Preliminares para los cursos de teorías de grupos, de Galois y de números algebraicos

Andrea Surroca Ortiz[1]

EMALCA Costa Rica 2019
Universidad de Costa Rica
Turrialba, 22 de julio - 3 de agosto 2019

En estas notas, recordaremos algunas nociones básicas de álgebra necesarias para la comprensión de los cursillos introductorios a la teoría de grupos, a la teoría de Galois y a la teoría algebraica de números. Si bien algunas nociones serán abordadas en el cursillo de teoría de Galois, no lo serán todas.

Les recomendamos leer y **estudiar** (si acaso manejan ya estas nociones, para recordarlas), **al menos** la sección 2, **antes de los cursos**, ya que estas nociones no serán impartidas durante los mismos.

Estos apuntes, a pesar de ser escasos en ejemplos y de faltar a las demostraciones, son parte de los preliminares necesarios para abordar los anillos de Dedekind (al igual que nociones básicas de álgebra lineal), y en todo caso bastan para enunciar la definición de una extensión de cuerpos de Galois. Son un borrador y no pretenden sustituirse a ningún libro.

Índice

1. Motivación *Pág. 1 de 12*

2. Preliminares (dados por conocidos) *Pág. 3 de 12*

3. Más preliminares sobre los anillos y los módulos *Pág. 5 de 12*

4. Elementos algebraicos *Pág. 8 de 12*

5. Elementos conjugados, cuerpos conjugados *Pág. 10 de 12*

1. Motivación

Una parte bellísima de la teoría de números es la geometría diofántica. Se trata del estudio de ecuaciones polinomiales $P(x_1, \ldots, x_n) = 0$, donde el polinomio $P \in \mathbb{Z}[X_1, \ldots, X_n]$ tiene coeficientes enteros (o racionales, $P \in \mathbb{Q}[X, 1, \ldots, X_n]$), y se buscan soluciones $(x_1, \ldots, x_n)$ en números enteros (o racionales). Tales ecuaciones son de gran interés al remplazar $\mathbb{Z}$ por otros anillos más generales, o $\mathbb{Q}$ por otros cuerpos.

[1]University of Manchester. andrea.surroca.o@gmail.com

Esta rama de la matemática debe su nombre a Diofantus de Alejandría, matemático griego del siglo XIII, autor de las "Aritméticas". En un ejemplar de las Aritméticas, el matémático francés Pierre de Fermat, hace la famosa anotación marginal, en el siglo XVII, traducida con nuestras notaciones actuales:

"La ecuación $x^n + y^n = z^n$ no tiene soluciones x, y, z enteras no triviales, si $n \geq 3$", y de la cual no pudo escribir la demostraciòn, ya que no cabía en el margen! Después de siglos de esfuerzo por grandes matemáticos, no fue si no hasta 1995 en que Andrew Wiles, con ayuda suplementaria de Richard Taylor, la demostrara. Justamente cabe citar la frase de Carl Friedrich Gauss (siglo XIX), sobre la teoría de números: *"su encanto particular viene de la simplicidad de sus enunciados junto con la dificultad de sus demostraciones "*.

Para $n = 2$ existen soluciones: son los llamados triplos pitagóricos, por ejemplo $(3, 4, 5)$. El teorema siguiente describe todas las soluciones (y que corresponden a las medidas de los tres lados de los triángulos rectángulos).

Teorema 1. *Sean x, y, z enteros ≥ 1 tal cual $x^2 + y^2 = z^2$. Entonces existe un entero d y enteros primos entre ellos u, v (es decir que su máximo denominador común es 1) tales que (permitiéndonos permutar x e y),*

$$x = d(u^2 - v^2), \;\; y = 2duv, \;\; z = d(u^2 + v^2).$$

Gauss demuestra el *teorema de Fermat* para $n = 3$ utilizando el anillo de enteros de Eisenstein $\mathbb{Z}[w]$, donde $w = e^{2i\pi/3}$.

Fermat, demuestra que las únicas soluciones enteras de la ecuación $y^2 + 2 = x^3$ son exactamente $y = \pm 5, x = \pm 3$. Para ello, utiliza el anillo de enteros cuadráticos $\mathbb{Z}[\sqrt{-2}]$.

Las demostraciones de Gauss y de Fermat se sustentan en la existencia de factorización única en factores primos de elementos en los anillos que utilizaron, $\mathbb{Z}[w]$, y, resp. $\mathbb{Z}[\sqrt{-2}]$. Sin embargo, no es cierto que todos los anillos de enteros cuadráticos sean dominio de factorización única (por ejemplo, $\mathbb{Z}[\sqrt{-5}]$ no lo es) y es esta una de las principales diferencias que presentan respecto al anillo $\mathbb{Z}$. Recordemos la forma más simple del teorema de factorización única.

