならば

$$x_1 + x_2 \equiv y_1 + y_2 \pmod{m}, \quad x_1 x_2 \equiv y_1 y_2 \pmod{m}.$$

練習 9.2. 命題 9.1 を証明せよ.

そこで, 整数 j について, \mathbb{Z} の部分集合

$$(9.3) \quad \begin{aligned} j + m\mathbb{Z} &= \{\dots, -m+j, j, j+m, j+2m, \dots\} \\ &= \text{“} m \text{ で割ったときに余りが } j \text{ のそれと同じになる整数の全体”} \end{aligned}$$

をそれぞれ $(j \pmod{m})$ または簡単に \bar{j} などと記す:

$$\bar{j} = (j \pmod{m}) = j + m\mathbb{Z} = \{\dots, -m+j, j, j+m, j+2m, \dots\}.$$

この記法では, 例へば $(2 \pmod{7}) = (9 \pmod{7}) = (-5 \pmod{7})$ 等が成り立つことに注意せよ. このとき, 上の (9.1) より

$$\begin{aligned} (x \pmod{m}) + (y \pmod{m}) &= (x + y \pmod{m}), \\ (x \pmod{m})(y \pmod{m}) &= (xy \pmod{m}) \end{aligned}$$

と定義すれば (右辺で左辺の演算を定義する), (9.3) の形の集合を元とする集合, つまり

$$\{(0 \pmod{m}), (1 \pmod{m}), (2 \pmod{m}), \dots, (m-1 \pmod{m})\}$$

が自然に環の構造を持つことがわかる. これを $\mathbb{Z}/m\mathbb{Z}$ と記し, 法 m に関する剰余類 (剰余類環) と呼ぶ

練習 9.4. 次が成り立つ:

- (1) $\gcd(a, m) = 1$ ならば, $\mathbb{Z}/m\mathbb{Z}$ において, $\bar{a}\bar{x} = \bar{1}$ となる元 \bar{x} が唯 1 つ存在する. (Hint: $\gcd(a, m) = 1$ ならば, 定理 7.6 より, $ax + my = 1$ となる整数 x, y が存在する.)
- (2) p を素数とするととき, $\mathbb{Z}/p\mathbb{Z}$ は体である.
- (3) m が合成数⁷ ならば $\mathbb{Z}/m\mathbb{Z}$ は体ではない. (Hint: $\ell | m$ ($0 < \ell < m$) のとき, $(\ell \pmod{m})(x \pmod{m}) = (1 \pmod{m})$ となる x は存在しない.)

練習 9.5. x, y, z は整数とする. $x^2 + y^2 = z^2$ ならば, $xyz \equiv 0 \pmod{60}$ であることを示せ. 以上をまとめておく:

定理 9.6. m を正の整数とする. 法 m に関する剰余類の全体 $\mathbb{Z}/m\mathbb{Z}$ は単位元を持つ可換環をなす. また, m と素な剰余類の全体 $(\mathbb{Z}/m\mathbb{Z})^\times$ は積に関して群 (既約剰余類群) をなす. $\mathbb{Z}/m\mathbb{Z}$ が体になるのは m が素数のときであり, そのときに限る.

⁷素数でも ± 1 でも 0 でもない数のこと.

次に、留保してきた (5.3) を証明する：

定理 9.7. 自然数 m と n について、 $\gcd(m, n) = 1$ ならば $\varphi(mn) = \varphi(m)\varphi(n)$ である。

証明 $(\mathbb{Z}/mn\mathbb{Z})^\times$ から $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ への写像 f を、

$$f : (x \bmod mn) \mapsto ((x \bmod m), (x \bmod n))$$

で定める。各 $(x \bmod mn)$ の f による像は集合 $(x \bmod mn)$ のみによつて決まり、 x の選び方には依らない。また $\gcd(x, mn) = 1$ だから $\gcd(x, m) = \gcd(x, n) = 1$ であることにも注意せよ。つまり、 f は矛盾なく定義される (well-defined)。また、この写像には逆写像が存在する。それは $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ の任意の元 $((a \bmod m), (b \bmod n))$ に対して $x \equiv a \bmod m$, $x \equiv b \bmod n$ を満たす x を対応させるものであるが、まづ、この様な x は存在する。なぜなら $tm + sn = 1$ なる t, s に対して $x = asn + btm$ とすれば

$$x \equiv asn \equiv a(1 - tm) \equiv a \bmod m, \quad x \equiv btm \equiv b(1 - sn) \equiv b \bmod n$$

となるから。しかも、この様な x は法 mn で一意的である。実際、もし 2 つの解 x と x' があると、 $m|(x - x')$, $n|(x - x')$ であるが、これらから $m|(x - x')$, $n|(x - x')$ ゆえ、 $mn|(x - x')$ となるから。さらに $((a' \bmod m), (b' \bmod n))$ に $(x' \bmod mn)$ が対応するとき、 $((aa' \bmod m), (bb' \bmod n))$ に $(xx' \bmod mn)$ が対応する (*). 特に、 $aa' \equiv 1 \bmod m$ かつ $bb' \equiv 1 \bmod n$ ならば $xx' \equiv 1 \bmod mn$. つまり、この逆写像は問題なく定義される。しかるに、各 $x \in \mathbb{Z}/mn\mathbb{Z}$ に対して、それぞれの元の個数は $\varphi(mn)$ と $\varphi(m)\varphi(n)$ であるから、所望の等式が成り立つ。□

練習 9.8. 上の証明で (*) の部分を確認せよ。

練習 9.9. $m, n \in \mathbb{Z}$ とし、 $d = \gcd(m, n)$ とせよ。 x の連立合同式

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$$

が解を持つためには、 $a \equiv b \bmod d$ であることが必要十分であることを示せ。また、 m と n の最小公倍数を l とすれば、解を持つ場合、解は $\bmod l$ でみれば唯 1 つである事を示せ。

練習 9.10. 整数 $n > 0$ の素因数分解を $n = \prod_{j=1}^g p_j^{e_j}$ とする。但し、 p_1, \dots, p_g は相異なる素数で、 e_1, \dots, e_g は自然数である。このとき、次の式が成り立つことを示せ。

$$\varphi(n) = \prod_{j=1}^g (p_j^{e_j} - p_j^{e_j-1}) = n \prod_{j=1}^g \left(1 - \frac{1}{p_j}\right).$$

練習 9.11. p を素数とする。2 次正方行列の成分に $\mathbb{Z}/p\mathbb{Z}$ の元を並べて

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}/p\mathbb{Z}, ad - bc \neq \bar{0} \right\} \quad (\text{これは、通常 } \text{GL}(2, \mathbb{Z}/p\mathbb{Z}) \text{ と書かれる。})$$

なる集合を考へる。このとき、 G に属する任意の 2 元について通常の行列の積の仕方で演算が定義できることを示し、さらに、その演算で G が群になることを証明せよ。

10 Fermat の小定理, Euler の定理

次の定理は定理 13.2 の証明で使用される.

