Tarea 2 – Aritmética

Profesor: Pedro Montero, Ayudante: Tobías Martínez

Departamento de Matemática, Universidad Técnica Federico Santa María

Fecha de entrega:[1] Hasta el Sábado 20 de Mayo 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**. Deben escoger 2 de los 3 problemas para resolver. Además, es posible realizar la tarea en grupos de 3 personas, pero en tal caso deben realizar **todos** los problemas.

Problema A: El Teorema 90 de Hilbert (50 puntos)

El objetivo de este problema es demostrar el famoso *Teorema 90 de Hilbert*. El nombre de dicho resultado proviene del hecho que es el Teorema 90 de un largo reporte de Hilbert en Teoría Algebraica de Números, llamado *Zahlbericht*. Originalmente, este resultado fue demostrado por Kummer (1855), y muchas veces es enunciado usando *cohomología de grupos*: el grupo $\mathrm{H}^1(\mathrm{Gal}(\mathbf{L}/\mathbf{K}), \mathbf{L}^\times)$ es trivial (E. Noether, 1933).

Teorema (Hilbert, 1897)**.** *Sea* $\mathbf{L}/\mathbf{K}$ *una* **extensión de Galois cíclica** (*i.e., tal que* $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ *es un grupo cíclico finito*) *y sea* σ *un generador del grupo de Galois. Entonces, para* $\alpha \in \mathbf{L}^\times$ *se tiene que*

$$\mathrm{N}_{\mathbf{L}/\mathbf{K}}(\alpha) = 1 \Leftrightarrow \alpha = \frac{\sigma(\beta)}{\beta} \text{ para algún } \beta \in \mathbf{L}^\times,$$

y

$$\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(\alpha) = 0 \Leftrightarrow \alpha = \sigma(\beta) - \beta \text{ para algún } \beta \in \mathbf{L}.$$

1. Pruebe que si $\alpha = \sigma(\beta)/\beta$ (resp. $\alpha = \sigma(\beta) - \beta$) entonces $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(\alpha) = 1$ (resp. $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(\alpha) = 0$).

Sea $n := [\mathbf{L} : \mathbf{K}]$. Para demostrar la otra implicancia del Teorema 90 de Hilbert, pruebe lo siguiente:

2. Para la norma, siga los siguientes pasos:
   (a) Sea $\alpha \in \mathbf{L}^\times$ tal que $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(\alpha) = 1$, y defina $f : \mathbf{L} \to \mathbf{L}$ por
   $$f(x) := \alpha x + \alpha\sigma(\alpha)\sigma(x) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^{n-1}(x).$$
   Probar que existe $x_0 \in \mathbf{L}^\times$ tal que $f(x_0) \neq 0$.
   Indicación: Utilice el Teorema de Dedekind sobre independencia de caracteres.
   (b) Demuestre que $f(x_0) = \alpha\sigma(f(x_0))$.
   (c) Concluya que podemos tomar $\beta := \dfrac{1}{f(x_0)}$.
3. Para la traza siga los siguientes pasos:
   (a) Sea $\alpha \in \mathbf{L}$ tal que $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(\alpha) = 0$, y defina $f : \mathbf{L} \to \mathbf{L}$ por
   $$f(x) = \alpha x + (\alpha + \sigma(\alpha))\sigma(x) + \cdots + (\alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha))\sigma^{n-1}(x).$$
   Demuestre que $f(x) = \sigma(f(x)) + \alpha\,\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(x)$ para todo $x \in \mathbf{L}$.
   (b) Justifique la existencia de $x_0 \in \mathbf{L}$ tal que $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(x_0) \neq 0$.
   (c) Concluya que podemos tomar $\beta := -\dfrac{f(x_0)}{\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(x_0)}$.
4. Utilice el Teorema 90 de Hilbert para probar que si $a, b \in \mathbf{Q}$ son tales que $a^2 + b^2 = 1$ entonces existen $c, d \in \mathbf{Z}$ tales que
   $$(a, b) = \left(\frac{c^2 - d^2}{c^2 + d^2}, \frac{2cd}{c^2 + d^2}\right).$$
   Indicación: Considerar la extensión $\mathbf{Q}(i)/\mathbf{Q}$ *y note que si* $a^2 + b^2 = 1$*, entonces* $\alpha = a + ib$ *tiene norma* 1*.*
5. Utilice el Teorema 90 de Hilbert para estudiar **extensiones de Kummer**. Más precisamente, para probar el siguiente resultado:

[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.

