前期のまとめと復習問題

● 整数の性質

前期の前半は高校の「数学 A」で扱われている整数の性質について復習した．教科書には次の用語が定義されて説明されているので，まずはそれらの意味を教科書，あるいはインターネット検索を用いていて確認しておこう．

倍数，公倍数，最小公倍数，約数，公約数，最大公約数，互いに素，素数，因数，素因数分解，除法，商，余り，割り切れる，...

とくに最大公約数のについて次の性質は重要である．

定理 1 (最大公約数の性質)**.** 正の整数 a, b の最大公約数を d とすると，

$$ax + by = d$$

をみたす整数 x, y が存在する．とくに p が素数で， a が p で割りきれない整数とすると， a と p は互いに素なので $ax + py = 1$ をみたす整数 x, y が存在する．

2 つの正の整数の最大公約数を求めるには「ユークリッド互除法」と呼ばれる方法を用いることができる．また，ユークリッド互除法を拡張して定理 1 の a, b も計算することが出来る．これを Excel を使って計算することは

1 次の整数の組の最大公約数をもとめよ．

a) $(756, 1176)$　　b) $(2160, 2268)$　　c) $(1368, 2952)$

【Exel を使える環境にあれば， https://kuwata.r.chuo-u.ac.jp/Current/Seminar_I_Thr.html にある，拡張ユークリッド互除法の Excel ファイルを用い， $ax + by = d$ を満たす x, y も求めてみよ．】

● 有限体 $\mathbf{F}_p = GF(p)$

つぎに，正の整数 n が 1 つ与えられたとき，すべての整数を n で割った余りによって分類することを考える．

定義 1. 2 つの正の整数 a, b が n を法として合同であるとは， $a - b$ が n の倍数であることである．言い換えると，ある整数 k を用いて $a - b = nk$ と表せることである．このとき， $a \equiv b \pmod{n}$ と表す．

整数 a を n で割ったときの商を q，余りを r とすると， $a = qn + r$ $(0 \leqq r \leqq n - 1)$ と表せる．これは $a \equiv r \pmod{n}$ を意味し，すべての整数は $0, 1, 2, \ldots, n - 1$ のいずれかと n を法として合同であることがわかる．いま，n を法として k と合同である整数全体を $\overline{k}$ で表すことにすると，すべての整数は， $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ のいずれかに属し，整数全体は n この類に分類される．これらの間に加法・減法・乗法が自然に定義され，結合法則，分配法則，交換法則が成り立つことがわかるが，除法については必ずしも定義されるとは限らない．例えば， $n = 6$ としたとき， $a = 2$ に対して $ak \equiv 1 \pmod{6}$ を満たす整数 k は存在しないので， 2 は逆数をもたず， 2 による割り算は行えない．

しかし， n として素数 p をとると，定理 1 により， $\bar{0}$ 以外はすべて逆数をもち， $\bar{0}$ 以外による割り算が可能となる． p を素数としたとき， p を法とする余りで分類された類 $\bar{0}, \bar{1}, \ldots, \overline{p-1}$ からなる集合を $\{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ を $\mathbf{F}_p$ または $GF(p)$ と表す．これは四則演算について閉じた「体」と呼ばれる数の体系となり， p-元体と呼ばれる．

2 a) 7-元体 $\mathbf{F}_7 = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{6}\}$ の乗法の表を作り，その表を利用して $\bar{2}, \bar{3}, \ldots, \bar{6}$ の逆数をそれぞれ求めよ．すなわち，$a = 2, 3, \ldots, 6$ それぞれについて $ak \equiv 1 \pmod 7$ を満たす整数 k を求めよ．

b) $\bar{3}^2, \bar{3}^3, \ldots,$ を計算し，$\mathbf{F}_7$ の元（要素）は $\bar{0}$ 以外はすべて $\bar{3}^k$ （k は自然数）の形に書けることを示せ．

定理 2. 有限体 $\mathbf{F}_p$ には，原始元 *(primitive element)* と呼ばれる元 $\bar{a}$ があり，$\bar{0}$ 以外の $\mathbf{F}_p$ のすべての元は整数 k によって $\bar{a}^k$ と表すことができる．