定理 10.1. n を正の整数とする. このとき

$$\sum_{k|n} \varphi(k) = n.$$

証明 いま整数 d を 1 つ決めて,

$$1, 2, \dots, n$$

の中に $\gcd(x, n) = d$ である x がいくつあるか数へる. もちろん, d が n の約数でなければ, 答は 0 個である. そこで $d|n$ として, $x = dx', n = dn'$ とおけば, $\gcd(x, n) = d$ は $\gcd(x', n') = 1$ と同じことである. その様な x' の個数は $\varphi(n') = \varphi(n/d)$ である. ここで $x = 1, 2, \dots, n$ を $\gcd(x, n)$ の値 d で分類すれば, $d = 1$ に対応するものが $\varphi(n)$ 個, $d = d_1$ に対応するものが $\varphi(n/d_1)$ 個, $d = d_2$ に対応するものが $\varphi(n/d_2)$ 個, 等であり, 最後に $d = n$ に対応するものが $\varphi(1) = 1$ 個ある. これらは重複がなく上のすべての数を尽くすから

$$\varphi(n) + \varphi\left(\frac{n}{d_1}\right) + \varphi\left(\frac{n}{d_2}\right) + \dots + \varphi(1) = n.$$

ここで $\frac{n}{d_j}$ はすべての約数 k を走るから, これが与式に他ならない. □

注意 10.2. 上の 10.1 の証明の内容を $n = 42 = 2 \cdot 3 \cdot 7$ の場合に表にしておく.

d	$\gcd(x, 42) = d$ となる $0 \leq x \leq 42$	$\varphi\left(\frac{42}{d}\right)$
1	{ 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41 }	12
2	{ 2, 4, 8, 10, 16, 20, 22, 26, 32, 34, 38, 40 }	12
3	{ 3, 9, 15, 27, 33, 39 }	6
6	{ 6, 12, 18, 24, 30, 36 }	6
7	{ 7, 35 }	2
14	{ 14, 28 }	2
21	{ 21 }	1
42	{ 42 }	1
計	{ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42 }	42

ここで有名な定理を 1 つ証明しておく :

定理 10.3. (Fermat の小定理) p を素数とせよ. $\gcd(a, p) = 1$ のとき

$$a^{p-1} \equiv 1 \pmod{p}.$$

証明 まず,

$$(10.4) \quad 1, 2, \dots, p-1$$

が \pmod{p} の剰余の全体である. このとき

$$(10.5) \quad 1a, 2a, \dots, (p-1)a$$

も \pmod{p} の剰余の全体である. 実際, もし $ka \equiv la \pmod{p}$ ならば $(k-l)a \equiv 0 \pmod{p}$ なので $k-l \equiv 0 \pmod{p}$ でなければならず, それゆえ $k \equiv l \pmod{p}$ となるが, 並べた元の個数が $p-1$ 個であるから, (10.5) は (10.4) の全体に一致せざるを得ない. このことより

$$1 \cdot 2 \cdots (p-1) \equiv 1a \cdot 2a \cdots (p-1)a \equiv a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

よつて

$$(a^{p-1} - 1) \cdot 1 \cdot 2 \cdots (p-1) \equiv 0 \pmod{p}$$

となり

$$a^{p-1} - 1 \equiv 0 \pmod{p}$$

を得る. □

定理 10.3 を自然に一般化したものが次の Euler の定理である :

定理 10.6. (Euler の定理) n を正の整数とせよ. $\gcd(a, n) = 1$ のとき

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

が成り立つ.

証明 まず \pmod{n} の既約剰余類を並べて, 定理 10.3 の証明と同様にそれら全体の a 倍 (の剰余類) を並べれば, それらは再び既約剰余類となり, 順序を無視すればすべての既約剰余類を並べたものに一致する. よつてそれらの積は一致する. この 2 つの積の違いは $a^{\varphi(n)}$ 倍なので

$$a^{\varphi(n)} - 1 \equiv 0 \pmod{n}$$

を得る. □

練習 10.7. 定理 10.6 の証明を $n = 15, a = 2$ について^{たど}辿れ.

11 多項式の基本的性質

当面の目標は定理 13.2 である. そのための準備をする.

x を文字 (不定元 と呼ばれる) とする. x の多項式で係数がすべて体 K に属するもの全体を

$$K[x]$$

と表す. これは自然な加法と乗法について可換環になることが容易に確かめられる.

命題 11.1. x を文字とする. $f(x), g(x) \in K[x]$ のとき, 多項式 $q(x), r(x) \in K[x]$ が存在して, $\deg r(x) < \deg g(x)$ かつ $f(x) = g(x)q(x) + r(x)$ となる. 但し, $\deg h(x)$ は $h(x)$ の次数.

証明 これは $K = \mathbb{Q}$ や $K = \mathbb{R}$ のときに, 高校で学んだものと全く同様である. 即ち, $f(x)$ を $g(x)$ で除したとき (筆算などで求められる) の商が $q(x)$ で余りが $r(x)$ である. \square

系 11.2. $c \in K$ のとき, $q(x) \in K[x]$ が存在して, $f(x) = (x - c)q(x) + f(c)$ となる.

系 11.3. 体 K 上の多項式 $f(x) \in K[x]$ について, $\deg f(x) = n$ ならば $f(x) = 0$ は高々 n 個の相異なる根を持つ.

証明 α_1 が根であれば, 系 11.2 より $f(x) = (x - \alpha_1)f_1(x)$, $\deg f_1(x) = n - 1$ となる. α_2 が根であれば, それは $f_1(x)$ の根であるから, 再び, 系 11.2 より, $f_1(x) = (x - \alpha_2)f_2(x)$ となる. これを繰り返すとき, 根の個数が n 個以上であつたならば, 0 次式が根を持つことになるので, 矛盾である. \square

練習 11.4. $K[x] = (\mathbb{Z}/5\mathbb{Z})[x]$ において, $f(x) = \bar{2}x^3 + x^2 + \bar{3}x + \bar{1}$, $g(x) = x^2 + \bar{2}x + \bar{3}$ のときに, 命題 11.1 に述べられてゐる $q(x)$ と $r(x)$ を求めよ.

練習 11.5. $(\mathbb{Z}/5\mathbb{Z})[x]$ において, $f(x) = \bar{2}x^3 + \bar{4}x^2 + \bar{3}x + \bar{1}$ のとき, $f(x) = 0$ の根をすべて見つけ, $f(x)$ を因数分解せよ.

練習 11.6. $(\mathbb{Z}/5\mathbb{Z})[x]$ において, $x^4 + \bar{1}$ を可能な限り因数分解せよ. (注意: 1 次式には分解できない)

12 Lagrange の定理

目標の定理 13.2 を証明するために, Lagrange の定理と呼ばれる有名な定理を証明したい. 群 G の元 x と部分集合 $A \subset G$ について $xA = \{xa \mid a \in A\}$ と記す. 勿論 $1A = A$ である.

練習 12.1. G を群とし, $x, y \in G, A \subset G$ とせよ. このとき $xG = G, x(yA) = (xy)A$ であることを示せ.

練習 12.2. 群 G とその部分群 H を考える. $x, y \in G$ のとき, $y \in xH \iff x^{-1}y \in H$ であることを示せ.

補題 12.3. 2 元 $x \in G$ と $y \in G$ について, $xH \cap yH = \emptyset$ さもなくば $xH = yH$ である.

