フィボナッチ数列の数理

原　信一郎

September 13, 2022

http://blade.nagaokaut.ac.jp/~hara/class/modern-math/

01 算数から数学へ

かけ算九九

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	10	12	14	16	18
3	3	6	9	12	15	18	21	24	27
4	4	8	12	16	20	24	28	32	36
5	5	10	15	20	25	30	35	40	45
6	6	12	18	24	30	36	42	48	54
7	7	14	21	28	35	42	49	56	63
8	8	16	24	32	40	48	56	64	72
9	9	18	27	36	45	54	63	72	81

かけ算九九

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9 (0 + 9 = 9)
2	2	4	6	8	10	12	14	16	18 (1 + 8 = 9)
3	3	6	9	12	15	18	21	24	27 (2 + 7 = 9)
4	4	8	12	16	20	24	28	32	36 (3 + 6 = 9)
5	5	10	15	20	25	30	35	40	45 (4 + 5 = 9)
6	6	12	18	24	30	36	42	48	54 (5 + 4 = 9)
7	7	14	21	28	35	42	49	56	63 (6 + 3 = 9)
8	8	16	24	32	40	48	56	64	72 (7 + 2 = 9)
9	9	18	27	36	45	54	63	72	81 (8 + 1 = 9)

かけ算九九

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7 $(7 \times 2 - 0 = 14)$	8	9
2	2	4	6	8	10	12	14 $(4 \times 2 - 1 = 7)$	16	18
3	3	6	9	12	15	18	21 $(1 \times 2 - 2 = 0)$	24	27
4	4	8	12	16	20	24	28 $(8 \times 2 - 2 = 14)$	32	36
5	5	10	15	20	25	30	35 $(5 \times 2 - 3 = 7)$	40	45
6	6	12	18	24	30	36	42 $(2 \times 2 - 4 = 0)$	48	54
7	7	14	21	28	35	42	49 $(9 \times 2 - 4 = 14)$	56	63
8	8	16	24	32	40	48	56 $(6 \times 2 - 5 = 7)$	64	72
9	9	18	27	36	45	54	63 $(3 \times 2 - 3 = 0)$	72	81

かけ算八八

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	11	13	15	17
3	3	6	10	13	16	20	23	26
4	4	8	13	17	22	26	31	35
5	5	11	16	22	27	33	38	44
6	6	13	20	26	33	40	46	53
7	7	15	23	31	38	46	54	62
8	8	17	26	35	44	53	62	71

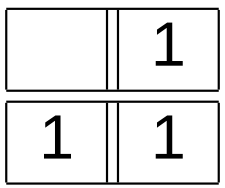
かけ算八八

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8 (0+8=8)
2	2	4	6	8	11	13	15	17 (1+7=8)
3	3	6	10	13	16	20	23	26 (2+6=8)
4	4	8	13	17	22	26	31	35 (3+5=8)
5	5	11	16	22	27	33	38	44 (4+4=8)
6	6	13	20	26	33	40	46	53 (5+3=8)
7	7	15	23	31	38	46	54	62 (6+2=8)
8	8	17	26	35	44	53	62	71 (7+1=8)

かけ算十十

	1	2	3	4	5	6	7	8	9	A
1	1	2	3	4	5	6	7	8	9	A
2	2	4	6	8	A	11	13	15	17	19
3	3	6	9	11	14	17	1A	22	25	28
4	4	8	11	15	19	22	26	2A	33	37
5	5	A	14	19	23	28	32	37	41	46
6	6	11	17	22	28	33	39	44	4A	55
7	7	13	1A	26	32	39	45	51	58	64
8	8	15	22	2A	37	44	51	59	66	73
9	9	17	25	33	41	4A	58	66	74	82
A	A	19	28	37	46	55	64	73	82	91

かけ算一々



02 Fibonacci 数列

定義 1

次の 2 項間漸化式で定義される数列をフィボナッチ *(fibonacci)* 数列と言う。

$$F_{n+2} = F_{n+1} + F_n$$

ただし、 $F_0 = 0,\ F_1 = 1$ とする。

最初の方を少し計算すると、
$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ F_7 = 13,\ F_8 = 21,\ F_9 = 34,\ F_{10} = 55,\ F_{11} = 89,\ F_{12} = 144,\ F_{13} = 233,\ F_{14} = 377,\ \cdots$

命題 2

$n \in \mathbb{Z}$ について、$F_{-n} = (-1)^{n-1} F_n$

Fibonacci 数列

$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ F_7 = 13,\ F_8 = 21,\ F_9 = 34,\ F_{10} = 55,\ F_{11} = 89,\ F_{12} = 144,\ F_{13} = 233,\ F_{14} = 377,\ F_{15} = 610,\ F_{16} = 987,\ F_{17} = 1597,\ F_{18} = 2584,\ F_{19} = 4181,\ F_{20} = 6765,\ F_{21} = 10946,\ F_{22} = 17711,\ F_{23} = 28657,\ F_{24} = 46368,\ F_{25} = 75025,\ F_{26} = 121393,\ F_{27} = 196418,\ F_{28} = 317811,\ F_{29} = 514229,\ F_{30} = 832040,\ F_{31} = 1346269,\ F_{32} = 2178309,\ F_{33} = 3524578,\ F_{34} = 5702887,\ F_{35} = 9227465,\ F_{36} = 14930352,\ F_{37} = 24157817,\ F_{38} = 39088169,\ F_{39} = 63245986,\ F_{40} = 102334155,$

$F_{-1} = 1,\ F_{-2} = -1,\ F_{-3} = 2,\ F_{-4} = -3,\ F_{-5} = 5,\ F_{-6} = -8,\ F_{-7} = 13,\ F_{-8} = -21,\ F_{-9} = 34,\ F_{-10} = -55,\ F_{-11} = 89,\ F_{-12} = -144,\ F_{-13} = 233,\ F_{-14} = -377,\ F_{-15} = 610,\ F_{-16} = -987,\ F_{-17} = 1597,\ F_{-18} = -2584,\ F_{-19} = 4181,\ F_{-20} = -6765,$

定理

定理 3 (一般項)

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

定理 4 (極限)

$$\lim_{n\to\infty}\frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2} = \text{黄金比}$$

定理 5 (加法定理)

$$F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$$

定理 6

$$F_{n+1}F_{n-1} - {F_n}^2 = (-1)^n$$
$${F_{n-1}}^2 + F_{n-1}F_n - {F_n}^2 = (-1)^n$$

定理 7

F_{n+1} と F_n は互いに素。

a と b を整数とするとき、$GCD(a,\ b)$ でその最大公約数を表すとする。$a|b$ で a が b を割切ることを表す。

定理 8

1. $F_{kn}\ (k \geqq 1)$ は F_n で割り切れる。
2. $GCD(F_m,\ F_n) = F_{GCD(m,\ n)}$
3. $m|n \Longleftrightarrow F_m|F_n\ (m \geqq 2$ とする)

fibonacci 数列の級数の性質

定理 9

1. $\sum_{k=1}^{n} F_k = F_{n+2} - 1$
2. $\sum_{k=1}^{n} F_{2k-1} = F_{2n}$
3. $\sum_{k=1}^{n} F_{2k} = F_{2n+1} - 1$
4. $\sum_{k=1}^{n} {F_k}^2 = F_{n+1}F_n$

03 Fibonacci数列の基本

基本的な設定

一般に、

$$x_{n+2} = x_{n+1} + x_n \cdots (\star)$$

とすると、

$$\begin{pmatrix} x_{n+1} \\ x_{n+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}$$

である。よって、$\boldsymbol{x}_n = \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}$, $\mathcal{F} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ とおけば $(\star)$ は、

$$\boldsymbol{x}_{n+1} = \mathcal{F}\boldsymbol{x}_n \cdots (*)$$

と同値である。よって、

$$\boldsymbol{x}_n = \mathcal{F}^n \boldsymbol{x}_0$$

となる。

注 1

$\mathcal{F}^2 = \mathcal{F} + E, \mathcal{F}^{-1} = \mathcal{F} - E$ である。

特に、$\boldsymbol{F}_n = \begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix}$ とおけば、

$$\boldsymbol{F}_n = \mathcal{F}^n \boldsymbol{F}_0 = \mathcal{F}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathcal{F}^n \text{の右側}$$

$$\boldsymbol{F}_{n-1} = \mathcal{F}^{n-1} \boldsymbol{F}_0 = \mathcal{F}^n \mathcal{F}^{-1} \boldsymbol{F}_0 = \mathcal{F}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \mathcal{F}^n \text{の左側}$$

なので、

$$\mathcal{F}^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$$

である。($F_{-1} = 1$ とおく。)

定理 3、定理 4 の証明

$\mathcal{F} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ の固有行列は、$tE - \mathcal{F} = \begin{pmatrix} t & -1 \\ -1 & t-1 \end{pmatrix}$、固有方程式は、$|tE - \mathcal{F}| = t^2 - t - 1 = 0$。固有値は、$\alpha = \dfrac{1+\sqrt{5}}{2}, \beta = \dfrac{1-\sqrt{5}}{2}$、固有ベクトルは、$\begin{pmatrix} 1 \\ \alpha \end{pmatrix}, \begin{pmatrix} 1 \\ \beta \end{pmatrix}$ である。($\alpha + \beta = 1,\ \alpha\beta = -1$ に注意。)

よって、$P = \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}$ とおくと、$\mathcal{F}P = P\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$。すなわち、$\mathcal{F} = P\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}P^{-1}$ である。よって、$\mathcal{F}^n = P\begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{pmatrix}P^{-1}$。すなわち、$\mathcal{F}^n = \begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}\begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{pmatrix}\dfrac{1}{\beta-\alpha}\begin{pmatrix} \beta & -1 \\ -\alpha & 1 \end{pmatrix} =$

$\dfrac{1}{\beta-\alpha}\begin{pmatrix} \beta^{n-1} - \alpha^{n-1} & \beta^n - \alpha^n \\ \beta^n - \alpha^n & \beta^{n+1} - \alpha^{n+1} \end{pmatrix}$。よって、$F_n = \dfrac{\beta^n - \alpha^n}{\beta - \alpha}$。

定理 5(加法定理) の証明

指数法則

$$\mathcal{F}^{m+n} = \mathcal{F}^m \mathcal{F}^n$$

より、

$$\begin{aligned}
\begin{pmatrix} F_{m+n-1} & F_{m+n} \\ F_{m+n} & F_{m+n+1} \end{pmatrix} &= \begin{pmatrix} F_{m-1} & F_m \\ F_m & F_{m+1} \end{pmatrix} \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \\
&= \begin{pmatrix} F_{m-1}F_{n-1} + F_m F_n & F_{m-1}F_n + F_m F_{n+1} \\ F_m F_{n-1} + F_{m+1} F_n & F_m F_n + F_{m+1} F_{n+1} \end{pmatrix}
\end{aligned}$$

である。よって、左下を見ると、

$$F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$$

である。

定理 5(加法定理) の別証明

差分方程式 (漸化式) $x_{n+2} = x_{n+1} + x_n \cdots (*)$ を考える。次が成り立つ。

補題 10

1. *(解の一意性)* 数列 A_n, B_n が $(*)$ を満たし、$A_0 = B_0$, $A_1 = B_1$ が成り立てば、すべての整数 n について、$A_n = B_n$ が成り立つ。
2. *(線形方程式における解の重ね合わせの原理)* k, l を定数とする。数列 A_n, B_n が $(*)$ を満たせば、その一次結合 $C_n = kA_n + lB_n$ も $(*)$ を満たす。

(加法定理の別証明) $f_n = F_{m+n}$, $g_n = F_m F_{n-1} + F_{m+1} F_n$ とおくと、f_n, g_n は $(*)$ を満たし、また $f_0 = F_m = g_0$, $f_1 = F_{m+1} = g_1$ である。よって、上の補題より、$f_n = g_n$ がすべての n について成り立つ。

三角関数の加法定理の証明

参考までに三角関数の加法定理
$\sin(x+a) = \sin x \cos a + \cos x \sin a$ の別証明ををあげる。微分方程式 $y'' = -y \cdots (*)$ を考える。次が成り立つ。

補題 11

1. *(解の一意性)* 関数 $y = a(x),\ y = b(x)$ が $(*)$ を満たし、$a(0) = b(0),\ a'(0) = b'(0)$ が成り立てば、すべての実数 x について、$a(x) = b(x)$ が成り立つ。
2. *(線形方程式における解の重ね合わせの原理)* $k,\ l$ を定数とする。数列 $y = a(s),\ b(x)$ が $(*)$ を満たせば、その一次結合 $y = ka(x) + lb(x)$ も $(*)$ を満たす。

