RAMIFICACIONES

BENJAMÍN MACÍAS QUEZADA

RESUMEN. La teoría de ramificaciones estudia el hecho de que, al levantar ideales primos en una extensión de anillos, la naturaleza de estos puede cambiar. A saber, tal ideal puede seguir siendo primo o no, caso en el que se factoriza únicamente como producto de ideales primos, factorización que puede ser o no libre de cuadrados. Así, es natural preguntar qué información sobre la extensión nos permite deducir el destino de los ideales primos, y qué efectos tiene este fenómeno sobre la aritmética de interés.

ÍNDICE

1. Preliminares sobre cuerpos de números 1
2. Generalidades sobre ramificación 2
3. Ramificación en extensiones galoisianas 3
4. El teorema de Dedekind–Kummer 5
Referencias 7

1. PRELIMINARES SOBRE CUERPOS DE NÚMEROS

En esta sección cubriremos superficialmente los fundamentos de la teoría de números algebraicos, orginalmente desarrollada por Richard Dedekind en apéndices a las *Vorlesungen über Zahlentheorie* (ver, por ejemplo, la traducción de John Stillwell, [DD99]). Existe abundante literatura sobre este tema, pero para los fines de esta exposición referimos a textos clásicos como [Sam67, Chs. II–V], [Mil20, Chs. 2–4], [Neu99, §§ I.2–I.6], [SD01, Chs. 1.1–1.3], o [Mar18, Ch. 2].

Un *cuerpo de números* es una extensión $K/\mathbb{Q}$ finita (i.e., de *grado* $[K:\mathbb{Q}] := \dim_{\mathbb{Q}} K$ finito). El conjunto de todos los elementos de K que son soluciones de algún polinomio mónico con coeficientes enteros es un anillo (conmutativo, con unidad), llamado el *anillo de enteros* de K, y es denotado $\mathcal{O}_K$. Algunas propiedades importantes de estos anillos son:

- Su cuerpo de fracciones es $\operatorname{Frac}\mathcal{O}_K = K$, ver [Mil20, Proposition 2.6].
- Son $\mathbb{Z}$-módulos libres de rango $[K:\mathbb{Q}]$, ver [Neu99, Proposition 2.10].
- Dado un ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, el cociente $\mathcal{O}_K/\mathfrak{a}$ es finito, y de hecho $\mathfrak{a}$ será un $\mathbb{Z}$-módulo libre de rango $[K:\mathbb{Q}]$, ver [Neu99, Proposition 2.10].
- Son *dominios de Dedekind*: son integralmente cerrados en K, son noetherianos, y todos sus ideales primos no-nulos son maximales (i.e., tienen dimensión de Krull 1, pues no son cuerpos), ver [Neu99, Theorem 3.1].

Estos anillos de enteros generalmente no son dominios de factorización única. Lo que sí ocurre es que las propiedades mencionadas anteriormente bastan para probar que de hecho gozan de factorización única (salvo orden de los factores) en ideales primos, lo que se puede encontrar en [Neu99, Theorem 3.3].

El producto de dos ideales $\mathfrak{a}, \mathfrak{b} \subseteq O_K$ es el $\mathcal{O}_K$-submódulo de K generado por todos los productos entre pares de sus generadores, a saber, si

$$\mathfrak{a} = (a_1, \ldots, a_r),\ \mathfrak{b} = (b_1, \ldots, b_s),$$

Date: 28 de marzo, 2024.

entonces definimos

$$\mathfrak{ab} := (a_i b_j : 1 \leq i \leq r,\ 1 \leq j \leq s).$$

Con este producto, es claro que el conjunto $\mathcal{I}_K$ de todos los $\mathcal{O}_K$-submódulos finitamente generados de K, llamados *módulos fraccionarios*, es un monoide conmutativo cuyo neutro es $\mathcal{O}_K$.

