1　事前準備

定義 1 (体)**.** 体とは加法 $(+)$ と乗法 $(\times)$ が定義されていて以下の性質を満たす集合である. (以下では体を k, 体の要素を a, b, c と書く.)

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. 特別な要素 (零元) 0 があって, 任意の要素 a に対し $a + 0 = 0 + a = a$
4. a に対して特別な要素 (和に関する逆元) $-a$ があって, $a + (-a) = (-a) + a = 0$
5. $a \times b = b \times a$
6. $(a \times b) \times c = a \times (b \times c)$
7. 特別な要素 (単位元) 1 があって, 任意の要素 a に対し $a \times 1 = 1 \times a = a$
8. a に対して特別な要素 (積に関する逆元) $1/a$ があって, $a \times 1/a = 1/a \times a = 1$
9. $a \times (b + c) = a \times b + a \times c$
10. $(a + b) \times c = a \times c + b \times c$

※ $a + (-b)$ を $a - b$ と略記する.

※ $a \times b$ を ab と略記する.

※ $a \times b = b \times a$ と仮定しない流儀もある.

(分数が出てくる小学校 4 年生相当.)

定義 2 (環, 可換環)**.** 環とは体の公理から $5, 8$ を抜いたもの.
$(5 \div 3 = 1$ あまり 2 と答えないといけない小学校 3 年生相当.)

※ a に対し $1/a$ が存在するとは限らない.

環の公理にさらに

5. $a \times b = b \times a$

という公理を入れたものを可換環と呼ぶ.

例 1 (環, 可換環)**.** 整数環 $\mathbb{Z}$ は可換環.
多項式環 $k[x_1, x_2, \ldots, x_n]$ は可換環.

定義 3 (群, 可換群)**.** 群とは体の公理から 1, 2, 3, 4, 5, 9, 10 を抜いたもの. 体では + を「加算」と言っていたが, 群では「演算」と言うことが多い.

(掛け算を習ってないので小学校 1 年生相当.)

群の公理にさらに

5. $a \times b = b \times a$

という公理を入れたものを可換群と呼ぶ.

例 2 (群)**.** 縦線が n 本のあみだくじは群. (あみだくじの連結が演算となる.)

正整数は乗法を演算として群となる. ただし, 加法を演算とすると群とならない.

> **定理 1** (ラグランジュの定理)**.** G を有限群とし、H を G の部分群とする。このとき、H の位数は、G の位数を割り切る。
>
> **系 1.** G が有限群のとき、G の任意の元の位数は、G の位数を割り切る。

(http://ja.wikipedia.org/wiki/ラグランジュの定理 (群論) より引用)

今回は系の方を使う. そのために「群の位数」と「群の元 (要素) の位数」を定義する.

定義 4 (群の位数)**.** 群 G の位数とは, G に含まれる元の個数のこと.

定義 5 (群の要素の位数)**.** 群 G の要素 a に対し, $\underbrace{a + a + \cdots + a}_{n \text{ 個}} = 0$ となる最小の $n\ (> 0)$ を a の位数 $ord(a)$ と呼ぶ.

例 3. 加法を演算とする群 $\mathbb{F}_6$ の要素と位数は以下の通り.

要素	位数
0	1
1	6
2	3
3	2
4	3
5	6

2 問題

p を素数とする. p を法とする整数がなす環は p 個の要素を持つ体 $\mathbb{F}_p$ となる.

a. $\mathbb{F}_p - \{0\}$ が乗算について群を成す理由を説明せよ

Proof. $\mathbb{F}_p - \{0\}$ の乗算を群の演算, 1 を零元と見たとき, 群になることを示す. そのために定義で挙げた群の公理を満たすことを示す.

公理 6.

$\mathbb{F}_p$ では, p の倍数の差を無視する. つまり $a \in \mathbb{F}_p$ に関する計算は a を $a + np$ (n: 整数) に置き換えて計算して, p の倍数の差を無視する.

$$\begin{aligned}((a+lp)\times(b+mp))\times(c+np) &= (ab+n'p)\times(c+np)\\ &= abc + (n'c+abn+nn'p)p\\ &(n' = bl+am+lmp \text{ と置いた})\\ (a+lp)\times((b+mp)\times(c+np)) &= (a+lp)\times(bc+m'p)\\ &= abc + (bcl+am'+lm'p)p\\ &(m' = cm+bn+mnp \text{ と置いた})\end{aligned}$$

以上から公理 6 が示せた.

公理 7.

公理 6 と同様に計算する.

$$(a+np)\times 1 = 1\times(a+np) = a+np$$

以上から公理 7 が示せた.

公理 8.

ある整数 b, n が存在して $ab + np = 1$ ($0 < a < p$ と取る) となることを示せば良い.

b, n を $0 < b < p$ の範囲で動かしたとき $ab + np$ が取る最小の正整数を d と置く. ($b = 1, n = 0$ と置くと, この式が少なくとも 1 つの正整数を取ることが分かる.)

n の取り方によって $0 < d \leq p$ として良い. $d = p$ とすると, $ab = (1-n)p$ となるが a も b も p では割れないので矛盾. よってさらに範囲を狭めて $0 < d < p$ として良い.

p を d で割って $p = dq - r$ (q, r : 整数, $q \geq 0, 0 \leq r < d$) と置く.

$$\begin{aligned}ab + np &= d\\ (ab+np)q - r &= dq - r = p\\ a(bq) + (nq-1)p &= r\end{aligned}$$

$bq > 0$ なので d の最小性から r は正整数ではあり得ず $r = 0$. $p = dq$ かつ p は素数なので, $d = 1, p$.

