NOTAS DE TRABAJO, 3

ÁLGEBRA CONMUTATIVA

Álgebra conmutativa elemental

Pascual Jara Martínez

Departamento de Álgebra. Universidad de Granada

Granada, 1997–2014

Primera redacción: 1997.
Segunda redacción: Octubre 2007.
Tercera redacción: Octubre 2008.
Cuarta redacción: Octubre 2009.
Quinta redacción: Agosto 2011.
Sexta redacción: Septiembre 2012.
Séptima redacción: Junio 2014.

Introducción general

This text is a compilation of Álgebra Conmutativa Elemental.

Índice general

Parte I

Álgebra Conmutativa Elemental

Introducción

Tradicionalmente la Matemática se divide en tres áreas: Álgebra, Análisis y Geometría, pero como es usual esta división no es excluyente, y existen diversas intersecciones que hacen difícil determinar a qué área pertenece un determinado método o resultado. Tenemos sin embargo que tener en cuenta que progresivamente se ha producido una algebraización de la Matemática, esto es, los métodos y el lenguaje del Álgebra se han extendido por toda la Matemática; de esta forma grupos, anillos y cuerpos juegan cada vez más un papel central en los estudios modernos de Álgebra, Análisis, Geometría, Topología, y otras ramas de la Matemática moderna.

El Álgebra abstracta o Álgebra moderna tiene su origen en dos disciplinas: la teoría de números y la teoría de ecuaciones. Por teoría de números nos referimos a la teoría de sistemas de números que tiene sus orígenes en el sistema de los números naturales y llega a los sistemas de números complejos e hipercomplejos. La fundamentación de la teoría de números podemos buscarla en los Elementos de Euclides; texto que dedica una sección a la teoría de números. Sin embargo su fundamentación moderna se encuentra en P. de Fermat hacia 1600, y posteriormente en C. F. Gauss, quien introduce los enteros de Gauss tratando de probar el último Teorema de Fermat. Son R. Dedekind y L. Kronecker quienes desarrollan la teoría de cuerpos de números y de números algebraicos. De estos trabajos surgen algunos problemas centrales del "*Algebra abstracta*" sobre dominios de factorización y otros, y también sobre la teoría de números algebraicos.

La segunda motivación del Álgebra abstracta viene de la teoría de ecuaciones y de los estudios de la resolución por radicales de la ecuación de quinto grado. Hacía 1800 Ruffini y Abel probaron que no era posible obtener una fórmula que diese la solución de una quíntica general por radicales, y en 1820 Galois extiende este resultado a cualquier ecuación de grado mayor o igual que cinco. En su trabajo Galois introduce el concepto de grupo y el de acción de un grupo sobre un conjunto; concepto que será fundamental para la Matemática moderna.

La confluencia de estas dos teorías puede buscarse en Gauss, quien hacia 1800 prueba que toda ecuación polinómica no constante en el cuerpo de los números complejos tiene al menos una solución (Teorema fundamental del Álgebra). La teoría de ecuaciones en una indeterminada se puede extender a varias indeterminadas, apareciendo de esta forma los conjuntos algebraicos como los lugares formados por puntos que son soluciones de sistemas de polinomios multivariados, y que en el caso en que el cuerpo base es algebraicamente cerrado produce una equivalencia entre conceptos geométricos (conjuntos algebraicos) y algebraicos (anillos de coordenadas), que permite un tratamiento algorítmico de los primeros.

En esta parte vamos a describir los fundamentos de la teoría de anillos conmutativos, y algunas de sus primeras aplicaciones. Concluiremos con un estudio elemental de teoría de módulos, encaminada a

probar el teorema de estructura de los grupos abelianos finitos y a aplicaciones el estudio de formas canónicas de matrices.

Capítulo I

Teoría intuitiva de conjuntos

Introducción

Vamos a comenzar por una introducción intuitiva al concepto que es la base del curso: el de **conjunto**. Hemos preferido hacer esto así ya que una introducción rigurosa del concepto de conjunto exigiría demasiado esfuerzo a un posible lector novel, y lo apartaría de los objetivos centrales de este curso que son la introducción a las técnicas del trabajo matemático, y porque deseamos fijar las notaciones y el lenguaje que vamos a emplear a lo largo del curso.

Para poder comprender en su totalidad el concepto de conjunto y el álgebra de subconjuntos es necesario hacer una pequeña introducción al álgebra de proposiciones; de esta forma ya tendremos dos ejemplos de álgebras de Boole.

El concepto de conjunto se complementa con el de función o aplicación entre conjuntos, veremos la definición y algunas de sus propiedades.

Otro concepto de interés es el de relación. Aquí vamos a estudiar relaciones de equivalencia y de orden, aunque las segundas las estudiaremos en profundidad en un capítulo posterior.

Acabamos el capítulo con una introducción a los cuantificadores y al álgebra de predicados y con algunos ejemplos cómo hacer una demostración.

Me gustaría volver a insistir que la aproximación a los conceptos aquí tratados no es una aproximación axiomática sino intuitiva. Para una introducción a la teoría de conjuntos amena, y a la vez rigurosa, recomendamos el siguiente texto: [10].

1101-00.tex

1. Teoría de conjuntos

Vamos a considerar un **conjunto** X como una *colección* de **elementos**. Los elementos de un conjunto son distintos dos a dos, esto es, cualesquiera dos elementos de un conjunto o son el mismo elemento o son elementos distintos, y no hay ningún orden o relación entre ellos.
Los conjuntos pueden ser definidos de dos formas distintas:

- por **extensión**, esto es, haciendo una lista de todos sus elementos, o
- por **comprensión**, esto es, mediante una propiedad que caracteriza a sus elementos.

Ejemplo. 1.1. (Definición por extensión)
Un ejemplo de un conjunto definido por **extensión** es:

$$A = \{1, 2, a, b, c\}.$$

Según lo dicho antes, observar que $\{1, 2, a, a\}$ no es un conjunto ya que en él aparecen dos elementos repetidos, esto es, un mismo elemento aparece dos veces.

Ejemplo. 1.2. (Definición por comprensión)
Un ejemplo de un conjunto definido por **comprensión** es:

$$P = \{x \mid x \text{ es un número natural par}\}.$$

Si un elemento x **pertenece** a un conjunto X, escribimos

$$\mathbf{x \in X},$$

y si **no pertenece**, escribimos

$$\mathbf{x \notin X}.$$

Ejemplo. 1.3.
En los ejemplos anteriores tenemos que

$$1 \in A = \{1, 2, a, b, c\},$$

y

$$1 \notin P = \{x \mid x \text{ es un número natural par}\}.$$

Subconjuntos

Dado un conjunto X, un **subconjunto** de X es un conjunto Y verificando que para cada elemento $y \in Y$ se tiene $y \in X$. Escribimos entonces $\mathbf{Y \subseteq X}$.
Dos subconjuntos X_1 y X_2 de un conjunto X son **iguales** si $X_1 \subseteq X_2$ y $X_2 \subseteq X_1$, y escribimos $\mathbf{X_1 = X_2}$.
Si dos subconjuntos X_1 y X_2 de un conjunto X no son iguales, entonces decimos que son **distintos**, y escribimos $\mathbf{X_1 \neq X_2}$.
Si X_1 es un subconjunto de X y $X_1 \neq X$, podemos escribir $\mathbf{X_1 \subset X}$ ó $\mathbf{X_1 \subsetneq X}$, y decimos que X_1 es un **subconjunto propio** de X.

1101-01.tex

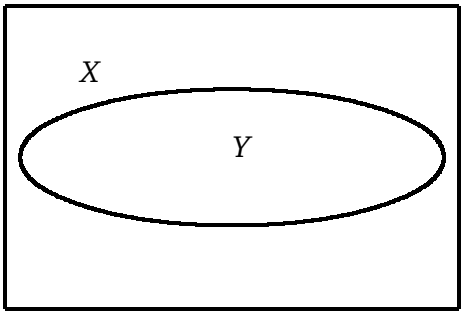
Ejemplo. 1.4.

(a) Cada conjunto es un subconjunto de sí mismo. Esto es, para cada conjunto X se tiene $X \subseteq X$; llamamos a X el **subconjunto impropio** de X.

(b) El conjunto $B = \{1, 2\}$ es un subconjunto de $A = \{1, 2, a, b, c\}$. Esto se representa por $B \subseteq A$. En cambio el conjunto $C = \{1, 2, 3\}$ no es un subconjunto de A. Esto se representa por $\mathbf{C} \nsubseteq \mathbf{A}$.

(c) El conjunto $B_0 = \{2, 1\}$ es igual al conjunto B; esto es, $\{1, 2\} = \{2, 1\}$.

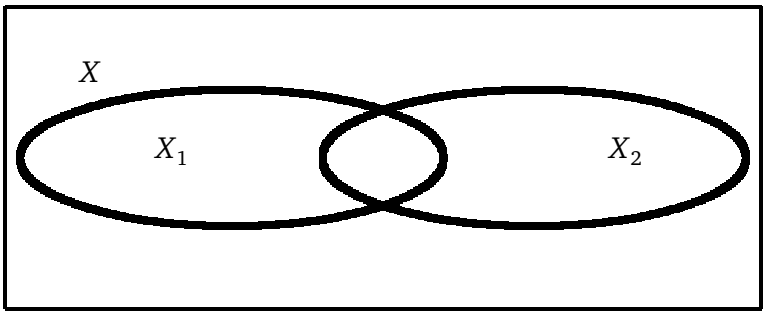
Si Y es un subconjunto de un conjunto X, a veces los representamos mediante un **diagrama de Venn**, esto es, el conjunto X se representa por el interior del cuadrado y el conjunto Y por el interior de la línea curva.



Operaciones con subconjuntos

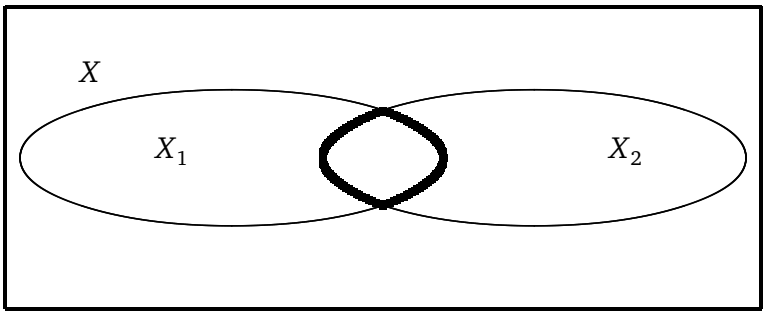
Si X_1 y X_2 son dos subconjuntos de un conjunto X, podemos definir su **unión** como el subconjunto de X definido por:

$$X_1 \cup X_2 = \{x \in X \mid \ x \in X_1 \text{ ó } x \in X_2\},$$



y su **intersección** como el subconjunto de X definido por:

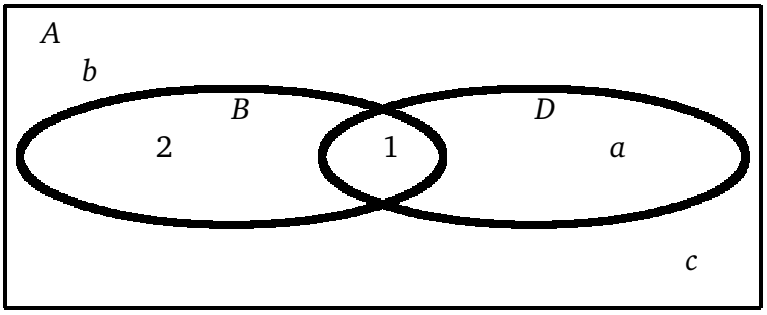
$$X_1 \cap X_2 = \{x \in X \mid \ x \in X_1 \text{ y } x \in X_2\},$$



Ejemplo. 1.5.

(a) Sea $D = \{1, a\}$. Como $B = \{1, 2\}$ y D son subconjuntos del conjunto $A = \{1, 2, a, b, c\}$, entonces podemos calcular su unión y su intersección. Se verifica:

$$B \cup D = \{1, 2, a\} \quad \text{y} \quad B \cap D = \{1\}.$$



(b) También $B = \{1, 2\}$ y $B_0 = \{2, 1\}$ son subconjuntos del conjunto A; en este caso tenemos

$$B \cup B_0 = B = B_0 \quad \text{y} \quad B \cap B_0 = B = B_0.$$

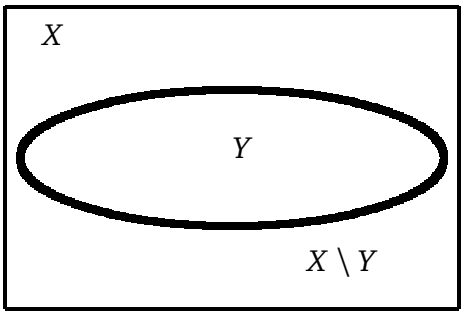
Existe un conjunto especial que está definido por la propiedad de no tener ningún elemento. Este conjunto se llama **vacío** y se representa por el símbolo $\varnothing$.

Cada conjunto X tiene un único subconjunto que no tiene ningún elemento, si representamos por $\varnothing$ a este subconjunto, entonces $\varnothing$ es un subconjunto de X. El subconjunto $\varnothing$ se llama **subconjunto vacío o trivial** de X.

Si la intersección de dos subconjuntos X_1 y X_2 de un conjunto X es igual a $\varnothing$, decimos que son **subconjuntos disjuntos**.

Sea Y un subconjunto de un conjunto X, llamamos **subconjunto complemento** de Y en X al siguiente subconjunto de X:

$$\overline{Y} = X \setminus Y = \{x \in X \mid x \notin Y\}.$$



Ejemplo. 1.6.
El complemento de $B = \{1, 2\}$ en $A = \{1, 2, a, b, c\}$ es:

$$\overline{B} = \{a, b, c\}.$$

Observación. 1.7.
Observa que para cada subconjunto Y de un conjunto X, los subconjuntos Y y $\overline{Y}$ son siempre disjuntos.

Ejercicio. 1.8.
Sea X un conjunto e Y un subconjunto de X. Probar que $\overline{\overline{Y}} = Y$.

SOLUCIÓN. Tenemos que probar que $\overline{\overline{Y}} \subseteq Y$ y que $Y \subseteq \overline{\overline{Y}}$. Para esto último cojamos un elemento $y \in Y$, entonces $y \in X$ y además $y \notin \overline{Y}$, luego $y \in \overline{\overline{Y}}$.

Recíprocamente, si $y \in \overline{\overline{Y}}$, por definición $y \in X$ y además $y \notin \overline{Y}$, luego $y \in Y$. □

Dado un conjunto X, existe un conjunto cuyos elementos son todos los subconjuntos de X. A este conjunto lo llamamos el **conjunto de las partes** ó **conjunto potencia** de X y lo representamos por $\mathscr{P}(X)$.

Ejemplo. 1.9.
(a) El conjunto de las partes del conjunto $A = \{1, 2, a, b, c\}$ es:

$$\begin{aligned}\mathscr{P}(A) = \{ &\varnothing, \{1\}, \{2\}, \{a\}, \{b\}, \{c\},\\ &\{1,2\}, \{1,a\}, \{1,b\}, \{1,c\}, \{2,a\}, \{2,b\}, \{2,c\}, \{a,b\}, \{a,c\}, \{b,c\},\\ &\{1,2,a\}, \{1,2,b\}, \{1,2,c\}, \{1,a,b\}, \{1,a,c\}, \{1,b,c\}, \{2,a,b\}, \{2,a,c\}, \{2,b,c\},\\ &\{a,b,c\}, \{1,2,a,b\}, \{1,2,a,c\}, \{1,2,b,c\}, \{1,a,b,c\}, \{2,a,b,c\},\\ &\{1,2,a,b,c\}\}.\end{aligned}$$

(b) El conjunto de las partes del conjunto $D = \{u, v, w\}$ es:

$$\mathscr{P}(D) = \{\varnothing, \{u\}, \{v\}, \{w\}, \{u,v\}, \{u,w\}, \{v,w\}, \{v,w\}, \{u,v,w\}\}.$$

(c) El conjunto de las partes del conjunto $\varnothing$ es:

$$\mathscr{P}(\varnothing) = \{\varnothing\}.$$

Observa que $\mathscr{P}(\varnothing) = \{\varnothing\}$ es un conjunto con un elemento.
(d) El conjunto de las partes del conjunto $\{\varnothing\}$ es:

$$\mathscr{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}.$$

A los conjuntos que tienen un número finito de elementos los llamaremos **conjuntos finitos**, y a los que no tienen un número finito de elementos los llamaremos **conjuntos infinitos**.

Ejemplo. 1.10.
(1) El conjunto $A = \{1, 2, a, b, c\}$ es un conjunto finito.
(2) El conjunto vacío, $\emptyset$, es un conjunto finito.
(3) El conjunto $\mathbb{R}$ de los números reales es un conjunto infinito.

Cuando X es un conjunto finito el número de sus elementos lo llamamos su **cardinal**. También se define el **cardinal** de conjuntos infinitos, pero no vamos a tratar este problema aquí.

Ejercicio. 1.11.
Si X es un conjunto con n elementos, probar que el conjunto $\mathscr{P}(X)$ tiene 2^n elementos.

SOLUCIÓN. Subconjunto de X con 0 elementos hay exactamente uno. Subconjunto de X con un elemento hay exactamente n, el número de elementos de X. Subconjuntos de X con dos elementos hay $n(n-1)/2 = \binom{n}{2}$. En general si $t \leq n$, el número de subconjuntos de X con t elementos es $\binom{n}{t}$. Luego en total tenemos

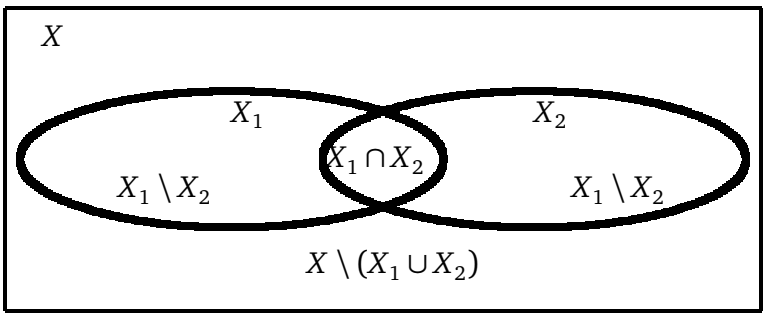
$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = (1+1)^n = 2^n.$$

□

Dados dos subconjuntos, X_1 y X_2, de un conjunto X llamamos **diferencia** de X_1 y X_2 al subconjunto $X_1 \setminus X_2$, definido por:

$$X_1 \setminus X_2 = X_1 \cap \overline{X_2}.$$

Observa que en general se tiene $X_1 \setminus X_2 \neq X_2 \setminus X_1$.



Antes de abordar el problema de estudiar las propiedades que verifican la unión, intersección y complemento, vamos a estudiar cómo trabajar con afirmaciones o proposiciones.

Nos planteamos la siguiente pregunta: si X_1, X_2 y X_3 son tres subconjuntos de un conjunto X,

¿Qué relación existe entre $(X_1 \cap X_2) \cup X_3$ y $(X_1 \cup X_3) \cap (X_2 \cup X_3)$?

Para establecer la relación existente entre ambos conjuntos, tenemos que analizar las expresiones que nos definen cada uno de ellos:

$$(x \in X_1 \text{ y } x \in X_2) \text{ ó } x \in X_3$$

y

$$(x \in X_1 \text{ ó } x \in X_3) \text{ y } (x \in X_2 \text{ ó } x \in X_3).$$

Ejercicios

Teoría de conjuntos

Ejercicio. 1.12.
Si A, B, y C son conjuntos tales que $C \subseteq B$ y $B \subseteq A$, prueba que $C \subseteq A$.
Ref.: 1101e_001 *SOLUCIÓN.*

2. Álgebra de proposiciones

Una **proposición** es una afirmación. Por lo tanto las proposiciones pueden tomar dos valores:

V, verdadero o,

F, falso.

Vamos a representar las proposiciones por letras mayúsculas en negrita **A**.

Ejemplo. 2.1.

(a) "Hoy es lunes", es un ejemplo de una proposición.
(b) "El hambre en el mundo se puede erradicar", es un ejemplo de una proposición.
(c) "*¿Para sacar dinero del cajero tienes primero que introducir la tarjeta?*", no es una proposición.

Si **A** y **B** son dos proposiciones, definimos nuevas proposiciones, a las que llamaremos **proposiciones compuestas**, o también simplemente proposiciones, mediante las siguientes construcciones:

A $\wedge$ **B**, que se lee "**A** y **B**", y su definición está dada por la tabla siguiente.

A $\wedge$ **B**

A	**A** $\wedge$ **B**	**B**
V	V	V
F	F	V
V	F	F
F	F	F

A $\vee$ **B**, que se lee "**A** ó **B**", y su definición está dada por la tabla siguiente.

A $\vee$ **B**

A	**A** $\vee$ **B**	**B**
V	V	V
F	V	V
V	V	F
F	F	F

$\neg$**A**, que se lee "no **A**", y su definición está dada por la tabla siguiente

$\neg$**A**

A	$\neg$**A**
V	F
F	V

Ejemplo. 2.2.

(a) "Hoy **no** es lunes" sería la negación de "Hoy es lunes".
(b) "El coche es rojo" o "La libreta es amarilla" sería la proposición "El coche es rojo **o** la libreta es amarilla".
(c) "El coche es mío" y "yo no tengo una bicicleta" sería la proposición "El coche es mío **y** yo no tengo una bicicleta".

1101-02.tex

(d) Podemos negar una proposición compuesta, por ejemplo la negación de "El coche es mío **y** yo no tengo una bicicleta" sería: "El coche **no** es mío **o** yo **tengo** una bicicleta".

Dos proposiciones **A** y **B** son **equivalentes** si **A** es verdadera cuando **B** lo es y **B** es verdadera cuando **A** lo es. Dadas dos proposiciones definimos una nueva proposición mediante

$\mathbf{A} \Longleftrightarrow \mathbf{B}$

A	**A** $\Longleftrightarrow$ **B**	**B**
V	V	V
F	F	V
V	F	F
F	V	F

Entonces dos proposiciones **A** y **B** son equivalentes si la proposición $\mathbf{A} \Longleftrightarrow \mathbf{B}$ toma solo el valor V.

Ejemplo. 2.3.
Las proposiciones $\mathbf{A} \vee \mathbf{B}$ y $\mathbf{B} \vee \mathbf{A}$ son proposiciones equivalentes para cualesquiera proposiciones **A** y **B**.

A	**A** $\vee$ **B**	**B**	(**A** $\vee$ **B**) $\Longleftrightarrow$ (**B** $\vee$ **A**)	**B**	**B** $\vee$ **A**	**A**
A	$\vee$	**B**	$\Longleftrightarrow$	**B**	$\vee$	**A**
V	V	V	V	V	V	V
F	V	V	V	V	V	F
V	V	F	V	F	V	V
F	F	F	V	F	F	F

Lo mismo ocurre con las proposiciones $\mathbf{A} \wedge \mathbf{B}$ y $\mathbf{B} \wedge \mathbf{A}$

Ejercicio. 2.4.
Probar que $\mathbf{A} \wedge \mathbf{B}$ *y* $\mathbf{B} \wedge \mathbf{A}$ *son proposiciones equivalentes para cualesquiera proposiciones* ***A*** *y* ***B****.*

Una proposición que toma siempre el valor V se llama una **tautología**.

Ejercicio. 2.5.
Probar que para cada proposición **A** *la proposición* $\mathbf{A} \vee \overline{\mathbf{A}}$ *es una tautología.*

Aplicación a la teoría de conjuntos

Podemos considerar ahora las propiedades elementales de las operaciones que hemos introducido entre los subconjuntos de un conjunto dado.

Proposición. 2.6.
Sea X un conjunto y sean X_1, X_2, X_3 subconjuntos de X, se verifica:

$$\begin{array}{rcll} X_1 \cup (X_2 \cup X_3) & = & (X_1 \cup X_2) \cup X_3 & \textbf{\textit{P. asociativa}} \\ X_1 \cap (X_2 \cap X_3) & = & (X_1 \cap X_2) \cap X_3 & \\ X_1 \cup X_2 & = & X_2 \cup X_1 & \textbf{\textit{P. conmutativa}} \\ X_1 \cap X_2 & = & X_2 \cap X_1 & \\ X_1 \cup X_1 & = & X_1 & \textbf{\textit{P. de idempotencia}} \\ X_1 \cap X_1 & = & X_1 & \\ X_1 \cup \varnothing & = & X_1 & \textbf{\textit{E. neutros}} \\ X_1 \cap X & = & X_1 & \\ X_1 \cap \varnothing & = & \varnothing & \textbf{\textit{P. absorción}} \\ X_1 \cup X & = & X & \end{array}$$

Otro tipo de propiedades son las siguientes:

Proposición. 2.7.
Sea X un conjunto y sean X_1, X_2, X_3 subconjuntos de X, se verifica:

$$\begin{array}{rcll} X_1 \cup (X_2 \cap X_3) & = & (X_1 \cup X_2) \cap (X_1 \cup X_3) & \textbf{\textit{P. distributiva}} \\ X_1 \cap (X_2 \cup X_3) & = & (X_1 \cap X_2) \cup (X_1 \cap X_3) & \\ \overline{X_1 \cup X_2} & = & \overline{X_1} \cap \overline{X_2} & \textbf{\textit{Ley de De Morgan}} \\ \overline{X_1 \cap X_2} & = & \overline{X_1} \cup \overline{X_2} & \\ X_1 \cup \overline{X_1} & = & X & \textbf{\textit{E. complementos}} \\ X_1 \cap \overline{X_1} & = & \varnothing & \end{array}$$

Observa que en estos casos todos los conjuntos que aparecen son siempre subconjuntos de un mismo conjunto X.

Para ver que estas igualdades son ciertas, esto es, que los conjuntos que en ellas aparecen son iguales, vamos a comprobar que tienen los mismos elementos. Haremos esto partiendo de la definición del subconjunto correspondiente y obteniendo las consecuencias oportunas.

Para este fin vamos a introducir la siguientes notación: *Cuando de una afirmación se deduce otra, escribimos las dos afirmaciones y entre ambas escribimos el símbolo* $\Rightarrow$.

En el párrafo anterior en realidad estamos introduciendo una nueva forma de obtener nuevas proposiciones a partir de otras dadas. Vamos a hacer una justificación de esto:

Si **A** y **B** son proposiciones, definimos una nueva proposición mediante

$$\mathbf{A} \Longrightarrow \mathbf{B} = (\neg \mathbf{A}) \vee \mathbf{B}$$

A	**A** $\Longrightarrow$ **B**	**B**
V	V	V
F	V	V
V	F	F
F	V	F

La nueva proposición **A** $\Longrightarrow$ **B** se lee:

"**A** implica **B**",
"de **A** se deduce **B**" ó
"si **A** entonces **B**".

Tal y como hemos señalado antes indica que si la afirmación **A** es verdadera, entonces *necesariamente* **B** también lo es.

Puede parecer extraño el hecho de que **A** $\Longrightarrow$ **B** es verdadera cuando **A** es falsa y **B** es verdadera o falsa; esto refleja el bien conocido hecho de que de premisas falsas se podría obtener cualquier resultado verdadero o falso.

Observar que el único caso en que **A** $\Longrightarrow$ **B** es falsa es cuando **A** es verdadera y **B** es falsa, esto significa que no se va a poder deducir un resultado falso de un resultado verdadero.

Para probar las Proposiciones (2.6.) y (2.7.), antes tenemos que probar los resultados sobre proposiciones.

En nuestro caso, como ya conocemos que **A** $\vee$ **B** y **B** $\vee$ **A** son proposiciones equivalentes, resulta que podemos hacer la siguiente demostración:

DEMOSTRACIÓN. [**Propiedad conmutativa de la unión: $\mathbf{X_1 \cup X_2 = X_2 \cup X_1}$**]

Comprobamos que se tiene $X_1 \cup X_2 \subseteq X_2 \cup X_1$ y también $X_2 \cup X_1 \subseteq X_1 \cup X_2$. Esto es, vemos que cada elemento $x \in X_1 \cup X_2$ verifica $x \in X_2 \cup X_1$.

$$\begin{aligned} x \in X_1 \cup X_2 &\Rightarrow x \in X_1 \ \vee \ x \in X_2 \\ &\Rightarrow x \in X_2 \ \vee \ x \in X_1 \\ &\Rightarrow x \in X_2 \cup X_1 \end{aligned}$$

En forma semejante se tiene que cada elemento $x \in X_2 \cup X_1$ verifica $x \in X_1 \cup X_2$; basta intercambiar X_1 y X_2. □

Aquí hemos utilizado que se tiene una equivalencia entre las proposiciones **A** $\vee$ **B** y **B** $\vee$ **A** para cualesquiera proposiciones **A** y **B**.

Veamos otro ejemplo. Si probamos que son equivalentes las proposiciones $\neg(\mathbf{A} \vee \mathbf{B})$ y $(\neg\mathbf{A}) \wedge (\neg\mathbf{B})$, para cualesquiera proposiciones **A** y **B** (ley de de Morgan), esto es, si en la tabla siguiente debajo del

símbolo $\Longleftrightarrow$ sólo parecen V,

$(\neg$	**A)**	$\wedge$	$(\neg$	**B)**	$\Longleftrightarrow$	$\neg$	**(A**	$\vee$	**B)**
F	V	F	F	V	V	F	V	V	V
V	F	F	F	V	V	F	F	V	V
F	V	F	V	F	V	F	V	V	F
V	F	V	V	F	V	V	F	F	F
2	1	3	2	1	4	3	1	2	1

entonces podemos hacer la demostración de la Ley de De Morgan para conjuntos.

DEMOSTRACIÓN. [**Demostración de la ley de De Morgan:** $\overline{\mathbf{X_1 \cup X_2}} = \overline{\mathbf{X_1}} \cap \overline{\mathbf{X_2}}$]
Comprobamos que se verifican las inclusiones $\overline{X_1 \cup X_2} \subseteq \overline{X_1} \cap \overline{X_2}$ y $\overline{X_1} \cap \overline{X_2} \subseteq \overline{X_1 \cup X_2}$.
Para la primera tenemos que ver que cada elemento $x \in \overline{X_1 \cup X_2}$ verifica también $x \in \overline{X_1} \cap \overline{X_2}$.

$$\begin{aligned} x \in \overline{X_1 \cup X_2} &\Rightarrow x \notin X_1 \cup X_2 \\ &\Rightarrow x \notin X_1 \ \wedge \ x \notin X_2 \\ &\Rightarrow x \in \overline{X_1} \ \wedge \ x \in \overline{X_2} \\ &\Rightarrow x \in \overline{X_1} \cap \overline{X_2} \end{aligned} \tag{I.1}$$

La inclusión $\overline{X_1} \cap \overline{X_2} \subseteq \overline{X_1 \cup X_2}$ se prueba simplemente invirtiendo las implicaciones que aparecen en la lista (I.1).

$$\begin{aligned} x \in \overline{X_1 \cup X_2} &\Leftarrow x \notin X_1 \cup X_2 \\ &\Leftarrow x \notin X_1 \ \wedge \ x \notin X_2 \\ &\Leftarrow x \in \overline{X_1} \ \wedge \ x \in \overline{X_2} \\ &\Leftarrow x \in \overline{X_1} \cap \overline{X_2} \end{aligned} \tag{I.2}$$

□

Esta lista (I.2) podríamos también haberla escrito como

$$\begin{aligned} x \in \overline{X_1} \cap \overline{X_2} &\Rightarrow x \in \overline{X_1} \ \wedge \ x \in \overline{X_2} \\ &\Rightarrow x \notin X_1 \ \wedge \ x \notin X_2 \\ &\Rightarrow x \notin X_1 \cup X_2 \\ &\Rightarrow x \in \overline{X_1 \cup X_2} \end{aligned} \tag{I.3}$$

Las listas (I.1) y (I.2) se pueden escribir abreviadamente como

$$\begin{aligned} x \in \overline{X_1 \cup X_2} &\Longleftrightarrow x \notin X_1 \cup X_2 \\ &\Longleftrightarrow x \notin X_1 \ \wedge \ x \notin X_2 \\ &\Longleftrightarrow x \in \overline{X_1} \ \wedge \ x \in \overline{X_2} \\ &\Longleftrightarrow x \in \overline{X_1} \cap \overline{X_2} \end{aligned} \tag{I.4}$$

Ejercicio. 2.8.
Probar todos los resultados que aparecen en la Proposición (2.6.) y la Proposición (2.7.) sobre propiedades de la unión, intersección y complementario de subconjuntos de un conjunto dado.

Existen muchos otros resultados sobre la unión, intersección y complementario que nos irán apareciendo a lo largo de este curso, y de otros cursos. Para su demostración podremos hacer uso de la misma técnica de demostración que hemos empleado aquí, pero también podemos hacer uso de los resultado que ya hayamos probado. Veamos un ejemplo.

Ejercicio. 2.9.
Sean X_1, X_2 subconjuntos de un conjunto X. Probar que se verifica:

$$(X_1 \cap \overline{X_2}) \cup (\overline{X_1} \cap X_2) = (X_1 \cup X_2) \cap \overline{(X_1 \cap X_2)}$$

SOLUCIÓN. En este caso podemos también probar que cada elemento del primer subconjunto es un elemento del segundo y viceversa. Podéis comprobar que este proceso es largo. Es mejor entonces utilizar las relaciones que se han establecido en la Proposición (2.6.) y la Proposición (2.7.). Tenemos entonces:

$$\begin{aligned}
(X_1 \cap \overline{X_2}) \cup (\overline{X_1} \cap X_2) &= [X_1 \cup (\overline{X_1} \cap X_2)] \cap [\overline{X_2} \cup (\overline{X_1} \cap X_2)] \\
&= [(X_1 \cup \overline{X_1}) \cap (X_1 \cup X_2)] \cap [(\overline{X_2} \cup \overline{X_1}) \cap (\overline{X_2} \cup X_2)] \\
&= [X \cap (X_1 \cup X_2)] \cap [(\overline{X_2} \cup \overline{X_1}) \cap X] \\
&= (X_1 \cup X_2) \cap (\overline{X_2} \cup \overline{X_1}) \\
&= (X_1 \cup X_2) \cap \overline{(X_2 \cap X_1)} \\
&= (X_1 \cup X_2) \cap \overline{(X_1 \cap X_2)}
\end{aligned}$$

□

El subconjunto $(X_1 \cap \overline{X_2}) \cup (\overline{X_1} \cap X_2)$ se llama la **diferencia simétrica** de X_1 y X_2. La vamos a representar por el símbolo Δ;

$$X_1 \Delta X_2 = (X_1 \cup X_2) \cap \overline{(X_1 \cap X_2)} = X_2 \Delta X_1.$$

Producto cartesiano de dos conjuntos

Dados dos conjuntos X e Y, existe un nuevo conjunto, al que llamamos el **producto cartesiano** de X e Y, cuyos elementos son:

$$X \times Y = \{(x, y) \mid x \in X \text{ y } y \in Y\}.$$

Si X' e Y' son subconjuntos de X e Y respectivamente, entonces $X' \times Y'$ se considera un subconjunto de $X \times Y$.