Teorema 2 (Decomposición única en números primos). *Todo número racional $x \in \mathbb{Q}$, se escribe de manera única como*

$$x = \pm p_1^{a_1} \cdots p_n^{a_n}$$

en donde los $p_1, \ldots, p_n$ son números primos, y los $a_1, \ldots, a_n \in \mathbb{Z}$.

Justamente, consideremos el anillo $A = \mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b; a, b \in \mathbb{Z}\}$. El elemento $6 \in A$ se puede descomponer de las dos maneras siguientes $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$. Los únicos divisores del elemento $(1 + \sqrt{-5})$ en A son 1 y él mismo, o sea que es primo. Sin embargo, divide el producto $2 \cdot 3$, y podemos mostrar que no divide ni 2 ni 3.

Para resolver el problema de la factorización única, Richard Dedekind[2] sugiere considerar *ideales* en lugar de elementos y demuestra la existencia de factorización única de *ideales* como producto de *ideales primos*.

Así pues, los métodos algebraicos son fructuosos en teoría de números, incluso en problemas de profundidad. Además, estos métodos son útiles en otras ramas de la matemática, como por ejemplo, la geometría algebraica.

[2]matemático alemán 1831-1916

2. Preliminares (dados por conocidos)

Definición 3. *Un* **grupo** $(G,+)$ *es un conjunto G no vacío, dotado de una operación $+$, que verifica las propiedades siguientes:*

$\forall a,b \in G,\ \ a+b \in G$ *(se dice que $+$ es una ley interna),*

$\forall a,b,c \in,\ \ a+(b+c)=(a+b)+c$ *(asociatividad),*

$\exists e \in G, \forall a \in G,\ \ e+a=a+e=a$ *(existencia de un elemento neutro o identidad),*

$\forall a \in G, \exists a* \in G,\ \ a+a*=a*+a=e$ *($a*$ se denomina el inverso de a).*

Si, además, $+$ verifica en G la propiedad de conmutatividad, a saber

$\forall a,b \in G,\ \ a+b=b+a,$

el grupo G se dice **abeliano** *o* **conmutativo**, *y a menudo el inverso de a se escribe $-a$.*

Ejercicio 1. *El conjunto de los enteros dotado de la suma $(\mathbb{Z},+)$ es un grupo abeliano. En cambio, dotado de la multiplicación, $(\mathbb{Z},\times)$ no es un grupo. ¿Es el conjunto de los números racionales $\mathbb{Q}=\{\frac{a}{b};\ \ a,b\in\mathbb{Z}, b\neq 0\}$ dotado de la suma un grupo? ¿y de la multiplicación?*

Definición 4. *Un* **anillo** $(A,+,\cdot)$ *es un grupo abeliano $(A,+)$ donde la operación conmutativa $+$ recibe el nombre de suma, junto con otra operación $\cdot$, usualmente llamada producto, y de la que obviaremos la notación, que satisface las propiedades siguientes*

$$a(b+c)=ab+ac,\ \ (b+c)a=ba+ca,\ \ (ab)c=a(bc).$$

Si además cumple que existe un elemento $1 \in A$ tal que $1a=a1=a$ para todo $a \in A$, se dice que 1 es el elemento unitario y que A es un **anillo unitario**.

Si $ab=ba$ para todo par de elementos a y b en A, se dice que el anillo A es **conmutativo**.

En estas notas, utilizaremos la palabra anillo en el sentido de **anillo unitario conmutativo**. Si necesitamos referirnos a un anillo no unitario (o no necesariamente unitario) lo diremos explícitamente.

Ejemplo. El anillo de los enteros $(\mathbb{Z},+,\times)$ es un anillo conmutativo y unitario.

Ejercicio 2. *El conjunto $2\mathbb{Z}=\{2t;t\in\mathbb{Z}\}$ de todos los enteros pares es un ejemplo de anillo no unitario.*

Notaciones Siendo A un anillo, usaremos la notación $A[X]$ para el anillo de polinomios con una variable sobre A, la notación $A[X_1,\ldots,X_n]$ para los polinomios de n variables y $A[[X]]$ para las series formales.

Por convención, si A es un subanillo de un anillo B, suponemos que A contiene el elemento unitario 1 de B.

Si B es un anillo, A un subanillo de B y x un elemento de B, escribiremos $A[x]$ el **subanillo de B generado por A y x**, o sea la intersección de todos los subanillos de B que contienen A y x:

$$A[x]=\{a_0+a_1x+\ldots+a_nx^n;i\in\mathbb{N};a_i\in A\}.$$

De manera análoga se escribe $A[x_1,\ldots,x_n]$ si se trata de una familia finita de elementos de B.