(加法定理の別証明) $f(x) = \sin(x+a)$,
$g(x) = \sin x \cos a + \cos x \sin a$ とおくと、$f(x),\ g(x)$ は $(*)$ を満たし、また、$f(0) = \sin a = g(0)$。また、$f'(x) = \cos(x+a)$,
$g'(x) = \cos x \cos a - \sin x \sin a$ より、$f'(0) = \cos a = g'(0)$ である。よって、上の補題より、$f(x) = g(x)$ がすべての x について成り立つ

定理 6 の証明

$$\mathcal{F} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},\ \mathcal{F}^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$$

なので、

$$F_{n-1}F_{n+1} - {F_n}^2 = |\mathcal{F}^n| = |\mathcal{F}|^n = (-1)^n$$

定理 7 の証明

$F_{n+1} = F_n + F_{n-1}$ より、F_n と F_{n-1} 公約数は F_{n+1} と F_n 公約数に等しい。F_1 と F_0 公約数は 1 のみなので、すべての n について、F_{n+1} と F_n 公約数は 1 のみである。

ユークリッドの互除法

整数 $(m,\ n)$ に対し，$GCD(m,\ n)$ でその最大公約数とする。
$GCD(m,\ n)$ には次の性質がある。

1. $GCD(m,\ n) = GCD(n,\ m)$
2. $GCD(m,\ 0) = m$
3. k を整数とすると，$GCD(m,\ n) = GCD(m,\ n + km)$
4. $m|n \Longleftrightarrow GCC(m,\ n) = m$
5. $n \neq 0$，m を n で割った余りを r とすると，
   $GCD(m,\ n) = GCD(n,\ r)$
6. ある整数 $a,\ b$ が存在して，$am + bn = GCD(m,\ n)$
7. $GCD(m',\ n) = 1 \implies GCD(mm',\ n) = GCD(m,\ n)$

ユークリッドの互差法

自然数のペア $(m,\ n)$ について

$$(m,\ n) \to \begin{cases} (m-n,\ n) & m \geqq n \text{ のとき} \\ (m,\ n-m) & m \leqq n \text{ のとき} \end{cases}$$

という変形を繰り返す。($m = n$ のときはどちらの $\to$ でもよい。)
例: $(20,\ 12) \to (8,\ 12) \to (8,\ 4) \to (4,\ 4) \to (0,\ 4)$

【定理】(ユークリッドの互除 (差) 法)
この変形は、いつか必ず停止し、そのときペアの一方は 0 であり、もう一方は $GCD(m,\ n)$ である。

【証明】$GCD(m,\ n) = GCD(m-n,\ n) = GCD(m,\ n-m)$ 等より明らか。

定理 8 の再録

1. F_{kn} $(k \geqq 1)$ は F_n で割り切れる。
2. $GCD(F_m,\ F_n) = F_{GCD(m,\ n)}$
3. $m \mid n \Longleftrightarrow F_m \mid F_n$ $(m \geqq 2$ とする$)$

定理 8 の証明

1. 加法定理 (定理 5) ($F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$) より、
   $F_{(k+1)n} = F_{kn+n} = F_{kn} F_{n-1} + F_{kn+1} F_n$
   よって、F_{kn} が F_n で割り切れるなら、$F_{(k+1)n}$ も F_n で割り切れる。
2. $m = n + (m - n)$ なので加法定理より、$GCD(F_m,\ F_n) = GCD(F_{m-n} F_{n-1} + F_{m-n+1} F_n,\ F_n) = GCD(F_{m-n} F_{n-1},\ F_n)$。
   更に、定理 7 より F_{n-1} は F_n と素、よって、
   $GCD(F_m,\ F_n) = GCD(F_{m-n},\ F_n)$。よって、ユークリッドの互除 (差) 法の論法より、
   $GCD(F_m,\ F_n) = GCD(F_{GCD(m,\ n)},\ F_0) = F_{GCD(m,\ n)}$。
3. $m \geqq 2,\ n \geqq 0$ なら、$m = n \iff F_m = F_n$ である。よって、$m \mid n \iff m = GCD(m,\ n) \iff F_m = F_{GCD(m,\ n)} \iff F_m = GCD(F_m,\ F_n) \iff F_m \mid F_n$。

定理 9 の証明

1. $$\sum_{k=1}^{n} F_k = \sum_{k=1}^{n} (F_{k+2} - F_{k+1}) = F_{n+2} - F_2 = F_{n+2} - 1$$
2. $$\sum_{k=1}^{n} F_{2k-1} = \sum_{k=1}^{n} (F_{2k} - F_{2k-2}) = F_{2n} - F_0 = F_{2n}$$
3. $$\sum_{k=1}^{n} F_{2k} = \sum_{k=1}^{n} (F_{2k+1} - F_{2k-1}) = F_{2n+1} - F_1 = F_{2n+1} - 1$$
4. $$\sum_{k=1}^{n} {F_k}^2 = \sum_{k=1}^{n} F_k(F_{k+1} - F_{k-1}) = \sum_{k=1}^{n} (F_{k+1}F_k - F_kF_{k-1}) = F_{n+1}F_n - F_1F_0 = F_{n+1}F_n$$

04 群

群の公理

定義 12 (群)

集合 G 上に演算

$$\cdot \ : \ G \times G \ \to \ G, \qquad (a,\ b) \ \mapsto \ a \cdot b$$

が定義され、更に、 1 つの要素 $e \in G$ が定められているとする。
これらが、以下の条件（群の **公理**）を満たしているとき、$(G,\ \cdot,\ e)$ は **群**であるという。

1. 【結合則】 任意の $a,\ b,\ c \in G$ について
   $(a \cdot b) \cdot c = a \cdot (b \cdot c).$
2. 【単位元の存在】任意の $a \in G$ について
   $a \cdot e = a,\ e \cdot a = a.$
3. 【逆元の存在】 任意の $a \in G$ について、ある $b \in G$ が存在して $a \cdot b = b \cdot a = e.$

4. 【交換則】 任意の $a, b \in G$ について $a \cdot b = b \cdot a.$
が成り立つならば、 **可換群**あるいは **アーベル群**であると言う。

記法 1

1. $\cdot$ を G の乗法と呼ぶ。
2. e を G の単位元と呼ぶ。
3. $a \cdot b$ はしばしば $\cdot$ を省略して ab と書く。
4. 定義 *12* の *(3)* の b を a の逆元と言い、a^{-1} と書く。

命題 13 (群の性質)

G を群とするとき以下が成り立つ。

1. G の単位元は一意的である。
2. $a \in G$ の逆元は存在すれば一意的である。

【単位元が一意であることの証明】
単位元が X, Y と二つあったとすると、$X = Y$ である。なぜなら、

$$Y \text{ が単位元なので、} X = XY$$
$$X \text{ が単位元なので、} XY = Y$$

以上合わせて、

$$X = XY = Y$$

となる。

群の例

1. 【加法群としての実数】$(\mathbb{R},\ +,\ 0)$.
2. 【加法群としての整数】$(\mathbb{Z},\ +,\ 0)$.
3. 【加法群としての整数】$(n\mathbb{Z},\ +,\ 0)$. ここで、$n\mathbb{Z} = \{n \text{ の倍数全体}\}$ を表す。
4. 【乗法群 0 でない実数】$(\mathbb{R}^{\times},\ \times,\ 1)$.
5. 【乗法群 0 でない複素数】$(\mathbb{C}^{\times},\ \times,\ 1)$.
6. 【円】$(S^1,\ ?,\ (1,0))$.
7. 【3 次元球面】$(S^3,\ ?,\ (1,0,0,0))$.
8. 【正則な n 次正方行列】$(GL_n,\ \cdot,\ E)$（非可換）.
9. 【行列式が 1 である n 次正方行列】$(SL_n,\ \cdot,\ E)$（非可換）.
10. 【正則な対角行列群】$(D_n^{\times}(k),\ \cdot,\ E)$.

単純な群

1. $Z_2 = \{0,\ 1\}$

$\cdot$	0	1
0	0	1
1	1	0

において、$e = 0$ としたもの。

2. $Z^{\times} = \{-1,\ 1\}$

$\cdot$	1	-1
1	1	-1
-1	-1	1

において、$e = 1$ としたもの。

抽象的な群

1. $G_2 = \{a,\ b\}$

$\cdot$	a	b
a	a	b
b	b	a

において、$e = a$ としたもの。

2. $G_3 = \{a,\ b,\ c\}$

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

において、$e = a$ としたもの。

置換群

1. S_n を $\{1, 2, 3, \cdots, n\}$ からそれ自身への $1:1$ 写像全体とする。$\cdot$ は写像の合成とする。
2. A_n を S_n の部分集合で、「偶置換」全体とする。

合同変換群 $\mathrm{Sym}(X)$

X を「図形」とするとき，X 上の変換 $f : X \to X$ で，逆変換を持ち，X の任意の 2 点の距離を保つもの全体を $\mathrm{Sym}(X)$ と書き，X の合同変換群と言う。

05 群の準同型

記法 2

- $\{a, b, c\}$: 順序のない集合。
- (a, b, c) : 順序のある集合。
- 論理記号

$\forall x \cdots$	:	任意の x について $\cdots$。
$\exists x \cdots$	:	ある x について $\cdots$。
$P \implies Q$	:	P ならば Q。
$P \iff Q$	:	P と Q は同値。
$P \vee Q$	:	P または Q。
$P \wedge Q$	:	P かつ Q。
$\neg P$	:	P でない。

定義 14 (全射と単射)

$f : X \to Y$ を写像とするとき、

1. 「$\forall y \in Y \exists x \in X\, f(x) = y$」が成り立つ時、$f$ は **全射**であるという。
2. 「$\forall x, x' \in X (x \neq x' \implies f(x) \neq f(x'))$」が成り立つ時、$f$ は **単射**であるという。
3. f が全射でかつ単射であるとき f は **全単射**という。

定義 15 (準同型)

G, G' を群とし、写像 $f : G \to G'$ に対して次の条件が成り立つとき、f は G から G' への **準同型写像**という。

1. $\forall a, b \in G\ f(a \cdot b) = f(a) \cdot f(b)$

また更に f が全単射であるとき、f は G から G' への **同型写像**であるという。群 G と G' の間に少なくとも一つ同型写像がある時、G と G' は **同型** であるといい、$G \cong G'$ と書く。

命題 16

$f : G \to G'$ を群の準同型とするとき以下が成り立つ。

1. $f(e) = e.$
2. $f(a^{-1}) = f(a)^{-1}.$
3. f が同型なら f^{-1} も同型。

代数学は同型で不変な性質を研究する。

例 1

1. 任意の群 G について、その恒等写像 $i : G \to G,\ x \mapsto x$ は同型。
2. $f : \mathbb{Z}_2 \to \mathbb{Z}^\times,\ f(0) = 1,\ f(1) = -1$ は同型である。
3. $f : G_2 \to \mathbb{Z}^\times,\ f(a) = 1,\ f(b) = -1$ は同型である。
4. $f : \mathbb{Z} \to \mathbb{Z}^\times,\ f(n) = (-1)^n$ は全射準同型である。
5. $f : S_n \to \mathbb{Z}^\times,\ f(\sigma) = \sigma$の符号 は全射準同型である。
6. $f : GL_n(\mathbb{R}) \to \mathbb{R}^\times,\ f(A) = \det A$ は全射準同型。
7. $f : \mathbb{R} \to GL_2,\ f(x) = \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}$ は準同型。

【問題】

$G = \left\{ 1\text{次分数関数} : \dfrac{ax+b}{cx+b} \,|\, a,b,c,d \in \mathbb{R}, ad-bc \neq 0 \right\}$ と置き，$f : GL_2(\mathbb{R}) \to G$ を $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \dfrac{ax+b}{cx+b}$ で定義する。次の問いに答えなさい。

1. G が写像の合成を積とする群であることを示しなさい。
2. f が準同型写像であることを示しなさい。
3. $\alpha(x) = 1-x$, $\beta(x) = \dfrac{1}{x}$ とするとき,, $\alpha\beta\alpha\beta\alpha\beta$ を求めなさい。

定義 17 (部分群)

$(G, \cdot, e)$ を群、H がその部分集合で、同じ $\cdot$, e で群になっているとき、H を G の 部分群 という。このとき恒等写像 $j : H \to G,\ x \mapsto x$ は単射準同型であり、これを 包含写像あるいは 埋め込み写像という。

例 2

1. $n\mathbb{Z}$ は $\mathbb{Z}$ の部分群。
2. $\mathbb{Z}^\times$ は $\mathbb{R}^\times$ の部分群。
3. S_2 は S_3 の部分群。
4. SL_n は GL_n の部分群。
5. A_n は S_n の部分群。