Ejercicio. 2.10.
Sean X e Y conjuntos y X_1, X_2 subconjuntos del conjunto X. Prueba que se verifica
(1) $X_1 \times Y \cup X_2 \times Y = (X_1 \cup X_2) \times Y$.
(2) $X_1 \times Y \cap X_2 \times Y = (X_1 \cap X_2) \times Y$.

Ejercicio. 2.11.
Sean X e Y dos conjuntos y X', Y' subconjuntos de X e Y respectivamente. Prueba que se verifica $\overline{X' \times Y'} = (\overline{X'} \times Y) \cup (X \times \overline{Y'})$.

Observación. 2.12.
Hasta ahora las operaciones que hemos realizados entre conjuntos en realidad lo han sido entre subconjuntos de un conjunto dado. Podemos definir la unión o la intersección de dos conjuntos arbitrarios, pero preferimos establecer la siguiente convención o axioma.

Dados dos conjuntos X e Y, existe un conjunto Z tal que $X \subseteq Z$ e $Y \subseteq Z$.

Entonces podemos definir la unión o intersección de dos conjuntos arbitrarios apelando a la definición de unión e intersección de subconjuntos de un conjunto.

Ejercicios

Álgebra de proposiciones

Ejercicio. 2.13.
Prueba que $[(A \vee B) \wedge A] \Leftrightarrow A$.
Ref.: 1101e_002 *SOLUCIÓN.*

3. Aplicaciones

Sean X e Y dos conjuntos, una **aplicación** de X a Y es una regla que permite asignar a cada elemento del conjunto X un *único* elemento del conjunto Y.
Si f es una aplicación de X en Y, vamos a representar f mediante:

$$f : X \longrightarrow Y \quad \text{ó} \quad X \xrightarrow{f} Y$$

Si $x \in X$ y $f : X \longrightarrow Y$ es una aplicación, llamamos $f(x)$ al único elemento de Y que asigna f a x, y lo llamamos **imagen** de x por f.
El conjunto

$$\mathrm{Im}(f) = \{f(x) \in Y \mid x \in X\}$$

se llama la **imagen de la aplicación** f, y es un subconjunto de Y.
En general, si X_1 es un subconjunto de X, llamamos **imagen** de X_1 por f al subconjunto $f(X_1)$ de Y definido como:

$$f(X_1) = \{f(x) \in Y \mid x \in X_1\}.$$

Si Y_1 es un subconjunto de Y, llamamos **imagen inversa** de Y_1 por f al subconjunto $f^{-1}(Y_1)$de X definido como:

$$f^{-1}(Y_1) = \{x \in X \mid f(x) \in Y_1\}.$$

Ejemplo. 3.1.
Sean $A = \{1, 2, a, b, c\}$ y $E = \{\alpha, \beta, \gamma, \delta\}$ dos conjuntos y $f : A \longrightarrow E$ la aplicación definida por $f(1) = \beta$, $f(2) = \delta$, $f(a) = \alpha$, $f(b) = \alpha$, $f(c) = \beta$.
Entonces la imagen de f es:

$$\mathrm{Im}(f) = \{\alpha, \beta, \delta\}.$$

La imagen de $B = \{1, 2\} \subseteq A$ es:

$$f(B) = \{\beta, \delta\}.$$

La imagen inversa de $F = \{\gamma, \delta\} \subseteq E$ es:

$$f^{-1}(F) = \{2\}.$$

Ejercicio. 3.2.
Sea $f : X \longrightarrow Y$ una aplicación y sean $A, B \subseteq X$ subconjuntos de X.
(a) Probar que $f(A \cup B) = f(A) \cup f(B)$.
(b) ¿Qué relación existe entre $f(A \cap B)$ y $f(A) \cap f(B)$?

1101-03.tex

Ejercicio. 3.3.
Sea $f : X \longrightarrow Y$ una aplicación y sean $C, D \subseteq Y$ subconjuntos de Y.
(a) Probar que $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.
(b) ¿Qué relación existe entre $f^{-1}(A \cap B)$ y $f^{-1}(A) \cap f^{-1}(B)$?

Vamos a establecer el concepto de aplicación de forma más formal. Sean X e Y dos conjuntos, un **grafo de aplicación** de X en Y es un subconjunto G del conjunto producto cartesiano $X \times Y$ verificando la siguiente propiedad:

$$\textit{para cada } x \in X \textit{ existe un único } y \in Y \textit{ tal que } (x, y) \in G.$$

De la definición se deduce que si un par (x, y) pertenece a G, el elemento y está unívocamente determinado por el elemento x, por lo que vamos a representar y por $G(x)$. Así pues un grafo de aplicación G determina una aplicación

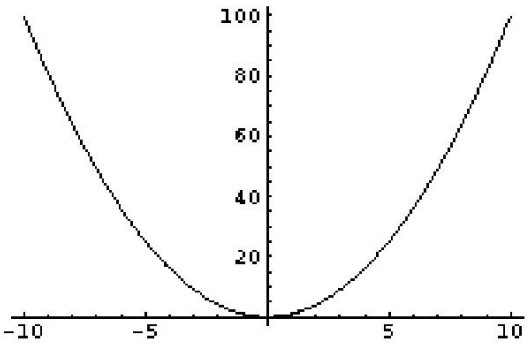
$$x \mapsto G(x),$$

en el sentido en el que las hemos definido anteriormente. Y recíprocamente, si $f : X \longrightarrow Y$ es una aplicación, definimos el **grafo** de f mediante

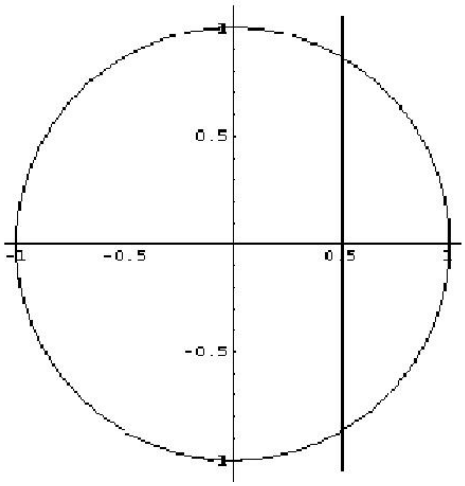
$$Gr(f) = \{(x, f(x)) \in X \times Y \mid x \in X\}.$$

Entonces $Gr(f)$ es un grafo de aplicación.
La formalización del concepto de aplicación pasa pues por identificar los dos conceptos, el de aplicación y el de grafo de aplicación.

Ejemplo. 3.4.
Observa que si consideramos la aplicación $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = x^2$, resulta que la **gráfica** de la función es la parábola siguiente. Por lo tanto f es una aplicación de $\mathbb{R}$ en $\mathbb{R}$ y su grafo son los puntos de la parábola.



Observa que si consideramos la gráfica de una circunferencia $x^2 + y^2 = 1$, esta gráfica *no es un grafo de aplicación*, $x \mapsto y$, de $\mathbb{R}$ a $\mathbb{R}$, pues hay puntos, por ejemplo $x = \frac{1}{2}$ que tienen dos posibles imágenes: $\frac{\sqrt{3}}{4}$ y $-\frac{\sqrt{3}}{4}$.



En resumen. *Dados dos conjuntos X e Y, dar una aplicación f de X a Y es lo mismo que dar un subconjunto $G \subseteq X \times Y$ que es un grafo de aplicación. En este caso la aplicación $f : X \longrightarrow Y$ lleva cada elemento $x \in X$ en el único elemento $y \in Y$ tal que el par $(x, y) \in G$, entonces el elemento y está determinado unívocamente por x y f, por lo que lo representaremos por $f(x)$.*

Dos aplicaciones $f, g : X \longrightarrow Y$ son **iguales** si para cada $x \in X$ se verifica $f(x) = g(x)$

Tipos de aplicaciones

Sea $f : X \longrightarrow Y$ una aplicación, decimos que f es **sobreyectiva** si $\mathrm{Im}(f) = Y$, esto es, si para cada elemento $y \in Y$ existe un elemento $x \in X$ tal que $f(x) = y$.

Llamamos **inyectiva** a una aplicación $f : X \longrightarrow Y$ tal que para cualesquiera dos elementos $x_1, x_2 \in X$, si $f(x_1) = f(x_2)$, entonces $x_1 = x_2$.

Ejercicio. 3.5.
Sea $g : \mathbb{Q}^+ \longrightarrow \mathbb{Q}^+$ definida por $f(x) = x^2$ para cada $x \in \mathbb{Q}^+$. Probar que la aplicación g es inyectiva y no es sobreyectiva.

SOLUCIÓN. Para comprobarlo procedemos como sigue: si $g(x_1) = g(x_2)$, entonces tenemos $x_1^2 = x_2^2$, de donde deducimos que $x_1 = x_2$, ya que ambos son positivos.

Sin embargo g no es una aplicación sobreyectiva, ya que por ejemplo $2 \notin \mathrm{Im}(g)$.

Para comprobarlo basta suponer que esto no fuese cierto, entonces existiría un elemento $x \in \mathbb{Q}^+$ tal que $x^2 = 2$, lo cual es imposible, ya que $\sqrt{2}$ no es un número racional. □

Ejemplo. 3.6.
La aplicación f del ejemplo de la página 23 no es sobreyectiva ya que $\gamma \notin \text{Im}(f)$, y no es inyectiva, ya que, por ejemplo, $f(1) = \beta = f(c)$.

Una aplicación $f : X \longrightarrow Y$ que es a la vez inyectiva y sobreyectiva se llama una **aplicación biyectiva** o una **biyección**.

Ejemplo. 3.7.
La aplicación $h : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ definida $h(x) = x^2$ para cada $x \in \mathbb{R}$ es una biyección.

Composición de aplicaciones

Supongamos que $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ son aplicaciones, definimos una nueva aplicación $g \circ f : X \longrightarrow Z$ como sigue:

$$(g \circ f)(x) = g(f(x)) \text{ para cada } x \in X.$$

La aplicación $g \circ f$ se llama la **composición** de f y g. La composición de f y g se suele representar también simplemente por gf.
Para cada conjunto X existe una aplicación especial, llamada **identidad** en X, a la que representamos por $\mathbf{id}_X$ y que está definida por $\text{id}_X(x) = x$ para cada $x \in X$.

Lema. 3.8.
Sea $f : X \longrightarrow Y$ una aplicación. Se verifica $f \circ id_X = f$ y $id_Y \circ f = f$.

Si $f : X \longrightarrow Y$ es una aplicación, llamamos una **aplicación inversa** de f a una aplicación $g : Y \longrightarrow X$ que verifica $f \circ g = \text{id}_Y$ y $g \circ f = \text{id}_X$.

Observación. 3.9.
En general si una aplicación f tiene una inversa, esta inversa se representa por f^{-1}.
¡OJO! No confundir con la notación f^{-1} utilizada para la imagen inversa de un subconjunto.

Lema. 3.10.
Si una aplicación $f : X \longrightarrow Y$ tiene una inversa, entonces es una biyección.

Ejercicio. 3.11.
Demuestra que si $f : X \longrightarrow Y$ es una biyección, entonces existe una inversa de f.

Tenemos entonces que una aplicación $f : X \longrightarrow Y$ es biyectiva si y solo si tiene una inversa.

Observación. 3.12.
Observa que al decir que una aplicación $f : X \longrightarrow Y$ tiene una inversa hemos dicho que existe una aplicación $g : Y \longrightarrow X$ verificando $fg = \mathrm{id}_Y$ y $gf = \mathrm{id}_X$, no basta con sólo una de las igualdades, ya que dada la aplicación $f : \{1,2\} \longrightarrow \{a\}$ existen dos aplicaciones $g_i : \{a\} \longrightarrow \{1,2\}$, para $i = 1,2$, definidas $g_i(a) = i$, y verificando $f g_i = \mathrm{id}_{\{a\}}$, pero no es biyectiva. En efecto, es fácil ver que f no es una aplicación inyectiva.

Ejercicio. 3.13.
Si $f : X \longrightarrow Y$ es una aplicación, y $g, h : Y \longrightarrow X$ son inversas de f, entonces $g = h$.

SOLUCIÓN. Para cada $y \in Y$ se tiene: $g(y) = (g(fh))(y) = ((gf)h)(y) = h(y)$. □

Ejercicios

Aplicaciones

Ejercicio. 3.14.
Prueba que para una aplicación $f : X \longrightarrow Y$ son equivalentes:
(a) f es inyectiva.
(b) Existe una aplicación $g : Y \longrightarrow X$ tal que $gf = id_X$.

Ref.: 1101e_003 *SOLUCIÓN.*

Ejercicio. 3.15.
Prueba que para toda aplicación $f : X \longrightarrow Y$ son equivalentes:
(a) f es sobreyectiva.
(b) Existe una aplicación $g : Y \longrightarrow X$ tal que $fg = id_Y$.

Ref.: 1101e_004 *SOLUCIÓN.*

4. Relaciones de equivalencia y de orden

Una **relación** R en un conjunto X es una regla que permite distinguir si dos elementos están o no relacionados. Si dos elementos $x,\ y \in X$ están relacionados mediante la relación R escribimos xRy.

Veamos algunas de las propiedades que *puede* verificar una relación.

Propiedad reflexiva. Decimos que la relación R verifica la propiedad reflexiva si para cada elemento $x \in X$ se verifica xRx.

$$\text{Para todo } x \in X,\ xRx.$$

Propiedad simétrica. Decimos que R verifica la propiedad simétrica si cuando para dos elementos $x, y \in X$ se verifica xRy, entonces también se tiene yRx.

$$\text{Para todos } x, y \in X,\ \text{si } xRy,\ \text{entonces } yRx.$$

Propiedad transitiva. Decimos que R verifica la propiedad transitiva si cuando para tres elementos $x, y, z \in X$ se verifica xRy e yRz, entonces también se verifica xRz.

$$\text{Para todos } x, y, z \in X,\ \text{si } xRy \text{ e } yRz,\ \text{entonces } xRz.$$

Propiedad antisimétrica. Decimos que R verifica la propiedad antisimétrica si cuando para dos elementos $x, y \in X$ se verifica xRy e yRx, entonces se verifica $x = y$.

$$\text{Para todos } x, y \in X,\ \text{si } xRy \text{ e } yRx,\ \text{entonces } x = y.$$

Vamos a poner ejemplos de relaciones que verifican algunas de estas propiedades.

Ejemplo. 4.1.
Consideramos el conjunto $\mathbb{N}$ de los números naturales y definimos aRb si existe $c \in \mathbb{N}$ tal que $a = b + 2c$ ó $b = a + 2c$. Entonces R verifica las propiedades reflexiva, simétrica y transitiva.

Ejemplo. 4.2.
Consideramos el conjunto $\mathbb{Z}$ de los números enteros y definimos aRb si $a - b$ es un múltiplo de 2, (existe $c \in \mathbb{Z}$ tal que $a - b = 2c$). Entonces R verifica las propiedades reflexiva, simétrica y transitiva.

Ejemplo. 4.3.
Consideramos el conjunto $\mathbb{N}$ de los números naturales y definimos la relación $a \mid b$ si existe $c \in \mathbb{N}$ tal que $b = ac$. Entonces $\mid$ verifica las propiedades reflexiva, antisimétrica y transitiva.

Ejemplo. 4.4.
Consideramos el conjunto $\mathbb{Z}$ de los números enteros y definimos la relación $a \mid b$ si existe $c \in \mathbb{Z}$ tal que $b = ac$. Entonces $\mid$ verifica las propiedades reflexiva y transitiva, y *no verifica la propiedad antisimétrica*.

1101-04.tex

Si R es una relación en un conjunto X, podemos considerar el **grafo** de R como el subconjunto

$$Gr(R) = \{(x, y) \in X \times X \mid \ xRy\}.$$

Está claro que definir una relación en un conjunto X es lo mismo que dar su grafo, esto es, un subconjunto de $X \times X$.

El uso de grafos permite hacer algunas construcciones sobre relaciones de forma fácil.

Observar los siguientes hechos para un conjunto X y los grafos de relaciones sobre X:

(I) Llamamos D a la diagonal de $X \times X$.

(II) Dada una relación R, definimos una nueva relación R^{sim} mediante

$$Gr(R^{sim}) = \{(a, b) \in X \times X \mid \ (b, a) \in Gr(R)\}.$$

(III) Dadas dos relaciones R_1 y R_2 en un conjunto X, definimos una nueva relación $R_1 \circ R_2$ en X mediante:

$$(a, b) \in R_1 \circ R_2 \text{ si existe } c \in X \text{ tal que } (a, c) \in R_1 \text{ y } (c, b) \in R_2.$$

Podemos caracterizar las propiedades de relaciones en términos de grafos como:

(1) Una relación R es *reflexiva* si, y solo si, $D \subseteq Gr(R)$.

(2) Una relación R es *simétrica* si, y solo si, $R = R^{sim}$, esto es, si $Gr(R)$ es simétrico respecto a la diagonal.

(3) Una relación R es *antisimétrica* si, y sólo si, $R \cap R^{sim} \subseteq D$.

(4) Una relación R es *transitiva* si, y sólo si, $R \circ R \subseteq R$.

Relación de equivalencia

Decimos que una relación R que verifica las propiedades reflexiva, simétrica y transitiva es una **relación de equivalencia**.

Si R es una relación de equivalencia en un conjunto X, para cada elemento $a \in X$ definimos la **clase de equivalencia** de a como el subconjunto

$$\overline{a} = [a] = \{x \in X \mid \ aRx\}.$$

Lema. 4.5.
Si $a,\ b \in X$, entonces se verifica $\overline{a} = \overline{b}$ ó $\overline{a} \cap \overline{b} = \emptyset$, esto es, cada dos clases de equivalencia ó son iguales ó son disjuntas.

Si R es una relación de equivalencia en un conjunto X, el conjunto de todas las clases de equivalencia para la relación R se llama el **conjunto cociente** de X por R, y se representa por X/R.

Ejercicio. 4.6.
En el conjunto $\mathbb{R}\times\mathbb{R}$ *se considera la relación*

$$(a_1,a_2)R(b_1,b_2) \text{ si } a_1^2+a_2^2=b_1^2+b_2^2.$$

Probar que R *es una relación de equivalencia en* $\mathbb{R}\times\mathbb{R}$ *y describir el conjunto cociente.*

Si R es una relación de equivalencia en un conjunto X y X/R es el conjunto cociente, existe una aplicación sobreyectiva $p : X \longrightarrow X/R$ que a cada elemento $x \in X$ le asocia su clase de equivalencia $p(x) = \overline{x}$. Llamamos a p la **proyección** de X sobre X/R.

Relación de orden

Decimos que una relación R que verifica las propiedades reflexiva, antisimétrica y transitiva es una **relación de orden**.
Un conjunto X junto con una relación de orden se llama un **conjunto parcialmente ordenado**.
Si Y es un subconjunto de un conjunto parcialmente ordenado X con relación orden R, llamamos:

- **elemento maximal** de Y a un elemento $m \in Y$ tal que no existe ningún elemento $y \in Y$ tal que mRy.
- **cota superior** de Y en X a un elemento $c \in X$ tal que yRc para cada elemento $y \in Y$.
- **elemento máximo** de Y a un elemento $m \in Y$ tal que yRm para cada elemento $y \in Y$. Esto es, un máximo de Y es una cota superior de Y en X que pertenece a Y.

Ejercicio. 4.7.
Demostrar que en un conjunto parcialmente ordenado el elemento máximo de un subconjunto, si existe, es único.

SOLUCIÓN. Sea Y un subconjunto de un conjunto X con una relación de orden R, y supongamos que Y tiene dos elementos máximos m_1 y m_2. Por ser m_1 un máximo de Y y ser $m_2 \in Y$ se verifica m_2Rm_1.
Por análogos motivos se verifica m_1Rm_2.
Entonces como R verifica la propiedad antisimétrica, se verifica $m_1 = m_2$ y el máximo de Y es único.
□

También existen las nociones duales, esto es, las nociones de **elemento minimal**, de **cota inferior** y de **elemento mínimo** ó **primer elemento**.

Finalmente, un elemento $s \in X$ se dice que es un **supremo** de Y si es un mínimo del conjunto de las cotas superiores de Y. El concepto dual es el de **ínfimo**.

Ejercicio. 4.8.
Escribir las nociones aquí mencionadas para una relación de orden en X representada por el símbolo $\leq$ en vez del símbolo R.

Ejercicio. 4.9. (Orden lexicográfico)
Se considera $\mathbb{N} \times \mathbb{N}$, y en él la relación:

$$(a, b) \leq (c, d), \text{ si } a < c \text{ ó } a = c \text{ y } b \leq d.$$

Demuestra que esta relación es una relación de orden en $\mathbb{N} \times \mathbb{N}$, y que para dos elementos $(a_1, a_2), (b_1, b_2) \in \mathbb{N} \times \mathbb{N}$ se tiene $(a_1, a_2) \leq (b_1, b_2)$ ó $(b_1, b_2) \leq (a_1, a_2)$.
En este caso decimos que $\leq$ es una relación de orden total en $\mathbb{N} \times \mathbb{N}$.

Una relación de orden $\leq$ en un conjunto X es una **relación de orden total** si para cualesquiera elementos $x, y \in X$ se tiene $x \leq y$ ó $y \leq x$. Decimos entonces que $(X, \leq)$ es un **conjunto totalmente ordenado**.

Ejercicio. 4.10. (Orden producto)
Se considera $\mathbb{N} \times \mathbb{N}$, y en él la relación:

$$(a, b) \leq (c, d), \text{ si } a \leq c \text{ y } b \leq d.$$

Demuestra que ésta es una relación de orden en $\mathbb{N} \times \mathbb{N}$, y que, en general, no es una relación de orden total.

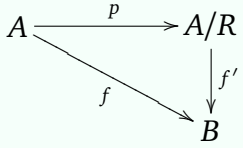
Observación. 4.11.
Es preciso destacar que las definiciones que hemos hecho de conjunto, aplicación entre conjuntos y relación en un conjunto carecen totalmente de rigurosidad. El objetivo hasta aquí ha sido señalar que, en este momento, nos interesa más el manejo de los conceptos que los conceptos en sí mismos.

De cualquier forma remitimos al alumno o alumnos interesados en profundizar en estos conceptos a los libros de la bibliografía para definiciones más rigurosas de las nociones aquí introducidas.

Ejercicios

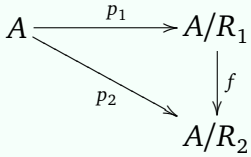
Relaciones de equivalencia

Ejercicio. 4.12. (Propiedad universal del conjunto cociente)
Sea R una relación de equivalencia en un conjunto A y $f : A \longrightarrow B$ una aplicación que verifica: si xRy, entonces $f(x) = f(y)$. Prueba que existe una única aplicación $f' : A/R \longrightarrow B$ tal que $f = pf'$, donde $p : A \longrightarrow A/R$ es la proyección canónica.



Ref.: 1101e_005 SOLUCIÓN.

Ejercicio. 4.13.
Sean R_1 y R_2 relaciones de equivalencia en un conjunto A; si $R_1 \subseteq R_2$, prueba que existe



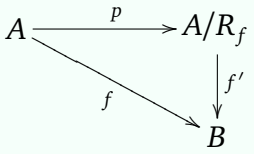
una única aplicación $f : A/R_1 \longrightarrow A/R_2$ tal que $p_2 = f p_1$, donde $p_i : X \longrightarrow A/R_i$, para $i = 1, 2$, son las proyecciones canónicas.
Ref.: 1101e_006 SOLUCIÓN.

Ejercicio. 4.14.
Sea $f : A \longrightarrow B$ una aplicación; definimos una relación R_f en A mediante:

$$xR_f y \text{ si } f(x) = f(y), \text{ para cualesquiera } x, y \in A.$$

(1) Prueba que R_f es una relación de equivalencia en A.

(2) *Prueba que existe una única aplicación* $f' : A/R_f \longrightarrow B$ *tal que* $f = pf'$, *donde* $p : A \longrightarrow A/R_f$ *es la proyección canónica.*



Ref.: 1101e_007 *SOLUCIÓN.*

Ejercicio. 4.15.
Determina una relación de equivalencia R *en* $\mathbb{N}$ *que tenga asociada la partición:*

$$\{\{0\},\{1,2\},\{3,4,5\},\{6,7,8,9\},\{10,11,12,13,14\},\ldots\}.$$

Ref.: 1101e_008 *SOLUCIÓN.*

Ejercicio. 4.16.
Si R *y* S *son relaciones en un conjunto* X, *decimos que* S *es menor que* R, *o que* R *es mayor que* S, *si* $S \subseteq R$.

Sea R *una relación en un conjunto* X *que verifica la propiedad transitiva.*

(1) *Prueba que existe una relación de equivalencia* S *que es la mayor entre las relaciones de equivalencia menores que* R.
(2) *Prueba que existe una relación de equivalencia* T *que es la menor entre las relaciones de equivalencia mayores que* R.

Ref.: 1101e_012 *SOLUCIÓN.*

Ejercicio. 4.17.
En el cuerpo $\mathbb{Q}$ *de los números racionales se define la relación* R *mediante:*

$$xRy \text{ si existe un entero } h \in \mathbb{Z} \text{ tal que } x = \frac{3y+h}{3}.$$

(1) Prueba que R es una relación de equivalencia en $\mathbb{Q}$.
(2) Determina el conjunto cociente $\mathbb{Q}/R$.
(3) Estudia si los elementos $\frac{2}{3}$ y $\frac{4}{5}$ pertenecen a la misma clase de equivalencia.

Ref.: 1101e_015 *SOLUCIÓN.*

Relaciones de orden

Ejercicio. 4.18.
Prueba que si A es un subconjunto no vacío de un conjunto parcialmente ordenado X que contiene una cota superior, entonces A tiene máximo.
Ref.: 1101e_009 *SOLUCIÓN.*

Ejercicio. 4.19.
Da un ejemplo de un conjunto parcialmente ordenado que contiene un subconjunto con al menos dos elementos maximales y una única cota superior.
Ref.: 1101e_010 *SOLUCIÓN.*

5. Cuantificadores

Sea $\mathbb{R}$ el conjunto de los números reales. Para cada número natural n definimos un subconjunto C_n de $\mathbb{R}$ mediante

$$C_n = [0, n) = \{r \in \mathbb{R} \mid \ 0 \leq r < n\} = [0, n).$$

El menor subconjunto de $\mathbb{R}$ que contiene a todos los C_n es exactamente $[0, \infty)$.

Podemos hablar entonces de la unión de todos los subconjuntos C_n, para n un número natural, y representamos esta unión como

$$\cup\{C_n \mid \ n \in \mathbb{N}\} \quad \text{ó} \quad \cup_{n\in\mathbb{N}} C_n.$$

Si consideramos ahora un conjunto X y subconjuntos X_n de X, entonces también podemos definir la unión de los subconjuntos X_n; ésta será:

$$\cup\{X_n \mid \ n \in \mathbb{N}\} \quad \text{ó} \quad \cup_{n\in\mathbb{N}} X_n,$$

y sus elementos son:

$$\{x \in X \mid \ \text{existe un } n \in \mathbb{N} \text{ tal que } x \in X_n\}.$$

Aquí hemos utilizado como conjunto de índices el conjunto $\mathbb{N}$, pero esto no es imprescindible y podríamos haber utilizado otro conjunto, supongamos que I, con elementos i. Tendremos entonces

$$\cup\{X_i \mid \ i \in I\} = \cup_{i\in I} X_i = \{x \in X \mid \ \text{existe un } i \in I \text{ tal que } x \in X_i\}.$$

La intersección de los subconjuntos X_i se define entonces como

$$\cap\{X_i \mid \ i \in I\} = \cap_{i\in I} X_i = \{x \in X \mid \ \text{para cada } i \in I \text{ se tiene } x \in X_i\}.$$

En todo este proceso nos aparecen dos cuantificadores, el **cuantificador existencial**, usado en la definición de unión, y el **cuantificador universal**, usado en la intersección. Vamos a representar por $\exists$ el cuantificador existencial y por $\forall$ el cuantificador universal.

Escribimos entonces

$$\cup\{X_i \mid \ i \in I\} = \{x \in X \mid \ \exists i \in I, \ x \in X_i\}.$$

y

$$\cap\{X_i \mid \ i \in I\} = \{x \in X \mid \ \forall i \in I, \ x \in X_i\}.$$

Las afirmaciones que tienen una variable en vez de proposiciones las vamos a llamar **funciones proposicionales**, de forma que si $\mathbf{A}(x)$ es una función proposicional, para cada valor a del argumento x tenemos que $\mathbf{A}(a)$ es una proposición.

En el ejemplo anterior $x \in X_i$ es una *función proposicional* con variable i. *Los cuantificadores actúan pues sobre las variables de las funciones proposicionales*.

1101-05.tex

Ejemplo. 5.1.

(I) Se considera la función proposicional $P(X)$ definida por: "X es mayor que 2".

(II) Se consideran el cuantificador $\exists$ y la proposición:

$$\exists x \in C,\ P(x).$$

Esta proposición se lee: *existe x en C tal que $P(x)$ es cierta*, esto es, "existe un elemento x en C tal que x es mayor que 2". Es cierta si C es, por ejemplo, el conjunto $\{0,1,2,3\}$ y falsa si C es el conjunto $\{-1,0,1,2\}$.

(III) Si se considera el cuantificador $\forall$ y la proposición:

$$\forall x \in C,\ P(x).$$

Esta proposición se lee: *para todo x en C se tiene que $P(x)$ es cierta*, esto es, "para todo elemento x en C se tiene que x es mayor que 2". Es cierta si C es por ejemplo el conjunto $\{3,4,5\}$ y es falsa si C es el conjunto $\{0,1,2,3\}$.

Relación de equivalencia y partición de un conjunto

Una **partición de un conjunto** X es un conjunto de subconjuntos de X, disjuntos dos a dos, cuya unión es X.

Si R es una relación de equivalencia en un conjunto X, entonces el conjunto de las clases de equivalencia, para la relación de equivalencia R, forma una partición de X; *la llamamos la partición definida por la relación R.*

El resultado recíproco también es cierto, esto es, para cualquier partición $\{X_i \mid i \in I\}$ de un conjunto X, existe una relación de equivalencia R en X de forma que la partición definida por R coincide con la partición $\{X_i \mid i \in I\}$.

En efecto, basta definir R como sigue: *"si x e y son elementos de X entonces xRy si x e y pertenecen a un mismo subconjunto X_i"*.

Lema. 5.2.
La relación R, así definida, es una relación de equivalencia.

DEMOSTRACIÓN. (1). Propiedad reflexiva. Para cada $x \in X$, ya que la unión de los subconjuntos X_i es X, existe un índice $i \in I$ tal que $x \in X_i$, luego xRx.

$$\forall x \in X,\ xRx$$

(2). Propiedad simétrica. Para cualesquiera x, $y \in X$, si xRy, entonces existe un índice $i \in I$ tal que $x, y \in X$, pero es claro que también se verifica $y, x \in X_i$, ya que el orden de los elementos x e y es irrelevante, entonces yRx.

$$\forall x \in X, \forall y \in X,\ xRy \implies yRx$$

(3). Propiedad transitiva. Para cualesquiera x, y, $z \in X$, si xRy e yRz, entonces existen índices $i, j \in I$ tales que $x, y \in X_i$ e $y, z \in X_j$. Como $X_i = X_j$ ó $X_i \cap X_j = \varnothing$ y se verifica $y \in X_i \cap X_j$, resulta $X_i = X_j$, luego $x, z \in X_i$ y tenemos xRz.

$$\forall x \in X, \forall y \in X, \forall z \in X,\ xRy \text{ e } yRz \implies xRz$$

□

Ejercicio. 5.3.
Se considera el conjunto $N = \{1, 2\}$. *Determinar una relación de equivalencia que define la partición* $\{\{1\}, \{2\}\}$.

Ejercicio. 5.4.
Obtener la partición dada por la relación de equivalencia del Ejemplo (4.1.).

Ejercicio. 5.5.
Dar una relación de equivalencia en $\mathbb{N} \setminus \{0\}$ *que da la siguiente partición:*

$$\{1, \ldots, 9\}, \{10, 11, \ldots, 99\}, \{100, 101, \ldots, 999\}, \ldots$$

Queremos hacer un comentario sobre las notaciones anteriores. Como ya hemos señalado, el símbolo $\implies$ indica que la afirmación tras el símbolo es cierta cuando lo es la afirmación que aparece antes de él. En la página 38 aparece $xRy \Rightarrow yRx$, esto es, *si se verifica* xRy, *entonces se verifica* yRx. Una forma alternativa de leerlo es la siguiente: xRy *implica* yRx.
Aquí vamos a usarlo, en combinación con los cuantificadores en múltiples contextos.
Veamos un ejemplo. Consideramos el conjunto $A = \{1, 2, a, b, c\}$ y los subconjuntos $B = \{1, 2\}$ y $B_1 = \{1, 2, a\}$. Como B es un subconjunto de B_1 se tiene:

$$\forall x \in A,\ x \in B \implies x \in B_1$$

Si quisiéramos expresar que B_1 no es un subconjunto de B tendríamos que escribir:

$$\exists x \in A,\ x \in B_1 \text{ y } x \notin B$$

En efecto esta segunda expresión es la negación de la primera, ya que $\mathbf{A} \Longrightarrow \mathbf{B}$ está definido como $(\neg\mathbf{A}) \vee \mathbf{B}$. En forma simbólica se escriben

$$\forall x \in A,\ \mathbf{A}(x) \Longrightarrow \mathbf{B}(x)$$

o equivalentemente

$$\forall x \in A,\ (\neg\mathbf{A}(x)) \vee \mathbf{B}(x)$$

y su negación, que sería:

$$\exists x \in A,\ \mathbf{A}(x) \wedge (\neg\mathbf{B}(x)) = \neg((\neg\mathbf{A}(x)) \vee \mathbf{B}(x)).$$

Ejercicios

Cuantificadores

Ejercicio. 5.6.
Expresa en términos de cuantificadores las siguientes afirmaciones:

(1) Para todo número real positivo existe una raíz cuadrada.
(2) Existe un número real que tiene una raíz cuadrada.
(3) Existe un número real que no tiene raíz cuadrada.
(4) Para todo número real existe un número entero que es el mayor entre los que son menores.
(5) Existe un número entero que es menor que todos los números reales positivos.
(6) No existe un número entero que es menor que todos los números reales.

Escribe, en términos de cuantificadores, la negación de cada una de las afirmaciones anteriores.
Ref.: 1101e_013 *SOLUCIÓN.*

6. Métodos de demostración

A continuación vamos a ver cómo hacer demostraciones de algunos resultados en Matemáticas. Aunque ya hemos hecho alguna en lo que llevamos expuesto, se trata aquí de hacer un pequeño resumen de estos métodos.

