Álgebra Conmutativa

Grado en Matemáticas

Colección manuales uex - 111

Pedro
Sancho de Salas

111

ÍNDICE

ÁLGEBRA CONMUTATIVA

GRADO EN MATEMÁTICAS

MANUALES UEX

111

ÍNDICE

PEDRO SANCHO DE SALAS

ÁLGEBRA CONMUTATIVA

GRADO EN MATEMÁTICAS

UNIVERSIDAD DE EXTREMADURA

2019

ÍNDICE

UNIVERSIDAD DE EXTREMADURA

Edita:

Universidad de Extremadura. Servicio de Publicaciones
C/ Caldereros, 2 - Planta 3ª. 10071 Cáceres (España)
Tel. 927 257 041; Fax 927 257 046
E-mail: publicac@unex.es
http://www.unex.es/publicaciones

ISSN 1135-870-X
ISBN de méritos 978-84-09-06821-0

ÍNDICE GENERAL

ÍN
DI
CE

INICIO

ÍNDICE

INICIO

INTRODUCCIÓN

El presente manual está concebido por el autor como el manual de la asignatura cuatrimestral Álgebra Conmutativa, del segundo curso del Grado en Matemáticas de la UEX. Introducimos estructuras básicas del Álgebra como las de grupo, anillo y módulo, herramientas fundamentales como el cociente de un grupo por un subgrupo, cociente de un anillo por un ideal, cociente de un módulo por un submódulo y la localización de un anillo o un módulo por un sistema multiplicativo.

El manual está divido en cuatro temas. En cada tema incluimos un cuestionario, una lista de problemas (con sus soluciones) y la biografía de un matemático relevante (en inglés).

Comentemos algunos de los conceptos y contenidos fundamentales del curso.

Los inicios de la filosofía griega (los presocráticos) fueron también los inicios de la matemática griega (los pitagóricos). Descubrir que en el conjunto de los números naturales destacaban los números primos, descubrir más tarde que todo número era producto de números primos de modo único, observar que las notas musicales dependían de las proporciones enteras de las longitudes de las cuerdas musicales, etc, se vivió como la aparición de un nuevo mundo independiente de toda contingencia que regía y explicaba el mundo real. En la escuela aprendimos la aritmética elemental de $\mathbb{Z}$. Si elevamos un poco la vista observaremos que en $\mathbb{Z}$ es fundamental la existencia de dos operaciones + y $\cdot$, la existencia de elementos primos (o irreducibles) y que esta estructura es igualmente existente en otros anillos (por ejemplo, en los anillos de polinomios). En el curso hablaremos de los anillos y fundamentalmente de los anillos euclídeos. Probaremos que en los anillos euclídeos ($\mathbb{Z}$, $k[x]$, el anillo de los enteros de Gauss, etc.) todo elemento se escribe de modo único como producto de irreducibles (salvo multiplicación por invertibles y orden). La propiedad aritmética fundamental de los anillos euclídeos es que sus ideales son principales, es decir, generados por un elemento (el de "grado" mínimo). Del mismo modo que en anillos euclídeos, probamos que si A es un dominio de ideales principales entonces todo elemento $a \in A$ (no nulo ni invertible) se escribe de modo único como producto de irreducibles (salvo multiplicación por invertibles y orden),

$$a = p_1 \cdots p_n, \quad (p_i \text{ irreducibles}).$$

Veremos que

$$a \cdot A + b \cdot A = m.c.d.(a,b) \cdot A$$
$$a \cdot A \cap b \cdot A = m.c.m.(a,b) \cdot A$$

Mediante el algoritmo de Euclides, calcularemos $\lambda, \mu \in A$, tales que

$$\lambda \cdot a + \mu \cdot b = m.c.d.(a,b).$$

Esta igualdad, "identidad de Bezout", tendrá múltiples aplicaciones tanto en Álgebra como para la resolución de ciertas ecuaciones diferenciales y ecuaciones en diferencias finitas.

Consideremos ahora el anillo de polinomios en una variable con coefcientes complejos. Probaremos el teorema fundamental del Álgebra, que nos dice que para todo polinomio $p(x) \in \mathbb{C}[x]$ existen $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ de modo que

$$p(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

O dicho de otro modo, salvo multiplicación por $c \in k$ no nulo, los polinomios irreducibles de $\mathbb{C}[x]$ son los polinomios $x - \alpha$. En general, el teorema de Kronecker, nos dice que dado $p(x) \in k[x]$ existe un cuerpo mayor $k \hookrightarrow K$ y $\alpha_1, \dots, \alpha_n \in K$ de modo que $p(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n)$.

Un concepto fundamental en Matemáticas es el concepto de equivalencia y es fundamental también el proceso de identificar las cosas que consideramos equivalentes. Un concepto y herramienta fundamental en el curso va a ser el concepto de cociente. Pongamos un par de ejemplos.

Si en $\mathbb{Z}$ considero equivalentes dos números cuando difieran en un múltiplo de 9 e igualo entre sí los números que considero equivalentes obtengo un nuevo conjunto de "números" que denotamos por $\mathbb{Z}/9\mathbb{Z}$, que por definición es el conjunto

$$\mathbb{Z}/9\mathbb{Z} := \{\bar{n}, \forall\, n \in \mathbb{Z} \colon \bar{n} = \bar{m} \iff n - m \in 9\mathbb{Z}\}.$$

Este nuevo conjunto, $\mathbb{Z}/9\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{8}\}$ es de modo natural un anillo, podemos definir como se suman y multiplican sus elementos:

$$\begin{aligned} \bar{r} + \bar{s} &:= \overline{r+s} \\ \bar{r} \cdot \bar{s} &:= \overline{rs} \end{aligned}$$

Si tenemos un número natural $n_r n_{r-1} \dots n_0 := \sum_i n_i 10^i$ escrito en base decimal, entonces en $\mathbb{Z}/9\mathbb{Z}$ tenemos que

$$\overline{n_r n_{r-1} \dots n_0} = \overline{\sum_i n_i 10^i} = \sum_i \bar{n}_i \bar{10}^i = \sum_i \bar{n}_i \bar{1}^i = \sum_i \bar{n}_i = \overline{\sum_i n_i}.$$

Por tanto, $n_r n_{r-1} \dots n_0$ es divisible por 9 (es decir, $\overline{n_r n_{r-1} \dots n_0} = \bar{0}$) si y sólo si $\sum_i n_i$ es divisible por 9.

Si en $\mathbb{R}[x]$ considero equivalentes dos polinomios cuando difieran en un múltiplo de x^2+1 e igualo entre sí los polinomios que sean equivalentes obtengo un nuevo conjunto que denotamos $\mathbb{R}[x]/(x^2+1)$, que por definición es el conjunto

$$\mathbb{R}[x]/(x^2+1) := \{\overline{p(x)}, \forall\, p(x) \in \mathbb{R}[x] \colon \overline{p(x)} = \overline{q(x)} \iff p(x) - q(x) \in (x^2+1) \cdot \mathbb{R}[x]\}.$$

Este nuevo conjunto es de modo natural un anillo: podemos definir como se suman y multiplican sus elementos

$$\begin{aligned} \overline{p(x)} + \overline{q(x)} &:= \overline{p(x) + q(x)} \\ \overline{p(x)} \cdot \overline{q(x)} &= \overline{p(x) \cdot q(x)} \end{aligned}$$

Observemos que $\bar{x}\cdot\bar{x} = \overline{x^2} = \overline{-1}$. Se cumple que la aplicación, $\mathbb{C} \to \mathbb{R}[x]/(x^2+1)$, $a+bi \mapsto \overline{a+bx}$ es un isomorfismo de anillos.

Una vez que hemos estudiado los anillos euclídeos, o más generalmente los anillos de ideales principales, pasamos a estudiar los módulos sobre dominios de ideales principales. Un A-módulo es un A-espacio vectorial, salvo que no se supone que A sea un cuerpo sino que se supone que es sólo un anillo. Igual que en la teoría de espacios vectoriales, puede hablarse de submódulos, cocientes por submódulos, sumas y productos directos de módulos, aplicaciones A-lineales, sistemas de generadores, pero no puede afirmarse en general la existencia de bases en los A-módulos. Demos dos ejemplos fundamentales de A-módulos. Si $(G,+)$ es un grupo abeliano entonces G es un $\mathbb{Z}$-módulo, porque además de que sabemos sumar los elementos de G, podemos definir la multiplicación de los elementos g de G por los enteros n de $\mathbb{Z}$:

$$n\cdot g := \begin{cases} g+\overset{n}{\cdots}+g, \text{ si } n>0 \\ (-g)+\overset{-n}{\cdots}+(-g), \text{ si } n<0 \\ 0, \text{ si } n=0 \end{cases}$$

Si E un k-espacio vectorial y $T\colon E\to E$ es un endomorfismo k-lineal, entonces E es un $k[x]$-módulo, porque además de que sabemos sumar los vectores de E, podemos definir la multiplicación de los vectores e de E por los polinomios $p(x)=\sum_i a_i x^i$ de $k[x]$:

$$(\sum_i a_i x^i)\cdot e := \sum_i a_i \cdot T^i(e).$$

Casos concretos de endomorfismos lineales que estudiaremos son:

1. $E=\{f:\mathbb{R}\to\mathbb{R} : f \text{ infinito derivable}\}$ y $T\colon E\to E$, $T(f):=f'$.
2. $E:=\{\text{sucesiones } (a_n) \text{ de números reales}\}$ y $T\colon E\to E$, $T(a_n):=(a_{n+1})-(a_n)$.

Como hemos dicho en los A-módulos no existen bases, en general. Si M es un A-módulo finito generado no existe en general un isomorfismo de A-módulos $A^n \simeq M$, como sucede con los espacios vectoriales. Existe un epimorfismo $A^n \to M$ y si A es un dominio de ideales principales existe un morfismo de A-módulos $\phi\colon A^m\to A^n$ de modo que $A^n/\operatorname{Im}\phi \simeq M$. Además, probaremos que existen bases en A^m y en A^n de modo que la matriz asociada a ϕ en estas bases es (a_{ij}) con $a_{ij}=0$ si $i\neq j$.

Como consecuencia probaremos que si A es un dominio de ideales principales y M es un A-módulo finito generado existen elementos irreducibles únicos $p_1,\dots,p_r\in A$ y números naturales $n\geq 0$, $n_{ij}>0$ únicos de modo que

$$M \simeq A^n \oplus (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A).$$

Como corolario clasificaremos los grupos abelianos. También clasificaremos los endomorfismos lineales de un espacio vectorial. Aplicaremos esta teoría a la resolución de los sistemas de ecuaciones lineales diofánticas, la resolución de las ecuaciones diferenciales de orden superior con coeficientes constantes, la resolución de los sistemas de ecuaciones diferenciales lineales con coeficientes constantes y la resolución de ecuaciones en diferencias finitas.

CAPÍTULO 1
TEORÍA DE GRUPOS

1.1. Introducción

La estructura más básica y fundamental en Álgebra es la estructura de grupo (y semigrupo). Los anillos, los espacios vectoriales, los módulos, etc. necesitan para su definición de la noción de grupo.

Demos una justificación de carácter muy general para la introducción de la teoría de grupos, siguiendo a Felix Klein en su Erlanger Programm. Dar una teoría (geométrica) es dar una estructura, un espacio con cierta estructura. En esta teoría es fundamental el estudio del grupo de automorfismos de la estructura, es decir, de aquellas biyecciones del espacio que respetan la estructura del espacio. Las nociones y objetos de este espacio, o de la teoría, serán aquéllos que queden invariantes por el grupo de automorfismos recién mencionado. El estudio de las funciones, campos diferenciables, etc., que quedan invariantes por el grupo y el estudio de las relaciones que verifican éstos, son todos los teoremas de la teoría. Es pues el estudio de los grupos (y la teoría de invariantes) un tópico fundamental en Matemáticas.

En el cálculo de las raíces de un polinomio, es conveniente conocer el grupo de aquellas permutaciones de las raíces, que respetan las relaciones algebraicas que verifican éstas. Este grupo se denomina grupo de Galois del polinomio. En el curso "Álgebra I"de tercero del grado de Matemáticas, se estudiará con profundidad este grupo.

1.2. Grupos

1. Definición: Sea X un conjunto. Diremos que una aplicación $m : X \times X \to X$ es una operación (interna) en X. Seguiremos las notaciones[1] $m(x,x') = x \cdot x' = xx'$.

2. Definición: Sea G un conjunto. Diremos que una operación $G \times G \to G, (g,g') \mapsto g \cdot g'$ dota a G de estructura de grupo si cumple las siguientes condiciones:

1. Propiedad asociativa: $g \cdot (g' \cdot g'') = (g \cdot g') \cdot g''$, para todo $g, g', g'' \in G$.
2. Existencia de elemento neutro: Existe un elemento de G, que denotamos por 1 y denominamos elemento neutro, tal que $1 \cdot g = g \cdot 1 = g$, para todo $g \in G$.

[1] La operación $\cdot$, a veces, se denota con otros símbolos: $*$, $\circ$, etc.

3. Existencia de inversos: Para cada $g \in G$ existe un elemento de G, que denotamos por g^{-1} y denominamos inverso de g, tal que $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Si además se cumple que $g \cdot g' = g' \cdot g$, para todo $g, g' \in G$, diremos que G es un grupo abeliano o conmutativo; en cuyo caso, a menudo denotaremos la operación del grupo por $+$, al elemento neutro por 0 y al inverso de cada g por $-g$ (y lo denominaremos opuesto de g).

Si 1 y $1'$ son elementos neutros del grupo G entonces $1 = 1'$: $1 = 1 \cdot 1' = 1'$. Si h y h' son inversos de $g \in G$, entonces $h = h'$: $h = h \cdot 1 = hgh' = 1 \cdot h' = h'$.

3. Ejemplos: 1. El conjunto de los números enteros, $\mathbb{Z}$, con la suma es un ejemplo básico de grupo conmutativo.

2. El conjunto de todas las biyecciones de un conjunto X en sí mismo, $Biy X$, con la operación composición de aplicaciones, es un grupo no conmutativo (cuando X contenga más de dos elementos).

3. $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$ son grupos abelianos.

4. $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ y $(\mathbb{C}^*, \cdot)$ son grupos abelianos.

5. El conjunto de las sucesiones de números reales con la suma es un grupo abeliano.

6. El conjunto de las funciones reales de variable real (es decir, el conjunto de las aplicaciones de $\mathbb{R}$ en $\mathbb{R}$) con la suma de funciones es un grupo abeliano.

7. El conjunto de las matrices, $M_{n\times m}(\mathbb{R})$ con la suma de matrices es un grupo abeliano.

8. El conjunto de las matrices cuadradas de orden n invertibles con coeficientes reales, con el producto de matrices, es un grupo (que no es abeliano para $n > 1$).

Producto directo de grupos:

Sean $(G, \cdot)$ y $(G', \cdot')$ dos grupos. Podemos dotar al producto cartesiano de G y G', $G \times G'$, de estructura de grupo definiendo la siguiente operación

$$(g, g') * (h, h') := (g \cdot h, g' \cdot' h'), \text{ para todo } (g, g'), (h, h') \in G \times G'.$$

Si 1 es el elemento neutro de G y $1'$ es elemento neutro de G', entonces $(1, 1')$ es el elemento neutro de $G \times G'$.

Dado $(g, g') \in G \times G'$, entonces $(g, g')^{-1} = (g^{-1}, g'^{-1})$.

Sea $\{G_i\}_{i\in I}$ un conjunto de grupos (la operación en todos los G_i la denotaremos $\cdot$). Podemos dotar al producto cartesiano de todos los G_i, $\prod_{i\in I} G_i$ de estructura de grupo definiendo la siguiente operación

$$(g_i)_{i\in I} \cdot (h_i)_{i\in I} := (g_i \cdot h_i)_{i\in I}, \text{ para todo } (g_i)_{i\in I}, (h_i)_{i\in I} \in \prod_{i\in I} G_i.$$

Si 1_i es el elemento neutro de G_i, entonces $(1_i)_{i\in I}$ es el elemento neutro de $\prod_{i\in I} G_i$.

Dado $(g_i)_{i\in I} \in \prod_{i\in I} G_i$, entonces $((g_i)_{i\in I})^{-1} = (g_i^{-1})_{i\in I}$.

1.3. Subgrupos

1. Definición: Sea $(G,\cdot)$ un grupo. Diremos que un subconjunto $H \subseteq G$ es un subgrupo de G si cumple las siguientes condiciones:

1. Si $h,h' \in H$ entonces $h \cdot h' \in H$.
2. $1 \in H$.
3. Si $h \in H$ entonces $h^{-1} \in H$.

Si H es un subgrupo de G, entonces la operación de G define en H una estructura de grupo. Recíprocamente, si H es un subconjunto de un grupo G y la operación de G define en H una estructura de grupo entonces H es un subgrupo.

2. Proposición: *La intersección de cualquier familia de subgrupos de un grupo es un subgrupo.*

3. Definición: Dado un subconjunto X de un grupo G, llamaremos subgrupo generado por X y lo denotaremos $\langle X\rangle$, al mínimo subgrupo de G que contiene a X, es decir, a la intersección de todos los subgrupos de G que contienen a X.

4. Notación: Sea $(G,\cdot)$ un grupo y $g \in G$. Si $n > 0$, se define $g^n := g \overset{n}{\cdots} g$; si $n < 0$, se define $g^n := g^{-1} \overset{-n}{\cdots} g^{-1}$; y $g^0 := 1$. Dado $g \in G$, entonces $\langle g\rangle = \{g^n$, con $n \in \mathbb{Z}\}$.

Si G es un grupo conmutativo y escribimos el grupo G con notaciones aditivas (en vez de $\cdot$ escribimos $+$), escribiremos $n \cdot g$, en vez de g^n (como es natural).

Por ejemplo, el subgrupo de $\mathbb{Z}$ generado por $n \in \mathbb{Z}$, es igual a $\langle n\rangle = \{m \cdot n, m \in \mathbb{Z}\} =: n\mathbb{Z}$. El subgrupo de $\mathbb{Z}$ generado por $n,n' \in \mathbb{Z}$, es $\langle n,n'\rangle = \{mn + m'n', m,m' \in \mathbb{Z}\}$.

Sea $(G,+)$ un grupo abeliano y $G_1,G_2 \subseteq G$ dos subgrupos. Denotamos $\langle G_1 \cup G_2\rangle = G_1 + G_2$ y el lector puede comprobar que $G_1 + G_2 = \{g_1 + g_2,\ g_1 \in G_1\ g_2 \in G_2\}$.

5. Ejercicio: Sea G un grupo y $X \subseteq G$ un subconjunto. Pruébese que

$$\langle X\rangle = \text{El conjunto de todas las palabras formadas con las letras } \{g,g^{-1}\}_{g\in X}.$$

Dado un número entero $z \in \mathbb{Z}$, llamaremos valor absoluto de z y denotaremos $|z|$, al máximo entre z y $-z$.

6. Teorema de división de números enteros: *Sean n y $d \neq 0$ dos números enteros. Existe una única pareja de números enteros c y r (denominados cociente y resto de dividir n por d), tales que $0 \leq r < |d|$ y*

$$n = c \cdot d + r.$$

Demostración. Procedamos por inducción sobre $|n|$, para probar la existencia de c y r.

Si $|n| = 0$, entonces $c = 0$ y $r = 0$. Podemos suponer que $|n| > 0$. El teorema es cierto para d si y sólo si lo es para $-d$ (sólo hay que cambiar c por $-c$), luego podemos suponer que $d > 0$.

Supongamos $n > 0$. Si $n < d$, entonces $c = 0$ y $r = n$. Si $n \geq m.c.d.(a,b)d$, sea $n' = n - d$, luego $|n'| = n - d < n = |n|$. Por hipótesis de inducción existen c' y r' (cumpliendo $0 \leq r' < |d| = d$) tales que $n' = c'd + r'$, luego $n = (c' + 1)d + r'$ y hemos concluido.

Supongamos, ahora, $n < 0$. Si $-n \leq d$, sea $c = -1$ y $r = d + n$. Si $-n > d$, sea $n' = n + d$. luego $|n'| < |n|$. Por hipótesis de inducción existen c' y r' (cumpliendo $0 \leq r' < |d| = d$) tales que $n' = c'd + r'$, luego $n = (c' - 1)d + r'$ y hemos concluido.

Veamos la unicidad de c y r. Sea $n = cd + r = c'd + r'$, cumpliendo c, c', r, r' lo exigido. Podemos suponer $r \geq r'$. Entonces, $(c - c')d + (r - r') = 0$ y $|c - c'| \cdot |d| = |(c - c')d| = r - r' \leq r < |d|$, luego $c - c' = 0$. Por tanto, $c = c'$ y $r = n - cd = r'$.

□

7. Teorema: *Si H es un subgrupo del grupo (aditivo) de los números enteros $\mathbb{Z}$, entonces existe un único número natural n tal que $H = n\mathbb{Z}$.*

Demostración. Si $H = \{0\}$ entonces $H = 0 \cdot \mathbb{Z}$.

Supongamos $H \neq \{0\}$. Existen naturales positivos en H, porque el opuesto de cada número entero de H pertenece a H. Sea $n \in H$ el mínimo número natural no nulo contenido en H. Veamos que $H = n\mathbb{Z}$: Obviamente, $n\mathbb{Z} \subseteq H$. Dado $m \in H \subset \mathbb{Z}$, existen números enteros c y r tales que

$$m = cn + r, \quad 0 \leq r < n.$$

Luego, $r = m - cn \in H$, porque $m, -cn \in H$. Por la definición de n, se tiene que $r = 0$. Luego, $m \in n\mathbb{Z}$, $H \subseteq n\mathbb{Z}$ y $H = n\mathbb{Z}$.

Por último, demostremos la unicidad: observemos que si un número natural m pertenece a $n\mathbb{Z}$, entonces $m \geq n$. Por tanto, si $m\mathbb{Z} = n\mathbb{Z}$, $m \geq n$ y $n \geq m$, luego $m = n$.

□

1.4. Morfismos de grupos

1. Definición: Diremos que una aplicación $f : G \to G'$ entre dos grupos es un morfismo de grupos si para todo $g, g' \in G$ se cumple que

$$f(g \cdot g') = f(g) \cdot f(g').$$

Diremos que f es un isomorfismo de grupos si f es biyectiva (en tal caso la aplicación inversa f^{-1} es un isomorfismo de grupos). Diremos que es un epimorfismo (resp. monomorfismo) de grupos si f es epiyectiva (resp. inyectiva).

Si $f : G \to G'$ es un morfismo de grupos entonces $f(1) = 1$: $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$ y multiplicando por $f(1)^{-1}$ obtenemos $1 = f(1)$. Además, $f(g^{-1}) = f(g)^{-1}$: $1 = f(1) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1})$ y multiplicando por $f(g)^{-1}$ obtenemos $f(g)^{-1} = f(g^{-1})$.

2. Ejemplo: Sea G un grupo y $g \in G$. La aplicación $\tau_g : G \to G$ "conjugar por g", definida por

$$\tau_g(g') := gg'g^{-1}, \quad \text{para todo } g' \in G,$$

es un isomorfismo de grupos: $\tau_g(g_1 g_2) = gg_1g_2g^{-1} = gg_1g^{-1}gg_2g^{-1} = \tau_g(g_1)\tau_g(g_2)$. Además, $(\tau_g)^{-1} = \tau_{g^{-1}}$. En efecto,

$$\tau_g(\tau_{g^{-1}}(g')) = g(g^{-1}g'g)g^{-1} = g' \text{ y } \tau_{g^{-1}}(\tau_g(g')) = g^{-1}(gg'g^{-1})g = g'.$$

Denotaremos $\mathrm{Hom}_{grp}(G,G')$ al conjunto de todos los morfismos de grupos de G en G'.

3. Ejemplo: Sean G_1 y G_2 dos grupos. La aplicación $\pi_1\colon G_1\times G_2\to G_1$, $\pi_1(g_1,g_2):=g_1$ es un morfismo de grupos. Igualmente, la aplicación $\pi_2\colon G_1\times G_2\to G_2$, $\pi_2(g_1,g_2):=g_2$ es un morfismo de grupos. Sea G otro grupo, se cumple que la aplicación

$$\mathrm{Hom}_{grp}(G,G_1\times G_2)\to \mathrm{Hom}_{grp}(G,G_1)\times \mathrm{Hom}_{grp}(G,G_2),\ f\mapsto(\pi_1\circ f,\pi_2\circ f)$$

es biyectiva.

4. Definición: Sea $f\colon G\to G'$ un morfismo de grupos. Llamaremos núcleo de f y lo denotaremos $\mathrm{Ker}\, f$, al subconjunto de G

$$\mathrm{Ker}\, f := f^{-1}(1)=\{g\in G\colon f(g)=1\}.$$

Llamaremos imagen de f, que denotaremos $\mathrm{Im}\, f$, a la imagen de la aplicación f, es decir,

$$\mathrm{Im}\, f:=\{f(g)\in G', g\in G\}.$$

5. Proposición: $\mathrm{Ker}\, f$ *es un subgrupo de* G *e* $\mathrm{Im}\, f$ *es un subgrupo de* G'. *Más aún, la antimagen por un morfismo de grupos de un subgrupo es subgrupo y la imagen de un subgrupo es subgrupo.*

Dado un morfismo de grupos $f\colon G\to G'$ y $g\in G$, calculemos el conjunto de elementos $g'\in G$ tales que $f(g')=f(g)$: $f(g')=f(g)$ si y sólo si $1=f(g)^{-1}\cdot f(g')=f(g^{-1}\cdot g')$, es decir, si y sólo si $g^{-1}\cdot g'\in \mathrm{Ker}\, f$, que equivale a decir que $g'\in g\cdot \mathrm{Ker}\, f:=\{g\cdot h, h\in \mathrm{Ker}\, f\}$.

6. Proposición: *Un morfismo de grupos* $f\colon G\to G'$ *es inyectivo si y sólo si* $\mathrm{Ker}\, f=\{1\}$.

Si identificamos los elementos de G cuando tengan la misma imagen, obtenemos un conjunto biyectivo con la imagen. Por tanto, el conjunto $\bar{G}:=\{\bar{g}, g\in G\colon \bar{g}'=\bar{g}$ si y sólo si $g'\in g\cdot \mathrm{Ker}\, f\}$ es biyectivo con $\mathrm{Im}\, f$. De hecho esta biyección es un isomorfismo de grupos como veremos.

1.5. Cocientes por subgrupos

Sea $H\subseteq G$ un subgrupo y $g,g'\in G$.

Si $g'\in gH$ entonces $g'H=gH$: Sea $h\in H$, tal que $g'=gh$. Entonces, $g'H=ghH=gH$.

Si $g'\notin gH$, entonces $g'H\cap gH=\emptyset$, pues si $z\in g'H\cap gH$, entonces $g'H=zH=gH$.

En conclusión, dados $g,g'\in G$, o $gH=g'H$ o bien $gH\cap g'H=\emptyset$.

1. Definición: Sea $H\subseteq G$ un subgrupo. Llamaremos conjunto cociente de G por H, que denotaremos G/H, al conjunto

$$G/H:=\{\bar{g},\ \text{con } g\in G\colon \bar{g'}=\bar{g} \text{ si y sólo si } g'\in g\cdot H \text{ (o equivalentemente } g'H=gH)\}.$$

Es decir, si en G identificamos cada $g\in G$ con todos los elementos de $gH\subseteq G$, obtenemos el conjunto G/H.

2. Notación: Se dice que g es congruente con g' módulo H y se denota $g \equiv g' \, mod \, H$, cuando $\bar{g} = \bar{g}'$ en G/H, es decir, $g \in g'H$ (o $g'^{-1}g \in H$). En notaciones aditivas, si $(G,+)$ es un grupo abeliano y $H \subset G$ es un subgrupo, entonces $g \equiv g' \, mod \, H$ cuando $\bar{g} = \bar{g}'$ en G/H, es decir, $g \in g' + H$ (o $-g' + g \in H$).

La aplicación $G \to G/H$, $g \mapsto \bar{g}$, se denomina el morfismo de paso cociente (por H).

3. Ejemplo: $G/\{1\}$ es biyectivo con G. En efecto, estamos identificando cada $g \in G$ sólo con $g \cdot 1 = g$. Con rigor, la aplicación de paso al cociente $\pi : G \to G/\{1\}$, $\pi(g) = \bar{g}$ es biyectiva: Es epiyectiva, pues dado $\bar{g} \in G/\{1\}$, $\pi(g) = \bar{g}$. Es inyectiva, porque si $\bar{g} = \bar{g}'$, entonces $g' = g \cdot 1 = g$.

4. Ejemplo: G/G es biyectivo con $\{1\}$. En efecto, estamos identificando cada $g \in G$ con todos los elementos de $g \cdot G = G$. Es decir, hacemos iguales todos los elementos de G. Con rigor, la aplicación $\{1\} \to G/G$, $1 \mapsto \bar{1}$ es biyectiva: Dado $\bar{g} \in G/G$ tenemos que $\bar{g} = \bar{1}$ porque $g = 1 \cdot g$.

5. Definición: Llamaremos orden de un conjunto X, que denotaremos $|X|$, al número de elementos del conjunto. Si el conjunto tiene un número infinito de elementos diremos que es de cardinal infinito.

6. Ejemplo: Si $n > 0$, entonces $\mathbb{Z}/n\mathbb{Z}$ es un conjunto de orden n, explícitamente $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \ldots, \overline{n-1}\}$: Dado $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$, por el teorema de división de números enteros, existen números enteros únicos c y r, con $0 \leq r < n$, de modo que $m = cn + r$. Por tanto, existe un único $r \in \{0, \ldots, n-1\}$, tal que $\bar{m} = \bar{r}$.

7. Teorema de Lagrange: *Sea G un grupo de orden finito. Si H es un subgrupo de G entonces*

$$|G| = |G/H| \cdot |H|.$$

En particular, el orden de H divide al de G.

Demostración. $G = \coprod_{\bar{g} \in G/H} g \cdot H$ y $|gH| = |H|$ (porque la aplicación $H \to gH$, $h \mapsto gh$ es biyectiva). Por tanto, $|G| = |G/H| \cdot |H|$.

□

8. Definición: Se dice que un subgrupo $H \subseteq G$ es normal (en G) cuando $gHg^{-1} \subseteq H$, para todo $g \in G$, es decir, si $ghg^{-1} \in H$, para todo $g \in G$ y $h \in H$.

9. Ejemplo: Si G es un grupo conmutativo, todo subgrupo de G es normal en G.

10. Ejemplo: Los subgrupos de G, $\{1\}$ y G son normales.

11. Ejemplo: $H = \{\mathrm{Id}, (1,2)\} \subset S_3$ no es un subgrupo normal.

Si H es un subgrupo normal de G y tomamos $g^{-1} \in G$, tendremos $g^{-1}Hg \subseteq H$, luego $H \subseteq gHg^{-1} \subseteq H$ y $gHg^{-1} = H$ (para todo $g \in G$). Por tanto, $gH = Hg$, para todo $g \in G$, y recíprocamente si un subgrupo cumple esta condición el subgrupo es normal.

Sea $H \subseteq G$ un subgrupo normal. Definamos en G/H la operación

$$\bar{g} \cdot \bar{g}' := \overline{gg'},$$

que está bien definida porque $gHg'H = gg'HH = gg'H$. La propiedad asociativa se cumple de modo obvio, $\bar{1}$ es el elemento neutro y $\overline{g^{-1}}$ es el inverso de $\bar{g} \in G/H$. Luego,

G/H es grupo. Además, $\pi: G \to G/H$ es morfismo de grupos, pues $\pi(g\cdot g') = \overline{gg'} = \bar{g}\cdot\bar{g'} = \pi(g)\cdot\pi(g')$.

12. Proposición: *Sea $f: G \to G'$ un morfismo de grupos. Se cumple que* $\operatorname{Ker} f$ *es un subgrupo normal de G.*

Demostración. Al lector. □

13. Teorema de isomorfía: *Sea $f: G \to G'$ un morfismo de grupos. La aplicación, $\bar{f}: G/\operatorname{Ker} f \to \operatorname{Im} f$, $\bar{f}(\bar{g}) := f(g)$, es un isomorfismo de grupos.*

Demostración. La aplicación $\bar{f}$ está bien definida: dado $\overline{gh} = \bar{g} \in G/H$ (con $h \in H$), tenemos que $f(gh) = f(g)f(h) = f(g)1 = f(g)$.

Veamos que $\bar{f}$ es inyectiva: si $1 = \bar{f}(\bar{g}) = f(g)$, entonces $g \in \operatorname{Ker} f$ y $\bar{g} = \bar{1}$, luego $\operatorname{Ker}\bar{f} = \{\bar{1}\}$. Veamos que es epiyectiva: dado $f(g) \in \operatorname{Im} f$, tenemos que $\bar{f}(\bar{g}) = f(g)$.

Dejamos que el lector compruebe que $\bar{f}$ es morfismo de grupos. □

Observemos que dado un morfismo de grupos $f: G \to G'$ tenemos el diagrama conmutativo

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow{\scriptstyle \pi} & & \uparrow \\ G/\operatorname{Ker} f & \xrightarrow{\bar{f}} & \operatorname{Im} f \end{array} \qquad \begin{array}{ccc} g & \longmapsto & f(g) \\ \downarrow{\scriptstyle \pi} & & \uparrow \\ \bar{g} & \longmapsto & f(g) \end{array}$$

14. Ejemplo: Consideremos el subgrupo $\mathbb{Z} \subset \mathbb{R}$. Dado $\bar{r} \in \mathbb{R}/\mathbb{Z}$, tenemos que $\bar{r} = \overline{r+1} = \overline{r-1} = \overline{r+2} = \overline{r-2} = \cdots$. Veamos que $\mathbb{R}/\mathbb{Z}$ es un grupo isomorfo al grupo $(0,1]$, donde $(0,1]$ es un grupo con la siguiente operación

$$\alpha * \beta = \begin{cases} \alpha+\beta, & \text{si } \alpha+\beta \le 1 \\ \alpha+\beta-1, & \text{si } \alpha+\beta > 1 \end{cases}$$

Consideremos la aplicación $(0,1] \to \mathbb{R}/\mathbb{Z}$, $\alpha \mapsto \bar{\alpha}$. Dejamos que el lector pruebe que es isomorfismo de grupos.

15. Ejercicio: Sea $f: G \to G'$ un morfismo de grupos. Sea H un subgrupo normal de G y supongamos que $H \subseteq \operatorname{Ker} f$. Demuéstrese que la aplicación $\bar{f}: G/H \to G'$ definida por $\bar{f}(\bar{g}) = f(g)$ está bien definida y es un morfismo de grupos.

1.6. Grupos cíclicos

1. Definición: Diremos que un grupo G es cíclico si está generado por uno de sus elementos, es decir, existe $g \in G$ de modo que $G = \langle g \rangle$.

2. Proposición: *Un grupo G es cíclico si y sólo si es isomorfo a $\mathbb{Z}/n\mathbb{Z}$, para algún número natural n.*

Demostración. $\mathbb{Z}/n\mathbb{Z}$ es un grupo (aditivo) cíclico, generado por $\bar{1}$.

Supongamos que $G = \langle g \rangle$ es cíclico. Sea $f: \mathbb{Z} \to G$, la aplicación definida por $f(n) := g^n$. Es fácil comprobar que f es un morfismo de grupos. $\operatorname{Im} f$ es un subgrupo de G, que contiene a g, luego $\operatorname{Im} f = G$ y f es epiyectivo. $\operatorname{Ker} f$ es un subgrupo de $\mathbb{Z}$, luego existe $n \in \mathbb{N}$ tal que $\operatorname{Ker} f = n\mathbb{Z}$. Por el teorema de isomorfía $\mathbb{Z}/n\mathbb{Z} \simeq G$. □

$\mathbb{Z}/n\mathbb{Z}$ es un grupo conmutativo, pues es cociente de $\mathbb{Z}$ que es conmutativo. Por tanto, todo grupo cíclico es conmutativo.

3. Definición: Llamaremos orden de un elemento g de un grupo G, al orden del subgrupo $\langle g\rangle$ de G que genera.

En la proposición anterior hemos dado el isomorfismo $\mathbb{Z}/n\mathbb{Z} \simeq \langle g\rangle$, $\bar{m} \mapsto g^m$. Por tanto, si $n > 0$, el orden de g es igual a $|\langle g\rangle| = |\mathbb{Z}/n\mathbb{Z}| = n$, $\langle g\rangle = \{1, g^1, \dots, g^{n-1}\}$ y n es el mínimo número natural positivo tal que $g^n = 1$, además, si $g^m = 1$, entonces m es un múltiplo del orden de g. Si $n = 0$, entonces el orden de g es $|\langle g\rangle| = |\mathbb{Z}| = \infty$ y $\langle g\rangle = \{\dots, g^{-m}, \dots, 1, g^1, \dots, g^m, \dots\}$ (cumpliendo $g^i \neq g^j$, para todo $i, j \in \mathbb{Z}$, $i \neq j$).

4. Si G es un grupo de orden $m < \infty$, entonces el orden de todo elemento $g \in G$ divide a m, ya que el orden de todo subgrupo $\langle g\rangle$ divide al orden del grupo G, por el teorema de Lagrange. Es decir, $g^{|G|} = 1$.

5. Proposición: *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración. Sea $G = \langle g\rangle$ un grupo cíclico y $\pi\colon \mathbb{Z} \to G$, $\pi(n) := g^n$ un epimorfismo de grupos. Dado un subgrupo $H \subseteq G$, se cumple que $H = \pi(\pi^{-1}(H))$. Ahora bien, $\pi^{-1}(H)$ es un subgrupo de $\mathbb{Z}$, luego es cíclico (es decir, generado por un elemento z). Por tanto, $H = \pi(\pi^{-1}(H))$ está generado por $\pi(z)$ y es cíclico. □

1.7. Grupo simétrico

El grupo simétrico S_n es el grupo de todas las biyecciones (o "permutaciones") de un conjunto de n-elementos en sí mismo, con la operación composición de aplicaciones.

Comentario: Una biyección entre dos conjuntos $\tau\colon X \to Y$, puede entenderse como una identificación de X con Y: "a $x \in X$ lo llamamos $\tau(x)$ en Y". Dada una aplicación $f\colon X \to X$, que aplica x en $f(x)$, tenemos la correspondiente aplicación en Y: "la que aplica $\tau(x)$ en $\tau(f(x))$, es decir, la aplicación $\tau \circ f \circ \tau^{-1}\colon Y \to Y$". Así el grupo de las permutaciones de X se identifica con el grupo de las permutaciones de Y (vía la identificación de X con Y). Con mayor precisión, el morfismo

$$BiyX \to BiyY, \quad \sigma \mapsto \tau \circ \sigma \circ \tau^{-1}$$

es un isomorfismo de grupos (como el lector puede comprobar).

Si Y es un conjunto de orden n, entonces Y es biyectivo con $\{1, \dots, n\} =: X$ y $BiyY = BiyX =: S_n$. El número de permutaciones de n elementos es $n!$, luego $|S_n| = n!$.

1. Proposición: *Sea G un grupo de orden n. La aplicación $G \to \mathrm{Biy}(G)$, $g \mapsto L_g$, donde $L_g(g') := gg'$ es un morfismo de grupos inyectivo, luego "G es isomorfo a un subgrupo de un grupo simétrico S_n".*

2. Definición: Dados r elementos distintos $x_1, \dots, x_r \in X$, con $r > 1$, denotaremos $(x_1, \dots, x_r) = \sigma \in BiyX$ a la permutación definida por $\sigma(x_i) = x_{i+1}$, para todo $i < r$; $\sigma(x_r) = x_1$; y $\sigma(x) = x$, para todo $x \notin \{x_1, \dots, x_r\}$. Diremos que $(x_1, \dots, x_r)$ es un ciclo y observemos que es de orden r. Si $r = 2$, diremos que el ciclo (x_1, x_2) es una transposición. Diremos que dos ciclos $(x_1, \dots, x_r), (x'_1, \dots, x'_{r'})$ de $BiyX$ son disjuntos si $x_i \neq x'_j$ para todo i, j.

3. Lema: *Si $\sigma = (x_1, \dots, x_r)$ y $\sigma' = (x'_1, \dots, x'_{r'})$ son disjuntos, entonces conmutan, es decir, $\sigma \circ \sigma' = \sigma' \circ \sigma$.*

Demostración. Para $x \in \{x_1, \dots, x_r\}$, $(\sigma \circ \sigma')(x) = \sigma(x) = (\sigma' \circ \sigma)(x)$. Para $x \in \{x'_1, \dots, x'_r\}$, $(\sigma \circ \sigma')(x) = \sigma'(x) = (\sigma' \circ \sigma)(x)$. Para $x \notin \{x_i, x'_j\}_{i,j}$, $(\sigma \circ \sigma')(x) = x = (\sigma' \circ \sigma)(x)$.

De otro modo (siguiendo el comentario anterior): $\sigma' \circ \sigma \circ \sigma'^{-1} = (\sigma'(x_1), \dots, \sigma'(x_r)) = (x_1, \dots, x_r) = \sigma$ y hemos concluido.

□

4. Teorema: *Toda permutación $\sigma \in S_n$, distinta de la identidad, es igual a un producto de ciclos disjuntos, de modo único salvo el orden de los factores.*

Demostración. Sea $x \in X$, tal que $\sigma(x) \neq x$. Sea r el mínimo número natural positivo tal que $\sigma^r(x) = x$ (tal número existe porque el orden de σ, que divide al orden de S_n, es finito). Para todo $0 \leq s < s' < r$, se cumple que $\sigma^{s'}(x) \neq \sigma^s(x)$: pues componiendo con σ^{-s} son distintos, pues $\sigma^{s'-s}(x) \neq x$, porque $0 < s' - s < r$. Sea $\sigma_1 = (x, \sigma(x), \dots, \sigma^{r-1}(x))$. Entonces, como σ_1 y σ coinciden sobre $\{x, \sigma(x), \dots, \sigma^{r-1}(x)\}$ y σ_1 es la identidad sobre $X \setminus \{x, \sigma(x), \dots, \sigma^{r-1}(x)\}$, se cumple que $\sigma_1^{-1} \circ \sigma$ deja fijos $\{x, \sigma(x), \dots, \sigma^{r-1}(x)\}$ y los que dejaba fijos σ. Reiterando el proceso obtenemos ciclos disjuntos $\sigma_1, \dots, \sigma_s$ tales que $\sigma_s^{-1} \circ \cdots \circ \sigma_1^{-1} \circ \sigma = \mathrm{Id}$. Luego, $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$.

Sea otra descomposición $\sigma = \tau_1 \circ \cdots \tau_t$ en producto de ciclos disjuntos. Reordenando, podemos suponer que $\tau_1(x) \neq x$. Es decir, x "aparece" en el ciclo τ_1 (y en el de σ_1). Luego, $\tau_1(x) = \sigma(x) = \sigma_1(x)$. Obviamente, $\tau_1(x) = \sigma(x) = \sigma_1(x)$ "aparece" en ciclo de τ_1 y en el de σ_1. Luego, $\tau_1^2(x) = \sigma^2(x) = \sigma_1^2(x)$. Así sucesivamente, $\tau_1^i(x) = \sigma^i(x) = \sigma_1^i(x)$, para todo i. Por tanto, $\tau_1 = \sigma_1$ y $\sigma_2 \circ \cdots \circ \sigma_s = \tau_2 \circ \cdots \circ \tau_t$. Reiterando el argumento concluimos que, después de reordenar los factores, $\sigma_2, \dots, \sigma_s$ coinciden con $\tau_2, \dots, \tau_t$.

□

5. Definición: Sea $\sigma \in S_n$ una permutación distinta de la identidad. Sea $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$ una descomposición en producto de ciclos disjuntos y d_i el orden de σ_i. Reordenando podemos suponer que $d_1 \geq d_2 \geq \cdots \geq d_s$. Diremos que $d_1, \dots, d_s$ es la forma de σ.

6. Definición: Dado un elemento $g \in G$, diremos que el morfismo $\tau_g : G \to G$, $\tau_g(g') := gg'g^{-1}$, es la conjugación en G por g. Diremos que $h, h' \in G$ son conjugados si y sólo si existe $g \in G$, de modo que $\tau_g(h) = h'$.

7. Teorema: *La condición necesaria y suficiente para que $\sigma, \sigma' \in S_n$ sean conjugadas es que tengan la misma forma.*

Demostración. Sea $\sigma = (x_{11}, \dots, x_{1d_1}) \circ \cdots \circ (x_{s1}, \cdots, x_{sd_s})$ una descomposición en producto de ciclos disjuntos y $\tau \in S_n$. Entonces,

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_{11}), \dots, \tau(x_{1d_1})) \circ \cdots \circ (\tau(x_{s1}), \cdots, \tau(x_{sd_s}))$$

tiene la misma forma que σ. Sea $\sigma' = (x'_{11}, \dots, x'_{1d_1}) \circ \cdots \circ (x'_{s1}, \cdots, x'_{sd_s})$. Si τ es cualquier permutación que cumpla $\tau(x_{ij}) = x'_{ij}$, para todo i, j, entonces $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. □

8. Proposición: *Si $d_1, \dots, d_s$ es la forma de $\sigma \in S_n$, entonces el orden de σ es el mínimo común múltiplo de $d_1, \dots, d_s$.*

Demostración. Escribamos $\sigma = \sigma_1 \cdots \sigma_s$ como producto de ciclos disjuntos. Entonces, $\sigma^n = \sigma_1^n \cdots \sigma_s^n$ y σ_i^n es "disjunta" con σ_j^n, para $i \neq j$. Luego, $\sigma^n = \mathrm{Id}$ si y sólo si $\sigma_1^n = \cdots = \sigma_s^n = \mathrm{Id}$. Luego el orden de σ es el mínimo común múltiplo de los órdenes de los σ_i. □

9. Proposición: *Todo permutación $\sigma \in S_n$ es producto de transposiciones.*

Demostración. Como toda permutación es producto de ciclos, basta probar que todo ciclo es producto de transposiciones. Sea, pues, un ciclo $(x_1, \ldots, x_r) \in S_n$. Obviamente,

$$(x_1, \ldots, x_r) = (x_1, x_2)(x_2, \ldots, x_r) = (x_1, x_2)(x_2, x_3)(x_3, \ldots, x_r) = \cdots = (x_1, x_2)(x_2, x_3) \cdots (x_{r-1}, x_r)$$

□

Signo de una permutación.

Cada permutación $\sigma \in S_n = Biy(\{1, 2, \ldots, n\})$ define una biyección del anillo de polinomios en n variables con coeficientes números racionales: $\mathbb{Q}[x_1, \ldots, x_n] \to \mathbb{Q}[x_1, \ldots, x_n]$, $p(x_1, \ldots, x_n) \mapsto p(x_1, \ldots, x_n)^\sigma := p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$.

Sea $\delta(x_1, \ldots, x_n) := \prod_{i<j}(x_i - x_j) \in \mathbb{Q}[x_1, \ldots, x_n]$. Dada una permutación $\sigma \in S_n = Biy(\{1, 2, \ldots, n\})$, es fácil comprobar que $\delta(x_1, \ldots, x_n)^\sigma = \delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \pm\delta(x_1, \ldots, x_n)$.

10. Definición: Dada $\sigma \in S_n$, llamaremos signo de σ, que denotaremos $\mathrm{sign}(\sigma)$, al número entero 1 ó -1 tal que $\delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \mathrm{sign}(\sigma) \cdot \delta(x_1, \ldots, x_n)$.

11. Proposición: *Consideremos el grupo (multiplicativo) $\{1, -1\}$. El morfismo natural*

$$\mathrm{sign}\colon S_n \to \{1, -1\},\ \sigma \mapsto \mathrm{sign}(\sigma)$$

es un morfismo de grupos.

Demostración. $\mathrm{sign}(\sigma'\sigma) \cdot \delta = \delta^{\sigma'\sigma} = (\delta^\sigma)^{\sigma'} = (\mathrm{sign}(\sigma)\delta)^{\sigma'} = \mathrm{sign}(\sigma') \cdot \mathrm{sign}(\sigma) \cdot \delta$. Luego, $\mathrm{sign}(\sigma) \cdot \mathrm{sign}(\sigma') = \mathrm{sign}(\sigma \cdot \sigma')$. □

Es fácil ver que $\mathrm{sign}(\mathrm{Id}) = 1$ y que $\mathrm{sign}((1, 2)) = -1$.

Observemos que el signo es invariante por conjugaciones, es decir,

$$\mathrm{sign}(\tau\sigma\tau^{-1}) = \mathrm{sign}(\tau) \cdot \mathrm{sign}(\sigma) \cdot \mathrm{sign}(\tau)^{-1} = \mathrm{sign}(\sigma).$$

En particular, el signo de toda transposición es -1, porque todas son conjugadas de la transposición $(1, 2)$.

12. Proposición: *Si la forma de una permutación $\sigma \in S_n$ es $d_1, \ldots, d_r$, entonces*

$$\mathrm{sign}(\sigma) = (-1)^{d_1 - 1} \cdots (-1)^{d_r - 1} = (-1)^{d_1 + \cdots + d_r - r}.$$

Demostración. Si $\sigma = (x_1, \ldots, x_r)$ es un ciclo, entonces

$$(x_1, \ldots, x_r) = (x_1, x_2)(x_2, x_3) \cdots (x_{r-1}, x_r)$$

es producto de $r - 1$ transposiciones. Como el morfismo sign es un morfismo de grupos, $\mathrm{sign}(\sigma) = (-1)^{r-1}$.

En general, $\sigma = \sigma_1 \cdots \sigma_r$, donde σ_i es un ciclo de orden d_i. Por tanto, $\mathrm{sign}(\sigma) = \mathrm{sign}(\sigma_1) \cdots \mathrm{sign}(\sigma_r) = (-1)^{d_1 - 1} \cdots (-1)^{d_r - 1}$. □

Evidentemente, sign es un epimorfismo (para $n > 1$).