$0 < d < p$ より $d = 1$. □

Proof. (公理 8 についての構成的な証明)

a と p にユークリッドの互除法を適用する.

$0 < a < p$ と取る.

$r_0 = p, r_1 = a$ と置く. $i \geq 2$ に対しては $r_{i-2} = q_{i-1}r_{i-1} + r_i$ $(0 \leq r_i < r_{i-1})$ と定める. r_i は整数で a と p は互いに素なので $r_0 > r_1 > r_2 > \cdots > r_n = 1$ といつかは 1 になる.

$$
\begin{aligned}
r_0 &= q_1 r_1 + r_2 \\
r_1 &= q_2 r_2 + r_3 \\
r_2 &= q_3 r_3 + r_4 \\
&\cdots \\
r_{n-3} &= q_{n-2} r_{n-2} + r_{n-1} \\
r_{n-2} &= q_{n-1} r_{n-1} + 1
\end{aligned}
$$

上の式を下に r_0 と r_1 を残すように代入していくと,

$$
\begin{aligned}
r_2 &= r_0 - q_1 r_1 \\
r_3 &= r_1 - q_2(r_0 - q_1 r_1) \\
&= -q_2 r_0 + (q_1 q_2 + 1) r_1 \\
&= s_3 r_0 + t_3 r_1 \\
&\text{(ここで } s_3 = -q_2, t_3 = q_1 q_2 + 1 \text{ と置いた)} \\
r_4 &= (r_0 - q_1 r_1) - q_3(s_2 r_0 + t_2 r_1) \\
&= (q_3 s_2 + 1) r_0 + (-q_1 - q_3 t_2) r_1 \\
&= s_4 r_0 + t_4 r_1 \\
&\text{(ここで } s_4 = q_3 s_2 + 1, t_4 = -q_1 - q_3 t_2 \text{と置いた)} \\
&\cdots \\
1 &= s_n r_0 + t_n r_1
\end{aligned}
$$

$r_0 = p, r_1 = a$ だったので $1 = s_n p + t_n a$. よって $\mathbb{F}_p$ で $t_n a = 1$ となり $1/a = t_n$ と求まる. □

例 4. $p = 31, a = 4$ で上記の計算をする.

最初にユークリッドの互除法を行う.

$$
\begin{aligned}
p &= 7 \cdot a + 3 \\
a &= 1 \cdot 3 + 1
\end{aligned}
$$

ここから a の逆元を求める.

$$
\begin{aligned}
1 &= a - 1 \cdot 3 \\
&= a - 1 \cdot (p - 7 \cdot a) \\
&= 8a - p
\end{aligned}
$$

確かに $8a = 8 \times 4 = 32 = 31 + 1$ より $1/a = 8$ となる.

例 5. $p = 137, a = 24$ で上記の計算をする.

$$
\begin{aligned}
p &= 5 \cdot a + 17 \\
a &= 1 \cdot 17 + 7 \\
17 &= 2 \cdot 7 + 3 \\
7 &= 2 \cdot 3 + 1
\end{aligned}
$$

ここから a の逆元を求める.

$$
\begin{aligned}
1 &= 7 - 2 \cdot 3 \\
&= 7 - 2 \cdot (17 - 2 \cdot 7) \\
&= 5 \cdot 7 - 2 \cdot 17 \\
&= 5 \cdot (a - 1 \cdot 17) - 2 \cdot 17 \\
&= 5 \cdot a - 7 \cdot 17 \\
&= 5 \cdot a - 7 \cdot (p - 5 \cdot a) \\
&= 40a - 7p
\end{aligned}
$$

確かに $40a = 40 \cdot 24 = 960 = 7 * 137 + 1$ より $1/a = 40$ となる.

b. ラグランジュの定理を使い, 全ての $a \in \mathbb{F}_p - \{0\}$ について $a^{p-1} = 1$ を説明せよ

Proof. $\mathbb{F}_p - \{0\}$ を群と見たときの要素 a の位数 $ord(a)$ を考える. 位数の定義から $a^{ord(a)} = 1$. ラグランジュの定理から, $ord(a)$ は $\mathbb{F}_p - \{0\}$ の位数 $p-1$ の約数なので $p - 1 = ord(a) \times e$. 以上から $a^{p-1} = a^{ord(a) \times e} = (a^{ord(a)})^e = 1^e = 1$ □

c. **全ての $a \in \mathbb{F}_p$ について $a^p = a$ であることを証明せよ．ヒント: $a = 0$ と $a \neq 0$ で場合分けせよ**

Proof. $a = 0$ の場合, $a^p = 0^p = 0 = a$.
$a \neq 0$ の場合, (b) から $a^p = a \times a^{p-1} = a \times 1 = a$. □

d. **$\mathbb{F}_p[x]$ の非零多項式で, $\mathbb{F}_p$ 上の全ての点で 0 になるものを見付けよ．ヒント: (c) を使え**

Proof. (c) より任意の $a \in \mathbb{F}_p$ で $a^p = a$. よって $f(x) = x^p - x$ は $\mathbb{F}_p$ 上の全ての点で 0 になる. □

例 6. $p = 3$ のとき $x^3 - x$ は $x = 0, 1, 2$ で 0 になる.
$x^3 - x$ は $\Pi_{a=0}^{2}(x - a)$ と一致する.