Método directo

Consiste en probar $\mathbf{A} \Longrightarrow \mathbf{B}$ directamente, haciendo uso de las definiciones y resultados previos.
Hasta ahora las demostraciones que hemos hecho son todas directas. Pero existen otros métodos de hacer demostraciones que vamos a detallar.

Método contra-recíproco

Consiste en probar $\mathbf{A} \Longrightarrow \mathbf{B}$ mediante una demostración directa de la proposición equivalente, esto es, $(\neg\mathbf{B}) \Longrightarrow (\neg\mathbf{A})$

Método de reducción al absurdo

Consiste en probar $\mathbf{A} \Longrightarrow \mathbf{B}$ mediante una demostración directa de una de las siguientes proposiciones:

$$\mathbf{A} \wedge (\neg\mathbf{B}) \Longrightarrow \neg\mathbf{A} \quad \text{ó}$$

$$\mathbf{A} \wedge (\neg\mathbf{B}) \Longrightarrow \mathbf{B}.$$

La siguiente es una demostración por reducción al absurdo utilizando el siguiente argumento: "*Si de una afirmación (A) se deduce una afirmación (B), que es falsa, entonces la afirmación (A) es falsa*".
(Nota. Observar la tabla de verdad de $\Rightarrow$.)

Teorema. 6.1. (Teorema de Euclides)
Existen infinitos números naturales primos.

DEMOSTRACIÓN. Supongamos que no es cierto el enunciado del Teorema, entonces hay únicamente un número finito de números naturales primos, sean estos $p_1, \ldots, p_t$. El número $q = p_1 \cdots p_t + 1$ da de resto 1 al dividirlo por todos los primos conocidos. Tenemos pues un número distinto de 0 y 1 que no es un producto de números primos, lo que es una contradicción.

Afirmación (**A**): *no es cierto el enunciado del Teorema*.

1101-06.tex

Afirmación (**B**): *existe un número natural distinto de 0 y 1 que no es un producto de números primos*.

Hemos probado que $\mathbf{A} \Rightarrow \mathbf{B}$, o equivalentemente $(\neg\mathbf{B}) \Rightarrow (\neg\mathbf{A})$. Y como sabemos que siempre se verifica $\neg\mathbf{B}$, tenemos por tanto que se verifica $\neg\mathbf{A}$, que era lo que queríamos. □

Otro ejemplo de demostración por reducción al absurdo se obtiene al probar el siguiente resultado:

Ejercicio. 6.2.
Demostrar que $\sqrt{2}$ no es un número racional.

Enunciados de teoremas

Teorema directo: $\mathbf{A} \implies \mathbf{B}$

Teorema contrario: $(\neg\mathbf{A}) \implies (\neg\mathbf{B})$

Teorema recíproco: $\mathbf{B} \implies \mathbf{A}$

Teorema contra-recíproco: $(\neg\mathbf{B}) \implies (\neg\mathbf{A})$

Son equivalentes

el teorema directo y el contra-recíproco

y también son equivalentes, entre sí

el teorema contrario y el recíproco.

Veamos un ejemplo.

Vamos a suponer que X e Y son conjuntos finitos y que $f : X \longrightarrow Y$ es una aplicación.

Enunciado directo:

Lema. 6.3.
Si f es inyectiva, entonces $\mathscr{C}ard(X) \leq \mathscr{C}ard(Y)$.

El enunciado contra-recíproco, y equivalente, de este Lema es el siguiente:

Lema. 6.4. (Principio del palomar)
Si $\mathscr{C}ard(Y) < \mathscr{C}ard(X)$, entonces f no es inyectiva.

Es claro que los enunciados son equivalentes:
Vamos a llamar **A** a la afirmación *"f es inyectiva"* y **B** a la afirmación *"$\mathscr{C}ard(X) \leq \mathscr{C}ard(Y)$"*. Entonces el Lema (6.3.) se escribe

$$\mathbf{A} \Longrightarrow \mathbf{B}$$

y el Lema (6.4.) se escribe

$$(\neg\mathbf{B}) \Longrightarrow (\neg\mathbf{A}).$$

Ejercicios

Métodos de demostración

Ejercicio. 6.5.
Prueba que todo entero positivo distinto de 1 se escribe de forma única, salvo el orden, como un producto de enteros primos positivos.
Ref.: 1101e_011 *SOLUCIÓN.*

Ejercicio. 6.6.
Si X es un conjunto totalmente ordenado: ¿Necesariamente tiene X un ínfimo?, ¿necesariamente tiene X un mínimo?
Estudia también el caso en el que X tiene una cota inferior.
Ref.: 1101e_014 *SOLUCIÓN.*

Capítulo II

Números naturales y enteros

Introducción

Los *números naturales*: 0, 1, 2, . . . , son la base de la Aritmética y de la Teoría de Conjuntos. No damos una introducción axiomática a los mismos, sino que, de forma intuitiva, hacemos una aproximación a los números naturales, dando una lista exhaustiva de las propiedades que de ellos mismos vamos a necesitar.

Tras estudiar los números naturales, y las operaciones suma y producto, construimos los *números enteros* con objeto de poder trabajar en un grupo abeliano, al considerar la suma, o en un anillo, al considerar conjuntamente las operaciones suma y producto. Haciendo uso de la división, y la divisibilidad, estudiaremos en detalle las propiedades elementales de los números enteros: Teorema Fundamental de la Aritmética, Teorema de Euclides sobre existencia de infinitos enteros primos, algoritmo de Euclides para el cálculo del máximo común divisor, etc.

El capítulo finaliza estudiando la aritmética modular: un ejemplo de anillo cociente; dando de esta forma una lista exhaustiva de los grupos abelianos cíclicos y, por otro lado, ejemplos de cuerpos finitos, al considerar los enteros módulo un entero primo.

7. Números naturales

Suponemos que el alumno conoce el conjunto $\mathbb{N}$ de los **números naturales** y que en él hay definidas dos operaciones (binarias): suma, representada por el signo "+", y producto, representada por el signo "·", o simplemente por la yuxtaposición de elementos. Estas operaciones verifican las siguientes propiedades.
La suma:

(I) **Propiedad asociativa**. $a+(b+c)=(a+b)+c$, para todos $a,b,c\in\mathbb{N}$.

(II) **Propiedad conmutativa**. $a+b=b+a$, para todos $a,b\in\mathbb{N}$.

(III) **Existencia de elemento neutro**. Existe un elemento $0\in\mathbb{N}$ tal que para todo $a\in\mathbb{N}$ tenemos $0+a=a$.

El producto:

(I) **Propiedad asociativa**. $a(bc)=(ab)c$, para todos $a,b,c\in\mathbb{N}$.

(II) **Propiedad conmutativa**. $ab=ba$, para todos $a,b\in\mathbb{N}$.

(III) **Existencia de elemento neutro**. Existe un elemento $1\in\mathbb{N}$ tal que para todo $a\in\mathbb{N}$ tenemos $1a=a$.

(IV) **Propiedad distributiva del producto respecto a la suma**. $a(b+c)=ab+ac$, para todos $a,b,c\in\mathbb{N}$.

Con estas propiedades podemos manejar los números naturales y obtener gran parte de sus propiedades. Existe además otro concepto fundamental en el conjunto $\mathbb{N}$: podemos definir en $\mathbb{N}$ una relación de orden, en la forma obvia,

$$a\leq b \text{ si existe } x\in\mathbb{N} \text{ tal que } a+x=b,$$

y para esta relación el conjunto $\mathbb{N}$ es **bien ordenado**, esto es: cualquier subconjunto no vacío $X\subseteq\mathbb{N}$ tiene un primer elemento (un mínimo).
Resulta entonces:

- que los números naturales están ordenados en una sucesión $0,1,2,3,\ldots$
- que para cada número natural n hay un **siguiente** $n+1$,
- que cada número natural n, distinto de 0, tiene un **anterior**, esto es; existe $m\in\mathbb{N}$ tal que $n=m+1$,

1102-01.tex

- etc.

Como consecuencia de estas ideas intuitivas podemos enunciar y demostrar el primer resultado de nuestra teoría, el Principio de inducción.

Lema. 7.1. (Primer Principio de inducción)
Sea $X \subseteq \mathbb{N}$ un subconjunto de números naturales verificando las dos propiedades siguientes:
(1) $0 \in X$,
(2) si x es un número natural tal que $x \in X$, entonces $x+1 \in X$,

entonces $X = \mathbb{N}$.

DEMOSTRACIÓN. Consideremos el subconjunto $Y = \mathbb{N} \setminus X$. Si $Y \neq \emptyset$, existe un primer elemento, llamémoslo y; como $y \neq 0$, existe $z \in \mathbb{N}$ tal que $z+1 = y$. Es claro que $z \notin Y$, entonces $z \in X$, y aplicando la hipótesis (2) obtenemos $y = z+1 \in X$; lo que es una contradicción. Como consecuencia $Y = \emptyset$ y por tanto $X = \mathbb{N}$. □

Existe un Segundo Principio de inducción que es una consecuencia directa del Primero, y cuya demostración dejamos al alumno.

Lema. 7.2. (Segundo Principio de inducción)
Sea $X \subseteq \mathbb{N}$ un subconjunto verificando las dos siguientes propiedades:
(1) $0 \in X$,
(2) si x es un número natural, distinto de 0, tal que $y \in X$ para todos los números naturales y anteriores a x, entonces $x \in X$,

entonces $X = \mathbb{N}$.

Ejercicios

Números naturales

Ejercicio. 7.3.
Sea n un número natural, demuestra por inducción los siguientes resultados:

(1) $1+2+\cdots+n=\frac{n(n+1)}{2}$.

(2) $1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$.

(3) $1^3+2^3+\cdots+n^3=\left(\frac{n(n+1)}{2}\right)^2$.

(4) $(1^5+2^5+\cdots+n^5)+(1^7+2^7+\cdots+n^7)=2\left(\frac{n(n+1)}{2}\right)^4$.

(5) $1+3+\cdots+(2n-1)=n^2$.

Ref.: 1102e_001 *SOLUCIÓN.*

Ejercicio. 7.4.
Sean a,b,n números naturales, demuestra por inducción el siguiente resultado.

$$(a+b)^n=\sum_{i=0}^{n}\binom{i}{n}a^i b^{n-i}.$$

Ref.: 1102e_002 *SOLUCIÓN.*

Ejercicio. 7.5.
Comprueba que si $n=0,1,2,\ldots,40$, entonces n^2-n+41 es un número primo, y que si $n=41$, evidentemente no lo es. Este ejercicio nos advierte sobre el Principio de inducción: el que un resultado sea cierto para los primeros números naturales no significa que sea cierto para todos los números naturales.
Ref.: 1102e_002 *SOLUCIÓN.*

Ejercicio. 7.6.
Sea $c \geq 1$ un número real y sea n un número natural. Demuestra que se verifica $(1+c)^n \geq 1+nc$.
Ref.: 1102e_004 SOLUCIÓN.

Ejercicio. 7.7.
Demuestra que para todo número natural n mayor ó igual que 4 se verifica $2^n < n!$
Ref.: 1102e_005 SOLUCIÓN.

Ejercicio. 7.8.
Demuestra que para todo número natural n mayor ó igual que 3 se verifica $2^n - 1 \geq 2n+1$.
Ref.: 1102e_006 SOLUCIÓN.

Ejercicio. 7.9.
Se define $S(k,n) = 1^k + 2^k + \cdots + n^k = \sum_{i=1}^{n} i^k$, para $n, k \in \mathbb{N}$.
(1) Prueba que se verifica $(n+1)^{k+1} - (n+1) = \binom{k+1}{k} S(k,n) + \cdots + \binom{k+1}{1} S(1,n)$.
(2) Calcula $S(k,n)$ para $k = 1, 2, 3, 4, \ldots$

Ref.: 1102e_007 SOLUCIÓN.

Ejercicio. 7.10.
Calcular el valor de $S = 1^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2$.
Ref.: 1102e_008 SOLUCIÓN.

8. Números enteros

Al igual que en el caso de $\mathbb{N}$, suponemos que el alumno conoce el conjunto $\mathbb{Z}$ de los **números enteros**, y que en él hay definidas dos operaciones: suma y producto, que verifican las siguientes propiedades.

La suma:

(I) **Propiedad asociativa**. $a+(b+c)=(a+b)+c$, para todos $a,b,c\in\mathbb{Z}$.
(II) **Propiedad conmutativa**. $a+b=b+a$, para todos $a,b\in\mathbb{Z}$.
(III) **Existencia de elemento neutro**. Existe un elemento $0\in\mathbb{Z}$ tal que para todo $a\in\mathbb{Z}$ tenemos $0+a=a$.
(IV) **Existencia de elemento opuesto**. Dado $a\in\mathbb{Z}$ existe $b\in\mathbb{Z}$ tal que $a+b=0$.

El producto:

(I) **Propiedad asociativa**. $a(bc)=(ab)c$, para todos $a,b,c\in\mathbb{Z}$.
(II) **Propiedad conmutativa**. $ab=ba$, para todos $a,b\in\mathbb{Z}$.
(III) **Existencia de elemento neutro**. Existe un elemento $1\in\mathbb{Z}$ tal que para todo $a\in\mathbb{Z}$ tenemos $1a=a$.
(IV) **Propiedad distributiva del producto respecto a la suma**. $a(b+c)=ab+ac$, para todos $a,b,c\in\mathbb{Z}$.

Estas operaciones nos permiten estudiar la aritmética de $\mathbb{Z}$ de forma fácil, más adelante haremos un estudio similar en el caso de un anillo (conmutativo).

El primer hecho a tener en cuenta es que $\mathbb{Z}$ verifica la siguiente propiedad: si $n,m\in\mathbb{Z}$ verifican $nm=0$, entonces $n=0$ ó $m=0$, esto es; $\mathbb{Z}$ es un **dominio de integridad**.

Sean $d,n\in\mathbb{Z}$ números enteros, decimos que d es un **divisor** de n, ó que n es un **múltiplo** de d, si existe otro número entero m tal que $n=dm$. Si d es un divisor de n escribiremos $d\mid n$, y si no lo es, entonces escribimos $d\nmid n$.

Los números enteros divisores de 1 se llaman elementos invertibles: los **elementos invertibles** en $\mathbb{Z}$ son 1 y -1.

Cada número entero no nulo y no invertible n tiene siempre cuatro divisores distintos; estos son: 1, -1, n y $-n$; a n y $-n$ los llamaremos **divisores impropios** de n, y a los restantes, que no son invertibles, los llamaremos **divisores propios** de n.

Dos números enteros n,m se llaman **asociados** si $n\mid m$ y $m\mid n$, es fácil demostrar que n y m son asociados si, y solo si, $n=\pm m$; esto es, se diferencian al multiplicar por un elemento invertible.

El uso de los divisores nos permite definir números enteros especiales: los números primos. Un número entero, distinto de 0, 1 y -1, es **primo** si no tiene divisores propios. Es claro que si p es un número entero primo, entonces $-p$ también lo es, y por tanto, dado un número primo siempre existe un número entero primo positivo asociado a él, que puede diferenciarse de él en el signo. Los números primos nos permiten dar una expresión sencilla y manejable (en algunos casos) de los números enteros.

1102-02.tex

Teorema. 8.1. (Teorema fundamental de la Aritmética)
Todo número entero n distinto de $0, 1$ y -1 se expresa de forma, esencialmente, única del siguiente modo:

$$n = \pm {p_1}^{e_1} \cdots {p_r}^{e_r},$$

donde $p_1 \leq \cdots \leq p_r$ son números enteros primos positivos y donde $e_1, \ldots, e_r$ y r son números enteros positivos.

Esta descomposición es interesante como más adelante veremos al estudiar el máximo común divisor y el mínimo común múltiplo. Antes de pasar a esto vamos a enunciar y demostrar un resultado clásico de la teoría de números en el que aplicaremos el Teorema Fundamental de la Aritmética.

Teorema. 8.2. (Teorema de Euclides)
Existe un número infinito de enteros primos.

DEMOSTRACIÓN. Supongamos que existan únicamente s enteros primos, $p_1, \ldots, p_s$, definimos $n = p_1 \cdots p_s + 1$. Entonces n es distinto de $0, 1$ y -1, y además no es divisible por ningún entero primo, lo que es una contradicción con el Teorema Fundamental de la Aritmética. □

Sean n y m números enteros positivos, definimos el **máximo común divisor**, mcd, de n y m como el mayor número entero positivo d que divide a n y m; es claro que d siempre existe, y que si n y m tienen las siguientes expresiones en función de números enteros primos positivos

$$n = p_1^{e_1} \cdots p_r^{e_r}, e_i > 0,$$

$$m = q_1^{f_1} \cdots q_s^{f_s}, f_j > 0,$$

entonces podemos obtener una expresión sencilla para d de la siguiente forma: primero extendemos las expresiones anteriores para que consten de los mismos factores primos, posiblemente con exponentes nulos, así obtenemos expresiones del tipo siguiente:

$$n = p_1^{e_1} \cdots p_t^{e_t},$$

$$m = p_1^{g_1} \cdots p_t^{g_t},$$

con $t \geq r$, $t \geq s$ y donde $e_i, g_i \geq 0$, entonces

$$d = p_1^{h_1} \cdots p_t^{h_t},$$

con $h_i = \min\{e_i, g_i\}$. De la misma forma se define el **mínimo común múltiplo**, mcm, M de n y m, como el menor número entero positivo múltiplo de n y m; siguiendo con las anteriores notaciones tenemos

$$M = p_1^{l_1} \cdots p_t^{l_t},$$

con $l_i = \max\{e_i, g_i\}$. Es un fácil ejercicio comprobar que se verifica la siguiente igualdad:

$$dM = nm,$$

como consecuencia calculado d ó M conocemos el otro.

Dos números enteros n y m se llaman **primos relativos** si $\text{mcd}\{n, m\} = 1$.

Vamos a determinar el mcd y el mcm de dos números enteros según sus propiedades de divisibilidad; resulta que el mcd, d, de n y m verifica la siguiente propiedad:

$$d \mid n,\ d \mid m,\ \text{y}$$

$$\text{si } x \text{ es otro número entero tal que } x \mid n \text{ y } x \mid m, \text{ entonces } x \mid d.$$

Es fácil ver que un número entero d que verifica la propiedad anterior es el mcd de n y m ó su opuesto, por lo tanto esta propiedad caracteriza al mcd. De forma análoga es sencillo comprobar que la siguiente propiedad caracteriza al mcm.

$$n \mid M,\ m \mid M,\ \text{y}$$

$$\text{si } x \text{ es otro número entero tal que } n \mid x \text{ y } m \mid x, \text{ entonces } M \mid x.$$

Existen otras formas de representar el mcd y el mcm (positivo ó nulo) de dos números enteros n y m, estas son (n, m) y $[n, m]$ respectivamente.

Recordemos rápidamente el Algoritmo de la división en $\mathbb{Z}$.

Teorema. 8.3. (Algoritmo de la división en $\mathbb{Z}$)
Dados dos números enteros a y b, con $b > 0$, existen dos únicos números enteros q y r verificando:
(1) $a = bq + r$,
(2) $0 \leq r < b$.

DEMOSTRACIÓN. Llamemos $S = \{a - bs \mid s \in \mathbb{Z}, a - bs \geq 0\}$, tenemos que S es no vacío ya que $a - b(-a^2) \geq 0$; entonces S tiene un primer elemento $r = a - bq$. Por hipótesis $r \geq 0$; si $r \geq b$, entonces $r = b + r'$, y despejando el valor de r' tenemos

$$r' = r - b = a - bq - b = a - b(q + 1) \in S,$$

y ya que $r' < r$, llegamos a una contradicción, luego $r < b$ y se tiene que el enunciado es cierto a falta de la unicidad. Supongamos que tenemos dos expresiones distintas

$$a = bq + r = bq' + r'$$

con $0 \leq r, r' < b$, entonces restando una de la otra tenemos la igualdad

$$0 = b(q - q') + (r - r'),$$

de donde deducimos que $r - r' = 0$, esto es que $r = r'$, y por tanto también $q = q'$. □

r se llama el **resto** y q el **cociente** de la división de a por b.

División por un entero arbitrario no nulo

Dados $n, m \in \mathbb{Z}$, con $m \neq 0$, vamos a probar que existen varios modos de dividir n por m, esto es, obtener una expresión del tipo $n = qm + r$, con $q, r \in \mathbb{Z}$ verificando ciertas propiedades. Según estas propiedades podremos obtener unicidad en esta expresión, tal y como ocurre en la división cuando m es un entero positivo. Vamos a estructurar estos modos de división a través de diferentes criterios de, cada uno con sus propiedades.

Criterio 1. El caso en el que m es un entero positivo no nulo. Dados $n, m \in \mathbb{Z}$, $m \geq 0$, existen $q, r \in \mathbb{Z}$, únicos verificando

(I) $n = qm + r$,
(II) $0 \leq r < m$.

Criterio 2. El caso en el que m es un entero arbitrario no nulo. Dados $n, m \in \mathbb{Z}$, $m \neq 0$, existen $q, r \in \mathbb{Z}$, únicos verificando

(I) $n = qm + r$,
(II) $0 \leq r < |\, m \,|$.

Criterio 3. El caso en el que m es un entero arbitrario no nulo, con el resto no necesariamente positivo. Dados $n, m \in \mathbb{Z}$, $m \neq 0$, existen $q, r \in \mathbb{Z}$, verificando

(I) $n = qm + r$,
(II) $|\, m \,| < r < |\, m \,|$.

En este caso no podemos afirmar la unicidad del resto; en general tenemos dos posibles valores, uno positivo y otro negativo.

Criterio 4. El caso en el que m es un entero arbitrario no nulo, con el resto único no necesariamente positivo. Dados $n, m \in \mathbb{Z}$, $m \neq 0$, existen $q, r \in \mathbb{Z}$, únicos verificando

(I) $n = qm + r$,
(II) $\begin{cases} \left\lfloor \dfrac{-|m|}{2} \right\rfloor < r \leq \left\lfloor \dfrac{|m|}{2} \right\rfloor, & \text{si } m \text{ es par,} \\ \left\lfloor \dfrac{-|m|}{2} \right\rfloor \leq r \leq \left\lfloor \dfrac{|m|}{2} \right\rfloor, & \text{si } m \text{ es impar.} \end{cases}$

Observa que en este caso el resto tiene el valor absoluto mínimo, de entre los posibles; eligiendo el positivo en caso de igualdad. La ventaja de esta división es que los posibles restos se toman en un conjunto más reducido de elemento, eso sí, afectados del signo, para tener en cada caso $\mid m \mid$ posibles restos.

Vamos a calcular el mcd de dos números enteros utilizando el Algoritmo de la división, pero antes veamos una propiedad interesante del mcd. Sean n y m números enteros (positivos), consideramos el conjunto

$$T = \{an + bm \mid \ a, b \in \mathbb{Z}\},$$

y hacemos $(T \cap \mathbb{N}) \setminus \{0\}$, este conjunto es no vacío ya que $n \in (T \cap \mathbb{N}) \setminus \{0\}$; existe por tanto un primer elemento d de $(T \cap \mathbb{N}) \setminus \{0\}$, supongamos $d = a_0 n + b_0 m$ con $a_0, b_0 \in \mathbb{Z}$. Vamos a demostrar que d es el mcd de n y m. Para ver que $d \mid n$ hacemos la división de n por d obteniendo $n = dq + r$ con $0 \leq r < d$, entonces

$$r = n - dq = n - (a_0 n + b_0 m)q = n(1 - a_0 q) - m b_0 q \in T \cap \mathbb{N},$$

lo que es una contradicción salvo que $r = 0$, y en este caso $d \mid n$. De igual forma se tiene $d \mid m$. Es sencillo comprobar que si x es otro número entero tal que $x \mid n$ y $x \mid m$, entonces también $x \mid d$, luego d es el mcd de n y m.

El resultado anterior se conoce como **Identidad de Bezout**, y se enuncia como sigue.

Lema. 8.4. (Identidad de Bezout)
Sean n y m números enteros (positivos) y sea d su mcd*, entonces existen números enteros a y b tales que $d = an + bm$.*

Algoritmo de Euclides para el cálculo del mcd

Una justificación de este algoritmo la veremos más adelante al estudiar los DE, baste por ahora hacer uso del mismo para habituarnos a la aritmética de $\mathbb{Z}$. Este algoritmo consiste en tomar los dos números n y m, ordenarlos de mayor a menor y hacer divisiones sucesivas de la siguiente forma:

(1) Dividimos n por m obteniendo un resto r_1.

$$n = mq_1 + r_1, \ 0 \leq r_1 < m.$$

Resulta que el mcd de n y m es el mismo que el de m y r_1. (Hacer como ejercicio).

(2) Dividimos m por r_1 obteniendo un resto r_2.

$$m = r_1 q_2 + r_2, \ 0 \leq r_2 < r_1.$$

Al igual que antes tenemos que el mcd de m y r_1 es igual al mcd de r_1 y r_2.

(3) Dividimos r_1 por r_2 obteniendo un resto r_3.

$$r_1 = r_2 q_3 + r_3,\ 0 \leq r_3 < r_2.$$

Al igual que antes tenemos que el mcd de r_1 y r_2 es igual al mcd de r_2 y r_3.

(4) Este proceso se repite hasta llegar a un resto igual a cero, resulta que el último resto no nulo es el mcd de n y m; además este proceso nos permite también obtener números enteros a y b que verifican la Identidad de Bezout.

Ejercicios

Números enteros

Ejercicio. 8.5.
Determina el número de soluciones en $\mathbb{N}$ *de la siguiente ecuación*

$$X + 2Y = n, \quad \text{con } n \in \mathbb{N}.$$

Ref.: 1102e_011 *SOLUCIÓN.*

Ejercicio. 8.6.
Calcula d*, el* mcd *de* 24230 *y* 586*, y encontrar números enteros* a *y* b *tales que* $d = 24230a + 586b$.
Ref.: 1102e_012 *SOLUCIÓN.*

Ejercicio. 8.7.
Hasta ahora hemos realizado la división por números enteros positivos y hemos estudiado el mcd *y el* mcm *para números enteros positivos, haz las definiciones necesarias para extender la teoría a todos los números enteros (no nulos).*
Ref.: 1102e_013 *SOLUCIÓN.*

Ejercicio. 8.8.
Aplica el Algoritmo de la división a los enteros 48 *y* -7.
Ref.: 1102e_014 *SOLUCIÓN.*

Ejercicio. 8.9.
Calcula el mcd *y la Identidad de Bezout de* 92 *y* 108.
Ref.: 1102e_015 *SOLUCIÓN.*

Con la definición de mcd y mcm dada por la relación de divisibilidad, resolver los siguientes ejercicios.

Ejercicio. 8.10.
Prueba que dados dos enteros primos relativos no nulos a y b se verifica $(a+b, ab) = 1 = (a-b, ab)$.
Ref.: 1102e_016 SOLUCIÓN.

Ejercicio. 8.11.
Prueba que si a, b, c son enteros y a es positivo, entonces $(ab, ac) = a(b, c)$.
Ref.: 1102e_017 SOLUCIÓN.

Ejercicio. 8.12.
Prueba que si a, b, c son enteros tales que $(a, c) = 1$ y $(b, c) = 1$, entonces $(ab, c) = 1$.
Ref.: 1102e_018 SOLUCIÓN.

Ejercicio. 8.13.
Sean a, b enteros y $d = (a, b)$, prueba que si $x \in \mathbb{Z}$ verifica $a \mid x$ y $b \mid x$, entonces $ab \mid dx$.
Ref.: 1102e_019 SOLUCIÓN.

Ejercicio. 8.14.
Sean a, b enteros no nulos y $d = (a, b)$, prueba que a/d y b/d son primos relativos.
Ref.: 1102e_020 SOLUCIÓN.

Ejercicio. 8.15.
Sean a, b, c enteros, prueba que $(a,(b,c)) = ((a,b),c)$.
Ref.: 1102e_021 *SOLUCIÓN.*

Un número entero p se llama **primo** si es distinto de $0, 1$ y -1, y no tiene factores propios, esto es; sus únicos factores son ± 1 y $\pm p$.

Ejercicio. 8.16.
Sea p un número entero distinto de 0, 1 y -1; demuestra que p es primo si, y sólo si, para cada par de números enteros a, b se tiene que si $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.
Ref.: 1102e_041 *SOLUCIÓN.*

Ejercicio. 8.17.
Sea n un número entero positivo, demuestra que $\binom{2n}{n}$ es divisible por cada número primo p tal que $n < p \leq 2n$.
Ref.: 1102e_042 *SOLUCIÓN.*

Ejercicio. 8.18.
Sean q, m, n números enteros, siendo n y m positivos, demuestra que

$$q-1 \mid q^n-1,$$

y deduce que si $m \mid n$, entonces

$$q^m-1 \mid q^n-1.$$

Ref.: 1102e_043 *SOLUCIÓN.*

Ejercicio. 8.19.
Sean q, m, n números enteros, siendo n y m positivos y $q \neq 1$, si $q^m - 1 \mid q^n - 1$, demuestra que $m \mid n$.
Ref.: 1102e_044 *SOLUCIÓN.*

Ejercicio. 8.20.
Vamos a estudiar en este ejercicio una primera división de los números enteros primos.

(1) Demostrar que todo número entero primo distinto de 2 es de la forma $4n+1$ ó de la forma $4n-1$.
(2) Demostrar que el producto de números enteros de la forma $4n+1$, $n \in \mathbb{Z}$, es otra vez de esta forma.
(3) Deducir que hay infinitos primos de la forma $4n-1$.

Ref.: 1102e_045 *SOLUCIÓN.*

Ejercicio. 8.21.
Si p es un número entero primo positivo, demuestra que para todo entero positivo n el número $n^p - n$ es divisible por p.
Ref.: 1102e_046 *SOLUCIÓN.*

9. Números enteros módulo m

Vamos a trabajar ahora módulo un entero (positivo) m, resulta que cualquier número entero n puede expresarse de forma única como $n = mq + r$, con $0 \leq r < m$, entonces diremos que n es **congruente con** r **módulo** m y lo representamos por $n \equiv r \pmod{m}$; para cada número entero $0 \leq r < m$, llamamos **clase de equivalencia** de r al conjunto

$$\overline{r} = \{n \in \mathbb{Z} \mid \ n \equiv r \pmod{m}\};$$

esto es, el conjunto de todos los números enteros que tienen resto r al hacer la división por m. Es claro que dos enteros s y t pertenecen a la misma clase de equivalencia si, y sólo si, su diferencia es un múltiplo de m.

Definimos $s \equiv t \pmod{m}$ si s y t están en la misma clase. Tenemos exactamente m clases de equivalencia distintas, estas son: $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. El conjunto formado por todas estas clases se representa por $\mathbb{Z}_m$.

Resulta que en $\mathbb{Z}_m$ es posible definir operaciones que lo dotan de estructura de anillo conmutativo, y en algunos casos de cuerpo. Vamos pues a estudiar cómo dotar de estructura a $\mathbb{Z}_m$. Para ello vamos a introducir algunos conceptos nuevos.

Sea X un conjunto, definimos una **relación** $\mathscr{R}$ en X como un subconjunto del conjunto producto $X \times X$, y diremos que el elemento $x \in X$ está **relacionado** con el elemento $y \in X$ si el par (x, y) pertenece a $\mathscr{R}$, esto se representa por:

$$x \mathscr{R} y \text{ si, y sólo si, } (x, y) \in \mathscr{R}.$$

De entre las propiedades que puede ó no verificar una relación destacamos las siguientes:

(I) **Propiedad reflexiva**. Para cada elemento $x \in X$ se tiene $x \mathscr{R} x$.

(II) **Propiedad simétrica**. Si para dos elementos $x, y \in X$ se verifica $x \mathscr{R} y$, entonces también se tiene $y \mathscr{R} x$.

(III) **Propiedad antisimétrica**. Si para dos elementos $x, y \in X$ se tiene $x \mathscr{R} y$ e $y \mathscr{R} x$, entonces se tiene $x = y$.

(IV) **Propiedad transitiva**. Si para tres elementos $x, y, z \in X$ se tiene $x \mathscr{R} y$ e $y \mathscr{R} z$, entonces se tiene $x \mathscr{R} z$.

Una relación $\mathscr{R}$ que verifique las propiedades reflexiva, simétrica y transitiva se llama una **relación de equivalencia**, y se llama una **relación de orden** si verifica las propiedades reflexiva, antisimétrica y transitiva.

Ejemplos. 9.1.

1. En el conjunto $\mathbb{N}$ de los números naturales la relación $\leq$ es una relación de orden, y también lo es en el conjunto $\mathbb{Z}$ de los números enteros.

2. En el conjunto $\mathbb{N}$ de los números naturales la relación $|$ es una relación de orden, sin embargo en el conjunto $\mathbb{Z}$ de los números enteros no lo es.

1102-03.tex

3. En el conjunto de los números enteros la relación "*... es asociado a ...*" es una relación de equivalencia.

4. En el conjunto de los números enteros la relación "*... es congruente con ... módulo m*" es una relación de equivalencia.

Si $\mathscr{R}$ es una relación de equivalencia en un conjunto X, dado un elemento $x \in X$ llamamos **clase de equivalencia** de x al conjunto

$$\overline{x} = \{y \in X \mid x \mathscr{R} y\},$$

Las clases de equivalencia verifican las siguientes propiedades:
(1) Para cada $x \in X$ tenemos $x \in \overline{x}$.
(2) Para $x, y \in X$ si $\overline{x} \cap \overline{y} \neq \emptyset$, entonces $\overline{x} = \overline{y}$.

DEMOSTRACIÓN. (1). Es claro ya que $x \mathscr{R} x$ para cada $x \in X$.
(2). Sea $w \in \overline{x}$ y supongamos que existe $z \in \overline{x} \cap \overline{y}$, entonces tenemos las siguientes relaciones entre estos elementos: $x \mathscr{R} w$, $x \mathscr{R} z$ e $y \mathscr{R} z$. Por las propiedades simétrica y transitiva tenemos que $z \mathscr{R} w$ y por la propiedad transitiva tenemos $y \mathscr{R} w$, luego $w \in \overline{y}$. La otra inclusión se prueba de forma análoga. □

Sea X un conjunto, una **partición de** X es una familia de subconjuntos $\{X_i \mid i \in I\}$ verificando las dos siguientes propiedades:
(I) $\cup\{X_i \mid i \in I\} = X$.
(II) $X_i \cap X_j = \emptyset$ para cada par de elementos distintos $i, j \in I$.

Al considerar las clases de equivalencia para una relación de equivalencia tenemos el siguiente resultado:

Teorema. 9.2.
Sea X un conjunto, dar una relación de equivalencia $\mathscr{R}$ en X es equivalente a dar una partición de X.