06 正規部分群

剰余集合

G を群、$g \in G$ 、X を G の部分群とするとき、

$$gX = \{gx \mid x \in X\},\ Xg = \{xg \mid x \in X\}$$

と置く。

定義 18 (剰余集合)

G を群、H をその部分群とするとき、

$$G/H = \{gH \mid g \in G\}$$

と書き、これを G の H による左剰余集合と言う。gH の形の G の部分集合を、剰余類と言う。右剰余集合も同様に定義される。

命題 19 (剰余類の性質)

G を群、H をその部分群とするとき、$a, b \in G$ について以下の条件は全て同値である。

1. $b^{-1}a \in H.$
2. $aH \cap bH \neq \phi.$
3. $aH = bH.$
4. $a \in bH.$

定義 20

1. x を剰余類 $x \in G/H$ とするとき、$a \in x$ となる a を x の 代表元 という。
2. $a_1, a_2, \cdots \in G$ について、$a_1H \cup a_2H \cup \cdots = G$ かつ、各剰余類 $a_1H, a_2H, \cdots$ に交わりがないとき、$\{a_1, a_2, \cdots\}$ を G/H の 代表系という。
3. 写像 $\pi : G \to G/H, a \mapsto aH$ を 標準射影 という。

例 3 (代表系の例)

1. $\{0,\ 1\}$ は $\mathbb{Z}/2\mathbb{Z}$ の代表系である。
2. $\{0,\ 1,\ 2,\ 3\}$ は $\mathbb{Z}/4\mathbb{Z}$ の代表系である。

定義 21 (正規部分群)

G を環、N をその空でない部分群で、

$$\forall g \in G \; gN = Ng.$$

を満たす時 N は G の正規部分群であるという。

例 4

1. 可換群の部分群は正規部分群である。
2. A_n は S_n の正規部分群である。
3. S_2 は S_3 の正規部分群でない。

定義 22 (剰余群)

G を群、N を G の正規部分群とする。G/N に演算 $\cdot$ と元 e を次のように定義する。(これを 剰余群という。)

1. $x \cdot y = abN$ だだし、$a \in x,\ b \in y$ とする。
2. $e = N$ とする。

記法 3

剰余群 G/N について、gN を $[g]$ と書くことがある。

定理 23

G を、N をその正規部分群とするとき、$(G/N, \cdot, e)$ は群をなす。標準射影 $\pi : G \to G/N,\ g \mapsto [g]$ は準同型である。

剰余群の例

1. 一般に可換群 G と $g \in G$ に対して G/gG
2. $\mathbb{Z}/2\mathbb{Z} = \{[0],\ [1]\}$

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

面倒なので、次のように書く。

$\mathbb{Z}/2\mathbb{Z} = \{0,\ 1\}$

$+$	0	1
0	0	1
1	1	0

剰余群の例

3. $\mathbb{Z}/4\mathbb{Z} = \{[0],\ [1],\ [2],\ [3]\}$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

.

面倒なので、次のように書く。

$\mathbb{Z}/4\mathbb{Z} = \{0,\ 1,\ 2,\ 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

07 群の準同型定理

定義 24 (核, 像)

$f : G \to G'$ を群の準同型とするとき、

1. $\mathrm{Im} f = \{f(x) \in G' \mid x \in G\}$ を f の 像 *(image)* という。
2. $\mathrm{Ker} f = \{x \in G \mid f(x) = e\}$ を f の 核 *(kernel)* という。

命題 25

1. $\mathrm{Im} f$ は G' の部分群である。
2. $\mathrm{Ker} f$ は G の正規部分群である。

群の準同型定理

定理 26 (準同型定理)

$f : G \to G'$ を群の準同型とするとき、

$$\begin{aligned} \overline{f} : \quad & G/\mathrm{Ker}\, f \to \mathrm{Im}\, f, \\ & [a] \mapsto f(a). \end{aligned}$$

は同型写像である。

[証明] 証明すべき事は (1) well-defined、(2) 全射、(3) 単射、(4) 準同型性である。□

系 27

1. $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}^\times \cong \mathbb{Z}_2 \cong G_2$.
2. $S_n/A_n \cong \mathbb{Z}^\times$.

08 fibonacci数列の約数

定理 8 の群論的 (?) 証明

加法定理 (定理 5)

$$F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$$

を標準射影

$$\pi : \quad \mathbb{Z} \to \mathbb{Z}/F_n\mathbb{Z}, \quad k \mapsto [k]$$

で「落として」考えると、

$$[F_{m+n}] = [F_m F_{n-1} + F_{m+1} F_n] = [F_m F_{n-1}]$$

である。よって、$k \geqq 1$ について、

$$[F_{kn}] = [F_{(k-1)n} F_{n-1}] = [F_{(k-2)n} {F_{n-1}}^2] = \cdots = [F_n {F_{n-1}}^{k-1}] = 0$$

すなわち、$\mathbb{Z}$ において F_{kn} は F_n で割り切れる。

09 環と体

環と体の公理

定義 28 (環と体)

集合 R 上に 2 つの演算

$$\begin{aligned} + &: R \times R \to R, & (a, b) &\mapsto a + b \\ \cdot &: R \times R \to R, & (a, b) &\mapsto a \cdot b \end{aligned}$$

が定義されているとする。更に 2 つの異なる要素 $0, 1 \in R$ が定められているとする。
これらが、以下の条件（環の **公理**）を満たしているとき、$(R, +, \cdot, 0, 1)$ は **環**であるという。

1. 【結合則】 任意の $a,\ b,\ c \in R$ について
$(a+b)+c = a+(b+c)$.
2. 【交換則】 任意の $a,\ b \in R$ について $a+b = b+a$.
3. 【零元の存在】任意の $a \in R$ について
$a+0 = a,\ 0+a = a$.
4. 【負元の存在】 任意の $a \in R$ について、ある $b \in R$ が存在して $a+b = b+a = 0$.
5. 【結合則】 任意の $a,\ b,\ c \in R$ について
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
6. 【単位元の存在】任意の $a \in R$ について
$a \cdot 1 = a,\ 1 \cdot a = a$.
7. 【分配則】 任意の $a,\ b,\ c \in R$ について
$a \cdot (b+c) = a \cdot b + a \cdot c,\ (a+b) \cdot c = a \cdot c + b \cdot c$.
8. 【交換則】 任意の $a,\ b \in R$ について $a \cdot b = b \cdot a$.

が成り立つならば、 **可換環**であると言う。

体

上記環の公理に加え、

9. 【逆元の存在】 任意の $a \in R$ について、$a \neq 0$ ならば、
ある $b \in R$ が存在して $a \cdot b = b \cdot a = 1$.
が成り立つならば、 体であると言う。

記法 4

1. $+, \cdot$ を R の加法、乗法と呼ぶ。
2. $0, 1$ を R の零元、単位元と呼ぶ。
3. $a \cdot b$ はしばしば $\cdot$ を省略して ab と書く。
4. 定義 *28* の *(4)* の b を a の負元と言い、$-a$ と書く。
5. $a + (-b)$ を $a - b$ と書く。
6. 定義 *28* の *(9)* の b を a の逆元と言い、a^{-1} と書く。
7. $a \cdot b^{-1}$ を a/b と書く。

注 2

1. この文書では「環」といえば「可換環」を指すことにする。
2. この文書では「体」といえば $0 \neq 1$ を仮定する。
3. 環 $(R,\ +,\ \cdot,\ 0,\ 1)$ を単に R と書くことがある。

定義 29 (単元, 可逆元)

環 R の要素で逆元を持つものを 単元あるいは 可逆元 という。単元全体を $R^\times$ と書く。

注 3

1. R が体 $\iff R^\times = R - \{0\}$。
2. R が体 $\Rightarrow (R[x])^\times = R^\times$。

命題 30 (環の性質)

R を環とするとき以下が成り立つ。

1. R の零元は一意的である。
2. R の単位元は一意的である。
3. $a \in R$ の負元は一意的である。
4. $a \in R$ の逆元は存在すれば一意的である。
5. $a \cdot 0 = 0.$
6. $a \cdot (-b) = -(a \cdot b).$

$* \times 0 = 0$

$a \times 0 = 0$ の厳密な証明

$* \times 0 = 0$

$a \times 0 = 0$ の厳密な証明

$$
\begin{aligned}
a \times 0 &= a \times 0 + 0 \\
&= a \times 0 + (a \times 0 + (-(a \times 0))) \\
&= (a \times 0 + a \times 0) + (-(a \times 0)) \\
&= (a \times (0 + 0) + (-(a \times 0)) \\
&= (a \times 0 + (-(a \times 0)) \\
&= 0
\end{aligned}
$$

マイナス × マイナス = プラス

$(-a) \times (-b) = a \times b$ の厳密な証明

マイナス × マイナス = プラス

$(-a) \times (-b) = a \times b$ の厳密な証明

$$
\begin{aligned}
(-a) \times (-b) &= (-a) \times (-b) + 0 \\
&= (-a) \times (-b) + a \times 0 \\
&= (-a) \times (-b) + a \times ((-b) + b) \\
&= (-a) \times (-b) + a \times (-b) + a \times b \\
&= ((-a) + a) \times (-b) + a \times b \\
&= 0 \times (-b) + a \times b \\
&= 0 + a \times b \\
&= a \times b
\end{aligned}
$$

例 5 (環と体の例)

1. 【整数環】$(\mathbb{Z},\ +,\ \cdot,\ 0,\ 1)$.
2. 【有理数体】$(\mathbb{Q},\ +,\ \cdot,\ 0,\ 1)$.
3. 【実数体】$(\mathbb{R},\ +,\ \cdot,\ 0,\ 1)$.
4. 【複素数体】$(\mathbb{C},\ +,\ \cdot,\ 0,\ 1)$.
5. $(\mathbb{Z}[\sqrt{d}],\ +,\ \cdot,\ 0,\ 1)$、ただし、$d$ を整数とする。
6. 【多項式環】$(R[x_1,\ x_2,\ \cdots,\ x_n],\ +,\ \cdot,\ 0,\ 1)$. ただし R を環とする。（以下同様）
7. 【R 上の正方行列環】$(M_n(R),\ +,\ \cdot,\ O,\ E)$ （非可換）.
8. 【対角行列環】$(D_n(R),\ +,\ \cdot,\ O,\ E)$.

例 6

9. $R_2 = \{a,\ b\}$

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

において、$0 = a,\ 1 = b$ としたもの。

10. $R_4 = \{a,\ b,\ c,\ d\}$

$+$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	a	c
d	a	d	c	b

において、$0 = a,\ 1 = b$ としたもの。

定義 31 (部分環)

$(R,\ +,\ \cdot,\ 0,\ 1)$ を環、S がその部分集合で、同じ $+,\ \cdot,\ 0,\ 1$ で環になっているとき、S を R の 部分環 という。このとき恒等写像 $j : S \to R,\ x \mapsto x$ は準同型であり、これを 包含写像あるいは 埋め込み写像という。

例 7

1. $\mathbb{Z}$ は $\mathbb{Q}$ の部分環。
2. $\mathbb{Q}$ は $\mathbb{R}$ の部分環。
3. $\mathbb{R}$ は $\mathbb{C}$ の部分環。
4. $D_n(k)$ は $M_n(k)$ の部分環。

10 多項式環

多項式環

定義 32

R を環、x を不定元変数とするとき、$R[x]$ で、係数を R とする多項式環を表す。

例えば、$\mathbb{Z}[x]$ は係数が整数である多項式全体、$\mathbb{Q}[x]$ は係数が有理数である多項式全体、$\mathbb{R}[x]$ は係数が実数である多項式全体、$\mathbb{C}[x]$ は係数が複素数である多項式全体を表す。

定義 33

R を環、r を R の元、S を R の部分環をとするとき、$S[r]$ で、係数を S とする r の多項式で書ける数全体を表す。

例えば、$\mathbb{Z}[\sqrt{2}]$ は $a + b\sqrt{2},\ (a,\ b \in \mathbb{Z})$ と書ける数全体を表す。

11 準同型

環の準同型

定義 34 (準同型)

R, S を環とし、写像 $f : R \to S$ に対して次の条件が成り立つとき、f は R から S への **準同型写像**という。

1. $\forall a, b \in R \ f(a+b) = f(a) + f(b)$
2. $\forall a, b \in R \ f(a \cdot b) = f(a) \cdot f(b)$
3. $f(1) = 1$

また更に f が全単射であるとき、f は R から S への **同型写像**であるという。環 R と S の間に少なくとも一つ同型写像がある時、R と S は **同型** であるといい、$R \cong S$ と書く。