En la demostración de la factorización única en ideales primos, es necesario "invertir" estos ideales primos. Este "módulo inverso" $\mathfrak{p}'$ de $\mathfrak{p}$ debe ser tal que $\mathfrak{p}\mathfrak{p}' = \mathcal{O}_K$. Esto se puede realizar usando que los ideales primos son maximales (por ejemplo, en [Sam67, Théorème 2, p. 60]), obteniendo que

$$\mathfrak{p}' := \{x \in K : x\mathfrak{p} \subseteq \mathcal{O}_K\} \in \mathcal{I}_K.$$

Después de demostrar factorización única en ideales primos se puede deducir fácilmente el hecho que todo $\mathfrak{a} \in \mathcal{I}_K$ es invertible en $\mathcal{O}_K$, es decir, $\mathcal{I}_K$ es un grupo abeliano.

En $\mathcal{I}_K$ podemos identificar dos $\mathcal{O}_K$-módulos fraccionarios $\mathfrak{a}, \mathfrak{a}'$ si existe $\alpha \in K^\times$ tal que $\mathfrak{a}' = \alpha\mathfrak{a}$, lo que define una relación de equivalencia. El subgrupo asociado a esta relación es el formado por los $\mathcal{O}_K$-módulos fraccionarios generados por un elemento,

$$\mathcal{P}_K := \left\{\alpha\mathcal{O}_K : \alpha \in K^\times\right\}.$$

Como estamos en el contexto abeliano, el cociente $\mathrm{Cl}(K) := \mathcal{I}_K/\mathcal{P}_K$ está bien definido, y se llama el *grupo de clases de módulos fraccionarios* de K, o simplemente el *grupo de clases* de K.

El grupo de clases detecta cuándo $\mathcal{O}_K$ es un dominio de factorización única, pues $|\mathrm{Cl}(K)| = 1$ si y solo si todos los elementos de $\mathcal{I}_K$—en particular todos los ideales de $\mathcal{O}_K$—son principales, y en dominios de Dedekind el ser dominio de ideales principales es equivalente a ser dominio de factorización única.

Un resultado fundamental sobre el grupo de clases es que es finito. Una demostración accesible se encuentra en [Mar18, pp. 91–92], y consiste en probar que cada $[\mathfrak{a}] \in \mathrm{Cl}(K)$ puede ser representada por algún ideal de norma actoada (la cota es independiente del ideal). Se concluye pues esto acota la cantidad de factores primos que puede tener un ideal de $\mathcal{O}_K$, en particular cualquier clase de $\mathrm{Cl}(K)$.

2. Generalidades sobre ramificación

Una *extensión relativa* es una extensión finita L/K de un cuerpo de números $K/\mathbb{Q}$ (por ley de torres, L también será un cuerpo de números). Dado un ideal primo $\mathfrak{P} \subseteq \mathcal{O}_L$, se verifica inmediatamente que $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$, y decimos que $\mathfrak{P}$ *está sobre* $\mathfrak{p}$. Recíprocamente, dado un ideal primo $\mathfrak{p} \subseteq \mathcal{O}_K$, se tiene que $\mathfrak{P} := \mathfrak{p}\mathcal{O}_L$ es un ideal de $\mathcal{O}_L$.

En tanto $\mathcal{O}_L$ es dominio de Dedekind, todo ideal primo $\mathfrak{p} \subseteq \mathcal{O}_K$ admite una factorización única

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}, \quad \text{con } \mathfrak{P}_i \supseteq \mathfrak{p} \text{ ideal primo de } \mathcal{O}_L. \tag{2.1}$$

Dependiendo de esta factorización, se adopta la siguiente terminología:

- Si $\mathfrak{p}\mathcal{O}_L$ es primo, decimos que $\mathfrak{p}$ es *inerte*. En este caso, en el lado derecho de la Ecuación 2.1, aparece un solo ideal primo (i.e., $g = 1$), con exponente 1.
- Si no, aparecerá más de un factor primo. Si esta factorización es libre de cuadrados (es decir, todos los exponentes son 1), decimos que $\mathfrak{p}$ *escinde*.
- Si no es libre de cuadrados (i.e., hay algún $e_i > 1$), decimos que $\mathfrak{p}$ *ramifica*. En particular, si hay un solo factor con exponente $e = [L : K]$, decimos que $\mathfrak{p}$ *ramifica completamente*.