証明 もし $xH \cap yH \neq \emptyset$ ならば, 左辺に元 $xh = yh'$ ($h, h' \in H$) があるが, これより $x = yh'h^{-1}$ で $h'h^{-1} \in H$ なので, 練習 12.1 により, $xH = y(h'h^{-1})H = yH$ である. \square

この補題 12.3 により, G は xH の形の部分集合 (G の H による 左剰余類⁸ と呼ばれる) の和に分割できる. いま, その個数が有限だとして⁹, g 個とし, それらの部分集合のすべてを

$$(12.4) \quad \{x_1H, x_2H, \dots, x_gH\} \quad (\text{これを } G/H \text{ と略記する})$$

と書くことにすれば (つまり, $i \neq j$ ならば $x_iH \cap x_jH = \emptyset$),

$$G = \bigcup_{j=1}^g x_jH$$

と表される. この表示式を 左剰余類分解 と呼ぶ. ここで (12.4) は一意的に定まるけれども, $\{x_1, x_2, \dots, x_g\}$ は一意的には定まらないことに注意されたい. この状況で $\{x_1, x_2, \dots, x_g\}$ をこの左剰余類分解の 代表系 と呼ぶ.

注意 12.5. 以上の様なことは無限位数の群でも論じられる. 実際, 例へば $G = \mathbb{Z}$ を加法群とみたとき, $\mathbb{Z}/m\mathbb{Z}$ は, 部分群 $H = m\mathbb{Z}$ による左剰余類分解に他ならない:

$$\mathbb{Z} = \bigcup_{j=0}^{m-1} (j + m\mathbb{Z}) \quad (\text{但し, } i \neq j \text{ ならば } (i+m\mathbb{Z}) \cap (j+m\mathbb{Z}) = \emptyset).$$

記号. 一般に, 集合 A の要素の個数 (濃度) を $|A|$ または $\#A$ で表す.

練習 12.6. 有限群 G とその部分群 H を考える. 任意の $x, y \in G$ について $|xH| = |yH|$ であることを証明せよ. (Hint: 各 $z \in H$ に対して, 写像 $H \rightarrow zH, h \mapsto zh$ が全単射であることを示せ. これより $|H| = |xH|, |H| = |yH|$ がわかり $|xH| = |yH|$ を得る.)

以上のことから G が同じ個数の要素を持ち, 互いに共通部分を持たない部分集合 (12.4) の和集合で表されることがわかった. これは顕著なことである. このことから次のことがわかる.

定理 12.7. (Lagrange の定理) 有限群 G の部分群 H の位数 $|H|$ は $|G|$ の約数である.

⁸文献によつては右剰余類と定義されてゐる場合がある.

⁹例へば G が有限群ならさうなる.

系 12.8. G を有限群とする. G の元の位数は $|G|$ の約数である.

証明 $x \in G$ の位数は部分群 $\langle x \rangle < G$ の位数に他ならないが, それは Lagrange の定理より $|G|$ の約数である. \square

系 12.9. G を位数 n の有限群とし, $x \in G$ とする. このとき $x^n = 1$.

証明 系 12.8 より, x の位数 (ℓ とする) は n の約数である. ゆえに $x^n = (x^\ell)^{n/\ell} = 1^{n/\ell} = 1$ である. \square

練習 12.10. 例 3.3 について, 次の問に答へよ.

- (1) S_4 とその部分群 S_3, V について, Lagrange の定理が成立してゐることを確認せよ.
- (2) S_4 を S_3 に関して左剰余類に分解し, 各左剰余類を要素を列記して記述せよ.
- (3) S_4 を V に関して左剰余類に分解し, 各左剰余類を要素を列記して記述せよ.

練習 12.11. 位数 15 の元 a で生成された巡回群 $G = \langle a \rangle$ と, その部分群 $H = \langle a^3 \rangle$ について, 左剰余類分解を記述せよ. また代表系を 1 つ挙げよ.

演習問題

12.12. 位数が素数の群は巡回群に限ることを示せ.

12.13. Lagrange の定理を前提にして, S_4 の部分群を全て求めよ.

12.14. G を群とし, $H < G$ とする. $x, y \in G$ に対して $x^{-1}y \in H$ で関係 $x \sim y$ を定めるとき, この関係は同値関係であることを確かめよ. 即ち, 次を示せ. 任意の $x, y, z \in G$ に対して,

- (i) $x \sim x$
- (ii) $x \sim y \implies y \sim x$
- (iii) $x \sim y$ かつ $y \sim z \implies x \sim z$

13 原始根

練習 13.1. 位数 n の有限巡回群 $G = \langle a \rangle$ において, $n = dl$ とするとき, $\{x \in G \mid x^d = 1\} = \langle a^l \rangle$ で, その元の個数は d に等しいことを示せ.

次の定理は有用である.

定理 13.2. G を有限群とする. G が巡回群であるためには, 任意の自然数 m について

$$\#\{x \in G \mid x^m = 1\} \leq m$$

であることが必要十分である.

証明 G の位数を n とする.

(必要性) $G = \langle a \rangle$ と書ける. $\gcd(n, m) = d$ と書くと, $x^m = 1 \iff x^d = 1$ であるから¹⁰ 練習 13.1 より, $\#\{x \in G \mid x^m = 1\} = \#\{x \in G \mid x^d = 1\} = d \leq m$ である.

(十分性) G の位数 m の元の集合を G_m と書くことにする. $G_m \neq \emptyset$ ならば, G_m の元から位数 m の部分群が生成されるのだから, Lagrange の定理により, $m \mid n$ である. ゆえに,

$$(13.3) \quad n = |G| = \sum_{m \mid n} |G_m|.$$

いま $m \mid n$ なる m をとり, $|G_m| > 0$ とする. このとき $a \in G_m$ について

$$\langle a \rangle = \{1, a, a^2, \dots, a^{m-1}\}$$

の元はどれも $x^m = 1$ の解であるから, 仮定により $\langle a \rangle = \{x \in G \mid x^m = 1\}$ でなければならない. 特に $G_m \subset \langle a \rangle$. つまり G_m は $\langle a \rangle$ 内の位数 m の元の全体になつてゐる. 以上から $|G_m| = 0$ または $|G_m| = \varphi(m)$ である. このことを念頭において, (13.3) と定理 10.1 とを比較すれば, すべての $m \mid n$ について $|G_m| = \varphi(m)$ でなければならないことがわかる. 特に $|G_n| = \varphi(n) \neq 0$ であるから, G は位数 n の元を持つ. その 1 つを b とすれば, $G = \langle b \rangle$ となる. □

練習 13.4. 巡回群ではない有限 Abel 群 の例を 1 つ挙げ, それが定理 13.2 の条件を満たさないことを具体的に示せ. (Hint: 例 3.3 の中からその様な例を見出せ.)

系 13.5. n を正の整数とする. K を体とする. このとき $\{x \in K \mid x^n = 1\}$ は n の約数を位数とする巡回群をなす.

証明 集合 $G = \{x \in K \mid x^n = 1\}$ が群であることは容易に確認できる. 任意の $m \in \mathbb{N}$ について, x の m 次方程式 $x^m = 1$ は K の中で高々 m 個しか解を持たない (系 11.3). ゆえに, $\#\{x \in G \mid x^m = 1\} \leq \#\{x \in K \mid x^m = 1\} \leq m$. このことと定理 13.2 より, 群 $\{x \in K \mid x^n = 1\}$ は巡回群である. いま, $a \in G$ を 1 つの生成元とする. $a^n = 1$ であるから, a の位数は n の約数でなければならない. □

系 13.6. 体 K の乗法群 K^\times のどんな有限部分群も巡回群である. 従つて, 有限体 $\mathbb{Z}/p\mathbb{Z}$ (p は素数) の乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群である.

¹⁰(\Leftarrow) は明らか. (\Rightarrow) $d = sn + tm$ と書くと系 12.9 と仮定から $x^d = (x^n)^s(x^m)^t = 1$.

