## P O L I N O M I O S

**E71.** En Bachillerato y en el curso de MAT1111 se define a veces un polinomio como "una función racional entera" es decir una función $R \to R$ cuya ley de correspondencia actúa por medio de las operaciones de suma algebráica y multiplicación.
**Explique** por qué esta definición no es conveniente para definir un polinomio con coeficientes en un cuerpo cualquiera.

**E72.**- Proporcione ejemplos de : un cuerpo K y un polinomio no nulo, f, de manera que f represente la función nula $K \to K$.

**E73.**- En cada uno de los siguientes casos, exprese el máximo común divisor de los polinomios indicados como combinación lineal de los mismos;
a título de ejemplo :
Sean, en $Z_5[x]$ , $a=x^2-1$, $b=x^2+x$, $c=x^3-x^2$ ;
$(a, b, c)= 1 = (-1)(2x^2+2x+1)a-2b+(-3x-1)c$.
**a**) en $Z_7[x]$ , $a=x^2-1$, $b=x^2+x$ ;
**b**) en $Z_3[x]$ , $a=x^3-1$, $b=2x^2-2x$ ;
**c**) en $Z_7[x]$ , $a=x^2+2x+1$, $b=x^4+x^3$ ;
**d**) en $Z_2[x]$ , $a=x^2-1$, $b=x^2+x$, $c=x^3-x^2$ .

**E74.**- Halle todos los polinómios mónicos irreducibles de segundo grado :
**a**) En $Z_2[x]$ ;
**b**) En $Z_3[x]$ ;
**c**) En $Z_5[x]$ .

**E75.**- demuestre que para todo primo p hay exáctamente $\frac{p(p-1)}{2}$ polinomios mónicos irreducibles de segundo grado en $Z_p[x]$.
[sugerencia : cuente el número de polinomios mónicos reducibles de segundo grado]

**E76.**- En $Z_2[x]$, **i**)halle los dos polinomios mónicos irreducibles de grado 3 ;
**ii**) Halle los tres polinomios mónicos irreducibles de grado 4.

**E77.**-Sean a, b, c, d, f polinomios mónicos, irreducibles, de grado $\geq 1$ en $Z_7[x]$ ; demuestre sin usar el teorema de factorización única que es imposible que $abc=df$ .

**E78.**- El teorema fundamental del álgebra afirma que :
" en el dominio de integridad **C**[x] de los polinomios con coeficientes complejos, todo polinomio de grado $\geq 1$ tiene almenos un cero ";
**i**) admitiendo el teorema fundamental del álgebra , demuestre que todo polinomio con coeficientes complejos se factoriza en producto de factores de primer grado;
**ii**) factorice en producto de factores de primer grado a cada uno de los siguientes polinomios, en **C**[x] :
**iia)** $x^2+3x+1$ ; **iib**) $2x^4-2$ ; **iic**) $x^4+x^2+1$ ; **iid**) $x^3+x-2$ ; **iie**) $3x^6-3$

**E79.-** Demuestre que la función **c** : **C**→**C** que asocia a todo número complejo su conjugado, [ es decir : **c**(a+ib)=a-ib ] es un isomorfismo de cuerpos.
[ Nota : una función **c**, cuyo dominio y codominio son anillos [en particular cuerpos], se llama un homomorfismo si y sólo si **c**(x+y)=**c**(x)+**c**(y) , **c**(xy)=**c**(x)**c**(y) para toda escogencia de los elementos x, y en el dominio; un homorfismo biyectivo se llama isomorfismo ].

**E80**.- **i**) Usando el resultado del ejercicio anterior, demuestre que si el número complejo a+ib es cero de un polinomio $f(x)=\sum_{k=0}^{n} a_k x^k$ con coeficientes reales [de manera que el conjugado de $a_k$ es el mismo $a_k$ ] entonces necesariamente a-ib también es cero del polinomio dado;
**ii**) demuestre que todo polinomio con coeficientes reales se factoriza en producto de polinomios de grado uno y polinomios de grado 2 con discriminante negativo.
[sugerencia : use el teorema fundamental y la parte **i**) de este ejercicio].

**E81**.- factorice cada uno de los siguientes polinomios en producto de factores irreducibles con coeficientes reales:
**a)** $x^2+3x+1$ ; **b**) $2x^4-2$ ; **c**) $x^4+x^2+1$ ; **d**) $x^3+x-2$ ; **e**) $3x^6-3$

En la casi totalidad de los ejercicios siguiente nos ocuparemos de los dominios de integridad **Z**[x] , **Q**[x] es decir de los dominios de integridad de los polinomios con coeficientes [respectivamente] enteros y racionales y en particular de las factorizaciones de los polinomios en producto de factores irreducibles.

**Def.22.-** Polinomios **primitivos** en **Z**[x].
Un polinomio con coeficientes enteros se llama primitivo si y sólo si sus coeficientes no nulos tienen MCD = 1 (con el convenio de considerar MCD positivo) , en forma equivalente : si y sólo si no existe ningún número primo que divida a todos los coeficientes del polinomio.
Por ejemplo : $6x^2+10x+15$ es polinomio primitivo, $3341x^3+1573x-2197$ no es primitivo.

**E82**.- Demuestre que $6x^2+10x+15$ es polinomio primitivo mientras que ` $3341x^3+1573x-2197$ no es primitivo.

**E83.-** Demuestre el primer lema de pag. 167 del texto de Lindsay Childs :
"el producto de dos polinomios primitivos es primitivo".

**E84.-**En la demostración del lema de Gauss (pag. 167 del texto de Lindsay Childs) a(x), b(x) son polinomios con coeficientes racionales mientras que s, t son números racionales (no necesariamente enteros) tales que los polinomios s.a(x), t.b(x) sean polinomios [con coeficientes enteros] primitivos;
**demuestre con detalle** que : $st=\pm 1$ .

**E85.-** Resuelva los ejercicios E1, E2, E4, E5 de las pag. 168-169 del texto.

**E86.-**Demuestre el teorema de pag. 168 del texto de Lindsay Childs.

[sugerencia : recuerde el ejemplo 12 de la pag. 12 y vea la solución del ejercicio **E19** de esta guía].

**E87.-** Enuncie el criterio de Eisenstein y aplíquelo para demostrar la irreducibilidad de los siguientes polinomios en **Q**[x] :

**i**) $x^5+84x^3+21$ ; **ii**) $2x^4+4x^3+8x^2+12$ ; **iii**) $x^4+\frac{5}{3}x^3+\frac{10}{7}x^2+45$ .

**E88.-** Sea $c(x)=\sum_{k=0}^{n}c_kx^k = c_0+c_1x+...+c_nx^n$ un polinomio de grado n, con coeficientes en un cuerpo K y sea $a\in K$, $c_0\neq 0$ ; **demuestre** que :
**i**) f(x) es irreducible si y sólo si f(x-a) es irreducible ;
**ii**) f(x) es irreducible si y sólo si $x^nf(\frac{1}{x})$ es irreducible.

**E89.-** Usando los resultados de los ejercicios anteriores, demuestre que los siguientes polinomios son irreducibles en **Q**[x] :
**i**) $x^4+5$ ; **ii**) $21x^5+84x^2+1$ ; **iii**) $6x^4+4x^2+2x+1$ ; **iv**) $x^5+10x+4$ ; **v**) $x^6+x^3+10$ .

**E90**.- Factorice el siguiente polinomio en producto de factores irreducibles en **Q**[x] luego halle un asociado primitivo del mismo y factorícelo en **Z**[x] :
$x^4+\frac{19}{6}x^3+\frac{7}{3}x^2+\frac{4}{3}x-\frac{5}{6}$ . [sugerencia : use el teorema de pag. 168 del texto de Linsay Childs] .

**E91.** Sea p un primo y sean $a(x)=\sum_{k=0}^{m}a_kx^k$ , $b(x)=\sum_{k=0}^{v}b_kx^k$ , $c(x)=\sum_{k=0}^{n}c_kx^k$ , polinomios con coeficientes enteros tales que $c(x)=a(x)b(x)$ , con $m\geq 1$, $v\geq 1$ , $n\geq 4$, $p\mid a_0$ , $p\mid c_0$ , $p\mid c_1$ , $p\mid c_2$ , $p\mid c_3$ , $(p, b_0) = 1$ ;
**demuestre con detalle** que :
**i**) grado(c) = grado(a)+grado(b) ;
**ii**) $p\mid a_3$ ;
**iii**) si todos los coeficientes del polinomio b(x) son múltiplos de cierto primo , q, entonces necesariamente todos los coeficientes del polinomio producto, c(x) también son múltiplos de q.