Definición 5. *Se dice que el anillo A es* **íntegro** *(también llamado* **dominio de integridad** *o* **dominio íntegro***) si carece de divisores de cero, o sea si el producto de dos elementos no nulos de A es no nulo, y si A no es* (0).

Si el anillo $(A, +, \times)$ es unitario (existe un elemento neutro para la segunda operación $\times$), y además de ser un grupo abeliano $(A, +)$ para la primera operación, tiene un inverso para cada elemento con respecto a segunda operación $\times$, se le denomina cuerpo. En otras palabras

Definición 6. *Un* **cuerpo** *o* **campo** $(G, +, \times)$ *es un conjunto no vacío, dotado de dos aplicaciones internas que es un grupo abeliano para cada una de las operaciónes y en para el cual la segunda operación es distributiva con respecto a la primera, o sea*

$$\forall a, b, c \in G, \;\; a \times (b + c) = a \times b + a \times c.$$

Por ejemplo, el conjunto de los números racionales dotado de la suma y la multiplicación $(\mathbb{Q}, +, \times)$ es un cuerpo.

Definición 7. *Se denomina* **cuerpo de fracciones** *o* **cuerpo de cocientes** *de un dominio de integridad A al mínimo cuerpo que contiene a A. Dicho cuerpo siempre existe y se denota por $Q(A)$ o* $\mathrm{Frac}(A)$.

El ejemplo más sencillo de un cuerpo de fracciones es el de los números racionales $\mathbb{Q}$, que es el cuerpo de fracciones de los números enteros $\mathbb{Z}$.

Definición 8. *Un* **ideal** $\mathfrak{b}$ *de un anillo A es un subgrupo aditivo tal que $x \in \mathfrak{b}$, $a \in A$ implican $ax \in \mathfrak{b}$.*

El anillo A y (0) son ideales **triviales**.

Ejercicio 3. *Un cuerpo (o campo) puede ser caracterizado por ser un anillo del cual los únicos ideales triviales son él mismo y* (0).

Si $\mathfrak{b}$ y $\mathfrak{c}$ son dos ideales de un anillo A, entonces se puede comprobar que el conjunto $\mathfrak{b} + \mathfrak{c} = \{x + y; x \in \mathfrak{b}, y \in \mathfrak{c}\}$ es un ideal.

Toda intersección de ideales es un ideal.

Definición 9. *Si (b_i) es una familia de elementos de A, la intersección de los ideales de A que contienen los b_i es un ideal de A, llamado* **ideal generado por los** *b_i. Es el conjunto de sumas finitas $\sum_i a_i b_i$ con $a_i \in A$.*

Un ideal generado por un único elemento b se llama **principal** *y se escribe Ab o (b).*

Un anillo íntegro A en donde cada ideal es principal, recibe el nombre de **dominio de ideales principales** *(DIP). Lo llamaremos* **anillo principal**.

Ejercicio 4. *Mostrar que el anillo de enteros $\mathbb{Z}$ es un dominio de ideales principales. (Usar la división euclidiana.)*

Teorema 10 (**Decomposición única en factores primos**). *Sean A un anillo* **principal** *y $K = \mathrm{Frac}(A)$ su cuerpo de fracciones. Todo elemento de K se escribe de manera única como*

$$x = u p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

en donde los $p_1, \ldots, p_n$ son elementos de A, u es una **unidad** *de A (o sea que posee un inverso), y los $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$.*

Observamos que el anillo de los enteros $\mathbb{Z}$ es principal, y que todo elemento de $\mathbb{Q}$ admite una decomposición en númros primos.

Definición 11. *Si A es un anillo y $\mathfrak{b}$ un ideal de A, las clases de equivalencia $a+\mathfrak{b}$, $a \in A$, forman un anillo, llamado* **cociente de A por $\mathfrak{b}$**, *y se escribe $A/\mathfrak{b}$.*

Los ideales de $A/\mathfrak{b}$ tienen la forma $\mathfrak{b}'/\mathfrak{b}$, donde $\mathfrak{b}'$ recorre los ideales de A que contienen $\mathfrak{b}$.

Un ideal $\mathfrak{b}$ es **irreducible** *si no se puede escribir como intersección de dos ideales diferentes de $\mathfrak{b}$.*

Un ideal $\mathfrak{m}$ se llama **ideal maximal** *si existen exactamente dos ideales que contienen a $\mathfrak{m}$, a saber, A y el mismo $\mathfrak{m}$.*

Un ideal $\mathfrak{p}$ se llama **ideal primo** *si $\mathfrak{p}$ es distinto de A y, para todo a y b pertenecientes a A tales que $ab \in \mathfrak{p}$ y si $a \notin \mathfrak{p}$, entonces $b \in \mathfrak{p}$.*

Ejercicio 5. *El cociente $A/\mathfrak{b}$ es un cuerpo (o campo) si y solo si $\mathfrak{b}$ es maximal entre los ideales de A distintos de A.*

Un ideal $\mathfrak{p}$ de A es primo si y solo si $A/\mathfrak{p}$ es dominio de integridad.