証明 K^\times の任意の有限部分群 G を考へる. このとき, 任意の自然数 m について

$$\{x \in G \mid x^m = 1\} \subset \{x \in K^\times \mid x^m = 1\}$$

$$\therefore \#\{x \in G \mid x^m = 1\} \leq \#\{x \in K^\times \mid x^m = 1\} \leq m$$

であるから, 定理 13.2 により, G は巡回群である. \square

定理 13.7. p を素数とする. このとき, $(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群である. その生成元を法 p の 原始根 と呼ぶ. 即ち, 次の様な整数 g が存在する: $1, g, g^2, \dots, g^{p-2}$ を並び替へれば, 法 p に関して, $1, 2, \dots, p-1$ に合同である.

証明 これは系 13.6 の後半の言ひ代へに過ぎないが, 別の証明を記しておく. Fermat の小定理 10.3 と系 11.3 より $\{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$ が丁度 $x^{p-1} = 1$ の根である. 系 13.5 により, これらは巡回群をなす. \square

例 13.8. 3 は法 7 の原始根である. つまり,

$$(\mathbb{Z}/7\mathbb{Z})^\times = \langle 3 \rangle = \{(3 \bmod 7), (3^2 \bmod 7), \dots, (3^6 \bmod 7)\}.$$

例 13.9. $p = 17$ のとき, 原始根は $g = 3$ と取れて下記の表の様になる:

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$(3^j \bmod 17)$	$\bar{3}$	$\bar{9}$	$\bar{10}$	$\bar{13}$	$\bar{5}$	$\bar{15}$	$\bar{11}$	$\bar{16}$	$\bar{14}$	$\bar{8}$	$\bar{7}$	$\bar{4}$	$\bar{12}$	$\bar{2}$	$\bar{6}$	$\bar{1}$

ちなみに 2 は原始根でない.

練習 13.10. 2 は法 11 の原始根であるか. また 2 は法 7 の原始根か.

練習 13.11. 有限体 $\mathbb{Z}/17\mathbb{Z}$ の原始根をすべて求めよ. その 1 つを用いて x の方程式

$$x^4 \equiv 1 \pmod{17}$$

を満たす剰余類 $(x \bmod 17)$ をすべて求めよ.

練習 13.12. (Wilson の定理) p が素数のとき

$$(p-1)! \equiv -1 \pmod{p}$$

であることを証明せよ.

練習 13.13. p は奇素数であつて, $a^{2^n} + 1$ の約数であるとせよ. このとき

$$p \equiv 1 \pmod{2^{n+1}}$$

であることを示せ. Hint: $(a \bmod p)$ の $(\mathbb{Z}/p\mathbb{Z})^\times$ における位数を求めよ.

練習 13.14. n は自然数で, $p = 2^n + 1$ は素数であるとせよ¹¹.

(1) 2 は法 p の原始根ではないことを示せ.

(2) (難) 3 は法 p の原始根であることを証明せよ¹².

¹¹ その様な p は Fermat 素数 と呼ばれる

¹² Hint: 法 p で -1 が平方元であることを示せ. もし, 3 が原始根でないのなら平方元であることを示せ. それゆゑ, $-3 \equiv a^2 \pmod{p}$ なる a が存在する. このとき $2u \equiv -1 + a \pmod{p}$ で定まる u は位数が 3 であることを示せ. これと Fermat の小定理から $3|p-1$ を示し, 矛盾を導け.)

14 平方剰余

定義 14.1. p を奇素数とする. p と素な整数 a は, 合同式 $x^2 \equiv a \pmod{p}$ が解を持つか否かによつて, p を法として 平方剰余 あるいは 平方非剰余 であるといはれ,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & (a \text{ が平方剰余のとき}), \\ -1 & (a \text{ が平方非剰余のとき}) \end{cases}$$

と定める. さらに $p|a$ の場合は $\left(\frac{a}{p}\right) = 0$ と定める. この記号

$$\left(\frac{a}{p}\right)$$

を 平方剰余記号 と呼ぶ. もちろん $a \equiv b \pmod{p}$ ならば $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ である.

定理 14.2. p を奇素数, a を p と素な整数とする. このとき $a^{\frac{p-1}{2}}$ は法 p で 1 または -1 と合同であり, それぞれの場合に応じて a は法 p の平方剰余あるいは平方非剰余である. 即ち,

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

証明 $b = a^{\frac{p-1}{2}}$ とおくと, Fermat の小定理より $b^2 = a^{p-1} \equiv 1 \pmod{p}$ なので,

$$(b-1)(b+1) \equiv 0 \pmod{p}$$

となり, 前半が示される. 法 p の原始根を g として, $a \equiv g^t \pmod{p}$ ($0 \leq t \leq p-2$) とせよ. $g^{\frac{p-1}{2}t} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ は $\frac{p-1}{2}t \equiv 0 \pmod{p-1}$ と同値で, これは $2|t$ を意味するから結論を得る. \square

練習 14.3. p を奇素数とする. $\gcd(a, p) = 1$ のとき, 整数 x についての方程式 $ax^2 + bx + c \equiv 0 \pmod{p}$ は $\left(\frac{b^2 - 4ac}{p}\right) = 1, 0, -1$ に従つて, それぞれ 2 つの解をもつ, 唯 1 つの解をもつ, 解をもたない, となる. これを示せ.

15 平方剰余の相互法則

自然数 n について剰余類分解 $\mathbb{Z}/n\mathbb{Z}$ の代表系を法 n の 剰余系 といふ. $p = 2n + 1$ を奇素数とする. n 個の整数の集合 $\{r_1, r_2, \dots, r_n\}$ は, これと $\{0, -r_1, -r_2, \dots, -r_n\}$ とを合はせた集合が丁度, 法 p の剰余系になるとき, 法 p の Gauss 代表系 であるといはれる.

補題 15.1. (Gauss の補題) $p = 2n + 1$ を奇素数とし, $\{r_1, r_2, \dots, r_n\}$ を法 p の Gauss 代表系とせよ. a を $\gcd(a, p) = 1$ なる整数とせよ. 定義より, 各 $i = 1, \dots, n$ について

$$(15.2) \quad ar_i \equiv e_i r_j \pmod{p}$$

となる $e_j \in \{1, -1\}$ と r_j が一意的に存在する. このとき,

$$\left(\frac{a}{p}\right) = \prod_{i=1}^n e_i.$$

特に, $a, 2a, \dots, na$ について, これらを p で割った余りが n よりも大きいものの個数を N とすれば

$$\left(\frac{a}{p}\right) = (-1)^N.$$

証明 $i = 1$ から n に渡つて (15.1) の積を取れば

$$a^n \prod_{i=1}^n r_i \equiv \prod_{i=1}^n e_i \prod_{i=1}^n r_i \pmod{p}.$$

ここで r_i はどれも p と素であるから,

$$a^n \equiv \prod_{i=1}^n e_i \pmod{p}.$$

定理 14.2 より結論を得る. □

最終目標の定理 16.14 までは, 以下の平方剰余の相互法則 (定理 15.3 と定理 15.4) のうち, 定理 15.3 (2) しか使はないので, 定理 15.4 を読み飛ばしても構はない.

