Álgebra I. Hoja de ejercicios 7: Dominios de factorización única (Aritmética III)
Universidad de El Salvador, ciclo impar 2019

Por cualquier pregunta, no duden en escribir al grupo ues-algebra-2019@googlegroups.com.

Ejercicio 1 (Euclides)**.** Sea A un dominio de factorización única que no es un cuerpo y que tiene un número finito de elementos invertibles $A^\times$. En este ejercicio vamos a probar que en A hay un número infinito de elementos primos no asociados entre sí.

0) Asumamos que $p_1, \dots, p_s$ son todos los primos no asociados entre sí en A.

1) Demuestre que para algún $n = 1, 2, 3, \dots$ se tiene

$$(p_1 \cdots p_s)^n + 1 \notin A^\times.$$

2) Demuestre que $(p_1 \cdots p_s)^n + 1$ no es divisible por ningún primo entre $p_1, \dots, p_s$. Esto nos da una contradicción: un elemento no nulo y no invertible que no es divisible por ningún primo.

Ejercicio 2. Demuestre que si k es un cuerpo finito, entonces hay un número infinito de polinomios irreducibles $f \in k[X]$.
Sugerencia: use el ejercicio anterior.

Ejercicio 3. Exprese el número 420 como un producto $u p_1^{k_1} \cdots p_s^{k_s}$ en $\mathbb{Z}[i]$, donde $u \in \mathbb{Z}[i]^\times$ y $p_1, \dots, p_s$ son primos de Gauss no asociados entre sí.

Ejercicio 4. Demuestre que en un dominio de factorización única A, si $\operatorname{mcd}(a, b) = 1$ y $ab = c^k$ para algún $c \in A$ y $k = 1, 2, 3, \dots$, entonces existen $a', b' \in A$ tales que $a \sim a'^k$ y $b \sim b'^k$.

Ejercicio 5. En el anillo $\mathbb{Z}[\sqrt{-7}]$ consideremos los números $\alpha = 1 + \sqrt{-7}$ y $\beta = 1 - \sqrt{-7}$.

1) Demuestre que $\operatorname{mcd}(\alpha, \beta) = 1$.

2) Demuestre que $\alpha\beta$ es un cubo, pero α y β no son asociados con cubos en $\mathbb{Z}[\sqrt{-7}]$.

Ejercicio 6. Asumamos que a, b, c son números enteros positivos tales que

$$a^2 + b^2 = c^2$$

y $\operatorname{mcd}(a, b) = 1$. En este caso se dice que (a, b, c) es una **terna pitagórica primitiva**.

1) Demuestre que uno de los números a y b debe ser impar y el otro debe ser par.
Asumamos que a es impar y b es par.

2) Usando el ejercicio 4, demuestre que existen números enteros u, v tales que

$$a + bi = (u + vi)^2 \quad \text{en } \mathbb{Z}[i],$$

y entonces

$$a = u^2 - v^2, \quad b = 2uv.$$