**E92.** Sea p un primo y sea $F_p : \mathbf{Z}[x]\rightarrow\mathbf{Z}_p[x]$ la función que asocia a todo polinomio $c(x)=\sum_{k=0}^{n}c_kx^k = c_0+c_1x+...+c_nx^n$ el polinomio F(c)

definido por : $F_p(c)(x) = \sum_{k=0}^{n}[c_k]_px^k = [c_0]_p+[c_1]_px+...+[c_n]_px^n$ ;
por ejemplo, si p=5 y $c(x) = 7+10x+3x^2+19x^3+30x^4+x^5$ entonces
$F_p(c)(x) = [2]_5+[10]_5x+[3]_5x^2+[19]_5x^3+[30]_5x^4+[1]_5x^5=$
$= [2]_5+[3]_5x^2+[4]_5x^3+x^5$ y si no hay peligro de ambigüedad escribiremos simplemente : $F_p(c)(x) = 2+3x^2+4x^3+x^5$ .
**i**) demuestre que $F_p$ es un homomorfismo de anillos.
[ Recuerde la nota en el ejercicio E79 ]

**ii**) Demuestre que si $(p, c_n)=1$ y si c=ab es una factorización propia de c entonces $F_p(c)(x) = F_p(a)(x)F_p(b)(x)$ es una factorización propia de $F_p(c)(x)$ ;

**iii**) Demuestre el corolario de pag. 171 del texto de Lindsay Childs .
**iv**) Demuestre que el polinomio $x^4+1$ es irreducible en **Z**[x].
**v**)Admita conocer la propiedad que en todo cuerpo $\mathbf{Z}_p$ el producto de dos elementos que no sean cuadrados es un cuadrado y demuestre que el polinomio $x^4+1$ es reducible en $\mathbf{Z}_p$[x] <u>para todo primo</u> p.
Sugerencia : observe que
**i**)si en $\mathbf{Z}_p$ se tiene $-1 = a^2$ [es decir si -1 es cuadrado] entonces
$x^4+1 = x^4 - a^2 = (x^2-a)(x^2+a)$ ;
**ii**) si $2=b^2$ entonces $x^4+1 = (x^4+2x^2+1) - b^2x^2 = (x^2+1+bx)(x^2+1-bx)$;
**iii**) si $-2=c^2$ entonces $x^4+1 = (x^4-2x^2+1) - c^2x^2 = (x^2-1+cx)(x^2-1-cx)$ ;
Como si ni -1 ni 2 es cuadrado, su producto $-2=(-1)(2)$ es cuadrado, siempre se cumplirá una de las tres factorizaciones consideradas.
Por ejemplo : en $\mathbf{Z}_3$ se tiene $1 = -2 = 2^2$ luego $x^4+1 = (x^2-1+2x)(x^2-1-2x)$;
en $\mathbf{Z}_5$ se tiene $-1=2^2$ luego $x^4+1 =(x^2-2)(x^2+2)$ ;
en $\mathbf{Z}_7$ se tiene $2=4^2$ luego $x^4+1 = (x^2+1+4x)(x^2+1-4x)$.

**E93.** considere el polinomio $c(x)=x^4+2x^2-1$ y observe que en $\mathbf{Z}_2$[x] este polinomio se escribe en la forma $F_2(c)(x)= x^4+1=(x^2+1)^2$ ; diga justificando si de esto se puede deducir que $x^4+2x^2-1$ es reducible en **Q**[x] .

**E94.-** Resuelva los ejercicios E1, E2, E3 de las páginas 126 hasta 128 del texto de Lindsay Childs.

**E95.-** Resuelva los ejercicios E2 hasta E11 de las páginas 131 hasta 134 del texto de Lindsay Childs.

**E96.-** Resuelva los ejercicios E17 hasta E24 de las páginas 134 ,135 del texto de Lindsay Childs.

**E97.-** Resuelva los ejercicios E4, E5 , E8, E9 , E11, E12 , E14, E15 , de las páginas 168 hasta 172 del texto de Lindsay Childs.

**E98.**- Dé un ejemplo de polinomio con coeficientes reales que se factorice en un producto de 3 factores irreducibles en **R**[x] y en producto de 5 factores irreducibles en **C**[x] .

**E99.**- Diga cual es el número mínimo y cual es el número máximo de factores irreducibles en que puede factorizarse un polinomio de grado 17 en **R**[x] .

**E100.**- Dé un ejemplo de polinomio mónico, con coeficientes enteros que sea irreducible en $\mathbf{Z}[x]$ pero reducible en $\mathbf{Z}_{23}[x]$ .

**E101.**- Averigüe (y justifique) si los siguientes polinomios son o no son es irreducibles en $\mathbf{Q}[x]$ :

**i**) $x^4+\frac{5}{3}x^3+10x^2+45$ ; **ii**) $309867.x^2+20000123.x+4056781.$

**E102.**- Factorice los siguientes polinomios en producto de factores irreducibles en $\mathbf{Z}[x]$ :

**i**) $2x^4+x^3+6x^2+9x+3$ ; **ii**) $5x^4+x^3+6x^2+9x+3$ .

**Soluciones de los ejercicios desde E71 hasta E102.**

**SE71, 72.** Polinomios diferentes puede que definan la misma función, si el cuerpo tiene un número finito de elementos; si el cuerpo K tiene n elementos : $a_1,a_2,...,a_n$, entonces por ejemplo el polinomio nulo y los dos polinomios $(x-a_1)(x-a_2)...(x-a_n)$ , $(x-a_1)^2(x-a_2)^2...(x-a_n)^2$ representan todos la función nula $K\to K$ .
En el caso particular de que $K=\mathbf{Z}_p$ (con p primo) , cualquier polinomio c(x) y el polinomio $c(x)+(x^p-x)^n$ representan la misma función $\mathbf{Z}_p \to \mathbf{Z}_p$ .

**SE73.- a**) $(x^2-1, x^2+x) = x+1 = 1.(x^2+x) + (-1)(x^2-1)$ ;
**b**) $(x^3-1, 2x^2-2x) = x-1 = 1.(x^3-1) +(x+1)(2x^2-2x)$ ( en $\mathbf{Z}_3[x]$ );
**c**) $(x^2+2x+1, x^4+x^3) = x+1 = (x^2-x+1)(x^2+2x+1) +(-1)(x^4+x^3)$ ;
**d**) $(x^2-1, x^2+x , x^3-x^2) = x+1 = 1.(x^2-1) + 1.(x^2+x) + 0.(x^3-x^2)$ .

**SE74.,75.-** Observemos que en $\mathbf{Z}_p[x]$ hay p polinomios mónicos de grado uno y que hay $p^2$ polinomios mónicos de grado 2. Si al número total de polinomios mónicos de grado 2 le restamos el número de polinomios mónicos de grado 2 que son producto de polinomios mónicos de grado uno, obtenemos el número de polinomios mónicos de grado 2 irreducibles. Hay p cuadrados de polinomios mónicos de grado uno y $\binom{p}{2} = \frac{p(p-1)}{2}$ productos de dos polinomios mónicos distintos de grado uno , de manera que el número total de polinomios mónicos de grado 2 reducibles es $p+\frac{p(p-1)}{2} = \frac{p(p+1)}{2}$ y el número de polinomios mónicos de grado 2 irreducibles serea entonces $p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$ ; de esto sigue que en $\mathbf{Z}_2[x]$ hay un polinomio mónico de grado 2 irreducible, en $\mathbf{Z}_3[x]$ hay 3 y en $\mathbf{Z}_5[x]$ hay 10 . Los mencionados polinomios son :
**a**) en $\mathbf{Z}_2[x]$ : $x^2+x+1$ ;
**b**) en $\mathbf{Z}_3[x]$ : $x^2+x+2, x^2+2x+2, x^2+1$ ;
**c**) en $\mathbf{Z}_5[x]$ : $x^2+x+1$ , $x^2+4x+1, x^2+2$ , $x^2+x+2$ , $x^2+4x+2$ ,
$x^2+3$ , $x^2+2x+3$ , $x^2+3x+3, x^2+2x+4, x^2+3x+4$ .

**SE76.-** Una posibilidad es de eliminar, del conjunto de todos los polinomios del tipo $x^3+ax^2+bx+1$ , $x^4+ax^3+bx^2+cx+1$ aquellos que son reducibles;
Un polinomio de grado 3 es reducible si y sólo si tiene un cero, lo cual es el caso de los polinomios : $x^3+x^2+x+1$ , $x^3+1$ así que los dos polinomios irreducibles de grado 3 son : $x^3+x^2+1$ , $x^3+x+1$ ;
Un polinomio de grado 4 es reducible si y sólo si tiene un cero o si es producto de dos irreducibles de grado 2, de manera que tenemos que eliminar los siguientes :
$x^4+x^3+x^2+1$ , $x^4+x^3+x+1$ , $x^4+x^2+x+1$ , que tienen un cero y
$x^4+x^2+1 = (x^2+x+1)^2$ así que los tres polinomios irreducibles de grado 4 son : $x^4+x^3+x^2+x+1$, $x^4+x^3+1$, $x^4+x+1$ .

