0716074
蔡育呈 ^^

1. Demonstrate whether each of these statements is true or false for polynomials over a field.

(a) The product of monic polynomials is monic. (5%)

(b) The product of polynomials of degrees m and n has degree $m+n$. (5%)

(c) The sum of polynomials of degrees m and n has degree $\max\{m,n\}$. (5%)

(a) let $f_1(x) = 1\cdot x^n + \sum_{k=1}^{n} a_k x^{n-k}$

$f_2(x) = 1\cdot x^m + \sum_{k=1}^{m} b_k x^{m-k}$,

$f_1(x)\cdot f_2(x) = 1\cdot x^{n+m} + \cdots$

已知領導係數 $=1$ 且 $1^{-1}=1$ in any field, $\Rightarrow$ True

(b) let $f_1(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$

$f_2(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$

$f_1(x)\cdot f_2(x) = a_0b_0\, x^{m+n} + \cdots$ (decreasing order)

because the polynomials are over a field, it's impossible to find zero diviser over a field; thus, $a_0 b_0 \neq 0$

$\therefore \deg(f_1(x)\cdot f_2(x)) = m+n$ # $\Rightarrow$ True

(c) let $m=n$

and $f_1(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m = f_2(x)$ over $GF(2)$

$f_1(x) + f_2(x) = 2(a_0x^m + a_1x^{m-1} + \cdots + a_m) = 0$ over $GF(2)$

$\therefore \deg(f_1(x) + f_2(x)) = 0 \neq \max\{m,n\}$ $\Rightarrow$ False

2. Determine which of the following polynomials are reducible over $GF(2)$.

(a) x^2+1. (5%)

(b) x^2+x+1. (5%)

(c) x^4+x+1. (5%)

(a) let $f(x) = x^2+1$

$f(0) = 0+1 = 1$

$f(1) = 1+1 = 2 \equiv 0$ over $GF(2)$

$x^2+1 = (x+1)(x+1)$ over $GF(2)$ $\therefore$ reducible

(b) let $f(x) = x^2+x+1$

$f(0) = 0+0+1 = 1$

$f(1) = 1+1+1 = 3 \equiv 1$ over $GF(2)$ $\therefore$ irreducible

(c) let $f(x) = x^4+x+1$

$f(0) = 0+0+1 = 1$

$f(1) = 1+1+1 = 3 \equiv 1$ over $GF(2)$ $\therefore$ irreducible

3. Determine the gcd of the following pairs of polynomials.

(a) $(x^3 + x + 1)$ and $(x^2 + 1)$ over $GF(3)$. (5%)

(b) $(x^3 - 2x + 1)$ and $(x^2 - x - 2)$ over $GF(5)$. (5%)

(a)

$$\begin{array}{r|l} & x \\ \hline x^2+1 & x^3+x+1 \\ & x^3+x \\ \hline & 1 \end{array} \qquad \begin{array}{r|l} & x^2+1 \\ \hline 1 & x^2+1 \\ & x^2+1 \\ \hline & 0 \end{array}$$

$\therefore$ gcd of two polynomials over $GF(3)$ is 1 #

(b)

$$\begin{array}{r|l} & x+1 \\ \hline x^2-x-2 & x^3-2x+1 \\ & x^3-x^2-2x \\ \hline & x^2+1 \\ & x^2-x-2 \\ \hline & x+3 \end{array} \qquad \begin{array}{r|l} & x-4 \\ \hline x+3 & x^2-x-2 \\ & x^2+3x \\ \hline & -4x-2 \\ & -4x-12 \\ \hline & 0 \end{array}$$

$\therefore$ gcd of two polynomials over $GF(3)$ is $x+3$

4. Determine the multiplicative inverse of $x^2 + 1$ in $GF(2^3)$ with $m(x) = x^3 + x - 1$. (10%)

$$GF(2^3) = \mathbb{Z}_2[x]/\langle x^3+x-1\rangle = \{0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1\}$$

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

$$\begin{array}{r|l} & 1 \\ \hline x^3+x-1 & x^3+x \\ & x^3+x-1 \\ \hline & 1 \end{array}$$

$\therefore$ inverse of x^2+1 in $GF(2^3)$: x #

5. Develop a set of tables similar to Table 5.3 for $GF(4)$ with $m(x) = x^2 + x + 1$. (10%)

$$GF(2^2) = \mathbb{Z}_2[x]/\langle x^2+x+1\rangle = \{0, 1, x, x+1\}$$

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

#

$$\begin{array}{r|l} & 1 \\ \hline x^2+x+1 & x^2+x \\ & x^2+x+1 \\ \hline & 1 \end{array}$$

×	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$$\begin{array}{r|l} & 1 \\ \hline x^2+x+1 & x^2 \\ & x^2+x+1 \\ \hline & x+1 \end{array}$$