定理 15.3. p が素数で a と b が $\gcd(ab, p) = 1$ なる整数のとき, 次が成り立つ.

$$(1) \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right),$$

$$(2) \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad (\text{第 1 補充法則}),$$

$$(3) \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad (\text{第 2 補充法則}).$$

証明 (1) 補題 15.1 で a, b についての e_i をそれぞれ e_{1i}, e_{2i} と書けば, ab についての e_i は $e_{1i}e_{2i}$ になるから,

$$\left(\frac{a}{p}\right) = \prod_{i=1}^n e_{1i}, \quad \left(\frac{b}{p}\right) = \prod_{i=1}^n e_{2i}, \quad \left(\frac{ab}{p}\right) = \prod_{i=1}^n e_{1i}e_{2i}$$

となつて所望の式が成り立つ.

(2) Gauss 代表系を $\{1, 2, \dots, \frac{p-1}{2}\}$ にとるとき, 補題 15.1 の e_1, \dots, e_n が全て -1 になるので, 主張は明らか.

(3) 同じく Gauss 代表系を $\{1, 2, \dots, \frac{p-1}{2}\}$ にとるとき, これらの 2 倍は

$$2, 4, 6, \dots, p-1$$

である. この中で補題 15.1 にいふ $\{e_i\}$ が負になるのは $\frac{p+1}{2}$ 以上のもので, その個数 N は 1 以上 $\frac{p-1}{2}$ 以下の奇数の個数に等しい. N の偶奇はそれらの和 $1+3+5+\dots$ の偶奇と一致する. しかるに, $\frac{p-1}{2}$ の偶奇に関はらず, この和の偶奇は

$$1+2+3+4+5+\dots+\frac{p-1}{2} = \frac{1}{2} \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} = \frac{p^2-1}{8}$$

と一致する:

$$N \equiv \frac{p^2-1}{8} \pmod{2}.$$

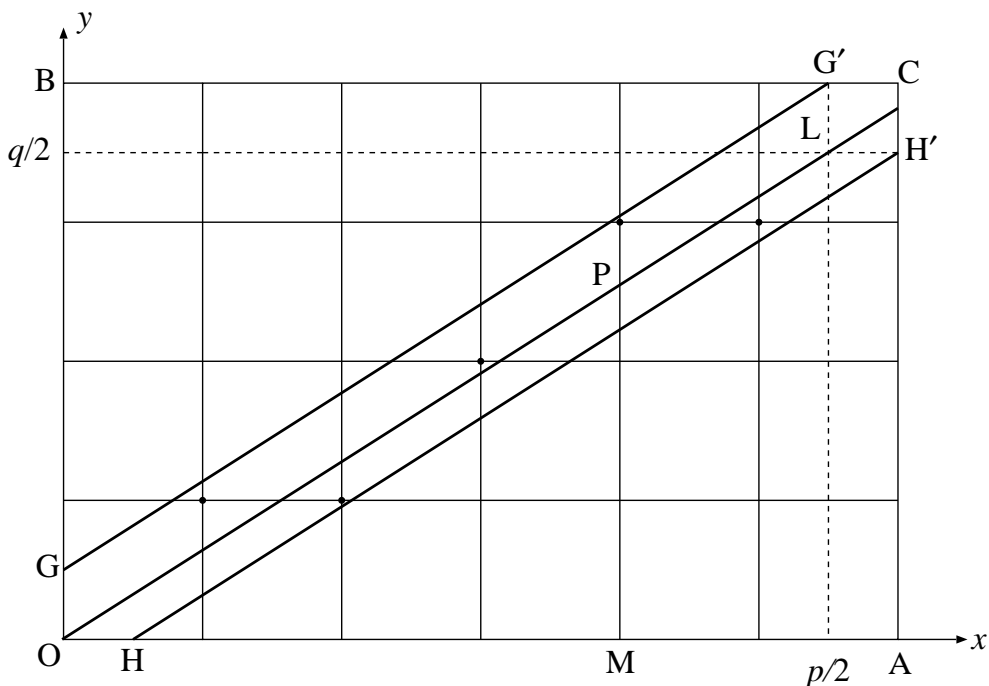
補題 15.1 により, これで (3) が示された. □

定理 15.4. (平方剰余の相互法則) p と q を相異なる奇素数とせよ. このとき

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

が成り立つ.

証明 ([高木], pp.78-79 より引用.) 図は xy 座標平面を表してゐる. x 座標と y 座標が共に整数である点を格子点といふ. x 軸上に $OA = (p+1)/2$ を, また y 軸上に $OB = (q+1)/2$ を取つて長方形 $OACB$ の内部の格子点を考察する. いま, $L(p/2, q/2)$ を取り, 原点 O と L を通る直線 $\frac{y}{x} = \frac{q}{p}$ を引く. さらに x 軸上の一般の点 $M(x, 0)$ に対し, $P(x, qx/p)$ を考へる.



$x = 1, 2, 3, \dots, (p-1)/2$ とするとき, qx を p で割った剰余が $p/2$ よりも大きいのは, qx/p の分数部分が $1/2$ よりも大きいときで, それは, P を通る縦線上で P から $1/2$ 以内の距離にある格子点が OL の上側にあるときに限る¹³. 故に $\left(\frac{q}{p}\right) = (-1)^n$ における n は OL とそれを y 軸の向きに $1/2$ だけ平行移動した GG' とに挟まれる平行四辺形 $OGG'L$ の内部にある格子点の数である.

同様に $\left(\frac{p}{q}\right) = (-1)^m$ における m は OL とそれを x 軸の向きに $1/2$ だけ平行移動した HH' とに挟まれる平行四辺形 $OHH'L$ の内部になる格子点の数である.

即ち $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m+n}$ における $m+n$ はこれら 2 つの平行四辺形の内部にある格子点の総数であるが, 図に示す様に格子点 $C((p+1)/2, (q+1)/2)$ を 1 頂点とする 1 辺が $1/2$ である小正方形 $CG'LH'$ を付け加えて 6 角形 $OGG'CH'H$ を作れば, その内部における格子点の数はやはり $m+n$ である.

さて OC の中点 $((p+1)/4, (q+1)/4)$ はこの 6 角形の対称の中心で, 格子点はこの点に関して 2 つずつ互ひに対称であることは作図によつて明白である. 故に $m+n$ が奇数であるか, 偶数であるかは中心 $(p+1)/4, (q+1)/4$ それ自身が格子点であるか, または格子点でないかによつて決定される.

故に $(p+1)/4, (q+1)/4$ がともに整数, 即ち p, q がともに $4j-1$ の形の素数であるときに限つて, $m+n$ は奇数, つまり

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$$

である. 即ち, 定理の主張は証明された.

あるいは次の様にも説明される. 3 角形 $GG'B, HH'A$ は同数の格子点を含むから, それを k とすれば, 長方形 $OACB$ の内部の格子点の総数は $m+n+2k$ である. しかるに長方形の内部には明らかに

$$\frac{p-1}{2} \cdot \frac{q-1}{2} \text{ 個}$$

の格子点があるから

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m+n} = (-1)^{m+n+2k} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

となる. □

例 15.5. ここまでで学んだ性質を使つて $\left(\frac{365}{1847}\right)$ を求めてみる.

$$\begin{aligned} \left(\frac{365}{1847}\right) &= \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right) = \left(\frac{1847}{5}\right)\left(\frac{1847}{73}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{73}\right)\left(\frac{11}{73}\right) = -\left(\frac{11}{73}\right) \\ &= -\left(\frac{73}{11}\right) = -\left(\frac{-4}{11}\right) = -\left(\frac{-1}{11}\right)\left(\frac{2^2}{11}\right) = -\left(\frac{-1}{11}\right) = +1 \end{aligned}$$

練習 15.6. $\left(\frac{311}{1321}\right)$ の値を求めよ.