**SE77.-** como a es irreducible y divide al producto df, a debe dividir (*) a uno de los dos factores, por ej. d , de manera que será d=ua con u unitario; luego se tiene abc=uaf (**) $\Rightarrow$ bc=uf lo cual no puede ser ya que el polinomio uf que es irreducible no puede tener la factorización propia uf = bc ;
**Observación importante** : si esta fuese una pregunta de examen sería obligatorio justificar los pasos (*), (**) y también justificar el hecho que el producto, uf, de un unitario, u, por un irreducible, f, es un irreducible.

**SE78.- i**) Sea P(n) la propiedad " todo polinomio de grado n se factoriza en producto de n factores de primer grado" (tratándose por supuesto de polinomios elementos de $\mathbf{C}[x]$ ) ;
P(1) es cierta, siendo todo polinomio de primer grado producto (de un solo factor) de polinomios de primer grado;
Admitamos cierta la hipótesis inductiva P(k), [ $k \geq 1$] , y consideremos un polinomio c(x) , de grado k+1 ; por el teorema fundamental del álgebra c(x) tiene almenos un cero, $a_{k+1}$, de lo cual sigue [**justificar !!**] $c(x)=(x-a_{k+1})g(x)$ siendo g(x) un polinomio de grado k [**justificar !!**] ; por hipótesis inductiva $g(x)= (ax+a_1)(x-a_2)...(x-a_k)$ y por lo tanto $c(x)=(x-a_{k+1})g(x)=(ax+a_1)(x-a_2)...(x-a_k)(x-a_{k+1})$;

**iia**) $x^2+3x+1 = (x+\frac{3}{2}+\frac{\sqrt{5}}{2})(x+\frac{3}{2}-\frac{\sqrt{5}}{2})$ ; **iib**) $2x^4-2 = (2x-2)(x+1)(x-i)(x+i)$ ;

**iic**) $x^4+x^2+1 = (x^2+1)^2-x^2 = (x^2+1-x)(x^2+1+x)$ ;

**iid**) $x^3+x-2 = (x-1)\,(x+\frac{1}{2}+\frac{\sqrt{7}}{2}\,i)(x+\frac{1}{2}-\frac{\sqrt{7}}{2}\,i)$ ;

**iie**) $3x^6-3 = (3x-3)(x+1)(x^2+x+1)(x^2-x+1) =$

$= (3x-3)(x-1)(x+\frac{1}{2}+\frac{\sqrt{3}}{2}\,i)(x+\frac{1}{2}-\frac{\sqrt{3}}{2}\,i)(x-\frac{1}{2}+\frac{\sqrt{3}}{2}\,i)(x-\frac{1}{2}-\frac{\sqrt{3}}{2}\,i)$ .

**SE79.-** $c((x+iy)+(u+iv)) = c((x+u)+i(y+v)) =$
$= (x+u)-i(y+v) = (x-iy)+(u-iv) = c(x+iy)+c(u+iv)$ ;

$c((x+iy)(u+iv)) = c((xu-yv)+i(yu+xv)) = (xu-yv)-i(yu+xv)$ ;
$c((x+iy)c(u+iv)) =(x-iy)(u-iv) = (xu-yv)+i(-yu-xv)= (xu-yv)-i(yu+xv)$ .
Hasta ahora hemos verificado que c es un homomorfismo de cuerpos;
falta verificar que c es inyectiva y sobreyectiva.
$c(x+iy)=c(u+iv) \Rightarrow x-iy=u-iv \Rightarrow x=u,\ y=v \Rightarrow (x+iy)=(u+iv)$ luego c es inyectiva;

para todo elemento a+ib del codominio de c, se tiene a+ib= c(a-ib) luego c es sobreyectiva.

**SE80.-** Indicaremos con **c**(a+ib)= a-ib el conjugado de a+ib y usaremos el hecho que la función **c** : **C**→**C** un homomorfismo.

Sea $f(x)=\sum_{k=0}^{n} a_k x^k$ , siendo los coeficientes $a_0,a_1,...,a_n$ número reales,
de manera que **c**$(a_k)=a_k$ .
Si f(a+ib)= 0 , entonces $0=\mathbf{c}(0)=\mathbf{c}(f(a+ib)) \underset{(0)}{=}$

$$= \mathbf{c}\left(\sum_{k=0}^{n} a_k(a+ib)^k\right) \underset{(1)}{=} \sum_{k=0}^{n} \mathbf{c}(a_k(a+ib)^k) \underset{(2)}{=} \sum_{k=0}^{n} \mathbf{c}(a_k)\mathbf{c}((a+ib))^k) \underset{(3)}{=} \sum_{k=0}^{n} a_k(a-ib)^k \underset{(4)}{=} f(a-ib) .$$

(1),(2) por ser **c** homomorfismo ; (3) por ser $a_k$ real ; (0), (4) por definición de f(x).
**ii**) Teniendo una factorización de un polinomio, f(x), con coeficientes reales en producto de factores de primer grado, por la parte **i**) de este ejercicio, cada vez que aparece un factor
del tipo (x-(a+ib)) también aparece otro igual a (x-(a-ib)) y multiplicándolos se obtiene $(x-a)^2+b^2$ , de manera que $f(x) = ((x-a)^2+b^2)g(x)$ siendo g(x) también un polinomio con coeficientes reales ; si a su vez g(x) tiene algún factor no real, del tipo (x-(c+id)) se repite el proceso, poniendo en evidencia al factor real $(x-c)^2+d^2$ etc.
Procediendo en esta forma, se logra factorizar al polinomio f(x) en un producto de cierto número (nulo o positivo) de polinomios reales de segundo grado con discriminante negativo y cierto número de factores reales de primer grado.
[una demostración rigurosa se puede elaborar por inducción...]
Para algunos ejemplos, véase el ejercicio siguiente.

**SE81.-**

**iia**) $x^2+3x+1 = (x+\frac{3}{2}+\frac{\sqrt{5}}{2})(x+\frac{3}{2}-\frac{\sqrt{5}}{2})$ ;

**iib**) $2x^4-2 = (2x-2)(x+1)(x-i)(x+i)=(2x-2)(x+1)(x^2+1)$

**iic**) $x^4+x^2+1 = (x^2+1)^2-x^2 = (x^2+1-x)(x^2+1+x)$ ;

**iid**) $x^3+x-2 = (x-1)(x+\frac{1}{2}+\frac{\sqrt{7}}{2}i)(x+\frac{1}{2}-\frac{\sqrt{7}}{2}i)= (x-1)(x^2+x+2)$ ;

**iie**) $3x^6-3 = (3x-3)(x+1)(x^2+x+1)(x^2-x+1)$ .

**SE82.-** $6x^2+10x+15$ es primitivo ya que (6, 10, 15) = 1 ;
$3341x^3+1573x-2197$ no es primitivo ya que (3341, 1573, 2197) = 13 .

**SE83.-** Consideraremos aca una demostración diferente de la del libro.
Para ilustrar la idea, antes de efectuar la demostración general, analizaremos un **ejemplo**.
Sean $a(x)=a_0+a_1x+a_2x^2= 6+15x+2x^2$ ,
$b(x)= b_0+b_1x+b_2x^2+b_3x^3+b_4x^4+b_5x^5= 12+3x+3x^2+7x^3+x^4+x^5$;

observemos que 3 no divide a todos los coeficientes de cada uno de los dos polinomios y de eso deduzcamos que 3 tampoco divide a todos los coeficientes del polinomio producto
$c(x)= c_0+c_1x+...+c_5x^7$ ; en particular verificaremos que como $a_2$ es el primer coeficiente de a(x) que no es múltiplo de 3 y $b_3$ es el primer coeficiente de b(x) que no es múltiplo de 3
el coeficiente $c_{2+3}=c_5= a_0b_5+ a_1b_4+ a_2b_3+ a_3b_2+ a_4b_1+ a_5b_0$ no es múltiplo de 3.
En efecto los primeros dos sumandos de la fórmula con la cual se calcula $c_5$ son múltiplos de 3 [ya que $a_0$, $a_1$ son múltiplos de 3] y los últimos tres sumandos de la misma fórmula también son múltiplos de 3 [por serlo $b_0$, $b_1$, $b_2$ ] ; por otra parte, como 3 es primo, el sumando $a_2b_3$ no es múltiplo de 3 así que por consiguiente $c_5$ no es múltiplo de 3.
Demostremos ahora que si los polinomios $a(x)=a_0+a_1x+...+a_sx^s$ , $b(x)= b_0+b_1x+...+b_tx^t$
son primitivos entonces por consiguiente el polinomio producto c(x)=a(x)b(x) también es primitivo. Para verificar que el máximo común divisor de los coeficientes de c(x) es =1, bastará verificar que para todo primo , p, existe un coeficiente de c(x) que no es múltiplo de p . En efecto, dado un primo, p, por ser a(x) primitivo, existen coeficientes de a(x) que no son múltiplos de p y podemos considerar el coeficiente $a_k$ de menor subíndice; análogamente sea $b_h$ el coeficiente de menor subíndice de b(x) que no es múltiplo de p; entonces, con el mismo procedimiento ilustrado en el ejemplo resulta que $c_{k+h}$ no es múltiplo de p.
$c_{k+h} =( a_0b_{k+h}+...+ a_{k-1}b_{h+1})+a_kb_h+( a_{k+1}b_{h-1}+... a_{k+h}b_0)$ ; como en el ejemplo, el único sumando que no es múltiplo de p resulta ser $a_kb_h$ , por lo cual $c_{k+h}$ nmo es múltiplo de p.

