Tarea 1 – Aritmética

Profesor: Pedro Montero, Ayudante: Tobías Martínez
Departamento de Matemática, Universidad Técnica Federico Santa María

Fecha de entrega:[1] Hasta el Domingo 16 de Abril de 2023 a las 23h59.

Esta Tarea puede ser realizada en grupos de 1 o 2 personas, y se debe indicar el nombre de cada integrante.

Problemas de clases

1. Recuerdos de Álgebra Abstracta (10 puntos)

Elija sólamente 1 ejercicio para resolver.

1. Sea $\mathbf{K}$ un cuerpo y $F \in \mathbf{K}[X] \setminus \{0\}$ polinomio irreducible. Probar que el anillo cociente $\mathbf{K}[X]/\langle F\rangle$ es un cuerpo.

   Indicación: Probar que $\langle F\rangle \subseteq \mathbf{K}[X]$ es un ideal maximal.

2. Sea A un anillo conmutativo, y sea $F \in A[X]$ con coeficiente líder 1. Probar que $A[X]/\langle F\rangle$ es un A-módulo libre con base dada por $(\overline{1}, \overline{X}, \ldots, \overline{X}^{\deg(F)-1})$.

2. Clausura integral (10 puntos)

Elija sólamente 1 ejercicio para resolver.

1. Sea B una A-álgebra conmutativa. Supongamos que B es un A-módulo finitamente generado por $\{e_1, \ldots, e_m\}$, y que M es un B-módulo finitamente generado por $\{f_1, \ldots, f_n\}$. Probar que

   $$\{e_i f_j,\ 1 \leq i \leq m,\ 1 \leq j \leq n\}$$

   es un conjunto generador de M como A-módulo. En particular, M es un A-módulo finitamente generado.

2. Encontrar $P \in \mathbf{Z}[X]$ mónico tal que $P(\sqrt{2}+\sqrt{3}) = 0$.

3. Sea $\tilde{A} \subseteq B$ la clausura integral de A en B. Demostrar que $\tilde{\tilde{A}} = \tilde{A}$, es decir, que si $\alpha \in B$ es entero sobre $\tilde{A}$ entonces necesariamente $\alpha \in \tilde{A}$.

4. Sean $A \subseteq B$ anillos conmutativos con B entero sobre A, sea $\mathfrak{q}$ un ideal primo de B y defina $\mathfrak{p} := \mathfrak{q} \cap A$. Demuestre que $\mathfrak{p}$ es un ideal primo y que $B/\mathfrak{q}$ es entero sobre $A/\mathfrak{p}$.

3. Extensiones de cuerpos y Anillos de enteros (20 puntos)

Elija 2 ejercicios para resolver.

1. Sean $\mathbf{L}/\mathbf{K}$ y $\mathbf{M}/\mathbf{L}$ extensiones de cuerpos. Probar que:

   (a) Si $\mathbf{L}/\mathbf{K}$ es una extensión finita, entonces $\mathbf{L}/\mathbf{K}$ es una extensión algebraica.

   (b) $[\mathbf{M} : \mathbf{K}] = [\mathbf{M} : \mathbf{L}][\mathbf{L} : \mathbf{K}]$.

   (c) Si $\alpha \in \mathbf{L}$ es algebraico sobre $\mathbf{K}$, entonces $\mu_\alpha^{\mathbf{K}} \in \mathbf{K}[X]$ es un polinomio irreducible, y además

   $$\mathbf{K}[X]/\langle \mu_\alpha^{\mathbf{K}}\rangle \xrightarrow{\simeq} \mathbf{K}[\alpha] =: \mathbf{K}(\alpha)$$

   es un isomorfismo de cuerpos.

   (d) Deducir que $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.

2. Calcular $\mathrm{Tr}_{\mathbf{C}/\mathbf{R}}(\alpha)$ y $\mathrm{N}_{\mathbf{C}/\mathbf{R}}(\alpha)$ para todo $\alpha \in \mathbf{C}$.