Un ideal maximal es necesariamente primo.

El ideal $\mathfrak{m}$ es un ideal maximal de A si y solo si $A/\mathfrak{m}$ es un cuerpo.

3. Más preliminares sobre los anillos y los módulos

La noción de módulo sobre un anillo A, también llamado A-módulo, es la generalización directa de la noción de espacio vectorial.

Definición 12. *Sean A y A' anillos con elementos unitarios e y e'. Un* **homomorfismo** *$f : A \to A'$ es una aplicación f de A hacia A' que verifica:*

$$f(a+b) = f(a) + f(b), \;\; f(ab) = f(a)f(b), \;\; f(e) = f(e').$$

Definición 13. *Un A-**módulo** M es un grupo abeliano (donde escribimos aditivamente la operación) dotado de una aplicación $A \times M \to M$ (donde escribimos multiplicativamente) tal que, para todos $a, b \in A$, $x, y \in M$, tenemos*

$$a(x+y) = ax + ay, \;\; (a+b)x = ax + bx, \;\; a(bx) = (ab)x, \;\; 1x = x.$$

Si M y M' son A-módulos, un homomorfismo (o aplicación linear) de M en M' es una aplicación $f : M \to M'$ tal que, para todos $a \in A$, $x, y \in M$,

$$f(x+y) = f(x) + f(y), \;\; f(ax) = af(x).$$

Si $f : X \to X'$ es un homomorfismo (de grupos, anillos o módulos X, X'), con elemetos neutrales respectivamente e y e', se denomina núcleo[3] y se escribe $\ker(f) = \{x \in X; f(x) = e'\}$ la imagen recíproca del elemento neutral e' de X' por f.

[3]ker del alemàn "Kernel"que quiere decir núcleo.

Se denomina imagen $\mathrm{im}(f)$ de f la parte $f(X)$ de X'.

Ejercicio 6. *Siguiendo las notaciones precedentes:*

El núcleo $\ker(f)$ *es un subgrupo invariante (respectivamente, un ideal, o un submódulo) de* X.

La aplicación f *es inyectiva si y solo si el núcleo* $\ker(f) = \{e\}$.

La imagen $\mathrm{im}(f)$ *es un subgrupo (resp., un subanillo, o un submódulo) de* X.

Teorema 14. *Si* $f : A \to A'$ *es un homomorfismo de anillos, entonces el núcleo* $\ker(f) = \{a \in A; f(a) = 0\}$ *de* f *es un ideal de* A. *Recíprocamente, si* $\mathfrak{b}$ *es un ideal de* A, *entonces la aplicación* $\pi : A \to A/\mathfrak{b}$ *dada por* $a \mapsto a + \mathfrak{b}$ *es un homomorfismo sobreyectivo de anillos cuyo núcleo es* $\mathfrak{b}$. *(La aplicación* π *se denomina homomorfismo canónico o proyección).*

Definición 15. *Un* A*-módulo* M *se dice* **finitamente generado** *si admite un sistema generador finito. O sea que cada elemento* x *de* M *se escribe como combinación linear de un número finito de elementos.*

El teorema siguiente es la base del estudio de los anillos y módulos noterianos.[4]

Teorema 16. *Sean* A*un anillo y* M *un* A*-módulo. Las aserciones siguientes son equivalentes.*

a) Toda familia no vacía de submódulos de M *posee un elemento maximal (para la relación de inclusión).*

b) Toda sucesión creciente $(M_n)_{n\geq 0}$ *de submódulos de* M *es estacionaria, o sea, que a partir de cierto rango son todos iguales.*

c) Todo submódulo de M *es finitamente generado.*

Definición 17. *Un* A*-módulo* M *se denomina* **noteriano** *si satisface las condiciones del teorema precedente.*

Un anillo A *se denomina noteriano si, considerado como* A*-módulo, es un módulo noteriano.*

Corolario 18. *En un anillo* A *que es dominio de ideales principales (que llamaremos anillo principal), toda familia no vacía de ideales de* A *admite un elemento maximal. O sea que* A *es un anillo noteriano.*

Recordamos que el anillo de los enteros $\mathbb{Z}$ es principal, y entonces noteriano.

A continuación, daremos algunos resultados sobre los anillos que nos serán útiles para estudiar los números algebraicos, y en particular, los campos de números.

Definición 19. *Sea* R *un anillo y* $A \subseteq R$ *un subanillo de* R. *Un elemento* x *de* R *es* **entero sobre** A *si existen* $a_0, \ldots, a_{n-1} \in A$ *tales que*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0. \tag{1}$$

O sea que x *es raiz de un polinomio mónico (i.e. el coeficiente del monomio de mayor grado es 1) de* A. *Esta relación se llama relación de dependencia integral de* x *sobre* A.