命題 35

$f : R \to S$ を環の準同型とするとき以下が成り立つ。

1. $f(0) = 0$.
2. $f(-a) = -f(a)$.
3. $f(a^{-1}) = f(a)^{-1}$, (a^{-1}が存在するとき).
4. f が同型なら f^{-1} も同型。

代数学は同型で不変な性質を研究する。

例 8

1. 任意の環 R について、その恒等写像 $i : R \to R,\ x \mapsto x$ は同型。
2. $f : R_2 \to R_4,\ f(a) = a,\ f(b) = c$ は単射準同型ではない。
3. $g : R_4 \to R_2,\ g(a) = a,\ g(b) = b, g(c) = a,\ g(d) = b$ は全射準同型。

12 イデアル

イデアルと剰余環

定義 36 (イデアル)

R を環、I をその空でない部分集合で、次の条件を満たすとき、I は R のイデアルであるという。

1. $\forall x, y \in I \; x + y \in I$
2. $\forall x \in R \; \forall y \in I \; x \cdot y \in I$

例 9

1. R と $\{0\}$ は R のイデアル。これらを 自明なイデアルという。
2. $n\mathbb{Z} = \{n \cdot m \mid m \in \mathbb{Z}\}$ は $\mathbb{Z}$ のイデアル。
3. 可換環 R の要素 a に対して、$\langle a \rangle$ を a の倍数全体を表す。$\mathbb{Z}$ においては、$n\mathbb{Z} = \langle n \rangle$。

定義 37

$s_1,\ s_2, \cdots,\ s_n \in R$ に対して、

$$\langle\, s_1,\ s_2, \cdots,\ s_n \,\rangle = \{r_1 s_1 + r_2 s_2 + \cdots + r_n s_n \mid r_1,\ r_2,\ \cdots,\ r_n \in R\}$$

とおき、これを $s_1,\ s_2, \cdots,\ s_n$ で 生成されたイデアルという。これを、$Rs_1 + Rs_2 + \cdots + Rs_n$ とも書く。一つの要素で生成されるイデアル $\langle\, a \,\rangle = Ra$ を 単項イデアルという。

剰余類

定義 38 (剰余類)

R を環、I をそのイデアルとするとき、$a \in R$ に対して $[a] = \{x \in R \mid x - a \in I\}$ と書き、これを a の 剰余類と呼ぶ。また、全ての剰余類の集合 (剰余集合) を

$$R/I = \{[a] \mid a \in R\}$$

と書く。

注 4

1. R/I を可換群 $R = (R, +, 0)$ の剰余集合である。
2. $[a] = \{a + x \in R \mid x \in I\}$ であるので、これを $a + I$ と書くことがある。
3. $a \in [a]$ である。

例 10 (剰余集合の例)

1. $\mathbb{Z}/2\mathbb{Z} = \{[0],\ [1]\},\ [0] = \{\cdots, -2, 0, 2, 4, \cdots\},\ [1] = \{\cdots, -1, 1, 3, 5, \cdots\}.$
2. $\mathbb{Z}/4\mathbb{Z} = \{[0],\ [1],\ [2],\ [3]\},\ [0] = \{\cdots, -4, 0, 4, 8, \cdots\}.$

命題 39 (剰余類の性質)

以下の条件は全て同値である。

1. $a - b \in I$.
2. $[a] \cap [b] \neq \phi$.
3. $[a] = [b]$.
4. $a \in [b]$.

定義 40

1. x を剰余類 $x \in R/I$ とするとき、$a \in x$ となる a を x の代表元 という。
2. 写像 $\pi : R \to R/I,\ a \mapsto [a]$ を 標準射影 という。

剰余環

定義 41 (剰余環)

R/I に演算 $+, \cdot$ と元 $0, 1$ を次のように定義する。(これを剰余環という。)

1. $x + y = [a + b]$ だだし、$a \in x,\ b \in y$ とする。
2. $x \cdot y = [a \cdot b]$ だだし、$a \in x,\ b \in y$ とする。
3. $0 = [0]$ とする。
4. $1 = [1]$ とする。

定理 42

R を環、I をイデアルとするとき、$(R/I,\ +,\ \cdot,\ 0,\ 1)$ は環をなす。標準射影 $\pi : R \to R/I,\ a \mapsto [a]$ は準同型である。

剰余環の例

1. $\mathbb{Z}/2\mathbb{Z} = \{[0],\ [1]\}$,

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

2. $\mathbb{Z}/4\mathbb{Z} = \{[0],\ [1],\ [2],\ [3]\}$,

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

.

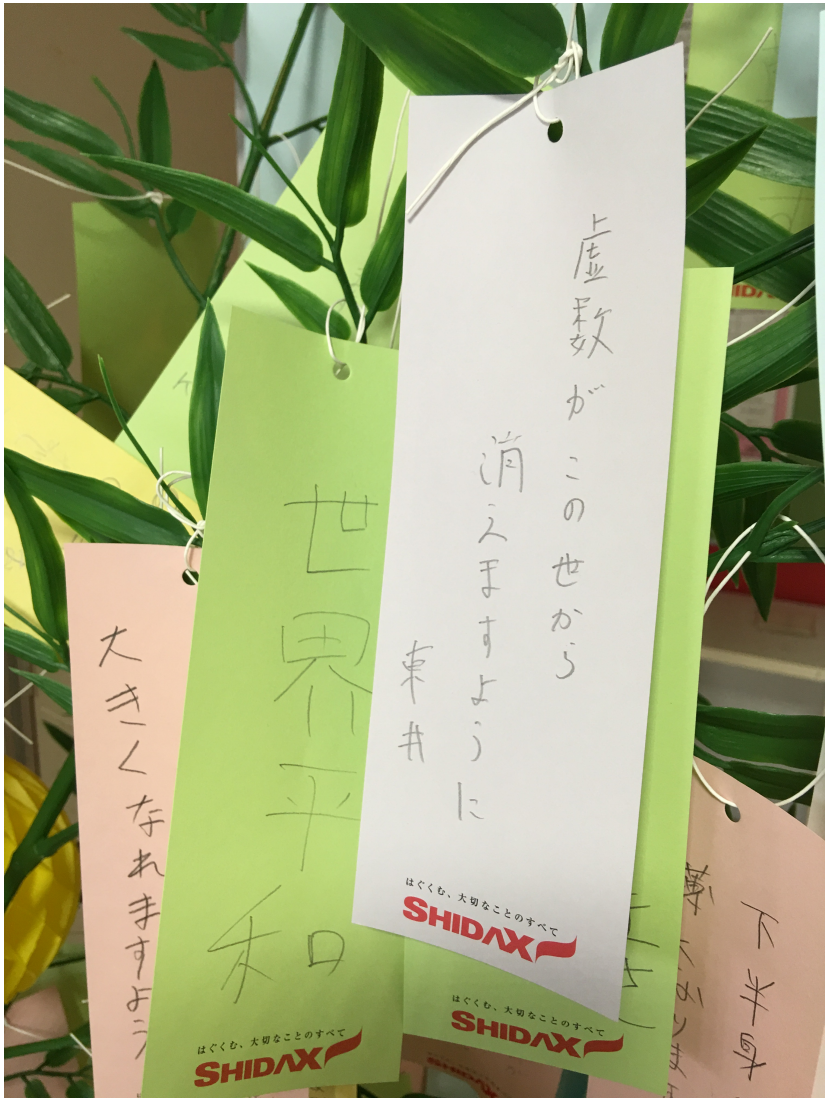
$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

.

剰余環の例

1. $\mathbb{Z}/n\mathbb{Z} = \{0,\ 1,\ 2,\ \cdots,\ n-1\},\ n = 0$
2. $\mathbb{R}[x]/\langle\, x^2+1 \,\rangle = \{[a+bx] \mid a,\ b \in \mathbb{R}\} = \{a+bi \mid a,\ b \in \mathbb{R}\},\ a = a \cdot 1,\ i = [x].$
   $0 = 0 + 0i, \quad 1 = 1 + 0i,$
   $(a+bi) + (c+di) = (a+c) + (b+d)i, \quad (a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i.$
3. $\mathbb{Z}[x]/\langle\, x^2 - x - 1 \,\rangle = \{ax + b \mid a,\ b \in \mathbb{Z}\}$
4. $(\mathbb{Z}/n\mathbb{Z})[x]/\langle\, x^2 - x - 1 \,\rangle = \{ax + b \mid a,\ b \in \mathbb{Z}/n\mathbb{Z}\}$

世界が平和でありますように



第３食堂前 2016 年７月７日

13 環の準同型定理

準同型定理

定義 43 (核, 像)

$f : R \to S$ を環の準同型とするとき、

1. $\mathrm{Im} f = \{f(x) \in S \mid x \in R\}$ を f の 像 *(image)* という。
2. $\mathrm{Ker} f = \{x \in R \mid f(x) = 0\}$ を f の 核 *(kernel)* という。

命題 44

1. $\mathrm{Im} f$ は S の部分環である。
2. $\mathrm{Ker} f$ は R のイデアルである。

定理 45 (準同型定理)

$f : R \to S$ を環の準同型とするとき、

$$\begin{aligned} \overline{f} : \quad & R/\mathrm{Ker}\, f \to \mathrm{Im}\, f, \\ & [a] \mapsto f(a). \end{aligned}$$

は同型写像である。

[証明] 証明すべき事は (1) well-defined、(2) 全射、(3) 単射、(4) 準同型性である。□

例 11

R を環、$a \in R$、$R[x]$ を R 上の多項式環とするとき、

$$\begin{array}{rcl} R[x]: & \to & R \\ p(x) & \mapsto & p(a) \end{array}$$

は、準同型。

例 12

1. $\mathbb{Z}/2\mathbb{Z} \cong R_2$.
2. $\mathbb{Z}/4\mathbb{Z} \cong R_4$.
3. $\mathbb{Z}[x]/\langle\, x^2 - 2 \,\rangle \cong \mathbb{Z}[\sqrt{2}]$.
4. $\mathbb{R}[x]/\langle\, x^2 + 1 \,\rangle \cong \mathbb{C}$.
5. $\mathbb{Z}[x]/\langle\, x^2 - x - 1 \,\rangle \cong \mathbb{Z}[\mathcal{F}]$. ただし、$\mathbb{Z}[\mathcal{F}]$ とは整数係数の $\mathcal{F} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ の多項式で表せる行列全体。

$i = \sqrt{-1}$ とする。$p(x) \in \mathbb{R}[x]$ について、$p(i) = 0$ が成り立つなら、$p(x)$ は $x^2 + 1$ で割り切れる。

14 三角関数の世界

三角関数！

定理 46 (加法定理)

$$\begin{cases} \cos(\alpha+\beta) &= \cos\alpha\cos\beta - \sin\alpha\sin\beta \\ \sin(\alpha+\beta) &= \sin\alpha\cos\beta + \cos\alpha\sin\beta \end{cases}$$

系 47

1. $\cos 2\theta = \cos^2\theta - \sin^2\theta,\ \sin 2\theta = 2\sin\theta\cos\theta$
2. $\cos 3\theta = 4\cos^3\theta - 3\cos\theta,\ \sin 3\theta = 3\sin\theta - 4\sin^3\theta$
3. $1 + \cos\theta + \cos 2\theta + \cos 3\theta = ?$
4. $\sin\theta + \sin 2\theta + \sin 3\theta = ?$

複素数の世界では

定理 48 (オイラーの公式)

$$e^{i\theta} = \cos\theta + i\sin\theta$$

定理 49 (オイラーの等式)

$$e^{i\pi} = -1$$

定理 50 (指数の加法定理)

$$e^{i(\alpha+\beta)} = e^{i\alpha}e^{i\beta}$$

[証明] 三角関数の加法定理より、

右辺 $= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) =$

$(\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta) =$

$\cos(\alpha+\beta) + i\sin(\alpha+\beta) =$ 左辺。□

定理 51 (ド・モアブルの公式)

$$(e^{i\theta})^n = e^{in\theta}$$

3 倍角の公式の証明：

$$\begin{aligned} & \cos 3\theta + i \sin 3\theta \\ = \ & (\cos\theta + i\sin\theta)^3 \\ = \ & \cos^3\theta + 3\cos^2\theta \cdot i\sin\theta + 3\cos\theta \cdot (-\sin^2\theta) + -i\sin^3\theta \\ = \ & (\cos^3\theta - 3\cos\theta\sin^2\theta) + i(3\cos^2\theta\sin\theta - \sin^3\theta) \end{aligned}$$

よって、

$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta, \quad \sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta$。

また、$1 + \cos\theta + \cos 2\theta + \cos 3\theta + i(\sin\theta + \sin 2\theta + \sin 3\theta) =$