El exponente e_i en factorización de la Ecuación 2.1 se llama el *índice de ramificación de* $\mathfrak{p}$ *en* $\mathfrak{P}_i$. En caso que sea necesario distinguir que este índice es relativo a $\mathfrak{p}$ y cada $\mathfrak{P}_i$ correspondiente, lo escribiremos $e_{\mathfrak{P}_i|\mathfrak{p}}$, aunque preferimos evitarlo para no sobrecargar la notación.

Dado un primo $\mathfrak{P} \subseteq \mathcal{O}_L$ sobre el primo $\mathfrak{p} \subseteq \mathcal{O}_K$, aplicar el teorema del kernel a la secuencia

$$\mathcal{O}_K \longrightarrow \mathcal{O}_L \longrightarrow \mathcal{O}_L/\mathfrak{P}$$

exhibe la extensión de cuerpos $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{P}$, que como involucra cuerpos finitos, debe ser una extensión finita. El grado de esta extención se llama el *grado de inercia de* $\mathfrak{p}$ *en* $\mathfrak{P}$. En el caso de una factorización como en la Ecuación 2.1, usaremos la notación f_i, o en caso que sea necesario, $f_{\mathfrak{P}_i|\mathfrak{p}}$.

La relación entre índice de ramificación, grado de inercia, y el grado de la extensión es la siguiente:

Teorema 2.1. *Sea L/K una extensión relativa. Si $\mathfrak{P}_1 \dots, \mathfrak{P}_g \subseteq \mathcal{O}_L$ son los ideales primos sobre un ideal primo $\mathfrak{p} \subseteq \mathcal{O}_K$, se tiene que*

$$[L : K] = \sum_{i=1}^{g} e_i f_i.$$

La idea es escribir la norma de $\mathfrak{p}\mathcal{O}_L$ de dos formas distintas. Recordemos que la *norma* de un ideal $\mathfrak{a} \subseteq \mathcal{O}_L$ es $\mathrm{N}_{L/K}(\mathfrak{a}) := |\mathcal{O}_K : \mathfrak{a}|$. Demostrar que es multiplicativa requiere trabajo no-trivial, y se puede encontrar desarrollado, por ejemplo, en [Mar18, pp. 46–47]. Asumiendo esto, y que $\mathrm{N}(\mathfrak{p}\mathcal{O}_L) = \mathrm{N}(\mathfrak{p})^{[L:K]}$ (en [Mar18, pp. 47–48]), la prueba es un cálculo directo:

Demostración. Comparar el final del párrafo anterior con

$$\mathrm{N}(\mathfrak{p}\mathcal{O}_L) = \mathrm{N}\left(\prod_{i=1}^{g} \mathfrak{P}_i^{e_i}\right) = \prod_{i=1}^{g} \mathrm{N}(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^{g} \mathrm{N}(\mathfrak{p})^{f_i e_i} = \mathrm{N}(\mathfrak{p})^{\sum_{i=1}^{g} e_i f_i}.$$

□

3. Ramificación en extensiones galoisianas

En muchos casos de interés, la extensión L/K será galoisiana, por lo que podemos someter a $\mathcal{O}_L$ y sus ideales primos a la acción natural del grupo $G := \mathrm{Gal}(L/K)$. Es claro que G actúa en $\mathcal{O}_L$. Resulta que, dado un primo $\mathfrak{p} \subseteq \mathcal{O}_K$, se tiene que:

Proposición 3.1. *G actúa en la colección de los primos $\mathfrak{P} \subseteq \mathcal{O}_L$ sobre $\mathfrak{p}$, es decir, $\sigma\mathfrak{P}$ también es un primo sobre $\mathfrak{p}$ para cada $\sigma \in G$.*