13. Definición: Llamaremos subgrupo alternado de S_n, que denotaremos A_n, al núcleo del morfismo sign, es decir, al subgrupo (normal) de S_n formado por las permutaciones de signo positivo.

Por el teorema de isomorfía $S_n/A_n \simeq \{1,-1\} \simeq \mathbb{Z}/2\mathbb{Z}$. Por el teorema de Lagrange, $|A_n| = |S_n|/2 = n!/2$ $(n > 1)$.

1.8. Cuestionario

1. ¿Es $(\mathbb{N},+)$ un grupo?¿Y $(\mathbb{Q},\cdot)$?
2. ¿Es S_3 con la composición de permutaciones un grupo abeliano?¿Es el grupo de las matrices $2x2$ con coeficientes reales invertibles, con la multiplicación de matrices, un grupo abeliano?
3. Sean g_1, g_2, g_3 tres elementos de un grupo G. Calcúlese $(g_1 \cdot g_2 \cdot g_3)^{-1}$ en términos de productos de los elementos g_1^{-1}, g_2^{-1} y g_3^{-1}.
4. Sean g, g' dos elementos de un grupo $(G,\cdot)$. Probar que si $g \cdot g' = g'$ entonces $g = 1$.
5. Sean x e y dos elementos de un grupo G. Si $x^5 = 1$, $y^4 = 1$ y $xy = yx^3$, probar que $x^2y = yx$ y $xy^3 = y^3x^2$.
6. Consideremos los grupos $(\mathbb{Z},+)$, $(\mathbb{R}^*,\cdot)$. Consideremos el grupo producto directo $\mathbb{Z} \times \mathbb{R}^*$ y $(3,3) \in \mathbb{Z} \times \mathbb{R}^*$. Calcúlese $(3,3)^{-1}$.
7. Sea $A = \begin{pmatrix} 0 & 0 & -1 \\ -1 & -0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Calcúlese A^{2001}.
8. Sea G el conjunto de los enteros que son múltiplos de 6 y 10 ¿Es G es un subgrupo de $(\mathbb{Z},+)$?¿Es G el conjunto de los múltiplos de algún número natural?
9. ¿Existe $(n,m) \in \mathbb{Z} \times \mathbb{Z}$ de modo que $\mathbb{Z} \times \mathbb{Z} = \langle (n,m) \rangle$?
10. Sea G un grupo. Pruébese que G es abeliano si y sólo si $gg'g^{-1}g'^{-1} = 1$ para todo $g, g' \in G$. Pruébese que la aplicación $G \to G$, $g \mapsto g^{-1}$, para todo g, es un morfismo de grupos si y sólo si G es abeliano.
11. Sea $f : G \to G'$ un morfismo de grupos. Demuéstrese que $\operatorname{Ker} f$ es un subgrupo de G.
12. Defínase una biyección entre $\mathbb{R}/\mathbb{Z}$ y $(0,1]$.
13. Sea $f : \mathbb{Z} \to \mathbb{C}^*$, $f(n) := e^{\frac{n \cdot 2 \cdot \pi \cdot i}{5}}$. Pruébese que f es un morfismo de grupos. Calcúlese $\operatorname{Ker} f$. Calcúlese $\operatorname{Im} f$. Pruébese que $\mathbb{Z}/5\mathbb{Z} \simeq \operatorname{Im} f$.
14. Demuéstrese que G/G es un grupo isomorfo al grupo $\{1\}$. Demuéstrese que $G/\{1\}$ es un grupo isomorfo a G.

15. Sea $H = \{\mathrm{Id}, (1,2)\} \subset S_3$ ¿Es H un subgrupo normal de S_3?¿Es H conmutativo?

16. Sea $H = \{\mathrm{Id}, (1,2)\} \subset S_3$. Demuéstrese que H es un grupo isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

17. Pruébese que todo grupo de orden primo es cíclico.

18. Sea $f : G \to G'$ un morfismo de grupos epiyectivo. Si G es cíclico pruébese que G' es cíclico.

19. ¿Es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ un grupo cíclico?

20. ¿Qué elementos de $\mu_6 := \{e^{\frac{2\cdot\pi\cdot i\cdot n}{6}} \in \mathbb{C}$, con n natural y $0 \leq n < 6\}$ lo generan?

21. Resuélvase el problema 9.

22. Explicítense todos los elementos de S_4 de signo positivo.

23. Explicítense todos los elementos de S_4 de orden 2.

24. Sea $\sigma \in S_7$ la permutación definida por $\sigma(1) = 7$, $\sigma(2) = 6$, $\sigma(3) = 4$, $\sigma(4) = 5$, $\sigma(5) = 3$, $\sigma(6) = 2$ y $\sigma(7) = 1$. Calcúlense $\mathrm{ord}(\sigma)$ y $\mathrm{sign}(\sigma)$.

1.9. Biografía de Georg Fröbenius

FRÖBENIUS BIOGRAPHY

Georg Fröbenius's father was Christian Ferdinand Fröbenius, a Protestant parson, and his mother was Christine Elizabeth Friedrich. Georg was born in Charlottenburg which was a district of Berlin which was not incorporated into the city until 1920. He entered the Joachimsthal Gymnasium in 1860 when he was nearly eleven years old and graduated from the school in 1867. In this same year he went to the University of Göttingen where he began his university studies but he only studied there for one semester before returning to Berlin.

Back at the University of Berlin he attended lectures by Kronecker, Kummer and Weierstrass. He continued to study there for his doctorate, attending the seminars of Kummer and Weierstrass, and he received his doctorate (awarded with distinction) in 1870 supervised by Weierstrass. In 1874, after having taught at secondary school level first at the Joachimsthal Gymnasium then at the Sophienrealschule, he was appointed to the University of Berlin as an extraordinary professor of mathematics.

For the description of Fröbenius's career so far, the attentive reader may have noticed that no mention has been made of him receiving his habilitation before being appointed to a teaching position. This is not an omission, rather it is surprising given the strictness of the German system that this was allowed. We should say that it must ultimately have been made possible due to strong support from Weierstrass who was extremely influential and considered Fröbenius one of his most gifted students.

Fröbenius was only in Berlin for a year before he went to Zürich to take up an appointment as an ordinary professor at the Eidgenössische Polytechnikum. For seventeen years, between 1875 and 1892, Fröbenius worked in Zürich. He married there and brought up a family and did much important work in widely differing areas of mathematics. We shall discuss some of the topics which he worked on below, but for the moment we shall continue to describe how Fröbenius's career developed.

In the last days of December 1891 Kronecker died and, therefore, his chair in Berlin became vacant. Weierstrass, strongly believing that Fröbenius was the right person to keep Berlin in the forefront of mathematics, used his considerable influence to have Fröbenius appointed. However, for reasons which we shall discuss in a moment, Fröbenius turned out to be something of a mixed blessing for mathematics at the University of Berlin.

The positive side of his appointment was undoubtedly his remarkable contributions to the representation theory of groups, in particular his development of character theory, and his position as one of the leading mathematicians of his day. The negative side came about largely through his personality which is described as:

"*... occasionally choleric, quarrelsome, and given to invectives.*"

Biermann described the strained relationships which developed between Fröbenius and his colleagues at Berlin:

"*... suspected at every opportunity a tendency of the Ministry to lower the standards at the University of Berlin, in the words of Fröbenius, to the rank of a technical school ... Even so, Fuchs and Schwarz yielded to him, and later Schottky, who was indebted to him alone for his call to Berlin. Fröbenius was the leading figure, on whom the fortunes of mathematics at Berlin university rested for 25 years. Of course, it did not escape him, that the number of doctorates, habilitations, and docents slowly but surely fell off, although the number of students increased considerably. That he could not prevent this, that he could not reach his goal of maintaining unchanged the times of Weierstrass, Kummer and Kronecker also in their external appearances, but to witness helplessly these developments, was doubly intolerable for him, with his choleric disposition.*"

We should not be too hard on Fröbenius for, as Haubrich explained:

"*They all felt deeply obliged to carry on the Prussian neo-humanistic tradition of university research and teaching as they themselves had experienced it as students. This is especially true of Fröbenius. He considered himself to be a scholar whose duty it was to contribute to the knowledge of pure mathematics. Applied mathematics, in his opinion, belonged to the technical colleges.*"

The view of mathematics at the University of Göttingen was, however, very different. This was a time when there was competition between mathematians in the University of Berlin and in the University of Göttingen, but it was a competition that Göttingen won, for there mathematics flourished under Klein, much to Fröbenius's annoyance. Biermann wrote:

"*The aversion of Fröbenius to Klein and S. Lie knew no limits ...*"

Fröbenius hated the style of mathematics which Göttingen represented. It was a new approach which represented a marked change from the traditional style of German universities. Fröbenius, as we said above, had extremely traditional views. In a

letter to Hurwitz, who was a product of the Göttingen system, he wrote on 3 February 1896:

"*If you were emerging from a school, in which one amuses oneself more with rosy images than hard ideas, and if, to my joy, you are also gradually becoming emancipated from that, then old loves don't rust. Please take this joke facetiously.*"

One should put the other side of the picture, however, for Siegel, who knew Fröbenius for two years from 1915 when he became a student until Fröbenius's death, related his impression of Fröbenius as having a warm personality and expresses his appreciation of his fast-paced varied and deep lectures. Others would describe his lectures as solid but not stimulating.

To gain an impression of the quality of Fröbenius's work before the time of his appointment to Berlin in 1892 we can do no better than to examine the recommendations of Weierstrass and Fuchs when Fröbenius was elected to the Prussian Academy of Sciences in 1892. We quote a short extract to show the power, variety and high quality of Fröbenius's work in his Zürich years. Weierstrass and Fuchs listed 15 topics on which Fröbenius had made major contributions:

"*-On the development of analytic functions in series.*

-On the algebraic solution of equations, whose coefficients are rational functions of one variable.

-The theory of linear differential equations.

-On Pfaff's problem.

-Linear forms with integer coefficients.

-On linear substitutions and bilinear forms...

-On adjoint linear differential operators...

-The theory of elliptic and Jacobi functions...

-On the relations among the 28 double tangents to a plane of degree 4.

-On Sylow's theorem.

-On double cosets arising from two finite groups.

-On Jacobi's covariants...

-On Jacobi functions in three variables.

-The theory of biquadratic forms.

-On the theory of surfaces with a differential parameter."

In his work in group theory, Fröbenius combined results from the theory of algebraic equations, geometry, and number theory, which led him to the study of abstract groups. He published Über Gruppen von vertauschbaren Elementen in 1879 (jointly with Stickelberger, a colleague at Zürich) which looks at permutable elements in groups. This paper also gives a proof of the structure theorem for finitely generated abelian groups. In 1884 he published his next paper on finite groups in which he proved Sylow's theorems for abstract groups (Sylow had proved his theorem as a result about permutation groups in his original paper). The proof which Fröbenius gives is the one, based on conjugacy classes, still used today in most undergraduate courses.

In his next paper in 1887 Fröbenius continued his investigation of conjugacy classes in groups which would prove important in his later work on characters. In the introduction to this paper he explains how he became interested in abstract groups, and this was through a study of one of Kronecker's papers. It was in the year 1896,

however, when Fröbenius was professor at Berlin that his really important work on groups began to appear. In that year he published five papers on group theory and one of them Über die Gruppencharactere on group characters is of fundamental importance. He wrote in this paper:

"*I shall develop the concept [of character for arbitrary finite groups] here in the belief that through its introduction, group theory will be substantially enriched.*"

This paper on group characters was presented to the Berlin Academy on July 16 1896 and it contains work which Fröbenius had undertaken in the preceding few months. In a series of letters to Dedekind, the first on 12 April 1896, his ideas on group characters quickly developed. Ideas from a paper by Dedekind in 1885 made an important contribution and Fröbenius was able to construct a complete set of representations by complex numbers. It is worth noting, however, that although we think today of Fröbenius's paper on group characters as a fundamental work on representations of groups, Fröbenius in fact introduced group characters in this work without any reference to representations. In was not until the following year that representations of groups began to enter the picture, and again it was a concept due to Fröbenius. Hence 1897 is the year in which the representation theory of groups was born.

Over the years 1897-1899 Fröbenius published two papers on group representations, one on induced characters, and one on tensor product of characters. In 1898 he introduced the notion of induced representations and the Fröbenius Reciprocity Theorem. It was a burst of activity which set up the foundations of the whole of the machinery of representation theory.

In a letter to Dedekind on 26 April 1896 Fröbenius gave the irreducible characters for the alternating groups A_4, A_5, the symmetric groups S_4, S_5 and the group $PSL(2,7)$ of order 168. He completely determined the characters of symmetric groups in 1900 and of characters of alternating groups in 1901, publishing definitive papers on each. He continued his applications of character theory in papers of 1900 and 1901 which studied the structure of Fröbenius groups.

Only in 1897 did Fröbenius learn of Molien's work which he described in a letter to Dedekind as "very beautiful but difficult". He reformulated Molien's work in terms of matrices and then showed that his characters are the traces of the irreducible representations. This work was published in 1897. Fröbenius's character theory was used with great effect by Burnside and was beautifully written up in Burnside's 1911 edition of his Theory of Groups of Finite Order.

Fröbenius had a number of doctoral students who made important contributions to mathematics. These included Edmund Landau who was awarded his doctorate in 1899, Issai Schur who was awarded his doctorate in 1901, and Robert Remak who was awarded his doctorate in 1910. Fröbenius collaborated with Schur in representation theory of groups and character theory of groups. It is certainly to Fröbenius's credit that he so quickly spotted the genius of his student Schur. Fröbenius's representation theory for finite groups was later to find important applications in quantum mechanics and theoretical physics which may not have entirely pleased the man who had such "pure" views about mathematics.

Among the topics which Fröbenius studied towards the end of his career were positive and non-negative matrices. He introduced the concept of irreducibility for matri-

ces and the papers which he wrote containing this theory around 1910 remain today the fundamental results in the discipline. The fact so many of Fröbenius's papers read like present day text-books on the topics which he studied is a clear indication of the importance that his work, in many different areas, has had in shaping the mathematics which is studied today. Having said that, it is also true that he made fundamental contributions to fields which had already come into existence and he did not introduce any totally new mathematical areas as some of the greatest mathematicians have done.

Haubrich gave the following overview of Fröbenius's work:

"*The most striking aspect of his mathematical practice is his extraordinary skill at calculations. In fact, Fröbenius tried to solve mathematical problems to a large extent by means of a calculative, algebraic approach. Even his analytical work was guided by algebraic and linear algebraic methods. For Fröbenius, conceptual argumentation played a somewhat secondary role. Although he argued in a comparatively abstract setting, abstraction was not an end in itself. Its advantages to him seemed to lie primarily in the fact that it can lead to much greater clearness and precision.*"

Article by: J.J. O'Connor and E.F. Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/).

1.10. Problemas

1. Las siguientes condiciones sobre un grupo G son equivalentes:

   a) G es un grupo abeliano.

   b) La aplicación $\phi\colon G \to G$, $\phi(g) = g^{-1}$, es morfismo de grupos.

   c) La aplicación $\phi\colon G \to G$, $\phi(g) = g^2$, es morfismo de grupos.

   d) La aplicación $\phi\colon G \times G \to G$, $\phi(g, g') = gg'$, es morfismo de grupos.

2. Sea G un grupo. Si $a, g \in G$, se dice que aga^{-1} es el *conjugado* de g por a. La conjugación $\tau_a\colon G \to G$, $\tau_a(g) = aga^{-1}$ es un automorfismo de grupos (tales automorfismos de G reciben el nombre de *automorfismos internos*), y la aplicación $G \to \mathrm{Aut}(G)$, $a \mapsto \tau_a$, es un morfismo de grupos.

3. Sea H un subconjunto finito y no vacío de un grupo G. Pruébese que H es un subgrupo de G precisamente cuando $x \cdot y \in H$ para todo $x, y \in H$. ¿Sigue siendo cierto el enunciado cuando H no es finito?

4. Sea H un subconjunto no vacío de un grupo G. Pruébese que H es un subgrupo de G si y sólo si $xH = H$ para todo $x \in H$.

5. Determinar los siguientes subgrupos:

   a) El subgrupo de $\mathbb{Z}$ generado por $X = \{3, 5\}$.

   b) El subgrupo de $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ generado por $X := \{(2,0), (0,5)\}$ y el generado por $Y = \{(2,3), (4,5)\}$.

c) El subgrupo de S_3 generado por $X = \{(1,2),(1,3)\}$.

d) El subgrupo de $\mathbb{Q}$ generado por $X = \{1\}$, el generado por $Y = \{1/2\}$ y el generado por $Z = \{1/6, 1/8\}$.

6. Sea G un grupo de orden primo. Pruébese que G es un grupo cíclico.

7. Si los únicos subgrupos de un grupo G, no trivial, son el trivial, $\{1\}$ y G, pruébese que G es un grupo finito y su orden es primo.

8. Sean a, b elementos de un grupo G. Demuéstrese que $ord(a) = ord(bab^{-1})$. ¿Es cierto que siempre $ord(ab) = ord(ba)$?

9. Sea $\mu_n := \{z \in \mathbb{C} : z^n = 1\}$ el conjunto de las raíces n-esimas de la unidad. Pruébese que

a) μ_n es un subgrupo de $(\mathbb{C}^*, \cdot)$.

b) μ_n es un grupo isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

10. Sea G un grupo abeliano y $\pi : G \to G'$ un morfismo de grupos. Si $s : G' \to G$ es un morfismo de grupos tal que $\pi \circ s = \mathrm{Id}$ (es decir, "s es una sección de π"), pruébese que G es isomorfo a $\mathrm{Ker}\,\pi \times G'$.

11. Sea G' un grupo abeliano. Sea $i : G \to G'$ un morfismo de grupos. Si existe un morfismo de grupos $r : G' \to G$ tal que $r \circ i = \mathrm{Id}$ (es decir, "r es un retracto de i"), pruébese que G' es isomorfo a $G \times \mathrm{Ker}\, r$.

12. Probar que si G es un grupo cíclico finito de orden n, entonces para cada divisor d de n existe un único subgrupo $H \subseteq G$ de orden d.

CAPÍTULO 2
DOMINIOS DE FACTORIZACIÓN ÚNICA

2.1. Introducción

El anillo por excelencia es el anillo de los números enteros, $\mathbb{Z}$. Clásicamente la rama de las Matemáticas que estudia el anillo de los números enteros es la Aritmética, actualmente la Teoría de Números.

Hay otros anillos también muy importantes. Dado un conjunto con cierta estructura se puede considerar el anillo formado por las funciones del conjunto que respeten la estructura considerada en el conjunto. Por ejemplo, dado $\mathbb{R}^n$ podemos estudiar el anillo de las funciones continuas reales de $\mathbb{R}^n$, o el anillo de las funciones infinito diferenciables de $\mathbb{R}^n$, o el anillo $\mathbb{R}[x_1,\ldots,x_n]$ de las funciones algebraicas de $\mathbb{R}^n$. Así desde este punto de vista, la Topología es la rama de las Matemáticas que estudia los anillos de las funciones continuas reales de los espacios topológicos, la Geometría Diferencial es la rama de las Matemáticas que estudia los anillos de las funciones infinito diferenciables reales de las variedades diferenciables, la Geometría Algebraica es la rama de las Matemáticas que estudia los anillos de las funciones algebraicas de las variedades algebraicas.

En este capítulo vamos a estudiar los anillos euclídeos o más generalmente los anillos de factorización única, es decir, los anillos donde todo elemento se escribe de modo único como producto de elementos irreducibles. Se introducirán también herramientas básicas como el cociente de un anillo por un ideal y la localización de un anillo por un sistema multiplicativo.

2.2. Anillos. Cuerpos

Comencemos con una revisión rápida de la definición y propiedades elementales de los anillos.

1. Definición: Un anillo A es un conjunto dotado con dos operaciones

$$A\times A \xrightarrow{+} A,\ (a,a')\mapsto a+a', \quad A\times A\xrightarrow{\cdot} A,\ (a,a')\mapsto a\cdot a',$$

que denominamos suma y producto[1], tales que

[1] Será usual utilizar la notación $a\cdot a' = aa'$.

1. A es un grupo abeliano con respecto a la suma (luego tiene un elemento neutro, que se denota por 0, y cada $a \in A$ tiene un opuesto que se denota por $-a$).

2. La multiplicación es asociativa ($(a \cdot b) \cdot c = a \cdot (b \cdot c)$) y distributiva ($a \cdot (b + c) = a \cdot b + a \cdot c$).

   Además, sólo consideraremos anillos conmutativos con unidad, es decir, cumpliendo

3. $ab = ba$, para todo $a, b \in A$.

4. Existe un elemento $1 \in A$ tal que $a1 = 1a = a$, para todo $a \in A$.

A lo largo del libro entenderemos anillo por anillo conmutativo con unidad.

Observemos que $a \cdot 0 = 0$, porque $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Observemos también que $-1 \cdot a = -a$, porque $0 = 0 \cdot a = (1 + (-1)) \cdot a = a + (-1 \cdot a)$.

2. Ejemplos: 1. El anillo de los números enteros, $\mathbb{Z}$. El anillo de los números racionales $\mathbb{Q}$. El anillo de los números reales $\mathbb{R}$. El anillo de los números complejos, $\mathbb{C}$.

2. El anillo de funciones reales continuas, $C(X)$ de un espacio topológico X, con la suma y producto de funciones.

3. Los anillos de polinomios $\mathbb{C}[x_1, \ldots, x_n]$.

4. Dado $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, denotamos $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Sea A un anillo, se define el "anillo de series formales en las variables $x_1, \ldots, x_n$ con coeficientes en A", que denotamos $A[[x_1, \ldots, x_n]]$, como

$$A[[x_1, \ldots, x_n]] := \{ \sum_{\alpha \in \mathbb{N}^n} a_\alpha \cdot x^\alpha,\ a_\alpha \in A \},$$

donde dadas $s(x) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \cdot x^\alpha$, $t(x) = \sum_{\alpha \in \mathbb{N}^n} b_\alpha \cdot x^\alpha \in A[[x_1, \ldots, x_n]]$, se define

$$\begin{aligned} s(x) + t(x) &:= \sum_{\alpha \in \mathbb{N}^n} (a_\alpha + b_\alpha) \cdot x^\alpha \\ s(x) \cdot t(x) &:= \sum_{\alpha \in \mathbb{N}^n} \Big(\sum_{\beta + \beta' = \alpha} a_\beta \cdot b_{\beta'} \Big) \cdot x^\alpha \end{aligned}$$

3. Definición: Un elemento $a \in A$, diremos que es un divisor de cero, si existe $b \in A$, no nulo tal que $ab = 0$. Diremos que un anillo es íntegro si el único divisor de cero es el cero.

4. Ejemplos: $\mathbb{Z}$ es un anillo íntegro. Si A es un anillo íntegro entonces el anillo de polinomios con coeficientes en A, $A[x]$ es un anillo íntegro.

5. Definición: Diremos que un elemento de un anillo es invertible si tiene inverso (en el anillo con la multiplicación).

6. Definición: Diremos que un anillo es un cuerpo si todo elemento no nulo es invertible.

Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.

Los cuerpos son anillos íntegros: si $a \cdot b = 0$ y $0 \neq a$, entonces $0 = a^{-1} \cdot a \cdot b = b$.

2.2.1. Anillos euclídeos

7. Definición: Un anillo íntegro A se dice que es euclídeo si existe una aplicación $\delta\colon A\setminus\{0\}\to\mathbb{N}$, que cumple

1. $\delta(a)\leq\delta(ab)$, para todo $a,b\in A\setminus\{0\}$.
2. Para cada $a\in A$ y $b\in A$ no nulo, existen $c,r\in A$, de modo que $a=bc+r$, y r es nulo ó $\delta(r)<\delta(b)$.

8. Ejemplo: $\mathbb{Z}$ es un anillo euclídeo. Definimos $\delta\colon\mathbb{Z}\setminus\{0\}\to\mathbb{N}$, $\delta(n):=|n|$, donde $|n|=n$ si n es positivo y $|n|=-n$ si n es negativo. Por el teorema 1.3.6, es fácil comprobar que $(\mathbb{Z},\delta)$ es euclídeo.

9. Ejercicio: Sea (A,δ) un anillo euclídeo. Pruébese que $a\in A\setminus\{0\}$ es invertible si y sólo si $\delta(a)=\delta(1)$. Pruébese que si $a\in A\setminus\{0\}$ no es invertible entonces $\delta(a)>\delta(1)$. Sea $\delta'\colon A\setminus\{0\}\to\mathbb{N}$, $\delta'(a):=\delta(a)-\delta(1)$. Pruébese que (A,δ') es un anillo euclídeo y que $a\in A\setminus\{0\}$ es invertible si y sólo si $\delta'(a)=0$.

10. Definición: Diremos que el grado de $p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in A[x]$, con $a_n\neq 0$ es n y denotaremos $gr(p(x))=n$. Seguiremos la convención: $gr(0)=-\infty$.

11. Observación: Si A es un anillo íntegro, entonces el grado de polinomios es aditivo, es decir, se verifica la fórmula

$$gr(p(x)q(x))=gr(p(x))+gr(q(x))\ .$$

para cada par de polinomios $p(x),q(x)\in A[x]$. Por tanto, si $p(x)$ es múltiplo de $q(x)$, entonces $gr\,p(x)\geq gr\,q(x)$.

12. Algoritmo de división en el anillo de polinomios: *Sea $A=k$ un cuerpo. Para cada par de polinomios no nulos $p(x),q(x)\in k[x]$, existen otros dos, $c(x),r(x)$, que denominaremos* **cociente** *y* **resto** *de dividir $p(x)$ por $q(x)$, únicos con las condiciones:*

1. $p(x)=c(x)\cdot q(x)+r(x)$.
2. $gr(r(x))<gr(q(x))$.

Demostración. Existencia: Si $\mathrm{gr}\,q(x)>\mathrm{gr}\,p(x)$ entonces $c(x)=0$ y $r(x)=p(x)$. Supongamos $\mathrm{gr}\,q(x)=m\leq n=\mathrm{gr}\,p(x)$ y escribamos $p(x)=a_0x^n+\ldots+a_n$ y $q(x)=b_0x^m+\cdots+b_m$. Procedemos por inducción sobre $\mathrm{gr}\,p(x)$. Si $\mathrm{gr}\,p(x)=0$, entonces $\mathrm{gr}\,q(x)=0$ y $c(x)=\frac{a_0}{b_0}$ y $r(x)=0$. Sea, pues, $\mathrm{gr}(p(x))>0$. El polinomio $p'(x):=p(x)-\frac{a_0}{b_0}\cdot x^{n-m}\cdot q(x)$ es de grado menor que el de $p(x)$, luego por hipótesis de inducción, existen $c'(x)$ y $r'(x)$ tales que $p'(x)=c'(x)\cdot q(x)+r'(x)$ y $gr(r'(x))<gr(q(x))$. Entonces, $c(x):=c'(x)+\frac{a_0}{b_0}\cdot x^{n-m}$ y $r(x):=r'(x)$ cumplen lo exigido.

Unicidad: Al lector. □

13. Corolario: $(k[x],\mathrm{gr})$ *es un anillo euclídeo.*

14. Ejemplo: Sea $\mathbb{Z}[i]:=\{a+bi\in\mathbb{C}\colon a,b\in\mathbb{Z}\}$. $\mathbb{Z}[i]$ es un anillo (subanillo de $\mathbb{C}$) y se denomina el anillo de los enteros de Gauss. Veamos que es un anillo euclídeo. Consideremos la aplicación

$$\delta\colon\mathbb{Z}[i]\to\mathbb{N},\quad \delta(a+bi):=(a+bi)\cdot(a-bi)=a^2+b^2$$

Dados $z, z' \in \mathbb{Z}[i]$ no nulos se cumple que $\delta(zz') = \delta(z)\delta(z') \geq \delta(z)$. Dado un número complejo $a+bi \in \mathbb{C}$, denotemos $|a+bi| = a^2+b^2 \in \mathbb{R}$. Consideremos el número complejo $z/z' \in \mathbb{C}$ y consideremos un entero de Gauss $c \in \mathbb{Z}[i]$ lo más cercano posible a z/z'. Tenemos que $|z/z' - c| < 1$. Sea $r := z - z'c$, si $r \neq 0$ entonces

$$\delta(r) = \delta(z - z'c) = |z'(z/z' - c)| = |z'||z/z' - c| < |z'|$$

Tenemos, pues, que $z = z'c + r$ con $r = 0$ ó $\delta(r) < \delta(z')$. En conclusión, $(\mathbb{Z}[i], \delta)$ es un anillo euclídeo.

2.3. Ideales de un anillo

1. Definición: Un subconjunto $I \subseteq A$ diremos que es un ideal de A si es un subgrupo para la suma y cumple que $a \cdot i \in I$, para todo $a \in A$ y todo $i \in I$.

Dado $a \in A$, el conjunto $a \cdot A := \{a \cdot b \in A, \forall b \in A\}$ es un ideal de A. Si $I \subseteq \mathbb{Z}$ es un ideal, entonces existe un $n \in \mathbb{Z}$ tal que $I = n \cdot \mathbb{Z}$ (por el teorema 1.3.7).

La intersección de ideales es un ideal. Dado un subconjunto $F \subseteq A$, denotaremos por (F) al ideal mínimo de A que contiene a F (que es la intersección de todos los ideales que contienen a F). Explícitamente $(F) = \{a \in A : a = \sum_{i=0}^{n} a_i f_i$ con $f_i \in F, a_i \in A$ y $n \in \mathbb{N}$ cualesquiera$\}$. Dado $a \in A$, tenemos que $(a) = aA$. Dados dos ideales I_1 e I_2 de A, llamaremos suma de los dos ideales, que denotaremos por $I_1 + I_2$, al ideal de A definido por $I_1 + I_2 := \{i_1 + i_2 : i_1 \in I_1, i_2 \in I_2\}$, que es el mínimo ideal de A que contiene a I_1 y I_2.

2. Definición: Sea A un anillo. Diremos que un ideal $I \subset A$ es principal si está generado, como A-módulo, por algún elemento, i.e., $I = aA$. Diremos que un anillo es un dominio de ideales principales si es un anillo íntegro cuyos ideales son principales.

$\mathbb{Z}$ es un dominio de ideales principales.

3. Proposición: *Los anillos euclídeos son dominios de ideales principales.*

Demostración. Sea (A, δ) un anillo euclídeo. Sea $I \subset A$ un ideal no nulo. Sea $i \in I$ un elemento no nulo tal que $\delta(i) = \min\{\delta(j)\}_{j \in I \setminus \{0\}}$. Veamos que $I = i \cdot A$: Sea $j \in I$ no nulo y $c, r \in A$ de modo que $j = c \cdot i + r$ y $r = 0$ ó $\delta(r) < \delta(j)$. Observemos que $r \in I$, luego no es posible que $\delta(r) < \delta(j)$. En conclusión, $j = c \cdot i$. Por tanto, $I = i \cdot A$.

□

El ideal $\mathfrak{p} = (2, x_1)$ del anillo $\mathbb{Z}[x_1, \ldots x_n]$ no es principal: un generador de $\mathfrak{p}$ sería un divisor de 2 y éstos son ± 1 y ± 2, y $1 \cdot \mathbb{Z}[x_1, \ldots, x_n]$ y $2 \cdot \mathbb{Z}[x_1, \ldots, x_n]$ son ideales distintos de $\mathfrak{p}$. En consecuencia, los anillos $\mathbb{Z}[x_1, \ldots, x_n]$ no son dominios de ideales principales.

Análogamente, si k es un cuerpo, el ideal (x_1, x_2) del anillo $k[x_1, \ldots, x_n]$ no es principal, así que los anillos $k[x_1, \ldots, x_n]$ no son dominios de ideales principales (para $n > 1$).

2.4. Morfismo de anillos. Cociente por un ideal

1. Definición: Una aplicación $f : A \to B$ entre los anillos A y B, diremos que es un morfismo de anillos si cumple

1. $f(a+a') = f(a) + f(a')$, para todo $a, a' \in A$.
2. $f(aa') = f(a)f(a')$, para todo $a, a' \in A$.
3. $f(1) = 1$.

2. Ejemplos: La aplicación $\mathbb{C}[x] \to \mathbb{C}$, $p(x) \mapsto p(33)$, es un morfismo de anillos. Dada una aplicación continua $\phi\colon X \to Y$ entre espacios topológicos, la aplicación $\tilde{\phi}\colon C(Y) \to C(X)$, $f \mapsto f \circ \phi$ es un morfismo de anillos.

La composición de morfismos de anillos es un morfismo de anillos. La imagen de un morfismo de anillos $f\colon A \to B$, $\operatorname{Im} f$, es un subanillo de B, es decir, un subconjunto de B que con las operaciones de B es anillo y $1 \in B$.

El núcleo de un morfismo de anillos f, $\operatorname{Ker} f := \{a \in A\colon f(a) = 0\}$, es un ideal. La antimagen por un morfismo de anillos de un ideal es un ideal. Si un morfismo de anillos es epiyectivo la imagen de un ideal es un ideal.

Sea $I \subseteq A$ un ideal. Como I es un subgrupo (aditivo) de A, podemos considerar el grupo cociente A/I, donde

$$A/I := \{\bar{a},\ a \in A,\ \text{de modo que } \bar{a} = \bar{a'} \iff a - a' \in I\}.$$

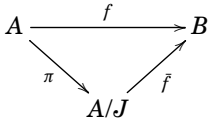
Podemos definir en A/I la operación "producto", $\bar{a} \cdot \bar{a'} := \overline{a \cdot a'}$, que dota a A/I de estructura de anillo (compruébese), y es la única estructura de anillo que podemos definir en A/I, de modo que el morfismo de paso al cociente $\pi\colon A \to A/I$, $a \mapsto \bar{a}$, sea un morfismo de anillos.

3. Ejemplo: Consideremos el ideal $9\cdot\mathbb{Z} \subseteq \mathbb{Z}$. En $\mathbb{Z}/9\cdot\mathbb{Z}$ tenemos que $\overline{10^n} = \overline{10}^n = \bar{1}^n = \bar{1}$. Por tanto, dado un número natural cualquiera, por ejemplo $7836 \in \mathbb{N}$, tenemos que

$$\overline{7836} = \overline{7\cdot 10^3 + 8\cdot 10^2 + 3\cdot 10 + 6} = \bar{7}\cdot\overline{10^3} + \bar{8}\cdot\overline{10^2} + \bar{3}\cdot\overline{10} + \bar{6} = \bar{7} + \bar{8} + \bar{3} + \bar{6} = \overline{7+8+3+6}$$

En general, un número natural $n = n_1 n_2 \dots n_r$, escrito en base decimal, es divisible por nueve si y sólo si la suma de sus cifras, $n_1 + \cdots + n_r$ es divisible por nueve.

Sea $f\colon A \to B$ un morfismo de anillos. Si $J \subseteq A$ es un ideal incluido en $\operatorname{Ker} f$, entonces existe un único morfismo de anillos $\bar{f}\colon A/J \to B$ (definido por $\bar{f}(\bar{a}) = f(a)$) de modo que el diagrama



es conmutativo, siendo π el morfismo de paso al cociente, $\pi(a) = \bar{a}$. Como consecuencia del teorema de isomorfía para morfismos de grupos obtenemos el siguiente teorema.

4. Teorema de isomorfía: *Sea $f\colon A \to B$ un morfismo de anillos. La aplicación*

$$\bar{f}\colon A/\operatorname{Ker} f \to \operatorname{Im} f,\ \bar{f}(\bar{a}) := f(a)$$

es un isomorfismo de anillos.

5. Ejemplo: El cuerpo de los números complejos es isomorfo a $\mathbb{R}[x]/(x^2+1)$: Consideremos el morfismo de anillos $f:\mathbb{R}[x]\to\mathbb{C}$, $f(p(x)):=p(i)$. El morfismo f es epiyectivo. Sea $\operatorname{Ker} f=(p(x))$. Obviamente, $x^2+1\in\operatorname{Ker} f$, luego $p(x)$ ha de dividir a x^2+1. Como no existe ningún polinomio de grado 1 en $\operatorname{Ker} f$, concluimos que $\operatorname{Ker} f=(x^2+1)$ y por el teorema de isomorfía $\mathbb{R}[x]/(x^2+1)\simeq\mathbb{C}$.

6. Ejemplo: Sea K un cuerpo, $k\subseteq K$ un subcuerpo, y sea $\alpha\in K$. Se denota $k[\alpha]:=\{p(\alpha)\in K:\ \text{para todo } p(x)\in k[x]\}$. Consideremos el morfismo $\phi:k[x]\to K$, $\phi(p(x)):=p(\alpha)$. Se cumple que ϕ es un morfismo de anillos y $\operatorname{Im}\phi=k[\alpha]$. $\operatorname{Ker}\phi$ es un ideal de $k[x]$. Si $\operatorname{Ker}\phi\neq\{0\}$, entonces está generado por el polinomio $p(x)$ no nulo mónico de grado más pequeño tal que $p(\alpha)=0$. Por tanto, por el teorema de isomorfía

$$k[\alpha]=\begin{cases} k[x], & \text{si no existe ningún polinomio no nulo } p(x) \text{ tal que } p(\alpha)=0\\ k[x]/(p(x)), & \text{donde } p(x)\in k[x] \text{ es el pol. no nulo mónico mín. anulador de } \alpha\end{cases}$$

Observemos que el polinomio mínimo anulador de α, $p(x)$, es irreducible (es decir, no es producto de dos polinomios de grado menor que el de $p(x)$), porque si no lo es entonces $p(x)=p_1(x)\cdot p_2(x)$, con $\operatorname{gr}(p_1(x)),\operatorname{gr}(p_2(x))<\operatorname{gr}(p(x))$ y $p_1(x)$ ó $p_2(x)$ anula a α. Recíprocamente, si $p(x)$ es mónico, anula a α y es irreducible, entonces es el polinomio mónico mínimo anulador de α.

$k[x]/(p(x))$ es un k-espacio vectorial de base $\{\bar1,\bar x,\cdots,\bar x^{n-1}\}$, con $n=\operatorname{gr}(p(x))$:En efecto dado $\overline{q(x)}\in k[x]/(p(x))$, como $q(x)=c(x)\cdot p(x)+r(x)$, con $\operatorname{gr}(r(x))<n$, tenemos que $\overline{q(x)}=\overline{r(x)}$. Como $r(x)$ es combinación lineal de $1,\cdots,x^{n-1}$, $\{\bar1,\bar x,\cdots,\bar x^{n-1}\}$ es un sistema generador. Veamos que $\bar1,\bar x,\cdots,\bar x^{n-1}$ son linealmente independientes. Si

$$0=\sum_{i=0}^{n-1}\lambda_i\bar x^i=\overline{\sum_{i=0}^{n-1}\lambda_i x^i}.$$

Entonces, $\sum_{i=0}^{n-1}\lambda_i x^i$ es múltiplo de $p(x)$, lo cual es imposible, salvo que $\sum_{i=0}^{n-1}\lambda_i x^i=0$, es decir, $\lambda_i=0$ para todo i.

Consideremos la inclusión $\mathbb{Q}\subset\mathbb{C}$ y $\sqrt[3]{2}\in\mathbb{C}$. El polinomio con coeficientes racionales mínimo anulador de $\sqrt[3]{2}$ es x^3-2, porque es irreducible ya que si no lo es x^3-2 tendría raíces en $\mathbb{Q}$, que es imposible. Por tanto,

$$\mathbb{Q}[x]/(x^3-2)=\mathbb{Q}[\sqrt[3]{2}].$$

Por tanto, $\mathbb{Q}[\sqrt[3]{2}]$ es un $\mathbb{Q}$-espacio vectorial de dimensión 3, de base $\{1,\sqrt[3]{2},\sqrt[3]{2}^2\}$.

7. Teorema chino de los restos: *Sea A un anillo e $I_1,I_2\subseteq A$ dos ideales tales que $I_1+I_2=A$. Entonces, el morfismo natural*

$$A/(I_1\cap I_2)\to A/I_1\times A/I_2,\quad \bar a\mapsto(\bar a,\bar a)$$

es un isomorfismo

Demostración. El núcleo del morfismo $f:A\to A/I_1\times A/I_2$, $f(a)=(\bar a,\bar a)$ es claramente $I_1\cap I_2$. Por el teorema de isomorfía, sólo nos falta probar que es epiyectivo. Sea $(\bar a,\bar b)\in A/I_1\times A/I_2$. Observemos que en A/I_2, $A/I_2=\overline{a+I_1+I_2}=\overline{a+I_1}$. Por tanto, existe $i_1\in I_1$ de modo que $\overline{a+i_1}=\bar b$ en A/I_2. Por tanto, $f(a+i_1)=(\overline{a+i_1},\overline{a+i_1})=(\bar a,\bar b)$. □

ÍNDICE

2.5. Ideales primos. Ideales maximales

1. Definición: Un ideal $\mathfrak{p} \underset{\neq}{\subset} A$, diremos que es un ideal primo de A, si cumple que si $ab \in \mathfrak{p}$ entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

2. Proposición: *Un ideal $\mathfrak{p} \underset{\neq}{\subset} A$ es un ideal primo si y sólo si $A/\mathfrak{p}$ es un anillo íntegro.*

Demostración. Supongamos que $\mathfrak{p} \subset A$ es un ideal primo. Si $\bar{a} \cdot \bar{a'} = 0$ en $A/\mathfrak{p}$ entonces $\overline{a \cdot a'} = 0$, luego $a \cdot a' \in \mathfrak{p}$. Por tanto, o $a \in \mathfrak{p}$ o $a' \in \mathfrak{p}$, luego o $\bar{a} = 0$ o $\bar{a'} = 0$. En conclusión $A/\mathfrak{p}$ es íntegro.

Recíprocamente, supongamos que $A/\mathfrak{p}$ es íntegro. Si $a \cdot a' \in \mathfrak{p}$, entonces $\overline{a \cdot a'} = 0$ en $A/\mathfrak{p}$. Por tanto, $\bar{a} \cdot \bar{a'} = 0$, luego o $\bar{a} = 0$ o $\bar{a'} = 0$. Es decir, o $a \in \mathfrak{p}$ o $a' \in \mathfrak{p}$. En conclusión, $\mathfrak{p}$ es un ideal primo. □

3. Definición: Diremos que un ideal $\mathfrak{m} \underset{\neq}{\subset} A$ es maximal si los únicos ideales que contienen a $\mathfrak{m}$ son $\mathfrak{m}$ y A.

4. Proposición: *En todo anillo $A \neq 0$ existen ideales maximales.*

Demostración. La demostración es una aplicación típica del lema de Zorn (que puede evitarse en anillos noetherianos). Sea X el conjunto de los ideales de A, distintos de A. En X podemos definir una relación de orden: decimos que un ideal I es menor o igual que otro I' cuando $I \subseteq I'$. Observemos que toda cadena de ideales, distintos de A tiene una cota superior: la unión de los ideales de la cadena (que es distinto de A, pues el 1 no está en ninguno de ellos, ni por tanto en la unión). El lema de Zorn nos dice que existen elementos de X maximales, es decir, existen ideales maximales. □

5. Definición: Se dice que un ideal primo es minimal si no contiene estrictamente ningún ideal primo.

6. Ejercicio: En todo anillo $A \neq 0$ existen ideales primos minimales.

7. Corolario: *Todo ideal $I \underset{\neq}{\subset} A$ está incluido en un ideal maximal.*

Demostración. Sea $\pi : A \to A/I$ el morfismo de paso al cociente. En la correspondencia biunívoca

$$\left\{\begin{matrix}\text{Ideales de } A \\ \text{que contienen a } I\end{matrix}\right\} = \{\text{Ideales de } A/I\}$$

$$J \longmapsto \pi(J)$$

$$\pi^{-1}(J') \longmapsfrom J'$$

los ideales maximales de A que contienen a I se corresponden con los ideales maximales de A/I, que no es vacío por la proposición anterior. □

Un elemento $a \in A$ es invertible si y sólo si $(a) = A$ (suponemos $A \neq 0$). Por tanto, $a \in A$ es invertible si y sólo si no está incluido en ningún ideal maximal. En particular, un anillo es un cuerpo si y sólo si los únicos ideales del anillo son el (0) y todo el anillo.

8. Proposición: *Un ideal $\mathfrak{m} \subsetneq A$ es maximal si y sólo si $A/\mathfrak{m}$ es un cuerpo. En particular, los ideales maximales son ideales primos, por la proposición 2.5.2.*

Demostración. $A/\mathfrak{m}$ es cuerpo si y sólo si el único ideal maximal es el (0). Que equivale a decir que el único ideal maximal que contiene a $\mathfrak{m}$ es $\mathfrak{m}$, es decir, que $\mathfrak{m}$ es maximal. □

9. Definición: Los elementos de un anillo íntegro que no son nulos ni invertibles se los denomina elementos propios del anillo.

10. Definición: Un elemento propio de un anillo íntegro se dice que es irreducible si no descompone en producto de dos elementos propios. Se dice que dos elementos propios son primos entre sí, si carecen de divisores propios comunes.

11. Notación: Los elementos irreducibles positivos de $\mathbb{Z}$ se denominan números primos. Los elementos irreducibles positivos de $k[x]$ se denominan polinomios irreducibles.

12. Proposición: *Sea A un anillo íntegro y $a \in A$ no nulo. Si (a) es un ideal primo, entonces a es un elemento irreducible de A.*

Demostración. Si $a = b \cdot c$, con b y c elementos propios de A, entonces $b \in (a)$ (o $c \in (a)$) porque a) es un ideal primo. Luego, $b = ad$ para cierto $d \in A$. Por tanto, $a = bc = adc$ y $dc = 1$. Es decir, c es invertible y hemos llegado a contradicción. □

13. Proposición: *Sea p un elemento no nulo de un dominio de ideales principales A. Las siguientes condiciones son equivalentes:*

1. *p es irreducible en A.*
2. *pA es un ideal primo de A.*
3. *pA es un ideal maximal de A.*

Demostración. 3. $\Rightarrow$ 2. Obvio.

2. $\Rightarrow$ 1. Es consecuencia de 2.5.12.

1. $\Rightarrow$ 3. Sea $I = aA$ un ideal cualquiera. Si $pA \subseteq I = aA$, entonces existe $b \in A$ tal que $ab = p$. Luego, a es invertible y $I = A$, o b es invertible y $I = pA$. En conclusión, pA es maximal.

□

2.6. Dominios de factorización única

1. Definición: Se dice que un anillo A es noetheriano si todo ideal es finito generado.

Evidentemente los dominios de ideales principales son anillos noetherianos. Por tanto, los anillos euclídeos son noetherianos.

2. Ejemplo: El teorema de la base de Hilbert afirma que los anillos de polinomios $k[x_1, \ldots, x_n]$ son noetherianos.

3. Proposición: *Un anillo A es noetheriano si y sólo si toda cadena creciente de ideales de A, $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ estabiliza, es decir, para $n >> 0$, $I_n = I_m$, para todo $m \geq n$.*

Demostración. Si A es noetheriano e $I_1 \subseteq I_2 \subset \cdots \subset I_n \subseteq \cdots$ una cadena creciente de ideales de A, consideremos el ideal $J := \cup_i I_i = (a_1, \ldots, a_r)$. Para $n >> 0$, $a_1, \ldots, a_r \in I_n$, luego $I_n \subseteq J \subseteq I_n$, es decir, $J = I_n$ y $I_n = I_m$, para todo $m \geq n$.

Veamos el recíproco. Sea I un ideal, si $I \neq 0$ sea $0 \neq a_1 \in I$ y $I_1 := (a_1)$, Si $I_1 \neq I$, sea $a_2 \in I \setminus I_1$ e $I_2 := (a_1, a_2)$. Así sucesivamente vamos construyendo una cadena $0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ que por la propiedad exigida a A ha de ser finita. Luego, para $n >> 0$, $I = I_n = (a_1, \ldots, a_n)$.

□

4. Lema: *Sea A un anillo íntegro y $a, b \in A$. Entonces, $(a) = (b)$ si y sólo si $a = b \cdot i$ para cierto invertible $i \in A$.*

Demostración. $\Rightarrow$) Si $(a) = (b)$ existen $i, i' \in A$ tales que $a = bi$ y $b = ai'$. Por tanto, $a = ai'i$. Como A es íntegro, $1 = ii'$, luego i es invertible.

□

5. Teorema de descomposición en factores irreducibles: *Todo elemento propio $a \in A$, de un anillo noetheriano íntegro, descompone en producto de factores irreducibles $a = p_1 \cdots p_n$.*

Demostración. Empecemos probando que a todo elemento $a \in A$ lo divide algún elemento irreducible: Si a no es irreducible entonces $a = a_1 \cdot b_1$, a_1, b_1 elementos propios. Si a_1 no es irreducible, entonces $a_1 = a_2 \cdot b_2$, con a_2, b_2 elementos propios. Así sucesivamente, vamos obteniendo una cadena $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$ que ha de ser finita por noetherianidad y terminará cuando a_n sea irreducible.

Ahora ya, sea a_1 irreducible que divide a a y escribamos $a = a_1 \cdot b_1$. Si b_1 no es irreducible sea a_2 irreducible, que divide a b_1 y escribamos $a = a_1 \cdot b_1 = a_1 \cdot a_2 \cdot b_2$. Así sucesivamente, vamos obteniendo la cadena $(a) \subsetneq (b_1) \subsetneq (b_2) \subsetneq \ldots$ que ha de ser finita y terminará cuando b_n sea irreducible. En tal caso $a = a_1 \cdots a_{n-1} \cdot b_n$ es producto de irreducibles. □

6. Definición: Un anillo íntegro se dice que es un dominio de factorización única si todo elemento propio (no nulo ni invertible) del anillo es producto de elementos irreducibles, de modo único salvo orden y factores invertibles. DFU significará dominio de factorización única.