$1 + e^{i\theta} + e^{2i\theta} + e^{3i\theta} = 1 + e^{i\theta} + (e^{i\theta})^2 + (e^{i\theta})^3 = \dfrac{1 - e^{4i\theta}}{1 - e^{i\theta}}$。

三角関数とは

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$$
$$\sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

$$De^{ix} = ie^{ix}$$
$$De^{zx} = ze^{zx}$$

(参考) オイラー・原の公式

$$c_{n+2} = -c_n,\ c_1 = 0,\ c_2 = -1$$
$$s_{n+2} = -s_n,\ s_1 = 1,\ s_2 = 0$$

つまり、

n	0	1	2	3	4	5	6	7	8	$\cdots$
c_n	1	0	-1	0	1	0	-1	0	1	$\cdots$
s_n	0	1	0	-1	0	1	0	-1	0	$\cdots$

となる、c_n, s_n を i^n と $(-i)^n$ を用いて表すと…

$$c_n = \frac{i^n + (-i)^n}{2}, \quad s_n = \frac{i^n - (-i)^n}{2i}$$

$$i^n = c_n + i\, s_n \quad \text{(オイラー・原の公式)}$$

動機

三角関数の公式はたくさんある。
が、オイラーの公式で統一的に扱えるようになった。

動機

フィボナッチ数列も成仏させたい！

15 代数的な枠組みで見たfibonacci数列

代数的な枠組みで見た fibonacci 数列

定義 52

$\mathbb{F} = \mathbb{Z}[x]/\langle x^2 - x - 1 \rangle$, $\mathbb{F}_0 = \mathbb{Q}[x]/\langle x^2 - x - 1 \rangle$ と置く。

$\mathcal{F} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ とおくと、$\mathcal{F}^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$ である。また、$\mathcal{F}^2 - \mathcal{F} - E = 0$ が成り立つ。よって、

F_nの性質を調べること $\Leftrightarrow$ $\mathcal{F} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$の性質を調べること

$\Leftrightarrow$ $\mathbb{F}$ の性質を調べること

$\mathcal{F}' = \begin{pmatrix} 3 & -1 \\ 7 & -2 \end{pmatrix}$ と置くと、やはり、$\mathcal{F}'^2 - \mathcal{F}' - E = 0$ を満たしているので、$\mathbb{F}$ は、F_n の情報を 100% 含んでいるわけではない…ようにも思えるが、そうでもない (定理 54 参照)。

$\mathbb{F}$ には次のような性質がある。証明は $\sqrt{5}$ が無理数であることを利用する。

命題 53

$x = [x] \in \mathbb{F}$ とする。

1. 全ての $\mathbb{F}$ の要素は、ある $a,\ b \in \mathbb{Z}$ で $ax + b$ と表される。
2. $ax + b = 0 \ \Leftrightarrow \ a = b = 0$
3. $s,\ t \in \mathbb{F},\ s \cdot t = 0 \ \Leftrightarrow \ s = 0$ または $t = 0$

$\mathbb{F}$ を $\mathbb{F}_0$ とし、$\mathbb{Z}$ を $\mathbb{Q}$ としても同様。

次の定理は F_n にある種の普遍性があることを示している。

定理 54

$\mathbb{F}$ において、$x^n = F_n x + F_{n-1}$ である。

[証明] $n = 0$ のとき正しい。$x(xF_n + F_{n-1}) = x^2F_n + xF_{n-1} = (x+1)F_n + xF_{n-1} = (F_n + F_{n-1})x + F_n = F_{n+1}x + F_n$ より。□

定理 5(加法定理) の再証明

加法定理 (定理 5) $F_{m+n} = F_{m+1}F_n + F_mF_{n-1}$ の証明
$x^{m+n} = x^m\, x^n$ に前定理を代入して

$$\begin{aligned} F_{m+n}x + F_{m+n-1} &= (F_mx + F_{m-1})(F_nx + F_{n-1}) \\ &= F_mF_nx^2 + (F_{m-1}F_n + F_mF_{n-1})x + F_{m-1}F_{n-1} \\ &= F_mF_n(x+1) + (F_{m-1}F_n + F_mF_{n-1})x + F_{m-1}F_{n-1} \\ &= (F_mF_n + F_{m-1}F_n + F_mF_{n-1})x + F_mF_n + F_{m-1}F_{n-1} \end{aligned}$$

よって、

$$\begin{aligned} F_{m+n} &= F_mF_n + F_{m-1}F_n + F_mF_{n-1} \\ F_{m+n-1} &= F_mF_n + F_{m-1}F_{n-1} \end{aligned}$$

である。これから加法定理はすぐ得られる。

注 5

この証明は、三角関数の加法定理 *(定理 46)*

$$\begin{cases} \cos(\alpha+\beta) &= \cos\alpha\cos\beta - \sin\alpha\sin\beta \\ \sin(\alpha+\beta) &= \sin\alpha\cos\beta + \cos\alpha\sin\beta \end{cases}$$

がオイラーの公式

$$e^{i\theta} = \cos\theta + i\sin\theta$$

と、指数定理

$$e^{i(\alpha+\beta)} = e^{i\alpha}e^{i\beta}$$

から、次のように証明されることを想起させる。

$$\begin{aligned} \text{左辺} &= \cos(\alpha+\beta) + i\sin(\alpha+\beta) \\ \text{右辺} &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta) \end{aligned}$$

定理 8 の再証明

標準射影 $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ k \mapsto [k]$ によって導かれる標準射影

$$\pi : \quad \mathbb{F} = \mathbb{Z}[x]/(x^2 - x - 1) \to (\mathbb{Z}/n\mathbb{Z})[x]/(x^2 - x - 1)$$
$$ax + b \mapsto [a]x + [b]$$

を考える。(今後 $[a]x + [b]$ も $ax + b$ と書くことにする。)
$x^n = F_n x + F_{n-1} \in \mathbb{F}$ より $x^n = F_{n-1} \in (\mathbb{Z}/F_n\mathbb{Z})[x]/(x^2 - x - 1)$ である。よって、$F_{kn}x + F_{kn-1} = x^{kn} = (x^n)^k = {F_{n-1}}^k$。従って $\mathbb{Z}/F_n\mathbb{Z}$ において、

$$F_{kn} = 0, \quad F_{kn-1} = {F_{n-1}}^k$$

である。よって $\mathbb{Z}$ において、F_{kn} は F_n で割り切れる。

定理 9 の再証明

(1) $F_k x + F_{k-1} = x^k$ より、

$$\sum_{k=1}^{n} F_k x + \sum_{k=1}^{n-1} F_k = \sum_{k=1}^{n} x^k = \sum_{k=1}^{n} (x^{k+2} - x^{k+1}) = x^{n+2} - x^2 =$$

$F_{n+2}x + F_{n+1} - (x+1) = (F_{n+2} - 1)x + F_{n+1} - 1$ よって、

$\sum_{k=1}^{n} F_k = F_{n+2} - 1$ である。

(2), (3) $F_{2k}x + F_{2k-1} = x^{2k}$ より、 $\sum_{k=1}^{n} F_{2k}x + \sum_{k=1}^{n} F_{2k-1} =$

$$\sum_{k=1}^{n} x^{2k} = \sum_{k=1}^{n} (x^{2k+1} - x^{2k-1}) = x^{2n+1} - x = (F_{2n+1} - 1)x + F_{2n}$$

よって、 $\sum_{k=1}^{n} F_{2k} = F_{2n+1} - 1$, $\sum_{k=1}^{n} F_{2k-1} = F_{2n}$ である。

$\mathbb{F}$ について更にいくつかの事

補題 55

$a, b \in \mathbb{Z}$(あるいは $\mathbb{Q}$) について、$a \neq 0$ または $b \neq 0$ ならば、$-a^2 + ab + b^2 \neq 0$ である。

【証明】$-a^2 + ab + b^2 = 0$ ならば、$(2b + a)^2 = 5a^2$ だが、5 は平方数でない。

命題 56

$\mathbb{F}$ において、

$$(ax + b)(-ax + a + b) = -a^2 + ab + b^2$$

命題 57

$$\frac{1}{ax + b} = \frac{-ax + a + b}{-a^2 + ab + b^2}$$

系 58

$\mathbb{F}_0$ は体である。

$\mathbb{F}$ について更にいくつかの事

系 59

$$\frac{1}{x} = x - 1, \quad \frac{1}{x-1} = x$$

系 60

$$\sqrt{5} = \pm(2x - 1)$$

直積と直和

定義 61

G_1, G_2 を群とするとき、

- $G = G_1 \times G_2 = \{(g_1,\ g_2) | g_1 \in G_1,\ g_2 \in G_2\}$
- $(g_1,\ g_2) \cdot (g_1',\ g_2') = (g_1 \cdot g_1',\ g_2 \cdot g_2')$
- $e = (e,\ e)$

と定義すると、G は群になる。G を単に $G_1 \times G_2$ と書き、G_1 と G_2 の直積という。G_1, G_2 がアーベル群であるとき、G を $G_1 \oplus G_2$、e を 0 と書き、G_1 と G_2 の直和と言う。

例 13

$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ である。次が互いに逆準同型を与えるから。

$$\begin{aligned} \phi : \mathbb{Z}/6\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \\ [x] &\mapsto ([x],\ [x]) \\ \psi : \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} &\to \mathbb{Z}/6\mathbb{Z} \\ ([x],\ [y]) &\mapsto [3x + 2y] \end{aligned}$$

$\mathbb{F}$ について更にいくつかの事 (その 2)

$\mathbb{Z}\{a\} = \{na \mid n \in \mathbb{Z}\}$ と書くことにする。

定理 62

$\mathbb{F} \cong \mathbb{Z}\{x\} \oplus \mathbb{Z}\{1\} \cong \mathbb{Z}\{x\} \oplus \mathbb{Z}\{1-x\}$

定理 63

$$\begin{aligned} \tau \quad &: \quad \mathbb{F} \to \mathbb{F} \\ &\qquad x \mapsto 1-x \end{aligned}$$

で定義される τ は環の同型を与える。(x と $1-x$ は「兄弟」である。)

【証明】 $f : \mathbb{Z}[x] \to \mathbb{F}$ を $f(x) = 1-x$ で定義する。
$\mathrm{Ker} f =< x^2 - x - 1 >$ となるので、準同型定理より証明される。

$\mathbb{F}$ について更にいくつかの事 (その 3)

命題 64

$\mathbb{F}$ において次が成り立つ。

1. $x^n = F_n x + F_{n-1}$
2. $(1-x)^n = F_n(1-x) + F_{n-1} = -F_n x + F_{n+1}$
3. $a_n = x^n,\ (1-x)^n$ は、漸化式 $a_{n+2} = a_{n+1} + a_n$ を満たす。

命題 65

$x(1-x) = -1,\ x^n(1-x)^n = (-1)^n$

定理 66

$$F_n = \frac{1}{2x-1}\left(x^n - (1-x)^n\right) = \frac{2x-1}{5}\left(x^n - (1-x)^n\right)$$

$\mathbb{F}$ について更にいくつかの事 (その 4)

定理 67

1. $x^{2n} = (2F_nF_{n-1} + {F_n}^2)x + {F_n}^2 + {F_{n-1}}^2$
2. $x^{2n+1} = ({F_{n+1}}^2 + {F_n}^2)x + 2F_{n+1}F_n - {F_n}^2$

定理 68

1. $\displaystyle\sum_{k=0}^{n} x^k = x^{n+2} - x = (F_{n+2} - 1)x + F_{n+1}$
2. $\displaystyle\sum_{k=0}^{n} x^{2k} = x^{2n+1} - x + 1 = (F_{2n+1} - 1)x + F_{2n} + 1$

$\mathbb{F}$ について更にいくつかの事 (その 5)

定理 69

t の形式的冪級数として、次が成り立つ。

$$F_1 + F_2 t + F_3 t^2 + F_4 t^4 + \cdots = \frac{1}{1 - t - t^2}$$

Fibonacci 数列について補足

定理 70

1. $F_{n+1}^2 + F_n^2 = F_{2n+1}$
2. $F_{n+2}^2 - F_n^2 = F_{2n+2}$
3. $F_{n+1}^2 - F_n^2 = F_{n+2}F_{n-1}$
4. $F_{2n} = F_{n+1}F_n + F_nF_{n-1}$
5. $F_{3n} = F_{n+1}^3 + F_n^3 - F_{n-1}^3$ （∗）
6. $\displaystyle\sum_{k=1}^{n} F_k^2 = F_{n+1}F_n = \frac{F_{2n+1} - F_n^2}{2}$
7. $\displaystyle\sum_{k=1}^{n} F_kF_{k+1} = F_{n+1}^2 + \frac{1-(-1)^n}{2} = \frac{F_{n+1}^2 + F_n^2 - 1}{2} = \frac{F_{2n+1} - 1}{2}$