Teorema (Kummer): Sea $\mathbf{L}/\mathbf{K}$ una extensión de Galois cíclica de grado n con $\mathrm{mcd}(\mathrm{char}(\mathbf{K}), n) = 1$ y tal que $\mathbf{K}$ contiene una raíz primitiva n-ésima de la unidad ζ_n. Entonces existe $\beta \in \mathbf{K}$ tal que $\mathbf{L} = \mathbf{K}(\sqrt[n]{\beta})$, donde $\alpha := \sqrt[n]{\beta} \in \mathbf{L}$ es cualquier elemento tal que $\alpha^n = \beta$.

En otras palabras (y tal como ocurre para extensiones cuadráticas), si el cuerpo base contiene una raíz primitiva n-ésima de la unidad, entonces toda extensión cíclica de grado n se obtiene añadiendo la raíz n-ésima de algún elemento conveniente. Para ello, pruebe:

(a) Sea σ un generador de $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$. Usar el Teorema 90 de Hilbert para probar que existe $\beta \in \mathbf{L}^\times$ tal que $\sigma(\beta) = \zeta_n \beta$.

(b) Demuestre la órbita de β por el grupo de Galois tiene n elementos distintos.

(c) Deduzca que $\mathbf{L} = \mathbf{K}(\beta)$.

(d) Demuestre que $\beta^n \in \mathbf{K}$ (e.g. probando que pertenece al cuerpo fijo por $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$) y concluya que $\mathbf{L} = \mathbf{K}(\sqrt[n]{\alpha})$ donde $\alpha = \beta^n \in \mathbf{K}$.

Problema B: Fórmula explícita para el discriminante (50 puntos)

El objetivo de este problema es probar una explícita para calcular el discriminante de una extensión primitiva. Para ello, recordemos el siguiente resultado visto en clases:

Hecho: Sea $\mathbf{L}/\mathbf{K}$ una extensión finita de grado d y fijemos un incrustamiento $\mathbf{L} \hookrightarrow \overline{\mathbf{K}}$ en una clausura algebraica de $\mathbf{K}$. Sea $\alpha \in \mathbf{L}$ y supongamos que $\alpha_1, \ldots, \alpha_d \in \overline{\mathbf{K}}$ son las raíces del polinomio característico $\chi_\alpha^{\mathbf{K}} \in \mathbf{K}[X]$ contadas con multiplicidad. Entonces,

$$\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(\alpha) = [\mathbf{L} : \mathbf{K}(\alpha)] \sum_{i=1}^{d} \alpha_i \quad \text{y} \quad \mathrm{N}_{\mathbf{L}/\mathbf{K}}(\alpha) = \left(\prod_{i=1}^{d} \alpha_i \right)^{[\mathbf{L}:\mathbf{K}(\alpha)]}.$$

Dado que cada elemento en $\mathbf{K}(\alpha)$ es de la forma $g(\alpha)$ para cierto $g \in \mathbf{K}[X]$, es natural tratar de calcular $\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(g(\alpha))$ y $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(g(\alpha))$ de manera más sencilla.

1. Probar que para $g \in \mathbf{K}[X]$, el polinomio $f(X) := \prod_{i=1}^{d} (X - g(\alpha_i)) \in \overline{\mathbf{K}}[X]$ tiene coeficientes en $\mathbf{K}$.

   Indicación: El Teorema Fundamental de las Funciones Simétricas *señala que todo polinomio $f \in \mathbf{M}[\alpha_1, \ldots, \alpha_d]$ que es invariante por el grupo simétrico S_d pertenece a $\mathbf{M}[s_1, \ldots, s_d]$ donde $s_i = s_i(\alpha_1, \ldots, \alpha_d) \in \mathbf{K}$ es el i-ésimo polinomio simétrico. Aquí, conviene $\mathbf{M} := \mathbf{K}(X)$.*

2. Considere el isomorfismos $\mathbf{K}(\alpha) \xrightarrow{\sim} \mathbf{K}(\alpha_i)$, $\alpha \mapsto \alpha_i$ y pruebe que $\mu_{g(\alpha)}^{\mathbf{K}} = \mu_{g(\alpha_i)}^{\mathbf{K}}$ para todo $i \in \{1, \ldots, d\}$. Deducir que
   $$\chi_{g(\alpha)}^{\mathbf{K}} = (X - g(\alpha_1)) \cdots (X - g(\alpha_d)) \text{ en } \overline{\mathbf{K}}[X].$$

En particular, el ítem (2) junto con el **Hecho** visto en clases implican que

$$\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(g(\alpha)) = [\mathbf{L} : \mathbf{K}(\alpha)] \sum_{i=1}^{d} g(\alpha_i) \quad \text{y} \quad \mathrm{N}_{\mathbf{L}/\mathbf{K}}(g(\alpha)) = \left(\prod_{i=1}^{d} g(\alpha_i) \right)^{[\mathbf{L}:\mathbf{K}(\alpha)]} \qquad (\star)$$