Demostración. Primero, veamos que $\sigma\mathfrak{P}$ es ideal primo. En efecto, dado $xy \in \sigma\mathfrak{P}$, entonces $\sigma^{-1}(x)\sigma^{-1}(y) \in \mathfrak{P}$, y como este es primo debe ser que $\sigma^{-1}(x) \in \mathfrak{P}$ o $\sigma^{-1}(y) \in \mathfrak{P}$, por lo que $x \in \sigma\mathfrak{P}$ o $y \in \sigma\mathfrak{P}$. Queda ver que $\sigma\mathfrak{P}$ está sobre $\mathfrak{p}$. Esto es una cuenta directa:

$$\sigma\mathfrak{P} \cap \mathcal{O}_K = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma\mathfrak{p} = \mathfrak{p}.$$

□

Esta acción de hecho es transitiva. La demostración está basada en [Mar18, Theorem 27]:

Proposición 3.2. *Consideremos L/K una extensión galoisiana de cuerpos de números. Dados ideales primos $\mathfrak{P}, \mathfrak{P}' \subseteq \mathcal{O}_L$ sobre el mismo primo $\mathfrak{p} \subseteq \mathcal{O}_K$, existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma\mathfrak{P} = \mathfrak{P}'$.*

Demostración. Si la acción no fuese transitiva, los ideales $\mathfrak{P}'$ y $\sigma\mathfrak{P}$ serían distintos para todos los $\sigma \in \mathrm{Gal}(L/K)$, por lo que existiría un elemento en $\mathfrak{P}'$ que no pertenece a ningún $\sigma\mathfrak{P}$, lo que bastaría para probar que la norma de tal elemento no queda bien definida.

Recordar que la *norma* de un elemento (en contraste a la de un ideal) $\alpha \in \mathcal{O}_L$ es $\mathrm{N}(\alpha) := \det(x \mapsto \alpha x)$ para $x \in L$, pero para efectos prácticos, es igual al producto de todos los G-conjugados de α (incluyendo a α), elevado a cierta potencia (ver [Mar18, Theorem 4', pp. 16–17] para detalles).

En efecto, si $\mathfrak{P}' \neq \sigma\mathfrak{P}$ para todo $\sigma \in \mathrm{Gal}(L/K)$, podemos aplicar el Teorema del Resto en Ideales para encontrar una solución $\alpha \in \mathcal{O}_L$ al sistema de congruencias

$$\begin{cases} x \equiv 0 & \text{mód } \mathfrak{P}' \\ x \equiv 1 & \text{mód } \sigma_1\mathfrak{P} \\ \vdots & \\ x \equiv 1 & \text{mód } \sigma_{[L:K]}\mathfrak{P}. \end{cases}$$

Por tanto, se tiene que $\mathrm{N}(\alpha) \in \mathcal{O}_K$, y como uno de sus factores es $\alpha \in \mathfrak{P}'$ (por la primera ecuación del sistema), también $\mathrm{N}_{L/K}(\alpha) \in \mathfrak{P}'$. Así, $\mathrm{N}(\alpha) \in \mathcal{O}_K \cap \mathfrak{P}' = \mathfrak{p} \subseteq \mathfrak{P}$.

Por otro lado, las otras ecuaciones del sistema indican que $\alpha \notin \sigma\mathfrak{P}$ para ninguno de los $\sigma \in \mathrm{Gal}(L/K)$, y por tanto $\sigma^{-1}\alpha \notin \mathfrak{P}$. Los elementos de esta forma corresponden exactamente a los K-conjugados de α, por lo que también podemos escribir

$$\mathrm{N}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma^{-1}\alpha,$$

por lo que $\mathrm{N}(\alpha) \notin \mathfrak{P}$, lo que es contradictorio. □

Con este resultado, se puede deducir que si L/K es galoisiana, en las factorizaciones de ideales primos de $\mathcal{O}_L$ (sobre un mismo primo de $\mathcal{O}_K$), los índices de ramificación y grados de inercia son todos iguales.

Proposición 3.3. *Consideremos L/K una extensión galoisiana de cuerpos de números, y un primo $\mathfrak{p} \subseteq \mathcal{O}_K$. En la factorización única*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_g^{e_g}$$

en primos de $\mathcal{O}_L$, se tiene que $e_1 = \cdots = e_g$ y $f_1 = \cdots = f_g$. En particular, $[L:K] = efg$.

