1.12.2 $f(x) \in \mathbb{F}_2[x]$ が5次の可約多項式であるとする.

$f(x)$ が1次の因子を持つとき

$\Leftrightarrow \exists \alpha \in \mathbb{F}_2,\ f(\alpha) = 0$ である.

ここで $f(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e$

$(a, b, c, d, e \in \mathbb{F}_2)$ とおくと

$\alpha = 0$ のとき $f(0) = e$, $\alpha = 1$ のとき $f(1) = a+b+c+d+e+1$

よって $f(x)$ が1次の因子を持って可約 $\Leftrightarrow e = 0$ or $a+b+c+d+e+1 = 0$

次に $f(x)$ が1次の因子を持たずに可約のとき

$f(x) = (2次) \times (3次)$ で表され, 因子はそれぞれ既約

(2次) については例. 1通り, $(0,1,1)$ x^2+x+1 と分かっているので

(3次) の既約多項式について調べる

$g(x) \in \mathbb{F}_2[x]$ が3次可約多項式である.

$\Leftrightarrow g(x)$ は1次の因子を持つ

$\Leftrightarrow \exists \alpha \in \mathbb{F}_2,\ g(\alpha) = 0$

$\Leftrightarrow u = 0$ or $s+t+u+1 = 0$

(ここで, $g(x) = x^3 + sx^2 + tx + u$ $(s,t,u \in \mathbb{F}_2)$ とおいた.)

特に, 3次の既約多項式は $u = 1$ かつ $s+t+u = 0$ より

x^3+x^2+1, x^3+x+1

よって この場合の5次の可約多項式は,

$(x^2+x+1)(x^3+x^2+1) = x^5+x+1$, $(x^2+x+1)(x^3+x+1) = x^5+x^4+1$

この場合分けより 求める多項式は,

x^5+x^2+1 $(0,0,1)$, x^5+x^3+1 $(0,1,0)$

$x^5+x^3+x^2+x+1$ $(0,1,1)$, $x^5+x^4+x^2+x+1$ $(1,0,1)$

$x^5+x^4+x^3+x+1$ $(1,1,0)$, $x^5+x^4+x^3+x^2+1$ $(1,1,1)$

既約の条件は $(e=0$ or $a+b+c+d+e+1=0)$ or $(x^5+x+1$ or $x^5+x^4+1)$ の否定なので:

ここで $e=1$ かつ $a+b+c+d = 1$ かつ x^5+x+1, x^5+x^4+1 でない,

$a+b+c+d=1$ は (a,b,c) を決めると解が定まるので

(a,b,c) の組合せだけ $a+b+c+d=1$ の解の個数がある

ことに注目し, x^5+x+1 と x^5+x^4+1 の

2つが除外されるので:

求める多項式の個数は 6個と分かる.

また (a,b,c) によって分けると分かりやすい

(2) $f(x) \in \mathbb{F}_3[x]$ を 2次のモニック可約多項式とすると
一次の因子をもつので $f(0)=0$ or $f(1)=0$ or $f(2)=0$

よって $f(x) = x^2+ax+b$ $(a, b \in \mathbb{F}_3)$ とすると

$f(0)=0$ より $b=0$

$f(1)=0$ より $1+a+b=0$

$f(2)=0$ より $1+2a+b=0$

故に $f(x)$ が可約 $\Leftrightarrow$ $b=0$ or $1+a+b=0$ or $1+2a+b=0$

従って $f(x)$ が既約 $\Leftrightarrow$ $b=1,2$ かつ $1+a+b=1,2$ かつ $1+2a+b=1,2$

$b=1$ のとき $a+2=1,2$ かつ $2a+2=1,2$ を満たす a は $a=0$ のみ.

$b=2$ のとき $a=1,2$ かつ $2a=1,2$ を満たす a は $a=1,2$.

これより 求める既約多項式は $x^2+1,\ x^2+x+2,\ x^2+2x+2.$ OK

(3) $f(x) \in \mathbb{F}_3[x]$ を4次のモニック既約多項式とする.
(2) より $f(x)$ が満たすべき条件は
$f(0) \neq 0$ かつ $f(1) \neq 0$ かつ $f(2) \neq 0$
かつ $x^2+1,\ x^2+x+2,\ x^2+2x+2$ のどれでも割り切れないことである

$f(x) = x^4+ax^3+bx^2+cx+d$ $(a, b, c, d \in \mathbb{F}_3)$ とおくと

$f(0) \neq 0$ より $d \neq 0$

$f(1) \neq 0$ より $a+b+c+d \neq 2$

$f(2) \neq 0$ より $2a+b+2c+d \neq 2$

これらを連立方程式として解くと $a+c \neq 0$ $b \neq 2,\ d \neq 0$

また、4次式で $x^2+1,\ x^2+x+2,\ x^2+2x+2$ のどれかで割り切れ、1次の因子を持たないものは
$x^2+1,\ x^2+x+2,\ x^2+2x+2$ を用いた積で表される.

よって それらを書き出すと

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

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

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

$a+c=1$

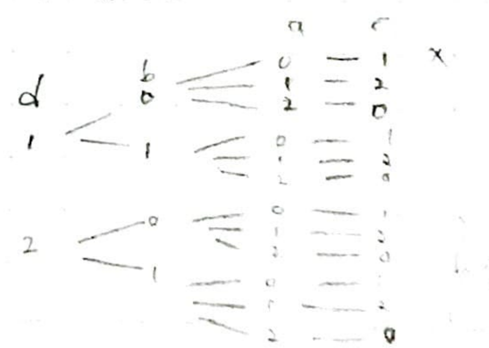
これらの条件より 求める多項式は

x^4+x+2, OK $x^4+x^3+2x+2.$

$x^4+2x^3+2,$ $x^4+x^2+x+2.$

$x^4+x^3+x^2+2x+2.$

だらいOK?



(4). (1)の多項式を5つ挙げればよい. OK