3. Sea $\mathbf{K} = \mathbf{Q}(\alpha)$ donde $\alpha \in \mathbf{C}$ es una raíz de $f(X) = \chi_\alpha^{\mathbf{Q}} = X^3 - X - 1$, donde $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(1) = [\mathbf{K} : \mathbf{Q}] = 3$ y donde $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\alpha) = 0$ es el coeficiente que acompaña a $-X^2$. Determine, *sin usar matrices*, $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\alpha^2)$.

   Indicación: Notar que si α, β, γ son las raíces de f, entonces $\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma)$.

Usando lo anterior, probaremos el siguiente resultado práctico:

Teorema: Sea $\mathbf{K}(\alpha)/\mathbf{K}$ extensión de grado $n \geq 2$ y sea $f = \mu_\alpha^{\mathbf{K}} \in \mathbf{K}[X]$ el polinomio minimal de α. Supongamos que
$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \text{ en } \overline{\mathbf{K}}[X].$$

Entonces,

$$\mathrm{disc}_{\mathbf{K}(\alpha)/\mathbf{K}}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j} (\alpha_j - \alpha_i)^2 = (-1)^{n(n-1)/2} \, \mathrm{N}_{\mathbf{K}(\alpha)/\mathbf{K}}(f'(\alpha)).$$

4. Defina el vector columna $\mathbf{v}_k$ mediante $\mathbf{v}_k = (\alpha_1^{k-1}, \ldots, \alpha_n^{k-1})$. Use $(\star)$ para demostrar que

$$\mathrm{Tr}_{\mathbf{K}(\alpha)/\mathbf{K}}(\alpha^{i-1}\alpha^{j-1}) = \langle \mathbf{v}_i, \mathbf{v}_j \rangle,$$

donde $\langle \cdot, \cdot \rangle$ denota el producto escalar usual en $\mathbf{K}(\alpha) \simeq \mathbf{K}^n$. Deducir que

$$\mathrm{disc}_{\mathbf{K}(\alpha)/\mathbf{K}}(1, \alpha, \ldots, \alpha^{n-1}) = \det(\langle (\mathbf{v}_i, \mathbf{v}_j) \rangle_{1 \leq i,j \leq n}).$$

5. Considere la matríz $A \in M_n(\mathbf{K}(\alpha))$ cuya columna i-ésima está dada por el vector $\mathbf{v}_i = (\alpha_1^{i-1}, \ldots, \alpha_n^{i-1})$. Deduzca que $\mathrm{disc}_{\mathbf{K}(\alpha)/\mathbf{K}}(1, \alpha, \ldots, \alpha^{n-1}) = \det(A)^2$.

6. Utilice la fórmula para el determinante de la *matriz de Vandermonde* para probar la primera igualdad del Teorema, i.e., para probar que

$$\mathrm{disc}_{\mathbf{K}(\alpha)/\mathbf{K}}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j} (\alpha_j - \alpha_i)^2.$$

7. Para demostrar la segunda igualdad del Teorema (i.e., probar que $\prod_{i<j}(\alpha_j - \alpha_i)^2 = (-1)^{n(n-1)/2}\, \mathrm{N}_{\mathbf{K}(\alpha)/\mathbf{K}}(f'(\alpha))$) muestre que

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_j - \alpha_j).$$

Luego, considere el producto de los $f'(\alpha_i)$ y reordenelo de tal suerte que esté indexado por pares $i < j$ (para ello, es útil juntar $\alpha_j - \alpha_i$ y $\alpha_i - \alpha_j$ en $-(\alpha_j - \alpha_i)^2$) y realice un conteo de los pares que fueron juntados. Por último, concluya aplicando $(\star)$ a $g(X) = f'(X)$.

Problema C: Factorización explícita de ideales primos (50 puntos)

El objetivo de este problema es utilizar el **Teorema de Factorización de Kummer-Dedekind**[2] para calcular explícitamente la factorización de ideales primos en anillos de enteros de cuerpos de números.