7. Teorema de descomposición única en factores irreducibles: *Sea A un anillo noetheriano íntegro. Entonces, A es un dominio de factorización única si y sólo si para todo elemento irreducible $a \in A$ se cumple que (a) es un ideal primo.*

Demostración. $\Leftarrow$) Si $b \cdot c \in (a)$, entonces existe $d \in A$ tal que $bc = ad$. Sea $b = b_1 \cdots b_r$, $c = c_1 \cdots c_s$ y $d = d_1 \cdots d_t$ las descomposiciones en factores irreducibles de b, c, d. Entonces,

$$b_1 \cdots b_r \cdot c_1 \cdots c_s = a \cdot d_1 \cdots d_t.$$

Como A es un dominio de factorización única, a ha de coincidir, salvo multiplicación por un invertible, con algún b_i o algún c_j. Luego, a divide a b, es decir. $b \in (a)$; o a divide a c, es decir, $c \in (a)$. En conclusión, (a) es un ideal primo.

$\Rightarrow$) Sean $p_1 \cdots p_n = q_1 \cdots q_m$ dos descomposiciones en factores irreducibles. Entonces, q_1 divide algún factor p_i, luego coincide con él (salvo multiplicación por un invertible). Pongamos $p_1 = q_1$ (salvo invertibles). Simplificando la igualdad original tenemos $p_2 \cdots p_n = q_2 \cdots q_m$ (salvo multiplicación por un invertible). Razonando con q_2 como hemos hecho antes con q_1 llegamos a que q_2 coincide con algún p_i. Reiterando el argumento, obtendremos que las dos descomposiciones son iguales (salvo orden y factores invertibles).

□

8. Teorema: *Los dominios de ideales principales son dominios de factorización única. En particular, los anillos euclídeos son dominos de factorización única.*

Demostración. Es consecuencia inmediata de la proposición 2.5.13 y el teorema 2.6.7.
□

Sea A un dominio de factorización única, $a, b \in A$ y escribamos $a = u \cdot p_1^{n_1} \cdots p_r^{n_r}$, $b = v \cdot p_1^{m_1} \cdots p_r^{m_r}$, con u, v invertibles, $n_i, m_i \geq 0$ y $p_1, \ldots, p_r$ irreducibles y primos entre sí. Definimos (salvo multiplicación por invertibles) el máximo común divisor de a y b, que denotaremos $m.c.d.(a,b)$ y el mínimo común múltiplo de a y b, que denotaremos $m.c.m.(a,b)$ como sigue:

$$m.c.d.(a,b) = p_1^{\text{mín}(n_1,m_1)} \cdots p_r^{\text{mín}(n_r,m_r)}$$
$$m.c.m.(a,b) = p_1^{\text{máx}(n_1,m_1)} \cdots p_r^{\text{máx}(n_r,m_r)}$$

Observemos que si m divide a a y b, entonces m divide a $m.c.d.(a,b)$; y si m es múltiplo de a y b, entonces m es múltiplo de $m.c.m.(a,b)$.

Si A es un dominio de ideales principales y $a, b \in A$, entonces $aA + bA = dA$, siendo d "el máximo común divisor de a y b": Si c divide á a y b entonces divide á d y obviamente d divide á a y b.

Igualmente, el mínimo común múltiplo de a y b es el generador del ideal $aA \cap bA$. Por tanto, el máximo común divisor y el mínimo común múltiplo de dos elementos de un dominio de ideales principales A siempre existen y están bien definidos salvo factores invertibles.

9. Identidad de Bézout: *Sea A un dominio de ideales principales y sean $a, b \in A$. Sea d el máximo común divisor de a y b. Existen elementos $\alpha, \beta \in A$ tales que*

$$d = \alpha a + \beta b.$$

10. Algoritmo de Euclides Este algoritmo nos permite calcular en anillos euclídeos el máximo común divisor de dos elementos del anillo: Dados $a_1, a_2 \in A$ definimos por recurrencia a_{i+1} el resto de dividir a_{i-1} por a_i. Entonces, escribimos

$$\begin{aligned} a_1 &= a_2 c_1 + a_3 \\ a_2 &= a_3 c_2 + a_4 \\ a_3 &= a_4 c_3 + a_5 \\ &\cdots \\ a_{s-2} &= a_{s-1} c_{s-2} + a_s \end{aligned}$$

y terminamos cuando s sea el primero tal que $a_s = 0$.

Observemos que d divide á a_1 y a_2 si y sólo si divide a a_2 y a_3, si y sólo si ... divide a a_{s-2} y a_{s-1}, si y sólo si divide a a_{s-1}. Luego, $m.c.d(a_1,a_2) = a_{s-1}$ (único salvo multiplicación por invertibles).

Además, el algoritmo de Euclides nos permite calcular λ, μ tales que $\lambda \cdot a_1 + \mu \cdot a_2 = m.c.d(a_1,a_2)$: Sabemos expresar a_3 como combinación A-lineal de a_1 y a_2, luego sabemos expresar a_4 como combinación lineal de a_1 y a_2, y así sucesivamente sabremos expresar a_{s-1} como combinación lineal de a_1 y a_2.

11. Dados dos números enteros $n, m \in \mathbb{Z}$, primos entre sí (luego $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ y $n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$), por el teorema chino de los restos se tiene el isomorfismo

$$\mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},\ \bar{r} \mapsto (\bar{r},\bar{r})$$

Calculemos el morfismo inverso: Sabemos calcular $\lambda, \mu \in \mathbb{Z}$ de modo que $\lambda \cdot n + \mu \cdot m = 1$. Luego, $\lambda \cdot n \mapsto (\bar{0},\bar{1})$ y $\mu \cdot m \mapsto (\bar{1},\bar{0})$. Luego, el morfismo $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/nm\mathbb{Z}$, $(\bar{r},\bar{s}) \mapsto \overline{r \cdot \mu \cdot m + s \cdot \lambda \cdot n}$ es el morfismo inverso buscado.

12. Calculemos las soluciones enteras de la siguiente ecuación diofántica (es decir, ecuación con coeficientes enteros),

$$2000x - 266y = -4.$$

Primero calculemos mediante el algoritmo de Euclides, $n, m \in \mathbb{Z}$, tales que

$$2000n + 266 \cdot (-m) = m.c.d(2000,266).$$

a. $2000 = 7 \cdot 266 + 138$. b. $266 = 1 \cdot 138 + 128$. c. $138 = 1 \cdot 128 + 10$. d. $128 = 12 \cdot 10 + 8$ e. $10 = 1 \cdot 8 + 2$. Luego, $m.c.d(2000,266) = 2$. Lo cual era evidente, pero ahora sabremos calcular n y m: $2 = 10 - 1 \cdot 8 = 10 - 1 \cdot (128 - 12 \cdot 10) = -128 + 13 \cdot 10 = -128 + 13(138 - 128) = 13 \cdot 138 - 14 \cdot 128 = 13 \cdot 138 - 14(266 - 138) = -14 \cdot 266 + 27 \cdot 138 = -14 \cdot 266 + 27(2000 - 7 \cdot 266) = 27 \cdot 2000 - 203 \cdot 266$.

Por tanto, una solución particular de nuestro sistema de ecuaciones diofánticas es $x_0 = -2 \cdot 27 = -54$, $y_0 = -2 \cdot 203 = -406$. Las soluciones de la ecuación homogénea $2000x - 266y = 0$ son las soluciones de $1000x - 133y = 0$, que son $x = n \cdot 133$, $y = n \cdot 1000$. Todas las soluciones de nuestro sistema de ecuaciones diofánticas son

$$\begin{cases} x = -54 + n \cdot 133 \\ y = -406 + n \cdot 1000 \end{cases}$$

2.7. Congruencias de Fermat, Euler y Wilson

1. Proposición: *El elemento $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es un generador de este grupo si y sólo m es primo con n.*

Demostración. Consideremos el epimorfismo natural $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\pi(z) = \bar{z}$. Es claro que $\pi^{-1}(\langle\bar{m}\rangle) = m\mathbb{Z} + n\mathbb{Z} = r\mathbb{Z}$, donde r es el máximo común divisor de m y n. Por otra parte, $\bar{m}$ es un generador de $\mathbb{Z}/n\mathbb{Z}$, es decir, $\langle\bar{m}\rangle = \mathbb{Z}/n\mathbb{Z}$, si y sólo $\pi^{-1}(\langle\bar{m}\rangle) = \mathbb{Z}$. Por tanto, $\bar{m}$ es un generador de $\mathbb{Z}/n\mathbb{Z}$ si y sólo si $r = 1$. □

Así pues, si $G = \langle g \rangle$ es un grupo cíclico de orden $n > 0$, entonces g^m es un generador de G si y sólo si m y n son primos entre sí.

2. Notación: Dado un anillo A, denotaremos A^* al grupo (con la multiplicación) formado por los elementos invertibles de A.

3. Proposición: *$\bar{m} \in (\mathbb{Z}/n\mathbb{Z})^*$ si y sólo si m es primo con n.*

Demostración. Un elemento $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ genera el grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ si y sólo si $\mathbb{Z} \cdot \bar{m} = \mathbb{Z}/n\mathbb{Z}$, y para esto es necesario y suficiente que exista m' tal que $m' \cdot \bar{m} = \bar{1}$, o equivalentemente, $\bar{m'} \cdot \bar{m} = \bar{1}$. Es decir, $\bar{m}$ genera el grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ si y sólo si $\bar{m}$ es un invertible de $\mathbb{Z}/n\mathbb{Z}$ con el producto. Por 2.7.1, $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ es invertible si y sólo si m es primo con n.

□

4. Definición: Sea $\phi\colon \mathbb{N} \to \mathbb{N}$ la aplicación definida por

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

A la aplicación ϕ la denominaremos operador de Euler.

Es decir, $\phi(n) = |$Conjunto de los números naturales inferiores a n y primos con él$|$.

5. Proposición: *Si n, m son números primos entre sí, entonces*

$$\phi(nm) = \phi(n)\phi(m).$$

Demostración. Por el teorema chino de los restos tenemos el isomorfismo de anillos $\mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Tomando los invertibles de los anillos

$$\boxed{(\mathbb{Z}/nm\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*}$$

luego $\phi(nm) = |(\mathbb{Z}/nm\mathbb{Z})^*| = |(\mathbb{Z}/n\mathbb{Z})^*| \cdot |(\mathbb{Z}/m\mathbb{Z})^*| = \phi(n)\phi(m)$. □

6. Proposición: *Si p es un número primo, entonces:*

$$\phi(p^n) = p^{n-1}(p-1).$$

Demostración. Un número r es primo con p^n si y sólo si es primo con p. Obviamente $1 \cdot p, 2 \cdot p, \ldots, p^{n-1} \cdot p$ son los números naturales m, con $0 < m \leq p^n$, que no son primos con p^n. Luego, $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. □

A partir de estas proposiciones se obtiene inmediatamente el siguiente:

7. Teorema: *Si $n = p_1^{n_1} \cdots p_r^{n_r}$ es la descomposición de n en producto de potencias de números primos, entonces:*

$$\phi(n) = p_1^{n_1-1} \cdots p_r^{n_r-1}(p_1 - 1) \cdots (p_r - 1)$$

8. Notación: Escribiremos $m \equiv m' \, mod \, n$ y leeremos m es congruente con m' módulo n, cuando $\bar{m} = \bar{m'}$ en $\mathbb{Z}/n\mathbb{Z}$ (es decir, el resto de dividir m por n coincide con el resto de dividir m' por n).

9. Congruencia de Euler: *Si n, m son naturales primos entre sí, se verifica la fórmula:*

$$m^{\phi(n)} \equiv 1 \, mod \, n.$$

Demostración. Es consecuencia de 1.6.4, aplicado al caso $G = (\mathbb{Z}/n\mathbb{Z})^*$ y $g = \bar{m}$. □

Si n es primo, la congruencia de Euler nos dice en particular:

10. Congruencia de Fermat: *Si p es primo y $m \not\equiv 0 \, mod \, p$, se entonces verifica la fórmula:*

$$m^{p-1} \equiv 1 \, mod \, p.$$

Si $p \in \mathbb{Z}$ es un número primo entonces $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, porque $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$ por la proposición 2.5.13

11. Congruencia de Wilson: *Si p es un número primo, entonces:*

$$(p-1)! \equiv -1 \, mod \, p.$$

Demostración. $(p-1)! \, mod \, p$ es el producto de todos los elementos del grupo $(\mathbb{Z}/p\mathbb{Z})^*$. Si $\bar{m} \in (\mathbb{Z}/p\mathbb{Z})^*$ no es igual a su inverso, entonces en este producto ambos se cancelan (dando 1) luego en el producto mencionado sólo permanecen aquellos $\bar{m}$ que verifiquen que son igual a su inverso. Ahora bien, $1 = \bar{m} \cdot \bar{m} = \bar{m}^2$ en $\mathbb{Z}/p\mathbb{Z}$ si y sólo si $\bar{m}$ es raíz del polinomio $x^2 - \bar{1} \in \mathbb{Z}/p\mathbb{Z}[x]$. Como las raíces de $x^2 - \bar{1} = (x+\bar{1}) \cdot (x-\bar{1})$. Es decir, $\bar{m}$ es igual a su inverso si y sólo si $\bar{m} = \pm\bar{1}$. Por tanto, $(p-1)! = 1 \cdot (-1) = -1$ en $\mathbb{Z}/p\mathbb{Z}$. □

2.8. $K[x_1, \ldots, x_n]$ es DFU

2.8.1. Localización

1. Definición: Sea A un anillo y $S \subseteq A$ un subconjunto. Diremos que S es un sistema multiplicativo de A si cumple

1. $1 \in S$.
2. Si $s, s' \in S$ entonces $s \cdot s' \in S$.

2. Ejemplo: $\mathbb{Z} \setminus \{0\}$ es un sistema multiplicativo de $\mathbb{Z}$.

3. Definición: Sea A un anillo y $S \subset A$ un sistema multiplicativo de A. La localización de A por S, A_S, es el conjunto

$$A_S := \left\{ \frac{a}{s},\ a \in A \text{ y } s \in S \colon \frac{a}{s} = \frac{a'}{s'} \text{ si existen } s_1, s_2 \in S \text{ tales que las fracciones } \frac{s_1 a}{s_1 s}, \frac{s_2 a'}{s_2 s'} \text{ tienen el mismo numerador y denominador} \right\}^{2}$$

Observemos que $\frac{a}{s} = \frac{s_1 a}{s_1 s}$, para todo $s_1 \in S$.

Sea B un conjunto. Dar una aplicación $\phi \colon A_S \to B$, es asignar a cada $\frac{a}{s} \in A_S$ un elemento $\varphi(a,s) \in B$ de modo que $\varphi(ta, ts) = \varphi(a,s)$ para todo $t \in S$.

[2] Observemos que $\frac{a}{s} = \frac{a}{s}$, que si $\frac{a}{s} = \frac{a'}{s'}$ entonces $\frac{a'}{s'} = \frac{a}{s}$, y que si $\frac{a}{s} = \frac{a'}{s'}$ y $\frac{a'}{s'} = \frac{a''}{s''}$ entonces $\frac{a}{s} = \frac{a''}{s''}$.

Con la suma y producto ordinarios de fracciones

$$\frac{a}{s}+\frac{a'}{s'}:=\frac{s'a+sa'}{ss'}$$
$$\frac{a}{s}\cdot\frac{a'}{s'}:=\frac{aa'}{ss'}$$

A_S es un anillo. El elemento unidad de A_S es la fracción $\frac{1}{1}$. Si $s\in S$ entonces la fracción $\frac{s}{1}$ es invertible, de inverso $\frac{1}{s}$. La fracción $\frac{0}{s}=\frac{0\cdot s}{1\cdot s}=\frac{0}{1}$ es el elemento nulo de A_S.

4. Definición: Si A es un anillo íntegro, obviamente $A_{A\setminus\{0\}}$ es un cuerpo y diremos que es el cuerpo de fracciones de A.

5. Ejemplos: 1. $\mathbb{Q}=\mathbb{Z}_{\mathbb{Z}\setminus\{0\}}$,

2. $\mathbb{Q}(x):=\mathbb{Q}[x]_{\mathbb{Q}[x]\setminus\{0\}}$

3. $k(x):=k[x]_{k[x]\setminus\{0\}}=\{p(x)/q(x)\colon\ p(x),q(x)\in k[x],q(x)\neq 0\}$, o con mayor generalidad, el cuerpo de funciones racionales en n-variables con coeficientes en k,

$$k(x_1,\dots,x_n):=k[x_1,\dots,x_n]_{k[x_1,\dots,x_n]\setminus\{0\}}=\{p(x)/q(x)\colon \\ p(x),0\neq q(x)\in k[x_1,\dots,x_n]\}$$

6. Proposición: *Sea A un anillo y $S\subset A$ un sistema multiplicativo. Entonces,*

1. *$\frac{a}{s}=0\in A_S$ si y sólo si existe $s'\in S$ tal que $s'\cdot a=0$ (en A).*

2. *$\frac{a}{s}=\frac{a'}{s'}$ en A_S si y sólo si existe un $t\in S$ de modo que $t\cdot(as'-a's)=0$.*

Demostración. 1. $\Rightarrow$) $0=\frac{0}{1}=\frac{a}{s}$ luego existen $t,t'\in S$ tales que $t\cdot 0=t'\cdot a$ (y $t\cdot 1=t'\cdot s$), luego $t'\cdot a=0$.
$\Leftarrow$) $\frac{a}{s}=\frac{as'}{ss'}=\frac{0}{ss'}=\frac{0}{1}=0$.
2. $\Rightarrow$) $0=\frac{a}{s}-\frac{a'}{s'}=\frac{as'-a's}{ss'}$, existe un $t\in S$ de modo que $t\cdot(as'-a's)=0$, por el punto 1.
$\Leftarrow$) Si $t\cdot(as'-a's)=0$, entonces $0=\frac{as'-a's}{ss'}=\frac{a}{s}-\frac{a'}{s'}$, entonces $\frac{a}{s}=\frac{a'}{s'}$.

□

7. Ejercicio: Sea A un anillo y $S\subseteq A$ un sistema multiplicativo. Entonces, $A_S=\{0\}$ $\iff 0\in S$.

8. Ejercicio: Sea A un anillo íntegro y $S\subseteq A$ un sistema multiplicativo. Entonces, $\frac{a}{s}=\frac{a'}{s'}$ en A_S si y sólo si $as'-a's=0$ (en A).

9. Definición: Al morfismo natural de anillos $A\to A_S$, $a\mapsto\frac{a}{1}$ se le denomina morfismo de localización por S.

10. Ejercicio: Pruébese que $(\mathbb{Z}[x])_{\mathbb{Z}\setminus\{0\}}=\mathbb{Q}[x]$.

11. Descomposición en suma de fracciones simples: Sea (A,δ) un anillo euclídeo. Sean $a,p,q\in A$ y supongamos que p y q son primos entre sí. Entonces,

1. Existen $a_1,a_2\in A$ de modo que $\frac{a}{pq}=\frac{a_1}{p}+\frac{a_2}{q}$.

2. Existen $a_0,\dots,a_n \in A$, con $a_i = 0$ ó $\mathrm{gr}(a_i) < \mathrm{gr}(p)$, para cada $i \geq 1$, de modo que

$$\frac{a}{p^n} = \sum_{i=0}^{n} \frac{a_i}{p^i}.$$

Demostración. 1. Sean $\lambda, \mu \in A$ tales que $\lambda p + \mu q = 1$. Entonces

$$\frac{a}{pq} = \frac{a(\lambda p + \mu q)}{pq} = \frac{a\mu}{p} + \frac{a\lambda}{q}$$

2. $a = c_0 p + b_0$, para ciertos c_0 y b_0, con $b_0 = 0$ ó $\delta(b_0) < \delta(p)$. Igualmente, $c_0 = c_1 p + b_1$, para ciertos c_1 y b_1, con $b_1 = 0$ ó $\delta(b_1) < \delta(p)$. Luego, $a = b_0 + b_1 p + c_1 p^2$. De nuevo, $c_1 = c_2 p + b_2$, para ciertos c_2 y b_2, con $b_2 = 0$ ó $\delta(b_2) < \delta(p)$. Luego, $a = b_0 + b_1 p + b_2 p^2 + c_2 p^3$. Así sucesivamente obtenemos que $a = (\sum_{i=0}^{n-1} b_i p^i) + c_{n-1} p^n$. Si tomamos $a_i = b_{n-i}$, para $1 \leq i \leq n$, y $a_0 = c_n$ concluimos que $\frac{a}{p^n} = \sum_{i=0}^{n} \frac{a_i}{p^i}$. □

2.8.2. Lema de Gauss

12. Definición: Un polinomio $p(x) \in A[x]$ se dice *primitivo* cuando sus coeficientes no admiten un divisor común no invertible, es decir, si $p(x) = a \cdot q(x)$ con $a \in A$, entonces a es invertible.

13. Lema: *Sea A un dominio de factorización única de cuerpo de fracciones $\Sigma = A_{A\setminus 0}$. Entonces,*

1. *Si $p(x), q(x) \in A[x]$ son dos polinomios primitivos entonces $p(x)\cdot q(x)$ es primitivo.*
2. *Para cada $h(x) \in \Sigma[x]$ existen $v \in \Sigma$ y $p(x) \in A[x]$ primitivo, únicos salvo multiplicación por un invertible de A, tales que*

$$h(x) = v \cdot p(x).$$

Demostración. 1. Supongamos que $p(x)\cdot q(x) = a \cdot r(x)$, con $r(x) \in A[x]$ y $a \in A$ no invertible. Sea $p \in A$ irreducible que divida a a. Pasando al cociente $A[x] \to (A/pA)[x]$, tenemos que

$$\overline{p(x)} \cdot \overline{q(x)} = 0 \in (A/pA)[x].$$

Lo cual es contradictorio, porque $(A/pA)[x]$ es íntegro y $\overline{p(x)}$ y $\overline{q(x)}$ son no nulos.

2. Sea $u \in A$ el producto de todos los denominadores de los coefiecientes de $h(x)$. Entonces, $u \cdot h(x) \in A[x]$. Sea u' el máximo común divisor de todos los coeficientes de $u \cdot h(x)$. Entonces, $p(x) := \frac{u}{u'} h(x) \in A[x]$ es primitivo. Si definimos $v := \frac{u'}{u}$, entonces $h(x) = v \cdot p(x)$.

Sea otra descomposición $h(x) = v' \cdot p(x)'$. Basta probar que $v = v'$ salvo multiplicación por un invertible. Como $v \cdot p(x) = v' \cdot p(x)'$, multiplicando por el producto de los denominadores de v y v', podemos suponer que $v, v' \in A$. Sea p un elemento irreducible que divida a v. Pasando al cociente $A[x] \to (A/pA)[x]$, tenemos que $0 = \bar{v} \cdot \overline{p(x)} = \bar{v'} \cdot \overline{p(x)'}$, luego $\bar{v'} = 0$ y p divide a v'. Dividiendo a v y v' a la vez por p y repitiendo sucesivamente este proceso obtendremos que v divide a v', y por simetría que v' divide a v. Luego, $v = u \cdot v'$, para cierto invertible $u \in A$. □

14. Lema de Gauss: *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Un polinomio no constante primitivo, $p(x) \in A[x]$, es irreducible en $A[x]$ si y sólo si es irreducible en $\Sigma[x]$.*

Demostración. Supongamos que $p(x)$ es irreducible en $\Sigma[x]$. Si $p(x) = p_1(x) \cdot p_2(x)$, con $p_1(x), p_2(x) \in A[x]$, entonces como $p(x)$ es irreducible en $\Sigma[x]$, uno de los dos polinomios $p_1(x)$ o $p_2(x)$ ha de ser de grado cero, digamos $p_1(x) = a$. Como $p(x)$ es primitivo $p_1(x) = a \in A$ es invertible. En conclusión, $p(x)$, es irreducible en $A[x]$.

Supongamos que $p(x)$ es irreducible en $A[x]$ (luego es primitivo). Supongamos que $p(x) = \tilde{p}_1(x) \cdot \tilde{p}_2(x)$, siendo $\tilde{p}_1(x)$ y $\tilde{p}_2(x)$ dos polinomios de $\Sigma[x]$. Sean $v_1, v_2 \in \Sigma$ y $p_1(x), p_2(x) \in A[x]$ primitivos, salvo multiplicación por invertibles de A, tales que $\tilde{p}_1(x) = v_1 \cdot p_1(x)$ y $\tilde{p}_2(x) = v_2 \cdot p_2(x)$. Entonces,

$$p(x) = (v_1 \cdot v_2) \cdot (p_1(x) \cdot p_2(x)).$$

Por el lema 2.8.13 1., $p_1(x) \cdot p_2(x)$ es primitivo. Por el lema 2.8.13 2., $v_1 \cdot v_2$ es un invertible de A. Luego $p(x)$ no es irreducible en $A[x]$ y hemos llegado a contradicción. □

15. Corolario: *Si A es un dominio de factorización única, entonces $A[x]$ también lo es.*

Demostración. Sea $\Sigma = A_{A\setminus\{0\}}$ el cuerpo de fracciones. Sea $p(x) \in A[x]$ y escribamos $p(x) = a \cdot q(x)$, con $a \in A$ y $q(x) \in A[x]$ primitivo. Sea

$$q(x) = \tilde{q}_1(x) \cdots \tilde{q}_r(x)$$

la descomposición en irreducibles en $\Sigma[x]$. Por el lema 2.8.13 se puede escribir $\tilde{q}_i(x) = v_i \cdot q_i(x)$ con $v_i \in \Sigma$ y $q_i(x) \in A[x]$ primitivos. Luego,

$$q(x) = v \cdot q_1(x) \cdots q_r(x).$$

• Por el lema 2.8.13 1., $q_1(x) \cdots q_r(x)$ es primitivo. Por el lema 2.8.13 2., v es un invertible de A.

• Cada $q_i(x)$ es irreducible en $A[x]$ porque lo es en $\Sigma[x]$ y por 2.8.14.

Descomponiendo $a = p_1 \cdots p_s$ en producto de irreducibles en A, se obtiene una descomposición en producto de irreducibles

$$p(x) = a \cdot q(x) = u \cdot p_1 \cdots p_s q_1(x) \cdots q_r(x)$$

en $A[x]$.

Unicidad: Si $p(x) = q_1 \cdots q_l p_1(x) \cdots p_t(x)$, entonces cada $p_i(x)$ es irreducible en $\Sigma[x]$ por 2.8.14. Por tanto, los polinomios $p_i(x)$ (una vez reordenados) son iguales a los $q_i(x)$, salvo multiplicación por invertibles de A. Tachando los términos polinómicos comunes se obtiene salvo multiplicación por invertibles de A la igualdad $q_1 \cdots q_l = p_1 \cdots p_s$, de donde salvo permutación de los factores es $q_i = p_i$ (salvo multiplicación por invertibles de A).

q □

Como corolario del teorema anterior, se obtiene el siguiente teorema.

16. Teorema: *Los anillos $\mathbb{Z}[x_1, \ldots, x_n]$ y $k[x_1, \ldots, x_n]$ (k un cuerpo) son dominios de factorización única.*

2.9. Raíces de un polinomio

1. Definición: Sea $p(x) \in k[x]$ un polinomio y $\alpha \in k$. Se dice que α es una raíz de $p(x)$ si $p(\alpha) = 0$.

2. Proposición: *Sea $p(x) \in k[x]$ un polinomio y $\alpha \in k$. Entonces, α es una raíz de $p(x)$ si y sólo si $p(x)$ es múltiplo de $x - \alpha$.*

Demostración. Por el algoritmo de Euclides, existen $c(x) \in k[x]$ y $\lambda \in k$, tales que $p(x) = c(x)(x-\alpha)+\lambda$. Si α es una raíz de $p(x)$ entonces $0 = p(\alpha) = \lambda$ y $p(x)$ es múltiplo de $x-\alpha$. El recíproco es obvio. □

La siguiente proposición nos muestra cómo calcular las raíces racionales de un polinomio con coeficientes racionales.

3. Proposición: *Sea $p(x) = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{Q}[x]$ un polinomio con coeficientes racionales. Supongamos que es de coeficientes enteros, multiplicando por un número entero conveniente. Sea $q = \frac{r}{s} \in \mathbb{Q}$ una fracción irreducible (r y s son números enteros primos entre sí). Si q es una raíz de $p(x)$, entonces r divide a a_n y s a a_0*

Demostración. Tenemos que $0 = (\frac{r}{s})^n a_0 + (\frac{r}{s})^{n-1} a_1 + \cdots + a_n$, luego $0 = r^n a_0 + r^{n-1} s a_1 + \cdots + s^n a_n$. Por tanto, $s^n a_n$ es múltiplo de r y $r^n a_0$ es múltiplo de s. Luego, a_n es múltiplo de r y a_0 es múltiplo de s. □

El teorema fundamental del álgebra afirma que todo polinomio de grado mayor que cero con coeficientes complejos tiene al menos una raíz compleja. Por tanto, si $p(x) \in \mathbb{C}[x]$ es irreducible entonces existe una raíz $\alpha \in \mathbb{C}$ de $p(x)$, luego $p(x) = \lambda \cdot (x - \alpha)$, para cierto $\lambda \in \mathbb{C}$. Por lo tanto, por el teorema de descomposición en factores irreducibles, dado $q[x] \in \mathbb{C}[x]$, existen $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ distintos de modo que

$$q(x) = \lambda \cdot (x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}$$

para cierto $\lambda \in \mathbb{C}$.

4. Proposición: *Si $p(x) \neq 0$ es un polinomio de grado $n \geq 0$, no puede tener más de n raíces distintas.*

Demostración. Procedamos por inducción sobre n. Si $n = 0$, entonces $p(x) = \lambda \in k$ y no tiene raíces. Si $\operatorname{gr} p(x) \geq 0$ y α es una raíz de $p(x)$, entonces $p(x) = (x-\alpha) \cdot q(x)$, con $\operatorname{gr} q(x) = \operatorname{gr}(p(x)) - 1$. Las raíces de $p(x)$ son las de $q(x)$ junto con α. Las raíces de $q(x)$ son a lo más $n-1$, por inducción. Luego, $p(x)$ tiene a lo más n raíces.

□

5. Fórmula de interpolación de Lagrange: *Dados $\alpha_0, \ldots, \alpha_n \in k$ distintos entre sí y $\lambda_0, \ldots, \lambda_n \in k$ existe un único polinomio $p(x)$ de grado menor o igual que n tal que $p(\alpha_i) = \lambda_i$, para todo i. Además,*

$$p(x) = \sum_{i=0}^{n} \lambda_i \cdot \frac{(x-\alpha_0)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n)}{(\alpha_i-\alpha_0)\cdots\widehat{(\alpha_i-\alpha_i)}\cdots(\alpha_i-\alpha_n)}.$$

Diremos que $p(x)$ es el polinomio de interpolación de $\alpha_0, \ldots, \alpha_n$ con valores $\lambda_0, \ldots, \lambda_n$.

Demostración. $p(x)$ es de grado menor o igual que n y $p(\alpha_i) = \lambda_i$, para todo i.

Si $q(x)$ fuese otro polinomio con las mismas propiedades entonces $p(x) - q(x)$ sería un polinomio de grado menor o igual que n con $n+1$ raíces:$\alpha_0, \ldots, \alpha_n$. Por tanto, $p(x) - q(x) = 0$ y $q(x) = p(x)$. □

6. Definición: Sea $p(x) \in k[x]$ un polinomio y $\alpha \in k$. Se dice que $\alpha \in k$ es una raíz múltiple de $p(x)$ si $p(x)$ es múltiplo de $(x-\alpha)^2$. Se dice que $r > 0$ es la multiplicidad de una raíz de $p(x)$ si $p(x) = (x-\alpha)^r \cdot q(x)$, con $q(\alpha) \neq 0$.

7. Ejercicio: Pruébese que si $\alpha_1, \ldots, \alpha_s$ son raíces distintas de $p(x)$ con multiplicidad $n_1, \ldots, n_s$ respectivamente, entonces $p(x) = (x-\alpha_1)^{n_1} \cdots (x-\alpha_s)^{n_s} \cdot q(x)$, con $q(\alpha_i) \neq 0$ para todo i.

8. Proposición: *Sea $p(x) \in k[x]$ un polinomio. Entonces, $\alpha \in k$ es una raíz múltiple de $p(x)$ si y sólo si es raíz de $p(x)$ y $p'(x)$ (la derivada "formal" de $p(x)$).*

Demostración. Tenemos que α es una raíz de $p(x)$, entonces $p(x) = (x-\alpha)\cdot q(x)$ y $p'(x) = q(x) + (x-\alpha)\cdot q'(x)$. Por tanto, α es una raíz de $p'(x)$ si y sólo si es raíz de $q(x)$, es decir, si y sólo si α es una raíz múltiple de $p(x)$. □

9. Definición: Dado un morfismo de anillos entre cuerpos $k \to K$, diremos que K es una extensión (de cuerpos) de k.

En todo cuerpo k no hay más ideales que el ideal $\{0\}$ y todo k. Por tanto, todo morfismo de anillos $k \to K$ entre cuerpos es inyectivo. Escribiremos habitualmente, dado morfismo de cuerpos $k \to K$, $\lambda \mapsto \lambda$.

10. Teorema de Kronecker: *Sea $p(x) \in k[x]$ un polinomio de grado $n > 0$. Existe una extensión de cuerpos K de k en la que $p(x)$ descompone en factores simples, es decir, existen $\alpha_1, \ldots, \alpha_n \in K$ tales que*

$$p(x) = \lambda \cdot (x-\alpha_1) \cdots (x-\alpha_n), \qquad \lambda \in k.$$

Demostración. Procedamos por inducción sobre n. Si $n = 1$, basta tomar $K = k$, pues $p(x) = \lambda(x-\alpha)$, con $\alpha \in k$. Supongamos que $n > 1$. Sea $p_1(x) \in k[x]$ un polinomio irreducible que divida a $p(x)$. Sea $K_1 = k[x]/(p_1(x))$ y denotemos $\bar{x} = \alpha_1$. Obviamente, $p_1(\alpha_1) = 0$, luego $p(\alpha_1) = 0$. Por tanto, en $K_1[x]$ tenemos que $p(x) = (x-\alpha_1)\cdot p_2(x)$. Por hipótesis de inducción, existe una extensión $K_1 \hookrightarrow K$ de modo que $p_2(x) = \lambda \cdot (x-\alpha_2) \cdots (x-\alpha_n)$. Luego en K, que es una extensión de k,

$$p(x) = \lambda \cdot (x-\alpha_1) \cdots (x-\alpha_n).$$

□

Dadas dos k-extensiones de cuerpos K y K', puede probarse que existe una extensión de cuerpos de k, L, que contiene a K y K' (véase problema 15). Por tanto, si K y K' son dos k-extensiones de cuerpos que contienen todas las raíces de $p(x)$ y consideramos una k-extensión L que contenga a K y K', entonces las raíces de $p(x)$ en K y K' han de coincidir en L.

El teorema fundamental del Álgebra, que probaremos más adelante, afirma que todas las raíces de un polinomio con coeficientes complejos son complejas.

11. Proposición : *Sean $p(x), q(x) \in k[x]$ dos polinomios y $k \hookrightarrow K$ una extensión de cuerpos. El máximo común divisor de $p(x)$ y $q(x)$ en $k[x]$ coincide con el máximo común divisor de $p(x)$ y $q(x)$ en $K[x]$.*

Demostración. El máximo común divisor de dos polinimios $p(x)$ y $q(x)$ se puede calcular por el algoritmo de Euclides, cálculo que es el mismo si consideramos que estamos en $k[x]$ o si consideramos que estamos en $K[x]$.

□

12. Proposición: *Sean $p(x), q(x) \in k[x]$ dos polinomios y K una extensión de cuerpos de k donde estén todas las raíces de $p(x)$ y $q(x)$. Entonces, $p(x)$ y $q(x)$ son primos entre sí si y sólo si no tienen raíces comunes (en K).*

2.10. Polinomios ciclotómicos

1. Definición: Sea k un cuerpo. Se dice que $\alpha \in k$ es una raíz n-ésima de la unidad si $\alpha^n = 1$. Se dice que α es una raíz n-ésima primitiva de la unidad si $\alpha^n = 1$ y $\alpha^m \neq 1$, para todo $0 < m < n$.

Consideremos ahora $k = \mathbb{C}$.

Observemos que

$$\mu_n := \{e^{k\cdot 2\pi i/n} = cos\,\frac{2k\pi}{n} + i sen\,\frac{2k\pi}{n} \in \mathbb{C},\ 0 \leq k < n\},$$

es el conjunto de todas las raíces n-ésimas de la unidad, que es un subgrupo (multiplicativo) de $\mathbb{C}^*$, de orden n.

El morfismo, $\mathbb{Z}/n\mathbb{Z} \to \mu_n$, $\bar{m} \mapsto e^{m\cdot 2\pi i/n}$ es un isomorfismo de grupos. Vía este isomorfismo, el conjunto de generadores $\mathbb{Z}/n\mathbb{Z}$ se identifica con el conjunto $R_n \subset \mu$, de todas las raíces n-ésimas primitivas de la unidad ($R_n = \{\varepsilon \in \mu_n$ tales que $\varepsilon^m \neq 1$ para cada $m < n\}$). El conjunto de generadores de $\mathbb{Z}/n\mathbb{Z}$ se identifica con los invertibles de $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z}, (k,n) = (1)\}$. Luego,

$$R_n = \{e^{k\cdot 2\pi i/n} = cos\,\frac{2k\pi}{n} + i sen\,\frac{2k\pi}{n},\ \text{con}\ \ 0 < k < n \text{ y } (k,n) = (1)\}.$$

2. Definición: Se dice que un polinomio $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in k[x]$, con $a_0 \neq 0$ es mónico si $a_0 = 1$.

3. Definición: Para cada $n \in \mathbb{N}$ se denomina n-ésimo *polinomio ciclotómico* al polinomio mónico

$$\Phi_n(x) = \prod_{k<n,(k,n)=(1)} (x - e^{k\cdot 2\pi i/n}).$$

Se cumple $\xi \in \mathbb{C}$ es una raíz n-ésima de la unidad si y sólo si ξ es una raíz primitiva d-ésima de la unidad para algún $d|n$. Por tanto,

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Luego,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d<n, d|n} \Phi_d(x)}.$$

Por recurrencia se demuestra que $\Phi_n(x) \in \mathbb{Z}[x]$ (obsérvese que $\Phi_1(x) = x - 1$).

Dejamos que el lector pruebe la siguiente proposición.

4. Proposición: *Se cumple*

1. $\Phi_1(x) = x - 1$.
2. $\Phi_2(x) = \frac{x^2-1}{\Phi_1(x)} = x + 1$.
3. $\Phi_3(x) = \frac{x^3-1}{\Phi_1(x)} = x^2 + x + 1$.
4. $\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\cdot\Phi_2(x)} = x^2 + 1$.
5. $\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = x^4 + x^3 + x^2 + x + 1$.
6. $\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\cdot\Phi_2(x)\cdot\Phi_3(x)} = x^2 - x + 1$.
7. *Si* $p > 0$ *es primo,* $\Phi_p(x) = \frac{x^p-1}{\Phi_1(x)} = x^{p-1} + x^{p-2} + \cdots + x + 1$.
8. *Si* $p > 0$ *es primo,* $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}}) = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + x^{p^{n-1}} + 1$. *También,* $\Phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1}$.
9. *Si* $p > 0$ *es primo y* r *no es divisible por* p, $\Phi_{r\cdot p^n}(x) = \frac{\Phi_r(x^{p^n})}{\Phi_r(x^{p^{n-1}})}$.
10. *Si* $r > 2$ *es impar,* $\Phi_{2r}(x) = \Phi_r(-x)$.

5. Lema: *Sea* $p \in \mathbb{N}$ *un número primo. Para todo* $q(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ *se cumple que*

$$q(x)^p = q(x^p).$$

Demostración. Para cada $a \in \mathbb{Z}/p\mathbb{Z}$ es $a^p = a$ y $(r(x) + s(x))^p = r(x)^p + s(x)^p$, para cada $r(x), s(x) \in \mathbb{Z}/p\mathbb{Z}[x]$, luego

$$q(x)^p = (a_0 + a_1 x + \cdots a_n x^n)^p = a_0^p + a_1^p x^p + \cdots a_n^p (x^p)^n = q(x^p).$$

□

6. Teorema: *Los polinomios ciclotómicos* $\Phi_n(x) \in \mathbb{Z}[x]$ *son polinomios irreducibles.*

Demostración. Sea $\Phi_n(x) = p(x) \cdot q(x)$ con $p(x) \in \mathbb{Z}[x]$, $\operatorname{gr} p(x) > 0$. Como se sabe, si ε es una raíz primitiva de la unidad, entonces las raíces primitivas n-ésimas de la unidad son exactamente las de la forma ε^m con $(m, n) = 1$. Por tanto, para ver que $p(x) = \Phi_n(x)$ basta ver que si ε es raíz de $p(x)$ y p un número primo no divisor de n, entonces ε^p es también raíz de $p(x)$. Sea pues ε una raíz de $p(x)$ tal que ε^p sea raíz de $q(x)$. Entonces, los polinomios $p(x)$ y $q(x^p)$ tienen la raíz ε en común, luego no son primos

entre sí. Entonces en $\mathbb{Z}/p\mathbb{Z}[x]$, $\overline{p(x)}$ y $\overline{q(x^p)} = \overline{q(x)}^p$ no son primos entre sí. Por tanto, $\overline{p(x)}$ y $\overline{q(x)}$ no son primos entre sí, y $\overline{\Phi_n(x)} = \overline{p(x)} \cdot \overline{q(x)}$ tiene raíces múltiples. Entonces, $x^n - \bar{1} \in \mathbb{Z}/p\mathbb{Z}[x]$ tiene raíces múltiples. Pero, $x^n - \bar{1}$ es primo con su derivada $\bar{n} \cdot x^{n-1}$ (donde $\bar{n} \neq 0$, porque p no divide a n), lo que implica que no tiene raíces múltiples. Hemos llegado a contradicción. □

7. Proposición: $\mathbb{Q}[e^{\frac{2\pi i}{n}}] \simeq \mathbb{Q}[x]/(\Phi_n(x))$.

Demostración. El polinomio mónico con coeficientes en $\mathbb{Q}$ mínimo anulador de $e^{\frac{2\pi i}{n}}$ es $\Phi_n(x)$, por el teorema 2.10.6 y el lema 2.8.14. Luego, $\mathbb{Q}[e^{\frac{2\pi i}{n}}] \simeq \mathbb{Q}[x]/(\Phi_n(x))$. □

2.11. Criterios de irreducibilidad de polinomios

1. Proposición: *Sean A y B anillos íntegros, $p(x) = \sum_{i=0}^{n} a_i \cdot x^{n-i} \in A[x]$ un polinomio primitivo y $f : A \to B$ un morfismo de anillos. Si $f(a_0) \neq 0$ y $\sum_{i=0}^{n} f(a_i) \cdot x^{n-i} \in B[x]$ es irreducible, entonces $p(x)$ es irreducible.*

Demostración. Al lector. □

2. Criterio de Eisenstein: *Sea A un dominio de factorización única, $p \in A$ irreducible y $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in A[x]$ un polinomio. Si se verifica:*

1. *$p(x)$ es primitivo,*
2. *$a_1, \ldots, a_n$ son múltiplos de p*
3. *a_n no es múltiplo de p^2.*

entonces $p(x)$ es irreducible.

Demostración. Si $p(x) = c(x) \cdot d(x)$ es una descomposición propia, entonces por ser $p(x)$ primitivo es $n > gr\, c(x), gr\, d(x) > 0$. Sean $\overline{p(x)}, \overline{c(x)}, \overline{d(x)} \in (A/(p))[x]$ las clases de $p(x), c(x)$ y $d(x)$ módulo p. Por 2., es $\overline{p(x)} = \overline{a}_0x^n$. Por tanto (ejercicio), $\overline{c(x)} = \overline{c}_{n-i}x^i$ y $\overline{d(x)} = \overline{d}_ix^{n-i}$ (con $n > n - i$ y $n > i$, es decir, $i, n - i > 0$). En particular, los términos independientes de $c(x), d(x)$ son múltiplos de p y, por tanto, el de $p(x)$ es múltiplo de p^2, lo que contradice 3.

□

3. Ejercicio: Probar que $x^n - 2 \in \mathbb{Z}[x]$ es un polinomio irreducible, para todo $n > 0$.

4. Descomposición de un polinomio con coeficientes racionales en factores irreducibles. Sea $p(x) \in \mathbb{Q}[x]$. $p(x) = m \cdot q(x)$, con $m \in \mathbb{Q}$ y $q(x) \in \mathbb{Z}[x]$ primitivo. Para descomponer $p(x)$ en factores irreducibles basta descomponer $q(x)$ en factores irreducibles en $\mathbb{Z}[x]$. Basta saber calcular los polinomios $q_n(x) \in \mathbb{Z}[x]$, con $n = \text{gr}\, q_n(x) \leq (\text{gr}\, q(x))/2$ que dividen a $q(x)$. Todo polinomio de grado n, $r(x)$, coincide con el polinomio de interpolación de $0, 1, \ldots, n$ con valores $r(0), \ldots, r(n)$. Si $q(x) = q_n(x) \cdot q_{n'}(x)$, entonces $q_n(i)$ divide a $q(i)$ (observemos que sólo hay un número finito de enteros que dividen al entero $q(i)$). Sea $Y = \{(\lambda_0, \ldots, \lambda_n) \in \mathbb{Z}^{n+1} : \ \lambda_i \text{ divide a } q(i), \text{ para todo } i\}$, y para cada $y = (\lambda_0, \ldots, \lambda_n) \in Y$ sea $q_y(x)$ el polinomio de interpolación de $0, 1, \ldots, n$ con valores

$\lambda_0,\dots,\lambda_n$. Entonces, $q_n(x)$ coincide con $q_y(x)$ para algún $y \in Y$ ($q_y(x)$ debe dividir a $q(x)$).

2.12. Apéndice: Teorema fundamental del Álgebra

Sea $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = c(x-\alpha_1)\cdots(x-\alpha_n)$. Desarrollando el último término e igualando coeficientes de los x^i se obtiene las fórmulas de Cardano:

$$\begin{aligned} a_0 &= c \\ a_1 &= -c\cdot(\alpha_1+\cdots+\alpha_n) \\ &\cdots \\ a_i &= (-1)^i c\cdot \sum_{1\le j_1<\cdots<j_i\le n} \alpha_{j_1}\cdots\alpha_{j_i} \\ &\cdots \\ a_n &= (-1)^n c\cdot\alpha_1\cdots\alpha_n \end{aligned}$$

1. Definición: Llamaremos *funciones simétricas elementales* (o polinomios simétricos elementales) en las letras $x_1,\dots,x_n$ a los polinomios $s_i \in \mathbb{Z}[x_1,\dots,x_n]$ $(i=1,\dots,n)$ definidos por:

$$\begin{aligned} s_1 &= x_1+\cdots+x_n \\ &\cdots \\ s_i &= \sum_{1\le j_1<\cdots<j_i\le n} x_{j_1}\cdots x_{j_i} \\ &\cdots \\ s_n &= x_1\cdots x_n \end{aligned}$$

Se cumple la igualdad:

$$\prod_i (x-x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$$

Sea S_n el grupo de las permutaciones de n letras. Para cada $\sigma \in S_n$ consideremos el morfismo de anillos, $\sigma\colon A[x_1,\dots,x_n] \to A[x_1,\dots,x_n]$ definido por

$$\sigma(p(x_1,\dots,x_n)) := p(x_{\sigma(1)},\dots,x_{\sigma(n)}).$$

2. Definición: Diremos que un polinomio $p(x_1,\dots,x_n) \in A[x_1,\dots x_n]$ es simétrico cuando $\sigma(p(x_1,\dots,x_n)) = p(x_1,\dots,x_n)$ para toda $\sigma \in S_n$. Al conjunto de las funciones simétricas las denotaremos $A[x_1,\dots x_n]^{S_n}$.

3. Teorema de las funciones simétricas: *Se verifica la igualdad:*

$$A[x_1,\dots,x_n]^{S_n} = A[s_1,\dots,s_n].$$

Es decir, un polinomio en $x_1,\dots,x_n$ con coeficientes en el anillo A es invariante por todas las permutaciones de las variables si y sólo si es un polinomio en las funciones simétricas elementales.

Demostración. Evidentemente todo polinomio en las funciones simétricas elementales es invariante por el grupo de las permutaciones. Por tanto, basta probar el recíproco.

