教育課題演習　第 5 回　GF(2)上の多項式

1．GF(2)

加減乗除のすべてについて閉じた代数系を体(field)という（除算は 0 で割ることを除く）。要素の個数が有限の体をガロア体(Galois filed)といい，要素の個数が n のガロア体を GF(n)で表す。

2 を法とする剰余系は体としての条件を満たすので，GF(2)と書かれる。

GF(2)の演算

a \ b	0	1
0	0	1
1	1	0

$a+b$

a \ b	0	1
0	0	0
1	0	1

$a\times b$

GF(2)において，2=0，-1=1，$a+a=0$，$-a=a$，$a-b=a+b$ などの等式が成立する。

Note. 以後，⊕を＋で表す。

2．GF(2)上の多項式

GF(2)の要素 $a_0, a_1, \cdots, a_n$ を係数とする多項式 $a_0+a_1x+\cdots+a_nx^n$ を GF(2)上の多項式という。GF(2)上の多項式にも，通常のやり方で加法と乗法を定義する。

例

$(1+x)+(1+x+x^2)=2+2x+x^2 = x^2$

$(1+x)(1+x+x^2) = (1+x+x^2)+x(1+x+x^2) = 1+x+x^2+x+x^2+x^3 = 1+2x+2x^2+x^3 = 1+x^3$

問題 1

次の計算をしなさい。

$(1+x)(1+x^2)$

$(1+x)(1+x+x^2+x^3)$

$(1+x+x^2)(1+x^2+x^3+x^4)$

$(1+x)^2$

$(1+x)^3$

$(1+x)^4$

$(1+x)^5$

Note. 多項式と，多項式で表される関数とは異なる。

GF(2)上，$f(x)=1+x$ で定義される関数 f と $g(x)=1+x^2$ で定義される関数 g について $f=g$ であるが，$1+x$ と $1+x^2$ は異なる多項式である。　別のいい方をすると，$1+x=1+x^2$ は GF(2)上の恒等式であるが，$1+x$ と $1+x^2$ は多項式としては異なるものである。

問題 2　多項式を多項式で割って商と余りを求める割り算は可能か。

たとえば，x^3+x+1 を x^2+1 で割ってみよう。

問題 3　因数定理は成立するだろうか。すなわち，多項式 $P(x)$において，

$P(0)=0$ であれば $P(x)$は x を因数に持つ

$P(1)=0$ であれば $P(x)$は $x+1$ を因数に持つ

といえるだろうか。

問題 4　2 つの 1 次以上の多項式の積で表せない 1 次以上の多項式を既約多項式という。1 次，2 次，3 次，4 次の既約多項式をすべて求めよ。

問題 5　$1+x^5$，$1+x^7$ を既約多項式の積に因数分解せよ。