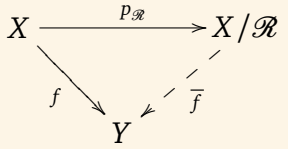
DEMOSTRACIÓN. Si $\mathscr{R}$ es una relación de equivalencia en X, entonces de la familia $\{\overline{x} \mid x \in X\}$ podemos extraer una partición dejando una clase y eliminando todas las clases iguales a ella. Por otro lado, si $\{X_i \mid i \in I\}$ es una partición definimos una relación $\mathscr{R}$ mediante

$$x \mathscr{R} y \text{ si } \exists i \in I, \text{ tal que } x, y \in X_i,$$

es claro que $\mathscr{R}$, así definida, es una relación de equivalencia, y que la partición dada por las clases de equivalencia es exactamente $\{X_i \mid i \in I\}$. □

Sea X un conjunto y $\mathscr{R}$ una relación de equivalencia en X, llamamos $X/\mathscr{R} = \{\overline{x} \mid x \in X\}$ y definimos una aplicación $p_{\mathscr{R}} : X \to X/\mathscr{R}$ mediante $p_{\mathscr{R}}(x) = \overline{x}$. El conjunto $X/\mathscr{R}$ se llama **conjunto cociente** de X *por la relación* $\mathscr{R}$ y la aplicación $p_{\mathscr{R}}$ se llama **proyección canónica**.

Teorema. 9.3. (Propiedad universal del conjunto cociente)
Si $\mathscr{R}$ es una relación de equivalencia en un conjunto X y $f : X \to Y$ una aplicación verificando que si $x\mathscr{R}y$, entonces $f(x) = f(y)$, entonces existe una única aplicación $\overline{f} : X/\mathscr{R} \to Y$ tal que $f = \overline{f} \circ p_{\mathscr{R}}$.



DEMOSTRACIÓN. Definimos $\overline{f}(\alpha) = f(x)$, donde x es un representante de la clase α. Es claro que si $\overline{f}$ es un aplicación entonces es la única que hace conmutar el anterior diagrama, veamos pues que es una aplicación. Para esto tenemos que comprobar que a cada elemento de $X/\mathscr{R}$ hace corresponder un único elemento de Y; como $\overline{f}$ está definida en función de los representantes de las clases que forman $X/\mathscr{R}$, tenemos que ver que esta definición no depende de los representantes que elijamos. Sean x e y dos representantes de la misma clase α, esto es; $\overline{x} = \alpha = \overline{y}$, entonces $x\mathscr{R}y$ y por tanto $f(x) = f(y)$, luego $\overline{f}$ es una aplicación. □

Volvamos ahora al caso de los enteros módulo m, si consideramos la relación de equivalencia "... es **congruente** con ... módulo m", y la representamos por $\equiv_m$, entonces el conjunto cociente $\mathbb{Z}/\equiv_m$ es precisamente $\mathbb{Z}_m$.
Vamos a definir operaciones suma y producto en $\mathbb{Z}_m$. Sean $\overline{x}, \overline{y} \in \mathbb{Z}_m$, definimos

$$\overline{x} + \overline{y} = \overline{x+y},$$

$$\overline{x} \cdot \overline{y} = \overline{xy}.$$

Así definidas, estas dos operaciones verifican las mismas propiedades que la suma y el producto de números enteros. Falta aún comprobar que podemos hacer las anteriores definiciones; esto es, que en ellas no importa el representante que se elija en cada una de las clases $\overline{x}$ e $\overline{y}$. Para comprobar esto supongamos que $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$, se verifica entonces que $x - x'$ e $y - y'$ son múltiplos de m, tenemos que

$$(x+y) - (x'+y') = (x-x') + (y-y')$$

es un múltiplo de m;

$$xy - x'y' = xy - xy' + xy' - x'y' = x(y-y') + (x-x')y'$$

es un múltiplo de m, así pues las definiciones de suma y producto son correctas y tenemos que $\mathbb{Z}_m$ es un anillo conmutativo. El cero es la clase $\overline{0}$, y el uno es la clase $\overline{1}$.
Estudiemos la aritmética de estos anillos, el primer anillo con el que nos encontramos es $\mathbb{Z}_2$, resulta que es un cuerpo. Lo mismo le ocurre a $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$, ... Esto podemos ponerlo en un Lema y obtenemos:

Lema. 9.4.
Sea m un entero positivo, $\mathbb{Z}_m$ es un cuerpo si, y sólo si, m es un número entero primo positivo.

DEMOSTRACIÓN. Supongamos que m sea un número entero primo positivo, entonces para cada $0 < n < m$ tenemos que n y m son primos relativos, luego existe una expresión $1 = an + bm$ con $a, b \in \mathbb{Z}$, entonces tenemos $\overline{1} = \overline{an}$. Por otro lado, supongamos que $\mathbb{Z}_m$ sea un cuerpo, entonces para cada número entero $0 < n < m$ existe otro número entero a tal que $\overline{1} = \overline{an}$, entonces $1 - an$ es un múltiplo de m y por tanto existe $b \in \mathbb{Z}$ tal que $1 - an = bm$, como consecuencia $1 = an + bm$, esto es; 1 es un divisor de n y m, por lo tanto n y m son primos relativos, y m no es divisible por ningún número entero positivo menor que él, esto es m es primo. □

Como se desprende de la demostración de este Lema, la Identidad de Bezout juega un papel importante en el estudio de los anillos del tipo $\mathbb{Z}_m$.
Si m no es un número entero primo resulta que el anillo $\mathbb{Z}_m$ tiene una propiedad especialmente extraña: existen elementos no nulos cuyo producto es nulo. A tales elementos los llamaremos **divisores de cero**, también incluimos entre los divisores de cero al cero del anillo. Por ejemplo, en $\mathbb{Z}_6$ los elementos $\overline{2}$ y $\overline{3}$ son no nulos y se verifica $\overline{2} \cdot \overline{3} = \overline{0}$, luego son divisores de cero. Los divisores de cero de $\mathbb{Z}_6$ son: $\overline{0}, \overline{2}, \overline{3}$ y $\overline{4}$; y los elementos $\overline{1}$ y $\overline{5}$ son elementos invertibles.

Ejercicios

Números enteros módulo n

Ejercicio. 9.5.
Calcula el inverso de $\overline{3}$ *en* $\mathbb{Z}_7$*, en* $\mathbb{Z}_{113}$ *y en* $\mathbb{Z}_{3001}$.
Ref.: 1102e_031 SOLUCIÓN.

Ejercicio. 9.6.
Resuelve en $\mathbb{Z}_5$ *las ecuaciones* $\overline{2}X+\overline{3}=\overline{3}X+\overline{1}$ *y* $X^2+X+\overline{3}=\overline{0}$.
Ref.: 1102e_032 SOLUCIÓN.

Ejercicio. 9.7.
Sean a *y* b *números enteros positivos y* $M=[a,b]$. *Prueba que si* $x\equiv y \pmod a$ *y* $x\equiv y \pmod b$, *entonces* $x\equiv y \pmod M$.
Ref.: 1102e_033 SOLUCIÓN.

Ejercicio. 9.8.
Prueba que el cuadrado de un número entero es congruente con 0, 1 *ó* 4 *módulo* 8.
Ref.: 1102e_034 SOLUCIÓN.

Ejercicio. 9.9.
Prueba que si x *es un número entero impar no divisible por* 3, *entonces* x^2 *es congruente con* 14 *módulo* 24.
Ref.: 1102e_035 SOLUCIÓN.

Ejercicio. 9.10.
Resuelve los siguientes sistemas de ecuaciones en congruencias

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \end{cases}$$

$$\begin{cases} 3x \equiv 2 \pmod 5 \\ 7x \equiv 4 \pmod{10} \end{cases}$$

Ref.: 1102e_036 SOLUCIÓN.

Ejercicio. 9.11.
Tres agricultores trabajan juntos y al recoger la cosecha se la reparten en partes iguales, van a mercados diferentes donde además usan medidas de peso distintas, en uno son de 70 *kilos, en otro de* 150 *y en el tercero de* 190*. Cada uno vendió todo lo que pudo en medidas enteras. Al regreso de los mercados el primero traía* 60 *kilos, el segundo* 110 *y el tercero* 140*. ¿Cual era el peso mínimo de la cosecha que habían recogido estos tres agricultores?*
Ref.: 1102e_037 SOLUCIÓN.

Ejercicio. 9.12.
Determina todos los números enteros x *que verifican las condiciones:*

- *Su cuadrado es congruente con* 3 *módulo* 6*.*
- *Su triple es congruente con* 5 *módulo* 25*.*
- *Su inverso módulo* 49 *es* 6*.*

Ref.: 1102e_038 SOLUCIÓN.

10. Introducción a los números naturales. Axiomas de Peano

Números naturales

Los **números naturales** se pueden definir axiomáticamente como una terna $(\mathbb{N}, 0, s)$, en donde:

(I) $\mathbb{N}$ es un conjunto.
(II) $0 \in \mathbb{N}$.
(III) $s : \mathbb{X} \longrightarrow \mathbb{N}$ es una aplicación inyectiva tal que $0 \notin \mathrm{Im}(s)$
(IV) **Principio de inducción.** Todo subconjunto $Y \subseteq \mathbb{N}$ que verifica $0 \in Y$ y para todo $x \in \mathbb{N}$ tal que $x \in Y$ se tiene $x^s = s(x) \in Y$ coincide con $\mathbb{N}$.

Los elementos de $\mathbb{N}$ se llaman **números naturales**.

Lema. 10.1.
En la situación anterior se tiene $\mathrm{Im}(s) = \mathbb{N} \setminus \{0\}$.

DEMOSTRACIÓN. Definimos $Y = \{0\} \cup \mathrm{Im}(s)$. Es claro que $0 \in Y$, y si $x \in Y$, entonces $x^s \in \mathrm{Im}(s) \subseteq Y$. Por el axioma de inducción se tiene $Y = \mathbb{N}$. □

Dada una aplicación $f : X \longrightarrow X$ definimos f^n para cada $n \in \mathbb{N}$ de la siguiente forma:

$$f^0 = \mathrm{id}_X,$$
$$f^{n^s} = f \circ f^n, \text{ para cada } n \in \mathbb{N}.$$

Observa que esta definición es correcta, ya que está definida para cada elemento de $\mathbb{N}$.
Dados dos aplicaciones $f, g : X \longrightarrow X$, decimos que f y g **conmutan** si $f \circ g = g \circ f$; esto es, $fg(x) = gf(x)$ para cada $x \in X$.

Proposición. 10.2.
Dadas dos aplicaciones que conmutan $f, g : X \longrightarrow X$ *se tiene* $f^n g^m = g^m f^n$, *para cada* $n, m \in \mathbb{N}$.
En particular se tiene $f^n f^m = f^m f^n$ *para cada aplicación* $f : X \longrightarrow X$ *y todos* $n, m \in \mathbb{N}$.

1102-04.tex

Proposición. 10.3.
Para toda aplicación $f : X \longrightarrow X$ se tiene $(f^n)^m = (f^m)^n$, para todos $n, m \in \mathbb{N}$.

Dados números naturales $n, m \in \mathbb{N}$, definimos la **suma** mediante:

$$n + m = s^n(m).$$

Lema. 10.4.
Para toda aplicación $f : X \longrightarrow X$ se tiene $f^n f^m = f^{n+m}$, para todos $n, m \in \mathbb{N}$.

Proposición. 10.5.
Para números naturales $n, m \in \mathbb{N}$ se verifica:
(1) $n + 0 = n$.
(2) $n + m^s = (n + m)^s$.
(3) La suma es conmutativa
(4) La suma es asociativa.
(5) La suma es cancelativa: si $n + m = h + m$, entonces $n = h$, para todos $n, mh \in \mathbb{N}$
(6) La suma verifica la propiedad de absorción: si $n + m = 0$, entonces $n = m = 0$, para todos $n, m \in \mathbb{N}$.

Dados números naturales $n, m \in \mathbb{N}$, definimos el **producto** mediante:

$$n \times m = (s^n)^m(0).$$

Lema. 10.6.
Para toda aplicación $f : X \longrightarrow X$ se tiene $(f^n)^m = f^{n \times m}$, para todos $n, m \in \mathbb{N}$.

Proposición. 10.7.
Para números naturales $n, m \in \mathbb{N}$ se verifica:
(1) $n \times m^s = n \times m + n$.
(2) $n \times 0 = 0$.
(3) $n \times 0^s = n$. *(El elemento* 0^s *lo representamos por 1.)*
(4) $(s^n)^m(k) = n \times m + k$, *para todos* $n, mk \in \mathbb{N}$.
(5) El producto es conmutativo.
(6) El producto es asociativo.
(7) El producto es distributivo con respecto a la suma.
(8) El producto es íntegro: si $n \times m = 0$, *entonces* $n = 0$ *ó* $m = 0$.

Ejercicio. 10.8.
Prueba que para todos los números enteros $n, m, k \in \mathbb{N}$ *se verifica: si* $n \times k = m \times k$ *y* $k \neq 0$, *entonces* $n = m$.

Dados números naturales $n, m \in \mathbb{N}$, definimos la potencia mediante:

$$n^0 = 1,$$
$$n^{m^s} = n \times n^m.$$

Proposición. 10.9.
Probar que para números naturales $n, m, k \in \mathbb{N}$ *se verifica:*
(1) $k^n k^m = k^{n+m}$.
(2) $(k^n)^m = k^{nm}$.
(3) $n^k m^k = (nm)^k$.

Para números enteros $n, m \in \mathbb{N}$ definimos

$$n \leq m \text{ si existe } x \in \mathbb{N} \text{ tal que } n + x = m.$$

Escribimos $n < m$ cuando $n \leq m$ y $n \neq m$.

Proposición. 10.10.
La relación "$\leq$" es una relación de orden total en $\mathbb{N}$.

Además esta relación de orden es **compatible** con la suma y el producto en el siguiente sentido:

Proposición. 10.11.
Dados números naturales $n, m, k \in \mathbb{N}$, *se verifica:*

(1) Si $n \leq m$, *entonces* $n + k \leq m + k$.
(2) Si $n \leq m$ *y* $k \neq 0$, *entonces* $nk \leq mk$.

En particular los recíprocos también son ciertos.

En particular $(\mathbb{N}, \leq)$ verifica una propiedad muy interesante: es un conjunto **bien ordenado**; esto es, cada subconjunto no vacío tiene un mínimo (primer elemento).

Proposición. 10.12.
$(\mathbb{N}, \leq)$ *es un conjunto bien ordenado.*

Corolario. 10.13.
No existen números naturales x *tales que* $0 < x < 1$.

Proposición. 10.14. (Segundo principio de inducción)
Si $Y \subseteq \mathbb{N}$ *es un conjunto con la propiedad* $x \in Y$ *si para todo* $n \in \mathbb{N}$ *tal que* $n < x$ *se tiene* $n \in Y$, *entonces* $Y = \mathbb{N}$.

¡Estudiar la unicidad de esta construcción!

Números enteros

Una vez construidos los números naturales observamos que no todo número natural tiene un opuesto, simétrico para la suma. La pregunta es si es posible construir otro sistema de números que extienda al sistema $\mathbb{N}$ de los números naturales, y en el que cada elemento tengo un opuesto. La construcción que presentamos a continuación nos responde a esta pregunta en afirmativo.

Consideramos el producto cartesiano $\mathbb{N}\times\mathbb{N}$, y en él definimos la operación suma a partir de la operación suma en $\mathbb{N}$; en este caso tenemos:

$$(n_1,n_2)+(m_1,m_2)=(n_1+m_1,n_2+m_2),\ \text{para } (n_1,n_2),(m_1,m_2)\in\mathbb{N}\times\mathbb{N}.$$

Lema. 10.15.
El par $(\mathbb{N}\times\mathbb{N},+)$ *es un monoide conmutativo.*

A continuación definimos en $\mathbb{N}\times\mathbb{N}$ una relación mediante:

$$(n_1,n_2)\mathscr{R}(m_1,m_2) \text{ si } n_1+m_2=n_2+m_1,\ \text{para } (n_1,n_2),(m_1,m_2)\in\mathbb{N}\times\mathbb{N}.$$

Lema. 10.16.
La relación $\mathscr{R}$ *en* $\mathbb{N}\times\mathbb{N}$ *es de equivalencia y es compatible con la operación suma.*
En particular, en el conjunto cociente $\mathbb{N}\times\mathbb{N}/\mathscr{R}$ *existe una operación suma definida por:*

$$\overline{(n_1,n_2)}+\overline{(m_1,m_2)}=\overline{(n_1+m_1,n_2+m_2)},\ \textit{para } (n_1,n_2),(m_1,m_2)\in\mathbb{N}\times\mathbb{N}.$$

Llamamos al conjunto $\mathbb{N}\times\mathbb{N}/\mathscr{R}$ simplemente $\mathbb{Z}$. Observa que cada elemento de $\mathbb{Z}$ es la clase de un par, por ejemplo (n_1,n_2); debido a que la relación de orden en $\mathbb{N}$ es total, se tiene $n_1\leq n_2$ ó $n_2\leq n_1$. En el primer caso existe $x\in\mathbb{N}$ tal que $n_2=n_1+x$; y por tanto $(n_1,n_2)\mathscr{R}(0,x)$; representamos a $\overline{(0,x)}$ por $-y$. En el segundo existe $y\in\mathbb{N}$ tal que $n_1=n_2+y$; y por tanto $(n_1,n_2)\mathscr{R}(y,0)$; representamos a $\overline{(y,0)}$ por $+y$. De forma que los elementos de $\mathbb{Z}$ son de la forma $+x$ ó $-x$, siendo $x\in\mathbb{N}$, y se tiene $+0=-0$. Los elementos de $\mathbb{Z}$ los llamamos **números enteros**.

Proposición. 10.17.
El par $(\mathbb{Z},+)$ *es un grupo abeliano.*

Tenemos una aplicación $i : \mathbb{N} \longrightarrow \mathbb{Z}$ definida $i(n) = +n$, para cada $n \in \mathbb{N}$, que evidentemente es inyectiva, por lo que podemos identificar $\mathbb{N}$ con su imagen en $\mathbb{Z}$, y por tanto a n con $+n$ para cada $n \in \mathbb{N}$.

Lema. 10.18.
En la situación anterior se tiene $i(n+m) = i(n) + i(m)$, para todos $n, m \in \mathbb{N}$.

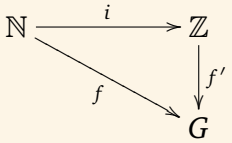
Si S_1, S_2 son semigrupos (resp. grupos) y $f : S_1 \longrightarrow S_2$ es una aplicación que verifica $f(x+y) = f(x) + f(y)$, para todos $x, y \in S_1$, decimos que f es un **homomorfismo de semigrupos** (resp. **grupos**).
Si S_1, S_2 son monoides y $f : S_1 \longrightarrow S_2$ es una aplicación que verifica $f(x+y) = f(x) + f(y)$, para todos $x, y \in S_1$, y $f(0) = 0$ decimos que f es un **homomorfismo de monoides**.
Un homomorfismo de semigrupos, monoides o grupos que tiene un inverso se llama un **isomorfismo**.

Lema. 10.19.
La aplicación $i : \mathbb{N} \longrightarrow \mathbb{Z}$ es un homomorfismo de monoides.

Ejercicio. 10.20.
Prueba que si $f : G_1 \longrightarrow G_2$ es un homomorfismo de grupos, entonces:
(1) $f(0) = 0$ y
(2) $f(-a) = -f(a)$, para todo $a \in G_1$.

La construcción del sistema de números enteros verifica una propiedad con respecto a los homomorfismos de monoides y de grupos.

Teorema. 10.21.
Dado un grupo G y un homomorfismo de monoides $f : \mathbb{N} \longrightarrow G$, existe un único homomorfismo de grupos $f' : \mathbb{Z} \longrightarrow G$ tal que $f'i = f$.



En particular el sistema de los números enteros está determinado de forma única, salvo isomorfismo, a partir del sistema de los números naturales.
En el conjunto $\mathbb{N}\times\mathbb{N}$ podemos definir un producto mediante:

$$(n_1,n_2)\times(m_1,m_2)=(n_1\times m_1, n_2\times m_2),\ \text{para } (n_1,n_2),(m_1,m_2)\in\mathbb{N}\times\mathbb{N}.$$

Ya que la relación de equivalencia $\mathscr{R}$ es compatible con el producto en $\mathbb{N}\times\mathbb{N}$, en el conjunto cociente $\mathbb{Z}$ existe una operación producto definida;

$$\overline{(n_1,n_2)}\times\overline{(m_1,m_2)}=\overline{(n_1\times m_1, n_2\times m_2)},\ \text{para } (n_1,n_2),(m_1,m_2)\in\mathbb{N}\times\mathbb{N}.$$

Lema. 10.22.
El par $(\mathbb{Z},\times)$ *es un monoide conmutativo, con elemento uno igual a* $+1$*, y elemento cero igual a* $+0$*.*

Lema. 10.23.
La aplicación $i:\mathbb{N}\longrightarrow\mathbb{Z}$ *es un homomorfismo de monoides que conserva el cero, cuando consideramos el producto en* $\mathbb{N}$ *y en* $\mathbb{Z}$*.*

Observa que el producto definido en $\mathbb{Z}$ es el único que hace que la aplicación $i:\mathbb{N}\longrightarrow\mathbb{Z}$ sea un homomorfismo de monoides.

Proposición. 10.24.
La terna $(\mathbb{Z},+,\times)$ *es un anillo conmutativo*

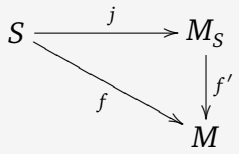
Los elementos de $\mathbb{Z}$ de la forma $+n$, con $n\in\mathbb{N}\setminus\{0\}$ los llamamos **números positivos**, y el conjunto de todos ellos se representa por $\mathbb{Z}^+$, y los elementos de la forma $-n$, con $n\in\mathbb{N}\setminus\{0\}$, los llamamos **números negativos**, y el conjunto de todos ellos se representa por $\mathbb{Z}^-$.
La relación de orden definida en $\mathbb{N}$ tiene un análogo en $\mathbb{Z}$ si definimos:

$$x\leq y \text{ si existe } n\in\mathbb{N} \text{ tal que } y=x+(+n).$$

Dados conjuntos parcialmente ordenados X e Y, una aplicación $f:X\longrightarrow Y$ que verifica: si $x_1\leq x_2$, entonces $f(x_1)\leq f(x_2)$ se llama un **homomorfismo de orden**.

Proposición. 10.25.
La aplicación $i : \mathbb{N} \longrightarrow \mathbb{Z}$ es un homomorfismo de orden.

Ejercicio. 10.26.
Sea S un semigrupo con operación $\times$; prueba que existe un único monoide M_S y un homomorfismo de semigrupos $j : S \longrightarrow M_S$ tal que para cada monoide M y cada homomorfismo de semigrupos $f : S \longrightarrow M$ existe un único homomorfismo de monoides $f' : M_S \longrightarrow M$ tal que $f'j = f$.

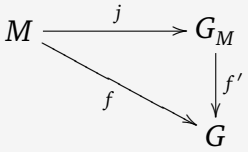


SOLUCIÓN. La construcción de M_S es la siguiente: $M_S = S \dot{\cup} \{1\}$, y la operación $\otimes$ en M_S está definida:

$$\begin{array}{ll} s \otimes t = s \times t, & \text{para todos } s, t \in S \\ 1 \otimes s = s = s \otimes 1, & \text{para todo } s \in S \\ 1 \otimes 1 = 1. & \end{array}$$

□

Ejercicio. 10.27.
Sea M un monoide conmutativo con operación "+" y elemento neutro "0"; prueba que existe un único grupo G_M y un homomorfismo de monoides $j : M \longrightarrow G_M$ tal que para cada grupo G y cada homomorfismo de monoides $f : M \longrightarrow G$ existe un único homomorfismo de grupos $f' : G_M \longrightarrow G$ tal que $f'j = f$.



SOLUCIÓN. La construcción de G_M es la siguiente: en $M \times M$ consideramos la relación

$$(n_1, n_2)\mathscr{R}(m_1, m_2) \text{ si existe } h \in M \text{ tal que } n_1 + m_2 + h = n_2 + m_1 + h,$$

para todos $(n_1, n_2), (m_1, m_2) \in M \times M$.
Esta relación es de equivalencia, y es compatible con la operación en $M \times M$ definida componente a componente. Tenemos pues una operación en $G_M = M \times M/\mathscr{R}$ definida:

$$\overline{(n_1, n_2)} \oplus \overline{(m_1, m_2)} = \overline{(n_1 + m_1, n_2 + m_2)}, \text{ para todos } (n_1, n_2), (m_1, m_2) \in M \times M.$$

El par $(G_M, \oplus)$ es un grupo abeliano; el opuesto de $\overline{(n_1, n_2)}$ es $\overline{(n_2, n_1)}$, y la aplicación $j : M \longrightarrow G_M$, definida $j(x) = (x, 0)$ es un homomorfismo de monoides que verifica la propiedad pedida.

$$\begin{array}{ll} s \oplus t = s + t, & \text{para todos } s, t \in S \\ 0 \oplus s = s = s \oplus 0, & \text{para todo } s \in S \\ 0 \oplus 0 = 0. & \end{array}$$

Observa que, en general, j no es inyectiva; lo es si, y sólo si, M es un monoide cancelativo. □

Ejercicio. 10.28.
Prueba que si M es un monoide conmutativo cancelativo, entonces la aplicación $j : M \longrightarrow G_M$ es inyectiva. El recíproco también es cierto.

Ejercicio. 10.29.
Prueba que si M es un monoide conmutativo, multiplicativo con elemento cero, entonces G_M es el grupo trivial. El recíproco también es cierto.

Ejercicios

HACER

Capítulo III

Anillos Conmutativos

Introducción

1103-00.tex

11. Operaciones en un conjunto

En esta sección vamos a introducir algunas nociones para simplificar la exposición de lo que sigue. Si X es un conjunto, una **operación binaria**, o simplemente una **operación**, "$\circ$" en X es una aplicación $\circ : X \times X \to X$. La imagen del par $(a,b) \in X \times X$ se suele representar por $a \circ b$ en vez de $\circ(a,b)$, y algunas veces simplemente por ab. Vamos a ir imponiendo a la operación "$\circ$" propiedades y a obtener resultados sobre la aritmética de los elementos de X.

Semigrupos

Una operación "$\circ$" en un conjunto X se llama **asociativa** si para cada terna de elementos $a,b,c \in X$ se verifica la igualdad:

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

Un conjunto X con una operación "$\circ$" que verifica la propiedad asociativa se llama un **semigrupo**. Para resaltar respecto a qué operación el conjunto X tiene la estructura, en este caso de semigrupo, se suele decir que el par $(X,\circ)$ es un semigrupo.

El primer resultado que destacamos es el siguiente, en un semigrupo $(X,\circ)$ se verifica la **propiedad asociativa generalizada**.

Lema. 11.1. (Propiedad asociativa generalizada)
Sea $(X,\circ)$ un semigrupo, y sean $a_1,\dots,a_n \in X$, entonces el resultado de la operación sobre la lista $a_1,\dots,a_n$ no depende de como estén dispuestos los paréntesis.

DEMOSTRACIÓN. Hacemos la demostración por inducción sobre n. Para n=0, 1, 2 y 3 el resultado ó es evidente ó no tiene sentido. Supongamos que $n > 3$, y que el resultado es cierto para cada conjunto de menos de n elementos, si $1 \le k < n$ podemos llamar $a_1 \cdots a_k$ al resultado de la operación sobre la lista $a_1,\dots,a_k$, y entonces por la hipótesis de inducción éste es un elemento perfectamente definido de X. Vamos a elegir una disposición especial de los paréntesis,

$$(\cdots((a_1a_2)a_3)\cdots a_{k-1})a_k$$

a la que vamos a llamar **forma estándar**. Para probar el resultado únicamente tenemos que probar que para cualquier $1 \le k < n$ se verifica

$$(a_1 \cdots a_k)(a_{k+1} \cdots a_n) = (\cdots((a_1a_2)a_3)\cdots a_{n-1})a_n.$$

Cuando $k = n-1$ el resultado se deduce inmediatamente aplicando la hipótesis de inducción, ya que tomando la forma estándar para $(a_1 \cdots a_{n-1})$ resulta:

$$(a_1 \cdots a_{n-1})a_n = (\cdots((a_1a_2)a_3)\cdots a_{n-1})a_n$$

1103-01.tex

es la forma estándar para $a_1 \cdots a_n$; si $k < n-1$, por la hipótesis de inducción podemos tomar la forma estándar para $a_{k+1} \cdots a_n$ y aplicando la propiedad asociativa tenemos:

$$(a_1 \cdots a_k)(a_{k+1} \cdots a_n) = (a_1 \cdots a_k)((a_{k+1} \cdots a_{n-1})a_n) =$$

$$((a_1 \cdots a_k)(a_{k+1} \cdots a_{n-1}))a_n = (a_1 \cdots a_{n-1})a_n,$$

tomando ahora la forma estándar para $(a_1 \cdots a_{n-1})$ tenemos el resultado. □

Como consecuencia, dada una lista $a_1, \ldots, a_n$ de elementos de un semigrupo X, el resultado de la operación sobre esta lista no depende de la disposición de los paréntesis y se representa por $a_1 \cdots a_n$ y también abreviadamente por $\prod_{i=1}^{n} a_i$.
Una construcción elemental que puede ser realizada en un semigrupo es la definición de las **potencias (positivas)** de un elemento. Sea X un semigrupo y $a \in X$, definimos

$$\begin{aligned} a^1 &= a, \\ a^{n+1} &= a^n \circ a, \text{ para } n \in \mathbb{N},\ n \geq 1. \end{aligned}$$

El elemento a^n se llama la ***n*-ésima potencia** de a; n se llama el **exponente** y a la **base** de la potencia.
El siguiente resultado se prueba por inducción sobre los exponentes de las potencias.

Lema. 11.2.
Sea $(X, \circ)$ un semigrupo, $a \in X$ y n, m números enteros positivos, entonces se verifica:
(1) $a^n a^m = a^{n+m}$,
(2) $(a^m)^n = a^{mn}$.

DEMOSTRACIÓN. Primer paso: demostramos que $aa^m = a^{m+1}$ para cada entero positivo m. Hacemos inducción sobre m, para $m = 1$ tenemos:

$$aa = a^2 = a^{1+1}.$$

Supongamos que el resultado sea cierto para un entero positivo m y vamos a probarlo para $m+1$, desarrollando la siguiente expresión tenemos:

$$aa^{m+1} = a(a^m a) = (aa^m)a = a^{m+1}a = a^{m+2},$$

entonces el resultado es cierto para todo entero positivo m.
Segundo paso: demostramos que $a^n a^m = a^{n+m}$ por inducción sobre n. Para $n = 1$ y para todo entero positivo m el resultado es cierto por el primer paso; supongamos que el resultado es cierto para un entero positivo n y para todo entero positivo m, vamos a probarlo para $n+1$, desarrollando la siguiente expresión tenemos:

$$a^{n+1}a^m = (aa^n)a^m = a(a^n a^m) = aa^{n+m} = a^{n+1+m},$$

como consecuencia el resultado es cierto para cada par de enteros positivos n y m.

Tercer paso: demostramos que $(a^m)^n = a^{mn}$ por inducción sobre n. Para $n = 1$ y para todo entero positivo m el resultado es cierto trivialmente; supongamos que el resultado es cierto para un entero positivo n y para todo entero positivo m, vamos a probarlo para $n+1$, desarrollando la siguiente expresión tenemos:

$$(a^m)^{n+1} = (a^m)^n a^m = a^{mn} a^m = a^{mn+m} = a^{m(n+1)},$$

como consecuencia el resultado es cierto para cada par de enteros positivos n y m. □

Semigrupos conmutativos

Una operación "$\circ$" en un conjunto X se llama **conmutativa** si para cada par de elementos $a, b \in X$ se verifica la igualdad:

$$a \circ b = b \circ a.$$

Si $(X, \circ)$ es un semigrupo y "$\circ$" es conmutativa, entonces $(X, \circ)$ se llama un **semigrupo conmutativo**. En un semigrupo conmutativo podemos establecer nuevas propiedades como en el Lema (11.2.).

Lema. 11.3.
Sea $(X, \circ)$ un semigrupo conmutativo, $a, b \in X$ y n un entero positivo, entonces se verifica

$$a^n b^n = (ab)^n.$$

DEMOSTRACIÓN. Probamos el resultado haciendo inducción sobre n. Para $n = 1$ el resultado es cierto, supongamos que sea cierto para un entero positivo n, vamos entonces a probarlo para $n+1$. Desarrollamos la siguiente expresión:

$$a^{n+1} b^{n+1} = a^n a b^n b = a^n b^n a b = (ab)^n (ab) = (ab)^{n+1}.$$

entonces el resultado es cierto para todo entero positivo n. □

Este Lema puede generalizarse inmediatamente a más de dos elementos en la siguiente forma, obteniendo la **propiedad conmutativa generalizada** sean $a_1, \ldots, a_r \in X$, entonces se verifica para cada entero positivo n la igualdad:

$$(a_1 \cdots a_r)^n = a_1^n \cdots a_r^n.$$

Monoides

Una operación "$\circ$" en un conjunto X se dice que tiene un **elemento neutro** si existe $e \in X$ tal que para cada $a \in X$ se verifica:

$$a \circ e = a = e \circ a.$$

Si $(X,\circ)$ es un semigrupo y "$\circ$" tiene un elemento neutro, entonces $(X,\circ)$ se llama un **monoide**, y si $(X,\circ)$ es un semigrupo conmutativo, entonces se llama un **monoide conmutativo**. La primera propiedad que hay que estudiar en un monoide es la unicidad del elemento neutro.

Lema. 11.4.
Si $(X,\circ)$ es un monoide, entonces existe un único elemento neutro.

DEMOSTRACIÓN. Supongamos que e y f son elementos neutros, entonces se verifica:

$$e = ef = f.$$

□

Por la unicidad del elemento neutro, en algunas ocasiones, se suele representar un monoide como una terna $(X,\circ,e)$ haciendo referencia así al elemento neutro. La segunda propiedad que se verifica en un monoide tiene relación con las potencias de un elemento $a \in X$. Si X es un monoide con elemento neutro e, definimos $a^0 = e$, como consecuencia en un monoide tenemos definida la **potencia** de cualquier elemento con exponente un número natural.

Grupos

Supongamos que "$\circ$" es una operación en un conjunto X que tiene un elemento neutro e, un elemento $a \in X$ se dice que tiene un **inverso** si existe un elemento $b \in X$ verificando:

$$a \circ b = e = b \circ a.$$

La primera propiedad elemental sobre los elementos inversos que se verifica en un monoide es la unicidad del inverso.

Lema. 11.5.
Sea $(X,\circ,e)$ un monoide, entonces si $a \in X$ tiene un inverso, este es único.

DEMOSTRACIÓN. Supongamos que b y c son inversos de a, entonces se verifica:

$$b = eb = (ca)b = c(ab) = ce = c.$$

□

Como consecuencia de la unicidad que establece el Lema anterior el inverso de un elemento $a \in X$ en un monoide, cuando existe, se suele representar por a^{-1}. La siguiente propiedad nos permite calcular algunos inversos de elementos especiales de forma simple.