$\mathbf{F}_p$ に対し，原始元は複数存在する．しかし，どの元が原始元になるかを簡単に求める公式はなく，それぞれの素数 p について個別に探していくほかない．

3 $\mathbf{F}_{11}, \mathbf{F}_{13}$ の原始元をそれぞれひとつ求めよ．

• 有限体 $\mathbf{F}_{2^n} = GF(2^n)$

整数 a を合成数 n で割ったときの余り全体は必ずしも四則演算について閉じていない．たとえば，$n = 4$ のとき，$2k \equiv 1 \pmod 4$ となる整数 k は存在しない．すなわち，$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ は四則演算について閉じた数の体系にはならない．しかしながら，4 つの元からなる数の体系は存在し，実数から複素数を作るのと同じ方法で作られる．

4 【復習】任意の複素数 z は実数 a, b と虚数単位 i を用いて $z = a + bi$ と表されるのであった．2 つの複素数の演算は $a + bi$ を多項式と思って計算し，i^2 が現れるたびに -1 に置き換えて得られる．また，$a + bi$ の逆数 $\dfrac{1}{a + bi}$ は，$a + bi$ の共役複素数 $a - bi$ を用いて分母を有理化し，$a' + b'i$ の形に表すことが出来る．

a) 複素数 $1 + i$ の逆数をもとめよ．

b) 複素数 $z = \dfrac{1 + i}{\sqrt{2}}$ について，z^k （$k = 1, 2, 3, \ldots$）を求めよ．

$\mathbf{F}_2$ は 2 を法として 0 に合同になる類 $\bar{0}$ （偶数全体）と 0 に合同になる類 $\bar{1}$ （奇数全体）の 2 つの類からなる．以後，$\bar{0}, \bar{1}$ を単に $0, 1$ と表すことにする．$\mathbf{F}_2 = \{0, 1\}$ の四則演算は $1 + 1 = 0$ となることを除いてはすべて普通の計算のままである．

5 $\mathbf{F}_2 = \{0, 1\}$ を係数とする多項式で，それよりも次数の低い多項式の積に因数分解できない多項式を $\mathbf{F}_2$ 上の既約多項式という．$\mathbf{F}_2$ 係数の 5 次以下の既約多項式をすべて求めよ．［ヒント：例えば $\mathbf{F}_2$ 係数の 3 次式は $x^3 + a_2x^2 + a_1x + a_0$ (a_0, a_1, a_2 は 0 または 1) と書けるので，全部で 8 個ある．このうち 1 次式と 2 次式の積になるものすべてを除いた残りが既約多項式である．］

6 $\mathbf{F}_{16}$ は通常 $\beta^4 + \beta + 1 = 0$ をみたす元 β を用いて，$\mathbf{F}_{16} = \{a\beta^3 + b\beta^2 + c\beta + d \mid a, b, c, d \in \mathbf{F}_2\}$ の形に表される．$\mathbf{F}_{16}$ の 0 以外のすべての元を β^k ($0 \leqq k \leqq 14$) の形に表せ．［復習］

7 0 以外の元 a に対し，$a^m = 1$ となる最小の正整数 m を a の位数という．

a) $\mathbf{F}_8$ の 0 以外の元は $\alpha^3 + \alpha + 1 = 0$ をみたす元 α を用いて，$\{\alpha^k \mid 0 \leqq k \leqq 6\}$ と表される．$\mathbf{F}_8$ の 0 と 1 以外の元の位数はすべて 7 であることを示せ．

b) $\mathbf{F}_{16}$ の 0 以外のすべての元 β^k ($0 \leqq k \leqq 14$) について，その位数を求めよ．

8 a) $x^7 - 1$ を $\mathbf{F}_2$ 上で因数分解せよ．

b) $x^7 - 1$ は $\mathbf{F}_8$ 上では $x^7 - 1 = (x - 1)(x - \alpha)(x - \alpha^2) \cdots (x - \alpha^6)$ と因数分解できることを示せ．
［ヒント：因数定理を用いるとよい］

c) a) で求めた $x^7 - 1$ の $\mathbf{F}_2$ 上での各因数を $\mathbf{F}_8$ 上で $(x - \alpha^k) \cdots (x - \alpha^l)$ の形に因数分解せよ．

担当： 鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)