## Álgebra II. Hoja de ejercicios 6: Aritmética
## Universidad de El Salvador, ciclo par 2018

Por cualquier pregunta, no duden en escribir al grupo ues-algebra-2@googlegroups.com.

**Ejercicio 13.1.** *Hemos notado que el anillo $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única. En este ejercicio vamos a probar que en efecto $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de ideales principales. De nuevo, nos va a servir la norma*

$$N(a+b\sqrt{-5}) := (a+b\sqrt{-5})\,(a-b\sqrt{-5}) = a^2+5\,b^2.$$

*Consideremos el ideal $I = (3, 2+\sqrt{-5})$. Supongamos que $I = (\alpha)$ para algún $\alpha \in \mathbb{Z}[\sqrt{-5}]$. En particular, existen $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$ tales que*

$$3 = \beta\alpha, \quad 2+\sqrt{-5} = \gamma\alpha.$$

*Analice las normas y obtenga una contradicción. Concluya que el ideal $I$ no es principal.*

**Ejercicio 13.2.** *Sea $n \ge 3$ un entero libre de cuadrados. En este ejercicio vamos a probar que el anillo $\mathbb{Z}[\sqrt{-n}]$ no es un dominio de factorización única. (Los anillos $\mathbb{Z}[\sqrt{-1}]$ y $\mathbb{Z}[\sqrt{-2}]$ son dominios euclidianos y por ende sí son dominios de factorización única.) Consideremos la norma*

$$N(a+b\sqrt{-n}) := (a+b\sqrt{-n})\,(a-b\sqrt{-n}) = a^2+n\,b^2.$$

1) *Demuestre que $2$ es irreducible en $\mathbb{Z}[\sqrt{-n}]$.*
2) *Demuestre que $1\pm\sqrt{-n}$ es irreducible en $\mathbb{Z}[\sqrt{-n}]$.*
   *Indicación: si $1\pm\sqrt{-n} = xy$ para $x,y \notin \mathbb{Z}[\sqrt{-n}]^\times$, analice las normas.*
3) *Si $n$ es par, demuestre que $2 \mid (\sqrt{-n})^2$, pero $2 \nmid \sqrt{-n}$.*
4) *Si $n$ es impar, demuestre que $2 \mid (1+\sqrt{-n})\,(1-\sqrt{-n})$, pero $2 \nmid (1\pm\sqrt{-n})$.*

*Concluya que $2$ es un elemento irreducible, pero no es primo, así que $\mathbb{Z}[\sqrt{-n}]$ no puede ser un dominio de factorización única.*

**Ejercicio 13.3.** *Ya sabemos que los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ forman un dominio de factorización única. En este ejercicio vamos a describir los elementos primos (irreducibles) en $\mathbb{Z}[\sqrt{-1}]$. Para encontrarlos, hay que factorizar los enteros primos $p = 2,3,5,7,11,\ldots$ en $\mathbb{Z}[\sqrt{-1}]$.*

1) *Demuestre que si para un elemento $\pi = a+b\,\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ la norma $N(\pi) = a^2+b^2 = p$ es un número entero primo, entonces $\pi$ es un elemento primo en $\mathbb{Z}[\sqrt{-1}]$.*
2) *Sea $\pi$ un elemento primo en $\mathbb{Z}[\sqrt{-1}]$. Demuestre que $\pi \mid p$ donde $p$ es un número entero primo. Factorice $2,3,5$ en elementos primos en $\mathbb{Z}[\sqrt{-1}]$.*
   *Sugerencia: note que $\pi \mid N(\pi)$.*
3) *Sea $p \in \mathbb{Z}$ un número entero primo. Demuestre que $p$ es compuesto en $\mathbb{Z}[\sqrt{-1}]$ si y solamente si $p = a^2+b^2$ para algunos $a,b \in \mathbb{Z}$, y en este caso $p$ se descompone en dos factores primos conjugados.*

**Comentario.** En la teoría de números elemental se demuestra que un primo $p \in \mathbb{Z}$ puede ser escrito como una suma de dos cuadrados $a^2+b^2$ si y solamente si $p = 2$ o $p \equiv 1 \pmod 4$.

**Ejercicio 13.4.** *Demuestre que el anillo $\mathbb{Z}[\sqrt{-2}]$ es un dominio euclidiano respecto a la norma habitual*

$$N(a+b\sqrt{-2}) := (a+b\sqrt{-2})\,(a-b\sqrt{-2}) = a^2+2\,b^2.$$

**Ejercicio 13.5.** *Demuestre que el anillo* $\mathbb{Z}[\omega]$ *donde* $\omega := \frac{1+\sqrt{-3}}{2}$ *es un dominio euclidiano respecto a la norma habitual*

$$N(a+b\,\omega) := (a+b\,\omega)\,(a+b\,\overline{\omega}) = a^2+ab+b^2.$$

**Ejercicio 13.6.** *Sea* $p$ *un número primo. Para el anillo* $\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \mid a,b \in \mathbb{Z},\ p \nmid b \right\}$ *definamos*

$$v_p\left(\frac{a}{b}\right) := \text{máx}\{k \mid p^k \mid a\}, \quad v_p(0) := +\infty.$$

1) *Demuestre que para cualesquiera* $x,y \in \mathbb{Z}_{(p)}$ *se cumple*

$$v_p(xy) = v_p(x) + v_p(y).$$

2) *Demuestre que todo elemento no nulo* $x \in \mathbb{Z}_{(p)}$ *puede ser escrito como* $up^n$ *donde* $u \in \mathbb{Z}_{(p)}^\times$ *y* $n = v_p(x)$.

3) *Demuestre que todo elemento irreducible en* $\mathbb{Z}_{(p)}$ *está asociado con* $p$.

4) *Demuestre que* $\mathbb{Z}_{(p)}$ *es un dominio euclidiano respecto a* $v_p$.

**Ejercicio 13.7.** *Sea* $k$ *un cuerpo. Consideremos el anillo de las series de potencias* $k[\![X]\!]$. *Definamos para* $f = \sum_{i\ge 0} a_i\,X^i \in k[\![X]\!]$

$$v_X(f) := \text{máx}\{i \mid a_i = 0\}, \quad v_X(0) := +\infty.$$

1) *Demuestre que para cualesquiera* $f,g \in k[\![X]\!]$ *se cumple*

$$v_X(fg) = v_X(f) + v_X(g).$$

2) *Demuestre que toda serie no nula* $f \in k[\![X]\!]$ *puede ser escrita como* $g\,X^n$ *donde* $g \in k[\![X]\!]^\times$ *y* $n = v_X(f)$.

3) *Demuestre que todo elemento irreducible en* $k[\![X]\!]$ *está asociado con* $X$.

4) *Demuestre que* $k[\![X]\!]$ *es un dominio euclidiano respecto a* $v_X$.

**Comentario.** $\mathbb{Z}_{(p)}$ y $k[\![X]\!]$ son ejemplos de **anillos de valuación discreta**.

**Ejercicio 13.8.** *Sea* $R$ *un dominio de integridad. Una* ***norma de Dedekind*** *es una función* $\delta\colon R\setminus\{0\} \to \mathbb{N}$ *que satisface la siguiente propiedad: para cualesquiera* $x,y \in R\setminus\{0\}$, *si* $x \nmid y$, *entonces existen* $a,b \in R$ *tales que*

$$ax+by \ne 0, \quad \delta(ax+by) < \delta(x).$$

*Demuestre que si sobre* $R$ *existe una norma de Dedekind, entonces* $R$ *es un dominio de ideales principales.*