Lema. 11.6.
Sea $(X, \circ, e)$ un monoide y sean $a, b \in X$ elementos que tienen inverso, entonces ab también tiene inverso y se verifica:

$$(ab)^{-1} = b^{-1}a^{-1}.$$

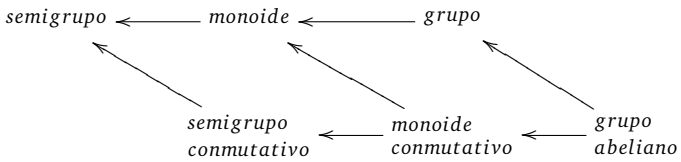
DEMOSTRACIÓN. Basta únicamente considerar las siguientes cadenas de igualdades:

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e,$$

y utilizar la unicidad del elemento inverso de ab. □

No siempre existe el inverso de un elemento de un monoide, sin embargo la existencia de inversos es deseable. Por esta razón introducimos el siguiente concepto. Llamamos **grupo** a un conjunto X con una operación "$\circ$" que es asociativa, tiene elemento neutro y tal que cada elemento tiene un inverso; si además la operación es conmutativa, el grupo se llama **grupo abeliano**.
Tenemos las siguientes relaciones entre las estructuras hasta ahora introducidas:



En un grupo podemos extender la definición de **potencias** a exponentes enteros definiendo

$$a^{-n} = (a^n)^{-1},$$

para n un entero positivo. El siguiente Lema recoge los resultados sobre este particular.

Lema. 11.7.
Sea $(G, \circ)$ un grupo, $a \in G$ y $n, m \in \mathbb{Z}$, entonces se verifica:
(1) $a^n a^m = a^{n+m}$.
(2) $(a^m)^n = a^{mn}$.

Si además G es un grupo abeliano, entonces para cada par de elementos $a, b \in G$ se verifica:
(3) $a^n b^n = (ab)^n$.

DEMOSTRACIÓN. (1). Conocemos que el resultado es cierto para todo par de números enteros no negativos, supongamos que ambos son negativos, entonces se tiene la siguiente igualdad

$$a^n a^m = (a^{-n})^{-1}(a^{-m})^{-1} = ((a^{-m})(a^{-n}))^{-1} = (a^{-m-n})^{-1} = a^{n+m}.$$

En el caso en que n es negativo y m es no negativo podemos probar el resultado haciendo inducción sobre m; para $m = 0$ el resultado es cierto para todo valor de n, vamos a probarlo para $m = 1$ y para cualquier valor de n, basta simplemente con desarrollar la siguiente expresión:

$$a^n a = (a^{-n})^{-1}a = (aa^{-n-1})^{-1}a = (a^{-n-1})^{-1}a^{-1}a = (a^{-n-1})^{-1} = a^{n+1};$$

supongamos ahora que el resultado sea cierto para $m \geq 1$ y para cualquier valor de n, y vamos a probarlo para $m+1$, desarrollamos la siguiente expresión:

$$a^n a^{m+1} = a^n a^m a = a^{n+m}a = a^{n+m+1},$$

y por tanto el resultado es cierto para cuando n es negativo y m es no negativo. En el caso en que n es no negativo y m es negativo se hace de la misma forma.

(2). Al igual que antes el resultado es cierto para n y m enteros no negativos, para probar el resultado basta con probar que se verifica la igualdad

$$(a^{-1})^n = a^{-n} \text{ para cada entero no negativo } n,$$

hacemos la demostración por inducción sobre n, para $n = 0$ el resultado es cierto, supongamos que se verifique para n y vamos a probarlo para $n+1$; se verifica:

$$(a^{-1})^{n+1} = (a^{-1})^n a^{-1} = a^{-n}a^{-1} = a^{-n-1},$$

por lo tanto tenemos el resultado. Ahora simplemente tenemos que considerar los distintos casos de los exponentes n y m para reduciendo al caso de exponente positivo o nulo obtener el resultado; por ejemplo, si m es negativo y n es no negativo se verifica:

$$(a^m)^n = \left((a^{-m})^{-1}\right)^n = (a^{-m})^{-n} = \left((a^{-m})^n\right)^{-1} = (a^{-mn})^{-1} = a^{mn}.$$

Los restantes casos se resuelven de la misma forma.

(3). Es inmediato aplicando los resultados anteriores. □

Hasta ahora hemos utilizado notación "multiplicativa" para la operación en el conjunto X. Supongamos que en X existe una operación representada por "+", y llamamos $a + b$ al resultado de la operación sobre el par $(a, b) \in X \times X$. Entonces se suelen emplear las siguientes definiciones, que expresan para una operación "aditiva" las reglas y propiedades que hemos estudiado en este capítulo. Así tenemos que para $a \in X$ se define:

$$\begin{aligned} 0 \cdot a &= e, && \text{donde } e \text{ es el elemento neutro, si existe,} \\ (n+1) \cdot a &= n \cdot a + a, && \text{para } n \text{ entero positivo ó nulo,} \\ (-n) \cdot a &= -(n \cdot a), && \text{para } n \text{ entero positivo ó nulo,} \end{aligned}$$

y donde $-a$ representa el inverso de a, que se suele llamar **opuesto** de a. Los resultados contenidos en los Lemas (11.2.), (11.3.), (11.4.), (11.7.) se escriben ahora en la siguiente forma:

$$(n+m)\cdot a = n\cdot a + m\cdot a,$$
$$(mn)\cdot a = n\cdot(n\cdot a),$$

para todo elemento $a \in X$ y para todos $n, m \in \mathbb{N}^*, \mathbb{N}, \mathbb{Z}$ según que $(X,+)$ sea un semigrupo, un monoide ó un grupo; si la operación es conmutativa, entonces se verifica:

$$n\cdot(a+b) = n\cdot a + n\cdot b,$$

para todo par de elementos $a, b \in X$ y para todo $n \in \mathbb{N}^*, \mathbb{N}, \mathbb{Z}$ según que $(X,+)$ sea un semigrupo, un monoide ó un grupo.

Recapitulando, sobre la notación aditiva ó multiplicativa tenemos las siguientes diferencias Cuando la notación es aditiva el elemento neutro se suele representar por 0, y se llama **cero**, y el inverso de $a \in X$ se representa por $-a$ y se llama **opuesto** de a; si la notación es multiplicativa, el elemento neutro se representa por 1, y se llama **uno**, y el elemento inverso de $a \in X$ se representa por a^{-1}, y se llama **inverso** de a.

notación	elemento neutro	elemento neutro	reiteración de la operación
aditiva	0 cero	$-a$ opuesto	$n\cdot a$
multiplicativa	1 uno	a^{-1} inverso	a^n

Subgrupos

Sea $(G,\circ)$ un grupo, un subconjunto $S \subseteq G$ se llama un **subgrupo** si es cerrado para la operación "$\circ$" y el par $(S,\circ)$ es un grupo. Resulta que los subgrupos pueden caracterizarse fácilmente de la siguiente forma:

Proposición. 11.8.
Sea $(G,\circ)$ un grupo y $S \subseteq G$ un subconjunto no vacío, son equivalentes:

(1) S es un subgrupo.
(2) Para cada par $x, y \in S$ se tiene $xy^{-1} \in S$.

DEMOSTRACIÓN. Si S es un subgrupo de G y si $y \in S$, entonces $y^{-1} \in S$ y por ser cerrado para la operación, si $x \in S$, entonces tenemos $xy^{-1} \in S$. Por otro lado, si S verifica la propiedad del enunciado, entonces tomando $x \in S$ se verifica $e = xx^{-1} \in S$, entonces aplicando la propiedad al par $e, x \in S$ resulta que $x^{-1} = ex^{-1} \in S$, y si $x, y \in S$, entonces ya que $y^{-1} \in S$, aplicando la propiedad al par $x, y^{-1} \in S$ tenemos que $xy = x(y^{-1})^{-1} \in S$, por lo tanto si recopilamos los resultados obtenidos resulta:

- S es cerrado para la operación.
- S tiene un elemento neutro, ya que $e \in S$.
- Cada elemento de S tiene un inverso en S, ya que si $x \in S$, entonces $x^{-1} \in S$.

Luego S es un subgrupo de G. □

Grupos finitos

Vamos a estudiar con detalle los grupos finitos, esto es; los grupos que tienen un número finito de elementos. Un elemento $a \in G$ se dice que tiene **orden** n si n es el menor entero positivo tal que $a^n = 1$; si para ningún entero positivo n se tiene que $a^n = 1$, entonces decimos que el orden de a es infinito, representamos el orden de a abreviadamente por $o(a)$.

Lema. 11.9.
Sea G un grupo y $a \in G$, definimos $\langle a \rangle = \{a^n \in G \mid n \in \mathbb{Z}\}$, entonces $\langle a \rangle$ es un subgrupo de G, y si a tiene orden finito n, entonces $\langle a \rangle$ tiene exactamente n elementos.

DEMOSTRACIÓN. Es claro que $\langle a \rangle$ es un subgrupo de G ya que es cerrado para la operación en G, contiene al elemento neutro y contiene al inverso de cada elemento. Supongamos que $o(a) = n$ es finito, entonces se verifica:

$$aa^{n-1} = a^{n-1}a = 1,$$

y por tanto a^{n-1} es el inverso de a. Consideramos el conjunto $A = \{a^i \in G \mid 0 \leq i \leq n-1\}$, entonces A es un subgrupo de G, ya que es cerrado para la operación: si $a^i, a^j \in A$, entonces tenemos que

$$a^i a^j = \begin{cases} a^{i+j} & \text{si } i+j \leq n-1, \\ a^{i+j-n} & \text{si } i+j > n-1. \end{cases}$$

Contiene al elemento neutro, ya que $1 = a^0 \in A$. Si $a^i \in A$ con $i \neq 0$, entonces a^{n-i} es el inverso de a^i ya que $a^i a^{n-i} = a^n = 1$. Es claro que en este caso se verifica $A = \langle a \rangle$. Vamos a contar el número de elementos de A, si existen $a^i = a^j$ con $0 \leq i < j \leq n-1$, entonces tenemos $1 = a^j a^i = a^{j-i}$, lo que es una contradicción con la propiedad que define a n; luego en A existen exactamente n elementos.
□

El subgrupo $\langle a \rangle$ se llama el **subgrupo cíclico** generado por a en G. Un grupo G se llama **cíclico** si existe $a \in G$ tal que $G = \langle a \rangle$. Llamamos **orden** de un grupo finito G a su número de elementos, y lo representamos por $| G |$. Para cada elemento $a \in G$ de orden finito se verifica $o(a) = | \langle a \rangle |$. Vamos a ver que en un grupo finito todo elemento es de orden finito.

Lema. 11.10.
Si G es un grupo finito, entonces cada elemento $a \in G$ tiene orden finito.

DEMOSTRACIÓN. Consideramos la sucesión $a, a^2, a^3, \ldots$ de elementos de G, ya que G es finito, no todos los elementos de la sucesión son distintos, luego existen al menos dos que son iguales, supongamos que $n < m$ y que $a^n = a^m$, entonces existe $k \in \mathbb{N}^*$ tal que $m = n + k$, desarrollando tenemos $a^n = a^m = a^{n+k}$, de donde se deduce que $1 = a^k$, y por tanto a tiene orden finito. □

Como consecuencia de los Lemas anteriores, para cada elemento a de un grupo finito G se verifica $o(a) \leq |\, G \,|$; y podemos afinar más en esta relación, vamos a demostrar que $o(a)$ divide a $|\, G \,|$.
Si G es un grupo y S es un subgrupo de G, definimos la relación $\sim$ mediante:

$$a \sim b \text{ si } ab^{-1} \in S.$$

Esta es una relación de equivalencia en G, vamos a determinar la clase de equivalencia de $a \in G$, tenemos:

$$\begin{array}{ll} \overline{a} = \{b \in G \mid\ b \sim a\} & = \{b \in G \mid\ ba^{-1} \in S\} \\ = \{b \in G \mid \text{ existe } s \in S,\ ba^{-1} = s\} & = \{b \in G \mid \text{ existe } s \in S,\ b = sa\} \\ = \{sa \in G \mid\ s \in S\} & = Sa. \end{array}$$

Llamamos a Sa una **clase a la derecha** de S en G. Vamos a contar el número de elementos de Sa.

Lema. 11.11.
Sea G un grupo y S un subgrupo de G, entonces existe una biyección entre cada dos clases a la derecha de S en G.

DEMOSTRACIÓN. Basta ver que existe una biyección entre S y cada clase a la derecha Sa de S en G. Definimos

$$f : S \to Sa : \qquad f(s) = sa.$$

Es claro que f es sobreyectiva. Además, si $s, t \in S$ verifican $f(s) = f(t)$, entonces $sa = ta$, luego $s = t$, y f es también inyectiva. □

Teorema. 11.12. (Teorema de Lagrange)
Sea G un grupo finito y S un subgrupo de G, entonces el orden de S divide al orden de G.

DEMOSTRACIÓN. La relación $\sim$ en G es de equivalencia y las clases de equivalencia dan lugar a una partición de G; ya que las clases de equivalencia son las clases a la derecha de H en G tenemos una partición de G, por ejemplo $G = Sa_1 \cup \ldots \cup Sa_r$, entonces el número de elementos de G es igual a r por el número de elementos de S. Luego $|G| = r|S|$, y tenemos el resultado. □

Como consecuencia, para cada elemento a de un grupo finito G se tiene que $o(a)$ divide a $|\ G\ |$. Dado un grupo finito G y un subgrupo S, se llama **índice** de S en G al número entero $|G|/|S|$, y se nota por $[G:S]$.
De forma análoga es posible definir las clases a la izquierda de H en G, obteniéndose análogos resultados.

Grupos cocientes

Sea G un grupo, una relación de equivalencia $\mathscr{R}$ en G se dice **compatible** con la estructura de grupo si verifica:

(1) Si $a_1, a_2, b \in G$ y $a_1 \mathscr{R} a_2$, entonces $a_1 b \mathscr{R} a_2 b$.
(2) Si $a_1, a_2 \in G$ y $a_1 \mathscr{R} a_2$, entonces $a_1^{-1} \mathscr{R} a_2^{-1}$.

Un subgrupo $N \subseteq G$ se dice **normal** si para cada $n \in N$ y cada $g \in G$ se tiene $gng^{-1} \in N$.

Lema. 11.13.
Sea G un grupo con elemento neutro e y $\mathscr{R}$ una relación de equivalencia en G. Son equivalentes:

(1) Si $\mathscr{R}$ es una relación de equivalencia compatible con la estructura de grupo de G, entonces el conjunto $\overline{e} = \{x \in G \mid\ x \mathscr{R} e\} \subseteq G$ es un subgrupo normal.
(2) Si $N \subseteq G$ es un subgrupo normal, la relación $\mathscr{R}_N$, definida $a_1 \mathscr{R}_N a_2$ si $a_1 a_2^{-1} \in N$ es una relación compatible con la estructura de grupo de G, y $N = \overline{e}$.

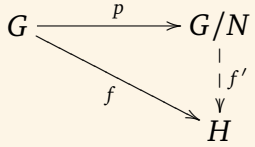
DEMOSTRACIÓN. (1). Es claro que $e \in \overline{e}$. Si $a_1, a_2 \in \overline{e}$, entonces $a_2 \mathscr{R} e$, luego $a_2^{-1} \mathscr{R} e$, y se tiene $a_1 a_2^{-1} \in \overline{e}$. Si $a \in \overline{e}$ y $x \in G$, se tiene $xax^{-1} \mathscr{R} xex^{-1} = e$, y por tanto $xax^{-1} \in \overline{e}$.
(2). Es claro que $\mathscr{R}_N$ es una relación de equivalencia, veamos que es compatible con la estructura de grupo de G. Sean $a_1, a_2, b \in G$ tales que $a_1 \mathscr{R}_N a_2$, entonces $a_1 a_2^{-1} \in G$, y para cada $b \in G$ se tiene $a_1 b (a_2 b)^{-1} = a_1 a_2^{-1} \in N$, luego $a_1 b \mathscr{R}_N a_2 b$. Sea $a_1, a_2 \in G$ tales que $a_1 \mathscr{R}_N a_2$, entonces $a_1 a_2^{-1} \in N$, y se tiene $a_2^{-1} a_1 = a_2^{-1} a_1 a_2^{-1} a_2 \in N$, luego $a_1^{-1} a_2 \in N$, y por tanto $a_1^{-1} \mathscr{R}_N a_2^{-1}$. □

Tenemos entonces una correspondencia biyectiva entre relaciones de equivalencia en G compatibles con la estructura de grupo y subgrupos normales de G.
Dados $\mathscr{R}_N$ y N en esta correspondencia, en el conjunto cociente $G/\mathscr{R}_N$ podemos definir una estructura de grupo mediante:

$$\overline{a_1}\ \overline{a_2} = \overline{a_1 a_2}.$$

Se tiene, de forma natural, que la proyección canónica $p : G \longrightarrow G/\mathscr{R}_N$ es un homomorfismo de grupos; para dada dos elementos $a_1, a_2 \in G$ se tiene $p(a_1) = p(a_2)$ si, y sólo si, $a_1 \mathscr{R}_N a_2$ si, y sólo si, $a_1 a_2^{-1} \in N$. Representamos a $G/\mathscr{R}_N$ por G/N, y lo llamamos el **grupo cociente** de G por el subgrupo normal N.
En conclusión, tenemos:

Teorema. 11.14. (Propiedad universal del grupo cociente)
Sea G un grupo y $N \subseteq G$ un subgrupo normal, para cada homomorfismo de grupo $f : G \longrightarrow H$ tal que $f(n) = e$, para cada $n \in N$, existe un único homomorfismo de grupos $f' : G/N \longrightarrow H$ tal que $f = f'p$. Esto es, el siguiente diagrama conmuta



Ejercicios

Operaciones en un conjunto

Ejercicio. 11.15.
Demuestra que $(\mathbb{N},+)$ *es un monoide conmutativo y que* $(\mathbb{Z},+)$ *es un grupo abeliano.*
Ref.: 1103e_001 *SOLUCIÓN.*

Ejercicio. 11.16.
Demuestra que $(\mathbb{N},\cdot)$ *y* $(\mathbb{Z},\cdot)$ *son monoides conmutativos.*
Ref.: 1103e_002 *SOLUCIÓN.*

Un monoide X se llama **cancelativo** si para todos $a,b,c,d \in X$ se verifica que si $ac = bc$ ó $da = db$, entonces $a = b$.

Ejercicio. 11.17.
Demostrar que $(\mathbb{N},+)$ *y* $(\mathbb{Z},+)$ *son monoides cancelativos, y que* $(\mathbb{N},\cdot)$ *y* $(\mathbb{Z},\cdot)$ *no lo son.*
Ref.: 1103e_003 *SOLUCIÓN.*

Ejercicio. 11.18.
Demostrar que todo grupo G *es un monoide cancelativo.*
Ref.: 1103e_004 *SOLUCIÓN.*

Ejercicio. 11.19.
Sea G *un grupo, demostrar que* G *es un grupo abeliano si, y sólo si, para todos* $a,b \in G$ *se verifica* $(ab)^2 = a^2b^2$.
Ref.: 1103e_005 *SOLUCIÓN.*

Ejercicio. 11.20.
Sea G un grupo, demostrar que si para todo $a \in G$ se verifica $a^2 = e$, entonces G es un grupo abeliano.
Ref.: 1103e_006 SOLUCIÓN.

Ejercicio. 11.21.
*Llamamos **grupo lineal general** $Gl(\mathbb{R},2)$ al conjunto de las matrices 2×2 con coeficientes en $\mathbb{R}$ y determinante no nulo. Demostrar que $Gl(\mathbb{R},2)$ es un grupo no abeliano.*
Ref.: 1103e_007 SOLUCIÓN.

Ejercicio. 11.22.
Consideramos el conjunto

$$M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \right\};$$

demostrar que M es un subgrupo del grupo lineal general $Gl(\mathbb{R},2)$.
Ref.: 1103e_008 SOLUCIÓN.

Ejercicio. 11.23.
*Si G es un grupo, se define el **centro** de G como*

$$Z(G) = \{g \in G \mid \ gx = xg, \ \textit{pata todo } x \in G\},$$

demostrar que $Z(G)$ es un subgrupo de G.
Ref.: 1103e_009 SOLUCIÓN.

Ejercicio. 11.24.
Calcular el centro de $Gl(\mathbb{R}, 2)$.
Ref.: 1103e_010 *SOLUCIÓN.*

Ejercicio. 11.25.
Sea $X = \{1, \ldots, n\}$ *un conjunto finito con* n *elementos, llamamos* S_n *al conjunto de todas la aplicaciones biyectivas de* X *en* X. *Demostrar que* S_n *es un grupo con operación la composición de aplicaciones. Calcular el número de elementos de* S_n.
Ref.: 1103e_011 *SOLUCIÓN.*

Ejercicio. 11.26.
Determinar todos los subgrupos del grupo aditivo de los números enteros.
Ref.: 1103e_012 *SOLUCIÓN.*

Ejercicio. 11.27.
Demostrar que la intersección de una familia de subgrupos de un grupo G *es un subgrupo de* G.
Ref.: 1103e_013 *SOLUCIÓN.*

Ejercicio. 11.28.
Sea G *un grupo y* H, K *subgrupos de* G *tales que para algunos* $a, b \in G$ *se tiene* $Ha = Kb$. *Demostrar que* $H = K$.
Ref.: 1103e_014 *SOLUCIÓN.*

Ejercicio. 11.29.
Si G es un grupo y $a \in G$ tiene orden finito n, entonces para cada número entero positivo h tal que $a^h = 1$ se verifica $o(a) = n \mid h$.
Ref.: 1103e_015 *SOLUCIÓN.*

Ejercicio. 11.30.
Sea G un grupo y $a, b \in G$ elementos que verifican $ab = ba$ de órdenes n y m respectivamente; si $\langle a \rangle \cap \langle b \rangle = 1$, demostrar que $o(ab) = \text{mcm}\{n, m\}$.
Ref.: 1103e_016 *SOLUCIÓN.*

Ejercicio. 11.31.
Sea G un grupo y $a, b \in G$ elementos de G verificando $ab = ba$. Si el orden de a es n y el orden de b es m, y ambos son primos relativos, demostrar que entonces el orden de ab es nm.
Ref.: 1103e_017 *SOLUCIÓN.*

Ejercicio. 11.32.
Dado un grupo G, llamamos ***exponente*** *de G al supremo de los órdenes de los elementos de G. Demostrar:*

(1) Si G tiene exponente finito, entonces existe un elemento $a \in G$ tal que el orden de a es igual al exponente de G.
(2) Si el orden de G es finito, entonces el exponente de G es un divisor del orden de G.
(3) Si G es abeliano y el exponente de G es finito, entonces el orden de cada elemento divide al exponente de G.

Ref.: 1103e_018 *SOLUCIÓN.*

Ejercicio. 11.33.
¿Si a y b son elementos de un grupo y tienen orden finito, es necesariamente ab de orden finito?
Nota: Considerar el grupo de matrices cuadradas con determinante no nulo y coeficientes en $\mathbb{Q}$, y los elementos

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad y \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Ref.: 1103e_019 SOLUCIÓN.

12. Definición de anillo y homomorfismo de anillos

Un **anillo** es una terna $(A,+,\circ)$, formada por un conjunto no vacío A, y dos operaciones binarias en A verificando los siguientes axiomas:

(I) $(A,+)$ es un grupo abeliano. El elemento neutro lo notamos por 0 y lo llamamos **cero** ó **elemento nulo** del anillo.

(II) $(A,\circ)$ es un monoide. El elemento neutro lo notamos por 1 y lo llamamos **uno** del anillo. Si $a,b\in A$, el elemento $a\circ b$ se notará también por ab.

(III) Para cada terna $a,b,c\in A$ se verifica:

$$a\circ(b+c)=a\circ b+a\circ c \quad \text{y} \quad (b+c)\circ a=b\circ a+c\circ a.$$

Si el monoide $(A,\circ)$ es conmutativo el anillo se llama **conmutativo**. Cuando $0=1$, el anillo se llama **trivial**, en nuestro desarrollo vamos a considerar anillos no triviales y conmutativos, salvo que digamos lo contrario.

Un elemento $r\in A$ se llama un **divisor de cero** si existe $0\neq s\in A$ tal que $rs=0$. Un anillo A se llama **dominio de integridad** si no tiene divisores de cero no nulos.

Un elemento $r\in A$ se llama **invertible**, o una **unidad**, si existe $s\in A$ tal que $rs=1$; el elemento s se llama el **inverso** de r. Un anillo en el que cada elemento no nulo es invertible se llama un **cuerpo**.

Los siguientes resultados son obvios a partir de la definición y puede decirse que constituyen la base de la aritmética de los anillos.

Lema. 12.1.
Sea A un anillo, se verifica:

(1) Los elementos cero y uno están determinados de forma única.
(2) Para cada elemento el opuesto y el inverso, si existen, están determinados de forma única.

Proposición. 12.2.
Sea A un anillo, se verifica:

(1) $r0=0$ *para todo* $r\in A$.
(2) A tiene más de un elemento si, y sólo si, $0\neq 1$.
(3) $(-r)s=-(rs)=r(-s)$, *para todos* $r,s\in A$. *En particular* $(-1)r=-r$.
(4) $(n\cdot r)s=n\cdot(rs)=r(n\cdot s)$, *para todos* $r,s\in A$ *y* $n\in\mathbb{Z}$.
(5) $(\sum_{i=1}^{n} r_i)(\sum_{j=1}^{m} s_j)=\sum_{i=1,j=1}^{n\ m} r_is_j$, *para todos* $r_i,s_j\in A$ *y* $n,m\in\mathbb{N}^*$.
(6) ***Fórmula de Newton.*** $(r+s)^n=\sum_{i=0}^{n}\binom{n}{i}r^is^{n-i}$, *para todos* $r,s\in A$ *y* $n\in\mathbb{N}$.

1103-02.tex

DEMOSTRACIÓN. (1). Consideramos el siguiente desarrollo:

$$r0 + r = r0 + r1 = r(0 + 1) = r1 = r,$$

y simplificando por r tenemos $r0 = 0$.
(2). Si $0 = 1$, entonces para cada $r \in A$ se tiene $r = r1 = r0 = 0$, luego todo elemento de A es nulo y por tanto $A = \{0\}$. Es evidente que si A tiene un sólo elemento, entonces $0 = 1$.
(3). Consideramos el siguiente desarrollo:

$$(-r)s + rs = (-r + r)s = 0s = 0,$$

luego $(-r)s$ es el opuesto de rs y por tanto tenemos el resultado. De la misma forma se demuestra que $r(-s) = -(rs)$.
(4). Para n entero positivo ó nulo hacemos la demostración por inducción sobre n. Para $n = 0, 1$ el resultado es evidente; supongamos que sea cierto para n, entonces se verifica:

$$((n + 1) \cdot r)s = (n \cdot r + r)s = (n \cdot r)s + rs = n \cdot (rs) + rs = (n + 1) \cdot (rs).$$

y por tanto el resultado es cierto para todo entero positivo ó nulo. Si n es negativo, entonces aplicando el apartado (3) se verifica:

$$(n \cdot r)s = (-(-n) \cdot r)s = -((-n) \cdot r)s = -((-n) \cdot (rs)) = n \cdot (rs),$$

ya que $-n$ es un entero positivo en este caso, luego el resultado es cierto para todo número entero.
(5). Hacemos la demostración por inducción sobre n y m enteros positivos. Supongamos que $n = 1$, probemos el resultado para todo entero positivo m; si $m = 1, 2$ el resultado es evidente, supongamos que sea cierto para m, y estudiemos el caso de $m + 1$, desarrollando la siguiente expresión tenemos:

$$r_1\left(\sum_{j=1}^{m+1} s_j\right) = r_1\left(\sum_{j=1}^{m} s_j + s_{m+1}\right) = r_1\left(\sum_{j=1}^{m} s_j\right) + r_1 s_{m+1}$$

$$= \sum_{j=1}^{m} r_1 s_j + r_1 s_{m+1} = \sum_{j=1}^{m+1} r_1 s_j,$$

por tanto el resultado es cierto para $n = 1$ y para todo número entero positivo m. Supongamos ahora que sea cierto para n y para todo entero positivo m, vamos a probarlo para $n + 1$, desarrollando la siguiente expresión tenemos:

$$\left(\sum_{i=1}^{n+1} r_i\right)\left(\sum_{j=1}^{m} s_j\right) = \left(\sum_{i=1}^{n} r_i + r_{n+1}\right)\left(\sum_{j=1}^{m} s_j\right) = \left(\sum_{i=1}^{n} r_i\right)\left(\sum_{j=1}^{m} s_j\right) + r_{n+1}\left(\sum_{j=1}^{m} s_j\right)$$

$$= \sum_{i=1,j=1}^{n\,m} r_i s_j + \sum_{j=1}^{m} r_{n+1} s_j = \sum_{i=1,j=1}^{n\,m} r_i s_j + \sum_{j=1}^{m} r_{n+1} s_j = \sum_{i=1,j=1}^{n+1\,m} r_i s_j,$$

por tanto el resultado es cierto para todo par de números enteros positivos n y m.
(6). La demostración de este hecho en un anillo (conmutativo) es análoga a la ya realizada en el caso de números naturales. □

Corolario. 12.3.
Sea A un anillo, para $a, b \in A$ y para $n, m \in \mathbb{Z}$ se verifica:

$$(n \cdot a)(m \cdot b) = (nm) \cdot (ab).$$

DEMOSTRACIÓN. Aplicando los resultados obtenidos en la Proposición podemos hacer el siguiente desarrollo:

$$(n \cdot a)(m \cdot b) = n \cdot (a(m \cdot b)) = n \cdot (m \cdot (ab)) = (nm) \cdot (ab).$$

□

Ejemplos. 12.4.

(1) El conjunto $\mathbb{Z}$ de los números enteros con la suma y el producto usuales es un anillo. También lo son los conjuntos de los números racionales, $\mathbb{Q}$, de los números reales, $\mathbb{R}$ y de los números complejos, $\mathbb{C}$. Sin embargo el conjunto $\mathbb{N}$ de los números naturales no es un anillo, ya que $(\mathbb{N}, +)$ no es un grupo abeliano.

(2) Consideramos el conjunto $M_2(\mathbb{C})$ de las matrices cuadradas de orden 2 sobre el cuerpo de los números complejos, y definimos la suma y el producto usuales, entonces obtenemos un anillo no conmutativo.

(3) Consideremos el conjunto $\mathbb{H}$ formado por todas las combinaciones de la forma

$$a_0 + a_1 i + a_2 j + a_3 k,$$

donde $a_0, a_1, a_2, a_3 \in \mathbb{R}$, y verificando las siguientes relaciones:

$1\backslash 2$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

las operaciones en $\mathbb{H}$ se definen: la suma componente a componente y el producto por distributividad aplicando las relaciones anteriores; resulta que $\mathbb{H}$ es un anillo no conmutativo, además cada elemento no nulo tiene un inverso. Los elementos de $\mathbb{H}$ se llaman **cuaternios**. Un anillo verificando estas propiedades se llama un **anillo de división**.

Dados dos anillos A y B, una aplicación $f : A \longrightarrow B$ es un **homomorfismo de anillos** si verifica:

(1) $f(r+s) = f(r) + f(s)$, para todos $r, s \in A$.
(2) $f(rs) = f(r)f(s)$, para todos $r, s \in A$.
(3) $f(1) = 1$.

Lema. 12.5.
La composición de dos homomorfismos de anillos, si está definida, es un homomorfismo de anillos.

Proposición. 12.6.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos, entonces se verifica:
(1) $f(0) = 0$.
(2) Para cada $a \in A$ se tiene $f(-a) = -f(a)$.

DEMOSTRACIÓN. (1). Se verifica $f(0) = f(0+0) = f(0) + f(0)$, luego $f(0) = 0$.
(2). Dado $a \in A$ se verifica:

$$0 = f(0) = f(a-a) = f(a) + f(-a),$$

luego $f(-a) = -f(a)$. □

Si $f : A \longrightarrow B$ es un homomorfismo de anillos, definimos la **imagen** de f como

$$\mathrm{Im}(f) = \{f(a) \mid a \in A\}.$$

Lema. 12.7.
Con la notación anterior $\mathrm{Im}(f)$ *verifica las siguientes propiedades:*
(1) Para $x, y \in \mathrm{Im}(f)$ se tienen $x - y \in \mathrm{Im}(f)$, esto es; $\mathrm{Im}(f)$ *es un* ***subgrupo aditivo*** *de B.*
(2) El producto de dos elementos de $\mathrm{Im}(f)$ *pertenece a* $\mathrm{Im}(f)$.
(3) $1 \in \mathrm{Im}(f)$.

En general diremos que un subconjunto $S \subseteq A$ de un anillo A verificando las propiedades (1-3) del Lema anterior es un **subanillo** de A. Los subanillos pueden caracterizarse de la siguiente forma:

Lema. 12.8.
Sea A un anillo y S un subconjunto de A, son equivalentes:
(a) S es un subanillo de A.
(b) S es un anillo con operaciones la restricción de las operaciones de A y con elemento uno el uno de A.
(c) La inclusión $i : S \hookrightarrow A$ es un homomorfismo de anillos.

DEMOSTRACIÓN. (a)⇒(b). Si S es un subanillo, entonces la restricción de las operaciones en A definen operaciones en S, además $(S,+)$ es un grupo abeliano, $(S,\cdot)$ es un monoide conmutativo y $1 \in S$ es el elemento uno.

(b)⇒(c). Es evidente.

(c)⇒(a). Resulta que tenemos en este caso $S = \mathrm{Im}(i)$, y como la imagen de un homomorfismo de anillos es un subanillo, entonces S es un subanillo de A. □

Proposición. 12.9.
Sea A un anillo y $\{S_i \mid i \in I\}$ una familia de subanillos de A, entonces $\cap\{S_i \mid i \in I\}$ es un subanillo de A.

DEMOSTRACIÓN. Sean $x, y \in \cap S_i$, entonces tenemos $x, y \in S_i$ para cada $i \in I$, ya que cada S_i es un subanillo resulta que $x-y, xy \in S_i$, luego tenemos $x-y, xy \in \cap S_i$. Es claro que $1 \in \cap S_i$. □

Ejemplos. 12.10.
Este resultado nos permite la construcción de subanillos de una forma cómoda; vamos a estudiar varios casos:

(1) Dado un subconjunto X de un anillo A, llamamos **subanillo de A generado por X** a la intersección de todos los subanillos de A que contienen a X, esto es; el menor subanillo que contiene a X.