¹³つまり, P から, P の直下の格子点までの距離が $\frac{1}{2}$ より大.

16 Gauss 整数

複素数体 \mathbb{C} の定義と四則演算については既知とする.

$z = x+yi \in \mathbb{C}$ ($x, y \in \mathbb{R}$) の 複素共役 とは, $\bar{z} = x-yi$ のことである.

写像 $z \mapsto \bar{z}$ で与えられる写像 $\mathbb{C} \rightarrow \mathbb{C}$ は \mathbb{C} の四則演算を保存する. つまり $z_1, z_2 \in \mathbb{C}$ のとき,

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \quad \overline{z_1 - z_2} = \bar{z}_1 - \bar{z}_2, \quad \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2, \quad \overline{\left(\frac{z_1}{z_2}\right)} = \frac{\bar{z}_1}{\bar{z}_2} \quad (z_2 \neq 0)$$

が成り立つ. 一般の体 K について, 四則演算を保存する写像 $K \rightarrow K$ を K の 自己同型 といふ. もちろん恒等写像も自己同型写像である.

複素数 $z = x+yi \in \mathbb{C}$ ($x, y \in \mathbb{R}$) に対して

$$Nz = N(z) = x^2 + y^2$$

と書いて, これを z の norm と呼ぶ. 通常 絶対値 $|z|$ は norm の平方根である:

$$|z| = \sqrt{Nz}.$$

練習 16.1. $z_1, z_2 \in \mathbb{Z}[i]$ について, 次の 2 つを証明せよ:

$$(16.2) \quad |z_1| < |z_2| \iff Nz_1 < Nz_2.$$

$$(16.3) \quad z_1 \mid z_2 \implies Nz_1 \mid Nz_2.$$

また (16.3) の逆は必ずしも成立しないことを反例を挙げて示せ.

これらの性質は以後よく使はれる. 例へば $N(1+i) = 2$ なので, $1+i$ を割る様な元は $\mathbb{Z}[i]$ は $\pm(1 \pm i)$ 以外には存在しないことがわかる. 実際, $\alpha = a+bi \mid 1+i$ ($a, b \in \mathbb{Z}$) ならば norm を取つて $a^2 + b^2 = N\alpha \leq 2$ なので $\alpha \in \{1, -1, i, -i, 1+i, 1-i, -1+i, -1-i\}$ である.

定義 16.4. 複素数体 \mathbb{C} の部分集合

$$\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$$

は \mathbb{C} の部分環である (確かめよ). これを Gauss 整数環 と呼ぶ. Gauss 整数環の元を Gauss 整数 といふ. さらに

$$\mathbb{Q}[i] = \{a+bi \mid a, b \in \mathbb{Q}\}$$

は体である (練習 6.5) が, これを Gauss 数体 と呼ぶ.

ここで 定義 8.3 や 定義 8.4 を思ひ出す. 約元, 倍元, 割り切る, 割り切れる, 素元, 既約元 などの用語.

定義 16.5. $\mathbb{Z}[i]$ の素元を Gauss 素数 と呼ぶ. いはゆる通常 \mathbb{Z} の素数をこれと区別して 有理素数 と呼ぶことがある.

例 16.6. あとで, 詳しく証明を付けるが $1 \pm i, 3, 1 \pm 2i, 2 \pm i, 7$ などは Gauss 素数である.

定義 16.7. 可換環 R において, 乗法の単位元 1 の約元を 単数 といふ. $\mathbb{Z}[i]$ においては, 単数は $1, -1, i, -i$ の 4 つだけである (確かめよ).

定義 16.8. 可換環 R の 2 つ元 a, b について, 一方が他方の単数倍であるとき, この 2 元は互いに 同伴 (あるいは 同伴数) であるといはれる.

例 16.9. $\mathbb{Z}[i]$ においては, $1 - i = (-i)(1 + i)$, $2 - 3i = i(-3 - 2i)$ なので $1 - i$ と $1 + i$, $2 - 3i$ と $-3 - 2i$ は, それぞれ, 互いに同伴である.

定義 16.10. $\alpha = x + yi$ の同伴数は, これ自身を含めて

$$i\alpha = -y + ix, \quad -\alpha = -x - yi, \quad -i\alpha = y - ix$$

の 4 つである. この中に, 実部が正で虚部が負でないものが唯 1 つ存在する. それを 正規化された Gauss 数 と呼ぶ.

補題 16.11. $a, b \in \mathbb{Z}[i]$, $b \neq 0$ とせよ. このとき, ある $q \in \mathbb{Z}[i]$ が存在して

$$N(a - bq) \leq \frac{1}{2} N(b)$$

となる.

証明 集合 $b\mathbb{Z}[i]$ は複素数平面上で 0 と b を結ぶ線分を 1 辺とする 1 つの正方形を基準にして, 全複素数平面を埋め尽くしたときの無数の正方形の頂点の全体 (それは格子を形成するが) と一致する. この格子点のうち a に最も近い点を bq とすれば, 与式が成り立つ. \square

定理 16.12. $M \subset \mathbb{Z}[i]$ を Gauss 整数環 $\mathbb{Z}[i]$ の 1 つの ideal とする. このとき, ある $d \in \mathbb{Z}[i]$ によつて

$$M = d\mathbb{Z}[i]$$

と書かれる. しかも, この様な d はその同伴数を除けば一意的に定まる.

証明 $M - \{0\}$ のうち, 原点に一番近いもの (つまり norm が最小になる点) を d とせよ. 任意に $a \in M$ を取れ. 補題 16.11 により, $N(a - dq) \leq \frac{1}{2}N(d)$ となる $q \in \mathbb{Z}[i]$ が存在する. しかるに M は ideal だから $a - dq \in M$ なので, $a - dq = 0$ でない限り矛盾が生じる. つまり $a = dq \in M$ よつて $M \subset d\mathbb{Z}[i]$ を得る. 逆の包含関係 $M \supset d\mathbb{Z}[i]$ は明らかだから, 主張の前半が証明された. 後半は d と d' が伴に主張を満たせば $d' = ud$ ($u \in \mathbb{Z}[i]$) と $d = vd'$ ($v \in \mathbb{Z}[i]$) が成り立ち, $uv = 1$ となるので u も v も単数である. \square

この定理 16.12 により, Gauss 整数環においても公約数, 最大公約数, 最小公倍数が (同伴性を無視すれば) 定まる. 即ち, $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}[i]$ のとき,

$$M = \{ \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n \mid x_1, x_2, \dots, x_n \in \mathbb{Z}[i] \}$$

が $\mathbb{Z}[i]$ の ideal であることは容易にわかるので, $\delta\mathbb{Z}[i] = M$ となる $\delta \in \mathbb{Z}[i]$ が, 同伴なものを無視すれば, 唯 1 つに定まる. そこで

$$\gcd(\alpha_1, \alpha_2, \dots, \alpha_n) = \delta$$

と書いて, これを $\alpha_1, \alpha_2, \dots, \alpha_n$ の 最大公約数 と呼ぶ. さらに $\delta'\mathbb{Z}[i] \supset \delta\mathbb{Z}[i]$ のとき, δ' は $\alpha_1, \dots, \alpha_n$ の 公約数 と呼ばれる. $\alpha\beta/\gcd(\alpha, \beta)$ (と同伴な数) を α と β の 最小公倍数 と呼ぶ.