Durante todo el problema, consideraremos $\mathbf{K}$ un cuerpo de números de grado $d = [\mathbf{K} : \mathbf{Q}]$. Para $\alpha \in \mathscr{O}_{\mathbf{K}}$ denotamos por $\mathbf{Z}[\alpha] \subseteq \mathscr{O}_{\mathbf{K}}$ a la $\mathbf{Z}$-álgebra generada por α (i.e., $\mathbf{Z}[\alpha] \simeq \mathbf{Z}[X]/\langle \mu_\alpha^{\mathbf{Q}} \rangle$ y $\mathbf{Z}[\alpha] \simeq \mathbf{Z}^d$ como $\mathbf{Z}$-módulo). En particular, el Teorema de la Base Adaptada implica que el cociente $\mathscr{O}_{\mathbf{K}}/\mathbf{Z}[\alpha]$ es un grupo finito, de orden $[\mathscr{O}_{\mathbf{K}} : \mathbf{Z}[\alpha]]$.

> **Teorema (Dedekind, 1838):** Sea $\mathbf{K}$ un cuerpo de números y sea $\alpha \in \mathscr{O}_{\mathbf{K}}$ tal que $\mathbf{K} = \mathbf{Q}(\alpha)$. Sea $f(X) = \mu_\alpha^{\mathbf{Q}}(X) \in \mathbf{Z}[X]$ el polinomio minimal de α. Sea $p \geq 2$ un primo que **no divide** a $[\mathscr{O}_{\mathbf{K}} : \mathbf{Z}[\alpha]]$, y escribamos
>
> $$f(X) \equiv Q_1(X)^{e_1} \cdots Q_g(X)^{e_g} \pmod{p} \text{ en } \mathbf{F}_p[X],$$
>
> donde cada $Q_i(X) \in \mathbf{F}_p[X]$ es mónico e irreducible. Entonces $p\mathscr{O}_{\mathbf{K}} \subseteq \mathscr{O}_{\mathbf{K}}$ se factoriza en producto de ideales primos
>
> $$p\mathscr{O}_{\mathbf{K}} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g},$$
>
> donde hay una biyección entre los primos $\mathfrak{q}_i \subseteq \mathscr{O}_{\mathbf{K}}$ y los factores $Q_i(X) \in \mathbf{F}_p[X]$, y donde $f_{\mathfrak{q}_i} = \deg(Q_i)$. Más aún, $\mathfrak{q}_i = \langle p, h_i(\alpha) \rangle \subseteq \mathscr{O}_{\mathbf{K}}$ donde $h_i \in \mathbf{Z}[X]$ es *cualquier* polinomio con $Q_i(X) \equiv h_i(X) \pmod{p}$.

En particular, si $\mathscr{O}_{\mathbf{K}} = \mathbf{Z}[\alpha]$ el Teorema anterior se aplica a todo primo p.

1. Probar que $D_{\mathscr{O}_{\mathbf{K}}/\mathbf{Z}}(\mathbf{Z}[\alpha]) = [\mathscr{O}_{\mathbf{K}} : \mathbf{Z}[\alpha]]^2 d_{\mathscr{O}_K/\mathbf{Z}}$. Deducir que para todo primo p que **no divide** al discriminante $\mathrm{disc}(\mathbf{Z}[\alpha]) \in \mathbf{N}^{\geq 1}$, donde $D_{\mathscr{O}_{\mathbf{K}}/\mathbf{Z}}(\mathbf{Z}[\alpha]) = \langle \mathrm{disc}(\mathbf{Z}[\alpha]) \rangle \subseteq \mathbf{Z}$, hay una biyección entre los factores primos de $p\mathscr{O}_{\mathbf{K}}$ y los factores irreducibles mónicos de $f(X) \pmod{p}$ en $\mathbf{F}_p[X]$.

Por ejemplo, si $\mathbf{K} = \mathbf{Q}(i)$ entonces $\mathscr{O}_{\mathbf{K}} = \mathbf{Z}[i]$ es el anillo de enteros de Gauss. Aquí $f(X) = X^2 + 1 \in \mathbf{Z}[X]$ es el polinomio minimal de $\alpha = i \in \mathscr{O}_{\mathbf{K}}$. Para $p = 2$ tenemos que

$$f \equiv (X+1)^2 \text{ en } \mathbf{F}_2[X].$$

Luego, $2\mathbf{Z}[i] = \mathfrak{q}^2$ donde $\mathfrak{q} = \langle 2, i+1 \rangle = \langle i+1 \rangle$ (pues $2 = (1+i)(1-i)$) ideal primo **ramificado** y $f_{\mathfrak{q}} = 1$. Por otra parte, si $a \in \mathbf{F}_p$ cumple que $a^2 = -1$ entonces $a^4 = 1$ y luego $4 \mid p-1$ (por el Pequeño Teorema de Fermat y el Teorema de Lagrange). Así, observamos que hay un comportamiento distinto según si $p \equiv 1$ o $p \equiv 3 \pmod{4}$. Para $p = 7$ tenemos que

$$f \equiv X^2 + 1 \text{ es irreducible en } \mathbf{F}_7[X].$$

[2] Originalmente demostrado por Dedekind en 1838, basado en ideas de Kummer. Ver Proposition 8.3 en el Capítulo I del libro de J. Neukirch *Algebraic Number Theory* para más detalles.