Demostración. La afirmación sobre los grados de inercia es porque cada $\sigma \in \mathrm{Gal}(L/K)$ otorga un isomorfismo $\mathcal{O}_L/\mathfrak{P}_i \cong \mathcal{O}_L/\sigma(\mathfrak{P}_i)$, por lo que todos los $\mathbb{F}_{\mathfrak{P}_i}$ son isomorfos entre sí, de lo que cada $\mathfrak{P}_i$ debe tener el mismo grado de inercia.

Para los índices de ramificación, notamos que cada $\sigma \in \mathrm{Gal}(L/K)$ fija $\mathfrak{p}\mathcal{O}_L$, por lo que podemos fabricar factorizaciones

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} (\sigma\mathfrak{P}_i)^{e_i}.$$

En este caso, como la acción es transitiva, cada $\mathfrak{P}_i$ puede aparecer con todos los índices de ramificación. Por la unicidad de la factorización, más el hecho que estos factores son distintos entre sí, debe ser que los índices de ramificación son iguales entre sí.

La última afirmación usa el Teorema 2.1, que en este caso indica que

$$[L:K] = \sum_{i=1}^{g} ef = gef. \tag{3.1}$$

□

Dado un primo $\mathfrak{P} \subseteq \mathcal{O}_L$, su *grupo de descomposición* es

$$D_{\mathfrak{P}} := \mathrm{Stab}_{\mathrm{Gal}(L/K)}(\mathfrak{P}) = \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Notemos que $[\mathrm{Gal}(L/K) : D_{\mathfrak{P}}]$ es la cantidad de factores primos distintos que dividen a $\mathfrak{p}\mathcal{O}_L$. Por la Proposición 3.3 (en particular, la Ecuación 3.1), se tiene que

$$[L:K] = ef[\mathrm{Gal}(L/K) : D_{\mathfrak{P}}] \iff [L:K] = ef[L:K]/|D_{\mathfrak{P}}|.$$

Cancelando y reordenando, se obtiene:

Corolario 3.4. $|D_{\mathfrak{P}}| = ef$.

Se verifica inmediatamente que cada $\sigma \in D_{\mathfrak{P}}$ induce un automorfismo ϕ_σ en $\mathcal{O}_L/\mathfrak{P}$ a través de $[\alpha] \mapsto [\sigma\alpha]$, que de hecho fija $\mathcal{O}_K/\mathfrak{p}$. Escribiendo los cuerpos en cuestión como $\mathbb{F}_{\mathfrak{P}}$ y $\mathbb{F}_{\mathfrak{p}}$, esto quiere decir que tenemos un morfismo de grupos

$$\begin{aligned} \phi \colon D_{\mathfrak{P}} &\longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \\ \sigma &\mapsto \phi_\sigma, \end{aligned}$$

cuyo kernel $I_{\mathfrak{P}}$ se llama el *grupo de inercia* de $\mathfrak{P}$. El morfismo ϕ es hecho sobreyectivo:

Proposición 3.5. *Sea L/K galoisiana, y $\mathfrak{P} \subseteq \mathcal{O}_L$ un primo sobre $\mathfrak{p} \subseteq \mathcal{O}_K$. Se tiene que cada $\gamma \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ es de la forma ϕ_σ para algún $\sigma \in D_{\mathfrak{P}}$.*

Demostración. Como $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ es finita y separable, el Teorema del Elemento Primitivo asegura que $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}([\theta])$ para algún $[\theta] \in \mathbb{F}_\mathfrak{P}$. Por el Teorema de los Restos, podemos encontrar $\alpha \in \mathcal{O}_L$ solución al sistema de congruencias

$$\begin{aligned} x &\equiv \theta \pmod{\sigma\mathfrak{P}} \text{ para } \sigma \in D_\mathfrak{P} \\ x &\equiv 0 \pmod{\sigma\mathfrak{P}} \text{ para } \sigma \notin D_\mathfrak{P}. \end{aligned}$$