Procedemos por inducción sobre el número n de variables. Para $n = 1$ es trivial. Sea $p(x_1,\dots,x_n) \in A[x_1,\dots,x_n]^{S_n}$. Descomponiendo $p(x_1,\dots,x_n)$ en la suma de sus componentes homogéneas, podemos suponer que $p(x_1,\dots,x_n)$ es homogéneo de grado m. Haciendo cociente por x_n se obtiene que $p(x_1,\dots,x_{n-1},0)$ es un polinomio homogéneo de grado m en $n-1$ variables e invariante por las permutaciones de éstas, luego $p(x_1,\dots,x_{n-1},0) = q'(s'_1,\dots,s'_{n-1})$, siendo s'_i la i-ésima función simétrica en las $n-1$ primeras variables. Cada sumando $\lambda_{m_1,\dots,m_{n-1}} s'^{m_1}_1 \cdots s'^{m_{n-1}}_{n-1}$ de $q'(s'_1,\dots,s'_{n-1})$ es un polinomio homogéneo en $x_1,\dots,x_{n-1}$ de grado $m_1 + 2m_2 + \cdots + (n-1)m_{n-1}$. Podemos suponer que $\lambda_{m_1,\dots,m_{n-1}} = 0$, cuando $m_1 + 2m_2 + \cdots + (n-1)m_{n-1} \neq m$. Por tanto, $q'(s_1,\dots,s_{n-1})$ es un polinomio en $x_1,\dots,x_n$ homogéneo de grado m. Sea $h(x_1,\dots,x_n) = p(x_1,\dots,x_n) - q'(s_1,\dots,s_{n-1})$. Se verifica que $h(x_1,\dots,x_n)$ es simétrico y homogéneo de grado m y se anula para $x_n = 0$ (ya que $s_i = s'_i \, mod \, x_n$), luego es múltiplo de x_n y por ser simétrico es múltiplo de $x_1 \cdots x_n = s_n$, es decir, $h(x_1,\dots,x_n) = s_n \cdot h'(x_1,\dots,x_n)$ y, por tanto, $h'(x_1,\dots,x_n)$ es simétrico también y homogéneo de grado $gr(h') = gr(h) - n = gr(p) - n < gr(p)$, luego por recurrencia sobre el grado m de p se concluye que $h'(x_1,\dots,x_n) = \widetilde{q}(s_1,\dots,s_n)$. Sustituyendo en la definición de h y despejando se obtiene:

$$p(x_1,\dots x_n) = q'(s_1,\dots,s_{n-1}) + s_n \cdot \widetilde{q}(s_1,\dots,s_n)$$

con lo que se concluye. □

4. Teorema fundamental del Álgebra: *Para todo polinomio $p(x) \in \mathbb{C}[x]$ de grado n, existen $\alpha_1,\dots,\alpha_n \in \mathbb{C}$ de modo que*

$$p(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n).$$

Demostración. Dado un polinomio cualquiera, $0 \neq p(x) \in \mathbb{C}[x]$, tenemos que probar que tiene una raíz en $\mathbb{C}$. Basta probar que todo polinomio con coeficientes reales tiene una raíz compleja, porque el producto de $p(x)$ por su conjugado, $q(x) = p(x) \cdot \overline{p(x)}$ es un polinomio con coeficientes reales y si α es una raíz de $q(x)$, entonces α o su conjugada es una raíz de $p(x)$. Si $q(x) \in \mathbb{R}[x]$ es un polinomio de grado impar entonces

$$\lim_{x\to+\infty} q(x) = -\lim_{x\to-\infty} q(x), \quad (\text{y } |\lim_{x\to+\infty} q(x)| = +\infty).$$

Luego por el teorema de Bolzano existe un $\alpha \in \mathbb{R}$ tal que $q(\alpha) = 0$. Supongamos que $\mathrm{gr}\, q(x) = r = 2^n \cdot m$, con m impar. Para probar que $q(x)$ tiene una raíz compleja procedamos por inducción sobre n. Para $n = 0$ lo hemos probado. Supongamos $n > 0$. Sean $\alpha_1,\dots,\alpha_r$ las raíces de $q(x)$ y fijado $\lambda \in \mathbb{R}$ sean $\beta_{ij} := \alpha_i + \alpha_j + \lambda\alpha_i \cdot \alpha_j$. El polinomio $h(x) := \prod_{i<j}(x - \beta_{ij}) \in \mathbb{R}[x]$, porque los coeficientes de $h(x)$ son funciones simétricas en $\alpha_1,\dots,\alpha_n$, luego por el teorema de las funciones simétricas, los coeficientes de $h(x)$ son polinomios en los coeficientes de $q(x)$. Observemos que $h(x)$ es un polinomio de grado $\binom{r}{2} = 2^{n-1} \cdot m \cdot (r-1) = 2^{n-1} \cdot m'$ con m' impar. Por inducción sobre n, cierto $\beta_{rs} = \alpha_r + \alpha_s + \lambda\alpha_r \cdot \alpha_s \in \mathbb{C}$. Variando el λ fijado (tómese $\binom{r}{2}+1$ distintos), existirán $\lambda \neq \lambda'$, para los que existen r, s, de modo que

$$\alpha_r + \alpha_s + \lambda\alpha_r \cdot \alpha_s,\ \alpha_r + \alpha_s + \lambda'\alpha_r \cdot \alpha_s \in \mathbb{C}.$$

Luego $a := \alpha_r + \alpha_s$ y $b := \alpha_r \cdot \alpha_s \in \mathbb{C}$. Como α_r y α_s son las raíces de $(x-\alpha_r)(x-\alpha_s) = x^2 - ax + b$, tenemos que $\alpha_r, \alpha_s = (a \pm \sqrt{a^2 - 4b})/2 \in \mathbb{C}$. □

2.13. Cuestionario

1. Consideremos el conjunto $A = \{0\}$ y consideremos las dos operaciones internas:

$$0 + 0 := 0 \text{ y } 0 \cdot 0 := 0$$

   ¿Es $(A, +, \cdot)$ un anillo?

2. Sean $(A, +, \cdot)$ y $(B, +, \cdot)$ dos anillos. Dotar a $A \times B$ de estructura de anillo.

3. ¿La serie $1 + x \in \mathbb{Q}[[x]]$ tiene inverso?

4. Sean A y B dos anillos y consideremos en $A \times B$ la estructura de anillo usual ¿Es $A \times B$ un anillo íntegro?

5. ¿Son los cuerpos anillos íntegros?

6. Sea A un anillo íntegro. Sean $a, b, c \in A$ y $a \neq 0$. Si $ab = ac$, pruébese que $b = c$.

7. Sea $I \subset A$ un ideal. Pruébese que $A[x]/(I) \simeq (A/I)[x]$.

8. Sean I_1, I_2 dos ideales de A. Pruébese que $I_1 + I_2 := \{i_1 + i_2 \in A : i_1 \in I_1, i_2 \in I_2\}$ es un ideal de A. Pruébese que $\bar{I}_2 := \{\bar{i}_2 \in A/I_1 : i_2 \in I_2\}$ es un ideal de A/I_1. Pruébese que

$$(A/I_1)/\bar{I}_2 = A/(I_1 + I_2).$$

9. Sea A un anillo íntegro. Pruébese que $(A[x])^* = A^*$ (definimos B^* como el conjunto de los invertibles de B).

10. Calcúlense los ideales primos de $A = \{0\}$.

11. Sea K un cuerpo. Calcúlense los ideales de K.

12. Dar un criterio para saber cuándo un número entero escrito en base dos es divisible por $3 \in \mathbb{Z}$.

13. ¿Es el ideal $(x, y) \subset \mathbb{Q}[x, y]$ principal?

14. Sea (A, δ) un anillo euclídeo. Dado $a \in A$ no nulo pruébese que $\delta(a) \geq \delta(1)$. Pruébese que a es invertible si y sólo si $\delta(a) = \delta(1)$.

15. Dados $p(x) = x^3 + x^2 + x + 1, q(x) = 2x^2 + 3x + 1 \in \mathbb{Q}[x]$, calcúlese $c(x), r(x)$ de modo que $p(x) = q(x)c(x) + r(x)$ y $r(x) = 0$ ó $\text{gr}(r(x)) < \text{gr}(q(x))$.

16. Dados $22 + 7i, 2 + 2i \in \mathbb{Z}[i]$. Calcúlense $c, r \in \mathbb{Z}[i]$, tales que $22 + 7i = (2 + 2i) \cdot c + r$, de modo que $r = 0$ ó $|r| < |2 + 2i|$.

17. ¿Es $2 \in \mathbb{Z}[i]$ irreducible? Descomponer 2 en producto de irreducibles de $\mathbb{Z}[i]$.

18. Sean $p(x) = x^3 - x^2 + x - 1$ y $q(x) = x^3 - 3x^2 + 3x - 1 \in \mathbb{Q}[x]$. Calcúlese mediante el algoritmo de Euclides el máximo común divisor de $p(x)$ y $q(x)$, calcúlese $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ de modo que $\lambda(x)p(x) + \mu(x)q(x) = m.c.d.(p(x), q(x))$.

19. Sea A un anillo euclídeo y $a, b \in A$. Pruébese que si $a^{33} = b^{33}$ entonces a es igual a b salvo un factor invertible.

20. Sea A un anillo euclídeo y $a, b \in A$. Pruébese que $m.c.d(a,b) \cdot m.c.m.(a,b)$ es igual a $a \cdot b$ salvo un factor invertible.

21. Sea A un anillo euclídeo y $a, b \in A$. Pruébese que $m.c.d.(a^2, b^2) = m.c.d.(a,b)^2$.

22. Pruébese que en $\mathbb{Z}$ hay infinitos números primos.

23. Calcúlense las raíces racionales de $x^5 - \frac{3}{2}x^3 + 1$.

24. Calcúlense las raíces múltiples de $x^4 + x^3 + x^2 + x - 1 \in \mathbb{R}[x]$.

25. Sea K un cuerpo. Pruébese que un polinomio no constante $p(x) \in K[x]$ es irreducible si y sólo si $K[x]/(p(x))$ es un cuerpo.

26. Calcúlese el inverso de $\bar{7}$ en $\mathbb{Z}/982\mathbb{Z}$.

27. Calcúlese el inverso de $\overline{1 + x + x^2} \in \mathbb{Q}[x]/(x^3 - 2)$. Calcúlese el inverso de $1 + \sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}]$.

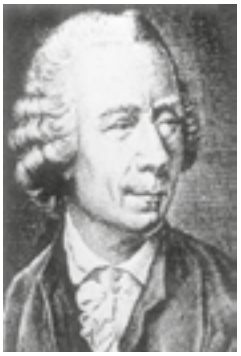
28. Calcúlese la clase de 12^{13} en $\mathbb{Z}/5\mathbb{Z}$, en $\mathbb{Z}/7\mathbb{Z}$ y en $\mathbb{Z}/35\mathbb{Z}$.

29. Calcúlese $\Phi_{18}(x)$.

30. Pruébese que el polinomio $y^2 - x^2 + x^3 \in \mathbb{R}[x, y]$ es irreducible.

31. Pruébese que $\frac{1}{7}x^{33} - \frac{2}{7} \in \mathbb{Q}[x]$ es irreducible.

2.14. Biografía de Leonhard Euler



EULER BIOGRAPHY

Leonhard Euler's father was Paul Euler. Paul Euler had studied theology at the University of Basel and had attended Jacob Bernoulli's lectures there. In fact Paul Euler and Johann Bernoulli had both lived in Jacob Bernoulli's house while undergraduates at Basel. Paul Euler became a Protestant minister and married Margaret Brucker, the daughter of another Protestant minister. Their son Leonhard Euler was born in Basel, but the family moved to Riehen when he was one year old and it was in Riehen, not far from Basel, that Leonard was brought up. Paul Euler had, as we have mentioned, some ma-

thematical training and he was able to teach his son elementary mathematics along with other subjects.

Leonhard was sent to school in Basel and during this time he lived with his grandmother on his mother's side. This school was a rather poor one, by all accounts, and Euler learnt no mathematics at all from the school. However his interest in mathematics had certainly been sparked by his father's teaching, and he read mathematics texts on his own and took some private lessons. Euler's father wanted his son to follow him into the church and sent him to the University of Basel to prepare for the ministry. He entered the University in 1720, at the age of 14, first to obtain a general education before going on to more advanced studies. Johann Bernoulli soon discovered Euler's great potential for mathematics in private tuition that Euler himself engineered. Euler's own account given in his unpublished autobiographical writings, is as follows:

... I soon found an opportunity to be introduced to a famous professor Johann Bernoulli. ... True, he was very busy and so refused flatly to give me private lessons; but he gave me much more valuable advice to start reading more difficult mathematical books on my own and to study them as diligently as I could; if I came across some obstacle or difficulty, I was given permission to visit him freely every Sunday afternoon and he kindly explained to me everything I could not understand ...

In 1723 Euler completed his Master's degree in philosophy having compared and contrasted the philosophical ideas of Descartes and Newton. He began his study of theology in the autumn of 1723, following his father's wishes, but, although he was to be a devout Christian all his life, he could not find the enthusiasm for the study of theology, Greek and Hebrew that he found in mathematics. Euler obtained his father's consent to change to mathematics after Johann Bernoulli had used his persuasion. The fact that Euler's father had been a friend of Johann Bernoulli's in their undergraduate days undoubtedly made the task of persuasion much easier.

Euler completed his studies at the University of Basel in 1726. He had studied many mathematical works during his time in Basel. They include works by Varignon, Descartes, Newton, Galileo, van Schooten, Jacob Bernoulli, Hermann, Taylor and Wallis. By 1726 Euler had already a paper in print, a short article on isochronous curves in a resisting medium. In 1727 he published another article on reciprocal trajectories and submitted an entry for the 1727 Grand Prize of the Paris Academy on the best arrangement of masts on a ship.

The Prize of 1727 went to Bouguer, an expert on mathematics relating to ships, but Euler's essay won him second place which was a fine achievement for the young graduate. However, Euler now had to find himself an academic appointment and when Nicolaus (II) Bernoulli died in St Petersburg in July 1726 creating a vacancy there, Euler was offered the post which would involve him in teaching applications of mathematics and mechanics to physiology. He accepted the post in November 1726 but stated that he did not want to travel to Russia until the spring of the following year. He had two reasons to delay. He wanted time to study the topics relating to his new post but also he had a chance of a post at the University of Basel since the professor of physics there had died. Euler wrote an article on acoustics, which went on to become a classic, in his bid for selection to the post but he was not chosen to go forward to the stage where lots were drawn to make the final decision on who would fill the chair.

Almost certainly his youth (he was 19 at the time) was against him. However Calinger suggests:

This decision ultimately benefited Euler, because it forced him to move from a small republic into a setting more adequate for his brilliant research and technological work.

As soon as he knew he would not be appointed to the chair of physics, Euler left Basel on 5 April 1727. He travelled down the Rhine by boat, crossed the German states by post wagon, then by boat from Lübeck arriving in St Petersburg on 17 May 1727. He had joined the St Petersburg Academy of Sciences two years after it had been founded by Catherine I the wife of Peter the Great. Through the requests of Daniel Bernoulli and Jakob Hermann, Euler was appointed to the mathematical-physical division of the Academy rather than to the physiology post he had originally been offered. At St Petersburg Euler had many colleagues who would provide an exceptional environment for him. Youschkevitch wrote:

Nowhere else could he have been surrounded by such a group of eminent scientists, including the analyst, geometer Jakob Hermann, a relative; Daniel Bernoulli, with whom Euler was connected not only by personal friendship but also by common interests in the field of applied mathematics; the versatile scholar Christian Goldbach, with whom Euler discussed numerous problems of analysis and the theory of numbers; F Maier, working in trigonometry; and the astronomer and geographer J-N Delisle.

Euler served as a medical lieutenant in the Russian navy from 1727 to 1730. In St Petersburg he lived with Daniel Bernoulli who, already unhappy in Russia, had requested that Euler bring him tea, coffee, brandy and other delicacies from Switzerland. Euler became professor of physics at the Academy in 1730 and, since this allowed him to become a full member of the Academy, he was able to give up his Russian navy post.

Daniel Bernoulli held the senior chair in mathematics at the Academy but when he left St Petersburg to return to Basel in 1733 it was Euler who was appointed to this senior chair of mathematics. The financial improvement which came from this appointment allowed Euler to marry which he did on 7 January 1734, marrying Katharina Gsell, the daughter of a painter from the St Petersburg Gymnasium. Katharina, like Euler, was from a Swiss family. They had 13 children altogether although only five survived their infancy. Euler claimed that he made some of his greatest mathematical discoveries while holding a baby in his arms with other children playing round his feet. D. Cameron wrote:

... after 1730 he carried out state projects dealing with cartography, science education, magnetism, fire engines, machines, and ship building. ... The core of his research program was now set in place: number theory; infinitary analysis including its emerging branches, differential equations and the calculus of variations; and rational mechanics. He viewed these three fields as intimately interconnected. Studies of number theory were vital to the foundations of calculus, and special functions and differential equations were essential to rational mechanics, which supplied concrete problems.

The publication of many articles and his book Mechanica (1736-37), which extensively presented Newtonian dynamics in the form of mathematical analysis for the first time, started Euler on the way to major mathematical work.

Euler's health problems began in 1735 when he had a severe fever and almost lost his life. However, he kept this news from his parents and members of the Bernoulli family back in Basel until he had recovered. In his autobiographical writings Euler says that his eyesight problems began in 1738 with overstrain due to his cartographic work and that by 1740 he wrote:

... lost an eye and [the other] currently may be in the same danger.

However, Calinger argued that Euler's eyesight problems almost certainly started earlier and that the severe fever of 1735 was a symptom of the eyestrain. He also argued that a portrait of Euler from 1753 suggests that by that stage the sight of his left eye was still good while that of his right eye was poor but not completely blind. Calinger suggested that Euler's left eye became blind from a later cataract rather than eyestrain.

By 1740 Euler had a very high reputation, having won the Grand Prize of the Paris Academy in 1738 and 1740. On both occasions he shared the first prize with others. Euler's reputation was to bring an offer to go to Berlin, but at first he preferred to remain in St Petersburg. However political turmoil in Russia made the position of foreigners particularly difficult and contributed to Euler changing his mind. Accepting an improved offer Euler, at the invitation of Frederick the Great, went to Berlin where an Academy of Science was planned to replace the Society of Sciences. He left St Petersburg on 19 June 1741, arriving in Berlin on 25 July. In a letter to a friend Euler wrote:

I can do just what I wish [in my research] ... The king calls me his professor, and I think I am the happiest man in the world.

Even while in Berlin Euler continued to receive part of his salary from Russia. For this remuneration he bought books and instruments for the St Petersburg Academy, he continued to write scientific reports for them, and he educated young Russians.

Maupertuis was the president of the Berlin Academy when it was founded in 1744 with Euler as director of mathematics. He deputised for Maupertuis in his absence and the two became great friends. Euler undertook an unbelievable amount of work for the Academy:

... he supervised the observatory and the botanical gardens; selected the personnel; oversaw various financial matters; and, in particular, managed the publication of various calendars and geographical maps, the sale of which was a source of income for the Academy. The king also charged Euler with practical problems, such as the project in 1749 of correcting the level of the Finow Canal ... At that time he also supervised the work on pumps and pipes of the hydraulic system at Sans Souci, the royal summer residence.

This was not the limit of his duties by any means. He served on the committee of the Academy dealing with the library and of scientific publications. He served as an advisor to the government on state lotteries, insurance, annuities and pensions and artillery. On top of this his scientific output during this period was phenomenal.

During the twenty-five years spent in Berlin, Euler wrote around 380 articles. He wrote books on the calculus of variations; on the calculation of planetary orbits; on artillery and ballistics (extending the book by Robins); on analysis; on shipbuilding and navigation; on the motion of the moon; lectures on the differential calculus; and a

popular scientific publication Letters to a Princess of Germany (3 vols., 1768-72).

In 1759 Maupertuis died and Euler assumed the leadership of the Berlin Academy, although not the title of President. The king was in overall charge and Euler was not now on good terms with Frederick despite the early good favour. Euler, who had argued with d'Alembert on scientific matters, was disturbed when Frederick offered d'Alembert the presidency of the Academy in 1763. However d'Alembert refused to move to Berlin but Frederick's continued interference with the running of the Academy made Euler decide that the time had come to leave.

In 1766 Euler returned to St Petersburg and Frederick was greatly angered at his departure. Soon after his return to Russia, Euler became almost entirely blind after an illness. In 1771 his home was destroyed by fire and he was able to save only himself and his mathematical manuscripts. A cataract operation shortly after the fire, still in 1771, restored his sight for a few days but Euler seems to have failed to take the necessary care of himself and he became totally blind. Because of his remarkable memory he was able to continue with his work on optics, algebra, and lunar motion. Amazingly after his return to St Petersburg (when Euler was 59) he produced almost half his total works despite the total blindness.

Euler of course did not achieve this remarkable level of output without help. He was helped by his sons, Johann Albrecht Euler who was appointed to the chair of physics at the Academy in St Petersburg in 1766 (becoming its secretary in 1769) and Christoph Euler who had a military career. Euler was also helped by two other members of the Academy, W. L. Krafft and A J. Lexell, and the young mathematician N. Fuss who was invited to the Academy from Switzerland in 1772. Fuss, who was Euler's grandson-in-law, became his assistant in 1776. Yushkevich wrote:

.. the scientists assisting Euler were not mere secretaries; he discussed the general scheme of the works with them, and they developed his ideas, calculating tables, and sometimes compiled examples.

For example Euler credits Albrecht, Krafft and Lexell for their help with his 775 page work on the motion of the moon, published in 1772. Fuss helped Euler prepare over 250 articles for publication over a period on about seven years in which he acted as Euler's assistant, including an important work on insurance which was published in 1776.

Yushkevich described the day of Euler's death:

On 18 September 1783 Euler spent the first half of the day as usual. He gave a mathematics lesson to one of his grandchildren, did some calculations with chalk on two boards on the motion of balloons; then discussed with Lexell and Fuss the recently discovered planet Uranus. About five o'clock in the afternoon he suffered a brain haemorrhage and uttered only Ï am dying"before he lost consciousness. He died about eleven o'clock in the evening.

After his death in 1783 the St Petersburg Academy continued to publish Euler's unpublished work for nearly 50 more years.

Euler's work in mathematics is so vast that an article of this nature cannot but give a very superficial account of it. He was the most prolific writer of mathematics of all time. He made large bounds forward in the study of modern analytic geometry and trigonometry where he was the first to consider sin, cos etc. as functions rather than

as chords as Ptolemy had done.

He made decisive and formative contributions to geometry, calculus and number theory. He integrated Leibniz's differential calculus and Newton's method of fluxions into mathematical analysis. He introduced beta and gamma functions, and integrating factors for differential equations. He studied continuum mechanics, lunar theory with Clairaut, the three body problem, elasticity, acoustics, the wave theory of light, hydraulics, and music. He laid the foundation of analytical mechanics, especially in his Theory of the Motions of Rigid Bodies (1765).

We owe to Euler the notation $f(x)$ for a function (1734), e for the base of natural logs (1727), i for the square root of -1 (1777), π for pi, $\sum$ for summation (1755), the notation for finite differences Δy and $\Delta^2 y$ and many others.

Let us examine in a little more detail some of Euler's work. Firstly his work in number theory seems to have been stimulated by Goldbach but probably originally came from the interest that the Bernoullis had in that topic. Goldbach asked Euler, in 1729, if he knew of Fermat's conjecture that the numbers $2n+1$ were always prime if n is a power of 2. Euler verified this for $n = 1, 2, 4, 8$ and 16 and, by 1732 at the latest, showed that the next case $2^{32}+1 = 4294967297$ is divisible by 641 and so is not prime. Euler also studied other unproved results of Fermat and in so doing introduced the Euler ϕ function $\phi(n)$, the number of integers k with $1 \le k \le n$ and k coprime to n. He proved another of Fermat's assertions, namely that if a and b are coprime then a^2+b^2 has no divisor of the form $4n-1$, in 1749.

Perhaps the result that brought Euler the most fame in his young days was his solution of what had become known as the Basel problem. This was to find a closed form for the sum of the infinite series $\zeta(2) = \sum(1/n^2)$, a problem which had defeated many of the top mathematicians including Jacob Bernoulli, Johann Bernoulli and Daniel Bernoulli. The problem had also been studied unsuccessfully by Leibniz, Stirling, de Moivre and others. Euler showed in 1735 that $\zeta(2) = \frac{\pi^2}{6}$ but he went on to prove much more, namely that $\zeta(4) = \pi^4/90, \zeta(6) = \frac{\pi^6}{945}$, $\zeta(8) = \frac{\pi^8}{9450}, \zeta(10) = \frac{pi^{10}}{93555}$ and $\zeta(12) = \frac{691\pi^{12}}{638512875}$. In 1737 he proved the connection of the zeta function with the series of prime numbers giving the famous relation

$$\zeta(s) = \sum(1/n^s) = \prod(1-p^{-s})^{-1}.$$

Here the sum is over all natural numbers n while the product is over all prime numbers.

By 1739 Euler had found the rational coefficients C in $\zeta(2n) = C\pi^{2n}$ in terms of the Bernoulli numbers.

Other work done by Euler on infinite series included the introduction of his famous Euler's constant γ, in 1735, which he showed to be the limit of

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+1/n-\log_e n$$

as n tends to infinity. He calculated the constant γ to 16 decimal places. Euler also studied Fourier series and in 1744 he was the first to express an algebraic function by such a series when he gave the result

$$\frac{\pi}{2} - \frac{x}{2} = \sin x + \frac{\sin 2x}{2} + \frac{\sin 3x}{3} + \dots$$

in a letter to Goldbach. Like most of Euler's work there was a fair time delay before the results were published; this result was not published until 1755.

Euler wrote to James Stirling on 8 June 1736 telling him about his results on summing reciprocals of powers, the harmonic series and Euler's constant and other results on series. In particular he wrote:

Concerning the summation of very slowly converging series, in the past year I have lectured to our Academy on a special method of which I have given the sums of very many series sufficiently accurately and with very little effort.

He then goes on to describe what is now called the Euler-Maclaurin summation formula. Two years later Stirling replied telling Euler that Maclaurin:

... will be publishing a book on fluxions. ... he has two theorems for summing series by means of derivatives of the terms, one of which is the self-same result that you sent me.

Euler replied:

... I have very little desire for anything to be detracted from the fame of the celebrated Mr Maclaurin since he probably came upon the same theorem for summing series before me, and consequently deserves to be named as its first discoverer. For I found that theorem about four years ago, at which time I also described its proof and application in greater detail to our Academy.

Some of Euler's number theory results have been mentioned above. Further important results in number theory by Euler included his proof of Fermat's Last Theorem for the case of $n = 3$. Perhaps more significant than the result here was the fact that he introduced a proof involving numbers of the form $a + b\sqrt{-3}$ for integers a and b. Although there were problems with his approach this eventually led to Kummer's major work on Fermat's Last Theorem and to the introduction of the concept of a ring.

One could claim that mathematical analysis began with Euler. In 1748 in Introductio in analysin infinitorum Euler made ideas of Johann Bernoulli more precise in defining a function, and he stated that mathematical analysis was the study of functions. This work bases the calculus on the theory of elementary functions rather than on geometric curves, as had been done previously. Also in this work Euler gave the formula

$$e^{ix} = \cos x + i \sin x$$

.

In Introductio in analysin infinitorum Euler dealt with logarithms of a variable taking only positive values although he had discovered the formula

$$\ln(-1) = \pi i$$

in 1727. He published his full theory of logarithms of complex numbers in 1751.

Analytic functions of a complex variable were investigated by Euler in a number of different contexts, including the study of orthogonal trajectories and cartography. He

discovered the Cauchy-Riemann equations in 1777, although d'Alembert had discovered them in 1752 while investigating hydrodynamics.

In 1755 Euler published Institutiones calculi differentialis which begins with a study of the calculus of finite differences. The work makes a thorough investigation of how differentiation behaves under substitutions.

In Institutiones calculi integralis (1768-70) Euler made a thorough investigation of integrals which can be expressed in terms of elementary functions. He also studied beta and gamma functions, which he had introduced first in 1729. Legendre called these 'Eulerian integrals of the first and second kind' respectively while they were given the names beta function and gamma function by Binet and Gauss respectively. As well as investigating double integrals, Euler considered ordinary and partial differential equations in this work.

The calculus of variations is another area in which Euler made fundamental discoveries. His work Methodus inveniendi lineas curvas ... published in 1740 began the proper study of the calculus of variations. In [12] it is noted that Carathéodory considered this as:

... one of the most beautiful mathematical works ever written.

Problems in mathematical physics had led Euler to a wide study of differential equations. He considered linear equations with constant coefficients, second order differential equations with variable coefficients, power series solutions of differential equations, a method of variation of constants, integrating factors, a method of approximating solutions, and many others. When considering vibrating membranes, Euler was led to the Bessel equation which he solved by introducing Bessel functions.

Euler made substantial contributions to differential geometry, investigating the theory of surfaces and curvature of surfaces. Many unpublished results by Euler in this area were rediscovered by Gauss. Other geometric investigations led him to fundamental ideas in topology such as the Euler characteristic of a polyhedron.

In 1736 Euler published Mechanica which provided a major advance in mechanics. As Yushkevich wrote:

The distinguishing feature of Euler's investigations in mechanics as compared to those of his predecessors is the systematic and successful application of analysis. Previously the methods of mechanics had been mostly synthetic and geometrical; they demanded too individual an approach to separate problems. Euler was the first to appreciate the importance of introducing uniform analytic methods into mechanics, thus enabling its problems to be solved in a clear and direct way.

In Mechanica Euler considered the motion of a point mass both in a vacuum and in a resisting medium. He analysed the motion of a point mass under a central force and also considered the motion of a point mass on a surface. In this latter topic he had to solve various problems of differential geometry and geodesics.

Mechanica was followed by another important work in rational mechanics, this time Euler's two volume work on naval science. D. cameron wrote:

Outstanding in both theoretical and applied mechanics, it addresses Euler's intense occupation with the problem of ship propulsion. It applies variational principles to determine the optimal ship design and first established the principles of hydrostatics ... Euler here also begins developing the kinematics and dynamics of rigid bodies,

introducing in part the differential equations for their motion.

Of course hydrostatics had been studied since Archimedes, but Euler gave a definitive version.

In 1765 Euler published another major work on mechanics Theoria motus corporum solidorum in which he decomposed the motion of a solid into a rectilinear motion and a rotational motion. He considered the Euler angles and studied rotational problems which were motivated by the problem of the precession of the equinoxes.

Euler's work on fluid mechanics is also quite remarkable. He published a number of major pieces of work through the 1750s setting up the main formulae for the topic, the continuity equation, the Laplace velocity potential equation, and the Euler equations for the motion of an inviscid incompressible fluid. In 1752 he wrote:

However sublime are the researches on fluids which we owe to Messrs Bernoulli, Clairaut and d'Alembert, they flow so naturally from my two general formulae that one cannot sufficiently admire this accord of their profound meditations with the simplicity of the principles from which I have drawn my two equations ...

Euler contributed to knowledge in many other areas, and in all of them he employed his mathematical knowledge and skill. He did important work in astronomy, theory of music and cartography.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/)

2.15. Problemas

1. Calcúlense todos los automorfismos de anillos de

   a) $\mathbb{Z}$.

   b) $\mathbb{Q}$.

   c) $\mathbb{R}$.

2. Pruébese que $\mathbb{R}[x]/(x^2+1)$ es un anillo isomorfo a $\mathbb{C}$.

3. Sea A un anillo, $a \in A$ y $p(x) \in A[x]$. Pruébese que $p(a) = 0$ si y sólo si $p(x)$ es múltiplo de $x-a$. Pruébese que $A[x]/(x-a) \simeq A$.

4. Pruébese que $\mathbb{R}[x]/((x^2+1)\cdot(x^2-1)) \simeq \mathbb{C} \times \mathbb{R} \times \mathbb{R}$.

5. Sea $I \subseteq A$, $J \subseteq B$ dos ideales. Pruébese que $I \times J \subseteq A \times B$ es un ideal. Pruébese que $(A \times B)/I \times J \simeq A/I \times B/J$.

6. Sea (A,δ) un anillo euclídeo y A^* los invertibles de A. Sea $n = \text{mín}\{\delta(a),$ para $a \in A\backslash A^*$ y no nulo$\}$. Pruébese que si $\delta(a) = n$ entonces a es irreducible.

7. Sea A un anillo y $\delta' \colon A\backslash\{0\} \to \mathbb{N}$ una aplicación que cumple: para cada $a \in A$ y $b \in A$ no nulo, existen $c, r \in A$, de modo que $a = bc + r$, y r es nulo ó $\delta'(r) < \delta'(b)$. Sea $\delta \colon A\backslash\{0\} \to \mathbb{N}$ definida por $\delta(a) := \text{mín}\{\delta'(ab)$, con $b \in A\backslash\{0\}\}$. Pruébese que (A,δ) es un anillo euclídeo.

8. Pruébese que $\sqrt{2} \notin \mathbb{Q}$.

9. Calcúlese el mínimo común múltiplo de los polinomios $x^4+x^3+x-1, x^4+x^3+2x^2+x+1 \in \mathbb{Q}[x]$.

10. Calcúlese el inverso de $\bar{7} \in \mathbb{Z}/982\mathbb{Z}$.

11. Calcúlese el inverso de $\overline{1+x+x^2} \in \mathbb{Q}[x]/(x^3-2)$. Calcúlese el inverso de $1+\sqrt[3]{2}+\sqrt[3]{2}^2$ (expresado como polinomio en $\sqrt[3]{2}$).

12. P ruébese que la aplicación :

$$(\mathbb{Z}/n\mathbb{Z})^* \to Aut_{grp}(\mathbb{Z}/n\mathbb{Z}),\ \bar{m} \mapsto h_{\bar{m}},$$

donde $h_{\bar{m}}(\bar{i}) := \bar{m} \cdot \bar{i}$, es un isomorfismo.

13. Sea A un anillo.

   a) Sea $p(x,y) \in A[x,y]$. Pruébese que $p(x,x) = 0$ si y sólo si $p(x,y)$ es un múltiplo de $x-y$.

   b) Pruébese que $A[x,y]/(x-y) = A[x]$.

14. Pruébese la igualdad

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i>j}(x_i - x_j)$$

15. Sean K y K' dos k-extensiones de cuerpos. Existe una k-extensión de cuerpos L que contiene a K y K'.

16. Sean $p(x), q(x) \in \mathbb{Q}[x]$. Pruébese que el máximo común divisor de $p(x)$ y $q(x)$ en $\mathbb{Q}[x]$ es igual al máximo común divisor de $p(x)$ y $q(x)$ en $\mathbb{R}[x]$.

17. Sean $p \in \mathbb{N}$ un número primo impar y $a \in \mathbb{N}$ no divisible por p. Pruébese que existe $b \in \mathbb{N}$ tal que $a = b^2 \mod p$ si y sólo si $a^{\frac{p-1}{2}} = 1 \mod p$.

18. Pruébese que *un número primo $p \in \mathbb{Z}$ descompone en suma de dos cuadrados perfectos si y sólo si p no es irreducible en $\mathbb{Z}[i]$*. Pruébese que p descompone en suma de dos cuadrados perfectos si y sólo si $p \equiv 1 \mod 4$ ó $p = 2$..

19. Resuélvase la ecuación diofántica

$$a^2 + b^2 = 2178$$

20. Prúebese que el anillo de los enteros de Kummer $\mathbb{Z}[e^{\frac{2\pi i}{3}}] := \{a + be^{\frac{2\pi i}{3}} \in \mathbb{C},\ \forall a, b \in \mathbb{Z}\}$ es un anillo euclídeo.

21. Sea A un anillo noetheriano íntegro. Probar que A es un dominio de ideales principales si y sólo si todo ideal maximal de A es principal.

22. Sea $p(x) = x^4 + 4x^3 + 3x^2 + 2x + 3$.

    a) Descompón en factores irreducibles la reducción módulo 2 de $p(x)$.

    b) Descompón en factores irreducibles la reducción módulo 3 de $p(x)$.

    c) Descompón $p(x)$ en factores irreducibles en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.

23. (Criterio de Nietsnesie) Sea $a_0 + a_1 x + \cdots + a_n x^n$ un polinomio no constante con coeficientes enteros. Si sus coeficientes no admiten factores primos comunes y existe un número primo p que divide a $a_1, \ldots, a_n$ y p^2 no divide a a_n, entonces el polinomio es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.

24. Sea $p(x)$ un polinomio con coeficientes racionales. Prueba que si $\sqrt{2}$ es raíz de $p(x)$, entonces $p(x)$ es múltiplo de $x^2 - 2$, y que si $\sqrt[3]{2}$ es raíz de $p(x)$, entonces $p(x)$ es múltiplo de $x^3 - 2$.

25. Pruébese que $n = \sum_{d|n} \phi(d)$.

26. Pruébese que un grupo finito es cíclico si y sólo si para cada divisor d de su orden admite como mucho un subgrupo de orden d.

27. Calcúlese $\int \frac{x^5}{x^4+2x^2+1}\, dx$.

28. Calcúlense $p(t), q(t) \in \mathbb{C}[t]$, tales que

$$\int \frac{\cos(x) \cdot \sin(x)}{\sin(x)^2 \cdot \cos(3x)} \cdot dx = \int \frac{p(t)}{q(t)} \cdot dt,$$

donde $t = e^{ix}$.

CAPÍTULO 3
MÓDULOS

3.1. Introducción

El espacio vectorial es el ejemplo más sencillo y usual de espacio geométrico. Muchos problemas se resuelven linealizándolos, lo que permite aplicarles además la intuición geométrica. Añadamos, que muchas de las estructuras usuales en Matemáticas son estructuras de espacios vectoriales.

Sea A un anillo. Sin precisar, un A-módulo es un A-espacio vectorial, pero donde A es un anillo y no necesariamente un cuerpo. En esta capítulo iniciaremos el estudio de la estructura de módulo sobre un anillo A y veremos que casi todas las definiciones del Álgebra Lineal (subespacios, sistemas generadores, cocientes, sumas y productos directos, etc.) pueden generalizarse para los A-módulos; aunque la frecuente existencia de módulos que no admiten bases introduzca grandes modificaciones en la teoría de módulos. La posibilidad de efectuar estas operaciones (cocientes, sumas directas, etc.) aclara y simplifica muchos enunciados y demostraciones.

Los módulos aparecen también con frecuencia en Matemáticas. Ya veremos que los grupos abelianos y los espacios vectoriales con un endomorfismo lineal son ejemplos de módulos, y que su clasificación es la clasificación de la estructura de módulo.

3.2. Módulos

1. Definición: Sea A un anillo y M un conjunto. Diremos que una operación

$$M \times M \xrightarrow{+} M, (m, m') \mapsto m + m' \text{ y una aplicación } A \times M \dashrightarrow M, (a, m) \mapsto a \cdot m,$$

definen en M una estructura de A-módulo cuando cumplen

1. $(M, +)$ es un grupo conmutativo.
2. $a \cdot (m + n) = a \cdot m + a \cdot n$, para todo $a \in A$ y $m, n \in M$.
3. $(a + b) \cdot m = a \cdot m + b \cdot m$, para todo $a, b \in A$ y $m \in M$.
4. $(ab) \cdot m = a \cdot (b \cdot m)$, para todo $a, b \in A$ y $m \in M$.

5. $1 \cdot m = m$, para todo $m \in M$.

Sea M un A-módulo. Cada elemento $a \in A$ define una aplicación

$$a\cdot\colon M \to M,\ m \mapsto a \cdot m.$$

El segundo punto expresa que $a\cdot$ es morfismo de grupos. En particular, $a \cdot 0 = 0$ y $a \cdot (-m) = -(a \cdot m)$.

Observemos que $0 \cdot m = 0$: $0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m$, luego $0 \cdot m = 0$. Observemos que $(-a) \cdot m = -(a \cdot m)$, para todo $m \in M$: $0 = 0 \cdot m = (a + -a) \cdot m = a \cdot m + (-a) \cdot m$, despejando $(-a) \cdot m = -(a \cdot m)$.

2. Notación: Alguna vez, escribiremos am en vez de $a \cdot m$ por sencillez de escritura.

3. Ejemplos: 1. Todo anillo A es un A-módulo: con la suma definida en A y con el producto por los elementos de A definido en A.

2. Si A es un cuerpo, entonces los A-módulos son los A-espacios vectoriales.

3. Si G es un grupo abeliano, entonces es un $\mathbb{Z}$-módulo de modo natural: $n \cdot g := g + \overset{n}{\ldots} + g$ si $n \in \mathbb{N}^+$, $n \cdot g := (-g) + \overset{-n}{\ldots} + (-g)$ si $-n \in \mathbb{N}^+$, y definimos $0 \cdot g := 0$. Recíprocamente, si G es un $\mathbb{Z}$-módulo, en particular es un grupo abeliano.

4. Si $T\colon E \to E$ es un endomorfismo de k-espacios vectoriales entonces E tiene estructura natural de $k[x]$-módulo: $(\sum \lambda_i x^i) \cdot e := \sum \lambda_i T^i(e)$. Recíprocamente, dado un $k[x]$-módulo E, la aplicación $T\colon E \to E$ definida por $T(e) = x \cdot e$, es un endomorfismo de k-espacios vectoriales.

5. Sea $\{M_i\}_{i\in I}$ una familia de A-módulos con índices en un conjunto I. Su producto directo se denotará $\prod_{i\in I} M_i$, mientras que $\oplus_{i\in I} M_i$ denotará el subconjunto de $\prod_{i\in I} M_i$ formado por los elementos (m_i) que tienen todas sus componentes nulas salvo un número finito de ellas, y se llamará suma directa de los $\{M_i\}_{i\in I}$. Tanto $\prod_{i\in I} M_i$ como $\oplus_{i\in I} M_i$ son A-módulos con la siguiente suma y producto por elementos de A:

$$(m_i)_{i\in I} + (m'_i)_{i\in I} := (m_i + m'_i)_{i\in I}$$
$$a \cdot (m_i)_{i\in I} := (a \cdot m_i)_{i\in I}$$

3.3. Submódulos. Sistema generador. Bases

1. Definición: Un subconjunto N de un A-módulo M, decimos que es un submódulo si con la operación + de M y con la multiplicación $\cdot$ por elementos de A, N es un A-módulo.

2. Ejemplo: Los K-subespacios vectoriales de un K-espacio vectorial E son justamente los K-submódulos de E.

3. Ejemplo: Los ideales de un anillo A son justamente los A-submódulos de A.

4. Ejemplo: $\oplus_{i\in I} M_i$ es un submódulo de $\prod_{i\in I} M_i$

Dado un conjunto $\{M_i\}_{i\in I}$ de submódulos de M, la intersección $\cap_{i\in I}M_i$ es un submódulo de M.

5. Definición: Dado un subconjunto $X \subseteq M$, llamaremos submódulo generado por X y lo denotaremos $\langle X\rangle$, al mínimo submódulo de M que contiene a X.

Se cumple que

$$\langle X\rangle = \{\sum_{i=1}^{n} a_i m_i \in M, \forall\ a_i \in A, m_i \in X, n \in \mathbb{N}\}.$$

Por ejemplo, $\langle m\rangle = \{am \in M : \forall\, a \in A\} =: A\cdot m$.

6. Definición: Diremos que un conjunto de elementos de M, $\{m_i\}_{i\in I}$, es un sistema generador de M si $\langle m_i\rangle_{i\in I} = M$, es decir, para cada $m \in M$ existen $i_1,\dots,i_n \in I$ y $a_{i_1},\dots,a_{i_n} \in A$ de modo que $m = a_{i_1}m_{i_1} + \cdots + a_{i_n}m_{i_n}$.

Evidentemente, todo módulo tiene sistemas generadores, por ejemplo el formado por todos los elementos de M.

7. Definición: Diremos que un módulo M es finito generado si existe un sistema generador de M formado por un número finito de elementos. Diremos que un conjunto de elementos $\{m_i\}_{i\in I}$ es base de M, si es un sistema generador y los elementos son linealmente independientes, es decir, cumplen que siempre que $\sum_i a_i m_i = 0$, entonces $a_i = 0$, para todo i.

8. Ejemplo: Por ejemplo, $\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ es un $\mathbb{Z}$-módulo finito generado, ya que $\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} = \langle(1,0),(0,\bar{1})\rangle$.

9. Definición: Se dice que un módulo es libre si existe una base en el módulo.

En general los módulos no son libres, no tienen bases. Ésta es la gran diferencia de la teoría de módulos con la teoría de espacios vectoriales.

10. Ejemplo: $\mathbb{Z}/2\mathbb{Z}$ no es un $\mathbb{Z}$-módulo libre, porque si $\{\bar{n}_i\}_{i\in I}$ fuese una base, entonces $0 \neq 2\cdot\bar{n}_i = \overline{2\cdot n_i} = 0$, contradicción.

11. Ejemplo: Denotaremos $A^{(I)} = \underset{i\in I}{\oplus} A_i$, siendo $A_i = A$, para todo i. $A^{(I)}$ es un A-módulo libre de base la base estándar: Definamos $1_j := (a_i)_{i\in I}$, con $a_i = 0$ para todo $i \neq j$ y $a_j = 1$. Entonces, $\{1_i\}_{i\in I}$ es una base de $A^{(I)}$.

12. Ejercicio: Dar una base del A-módulo libre $A[x]$.

3.4. Morfismos de módulos

1. Definición: Una aplicación $f : M \to M'$ entre A-módulos M, M', diremos que es un morfismo de A-módulos (o una aplicación A-lineal) si cumple

1. $f(m+n) = f(m) + f(n)$, para todo $m, n \in M$.
2. $f(am) = af(m)$, para todo $a \in A$ y $m \in M$.

Cuando $f : M \to M'$ sea biyectiva diremos que f es un isomorfismo de A-módulos.

2. Ejemplo: Sean G y G' dos grupos abelianos, luego dos $\mathbb{Z}$-módulos. Obviamente $f: G \to G'$ es un morfismo de grupos si y sólo si es un morfismo de $\mathbb{Z}$-módulos, y f es un isomorfismo de grupos si y sólo si f es un isomorfismo de $\mathbb{Z}$-módulos.

3. Definición: Sea $f: M \to M'$ un morfismo de A-módulos. El conjunto

$$\operatorname{Ker} f := \{m \in M : f(m) = 0\}.$$

se denomina núcleo de f.

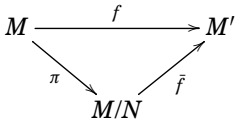
Se cumple que $\operatorname{Ker} f$ es un submódulo de M y que f es inyectiva si y sólo si $\operatorname{Ker} f = 0$. El conjunto de los elementos de la imagen, $\operatorname{Im} f$, forman un submódulo de M'.

Si N es un submódulo de M entonces es un subgrupo conmutativo de M. Por tanto, podemos considerar el grupo cociente M/N, donde

$$M/N = \{\bar{m},\ m \in M,\ \text{de modo que } \bar{m} = \bar{m'} \iff m - m' \in N\}$$

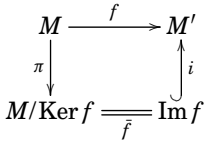
El producto $a \cdot \bar{m} := \overline{a \cdot m}$ dota a M/N de estructura de A-módulo (compruébese) y es la única estructura de A-módulo que podemos definir en M/N, de modo que el morfismo de paso al cociente $M \to M/N$, $m \mapsto \bar{m}$, sea un morfismo de módulos.

4. Teorema: *Sea $f: M \to M'$ un morfismo de A-módulos. Sea $N \subseteq \operatorname{Ker} f$ un A-submódulo. Existe un único morfismo $\bar{f}: M/N \to M'$ (que vendrá definido por $\bar{f}(\bar{m}) = f(m)$) de modo que el diagrama*



es conmutativo, siendo π el morfismo de paso al cociente.

5. Teorema de isomorfía: *Sea $f: M \to M'$ un morfismo de A-módulos. Se cumple que el diagrama*



donde $\pi(m) = \bar{m}$, $\bar{f}(\bar{m}) = f(m)$ (que está bien definida) e $i(m') = m'$, es conmutativo, $\bar{f}$ es un isomorfismo, π es epiyectiva e i inyectiva.

Demostración. Al lector. □

6. Ejemplo: Dado un conjunto $\{M_i\}_{i \in I}$ de submódulos de M denotaremos

$$\sum_{i \in I} M_i = \{m \in M : m = \sum_{i \in I} m_i \text{ con } m_i \in M_i$$

$$\text{nulos para todo } i \in I \text{ salvo un número finito}\},$$

que es el menor submódulo de M que contiene a los submódulos M_i. Diremos que dos submódulos M_1, M_2 de M están en suma directa si $M_1 \cap M_2 = 0$, que equivale a decir que el morfismo $M_1 \oplus M_2 \to M_1 + M_2$, $(m_1, m_2) \mapsto m_1 + m_2$ es un isomorfismo. Se dice que M es la suma directa de dos submódulos M_1, M_2 si $M_1 \cap M_2 = 0$ y $M_1 + M_2 = M$, que equivale a decir que el morfismo $M_1 \oplus M_2 \to M$, $(m_1, m_2) \mapsto m_1 + m_2$ es un isomorfismo.

3.5. Módulos libres

1. Proposición: *Sea $f: M \to N$ un isomorfismo de A-módulos. Si $\{m_i\}_{i\in I}$ es un sistema generador de M, entonces $\{f(m_i)\}_{i\in I}$ es un sistema generador de N. Si $\{m_i\}_{i\in I}$ es una base de M, entonces $\{f(m_i)\}_{i\in I}$ es una base de N.*

Sea $\{m_i\}_{i\in I}$ un conjunto de elementos de M, y definamos el morfismo

$$\phi: A^{(I)} \to M, (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i m_i$$

Se cumple que ϕ es epiyectivo si y sólo si $\{m_i\}_{i\in I}$ es un sistema generador de M. Como en todo módulo existen sistema generadores, todo módulo es isomorfo a un cociente de un libre.

Observemos que ϕ es inyectivo si y sólo si los elementos $\{m_i\}_{i\in I}$ son linealmente independientes. Por tanto, ϕ es isomorfismo si y sólo si $\{m_i\}_{i\in I}$ es una base de M, y un módulo es libre si y sólo si es isomorfo a un $A^{(I)}$.

2. Definición: Si un A-módulo L es isomorfo a A^n (con $n \in \mathbb{N}$) se dice que L es un A-módulo libre de rango n.