**E84.-** f(x) es primitivo , s, t son números racionales ; f(x)=a(x)b(x) ;
stf(x)=(s.a(x))(t.b(x)) ;
(s.a(x)), (t.b(x)) son con coeficientes enteros y primitivos, a(x), b(x) son con coeficientes racionales (no necesariamente enteros).
Observemos que : como (s.a(x)), (t.b(x)) $\in$ **Z**[x], por consiguiente stf(x) $\in$ **Z**[x] ;
como (s.a(x)), (t.b(x)) son primitivos, por consiguiente stf(x) será primitivo;
como f(x) es primitivo, el número racional st debe ser entero [explique] ;
si fuese st $\neq \pm 1$ todos los coeficientes de stf(x) serían múltiplos de st y stf(x) no sería primitivo, por lo tanto necesariamente st=±1.

**E85.-** Ejercicio E1 de la pag. 168 del texto.

" si $r=\frac{a}{b} \in \mathbf{Q}$ , f(x) primitivo, rf(x) primitivo y si $\frac{a}{b}$ es fracción irreducible, entonces necesariamente b=±1, ya que si $f(x)= c_0+c_1x+...+c_nx^n$ con $( c_0, c_1,...,c_n) = 1$ entonces $r.f(x) = \frac{a}{b} c_0+ \frac{a}{b} c_1x+...+ \frac{a}{b} c_nx^n$ y si b tuviese algún factor primo, p, este no podría ser factor ni de a ni de todos los $c_k$ y rf(x) no tendría coeficientes todos enteros ni podría ser primitivo; por lo tanto $r \in \mathbf{Z}$ y como f(x) $\in$ **Z**[x] , fuese $r \neq \pm 1$ rf(x) no sería primitivo.

Ejercicio E2 de la pag. 168 del texto.

**a**) primitivo asociado a : $\frac{4}{3}x^4+6x^3+\frac{2}{9}x^2+\frac{9}{2}x+18 \Rightarrow 18(\frac{4}{3}x^4+6x^3+\frac{2}{9}x^2+\frac{9}{2}x+18) =$
$= 24x^4+108x^3+4x^2+81x+324$ ;

**b**) primitivo asociado a : $36x^3+180x^2+24x+\frac{1}{7} \Rightarrow 7(36x^3+180x^2+24x+\frac{1}{7}) =$
$= 252x^3+1260x^2+168x+1$ .

Ejercicios E4, E5 de las pag. 168-169 del texto.
" halle todos los ceros racionales de los siguientes polinomios: "
Recordemos que los posibles ceros racionales de un polinomio $c_0+c_1x+...+c_nx^n$ con coeficientes enteros estan representados por fracciones $\frac{a}{b}$ donde $a|c_0, b|c_n$ .

**a, b**) $x^3-x+1$ , $x^3-x-1$;
hay que averiguar con los racionales ±1 , ninguno de los cuales es cero
[por lo cual no hay ningún cero racional].
**c**) $x^3+2x+10$ ; ±1, ±2, ±5, ±10 ; no hay ;
**d**) $x^3-2x^2+x+15$ ; ±1, ±3, ±5, ±15 ; no hay ;
**e**) $x^7 - 7$ ; ±1, ±7 ; no hay;
**f**) $2x^2-3x+4$ ; ±1, ±2, ±4, $\pm\frac{1}{2}$ ; no hay;
**g**) $2x^4-4x+3$ ; ±1, ±3, $\pm\frac{1}{2}$ , $\pm\frac{3}{2}$ ; no hay.

**E86**.- ver **SE19**, pag. 21 de esta guía.

**E87.- i**) p=7 divide a todos los coeficientes del polinomio $x^5+84x^3+21$ , menos a $a_5$ , además $7^2=49$ no divide a $a_0=21$ , por lo tanto el polinomio es irreducible en **Z**[x] y **Q**[x] ;
**ii**) $2x^4+4x^3+8x^2+12$ es asociado de $x^4+2x^3+4x^2+6$ en **Q**[x] (siendo 2 unitario); con p=2 actúa el criterio de Eisenstein, luego $x^4+2x^3+4x^2+6$ es irreducible en **Z**[x] y **Q**[x] e igualmente irreducible es cualquier asociado [explique];
**iii**) $x^4+\frac{5}{3}x^3+\frac{10}{7}x^2+45$ es asociado de $21x^4+35x^3+30x^2+945$ en el cual actúa el criterio de Eisenstein con p=5. Por lo tanto el polinomio dado es irreducible.

**E88.- i**) bastará verificar que f(x) tiene una factorización propia si y sólo si f(x-a) tiene una factorización propia; en efecto si f(x)=c(x)b(x) siendo c, b polinomios de grados ≥ 1, entonces f(x-a)=c(x-a)b(x-a) es una factorización propia de f(x-a) ; inversamente, si f(x-a)= h(x)k(x) con h, k polinomios de grados ≥ 1 , entonces f(x)= h(x+a)k(x+a) es una factorización propia de f(x) ;
**ii**) Consideremos primero un ejemplo:
$f(x)= (x-3)(x^2+5x+6)$ ; $x^3(\frac{1}{x}-3)((\frac{1}{x})^2+5\frac{1}{x}+6) =(1-3x)(1+5x+6x^2)$ ;
en general :
si $f(x)=c(x)b(x)$ con $c(x)= c_0+c_1x+...+c_sx^s$, $b(x) = b_0+b_1x+...+b_tx^t$ , $s+t = n$ , $f_0\neq 0$ [ por lo cual $c_0\neq 0$ , $b_0\neq 0$ ] entonces

$x^{s+t}c(\frac{1}{x})\,b(\frac{1}{x}) = x^s c(\frac{1}{x})x^t.b(\frac{1}{x}) = (\,c_0x^s+c_1x^{s-1}+...+c_s)(\,b_0x^t+b_1x^{t-1}+...+b_t)$
de manera que la factorización dada de f es propia si y sólo si los grados de los factores c(x), b(x) son ≥ 1 , si y sólo si los grados de los factores $(\,c_0x^s+c_1x^{s-1}+...+c_s)$, $(\,b_0x^t+b_1x^{t-1}+...+b_t)$ son ≥ 1 es decir si y sólo si la factorización de $x^n f(\frac{1}{x})$ es propia.

**SE89.- i**) $x^4+5$ ; Criterio de Eisenstein con p=5 ⇒ el polinomio dado es irreducible;

**ii**) $21x^5+84x^2+1 \Rightarrow x^5+84x^3+21$ ;
Criterio de Eisenstein con p=7 ⇒ el polinomio dado es irreducible;
**iii**) $6x^4+4x^2+2x+1 \Rightarrow x^4+2x^3+4x^2+6$ ;
Criterio de Eisenstein con p=2 ⇒ el polinomio dado es irreducible;
**iv**) $f(x)= x^5+10x+4$ ; $f(x+1) = (x^5+5x^4+10x^3+10x^2+5x+1)+(10x+10)+4 = x^5+5x^4+10x^3+10x^2+15x+15$ ;
Criterio de Eisenstein con p=5 ⇒ el polinomio dado es irreducible;
**v**) $f(x)= x^6+x^3+10$ ; $f(x+1)=(x^6+6x^5+15x^4+20x^3+15x^2+6x+1)+(x^3+3x^2+3x+1)+10=$
$= x^6+6x^5+15x^4+21x^3+18x^2+9x+12$ ;
Criterio de Eisenstein con p=3 ⇒ el polinomio dado es irreducible.

**SE90**.-
$x^4+\frac{19}{6}x^3+\frac{7}{3}x^2+\frac{4}{3}x-\frac{5}{6}$ es asociado de $f(x)= 6x^4+19x^3+14x^2+8x-5$ ;
Como los divisores de 6 son ±1, ±2, ±3, ±6, y los divisores de -5 son ±1, ±5 , sigue que posibles ceros racionales de este polinomio son :
$\pm1, \pm5, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{6}, \pm\frac{5}{2}, \pm\frac{5}{3}, \pm\frac{5}{6}$,.
Ensayando con paciencia, se averigua que $f(\frac{1}{3})=f(-\frac{5}{2})= 0$ y dividiendo [si se quiere con el algoritmo de Ruffini], se obtiene :
$x^4+\frac{19}{6}x^3+\frac{7}{3}x^2+\frac{4}{3}x-\frac{5}{6} = (x-\frac{1}{3})(x+\frac{5}{2})(x^2+x+1) \in \mathbf{Q}[x]$ .
Una factorización en $\mathbf{Z}[x]$ del polinomio primitivo asociado $6x^4+19x^3+14x^2+8x-5$ es entonces : $(3x-1)(2x+5)(x^2+x+1)$.

