教育課題演習　第 9 回　有限体 GF(2)の拡大

1．拡大体を作る

多項式の根

多項式に含まれる文字に代入したとき，多項式の値が 0 となるものを，多項式の根という。別のいい方をすると，多項式の根とは，多項式＝0 の解のこと。

複素数体

x^2+1 は実数係数の多項式として既約である。x^2+1 の根を i で表し，実数体に i を付け加えて複素数体が得られた。

GF(2)の拡大

同様の手法で，GF(2)の拡大体を作る。

$1+x+x^2$ は GF(2)上の多項式として既約である。$1+\alpha+\alpha^2=0$ となる α（アルファ）を GF(2)に追加する。

問題 1

(1)　$\{0, 1, \alpha, \alpha^2\}$は体であることを示せ。

ヒント　$\alpha^2=1+\alpha$

$a+b$

a \ b	0	1	α	$1+\alpha$
0	0	1		
1	1	0		
α				
$1+\alpha$				

$a\times b$

a \ b	0	1	α	$1+\alpha$
0	0	0		
1	0	1		
α				
$1+\alpha$				

(2)　$\{0, 1, \alpha, 1+\alpha\}$上で $1+x+x^2$ を因数分解せよ。

ヒント　$1+x+x^2 = 1+x+x^2-(1+\alpha+\alpha^2)= x-\alpha+x^2-\alpha^2$

(3)　$\{0, 1, \alpha, 1+\alpha\}$における原始根を求めよ。

(4)　$\{0, 1, \alpha, 1+\alpha\}$上で $x^3-1(=x^3+1)$を因数分解せよ。

問題 2

$1+x+x^3$ は GF(2)上の既約多項式である。$1+\alpha+\alpha^3=0$ となる α を GF(2)に追加することで GF(2)の拡大体を作ることができるか。そのとき，x^3+x+1, x^3+x^2+1 はどう因数分解されるか。また，原始根をすべて求めよ。x^7-1 を因数分解せよ。

ヒント　$\alpha^3=1+\alpha$ を土台として，$\alpha^4, \alpha^5, \alpha^6,\cdots$ を計算してみる。

$a+b$

a \ b	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0	0	1						
1	1	0						
α								
$1+\alpha$								
α^2								
$1+\alpha^2$								
$\alpha+\alpha^2$								
$1+\alpha+\alpha^2$								

$a\times b$

a \ b	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0	0	0						
1	0	1						
α								
$1+\alpha$								
α^2								
$1+\alpha^2$								
$\alpha+\alpha^2$								
$1+\alpha+\alpha^2$								

x^3+x+1 =

x^3+x^2+1 =

x^7-1=

問題 3

$1+x^2+x^3$ は GF(2)上の既約多項式である。$1+\beta^2+\beta^3=0$ となる β を GF(2)に追加することで GF(2)の拡大体を作ることができるか。そのとき，x^3+x+1, x^3+x^2+1 はどう因数分解されるか。また，原始根をすべて求めよ。x^7-1 を因数分解せよ。

$a+b$

a \ b	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
0	0	1						
1	1	0						
β								
$1+\beta$								
β^2								
$1+\beta^2$								
$\beta+\beta^2$								
$1+\beta+\beta^2$								

$a\times b$

a \ b	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
0	0	0						
1	0	1						
β								
$1+\beta$								
β^2								
$1+\beta^2$								
$\beta+\beta^2$								
$1+\beta+\beta^2$								

x^3+x+1 =

x^3+x^2+1 =

x^7-1=

問題 4

$1+x+x^4$ は GF(2)上の既約多項式である。$1+\alpha+\alpha^4=0$ となる α を GF(2)に追加することで GF(2)の拡大体を作ることができるか。そのとき，$1+x+x^4$ と $x^{15}-1$ を因数分解せよ。

ヒント　α^4，α^5，α^6，… を 1, α，α^2，α^3 の和で表す。

$\alpha^4=1+\alpha$　　α^{10}=

α^5=　　α^{11}=

α^6=　　α^{12}=

α^7=　　α^{13}=

α^8=　　α^{14}=

α^9=　　α^{15}=

$a+b$

	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0																
1																
α																
α^2																
α^3																
α^4																
α^5																
α^6																
α^7																
α^8																
α^9																
α^{10}																
α^{11}																
α^{12}																
α^{13}																
α^{14}																

問題 5

$1+x^2+x^4$ は GF(2)上に根を持たない。$1+\alpha^2+\alpha^4=0$ となる α を GF(2)に追加することで GF(2)の拡大体を作ることができるか。