Sabemos que $\gamma([\alpha]) = [\sigma(\alpha)]$ para algún $\sigma \in \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$. Si fuese el caso que $\sigma \notin D_\mathfrak{P}$, se tendría que $= \gamma([\alpha]) = [0]$, lo que no puede ser. Así, debe ser que $\sigma \in D_\mathfrak{P}$. □ □

Aplicando el Teorema del Kernel a ϕ, se obtiene el isomorfismo

$$\frac{D_\mathfrak{P}}{I_\mathfrak{P}} \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}),$$

por lo que $|D_\mathfrak{P}| = |I_\mathfrak{P}||\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})|$. Se verifica rápidamente que $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ es galoisiana, por lo que $|\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})| = [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}]$, lo que sumado al Corolario 3.4, indica que $ef = |I_\mathfrak{P}|f$. Reordenando, esto prueba que:

Corolario 3.6. *$|I_\mathfrak{P}| = e$. En particular, $\mathfrak{p}$ es no-ramificado si y solo $I_\mathfrak{P}$ es el grupo trivial.*

Toda extensión finita de un cuerpo finito es cíclica (i.e., tiene grupo de Galois cíclico), por lo que $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ es generado por un solo elemento,

$$x \longmapsto x^{|\mathbb{F}_\mathfrak{p}|}.$$

Un *elemento de Frobenius* para $\mathfrak{P}$ es cualquier $\sigma \in D_\mathfrak{P}$ cuya imagen en $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ es dicho generador. Todos los elementos de Frobenius son conjugados entre sí por elementos de $I_\mathfrak{P}$, de modo que cuando este es trivial (es decir, cuando $\mathfrak{p}$ es no-ramificado según el Corolario 3.6), solo hay un único $\sigma \in D_\mathfrak{P}$ que corresponde al generador de $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$, caso en el que podemos referir *al* elemento de Frobenius de $\mathfrak{P}$ sin amigüedad.

4. El teorema de Dedekind–Kummer

En general, obtener las factorizaciones en ideales primos es no-trivial. El siguiente resultado indica cómo podemos conocer la descomposición de ideales primos en función de la factorización de un polinomio mínimo cuando la extensión $\mathcal{O}_L/\mathcal{O}_K$ es primitiva. Fue demostrado por Kummer para ciertos casos particulares (sobre $\mathbb{Z}$) en [Kum47, pp. 319–326], y posteriormente generalizado por Dedekind en [Ded78]. La versión que estudiaremos está adaptada de [Cox89, Proposition 5.11]:

Teorema 4.1. *Sea L/K una extensión galoisiana tal que $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ para algún $\alpha \in \mathcal{O}_L$, y $\mathfrak{p} \subseteq \mathcal{O}_K$ un ideal primo. Si $f_\alpha \in \mathcal{O}_K[x]$, el polinomio mínimo de α sobre K, es separable en $\mathbb{F}_\mathfrak{p}$, entonces $\mathfrak{p}$ es no-ramificado en L.*

Además, si $[f_\alpha] = [f_1] \dots [f_g]$ es la factorización en $\mathbb{F}_\mathfrak{p}$ de f_α en polinomios mónicos, coprimos, e irredudibles en $\mathbb{F}_\mathfrak{p}[x]$, entonces los primos sobre $\mathfrak{p}$ son precisamente los $I_i := (\mathfrak{p}, f_i(\alpha)) \subseteq \mathcal{O}_L$, donde $f_i \in \mathcal{O}_K[x]$ es el polinomio mónico cuya reducción módulo $\mathfrak{p}$ es precisamente $[f_i]$. Así, se tiene que

$$\mathfrak{p}\mathcal{O}_L = I_1 \dots I_g. \tag{4.1}$$

Antes de proseguir con la demostración, la experiencia ha dictado que es conveniente detenerse a reparar sobre el enunciado. En primer lugar, esta versión es más bien especializada. El ojo experto es quizás más familiar con el enunciado de [Neu99, Proposition 8.3, pp. 47–48], en el se considera L/K separable y primitiva (digamos, generada por $\alpha \in \mathcal{O}_L$), y adicionalmente se impone que $\mathfrak{p}$ sea coprimo al conductor $\mathfrak{c}$ de $\mathcal{O}_K(\alpha)$. En este caso, en la factorización de $[f_\alpha]$ los factores pueden aparecer con multiplicidad mayor a 1. Las conclusiones a las que se llegan son análogas las que enunciamos, con la diferencia que $\mathfrak{p}$ puede ramificar.