(2) Como caso particular de esta construcción vamos a definir la **suma de dos subanillos**, ó en general de una familia de subanillos. Sean S_1 y S_2 subanillos de un anillo A definimos $S_1 \vee S_2$ como el subanillo generado por el subconjunto $S_1 \cup S_2$; es fácil ver que

$$S_1 \vee S_2 = \{\text{sumas finitas de productos } s_1 s_2 \in A \text{ con } s_i \in S_i,\ i = 1,2 \text{ y coeficientes en } \mathbb{Z}\}.$$

En general el menor subanillo que contiene a cada uno de los elementos de una familia de subanillos $\{S_i \mid i \in I\}$ es el subanillo generado por el subconjunto unión $\cup\{S_i \mid i \in I\}$, y se representa por $\vee\{S_i \mid i \in I\}$; sus elementos son sumas finitas $\sum t_i$, donde t_i es un producto de elementos de $\cup\{S_i \mid i \in I\}$.

(3) Si S es un subanillo de A y X es un subconjunto de A, el subanillo de A generado por $S \cup X$ se nota por $S[X]$. Sus elementos son expresiones del tipo $s_0 + \sum_i s_i x_i$, en donde $s_j \in S$ y x_i es un producto de elementos de XÂ·

(4) Cuando X consta de un sólo elemento $X = \{x\}$, resulta que el subanillo generado por x tiene una forma especialmente sencilla, sus elementos son

$$\{n_0 \cdot 1 + n_1 \cdot x + \cdots n_r \cdot x^r \mid n_0, n_1, \ldots, n_r \in \mathbb{Z}\},$$

por lo que el subanillo se representa por $\mathbb{Z}[x]$.

(5) Si X consta de más de un elemento, entonces el subanillo generado por X se obtiene a partir de los subanillos generados por cada uno de sus elementos, y como consecuencia tenemos una fácil descripción del mismo.

Si $f : A \longrightarrow B$ es un homomorfismo de anillos, para $X \subseteq B$ definimos la **imagen inversa** de X como $f^{-1}(X) = \{a \in A \mid f(a) \in X\}$, y para $Y \subseteq A$ definimos la **imagen directa** de Y como $f(Y) = \{f(y) \in B \mid y \in Y\}$.

Proposición. 12.11.
Si $f : A \longrightarrow B$ es un homomorfismo de anillos, se verifica:
(1) Si S es un subanillo de A, entonces $f(S)$ es un subanillo de B.
(2) Si T es un subanillo de B, entonces $f^{-1}(T)$ es un subanillo de A.

DEMOSTRACIÓN. (1). Sean $x, y \in f(S)$, entonces existen $a, b \in S$ tales que $x = f(a)$ e $y = f(b)$, y tenemos:

$$x - y = f(a) - f(b) = f(a - b),$$

ya que S es un subanillo de A resulta que $a - b \in S$ y por tanto $x - y \in f(S)$; por otro lado:

$$xy = f(a)f(b) = f(ab),$$

ya que S es un subanillo de A resulta que $ab \in S$ y por tanto $xy \in f(S)$; finalmente es claro que $1 = f(1) \in f(S)$.
(2). Sean $x, y \in f^{-1}(T)$, entonces tenemos $f(x), f(y) \in T$, y por tanto se verifica:

$$f(x - y) = f(x) - f(y) \in T,$$

$$f(xy) = f(x)f(y) \in T,$$

luego $x - y, xy \in f^{-1}(T)$, y ya que $f(1) = 1$, resulta que $f^{-1}(T)$ es un subanillo de A. □

Como consecuencia de esta Proposición obtenemos un resultado ya conocido sobre la imagen de un homomorfismo de anillos.

Corolario. 12.12.
Si $f : A \longrightarrow B$ es un homomorfismo de anillos, entonces $\mathrm{Im}(f)$ *es un subanillo de S.*

Ejemplos. 12.13.
(1) Las siguientes inclusiones son inclusiones de anillos: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$.

(2) El subanillo $\mathbb{Z}[i]$ de $\mathbb{C}$ es el subanillo generado por i en $\mathbb{C}$, y está formado por los siguientes elementos:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

$\mathbb{Z}[i]$ se llama el **anillo de los enteros de Gauss**.

(3) El conjunto $2\mathbb{Z}$ de los números enteros pares no es un subanillo de $\mathbb{Z}$ ya que no contiene al elemento uno, y por lo tanto no es un anillo.

(4) La aplicación $f : \mathbb{R} \longrightarrow M_2(\mathbb{R})$ definida $f(c) = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$ es un homomorfismo de anillos, por lo tanto su imagen es un subanillo (conmutativo) de $M_2(\mathbb{R})$.

(5) Otro subanillo (conmutativo) de $M_2(\mathbb{R})$ es el siguiente:

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\},$$

este subanillo es precisamente la imagen del homomorfismo de anillos

$$f : \mathbb{C} \longrightarrow M_2(\mathbb{R}),$$

definido por

$$f(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Si $f : A \longrightarrow B$ es un homomorfismo de anillos, definimos el **núcleo** de f

$$\mathrm{Ker}(f) = \{a \in A \mid f(a) = 0\}.$$

El núcleo sirve, entre otras cosas, para caracterizar aquellos homomorfismos de anillos que son aplicaciones inyectivas.

Lema. 12.14.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos, entonces f es una aplicación inyectiva si, y sólo si, $\mathrm{Ker}(f) = \{0\}$.

DEMOSTRACIÓN. Si f es una aplicación inyectiva, entonces para $a \in \mathrm{Ker}(f)$ se verifica $f(a) = 0 = f(0)$, luego $a = 0$, y por tanto $\mathrm{Ker}(f) = \{0\}$. Supongamos ahora que $\mathrm{Ker}(f) = \{0\}$, entonces si para $a, b \in A$ se verifica $f(a) = f(b)$, se tiene $f(a - b) = f(a) - f(b) = 0$, y por tanto $a - b \in \mathrm{Ker}(f)$ y resulta $a = b$, luego f es inyectiva. □

Lema. 12.15.
Con la notación anterior, $\mathrm{Ker}(f)$ *verifica las siguientes propiedades:*
(1) $\mathrm{Ker}(f)$ *es un subgrupo aditivo de A.*
(2) Para elementos $a \in A$ *y* $x \in \mathrm{Ker}(f)$ *se tiene* $ax \in \mathrm{Ker}(f)$.

DEMOSTRACIÓN. (1). Sean $x, y \in \mathrm{Ker}(f)$, entonces se verifica:

$$f(x-y) = f(x) - f(y) = 0 - 0 = 0,$$

luego $x - y \in \mathrm{Ker}(f)$.
(2). Supongamos ahora que $a \in A$ y que $x \in \mathrm{Ker}(f)$, entonces se verifica:

$$f(ax) = f(a)f(x) = f(a)0 = 0.$$

□

En general diremos que un subconjunto $\mathfrak{a} \subseteq A$ de un anillo A verificando las propiedades (1-2) del Lema anterior es un **ideal** de A.

Proposición. 12.16.
Sea A un anillo y $\{\mathfrak{a}_i \mid i \in I\}$ *una familia de ideales de A, entonces* $\cap\{\mathfrak{a}_i \mid i \in I\}$ *es un ideal de A.*

DEMOSTRACIÓN. Sean $x, y \in \cap\{\mathfrak{a}_i \mid i \in I\}$, entonces $x, y \in \mathfrak{a}_i$ para cada $i \in I$, ya que cada $\mathfrak{a}_i$ es un ideal resulta que $x - y \in \mathfrak{a}_i$, luego $x - y \in \cap\{\mathfrak{a}_i \mid i \in I\}$. Por otro lado, sean $a \in A$ y $x \in \cap\{\mathfrak{a}_i \mid i \in I\}$, entonces $x \in \mathfrak{a}_i$ para cada $i \in I$, ya que $\mathfrak{a}_i$ es un ideal resulta que $ax \in \mathfrak{a}_i$, y por tanto $ax \in \cap\{\mathfrak{a}_i \mid i \in I\}$. □

Dado un subconjunto X de un anillo A, llamamos **ideal de** A **generado por** X a la intersección de todos los ideales de A que contienen a X y lo representamos por (X) ó XA. Los elementos de (X) pueden ser descritos de forma simple como:

$$(X) = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_i \in A, x_i \in X, n \in \mathbb{N} \right\}.$$

Cuando $X = \{x_1, \ldots, x_n\}$, el ideal (X) se suele escribir $(x_1, \ldots, x_n)$, si $n = 1$, se representa también por xA, y se llama **ideal principal generado por** x.

Dada una familia de ideales $\{\mathfrak{a}_i \mid i \in I\}$, llamamos **suma** de la familia al ideal generado por $X = \cup\{\mathfrak{a}_i \mid i \in I\}$, sus elementos son de la forma

$$\sum_{j=1}^{n} a_j x_{i_j},$$

con $a_j \in A$, $i_j \in I$, $x_{i_j} \in \mathfrak{a}_{i_j}$ y $n \in \mathbb{N}$, y se suele representar por $\sum\{\mathfrak{a}_i \mid i \in I\}$.
Si $\mathfrak{a}$ y $\mathfrak{b}$ son dos ideales de A, llamamos **producto** de $\mathfrak{a}$ y $\mathfrak{b}$ al ideal

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \in \mathbb{N} \right\}.$$

Lema. 12.17.
Para un anillo A e ideales $\mathfrak{a}, \mathfrak{b}$ y K de A, se verifica:
(1) $\mathfrak{a}(\mathfrak{b} + K) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}K$.
(2) $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

DEMOSTRACIÓN. Es un fácil ejercicio para el lector aplicado. □

Sea A un anillo, dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ de A se llaman **comaximales** ó **primos relativos** si $\mathfrak{a} + \mathfrak{b} = A$. Para ideales comaximales existen propiedades interesantes que relacionan el producto y la intersección. Veamos dos de estas propiedades.

Lema. 12.18.
Sea A un anillo y $\mathfrak{b}, \mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales de A, si $\mathfrak{b} + \mathfrak{a}_i = A$, $1 \leq i \leq n$, entonces $A = \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{b} + (\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n)$.

DEMOSTRACIÓN. Ya que se verifica $\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$, basta probar que $A = \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Hacemos inducción sobre n. Si $n = 1$ el resultado es cierto. Vamos a ver qué ocurre con $n = 2$, tenemos

$$A = \mathfrak{b} + \mathfrak{a}_1 = \mathfrak{b} + \mathfrak{a}_2,$$

luego existen $a_1, a_2 \in \mathfrak{b}$, $b_1 \in \mathfrak{a}_1$, $b_2 \in \mathfrak{a}_2$ tales que $1 = a_1 + b_1 = a_2 + b_2$, y haciendo el siguiente desarrollo tenemos:

$$1 = a_2 + (a_1 + b_1)b_2 = a_2 + a_1 b_2 + b_1 b_2 \in \mathfrak{b} + \mathfrak{a}_1\mathfrak{a}_2,$$

Supongamos ahora que el resultado es cierto para n, y vamos a probarlo para $n+1$, por hipótesis se verifica:

$$A = \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n, \qquad A = \mathfrak{b} + \mathfrak{a}_{n+1},$$

y aplicando el resultado para el caso $n = 2$ resulta que $A = \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n \mathfrak{a}_{n+1}$, de donde se deduce el enunciado del Lema. □

Proposición. 12.19.
Sea A un anillo e $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales de A tales que $\mathfrak{a}_i + \mathfrak{a}_j = A$, $1 \leq i, j \leq n$, $i \neq j$, entonces $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$.

DEMOSTRACIÓN. Hagamos la demostración por inducción sobre n; para $n = 1$ el resultado es cierto; vamos a probarlo para $n = 2$, resulta que $A = \mathfrak{a}_1 + \mathfrak{a}_2$, luego existen $a_1 \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$ tales que $1 = a_1 + a_2$, entonces para cada $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ se tiene:

$$x = (a_1 + a_2)x = a_1 x + a_2 x \in \mathfrak{a}_1 \mathfrak{a}_2,$$

y por tanto $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1 \mathfrak{a}_2$. Supongamos que el resultado es cierto para n y vamos a probarlo para $n+1$; usando el Lema anterior tenemos que $\mathfrak{a}_{n+1}$ verifica $\mathfrak{a}_{n+1} + \mathfrak{a}_1 \cdots \mathfrak{a}_n = A$, entonces aplicando el resultado para $n = 2$ tenemos:

$$(\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n) \cap \mathfrak{a}_{n+1} = (\mathfrak{a}_1 \cdots \mathfrak{a}_n) \cap \mathfrak{a}_{n+1} = (\mathfrak{a}_1 \cdots \mathfrak{a}_n)\mathfrak{a}_{n+1},$$

y tenemos el resultado. □

Pasamos ahora a estudiar el comportamiento de los ideales ante los homomorfismos de anillos, estudiemos primero la imagen y preimagen de un ideal.

Lema. 12.20.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos, se verifica:

(1) Si $\mathfrak{a}$ es un ideal de A, entonces $f(\mathfrak{a})$ es un ideal de $\mathrm{Im}(f)$.
(2) Si $\mathfrak{b}$ es un ideal de B, entonces $f^{-1}(\mathfrak{b})$ es un ideal de A.

DEMOSTRACIÓN. (1). Es claro que $f(\mathfrak{a})$ es un subgrupo de $\mathrm{Im}(f)$, por otro lado, sean $a \in \mathrm{Im}(f)$ y $x \in f(\mathfrak{a})$, entonces existen $b \in A$ e $y \in \mathfrak{a}$ tales que $f(b) = a$ y $f(y) = x$, y se verifica:

$$ax = f(b)f(y) = f(by),$$

ya que $\mathfrak{a}$ es un ideal deA, resulta que $by \in \mathfrak{a}$, luego $ax = f(by) \in f(\mathfrak{a})$; por lo tanto $f(\mathfrak{a})$ es un ideal de $\mathrm{Im}(f)$.
(2). Tenemos que $f^{-1}(\mathfrak{b})$ es un subgrupo de A, y si $a \in A$ y $x \in f^{-1}(\mathfrak{b})$, entonces se verifica $f(x) \in \mathfrak{b}$, y tenemos:

$$f(ax) = f(a)f(x) \in \mathfrak{b},$$

luego $ax \in f^{-1}(\mathfrak{b})$ y $f^{-1}(\mathfrak{b})$ es un ideal de A. □

Como consecuencia de este Lema tenemos un resultado ya conocido sobre el núcleo de un homomorfismo de anillos.

Corolario. 12.21.
Para cada homomorfismo de anillos $f : A \longrightarrow B$ se tiene que $\mathrm{Ker}(f)$ *es un ideal de A.*

Al igual que en el caso de subanillos, que eran caracterizados como las imágenes de los homomorfismos de anillos, podemos caracterizar los ideales como los núcleos de los homomorfismos de anillos, para ello necesitamos de la siguiente construcción.
Sea A un anillo y $\mathfrak{a} \subseteq A$ un ideal de A, definimos en A una relación, que es de equivalencia, $\equiv_{\mathfrak{a}}$, mediante:

$$r \equiv_{\mathfrak{a}} s \text{ si } r - s \in \mathfrak{a}.$$

También se suele escribir $a \equiv b \pmod{\mathfrak{a}}$.

Teorema. 12.22.
Sea A un anillo y $\mathfrak{a} \subseteq A$ un ideal, existe una única estructura de anillo en $A/\equiv_{\mathfrak{a}}$ de forma que la ***proyección canónica*** *$p : A \longrightarrow A/\equiv_{\mathfrak{a}}$ sea un homomorfismo de anillos.*

DEMOSTRACIÓN. Antes de definir operaciones en $A/\equiv_{\mathfrak{a}}$, vamos a establecer una notación más sencilla, llamaremos al conjunto $A/\equiv_{\mathfrak{a}}$ simplemente $A/\mathfrak{a}$, y la clase del elemento $a \in A$, cuyos elementos son:

$$\{x \in A \mid \ x = a + y,\ y \in \mathfrak{a}\},$$

la representaremos por $a + \mathfrak{a}$. Si pretendemos que la proyección canónica $p : A \longrightarrow A/\mathfrak{a}$ sea un homomorfismo de anillos se debe de verificar:

$$(a + \mathfrak{a}) + (b + \mathfrak{a}) = p(a) + p(b) = p(a + b) = (a + b) + \mathfrak{a},$$

$$(a + \mathfrak{a})(b + \mathfrak{a}) = p(a)p(b) = p(ab) = ab + \mathfrak{a},$$

por lo tanto haremos esta definición para las operaciones en $A/\mathfrak{a}$, tenemos que probar que la definición anterior no depende de los representantes elegidos; sean $a+\mathfrak{a}=a'+\mathfrak{a}$ y $b+\mathfrak{a}=b'+\mathfrak{a}$, entonces tenemos $a-a', b-b'\in\mathfrak{a}$ y se verifica:

$$(a+b)-(a'+b')=(a-a')+(b-b')\in\mathfrak{a},$$

$$ab-a'b'=ab-ab'+ab'-a'b'=a(b-b')+(a-a')b'\in\mathfrak{a}.$$

Finalmente el elemento uno es la clase del uno, $1+\mathfrak{a}$, y $(A/\mathfrak{a},+,\cdot)$ es un anillo. Por la construcción es claro que esta es la única estructura de anillo posible en $A/\mathfrak{a}$ de forma que p sea un homomorfismo de anillos. □

Observación. 12.23.
Dado un anillo A, una relación de equivalencia $\mathscr{R}$ en A se dice **compatible** con la estructura de anillo de A si verifica:

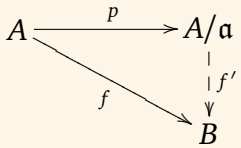
(1) Si $a_1, a_2, b\in A$ y $a_1\mathscr{R}a_2$, entonces $(a_1+b)\mathscr{R}(a_2+b)$.
(2) Si $a_1, a_2\in A$ y $a_1\mathscr{R}a_2$, entonces $(-a_1)\mathscr{R}(-a_2)$.
(3) Si $a_1, a_2, b\in A$ y $a_1\mathscr{R}a_2$, entonces $(a_1b)\mathscr{R}(a_2b)$.

Existe una biyección entre relaciones de equivalencia compatibles con la estructura de anillo en A e ideales de A dada por;

$$\begin{aligned}\mathscr{R} &\Leftrightarrow \overline{0}\\ \mathfrak{a} &\Leftrightarrow \equiv_{\mathfrak{a}}\end{aligned}$$

El anillo $A/\mathfrak{a}$ se llama el **anillo cociente** de A por $\mathfrak{a}$ y está caracterizado por la siguiente propiedad universal.

Teorema. 12.24. (Propiedad universal del anillo cociente)
Sea $\mathfrak{a}$ un ideal de un anillo A, para cada homomorfismo de anillos $f: A\longrightarrow B$ verificando $\mathfrak{a}\subseteq \mathrm{Ker}(f)$, existe un único homomorfismo de anillos $f': A/\mathfrak{a}\longrightarrow B$ tal que $f'p=f$.



DEMOSTRACIÓN. La existencia de f' verificando las condiciones del enunciado fuerza a hacer la siguiente definición:

$$f'(a+\mathfrak{a})=f'(p(a))=f'p(a)=f(a),$$

es necesario entonces comprobar que f', así definida, no depende del representante de la clase $a+\mathfrak{a}$ elegido, y que es un homomorfismo de anillos. Para lo primero supongamos que $a+\mathfrak{a}=a'+\mathfrak{a}$,

entonces se tiene $a-a' \in \mathfrak{a} \subseteq \mathrm{Ker}(f)$, y se verifica $f(a-a')=0$, esto es; $f(a)=f(a')$. Por otro lado, si $a+\mathfrak{a}, b+\mathfrak{a} \in A/\mathfrak{a}$, entonces se tiene:

$$f'((a+\mathfrak{a})+(b+\mathfrak{a})) = f'((a+b)+\mathfrak{a}) = f(a+b) = f(a)+f(b) = f'(a+\mathfrak{a})+f'(b+\mathfrak{a}),$$

$$f'((a+\mathfrak{a})(b+\mathfrak{a})) = f'(ab+\mathfrak{a}) = f(ab) = f(a)f(b) = f'(a+\mathfrak{a})f'(b+\mathfrak{a}),$$

$$f'(1+\mathfrak{a}) = f(1) = 1,$$

luego f' es un homomorfismo de anillos. □

Corolario. 12.25.
En la situación anterior, si f es sobreyectiva, entonces f' también lo es, y si $\mathfrak{a} = \mathrm{Ker}(f)$, entonces f' es inyectiva.

DEMOSTRACIÓN. Si f es sobreyectiva, ya que $f = f'p$, resulta que f' también lo es. Si $\mathfrak{a} = \mathrm{Ker}(f)$, entonces calculando el núcleo de f' tenemos:

$$\mathrm{Ker}(f) = \{a+\mathfrak{a} \in A/\mathfrak{a} \mid\ f'(a+\mathfrak{a})=0\} = \{a+\mathfrak{a} \in A/\mathfrak{a} \mid\ f(a)=0\} =$$

$$\{a+\mathfrak{a} \in A/\mathfrak{a} \mid\ a \in \mathrm{Ker}(f)\} = \{a+\mathfrak{a} \in A/\mathfrak{a} \mid\ a \in \mathfrak{a}\} = \{0+\mathfrak{a}\},$$

luego f' es inyectiva. □

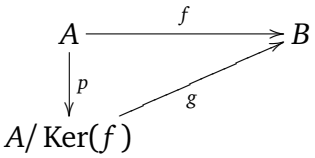
Un homomorfismo de anillos $f : A \longrightarrow B$ se llama un **isomorfismo** si es una aplicación biyectiva; si f es un isomorfismo, entonces existe una aplicación $f^{-1} : B \longrightarrow A$ definida $f^{-1}(b) = a$ tal que $f(a) = b$, como consecuencia $ff^{-1} = 1_B$ y $f^{-1}f = 1_A$, y resulta que f^{-1} es también un homomorfismo de anillos; f^{-1} se llama el **homomorfismo inverso** de f.

Teorema. 12.26. (Primer Teorema de isomorfía)
Sea $f : A \longrightarrow B$ un homomorfismo de anillos, entonces existe un isomorfismo $f' : A/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$ que hace conmutar el diagrama.

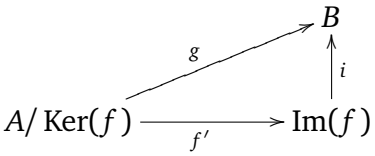
$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ A/\mathrm{Ker}(f) & \xrightarrow{\ f'\ } & \mathrm{Im}(f) \end{array}$$

donde p es la proyección canónica e i es la inclusión.

DEMOSTRACIÓN. Consideramos el homomorfismo $f : A \longrightarrow B$, aplicando la propiedad universal del anillo cociente $A/\operatorname{Ker}(f)$, existe un único homomorfismo de anillos $g : A/\operatorname{Ker}(f) \longrightarrow B$ verificando: $f = gp$,



Ahora consideramos el homomorfismo $g : A/\operatorname{Ker}(f) \longrightarrow B$, aplicando el Corolario (12.25.) g es una aplicación inyectiva; se verifica $\operatorname{Im}(g) = \operatorname{Im}(f)$, y tenemos una factorización de g a través de la imagen de f:



donde i es la inclusión, y f' está definida $f'(a + \operatorname{Ker}(f)) = f(a)$; entonces f' es una biyección, y por tanto un isomorfismo. □

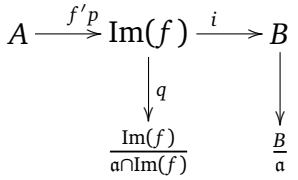
Para representar que f es un isomorfismo de A en B se escribe $f : A \cong B$, y para representar simplemente que existe un isomorfismo de A en B se escribe $A \cong B$.

Corolario. 12.27.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos e $\mathfrak{a}$ un ideal de B, entonces existe un isomorfismo de anillos

$$f' : A/f^{-1}(\mathfrak{a}) \longrightarrow \operatorname{Im}(f)/(\mathfrak{a} \cap \operatorname{Im}(f))$$

definido por $f'(a + f^{-1}(\mathfrak{a})) = f(a) + (\mathfrak{a} \cap \operatorname{Im}(f))$, para cada $a \in A$.

DEMOSTRACIÓN. Consideramos el siguiente diagrama conmutativo de homomorfismos de anillos:



donde seguimos con la notación del Primer Teorema de isomorfía, además q es la proyección canónica. Y podemos considerar la composición $qf'p$ que es sobreyectiva; entonces su imagen es $\frac{\operatorname{Im}(f)}{\mathfrak{a} \cap \operatorname{Im}(f)}$, y para calcular su núcleo basta estudiar cómo está definida; tenemos:

$$qf'p(a) = qf(a) = f(a) + (\mathfrak{a} \cap \operatorname{Im}(f)),$$

por tanto el núcleo es $\{a \in A \mid \ f(a) \in \mathfrak{a} \cap \mathrm{Im}(f)\} = f^{-1}(\mathfrak{a})$. Y aplicando el Primer Teorema de isomorfía tenemos el resultado. □

Teorema. 12.28. (Segundo Teorema de isomorfía)
Sea A un anillo, S un subanillo e $\mathfrak{a}$ un ideal de A, entonces se verifica:

(1) $S+\mathfrak{a}$ es un subanillo de A que contiene a $\mathfrak{a}$ como ideal.
(2) $S \cap \mathfrak{a}$ es un ideal de S.
(3) Existe un isomorfismo $f : \frac{S}{S\cap\mathfrak{a}} \longrightarrow \frac{S+\mathfrak{a}}{\mathfrak{a}}$ definido por $f(s+(S\cap\mathfrak{a})) = s+\mathfrak{a}$, para cada $s \in S$.

DEMOSTRACIÓN. (1). Definimos $S+\mathfrak{a} = \{s+y \mid \ s \in S,\ y \in \mathfrak{a}\}$, entonces vamos a probar que $S+\mathfrak{a}$ es un subanillo de A, para $s_1+y_1, s_2+y_2 \in S+\mathfrak{a}$ se verifica:

$$(s_1+y_1)-(s_2+y_2) = (s_1-s_2)+(y_1-y_2) \in S+\mathfrak{a},$$

$$(s_1+y_1)(s_2+y_2) = s_1s_2+(s_1y_2+y_1s_2+y_1y_2) \in S+\mathfrak{a},$$

finalmente $1 \in S+\mathfrak{a}$, luego tenemos el resultado. Es claro que $\mathfrak{a} \subseteq S+\mathfrak{a}$ es un ideal.
(2). Es claro que para $x, y \in S\cap\mathfrak{a}$ se tiene $x-y \in S\cap\mathfrak{a}$; supongamos que $x \in S\cap\mathfrak{a}$ y $s \in S$, entonces $sx \in S$ ya que los dos factores pertenecen a S, y por estar $S \subseteq A$ y ser $\mathfrak{a}$ un ideal tenemos $sx \in \mathfrak{a}$, luego $sx \in S\cap\mathfrak{a}$ y es un ideal de $S\cap\mathfrak{a}$.

(3). Consideramos la composición de homomorfismos de anillos $S \overset{i}{\hookrightarrow} S+\mathfrak{a} \overset{p}{\longrightarrow} \frac{S+\mathfrak{a}}{\mathfrak{a}}$, donde p es la proyección canónica e i es la inclusión. Los elementos de $\frac{S+\mathfrak{a}}{\mathfrak{a}}$ son de la forma $(s+y)+\mathfrak{a}$ con $s \in S$, $y \in \mathfrak{a}$, por lo tanto se pueden escribir como $s+\mathfrak{a}$, con $s \in S$, y como consecuencia pi es una aplicación sobreyectiva ya que para cada $s \in S$ se verifica $pi(s) = s+\mathfrak{a}$. Vamos ahora a calcular el núcleo de pi, tenemos:

$$\mathrm{Ker}(pi) = \{s \in S \mid \ pi(s) = 0\} = \{s \in S \mid \ s+\mathfrak{a} = 0\} = \{s \in S \mid \ s \in \mathfrak{a}\} = S\cap\mathfrak{a};$$

y aplicando el Primer Teorema de isomorfía resulta que existe un isomorfismo $f : \frac{S}{S\cap\mathfrak{a}} \cong \frac{S+\mathfrak{a}}{\mathfrak{a}}$ definido $f(s+(S\cap\mathfrak{a})) = s+\mathfrak{a}$. □

Teorema. 12.29. (Tercer Teorema de isomorfía)
Sea A un anillo e $\mathfrak{a}$ un ideal de A, se verifica:

(1) Existe una biyección, que conserva el orden, entre los ideales de A que contienen a $\mathfrak{a}$ y los ideales de $A/\mathfrak{a}$, definida por $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$.
(2) Para ideales $\mathfrak{a} \subseteq \mathfrak{b}$ de A se tiene $(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong A/\mathfrak{b}$.

DEMOSTRACIÓN. (1). Supongamos que $\mathfrak{b}$ es un ideal de A verificando $\mathfrak{a} \subseteq \mathfrak{b} \subseteq A$, y sea $p : A \longrightarrow A/\mathfrak{a}$ la proyección canónica, entonces $p(\mathfrak{b})$ es un ideal de $A/\mathfrak{a}$ ya que p es una aplicación sobreyectiva, ver Lema (12.20.). Los elementos de $p(\mathfrak{b})$ son $\{j+\mathfrak{a} \mid j \in \mathfrak{b}\}$, por esta razón se suele representar por $\mathfrak{b}/\mathfrak{a}$; por esta descripción de los elementos de $p(\mathfrak{b})$ se deduce fácilmente que $p^{-1}p(\mathfrak{b}) = \mathfrak{b}$. Sea ahora $\mathfrak{c} \subseteq A/\mathfrak{a}$ un ideal, entonces $p^{-1}(\mathfrak{c})$ es un ideal de A, ver Lema (12.20.), que contiene a $\mathfrak{a}$; se verifica $p(p^{-1}(\mathfrak{c})) = \mathfrak{c}$, entonces las aplicaciones p y p^{-1} establecen una biyección entre los ideales de $A/\mathfrak{a}$ y los ideales de A que contienen a $\mathfrak{a}$, es claro que si $\mathfrak{a} \subseteq \mathfrak{b}_1 \subseteq \mathfrak{b}_2 \subseteq A$, entonces se tiene $p(\mathfrak{b}_1) \subseteq p(\mathfrak{b}_2)$, y por lo tanto esta biyección mantiene el orden.

(2). Supongamos que tenemos ideales $\mathfrak{a} \subseteq \mathfrak{b}$ de A, entonces existe un homomorfismo de anillos $f : A/\mathfrak{a} \longrightarrow A/\mathfrak{b}$ inducido por la propiedad universal del anillo cociente, y definido por $f(a+\mathfrak{a}) = a+\mathfrak{b}$; además este homomorfismo es sobreyectivo; vamos a calcular su núcleo,

$$\mathrm{Ker}(f) = \{a+\mathfrak{a} \in A/\mathfrak{a} \mid f(a+\mathfrak{a}) = 0\} = \{a+\mathfrak{a} \in A/\mathfrak{a} \mid a+\mathfrak{b} = 0\} =$$

$$\{a+\mathfrak{a} \in A/\mathfrak{a} \mid a \in \mathfrak{b}\} = \mathfrak{b}/\mathfrak{a},$$

según la biyección establecida en el apartado (1). □

Sea $\{A_i \mid i \in I\}$ una familia de anillos, consideramos el producto cartesiano $\prod\{A_i \mid i \in I\}$, y las **proyecciones canónicas** $p_j : \prod\{A_i \mid i \in I\} \longrightarrow A_j$, para $j \in I$. Tenemos:

Lema. 12.30.
Existe una única estructura de anillo en $\prod\{A_i \mid i \in I\}$ de forma que las proyecciones canónicas p_j, $j \in I$, sean homomorfismos de anillos.

DEMOSTRACIÓN. Los elementos de $\prod\{A_i \mid i \in I\}$ los representamos por $(a_i)_i$, con $a_i \in A_i$. Si cada p_i es un homomorfismo de anillos resulta que la suma y el producto han de estar definidos componente a componente, y el elemento uno es la *upla* que tiene el elemento uno de cada anillo A_i, como consecuencia las operaciones se deben definir de la siguiente forma:

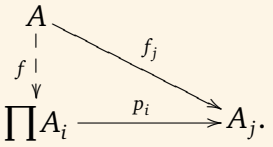
$$(a_i)_i + (b_i)_i = (a_i + b_i)_i,$$

$$(a_i)_i (b_i)_i = (a_i b_i)_i;$$

falta ahora comprobar que con estas operaciones y el elemento uno antes mencionado el producto cartesiano es un anillo, pero esto es inmediato. □

El anillo $\prod\{A_i \mid i \in I\}$ con las operaciones definidas antes se llama **anillo producto** de la familia $\{A_i \mid i \in I\}$.

Teorema. 12.31. (Propiedad universal del anillo producto)
Sea $\{A_i \mid i \in I\}$ una familia de anillos y $\{f_i : A \longrightarrow A_i \mid i \in I\}$, una familia de homomorfismos de anillos, entonces existe un único homomorfismo de anillos $f : A \longrightarrow \prod\{A_i \mid i \in I\}$ tal que $f_j = p_j f$, para cada $j \in I$



DEMOSTRACIÓN. Si f existe verificando las condiciones del enunciado y la imagen de $a \in A$ es $(a_i)_i$, entonces se verifica:

$$a_j = p_j(f(a)) = p_j f(a) = f_j(a),$$

por lo tanto vamos a definir f de esta forma, esto es;

$$f(a) = (f_i(a))_i;$$

así definida f es una aplicación, y es la única que verifica $p_j f = f_j$ para cada $j \in I$. Veamos que es un homomorfismo de anillos y esto acabará la demostración; sean $a, b \in A$, se verifica:

$$f(a+b) = (f_i(a+b))_i = (f_i(a) + f_i(b))_i = (f_i(a))_i + (f_i(b))_i = f(a) + f(b),$$
$$f(ab) = (f_i(ab))_i = (f_i(a)f_i(b))_i = (f_i(a))_i(f_i(b))_i = f(a)f(b),$$
$$f(1) = (f_i(1))_i = (1_i)_i.$$

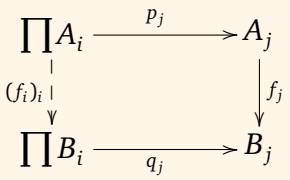
□

Proposición. 12.32.
Sea $\{f_i : A_i \longrightarrow B_i \mid i \in I\}$ una familia de homomorfismos de anillos, y $p_i : \prod A_i \to A_i$, $q_i : \prod B_i \to B_i$ las proyecciones canónicas, entonces existe un único homomorfismo de anillos

$$(f_i)_i : \prod\{A_i \mid i \in I\} \longrightarrow \prod\{B_i \mid i \in I\}$$

que verifica: $q_j(f_i)_i = f_j p_j$ para cada $j \in I$. Además

$$\mathrm{Ker}((f_i)_i) = \prod\{\mathrm{Ker}(f_i) \mid i \in I\}.$$



DEMOSTRACIÓN. Consideramos las composiciones $f_j p_j$, aplicando la propiedad universal del anillo producto, resulta que existe un único homomorfismo de anillos $f : \prod A_i \longrightarrow \prod B_i$ verificando $p_j f = f_j p_j$, este es el homomorfismo que verifica las condiciones del enunciado. Finalmente destacar que para $(a_i)_i \in \prod A_i$ se verifica $f((a_i)_i) = (f_i(a_i))_i$, y que por esta razón a f se suele representar por $(f_i)_i$. Vamos a calcular el núcleo de $(f_i)_i$, tenemos:

$$\begin{aligned}\operatorname{Ker}((f_i)_i) &= \{(a_i)_i \in \textstyle\prod A_i \mid (f_i)_i((a_i)_i) = 0\}\\ &= \{(a_i)_i \in \textstyle\prod A_i \mid (f_i(a_i))_i = 0\}\\ &= \{(a_i)_i \in \textstyle\prod A_i \mid f_i(a_i) = 0 \text{ para cada } i \in I\}\\ &= \{(a_i)_i \in \textstyle\prod A_i \mid a_i \in \operatorname{Ker}(f_i) \text{ para cada } i \in I\}\\ &= \textstyle\prod\{\operatorname{Ker}(f_i) \mid i \in I\}.\end{aligned}$$

□

Lema. 12.33.
Sea $\{A_i \mid i \in I\}$ una familia de anillos y $\{\mathfrak{a}_i \mid i \in I\}$ una familia de ideales con $\mathfrak{a}_i$ ideal de A_i, para cada $i \in I$, se verifica:
(1) $\prod\{\mathfrak{a}_i \mid i \in I\}$ es un ideal de $\prod\{A_i \mid i \in I\}$.
(2) Existe un isomorfismo $\prod\{\frac{A_i}{\mathfrak{a}_i} \mid i \in I\} \cong \dfrac{\prod\{A_i \mid i \in I\}}{\prod\{\mathfrak{a}_i \mid i \in I\}}$.

