Introducción a los Números Algebraicos
1. Introducción - entrega 27/3

Entrega de ejercicios. Cada ejercicio vale tantos puntos como partes o según se indique. Habrá 5 listas regulares con entregas 27/3, 12/4, 26/4, 10/5, 24/5 y una lista final. Hay que entregar ejercicios que sumen al menos 10 puntos en cada una de las listas regulares. La entrega de la lista final será luego de finalizado el curso y hay que sumar 20 puntos.

Página del curso. `http://www.cmat.edu.uy/~tornaria/2007/TNA/`

1. Se define $N : \mathbb{Z}[i] \to \mathbb{Z}$ (la *norma*) por $N(a+bi) = a^2 + b^2$.
   (a) Verificar que para todo $\alpha, \beta \in \mathbb{Z}[i]$, se tiene $N(\alpha\beta) = N(\alpha)N(\beta)$. Concluir que si $\alpha \mid \gamma$ en $\mathbb{Z}[i]$, entonces $N(\alpha) \mid N(\gamma)$ en $\mathbb{Z}$.
   (b) Sea $\alpha \in \mathbb{Z}[i]$. Mostrar que α es una *unidad* (i.e. inversible) sii $N(\alpha) = 1$. Concluir que las únicas unidades son ± 1 y $\pm i$.
   (c) Sea $\alpha \in \mathbb{Z}[i]$. Mostrar que si $N(\alpha)$ es un primo en $\mathbb{Z}$ entonces α es irreducible en $\mathbb{Z}[i]$. Mostrar que la misma conclusión vale si $N(\alpha) = p^2$ donde p es un primo en $\mathbb{Z}$ con $p \equiv 3 \pmod 4$.
2. (a) Mostrar que $1 - i$ es irreducible en $\mathbb{Z}[i]$, y que $2 = u(1-i)^2$ para alguna unidad u.
   (b) Notar que $(2+i)(2-i) = 5 = (1+2i)(1-2i)$. ¿Es esto consistente con factorización única?
3. Mostrar que $\mathbb{Z}[i]$ es un dominio de ideales principales (y, por lo tanto, es un dominio de factorización única). Sugerencia:
   (a) dado I un ideal de $\mathbb{Z}[i]$, ver que existe $\alpha \in I - \{0\}$ con $N(\alpha)$ minimal.
   (b) Mostrar que los múltiplos $\gamma\alpha$ con $\gamma \in \mathbb{Z}[i]$ son vértices de una familia infinita de cuadrados que cubren todo el plano complejo.
   (c) I contiene todos los $\gamma\alpha$. Mostrar por un argumento geométrico que si I contuviera otro número se contradeciría la minimalidad de $N(\alpha)$
4. Usar la factorización única de $\mathbb{Z}[i]$ para mostrar que todo primo $p \equiv 1 \pmod 4$ es suma de dos cuadrados.
   (a) Recordar que el grupo multiplicativo $(\mathbb{Z}/p)^\times$ de enteros módulo p es cíclico para mostrar que si $p \equiv 1 \pmod 4$ entonces $r^2 \equiv -1 \pmod p$ para algún $r \in \mathbb{Z}$.
   (b) Mostrar que p no puede ser irreducible en $\mathbb{Z}[i]$.
   (c) Concluir que p es suma de dos cuadrados.
5. (2p.) Describir todos los elementos irreducibles en $\mathbb{Z}[i]$.

6. Sea $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Se define $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ por $N(a + b\omega) = a^2 - ab + b^2$.

   (a) Mostrar que si $a+b\omega$ se escribe como $u+vi$ con u y v reales, entonces $N(a+b\omega) = u^2 + v^2$.

   (b) Mostrar que para todo $\alpha, \beta \in \mathbb{Z}[\omega]$, se tiene $N(\alpha\beta) = N(\alpha)N(\beta)$. Concluir que si $\alpha \mid \gamma$ en $\mathbb{Z}[\omega]$, entonces $N(\alpha) \mid N(\gamma)$ en $\mathbb{Z}$.

7. (a) Sea $\alpha \in \mathbb{Z}[\omega]$. Mostrar que α es una unidad sii $N(\alpha) = 1$, y encontrar todas las unidades en $\mathbb{Z}[\omega]$ (hay seis).

   (b) Mostrar que $1 - \omega$ es irreducible en $\mathbb{Z}[\omega]$, y que $3 = u(1 - \omega)^2$ para alguna unidad u.

8. (3p.) Modificar el ejercicio 3 para probar que $\mathbb{Z}[\omega]$ es un dominio de ideales principales (luego, es un dominio de factorización única). Aquí los cuadrados serán remplazados por paralelogramos.