También, estamos imponiendo explícitamente que $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ para $\alpha \in \mathcal{O}_L$. Otras fuentes piden la condición más débil que la extensión L/K sea generada por tal α (i.e., $L = K(\alpha)$). Sin embargo, esto no necesariamente implica que $\mathcal{O}_L = \mathcal{O}_K[\alpha]$: en [Con, Theorem 1.1] se describe un ejemplo de Dedekind, que consiste en la extensión $K := \mathbb{Q}(\theta)/\mathbb{Q}$, con θ raíz de $x^3 - x^2 - 2x - 8 \in \mathbb{Z}[x]$, que ciertamente es primitiva, pero $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ para ningún $\alpha \in \mathcal{O}_K$.

La demostración que seguimos está inspirada en la que aparece guiada en [Cox89, Exercise 5.6], que hace uso del orden del grupo de descomposición.

Demostración. A priori, $\mathfrak{p}\mathcal{O}_L$ tiene una factorización en ideales primos en $\mathcal{O}_L$ de la forma $\prod_{i=1}^{h}\mathfrak{P}_i^{e_i}$, donde todos los e_i son iguales entre sí gracias a la Proposición 3.3, y los $\mathfrak{P}_i$ están sobre $\mathfrak{p}$.

Para probar que $\mathfrak{p}$ es no-ramificado, el plan es verificar que existe alguno de los $[f_k]$ satisface

$$f \geq \deg[f_k] \geq ef, \tag{4.2}$$

lo que forzará $e = 1$. Primero, determinemos este polinomio. Al evaluar $f \equiv f_1 \dots f_g \pmod{\mathfrak{p}}$ en α, resulta en que $f_1(\alpha)\dots f_g(\alpha) \equiv 0 \pmod{\mathfrak{p}}$, y por tanto hay algún k tal que $f_k(\alpha) \in \mathfrak{P}_i$ para algún i.

Verifiquemos que este f_k efectivamente satisface las desigualdades en 4.2. Para la primera (de la izquierda), se tiene que si $\theta_1, \dots, \theta_r$ son las raíces de $[f_k]$ en $\mathbb{F}_\mathfrak{p}$, entonces $F' := \mathbb{F}_\mathfrak{p}(\theta_1, \dots, \theta_r)$ es un extensión intermedia a $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$, y por tanto

$$\deg[f_k] = [F' : \mathbb{F}_\mathfrak{p}] \leq [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}] = f.$$

Z Para la otra, notemos que como $f_k(\alpha) \in \mathfrak{P}_i$, se tiene que $f_k(\sigma\alpha) = 0 \pmod{\mathfrak{P})_i}$ para cada $\sigma \in D_{\mathfrak{P}_i}$. Por tanto $[f_k]$ tiene al menos una raíz en $\mathbb{F}_{\mathfrak{P}_i}$ por cada $\sigma \in D_{\mathfrak{P}_i}$, es decir,

$$\deg[f_k] \geq |D_{\mathfrak{P}_i}| = ef,$$

donde la última igualdad es por la Proposición 3.4, que es válida pues L/K es galoisiana. Así, la factorización de $\mathfrak{p}\mathcal{O}_L$ es efectivamente de la forma $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{h}\mathfrak{P}_i$ para algunos ideales primos $\mathfrak{P}_i \subseteq \mathcal{O}_L$.

