

問題 10-1

$p=17, 23, 41$ について $\mathbb{F}_p^\times = \langle a \rangle$ をみたす $a \in \mathbb{F}_p^\times$ を求めよ, \square

解答例

コンピュータを使ってもよいことにして, <https://www.wolframalpha.com/> を使ってみた.

まずは答えから:

$$\mathbb{F}_{17}^\times = \langle 3 \rangle, \quad \mathbb{F}_{23}^\times = \langle 5 \rangle, \quad \mathbb{F}_{41}^\times = \langle 6 \rangle.$$

17, 23 では,
手で計算しても
そう手間は増えない
41 はちょっと大変.

2^k mod 17 for k=1 to 16

Input

Table[2^k mod 17, {k, 1, 16}]

Result

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2^k mod 17	2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1

↓ 上のリストに3がないので3を確認.

← 2^k mod 17 の計算

$$\mathbb{F}_{17}^\times \not\cong \langle 2 \rangle = \{2, 4, 8, 16, 15, 13, 9, 1\}$$

↑
8個

元の個数は16個

3^k mod 17 for k=1 to 16

Input

Table[3^k mod 17, {k, 1, 16}]

Result

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^k mod 17	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

← 3^k mod 17 の計算

$$\mathbb{F}_{17}^\times = \langle 3 \rangle$$

以下より, $\mathbb{F}_{23}^{\times} = \langle 5 \rangle$

$2^k \bmod 23$ for $k=1$ to 22

Input

Table[$2^k \bmod 23$, { k , 1, 22}]

Result

{2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1}

$$2^{11} \bmod 23 = 1$$

2, 3, 4 を省いて ↓ 5 を確認

$5^k \bmod 23$ for $k=1$ to 22

Input

Table[$5^k \bmod 23$, { k , 1, 22}]

Result

{5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14, 1}

以下より, $\mathbb{F}_{41}^{\times} = \langle 6 \rangle$

$2^k \bmod 41$ for $k=1$ to 40

Input

Table[$2^k \bmod 41$, { k , 1, 40}]

Result

{2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1, 2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1}

$$2^{20} \bmod 41 = 1$$

$3^k \bmod 41$ for $k=1$ to 40

Input

Table[$3^k \bmod 41$, { k , 1, 40}]

Result

{3, 9, 27, 40, 38, 32, 14, 1, 3, 9, 27, 40, 38, 32, 14, 1, 3, 9, 27, 40, 38, 32, 14, 1, 3, 9, 27, 40, 38, 32, 14, 1}

$$3^8 \bmod 41 = 1$$

$6^k \bmod 41$ for $k=1$ to 40

Input

Table[$6^k \bmod 41$, { k , 1, 40}]

Result

{6, 36, 11, 25, 27, 39, 29, 10, 19, 32, 28, 4, 24, 21, 3, 18, 26, 33, 34, 40, 35, 5, 30, 16, 14, 2, 12, 31, 22, 9, 13, 37, 17, 20, 38, 23, 15, 8, 7, 1}

おまけ $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1) = \{0, 1, \omega, 1+\omega\}$

$$\omega^2 + \omega + 1 = 0, \text{ このとき,}$$

$$\mathbb{F}_4^{\times} = \langle \omega \rangle = \{\omega, 1+\omega, 1\}$$

$$\omega + \omega^2 = \omega + 1 + \omega = 1 \uparrow$$

$$\omega^2 = 1 + \omega$$

問題 10-2 K は正標数 p の体で $a, b \in K$ であるとし,

$x^p - a$ と $x^p - x - b$ は K 上既約であると仮定し,

L, M をそれぞれの K 上での最小分解体であるとする.

L と M が体 K 上で同型になることはあるか? \square

解答例 $f(x) = x^p - a$, $g(x) = x^p - x - b$ とおく. このとき,

$$f'(x) = \underbrace{p}_{=0 \text{ (正標数 } p)} x^{p-1} = 0, \quad g'(x) = \underbrace{px^{p-1}}_{\text{左と同様に } =0} - 1 = -1 \neq 0.$$

これより, $f(x)$ は重根を持ち, $g(x)$ は重根を持たない. \leftarrow

すなわち, $f(x)$ は非分離的であり, $g(x)$ は分離的である.