[4]Llevan ese nombre en honor a la matemática alemana Emmy Noether 1882-1935, descrita por Albert Einstein como *el genio matemático creativo más considerable desde que las mujeres tiene acceso a los estudios superiores.*

Por falta de tiempo, vamos a admitir, lamentablemente, el teorema siguiente, del cual deducimos los resultados de esta sección. (Para la demostración, ver teorema 1 del capítulo II §1 del libro de Pierre Samuel.)

Teorema 20. *Sea R un anillo*[5]*, $A \subseteq R$ un subanillo de R, y x un elemento de R. Las propiedades siguientes son equivalentes.*

a) El elemento x de R es entero sobre A.

b) El anillo $A[x]$ es un A-módulo finitamente generado.

c) Existe un subanillo B de R conteniendo A y x, que es un A-módulo finitamente generado. ($A \subseteq B \subseteq R$, $x \in B$)

Proposición 21. *Sea R un anillo, $A \subseteq R$ un subanillo de R, y sea $(x_i)_{i=1,\dots,n}$ una familia finita de elementos de R. Si, para todo i, el elemento $x_i \in R$ es entero sobre el anillo $A[x_1, \dots, x_{i-1}]$ (y en particular, si todos los x_i son enteros sobre A), entonces $A[x_1, \dots, x_n]$ es un A-módulo finitamente generado.*

Demostración. Por recurrencia sobre n. El caso $n = 1$ es el teorema 20 b).

Deducimos el corolario siguiente de la proposición y el teorema 20 b).

Corolario 22. *Sea R un anillo, $A \subseteq R$ un subanillo de R. El conjunto A' de los elementos de R enteros sobre A, es un subanillo de R que contiene A.*

Definición 23. *Con las notaciones del corolario precedente, el subanillo A' se llama la* **clausura entera de** *A* **en** *R (tenemos $A \subseteq A' \subseteq R$.)*

Además, si $A = A'$, se dice que A es **integralmente cerrado en** *R.*

Deducimos del corolario precedente

Corolario 24. *Sea R un anillo, $A \subseteq R$ un subanillo de R, y sean x, y elementos de R enteros sobre A. Entonces $x + y, x - y, xy$ son enteros sobre A.*

Definición 25. *Sea A un anillo íntegro (también llamado dominio de integridad o dominio íntegro, o sea que carece de divisores de cero) y $K = \mathrm{Frac}(A)$ su cuerpo de fracciones. La clausura entera de A en $K = \mathrm{Frac}(A)$ se llama la* **clausura entera de** *A.*

Si además, A es integralmente cerrado en $K = \mathrm{Frac}(A)$, se dice que es **integralmente cerrado** *(o normal).*

Ejercicio 7. *Mostrar que el anillo $A = \mathbb{Z}[\sqrt{-3}]$ no es integralmente cerrado.*

Ejercicio 8. *Mostrar que el anillo $A = \mathbb{Z}[\sqrt{5}]$ no es integralmente cerrado.*

Definición 26. *Sean B un anillo y $A \subseteq B$ un subanillo de B. Se dice que* **el anillo** *B* **es entero sobre** *A si todo elemento de B es entero sobre A, o sea que la clausura entera A' de A en B, es igual a B (tenemos $A' = B$).*

Proposición 27 (Transitividad)**.** *Sean A, B y C anillos tales que $A \subseteq B \subseteq C$. Si C es entero sobre B y B es entero sobre A, entonces C es entero sobre A.*

[5] R como "ring", que quiere decir anillo en inglés

Demostración. Considerar $x \in C$. Usar proposición 21 y teorema 20.

Proposición 28. *Sean B un anillo integro y $A \subseteq B$ un subanillo de B tal que B es entero sobre A. Entonces B es un cuerpo si y solo si A es un cuerpo.*

Demostración. Usar teorema 20.

4. Elementos algebraicos

Definición 29. *Un número complejo α ($\in \mathbb{C}$) se dice* **algebraico** *si existe un polinomio $P \in \mathbb{Q}[X]$ non nulo (de grado $n \geq 2$), tal cual $P(\alpha) = 0$. Es decir que existen números rationales $a_i \in \mathbb{Q}$, tales que*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

Multiplicando por el inverso de a_n, podemos suponer que $a_n = 1$.

Si $a_n = 1$ y los otros a_i son enteros ($\in \mathbb{Z}$), α se dice ser un **entero algebraico**.

Si, en cambio, no existe tal relación de dependencia entre potencias de α, al número α se le dice **transcendente**.