3. Calcular el discriminante $d_{\mathbf{K}}$ para $\mathbf{K} = \mathbf{Q}(\sqrt{d})$ con $d \in \mathbf{Z} \setminus \{0\}$ entero libre de cuadrados (i.e., de la forma $d = \pm p_1 \cdots p_r$ donde los p_i son primos distintos).

[1] Factor de retraso: 0.7 por 1 día de retraso, 0.55 por 2 días de retraso, 0.01 por 3 días de retraso.

4. Sea $\mathbf{L}/\mathbf{K}$ una extensión cuadrática (i.e., $[\mathbf{L} : \mathbf{K}] = 2$) y sea $\alpha \in \mathbf{L} \setminus \mathbf{K}$ tal que $\mathbf{L} = \mathbf{K}(\alpha)$, y donde $\mu_\alpha^{\mathbf{K}} = X^2+bX+c \in \mathbf{K}[X]$ es el correspondiente polinomio minimal. Calcular $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(1), \mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(\alpha)$ y $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(\alpha^2)$ en términos de $b, c \in \mathbf{K}$ y deducir que el discriminante de la forma bilineal

$$B : \mathbf{L} \times \mathbf{L} \longrightarrow \mathbf{K},\ (x, y) \longmapsto B(x, y) := \mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(xy)$$

está dado por $b^2 - 4c$ (i.e., coincide con el discriminante del polinomio $X^2 + bX + c$).

Problema 1 (20 puntos)

El objetivo de este problema es probar una versión efectiva del **Teorema del Elemento Primitivo** para cuerpos de números. Concretamente, probaremos que si $\mathbf{K} = \mathbf{Q}(\alpha_1, \ldots, \alpha_d)$ es una extensión finita de $\mathbf{Q}$ entonces existe $\alpha \in \mathbf{K}$ tal que $\mathbf{K} = \mathbf{Q}(\alpha)$.

Para comenzar, considere el caso particular en que $\mathbf{K} := \mathbf{Q}(\alpha, \beta)$. Sean $f(X) := \mu_\alpha^{\mathbf{Q}}(X), g(X) := \mu_\beta^{\mathbf{Q}}(X)$ los polinomios minimales de α y β sobre $\mathbf{Q}$ con $\deg(f) = n, \deg(g) = m$, y sean $\alpha_1, \ldots, \alpha_n \in \mathbf{C}$ y $\beta_1, \ldots, \beta_m \in \mathbf{C}$ las raíces de f y g con $\alpha_1 = \alpha, \beta_1 = \beta$.

1. Pruebe que $\alpha_i \neq \alpha_j$ para $i \neq j$.
2. Pruebe que existe $\lambda \in \mathbf{Q}$ tal que
$$\lambda \neq \frac{\alpha_i - \alpha}{\beta - \beta_j},$$
para todos $i \in \{1, \ldots, n\}$ y $j \in \{2, \ldots, m\}$.
Indicación: Notar que $\mathbf{Q}$ *es un cuerpo infinito.*

Con la notación del ítem (2), definamos $\theta := \alpha + \lambda\beta$ y $h(X) := f(\theta - \lambda X)$.

3. Demuestre que $\mathrm{mcd}(g(X), h(X)) = X - \beta$ en el anillo $\mathbf{Q}(\theta)[X]$.
4. Del resultado anterior (y de la definición de θ) concluya que $\alpha, \beta \in \mathbf{Q}(\theta)$ y luego $\mathbf{K} = \mathbf{Q}(\theta)$.
5. Demuestre, usando inducción, el caso general en que $\mathbf{K} = \mathbf{Q}(\alpha_1, \ldots, \alpha_d)$.

Problema 2 (20 puntos)

El objetivo de este problema es estudiar **cuerpos ciclotómicos**. Para ello consideremos $m \in \mathbf{N}^{\geq 1}$ fijo, y definamos inductivamente el m-ésimo polinomio ciclotómico $\Phi_m(T) \in \mathbf{Z}[T]$ mediante la fórmula

$$T^m - 1 = \prod_{d|m} \Phi_d(T).$$

Alternativamente, $\Phi_m(T) = \prod_{\substack{1 \leq k \leq m \\ \mathrm{mcd}(k,m)=1}} (T - e^{2\pi i k/m})$, donde $\deg(\Phi_m) := \varphi(m)$ es la función φ de Euler.