したがって, $f(x)$ の K 上での最小分解体は K 上の非分離拡大になり,

$g(x)$ の K 上での最小分解体は K 上の分離拡大になる.

ゆえに L と M が K 上で同型になることはない, \square

一般に多項式 $h(x) \in K[x]$
が重根を持つことと,
 $h(x)$ と $h'(x)$ が共通根を
持つことは同値である.

問題 10-3 有限体の有限次拡大が単拡大になることを示せ、 \square

解答例 有限体 K の n 次の有限次拡大 L は K 上のベクトル空間として K^n に同型なので有限集合になる。

ゆえに、 L は有限体になる。

有限体の乗法群は巡回群になるので、ある $\alpha \in L$ が存在して $L^\times = \langle \alpha \rangle$ 。

これより、 $L = K(\alpha)$ となることがわかる、 \square

ポイント (前回、非常に詳しく説明した。)

注意 一般に体の乗法群の有限部分群は巡回群になる、

この証明法はたくさんある:

- 有限 (生成) Abel 群の基本定理 (大道具) を使う、使えば易しい、
- 初等的な証明、色々あって面白いが少しテクニカルになる、 \square

問題 10-4 k は正標数 p の体であるとし, $L = k(s, t)$, $K = k(s^p, t^p)$ とおく,

このとき, 拡大 L/K について, $[L:K] = p^2$ で L が K の単拡大にならないことを示せ.

ここで, $k(s, t)$ は体 K 上の 2 変数有理函数体である. (cf. 問題 5-3) \square

正標数では有限次拡大が単拡大にならない場合がある.

解答例 ① $[L:K] = p^2$ を示そう.

$M = k(s, t^p)$ とおく. $L = M(t)$, $M = K(s)$ である.

$f(x) \in M[x]$ を $f(x) = x^p - t^p$ とおく,

M を t^p を素元に持つ UFD $k(s)[t^p]$ の商体とみなして Eisenstein の判定法を使うと,
 $t^p \nmid 1$, $t^p \mid 0$, ..., $t^p \mid 0$, $t^p \mid -t^p$, $(t^p)^2 \nmid -t^p$ より, $f(x)$ は M 上既約である.

$f(x)$ は t の M 上での最小多項式であるので, $[L:M] = [M(t):M] = \deg f = p$.

$g(x) \in K[x]$ を $g(x) = x^p - s^p$ とおく,

K を s^p を素元に持つ UFD $k(t^p)[s^p]$ の商体とみなして Eisenstein の判定法を使うと,
 $s^p \nmid 1$, $s^p \mid 0$, ..., $s^p \mid 0$, $s^p \mid -s^p$, $(s^p)^2 \nmid -s^p$ より, $g(x)$ は K 上既約である.

$g(x)$ は s の K 上での最小多項式であるので, $[M:K] = [K(s), K] = \deg g = p$.

したがって, $[L:K] = [L:M][M:K] = p^2$.

□ 2 任意の $\alpha \in L$ について $\alpha^p \in K$ を示そう. $\leftarrow (L^p \subset K)$

$$L = k(s, t) \text{ より, } \alpha = \frac{\sum a_{ij} s^i t^j}{\sum b_{ij} s^i t^j}, \quad a_{ij}, b_{ij} \in k \text{ と書ける.}$$

$$\text{標数 } p \text{ なので } \alpha^p = \frac{(\sum a_{ij} s^i t^j)^p}{(\sum b_{ij} s^i t^j)^p} = \frac{\sum a_{ij}^p (s^p)^i (t^p)^j}{\sum b_{ij}^p (s^p)^i (t^p)^j} \in k(s^p, t^p) = K.$$

$((\beta + \gamma)^p = \beta^p + \gamma^p) \uparrow$

□ 3 任意の $\alpha \in L$ について, $[K(\alpha) : K] \leq p$ を示そう.

上で $\alpha^p \in K$ となることを示したので α は $x^p - \underbrace{\alpha^p}_{\in K} \in K[x]$ の根になる
ゆえに, $[K(\alpha) : K] \leq \deg(x^p - \alpha^p) = p$.

□ 4 任意の $\alpha \in L$ について, $L \not\supsetneq K(\alpha)$ を示そう.

$[L : K] = p^2$ で $[K(\alpha) : K] \leq p$ なので $L \not\supsetneq K(\alpha)$.

これで L が K の単拡大にならないことが示された.

□