（∗）両辺とも F_n と F_{n-1} の 3 次式で書けるので、比較は易しい。

16 Lucas 数列

リュカ数列

定義 71

次の 2 項間漸化式で定義される数列をリュカ *(Lucas)* 数列と言う。

$$G_{n+2} = G_{n+1} + G_n$$

ただし、 $G_0 = 2,\ G_1 = 1$ とする。

最初の方を少し計算すると、
$G_0 = 2,\ G_1 = 1,\ G_2 = 3,\ G_3 = 4,\ G_4 = 7,\ G_5 = 11,\ \cdots$

命題 72

$n \in \mathbb{Z}$ について、$G_{-n} = (-1)^n G_n$

Lucas 数列

$G_0 = 2,\ G_1 = 1,\ G_2 = 3,\ G_3 = 4,\ G_4 = 7,\ G_5 = 11,\ G_6 = 18,\ G_7 = 29,\ G_8 = 47,\ G_9 = 76,\ G_{10} = 123,\ G_{11} = 199,\ G_{12} = 322,\ G_{13} = 521,\ G_{14} = 843,\ G_{15} = 1364,\ G_{16} = 2207,\ G_{17} = 3571,\ G_{18} = 5778,\ G_{19} = 9349,\ G_{20} = 15127,\ G_{21} = 24476,\ G_{22} = 39603,\ G_{23} = 64079,\ G_{24} = 103682,\ G_{25} = 167761,\ G_{26} = 271443,\ G_{27} = 439204,\ G_{28} = 710647,\ G_{29} = 1149851,\ G_{30} = 1860498,\ G_{31} = 3010349,\ G_{32} = 4870847,\ G_{33} = 7881196,\ G_{34} = 12752043,\ G_{35} = 20633239,\ G_{36} = 33385282,\ G_{37} = 54018521,\ G_{38} = 87403803,\ G_{39} = 141422324,\ G_{40} = 228826127,$

$G_{-1} = -1,\ G_{-2} = 3,\ G_{-3} = -4,\ G_{-4} = 7,\ G_{-5} = -11,\ G_{-6} = 18,\ G_{-7} = -29,\ G_{-8} = 47,\ G_{-9} = -76,\ G_{-10} = 123,\ G_{-11} = -199,\ G_{-12} = 322,\ G_{-13} = -521,\ G_{-14} = 843,\ G_{-15} = -1364,\ G_{-16} = 2207,\ G_{-17} = -3571,\ G_{-18} = 5778,\ G_{-19} = -9349,\ G_{-20} = 15127,$

様々な定理

定理 73

1. $G_n = x^n + (1-x)^n$
2. $x^{n+1} + x^{n-1} = G_n x + G_{n-1}$
3. $G_n = F_{n+1} + F_{n-1}$
4. $F_n = \frac{1}{5}(G_{n+1} + G_{n-1})$
5. $G_{m+n} = F_m G_{n+1} + F_{m-1} G_n$ (加法定理)
6. $F_{2n} = G_n F_n$

一般定理

定理 74 (一般解)

数列 $\{a_n\}_n$ が $a_{n+2} = a_{n+1} + a_n$ を満たすとき、次が成り立つ。

$$a_n = F_n a_1 + F_{n-1} a_0$$

定理 75 (一般加法定理 1)

数列 $\{a_n\}_n$ が $a_{n+2} = a_{n+1} + a_n$ を満たすとき、次が成り立つ。

$$a_{m+n} = F_m a_{n+1} + F_{m-1} a_n$$

定理 76 (一般加法定理 2)

$k_1, k_2, \cdots, k_t$ を定数とし、$a_n = k_1 F_n + k_2 F_{n+1} + \cdots + k_t F_{n+t-1}$ と置くと次が成り立つ。

$$a_{m+n} = F_m a_{n+1} + F_{m-1} a_n$$

様々な定理 (その 2)

定理 77

1. $2G_{m+n} = G_m G_n + 5F_m F_n$
2. $2F_{m+n} = F_m G_n + G_m F_n$
3. $5F_{m+n} = G_m G_{n+1} + G_{m-1} G_n$
4. $G_{2n} = {G_n}^2 - 2(-1)^n$
5. $G_{n+1} G_{n-1} - {G_n}^2 = (-1)^{n-1} 5$
6. $5{F_n}^2 = {G_n}^2 - 4(-1)^n$
7. $F_{n+m} + (-1)^m F_{n-m} = G_m F_n$
8. $F_{n+m} - (-1)^m F_{n-m} = F_m G_n$
9. $G_{n+m} + (-1)^m G_{n-m} = G_m G_n$
10. $G_{n+m} - (-1)^m G_{n-m} = 5F_m F_n$

17 素イデアルと極大イデアル

整域

定義 78 (整域)

環 R が次の条件を満たすとき、 整域という。

$$\forall a,\ b \in R\ a \cdot b = 0 \implies a = 0 \ \vee \ b = 0.$$

定理 79

体は整域である。

定理 80

$\mathbb{F}_0$, $\mathbb{F}$ は整域である。

(証明は後で)

素イデアル

定義 81 (素イデアル)

R と異なるイデアル $I \subset R$ が次の条件を満たすとき、 素イデアルという。

$$\forall a,\ b \in R\ a \cdot b \in I \implies a \in I \ \vee \ b \in I.$$

命題 82

イデアル $I \subset R$ に対して R/I が整域であるための必要十分条件は I が素イデアルであることである。

例 14

1. $R = \mathbb{Z},\ I = 3\mathbb{Z}$ のとき、I は素イデアル。
2. $R = \mathbb{Z},\ I = 4\mathbb{Z}$ のとき、I は素イデアルでない。

極大イデアル

定義 83 (極大イデアル)

R と異なるイデアル $I \subset R$ が次の条件を満たすとき、 極大イデアルという。

$I \subset J \subset R$ となるイデアル J は $J = I$ または $J = R$ のみである。

定理 84

R を環、I をその R と異なるイデアルとする。剰余環 R/I が体であることは、I が極大イデアルであることの必要十分条件である。

[証明]

- （十分性）R/I が体であるとする。J を I より真に大きい R のイデアルとする。$a \in J - I$ をとると $a \notin I$ なので、$[a] \neq 0$ ここで R/I が体であることから $[a]$ の逆元 $[b]$ が存在する。$[a][b] = [1]$ より $[ab - 1] = 0$ ゆえに $ab - 1 \in I \subset J$。一方 $ab \in J$ であるから、$1 \in J$ が言える。よって $J = R$。
- （必要性）I が極大イデアルだと仮定する。$I \neq R$ より R/I は $0 \neq 1$ の環である。今、$[a] \in R/I$, $[a] \neq 0$ を任意にとると、$a \notin I$ より $\langle a, I \rangle = R$。よってある $r \in R$ と $s \in I$ で $ra + s = 1$ となる。このとき、$[r][a] = [1] = 1$ すなわち $[r]$ は $[a]$ の逆元となっている。よって、R/I は、体である。

□

後で述べるように、素数 p に対して $p\mathbb{Z}$ は $\mathbb{Z}$ の極大イデアルである。

定義 85

p を素数とするとき、$\mathbb{Z}/p\mathbb{Z}$ を F_p と書き、標数 p の 素体という。

系 86

極大イデアルは素イデアルである。

18 1変数多項式環

1 変数多項式環

今後 k は体とする。実際には $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ と思っていてよい。$\mathbb{N} = \mathbb{Z}_{\geq 0} = \{0 \text{ 以上の整数}\}$ とする。

定義 87 (多項式環)

$k[x] = \{a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0 \mid \forall i\ a_i \in k,\ m \in \mathbb{N}\}$ に通常の和と積を定義したものを、k 上の *(1 変数)* 多項式環という。

定義 88

多項式 $f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0,\ (a_m \neq 0)$ について、次のように定義する。

- $\deg(f) = m$ $\cdots$ 次数 *(degree)*
- $\mathbf{LC}(f) = a_m$ $\cdots$ 先頭係数 *(leading coefficient)*
- $\mathbf{LM}(f) = x^m$ $\cdots$ 先頭単項式 *(leading monomial)*
- $\mathbf{LT}(f) = a_m x^m$ $\cdots$ 先頭項 *(leading term)*
- $\mathbf{RT}(f) = f - \mathbf{LT}(f)$ $\cdots$ 残余 *(rest term)*

命題 89

$f,\ g \neq 0$ について

1. $\deg(fg) = \deg(f) + \deg(g)$.
2. $f + g \neq 0 \ \Rightarrow\ \deg(f+g) \leq \max\{\deg(f),\ \deg(g)\}$.
3. $f + g \neq 0$ かつ $\deg(f) \neq \deg(g) \ \Rightarrow\ \deg(f+g) = \max\{\deg(f),\ \deg(g)\}$.

定義 90 (整除)

$f, g \in k[x], g \neq 0$ とする。ある $q \in k[x]$ が存在して $f = g \cdot q$ となるとき g は f を 割り切るといい、$g|f$ と書く。また、$q = f/g$ と書き、これを f の g による 商と言う。

補題 91

$f, g \neq 0$ とする。

1. $\deg(g) \leq \deg(f) \iff \mathbf{LT}(g)|\mathbf{LT}(f)$.
2. $\deg(g) \leq \deg(f), h = f - \dfrac{\mathbf{LT}(f)}{\mathbf{LT}(g)}g \Rightarrow h = 0 \vee (h \neq 0 \wedge \deg(f) > \deg(h))$.

割り算アルゴリズム

注 6

以下の議論は $k[x]$ で行っているが、$\mathbb{Z}$ でもほぼパラレルに話を進めることができる。その場合、$\deg(f)$ に相当するのものは、$|n|$(絶対値) である。

定理 92 (割り算アルゴリズム)

$f, g \in k[x], g \neq 0$ とする。f の g による 割り算とは次の条件を満たすものであり、以下に述べるアルゴリズムで得ることができる。

1. $f = g \cdot q + r, \quad q, r \in k[x].$
2. $r = 0 \vee (r \neq 0 \wedge \deg r < \deg g).$

```
Input : f, g
Output : q, r
  q := 0; r := f
  WHILE r != 0 AND LT(g) | LT(r) DO
    q := q + LT(r) / LT(g)
    r := r - ( LT(r) / LT(g) ) * g
```

また、(1), (2) を満たす q, r は一意である。

[証明] 略。□

例 16

$f = x^3 + 2x^2 + x + 1$ を $g = 2x + 1$ で割る過程を示す。

```
                  1/2x^2 + 3/4x + 1/8 ... 商
            ------------------------
2x + 1    |x^3 +   2x^2 +     x +   1
           x^3 + 1/2x^2
           ------------------------
                  3/2x^2 +     x +   1
                  3/2x^2 + 3/4x
                  --------------------
                           1/4x +   1
                           1/4x + 1/8
                                  ---
                                  7/8 ... 余り
```

定義 93 (商と余り)

上のアルゴリズムで求めた q, r に対し、q を 商と言い、f div g あるいは quotient(f, g) と書く。また、r を 余りあるいは 剰余と言い、$f \mod g$ あるいは remainder(f, g) と書く。

注 7

1. $f \mapsto (f \mod g)$ は、f に関する k 上の線形写像である。
2. $h \in k[x],\ h \neq 0 \implies h(f \mod g) = (hf) \mod (hg)$.