DEMOSTRACIÓN. Es un fácil ejercicio para el lector. □

Teorema. 12.34. (Teorema chino del resto)
Sea A un anillo e $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales propios de A tales que $\mathfrak{a}_i + \mathfrak{a}_j = A$, para $1 \leq i, j \leq n$, $i \neq j$, entonces el homomorfismo canónico $f : A \longrightarrow \prod\{\frac{R}{\mathfrak{a}_i} \mid 1 \leq i \leq n\}$ es sobreyectivo. Además $\operatorname{Ker}(f) = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.

DEMOSTRACIÓN. El homomorfismo f está inducido por las proyecciones canónicas $p_i : A \longrightarrow \frac{A}{\mathfrak{a}_i}$, por lo tanto está definido:

$$f(a) = (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n), \qquad \text{para todo } a \in A;$$

el cálculo del núcleo es sencillo:

$$\operatorname{Ker}(f) = \{a \in A \mid f(a) = 0\} = \{a \in A \mid a + \mathfrak{a}_i = 0 \quad \forall 1 \leq i \leq n\} =$$

$$\{a \in A \mid \ a \in \mathfrak{a}_i \quad \forall 1 \leq i \leq n\} = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n,$$

donde para la última igualdad hemos aplicado la Proposición (12.19.). Para estudiar la sobreyectividad hacemos inducción sobre n; para $n = 1$ el resultado es cierto; supongamos que sea cierto para n y vamos a probarlo para $n+1$, esto es; tenemos que probar que dados $x_1, \ldots x_{n+1} \in A$, existe $x \in A$ tal que

$$x \equiv x_i \,(\mathrm{mod}\ \mathfrak{a}_i), \quad 1 \leq i \leq n+1;$$

por la hipótesis de inducción resulta que existe $y \in A$ tal que

$$y \equiv x_i \,(\mathrm{mod}\ \mathfrak{a}_i) \quad \text{para } 1 \leq i \leq n;$$

ya que $\mathfrak{a}_{n+1} + \mathfrak{a}_i = A$ para todo $1 \leq i \leq n$, resulta, aplicando el Lema (12.18.) que tenemos la igualdad

$$A = \mathfrak{a}_{n+1} + \mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}_{n+1} + \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n,$$

y por tanto podemos expresar $y - x_{n+1}$ de la siguiente forma:

$$y - x_{n+1} = a + b, \quad \text{con } a \in \mathfrak{a}_{n+1}, b \in \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n,$$

definimos entonces $x = y - b$, vamos a comprobar que x así definido verifica las condiciones del enunciado.

$$x - x_{n+1} = y - b - x_{n+1} = a \in \mathfrak{a}_{n+1},$$
$$x - x_i = y - b - x_i = (y - x_i) - b \in \mathfrak{a}_i, \quad \text{para todo } 1 \leq i \leq n.$$

□

Sea A un anillo, un ideal $\mathfrak{m}$ de R se llama **maximal** en A si es un ideal propio de A, esto es; $\mathfrak{m} \neq A$, y para cada ideal $\mathfrak{b}$ de A verificando $\mathfrak{m} \subseteq \mathfrak{b} \subseteq A$, se tiene $\mathfrak{m} = \mathfrak{b}$ ó $\mathfrak{b} = A$.

Lema. 12.35. (Teorema de Krull)
Sea A un anillo, y $\mathfrak{a}$ un ideal propio, entonces existe un ideal maximal $\mathfrak{m}$ de A tal que $\mathfrak{a} \subseteq \mathfrak{m}$.

DEMOSTRACIÓN. Llamamos Γ al conjunto de todos los ideales propios de A que contienen a $\mathfrak{a}$, esto es;

$$\Gamma = \{\mathfrak{b} \subseteq A \mid \ \mathfrak{b} \text{ es un ideal propio de } A \text{ y } \mathfrak{a} \subseteq \mathfrak{b}\}.$$

La familia Γ es no vacía ya que $\mathfrak{a} \in \Gamma$, además si $\mathfrak{b}_1 \subseteq \mathfrak{b}_2 \subseteq \ldots \subseteq \mathfrak{b}_n \subseteq \ldots$ es una cadena ascendente de elementos de Γ, entonces $\cup \mathfrak{b}_n$ es un ideal propio de A y contiene a $\mathfrak{a}$. Aplicando el Lema de Zorn, en Γ existen elementos maximales, sea $\mathfrak{b} \in \Gamma$ maximal, entonces $\mathfrak{b}$ es un ideal maximal de A y tenemos el resultado. □

Corolario. 12.36.
Todo anillo A contiene al menos un ideal maximal.

DEMOSTRACIÓN. Basta tomar $\mathfrak{a} = 0$ en el Lema anterior. □

Proposición. 12.37.
Sea A un anillo y $\mathfrak{m}$ un ideal de A, son equivalentes:

(a) $\mathfrak{m}$ es un ideal maximal de A.
(b) $A/\mathfrak{m}$ es un cuerpo.

DEMOSTRACIÓN. Supongamos que $\mathfrak{m}$ sea un ideal maximal, y consideremos el cociente $A/\mathfrak{m}$, si $0 \neq a + \mathfrak{m} \in A/\mathfrak{m}$, entonces $a \notin \mathfrak{m}$, y tenemos $(a) + \mathfrak{m} = A$, y como consecuencia existen $r \in A$ y $m \in \mathfrak{m}$ tales que $1 = ar + m$; tomando clases resulta que $1 + \mathfrak{m} = (a + \mathfrak{m})(r + \mathfrak{m})$, y por tanto $A/\mathfrak{m}$ es un cuerpo. Supongamos ahora que $A/\mathfrak{m}$ es un cuerpo, y que existe un ideal $\mathfrak{m} \subset \mathfrak{b} \subseteq A$, entonces para $y \in \mathfrak{b} \setminus \mathfrak{m}$ se verifica que $y + \mathfrak{m}$ es no nulo en $A/\mathfrak{m}$, entonces existe un inverso, $s + \mathfrak{m}$; existe pues $m \in \mathfrak{m}$ tal que $ys + m = 1$, y ya que $\mathfrak{m} \subset \mathfrak{b}$, resulta que $1 = ys + m \in \mathfrak{b}$, esto es; $\mathfrak{b} = A$ por tanto $\mathfrak{m}$ es un ideal maximal. □

Sea A un anillo, un ideal $\mathfrak{p}$ de A se llama **primo** si es un ideal propio y para cualesquiera elementos $a, b \in A$ se tiene que si $ab \in \mathfrak{p}$, entonces $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$.

Lema. 12.38.
Sea A un anillo, todo ideal maximal de A es un ideal primo.

DEMOSTRACIÓN. Sea $\mathfrak{m}$ un ideal maximal de A, y $a, b \in A$ tales que $ab \in \mathfrak{m}$, si $a \notin \mathfrak{m}$ existen $r \in A$ y $m \in \mathfrak{m}$ tales que $ar + m = 1$, y por tanto $b = abr + mb \in \mathfrak{m}$. □

Proposición. 12.39.
Sea A un anillo y $\mathfrak{p}$ un ideal de A, son equivalentes:

(a) $\mathfrak{p}$ es un ideal primo de A.
(b) $A/\mathfrak{p}$ es un dominio de integridad.

DEMOSTRACIÓN. Supongamos que $\mathfrak{p}$ es un ideal primo y sean $0 \neq a+\mathfrak{p}, b+\mathfrak{p} \in A/\mathfrak{p}$, entonces $a, b \notin \mathfrak{p}$ y por tanto $ab \notin \mathfrak{p}$, luego $0 \neq ab+\mathfrak{p} = (a+\mathfrak{p})(b+\mathfrak{p})$, y $A/\mathfrak{p}$ es un dominio de integridad. Supongamos ahora que $A/\mathfrak{p}$ es un dominio de integridad, si para $a, b \in A$ se verifica $ab \in \mathfrak{p}$, entonces en el anillo $A/\mathfrak{p}$ se tiene: $0 = ab+\mathfrak{p} = (a+\mathfrak{p})(b+\mathfrak{p})$, y por tanto $a+\mathfrak{p} = 0$, esto es; $a \in \mathfrak{p}$ ó $b+\mathfrak{p} = 0$, esto es; $b \in \mathfrak{p}$. □

Sea A un dominio de integridad, consideramos el producto cartesiano

$$X = A \times (A \backslash \{0\}),$$

y en X definimos una relación, que es de equivalencia;

$$(a,s) \sim (b,t) \text{ si } at = sb.$$

La clase de (a,s) en $X/\sim$ la notaremos por a/s. Y el conjunto cociente $X/\sim$ lo notaremos por K; los elementos de K se llaman **fracciones**. En K definimos dos operaciones:

$$a/s + b/t = (at+bs)/(st) \text{ y}$$

$$a/s \circ b/t = (ab)/(st).$$

Y una aplicación

$$\rho : A \longrightarrow K \text{ definida } \rho(a) = \frac{a}{1}.$$

Lema. 12.40.
En la situación anterior las operaciones "+" y "∘" no dependen de los representantes elegidos, y $(K,+,\circ)$ *es un anillo con elemento uno igual a* $1/1$. *Además* $\rho : A \longrightarrow K$ *es un homomorfismo de anillos inyectivo.*

DEMOSTRACIÓN. Vamos a comprobar que la definición de las operaciones no dependen de los representantes elegidos; supongamos $a/s = a'/s'$ y $b/t = b'/t'$, entonces tenemos que probar $(at+bs)/(st) = (a't'+b's')/(s't')$ desarrollamos la siguiente expresión:

$$(at+bs)s't' - (a't'+b's')st =$$

$$(ats't' + bss't' - a't'st + b's'st =$$

$$(as'-a's)tt' + (bt'-b't)ss' = 0,$$

luego las dos fracciones son iguales; para probar que $(ab)/(st) = (a'b')/(s't')$ desarrollamos la siguiente expresión:

$$abs't' - a'b'st =$$

$$abs't' - a'sbt' + a'sbt' - a'b'st =$$

$$(as' - a's)bt' + a's(bt' - b't) = 0,$$

luego las dos fracciones son iguales. Probar que $(K, +, \circ)$ es un anillo y que ρ es un homomorfismo inyectivo de anillos es un sencillo pero laborioso ejercicio. □

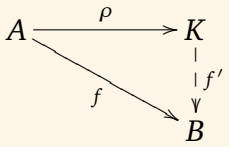
Corolario. 12.41.
En la situación anterior K es un cuerpo.

DEMOSTRACIÓN. Y conocemos que K es un anillo, falta probar únicamente que cada elemento no nulo tiene un inverso; sea $0 \neq a/s \in K$, entonces $a \neq 0$ y por tanto podemos considerar la fracción s/a, es claro entonces que $(a/s)^{-1} = s/a$. □

El cuerpo K se llama el **cuerpo de fracciones** de A. Tenemos pues una descripción de los elementos de K en función de las imágenes de los elementos de A de forma sencilla,

$$a/s = \rho(a)\rho(s)^{-1}.$$

Teorema. 12.42. (Propiedad universal del cuerpo de fracciones)
Sea A un dominio de integridad y $f : A \longrightarrow B$ un homomorfismo de anillos tal que $f(a)$ es invertible en B, si $a \neq 0$, entonces existe un único homomorfismo de anillos $f' : K \longrightarrow B$ tal que $f = f'\rho$



DEMOSTRACIÓN. Al igual que en otros resultados similares, supongamos que existe la aplicación f' verificando las condiciones del enunciado, entonces resulta:

$$f'(a/s) = f'(\rho(a)\rho(s)^{-1}) = f'(\rho(a))f'(\rho(s)^{-1}) =$$
$$f'(\rho(a))f'(\rho(s)^{-1} = f(a)f(s)^{-1}.$$

Entonces hacemos esta definición: $f'(a/s) = f(a)f(s)^{-1}$. Falta demostrar que f' está bien definida y que es un homomorfismo de anillos, evidentemente es el único que verifica las condiciones del enunciado. Sea $a/s = a'/s'$, entonces $as' - a's = 0$, y se verifica $f(a)f(s') - f(a')f(s) = 0$, luego $f(a)f(s)^{-1} = f(a')f(s')$. Probar que f' es un homomorfismo de anillos es hacer un sencillo cálculo. □

Ejemplo. 12.43.
El ejemplo más conocido de cuerpo de fracciones de un dominio de integridad es el cuerpo $\mathbb{Q}$ de los números racionales, que es el cuerpo de fracciones de $\mathbb{Z}$.

Ejercicios

Definición de anillo y morfismo de anillos

Ejercicio. 12.44.
Determinar todos los subanillos e ideales del anillo $\mathbb{Z}$ de los números enteros.
Ref.: 1103e_031 SOLUCIÓN.

Ejercicio. 12.45.
Sean $n\mathbb{Z}$ y $m\mathbb{Z}$ ideales de $\mathbb{Z}$. Determinar su suma, su intersección y su producto.
Ref.: 1103e_032 SOLUCIÓN.

Ejercicio. 12.46.
Si A es un anillo, un homomorfismo de anillos $f : A \longrightarrow A$ se llama un ***endomorfismo*** *de A. Sea A un anillo y $f : A \longrightarrow A$ un endomorfismo, demostrar que*

$$\{a \in A \mid f(a) = a\}$$

es un subanillo de A, se llama el ***subanillo fijo para*** *f.*
Ref.: 1103e_033 SOLUCIÓN.

Ejercicio. 12.47.
Sea A un anillo, demostrar que existe un único homomorfismo de anillos $f_A : \mathbb{Z} \longrightarrow A$. Resulta que $\mathrm{Im}(f_A)$ es el subanillo de A generado por el 1. f_A se llama el ***homomorfismo característico*** *de A.*
Ref.: 1103e_034 SOLUCIÓN.

Ejercicio. 12.48.
Si A es un anillo, llamamos ***característica*** *de A al número entero positivo ó nulo n tal que $n\mathbb{Z} = \mathrm{Ker}(f_A)$, y se representa por* $\mathrm{car}(A)$.

(1) Demuestra que si $\mathrm{car}(A) = n \neq 0$, entonces n es el menor número entero positivo tal que $n \cdot 1 = 0$.
(2) Demuestra que si A es un dominio de integridad, entonces $\mathrm{car}(A) = 0$ ó es un número primo.
(3) ¿Bajo qué condición para las características de dos anillos A y B podemos asegurar que no existe un homomorfismo de anillos de A en B?
(4) Calcula la característica de los siguientes anillos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{Z}_m$.
(5) Demuestra que si S es un subanillo de un anillo A, entonces $\mathrm{car}(S) = \mathrm{car}(A)$.
(6) Si p es un entero primo positivo y A es un anillo de característica p, demuestra que para $a, b \in A$ se verifica $(a+b)^p = a^p + b^p$.
(7) ***Endomorfismo de Frobenius****. Si A es un anillo de característica p, con p entero primo positivo, demuestra que $f : A \longrightarrow A$ definido $f(a) = a^p$ para cada $a \in A$ es un endomorfismo de A.*

Ref.: 1103e_035 *SOLUCIÓN.*

Ejercicio. 12.49.
Consideramos los subanillos de $\mathbb{R}$ siguientes:

$$\mathbb{Z}[\sqrt{2}], \quad \mathbb{Z}[\sqrt{2}, \sqrt{3}], \quad \mathbb{Z}[\sqrt[3]{2}], \quad \mathbb{Z}[\sqrt[5]{3}, \sqrt{2}].$$

(1) Describir los elementos de cada uno de ellos.
(2) ¿Existe algún homomorfismo de anillos de $\mathbb{Z}[\sqrt{2}]$ en $\mathbb{Z}[\sqrt{3}]$? ¿Y de $\mathbb{Z}[\sqrt[3]{2}]$ en $\mathbb{Z}[\sqrt{2}]$?

Ref.: 1103e_036 *SOLUCIÓN.*

Ejercicio. 12.50.
Sea A un anillo, probar que las siguientes condiciones son equivalentes:

(a) A es un cuerpo.
(b) Los únicos ideales de A son el cero y el total.
(c) Todo homomorfismo de anillos $f : A \longrightarrow B$ es inyectivo.

Ref.: 1103e_037 *SOLUCIÓN.*

Ejercicio. 12.51.
Demostrar que si A es un dominio de integridad, entonces se verifica la ***propiedad cancelativa*** *del producto para los elementos no nulos.*
Ref.: 1103e_038 SOLUCIÓN.

Ejercicio. 12.52.
Sea A un anillo, un elemento $a \in A$ se llama ***idempotente*** *si $a^2 = a$. Demuestra que si todos los elementos de un anillo son idempotentes, entonces el anillo tiene característica 2. Demuestra que en un dominio de integridad los únicos elementos idempotentes que existen son el cero y el uno.*
Ref.: 1103e_039 SOLUCIÓN.

Ejercicio. 12.53. (Anillo de Boole de las partes de un conjunto)
Sea X un conjunto no vacío, llamamos A al conjunto de las partes de X, esto es; $A = \mathscr{P}(X)$. En A definimos dos operaciones:

$$A\Delta B = (A \cap B') \cup (A' \cap B),$$
$$A\nabla B = A \cap B,$$

donde A' y B' representan los ***complementos*** *de A y B, respectivamente, en X. Demostrar que (A, Δ, ∇) es un anillo con elemento uno el elemento X.*
Ref.: 1103e_040 SOLUCIÓN.

Ejercicio. 12.54.
Sea A un anillo, un elemento $a \in A$ se llama ***nilpotente*** *si existe un número entero positivo n tal que $a^n = 0$. Demostrar que los elementos nilpotentes de un anillo forman un ideal. Demostrar que en un dominio de integridad el único elemento nilpotente que existe es el cero.*
Ref.: 1103e_041 SOLUCIÓN.

Ejercicio. 12.55.
Demostrar que todo dominio de integridad finito es un cuerpo.
Ref.: 1103e_042 *SOLUCIÓN.*

Ejercicio. 12.56.
Si A es un anillo, un ***automorfismo*** *f de A es un endomorfismo de anillos $f : A \longrightarrow A$ que es un isomorfismo. Sea A un anillo y $u \in A$ un elemento invertible, definimos $f_u : A \longrightarrow A$ mediante $f_u(a) = uau^{-1}$, para cada $a \in A$. Demostrar que f_u es un automorfismo de A.*
Ref.: 1103e_043 *SOLUCIÓN.*

Ejercicio. 12.57.
Determinar para qué valores de m se tiene que $\mathbb{Z}_m$ es un dominio de integridad.
Ref.: 1103e_044 *SOLUCIÓN.*

Ejercicio. 12.58.
Determinar los ideales del anillo $\mathbb{Z}_m$. Dar una representación gráfica de los ideales de los siguientes anillos: $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, y en general de $\mathbb{Z}_{p_1^{e_1}\cdots p_n^{e_n}}$ para $p_1, \ldots, p_n$ enteros primos positivos y $e_1, \ldots, e_n$ enteros positivos.
Ref.: 1103e_045 *SOLUCIÓN.*

Ejercicio. 12.59.
Dados dos números enteros positivos n y m, dar condiciones para que exista un homomorfismo de $\mathbb{Z}_n$ en $\mathbb{Z}_m$.
Ref.: 1103e_046 *SOLUCIÓN.*

Ejercicio. 12.60.
Si A es un anillo de característica no nula m, demostrar que existe un único morfismo de anillos $f : \mathbb{Z}_m \longrightarrow A$, y que este homomorfismo es inyectivo.
Ref.: 1103e_047 *SOLUCIÓN.*

Ejercicio. 12.61.
Demostrar que el anillo $\mathbb{Z}_m$ tiene un elemento nilpotente no nulo si, y sólo si, m es divisible por el cuadrado de un número entero primo. Determinar los elementos nilpotentes de $\mathbb{Z}_m$.
Ref.: 1103e_048 *SOLUCIÓN.*

Ejercicio. 12.62.
Demostrar que los anillos $\mathbb{Z}_{nm}$ y $\mathbb{Z}_n \times \mathbb{Z}_m$ son isomorfos si y sólo si n y m son primos relativos.
Ref.: 1103e_049 *SOLUCIÓN.*

Ejercicio. 12.63.
Demostrar que el producto de dos dominios de integridad no es nunca un dominio de integridad.
Ref.: 1103e_050 *SOLUCIÓN.*

Ejercicio. 12.64.
Sea $\{A_i \mid i \in I\}$ una familia finita de anillos, demostrar que $\mathfrak{a}$ es un ideal del producto $\prod_i A_i$ si, y sólo si, $\mathfrak{a} = \prod_i \mathfrak{a}_i$ para una familia de ideales $\{\mathfrak{a}_i \mid i \in I\}$, donde $\mathfrak{a}_i = p_i(\mathfrak{a})$ para cada $i \in I$.
Ref.: 1103e_051 *SOLUCIÓN.*

Ejercicio. 12.65.
Determinar explícitamente los siguientes isomorfismos de anillos, cuando los haya:
(1) $\mathbb{Z}_{96}/6\mathbb{Z}_{96} \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.
(2) ¿$\mathbb{Z}_{48}/4\mathbb{Z}_{48} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$?

Ref.: 1103e_052 *SOLUCIÓN.*

Ejercicio. 12.66. (Función φ de Euler)
Si A es un anillo, llamamos $\mathcal{U}(A)$ al conjunto de los elementos invertible de A.
(1) Demostrar que $(\mathcal{U}(A), \cdot)$ es un grupo abeliano.

Para cada número entero positivo n definimos

$$\varphi(n) = \text{número de enteros positivos menores que } n \text{ primos relativos con } n.$$

(2) Demostrar que para cada número entero positivo n se verifica $\varphi(n) = Card(\mathcal{U}(\mathbb{Z}_n))$.
(3) Demostrar que si n y m son números enteros positivos primos relativos, entonces se verifica: $\varphi(nm) = \varphi(n)\varphi(m)$.
(4) Demostrar que si p es un número entero primo positivo, entonces para cada entero positivo e se tiene $\varphi(p^e) = p^e - p^{e-1}$.
(5) Demostrar que si $n = p_1^{e_1} \cdots p_r^{e_r}$ para $p_1, \ldots, p_r$ enteros primos positivos y $e_1, \ldots, e_r$ enteros positivos, entonces se verifica:

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Ref.: 1103e_053 *SOLUCIÓN.*

Ejercicio. 12.67. (Ideales primos de $\mathbb{Z}$.)
Estudia los siguientes enunciados:
(1) Demuestra que un ideal $n\mathbb{Z}$ de $\mathbb{Z}$ es primo si, y sólo si, n es cero ó un número entero primo positivo.
(2) Demuestra que en $\mathbb{Z}$ todo ideal primo no nulo es maximal.

Ref.: 1103e_054 *SOLUCIÓN.*

Ejercicio. 12.68.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos.

(1) Si $\mathfrak{p}$ es un ideal primo de B, demostrar que $f^{-1}(\mathfrak{p})$ es un ideal primo de A.
(2) Si f es sobreyectiva y $\mathfrak{m}$ es un ideal maximal de B, demostrar que $f^{-1}(\mathfrak{m})$ es un ideal maximal de A.
(3) Si f es sobreyectiva y $\mathfrak{q}$ es un ideal primo de A tal que $\mathrm{Ker}(f) \subseteq \mathfrak{q}$, demostrar que entonces $f(\mathfrak{q})$ es un ideal primo de B.
(4) Si f es sobreyectiva y $\mathfrak{m}$ es un ideal maximal de A tal que $\mathrm{Ker}(f) \subseteq \mathfrak{m}$, demostrar que entonces $f(\mathfrak{m})$ es un ideal primo de B.
(5) Demostrar que si f es sobreyectiva, entonces existe una correspondencia biyectiva entre los ideales primos (resp. maximales) de A que contienen al núcleo de f y los ideales primos (resp. maximales) de B.

Ref.: 1103e_055 *SOLUCIÓN.*

Ejercicio. 12.69.
Llamemos $G = \mathbb{Z}[i]$ al anillo de los enteros de Gauss, demostrar que es un dominio de integridad y que su cuerpo de fracciones es $\mathbb{Q}[i]$.
Ref.: 1103e_056 *SOLUCIÓN.*

Ejercicio. 12.70.
Describir el cuerpo de fracciones del anillo $\mathbb{Z}[\sqrt{2}]$.
Ref.: 1103e_057 *SOLUCIÓN.*

Ejercicio. 12.71.
La construcción del cuerpo de fracciones se puede extender de la siguiente forma. Sea A un anillo, y sea $\mathbb{S}$ un subconjunto cerrado para el producto y que contiene al uno, esto es; un subconjunto ***multiplicativamente cerrado****. En el producto cartesiano*

$$X = A \times \mathbb{S}$$

definimos una relación de equivalencia

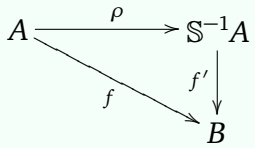
$$(a,s)\sim(b,t)\ si\ \exists u\in\mathbb{S}\ tal\ que\ u(at-sb)=0.$$

La clase de (a,s) *la notamos por* a/s*, y el conjunto cociente* $X/\sim$ *lo notamos por* $\mathbb{S}^{-1}A$*. En* $\mathbb{S}^{-1}A$ *definimos dos operaciones:*

$$a/s+b/t=(at+bs)/st\ y$$

$$a/s\circ b/t=(ab)/(st).$$

Entonces $(\mathbb{S}^{-1}A,+,\circ)$ *es un anillo con elemento uno igual a* $1/1$*. Existe un homomorfismo de anillos* $\rho:A\longrightarrow\mathbb{S}^{-1}A$ *verificando la siguiente propiedad universal: para cada homomorfismo de anillos* $f:A\longrightarrow B$ *tal que* $f(s)$ *es invertible en* B *para cada* $s\in\mathbb{S}$*, existe un único homomorfismo de anillos* $f':\mathbb{S}^{-1}A\longrightarrow B$ *tal que* $f=f'\rho$*.*



Comprobar todas las afirmaciones contenidas en las líneas anteriores. Calcular el núcleo de ρ*.*
Ref.: 1103e_058 SOLUCIÓN.

Ejercicio. 12.72. (Subanillos de $\mathbb{Q}$.)
Tomemos $\mathscr{P}$ *un conjunto de números enteros primos de* $\mathbb{Z}$*, y definimos*

$$\mathbb{P}=\{productos\ finitos\ de\ elementos\ de\ \mathscr{P}\}\cup\{1\},$$

(1) Demostrar que $\mathbb{P}$ *es un subconjunto de* $\mathbb{Z}$ *multiplicativamente cerrado.*
(2) Demostrar que $\mathbb{P}^{-1}\mathbb{Z}$ *es un subanillo de* $\mathbb{Q}$*.*
(3) Demostrar que todo subanillo de $\mathbb{Q}$ *es de esta forma.*
(4) Como consecuencia deducir que $\mathbb{Q}$ *no contiene ningún subanillo propio que sea un cuerpo.*

Ref.: 1103e_059 SOLUCIÓN.

Ejercicio. 12.73.
Demostrar que todo cuerpo de característica cero contiene un subcuerpo isomorfo a $\mathbb{Q}$*.*
Ref.: 1103e_060 SOLUCIÓN.

Ejercicio. 12.74.
Sean $a, b \in A$, con $a \neq 0$ y no divisor de cero. Si $(a) \subseteq A$ es un ideal primo y $(a) \subseteq (b) \subsetneq A$, prueba que $(a) = (b)$.
Ref.: 1103e_061 *SOLUCIÓN.*

Ejercicio. 12.75.
Sea D un dominio de integridad, y $p \in D$. Son equivalentes:
(a) p es irreducible.
(b) $p \neq 0$ y $(p) \subseteq D$ es un ideal maximal en el conjunto de los ideales principales propios de D.

Ref.: 1103e_062 *SOLUCIÓN.*

Ejercicio. 12.76.
Sea D un dominio de integridad y $0 \neq a \in D$ un elemento no invertible.
(1) Si para todo $x \in D$ tal que $a \nmid x$ existen $u, v \in D$ tales que $ua + vx = 1$, entonces a es un elemento primo.
(2) Prueba que esta condición no es equivalente a ser primo.

Ref.: 1103e_063 *SOLUCIÓN.*

Ejercicio. 12.77.
Sea D un DFU y $a_1, \ldots, a_n \in D$ elemento que son primos relativos dos a dos (no nulos y no invertibles).
(1) Si $a_1 \cdots a_n$ es una potencia m–ésima, entonces cada a_i es un elemento asociado a una potencia m–ésima.
(2) ¿Es cada a_i una potencia m–ésima?

Ref.: 1103e_064 *SOLUCIÓN.*

Ejercicio. 12.78.
Sea D un DI. Prueba que son equivalentes:

(a) D es un DFU.
(b) Cada ideal primo no nulo de D contiene un ideal primo no nulo principal.

Ref.: 1103e_023 *SOLUCIÓN.*

Ejercicio. 12.79.
Sea $k \in \mathbb{Z}$ un número entero libre de cuadrados, y definimos $N : \mathbb{Z}[\sqrt{k}] \longrightarrow \mathbb{Z}$ mediante $N(a + b\sqrt{k}) = a^2 - kb^2$. Prueba:

(1) $N(\alpha\beta) = N(\alpha)N(\beta)$ para todos $\alpha, \beta \in \mathbb{Z}[\sqrt{k}]$.
(2) $N(\alpha) = \pm 1$ si y solo si $\alpha \in \mathbb{Z}[\sqrt{k}]$ es invertible.
(3) $\alpha \sim \beta$, son asociados, entonces $N(\alpha) = \pm N(\beta)$, y el recíproco no es cierto en general.
(4) Si $N(\alpha) \in \mathbb{Z}$ es irreducible, entonces $\alpha \in \mathbb{Z}[\sqrt{k}]$ es irreducible, y el recíproco no es cierto en general.

Ref.: 1103e_066 *SOLUCIÓN.*

Ejercicio. 12.80.
Sea D un domino que contiene un cuerpo K tal que $\dim_K(D) < \infty$. Prueba que D es un cuerpo.
Este ejercicio es una extensión de aquel que dice que todo dominio de integridad finito es un cuerpo.
Ref.: 1103e_067 *SOLUCIÓN.*

13. Dominios euclídeos

Divisibilidad

Sea D un dominio de integridad, abreviadamente **DI**, y sean $a, b \in D$, decimos que

(1) a **divide** a b, $a|b$, si existe $c \in D$ tal que $b = ac$. También decimos que b es un **múltiplo** de a ó que a es un **divisor** de b.
(2) Si a no divide a b lo representamos por $a \nmid b$.
(3) a es **invertible** si existe $x \in D$ tal que $ax = 1$. Llamamos $\mathscr{U}(D)$ al conjunto de los elementos invertible de D.

Vamos a reunir en un Lema las principales propiedades de la relación de divisibilidad.

Lema. 13.1.
Si D es un DI, se verifica:

*(1) La relación de divisibilidad es reflexiva y transitiva. Una relación que verifica estas dos propiedades se llama un **preorden** en D.*
(2) Para todo $a \in D$ tenemos que $a|0$.
(3) Si $a \in D$, entonces $0|a$ si, y sólo si, $a = 0$.
(4) Si $u \in D$, entonces $u \in \mathscr{U}(D)$ si, y sólo si, $u|1$.
(5) Si $u \in \mathscr{U}(D)$, entonces $u|a$ para todo $a \in D$.
(6) Si $a \in D$ y $u \in \mathscr{U}(D)$ verifican $a|u$, entonces $a \in \mathscr{U}(D)$.

DEMOSTRACIÓN. (1). Es claro que para cada $a \in D$ se tiene $a = a1$, luego $a|a$; sean ahora $a, b, c \in D$ tales que $a|b$ y $b|c$, entonces existen $e, f \in D$ tales que $b = ae$ y $c = bf$, y por tanto tenemos las igualdades $c = bf = aef$, de donde se deduce que $a|c$.

(2). Es claro, ya que para cada $a \in D$ se verifica $0 = a0$, luego $a|0$.

(3). Si $0|a$, entonces existe $b \in D$ tales que $a = 0b$, y por tanto $a = 0$.

(4). Sea $u \in D$, se verifica $u|1$ si, y sólo si, existe $v \in D$ tal que $1 = uv$, y esto pasa si, y sólo si, u es invertible.

(5). Si $u \in \mathscr{U}(D)$, entonces $u|1$, y como para cada $a \in D$ se tiene $1|a$, resulta que $u|a$.

(6). Si $a|u$ y $u \in \mathscr{U}(D)$, entonces tenemos $u|1$, luego $a|1$, y por tanto es invertible. □

Sean D un DI, y a, b elementos de D. Decimos que a es **asociado** a b si $a|b$ y $b|a$, y lo notamos por $a \sim b$.

Al igual que antes, vamos a reunir en un Lema las propiedades de la relación de asociación.

1103-03.tex

Lema. 13.2.
Sea D un DI, se verifica:
(1) Si $a, b \in D$, entonces $a \sim b$ si, y sólo si, existe $u \in \mathscr{U}(D)$ tal que $a = bu$.
(2) La relación de asociación es una relación de equivalencia.