3. Ejemplo: Los k-espacios vectoriales de dimensión n son k-módulos libres de rango n.

4. Notación: Sea M un A-módulo e $I \subseteq A$ un ideal. Denotaremos $I \cdot M$ como el mínimo submódulo de M que contiene a $\{i \cdot m : \forall\, i \in I, \forall\, m \in M\}$. Es fácil comprobar que

$$I \cdot M := \{i_1 \cdot m_1 + \cdots + i_n \cdot m_n : \forall\, i_j \in I, \forall\, m_j \in M, \forall\, n > 0\}.$$

5. Proposición: *Si $A^n \simeq A^m$ entonces $n = m$ ($A \neq 0$).*

Demostración. Sea $\mathfrak{m} \subset A$ un ideal maximal. Entonces,

$$A^n/\mathfrak{m}\cdot A^n = (A \overset{n}{\cdots} \oplus A)/(\mathfrak{m} \overset{n}{\cdots} \oplus \mathfrak{m}) = A/\mathfrak{m} \overset{n}{\cdots} \oplus A/\mathfrak{m}.$$

Obviamente, $A^n/\mathfrak{m}\cdot A^n \simeq A^m/\mathfrak{m}\cdot A^m$. Por tanto,

$$n = \dim_{A/\mathfrak{m}} A^n/\mathfrak{m}\cdot A^n = \dim_{A/\mathfrak{m}} A^m/\mathfrak{m}\cdot A^m = m.$$

□

6. Definición: Sean L y L' dos A-módulos libres de bases $\{u_1,\ldots,u_n\}$ y $\{u'_1,\ldots,u'_m\}$, respectivamente. Sea $f: L \to L'$ un morfismo de A-módulos y sea

$$f(u_j) = \sum_{i=1}^{m} a_{ij} u'_i, \text{ para } a_{ij} \in A \text{ únicos.}$$

Diremos que $(a_{ij}) \in A^{m\times n}$ es la matriz asociada a f en las bases $\{u_j\}$ de L y $\{u'_i\}$ de L'.

Tenemos una correspondencia biunívoca entre el conjunto de los morfismos de módulos de L en L' y el conjunto de las matrices con coeficientes en A, $(a_{ij}) \in A^{m\times n}$.

Sean L, L' y L'' A-módulos libres de bases $\{u_1,\dots,u_n\}$, $\{u'_1,\dots,u'_m\}$ y $\{u''_1,\dots,u''_r\}$. Sean $f: L \to L'$ y $g: L' \to L''$ morfismos de A-módulos, de matrices en las bases consideradas (a_{ij}) y (b_{rs}). Entonces la matriz de $g \circ f: L \to L''$ en las bases consideradas es igual al producto de matrices (usual)

$$(b_{rs}) \cdot (a_{ij}) = (c_{uv}),$$

con $c_{uv} = \sum_{l=1}^{m} b_{ul} \cdot a_{lv}$.

3.6. Presentación de un módulo por módulos libres

Sea M un A-módulo cualquiera. Por desgracia, no podemos afirmar que sea libre. Sólo podemos afirmar la existencia de sistemas de generadores $\{m_i\}_{i\in I}$, luego la existencia de epimorfismos $A^{(I)} \to M$, $(a_i)_{i\in I} \mapsto \sum_i a_i m_i$.

Consideremos un epimorfismo $\pi: A^{(I)} \to M$. Igualmente, podemos definir un epimorfismo $\pi': A^{(J)} \to \operatorname{Ker}\pi$. Componiendo este último morfismo con la inclusión natural $\operatorname{Ker}\pi \overset{i}{\hookrightarrow} A^{(I)}$, tenemos un morfismo natural $f = i \circ \pi': A^{(J)} \to A^{(I)}$. Consideremos la sucesión de morfismos

$$A^{(J)} \overset{f}{\to} A^{(I)} \overset{\pi}{\to} M.$$

Recordemos que π es epiyectiva, que $\operatorname{Im} f = \operatorname{Ker}\pi$ y que $M \simeq A^{(I)}/\operatorname{Ker}\pi$. Luego,

$$\boxed{M \simeq A^{(I)}/\operatorname{Im} f}$$

Por tanto, el estudio de M se reduce al estudio de f, que es una aplicación A-lineal entre módulos libres.

1. Lema: *Sea M un A-módulo y $N \subseteq M$ un submódulo. Si N y M/N son A-módulos finito generados, entonces M es un A-módulo finito generado.*

Demostración. Escribamos, $N = \langle n_1,\dots,n_r\rangle$ y $M/N = \langle \bar{n}_{r+1},\dots,\bar{n}_s\rangle$. Veamos que $M = \langle n_1,\dots,n_s\rangle$: Dado $m \in M$, tenemos que $\bar{m} = \sum_{i=r+1}^{s} a_i \cdot \bar{n}_i$, para ciertos $a_i \in A$. Luego, $\bar{m} - \sum_{i=r+1}^{s} a_i \cdot \bar{n}_i = 0$ y $m - \sum_{i=r+1}^{s} a_i \cdot n_i \in N$. Por tanto, $m - \sum_{i=r+1}^{s} a_i n_i = \sum_{j=1}^{r} a_j n_j$ para ciertos $a_j \in A$, y por tanto

$$m = \sum_{k=1}^{s} a_k n_k.$$

□

2. Proposición: *Sea A un anillo noetheriano y M un A-módulo finito generado. Se cumple que todo submódulo $N \subseteq M$ es finito generado.*

Demostración. Supongamos $M = \langle m\rangle$. Consideremos el epimorfismo

$$\pi: A \to M, a \mapsto a \cdot m.$$

$\pi^{-1}(N)$ es un submódulo de A, luego es finito generado. Entonces, $N = \pi(\pi^{-1}(N))$ es finito generado.

Tenemos $M = \langle m_1, \dots, m_r \rangle$. Demostremos la proposición por inducción sobre r. Si $r = 1$, lo acabamos de demostrar. Supongamos que el teorema es cierto para $1, \dots, r-1$. Sea $\pi\colon M \to M/\langle m_r \rangle$ el morfismo de paso al cociente. $\pi(N)$ es un submódulo de $M/\langle m_r \rangle = \langle \bar{m}_1, \dots, \bar{m}_{r-1} \rangle$, luego por hipótesis de inducción $\pi(N)$ es finito generado. Consideremos el epimorfismo

$$\pi_{|N}\colon N \to \pi(N),\ n \mapsto \pi(n).$$

Obviamente,

$$\operatorname{Ker} \pi_{|N} = \operatorname{Ker} \pi \cap N \subseteq \operatorname{Ker} \pi = \langle m_r \rangle$$

Por tanto, $\operatorname{Ker} \pi_{|N}$ es finito generado. $N/\operatorname{Ker} \pi_{|N} \simeq \pi(N)$ es finito generado. Por el lema anterior N es finito generado.

□

3. Teorema: *Sea A un anillo noetheriano y M un A-módulo finito generado. Existe un morfismo de A-módulos $f\colon A^r \to A^s$ (con $r, s \in \mathbb{N}$) de modo que $A^s/\operatorname{Im} f \simeq M$, es decir, "existe una presentación de M por módulos libres finito generados".*

Demostración. Escribamos $M = \langle m_1, \dots, m_s \rangle$. Consideremos el epimorfismo $\pi\colon A^s \to M, (a_i) \mapsto \sum_i a_i \cdot m_i$. $\operatorname{Ker} \pi$ es un submódulo de A^s, luego es finito generado. Escribamos $\operatorname{Ker} \pi = \langle n_1, \dots, n_r \rangle$ y consideremos el epimorfismo $g\colon A^r \to \operatorname{Ker} \pi, (a_i) \mapsto \sum_i a_i n_i$ y sea $f\colon A^r \to A^s$ la composición de los morfismos $A^r \xrightarrow{g} \operatorname{Ker} \pi \hookrightarrow A^s$. Tenemos que $\operatorname{Im} f = \operatorname{Im} g = \operatorname{Ker} \pi$. Por tanto, $A^s/\operatorname{Im} f = A^s/\operatorname{Ker} \pi \simeq M$. □

Cuando A sea un anillo euclídeo, veremos cómo puede calcularse f y cómo encontrar bases donde f "diagonalice", y con ello clasificaremos los A-módulos finito generados.

3.7. Teorema de descomposición

Sea M un A-módulo y $a \in A$. Denotaremos por $a\cdot$ el endomorfismo A-lineal

$$a\cdot\colon M \to M, m \mapsto a \cdot m.$$

1. Lema: *Sea M un A-módulo. Sea $pq \in A$, siendo $p, q \in A$ primos entre sí, es decir, $(p, q) = A$. Entonces,* $\operatorname{Ker} pq\cdot$ *descompone de modo único en suma directa de un submódulo anulado por p y otro submódulo anulado por q, en concreto*

$$\operatorname{Ker} pq\cdot = \operatorname{Ker} p\cdot \oplus \operatorname{Ker} q\cdot.$$

Demostración. Sean $\lambda, \mu \in A$ tales que

$$\lambda p + \mu q = 1.$$

Por tanto, cada $m \in \operatorname{Ker} pq\cdot$ cumple $\lambda pm + \mu qm = 1 \cdot m = m$, y $\lambda pm \in \operatorname{Ker} q\cdot$ y $\mu qm \in \operatorname{Ker} p\cdot$. Por tanto, $\operatorname{Ker} pq\cdot = \operatorname{Ker} p\cdot + \operatorname{Ker} q\cdot$.

$\operatorname{Ker} p\cdot \cap \operatorname{Ker} q\cdot = 0$: Si $m \in \operatorname{Ker} p\cdot \cap \operatorname{Ker} q\cdot$ entonces $m = \lambda pm + \mu qm = 0 + 0 = 0$.

Si $\operatorname{Ker} pq\cdot = M_1 \oplus M_2$, $pM_1 = 0$ y $qM_2 = 0$, entonces $M_1 \subseteq \operatorname{Ker} p\cdot$ y $M_2 \subseteq \operatorname{Ker} q\cdot$ y de las inclusiones

$$\operatorname{Ker} pq\cdot = M_1 \oplus M_2 \subseteq \operatorname{Ker} p\cdot \oplus \operatorname{Ker} q\cdot = \operatorname{Ker} pq\cdot$$

obtenemos que $M_1 = \operatorname{Ker} p\cdot$ y $M_2 = \operatorname{Ker} q\cdot$.

□

Para los cálculos será conveniente conocer la siguiente proposición.

2. Proposición: *Sean $p, q \in A$ primos entre sí y M un A-módulo anulado por $p\cdot q$. Se cumple que* $\operatorname{Ker} p\cdot = q\cdot M$.

Demostración. Obviamente $q\cdot M \subseteq \operatorname{Ker} p\cdot$. Sean $\lambda, \mu \in A$ tales que $\lambda p + \mu q = 1$. Dado $m \in \operatorname{Ker} p\cdot$ tenemos que $m = (\lambda p + \mu q)\cdot m = \mu q \cdot m \in q\cdot M$, luego $\operatorname{Ker} p\cdot \subseteq q\cdot M$ y $\operatorname{Ker} p\cdot = q\cdot M$. □

3. Teorema de descomposición Sea M un A-módulo y $a = a_1 \cdots a_s \in A$, con a_i primo con a_j para todo $i \neq j$. Entonces, $\operatorname{Ker} a\cdot$ descompone de modo único en suma directa de submódulos M_i anulados por a_i, en concreto

$$\operatorname{Ker}(a_1 \cdots a_s)\cdot = \operatorname{Ker} a_1\cdot \oplus \cdots \oplus \operatorname{Ker} a_s\cdot .$$

Demostración. Si a es primo con b, y a es primo con c, entonces a es primo con bc: Tenemos que $(a) + (c) = A$, entonces $(ba) + (bc) = (b)$ y

$$A = (a) + (b) = (a) + (ba) + (bc) = (a) + (bc).$$

Recurrentemente, obtenemos que a_1 es primo con $a_2 \cdots a_s$. Por el lema anterior,

$$\operatorname{Ker}(a_1 \cdots a_s)\cdot = \operatorname{Ker} a_1\cdot \oplus \operatorname{Ker}(a_2 \cdots a_s\cdot) = \cdots = \operatorname{Ker} a_1\cdot \oplus \cdots \oplus \operatorname{Ker} a_s\cdot$$

Si $\operatorname{Ker} a\cdot = \oplus_i M_i$, de modo que $a_i M_i = 0$, entonces evidentemente $M_i \subseteq \operatorname{Ker} a_i\cdot$ y de nuevo obtenemos que $M_i = \operatorname{Ker} a_i\cdot$.

□

4. Corolario: *Sea $T\colon E \to E$ un endomorfismo k-lineal. Sea $p(x) = p_1(x)\cdots p_r(x) \in k[x]$, con $p_i(x)$ primo con $p_j(x)$, para todo $i \neq j$. Entonces,*

$$\operatorname{Ker} p(T) = \operatorname{Ker} p_1(T) \oplus \cdots \oplus \operatorname{Ker} p_r(T).$$

Demostración. E es un $k[x]$-módulo: $q(T)(e) = q(x)\cdot e$, para todo $q(x) \in k[x]$. Entonces,

$$\operatorname{Ker} p(T) = \operatorname{Ker} p(x)\cdot \overset{3.7.3}{=} \operatorname{Ker} p_1(x)\cdot \oplus \cdots \oplus \operatorname{Ker} p_r(x)\cdot = \operatorname{Ker} p_1(T) \oplus \cdots \oplus \operatorname{Ker} p_r(T).$$

□

3.7.1. Ecuaciones diferenciales con coeficientes constantes

Sea F el $\mathbb{C}$-espacio vectorial de todas las funciones reales con valores complejos infinitamente diferenciables. Se designa por $D: F \to F$, $D(f) := f'$ el operador derivada. Es claro que D es un endomorfismo $\mathbb{C}$-lineal de F.

1. Sea $p(x) \in \mathbb{C}[x]$. Se cumple la fórmula de conmutación

$$\boxed{p(D)(e^{\alpha x} \cdot f(x)) = e^{\alpha x} p(D+\alpha) f(x)}$$

para $f(x) \in F$, $\alpha \in \mathbb{C}$ y $p(x) \in \mathbb{C}[x]$: En efecto, $D(e^{\alpha x} \cdot f) = \alpha e^{\alpha x} f + e^{\alpha x} Df = e^{\alpha x} \cdot (D+\alpha) f$. Por recurrencia,

$$\begin{aligned} D^n(e^{\alpha x} f) &= D^{n-1}(D(e^{\alpha x} f)) = D^{n-1}(e^{\alpha x}(D+\alpha) f) = \cdots = e^{\alpha x}(D+\alpha)^{n-1}(D+\alpha) f \\ &= e^{\alpha x}(D+\alpha)^n f. \end{aligned}$$

Luego, $(\sum_i \lambda_i D^i)(e^{\alpha x} f) = \sum_i \lambda_i (D^i(e^{\alpha x} f)) = \sum_i \lambda_i e^{\alpha x}(D+\alpha)^i f = e^{\alpha x}(\sum_i \lambda_i (D+\alpha)^i f)$.

2. Se cumple que $\operatorname{Ker} D^r = \{p(x) \in \mathbb{C}[x],\ \operatorname{gr}(p(x)) < r\}$: Procedamos por inducción sobre r. Si $r = 1$, obviamente $\operatorname{Ker} D = \mathbb{C}$. Supongamos que la afirmación es cierta para $1, \cdots, r-1$. Si $f \in \operatorname{Ker} D^r$, entonces $D^{r-1}(Df) = 0$ y por hipótesis de inducción $Df = \sum_{i=0}^{r-2} \lambda_i x^i$. Por tanto, $f = \int \sum_{i=0}^{r-2} \lambda_i x^i dx$ y f es un polinomio de grado menor que r. Recíprocamente, es obvio que $\{p(x) \in \mathbb{C}[x],\ \operatorname{gr}(p(x)) < r\} \subseteq \operatorname{Ker} D^r$.

3. Se cumple que $\operatorname{Ker}(D-\alpha)^r = e^{\alpha x} \cdot \{p(x) \in \mathbb{C}[x],\ \operatorname{gr}(p(x)) < r\}$: $f \in \operatorname{Ker}(D-\alpha)^r$ si y sólo si $e^{-\alpha x} \cdot f \in \operatorname{Ker} D^r$, por la fórmula de conmutación. Por último, $e^{-\alpha x} \cdot f \in \operatorname{Ker} D^r$ si y sólo si $f \in e^{\alpha x} \cdot \operatorname{Ker} D^r = e^{\alpha x} \cdot \{p(x) \in \mathbb{C}[x],\ \operatorname{gr}(p(x)) < r\}$.

4. Si $p(x) = (x-\alpha_1)^{n_1} \cdots (x-\alpha_r)^{n_r}$, por el corolario 3.7.4,

$$\begin{aligned} \operatorname{Ker} p(D) &= \operatorname{Ker}(D-\alpha_1)^{n_1} \oplus \cdots \oplus \operatorname{Ker}(D-\alpha_r)^{n_r} \\ &= e^{\alpha_1 x} \cdot \{p(x) \in \mathbb{C}[x],\ \operatorname{gr}(p(x)) < n_1\} \oplus \cdots \oplus e^{\alpha_r x} \cdot \{p(x) \in \mathbb{C}[x],\ \operatorname{gr}(p(x)) < n_r\}. \end{aligned}$$

5. Ejercicio: Resuélvase la ecuación diferencial $y'' + y = 0$.

6. Ejercicio: Resuélvase la ecuación diferencial: $y'''' - 2y''' + 2y'' = 0$,

7. Dada una ecuación diferencial $p(D)y = z$. Si y_0 es una solución particular, es decir, $p(D)y_0 = z$, entonces $y_0 + \operatorname{Ker} p(D)$ es el conjunto de todas las soluciones de la ecuación diferencial.

8. Consideremos la ecuación diferencial $p(D)y = z$, con $z \in F$. Supongamos que existe un polinomio $q(x)$ primo con $p(x)$ de modo que $q(D)z = 0$. Entonces, existen $\lambda(x), \mu(x) \in \mathbb{C}[x]$, de modo que $\lambda(x)p(x) + \mu(x)q(x) = 1$. Por tanto,

$$z = (\lambda(x)p(x) + \mu(x)q(x))z = \lambda(D)p(D)z + \mu(D)q(D)z = \lambda(D)p(D)z = p(D)(\lambda(D)z).$$

Luego, $y = \lambda(D)z$ es una solucion particular de la ecuación diferencial.

9. Ejercicio: Resuélvase la ecuación $y^{(n} - y = x^n$.

10. Dada la ecuación diferencial $p(D)y = z$, escribamos formalmente $y = \frac{1}{p(D)} z$. Si $p(x) = (x-\alpha_1)^{n_1} \cdots (x-\alpha_r)^{n_r}$, tendremos que

$$\frac{1}{p(x)} = \sum_{j=1}^{r} \sum_{k=1}^{n_j} \frac{\lambda_{jk}}{(x-\alpha_j)^k}.$$

Luego,

$$y = \frac{1}{p(D)}z = (\sum_{j=1}^{r}\sum_{k=1}^{n_j}\frac{\lambda_{jk}}{(D-\alpha_j)^k})z = \sum_{j=1}^{r}\sum_{k=1}^{n_j}(\frac{\lambda_{jk}}{(D-\alpha_j)^k}z) = \sum_{j=1}^{r}\sum_{k=1}^{n_j}(\frac{\lambda_{jk}}{(D-\alpha_j)^k}e^{\alpha_j x}e^{-\alpha_j x}z)$$
$$= \sum_{j=1}^{r}\sum_{k=1}^{n_j}(\frac{\lambda_{jk}e^{\alpha_j x}}{D^k}e^{-\alpha_j x}z) = \sum_{j=1}^{r}\sum_{k=1}^{n_j}\lambda_{jk}e^{\alpha_j x}\int\overset{k}{\cdots}\int e^{-\alpha_j x}z.$$

11. Ejercicio: Resuélvase $y'' - y = senx$.

3.7.2. Ecuaciones en diferencias finitas

Sea $Suc(\mathbb{C}) = \{(a_n)_{n\in\mathbb{N}}, a_n \in \mathbb{C}\}$ el $\mathbb{C}$-espacio vectorial de las sucesiones de números complejos. Consideremos el "operador siguiente" $\nabla\colon Suc(\mathbb{C}) \to Suc(\mathbb{C})$, que es la aplicación $\mathbb{C}$-lineal definida por $\nabla(a_n) = (a'_n)$, donde $a'_n := a_{n+1}$. Sea $\Delta := \nabla - \mathrm{Id}$, el "operador diferencia".

12. Fórmula de conmutación: Sea $p(x) \in \mathbb{C}[x]$ y (a_n) una sucesión de números complejos. Entonces,

$$p(\nabla)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot p(\alpha\nabla)(a_n).$$

Demostración. En efecto, $\nabla((\alpha^n)\cdot(a_n)) = \nabla(\alpha^n \cdot a_n) = (\alpha^{n+1}\cdot a_{n+1}) = (\alpha^n)\cdot(\alpha\cdot\nabla)(a_n)$. Por tanto, $\nabla^2((\alpha^n)\cdot(a_n)) = \nabla((\alpha^n)\cdot(\alpha\nabla)(a_n)) = (\alpha^n)\cdot(\alpha\cdot\nabla)^2(a_n)$. Recurrrentemente, $\nabla^r((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot(\alpha\nabla)^r(a_n)$ y $p(\nabla)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot p(\alpha\nabla)(a_n)$. □

Por lo tanto,

$$\boxed{p(\nabla-\alpha)((\alpha^n)\cdot(a_n)) = (\alpha^n)\cdot p(\alpha\cdot\Delta)(a_n)}$$

13. Proposición: *Se cumple que* $\{(1),(n),\ldots,(n^{r-1})\}$ *es una base de* $\mathrm{Ker}\,\Delta^r$

Demostración. Obviamente, $\mathrm{Ker}\,\Delta = \langle(1)\rangle$. Si $p(n)$ es un polinomio de grado s, es fácil ver que $\Delta(p(n))$ es un polinomio de grado $s-1$. Por tanto, $\{(1),(n),\ldots,(n^{r-1})\} \subseteq \mathrm{Ker}\,\Delta^r$. Consideremos la aplicación lineal

$$\Delta\colon \mathrm{Ker}\,\Delta^s \to \mathrm{Ker}\,\Delta^{s-1},\ (a_n) \mapsto \Delta(a_n),$$

cuyo núcleo es $\mathrm{Ker}\,\Delta = \langle(1)\rangle$. Por tanto, $\dim_{\mathbb{C}}\mathrm{Ker}\,\Delta^s \le \dim_{\mathbb{C}}\mathrm{Ker}\,\Delta^{s-1} + 1$. Recurrentemente, obtenemos que $\dim_{\mathbb{C}}\mathrm{Ker}\,\Delta^r \le r$. Por dimensiones $\langle(1),(n),\ldots,(n^{r-1})\rangle = \mathrm{Ker}\,\Delta^r$. □

14. Proposición: *Se cumple que* $\mathrm{Ker}(\nabla-\alpha)^r = (\alpha^n)\cdot\{(a_0 + a_1 n + \cdots + a_{r-1}n^{r-1}),\ a_i \in \mathbb{C},\ \forall i\}$, *para* $\alpha \neq 0$

Demostración. Tenemos que

$$(\nabla-\alpha)^r(a_n) = (\nabla-\alpha)^r((\alpha^n)\cdot(\alpha^{-n})\cdot(a_n)) = (\alpha^n)\cdot(\alpha\cdot\Delta)^r((\alpha^{-n})\cdot(a_n)).$$

Luego, $(\nabla-\alpha)^r(a_n) = 0$ si y sólo si $\Delta^r((\alpha^{-n})\cdot(a_n)) = 0$, es decir, $(\alpha^{-n})\cdot(a_n) \in \mathrm{Ker}\,\Delta^r$, o equivalentemente $(a_n) \in (\alpha^n)\cdot\mathrm{Ker}\,\Delta^r$. □

Por último, dado $p(x) = (x-\alpha_1)^{n_1}\cdots(x-\alpha_r)^{n_r}$, $\alpha_i \neq \alpha_j$ para todo $i \neq j$, por el corolario 3.7.4, se cumple que

$$\operatorname{Ker} p(\nabla) = \operatorname{Ker}(\nabla-\alpha_1)^{n_1} \oplus \cdots \oplus \operatorname{Ker}(\nabla-\alpha_r)^{n_r}.$$

15. Ejercicio: Resuélvase la ecuación $a_{n+2} = a_{n+1} + a_n$, con las condiciones iniciales $a_0 = 0, a_1 = 1$ (sucesión de Fibonacci).

16. Ejercicio: Sea (a_n) una sucesión de números complejos y $b_n := \sum_{i=0}^{n-1} a_i$. Pruébese que $\Delta(b_n) = (a_n)$. Justificar, la igualdad $(\sum_{i=0}^{n-1} a_i) + cte = \frac{1}{\Delta}(a_n)$.

17. Dada la ecuación inhomogénea $p(\nabla)(a_n) = (b_n)$, supóngase que existe un polinomio $q(x)$, primo con $p(x)$, tal que $q(\nabla)(b_n) = 0$. Sean $\lambda(x), \mu(x)$ polinomios tales que $\lambda(x)\cdot p(x) + \mu(x)\cdot q(x) = 1$. Se cumple que una solución particular de la ecuación es $\lambda(\nabla)(b_n)$.

18. Ejercicio: Un banco nos presta un capital K, a devolver en N años, a un tipo de interés anual I. ¿Cuánto dinero D deberemos pagar al año, de modo que todos los años paguemos la misma cantidad y en los N años hayamos saldado nuestra deuda con el banco?

Resolución: Sea i_n el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n por el capital prestado. Entonces $D = a_n + i_n$. Además, $i_n = I\cdot(K - \sum_{r=1}^{n-1} a_r)$. Por tanto, $D = a_n + I\cdot(K - \sum_{r=1}^{n-1} a_r)$. Si aplicamos el operador diferencia Δ entonces

$$0 = \Delta(a_n) - I\cdot a_n = (\nabla - (1+I))(a_n).$$

Por tanto, $a_n = (1+I)^n\cdot\lambda$. Tenemos que calcular λ. Nos falta decir que amortizamos la hipoteca en N años, es decir, $K = \sum_{r=1}^{N} a_r$, que equivale a decir que

$$D = a_{N+1} = (1+I)^{N+1}\cdot\lambda.$$

Sabemos también que $D = a_1 + IK = (1+I)\cdot\lambda + IK$. Eliminando la λ obtendremos que

$$D = \frac{IK}{1 - \frac{1}{(1+I)^N}}.$$

19. Ejercicio: Un préstamo de $K = 10^5$ euros se quiere devolver durante $N = 20$ años, pagando cada año n una anualidad d_n de modo que $d_n = I' d_{n-1}$ ($I' = 1 + 2\%$). Se suponen que nos prestan el dinero a un tipo de interés anual del $I = 5\%$. Determinar d_1.

Resolución: Sea i_n es el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n por el capital prestado. Entonces, $d_n = i_n + a_n$. Tenemos que $i_n = I\cdot(K - \sum_{r=1}^{n-1} a_r)$. Por tanto,

$$d_n = a_n + I\cdot(K - \sum_{r=1}^{n-1} a_r).$$

Si aplicamos el operador diferencia Δ, entonces $\Delta(d_n) = \Delta(a_n) - I \cdot a_n = (\nabla - (1+I))(a_n)$. Por otra parte, $(\nabla - I')(d_n) = 0$ (luego $d_n = \lambda' I'^n$). Por tanto, si aplicamos $\nabla - I'$, obtenemos que

$$(\nabla - I')(\nabla - (1+I))(a_n) = 0$$

Por tanto, $a_n = \lambda I'^n + \mu(1+I)^n$. Sabemos que $d_{N+1} = a_{N+1}$, de lo que se deduce que $\lambda' = \lambda + \mu(\frac{1+I}{I'})^{N+1}$. De las ecuaciones

$$\lambda' I' = d_1 = a_1 + IK = \lambda I' + \mu(1+I) + IK$$
$$\lambda' I'^2 = d_2 = a_2 + I(K - a_1) = \lambda I'(I' - I) + \mu(1+I) + IK$$

se obtiene que $d_1 = \frac{K(1-I'+I)}{1-(\frac{I'}{1+I})^N}$.

3.8. Cuestionario

1. Sea M un A-módulo. Pruébese que $0 \cdot m = 0$, $(-1) \cdot m = -m$, $a \cdot 0 = 0$ y $a \cdot (-m) = (-a) \cdot m$.
2. Dotar a $A[x]$ de estructura de A-módulo.
3. Sea $\mathscr{C}(\mathbb{R}^2)$ el conjunto de todas las funciones continuas de $\mathbb{R}^2$ en $\mathbb{R}$. Dotar a $\mathscr{C}(\mathbb{R}^2)$ de estructura de $\mathbb{R}$-espacio vectorial.
4. Pruébese que los A-submódulos de A^3, $\langle (1,2,3),(1,0,0)\rangle$ y $\langle (0,2,3),(1,0,0)\rangle$ son iguales.
5. Resuélvase el problema 4.
6. Resuélvase el problema 5.
7. Resuélvase el problema 6.
8. Resuélvase el problema 10.
9. Sea $E = \mathbb{Q}[x]/(x-1) \oplus \mathbb{Q}[x]/(x+1) \oplus \mathbb{Q}[x]/(x^2-5)$ y $e_1 = (\bar{1},0,0)$, $e_2 = (0,\bar{1},0)$, $e_3 = (0,0,\bar{1})$ y $e_4 = (0,0,\bar{x})$ una base del $\mathbb{Q}$-espacio vectorial E. Calcular la matriz del endomorfismo $x\cdot\colon E \to E$, $e \mapsto x \cdot e$, en la base dada.
10. Resuélvase la ecuación diferencial $y'' + y = 0$.
11. Resuélvase la ecuación diferencial: $y'''' - 2y''' + 2y'' = 0$,
12. Resuélvase $y'' - y = x^3$.
13. Resuélvase $y'' - y = senx$.
14. Resuélvase $y''' - 2y'' + y = xe^x$.
15. Resuélvase el ejercicio 3.7.15.
16. Calcúlese $\sum_{i=0}^{n} i^2$.

3.9. Biografía de Hermann Grassmann

Hermann Günther Grassmann (Stettin, 15 de abril de 1809 - ibíd., 26 de septiembre de 1877) fue un lingüista y matemático alemán. También ejerció de físico, humanista, erudito y editor, por lo que se le considera un claro ejemplo de polimatía.
Hermann Grassmann era el tercero de los doce hijos de Justus Günter Grassmann y Johanne Luise Friederike Medenwald. Su madre era hija de un pastor de Klein-Schönfeld. Su padre había sido también consagrado pastor, pero consiguió una plaza de profesor de matemáticas y física en el Instituto de Stettin, y fue un académico notable, autor de varios libros de texto escolar de Física y Matemáticas, además de llevar a cabo interesantes investigaciones en el campo de la cristalografía. Otro hermano de Hermann, Robert, también se dedicó a las matemáticas y ambos trabajaron conjuntamente en muchos proyectos.

Durante su juventud, Hermann fue educado por su madre, mujer de una vasta cultura. Luego asistió a una escuela privada, antes de ingresar en el Instituto de Stettin, en el que daba clases su padre. La mayoría de los matemáticos despuntan ante sus profesores desde muy jóvenes. Sin embargo, y a pesar de tener unas extraordinarias oportunidades al pertenecer a una familia proclive a la educación, Hermann no destacó de modo especial en sus años de estudios secundarios, hasta el punto de que su padre pensó que debía dedicarse a algún tipo de trabajo manual, como el de jardinero o artesano.

Hermann apreciaba la música y aprendió a tocar el piano, a la vez que proseguía sus estudios, en los que poco a poco iba mejorando, y en los exámenes finales de los estudios secundarios, con 18 años, terminó el segundo de su promoción. Tras demostrar al final de sus estudios su competencia académica, Hermann decidió estudiar Teología, y en 1827 se trasladó a Berlín junto a su hermano mayor para cursar estudios en la Universidad. Realizó estudios de Teología, lenguas clásicas, Filosofía y Literatura, y no parece que acudiera a ninguna clase de Matemáticas o Física.

A pesar de que parece evidente que Hermann no tuvo formación universitaria formal alguna en matemáticas, ésta era la materia que más le interesaba cuando regresó a Stettin, en otoño de 1830, tras haber completado sus estudios universitarios en Berlín. Evidentemente, la influencia de su padre en esta vía fue muy importante, y pudo haber llegado a ser profesor de matemáticas, pero ya se había decidido a llevar a cabo investigaciones matemáticas por su cuenta. Después de pasar un año investigando en matemáticas y preparando el examen para profesor de instituto, Hermann se fue a a Berlín en diciembre de 1831 para presentarse a dichos exámenes.

Parece ser que sus ejercicios escritos no debieron ser muy bien valorados, puesto que sus examinadores le dieron el título para enseñar sólo en los primeros niveles de la secundaria. Se le dijo que, antes de poder enseñar en los niveles superiores, debería volver a examinarse y demostrar unos mayores conocimientos en los temas por los que había concursado. En la primavera de 1832 obtuvo una plaza de profesor ayudante en el Instituto de Stettin.

Fue sobre esta época cuando realizó sus dos primeros descubrimientos matemáti-

cos significativos, que estaban destinados a llevarlo a las importantes ideas que desarrollaría años después. En la premisa de su Die Lineale Ausdehnungslehre, ein neuer Zweig der Mathematik (Teoría de la extensión lineal, una nueva rama de las matemáticas, 1844), Grassmann describe cómo había ido llegando a estas ideas ya alrededor del año 1832.

En 1834, Grassmann empezó a dar clases de matemáticas en la Gewerbeschule (Escuela de artes y oficios) de Berlín. Un año más tarde regresó a Stettin para dar clases de matemáticas, física, lengua alemana, latín y religión en un centro educativo nuevo, la Otto Schule. Esta gran variedad de materias a impartir es prueba de que aún estaba habilitado solamente para impartir clases en las escuelas en los niveles más bajos. En los cuatro años siguientes, Grassmann superó los exámenes que le permitieron dar clases de matemáticas, física, química y mineralogía en todos los niveles de los centros de educación secundaria.

Grassmann se sentía en parte frustrado por el hecho de tener que dar clases sólo en niveles de secundaria, a pesar de ser capaz de elaborar una matemática innovadora. En 1847 pasa a ser"Oberlehre". En 1852 se le asignó el puesto que anteriormente había desempeñado su padre en el Instituto de Stettin, y obtuvo de ese modo el título de profesor. En 1847 solicitó al ministro prusiano de Educación ser tenido en cuenta para el desempeño de un puesto de profesor universitario, y el ministro solicitó a Ernst Eduard Kummer su opinión acerca de Grassmann. Kummer contestó diciendo que el ensayo de Grassman, que había sido premiado en 1846, tenía "(...) buen material expresado de modo inadecuado". Este informe de Kummer acabó con la esperanza de Grassmann de llegar a obtener una plaza de profesor universitario. Este episodio confirma además el hecho de que las autoridades con las que Grassmann contactó nunca reconocieron la importancia real de sus ideas.

Durante los disturbios políticos que se desarrollan en Alemania en 1848-49, Hermann y Robert Grassmann editaron un periódico en Stettin para apoyar la unificación de Alemania en el marco de una monarquía constitucional. Después de escribir una serie de artículos sobre leyes constitucionales, Hermann, cada vez menos de acuerdo con la línea política del periódico, lo dejó.

Grassmann tuvo once hijos, de los que siete llegaron a adultos. Uno de sus hijos, Hermann Ernst Grassmann, llegó a profesor de matemáticas en la Universidad de Giessen.

Entre los muchos temas que abordó Grassmann está su ensayo sobre la teoría de las mareas. Lo elaboró en 1840, tomando como base la teoría de la Méchanique analytique de Lagrange y de la Méchanique céleste de Laplace, pero exponiendo esta teoría por métodos vectoriales, sobre los que trabajaba desde 1832. Este ensayo, publicado por primera en los Collected Works de 1894-1911, contiene el primer testimonio escrito de lo que hoy se conoce como Álgebra Lineal y la noción de espacio vectorial. Grassmann desarrolló estos métodos en Die Lineale Ausdehnungslehre, ein neuer Zweig der Mathematik y Die Ausdehnungslehre: Vollständig und in strenger Form bearbeitet.

En 1844, Grassmann publica su obra maestra, Die Lineale Ausdehnungslehre, ein neuer Zweig der Mathematik, más conocido como Ausdehnungslehre, que se puede traducir como "teoría de la extensión" o"teoría de las magnitudes extensiva". Después de proponer en Ausdehnungslehre nuevas bases para todas las matemáticas, el trabajo

empieza con definiciones de naturaleza más bien filosófica. Grassmann demostró además que si la geometría se hubiese expresado en forma algebraica como él proponía, el número tres no hubiese desempeñado el papel privilegiado que tiene como número que expresa la dimensiones espaciales; de hecho, el número de posibles dimensiones de interés para la geometría es ilimitado.

Fearnley-Sander (1979) describe la creación del Álgebra Lineal de Grassmann de este modo:

"La definición de espacio lineal (...) se reconoce abiertamente alrededor de 1920, cuando Hermann Weyl y otros publicaron la definición formal. En realidad dicha definición había sido formulada unos treinta años antes por Peano, que había estudiado a fondo el trabajo matemático de Grassmann. Grassmann no formuló una definición formal - no existía entonces un lenguaje adecuado - pero no hay duda de que tuviera claro el concepto"

"Empezando con una colección de 'unidades' $e_1, e_2, e_3, \ldots$, él, efectivamente, definió el espacio lineal libre que generaban; en otros términos, considera la combinación lineal formal $a_1e_1 + a_2e_2 + a_3e_3 + \cdots$ donde a_j son números reales, define la suma y la multiplicación por números reales [en el modo que se usa actualmente] y demuestra formalmente las propiedades de espacio lineal de estas operaciones. (...) Desarrolla la teoría del la independencia lineal de modo extraordinariamente similar a la presentación que podemos encontrar en los textos modernos de álgebra lineal. Define la noción de subespacio, independencia, longitud, desdoblamiento, dimensión, suma e intersección de subespacios, y proyección de elementos en los subespacios"

"...pocos estuvieron tan cerca como Hermann Grassmann de crear, trabajando en solitario, una nueva disciplina"

Desarrollando una idea de su padre, Grassmann definió también en Ausdehnungslehre el producto exterior, llamado también "producto combinatorio" (en alemán: äußeres Produkt o kombinatorisches Produkt), la operación clave en el álgebra que hoy se conoce como álgebra exterior. (Conviene no olvidar que en los tiempos de Grassmann la única teoría axiomática disponible era la Geometría euclidiana, y que la noción general de álgebra abstracta aún no había sido definida.) En 1878, William Kingdon Clifford unió el álgebra exterior con los cuaterniones de William Rowan Hamilton, sustituyendo la regla de Grassmann $e_pe_p = 0$ por $e_pe_p = 1$.

El Ausdehnungslehre fue un texto revolucionario, muy avanzado en su época como para poder ser apreciado. Grassmann lo expuso como tesis doctoral, pero Möbius no se consideró capaz de valoralrlo y se lo remitió a Ernst Kummer, que lo rechazó sin haber llevado a cabo una lectura atenta. En los 10 años siguientes, Grassmann escribió una serie de trabajos aplicando su teoría de la extensión, incluyendo una Neue Theorie der Elektrodynamik de 1845, y diversos trabajos sobre curvas y superficies alegbraicas, con la esperanza de que estas aplicaciones movieran a los demás a tomar más en serio su teoría.

En 1846, Möbius invitó a Grassmann a una competición para resolver un problema originalmente planteado por Leibniz: idear un cálculo geométrico privado de coordenadas y propiedades métricas. Geometrische Analyse geknüpft an die von Leibniz erfundene geometrische Charakteristik de Grassmann, fue la idea ganadora. Hay que decir sin embargo que el resultado de Grassmann fue el único presentado. De cual-

quier manera, Möbius, que era uno de los miembros del jurado, criticó el modo en que Grassmann introdujo la noción abstracta sin proporcionar al lector intuición alguna sobre la validez de estas nociones.

En 1853, Grassmann publicó una teoría sobre el modo en que se mezclan los colores; ésta y sus tres leyes de los colores siguen enseñándose hoy en día. El trabajo de Grassmann entraba en contradicción con el de Helmholtz. Grassmann escribió también sobre cristalografía, electromagnetismo, y mecánica.

En 1861 Grassmann expuso la primera formulación axiomática de la Aritmética, usando ampliamente el principio de inducción. Giuseppe Peano y sus seguidores citaron ampliamente este trabajo a partir de 1890.

En 1862, Grassman, tratando de conseguir el reconocimiento de su teoría de la extensión, publicó la segunda edición de la "Ausdehnungslehre", ampliamente reescrita, y con la exposición definitiva de su álgebra lineal. El resultado, Die Ausdehnungslehre: Vollständig und in strenger Form bearbeitet, que se conoce como"Enseñanza de la dilatació" no fue mejor considerada que la edición original, a pesar de que el método de exposición de esta segunda versión de "Ausdehnungslehre" se anticipara a lo que han sido los libros de texto en el Siglo XX. En esta obra desarrolla un cálculo operatorio directo para las diversas magnitudes geométricas, que se conoce como números de Grassmann.

El único matemático que valoró en su justa medida las ideas Grassmann en vida de éste fue Hermann Hankel. En su obra Theorie der complexen Zahlensysteme (1867) ayudó a que se conocieran mejor las ideas de Grassmann. Este trabajo:

"... desarrolló una parte del álgebra de Hermann Grassmann y de los cuaterniones de Hamilton. Hankel fue el primero que reconoció la importancia de los textos de Grassmann, que habían sido menospreciados durante mucho tiempo.." (introducción de Hankel en el Dictionary of Scientific Biography. New York: 1970-1990)

Se tardó en adoptar los métodos matemáticos de Grassmann pero influyeron directamente en Felix Klein y Élie Cartan. La primera monografía de A. N. Whitehead, Universal Algebra de 1898, incluía la primera exposición sistemática en inglés de la teoría de la extensión y del álgebra exterior. La teoría de la extensión se aplicó al estudio de las formas diferenciales y en las aplicaciones de dichas formas al Análisis y a la Geometría. La Geometría Diferencial usa el Álgebra Exterior.

Contrariado por su incapacidad de conseguir que se le reconociera como matemático, Grassmann se dedicó a la lingüística histórica. Escribió libros de gramática alemana, elaboró catálogos de canciones populares y aprendió sánscrito. Su diccionario y su traducción del Ayurveda (que se sigue publicando hoy en día) tuvieron un gran reconocimiento entre los filólogos. Formuló una ley relativa a los fonemas de las lenguas indoeuropeas, que se conoce hoy como ley de Grassmann en su honor. También elaboró un Diccionario sobre el Rig-veda (1873-1875). Sus cualidades filológicas fueron reconocidas en vida; fue admitido en la American Oriental Society y en 1876 fue nombrado doctor honoris causa por la Universidad de Tubinga.

(Artículo tomado de wikipedia).

3.10. Problemas

1. Sea $(G,+)$ un grupo abeliano y consideremos en G su estructura natural de $\mathbb{Z}$-módulo. Pruébese que lo subgrupos de G coinciden con los $\mathbb{Z}$-submódulos de G. Sea $(G',+)$ otro grupo abeliano y consideremos también su estructura natural de $\mathbb{Z}$-módulo. Pruébese que los morfismos de grupos de G en G' coinciden con los morfismos de $\mathbb{Z}$-módulos de G en G'.

2. Sea E un K-espacio vectorial y $T\colon E\to E$ una aplicación K-lineal. Consideremos en E su estructura natural de $K[x]$-módulo. Pruébese que los subespacios vectoriales de E, estables por el endomorfismo T, coinciden con los $K[x]$-submódulos de E. Sea $\phi\colon E\to E$ un isomorfismo de $K[x]$-módulos. Pruébese que la matriz de T en una base $\{e_i\}_{i\in I}$ de E es igual a la matriz del endomorfismo lineal $x\cdot\colon E'\to E'$ en la base $\{\phi(e_i)\}_{i\in I}$.

3. Sea $f\colon A\to B$ un morfismo de anillos y M un B-módulo. Dotar a M de estructura de A-módulo.

4. Sean $N\subseteq M$ y $N'\subseteq M'$ submódulos. Considerar la inclusión obvia $N\oplus N'\subseteq M\oplus M'$. Pruébese que
$$(M\oplus M')/(N\oplus N')\simeq M/N\oplus M'/N'.$$

5. Sea $I\subseteq A$ un ideal y M un A-módulo. Denotemos $I\cdot M$ como el mínimo submódulo de M que contiene a $\{i\cdot m\}_{i\in I,m\in M}$. Pruébese que
$$I\cdot M=\{i_1\cdot m_1+\cdots+i_n\cdot m_n\in M,\text{ variando los } i_j\in I, m_j\in M,\text{ y } n\in\mathbb{N}\}$$

6. Sea $I\subseteq A$ un ideal y M un A-módulo. Dotar a M/IM de estructura de A/I-módulo.

7. Sea $I\subset A$ un ideal y M, M' A-módulos. Pruébese que
$$I\cdot(M\oplus M')=I\cdot M\oplus I\cdot M'.$$

8. Sea A un anillo y $n,m\in\mathbb{N}$. Pruébese que si $A^n\simeq A^m$ como A-módulo entonces $n=m$. Pruébese que todas las bases de un A-módulo libre (finito generado) tienen el mismo número de elementos.

9. Sea $\pi\colon M\to N$ un morfismo de módulos. Si existe un morfismo de módulos $s\colon N\to M$ tal que $\pi\circ s=\mathrm{Id}$ entonces, $M\simeq\operatorname{Ker}\pi\oplus N$.

10. Sean $N_1,N_2\subseteq M$ dos submódulos y sea $\bar{N}_2=\{\bar{n}_2\in M/N_1\colon n_2\in N_2\}$. Pruébese que $(M/N_1)/\bar{N}_2\simeq M/(N_1+N_2)$.

11. Pruébese que $\Delta\binom{n}{i}=\binom{n}{i-1}$. Pruébese que $\{\binom{n}{0},\binom{n}{1},\dots,\binom{n}{r}\}$ es una base de $\operatorname{Ker}\Delta^{r+1}$. Sea $p(n)=\sum_{i=0}^{r}\lambda_i\binom{n}{i}$, pruébese que λ_i es el término 0 de la sucesión $\Delta^i(p(n))$, es decir,
$$\lambda_i=\sum_{j=0}^{i}\binom{i}{j}\cdot(-1)^j p(i-j).$$

Calcúlese $\sum_{i=0}^{n} i^3$.

12. Calcúlense cuántos números de longitud n se pueden escribir con ceros y unos, de modo que nunca aparezcan dos ceros seguidos (ejemplo: los números de longitud tres cumpliendo lo dicho son $010, 011, 101, 110, 111$, que son cinco distintos).

13. Resuélvase la ecuación $a_{n+2} + 2a_{n+1} - 8a_n = 2^n$.

14. Calcúlese $\sum_{i=0}^{n} g^i$.

15. Un préstamo de $K = 10^5$ euros se quiere devolver durante $N = 20$ años, pagando cada año n una anualidad d_n de modo que $d_n = d_{n-1} + 10^3$. Se suponen que nos prestan el dinero a un tipo de interés anual del $I = 5\,\%$. Determinar d_1.

16. Sea $p(x) \in \mathbb{R}[x]$ un polinomio mónico de grado n. Sean $s_1(x), \ldots, s_n(x)$ soluciones, linealmente independientes, de la ecuación diferencial $p(D)y = 0$. Pruébese que si las funciones $c_1(x), \ldots, c_n(x)$ cumplen las ecuaciones

$$\begin{aligned} &c_1(x)'s_1(x) + \ldots + c_n(x)'s_n(x) = 0 \\ &\ldots \\ &c_1(x)'s_1(x)^{n-2)} + \ldots + c_n(x)'s_n(x)^{n-2)} = 0 \\ &c_1(x)'s_1(x)^{n-1)} + \ldots + c_n(x)'s_n(x)^{n-1)} = f(x) \end{aligned}$$

entonces $c_1(x)s_1(x) + \ldots + c_n(x)s_n(x)$ es una solución particular de $p(D)y = f(x)$.

CAPÍTULO 4
MÓDULOS SOBRE DOMINIOS DE IDEALES PRINCIPALES

4.1. Introducción

En este capítulo clasificamos los módulos finito generados sobre anillos euclídeos.

En particular clasificaremos los grupos abelianos finito generados. Recordemos que los grupos abelianos son justamente los $\mathbb{Z}$-módulos. Veremos que todo grupo abeliano finito generado G es una suma directa finita de grupos cíclicos, es decir,

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \overset{r}{\cdots} \oplus \mathbb{Z}/n_r\mathbb{Z} \qquad (*)$$

Recordemos que si $n = p_1^{n_1} \cdots p_r^{n_r}$ es la descomposición de n en producto de potencias de primos, el teorema chino de los restos nos dice que $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{n_r}\mathbb{Z}$. Por tanto, en la descomposición $(*)$ podemos suponer que los n_i son potencias de primos (o nulos). En esta situación, demostraremos que los enteros n_i clasifican G.

Clasificaremos también los endomorfismos de un espacio vectorial de dimensión finita. Recordemos que dar un endomorfismo de un k-espacio vectorial equivale a dotar al espacio vectorial de estructura de $k[x]$-módulo: dado un espacio vectorial E y un endomorfismo $T\colon E \to E$, definimos $x \cdot e = T(e)$, para todo $e \in E$, y en general $p(x) \cdot e = p(T)(e)$. Demostramos que existen unos polinomio mónicos irreducibles $p_1(x), \cdots, p_r(x)$ únicos, y un conjunto de números naturales n_{ij} únicos de modo que

$$E \simeq (k[x]/(p_1(x)^{n_{11}}) \oplus \cdots \oplus k[x]/(p_1(x)^{n_{1s_1}})) \oplus \cdots \oplus (k[x]/(p_r(x)^{n_{r1}}) \oplus \cdots \oplus k[x]/(p_r(x)^{n_{rs_r}})).$$

como $k[x]$-módulos. Este isomorfismo nos permitirá, cuando $k = \mathbb{C}$, definir las bases de Jordan y expresar la matriz de T en una base de Jordan.

Aplicamos estos teoremas para resolver los sistemas de ecuaciones diofánticas y los sistemas de ecuaciones diferenciales lineales con coeficientes constantes.