Por ejemplo, es fácil de demostrar que $\sqrt{2}, \sqrt{3}, \sqrt[3]{5}, \sqrt[3]{7}, i, e^{2i\pi/5}$ son algebraicos, incluso enteros algebraicos. En cambio es más difícil demostrar que e o π son transcendentes.

¿Podemos demostrar que la suma, o el producto, de números algebraicos es algebraico? Por ejemplo, es fácil mostrar que $\alpha = \sqrt{2} + \sqrt{3}$ es algebraico (**Ejercicio**), pero menos fácil mostrar que $\beta =^3 \sqrt{5} +^3 \sqrt{7}$ lo es.

Para sobrellevar esta dificultad, Dedekind generalizó la noción a los anillos conmutativos, remplazando $\mathbb{C}$ y $\mathbb{Z}$ por anillos más generales.

Definición 30. *Sea R un anillo y $K \subseteq R$ un sub***cuerpo**[6] *de R. Un elemento x de R es* **algebraico sobre el cuerpo** *K si existen $a_0, \ldots, a_{n-1} \in K$ no todos nulos, tales que*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0. \tag{2}$$

Ejercicio 9. *Con las notaciones de la definición 30,*
1. verificar que x algebraico sobre K implica x **entero** *algebraico sobre K,*
2. deducir del teorema 20 b), que x algebraico sobre K equivale a que la dimension $[K[x] : K]$ de la extensión $K[x]$ sobre K sea finita.

Definición 31. *Un anillo R que contiene un cuerpo K se dice* **algebraico sobre** *K si todo elemento de R es algebraico sobre K.*

Si $R = L$ también es un cuerpo, se dice que L es una **extensión algebraica de** *K.*

Si L y K son cuerpos, $K \subseteq L$, la dimension $[L : K]$ se denomina el **grado de** *L* **sobre** *K.*

Ejercicio 10. *Sean L y K son cuerpos tales cuales $K \subseteq L$. Mostrar que si el grado $[L : K]$ de L sobre K es finito, entonces L es una extensión algebraica de K. (Aplicar el teorema 20 c).)*

[6] K como "Körper", que quiere decir cuerpo en alemán

Definición 32. *Se denomina* **cuerpo o campo de números** *toda extensión (algebraica) finita (i.e. de grado finito) de* $\mathbb{Q}$.

Ejercicio 11. *Demostrar la proposición siguiente.*

Proposición 33. *Sean K un cuerpo, L una extensión algebraica de K y M una extensión algebraica de L. Entonces*
1) M es una extensión algebraica de K.
2) Vale la multiplicidad de los grados, a saber $[M : K] = [M : L] \cdot [L : K]$.

Demostración.
1) Aplicar la proposición 27.
2) Trabajar con las bases de L sobre K y de M sobre L y buscar una base de M sobre K.

Proposición 34. *Sea R un anillo que contiene un subcuerpo $K \subset R$. Sea $K' \subset R$ el conjunto de los elementos de R que son algebraicos sobre K.*
a) K' es un subanillo de R que contiene K.
b) Si R es íntegro, K' es un subcuerpo de R.

Demostración.
1) Aplicar el corolario 22.
2) Aplicar la proposición 28.

Volvamos a la definición de un número algebraico. El número racional α es algebraico si existe un polinomio $P \in \mathbb{Q}[X]$, no nulo y mónico, que se anula en α. Consideremos el ideal (P) del anillo $\mathbb{Q}[X]$, o sea, el ideal generado por P. Visto que el anillo $\mathbb{Q}[X]$ es principal, el ideal (P) es principal, o sea que existe un polinomio mínimo que lo genera. Llamémoslo P_α. Cualquier otro polinomio que se anula en α será un multiple de P_α.

Ejercicio 12. *¿Cuál es el polinomio minimal de $\alpha = \frac{1+\sqrt{5}}{2}$?*

Formalizemos esto de manera más general. Sean R un anillo, $K \subseteq R$ un subcuerpo de R y x un elemento de R. Definamos un homomorfismo

$$\varphi : K[X] \to R$$

tal cual $\varphi(X) = x$, $\varphi(a) = a$, para todo $a \in K$. Un tal homomorfismo es único. Su imagen es $\varphi(K[X]) = K[x]$. Además

$$x \text{ es algebraico sobre } K \Leftrightarrow \ker(\varphi) \neq 0. \tag{3}$$

El núcleo $\ker(\varphi)$ es un ideal del anillo principal $K[X]$, y por ende, es un ideal principal. Notemos F su polinomio minimo non nulo que lo genera. Sea $G \in K[X]$. Entonces $G(x) = 0$ equivale a $F(X)$ divide $G(X)$. Siendo K un cuerpo, podemos suponer que F es mónico. Este polinomio es determinado de manera única por K y x. Se denomina el **polinomio minimo de x sobre K**.