Acá, nos desvíamos de [Cox89, Exercise 5.6], y probamos directamente que los I_j definidos en el enunciado son efectivamente los constituyentes de la factorización de $\mathfrak{p}\mathcal{O}_L$. Primero, hay que verificar que los I_j son efectivamente ideales primos, y que son distintos. Para ello, es suficiente probar que cada cociente

$$\frac{\mathcal{O}_L}{(\mathfrak{p}, f_i(\alpha))} \tag{4.3}$$

es un cuerpo (en particular, será un dominio entero). La demostración de ello explota el hecho que $\mathcal{O}_L \cong \mathcal{O}_K[\alpha] \cong \mathcal{O}_K[x]/(f_\alpha)$, que otorga los isomorfismos

$$\frac{\mathcal{O}_L}{(\mathfrak{p}, f_i(\alpha))} \cong \frac{\mathcal{O}_K[x]/(f_\alpha)}{(\mathfrak{p}, f_i(x))} \cong \frac{\mathcal{O}_K[x]}{(\mathfrak{p}, f_\alpha, f_i)} \cong \frac{(\mathcal{O}_K/\mathfrak{p})[x]}{(f_\alpha, f_i)} \cong \frac{(\mathcal{O}_K/\mathfrak{p})[x]}{(f_i)}.$$

Se tiene que (f_i) es un ideal generado por un elemento irreducible en un dominio de factorización única, por lo que dicho ideal es maximal. Eso hace de este último cociente un cuerpo, y por tanto el cociente de 4.3 es efectivamente un cuerpo.

Para probar que los I_j son distintos entre sí, supongamos lo contrario. En tal caso, existirían i, j tales que $(\mathfrak{p}, f_i(\alpha)) = (\mathfrak{p}, f_j(\alpha))$, por lo que podríamos escribir

$$f_i(\alpha) = x + af_j(\alpha),$$

para $x \in \mathfrak{p}$, $a \in \mathcal{O}_L$. Así, $f_i(\alpha)f_j(\alpha) = xf_j(\alpha) + af_j(\alpha)^2$, es decir, f_j tendría multiplicidad 2 en la factorización de f_α módulo $\mathfrak{p}$, lo que contradice la separabilidad.

Finalmente, probemos que la factorización de $\mathfrak{p}\mathcal{O}_L$ es la de la Ecuación 4.1. Para ello, notemos que

$$I_1 \dots I_g = \prod_{i=1}^{g}(\mathfrak{p}, f_i(\alpha)) \subseteq \mathfrak{p}\mathcal{O}_L,$$

por lo que bastaría probar la otra contención. Esto viene de que al expandir el producto, cada término que aparece será divisible por $\mathfrak{p}\mathcal{O}_L$, incluyendo al término

$$\begin{aligned} f_1(\alpha)\dots f_g(\alpha) &\equiv f_\alpha(\alpha) \pmod{\mathfrak{p}} \\ &\equiv 0 \pmod{\mathfrak{p}}, \end{aligned}$$

pues esto quiere decir que $f_1(\alpha)\dots f_g(\alpha) \in \mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_L$. □ □

Referencias

[Con] Keith Conrad, *Rings of integers without a power basis*, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/nopowerbasis.pdf`.

[Cox89] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, A Wiley-Interscience publication, Wiley, New York Weinheim, 1989 (eng).

[DD99] Peter Gustav Dirichlet and Richard Dedekind, *Lectures on number theory*, History of mathematics, American Mathematical Society; London Mathematical Society, Providence, RI: [London], 1999 (eng).

[Ded78] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen*, Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen **23** (1878), 3–38.

[Kum47] E. E. Kummer, *Zur Theorie der complexen Zahlen*, Journal für die reine und angewandte Mathematik **35** (1847), 319–326.

[Mar18] Daniel A. Marcus, *Number Fields*, 2nd ed. 2018 ed., Universitext, Springer International Publishing: Imprint: Springer, Cham, 2018.

[Mil20] James S. Milne, *Algebraic Number Theory (v3.08)*, 2020, Disponible en www.jmilne.org/math/.

[Neu99] Jürgen Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, Springer, Berlin; New York, 1999.

[Sam67] Pierre Samuel, *Théorie Algébrique des Nombres*, Méthodes, Hermann, Paris, France, 1967.

[SD01] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society student texts, Cambridge University Press, Cambridge; New York, 2001.

Email address: `benjaquezadam@uc.cl`