Por último, probaremos que si A es un dominio de ideales principales y M es un A-módulo finito generado entonces existen, elementos irreducibles $p_i \in A$ (únicos salvo multiplicación por invertibles) y $n_{ij} > 0$, $n \in \mathbb{N}$ únicos de modo que

$$M \simeq A^n \oplus (A/(p_1^{n_{11}}) \oplus \cdots \oplus A/(p_1^{n_{1s_1}})) \oplus \cdots \oplus (A/(p_r^{n_{r1}}) \oplus \cdots \oplus A/(p_r^{n_{rs_r}})).$$

4.2. Transformaciones elementales

Sea $\{u_1,\dots,u_m\}$, $\{u'_1,\dots,u'_n\}$ bases de los módulos libres L y L', respectivamente. Sea (a_{ij}) la matriz asociada a la aplicación A-lineal $\phi\colon L \to L'$, en dichas bases.

Si en vez de $\{u_1,\dots,u_m\}$, consideramos la base que se obtiene permutando los vectores u_r y u_s de $\{u_1,\dots,u_m\}$, la matriz de ϕ en las nuevas bases (a'_{ij}), se obtiene permutando las columnas r y s de la matriz (a_{ij}). Denotemos δ_{sr} la matriz cuyos coeficientes son todos nulos salvo el coeficiente sr que vale 1. Denotemos por $X_{sr} := \mathrm{Id} - \delta_{rr} - \delta_{ss} + \delta_{rs} + \delta_{sr}$. Entonces,

$$(a'_{ij}) = (a_{ij}) \cdot X_{sr}$$

Si en vez de $\{u_1,\dots,u_m\}$, consideramos la base $\{u_1,\dots,u_r \overset{r}{+} au_s,\dots,u_m\}$, la matriz de ϕ en las nuevas bases (a'_{ij}), se obtiene cambiando la columna r, C_r, de la matriz (a_{ij}) por la columna $C_r + aC_s$. Es decir,

$$(a'_{ij}) = (a_{ij}) \cdot (\mathrm{Id} + a \cdot \delta_{sr})$$

Igualmente, si permutamos los vectores u'_r, u'_s de $\{u'_1,\dots,u'_n\}$, la matriz de ϕ en las nuevas bases, (a'_{ij}), se obtiene permutando las filas r y s de (a_{ij}). Es decir,

$$(a'_{ij}) = X_{sr} \cdot (a_{ij}).$$

Si en vez de la base $\{u'_1,\dots,u'_n\}$, consideramos la base $\{u'_1,\dots,u'_s \overset{s}{-} au'_r,\dots,u'_n\}$, la matriz de ϕ en las nuevas bases, se obtiene cambiando la fila r, F_r, de la matriz (a_{ij}) por la fila $F_r + aF_s$. Es decir,

$$(a'_{ij}) = (\mathrm{Id} + a \cdot \delta_{rs}) \cdot (a_{ij})$$

Este tipo de transformaciones de la matriz (a_{ij}) (o equivalentemente de las bases $\{u_i\},\{u'_i\}$) las denominaremos transformaciones elementales.

1. Proposición : *Sea (A,δ) un anillo euclídeo. Sea $\phi\colon L \to L'$ un morfismo de A-módulos, entre A-módulos libres finito generados. Existen bases $\{e_1,\dots,e_m\}$ en L y $\{e'_1,\dots,e'_n\}$ en L', de modo que $\phi(e_i) = \lambda_i e'_i$, para ciertos $\lambda_i \in A$, si $i \le n$, y $\phi(e_i) = 0$ si $i > n$.*

Demostración. Vamos a probar que mediante transformaciones elementales la matriz de ϕ es "diagonal", es decir, $\phi(e_i) = \lambda_i e'_i$, para todo i.

Probemos que mediante transformaciones elementales obtenemos una matriz de la forma

$$\begin{pmatrix} c_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & b_{ij} & \\ 0 & & & \end{pmatrix}$$

Procedemos por inducción sobre $\delta(a_{11})$ (sigamos la convención $\delta(0) = +\infty$). Si $\delta(a_{11}) = 0$, entonces a_{11} es invertible y es fácil mediante transformaciones elementales conseguir que $a_{1j} = a_{j'1} = 0$, para todo $j, j' \neq 0$. Y hemos concluido. Supongamos que la

afirmación hecha es cierta si $\delta(a_{11}) < n$. Sea $\delta(a_{11}) = n$. Si algún a_{1i} cumple $\delta(a_{i1}) < n$, permutando las filas 1 e i, obtenemos una nueva matriz cuyo coeficiente a_{11} cumple que $\delta(a_{11}) < n$ y concluimos por hipótesis de inducción. Podemos suponer que $\delta(a_{i1}) \geq \delta(a_{11})$ para todo i, e igualmente que $\delta(a_{1j}) \geq \delta(a_{11})$, para todo j. Si algún $a_{i1} \neq 0$, entonces $a_{i1} = a_{11} \cdot c + a'_{i1}$, con $\delta(a'_{i1}) < \delta(a_{11}) = n$ ó $a_{1i} = 0$. Cambiando la fila i, F_i, por $F_i - cF_1$, obtenemos una nueva matriz con la misma primera fila y primera columna, salvo que el coeficiente $i1$, que es a'_{i1} cumple que $a'_{i1} = 0$ ó $\delta(a'_{i1}) < n$ (en este último caso terminaríamos por induccción). En conclusión, por transformaciones elementales obtenemos una matriz de la forma

$$\begin{pmatrix} c_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & b_{ij} & \\ 0 & & & \end{pmatrix}$$

Procediendo del mismo modo reiteradamente, con la matriz (b_{ij}), "diagonalizaremos" ϕ.

□

4.3. Sistemas de ecuaciones lineales diofánticas

Resolvamos los sistemas de ecuaciones lineales diofánticos. Consideremos el sistema de ecuaciones

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

con $a_{ij}, b_k \in \mathbb{Z}$ para todo $i, j.k$, que escribimos abreviadamente $A \cdot x = b$. Mediante transformaciones elementales (en columnas y filas) diagonalizamos la matriz A. Es decir, sabemos calcular matrices cuadradas invertibles F y C de modo que $F \cdot A \cdot C = D$, donde $D = (d_{ij})$, con $d_{ij} = 0$ para todo $i \neq j$. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{A} & \mathbb{Z}^m \\ {\scriptstyle C}\uparrow & & \downarrow{\scriptstyle F} \\ \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m \end{array} \qquad \begin{array}{ccc} x & \xmapsto{A} & b \\ {\scriptstyle C}\uparrow & & \downarrow{\scriptstyle F} \\ x' & \xmapsto{D} & F \cdot b \end{array}$$

(con $x' := C^{-1}x$). Entonces, $D \cdot x' = F \cdot b$. Si calculamos x' (que es fácil), tenemos que $x = C \cdot x'$.

Escribamos los cálculos. Mediante transformaciones elementales de las n-primeras columnas y m-primeras filas de la matriz

$$\left(\begin{array}{c|c} A & b \\ \hline \mathrm{Id} & 0 \end{array}\right)$$

obtenemos la matriz

$$\left(\begin{array}{c|c} F \cdot A \cdot C & F \cdot b \\ \hline C & 0 \end{array}\right) = \left(\begin{array}{c|c} D & F \cdot b \\ \hline C & 0 \end{array}\right)$$

Finalmente, x' cumple $D\cdot x' = F\cdot b$ si y sólo si $x = C\cdot x'$ cumple $A\cdot x = b$.

1. Ejemplo: Resolvamos la ecuación diofántica $2\cdot x + 3\cdot y = 5$:

$$\left(\begin{array}{cc|c} 2 & 3 & 5 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right) \overset{C_2-C_1}{\rightsquigarrow} \left(\begin{array}{cc|c} 2 & 1 & 5 \\ \hline 1 & -1 & 0 \\ 0 & 1 & 0 \end{array}\right) \overset{C_1-2C_2}{\rightsquigarrow} \left(\begin{array}{cc|c} 0 & 1 & 5 \\ \hline 3 & -1 & 0 \\ -2 & 1 & 0 \end{array}\right)$$

Tenemos que $x' = x'$, $y' = 5$ son las soluciones del sistema $0\cdot x' + 1\cdot y' = 5$. Por tanto,

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} x' \\ 5 \end{pmatrix} = \begin{pmatrix} 3x' - 5 \\ -2x' + 5 \end{pmatrix}$$

son las soluciones de nuestra ecuación diofántica.

Con menos cálculos: Tenemos que $\binom{x}{y} = C\cdot\binom{x'}{5} = (\mathrm{Id} - \delta_{12})\circ(\mathrm{Id} - 2\delta_{21})\circ\binom{x'}{5}$. Luego,

$$\begin{pmatrix} x' \\ 5 \end{pmatrix} \overset{F_2-2F_1}{\rightsquigarrow} \begin{pmatrix} x' \\ 5 - 2x' \end{pmatrix} \overset{F_1-F_2}{\rightsquigarrow} \begin{pmatrix} 3x' - 5 \\ 5 - 2x' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

2. Ejemplo: Resolvamos el sistema de ecuaciones diofánticas

$$\begin{aligned} 2x + 3y + z &= 6 \\ 4x + 2y + z &= 5 \end{aligned}$$

$$\left(\begin{array}{ccc|c} 2 & 3 & 1 & 6 \\ \hline 4 & 2 & 1 & 5 \end{array}\right) \overset{C_1 x C_3}{\rightsquigarrow} \left(\begin{array}{ccc|c} 1 & 3 & 2 & 6 \\ \hline 1 & 2 & 4 & 5 \end{array}\right) \overset{F_2-F_1}{\rightsquigarrow} \left(\begin{array}{ccc|c} 1 & 3 & 2 & 6 \\ \hline 0 & -1 & 2 & -1 \end{array}\right) \overset{C_3+2C_2}{\rightsquigarrow} \left(\begin{array}{ccc|c} 1 & 3 & 8 & 6 \\ \hline 0 & -1 & 0 & -1 \end{array}\right)$$

Las soluciones del sistema

$$\begin{aligned} x' + 3y' + 8z' &= 6 \\ -y' &= -1 \end{aligned}$$

son $z' = z'$, $y' = 1$ y $x' = 3 - 8z'$. Luego las soluciones de nuestro sistema son

$$\begin{pmatrix} 3 - 8z' \\ 1 \\ z' \end{pmatrix} \overset{F_2+2F_3}{\rightsquigarrow} \begin{pmatrix} 3 - 8z' \\ 1 + 2z' \\ z' \end{pmatrix} \overset{F_1 x F_3}{\rightsquigarrow} \begin{pmatrix} z' \\ 1 + 2z' \\ 3 - 8z' \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

4.4. Clasificación de módulos sobre anillos euclídeos

1. Teorema: *Sea A un anillo euclídeo y M un A-módulo finito generado. Entonces, existen $a_1, \ldots, a_n \in A$ no invertibles de modo que*

$$M \simeq A/a_1A \oplus \cdots \oplus A/a_nA.$$

Demostración. Sea $L \xrightarrow{\phi} L' \xrightarrow{\pi} M$ una presentación de M por módulos libres finito generados. Sean $\{e_1, \ldots, e_m\}$ y $\{e'_1, \ldots, e'_n\}$ bases de L y L' de modo que $\phi(e_i) = \lambda_i e'_i$ si $1 \le i \le n$ y $\phi(e_i) = 0$ si $i > n$ (en el caso de que $m < n$, definimos $\lambda_i := 0$ para los $m < i \le n$). Consideremos los isomorfismos $B\colon L \simeq A^m$, $B(\sum_i a_i e_i) = (a_i)$, $B'\colon L' \simeq A^n$, $B'(\sum_j a'_j e'_j) = (a'_j)$ y el morfismo $D\colon A^m \to A^n$, $D(1_i) = \lambda_i 1_i$. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} L & \xrightarrow{\phi} & L' \\ {\scriptstyle B}\downarrow\wr & & \wr\downarrow{\scriptstyle B'} \\ A^m & \xrightarrow[D]{} & A^n \end{array}$$

Luego,

$$M \simeq L'/\mathrm{Im}\,\phi \simeq A^n/\mathrm{Im}\,D = (A \oplus \overset{n}{\cdots} \oplus A)/(\lambda_1 A \oplus \overset{n}{\cdots} \oplus \lambda_n A) \simeq A/\lambda_1 A \oplus \overset{n}{\cdots} \oplus A/\lambda_n A.$$

□

Si $a \in A$ no es nulo ni invertible, entonces $a = p_1^{n_1} \cdots p_r^{n_r}$ con p_i irreducible, para todo i, y primo con p_j, para todo $j \neq i$. Además, por el teorema chino de los restos

$$A/aA \simeq A/p_1^{n_1}A \oplus \cdots \oplus A/p_r^{n_r}A.$$

Por tanto, tenemos demostrado el siguiente teorema.

2. Teorema de clasificación: *Sea A un anillo euclídeo y M un A-módulo finito generado. Entonces, existen elementos irreducibles $p_1, \ldots, p_r \in A$ (p_i primo con p_j, para todo $i \neq j$) de modo que*

$$M \simeq A^n \oplus (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A).$$

4.4.1. Unicidad de los divisores elementales

Vamos a probar que n, los p_{ij} (salvo multiplicación por invertibles) y los n_{ij} del teorema de clasificación son únicos.

3. Definición: Sea M un A-módulo. Se denomina ideal anulador de M, que denotaremos $\mathrm{Anul}_A(M)$, al ideal $\mathrm{Anul}_A(M) := \{a \in A : a \cdot m = 0, \text{ para todo } m \in M\}$.

4. Ejemplos: $\mathrm{Anul}_{\mathbb{Z}}(\mathbb{Z}) = 0$ y $\mathrm{Anul}_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}) = 6\mathbb{Z}$.

5. Ejemplo: Sea $m \in M$. El morfismo

$$A/\mathrm{Anul}(\langle m \rangle) \to \langle m \rangle, \bar{a} \mapsto a \cdot m$$

es un isomorfismo de A-módulos.

6. Lema: *Sea A un anillo íntegro y $a, b \in A$ primos entre sí (es decir, $(a,b) = A$).*

1. *El morfismo $b\cdot : A/aA \to A/aA$, $\bar{c} \mapsto \overline{bc}$ es un isomorfismo.*
2. *Consideremos el morfismo $a\cdot : A/a^nA \to A/a^nA$. Entonces,*

$$\mathrm{Ker}\, a\cdot \simeq A/aA$$
$$\mathrm{Im}\, a\cdot \simeq A/a^{n-1}A$$

Demostración. 1. Sean $\lambda, \mu \in A$ tales que $\lambda a + \mu b = 1$. Entonces, $\bar{c} = \overline{(\lambda a + \mu b)\cdot c} = \overline{\mu bc}$. Luego el morfismo inverso de $b\cdot$ es $\mu\cdot$.

2. $\mathrm{Ker}\, a\cdot = \{\bar{c} \in A/a^nA : \overline{ac} = 0\} = \{\bar{c} \in A/a^nA : ac \in a^nA\} = \langle \overline{a^{n-1}} \rangle \simeq A/aA$. Por último, $\mathrm{Im}\, a\cdot = \langle \bar{a} \rangle \simeq A/a^{n-1}A$.

□

ÍNDICE

7. Ejercicio: Sea A un anillo íntegro y $a,b \in A$ primos entre sí (es decir, $(a,b)=A$). Entonces, el morfismo de A-módulos

$$A/aA \oplus A/bA \xrightarrow{\phi} A/abA, (\bar{r},\bar{s}) \mapsto \overline{br+as},$$

es un isomorfismo

Resolución: El morfismo $\pi\colon A/abA \to A/aA \oplus A/bA$, $\pi(\bar{t}) = (\bar{t},\bar{t})$ es un isomorfismo por el teorema chino de los restos. La composición $\pi \circ \phi$ es un isomorfismo por el lema 4.4.6 1. Por tanto, ϕ es un isomorfismo.

8. Teorema: *Sea A un dominio de ideales principales. Sea $\{p_1,\dots,p_r\}$ un número finito de irreducibles de A, de modo que p_i es primo con $p_{i'}$, para todo $i \neq i'$. Sea $\{q_1,\dots,q_u\}$ un número finito de irreducibles de A, de modo que q_j es primo con $q_{j'}$, para todo $j \neq j'$. Entonces, existe un isomorfismo*

$$\begin{aligned}(A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A)\\ \simeq (A/q_1^{m_{11}}A \oplus \cdots \oplus A/q_1^{m_{1t_1}}A) \oplus \cdots \oplus (A/q_u^{m_{u1}}A \oplus \cdots \oplus A/q_u^{m_{ut_u}}A)\end{aligned}$$

si y sólo si, reordenando, $p_i = q_i$(salvo multiplicación por invertibles), para todo i y $n_{uv} = m_{uv}$, para todo uv.

Demostración. $\Rightarrow$) Por el lema 4.4.6, $\operatorname{Ker} p_1^N\cdot = \oplus_i A/p_1^{n_{1i}}A$, para $N >> 0$. Si los q_i son primos con p_1 para todo i, entonces tendríamos por otra parte que $\operatorname{Ker} p_1^N\cdot = 0$, lo cual es contradictorio. Reordenando, podemos suponer que $p_1 = q_1$ y en este caso $\operatorname{Ker} p_1^N\cdot = \oplus_j A/p_1^{m_{1j}}A$. Reordenando podemos suponer que $n_{11} \geq n_{12} \geq \cdots \geq n_{1s_1}$ y que $m_{11} \geq m_{12} \geq \cdots \geq m_{1t_1}$.

Consideremos el módulo $M = \operatorname{Ker} p_1^N\cdot$. Por el lema 4.4.6,

$$\operatorname{Ker} p_1\cdot \simeq A/p_1A \oplus \overset{s_1}{\cdots} \oplus A/p_1A \simeq A/p_1A \oplus \overset{t_1}{\cdots} \oplus A/p_1A$$

Luego, $s_1 = t_1$. Por el lema 4.4.6,

$$\operatorname{Im} p_1\cdot \simeq A/p_1^{n_{11}-1}A \oplus \cdots \oplus A/p_1^{n_{1s_1}-1}A \simeq A/p_1^{m_{11}-1}A \oplus \cdots \oplus A/p_1^{m_{1t_1}-1}A.$$

Por inducción sobre la suma $\sum_i n_{1i}$, tenemos que $n_{1i}-1 = m_{1i}-1$, siempre que $n_{1i}-1 \neq 0$ y $m_{1i}-1 \neq 0$. Si s_1' es el numero de los $n_{1i} \neq 1$ y t_1' es el número de los $m_{1i} \neq 1$, entonces $s_1' = t_1'$. Como $s_1 = t_1$, entonces $s_1 - s_1' = t_1 - t_1'$, luego $n_{1i} = 1$ si y sólo si $m_{1i} = 1$. Con todo junto, concluimos que $n_{1i} = m_{1i}$, para todo i.

□

9. Definición: Sea A un anillo íntegro y M un A-módulo. Llamaremos torsión de M, que denotaremos $T(M)$, a

$$T(M) = \{m \in M\colon \text{existe } a \in A \text{ no nulo tal que } am = 0\}$$

Es fácil probar que $T(M)$ es un submódulo de M.

10. Teorema: *Sea A un anillo euclídeo y M un A-módulo finito generado. Entonces, existen elementos irreducibles $p_1,\dots,p_r \in A$ (p_i primo con p_j, para todo $i \neq j$), únicos salvo invertibles, y $n \in \mathbb{N}$ y $0 \neq n_{ij} \in \mathbb{N}$ únicos de modo que*

$$M \simeq A^n \oplus (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A).$$

Se dirá que n es el rango de M y que los $p_i^{n_{ij}}$ son los divisores elementales de M.

Demostración. Sólo nos falta probar la unicidad.

Observemos que $T(M) \simeq (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A)$ y $M/T(M) \simeq A^n$. Por tanto, n está determinado por M (es el rango de $M/T(M)$). Tenemos que probar las unicidad de los $p_i^{n_{ij}}$. Esto es consecuencia del teorema 4.4.8. □

4.4.2. Factores invariantes

11. Proposición: *Sean M y N dos A-módulos. Entonces,*

$$\mathrm{Anul}_A(M \oplus N) = \mathrm{Anul}_A(M) \cap \mathrm{Anul}_A(N).$$

Demostración. Es fácil de probar. □

12. Proposición: *Sea A un anillo euclídeo y M un A-módulo finito generado de torsión. El ideal anulador de M está generado por el mínimo común múltiplo de los divisores elementales asociados a M.*

Demostración. Por el teorema de clasificación sabemos que

$$M \simeq (A/p_1^{n_{11}}A \oplus \cdots A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_1^{n_{r1}}A \oplus \cdots A/p_r^{n_{rs_r}}A)$$

con p_i irreducibles, p_i primos con p_j para $i \neq j$, y podemos suponer que $n_{11} \geq n_{12} \geq \cdots \geq n_{1s_1}$,..., $n_{r1} \geq n_{r2} \geq \cdots \geq n_{rs_r}$. Entonces,

$$\mathrm{Anul}_A(M) = p_1^{n_{11}} \cdot p_2^{n_{21}} \cdots p_r^{n_{r1}} = m.c.m.\{p_i^{n_{ij}}, \forall ij\}.$$

□

Sigamos con las hipótesis de la proposición anterior y con las notaciones de la demostración anterior. Definamos $\phi_1 = \mathrm{Anul}_A(M) = p_1^{n_{11}} \cdots p_r^{n_{r1}}$. Observemos que

$$M = (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_r^{n_{r1}}A) \oplus M_2 = A/\phi_1 A \oplus M_2$$

Argumentando igual con M_2, tenemos $\phi_2 \in A$ de modo que $\mathrm{Anul}_A(M_2) = \phi_2 A$ (ϕ_2 divide a ϕ_1, ya que $\mathrm{Anul}_A(M) \subseteq \mathrm{Anul}_A(M_2)$) y

$$M = A/\phi_1 A \oplus M_2 = A/\phi_1 A \oplus A/\phi_2 A \oplus M_3.$$

Recurrentemente, tenemos que

$$M = A/\phi_1 A \oplus A/\phi_2 A \oplus \cdots \oplus A/\phi_r A.$$

con $\phi_r | \phi_{r-1} | \cdots | \phi_1$, que se dice que son los factores invariantes de M.

4.5. Clasificación de los grupos abelianos

1. Teorema de clasificación: *Sea $(G,+)$ un grupo abeliano finito. Entonces, existen números primos $p_1,\dots,p_r \in \mathbb{N}$ y números naturales no nulos $n_{ij} \in \mathbb{N}$ únicos de modo que*

$$\begin{aligned} G &\simeq (\mathbb{Z}/p_1^{n_{11}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_1^{n_{1s_1}}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_r^{n_{r1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{n_{rs_r}}\mathbb{Z}) \\ &= \oplus_{ij}\mathbb{Z}/p_i^{n_{ij}}\mathbb{Z}. \end{aligned}$$

como grupo abeliano.

Demostración. Es consecuencia del teorema 4.4.10. □

2. Ejemplo: Clasifiquemos el $\mathbb{Z}$-módulo $M = \mathbb{Z}^3/\langle(2,4,2),(3,4,2),(2,2,2)\rangle$. Consideremos la aplicación lineal $\phi\colon \mathbb{Z}^3 \to \mathbb{Z}^3$, de matriz en las bases usuales

$$\phi \equiv \begin{pmatrix} 2 & 3 & 2 \\ 4 & 4 & 2 \\ 2 & 2 & 2 \end{pmatrix}$$

Tenemos que $M = \mathbb{Z}^3/\operatorname{Im}\phi$. Por transformaciones elementales obtenemos

$$\begin{pmatrix} 2 & 3 & 2 \\ 4 & 4 & 2 \\ 2 & 2 & 2 \end{pmatrix} \overset{C_2-C_1}{\rightsquigarrow} \begin{pmatrix} 2 & 1 & 2 \\ 4 & 0 & 2 \\ 2 & 0 & 2 \end{pmatrix} \overset{C_1xC_2}{\rightsquigarrow} \begin{pmatrix} 1 & 2 & 2 \\ 0 & 4 & 2 \\ 0 & 2 & 2 \end{pmatrix} \overset{\substack{C_2-2C_1 \\ C_3-2C_1}}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 2 & 2 \end{pmatrix} \overset{F_2xF_3}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 4 & 2 \end{pmatrix}$$

$$\overset{F_3-2F_2}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & -2 \end{pmatrix} \overset{C_3-C_2}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

Tenemos el diagrama

$$\begin{array}{ccccc} \mathbb{Z}^3 & \xrightarrow{\phi} & \mathbb{Z}^3 & \longrightarrow & \mathbb{Z}^3/\operatorname{Im}\phi = M \\ \uparrow{\scriptstyle C} & & \downarrow{\scriptstyle F} & & \| \downarrow{\scriptstyle \bar{F}} \\ \mathbb{Z}^3 & \xrightarrow{D} & \mathbb{Z}^3 & \longrightarrow & \mathbb{Z}^3/\operatorname{Im}D = \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \end{array}$$

Donde C viene dado por la composición de las transformaciones elementales de las columnas que hemos realizado, F por la composición de las transformaciones elementales de las filas que hemos realizado y D es la matriz diagonal de diagonal $1,2,2$. Por tanto, $M \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ y tenemos clasificado M: los divisores elementales de M son $2,2$.

Calculemos F^{-1}. Tenemos que $F = (\mathrm{Id} - 2\delta_{23}) \cdot X_{23}$, luego $F^{-1} = X_{23} \cdot (\mathrm{Id} + 2\delta_{23})$. Multiplicando por la derecha por la matriz identidad obtenemos que

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{F_3+2F_2}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} \overset{F_2\times F_3}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 0 \end{pmatrix} = F^{-1}.$$

Tenemos que $M = \overline{\langle(0,2,1)\rangle} \oplus \overline{\langle(0,1,0)\rangle} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

4.6. Clasificación de los endomorfismos lineales

1. Definición: Sean $T: E \to E$ y $T': E' \to E'$ dos endomorfismos k-lineales. Diremos que T es equivalente a T' si existe un isomorfismo lineal $\phi: E \to E'$, de modo que el diagrama

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ {\scriptstyle\phi}\downarrow\wr & & \wr\downarrow{\scriptstyle\phi} \\ E' & \xrightarrow[T']{} & E' \end{array}$$

es conmutativo (es decir, $T' = \phi \circ T \circ \phi^{-1}$).

En lenguaje matricial: "se dice que dos matrices cuadradas de orden n, A y A', son equivalentes si existe una matriz cuadrada invertible de orden n, B, tal que $A' = B \cdot A \cdot B^{-1}$".

2. Proposición: *Sean $T: E \to E$ y $T': E' \to E'$ dos endomorfismos k-lineales. T es equivalente a T' si y sólo si existen bases $\{e_i\}$ en E y $\{e'_j\}$ en E' de modo que la matriz de T en la base $\{e_i\}$ es igual a la matriz de T' en la base $\{e'_j\}$.*

Demostración. $\Rightarrow$) Consideremos un isomorfismo k-lineal $\phi: E \to E'$, de modo que el diagrama

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ {\scriptstyle\phi}\downarrow\wr & & \wr\downarrow{\scriptstyle\phi} \\ E' & \xrightarrow[T']{} & E' \end{array}$$

es conmutativo. Sea $\{e_i\}$ una base cualquiera de E. Entonces, $\{\phi(e_i)\}$ es una base de E' y la matriz de T en la base $\{e_i\}$ es igual a la matriz de T' en la base $\{\phi(e_i)\}$.

$\Leftarrow$) Sean $\{e_i\}$ en E y $\{e'_j\}$ en E' bases de modo que la matriz de T en la base $\{e_i\}_{i\in I}$ es igual a la matriz de T' en la base $\{e'_j\}_{i\in J}$. Implícitamente se está suponiendo que $I = J$. Entonces, el endomorfismo $\phi: E \to E'$ que cumple que $\phi(e_i) := e'_i$ es un isomorfismo k-lineal tal que el diagrama

$$\begin{array}{ccc} E & \xrightarrow{T} & E' \\ {\scriptstyle\phi}\downarrow\wr & & \wr\downarrow{\scriptstyle\phi} \\ E' & \xrightarrow[T']{} & E' \end{array}$$

es conmutativo.

□

3. Proposición: *Sean $T: E \to E$ y $T': E' \to E'$ dos endomorfismos k-lineales. T y T' son equivalentes si y sólo si E y E' son $k[x]$-módulos isomorfos.*

Demostración. $\Rightarrow$) Sea $\phi: E \to E'$ un isomorfismo k-lineal tal que $\phi \circ T = T' \circ \phi$. Entonces, ϕ es un isomorfismo de $k[x]$-módulos:

$$\phi(x \cdot e) = \phi(T(e)) = T'(\phi(e)) = x \cdot \phi(e),$$

para todo $e \in E$. Por tanto, $\phi(x^n \cdot e) = x^n \cdot \phi(e)$ y ϕ es un isomorfismo de $k[x]$-módulos.

$\Leftarrow$) Sea $\phi\colon E \to E'$ un isomorfismo de $k[x]$-módulos, En particular, $\phi(T(e)) = \phi(x \cdot e) = x \cdot \phi/e) = T'(\phi(e))$, para todo $e \in E$. Luego, $\phi \circ T = T' \circ \phi$ y T y T' son equivalentes.

□

4. Teorema de clasificación: *Sea E un k-espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal. Entonces, existen polinomios irreducibles mónicos $p_1(x), \dots, p_r(x) \in k[x]$ y $0 \neq n_{ij} \in \mathbb{N}$ únicos de modo que*

$$E \simeq (k[x]/(p_1(x)^{n_{11}}) \oplus \cdots \oplus k[x]/(p_1(x)^{n_{1s_1}})) \oplus \cdots \oplus (k[x]/(p_r(x)^{n_{r1}}) \oplus \cdots \oplus k[x]/(p_r(x)^{n_{rs_r}})) = \oplus_{ij} k[x]/(p_i(x)^{n_{ij}}).$$

como $k[x]$-módulos.

(Se dice que los $p_i(x)^{n_{ij}}$ son los divisores elementales asociados a T).

Demostración. Es consecuencia del teorema 4.4.10. □

Por tanto, los endomorfismos lineales, están clasificados, salvo equivalencia, por sus divisores elementales.

5. Corolario: *Sea E un $\mathbb{C}$-espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo $\mathbb{C}$-lineal. Entonces, existen $\alpha_1, \dots, \alpha_r \in \mathbb{C}$ y $0 \neq n_{ij} \in \mathbb{N}$ únicos de modo que*

$$E \simeq \oplus_{ij} \mathbb{C}[x]/((x - \alpha_i)^{n_{ij}}).$$

como $\mathbb{C}[x]$-módulos.

4.6.1. Matriz característica

Sea A un anillo euclídeo. Para el cálculo de los divisores elementales asociados a un A-módulo finito generado M es fundamental dar una presentación por módulos libres de M.

Sea E un k-espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal. Como sabemos, podemos considerar E como $k[x]$-módulo: $p(x) \cdot e = p(T)(e)$, para todo $e \in E$ y $p(x) \in k[x]$. Demos una presentación de E por $k[x]$-módulos libres.

Sea $\{e_1, \dots, e_n\}$ una base de E y (a_{ij}) la matriz asociada a T en la base dada. Consideremos el $k[x]$-módulo libre

$$L = k[x] \oplus \overset{n}{\cdots} \oplus k[x] \underset{Not.}{=} k[x] * e_1 \oplus \overset{n}{\cdots} \oplus k[x] * e_n.$$

Entonces, L es un $k[x]$-módulo libre de base $\{e_1, \dots, e_n\}$.

6. Definición: Consideremos los morfismos de $k[x]$-módulos $T\colon L \to L$, determinado por $T(e_i) := \sum_j a_{ij} e_i$ y $x \cdot \mathrm{Id}\colon L \to L$, determinado por $(x \cdot \mathrm{Id})(e_i) = x * e_i$. La matriz del el endomorfismo de $k[x]$-módulos $x \cdot \mathrm{Id} - T\colon L \to L$ en la base $\{e_i\}$ es igual a

$$x \cdot \mathrm{Id} - (a_{ij}),$$

y se denomina la matriz característica de T.

Consideremos el morfismo de $k[x]$-módulos $\pi\colon L \to E$, $\pi(e_i) := e_i$. Obviamente, π es un epimorfismo. Veamos que $\operatorname{Ker}\pi = \operatorname{Im}(x\cdot \operatorname{Id} - T)$: Dado $(x\cdot \operatorname{Id} - T)(e_i) \in \operatorname{Im}(x\cdot \operatorname{Id} - T)$, tenemos que

$$\pi((x\cdot \operatorname{Id} - T)(e_i)) = \pi(\sum_i x * e_i - T(e_i)) = \sum_i (x\cdot e_i - T(e_i)) = 0.$$

Luego, $\operatorname{Im}(x\cdot \operatorname{Id} - T) \subseteq \operatorname{Ker}\pi$. Veamos que $\operatorname{Ker}\pi \subseteq \operatorname{Im}(x\cdot \operatorname{Id} - T)$: Sea $\sum_i p_i(x) * e_i \in \operatorname{Ker}\pi$ (luego, $\sum_i p_i(T)(e_i) = 0$). En $L/\operatorname{Im}(x\cdot \operatorname{Id} - T)$ tenemos que $\overline{x\cdot m} = \overline{T(m)}$, para todo $m \in L$. Por tanto, $\overline{x^2\cdot m} = x\cdot \overline{x\cdot m} = x\cdot \overline{T(m)} = \overline{x\cdot T(m)} = \overline{T^2(m)}$. Recurrentemente, $\overline{x^n\cdot m} = \overline{T^n(m)}$ y $\overline{p(x)\cdot m} = \overline{p(T)(m)}$, para todo $p(x) \in k[x]$. Luego,

$$\overline{\sum_i p_i(x) * e_i} = \overline{\sum_i p_i(T)(e_i)} = \overline{0}$$

Entonces, $\sum_i p_i(x) * e_i \in \operatorname{Im}(x\cdot \operatorname{Id} - T)$ y $\operatorname{Im}(x\cdot \operatorname{Id} - T) = \operatorname{Ker}\pi$.

En conclusión, tenemos que L es un $k[x]$-módulo libre de base $\{e_i\}$, los morfismos de $k[x]$-módulos

$$\boxed{L \xrightarrow{x\cdot \operatorname{Id} - T} L \xrightarrow{\pi} E}$$

de modo que $L/\operatorname{Im}(x\cdot \operatorname{Id} - T) \simeq E$, $\bar{l} \mapsto \pi(l)$, y la matriz del endomorfismo $T - x\cdot$ en la base $\{e_i\}$ de L es igual a $x\cdot \operatorname{Id} - (a_{ij})$.

Mediante transformaciones elementales de la matriz $x\cdot \operatorname{Id}(a_{ij})$ obtenemos una matriz diagonal D (cuyos coeficientes de la diagonal son ciertos polinomios $p_1(x), \ldots, p_n(x)$ con coeficientes en k) y un diagrama conmutativo

$$\begin{array}{ccccc} L & \xrightarrow{x\cdot \operatorname{Id} - T} & L & \xrightarrow{\quad\pi\quad} & E \\ {\scriptstyle C}\uparrow\wr & & \wr\downarrow{\scriptstyle F} & & \wr\downarrow{\scriptstyle \bar{F}} \\ L & \xrightarrow[D]{} & L & \xrightarrow{\pi'} & L/\operatorname{Im} D = k[x]/(p_1(x)) \oplus \cdots \oplus k[x]/(p_n(x)) \end{array}$$

donde π' es el morfismo de paso al cociente y $\bar{F}(e) = \overline{F(e)}$. Por último, $\bar{F}^{-1}((\overline{q_i(x)})) = \pi(F^{-1}((q_i(x))))$.

7. Ejemplo: Clasifiquemos el endomorfismo $\mathbb{Q}$-lineal $T\colon \mathbb{Q}^4 \to \mathbb{Q}^4$ de matriz

$$\begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 0 & 2 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \end{pmatrix}$$

en la base estándar. Diagonalicemos la matriz característica

$$\begin{pmatrix} x-2 & 0 & 1 & 0 \\ 0 & x & -2 & 1 \\ -1 & 0 & x & 0 \\ 0 & -1 & 0 & x+2 \end{pmatrix} \overset{F_1 x F_3}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & x & 0 \\ 0 & x & -2 & 1 \\ x-2 & 0 & 1 & 0 \\ 0 & -1 & 0 & x+2 \end{pmatrix}$$

$$\overset{F_3+(-2+x)F_1}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & x & 0 \\ 0 & x & -2 & 1 \\ 0 & 0 & x^2-2x+1 & 0 \\ 0 & -1 & 0 & x+2 \end{pmatrix} \overset{C_3+xC_1}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & x & -2 & 1 \\ 0 & 0 & x^2-2x+1 & 0 \\ 0 & -1 & 0 & x+2 \end{pmatrix}$$

$$\overset{F_2 x F_4}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & x+2 \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & x & -2 & 1 \end{pmatrix} \overset{F_4+xF_2}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 2+x \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & -2 & (x+1)^2 \end{pmatrix}$$

$$\overset{C_4+(x+2)C_2}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & -2 & (x+1)^2 \end{pmatrix} \overset{F_3 \times F_4}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & (x+1)^2 \\ 0 & 0 & (x-1)^2 & 0 \end{pmatrix}$$

$$\overset{F_4+\frac{(x-1)^2}{2}F_3}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & (x+1)^2 \\ 0 & 0 & 0 & \frac{(x-1)^2(x+1)^2}{2} \end{pmatrix} \overset{C_4+\frac{(x+1)^2}{2}C_3}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & \frac{(x-1)^2(x+1)^2}{2} \end{pmatrix}$$

Por tanto, los divisores elementales asociados a T son $(x-1)^2, (x+1)^2$. El endomorfismo T es equivalente al endomorfismo

$$x\cdot : \mathbb{Q}[x]/((x-1)^2(x+1)^2) \to \mathbb{Q}[x]/((x-1)^2(x+1)^2)$$

Si en $\mathbb{Q}[x]/((x-1)^2(x+1)^2)$ tomamos la base

$$(*) \qquad \{\overline{(x+1)^2}, \overline{(x-1)(x+1)^2}, \overline{(x-1)^2}, \overline{(x+1)(x-1)^2}\},$$

la matriz de $x\cdot$ es

$$(**) \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Por último detallemos el isomorfismo $\bar{F}^{-1}: \mathbb{Q}[x]/((x-1)^2(x-1)(x+1)^2) \simeq \mathbb{Q}^4$:

$$F^{-1} = X_{13} \circ (\mathrm{Id} + (2-x)\delta_{31}) \circ (\mathrm{Id} - x\delta_{42}) \circ X_{34} \circ (\mathrm{Id} - \frac{(x-1)^2}{2}\delta_{43})$$

$\bar{F}^{-1}(\bar{1}) = \pi(F^{-1}(0,0,0,1))$ y

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \overset{F_4-\frac{(x-1)^2}{2}F_3}{\rightsquigarrow} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \overset{F_3 \times F_4}{\rightsquigarrow} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \overset{F_4-xF_2}{\rightsquigarrow} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \overset{F_3+(2-x)F_1}{\rightsquigarrow} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \overset{F_1 \times F_3}{\rightsquigarrow} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = F^{-1} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Luego, $\bar{F}^{-1}(\bar{1}) = (1,0,0,0)$. Vía $\bar{F}^{-1}$ la base correspondiente a la base $(*)$ es

$$\{(8,2,4,0),(4,6,4,2),(0,2,0,0),(0,2,0,2)\}$$

La matriz asociada a T en esta base es $(**)$.

4.6.2. Polinomio característico. Teorema de Hamilton-Cayley

Sea E un k-espacio vectorial y $T\colon E \to E$ un endomorfismo k-lineal. Consideremos en E la estructura de $k[x]$-módulo definida por T. Se cumple que el ideal anulador del $k[x]$-módulo E, está generado por el polinomio anulador mínimo de T:

$\mathrm{Anul}(E) := \{p(x) \in k[x]\colon\ p(x)\cdot e = 0,\ \forall e \in E\} = \{p(x) \in k[x]\colon\ p(T)(e) = 0,\ \forall e \in E\} = \{p(x) \in k[x]\colon\ p(T) = 0\}$. $\mathrm{Anul}(E)$ está generado, como todo ideal de $k[x]$, por el polinomio mónico de grado mínimo que pertenezca a $\mathrm{Anul}(E)$, es decir, por el polinomio mínimo anulador de T.

Por la proposición 4.4.12, el polinomio mínimo anulador de T es igual al mínimo común múltiplo de los divisores elementales.

8. Definición: Sea E un k-espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal. Se dice que $c_T(x) := \det(x\cdot \mathrm{Id} - T) \in k[x]$ es el polinomio característico de T.

9. Observación: Dada una base de E, y la matriz (a_{ij}) asociada a T en dicha base, se define $\det(x\cdot \mathrm{Id} - T) := \det(x\cdot \mathrm{Id} - (a_{ij}))$. Si consideramos otra base de E, entonces la matriz asociada a T en la nueva base es $(a'_{ij}) = (b_{ij})\cdot(a_{ij})\cdot(b_{ij})^{-1}$ (donde (b_{ij}) es la matriz de cambio de base. Observemos que

$$\begin{aligned}\det(x\cdot \mathrm{Id} - (a_{ij})) &= \det((b_{ij})\cdot(x\cdot \mathrm{Id} - (a_{ij}))\cdot(b_{ij})^{-1}) = \det(x\cdot \mathrm{Id} - (b_{ij})\cdot(a_{ij})\cdot(b_{ij})^{-1}) \\ &= \det(x\cdot \mathrm{Id} - (a'_{ij}))\end{aligned}$$

10. Proposición: *Sea E un k-espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal. El polinomio característico de T es igual al producto de los divisores elementales de T.*

Demostración. Sea $\{e_1,\dots,e_n\}$ una base de E, sea (a_{ij}) la matriz asociada a T en esta base, $L = \oplus_{i=1}^n k[x] * e_i$ y $\phi\colon L \to L$ el endomorfismo de $k[x]$-módulos de matriz en la base $\{e_i\}$, $x\,\mathrm{Id} - (a_{ij})$. Sabemos que $E \simeq L/\mathrm{Im}\,\phi$. Por transformaciones elementales de los vectores de la base $\{e_i\}$ de L, que son cambios de base de determinante ± 1, sabemos que podemos obetener unas nuevas bases donde la matriz de ϕ es diagonal

$$\phi \equiv \begin{pmatrix} q_1(x) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & q_n(x) \end{pmatrix}$$

Por tanto,

$$c_T(x) = \pm\det(\phi) = \pm q_1(x)\cdots q_n(x).$$

Por otra parte, obtenemos que $E \simeq k[x]/(q_1(x)) \oplus \cdots \oplus k[x]/(q_n(x))$. Descomponiendo cada polinomio $q_i(x)$ en potencias de irreducibles (y aplicando el teorema chino de los restos)

obteníamos los divisores elementales de T. Luego, $q_1(x)\cdots q_n(x)$ es el producto de los divisores elementales de T (salvo signo). En conclusión, $c_T(x)$ (que es mónico) coincide con el producto de los divisores elementales (que son mónicos).

□

11. Teorema de Hamilton-Cayley: *Sea E un espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal. Sea $c_T(x)$ el polinomio característico de T. El polinomio característico es múltiplo del polinomio mínimo anulador, es decir,*

$$c_T(T) = 0.$$

Además, los polinomios irreducibles que dividen al polinomio característico son los mismos que los que dividen al polinomio mínimo anulador.

Demostración. El polinomio característico es el producto de todos los divisores elementales y el polinomio mínimo anulador es el mínimo común múltiplo de ellos. Por lo tanto, el polinomio característico es múltiplo del anulador, es decir, $c_T(T) = 0$; y los polinomios irreducibles que dividen al polinomio característico son los mismos que los que dividen al polinomio mínimo anulador.

□

12. Definición: Se dice que un vector no nulo $e \in E$ es un vector propio de valor propio $\lambda \in k$ si $T(e) = \lambda e$.

13. Proposición: *Existe un vector propio $e \in E$ de valor propio $\lambda \in k$ si y sólo si λ es una raíz de $c_T(x)$.*

Demostración. Existe un vector propio $e \in E$ de valor propio $\lambda \in k$ si y sólo si $\operatorname{Ker}(\lambda \cdot \operatorname{Id} - T) \neq 0$, que equivale a que $\det(\lambda \cdot \operatorname{Id} - T) = 0$, que equivale a $c_T(\lambda) = 0$. □

14. Definición: Se dice que un endomorfismo k-lineal $T\colon E \to E$ diagonaliza si y sólo si existe una base de E formada por vectores propios.

15. Proposición: *Sea E un k-espacio vectorial de dimensión finita y $T\colon E \to E$ un endomorfismo k-lineal. T diagonaliza si y sólo si el polinomio mínimo anulador de T tiene todas sus raíces en k y son de multiplicidad* 1.

Demostración. $\Rightarrow$) Sea $\{e_1,\dots,e_n\}$ una base de E tal que $T(e_i) = \lambda_i e_i$. Sean $\lambda_{i_1},\dots,\lambda_{i_r}$ distintos entre sí de modo que $\{\lambda_{i_1},\dots,\lambda_{i_r}\} = \{\lambda_1,\dots,\lambda_n\}$. Entonces, el polinomio anulador de T es $\prod_{j=1}^{r}(x - \lambda_{i_j})$

$\Leftarrow$) Sean $\lambda_1,\dots,\lambda_r \in k$ distintos tal que el polinomio anulador de T sea $p(x) = \prod_{i=1}^{r}(x - \lambda_i)$, con $\lambda_i \neq \lambda j$ cuando $i \neq j$. Entonces,

$$E = \operatorname{Ker} p(x)\cdot = \operatorname{Ker}(x - \lambda_1)\cdot \oplus \cdots \oplus \operatorname{Ker}(x - \lambda_r)\cdot$$

Sea $\{e_{ij}\}_j$ una base de $\operatorname{Ker}(x - \lambda_i)\cdot = \operatorname{Ker}(T - \lambda_i \operatorname{Id})$. Entonces, $\{e_{ij}\}_{ij}$ es una base de E formada por vectores propios.

□

16. Corolario: *Sea E un k-espacio vectorial de dimensión finita y $T: E \to E$ un endomorfismo k-lineal. Si todas las raíces del polinomio característico de T están en k y son de multiplicidad 1, entonces T diagonaliza.*

Demostración. Si todas las raíces del polinomio característico son de multiplicidad 1 entonces el polinomio característico coincide con el polinomio anulador. Se concluye por la proposición 4.6.15. □

4.6.3. Bases de Jordan

Sea E un $\mathbb{C}$-espacio vectorial de dimensión finita y $T: E \to E$ un endomorfismo $\mathbb{C}$-lineal. Mediante la matriz característica y las transformaciones elementales sabemos construir un diagrama conmutativo

$$\begin{array}{ccc} E & \xrightarrow[\sim]{\phi} & \oplus_{ij}\mathbb{C}[x]/((x-\alpha_i)^{n_{ij}}) \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle x\cdot} \\ E & \xrightarrow[\phi]{\sim} & \oplus_{ij}\mathbb{C}[x]/((x-\alpha_i)^{n_{ij}}) \end{array}$$

Por tanto, la matriz de T en una base $\{e_i\}$ es igual a la matriz de $x\cdot$ en la base $\{\phi(e_i)\}$.

Calculemos la matriz de $x\cdot$ en una base conveniente.

17. Lema: *Sea $\lambda \in k$. Entonces, $\{\bar{1}, \overline{x-\lambda}, \ldots, \overline{(x-\lambda)}^{n-1}\}$ es una base del k-espacio vectorial $k[x]/((x-\lambda)^n)$.*

Demostración. Sabemos que las clases $\bar{1}, \bar{y}, \ldots, \bar{y}^{n-1}$ forman una base de $k[y]/(y^n)$. Haciendo el cambio $y = x - \lambda$ concluimos. □

Consideremos la aplicación lineal

$$x\cdot : k[x]/((x-\lambda)^n) \to k[x]/((x-\lambda)^n),\ \overline{p(x)} \mapsto \overline{x\cdot p(x)}.$$

Tomemos la base $\{e_j = \overline{(x-\lambda)}^j \mid 0 \le j \le n-1\}$. Se tiene

$$x\cdot e_j = x\cdot\overline{(x-\lambda)}^j = (x-\lambda)\cdot\overline{(x-\lambda)}^j + \lambda\overline{(x-\lambda)}^j = e_{j+1} + \lambda e_j$$

Por lo tanto, la matriz de $x\cdot$ es igual a

$$\begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix}$$

En general, dado un endomorfismo $\mathbb{C}$-lineal $T: E \to E$, sabemos que

$$E \simeq \underset{i,j}{\oplus}\mathbb{C}[x]/((x-\lambda_i)^{n_{ij}})$$

Tomando una base en cada sumando $\mathbb{C}[x]/((x-\lambda_i)^{n_{ij}})$, como acabamos de hacer, obtendremos una base de E, llamada base de Jordan. La matriz de T en esta base es de la forma llamada de Jordan:

$$\begin{pmatrix} (B_{11}) & & & \\ & \ddots & & \\ & & (B_{ij}) & \\ & & & \ddots \end{pmatrix}$$

siendo (B_{ij}) la siguiente matriz $n_{ij} \times n_{ij}$

$$(B_{ij}) = \begin{pmatrix} \lambda_i & & & \\ 1 & \lambda_i & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_i \end{pmatrix}$$

18. Ejercicio: Sea $E = k[x]/((x-\lambda_1)^{n_1}\cdots(x-\lambda_r)^{n_r})$, con $\lambda_i \neq \lambda_j$ para todo $i \neq j$ y $n_i > 0$ para todo i. Calcular la matrix de $x\cdot$ en la base

$$\{\overline{(x-\lambda_1)^{n_1}\cdots(x-\lambda_i)^{m_i}\cdots(x-\lambda_r)^{n_r}}\}_{1\leq i\leq r, 0\leq m_i<n_i}$$

Demos otro método para calcular una base de Jordan de T, una vez que hemos calculado los valores propios $\{\lambda_1,\cdots,\lambda_r\}$ de T, es decir, las raíces complejas del polinomio característico de T. Sea n_i el mínimo número natural tal que $\operatorname{Ker}(T-\lambda_i\cdot \mathrm{Id})^{n_i} = \operatorname{Ker}(T-\lambda_i\cdot \mathrm{Id})^{n_i+1}$. Puede comprobarse que el polinomio mínimo anulador de T es igual a $\prod_{i=1}^{r}(x-\lambda_i)^{n_i}$ y como sabemos

$$E = \oplus_{i=1}^{r} \operatorname{Ker}(T-\lambda_i\cdot \mathrm{Id})^{n_i}.$$

Demos una base de Jordan en cada sumando directo $\operatorname{Ker}(T-\lambda_i\cdot \mathrm{Id})^{n_i}$. Para no ir arrastrando índices, escribamos $\lambda_i = \lambda$, $n_i = n$ y $S = T - \lambda\cdot \mathrm{Id}$.