Luego, $7\mathbf{Z}[i] = \langle 7, i^2+1\rangle = \langle 7\rangle \subseteq \mathbf{Z}[i]$ con $\mathfrak{q} = \langle 7\rangle$ ideal primo **no-ramificado** con $e_{\mathfrak{q}} = 1$ y $f_{\mathfrak{q}} = 2$. Para $p = 13$ tenemos que

$$f \equiv (X+5)(X-5) \text{ en } \mathbf{F}_{13}.$$

Así, $7\mathbf{Z}[i] = \mathfrak{q}_1\mathfrak{q}_2$ donde $\mathfrak{q}_1 = \langle 13, i+5\rangle = \langle 2+3i\rangle$ (pues $13 = (2+3i)(2-3i)$ y $i+5 = (2+3i)(1-i)$) y donde $\mathfrak{q}_2 = \langle 13, i-5\rangle = \langle 2-3i\rangle = \sigma(\langle 2+3i\rangle)$ donde $\sigma \in \mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$ es la conjugación compleja.

> **Definición:** Sea $A \subseteq \mathbf{K} = \mathrm{Fr}(A)$ un anillo de Dedekind, $\mathbf{L}/\mathbf{K}$ una extensión finita y separable y sea $B \subseteq \mathbf{L}$ la clausura integral de A en $\mathbf{L}$. Dado $\mathfrak{p} \subseteq A$ ideal primo no-nulo, escribamos
>
> $$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g},$$
>
> por lo que $[\mathbf{L} : \mathbf{K}] = \sum_{i=1}^{g} e_{\mathfrak{q}_i} f_{\mathfrak{q}_i}$. Decimos que el ideal primo $\mathfrak{p} \subseteq A$:
>
> (i) **Escinde completamente** en $\mathbf{L}$ si $f_{\mathfrak{q}_i} = 1$ y $e_{\mathfrak{q}_i} = 1$ para todo $i \in \{1, \ldots, g\}$, i.e., si $g = [\mathbf{L} : \mathbf{K}]$.
>
> (ii) **Ramifica completamente** en $\mathbf{L}$ si $g = 1$ (i.e., $\mathfrak{p}B = \mathfrak{q}^e$) y si $f_{\mathfrak{q}} = 1$, i.e., $\mathfrak{p}B = \mathfrak{q}^{[\mathbf{L}:\mathbf{K}]}$.
>
> (iii) Es **Inerte** en $\mathbf{L}$ si $g = 1$ (i.e., $\mathfrak{p}B = \mathfrak{q}^e$) y si $e_{\mathfrak{q}} = 1$, i.e., $\mathfrak{p}B = \mathfrak{q}$ con $f_{\mathfrak{q}} = [\mathbf{L} : \mathbf{K}]$.

Utilizando la terminología anterior:

2. Determine las factorizaciones $p\mathscr{O}_{\mathbf{K}} = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_g^{e_g}$ para todo primo $p \leq 13$ cuando $\mathbf{K} = \mathbf{Q}(\sqrt{3})$.
3. Determine las factorizaciones $p\mathscr{O}_{\mathbf{K}} = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_g^{e_g}$ para todo primo $p \leq 13$ cuando $\mathbf{K} = \mathbf{Q}(\sqrt{5})$.
4. Factorice $7\mathscr{O}_{\mathbf{K}} = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_g^{e_g}$, y calcule los correspondientes grados residuales $f_{\mathfrak{q}_i}$, cuando $\mathbf{K} = \mathbf{Q}(\sqrt[4]{2})$.

   Indicación: No es necesario calcular explícitamente $\mathscr{O}_{\mathbf{K}}$. Basta justificar que $\mathrm{disc}(\mathbf{Z}[\sqrt[4]{2}]) = -2^{11}$*, lo que se puede hacer utilizando el resultado principal del* Problema B.

Cultura general: El **Teorema de Densidad de Chebotarev** (1926) afirma que la densidad de números primos que ramifican completamente en un cuerpo de números $\mathbf{K}$ es exactamente

$$\frac{1}{[\mathbf{K} : \mathbf{Q}]}$$

respecto a una medida de probabilidad adecuada. La Hipótesis de Riemann Generalizada implica versiones más precisas de este resultado.