Si pasamos al cociente, obtenemos el isomorfismo canónico

$$K[X]/(F(X)) \xrightarrow{\sim} K[x]. \tag{4}$$

Proposición 35.

$$K[x] \text{ cuerpo } \Leftrightarrow K[x] \text{ integro } \Leftrightarrow F(X) \text{ irredicible.}$$

Demostración. Mostremos la primera equivalencia (y dejemos la segunda como ejercicio). Supongamos que $K[x]$ es integro (o sea sin divisores de cero). Apliquemos la proposición 27 de los preliminares a $B = K[x]$ que es un anillo entero sobre $A = K$. Como K es un cuerpo, entonces $K[x]$ lo es también.

Supongamos ahora que $K[x]$ es un cuerpo. Como cada elemento tiene un inverso, entonces, como anillo, es integro.

Recíprocamente, sean K un cuerpo y $F(X) \in K[X]$ un polinomio irreducible. Entonces el cociente $K[X]/(F(X))$ es un cuerpo y contiene K. Si notamos x la clase de X en ese cuerpo, entonces $F(x) = 0$. Vemos como $F(X)$ es divisible por el factor de primer grado $X - x$ en ese cuerpo $K[x]$. De manera más general, mostramos

Proposición 36. *Sea K un cuerpo, $P(X) \in K[X]$ un polinomio no constante. Existe una extensión alegbraica K' de grado finito sobre K tal cual $P(X)$ se descompone en factores de primer grado en $K'[X]$.*

Demostración. Por recurrencia sobre el grado d de $P(X)$.

5. Elementos conjugados, cuerpos conjugados

Ejemplo. Volvamos a nuestros números algebraicos. Por ejemplo $\sqrt{5}$ es un número algebraico y $\mathbb{Q}[\sqrt{5}] = \{a + \sqrt{5}b; a, b \in \mathbb{Q}\}$ es un cuerpo. Su polinomio minimal (irreducuble) es $F(X) = X^2 - 5$, que es de grado 2. La extensión de cuerpos $\mathbb{Q}[\sqrt{5}]/\mathbb{Q}$ es de grado $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = 2$. Una base es $\{1, \sqrt{5}\}$. Su anillo de enteros es $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

El polinomio $F(X)$ tiene otra raíz, a saber $-\sqrt{5}$. El número $-\sqrt{5}$ es también algebraico, y el cuerpo $\mathbb{Q}[-\sqrt{5}] = \mathbb{Q}[\sqrt{5}]$. O sea que $-\sqrt{5}$ comparte ciertas propiedades con $\sqrt{5}$.

Ejercicio 13. *Definamos la función*

$$\varphi : \mathbb{Q}[\sqrt{5}] \to \mathbb{Q}[\sqrt{5}]$$

tal cual $\varphi(\sqrt{5}) = -\sqrt{5}$, y $\varphi(\mathbb{Q}) \subset \mathbb{Q}$. Mostrar que φ es un isomorfismo y que es único. Decimos que φ es un $\mathbb{Q}$-isomorfismo.

Ejercicio 14. *Veamos el número $\omega = \frac{-1+\sqrt{-3}}{2}$. Es también algebraico y $\mathbb{Z}[w]$ es el llamado anillo de los enteros de Eisenstein. Su polinomio minimal es $F(X) = X^3 - 1$, y es de grado 3. ¿Qué pasa con $\mathbb{Q}[w]$ y las otras raíces de F?*

Veamos la teoria general.

Definición 37. *Sean L y L' cuerpos conteniendo un cuerpo K. Un isomorfismo $\varphi : L \to L'$ se denomina* **K-isomorfismo de L sobre L'** *si $\varphi(K) \subseteq K$. Se dice entonces que L y L' son* **K-isomorfos**. *Si L y L' son algebraicos sobre K; se dice que son* **cuerpos conjugados sobre K**.

Si L, L' son extensiones de K, se dice que los elementos $x \in L$, $x' \in L'$ son **conjugados sobre** *K si existe un K-isomorfismo $\varphi : K(x) \to K(x')$ tal cual $\varphi(x) = x'$. Entonces φ es único.*

En este caso, ya sea x, x' son ambos transcendentes sobre K, o bien, son ambos algebraicos sobre K y tienen mismo polinomio minimal.

Ejemplo. Sean $F(X)$ un polinomio irreducible de grado n sobre K, y $x_1, \ldots, x_n$ sus raíces en una extensión K' de K (ver Proposición 36). Entonces los x_i son conjugados dos a dos sobre K (ver (4)), y los cuerpos $K[x_i]$ son conjugados dos a dos.