Consideremos la cadena de subespacios vectoriales $0 = \operatorname{Ker} S^0 \subset \operatorname{Ker} S^1 \subset \cdots \subset \operatorname{Ker} S^n$. Sea $\{e_{11},\ldots,e_{1r_1}\}$ una base suplementaria de $\operatorname{Ker} S^{n-1}$ en $\operatorname{Ker} S^n$. Sea $\{e_{21} := S(e_{11}),\ldots,e_{2r_1} = S(e_{1r_1}),e_{2,r_1+1},\ldots,e_{2,r_1+r_2}\}$ una base suplementaria de $\operatorname{Ker} S^{n-2}$ en $\operatorname{Ker} S^{n-1}$. Sea $\{e_{31} := S(e_{21}),\ldots,e_{3,r_1+r_2} = S(e_{2,r_1+r_2}),\ldots,e_{3,r_1+r_2+r_3}\}$ una base suplementaria de $\operatorname{Ker} S^{n-3}$ en $\operatorname{Ker} S^{n-2}$. Procediendo así sucesivamente, $\{e_{ij}\}$ es una base de $\operatorname{Ker} S^n$. Ordenemosla por columnas como sigue

$\operatorname{Ker} S^n \downarrow$	e_{11}	$\cdots$	e_{1r_1}							
$\operatorname{Ker} S^{n-1} \downarrow$	e_{21}	$\cdots$	e_{2r_1}	e_{2,r_1+1}	$\cdots$	e_{2,r_1+r_2}				
$\cup$	$\vdots$		$\vdots$	$\vdots$		$\vdots$	$\cdots$			
$\operatorname{Ker} S$	e_{n1}	$\cdots$	e_{nr_1}	e_{n,r_1+1}	$\cdots$	e_{n,r_1+r_2}	$\cdots$	$e_{n,\sum_{j=1}^{n-1} r_j+1}$	$\cdots$	$e_{n,\sum_{j=1}^{n} r_j}$

Observemos que cada columna j, $\{e_{i,j},e_{i+1,j},\ldots,e_{n,j}\}$ (con $0 < j - r_1 - \cdots - r_{i-1} \leq r_i$), es estable por S y la matriz de S sobre los vectores de esta columna es

$$B_{ii} = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \quad \text{(}n-i+1\text{ columnas)}$$

En la base $\{e_{ij}\}$, ordenada como sigue: $e_{ij} < e_{i'j'}$ si $j < j'$ ó $j = j'$ y $i < i'$, la matriz de S es

$$S \equiv \left(\begin{array}{c|c|c} B_1 & 0 & 0 \\ \hline 0 & \ddots & 0 \\ \hline 0 & 0 & B_n \end{array}\right), \quad B_i = \left(\begin{array}{c|c|c} B_{ii} & 0 & 0 \\ \hline 0 & \ddots\ r_i & 0 \\ \hline 0 & 0 & B_{ii} \end{array}\right), \quad B_{ii} = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}_{n-i+1}$$

Por último, recordemos que $T = S + \lambda \cdot \mathrm{Id}$. En la base escogida para S, la matriz de T es

$$T \equiv \left(\begin{array}{c|c|c} B_1 & 0 & 0 \\ \hline 0 & \ddots & 0 \\ \hline 0 & 0 & B_n \end{array}\right), \quad B_i = \left(\begin{array}{c|c|c} B_{ii} & 0 & 0 \\ \hline 0 & \ddots\ r_i & 0 \\ \hline 0 & 0 & B_{ii} \end{array}\right), \quad B_{ii} = \begin{pmatrix} \lambda & \cdots & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & \lambda \end{pmatrix}_{n-i+1}$$

4.6.4. Sistemas de ecuaciones diferenciales lineales

19. Consideremos el sistema de ecuaciones diferenciales con coeficientes constantes

$$\begin{array}{rcl} \frac{dx_1}{dt} & = & a_{11}x_1 + \cdots + a_{1n}x_n \\ \cdots & = & \cdots \\ \frac{dx_n}{dt} & = & a_{n1}x_1 + \cdots + a_{nn}x_n \end{array}$$

donde $A = (a_{ij})$ es una matriz cuadrada de orden n, con coeficentes complejos. De modo conciso escribiremos el sistema anterior $X' = AX$. Por cambio lineal de coordenadas. $Y = BX$, tenemos $Y' = BAB^{-1}Y$ y para B conveniente podemos conseguir que $J = BAB^{-1}$ sea una matriz de Jordan (que es una matriz triangular). Ahora ya es fácil calcular Y y por tanto podemos calcular X.

Demos otro modo de calcular las soluciones: Se define $e^{At} := \sum_{n=0}^{\infty} A^n \cdot \frac{t^n}{n!}$. Las soluciones del sistema $X' = AX$ son $\{X = e^{At} \cdot C\}$, siendo C una matriz columna de constantes. Para calcular e^{At} observemos que

$$e^{At} = e^{B^{-1}JBt} = B^{-1}e^{Jt}B$$

Sea D la matriz diagonal cuyos coeficientes en la diagonal son los de J. Escribamos $J = D + N$. Observemos que D y N conmutan y que $N^n = 0$. Entonces,

$$e^{Jt} = e^{Dt}e^{Nt} = e^{Dt} \cdot (Nt + \frac{N^2t^2}{2!} + \cdots + \frac{N^{n-1}t^{n-1}}{(n-1)!}).$$

20. Sea $X' = AX + B(t)$ un sistema lineal de ecuaciones diferenciales. Tenemos que $(D - A)X = B(t)$, luego una solución particular es

$$X = \frac{1}{D-A}B(t) = \frac{1}{D-A}(e^{At}e^{-At}B(t)) = e^{At}\frac{1}{D}(e^{-At}B(t))) = e^{At}\int e^{-At}B(t)dt.$$

21. Ejercicio: Resuélvanse los siguientes sistemas de ecuaciones diferenciales

$$\begin{array}{lll} \frac{dx}{dt} = x - 3y + 3z & \frac{dx}{dt} = 3x - y & \frac{dx}{dt} = -11x - 4y \\ \frac{dy}{dt} = -2x - 6y + 13z & \frac{dy}{dt} = x + y & \frac{dy}{dt} = 15x + 6y \\ \frac{dz}{dt} = -x - 4y + 8z & \frac{dy}{dt} = 3x + 5z - 3u & \\ & \frac{du}{dt} = 4x - y + 3z - u & \end{array}$$

22. Sea $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{R}[x]$ un polinomio de grado n. La ecuación diferencial

$$p(D)y = f(x)$$

es equivalente a al sistema de ecuaciones diferenciales lineales con coeficientes constantes de primer orden de n variables:

$$\begin{array}{l} x_1' = x_2 \\ \cdots \\ x_{n-1}' = x_n \\ x_n' = \frac{-1}{a_n} \cdot (\sum_{i=0}^{n-1} a_i x_{i+1}) + f(x) \end{array}$$

23. Ejercicio: Sea $A = (p_{ij}(D))$ una matriz, con $p_{ij}(x) \in \mathbb{C}[x]$. Pruébese que mediante las transformaciones elementales, el problema de resolver el sistema $AX(t) = Y(t)$, se reduce al problema de resolver ecuaciones $p(D)f(t) = h(t)$.

Resolver el sistema de ecuaciones diferenciales

$$\begin{array}{l} x'' - x + y' = e^t \\ x'' + 2x' + x + y'' = e^t \end{array}$$

4.7. Localización de módulos

1. Definición: Sea S un sistema multiplicativo de un anillo A y M un A-módulo, denotaremos por M_S:

$$\begin{aligned} M_S = \{ & \frac{m}{s},\ m \in M, s \in S \text{ de modo que} \\ & \frac{m}{s} = \frac{m'}{s'} \text{ si existen } t, t' \in S \text{ tales que } tm = t'm' \text{ y } ts = t's' \} \end{aligned}$$

y diremos que M_S es la localización de M por el sistema multiplicativo S.

Para definir una aplicación $f : M_S \to X$, tenemos que asignar a cada $\frac{m}{s} \in M_S$ un elemento $\phi(m,s)$, de modo que $\phi(tm, ts) = \phi(m,s)$, para todo $t \in S$.

Con las operaciones (bien definidas)

$$\begin{array}{c} \frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'} \\ \frac{a}{s} \cdot \frac{m}{s'} := \frac{am}{ss'} \end{array}$$

M_S tiene estructura de A_S-módulo. La aplicación canónica

$$M \to M_S,\ m \mapsto \frac{m}{1}$$

es un morfismo de A-módulos y diremos que es el morfismo de localización.

2. Ejercicio: Pruébese que $\frac{m}{s} = 0$ si y sólo sí existe un $t \in S$ de modo que $t \cdot m = 0$.

Todo morfismo $f : M \to N$ de A-módulos, induce la aplicación (bien definida)

$$f_S : M_S \to N_S, \frac{m}{s} \underset{\text{def}}{\mapsto} \frac{f(m)}{s},$$

que es morfismo de A_S-módulos.

3. Proposición: *Sea A un anillo y $S \subset A$ un sistema multiplicativo. Sean M y M' dos A-módulos. Entonces,*

$$(M \oplus M')_S = M_S \oplus M'_S$$

Demostración. Los morfismos $(M \oplus M')_S \to M_S \oplus M'_S$, $\frac{(m,m')}{s} \mapsto (\frac{m}{s}, \frac{m'}{s})$ y $M_S \oplus M'_S \to (M \oplus M')_S$, $(\frac{m}{s}, \frac{m'}{s'}) \mapsto \frac{(s'm, sm')}{ss'}$ son inversos entre sí. □

4. Ejemplo: Sea A un anillo íntegro y $\Sigma = A_{A\setminus\{0\}}$. Entonces,

$$(A^n)_{A\setminus\{0\}} = A_{A\setminus\{0\}} \oplus \overset{n}{\cdots} \oplus A_{A\setminus\{0\}} = \Sigma^n.$$

5. Proposición: *Sea A un anillo y $S \subset A$ un sistema multiplicativo. Sea M un A-módulo y $N \subseteq M$ un submódulo. Entonces, N_S es un submódulo de M_S (es decir, el morfismo $N_S \to M_S$ es inyectivo) y tenemos un isomorfismo natural*

$$M_S/N_S \simeq (M/N)_S.$$

Demostración. El morfismo $N_S \to M_S$ es inyectivo: Dado $\frac{n}{s} \in N_S$, si $\frac{n}{s} = 0$ en M_S, existe un elemento $s' \in S$ de modo que $s' \cdot n = 0$ en M (luego en N, por tanto $\frac{n}{s} = 0$ en N_S.

Consideremos el epimorfismo de paso al cociente $M \to M/N$. Localizando por S tenemos el morfismo $M_S \to (M/N)_S$, $m/s \mapsto \bar{m}/s$ que es claramente epiyectivo. Calculemos el núcleo: si $\bar{m}/s = 0$ entonces existe un elemento $s' \in S$ tal que $s' \cdot \bar{m} = 0$, es decir, $s' \cdot m \in N$, es decir, existe $n \in N$ de modo que $s' \cdot m = n$, luego $m/s = n/ss' \in N_S$. Recíprocamente, dado $n/s \in N_S$, entonces $\bar{n}/s = 0/s = 0$. □

6. Ejercicio: Sea $I \subseteq A$ un ideal y $S \subset A$ un sistema multiplicativo. Pruébese que $I_S = I \cdot A_S$.

4.8. Clasificación de los módulos sobre domios de ideales principales

El objetivo de esta sección es probar que el teorema de descomposición de un módulo finito generado M, sobre un anillo euclídeo, como suma directa de de A-módulos A/a_iA, es igualmente cierto para módulos finito generados sobre dominios de ideales principales.

Sea M un A-módulo. Recordemos que definíamos

$$T(M) = \{m \in M : \text{existe } a \in A \text{ no nulo tal que } am = 0\}$$

Es fácil comprobar que $T(M)$ coincide con el núcleo del morfismo de localización $M \to M_{A-\{0\}}$, $m \mapsto \frac{m}{1}$.

1. Proposición: *Sea A un anillo íntegro. Si M es un A-módulo finito generado libre de torsión entonces es un submódulo de un A-módulo libre del mismo rango.*

Demostración. Sea $\Sigma := A_{A\setminus\{0\}}$. Tenemos que $M = \langle m_1,\dots,m_n\rangle$ y el morfismo de localización $M \hookrightarrow M_{A\setminus\{0\}}$ es inyectivo. Evidentemente $\{\frac{m_1}{1},\dots,\frac{m_n}{1}\}$ es un sistema generador del Σ-espacio vectorial $M_{A\setminus\{0\}}$. Reordenado, podemos suponer que $\frac{m_1}{1},\dots,\frac{m_r}{1}$ es una base del Σ-espacio vectorial $M_{A\setminus\{0\}}$, $(r \le n)$. Por tanto, para cada m_j tendremos $\frac{m_j}{1} = \sum_{s=1}^{r} \frac{a_{js}}{b_{js}}\frac{m_s}{1}$. Denotemos $b = \prod_{i,j} b_{ij}$. Con las notaciones obvias, tendremos el siguiente diagrama conmutativo de morfismos inyectivos

$$\begin{array}{ccc} M & \hookrightarrow & M_{A\setminus\{0\}} \\ & \searrow & \uparrow \\ & & A\frac{m_1}{b}\oplus\cdots\oplus A\frac{m_r}{b} \end{array}$$

□

2. Proposición: *Sea A un dominio de ideales principales. Si M es un A-módulo finito generado libre de torsión entonces es un A-módulo libre.*

Demostración. Por la proposición 4.8.1, basta probar que los submódulos de un A-módulo libre son libres. Procederemos por inducción sobre el rango del módulo libre, que denotaremos L.

Si el rango de L es cero es obvio. Si el rango de L es uno entonces $L \simeq A$. Por tanto, todo submódulo M de L es isomorfo a un ideal de A, luego $M \simeq aA$. Si $a \neq 0$ entonces $A \simeq aA$, $b \mapsto ab$, luego M es libre de rango 1. Si $a = 0$ entonces $M = 0$.

Supongamos que el rango de L es $n > 1$. Podemos suponer que $L = A^n$. Sea $L' = A$ el submódulo de L, $L' := \{(a,0,\dots,0) \in L,\ \forall a \in A\}$. Obviamente $L'' := L/L'$, es un módulo libre de rango $n-1$. Sea $\pi\colon L \to L''$ el morfismo de paso al cociente. Dado $M \subseteq L$ consideremos el diagrama conmutativo

$$\begin{array}{ccccc} L' & \hookrightarrow & L & \xrightarrow{\pi} & L'' \\ \uparrow & & \uparrow & & \uparrow \\ L'\cap M = \operatorname{Ker}\pi_{|M} & \hookrightarrow & M & \xrightarrow{\pi_{|M}} & \pi(M) \end{array}$$

Por inducción $L' \cap M$ y $\pi(M)$ son libres de rango finito. Por tanto, como $\pi(M)$ es libre, el epimorfismo $M \to \pi(M)$ tiene sección y por el problema 9, $M = (L' \cap M) \oplus \pi(M)$. En conclusión, M es libre. □

3. Primer teorema de descomposición: Sea A un dominio de ideales principales y M un A-módulo finito generado. Se cumple que

$$M \simeq T(M) \oplus (M/T(M)),$$

(observemos que $T(M)$ es un módulo finito generado de torsión y $M/T(M)$ es un módulo finito generado libre). Además, si $M \simeq M' \oplus L$, siendo M' un A-módulo de torsión y L libre, entonces $M' \simeq T(M)$ y $L \simeq (M/T(M))$.

Demostración. $M/T(M)$ es un módulo finito libre de torsión. Por la proposición anterior $M/T(M)$ es un módulo libre. El epimorfismo de paso al cociente $M \to M/T(M)$ tiene sección, porque $M/T(M)$ es libre, luego $M \simeq T(M) \oplus (M/T(M))$.

Si $M \simeq M' \oplus L$, entonces $T(M) \simeq T(M' \oplus L) = T(M') \oplus T(L) = M'$. Luego $(M/T(M)) \simeq (M' \oplus L)/M' = L$. Hemos concluido.

□

Observemos que $M_{A-\{0\}} = (M/T(M))_{A-\{0\}}$. Por tanto, el rango de $M/T(M)$ es el de M. Así pues, en el teorema anterior $M/T(M)$ es un módulo libre de rango el de M.

Hemos reducido el problema de la clasificación de los módulos finitos sobre dominios de ideales principales, a la clasificación de los módulos finitos de torsión.

4. Notación: A partir de ahora, en esta sección, supondremos siempre que A es un dominio de ideales principales.

5. Proposición: *Sea $p \in A$ un elemento irreducible y sea $S = A\backslash(p)$. Para cada $f \in A_S$ existe un único $n \in \mathbb{N}$ de modo que $f = p^n \cdot g$, con $g \in A_S$ invertible. Por tanto, el único elemento irreducible de A_S, salvo multiplicación por invertibles, es p. Sea*

$$\delta : A_S\backslash\{0\} \to \mathbb{N},\ \delta(f) = n, \quad (\text{con } f = p^n \cdot g,\ g \in A_S \text{ invertible}).$$

Entonces, (A_S, δ) es un anillo euclídeo.

Demostración. Escribamos $f = \frac{a}{s} \in A_S$ y escribamos $a = p^n \cdot b$, con $b \in A$ no divisible por p, es decir, $b \in S$. Tenemos que en A_S, b es invertible, $g := \frac{b}{s}$ es invertible y $f = p^n \cdot g$.

Observemos que si $c \in A$ es invertible en A_S entonces $c \in S$: si $c \cdot \frac{a'}{s'} = 1$ entonces $c \cdot a' = s'$, si c fuese múltiplo de p, s' sería múltiplo de p y llegamos a contradicción.

Supongamos que $f = p^m \cdot g'$, con $g' = \frac{b'}{s'} \in A_S$ invertible. Tenemos que b' es invertible en A_S, luego no es múltiplo de p. Como $p^m \cdot g' = p^n \cdot g$, tenemos que $p^m \cdot b' \cdot s = p^n \cdot b \cdot s'$, luego $m = n$ (y $g' = g$).

La comprobación de que (A_S, δ) es un anillo euclídeo es sencilla. Como $\delta(p) = 1$ entonces p es irreducible en A_S: si $p = f_1 \cdot f_2$ en A_S, entonces $1 = \delta(p) = \delta(f_1) + \delta(f_2)$, luego $\delta(f_1) = 0$ (y f_1 es invertible) ó $\delta(f_2) = 0$ (y f_2 es invertible).

□

6. Proposición: *Sea $p \in A$ un elemento irreducible y sea $S = A\backslash(p)$. Sea M un A-módulo y supongamos que* $\mathrm{Anul}(M) = (p^n)$*, para cierto $n > 0$. Entonces, el morfismo natural de localización*

$$f : M \to M_S,\ m \mapsto \frac{m}{1},$$

es un isomorfismo.

Demostración. Si $f(m) = 0$, es decir, $\frac{m}{1} = 0$, existe un elemento del sistema multiplicativo $s \in S$ tal que $s \cdot m = 0$. Como s y p^n son primos entre sí, existen $\lambda, \mu \in A$ de modo que $\lambda \cdot s + \mu \cdot p^n = 1$, entonces $m = (\lambda \cdot s + \mu \cdot p^n) \cdot m = 0$.

Sea $\frac{m}{s} \in M_S$. Sean $\lambda, \mu \in A$ de modo que $\lambda \cdot s + \mu \cdot p^n = 1$. entonces

$$\frac{m}{s} = \frac{(\lambda \cdot s + \mu \cdot p^n)m}{s} = \frac{\lambda \cdot s \cdot m}{s} = \frac{\lambda \cdot m}{1} = f(\lambda \cdot m).$$

□

7. Proposición: *Sea M un A-módulo finito generado tal que* $\mathrm{Anul}(M) = p^n A$, *para cierto elemento irreducible $p \in A$ y cierto $0 \neq n \in \mathbb{N}$. Entonces, existen números naturales únicos $n_i \neq 0$ de modo que*

$$M \simeq \oplus_{n_i} A/p^{n_i}A.$$

Demostración. Sea $S = A\backslash(p)$. M_S es un A_S-módulo finito generado de torsión. Por tanto, por el teorema 4.4.10, existen números naturales n_i tales que $M_S = \oplus_{n_i} A_S/p^{n_i}A_S$. Luego,

$$M \overset{4.8.6}{=} M_S = \oplus_{n_i} A_S/p^{n_i}A_S = \oplus_{n_i}(A/p^{n_i}A)_S \overset{4.8.6}{=} \oplus_{n_i} A/p^{n_i}A.$$

La unicidad es consecuencia del teorema 4.4.8.

□

8. Teorema: *Sea A un dominio de ideales principales y M un A-módulo finito generado. Entonces, existen elementos irreducibles $p_1, \ldots, p_r \in A$ (p_i primo con p_j, para todo $i \neq j$), únicos salvo invertibles, y $n, 0 \neq n_{ij} \in \mathbb{N}$ únicos de modo que*

$$M \simeq A^n \oplus (A/p_1^{n_{11}}A \oplus \cdots \oplus A/p_1^{n_{1s_1}}A) \oplus \cdots \oplus (A/p_r^{n_{r1}}A \oplus \cdots \oplus A/p_r^{n_{rs_r}}A).$$

Demostración. La existencia de tal descomposición, es consecuencia de 4.8.3, 3.7.3 y 4.8.7. La unicidad es consecuencia de 4.4.8. □

4.9. Cuestionario

1. Diagonalizar mediante transformaciones elementales la matriz $\begin{pmatrix} 4 & 5 & 2 \\ 2 & 7 & 5 \\ 4 & 2 & 3 \end{pmatrix}$.
2. Resuélvase el sistema de ecuaciones diofánticas
$$2x + 3y + z = 6$$
$$4x + 2y + z = 5$$
3. Sean $M_1, M_2 \subseteq M$ dos A-submódulos. Pruébese que
$$\mathrm{Anul}(M_1 + M_2) = \mathrm{Anul}(M_1) \cap \mathrm{Anul}(M_2).$$
4. Calcúlese el ideal anulador del $k[x]$-módulo $k[x]/((x+1)^2) \oplus k[x]/(x^2 - 1)$.
5. Clasifíquense los grupos abelianos de orden 36.
6. Clasifíquese el grupo abeliano $M = \mathbb{Z}^3/\langle(2,3,2),(3,4,2),(2,2,2)\rangle$.
7. Sea G un grupo abeliano finito ¿a qué es igual el producto de los divisores elementales de G?
8. Sea T un endomorfismo lineal de un espacio vectorial de dimensión finita ¿a qué es igual el producto de los divisores elementales de T?

9. Sea $p(x) \in k[x]$ un polinomio mónico ¿Cálculese el polinomio característico del endomorfismo k-lineal $x\cdot\colon k[x]/(p(x)) \to k[x]/(p(x)), \overline{q(x)} \mapsto \overline{xq(x)}$?

10. Clasifíquense todos los endomorfismos nihilpotentes de un espacio vectorial de dimensión 4.

11. Clasifíquese el endomorfismo $\mathbb{R}$-lineal de matriz $\begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & -2 \\ 1 & 1 & 3 \end{pmatrix}$.

12. Calcúlese $(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z})_{\mathbb{Z}\setminus\{0\}}$.

13. Sea A un anillo íntegro y M un A-módulo. Probar que el núcleo del morfismo de localización $M \to M_{A\setminus\{0\}}$, $m \mapsto \frac{m}{1}$ es igual a $T(M)$.

4.10. Biografía de Camile Jordan

Camille Jordan's father, Esprit-Alexandre Jordan (1800-1888), was an engineer who had been educated at the École Polytechnique. Camille's mother, Joséphine Puvis de Chavannes, was the sister of the famous painter Pierre Puvis de Chavannes who was the foremost French mural painter of the second half of the 19th century. Camille's father's family were also quite well known; a grand-uncle also called Ennemond-Camille Jordan (1771-1821) achieved a high political position while a cousin Alexis Jordan (1814-1897) was a famous botanist.

Jordan studied at the Lycée de Lyon and at the Collège d'Oullins. He entered the École Polytechnique to study mathematics in 1855. This establishment provided training to be an engineer and Jordan, like many other French mathematicians of his time, qualified as an engineer and took up that profession. Cauchy in particular had been one to take this route and, like Cauchy, Jordan was able to work as an engineer and still devote considerable time to mathematical research. Jordan's doctoral thesis was in two parts with the first part Sur le nombre des valeurs des fonctions being on algebra. The second part entitled Sur des periodes des fonctions inverses des intégrales des différentielles algebriques was on integrals of the form $\int u\,dz$ where u is a function satisfying an algebraic equation $f(u,z) = 0$. Jordan was examined on 14 January 1861 by Duhamel, Serret and Puiseux. In fact the topic of the second part of Jordan's thesis had been proposed by Puiseux and it was this second part which the examiners preferred. After the examination he continued to work as an engineer, first at Privas, then at Chalon-sur-Saône, and finally in Paris.

Jordan married Marie-Isabelle Munet, the daughter of the deputy mayor of Lyon, in 1862. They had eight children, two daughters and six sons.

From 1873 he was an examiner at the École Polytechnique where he became professor of analysis on 25 November 1876. He was also a professor at the Collège de France from 1883 although until 1885 he was at least theoretically still an engineer

by profession. It is significant, however, that he found more time to undertake research when he was an engineer. Most of his original research dates from this period.

Jordan was a mathematician who worked in a wide variety of different areas essentially contributing to every mathematical topic which was studied at that time: on finite groups, on linear and multilinear algebra, on the theory of numbers, on the topology of polyhedra, differential equations, and mechanics.

Topology (called analysis situs at that time) played a major role in some of his first publications which were a combinatorial approach to symmetries. He introduced important topological concepts in 1866 built on his knowledge of Riemann's work in topology but not the work by Möbius for he was unaware of it. Jordan introduced the notion of homotopy of paths looking at the deformation of paths one into the other. He defined a homotopy group of a surface without explicitly using group terminology.

Jordan was particularly interested in the theory of finite groups. In fact this is not really an accurate statement, for it would be reasonable to argue that before Jordan began his research in this area there was no theory of finite groups. It was Jordan who was the first to develop a systematic approach to the topic. It was not until Liouville republished Galois's original work in 1846 that its significance was noticed at all. Serret, Bertrand and Hermite had attended Liouville's lectures on Galois theory and had begun to contribute to the topic but it was Jordan who was the first to formulate the direction the subject would take.

To Jordan a group was what we would call today a permutation group; the concept of an abstract group would only be studied later. To give an illustration of the way he tried to build up groups theory we will say a little about his contributions to finite soluble groups. The standard way to define such groups today would be to say that they are groups whose composition factors are abelian groups. Indeed Jordan introduced the concept of a composition series (a series of subgroups each normal in the preceding with the property that no further terms could be added to the series so that it retains that property). The composition factors of a group G are the groups obtained by computing the factor groups of adjacent groups in the composition series. Jordan proved the Jordan-Hölder theorem, namely that although groups can have different composition series, the set of composition factors is an invariant of the group.

Although the classification of finite abelian groups is straightforward, the classification of finite soluble groups is well beyond mathematicians today and for the foreseeable future. Jordan, however, clearly saw this as an aim of the subject, even if it was not one which might ever be solved. He made some remarkable contributions to how such a classification might proceed setting up a recursive method to determine all soluble groups of order n for a given n.

A second major piece of work on finite groups was the study of the general linear group over the field with p elements, p prime. He applied his work on classical groups to determine the structure of the Galois group of equations whose roots were chosen to be associated with certain geometrical configurations.

His work on group theory done between 1860 and 1870 was written up into a major text "Traité des substitutions et des équations algebraique" which he published in 1870. This treatise gave a comprehensive study of Galois theory as well as providing the first ever group theory book. For this work he was awarded the Poncelet Prize of

the Académie des Sciences. The treatise contains the "Jordan normal form" theorem for matrices, not over the complex numbers but over a finite field. He appears not to have known of earlier results of this type by Weierstrass. His book brought permutation groups into a central role in mathematics and, until Burnside wrote his famous group theory text nearly 30 years later, this work provided the foundation on which the whole subject was built. It would also be fair to say that group theory was one of the major areas of mathematical research for 100 years following Jordan's fundamental publication.

Jordan's use of the group concept in geometry in 1869 was motivated by studies of crystal structure. He considered the classification of groups of Euclidean motions. His work had gained him a wide international reputation and both Sophus Lie and Felix Klein visited him in Paris in 1870 to study with him. Jordan's interest in groups of Euclidean transformations in three dimensional space influenced Lie and Klein in their own theories of continuous and discontinuous groups.

The publication of Traité des substitutions et des équations algebraique did not mark the end of Jordan's contribution to group theory. He went on over the next decade to produce further results of fundamental importance. He studied primitive permutation groups and proved a finiteness theorem. He defined the class of a subgroup of the symmetric group to be $c > 1$ if c was the smallest number such that the subgroup had an element moving c points. His finiteness theorem showed that for a given c there are only finitely many primitive groups with class c other than the symmetric and alternating groups.

Generalising a result of Fuchs on linear differential equations, Jordan was led to study the finite subgroups of the general linear group of $n \times n$ matrices over the complex numbers. Although there are infinite families of such finite subgroups, Jordan found that they were of a very specific group theoretic structure which he was able to describe.

Another generalisation, this time of work by Hermite on quadratic forms with integral coefficients, led Jordan to consider the special linear group of $n \times n$ matrices of determinant 1 over the complex numbers acting on the vector space of complex polynomials in n indeterminates of degree m.

Jordan is best remembered today among analysts and topologists for his proof that a simply closed curve divides a plane into exactly two regions, now called the Jordan curve theorem. It was only his increased understanding of mathematical rigour which made him realise that a proof of such a result was necessary. He also originated the concept of functions of bounded variation and is known especially for his definition of the length of a curve. These concepts appears in his Cours d'analyse de l'École Polytechnique . Jordan was lecturing at the École Polytechnique and the book was written as a text for the students there. In some respects this is a little strange since it is a rigorous analysis text built on top of the attempts to put the topic on a firm foundation begun by Cauchy and given considerable impetus by Weierstrass. However, the courses at the École Polytechnique were supposed to train students to become civil and military engineers and this does not seem to be the approach which one would take trying to teach applications of the calculus to engineers. There had been a tradition of rigorous analysis at the École Polytechnique begun, of course, by Cauchy himself.

Jordan was aware that his work was at a level that would be somewhat inappropriate for engineering students for he once said to Lebesgue that he called it "École Polytechnique analysis course"since:

"*... one puts that on the cover to please the publisher...*"

Among Jordan's many contributions to analysis we should also mention his generalisation of the criteria for the convergence of a Fourier series.

The Journal de Mathématiques Pure et Appliquées was a leading mathematical journal and played a very significant part in the development of mathematics throughout the 19th century. It was usually known as the Journal de Liouville since Liouville had founded the journal in 1836. Liouville died in 1882 and in 1885 Jordan became editor of the Journal, a role he kept for over 35 years until his death.

In 1912 Jordan retired from his positions. The final years of his life were saddened, however, because of World War I which began in 1914. Between 1914 and 1916 three of his six sons were killed in the war. Of his three remaining sons, Camille was a government minister, Édouard was a professor of history at the Sorbonne, and the third son was an engineer.

Among the honours given to Jordan was his election to the Académie des Sciences on 4 April 1881. On 12 July 1890 he became an officer of the Légion d'Honneur. He was the Honorary President of the International Congress of Mathematicians at Strasbourg in September 1920.

Finally we should note some rather confusing facts. Although given Jordan's work on matrices and the fact that the Jordan normal form is named after him, the Gauss-Jordan pivoting elimination method for solving the matrix equation $Ax = b$ is not. The Jordan of Gauss-Jordan is Wilhelm Jordan (1842 to 1899) who applied the method to finding squared errors to work on surveying.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/)

4.11. Problemas

1. Sean p y q números primos distintos. Calcúlese el número de grupos abelianos finitos desisomorfos de orden p^2q.

2. Pruébese que un grupo abeliano finito que no sea cíclico contiene un subgrupo isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, para un cierto entero primo p.

3. Sea G un grupo abeliano finito. Demuéstrese que G es cíclico si y sólo si para cada n divisor del orden de G, existe un único subgrupo de G de orden n.

4. Sea G un subgrupo discreto del grupo aditivo de $\mathbb{R}^n$. Pruébese que existe un número natural $r \leq n$, tal que G está generado como $\mathbb{Z}$-módulo por r vectores linealmente independientes sobre $\mathbb{R}$.

5. Clasifíquese el endomorfismo "multiplicar por x" sobre el espacio

$$E = k[x]/(x) \oplus k[x]/(x^3) \oplus k[x]/(x^5)$$

6. Clasifíquense los endomorfismos nilpotentes de un espacio vectorial de dimensión 3. Problema análogo para espacios de dimensión 4 y 5.

7. Clasifíquense los endomorfismos T de un espacio vectorial real E, que cumplan

   a) Anulador de $T = (x-1)^2$, $\dim E = 5$.

   b) Anulador de $T = (x^2+4)^2(x+8)^2$, $\dim E = 8$.

8. Sea E el espacio vectorial real de todos los polinomios con coeficientes reales de grado menor que 6, y sea D el operador derivada sobre E. Clasifíquese el endomorfismo $T = D^2$.

9. Sea $(G,+)$ un grupo finito abeliano. Probar que G es cíclico si y sólo si $n = |G|$ es el mínimo número natural (no nulo) tal que $n \cdot g = 0$ para todo $g \in G$.

10. Pruébese que un grupo abeliano finito generado es cíclico si y sólo si tiene un único factor invariante.

11. Clasifíquense sobre el cuerpo racional los endomorfismos

$$A = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 2 & -1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & -1 \end{pmatrix}$$

    Dar una base de Jordan, para B.

12. Sean $T, T' : E \to E$ dos endomorfismos lineales de un espacio vectorial de dimensión finita, de modo que en cierta base la matriz de T es la transpuesta de la de T'. Pruébese que T y T' son endomorfismos equivalentes.

13. Sea A un anillo euclídeo y (a_{ij}) una matriz con coeficientes $a_{ij} \in A$. Sustituyendo de modo conveniente y sucesivo la fila F_i por la fila $F_i + b_j F_j$, $i \neq j$, $b_j \in A$ o permutando la fila F_i por la F_j ($i \neq j$ y b_j arbitrarios) , demuéstrese que la matriz (a_{ij}) es triangulable. Si admitimos, además, las mismas transformaciones "elementales" con las columnas, demuéstrese que (a_{ij}) es diagonalizable. Resolver el sistema de ecuaciones diofánticas

$$\begin{aligned} 7x + 5y &= 1 \\ 5x + 3y &= 3 \end{aligned}$$

14. Clasifíquense los $\mathbb{Z}$-módulos

$$(\mathbb{Z}\times\mathbb{Z})/\langle(7,5),(5,3)\rangle \text{ y } (\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z})/\langle(12,30,24),(4,8,6),(6,4,8)\rangle.$$

15. Sea $p(x) = \prod_{i=1}^{r}(x-\alpha_i)^{n_i} \in k[x]$, con $\alpha_i \neq \alpha_j$ para todo $i \neq j$. Consideremos el endomorfismo k-lineal

$$x\cdot : k[x]/(p(x)) \to k[x]/(p(x)),\ \overline{q(x)} \mapsto \overline{x\cdot q(x)}.$$

    Pruébese que $\{\overline{(x-\alpha_1)^{n_1}\cdots(x-\alpha_j)^{m_j}\cdots(x-\alpha_r)^{n_r}}, \forall\, 0 \leq m_j < n_j, \forall j\}$ es una base de Jordan de $x\cdot$.

16. Mediante transformaciones elementales de la matriz característica calcúlese los divisores elementales $p_i(x)^{n_{ij}}$ del endomorfismo de $\mathbb{R}^3$ de matriz

$$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & -2 \\ 1 & 1 & 3 \end{pmatrix}$$

Calcúlense $e_{ij} \in \mathbb{R}^3$ de modo que $\mathbb{R}^3 = \oplus_{ij}(k[x]/(p_i(x)^{n_{ij}})e_{ij}$.

17. Pruébese que si el polinomio característico de un endomorfismo lineal tiene todas sus raíces distintas entonces coincide con el polinomio anulador del endomorfismo.

18. Sea $T\colon E \to E$ un endomorfismo lineal de un espacio vectorial de dimensión finita. Pruébese que la condición necesaria y suficiente para que el endomorfismo $p(T)$ sea invertible es que $p(x)$ y $c_T(x)$ sean primos entre sí.

19. Sea $T\colon E \to E$ un endomorfismo lineal de un espacio vectorial de dimensión finita. Sea $E' \subseteq E$ un subespacio estable por T. Denotemos $\bar{T}\colon E/E' \to E/E'$, $\bar{T}(\bar{e}) = \overline{T(e)}$, el endomorfismo inducido por T en E/E'. Pruébese que

$$c_T(x) = c_{T_{|E'}}(x) \cdot c_{\bar{T}}(x)$$

20. Sea E un $\mathbb{C}$-espacio vectorial de dimensión n y T un endomorfismo de E. Sea $c_T(x) = \prod_{i=1}^{n}(x - \alpha_i)$ la descomposición en factores irreducibles del polinomio característico de T. Pruébese que si $p(x)$ es un polinomio con coeficientes en $\mathbb{C}$, entonces

$$c_{p(T)}(x) = \prod_{i=1}^{n}(x - p(\alpha_i))$$

En particular, se tiene que $\operatorname{tr}(p(T)) = \sum_{i=1}^{n} p(\alpha_i)$, $\det(p(T)) = \prod_{i=1}^{n} p(\alpha_i)$.

21. Sea E un $\mathbb{C}$-espacio vectorial de dimensión finita. Sea $T\colon E \to E$ un endomorfismo $\mathbb{C}$-lineal de E. Demuéstrese que si $c_T(x)$ es el polinomio característico de T considerado como endomorfismo $\mathbb{C}$-lineal, entonces el polinomio característico de T considerado como endomorfismo $\mathbb{R}$-lineal es $c_T(x) \cdot \overline{c_T(x)}$ (donde $\overline{c_T(x)}$ es el conjugado de $c_T(x)$).

22. Consideremos un sistema de ecuaciones

$$\begin{aligned} x_{n+1} &= a_{11}x_n + a_{12}y_n + a_{13}z_n \\ y_{n+1} &= a_{21}x_n + a_{22}y_n + a_{23}z_n \\ z_{n+1} &= a_{31}x_n + a_{32}y_n + a_{33}z_n \end{aligned}$$

con $a_{ij} \in \mathbb{C}$, para todo i, j. Plantéese la resolución de este sistema de ecuaciones.

Solución de los problemas del capítulo primero

P1. a $\Rightarrow$ b. $\phi(gg') = (gg')^{-1} = g'^{-1}g^{-1} = g^{-1}g'^{-1} = \phi(g)\phi(g')$. b. $\Rightarrow$ a. Sabemos que $(gg')^{-1} = g^{-1}g'^{-1}$, luego tomando inversos, $gg' = g'g$.

a. $\Rightarrow$ c. $\phi(gg') = (gg')^2 = gg'gg' = g^2g'^2 = \phi(g)\phi(g')$. c. $\Rightarrow$ a. Como $gg'gg' = g^2g'^2$, multiplicando a la derecha por g^{-1} y por la izquierda por g'^{-1}, obtenemos $gg' = g'g$.

a. $\Rightarrow$ d. $\phi((g,g')\cdot(h,h')) = \phi(gh,g'h') = ghg'h' = gg'hh' = \phi(g,g')\cdot\phi(h,h')$. d. $\Rightarrow$ a. Como $ghg'h' = gg'hh'$ entonces $hg' = g'h$.

P2. Veamos que τ_a es un morfismo de grupos: $\tau_a(gg') = agg'a^{-1} = aga^{-1}ag'a^{-1} = \tau_a(g)\tau_a(g')$. Veamos que la aplicación inversa de τ_a es $\tau_{a^{-1}}$:

$$\tau_{a^{-1}}(\tau_a(g)) = \tau_{a^{-1}}(aga^{-1}) = a^{-1}aga^{-1}a = g,$$

e igualmente $\tau_a(\tau_{a^{-1}}(g)) = g$. Veamos que el morfismo $\tau\colon G \to \mathrm{Aut}(G)$, $\tau(a) := \tau_a$ es morfismo de grupos:

$$\tau(aa')(g) = \tau_{aa'}(g) = aa'g(aa')^{-1} = aa'ga'^{-1}a^{-1} = \tau_a(\tau_{a'}(g)) = \tau(a)(\tau(a')(g)),$$

luego $\tau(aa') = \tau(a)\circ\tau(a')$.

P3. Supongamos $x\cdot y \in H$, para todo $x,y \in H$. Entonces, dado $x \in H$, $x^2 \in H$, luego $x^3 \in H$, luego $x^n \in H$, para todo $n > 0$. Como H es finito, existen $n > m$ tales que $x^n = x^m$, luego $x^{n-m} = 1$ y tenemos que $1 \in H$ y $x^{-1} = x^{n-m-1} \in H$. Luego, H es subgrupo.

Si $G = \mathbb{Z}$ y $H = \mathbb{N}$, tenemos que s $x + y \in H$, para todo $x,y \in H$, pero H no es un subgrupo de G.

P4. Supongamos que $xH = H$, para todo $x \in H$. Entonces, dado $x \in H$, $x^2 \in H$, luego $x^3 \in H$, luego $x^n \in H$, para todo $n > 0$. Como H es finito, existen $n > m$ tales que $x^n = x^m$, luego $x^{n-m} = 1$ y tenemos que $1 \in H$ y $x^{-1} = x^{n-m-1} \in H$. Luego, H es subgrupo.

P5. a) $\langle 3,5\rangle = m.c.d.(3,5)\mathbb{Z} = \mathbb{Z}$.

b) $\langle (2,0),(0,5)\rangle 2\mathbb{Z}\times 5\mathbb{Z}$. $\langle (2,3),(4,5)\rangle = \langle (2,3),(0,-1)\rangle = \langle (2,0),(0,1)\rangle = 2\mathbb{Z}\times\mathbb{Z}$.

c) $(1,2,3) = (1,2)(2,3)$. En el grupo generado tenemos ya 4 elementos (contando Id), luego por el teorema de Lagrange, el grupo generado es S_3.

d) $\langle 1\rangle = \mathbb{Z}$. $\langle \frac{1}{2}\rangle = \mathbb{Z}\cdot\frac{1}{2} = \{\frac{n}{2},\ n\in\mathbb{Z}\}$. $\langle \frac{1}{6},\frac{1}{8}\rangle = \langle \frac{4}{24},\frac{3}{24}\rangle = \frac{1}{24}\cdot\langle 4,3\rangle = \frac{1}{24}\mathbb{Z}$.

P6. Por el teorema de Lagrange, el orden de todo subgrupo H de G es 1 o $p = |G|$. Por tanto, G no contiene más subrgupos que el trivial $\{1\}$ y el total. Por tanto, dado $g \neq 1$, tenemos que $\langle g\rangle = G$.

P7. Sea $g \in G$, $g \neq 1$. Tenemos que $\langle g\rangle = G$. Si $|G| = \infty$, entonces $G \simeq \mathbb{Z}$, que contiene muchos subgrupos y llegamos a contradicción. Luego, $G \simeq \mathbb{Z}/n\mathbb{Z}$. Si n no es primo, $n = mm'$, con $1 < m, m' < n$, entonces el subgrupo $\langle \bar{m}\rangle$ es de orden m' y tenemos un subgrupo que no es el trivial ni el total y llegamos a contradicción.

P8. Si $f : G \to G'$ es un isomorfismo de grupos, entonces $\mathrm{ord}(g) = \mathrm{ord}(f(g))$, para todo g. El morfismo $\tau_b : G \to G$, $\tau_b(a) = bab^{-1}$ es un isomorfismo de grupos, luego $\mathrm{ord}(a) = \mathrm{ord}(\tau(a))$. Sea $a' = ab$, entonces

$$\mathrm{ord}(ab) = \mathrm{ord}(a') = \mathrm{ord}(ba'b^{-1}) = \mathrm{ord}(ba).$$

P9. a) Dados $z, z' \in \mu_n$, entonces $zz' \in \mu_n$, porque $(zz')^n = z^n z'^n = 1\cdot 1 = 1$. También, $z^{-1} \in \mu_n$, porque $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$.

b) μ_n está generado por $e^{\frac{2\pi i}{n}}$, que tiene orden n.

P10. El morfismo $\phi : \mathrm{Ker}\,\pi \times G' \to G$, $\phi(k,g') := k\cdot s(g')$ es un isomorfismo. Si $(k,g') \in \mathrm{Ker}\,\phi$, entonces $\phi(k,g') = 1$, entonces $k\cdot s(g') = 1$, tomando π, $1 = \pi(k)\cdot\pi s(g') = 1\cdot g'$, luego $g' = 1$ y $k = 1$. Entonces, $(k,g') = 1$ y ϕ es inyectiva. Dado $g \in G$, entonces $(s\pi(g))^{-1} \in \mathrm{Ker}\,\pi$ y $\phi(g\cdot(s\pi(g))^{-1}, \pi(g)) = g$. Luego, ϕ es epiyectiva.

P11. Salvo notaciones es el mismo problema que el anterior.

P12. Sea $G = \mathbb{Z}/n\mathbb{Z}$. Todo subgrupo $H \subset G$ es cíclico. Luego, $H = \langle \bar{m}\rangle$ (donde $0 \leq m < n$). El orden d de H, que es el de $\bar{m}$, divide al orden de G, que es n. Sea $m' := \frac{n}{d} \in \mathbb{N}$. Entonces, $d\cdot\bar{m} = \bar{0}$, es decir, $d\cdot m = r\cdot n$, para cierto $r > 0$, y $m = r\cdot m'$. Por tanto, $H \subseteq \langle \bar{m'}\rangle$. Como el subgrupo de G generado por $\bar{m'}$ es de orden d, $H = \langle \bar{m'}\rangle$.

Solución de los problemas del capítulo segundo

P1. a) Sea $f : \mathbb{Z} \to \mathbb{Z}$ un morfismo de anillos. Tenemos que $f(1) = 1$, luego $f(2) = f(1+1) = f(1)+f(1) = 1+1 =: 2, \ldots, f(n) = n$, para todo $n \in \mathbb{N}$ y por tanto $f(-n) = -n$ para todo $n \in \mathbb{N}$. Es decir, $f = \mathrm{Id}$.

b) Sea $f : \mathbb{Q} \to \mathbb{Q}$ un morfismo de anillos. $f_{|\mathbb{Z}} = \mathrm{Id}_{|\mathbb{Z}}$. Entonces, $f(\frac{n}{m}) = f(n\cdot m^{-1}) = n\cdot m^{-1} = \frac{n}{m}$ y $f = \mathrm{Id}$.

c) Sea $f : \mathbb{R} \to \mathbb{R}$ un morfismo de anillos. $f_{|\mathbb{Q}} = \mathrm{Id}_{|\mathbb{Q}}$. Dado $r > 0$, tenemos que $r = s^2$, para un $s > 0$. Entonces, $f(r) = f(s)^2 > 0$. Si $r > s$ entonces $r - s > 0$, luego $f(r) - f(s) = f(r-s) > 0$ y $f(r) > f(s)$. Dado $r \in \mathbb{R}$, sean $q_1, q_2 \in \mathbb{Q}$ tales que $q_1 < r < q_2$, entonces $q_1 = f(q_1) < f(r) < f(q_2) = q_2$. Por tanto, $f(r) = r$ y $f = \mathrm{Id}$.

P2. Consideremos el morfismo de anillos $f:\mathbb{R}[x]\to\mathbb{C}[x]$, $f(p(x))=p(i)$. El morfismo f es epiyectivo, pues dado $a+bi\in\mathbb{C}$, $f(a+bx)a+bi$. $\operatorname{Ker} f$ es el ideal generado por el polinomio mónico $p(x)\in\mathbb{R}[x]$ de grado más pequeño tal que $p(i)=0$. Obviamente, $x^2+1\in\operatorname{Ker} f$. Este polinomio es irreducible, luego $p(x)=x^2+1$. Por tanto, por el teorema de isomorfía $\mathbb{R}[x]/(x^2+1)=\mathbb{C}$.

P3. Observemos que dado $p(x)\in A[x]$ existen un polinomio único $q(x)\in A[x]$ y $b\in A$ tales que $p(x)=q(x)\cdot(x-a)+b$. Por tanto, $p(a)=0$ si y sólo si $b=0$, es decir, $p(x)\in(x-a)$. Consideremos el epimorfismo $\pi:A[x]\to A$, $\pi(p(x)):=p(a)$. Tenemos que $\operatorname{Ker}\pi=(x-a)$, luego por el teorema de isomorfía, $A[x]/(x-a)\simeq A$.