**SE91.-** $c_k= \sum_{i=0}^{k} a_i b_{k-i}$ .
**i**) Observemos que si k > s+t entonces $c_k=0$ ; en efecto si i < k-t entonces $b_{k-i} = 0$ mientras que si i ≥ k-t entonces i ≥ k-t > s por lo cual $a_i = 0$ .
Con un análisis análogo para el coeficiente $c_{s+t}$ se constata que el único sumando no nulo resulta ser el producto $a_s b_t$ cuyos factores son ámbos no nulos por ser grado(a)=s , grado(b) = t . Queda así demostrado que grado(a.b)=grado(a)+grado(b) .
**ii**) $c_1=a_0b_1+a_1b_0$ luego como por hipótesis $a_0$, $c_1$ son múltiplos de p será múltiplo de p también $a_1b_0$ $[=c_1 - a_0b_1]$ y $a_1$ [ya que por hipótesis $b_0$ no es múltiplo de p ] ;

análogamente de $c_2=a_0b_2+a_1b_1+a_2b_0$ [y tomando en cuenta que también $a_1$ es múltiplo de p ] se deduce que $a_2$ es múltiplo de p y por último de $c_3=a_0b_3+a_1b_2+a_2b_1+a_3b_0$ se deduce que $a_3b_0$ [y por consiguiente $a_3$ ] es múltiplo de p.

**iii**) si para todo coeficiente del polinomio b se tiene $b_i=p.d_i$ entonces

$$c_k=\sum_{i=0}^{k}a_ib_{k-i}=\sum_{i=0}^{k}a_ip.d_{k-i}=p\sum_{i=0}^{k}a_id_{k-i}\ [=\text{múltiplo de p}]\ .$$

**SE92.-**

**i**) Tenemos que verificar que para toda escogencia de dos polinomios a, b $\in$ **Z**[x] , se tiene : $F_p(a+b)=F_p(a)+F_p(b)$ ; $F_p(ab)=F_p(a)F_p(b)$ . En efecto :

¿ $F_p(a+b)=F_p(a)+F_p(b)$ ?

consideremos dos polinomios $a(x)=a_0+a_1x+...+a_nx^n$ , $b(x)=b_0+b_1x+...+b_nx^n$ ; [ nota n es el mayor de los grados de los dos poilinomios, de manera que si por ejemplo fuese grado(b) = m < n simplemente se tomará en cuenta que $b_{m+1}=...=b_n=0$ ]

$F_p$ asocia el polinomio $[a_0]+[a_1]x+...+[a_n]x^n$ al polinomio a , $[b_0]+[b_1]x+...+[b_n]x^n$ al polinomio b , $[a_0+b_0]+[a_1+b_1]x+...+[a_n+b_n]x^n$ al polinomio a+b , de manera que para comprobar que $F_p(a+b)=F_p(a)+F_p(b)$ bastará verificar que :

$([a_0]+[a_1]x+...+[a_n]x^n)+([b_0]+[b_1]x+...+[b_n]x^n)=[a_0+b_0]+[a_1+b_1]x+...+[a_n+b_n]x^n$

y esta igualdad es consecuencia inmediata de las definiciones de suma de polinomios (1) y de suma en $Z_p$ (2) :

$$([a_0]+[a_1]x+...+[a_n]x^n)+([b_0]+[b_1]x+...+[b_n]x^n) \underset{1}{=}$$

$$=([a_0]+[b_0])+([a_1]+[b_1])+...+([a_n]+[b_n])x^n \underset{2}{=}$$

$$=[a_0+b_0]+[a_1+b_1]x+...+[a_n+b_n]x^n\ .$$

¿ $F_p(ab)=F_p(a)F_p(b)$ ?

Teniendo en cuenta esta vez la definición de multiplicación de polinomios, bastará verificar que [comparando los coeficientes de los términos de igual grado de los polinomios $F_p(ab)$ y $F_p(a)F_p(b)$] :

$[a_0b_k+a_1b_{k-1}+...+a_kb_0]=[a_0][b_k]+[a_1][b_{k-1}]+...+[a_k][b_0]$ y esta igualdad es consecuencia inmediata de las definiciones de suma y multiplicación en $Z_p$ .

**ii**) si c=ab es una factorización propia del polinomio c y si p no divide al coeficiente del término de grado máximo del polinomio c entonces se tiene :

por el resultado de la parte **i**) de este ejercicio :

(*)$F_p(c)(x)=[c_0]+[c_1]x+...+[c_n]x^n=([a_0]+[a_1]x+...+[a_s]x^s)([b_0]+[b_1]x+...+[b_t]x^t)$, siendo s, t $\geq 1$ , $[c_n]\neq 0$ y como $c_n=a_sb_t$ , sigue también $[a_s]\neq 0$ , $[b_t]\neq 0$ . Por lo tanto se trata de una factorización propia de $F_p(c)(x)$ .

**iii**) En el caso en que el entero m positivo no sea primo, la parte **i**) de este ejercicio sigue valiendo igual. En cuanto a la parte **ii**), la hipótesis de que m no divida a $c_n$ es suficiente para asegurar que ninguno de los dos coeficientes $[a_s]$, $[b_t]$ sea nulo, lo cual asegura que la factorización (*) es propia.

Por lo tanto si es cierto que toda factorización propia del polinomio c en **Z**[x] proporciona una factorización propia en $\mathbf{Z}_m[x]$ (siempre y cuando m no sea divisor del coeficiente del término de grado máximo de c ) al no existir ninguna factorización propia (de la imagen] del polinomio dado en $Z_m[x]$ el polinomio c es irreducible en **Z**[x] y en **Q**[x].

**iv**) $f(x)=x^4+1$ ; sea $g(x)=f(x+1) = x^4+4x^3+6x^2+4x+2 \Rightarrow$ [por Eisenstein con p=2] $g(x)$ (y por consiguiente $f(x)$ ) es irreducible.
**v**) la sugerencia lo explica todo.

**SE93.**- NO . El polinomio dado es irreducible en $\mathbf{Z}[x]$ como se puede averiguar considerando $g(x+1) = (x+1)^4+2(x+1)^2-1 = x^4+4x^3+8x^2+6x+2$ y aplicando el criterio de Eisenstein con p=2. Observe que si acaso el polinomio hubiese resultado ser reducible, esto **no** hubiese sido consecuencia del hecho que [su imagen] en $\mathbf{Z}_2[x]$ fuese reducible.

**SE94.**- Ejercicio **E1** de pag. 126 del texto de Lindsay Childs :
"usando el teorema de Fermat, hallar para todo primo p dos polinomios que definan la misma función $\mathbf{Z}_p \rightarrow \mathbf{Z}_p$ ".
Por el teorema de Fermat se tiene (en $\mathbf{Z}_p$ ) : $a^p=a$ para todo $a \in \mathbf{Z}_p$ ; por consiguiente los dos polinomios : $x$ , $x^p$ definen la misma función.
Ejercicio **E2** de pag. 128 del texto :
" para cuales primos, p, los dos polinomios $f(x) = x^6+2x^2+x$ , $g(x) = x^9+8x^3+x$ definen la misma función $\mathbf{Z}_p \rightarrow \mathbf{Z}_p$ ? ".
Si f, g definen la misma función, deberá ser : $f(1)=g(1)$ , es decir $4=10$, lo cual es posible si y sólo si $[4]_p=[10]_p \Leftrightarrow [6]_p=0 \Leftrightarrow p \mid 6 \Leftrightarrow p=2$ o 3 ; esta es por lo tanto una condición necesaria .
En el caso de $\mathbf{Z}_2$ , como $f(0)=g(0)$ la condición resulta evidentemente también suficiente;
En el caso de $\mathbf{Z}_3$ falta averiguar si $f(2)=g(2)$ [módulo 3] y en efecto tenemos :
$f(2)-g(2) = (64+8+2)-(512+64+2)= -504 \underset{3}{\equiv} 0$ .
Nota : hubiésemos podido simplificar un poco las cuentas usando el teorema de Fermat.
Ejercicio **E3** de pag. 128 del texto :
"demuestre que un polinomio $c(x) \in K[x]$ tcon coeficientes en un cuerpo K tiene inverso multiplicativo si y sólo si su grado es =0 "
Como grado (pq) = grado(p)+grado(q), [ ver parte **i**) del ejercicio **E91** ] si p tiene inverso, q , deberá ser grado(p)+grado(q) = grado(1) = 0 lo cual es posible [teniendo que ser p, q polinomios no nulos] si y sólo si ámbos tienen grado cero; por otra parte si p tiene grado cero entonces p es una constante no nula del cuerpo K y por lo tanto tiene inverso multiplicativo.