系 94

$g|f \iff f \mod g = 0.$

[証明] $\Leftarrow$ は明らか。 $\Rightarrow$ は、定理 92 の一意性より得られる。□

系 95 (因数定理)

1. $f \mod (x-a) = f(a).$
2. $(x-a)|f \iff f(a) = 0.$

系 96 (根の数)

$f(x) = 0$ の根の数は $\deg f$ 以下である。

定理 97 (1 変数多項式環のイデアルの性質)

$k[x]$ の任意のイデアルは単項イデアルである。

[証明] I を $k[x]$ の $\{0\}$ でない任意のイデアルとする。$I - \{0\}$ の中で deg が最小のものを h とすると、$I = \langle h \rangle$ である。なぜなら、$\langle h \rangle \subset I$ は明らか。$I \subset \langle h \rangle$ は、任意の $f \in I$ について、$r = f \mod h$ とすると、$r \in I$。もし $r \neq 0$ なら、$\deg r < \deg h$ となって $\deg h$ の最小性に矛盾。よって $r = 0$ がいえるから $h|f$。すなわち $f \in \langle h \rangle$。すなわち $I \subset \langle h \rangle$。□

定義 98 (単項イデアル整域, PID)

任意のイデアルが単項イデアルである整域を単項イデアル整域あるいは、*PID (Principal Ideal Domain)* と言う。

19 ユークリッドの互除法

GCD

定義 99

R を環とする。$f, g \in R$ について、f, g の 最大公約数 $GCD(f, g)$ *(gratest common devisor)* とは、以下の条件を満たす h のことを言う。

1. $h|f,\ h|g$. *(h は，f と g の公約数である。)*
2. $\forall p\ (p|f,\ p|g \ \Rightarrow\ p|h)$. *($f$ と g の公約数は h の約数である。)*

注 8

この定義は，最大公約数の「最大」という言葉を使わないように工夫したものである。$R = k[x]$ ならその deg が最大，$R = \mathbb{Z}$ なら，その絶対値が最大であると言える。

ユークリッドの互除法

定理 100 (ユークリッドの互除法)

$f, g \in k[x]$ について以下が成り立つ。

1. $GCD(f, g)$ が存在して $k[x]$ の単元を除いて一意である。
2. $\langle f, g \rangle = \langle GCD(f, g) \rangle$.
3. 次のアルゴリズムで $GCD(f, g)$ を求める事ができる。

```
Input : f, g
Output : h
  h := f
  s := g
  WHILE s != 0 DO
    r := remainder(h, s)
    h := s
    s := r
```

[証明] (1), (2): イデアル $\langle f, g \rangle$ は単項イデアルなので、$\langle f, g \rangle = \langle h \rangle$ となる h が存在する。この h は f と g の GCD である。なぜなら、$f, g \in \langle h \rangle$ より、$h|f, h|g$。また、もし $p|f, p|g$ ならば、$\langle f, g \rangle \subset \langle p \rangle$。よって $p|h$。よって, $h = GCD(f, g)$ であることが言えた。
また、h, h' が GCD なら $h|h'$ かつ $h'|h$ なので、h' は h の単元倍しか違わない。
(3): 略。□

例 17

1. $GCD(x^4 - 1,\ x^6 - 1) = x^2 - 1.$
2. $GCD(x^5 + 2x^3,\ x^4 + x^2 - x) = x.$

定義 101 (素)

$f, g \in k[x]$ が素であるとは、「$h|f$ かつ $h|g$ ならば h は単元」が言える事である。すなわち、$GCD(f, g)$ が単元であることである。これは、$\deg GCD(f, g) = 0$、$\langle f, g \rangle = k[x]$、$\langle f, g \rangle \ni 1$ と同値である。

定理 102

$f, g, h \in k[x]$、f と g が素とするとき、以下が成り立つ。

1. $f|h$ かつ $g|h$ ならば、$(fg)|h$。
2. $f|(gh)$ ならば $f|h$。

[証明]

1. $1 = af + bg$ となる $a, b \in k[x]$ があるので、
   $h = h \cdot 1 = h(af + bg) = ahf + bhg$ ここで、hf, hg が fg で割り切れる。
2. 同様に、$h = ahf + bhg$ を使って示すことができる。

□

$k[x]$ で、deg が n より小さいものと 0 をあわせて、$k[x]_{(n)}$ と書くことにする。

定理 103

$f,\ g \in k[x]$ が素であるとする。$m = \deg f,\ n = \deg g$ に対して、

$$\begin{aligned} \phi :\ k[x]_{(m)} \oplus k[x]_{(n)} &\to k[x]_{(m+n)} \\ (u,\ v) &\mapsto gu + fv \end{aligned}$$

と定義すると、これは k 上のベクトル空間の同型である。

[証明] 前定理 (2) より、ϕ は単射であることがわかる。ϕ のソースとターゲットの次元は、どちらも k 上 $m+n$ なので、ϕ は同型である。□

注 9

1. この定理は、次定理の前半を証明する。
2. $af + bg = 1$ となる $a,\ b \in k[x]$ を見つければ、$\phi^{-1}(w) = (bw \mod f,\quad aw \mod g)$ である。

定理 104 (拡張されたユークリッドの互除法)

$f,\ g \in k[x]$ について、

$$af + bg = GCD(f,\ g)$$

となる $a,\ b$ が

$$\begin{aligned} \deg a &< \deg g - \deg GCD(f,g), \\ \deg b &< \deg f - \deg GCD(f,g). \end{aligned}$$

という条件の下でただ一組存在する。
特に、f と g が素なら、

$$af + bg = 1$$

となる $a,\ b$ が $\deg a < \deg g,\ \deg b < \deg f$ という条件の下でただ一組存在する。

また、a, b は以下のアルゴリズムで求める事ができる:

```
Input : f, g (!= 0)
Output : h, a, b
  h, s := f, g
  a, b, c, d = 1, 0, 0, 1
  WHILE s != 0 DO
    q  := quotient(h, s)
    r  := h - qs
    r0 := a - qc
    r1 := b - qd
    h, s := s, r
    a, c := c, r0
    b, d := d, r1
```

[証明] (存在) $\boldsymbol{F}_i = \begin{pmatrix} F_i \\ F_{i+1} \end{pmatrix}$, $Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$ とおくと、
$F_{i+2} = F_i - q_i F_{i+1} \Longleftrightarrow \boldsymbol{F}_{i+1} = Q_i \boldsymbol{F}_i$。 ここで、
$R_i = Q_{i-1} Q_{i-2} \cdots Q_0$ とおけば、$\boldsymbol{F}_i = R_i \boldsymbol{F}_0$。 R_i は、
$R_0 = E$, $R_{i+1} = Q_i R_i$ で定められ、$R_i = \begin{pmatrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{pmatrix}$ と置けて、
$a_{i+2} = a_i - q_i a_{i+1}$, $b_{i+2} = b_i - q_i b_{i+1}$, $F_{i+2} = a_i F_i + b_i F_{i+1}$ が成り立つ。
さて、$F_0 = f$, $F_1 = g$ とおくと、ある n があって、
$F_n = GCD(F_0, F_1)$, $F_{n+1} = 0$。 すなわち、
$\begin{pmatrix} GCD(F_0, F_1) \\ 0 \end{pmatrix} = \boldsymbol{F}_n = R_n \boldsymbol{F}_0$。 このとき、
$GCD(F_0, F_1) = a_n F_0 + b_n F_1$, $0 = a_{n+1} F_0 + b_{n+1} F_1$ である。
また、$\deg F_0 \geq \deg F_1$ を仮定して良く、このとき、
$\deg q_i = \deg F_i - \deg F_{i+1}$。 また、帰納的に、
$\deg a_i = \deg F_1 - \deg F_{i-1}$ $(2 \leq i \leq n+1)$ と
$\deg b_i = \deg F_0 - \deg F_{i-1}$ $(1 \leq i \leq n+1)$ が言えるので、$i = n$ とすれば、次数の条件が言える。□

(一意性) $GCD(f,\ g) = 1$ としてよい。$af + bg = a'f + b'g = 1$ なら $(a - a')f = (b' - b)g$ なので、定理 102 より、
$f|(b' - b),\ g|(a - a')$ より $b' - b = a - a' = 0$。(多項の場合も OK な別証)
$a - a' = a(a'f + b'g) - a'(af + bg) = (ab' - a'b)g \equiv 0(\mod g)$。

注 10

1. $a_{n+1}F_0 = -b_{n+1}F_1 = LCM(F_0,\ F_1)$ となっている。
2. $a_0 = 1,\ a_1 = 0,\ a_2 = 1,\ a_3 = -q_1,\ a_4 = 1 + q_2q_1,\ a_5 = -q_1 - q_3 - q_3q_2q_1,\ a_6 = 1 + q_2q_1 + q_4q_1 + q_4q_3 + q_4q_3q_2q_1,$
$b_0 = 0,\ b_1 = 1,\ b_2 = -q_0,\ b_3 = 1 + q_1q_0,\ b_4 = -q_0 - q_2 - q_2q_1q_0,\ b_5 = 1 + q_1q_0 + q_3q_1 + q_3q_2 + q_3q_2q_1q_0,\ b_6 = -q_0 - q_2 - q_4 - q_2q_1q_0 - q_4q_1q_0 - q_4q_3q_1 - q_4q_3q_2 - q_4q_3q_2q_1q_0.$

系 105

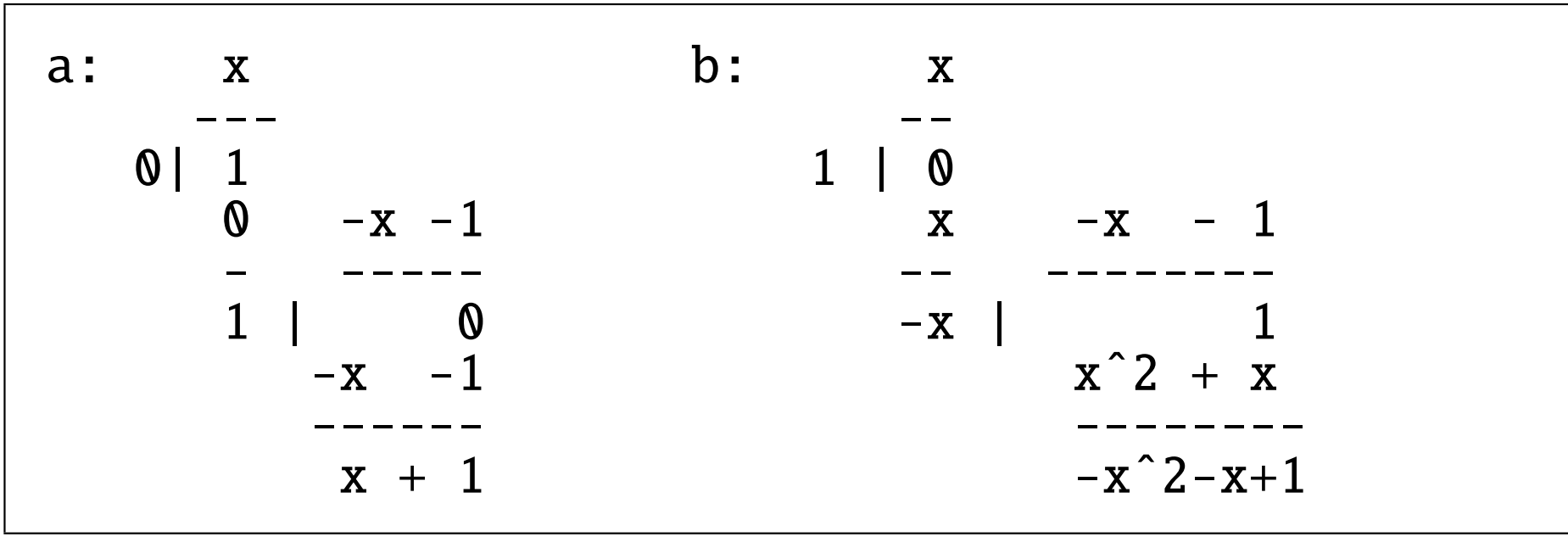
f, g が素であるとき、以下が成り立つ。

1. $\dfrac{1}{fg} = \dfrac{b}{f} + \dfrac{a}{g}$ となる a, b で $\dfrac{b}{f}, \dfrac{a}{g}$ が「真分数」になるものが一意に存在する。
2. $\deg h < \deg f + \deg g$ なら、$\dfrac{h}{fg} = \dfrac{b}{f} + \dfrac{a}{g}$ となる a, b で $\dfrac{b}{f}, \dfrac{a}{g}$ が「真分数」になるものが一意に存在する。

[証明] (1), (2) 共に容易。□

$f = x^4 - x^2$, $g = x^3 - 1$ について、
$GCD(f,\ g) = x - 1 = (x+1)f + (-x^2 - x + 1)g$.

```
                  x
          -------
x^3-1 | x^4-x^2
        x^4 - x      -x - 1
        -------    --------
         -x^2+x  | x^3 - 1
                   x^3-x^2
                   ---------
                   x^2 - 1
                   x^2 - x          -x
                   ---------   ---------
                     x - 1  | -x^2 + x
                              -x^2 + x
                              --------
                                     0
```


a:
x

0| 1
0 -x -1
- -----
1 | 0
-x -1
------
x + 1
b:
x
--
1 | 0
x -x - 1
-- --------
-x | 1
x^2 + x

-x^2-x+1

各ステージで次が成り立っていることに注目せよ。

$$
\begin{array}{rcrcrcrcr}
x^4-x^2 & = & 1 & \cdot & (x^4-x^2) & + & 0 & \cdot & (x^3-1) \\
x^3-1 & = & 0 & \cdot & (x^4-x^2) & + & 1 & \cdot & (x^3-1) \\
-x^2+x & = & 1 & \cdot & (x^4-x^2) & + & (-x) & \cdot & (x^3-1) \\
x-1 & = & (x+1) & \cdot & (x^4-x^2) & + & (-x^2-x-1) & \cdot & (x^3-1)
\end{array}
$$

