情報数学Ⅰ

第 9 回「代数構造-体」

3-3 体 (field)

<keywords>

① 体

集合Fに加法演算+および乗法演算×が定義され、次の 2 つの条件を満たす集合Fを体という。

(1) Fは単位元をもつ環である。 (加法、減法、乗法が定義される)

(2) Fは零元oを除いた集合は可換群をなす。(除法 x/y は、xに乗法逆元y^{-1}を乗算したものである。零元(加法単位元o)による除法を除いている)

有理数全体の集合$\mathbb{Q}$	…	有理数体
実数全体の集合$\mathbb{R}$	…	実数体
複素数全体の集合$\mathbb{C}$	…	複素数体

② 有限体 (finite field), ガロア体 (Galois field)

要素の数が有限な体をガロア体、または、有限体といい、要素の数がqであるガロア体を$GF(q)$で表す。

(注) 有限体は有限の要素で四則演算ができる。

③ 素体 (prime field)

要素の数qが素数であるガロア体を素体といい、$GF(P)$で表す。すなわち、$GF(P) = \{0,1,2,3,\cdots,P-1\}$であり、四則演算は以下の定義で表される。

$\forall x, y \in GF(P)$に対して

加算: $x + y \pmod{P}$

(意味) 通常の加算 $x + y$ を P で割った余りをその値とする。

乗算: $x \times y \pmod{P}$

(意味) 通常の乗算$x \times y$をPで割った余りをその値とする。

減算: $x + (-y) \pmod{P}$

(意味) xにyの加法逆元$-y$を加算した値をPで割った余りをその値とする。

除算: $x \times (y^{-1}) \pmod P$
(意味) xにyの乗法逆元y^{-1}を乗算した値をPで割った余りをその値とする。

(注) 有限体は素数Pによる余りをその値とするので、大小関係は成り立たない。

(例) ガロア体 $GF(5) = \{0,1,2,3,4\}$の加算表、乗算表を作成せよ。また、加法および乗法の逆元を求め、減算表、除算表を作成せよ。
(解) 5は素数であるので、$GF(5)$は素体である。
加算表 $(x + y \pmod 5)$

$x \setminus y$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

乗算表 $(x \times y \pmod 5)$

$x \setminus y$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

加法逆元

x	$-x$
0	0
1	4
2	3
3	2
4	1

減算表 $(x + (-y) \pmod 5)$

$x \setminus y$	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

(注) 体の定義よりy^{-1}は加法単位元（零元0)を除く。

乗法逆元（$x \cdot x^{-1} = 1 \pmod 5$）（1は乗法単位元）

x	x^{-1}
1	1
2	3
3	2
4	4

除算表（$x \times (y^{-1}) \pmod 5$)

$x \setminus y$	1	2	3	4
0	0	0	0	0
1	1	3	2	4
2	2	1	4	3
3	3	4	1	2
4	4	2	3	1

『ガロア体の理論は符号理論(誤り訂正)、暗号理論に用いられる』