Definición 38. *Para todo cuerpo K existe un único homomorfismo de anillos $\varphi : \mathbb{Z} \to K$, definido por $\varphi(n) = 1 + 1 + \ldots + 1$, n veces, para $n \geq 0$, y por $\varphi(-n) - \varphi(n)$.*

Si φ es inyectivo, identifica $\mathbb{Z}$ a un subanillo de K, y entonces K contiene también el cuerpo de fracciones $\mathbb{Q}$ de $\mathbb{Z}$. Se dice que K **es de característica 0**.

Si φ no es inyectivo, su núcleo es un ideal $p\mathbb{Z}$, $p > 0$. Entonces $\mathbb{Z}/p\mathbb{Z}$ se identifica a un subanillo de K, y por ende es íntegro; o sea que p es un número primo. Se dice que K **es de característica** *p.*

Lema 39. *Sean K un cuerpo de característica 0, o un cuerpo finito, $F(X) \in K[X]$ un polinomio mónico irreducible, y $F(X) = \prod_{i=1}^{n}(X - x_i)$ se decomposición en factores de primer grado en una extensión K' de K (ver Proposición 36). Entonces las n raíces x_i son distinctas.*

Demostración. Razonar por el absurdo, tomar en cuenta la derivada de F, que es de grado inferior a F.

Teorema 40. *Sean K un cuerpo de característica 0, o un cuerpo finito, K' una extensión de grado finito n sobre K, y $\mathbb{C}$ un cuerpo algebraicamente cerrado y que contiene K. Existen n K-isomorfismos distintos de K' en $\mathbb{C}$.*

Demostración. Supongamos primero $K' = K[x]$, con $x \in K'$. El polinomio minimal $F(X)$ de x sobre K es de grado n. Por ende admite n raíces $x_1, \ldots, x_n$ en $\mathbb{C}$, que son distintas (ver lema). Para cada $i = 1, \ldots, n$ tenemos un K-isomorfismo $\sigma_i : K' \to \mathbb{C}$, tal cual $\sigma(x_) = x_i$.

En el caso general, se procede por recurrencia sobre el grado de K' sobre K.

Corolario 41 (Teorema del elemento primitivo)**.** *Sea K un cuerpo finito o de característica 0, y K' una extensión finita de K de grado n. Existe un único elemento x de K' (denominado* **elemento primitivo***) tal cual $K' = K[x]$.*

Disponemos ahora de todos los elementos necesarios para considerar, junto con un cuerpo, sus automorfismos.

Ejercicio 15. *Sean L un cuerpo y G un conjunto de automorfismos de L. Sea $K(G)$ el conjunto de los elementos $x \in L$ tales cuales $\sigma(x) = x$ para todo $\sigma \in G$.*

Mostrar que $K(G)$ es un subcuerpo de L. Se denomina **el cuerpo de los invariantes de** *G.*

Ejercicio 16. *Sea L/K una extensión de cuerpos. Mostrar que el conjunto de los K-automorfismos de L, dotado de la composición para las funciones, es un grupo.*

Teorema 42. *Sean K un cuerpo finito o de caracteriítica 0, y L una extensión finita de K de grado n. Sea G el grupo de los K-automorfismos de L. Las condiciones siguientes son equivalentes:*

a) K es el cuerpo de los invariantes de G;

b) para todo $x \in L$, el polinomio minimal de x sobre K posee todas sus raíces en L;

c) L es generado por las raíces de un polinomio sobre K.

Bajo estas condiciones, el grupo G posee n elementos.

Definición 43. *Si las condiciones del teorema son satisfechas, se dice que L* **es una extensión de Galois**[7] **de** *K y que G* **es el grupo de Galois de** *L* **sobre** *K.*

Los resultados enunciados en estas notas permiten de demostrar el teorema 42.

Esquisa de demostración del terorema 42.

a) $\implies$ b) Usar (3).

b) $\implies$ c) Considerar un elemento primitivo x de L sobre K.

c) $\implies$ a) Usar lo visto en la sección 5 y aplicar el teorema 40 y el corolario 41.

Referencias bibliográficas:

- Los resultados aquí expuestos los traduje mayoritariamente del libro de
Pierre Samuel, *Théorie algébriques de nombres*, ediciones Hermann, ISBN 2 7056 5589 1, (2003).

El libro se encuentra en la ned en francés y también en inglés. Existe en español (ediciones Omega), aunque parece estar agotado. Con un poco de suerte lo encuentran en alguna biblioteca universitaria o en la ned.

- Algunas notas de cursos (en diferentes temas) en español:

Luis Arenas https://sites.google.com/a/u.uchile.cl/mat-ciencias-prof-luis-arenas/home/apuntes

Joseph Várilly http://www.kerwa.ucr.ac.cr/handle/10669/15621

Andrea Surroca Ortiz
andrea.surroca.o@gmail.com

[7] según el matématico francés Evariste Galois 1811-1832