Septiembre 2020 Original.

Ejercicio 1. Justifique si el anillo Z x Z/(32) es un dominio de integridad o no. Determine sus unidades.

Solución: Los elementos de anillo producto Z x Z/(32) son de la forma (a,[b]) donde [b] es una clase de resto módulo 32. El producto se hace coordenada a coordenada.

No es dominio de integridad pues tiene divisores de cero. Por ejemplo, (1,[0]) y (0,[1]) lo son ya que no son nulos y (1,[0]) · (0,[1]) = (0,[0]).

Las unidades son (u,[v]) con u unidad de Z y [v] unidad de Z/(32), pues si (u,[v]) · (u',[v']) = (1,[1]) entonces u·u' = 1 y [v]·[v'] = [1]. La penúltima igualdad implica que u es unidad de Z y la última, que [v] es unidad en Z/(32).

Las unidades de Z son +1 y -1. Las unidades de Z/(32) son los restos que son primos con 32. Como 32 es una potencia de 2, los primos con 32 son los números impares. Por tanto, las unidades son (1,[v]) y (-1,[v]) con v impar.

Ejercicio 2. Hay que hallar el resto de la división de 2020^2020 entre 19.

Solución: Como 19 es un número primo y 2020 y 19 son primos entre sí, podemos aplicar el Pequeño Teorema de Fermat. Por tanto, sabemos que 2020^18 CONG 1 (mod 19).
Por otra parte, 2020^2020 = 2020^(18 · 112 + 4) = (2020^18)^112 · 2020^4. El primer factor es CONG 1 (mod 19). Para el segundo factor tenemos 2020 CONG 6 (mod 19). 2020^2 CONG -2 (mod19), 2020^4 CONG 4 (mod 19).

Así pues, el resto de la división de 2020^2020 entre 19 es 4.

Ejercicio 3. Estudie si el polinomio f(T)= T^4-T^3+2T+1 es irreducible en Z[T] y en Q[T].

Solución:
Estudiamos en primer lugar si f tiene raíces enteras. Si r es una raíz entera de f, entonces r divide al término independiente de f. Por tanto, en este caso es suficiente con probar con los divisores de 1 que son +1 y -1. Por ser

$f(1)=3$, $f(-1)=1$ ambos distintos de cero, queda probado que f no tiene raíces enteras.

Veamos si el polinomio se puede factorizar como producto de dos polinomios de grado 2, es decir,

f(T)=(T^2+aT +b)(T^2+cT+d)= T^4+(a+c)T^3+(b+d+ac)T^2+(ad+bc)T +db.

Igualando coeficientes:

a+c=-1
b+d+ac=0
ad+bc=2
db=1

De la última igualdad obtenemos dos casos

d=b=1
d=b=-1

Multiplicamos la primera ecuación por b y obtenemos, en ambos casos

ab+bc=-b. Por ser b=d resulta
ad+bc=-b distinto de 2, que contradice la tercera igualdad.

Por lo que el sistema no tiene solución en Z.

Por el lema de Gauss, al pertenecer f a Z[T],   f es irreducible en   Z[T] si y solo si   lo es Q[T], por lo que tampoco es irreducible en Q[T].

Ejercicio 4.
(a) Determine el grado de la extensión de cuerpos Q(raiz(3), raiz(5))/Q
(b) Estudie si Q(raiz(3), raiz(5))/Q es una extensión de Galois.

Solución: (a) Grado de la extensión:
- El grado de la extensión Q(raiz(3))/Q es 2.
- raíz(5) no pertenece a Q(raiz(3)) pues en tal caso sería raiz(5)=a + b raiz (3) con a y b pertenecientes a Q, y elevando al cuadrado los dos miembros de la igualdad se llega a una contradicción.

El polinomio mínimo de raiz(5) sobre Q(raiz(3)) es T^2-5 irreducible por Eisenstein, luego

[Q(raiz(3), raiz(5)): Q(raíz(3))]=2 y por tanto

[Q(raiz(3), raiz(5)): Q] = [Q(raiz(3), raiz(5)) : Q(raiz(3))] [Q(raiz(3)) : Q]=**4**

(b) Para determinar si es de Galois hay que buscar un elemento primitivo **u**, su polinomio mínimo sobre Q, y comprobar si todas las raíces del polinomio pertenecen a Q(u)**.**

<u>Un elemento primitivo</u> es **u=raíz(3)+raíz(5)** , es decir, Q(u)= Q(raíz(3), raíz(5)). Un contenido es trivial. Vemos el otro: Q(raiz(3), raiz(5)) contenido en Q(u):

u=raiz(3)+raiz(5), u^2=8+2raiz(15), u^3=18 raiz(3)+14raiz(5), entonces

raiz(3)=(u^3-14u)/4 pertenece a Q(u) y raiz(5)= (u^3-18u)/-4 pertence a Q(u),

Por tanto Q(u)= Q(raiz(3), raiz(5)).

<u>Polinomio mínimo de u</u>: De las potencias calculadas se tiene que (u^2-8)^2=60 implica u^4-16u+4=0. Luego

f = T^4 - 16T^2 + 4

es un polinomio anulador de u. No hace falta probar que es irreducible, si previamente hemos demostrado que el grado de la extensión es 4 y que u es un elemento primitivo, ya que el polinomio mínimo es el único polinomio de grado cuatro, mónico que tiene a u por raíz. Sí hace falta demostrar que es irreducible si previamente no hemos demostrado que el grado de la extensión es 4 y u es elemento primitivo. Para demostrar la irreducibilidad del polinomio, en algunos exámenes se ha aplicado erróneamente el criterio de Eisenstein con p=4, pues 4 no es irreducible.

Las raíces de f, soluciones de la ecuación bicuadrada T^4-16T^2+4=0, cumplen

T^2 = 8 + 2 raíz(5) o bien T^2 = 8 - 2 raíz(5)

Además las raíces son: u, -u , v y -v tales que

u^2=8+2 raíz(5) y v^2=8-2 raíz(5)

Haciendo el producto

u^2 v^2=4 implica (uv=2 o uv=-2) implica (v=2 inverso(u) o v=-2 inverso(u))

en cualquier caso, v pertenece a Q(u) y así, Q(u)/Q es una extensión de Galois.