9. En este ejercicio se demuestra la Conjetura de Fermat para $n = 4$. Si $x^4 + y^4 = z^4$ tiene solución en enteros positivos, entonces también $x^4 + y^4 = w^2$ tendrá solución. Sea x, y, w una tal solución con w el mínimo posible. Entonces x^2, y^2, w es una terna pitagórica primitiva. Asumiendo (sin pérdida de generalidad) que x es impar, podemos escribir

$$x^2 = m^2 - n^2, \qquad y^2 = 2mn, \qquad w = m^2 + n^2,$$

   con m y n enteros positivos relativamente primos, no ambos impares.

   (a) Mostrar que

$$x = r^2 - s^2, \qquad n = 2rs, \qquad m = r^2 + s^2,$$

   con r y s enteros positivos relativamente primos, no ambos impares.

   (b) Mostrar que r, s, y m son relativamente primos dos a dos. Usando que $y^2 = 4rsm$ concluir que r, s, y m son todos cuadrados, digamos a^2, b^2, y c^2.

   (c) Mostrar que $a^4 + b^4 = c^2$, y que esto contradice la minimalidad de w.

10. Sea R un dominio de integridad (anillo conmutativo con 1 y sin divisores de cero). Definimos una relación de equivalencia $\sim$ en el conjunto de ideales de R de la siguiente manera: dados dos ideales A y B

$$A \sim B \qquad \Longleftrightarrow \qquad \alpha A = \beta B \ \text{ con } \alpha, \beta \in R.$$

   (a) Probar que $\sim$ es una relación de equivalencia.

   (b) Mostrar que $A \sim B$ sii $A \cong B$ como R-módulos.

   (c) Ver que si A es un ideal en R y αA es principal para algún $\alpha \in R$ entonces A es principal. Concluir que los ideales principales forman una clase.

   (d) Mostrar que las clases en R forman un grupo sii para cada ideal A existe un ideal B tal que AB es principal.

11. Sea $K_m = \mathbb{Q}[\omega_m]$, donde $w_m = e^{\frac{2\pi i}{m}}$, el m-ésimo cuerpo ciclotómico.

    (a) Ver que $K_m = K_{2m}$ si m es impar.

    (b) Mostrar que $[K_m : \mathbb{Q}] = \varphi(m)$ y concluir que los K_m con m par son no isomorfos dos a dos.

12. (a) Mostrar que todo cuerpo de números de grado 2 sobre $\mathbb{Q}$ es uno de los cuerpos cuadráticos $\mathbb{Q}[\sqrt{m}]$ con $m \in \mathbb{Z}$.

    (b) Mostrar que los cuerpos $\mathbb{Q}[\sqrt{m}]$, con m libre de cuadrados, son no isomorfos dos a dos.

13. Sea I el ideal generado por 2 y $1 + \sqrt{-3}$ en el anillo $\mathbb{Z}[\sqrt{-3}] = \left\{a + b\sqrt{-3} \ : \ a, b \in \mathbb{Z}\right\}$.

    (a) Mostrar que $I \neq (2)$, pero $I^2 = 2I$; concluir que no hay factorización única para ideales de $\mathbb{Z}[\sqrt{-3}]$.

    (b) Mostrar que I es el único ideal primo conteniendo al ideal (2), y concluir que (2) no es producto de ideales primos.

14. (2p.) Sea $m \in \mathbb{Z}$ libre de cuadrados. Mostrar que el anillo de enteros de $\mathbb{Q}[\sqrt{m}]$ está dado por

$$\begin{cases} \mathbb{Z}\left[\sqrt{m}\right] & \text{si } m \equiv 2, 3 \pmod 4; \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

15. El anillo de *cuaterniones de Hamilton* es

$$\mathbb{H} := \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$$

    con la multiplicación dada por

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k$$

    (a) Mostrar que $(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$, y concluir que $\mathbb{H}$ es un anillo de división ("cuerpo" no conmutativo)

    (b) Ver que i y que $\frac{4i+3j}{5}$ son enteros, pero que ni su suma ni su producto lo son. Concluir que el conjunto de enteros de $\mathbb{H}$ *no* es un anillo, y que existe más de un orden (anillo de enteros) maximal.

16. (a) Mostrar que 1 y -1 son las únicas unidades en el anillo de enteros de $\mathbb{Q}[\sqrt{m}]$ con m libre de cuadrados, $m < 0$ y $m \neq -1, -3$.

    (b) ¿Qué pasa cuando $m = -1$ o $m = -3$?

17. (a) Mostrar que $1 + \sqrt{2}$ es una unidad en $\mathbb{Z}[\sqrt{2}]$, pero no es una raíz de 1.

    (b) Usar las potencias de $1 + \sqrt{2}$ para generar infinitas soluciones en enteros de la ecuación $a^2 - 2b^2 = \pm 1$.

18. (a) Mostrar que $\mathbb{Z}[\sqrt{-5}]$ no contiene elementos de norma 2 o 3.

    (b) Verificar que $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ es un ejemplo de factorización no única en el anillo de enteros $\mathbb{Z}[\sqrt{-5}]$.