例 18

1. $f = x^4 - 1,\ g = x^6 - 1$ について、
   $GCD(f,\ g) = x^2 - 1 = x^2 \cdot f + 1 \cdot g.$
2. $f = x^5 + 2x^3,\ g = x^4 + x^2 - x$ について、
   $GCD(f,\ g) = x = \frac{1}{3}(2x^2+x+1) \cdot f - \frac{1}{3}(2x^3+x^2+3x+3) \cdot g.$

既約元

定義 106 (既約元)

$a \in R$ について、「a の約数は自分自身か 1 のみ」のとき、すなわち「$a = bc,\ (b,\ c \in R)$ ならば b または c は単元」となるとき、a を 既約元という。

例 19

$\mathbb{Z}$ における既約元とは素数のことである。

命題 107

$R =$ あるいは $k[x]$ (k は体) あるいは *PID* とする。$p \in R$ が既約元なら、$R/\langle p \rangle$ は体である。

[証明] $[f] \in R/\langle p \rangle$, $[f] \neq 0$ とする。$p|f$ ではないので、$GCD(f,\ p) = 1$ である。（なぜなら、$h = GCD(f,\ p)$ とすると、$h|p,\ h|f$。 $h|p$ より $h = 1$ または $h = p$。$h = p$ とすると $p|f$ で矛盾。よって $h = 1$。）よって $af + bp = 1$ となる $a,\ b \in R$ が存在する。このとき $[a][f] = 1$ よって $[a]$ は $[f]$ の逆元になっている。□

素元の定義

定義 108 (素元)

$p \in R$ について「$p|(ab),\ (a,\ b \in R)$ ならば $p|a$ または $p|b$」となるとき、p を 素元という。

p が素元であることと $\langle p \rangle$ が素イデアルであることは、同値である。よって、命題 82 より、次が言える。

命題 109

$p \in R$ が素元であることと $\langle p \rangle$ が素イデアルであることと $R/\langle p \rangle$ が整域であることは、同値である。

既約元と素元の関係

定理 110

$\mathbb{Z}$ あるいは $k[x]$ あるいは *PID* において、既約元は素元である。

[証明] 命題 107 より、$p \in R$ が既約元なら $R/\langle p \rangle$ は体である。よって整域である。よって、命題 109 より、p は素元である。□

命題 111

整域において 0 でない素元は既約元である。

[証明] $p \neq 0$ を素元、$p = ab$ とする。$p|a$ または $p|b$ なので $p|a$ とすれば、$pu = a$ となる $u \in R$ が存在する。$p = pub$ よって $p(1 - ub) = 0$ よって $ub = 1$ すなわち b は単元である。$p|b$ の時も同様。□

注 11

上の命題より、$\mathbb{Z}$ あるいは $k[x]$ あるいは *PID* においては既約元と 0 でない素元は一致する。（実は $k[x_1, x_2, \cdots, x_n]$ においても既約元と 0 でない素元は一致する。）

例 20

$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ では $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ は既約元であるが、$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ なので、どれも素元ではない。つまり $\mathbb{Z}[\sqrt{-5}]$ は *PID* でない。

20 ユークリッドの互除法の応用

例 21

$\mathbf{F}_7 = \mathbb{Z}/7\mathbb{Z}$ で 3 の逆数を求める。
拡張されたユークリッドの互除法 (整数版) より、
$7 + (-2)3 = 1$。よって、$3^{-1} = -2 = 5$。

乗法群

R を環とするとき、$R^\times$ を R の可逆元全体とするのであった。
$R^\times$ はかけ算で群をなす。
$(\mathbb{Z}/7\mathbb{Z})^\times = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

これを $\mathbb{Z}/7\mathbb{Z}$ の乗法群と言う。

$$10a + b = 0 \ \Leftrightarrow\ 2(10a + b) = 0 \ \Leftrightarrow\ -a + 2b = 0$$

中国式剰余定理

定理 112

R を環とし、$f, g \in R, af + bg = 1$ とすると、以下が成り立つ。

1. $$\begin{aligned} \pi : R/\langle fg \rangle &\to R/\langle f \rangle \oplus R/\langle g \rangle \\ [x] &\mapsto ([x], [x]) \end{aligned}$$

   は加群の同型写像であり、$\pi^{-1}([x], [y]) = [bgx + afy]$ である。

2. $$\begin{aligned} \phi : R/\langle fg \rangle &\to R/\langle f \rangle \oplus R/\langle g \rangle \\ [x] &\mapsto ([bx], [ax]) \end{aligned}$$

   は加群の同型写像であり、$\phi^{-1}([x], [y]) = ([gx + fy])$ である。

【証明】

1. π, π^{-1} の well-definedness は明らか。
   $\pi^{-1} \circ \pi([x]) = \pi^{-1}([x], [x]) = [bgx + af x] = [(bg + af)x] = [x]$。
   $\pi \circ \pi^{-1}([x], [y]) = \pi([bgx + afy]) = ([bgx + afy], [bgx + afy]) = ([(af + bg)x], [(af + bg)y]) = ([x], [y])$。
2. ϕ, ϕ^{-1} の well-definedness は明らか。
   $\phi^{-1} \circ \phi([x]) = \phi^{-1}([bx], [ax]) = [gbx + fax] = [(gb + fa)x] = [x]$。
   $\phi \circ \phi^{-1}([x], [y]) = \phi([gx + fy]) = ([b(gx + fy)], [a(gx + fy)]]) = ([(af + bg)x], [(af + bg)y]) = ([x], [y])$。

中国式剰余定理

【問】17 で割った余りが 13、5 で割った余りが 4 である整数を求めなさい。

【答】拡張されたユークリッドの互除法で、
$-2 \cdot 17 + 7 \cdot 5 = 1$
を得る。定理 112 より 17 で割った余りが x、5 で割った余りが y である自然として、

$$n = 7 \cdot 5 \cdot x + (-2) \cdot 17 \cdot y$$

が取れる。ここでは、$n = 7 \cdot 5 \cdot 13 + (-2) \cdot 17 \cdot 4 = 319$。
答えは、$\mathrm{remainder}(319, 17 \cdot 5) = 64$。

中国式剰余定理 (フィボナッチ数版)

【問】377 で割った余りが 13、233 で割った余りが 7 である整数を求めなさい。

【答】$-144 \cdot 377 + 233 \cdot 233 = 1$ より、 377 で割った余りが x、233 で割った余りが y である自然として、

$$n = 233 \cdot 233 \cdot x + (-144) \cdot 377 \cdot y$$

が取れる。
よって、$n = 233 \cdot 233 \cdot 13 + (-144) \cdot 377 \cdot 7 = 325741$。
答えは、$\mathrm{remainder}(325741, 377 \cdot 233) = 62218$。
ちなみに、$F_{12} = 144,\ F_{13} = 233,\ F_{14} = 377$ であるが…（次ページ）

フィボナッチ数とユークリッドの互除法

隣り合う 2 つのフィボナッチ数、F_{n+1}, F_n は、最もユークリッドの互除法が苦手とするペアである。(除算の回数が $n-1$ 回になる。)
しかし、$F_{n-1}F_{n+1} - {F_n}^2 = (-1)^n$ であるから、$aF_{n+1} + bF_n = 1$ となる a, b として、$a = (-1)^n F_{n-1}$, $b = (-1)^{n-1} F_n$ が取れる。

中国式剰余定理3項バージョン

定理 113

R を環とし、$f,\ g,\ h \in R,\ agh + bfh + cfg = 1$ とすると、以下が成り立つ。

1. $$\begin{aligned} \pi :\ R/\langle\, fgh \,\rangle &\to R/\langle\, f \,\rangle \oplus R/\langle\, g \,\rangle \oplus R/\langle\, h \,\rangle \\ [x] &\mapsto ([x],\ [x],\ [x]) \end{aligned}$$

   は加群の同型写像であり、
   $\pi^{-1}([x],\ [y],\ [z]) = [aghx + bfhy + cfgz]$ である。

2. $$\begin{aligned} \phi :\ R/\langle\, fgh \,\rangle &\to R/\langle\, f \,\rangle \oplus R/\langle\, g \,\rangle \oplus R/\langle\, h \,\rangle \\ [x] &\mapsto ([ax],\ [bx],\ [cx]) \end{aligned}$$

   は加群の同型写像であり、
   $\phi^{-1}([x],\ [y],\ [z]) = ([ghx + fhy + fgz])$ である。

【証明】

1. π, π^{-1} の well-definedness は明らか。
   $\pi^{-1} \circ \pi([x]) = \pi^{-1}([x], [x], [x]) = [aghx + bfhx + cfgx] =$
   $[(agh + bfh + cfg)x] = [x]$。
   $\pi \circ \pi^{-1}([x], [y], [z]) = \pi([aghx + bfhy + cfgz]) =$
   $([aghx + bfhy + cfgz], [aghx + bfhy + cfgz], [aghx +$
   $bfhy + cfgz]) = ([(agh + bfh + cfg)x], [(agh + bfh +$
   $cfg)y], [(agh + bfh + cfg)z]) = ([x], [y], [z])$。
2. ϕ, ϕ^{-1} の well-definedness は明らか。
   $\phi^{-1} \circ \phi([x]) = \phi^{-1}([ax], [bx], [cx]) =$
   $[ghax + fhbx + fgcx] = [(agh + bfh + cfg)x] = [x]$。
   $\phi \circ \phi^{-1}([x], [y], [z]) = \phi([ghx + fhy + fgz]) =$
   $([a(ghx + fhy + fgz)], [b(ghx + fhy + fgz)], [b(ghx +$
   $fhy + fgz)]) = ([(agh + bfh + cfg)x], [(agh + bfh +$
   $cfg)y], [(agh + bfh + cfg)z]) = ([x], [y], [z])$。

【問】17 で割った余りが 13、5 で割った余りが 4、8 で割った余りが 1 である整数を求めなさい。

【答】拡張されたユークリッドの互除法で、
$7 \cdot 5 + (-2) \cdot 17 = 1$
$32 \cdot 8 + (-3) \cdot 5 \cdot 17 = 1$
を得る。よって、
$32 \cdot 7 \cdot 5 \cdot 8 + 32 \cdot (-2) \cdot 17 \cdot 8 + (-3) \cdot 5 \cdot 17 = 1$
すなわち、
$224 \cdot 5 \cdot 8 + (-64) \cdot 17 \cdot 8 + (-3) \cdot 5 \cdot 17 = 1$
を得る。
定理 113 より 17 で割った余りが x、5 で割った余りが y、8 で割った余りが z である自然数として、

$$n = 224 \cdot 5 \cdot 8 \cdot x + (-64) \cdot 17 \cdot 8 \cdot y + (-3) \cdot 5 \cdot 17 \cdot z$$

が取れる。ここでは、
$n = 224 \cdot 5 \cdot 8 \cdot 13 + (-64) \cdot 17 \cdot 8 \cdot 4 + (-3) \cdot 5 \cdot 17 \cdot 1 = 81409$。
答えは、$\mathrm{remainder}(81409, 17 \cdot 5 \cdot 8) = 489$。

逆数・分母の有理化

例 22

$\mathbb{Q}[x]/\langle x^2-2\rangle$ で x^2+x+1 の逆数を求める。
拡張されたユークリッドの互除法より、
$(x-2)(x^2-2)+(-x+3)(x^2+x+1)=7.$ よって、
$[x^2+x+1]^{-1}=\frac{1}{7}[-x+3]$。
このことから、$\dfrac{1}{\sqrt{2}^2+\sqrt{2}+1}=\dfrac{1}{7}(-\sqrt{2}+3).$

微分方程式の解法

例 23

微分方程式 $y'' - y' - y = x^2$ の特殊解を求める。

$D = \dfrac{d}{dx}$ と置く。$D^2 - D - 1$ と D^3 について、拡張されたユークリッドの互除法により、

$$(-2D^2 + D - 1)(D^2 - D - 1) + (2D - 3)D^3 = 1.$$

よってこれを x^2 に左から作用させると、

$$(-2D^2 + D - 1)(D^2 - D - 1)x^2 + (2D - 3)D^3 x^2 = x^2.$$

よって、

$$(D^2 - D - 1)(-2D^2 + D - 1)x^2 = x^2.$$

すなわち、$y = (-2D^2 + D - 1)x^2 = -4 + 2x - x^2$ とおけば、

$$(D^2 - D - 1)y = y'' - y' - y = x^2.$$

〔練習問題〕$y'' - y' - y = \sin x$.　(ヒント:
$(D-2)(D^2 - D - 1) + (-D + 3)(D^2 + 1) = 5$.)