**SE95.**-Ejercicio **E2** de pag. 131 del texto :
"divisibilidad de $f(x)= x^4+x^3+x+4$ por $(x-3)$" :
Trabajando en un cuerpo, podemos usar el teorema del resto y obtenemos que el resto de la división es $f(3)= 115 = 5.23$ . Esto implica que en $\mathbf{Q}[x]$
[ y por consiguiente en $\mathbf{Z}x$] ¿ por qué ? ] $x-3$ no divide a f ;
tampoco lo divide en $\mathbf{Z}_p$ , si $p \neq 5$, $p \neq 23$ ;
Aunque $\mathbf{Z}_4$ no sea un cuerpo, podemos igualmente aplicar el teorema del resto a la división de f por $x-3$ ya que $x-3$ es mónico así que no tendremos que efectuar ninguna división y resulta que en $\mathbf{Z}_4[x]$ tampoco $x-3$ divide a f.
Ejercicio **E3** de pag. 131 del texto :
"Hallar todos los enteros positivos [ m >1 ] tales que en $\mathbf{Z}_m[x]$
$x^3+1$ divida a $f(x)=x^5+x^3+x^2-9$ "
Se tiene $x^5+x^3+x^2-9 = (x^3+1)(x^2+1) - 2x^2-12$ , por lo cual el único es m=2.

Ejercicio **E4** de pag. 132 del texto :
" En el algoritmo de Euclides, aplicado a dos polinomios f, g ∈ K[x] , el último resto no nulo es un máximo común divisor de f, g "
La demostración es casi prácticamente la misma que para el máximo común divisor de dos enteros no nulos, con algunas modificaciones : en la división de polinomios el resto siempre debe tener grado estrictamente menor que el divisor y la única condición para el divisor es que sea un polinomio no nulo.
Ejercicio **E5** de pag. 132 del texto :
" si d = (f, g) es un máximo común divisor obtenido con el algoritmo de Euclides y si a es cualquier divisor común de f, g , entonces necesariamente $a \mid d$ "
La demostración es la misma que para enteros.
Si denotamos $f=r_1$ , $g=r_2$ , en la primera división de f por g : $r_1=r_2.q_1+r_3$ y si luego seguimos con las divisiones : $r_{k-2}=r_{k-1}.q_{k-2}+r_k$ siendo (f, g) = último resto no nulo, observamos que si a es un polinomio que divide f, g [es decir $r_1$, $r_2$ ] entonces despejando $r_3$ de la primera fórmula deducimos que $a \mid r_3$ , luego al saber que a divide $r_2$, $r_3$ , despejando $r_4$ de la segunda fórmula se deduce que $a \mid r_4$ etc. así siguiendo se llega a poner en evidencia que a divide al último resto no nulo, es decir $a \mid (f, g)$ .
[este proceso se puede formular rigurosamente por inducción].
Ejercicio **E6** de pag. 133 del texto :
Para poner en evidencia que (f, g) se puede expresar como combinación lineal de f, g [esta vez con coeficientes polinomiales] basta usar (y justificar) el algoritmo ilustrado al final de la pag. 9 de esta guia (y comienzo de la pag. 10, que para comodidad del lector volvemos a copiar a continuación :
**********
Una segunda alternativa (que resulta mejor si se quiere efectuar el proceso por medio de un programa de computadora) es la siguiente :
Construyamos dos sucesiones de números ,
$x_1, x_2, \ldots , y_1, y_2, \ldots$ , en la manera siguiente :
$x_1=1$, $x_2=0$, $y_1=0$, $y_2= 1$ y a partir del subíndice 3, contruyamos
$x_i$ por medio de $x_{i-1}$ , $x_{i-2}$ con la misma fórmula con la cual se genera $r_i$ por medio de $r_{i-1}$ , $r_{i-2}$ y lo mismo con $y_i$ por medio de $y_{i-1}$ , $y_{i-2}$ a título de ejemplo, teníamos
$r_1 = q_1.r_2 + r_3$ es decir : $r_3= r_1 - q_1.r_2$ luego pondremos
$x_3= x_1 - q_1.x_2$ y lo mismo haremos con la sucesión de las $y_i$ :
$y_3= y_1 - q_1.y_2$ ; en general, para un genérico subíndice k será :
$x_k= x_{k-2} - q_{k-2}.x_{k-1}$ , $y_k= y_{k-2} - q_{k-2}.y_{k-1}$ .

Se puede demostrar entonces por inducción (2a forma), $I_2$, que para todo subíndice k, se tiene : $x_k.m + y_k.n= r_k$ y por lo tanto, con aquel subíndice "k" que corresponde al último resto no nulo, se obtiene la combinación lineal buscada.
**********
Ejercicio **E7** de pag. 133 del texto :
$f(x) = x^4+2x^3- 6x -9$ , $g(x)= 3x^4+8x^3+14x^2+8x+3$ ;
$(f, g) = x^2+2x+3 = \frac{-x+5}{44} f(x) + \frac{3x-13}{44} g(x)$ .
Ejercicio **E8** de pag. 134 del texto :
" Demuestre que si para tres polinomios no nulos f, g, h se tiene : (f, g)=1 , $h \mid f$ entonces necesariamente (h, g) = 1 "
(f, g)=1 , $h \mid f \Rightarrow f=f_1h$ y existen polinomios a, b tales que af+bg = 1 ; luego

$1 = af+bg = af_1h + bg = (af_1)h+bg$ por lo cual (h, g) = 1 ya que si hubiese algún factor irreducible, q(x) que divide h, g este dividiría también a su combinación lineal $(af_1)h+bg = 1$.

Ejercicio **E9** de pag. 134 del texto :

" Demuestre que si para tres polinomios no nulos f, g, h se tiene :
(f, g)=1 , entonces (fh, g) = (h, g) "

Bastará verificar que (fh, g) divide a (h, g) y que (h, g) divide a (fh, g) ;
Es evidente que (h, g) divide a (fh, g) ya que si un polinomio, q, divide h a mayor razón dividirá fh;
Para demostrar que (fh, g) divide a (h, g) deberemos usar la hipótesis (f, g)=1 por la cual existen polinomios a, b tales que af+bg = 1; multiplicando ámbos miembros de esta igualdad por h obtenemos : afh+bgh = h de lo cual se desprende que si q divide fh , g por consiguiente q también divide h.

Ejercicio **E10** de pag. 134 del texto :

Hallar el MCD : **i**) en $Z_2[x]$ de $x^2+1$ , $x^5+1$ :

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

**ii**) en $Z_3[x]$ de $x^2-x+4 = x^2+2x+1$ , $x^3+2x^2+3x+2 = x^3+2x^2+2$ ;

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

Ejercicio **E11** de pag. 134 del texto :

"Resuelva las siguientes ecuaciones en **Q**[x] :

**i**) $p(x)(x^2-3x+2)+q(x)(x^2+x+1) = 1$ ;

Con el algoritmo de Euclides se obtiene :

$\frac{21}{16} = (-\frac{1}{4}x+\frac{11}{16})(x^2+x+1) + (\frac{x}{4}+\frac{5}{16})(x^2-3x+2)$ por lo cual

$1 = \frac{1}{21}(-4x+11)(x^2+x+1) + (4x+5)(x^2-3x+2)$ de manera que

$p_1(x) = \frac{4x+5}{21}$ , $q_1(x) = \frac{-4x+11}{21}$ proporcionan una solución particular ;

si ahora [ igual a como se procede trabajando con enteros...]
restamos miembro a miembro las dos igualdades :

$(x^2-3x+2)p+(x^2+x+1)q = 1$ , $(x^2-3x+2)p_1+(x^2+x+1)q_1 = 1$ ,

obtenemos : $(x^2-3x+2)(p-p_1) + (x^2+x+1)(q-q_1) = 0$ ,

$(x^2-3x+2)(p-p_1) = (x^2+x+1)(q_1-q)$ y tomando en cuenta que los dos polinomios dados tienen máximo común divisor =1 podemos afirmar que $(x^2+x+1) \mid (p-p_1)$ de manera que $(p-p_1) = a(x)(x^2+x+1)$ y por consiguiente $(q_1-q) = a(x)(x^2-3x+2)$.