1. Calcular explícitamente $\Phi_6(T)$.
2. Sea p un número primo. Pruebe que $\Phi_p(T)$ es irreducible sobre $\mathbf{Q}[T]$ aplicando el *criterio de Eisenstein*[2] al polinomio $F(T) := \Phi_p(T + 1) \in \mathbf{Z}[T]$.
3. Sea p un número primo y $k \in \mathbf{N}^{\geq 1}$. Demuestre que $\Phi_{p^k}(T) = \Phi_p(T^{p^{k-1}})$ y concluya que $\Phi_m(T)$ es irreducible en $\mathbf{Q}[T]$ cuando $m = p^k$ es una potencia de un primo.

Para analizar el caso general con $m \in \mathbf{N}^{\geq 1}$ arbitrario, consideremos un primo p que no divida a m y supongamos (por contradicción) que $\Phi_m(T)$ tiene un factor $g(T)$ mónico irreducible. Así,

$$T^m - 1 = g(T)h(T) \text{ donde } g(T), h(T) \in \mathbf{Z}[T]$$

por el Lema de Gauss. Sea $\alpha \in \mathbf{C}$ una raíz de $g(T)$.

3. Probar que α^p es una raíz de $T^m - 1$. Deducir que si $g(\alpha^p) \neq 0$ entonces $g(T)$ divide a $h(T^p)$.

[2] El **criterio de Eisenstein** afirma que si p es un número primo y $F(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1T + a_0 \in \mathbf{Z}[T]$ es tal que p divide a todo a_i con $i \in \{0, \ldots, n-1\}$ pero p^2 no divide a_0, entonces $F(T)$ es irreducible en $\mathbf{Q}[T]$.

4. Use el hecho de que en el anillo $\mathbf{F}_p[T]$ se cumple el *freshman's dream* $h(T^p) = h(T)^p$ para demostrar que si $h(\alpha^p) = 0$, entonces $T^m - 1$ tiene una raíz doble en $\mathbf{F}_p$. Use el criterio de la derivada[3] para verificar que esto no es posible y concluya que $g(\alpha^p) = 0$ para *todo* primo p que no divide a m.

5. Concluya que $\Phi_m(T)$ y $g(T)$ tienen los mismos ceros y por tanto son iguales, con lo cual $\Phi_m(T)$ es irreducible.

Observación: La extensión $\mathbf{Q}(\zeta_m) \simeq \mathbf{Q}[T]/\Phi_m(T)$ es llamada la m-ésima extensión ciclotómica de $\mathbf{Q}$, donde ζ_m es una raíz m-ésima primitiva de la unidad. Note que $[\mathbf{Q}(\zeta_m) : \mathbf{Q}] = \varphi(m)$, el valor de la función φ de Euler en m.

Problema 3 (20 puntos)

El objetivo de este problema es calcular explícitamente anillos de enteros y discriminantes. Para ello consideramos el siguiente algoritmo (que, en la Tarea 1, aceptaremos como correcto):

Paso 1 Sea $\mathbf{K} = \mathbf{Q}(\alpha_1, \ldots, \alpha_r)$ una extensión de grado $[\mathbf{K} : \mathbf{Q}] = d$. Use el Problema 1 para determinar $\gamma \in \mathbf{K}$ tal que $\mathbf{K} = \mathbf{Q}(\gamma)$.

Paso 2 Encuentre $m \in \mathbf{Z}$ tal que $\alpha = m\gamma \in \mathscr{O}_{\mathbf{K}}$. De esta forma $\mathbf{K} = \mathbf{Q}(\alpha)$.