P4. Por el teorema chino de los restos

$$\begin{aligned}\mathbb{R}[x]/((x^2+1)\cdot(x^2-1)) &= \mathbb{R}[x]/(x^2+1)\times\mathbb{R}[x]/(x^2-1)\\ &= \mathbb{R}[x]/(x^2+1)\times\mathbb{R}[x]/(x-1)\times\mathbb{R}[x]/(x+1)=\mathbb{C}\times\mathbb{R}\times\mathbb{R}.\end{aligned}$$

P5. Sabemos que $I\times J$ es un subgrupo de $A\times B$, con la operación $+$. Dado $(i,j)\in I\times J$ y $(a,b)\in A\times B$, entonces $(a,b)\cdot(i,j)=(ai,bj)\in I\times J$. El núcleo del epimorfismo $A\times B\to A/I\times B/J$, $(a,b)\mapsto(\bar{a},\bar{b})$ es $I\times J$. Luego, $(A\times B)/I\times J=A/I\times B/J$.

P6. Si $a=bc$, con b y c propios, entonces $\delta(b)<\delta(a)$ y llegamos a contradicción.

P7. Tenemos que $\delta(ab)=\min\{\delta'(abc),c\in A\setminus\{0\}\}\geq\min\{\delta'(ad),d\in A\setminus\{0\}\}=\delta(a)$. Sean $a,b\in A$, y sea s tal que $\delta(b)=\delta'(bs)$. Sean c',r' tales que $as=c'bs+r'$, con $\delta'(r')<\delta'(bs)$ ó $r'=0$. Sea r tal que $r'=rs$. Tenemos que $a=c'b+r$ y $\delta(r)\leq\delta'(r')<\delta'(bs)=\delta(b)$ ó $r=0$.

P8. Sea $\frac{a}{b}\in\mathbb{Q}$, que podemos suponer irreducible (es decir, a y b primos entre sí), tal que $(\frac{a}{b})^2=2$, entonces $a^2=2b^2$. Entonces 2 divide á a, $a=2a'$ y $2a'=b$, luego divide también a b, hemos llegado a contradicción. No existe $\frac{a}{b}$ tal que $(\frac{a}{b})^2=2$.

P9. Por el algoritmo de Euclides, obtenemos que x^2+1 es el máximo común divisor de ambos polinomios. Tenemos $x^4+x^3+x-1=(x^2+1)\cdot(x^2+x-1)$. Luego, el mínimo común múltiplo es $(x^2+x-1)\cdot(x^4+x^3+2x^2+x+1)$.

P10. Buscamos $\bar{\lambda}$ tal que $\bar{\lambda}\cdot\bar{7}=\bar{1}$, es decir, λ del modo que exista μ tal que $\lambda\cdot 7=1+\mu\cdot 982$. Es decir, $\lambda\cdot 7+(-\mu)\cdot 982=1$. Efectivamente, 7 y 982 son primos entre sí y λ y $-\mu$ se calculan con el algoritmo de Euclídes...$\lambda=421$.

P11. Tenemos que $1+x+x^2$ y x^3-2 son primos entre sí. Con el algoritmo de Euclídes obtenemos que

$$(x-1)(x^2+x+1)-(x^3-2)=1.$$

Luego, $\overline{1+x+x^2}^{-1}=\overline{x-1}$. Consideremos el epimorfismo $\mathbb{Q}[x]/(x^3-2)\to\mathbb{Q}[\sqrt[3]{2}]$, $\overline{p(x)}\mapsto p(\sqrt[3]{2})$ (de hecho es un isomorfismo). Por un morfismo de anillos los inversos se aplican en inversos. Luego, como $\overline{1+x+x^2}^{-1}=\overline{x-1}$, entonces $(1+\sqrt[3]{2}+(\sqrt[3]{2})^2)^{-1}=\sqrt[3]{2}-1$.

P12. Sea $\tau \in \mathrm{Hom}_{grp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ y denotemos $\bar{m} = \tau(\bar{1})$. Se cumple que

$$\tau(\bar{i}) = \tau(\bar{1} + \overset{i}{\cdots} + \bar{1}) = \tau(\bar{1}) + \overset{i}{\cdots} + \tau(\bar{1}) = i \cdot \bar{m} = h_{\bar{m}}(\bar{i}),$$

es decir, $\tau = h_{\bar{m}}$ es una homotecia. Luego, $\mathbb{Z}/n\mathbb{Z} = \mathrm{Hom}_{grp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$, $\bar{m} \mapsto h_{\bar{m}}$. Como $h_{\bar{m}\cdot\bar{m}'} = h_{\bar{m}} \circ h_{\bar{m}'}$, los invertibles (con el producto) de $\mathbb{Z}/n\mathbb{Z}$ se identifican con los invertibles de $\mathrm{Hom}_{grp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ con la composición.

P13. Observemos que $A[x,y] = A[x][y]$. Por el problema anterior $p(x,x) = 0$ si y sólo si $p(x,y) \in (y-x)$ y $A[x,y]/(y-x) = A[x]$.

P14. Denotemos el determinante por $p(x_1, \ldots, x_n)$. Observemos que

$$p(x_1, \ldots, \underset{j}{x_i}, \ldots, \underset{i}{x_i}, \ldots, x_n) = 0,$$

para $i > j$. Por lo tanto, $p(x_1, \ldots, x_n) = (x_n - x_{n-1}) \cdot q(x_1, \ldots, x_n)$. Observemos que $q(x_1, \ldots, x_n, x_{n-1}, x_n) = 0$, luego $p(x_1, \ldots, x_n) = (x_n - x_{n-1})(x_n - x_{n-2}) \cdot h(x_1, \ldots, x_n)$. Recurrentemente, $p(x_1, \ldots, x_n)$ es múltiplo de $\prod_{i>j}(x_i - x_j)$. Ambos son polinomios homogéneos de grado $\frac{n\cdot(n-1)}{2}$. Luego, son iguales salvo multiplicación por un número racional. El coeficiente que acompaña al monomio $x_n^{n-1}x_{n-1}^{n-2}\cdots x_2$ es el 1 en ambos polinomios, luego son iguales.

P15. Consideremos un epimorfismo $\pi\colon k[x_i]_{i\in I} \to K'$. Sea $\{e_j\}_{j\in J}$ una base del k-espacio vectorial $\mathrm{Ker}\,\pi$ y $\{e_j, e_{j'}\}_{j\in J, j'\in J'}$ una base del k-espacio vectorial $k[x_i]_{i\in I}$. Se cumple que $\{e_j, e_{j'}\}_{j\in J, j'\in J'}$ es una base del K-espacio vectorial $K[x_i]_{i\in I}$. Además, $\langle e_j | j \in J\rangle_K$ es un ideal de $K[x_i]_{i\in I}$ y $\langle e_j | j \in J\rangle_K \cap k[x_i]_{i\in I} = \langle e_j | j \in J\rangle_k$. Por tanto, tenemos las inyecciones

$$K' = k[x_i]_{i\in I}/\langle e_j | j \in J\rangle_k \hookrightarrow K[x_i]_{i\in I}/\langle e_j | j \in J\rangle_K =: B$$
$$K \hookrightarrow K[x_i]_{i\in I}/\langle e_j | j \in J\rangle_K =: B.$$

Si $\mathfrak{m} \subset B$ es un ideal maximal, $L = B/\mathfrak{m}$ es la extensión de cuerpos buscada.

P16. El máximo común divisor se puede calcular por el algoritmo de Euclides. Las operaciones que se realizan no dependen de si estamos en $\mathbb{Q}[x]$ o en $\mathbb{R}[x]$.

P17. Sea $\mathbb{F}_p^{*2} = \{c^2, c \in \mathbb{F}_p^*\}$, $(p \neq 2)$. El núcleo del epimorfismo $\mathbb{F}_p^* \to \mathbb{F}_p^{*2}$, $c \mapsto c^2$ es $\{\pm 1\}$. Por tanto, $|\mathbb{F}_p^{*2}| = (p-1)/2$. Luego, $\mathbb{F}_p^{*2}$ es un subgrupo de $\mathbb{F}_p^*$ de índice 2 y coincide con el núcleo del epimorfismo $\mathbb{F}_p^* \to \{\pm 1\}$, $c \mapsto c^{\frac{p-1}{2}}$.

P18. Si $p = a^2 + b^2$ entonces $p = (a+bi)\cdot(a-bi)$ y p no es irreducible en $\mathbb{Z}[i]$. Recíprocamente, si $p = z \cdot z'$, con $z, z' \in \mathbb{Z}[i]$ y no invertibles, entonces $p^2 = \delta(p) = \delta(z)\cdot\delta(z')$, luego $p = \delta(z) = \delta(z')$ (si $\delta(z) = 1$, entonces z sería uno de los invertibles $\pm 1, \pm i$), luego $p = a^2 + b^2$ (donde $z = a + bi$).

Veamos cuándo el número primo p es irreducible en $\mathbb{Z}[i]$. Que p sea irreducible equivale a que $\mathbb{Z}[i]/(p)$ sea cuerpo. Denotemos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ y observemos que $\mathbb{Z}[i] =$

$\mathbb{Z}[x]/(x^2+1)$. Entonces, $\mathbb{Z}[i]/(p) = \mathbb{F}_p[x]/(x^2+1)$ es cuerpo si y sólo si x^2+1 no tiene raíces en $\mathbb{F}_p$, es decir, -1 no es un resto cuadrático módulo p.

Por el problema 17, $-1 \in \mathbb{F}_p^{*2}$ si y sólo si $(-1)^{\frac{p-1}{2}} = 1$ (o $p=2$), que equivale a que $\frac{p-1}{2}$ sea par, que equivale a que $p \equiv 1 \mod 4$. Con todo, p es irreducible en $\mathbb{Z}[i]$ si y sólo si $p \equiv 3 \mod 4$.

En conclusión, un número primo $p \in \mathbb{Z}$ descompone en suma de dos cuadrados perfectos si y sólo si $p \equiv 1 \mod 4$ ó $p = 2$.

P19. Tenemos que calcular los enteros de Gauss $a+bi \in \mathbb{Z}[i]$, tales que $\delta(a+bi) = (a+bi)(a-bi) = a^2+b^2 = 2178 = 2\cdot 3^2 \cdot 11^2$. Observemos que $3, 11 = 3 \mod 4$, luego son primos en $\mathbb{Z}[i]$ y han de dividir a $a+bi$, es decir, $a+bi = 3\cdot 11\cdot(a'+b'i)$ y $\delta(a'+b'i) = 2$. Por tanto, $\{(a',b') = (1,1),(-1,-1),(-1,1),(1,-1)\}$ y

$$\{(a,b) = (33,33),(-33,-33),(-33,33),(33,-33)\}.$$

P20. Observemos que $x^3-1 = (x-1)(x^2+x+1)$. Luego las raíces de x^2+x+1 son $e^{\frac{2\pi i}{3}}$ y $e^{\frac{4\pi i}{3}}$. Sea

$$\delta\colon \mathbb{Z}[e^{\frac{2\pi i}{3}}] \to \mathbb{N},\ \delta(a+be^{\frac{2\pi i}{3}}) := (a+be^{\frac{2\pi i}{3}})\cdot(a+be^{\frac{4\pi i}{3}}) = a^2+b^2-ab.$$

Para probar que $(\mathbb{Z}[e^{\frac{2\pi i}{3}}],\delta)$ es un anillo euclídeo se procede del mismo modo con el que hemos probado que el anillo de los enteros de Gauss es euclídeo.

P21. Veamos el recíproco. Sea $a \in A$ un elemento irreducible. El ideal (a) está incluido en algún ideal maximal $\mathfrak{m} = (b)$. Por tanto, $a = bc$, para algún $c \in A$. Como a es irreducible, c ha de ser invertible, luego $(a) = (b) = \mathfrak{m}$. Por el teorema 2.6.7, A es un dominio de factorización única. Sea (a_1,a_2) un ideal de A y $b = m.c.d(a_1,a_2)$. Entonces, $a_1 = bc_1$ y $a_2 = bc_2$, de modo que no existe ningún elemento propio que divida a a_1 y a_2 a la vez. Por tanto, el ideal (c_1,c_2) no está incluido en ningún maximal, luego $(c_1,c_2) = A$ y $(a_1,a_2) = b\cdot(c_1,c_2) = b\cdot A$. Ahora es fácil concluir que todo ideal (que es finito generado) es principal.

P22. a) $x^4+x^2+1 = (x^2+x+1)^2$ en $\mathbb{Z}/2\mathbb{Z}[x]$.

b) $x^4+x^3-x = x\cdot(x^3+x^2-1)$ en $\mathbb{Z}/3\mathbb{Z}[x]$.

c) Si $x^4+4x^3+3x^2+2x+3 = p(x)\cdot q(x)$ en $\mathbb{Z}[x]$, entonces $p(x)$ y $q(x)$ son de grados dos, porque al hacer módulo 2 el polinomio descompone en producto de dos polinomios irreducibles de grado 2. Pero por otra parte uno ha de ser de grado 3 y el otro de grado 1, porque así sucede al hacer cociente por 3. Contradicción, Luego $p(x)$ es irreducible. Como es primitivo también es irreducible en $\mathbb{Q}[x]$.

P23. El morfismo que asigna a cada polinomio su recíproco,

$$\mathbb{Q}[x]\backslash\{0\} \to \mathbb{Q}[x]\backslash\{0\},\ p(x) \mapsto p(1/x)\cdot x^{\mathrm{gr}(p(x)},$$

es una biyección que respeta el producto. Por tanto, un polinomio es irreducible si y sólo si lo es su recíproco. El criterio de Nietsnesie es consecuencia del criterio de Eisenstein.

P24. Consideremos el morfismo $f\colon \mathbb{Q}[x] \to \mathbb{C}$, $f(q(x)) = q(\sqrt{2})$. $\operatorname{Ker} f = (x^2-2)$. Luego, $p(\sqrt{2}) = 0$ si y sólo si $p(x) \in \operatorname{Ker} f = (x^2-2)$.

Consideremos el morfismo $f\colon \mathbb{Q}[x] \to \mathbb{C}$, $f(q(x)) = q(\sqrt[3]{2})$. $\operatorname{Ker} f = (x^3-2)$, porque x^3-2 es irreducible por el criterio de Eisenstein y porque $x^3-2 \in \operatorname{Ker} f$. Luego, $p(\sqrt[3]{2}) = 0$ si y sólo si $p(x) \in \operatorname{Ker} f = (x^3-2)$.

P25. Sea $\mu_n := \{z \in \mathbb{C}\colon z^n = 1\}$ y X_d el conjunto de las ráices d-ésimas primitivas de la unidad. Como $\mu_n = \coprod_{d|n} X_d$, tenemos que

$$n = |\mu_n| = \sum_{d|n} |X_d| = \sum_{d|n} \phi(d)$$

P26. El directo es el problema 12 del primer capítulo.

Recíproco: sea G verificando la hipótesis. Sea $G = \coprod_{d|n} G_d$, siendo $G_d \subset G$ los elementos de orden d. Si existe un elemento de orden d, entonces el grupo generado H es el único de dicho orden, luego G_d es el conjunto de generadores de H y, por tanto, $|G_d| = \phi(d)$. Por tanto, $|G_d| = 0, \phi(d)$. Pero como $\sum_{d|n} \phi(d) = n = |G| = \sum_{d|n} |G_d|$, se concluye que para cada d divisor de n es $|G_d| = \phi(d) \neq 0$. En particular, $G_n \neq \emptyset$, es decir, G admite un generador y por tanto es cíclico.

P27. Observemos que $x^4+2x^2+1 = (x+i)^2 \cdot (x-i)^2$. Por el algoritmo de Euclides obtenemos que $1 = (\frac{x}{4i} - \frac{1}{2})(x+i)^2 + (\frac{-x}{4i} - \frac{1}{2})(x-i)^2$. Por tanto,

$$\int \frac{x^5}{x^4+2x^2+1}dx = \int x + \frac{\frac{-x^4}{2i} + x^3 - \frac{x^2}{4i} + \frac{x}{2}}{(x-i)^2} + \frac{\frac{x^4}{2i} + x^3 + \frac{x^2}{4i} + \frac{x}{2}}{(x+i)^2}dx$$

Tenemos que

$$\frac{-x^4}{2i} + x^3 - \frac{x^2}{4i} + \frac{x}{2} = (x-i)^2 \cdot (\frac{-x^2}{2i} - \frac{3}{4i}) - \frac{x}{2} - \frac{3}{4i} = (x-i)^2 \cdot (\frac{-x^2}{2i} - \frac{3}{4i}) - \frac{1}{2}(x-i) - \frac{5}{4i}.$$

$$\frac{x^4}{2i} + x^3 + \frac{x^2}{4i} + \frac{x}{2} = (x+i)^2 \cdot (\frac{x^2}{2i} + \frac{3}{4i}) - \frac{x}{2} + \frac{3}{4i} = (x+i)^2 \cdot (\frac{x^2}{2i} + \frac{3}{4i}) - \frac{1}{2}(x+i) + \frac{5}{4i}.$$

Luego, $\int \frac{x^5}{x^4+2x^2+1}dx = \frac{x^2}{2} - \frac{\ln(x-i)}{2} + \frac{5}{4(x-i)} - \frac{\ln(x+i)}{2} - \frac{5}{4(x+i)} = \frac{x^2}{2} - \frac{\ln(x^2+1)}{2} + \frac{5}{2(x^2+1)}$.

P28. Tenemos que $dt = e^{ix}dx$, luego $dx = \frac{dt}{t}$, $cos(x) = \frac{e^{ix}+e^{-ix}}{2} = \frac{t+t^{-1}}{2}$, $\sin(x) = \frac{e^{ix}-e^{-ix}}{2i} = \frac{t-t^{-1}}{2i}$ y $\cos(3x) = \frac{e^{3ix}+e^{-3ix}}{2} = \frac{t^3+t^{-3}}{2}$.

Solución de los problemas del capítulo tercero

P1. Sea $G' \subseteq G$ un subgrupo. Sean $g \in G'$. Dado $n \in \mathbb{N}$, tenemos que $ng = g \overset{n}{\cdots} + g \in G'$ y $-n \cdot g = (-g) \overset{n}{\cdots} + (-g) \in G'$. En conclusión, G' es un $\mathbb{Z}$-submódulo de G. Sea $H \subseteq G$ un submódulo, en particular es un subgrupo. Sea $f\colon G \to G'$ un morfismo de grupos. Dado $n \in \mathbb{N}$, tenemos que $f(n \cdot g) = f(g \overset{n}{\cdots} + g) = f(g) \overset{n}{\cdots} + f(g) = n \cdot f(g)$ y $f(-n \cdot g) = f(-g \overset{n}{\cdots} + (-g)) = f(-g) \overset{n}{\cdots} + f(-g) = n \cdot f(-g) = n(-f(g)) = -n \cdot f(g)$. Luego, f es un morfismo de $\mathbb{Z}$-módulos. Recírpocamente si f es un morfismo de $\mathbb{Z}$-módulos en particular es un morfismo de grupos.

P2. Sea $E' \subseteq E$ estable por T, es decir, tenemos el endomorfismo $T_{|E'}: E' \to E'$, $T_{|E'}(e') = T(e')$. Por tanto, E' es un $K[x]$-módulo y la estructura de $K[x]$-módulo es la inducida por E, porque $p(T_{|E'})(e') = p(T)(e')$, para todo $p(x) \in K[x]$ y $e' \in E'$. Luego, E' es un $K[x]$-submódulo de E. Recíprocamente. si E' es un $K[x]$-submódulo de E, dado $e' \in E'$, tenemos que $= T(e') = x \cdot e' \in E'$, luego E' es estable por T.

Sea (a_{ij}) la matriz de T en la base $\{e_i\}$, es decir, $T(e_i) = \sum_j a_{ij} e_j$. Tenemos que $x \cdot \phi(e_i) = \phi(x \cdot e_i) = \phi(T(e_i)) = \phi(\sum_j a_{ij} e_j) = \sum_j a_{ij} \phi(e_i)$. Luego la matriz asociada a $x\cdot$ en la base $\{\phi(e_i)\}$ es (a_{ij}).

P3. Dado $a \in A$ y $m \in M$, definimos $a \cdot m := f(a) \cdot m$.

P4. El morfismo $M \oplus M' \to M/N \oplus M'/N'$, $(m, m') \mapsto (\bar{m}, \bar{m}')$ es epiyectivo y el núcleo es $N \oplus N'$. Por el teorema de isomorfía se concluye.

P5. El subconjunto $N := \{i_1 \cdot m_1 + \cdots + i_n \cdot m_n \in M,$ variando los $i_j \in I, m_j \in M,$ y $r \in \mathbb{N}\}$ es un submódulo de M y es el mínimo que contiene a $\{i \cdot m\}_{i \in I, m \in M}$.

P6. Dado $\bar{a} \in A/I$ y $\bar{m} \in M/IM$, se define $\bar{a} \cdot \bar{m} := \overline{am}$. Que está bien definido: Dado $i \in I$ y $m' \in M$, tenemos

$$\overline{a+i} \cdot \bar{m} = \overline{(a+i) \cdot m} = \overline{am + im} = \overline{am}$$
$$\bar{a} \cdot \overline{(m + im')} = \overline{a \cdot (m + im')} = \overline{am + aim'} = \overline{am}$$

P7. El conjunto $\{i \cdot (m, m'),\ \forall i \in I, (m.m') \in M \oplus M'\}$ está incluido en $IM \oplus IM'$, luego $I \cdot (M \oplus M') \subseteq IM \oplus IM'$. Los conjuntos $\{im,\ \forall i \in I, m \in M\}$, $\{im',\ \forall i \in I, m' \in M'\}$ están incluidos en $I \cdot (M \oplus M')$, luego $IM, IM' \subseteq I \cdot (M \oplus M')$, luego $IM \oplus IM' \subseteq I \cdot (M \oplus M')$.

P8. Sea $\mathfrak{m} \subset A$ un ideal maximal. Entonces,

$$A/\mathfrak{m} \oplus \overset{n}{\cdots} \oplus A/\mathfrak{m} = (A \oplus \overset{n}{\cdots} \oplus A)/(\mathfrak{m} \oplus \overset{n}{\cdots} \oplus \mathfrak{m}) = A^n/\mathfrak{m}A^n \simeq A^m/\mathfrak{m}A^m$$
$$= (A \oplus \overset{m}{\cdots} \oplus A)/(\mathfrak{m} \oplus \overset{n}{\cdots} \oplus \mathfrak{m}) = A/\mathfrak{m} \oplus \overset{m}{\cdots} \oplus A/\mathfrak{m}$$

Tomando $\dim_{A/\mathfrak{m}}$ tenemos que $n = m$.

P9. El morfismo $f: \operatorname{Ker}\pi \oplus N \to M$, $f(k, n) = k + s(n)$ es inyectivo: si $f(k, n) = 0$, es decir, $k + s(n) = 0$, entonces tomando π obtenemos que $0 + n = 0$, luego $n = 0$ y $k = 0$ y $(k, n) = 0$. Por último, f es epiyectivo: dado m, tenemos que $m - s(\pi(n)) \in \operatorname{Ker}\pi$ y $f(m - s(\pi(n)), \pi(n)) = m$.

P10. El morfismo $\pi: M \to (M/N_1)/\bar{N}_2$, $\pi(m) := \overline{\bar{m}}$ es epiyectivo. Como

$$\operatorname{Ker}\pi = \{m \in M : \overline{\bar{m}} = 0\} = \{m \in M : \bar{m} \in \bar{N}_2\} = \{m \in M : \exists n_2 \in N_2 \text{ tal que } \bar{m} = \bar{n}_2\}$$
$$= \{m \in M : \bar{m} \in \bar{N}_2\} = \{m \in M : \exists n_2 \in N_2, n_1 \in N_1 \text{ tales que } m = n_1 + n_2\} = N_1 + N_2$$

terminamos por el teorema de isomorfía.

P11. Tenemos que $\Delta\binom{n}{j} = (\binom{n+1}{j} - \binom{n}{j}) = (\binom{n}{j-1})$. $\{\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{r}\}$ son linealmente independientes: Si $p(n) = \sum_{j=0}^{r} \lambda_j \binom{n}{j}$, entonces $\Delta^i(p(n)) = \sum_{j=i}^{r} \lambda_i \binom{n}{j-i}$ y el término 0 es λ_i. Por tanto, si $p(n) = 0$, entonces $\lambda_j = 0$ para todo j. Por dimensiones, tenemos que $\{\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{r}\}$ es una base de $\operatorname{Ker}\Delta^{r+1}$.

Por último, observemos que $\Delta^i = (\nabla - 1)^i = \sum_{j=0}^{i} (-1)^j \nabla^{i-j}$.

$p(n) = \sum_{i=0}^{n} i^2 = \lambda_0 + \lambda_1 \binom{n}{1} + \lambda_2 \binom{n}{2} + \lambda_3 \binom{n}{3}$. Con

$$\lambda_0 = \binom{0}{0}(-1)^0 p(0) = 0, \quad \lambda_1 = \binom{1}{0}(-1)^0 p(1) + \binom{1}{1}(-1)^1 p(0) = 1,$$
$$\lambda_2 = \binom{2}{0}(-1)^0 p(2) + \binom{2}{1}(-1)^1 p(1) + \binom{2}{2}(-1)^2 p(0) = 5 - 2 = 3,$$
$$\lambda_3 = \binom{3}{0}(-1)^0 p(3) + \binom{3}{1}(-1)^1 p(2) + \binom{3}{2}(-1)^2 p(1) = 14 - 3 \cdot 5 + 3 \cdot 1 = 2.$$

P12. Sea a_n los números de longitud n con las condiciones exigidas. Sea b_n los números de longitud n con las condiciones exigidas y que acaben en 1, sea c_n los números de longitud n con las condiciones exigidas y que acaben en 0. Tenemos que $b_n = a_{n-1}$, $a_n = b_n + c_n$ y $a_n = 2b_{n-1} + c_{n-1}$. Por tanto,

$$a_n = 2b_{n-1} + c_{n-1} = 2b_{n-1} + (a_{n-1} - b_{n-1}) = a_{n-2} + a_{n-1}$$

Luego, $(\nabla^2 - \nabla - 1)(a_n) = 0$ y además $a_1 = 2$ y $a_2 = 3$. Que sabemos resolver.

P13. La ecuación es $(\nabla^2 + 2\nabla - 8)(a_n) = (2^n)$. Observemos que $\nabla^2 + 2\nabla - 8 = (\nabla - 2)(\nabla + 4)$ y que $(\nabla - 2)(2^n) = 0$. Por lo tanto, $(\nabla - 2)^2(\nabla + 4)(a_n) = 0$. Luego, $a_n = 2^n(an + b) + (-4)^n c$. Si aplicamos $(\nabla - 2)(\nabla + 4)$ a a_n, obtenemos

$$2^n = (\nabla + 4)(\nabla - 2)(2^n(an + b)) = (\nabla + 4)(2^n(2\Delta)(an + b)) = (\nabla + 4)(2^{n+1}a) = 2^n(4 + 8)a,$$

luego $a = \frac{1}{12}$.

P14. Sea $a_n := \sum_{i=0}^{n-1} g^i$. Entonces, $(a_n) = \frac{1}{\Delta}(g^n)$. Observemos que $(\nabla - g)(g^n) = 0$. Entonces, una solución particular es

$$(a_n) = \frac{1}{\Delta}(g^n) = \frac{1}{\nabla - 1}(g^n) = (\frac{1}{g-1} + s(\nabla)(\nabla - g))(g^n) = \frac{1}{g-1}(g^n)$$

Todas las soluciones son $(a_n) = (\frac{g^n}{g-1}) + \operatorname{Ker}\Delta = (\frac{g^n}{g-1}) + (\mu)$ Ahora bien, $1 = a_1 = \frac{g}{g-1} + \mu$. Luego $\mu = 1 - \frac{g}{g-1} = \frac{-1}{g-1}$. En conclusión,

$$\sum_{i=0}^{n} g^i = \frac{g^{n+1}}{g-1} + \frac{-1}{g-1} = \frac{g^{n+1} - 1}{g-1}$$

P15. Sea i_n es el dinero que pagamos en el año n por los intereses del capital que tenemos prestado durante el año n y a_n el dinero que amortizamos en el año n por el capital prestado. Entonces, $d_n = i_n + a_n$. Tenemos que $i_n = I \cdot (K - \sum_{r=1}^{n-1} a_r)$. Por tanto,

$$d_n = a_n + I \cdot (K - \sum_{r=1}^{n-1} a_r).$$

Si aplicamos el operador diferencia Δ, entonces $10^3 = \Delta(a_n) - I \cdot a_n = (\nabla - (1+I))(a_n)$. Por tanto, $a_n = (1+I)^n \cdot \lambda + \frac{-10^3}{I}$. Tenemos que calcular λ. Nos falta decir que amortizamos la hipoteca en N años, es decir,

$$K = \sum_{r=1}^{N} a_r$$

Tenemos que $b_n := \sum_{r=1}^{n-1} a_r = \frac{(1+I)^n \lambda}{I} - \frac{10^3 \cdot (n-1)}{I} + \mu$. Como $b_1 = 0$, tenemos que $\mu = \frac{-(1+I)\lambda}{I}$. Luego $K = b_{N+1} = \frac{(1+I)^{N+1}\lambda}{I} - \frac{10^3 \cdot N}{I} - \frac{\lambda(1+I)}{I}$ y despejando obtenemos que $\lambda = \frac{IK + 10^3 N}{(1+I)^{N+1} - (1+I)}$ Entonces,

$$d_1 = a_1 + IK = (1+I)\lambda + \frac{-10^3}{I} + IK = \frac{IK + \frac{10^3 N}{(1+I)^N}}{1 - \frac{1}{(1+I)^N}} - \frac{10^3}{I}$$

P16. Observemos que $D^i(\sum_i c_i(x)s_i(x)) = \sum_i c_i(x) D^i s_i(x)$, para $i < n$. Entonces,

$$D^n(\sum_i c_i(x)s_i(x)) = D(\sum_i c_i(x) D^{n-1} s_i(x)) = \sum_i c_i(x) D^n s_i(x) + \sum_i c_i(x)' D^{n-1} s_i(x).$$

Luego, $p(D)(\sum_i c_i(x)s_i(x)) = \sum_i c_i(x) p(D)(s_i(x)) + \sum_i c_i(x)' s_i(x)^{n-1)} = 0 + f(x)$.

Solución de los problemas del capítulo cuarto

P1. Los grupos abelianos desisomorfos de orden $p^2 q$ son

$$\mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z},\ \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$$

P2. Sea G un grupo abeliano de orden finito. Entonces, $G \simeq \mathbb{Z}/p_i^{n_{ij}}\mathbb{Z}$, para ciertos primos p_i (p_i primo con p_j, para $i \neq j$) y ciertos n_{ij}. Si no existe un i, con dos n_{ij}, entonces por el teorema chino de los restos G sería cíclico. Tenemos pues un subgrupo $G' = \mathbb{Z}/p_i^{n_{i1}}\mathbb{Z} \oplus \mathbb{Z}/p_i^{n_{i2}}\mathbb{Z}$ de G. $G'' = \langle \overline{p^{n_{i1}-1}} \rangle \times \langle \overline{p^{n_{i2}-1}} \rangle$ es el subgrupo buscado.

P3. Por el problema anterior, si G no es cíclico contiene un subgrupo $G' \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, que contiene al menos dos subgrupos $\mathbb{Z}/p\mathbb{Z}$.

Si $G \simeq \mathbb{Z}/n\mathbb{Z}$ y $d|n$, sea $m = n/d$. Entonces, $\langle \bar{m} \rangle$ es un subgrupo de orden d. Si H es un subgrupo de orden d, entonces $H \subseteq \mathrm{Ker}\, d\cdot = \langle \bar{m} \rangle$, luego $H = \langle \bar{m} \rangle$.

P4. Que G sea un subgrupo discreto equivale a decir que si una sucesión $\{g_n\}_{n\in\mathbb{N}}$ de elementos de G es converge a un punto $g\in\mathbb{R}^n$, entonces $g_n = g$, para todo $n \geq m$, para cierto m. Esto es equivalente a decir, que si una sucesión $\{g_n\}_{n\in\mathbb{N}}$ de elementos de G es converge a 0, entonces $g_n = 0$, para todo $n \geq m$, para cierto m.

Procedamos por inducción sobre n.

Supongamos que $n = 1$. Dados $g_1, g_2 \in G$ no nulos, tenemos que $\langle g_1, g_2\rangle$ es un grupo abeliano finito generado sin torsión, luego es libre. Veamos que es de rango 1. Consideremos , el epimorfismo $\pi\colon \mathbb{Z}^2 \to \langle g_1, g_2\rangle$, $\pi(n,m) = ng_1 + mg_2$. Tenemos que $\mathbb{Z}^2 = \langle g_1, g_2\rangle \oplus \operatorname{Ker}\pi$. Por tanto, el rango o es 1 (y hemos terminado), ó es 2 y en este caso $\operatorname{Ker}\pi = 0$, es decir, g_1 y g_2 son $\mathbb{Z}$-linealmente independientes. Ahora bien, dados dos números reales ($g_1 \neq g_2$) existen $\lambda_n, \mu_n \in \mathbb{Z}$, no nulos, de modo que $|\lambda_n g_1 + \mu_n g_2| < 1/n$. Entonces, la sucesión $\{\lambda_n g_1 + \mu_n g_2\}$ converge a cero y llegamos a contradicción. Sea $g_1 \in G$ no nulo, si $\langle g_1\rangle \subsetneq G$, sea $g_1' \in G\setminus\langle g_1\rangle$, tenemos $\langle g_1\rangle \subsetneq \langle g_1, g_1'\rangle = \langle g_2\rangle$. Si $\langle g_2\rangle \subsetneq G$, sea $g_2' \in G\setminus\langle g_2\rangle$, tenemos $\langle g_2\rangle \subsetneq \langle g_2, g_2'\rangle = \langle g_3\rangle$. Así sucesivamente vamos obteniendo una cadena

$$\langle g_1\rangle \subsetneq \langle g_2\rangle \subsetneq \cdots \langle g_n\rangle \subsetneq \cdots$$

que ha de estabilizar, porque si no la sucesión de números reales no nulos $\{g_n\}$ sería convergente a cero. Por tanto, $G = \langle g_n\rangle$, para un $n >> 0$, y es libre de rango 1.

Supongamos $G \subset \mathbb{R}^n$, con $n > 1$. Sea $\pi\colon \mathbb{R}^n \to \mathbb{R}^{n-1}$, $\pi(x_1,\ldots,x_n) = (x_2,\ldots,x_n)$. Veamos que $\pi(G)$ es un subgrupo discreto de $\mathbb{R}^{n-1}$: Sea $\{\pi(g_n)\}$, con $g_n \in G$ y $\pi(g_n) \neq 0$ para todo n, una sucesión convergente a 0. Podemos suponer que $||\pi(g_n)|| < 1$ para todo n. El núcleo del morfismo $\pi_{|G}\colon G \to \pi(G)$, es igual a $G \cap \mathbb{R}\times 0 \times \overset{n-1}{\cdots} \times 0 = \langle g\rangle$, por el caso $n = 1$. Tomando $g_n + m\cdot g$, con $m \in \mathbb{Z}$ conveniente, en vez de g_n, podemos suponer que la primera coordenada es de módulo menor que $||g||$. Por tanto, $||g_n|| \leq ||\pi(g_n)|| + ||g|| \leq 1 + ||g||$. Por tanto, $\{g_n\}$ es una sucesión de puntos que yacen en un compacto de $\mathbb{R}^n$. Luego, contiene una subsucesión convergente y llegamos a contradicción. Por hipótesis de inducción, $\pi(G)$ es un grupo abeliano libre de rango menor o igual que $n-1$. Por tanto, el epimorfismo $\pi_{|G}\colon G \to \pi(G)$ tiene sección y $G \simeq \pi(G) \oplus \operatorname{Ker}\pi_{|G}$ y como $\operatorname{Ker}\pi_{|G}$ es libre de rango menor o igual que 1, hemos concluido.

P5. Los divisores elementales de $x\cdot$ son x, x^3, x^5.

P6. El polinomio anulador divide a x^n, para $n >> 0$. Luego los divisores elementales son potencias de x. Por tanto, sólo hay tres casos $\{x^3\}$, $\{x^2, x\}$, $\{x, x, x\}$.

En dimensión 4, $\{x^4\}, \{x^3, x\}$, $\{x^2, x^2\}$, $\{x^2, x, x\}$, $\{x, x, x, x\}$.

En dimensión 5, $\{x^5\}, \{x^4, x\}, \{x^3, x^2\}$, $\{x^3, x, x\}$, $\{x^2, x^2, x\}$, $\{x^2, x, x, x\}$, $\{x, x, x, x, x\}$.

P7. a) Los divisores elementales pueden ser $\{x-1, x-1, x-1, x-1, x+1\}$, $\{x-1, x-1, x-1, x+1, x+1\}$, $\{x-1, x-1, x+1, x+1, x+1\}$, $\{x-1, x+1, x+1, x+1, x+1\}$.

b) Los divisores elementales pueden ser $\{(x^2+4)^2, (x+8)^2, (x+8)^2\}$, $\{(x^2+4)^2, (x+8)^2, x+8, x+8\}$.

ÍNDICE

P8. El polinomio anulador de T es x^3, $\dim_{\mathbb{R}} \operatorname{Ker} x\cdot = \dim_{\mathbb{R}} \operatorname{Ker} D^2 = 2$. Luego, sólo hay dos divisores elementales que han de ser $\{x^3, x^3\}$.

P9. Escribamos

$$G \simeq (\mathbb{Z}/p_1^{n_{11}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_1^{n_{1s_1}}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_r^{n_{r1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{n_{rs_r}}\mathbb{Z}),$$

con $p_{11} \geq p_{12} \geq \cdots$, …, $p_{r1} \geq p_{r2} \geq \cdots$. El mínimo número natural n no nulo tal que $n \cdot g = 0$ para todo $g \in G$ es $n = p_1^{n_{11}} \cdots p_r^{n_{r1}}$ y $|G| = \prod_{ij} p_i^{n_{ij}}$. G es cíclico si y sólo si $s_1 = \cdots = s_r = 1$, que equivale a que $n = |G|$.

P10. Obvio.

P11. El polinomio característico de A es $x^4 - 7x + 5$ que no tiene raíces múltiples. Luego, A sólo tiene un factor invariante $x^4 - 7x + 5$.

El polinomio característico de B es $x^2(2+x)^2$. La dimensión de $\operatorname{Ker} B$ es 1 y la dimensión de $\operatorname{Ker}(B+2)$ es 1. Luego, los divisores elementales son $x^2, (2+x)^2$.

El ideal anulador de $e = (1,0,0,0)$ es $x^2(2+x)^2$. Entonces una base de Jordan es $\{(2+x)^2 \cdot e, x \cdot (2+x)^2 \cdot e, x^2 \cdot e, (2+x) \cdot x^2 \cdot e\}$, es decir,

$$\{(2,4,2,4), (0,4,0,4), (2,-4,-2,4), (0,4,0,-4)\}.$$

En esta base la matriz asociada a B es

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & -2 \end{pmatrix}$$

P12. Dado un $k[x]$-módulo M, entonces $M^* = \operatorname{Hom}_k(M,k)$ es un $k[x]$-módulo de modo natural: Dados $p(x) \in k[x]$ y $w \in M^*$, se define $(p(x) \cdot w)(m) := w(p(x) \cdot m)$.

Se cumple que el ideal anulador de M es igual al ideal anulador de M^*: Si $p(x) \cdot M = 0$, entonces $p(x) \cdot M^* = 0$. Por tanto, $\operatorname{Anul}(M) \subseteq \operatorname{Anul}(M^*)$. Si $p(x) \cdot M \neq 0$, existe $m \in M$ tal que $p(x) \cdot m \neq 0$. Sea $w \in M^*$ tal que $w(p(x) \cdot m) \neq 0$, entonces $p(x) \cdot w \neq 0$, ya que $(p(x) \cdot w)(m) = w(p(x) \cdot m) \neq 0$. Con todo, $\operatorname{Anul}(M) = \operatorname{Anul}(M^*)$.

Si $\dim_k M = n < \infty$, entonces $\dim_k M^* = n$. Si $M = k[x]/(p(x))$ entonces $M^* \simeq k[x]/(p(x))$, porque $\operatorname{Anul}(M^*) = \operatorname{Anul}(M) = (p(x))$, y $M^* \simeq k[x]/(p(x))$ por dimensiones. Si $M = M_1 \oplus M_2$, entonces $M^* = M_1^* \oplus M_2^*$ como $k[x]$-módulos. Por último si $M = \oplus_i k[x]/(p_i(x))$ entonces $M^* = \oplus_i k[x]/(p_i(x))^* = \oplus_i k[x]/(p_i(x))$.

Por último, si la matriz asociada a $x\cdot\colon M \to M$ en una base es (a_{ij}), entonces la matriz asociada a $x\cdot\colon M^* \to M^*$ en la base dual es la transpuesta de (a_{ij}).

P13. Por transformaciones elementales obtenemos

$$\left(\begin{array}{cc|c} 7 & 5 & 1 \\ 5 & 3 & 3 \end{array}\right) \overset{F_1 - F_2}{\rightsquigarrow} \left(\begin{array}{cc|c} 2 & 2 & -2 \\ 5 & 3 & 3 \end{array}\right) \overset{F_2 - 2F_1}{\rightsquigarrow} \left(\begin{array}{cc|c} 2 & 2 & -2 \\ 1 & -1 & 7 \end{array}\right) \overset{F_1 x F_2}{\rightsquigarrow} \left(\begin{array}{cc|c} 1 & -1 & 7 \\ 2 & 2 & -2 \end{array}\right)$$
$$\overset{F_2 - 2F_1}{\rightsquigarrow} \left(\begin{array}{cc|c} 1 & -1 & 7 \\ 0 & 4 & -16 \end{array}\right)$$

Luego, $y=-4$ y $x=3$.

P14. Por transformaciones elementales obtenemos

$$\begin{pmatrix}7&5\\5&3\end{pmatrix}\rightsquigarrow\begin{pmatrix}1&0\\0&4\end{pmatrix},\quad \begin{pmatrix}12&4&6\\30&8&4\\24&6&8\end{pmatrix}\rightsquigarrow\begin{pmatrix}2&0&0\\0&-42&0\\0&0&-2\end{pmatrix}$$

Luego el primer grupo es isomorfo a $\mathbb{Z}/4\mathbb{Z}$ y el segundo a $\mathbb{Z}/2\mathbb{Z}Z\oplus\mathbb{Z}/42\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

P15. Es una sencilla comprobación.

P16.

$$\begin{pmatrix}x&1&0\\0&x-1&2\\-1&-1&x-3\end{pmatrix}\overset{F_1xF_3}{\rightsquigarrow}\begin{pmatrix}-1&-1&x-3\\0&x-1&2\\x&1&0\end{pmatrix}\overset{F_3+xF_1}{\rightsquigarrow}\begin{pmatrix}-1&-1&x-3\\0&x-1&2\\0&1-x&x(x-3)\end{pmatrix}$$
$$\overset{\substack{C_2-C_1\\C_3+(x-3)C_1}}{\rightsquigarrow}\begin{pmatrix}-1&0&0\\0&x-1&2\\0&1-x&x(x-3)\end{pmatrix}\overset{C_2xC_3}{\rightsquigarrow}\begin{pmatrix}-1&0&0\\0&2&x-1\\0&x(x-3)&1-x\end{pmatrix}\overset{F_3+\frac{x(3-x)}{2}F_2}{\rightsquigarrow}$$
$$\begin{pmatrix}-1&0&0\\0&2&x-1\\0&0&\frac{(x-1)^2(x-2)}{2}\end{pmatrix}\overset{C_3+\frac{1-x}{2}C_2}{\rightsquigarrow}\begin{pmatrix}-1&0&0\\0&2&0\\0&0&\frac{(x-1)^2(2-x)}{2}\end{pmatrix}$$

Por tanto, $\mathbb{R}^3\simeq\mathbb{R}[x]/((x-1)^2(2-x))=\mathbb{R}[x]/(x-2)\oplus\mathbb{R}[x]/((x-1)^2)$ y los divisores elementales son $(x-2)$ y $(x-1)^2$.

Sea $e=(1,0,0)$ entonces una base de Jordan de T, es

$$\{(x-1)^2e=(1-2,1),(x-2)e=(-2,0,1),(x-1)(x-2)e=(2,-2,0)\}.$$

$\mathbb{R}^3=\mathbb{R}[x]/(x-2)\cdot(1-2,1)\oplus\mathbb{R}[x]/((x-1)^2)\cdot(-2,0,1)$.

P17. Es consecuencia inmediata del teorema de Hamilton-Cayley.

P18. El polinomio característico $c_T(x)$ y el polinomio anulador $p_{anul}(x)$ tienen las mismas raíces, por tanto, un polinomio es primo con $c_T(x)$ si y sólo si es primo con $p_{anul}(x)$. Si $p(x)$ es primo con $p_{anul}(x)$ existen $\lambda(x)$ y $\mu(x)$ tales que $\lambda(x)p(x)+\mu(x)p_{anul}(x)=1$. Por tanto, $\lambda(T)\circ p(T)+0=\mathrm{Id}$ y el inverso de $p(T)$ es $\lambda(T)$. Si $p(x)$ y $p_{anul}(x)$ no son primos entre sí, sea $q(x)$ el máximo común divisor. Observemos que si $q(T)$ es inyectivo, entonces el polinomio anulador sería $p_{anul}(x)/q(x)$, y esto es contradictorio. Como $\mathrm{Ker}\,q(T)\subseteq\mathrm{Ker}\,p(T)$. tenemos que $p(T)$ no es inyectivo, luego no es invertible.

P19. Sea $\{e_1,\dots,e_r\}$ una base de E' y (a_{ij}) la matriz de $T_{|E'}$. Sea $\{e_1,\dots,e_n\}$ una base de E, luego $\{\bar{e}_{r+1},\dots,\bar{e}_n\}$ es una base de E/E'. Sea (b_{kl}) la matriz de $\bar{T}$ en la base $\{\bar{e}_{r+1},\dots,\bar{e}_n\}$. La matriz de T en la base $\{e_1,\dots,e_n\}$ es de la forma

$$\left(\begin{array}{c|c}(a_{ij})&(c_{rs})\\\hline 0&(b_{kl})\end{array}\right)$$

y el polinomio característico es

$$c_T(x) = \left|\begin{array}{c|c} (a_{ij}) - x\,\mathrm{Id} & (c_{rs}) \\ \hline 0 & (b_{kl}) - x\,\mathrm{Id} \end{array}\right| = c_{T_{|E'}}(x) \cdot c_{\bar{T}}(x)$$

P20. Sea $\{e_1, \ldots, e_n\}$ una base de Jordan de T. La matriz de T es la base de Jordan es triangular, de diagonal $\alpha_1, \ldots, \alpha_n$. Es fácil comprobar que la matriz de $p(T)$ en la base $\{e_1, \ldots, e_n\}$ es triangular de diagonal $p(\alpha_1), \ldots, p(\alpha_)n$. Luego el polinomio característico de $p(T)$ es $\prod_{i=1}^{n}(x - p(\alpha_i))$.

P21. Si $\alpha \in \mathbb{R}$, $E = \mathbb{C}[x]/(x_\alpha)^n$ y $T = x\cdot$, entonces tenemos el isomorfismo de $\mathbb{R}[x]$-módulos

$$\mathbb{C}[x]/((x-\alpha)^n) = \langle \bar{1} \rangle \oplus \langle \bar{i} \rangle \simeq \mathbb{R}[x]/((x-\alpha)^n) \oplus \mathbb{R}[x]/((x-\alpha)^n).$$

Si $\alpha \in \mathbb{C}\backslash\mathbb{R}$, $E = \mathbb{C}[x]/(x_\alpha)^n$ y $T = x\cdot$, entonces tenemos el isomorfismo de $\mathbb{R}[x]$-módulos

$$\mathbb{C}[x]/((x-\alpha)^n) = \langle \bar{1} \rangle \simeq \mathbb{R}[x]/(((x-\alpha)\cdot(x-\overline{\alpha}))^n).$$

En ambos casos, el polinomio característico de T como endomorfismo $\mathbb{R}$-lineal es $c_T(x) \cdot \overline{c_T(x)}$.

El caso general se deduce de que $E \simeq \oplus_{n_{\alpha,i}} \mathbb{C}[x]/((x-\alpha)^{n_{\alpha,i}})$.

P22. Escribamos el sistema de ecuaciones $\nabla(X_n) = A \cdot X_n$, con

$$X_n := \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix}, \quad \nabla(X_n) := X_{n+1} = \begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix}, \quad A := (a_{ij}).$$

Entonces, las soluciones serán $X_n = A^n \cdot C$, siendo C una matriz de una columna y tres filas con coeficientes constantes cualesquiera. Para calcular A^n para todo n, recordemos que $A = B \cdot J \cdot B^{-1}$, siendo J la matriz de Jordan asociada y que $A^n = B \cdot J^n \cdot B^{-1}$.

BIBLIOGRAFÍA

[1] ATIYAH, M.F., MACDONALD, I.G. : *Introducción al Álgebra Conmutativa*, Ed. Reverté, 1973.

[2] BOURBAKI, N.: *Elements of Mathematics. Commutative Algebra*, Ed. Hermann - Adissson-Wesley, 1972.

[3] JACOBSON, N. : *Basic Algebra I*, W. H. Freeman and Company, San Francisco, 1974.

[4] KOSTRIKIN, A. I. : *Introducción al álgebra*, McGraw-Hill, Madrid, 1992.

[5] LANG, S. : *Álgebra*, Ed. Aguilar, Madrid, 1971.

[6] VAN DER WAERDEN, B.L. : *Modern Algebra*, Vol I. Frederick Ungar, New York, 1964.

[7] NAVARRO, J.A. : *Álgebra Conmutativa Básica*, Manuales UEX 19, 1996.

ÍNDICE ALFABÉTICO

UNIVERSIDAD DE EXTREMADURA

111

ÍNDICE