命題 16.13. $\mathbb{Z}[i]$ の既約元は素元である. 従つて Gauss 整数環においては, 素元と既約元の間概念は一致する.

証明 p を $\mathbb{Z}[i]$ の既約元とせよ. $p|ab$ ($a, b \in \mathbb{Z}[i]$) であるとする. $d = \gcd(p, a)$ とおく. d は p の約数であるから, d は単数か p と同伴かのいずれかである. d が単数ならば, $1 = ps + at$ と書ける. このとき $b = pbs + abt$ なので $p|b$ がわかる. もし d が p と同伴ならば, $p|a$ である. よつて p は素元である. 素元は常に既約元である (8.4 を参照) から後半の主張も正しい. \square

定理 16.14. (Gauss 整数環における素因数分解の一意分解性)

0 でないどんな Gauss 整数も, 1 つの単数といくつかの Gauss 素数の積に書かれる. しかも, その様な積に現れる Gauss 素数は, それら Gauss 素数の同伴であることを除けば, 現れる個数を込めて一意的である.

証明 16.13 に注意すれば, norm に関する帰納法で, 定理 8.1 の証明と同様に示される. \square

命題 16.15. p を奇素数とする. p は Gauss 素数であるか, またはある Gauss 素数 q の norm である. 後者の場合, $p = q\bar{q}$ であり, q と \bar{q} は同伴数ではなく, p は q または \bar{q} とこれらの同伴数のみを約数を持つ.

証明 p が Gauss 素数でないとしてよ. さすれば, $a + bi | p$ なる Gauss 素数 $a + bi \in \mathbb{Z}[i]$ が存在する. このとき $\gcd(a, b) = 1$. さらに複素共役を考へれば $a - bi | p$ でなくてはならない. しかるに $\gcd(a + bi, a - bi) | \gcd(2a, 2b) = 2$ であるが p が奇数なので, $\gcd(a + bi, a - bi) = 1$ である. よつて $a^2 + b^2 = (a + bi)(a - bi) | p$. ここで, もし $a^2 + b^2 = p$ でないとすると p が素数であることに反する. 従つて $a^2 + b^2 = p$ となる. この状況は主張の後半の記号で $q = a + bi$ であり, それも示されてゐる. \square

定理 16.16. p を奇素数とする. このとき

$p \equiv 1 \pmod{4}$ ならば p は Gauss 素数の norm であり,
 $p \equiv 3 \pmod{4}$ ならば p は Gauss 素数である.

証明 定理 15.3 より, $p \equiv 1 \pmod{4}$ ならば, $x^2 \equiv -1 \pmod{p}$ が解 x を持つ. つまり $x^2 + 1 = py$ となる $y \in \mathbb{Z}$ がある. このとき, $p | (x + i)(x - i)$ なので, もし p が Gauss 素数なら $p | (x + i)$ または $p | (x - i)$ である. しかし, 共役を考へれば, この 2 つは共に成り立つ. しかるに p は奇数なので $p | x$ でなければならぬ. これは矛盾である. よつて p は Gauss 素数ではない. 命題 16.15 により, それは Gauss 素数の norm である. 逆に $p = a^2 + b^2$ と書けるとき a, b を法 4 で観察することで, $p \equiv 1 \pmod{4}$ であることがわかる. 転換法により残りの方も示される. \square

以上をまとめると次の様になる.

系 16.17. Gauss 素数は以下で尽くされる :

$$\{1+i, 1-i, -1+i, -1-i\} \cup \{p, -p, ip, -ip \mid p \text{ は } p \equiv 3 \pmod{4} \text{ なる素数}\} \\ \cup \{a+bi \mid a, b \in \mathbb{Z} \text{ で } p = a^2 + b^2 \text{ は } \equiv 1 \pmod{4} \text{ なる素数}\}.$$

例 16.18. Gauss 整数環における素因数分解の例を与える :

$17190 + 43920i$ の素因数分解を得るために, まず互除法で

$$\gcd(17190, 43920) = 2 \cdot 3^2 \cdot 5$$

を得ておく. これにより有理整数の因数を見出すことができ

$$17190 + 43920i = 2 \cdot 3^2 \cdot 5 \cdot (191 + 488i)$$

と分解される. 次に $191 + 488i$ の分解をする. まず, この norm を素因数分解すると

$$N(191 + 488i) = (191 + 488i)(191 - 488i) = 274625 = 5^3 \cdot 13^3$$

となるから $191 + 488i$ は 5 と 13 を割る Gauss 素数を因数に持つことがわかる. そこで $5 = (1 + 2i)(1 - 2i)$ の素因数 $1 + 2i$ と $2 + 3i$ による除法を試ると

$$(191 + 488i)/(1 + 2i) = \frac{1167}{5} + \frac{106}{5}i, \quad (191 + 488i)/(1 - 2i) = -157 + 174i$$

から $1 - 2i$ のみを因子にもつことがわかる. さらに除法を続ければ

$$(191 + 488i)/(1 - 2i)^3 = -9 - 46i$$

がわかり, これ以上は $1 - 2i$ では割れない. そこで, 今度は $13 = (2 + 3i)(2 - 3i)$ の素因数 $2 + 3i$ による除法を試ることにより,

$$(-9 - 46i)/(2 + 3i)^3 = i$$

がわかる. 以上をまとめて, 素因数分解は次の通り :

$$\begin{aligned} 17190 + 43920i &= 2 \cdot 3^2 \cdot 5 \cdot (191 + 488i) = 2 \cdot 3^2 \cdot 5(1 - 2i)^3(-9 - 46i) \\ &= 2 \cdot 3^2 \cdot 5(1 - 2i)^3(2 + 3i)^3i \\ &= -i(1 + i)^2 \cdot 3^2 \cdot (1 + 2i)(1 - 2i)(1 - 2i)^3(2 + 3i)^3i \\ &= (1 + i)^2 \cdot 3^2 \cdot (1 + 2i)(1 - 2i)^4(2 + 3i)^3. \end{aligned}$$

練習 16.19. Gauss 整数 $270578 + 7475930i$ を Gauss 素数の積に分解せよ. できるだけ, 計算機や computer を使わないでやってみて欲しい.

これで, この講義の 1 つの目標であった Gauss 整数環 $\mathbb{Z}[i]$ の基本事項の解説が終った.

演習問題

16.20. 整数 n が 2 つの互いに素な平方数の和に書けるとき, n のすべての約数もさうであることを示せ.

16.21. 自然数を n^2a (但し a は平方因数を持たない) と表したとき, a のすべての奇数の素因数 p が $p \equiv 1 \pmod{4}$ であるとき, かつそのときに限り, n^2a は 2 つの整数の平方の和として表せる. これを証明せよ. また a が r 個の素数の積であるとき, a を 2 整数の平方和で表す仕方は何通りか.

この後の節では, ここまでの話の補足的な話題を述べる.