En definitiva <u>todas</u> las soluciones de nuestra ecuación en dos incógnitas polinomiales p, q estan representadas por :

$$\begin{cases} p=p_1+a(x)(x^2+x+1) \\ q=q_1-a(x)(x^2-3x+2) \end{cases} ; \qquad \begin{cases} p=\frac{4x+5}{21}+a(x)(x^2+x+1) \\ q=\frac{-4x+11}{21}-a(x)(x^2-3x+2) \end{cases}$$

**ii**) $A(x)p(x)+B(x)q(x)= p(x)(2x^3-7x^2+7x-2)+q(x)(2x^3+x^2+x-1) =2x-1$ ;
Con el algoritmo de Euclides se obtiene :
$\frac{21}{16}(2x-1) = (\frac{4x+5}{16})A(x) + (\frac{-4x+11}{16})B(x)$ de donde se obtiene :

$2x-1 = (\frac{4x+5}{21})A(x) + (\frac{-4x+11}{21})B(x)$ , de manera que una solución particular es :
$p_1(x) = \frac{4x+5}{21}$ , $q_1(x) = \frac{-4x+11}{21}$ etc.
Observación : de los resultados obtenidos se desprende que la ecuación **ii**) se generó multiplicando por 2x-1 la ecuación **i**)

**SE96.**- Resuelva los ejercicios E17 hasta E24 de las páginas 134 ,135 del texto de Lindsay Childs.

Ejercicio **E17** de pag. 134 del texto :
" Demuestre que todo polinomio, f, de grado ≥ 1, con coeficientes en un cuerpo, F, es producto de uno o más factores irreducibles "
[sugerencia : induicción sobre el grado del polinomio, usando el principio de inducción en la segunda forma]
Sea P(n) la propiedad : " todo polinomio de hrado n es irreducible o es producto de polinomios irreducibles".
P(1) es cierta ya que todo polinomio de grado 1 es irreducible.
Nota : si f=a.b fuese una factorización propia de f, de manera que ni a ni b pueda ser unitario, entonces grado(a) ≥ 1 , grado(b) ≥ 1 por lo cual grado(f) ≥ 1+1 = 2 .
Supongamos P(n) cierta para todo n tal que $1 \le n \le k$ , con $k \ge 1$ ;
si grado(f)=k+1 y f es irreducible entonces P(k+1) se cumple; si f no es irreducible y por lo tanto tiene una factorización propia : f=a.b entonces necesariamente [ por qué? ] grado(a) < k+1 , grado(b) < k+1 y por la hipótesis inductiva los polinomios a, b son irreducibles o se factorizan en producto de factores irreducibles : $a=a_1...a_s$ , $b=b_1...b_t$ [con $s \ge 1$ , $t \ge 1$ ] y por consiguiente $f=ab=(a_1...a_s)(b=b_1...b_t)$= producto de factores irreducibles.

Ejercicio **E18** de pag. 134 del texto :
" si p es polinomio irreducible y si p divide al producto fg entonces necesariamente p divide a almenos uno de los dos factores".
Esta afirmación es equivalente [se puede comprobar esto usando "tablas de verdad" (ver guía opcional de elementos de análisis lógico")] a la afirmación siguiente :
"sea p un polinomio irreducible; si p divide al producto fg y si p no divide f entonces necesariamente p divide a g". Demostraremos esto usando el "lema de Bezout" (pag. 133 del texto).
Observemos que si p es irreducible y p no divide f entonces (p, f)=1 ya que si hubiese algún divisor (irreducible) común a los dos polinomios p, f este solamente podría ser p, lo cual no es posible por estar suponiendo que p no divide f.
(p, f)= 1 implica la existencia de dos polinomios a, b tales que ap+bf = 1 de lo cual sigue g=g.1 = g(ap+bf) = (ga)p+b(fg) y como evidentemente p divide (ga)p y también, por hipótesis divide fg, sigue que p divide a la combinación lineal (ga)p+b(fg) = g .

Ejercicio **E19** de pag. 134 del texto :
Demuestre el teorema : " si $f=p_1...p_s=q_1...q_t$ son dos factorizaciones del polinomio f en producto de irreducibles entonces necesariamente : **i**) s=t , **ii**) reordenando convenientemente los factores resulta que para todo i = 1, 2,...,s $p_i$ , $q_i$ son asociados.
Sugerencia : demostralo por inducción sobre s.
Sea s=1, entonces $f = p_1=q_1...q_t$ y como el polinomio irreducible $p_1$. divide al producto $q_1...q_t$ deberá necesariamente dividir a almenos un de los factores, que podemos (cambiando eventualmente el orden) indicar con $q_1$. Podemos escribir entonces $q_1=up_1$, siendo u unitario. Por consiguiente : $p_1=up_1...q_t \Rightarrow 1= uq_2..q_t$ lo cual no es posible si fuese $t \geq 2$ [por qué ? ] ; en conclusión se tiene [en el caso s=1 ] :
s= t = 1, $f=p_1=q_1$ ;
Supongamos cierta la propiedad para k (con $k \geq 1$ ) y consideremos el caso :
$f=p_1...p_{k+1} = q_1...q_t$ ; como el polinomio irreducible $p_{k+1}$ divide al producto $q_1...q_t$ , debe dividir a almenos uno de los factores y podemos suponer (cambiando el orden de los facroes en caso de necesidad) $p_{k+1} | q_t$ , de lo cual sigue $q_t=up_{k+1}$ , $f=p_1...p_{k+1} = q_1...up_{k+1} \Rightarrow p_1...p_k = uq_1...q_{t-1}$ ; por hipótesis inductiva entonces k=t-1 y cambiando si necesario el orden de los factores :
$p_1$, $uq_1$ son asociados e igualmente $p_2$, $q_2$, ...,$p_k$, $q_{t-1}$ y como $q_t=up_{k+1}$ , también son asociados $p_{k+1}$, $q_t$ . En definitiva : el número de factores k+1=t de las dos factorizaciones es el mismo y con un conveniente orden los factores son dos a dos asociados.

Ejercicio **E20** de pag. 134 del texto :
"demuestre que si f, g son polinomios irreducibles y mónicos y si $f|g$ entonces f=g"
En efecto $f|g \Rightarrow g=fh$ y por ser f, g irreducibles h debe ser unitario; si h es unitario, h es una constante del cuerpo de los coeficientes y como f, g tienen el mismo grado (por qué? ) y f es mónico, sigue que el coeficiente del término de grado máximo de g es h pero como g es mónico entonces debe ser h=1.
Ejercicio **E21** de pag. 134 del texto :
" demuestre que en $\mathbf{R}[x]$ ningún polinomio de grado impar > 1 es irreducible y que en $\mathbf{C}[x]$ ningún polinomio de segundo grado es irreducible".
Si admitimos el teorema fundamental del ålgebra, este implica [ ver **E78i** , **E80ii**] el resultado pedido.
Sin admitir el teorema fundamental del álgebra :
Sea f es polinomio real de grado impar $\geq 3$, que no es restrictivo suponer mónico; como los límites de f(x) cuando x tiende , respectivamente a $\pm \infty$ son $\pm \infty$ , es posible hallar valores de x : a, b tales que $a < b$ , $f(a) < 0 < f(b)$ y aplicar el teorema del valor intermedio (Bolzano), siendo la función definida por f una función continua; de esto sigue que f tiene almenos un cero real y por el teorema del resto, que f tiene almenos un factor real de primer grado.
Para el caso de un polinomio complejo de segundo grado, es suficiente aplicar la fórmula para resolver ecuaciones de segundo grado y observar que todo número complejo tiene raíces cuadrada [como se puede verificar representando el número en forma trigonométrica].

Ejercicio **E22** de pag. 134 del texto :
En $\mathbf{Z}_5[x]$ : $x^5-x = x(x-1)(x-2)(x-3)(x-4)$ ; más en general en todo $\mathbf{Z}_p[x]$ , con p primo, se tiene : $x^p-x = x(x-1)(x-2)...(x-(p-2))(x-(p-1))$ , como se puede verificar observando que [por el teorema de Fermat] todo elemento de $\mathbf{Z}_p$ es cero del polinomio $x^p-x$ .

Ejercicio **E23** de pag. 134 del texto :
" En $\mathbf{Z}_2[x]$ , factorice los siguientes polinomios en producto de factores irreducibles : "
**a**) $x^8+x^7+x^6+x^4+1$ ; **b**) $x^6+x^4+x^3+x^2+1$ ; **c**) $x^{16}-x$ ; **d**) $x^7+x^6+x^4+1$ .

Averiguemos previamente cuales polinomios irreducible hay, de grados 1 hasta 4 :
$x$, $x+1$ ; $x^2+x+1$ ; $x^3+x^2+1$ ; $x^3+x+1$ ; $x^4+x^3+x^2+x+1$ ; $x^4+x^3+1$ ; $x^4+x+1$ ;

**a**) $x^8+x^7+x^6+x^4+1 = (x^4+x^3+x^2+x+1)(x^4+x+1)$ ;
**b**) $x^6+x^4+x^3+x^2+1 = (x^4+x^3+x^2+x+1)\ x^2+x+1)$ ;
**c**) $x^{16}-x = x\ (x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)$ ;
**d**) $x^7+x^6+x^4+1 = (x+1)(x^6+x^3+x^2+x+1) = (x+1)(x^2+x+1)(x^4+x^3+1)$.