Paso 3 Defina $\beta_i = \alpha^{i-1}$ para cada $i \in \{1, \ldots, d-1\}$. Calcular $\Delta(\beta_1, \ldots, \beta_n) := \det((\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\beta_i\beta_j)_{1\leq i,j\leq d}) \in \mathbf{Z}$. Para esto último, puede utilizar directamente el siguiente hecho (sin demostración):

> **Hecho:** Supongamos que $[\mathbf{Q}(\alpha) : \mathbf{Q}] = d$ y escribamos $f := \mu_\alpha^{\mathbf{Q}} = (X - \alpha_1) \cdots (X - \alpha_d)$ en $\mathbf{C}[X]$. Entonces, $\Delta(1, \alpha, \ldots, \alpha^{d-1}) = \prod_{i<j}(\alpha_j - \alpha_i)^2 = (-1)^{d(d-1)/2} N_{\mathbf{Q}(\alpha)/\mathbf{Q}}(f'(\alpha))$.

Paso 4 Si $\Delta(\beta_1, \ldots, \beta_d)$ es libre de cuadrados, entonces $\mathscr{O}_{\mathbf{K}} = \mathbf{Z}[\alpha]$ y $d_{\mathbf{K}} = \Delta(\beta_1, \ldots, \beta_d)$. En caso contrario, considere el siguiente paso.

Paso 5 Considere el conjunto

$$A := \{p \in \mathbf{N} \text{ primo tal que } p^2 | \Delta(\beta_1, \ldots, \beta_d)\}.$$

Para cada $p \in A$ defina el conjunto *finito*

$$A_p = \{y = m_1\beta_1 + \ldots + m_d\beta_d \text{ donde } m_i \in \{0, 1, \ldots, p-1\}, (m_1, \ldots, m_d) \neq (0, \ldots, 0)\}.$$

Si para todo $p \in A$ **no existe** $y \in A_p$ tal que y/p es entero, entonces los β_i generan a $\mathscr{O}_{\mathbf{K}}$ y deducimos que $\mathscr{O}_{\mathbf{K}} = \mathbf{Z}[\alpha]$ y $d_{\mathbf{K}} = \Delta(\beta_1, \ldots, \beta_d)$. En caso contrario, considere el siguiente paso.

Paso 6 Sea $p \in A$ tal que p^2 divide $\Delta(\beta_1, \ldots, \beta_d)$ y sean $m_1, \ldots, m_d \in \{0, 1, \ldots, p-1\}$ no todos nulos tales que y/p es entero, donde $y = m_1\beta_1 + \ldots + m_d\beta_d$. Si algún $m_j = 1$, considere el siguiente paso. En caso contrario, tome un $m_j \neq 0$ y escoja un entero r tal que $rm_j \equiv 1 \pmod{p}$. Para $i \in \{1, \ldots, d\}$, sea $\mu_i \in \{0, 1, \ldots, p-1\}$ el *único entero* congruente a $rm_i \pmod{p}$. Note que $\mu_j = 1$, por construcción. Reemplace y por $\mu_1\beta_1 + \cdots + \mu_d\beta_d$.

Paso 7 Escoja el índice j tal que $m_j = 1$, y defina

$$\beta_i' := \begin{cases} \beta_i, & \text{si } i \neq j, \\ y/p, & \text{si } i = j. \end{cases}$$

Por construcción, los $\beta_1', \ldots, \beta_d' \in \mathscr{O}_{\mathbf{K}}$ y además $\Delta(\beta_1', \ldots, \beta_d') = \frac{1}{p^2}\Delta(\beta_1, \ldots, \beta_d)$.

Paso 8 Repita el procedimiento para $\beta_1', \ldots, \beta_d'$

Use el algoritmo anterior para encontrar el discriminante y el anillo de enteros del cuerpo $\mathbf{K} = \mathbf{Q}(\alpha)$, con

$$\alpha = \frac{1}{\sqrt[3]{2}}.$$

[3] Un polinomio no-constante $F \in \mathbf{K}[X]$ tiene una raíz múltiple en $\mathbf{K}$ si F y su derivada F' tienen al menos una raíz en común.