17 剰余類

第 12 節で述べた左剰余類と同様に右剰余類といふものを考えることができる。

定義 17.1. 群 G と $H < G$ について Ha ($a \in G$) の形の部分集合を G における H の 右剰余類 とよび, 特に $H1 = 1H = H$ なので H 自身も 1 つの右剰余類である。

練習 17.2. 次のことを証明せよ。

$$(17.3) \quad Ha = Hb \iff ab^{-1} \in H.$$

(17.3) が満たされておるとき, a と b は 右合同 であるといふ。それは, a と b が同じ右剰余類に属することに他ならない。

群 G とその部分群 H に対して, G を H に関する右剰余類の和集合に表すこと, つまり

$$G = \bigcup_{\lambda \in \Lambda} Ha_\lambda$$

の形に書くことを G の H による 右分解 といふ。また, 集合

$$\{Ha_\lambda \mid \lambda \in \Lambda\}$$

を $H \backslash G$ と書く。

例 17.4. G が Abel 群でないとき, 一般に $H < G$ について, H に関する左分解と右分解は一致しない。 しかし, Abel でない場合でも右分解と左分解が一致することがある。

例へば例 3.3 で説明した S_4 の Klein の 4 元群と呼ばれる部分群

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

の左剰余類と右剰余類を書いてみる。左剰余類は

$$\begin{aligned} (12)V &= \{(12), (12)(12)(34), (12)(13)(24), (12)(14)(23)\} \\ &= \{(12), (34), (1324), (1423)\}, \end{aligned}$$

$$\begin{aligned} (13)V &= \{(13), (13)(12)(34), (13)(13)(24), (13)(14)(23)\} \\ &= \{(13), (1234), (24), (1432)\}, \end{aligned}$$

$$\begin{aligned} (14)V &= \{(14), (14)(12)(34), (14)(13)(24), (14)(14)(23)\} \\ &= \{(14), (1243), (1342), (23)\} = (23)V, \end{aligned}$$

$$\begin{aligned} (123)V &= \{(123), (123)(12)(34), (123)(13)(24), (123)(14)(23)\} \\ &= \{(123), (134), (243), (142)\}, \end{aligned}$$

$$\begin{aligned} (132)V &= \{(132), (132)(12)(34), (132)(13)(24), (132)(14)(23)\} \\ &= \{(132), (234), (124), (143)\}, \end{aligned}$$

右剰余類は

$$\begin{aligned} V(12) &= \{ (12), (12)(34)(12), (13)(24)(12), (14)(23)(12) \} \\ &= \{ (12), (34), (1423), (1324) \}, \\ V(13) &= \{ (13), (12)(34)(13), (13)(24)(13), (14)(23)(13) \} \\ &= \{ (13), (1432), (24), (1234) \}, \\ V(14) &= \{ (14), (12)(34)(14), (13)(24)(14), (14)(23)(14) \} \\ &= \{ (14), (1342), (1243), (23) \} = V(23), \\ V(123) &= \{ (123), (12)(34)(123), (13)(24)(123), (14)(23)(123) \} \\ &= \{ (123), (243), (142), (134) \}, \\ V(132) &= \{ (132), (12)(34)(132), (13)(24)(132), (14)(23)(132) \} \\ &= \{ (132), (143), (234), (124) \} \end{aligned}$$

となり, $(12)V = V(12)$, $(13)V = V(13)$ 等, 常に左剰余類と右剰余類が一致してゐる.

練習 17.5. 例 3.3 の様に S_3 を S_4 の部分群と思ふとき, S_4 の S_3 による右分解を例 18.4 の様に具体的に記せ. S_4 の S_3 による左分解と右分解は一致するか答へよ.

18 正規部分群と剰余類群

定義 18.1. 群 G と $H < G$ について, G の H による左分解と右分解が一致するとき, H は G の 正規部分群 と呼ばれ, $H \triangleleft G$ と書かれる.

G を群とし, $H \triangleleft G$ とする. このとき, 右分解と左分解が一致するから $xH = Hx$ ($x \in G$) であるが, 剰余類の全体 $G/H = H \backslash G = \{x_\lambda H \mid \lambda \in \Lambda\}$ を考へる. このとき,

命題 18.2. 等式 $(xH)(yH) = xyH$ が代表元 $x, y \in G$ の選び方に依らず意味を持つ.

証明 以下 h_j は H の元を表すものとする. $x' = xh_1 \in xH$, $y' = yh_2 \in yH$ のとき, $h_1y \in Hy = yH$ より $h_1y = yh_4$ と書けるから, $x'y' = (xh_1)(yh_2) = x(h_1y)h_2 = x(yh_4)h_2 \in xyH$ である. $(xH)(yH) = (x(Hy))H = (x(yH))H = ((xy)H)H = (xy)(HH) = (xy)H$ と考へてもよい. □

系 18.3. $H \triangleleft G$ のとき G/H は演算 $(xH)(yH) = xyH$ について群になる. 単位元は $H(=1H)$ で xH の逆元は $x^{-1}H$ である.

注意 18.4. 例に挙げた剰余類 $S_4/V (= V \backslash S_4)$ の代表元をみれば, これが S_3 と“同じ振舞ひ”をする群であることがわかる. この様な状況のとき, 群 S_4/V は S_3 と 同型 であるといはれる.

19 中国の剰余定理

ここでは 中国の剰余定理 (Chinese Remeinder Theorem) と呼ばれる重要な定理を述べる.

定理 19.1. (中国の剰余定理) g 個の整数 m_1, m_2, \dots, m_g は, どの 2 つも互いに素であるとする. つまり, すべての i, j ($i \neq j$) について $\gcd(m_i, m_j) = 1$ とする. さらに g 個の整数 b_1, b_2, \dots, b_g が与へられたとする. このとき, 方程式

$$x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \dots, x \equiv b_g \pmod{m_g}$$

を満たす整数 x が存在する. しかも x はすべての m_j の積 $m_1 m_2 \dots m_g$ を法として一意的に定まる.

証明 $M = m_1 m_2 \dots m_g$ とおき, 各 j について $n_j = M/m_j$ とおく. 仮定より $\gcd(m_j, n_j) = 1$ であるから, 定理 7.6 より $t_j m_j + s_j n_j = 1$ となる t_j, s_j が存在する. このとき, $e_j = s_j n_j$ とおくと

$$e_j \equiv \begin{cases} 1 \pmod{m_j} \\ 0 \pmod{m_i} \text{ if } i \neq j \end{cases}$$

が成り立つ. それゆゑ

$$x = \sum_{i=1}^g b_i e_i$$

とおけば所望の解がひとつ得られる.

一意性: x' が他の解であれば $m_j | (x - x')$ がすべての j について成り立つから,

仮定 $\gcd(m_i, m_j) = 1$ により, $M | (x - x')$, つまり $x \equiv x' \pmod{M}$ となることがわかる. \square

練習 19.2. 次の 3 つの合同式を同時に満たす整数 x を定理 19.1 の証明に沿つて求めよ.

$$x \equiv 2 \pmod{5}, x \equiv 3 \pmod{7}, x \equiv 1 \pmod{11}.$$

References

[高木] 高木貞治: 初等整数論講義, 共立出版

[IR] Ireland, K. and Rosen, M.: A Classical Introduction to Modern Number Theory, Graduate Text in Mathematics 84, Springer-Verlag

[W] Weil, A.: Number Theory for Beginners, Springer-Verlag, 1979
(邦訳 “初学者のための整数論” (訳 片山他) ちくま学芸文庫)

[永尾] 永尾汎 著: 代数学 (新数学講座 4), 1983, 朝倉書店

[彌永他] 彌永昌吉, 有馬哲, 浅茅陽 著: 詳解 代数入門, 1990, 東京図書