Ejercicio **E24** de pag. 134 del texto :
" En $\mathbf{C}[x]$ , halle el máximo común divisor de los dos polinomios :
$(t-2)^3(t-3)^4(t-i)$ , $(t-1)(t-2)(t-3)^3$ " $\Rightarrow$ $(t-2)(t-3)^3$ ,
[ considerando los factore scomunes con el mínimo exponente ]

**SE97.-** Resuelva los ejercicios E4, E5 , E8, E9 , E11, E12 , E14, E15 , de las páginas 168 hasta 172 del texto de Lindsay Childs.
Ejercicios **E4,E5** de pag. 168-169 del texto :
" halle todos los ceros racionales de cada uno de los siguientes polinomios :
$x^3-x+1$ , $x^3-x-1$ , $x^3+2x+10$, $x^3-2x^2+x+15$ , $x^7-7$ , $2x^2-3x+4$ , $2x^4-4x+3$ ".
Recordando el teorema del resto y el hecho que si $\frac{a}{b}$ es una fracción irreducible que anula al polinomio $a_0+a_1x+...a_nx^n$ entonces $a \mid a_0$ y $b \mid a_n$ resulta que ninguno de los polinomios dado tiene algun cero racional.

Ejercicio **E8** de pag. 171 del texto :
" Es posible que $f(x)$ sea reducible en $\mathbf{Z}[x]$ , irreducible en $\mathbf{Z}_p[x]$ en el caso que p divida al coeficiente del monomio de grado máximo de f ? "
Es posible; por ejemplo sean $p=2$ , $f(x) = 2x^2-x-1$ .

Ejercicio **E9** de pag. 171 del texto :
"Dé un ejemplo de polinomio mónico $f(x) \in \mathbf{Z}[x]$ que sea irreducible en $\mathbf{Q}[x]$ pero se factorice módulo 2, 3, 5 " .
Ver **iv**), **v**) del ejercicio **E92** : el polinomio $x^4+1$ es irreducible en $\mathbf{Q}[x]$ y sin embargo se factoriz en todo $\mathbf{Z}_p[x]$ en producto de dos polinomios de primer grado.
Ejercicio **E11** de pag. 171 del texto : "factorice $x^4+4$ en $\mathbf{Q}[x]$ " .
$x^4+4 = x^4+4x^2+4 - 4x^2 = (x^2+2)^2-(2x)^2 = (x^2+2+2x)((x^2+2-2x)$ .

Ejercicio **E12** de pag. 171 del texto :
"demuestre que $f(x) = 2x^4-8x^2+1$ es irreducible en $\mathbf{Q}[x]$ "
recordando el ejercicio **E88-ii**) :
$x^4f(\frac{1}{x}) = x^4-8x^2+2$ = irreducible aplicando criterio de Eisenstein con $p=2$ .

Ejercicio **E14** de pag. 172 del texto :
"demuestre que cada uno de los siguientes polinomios es irreducible en **Q**[x] :"
**a**) $x^4+x+1$ ; **b**) $x^4+3x+5$ ; **c**) $3x^4+2x^3+4x^2+5x+1$ son irreducibles ya que en $\mathbf{Z}_2[x]$ los tres estan representados por el polinomio $x^4+x+1$ que es irreducible en $\mathbf{Z}_2[x]$ ( y 2 no divide al coeficiente de $x^4$) ; en efecto este polinomio no se anula para ningín valor de x ($\in \mathbf{Z}_2$) y por otra parte no es producto de polinomios irreducibles de segundo grado en $\mathbf{Z}_2[x]$ , ya que el único polinomio irreducible de segundo grado en $\mathbf{Z}_2[x]$ es $x^2+x+1$ y se tiene $(x^2+x+1)^2= x^4+x^2+1 \neq x^4+x+1$ ;
**d**)$x^5+5x^2+4x+7$ **e**) $15x^5-2x^4+15x^2-2x+15$ : actuando de nuevo en $\mathbf{Z}_2[x]$ , observamos que ámbos polinomios se escriben $x^5+x^2+1$ ; si este polinomio tiene alguna factorización propia, necesariamente uno de los factores tiene grado 1 o 2; observemos entonces que el polinomio dado no se anula para ningín valor de x ($\in \mathbf{Z}_2$) y tampoco es divisible por el único polinomio irreducible de grado 2 en $\mathbf{Z}_2[x]$ ya que $x^5+x^2+1=(x^2+x+1)(x^3+x^2)+1$ . Por lo tanto el polinomio dado es irreducible en $\mathbf{Z}_2[x]$ y por consiguiente en **Z**[x] y en **Q**[x] ;

Ejercicio **E15** de pag. 172 del texto :
"demuestre que el siguiente polinomio es irreducible módulo 3 pero es reducible módulo 2 : $f(x)= x^5+4x^4+2x^3+3x^2-x+5$ ".
En $\mathbf{Z}_2[x]$ se tiene f(1)= 0 por lo cual x+1 =x-1 es un factor propio del polinomio dado;
En $\mathbf{Z}_3[x]$ se tiene $f(x) = x^5+x^4+2x^3+2x+2$ ; si f(x) fuese reducible, debería tener almenos un factor irreducible de grado uno o dos ; en **SE74** se halló que hay tres polinomios (mónicos) irreducibles de grado 2 en $\mathbf{Z}_3[x]$ : $x^2+x+2$, $x^2+2x+2$, $x^2+1$ ;
Como f(0)=f(1)=f(2)=2≠0 por el teorema del resto tenemos que f no tiene ningún factor de primer grado;
por otra parte efectuando las correspondientes divisiones, obtenemos :
$x^5+x^4+2x^3+2x+2 = (x^2+1)(x^3+x^2+2) + 2x$ ;
$x^5+x^4+2x^3+2x+2 =( x^2+x+2)x^3 + 2x+2$ ;
$x^5+x^4+2x^3+2x+2 = (x^2+2x+2)(x^3+2x^2+2x+1)+2x$ de lo cual sigue que ninguno de los tres polinomios mónicos irreducibles es factor de f(x), así que en definitiva f(x) es irreducible en $\mathbf{Z}_3[x]$ .

**SE98.**- Ejemplo de polinomio con coeficientes reales que se factorice en un producto de 3 factores irreducibles en **R**[x] y en producto de 5 factores irreducibles en **C**[x] :

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

**E99.**- Diga cual es el número mínimo y cual es el número máximo de factores irreducibles en que puede factorizarse un polinomio de grado 17 en **R**[x] .
mínimo 9 , máximo 17.

**E100.**- Dé un ejemplo de polinomio mónico, con coeficientes enteros que sea irreducible en **Z**[x] pero reducible en $\mathbf{Z}_{23}[x]$ .
$x^2+23$

**E101.-** Averigüe (y justifique) si los siguientes polinomios son o no son irreducibles en **Q**[x] :

**i**) $x^4+\frac{5}{3}x^3+10x^2+45$ es asociado de $3x^4+5x^3+30x^2+135$ y es irreducible como se constata aplicando el criterio de Eisenstein con p=5;

**ii**) $309867.x^2+20000123.x+4056781$ se escribe $x^2+x+1$ en $\mathbf{Z}_2[x]$ por locual resulta ser irreducible.

**E102.-** Factorice los siguientes polinomios en producto de factores irreducibles en **Z**[x] :

**i**) $f(x) = 2x^4+x^3+6x^2+9x+3$ ; posibles ceros racionales son $\pm1$, $\pm3$, $\pm\frac{1}{2}$, $\pm\frac{3}{2}$

y se halla que $f(-\frac{1}{2})= 0$ de lo cual sigue :

$2x^4+x^3+6x^2+9x+3 = (2x+1)(x^3+3x+3)$ y esta es la factorización pedida ya que el polinomio $x^3+3x+3$ es irreducible [Eisenstein con p=3] ;

**ii**) $g(x) = 5x^4+x^3+6x^2+9x+3$ ; posibles ceros racionales son $\pm1$, $\pm3$, $\pm\frac{1}{5}$, $\pm\frac{3}{5}$ sin embargo ninguno de ellos anula al polinomio dado.

Por consiguiente, si g(x) es reducible será producto de dos polinomios irreducibles de grado 2 : $g(x)=a(x)b(x)$ con
$a(x) = a_0+a_1x+a_2x^2$ , $b(x)= b_0+b_1x+b_2x^2$ ;
$5x^4+x^3+6x^2+9x+3= a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2$;
$a_0b_0=3 \Rightarrow$ uno de los dos factores (y uno solo) es =3 ; sea por ej. $a_0=3$ , $b_0=1$ ;
[nota: si fuese $a_0=-3$, $b_0=-1$ bastaría considerar los opuestos de los dos polinomios a, b];
$(a_0b_1+a_1b_0) = 9 \Rightarrow a_1b_0 = 9 - a_0b_1 = 3(3 - b_1) =$ múltiplo de $3 \Rightarrow a_1=$ múltiplo de 3;
$(a_0b_2+a_1b_1+a_2b_0)=6 \Rightarrow a_2b_0= 6 - (a_0b_2+a_1b_1)=$ múltiplo de $3 \Rightarrow a_2=$ múltiplo de 3
por lo cual todo el polinomio a(x) resultaría ser múltiplo de 3, lo cual no es posible ya que por ejemplo tendríamos $5 = a_2b_2=$ múltiplo de 3, lo cual no se cumple.
En conclusión el polinomio $5x^4+x^3+6x^2+9x+3$ es irreducible.