ÁLGEBRA ABSTRACTA Y CODIFICACIÓN: EJERCICIOS SEMANA 9

MAURO ARTIGIANI

Reglas del juego

Los ejercicios serán resueltos en la monitoria y se evaluará, a todos los estudiantes, el mismo ejercicio elegido al azar (1). Las notas de estas entregas semanales constituirá el 15 % de nota de la monitoria. Se aconseja de solucionar estos ejercicios en grupos pequeños.

Las entregas de ejercicios serán aceptadas en formato `pdf`, escribiendo las soluciones en LaTeX(u otro editor de texto). También se pueden enviar escaneos o fotografiás de ejercicios escritos a mano. En este caso se pide utilizar hojas blancas o con lineas (no cuadriculados) y escribir con un bolígrafo negro o azul oscuro (para facilitar el contraste). También se pide que las soluciones sean escritas de manera ordenada; se puede cambiar el orden de las soluciones.

Importante: Si las fotos no son legibles los ejercicios **no** serán calificados.

Fecha de entrega: 08 Octubre 2020.

Ejercicios

1. Demuestre que 3, $1+\sqrt{-5}$ y $1-\sqrt{-5}$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$.
2. Sea R un PID. Sean $a, b, c \in R$ con $\gcd(a, b) = 1$. Demuestre que si $a \mid bc$ entonces $a \mid c$.
3. *a*) Sea $U \subseteq R$ un ideal. Demuestre que se U contiene una unidad entonces $U = R$.
   b) Sea R un anillo conmutativo con unidad. Demuestre que R es un campo si y solo si los únicos ideales de R son $\langle 0\rangle$ y $\langle 1\rangle$.
4. Sea R un PID y sea $a \in R$ con $a \neq 0$. Demuestre que $\langle a\rangle$ es un ideal maximal de R si y solo si a es irreducible.
   [*Sugerencia: utilize el ejercicio 3.a*]
5. *a*) Sea p un número entero primo. Demuestre que o p sigue siendo primo en $\mathbb{Z}[i]$ o p es el producto de dos primos en los enteros de Gauss conjugados: $p = \pi\overline{\pi}$;
   [*Sugerencia:* $\pi \mid p \implies \overline{\pi} \mid p$.]
   b) Sea π un primo en los enteros de Gauss. Luego o $\pi\overline{\pi}$ es un primo en $\mathbb{Z}$ o es el cuadrado de un primo en $\mathbb{Z}$.
   [*Sugerencia: una factorización en primos en $\mathbb{Z}$ es todavía una factorización en $\mathbb{Z}[i]$, no necesariamente en irreducibles.*]

   Observación: este ejercicio implica que los primos en $\mathbb{Z}[i]$ son los primos $p \in \mathbb{Z}$ que no se pueden escribir como suma de cuadrados o los elementos de la forma $a + bi$ tales que $a^2 + b^2$ sea un primo en $\mathbb{Z}$. Un teorema de teoría de los números dice que $p \in \mathbb{Z}$ es una suma de cuadrados si y solo si $p = 2$ o $p \equiv 1 \pmod 4$.

Date: 02 Octubre 2020.