DEMOSTRACIÓN. (1). Si $a \sim b$, existen $c, d \in D$ tales que $a = bc$ y $b = ad$, deducimos entonces que $a = adc$ y $b = bcd$. Si $a = 0$, entonces $b = 0 = a$; si $a \neq 0$, entonces de $a = adc$ deducimos $1 = dc$, luego d y c son invertibles y tomando $u = c$ tenemos el resultado.
(2). Probar que la relación $\sim$ es de equivalencia es ahora un simple ejercicio. □

Máximo común divisor y mínimo común múltiplo

Vamos a desarrollar en un DI la aritmética que ya hemos visto en el anillo $\mathbb{Z}$. Sea D un DI y $a, b \in D$, llamamos **máximo común divisor** de a y b, y se representa por $\text{mcd}\{a, b\}$ ó (a, b), a un elemento $d \in D$ tal que $d|a$, $d|b$, y si $e \in D$ verifica $e|a$, $e|b$, entonces $e|d$. De la definición se deduce que el mcd no es único, aunque sí existe una cierta unicidad según el siguiente Lema.

Lema. 13.3.
Sea D un DI, y $a, b, d, d' \in D$, se verifica:
(1) Si d y d' son dos mcd *de a y b, entonces $d \sim d'$.*
(2) Si $d = \text{mcd}\{a, b\}$ y $d \sim d'$, entonces $d' = \text{mcd}\{a, b\}$.

DEMOSTRACIÓN. (1). Ya que d y d' son mcd de a y de b, resulta que $d|d'$ y $d'|d$, luego $d \sim d'$.
(2). Si $d \sim d'$, entonces $d'|d$, y por tanto $d'|a$ y $d'|b$; sea ahora $e \in D$ tal que $e|a$ y $e|b$, entonces $e|d$, pero como $d|d'$, resulta que $e|d'$, y por tanto d' es un mcd de a y b. □

Dos elementos $a, b \in D$ se llaman **primos relativos** si su mcd es igual a 1.

Proposición. 13.4.
Sea D un DI, y $a, b, c \in D$, si existen los mcd*, se verifica:*
(1) $(ac, bc) = (a, b)c$.
(2) $((a, b), c) = (a, (b, c))$.
(3) $(a, b) \sim a$ si, y sólo si, $a|b$.

(4) $(a,0)=a$ *y* $(a,1)=1$.
(5) Si $(a,b)=1$ *y* $(a,c)=1$, *entonces* $(a,bc)=1$.
(6) $(a,b)=(a+kb,b)$ *para todo* $k\in D$.
(7) Si $(a,b)=1$, $a|c$ *y* $b|c$, *entonces* $ab|c$.

DEMOSTRACIÓN. (1). Llamamos $d_1=(a,b)$ y $d_2=(ac,ba)$, entonces $d_1c|ac$ y $d_1c|bc$, luego $d_1c|d_2$. Ya que $c|ac$ y $c|bc$, existe e_2 tal que $e_2c=d_2$, entonces $e_2c|ac$ y $e_2c|bc$, luego tenemos $e_2|a$ y $e_2|b$ y por tanto $e_2|d_1$, de donde se deduce que $d_2\sim e_2c|d_1c$.
(2). Llamamos $d_1=(a,b)$, $d_2=((a,b),c)$, $d_3=(b,c)$ y $d_4=(a,(b,c))$; tenemos $d_2|d_1$, luego $d_2|a$, $d_2|b$ y $d_2|c$, entonces $d_2|d_3$ y $d_2|d_4$. Análogamente se tiene $d_4|d_2$, y por tanto $d_2\sim d_4$.
(3). Si $(a,b)\sim a$, entonces $a\sim(a,b)$ y por tanto $a\,|\,b$. Por otro lado, si $a\,|\,b$, entonces $a\,|\,(a,b)$ y $a\sim(a,b)$.
(4). Es claro que $(a,0)=a$, ya que $a|0$. Si $d|(a,1)$, entonces d es invertible y $d\sim 1$.
(5). Si $(a,b)=1$, aplicando (1) tenemos que $(ac,bc)=c$; por otro lado $(a,ac)=a$ por (3); ahora, aplicando (2), tenemos

$$1=(a,c)=(a,(ac,bc))=((a,ac),bc)=(a,bc).$$

(6). Sea $d_1=(a,b)$ y $d_2=(a+bk,b)$, tenemos $d_1|a$ y $d_1|b$, entonces $d_1|d_2$; recíprocamente, $d_2|b$ y $d_2|a+bk$, entonces $d_2|a$ y resulta que $d_2|d_1$, de donde $d_1\sim d_2$.
(7). Si $(a,b)=1$, entonces $(ac,bc)=c$. Por otro lado, si $a|c$, entonces $a=(a,c)$, luego $ab=(ab,cb)$ y $ab|cb$; de la misma forma $ab|ac$, luego $ab|(ac,cb)=c$. □

La apostilla "*si existen los* mcd" es necesario hacerla, ya que en un DI no siempre existe el mcd de dos elementos.
Sea D un DI, y $a,b\in D$, llamamos **mínimo común múltiplo** de a y b, y se representa por $\text{mcm}\{a,b\}$ ó $[a,b]$, a un elemento $m\in D$ tal que $a|m$, $b|m$, y si $n\in D$ verifica $a|n$, $b|n$, entonces $m|n$. De la definición se deduce que el mcm no es único, aunque sí existe una cierta unicidad según el siguiente Lema cuya demostración es análoga a la realizada en el caso del mcd.

Lema. 13.5.
Sea D *un DI, y* $a,b,m,m'\in D$, *se verifica:*
(1) Si m *y* m' *son* mcm *de* a *y* b, *entonces* $m\sim m'$.
(2) Si $m=\text{mcm}\{a,b\}$ *y* $m\sim m'$, *entonces* $m'=\text{mcm}\{a,b\}$.

Resultados análogos, salvo (5) y (6) de la Proposición (13.4.), se verifican para el mcm. La apostilla "*si existen los* mcm" es necesario hacerla, ya que en un DI no siempre existe el mcm de dos elementos. También puede ocurrir que exista el mcd y no exista el mcm.

Proposición. 13.6.
Sea D un DI, y $a, b, c \in D$, si existen los mcm*, se verifica:*
(1) $[ac, bc] = [a, b]c$.
(2) $[[a, b], c] = [a, [b, c]]$.
(3) $[a, b] \sim a$ *si, y sólo si,* $b|a$.
(4) $[a, 0] = 0$.

Ejemplos. 13.7.
(1) En el anillo $\mathbb{Z}[\sqrt{-5}]$ los elementos $2(1+\sqrt{-5})$ y 6 no tienen mcd, ya que 2 y $1+\sqrt{-5}$ son divisores comunes y no existe otro divisor común que sea múltiplo de 2 y $1+\sqrt{-5}$.
(2) Consideramos el anillo $\mathbb{Z}[\sqrt{-5}]$, los elementos $1+\sqrt{-5}$ y 2 tienen mcd igual a 1, y no tienen mcm.

En cambio la existencia de mcm implica la existencia de mcd como prueba el siguiente Lema.

Lema. 13.8.
Sea D un DI, y $0 \neq a, b \in D$, si existe el mcm *de a y b, $m = [a, b]$, entonces $m \neq 0$ y $d = \frac{ab}{m}$ es un* mcd *de a y b.*
En particular, si existe $[a, b]$, se verifica: $(a, b)[a, b] = ab$.

DEMOSTRACIÓN. Ya que tenemos $ab \neq 0$ y $m|ab$, se tiene $m \neq 0$ y existe $x \in D$ tal que $ab = xm$; ya que $a|m$ y $b|m$, existen $a', b' \in D$ tales que $aa' = m = bb'$; desarrollando ahora la expresión de ab tenemos:

$$ab = xm = xaa', \qquad ab = xm = xbb',$$

simplificando tenemos las siguientes expresiones de a y b:

$$b = xa', \qquad a = xb',$$

luego $x|a$ y $x|b$. Supongamos que existe $e \in D$ tal que $e|a$ y $e|b$, entonces existen $a'', b'' \in D$ tales que $a = ea''$ y $b = eb''$; definimos $m' = \frac{ab}{e}$, entonces $m' = a''b = b''a$, de donde se deduce que $a|m'$ y $b|m'$, se tiene pues $m|m'$, luego existe $m'' \in D$ tal que $m' = mm''$; sustituyendo estos valores en la expresión de ab resulta:

$$xm = ab = m'e = mm''e,$$

y simplificando por m resulta $x = m''e$, de donde se deduce que $e \mid x$ y que x es un mcd de a y b. □

Un DI verifica la **condición MDC**, o es un **GCD–dominio**, si cada par de elemento de D tiene un mcd.

Dominio de factorización única

Sea D un DI,

(1) Un elemento $a \in D$ se llama **divisor propio** ó un **factor propio** de un elemento $b \in D$ si a no es invertible, $a|b$ y $b \nmid a$.
(2) Un elemento $a \in D$ se llama **irreducible** en D si no es cero ni invertible y no tiene divisores propios.

Lema. 13.9.
Sea D un DI, se verifica:

(1) Para todo $u \in D$, si $u \in \mathcal{U}(D)$ entonces u no tiene divisores propios.
(2) Si $a \in D$ es un elemento irreducible, y $b \in D$ verifica $b \sim a$, entonces b es irreducible.
(3) Si $a \in D$ es invertible y $b \in D$ verifica $a \sim b$, entonces b es invertible.

DEMOSTRACIÓN. (1). Si $u \in \mathcal{U}(D)$, los únicos divisores de u son invertibles, por tanto no tiene divisores propios.

(2). Si $a \sim b$, tenemos que a y b tienen los mismos divisores. Por otro lado, c es un divisor propio de a, también c es un divisor propio de b. Por tanto a es irreducible si, y sólo si, lo es b.

(3). Si a es invertible, entonces $a|1$, y si $a \sim b$, entonces $b|a$; combinando los dos resultados tenemos $b|1$, y b es invertible. □

Sea D un DI, llamamos

(1) D^* al conjunto $D \setminus \{0\}$.
(2) Un elemento $a \in D^* \setminus \mathcal{U}(D)$ tiene una **factorización en elementos irreducibles** si existen elementos irreducibles $p_1, \ldots, p_n \in D$ tales que $a = p_1 \cdots p_n$.
(3) Un DI en el que todo elemento no nulo y no invertible tiene una factorización en elementos irreducibles se llama un **dominio atómico**.
(4) Dos factorizaciones en elementos irreducibles de $a \in D^* \setminus \mathcal{U}(D)$, $a = p_1 \cdots p_n = q_1 \cdots q_m$, se llaman **esencialmente iguales** si $n = m$ y existe $\sigma \in S_n$ tal que $q_i \sim p_{\sigma}(i)$, $1 \leq i \leq n$.
(5) Un elemento $a \in D^* \setminus \mathcal{U}(D)$ tiene una **factorización única en elementos irreducibles** si tiene una factorización en elementos irreducibles y cada dos factorizaciones en elementos irreducibles son esencialmente iguales.
(6) Un DI es un **dominio de factorización única**, abreviadamente **DFU**, si cada elemento no nulo y no invertible, tiene una factorización única en elementos irreducibles.

Ejemplos. 13.10.
(1) Todo cuerpo es un DFU.
(2) No todo DI es un DFU. Es claro que el anillo $\mathbb{Z}[\sqrt{-5}]$ es un DI ya que está contenido en el cuerpo $\mathbb{C}$, sin embargo el elemento 6 tiene dos descomposiciones en elementos irreducibles que no son esencialmente iguales:

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3.$$

Igual ocurre para las siguientes factorizaciones de 9,

$$9 = (2+\sqrt{-5})(2-\sqrt{-5}) = 3\times 3.$$

(3) El anillo $\mathbb{Z}[\sqrt{-6}]$ es un DI y no es un DFU. (Estudiar distintas descomposiciones del elemento $6 \in \mathbb{Z}[\sqrt{-6}]$.)

Sea D un DI, un elemento $p \in D$ se llama **primo** si p no es cero ni invertible y verifica, para cualquier par de elementos $a, b \in D$, que si $p|ab$, entonces $p|a$ ó $p|b$.

Ejercicio. 13.11.
Sea D un DI y $0 \neq a \in D$, demostrar que a es un elemento primo de D si, y sólo si, el ideal (a) de D es un ideal primo no nulo.

Lema. 13.12.
En un DI todo elemento primo es irreducible.

DEMOSTRACIÓN. Supongamos que $p \in D$ es primo, y que a un factor propio de p, entonces existe $b \in D$ tal que $p = ab$ y b no es invertible. Ya que p es primo, ha de dividir a uno de los factores, pero $p \nmid a$, luego necesariamente $p \mid b$ y por tanto $p \sim b$, esto es; a es invertible, lo que es una contradicción. □

El recíproco de este resultado no es cierto en general como prueba el Ejemplo (2) de (13.10.), ya que $2\,|\,(1+\sqrt{-5})(1-\sqrt{-5})$, y sin embargo $2 \nmid (1+\sqrt{-5})$ ni $2 \nmid (1-\sqrt{-5})$. Sin embargo existen anillos en los que los conceptos de elemento irreducible y elemento primo coinciden.

Teorema. 13.13. (Condición de primo, CP)
En un DFU todo elemento irreducible es primo.

DEMOSTRACIÓN. Sea $p \in D$ un elemento irreducible de un DFU, y supongamos que $p \mid ab$, para algunos $a, b \in D$; si $a \in \mathscr{U}(D)$, entonces $b \sim p$ y $p|b$; análogamente ocurre si $b \in \mathscr{U}(D)$. Supongamos ahora que $a, b \notin \mathscr{U}(D)$, entonces existen factorizaciones en elementos irreducibles de a y de b, supongamos que

$$a = p_1 \cdots p_r, \qquad \text{y} \qquad b = q_1 \cdots q_s,$$

ya que $p\,|\,ab$, existe $c \in D$ tal que $ab = pc$, y sustituyendo los valores de a y b en esta expresión tenemos las siguientes igualdades:

$$(p_1 \cdots p_r)(q_1 \cdots q_s) = ab = pc,$$

por la unicidad de la descomposición existe $i \in \{1,\dots,r\}$ ó $j \in \{1,\dots,s\}$ tal que $p \sim p_i$ ó $p \sim q_j$, esto es; $p|a$ ó $p|b$, y por tanto p es un elemento primo de D. □

Ya que todo elemento irreducible es primo, podemos dar una caracterización de DFU atendiendo a elementos primos.

Proposición. 13.14.
Sea D un dominio de integridad, son equivalentes:
(a) D es un DFU.
(b) Cada elemento no nulo y no invertible tiene una factorización en elementos primos.

DEMOSTRACIÓN. (b) ⇒ (a). Dado un elemento no nulo y no invertible a con factorización en primos $a = p_1 \cdots p_n$, tenemos que probar que ésta es única. Si existe otra $a = q_1 \cdots q_m$, como $p_1 \cdots p_n = q_1 \cdots q_m$, se tiene que $p_1 | q_1 \cdots q_m$, y existe q_j tal que $p_1 | q_j$, como ambos son primos, son irreducibles, y se tiene $p_1 \sim q_j$, supongamos que $q_j = q_1$; simplificando por p_1 se tiene $p_2 \cdots p_n = q_2 \cdots q_m$. Por inducción sobre la longitud de la factorización tenemos el resultado. □

Tenemos también la siguiente caracterización de DFU.

Proposición. 13.15. ([13, Theorem 5])
Sea D un dominio de integridad, los siguientes enunciados son equivalentes:
(a) D es un DFU.
(b) Cada ideal primo no nulo contiene elemento primo.
(c) Cada ideal primo no nulo está generado por elementos primos.

DEMOSTRACIÓN. (a) ⇒ (b). Dado un ideal primo no nulo $\mathfrak{p}$, para $0 \neq a \in \mathfrak{p}$ existe un factor primo de a que pertenece a $\mathfrak{p}$.
(b) ⇒ (a). Si cada ideal primo no nulo contiene un elemento primo, llamamos

$$H = \{\text{productos de elementos primos}\}.$$

Si existe un elemento no nulo y no invertible a tal que $a \notin H$, como H es un conjunto multiplicativo saturado, su complemento es una unión de ideales primos, sea $D \setminus H = \cup_i \mathfrak{p}_i$. Como $a \in D \setminus H$, existe un ideal primo p_i tal que $a \in \mathfrak{p}_i$. Como $\mathfrak{p}_i \cap H = \emptyset$, se tiene que existe un elemento primo en $\mathfrak{p}_i$ que no pertenece a H, lo que es una contradicción.
(a) ⇒ (c). Dado un ideal primo $0 \neq \mathfrak{p} \subseteq D$, si $\{a_i \mid i \in I\}$ es un sistema de generadores, para cada a_i tenemos una factorización en elementos primos: $a_i = p_{i1} \cdots p_{in}$, por tanto uno de los factores, sea

p_{ij}, pertenece a $\mathfrak{p}$; podemos sustituir a_i por p_{ij} y tenemos un sistema de generadores formado por elementos primos. □

Un dominio de integridad D verifica la **condición de cadena de divisores**, abreviadamente **CCD**, o equivalentemente la **condición de cadena ascendente para ideales principales**, abreviadamente **CCAP**, si no existe una sucesión infinita $a_0, a_1, \ldots$ tal que $a_{i+1}|a_i$ para cada índice $i \geq 1$, o equivalentemente, no existe una cadena ascendente estricta de ideales principales $(a_0) \subset (a_1) \subset (a_2) \subset \cdots$

Ejercicio. 13.16.
Si D es un DI son equivalentes:
(1) D verifica la CCAP.
(2) Cada conjunto no vacío de ideales principales tiene un elemento maximal.

SOLUCIÓN. (b) $\Rightarrow$ (c). Es evidente.
(a) $\Rightarrow$ (b). Dado un conjunto no vacío de ideales principales, Γ, tomamos un elemento $(a_1) \in \Gamma$.. Si (a_1) no es maximal, existe $(a_2) \in \Gamma$ tal que $(a_1) \subsetneq (a_2)$. Siguiendo el proceso construimos una cadena estrictamente ascendente de ideals principales, lo que es una contradicción. □

Ejercicio. 13.17.
Si D es un DI, para un elemento no nulo y no invertible $a \in D$ son equivalentes:
(a) a es irreducible.
(b) (a) es un ideal maximal en el conjunto de los ideales principales propios no nulos.

SOLUCIÓN. (a) $\Rightarrow$ (b). Si a es irreducible, tenemos $0 \neq (a) \subsetneq D$. Si existe un ideal principal $(a) \subseteq (b) \subsetneq D$, existe $c \in D$ tal que $a = bc$; como b no es invertible, se tiene que c lo es, y por tanto $(a) = (b)$.
(b) $\Rightarrow$ (a). Supongamos que (a) es maximal en el conjunto de los ideales principales propios no nulos. Si $a = bc$, y b no es invertible, entonces $(a) \subseteq (b) \subsetneq D$, por tanto $(a) = (b)$, y c es invertible. □

Ejercicio. 13.18.
Sea D un DI. Si D verifica la CCD, entonces cada elemento no nulo y no invertible tiene una factorización en irreducibles.

SOLUCIÓN. Sea $0 \neq a \in D$ no invertible, si a no es irreducible, tiene una factorización propia: $a = a_1 b_1$. Si a_1 no es irreducible, existe una factorización propia: $a_1 = a_2 b_2$, etc. Si en el proceso no encontramos un factor irreducible, tenemos una sucesión infinita $a_0 = a, a_1, a_2, \ldots$, con $a_{i+1} | a_i$, para $i \geq 1$, lo que contradice la CCD. □

Proposición. 13.19.
Todo DFU verifica la CCD.

DEMOSTRACIÓN. Dada una sucesión de divisores $a_0, a_1, \ldots$, se tiene $a_{i+1} \mid a_i$, por tanto a_{i+1} tiene como factores a $a_0, a_1, \ldots, a_i$. Si $a_j \nmid a_{j+1}$, para $j = 0, 1, \ldots$, llegamos a una contradicción con el número de posibles factores no asociados. □

Ejercicio. 13.20.
Si D es un dominio que verifica la CCD, entonces $D[X]$ verifica la CCD.

SOLUCIÓN. Dada una cadena ascendente de ideales principales $(F_1) \subseteq (F_2) \subseteq \cdots$. Se tiene $F_{i+1} | F_i$, y por tanto $\operatorname{grad}(F_{i+1}) \leq \operatorname{grad}(F_i) \leq \operatorname{grad}(F_1)$, para cada $i \geq 1$. Existe un índice n tal que $\operatorname{grad}(F_n) = \operatorname{grad}(F_{n+1}) = \cdots$, y como $F_{i+1} \mid F_i$ para $i \geq n$, existe $a_i \in D$ tal que $F_i = a_i F_{i+1}$, y tenemos una cadena de ideales principales $(\operatorname{lc}(F_n)) \subseteq (\operatorname{lc}(F_{n+1})) \subseteq \cdots$, que por hipótesis estabiliza. Por tanto existe $m \geq n$ tal que $(\operatorname{lc}(F_m)) \subseteq (\operatorname{lc}(F_{m+1})) \subseteq \cdots$, y se tiene $\operatorname{lc}(F_i) \sim \operatorname{lc}(F_{i+1})$ para $i \geq m$. En particular, ya que $\operatorname{lc}(F_i) = a_i \operatorname{lc}(F_{i+1})$, se tiene que a_i es invertible para $i \geq m$, y por tanto $(F_m) = (F_{m+1}) = \cdots$ estabiliza. □

Teorema. 13.21.
Sea D in DI, son equivalentes:

(a) D es un DFU.
(b) D verifica la CCD y la CP.

DEMOSTRACIÓN. Es claro que (a) ⇒ (b).
(b) ⇒ (a). Dado $0 \neq a \in D$ no invertible, si a no es irreducible, existe una factorización $a = a_a b_1$. Si a_1 no es irreducible, existe una factorización $a_1 = a_2 b_2$, etc. No en este proceso no se encuentra un elemento irreducible a_i, tenemos una sucesión infinita de divisores $a_1, a_2, \ldots$, lo que es una contradicción. Por tanto cada elemento no nulo y no invertible tiene un factor irreducible.

Dado $0 \neq a \in D$ no invertible, existe una factorización $a = p_1 b_1$, con p_1 irreducible, si b_1 no es irreducible, existe una factorización $b_1 = p_2 b_2$, etc. Si en este proceso no se encuentra un b_i irreducible, tenemos una sucesión infinita de divisores $b_1, b_2, \ldots$, lo que es una contradicción. Por tanto todo elemento no nulo y no invertible es un producto de irreducibles.

Dado $0 \neq a \in D$, si a tiene dos factorizaciones $a = p_1 \cdots p_t = q_1 \cdots q_s$, la demostración en el Teorema (13.34.) prueba que $t = s$ y que, salvo una permutación, los $p_i's$ y los $q_i's$ son los mismos. □

Lema. 13.22. (Criterio de Nagata)
Sea D una dominio de integridad, $\mathcal{N}$ el conjunto de los productos de elementos primos de D y $x \in D$ un elemento irreducible. Se verifica:

(1) $\mathcal{N} \subseteq D$ es un subconjunto multiplicativo.
(2) $x/1 \in \mathcal{N}^{-1}D$ es irreducible ó invertible.
(3) $x \in D$ es primo si, y solo si, $x/1 \in \mathcal{N}^{-1}D$ es invertible ó primo.

DEMOSTRACIÓN. (1). Es inmediato.

(2). Si existe una factorización propia $x/1 = (a/s)(b/s)$, entonces $xs = ab$. Si $s = p_1 \cdots p_t$, se tiene $ab = xp_1 \cdots p_t$, y cada p_i divide a a ó a b, simplificando se tiene $a'b' = x$, con a' un divisor de a y b' un divisor de b. Como x es irreducible entonces a' ó b' es invertible. Si a' es invertible, entonces a/s es invertible.

(3). ($\Rightarrow$). Si x es primo, entonces D/xD es un dominio, y $\mathcal{N}^{-1}D/x\mathcal{N}^{-1}D = \mathcal{N}^{-1}(D/xD)$ es un dominio ó es cero. En el prime caso $x/1$ es invertible, y en el segundo $x/1$ es invertible.

($\Leftarrow$). Si $x/1$ es invertible, existen $a \in D$, $s \in \mathcal{N}$ tales que $ax = s = p_1 \cdots p_t$. Si existe p_i tal que $p_i | x$, entonces x es primo; en caso contrario, $p_1 \cdots p_t | a$, y x es invertible, lo que es una contradicción.

Si $x/1$ es primo y $x|ab$, entonces $x/1|(a/1)(b/1)$, y se tiene $x/1|a/1$ ó $x/1|b/1$. En el primer caso existen $a' \in D$ y $s \in \mathcal{N}$ tales que $xa' = as = ap_1 \cdots p_t$. Si existe p_i tal que $p_i | x$, entonces x es primo; en caso contrario, $p_1 \cdots p_t | a'$, y existe $a'' \in D$ tal que $xa'' = a$, por tanto $x|a$. □

Corolario. 13.23. (Criterio de Nagata para DFU)
Con la notación anterior. Si D es un dominio de integridad, son equivalentes:

(a) D es un DFU.
(b) Cada elemento no nulo no invertible tiene una factorización en irreducibles y $\mathcal{N}^{-1}D$ es un DFU.

DEMOSTRACIÓN. (b) $\Rightarrow$ (a). Si $\mathcal{N}^{-1}D$ es un DFU, cada elemento irreducible $x \in D$ es primo, y se tiene el resultado. □

Ejercicio. 13.24.
Si D es un DFU, para cada subconjunto multiplicativo Σ, ($0 \notin \Sigma$) se tiene que $\Sigma^{-1}D$ es un DFU.

DEMOSTRACIÓN. [Uno] Dado un subconjunto multiplicativo $\Sigma \subseteq D$, definimos

$$\Sigma_1 = \{p \mid p \text{ es irreducible y un factor de un elemento de } \Sigma\},$$
$$\Sigma_2 = \{p \mid p \text{ es irreducible y } p \notin \Sigma_1\}.$$

Tenemos los siguientes hechos:

(1) $p \in \Sigma_1$ si, y sólo si, $p/1 \in \Sigma^{-1}D$ es invertible.

($\Rightarrow$). Es claro.

($\Leftarrow$). Si $(p/1)(a/s) = 1$, se tiene $pa = s \in \Sigma$, luego $p \in \Sigma_1$.

(2) Si $p \in \sigma_2$, entonces $p/1 \in \Sigma^{-1}D$ es irreducible.

Si $p/1 = (a/s)(b/s)$, se tiene $ps = ab$, y por tanto p ó divide a a ó divide a b. Si $p|a$, los factores irreducibles de b son de Σ_1, y por tanto b/s es invertible.

(3) $\Sigma^{-1}D$ es atómico (cada elemento no nulo y no invertibles es un producto de irreducibles).

Dado $a/1 \in \Sigma^{-1}D$ no nulo y no invertible, se tiene $a = p_1 \cdots p_n q_1 \cdots q_m$, con $p_i \in \Sigma_1$ y $q_j \in \Sigma_2$, entonces $a/1 = (p_1/1)\cdots(p_n/1)(q_1/1)\cdots(q_m/1)$ es una factorización en irreducibles.

(4) Cada elemento irreducible de $\Sigma^{-1}D$ es de la forma $u(q/1)$, con $u \in \Sigma^{-1}D$ invertible y $q \in \Sigma_2$.

Si a/s es irreducible, y $a = p_1 \cdots p_n q_1 \cdots q_m$, entonces $a/s = (p_1/s)(p_2/1)\cdots(p_n/1)(q_1/1)\cdots(q_m/1)$, y por tanto $m = 1$.

(5) Las factorizaciones en irreducibles son únicas.

Dadas dos factorizaciones $u(q_1/1)\cdots(q_m/1) = u'(q'_1/1)\cdots(q'_t/1)$, se tiene $q_1 \cdots q_m s_1 = q'_1 \cdots q'_t$, con $s_1, s_2 \in \Sigma$. Por ser D un DFU, se tiene $q_1 \cdots q_m \sim q'_1 \cdots q'_t$, y por tanto la factorización es única.

□

DEMOSTRACIÓN. [Dos] Aplicamos que D es un DFU si, y sólo si, cada ideal primo no nulo contiene un elemento primo (Teorema de Kaplansky). Dado un ideal primo no nulo $\mathfrak{P} \subseteq \Sigma^{-1}D$, existe un ideal primo $\mathfrak{p} \subseteq D$ tal que $\mathfrak{p} \cap \Sigma = \varnothing$, y $\mathfrak{p}\Sigma^{-1}D = \mathfrak{P}$. Por la hipótesis existe un elemento primo $p \in \mathfrak{p}$. Falta probar que $p/1 \in \Sigma^{-1}D$ es primo. Si $p/1 \mid (a/s)(b/s)$, existe c/t tal que $(p/1)(c/t) = (a/s)(b/s)$, luego $ps^2c = abt$, como $p \nmid t$, se tiene $p \mid a$ ó $p \mid b$. Si $p \mid a$, existe $d \in D$ tal que $a = dp$, se tiene entonces $a/s = (p/1)(d/s)$. □

Ejercicio. 13.25.
Si K es un cuerpo, el anillo $[X, X^{-1}]$ es un DFU.

SOLUCIÓN. Si K es un cuerpo, entonces $K[X]$ es un DFU, y $K[X,X^{-1}]$, que es una localización de $K[X]$, es un DFU. □

Teorema. 13.26. (Condición máximo común divisor, MCD)
Si D es un DFU entonces cada par de elementos de D tiene un mcd *y un* mcm.

DEMOSTRACIÓN. Consideramos la relación de asociación en el conjunto de los elementos irreducibles de D, y una familia de representantes de las clases de equivalencia, llamémosla $\mathscr{P}$, entonces cada elemento a de D no nulo, que no es invertible, admite una expresión única en la forma:

$$a = up_1^{e_1} \cdots p_r^{e_r},$$

donde $u \in \mathscr{U}(D)$, $p_1, \ldots, p_r \in \mathscr{P}$ son elementos irreducibles distintos, $e_1, \ldots, e_r$ y r son números enteros positivos. Entonces el mcd y el mcm de un par de elementos de D existen, y se pueden describir fácilmente atendiendo a sus factorizaciones. □

Lema. 13.27.
Todo dominio de integridad D que verifica la condición MCD también verifica la CP.

DEMOSTRACIÓN. Si p es irreducible, para cada $0 \neq a \in D$ se tiene $\mathrm{mcd}\{p,a\} = 1$. Dados $a, b \in D$ tales que $\mathrm{mcd}\{p,a\} = 1 = \mathrm{mcd}\{p,b\}$, entonces $\mathrm{mcd}\{ab,p\} = 1$, por tanto p es primo. □

Como consecuencia tenemos:

Teorema. 13.28.
Sea D in DI, son equivalentes:
(a) D es un DFU.
(b) D verifica la CCD y la MCD.

Ejercicio. 13.29.
Si D es un DFU y $\mathfrak{p} = pD$ un ideal primo, no existen ideales primos $\mathfrak{q}$ tales que $0 \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{p}$.

SOLUCIÓN. Supongamos que existe un ideal primo $\mathfrak{q}$ verificando la condición, para $0 \neq x \in \mathfrak{q}$ existe $x_1 \in D$ tal que $x = tx_1$. Por ser $\mathfrak{q}$ primo, se tiene $x_1 \in \mathfrak{q}$, y existe x_2 tal que $x_1 = tx_2$, por tanto $x = t^2x_2$, y $x_2 \in \mathfrak{q}$. Por tanto, para cada $n \in \mathbb{N}$ existe $x_n \in \mathfrak{q}$ tal que $x = t^n x_n$, lo que es imposible en un DFU. □

Ejercicio. 13.30.
Sea D un DFU, para cada elemento primo $p \in D$ se tiene que $D_{(p)}$ es un dominio de valoración discreta.

SOLUCIÓN. Dado $p \in D$, se tiene que $pD = \mathfrak{p}$ es un ideal primo de altura 1, esto es, no existen ideales primos $0 \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{p}$. Como consecuencia, $D_{(p)}$ es un anillo de dimensión 1; es un DFU, y cada ideal no nulo es maximal, por tanto $D_{(p)}$ es un DIP, por tanto noetheriano, y sus ideales son las potencias de $pD_{(p)}$. □

Dominio de ideales principales

Aunque los DFU se pueden caracterizar a partir de la propiedad de que cada par de elementos tiene un mcd, no vamos a continuar por este camino, sino que vamos a introducir nuevas clases de anillos y probaremos que están contenidas en la clase de los DFU. La primera está formada por los anillos en los que todos los ideales son principales.

Si D es un DI, decimos que D es un **dominio de ideales principales**, abreviadamente **DIP**, si todo ideal de D es principal. Veamos las propiedades elementales de los DIP y que todo DIP es un DFU.

Lema. 13.31.
En un DIP cada elemento irreducible genera un ideal maximal.

DEMOSTRACIÓN. Supongamos que D es un DIP y que $p \in D$ es irreducible; ya que p no es invertible, tenemos que (p) es un ideal propio; sea (x) un ideal verificando: $(p) \subseteq (x) \subseteq D$, entonces $p \in (x)$ y por tanto existe $c \in D$ tal que $p = xc$, ya que p es irreducible, resulta que, uno de los dos, x ó c es invertible. Si x es invertible, entonces $(x) = D$, y si c es invertible, $p \sim x$ y $(p) = (x)$. □

Corolario. 13.32. (Condición de primo)
En un DIP cada elemento irreducible es primo.

DEMOSTRACIÓN. Si D es un DIP y $p \in D$ es irreducible, entonces (p) es un ideal maximal de D, luego es un ideal primo, y como consecuencia, ver Ejercicio (13.11.), tenemos que p es un elemento primo. □

Proposición. 13.33.
Sea D un DIP, y $(a_1) \subseteq (a_2) \subseteq \ldots$ una cadena ascendente de ideales, entonces existe m tal que $(a_m) = (a_{m+k})$ para cada $k \geq 0$.

DEMOSTRACIÓN. Ya que $\cup(a_i)$ es un ideal de D, existe $a \in D$ tal que $\cup(a_i) = (a)$, y existe $m \in \mathbb{N}^*$ con $a \in (a_m)$. Como consecuencia $(a) \subseteq (a_m) \subseteq \cup(a_i) = (a)$, y $(a) = (a_m) = (a_{m+k})$ para cada $k \geq 0$. □

Teorema. 13.34.
Todo DIP es un DFU.

DEMOSTRACIÓN. Sea D un DIP y $a \in D$ un elemento no nulo que no es invertible,
(1). Vamos a probar que a tiene un factor irreducible; si a es irreducible entonces tenemos el resultado, supongamos que no lo es, entonces existe una factorización $a = a_1 a_1'$, con a_1, a_1' no invertibles. Si a_1 es irreducible tenemos el resultado, en caso contrario tenemos una factorización $a_1 = a_2 a_2'$, con a_2, a_2' no invertibles; si a_2 es irreducible tenemos el resultado, en caso contrario tenemos una factorización ... Siguiendo el proceso tenemos una sucesión de factores $a_1, a_2, \ldots$, y si no encontramos una factor irreducible, esta sucesión se prolonga indefinidamente, ya que $a_i | a_{i-1}$, para cada i, obtenemos así una cadena de ideales:

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$$

y aplicando la Proposición (13.33.), la cadena es estacionaria, esto es; existe m tal que $(a_m) = (a_{m+k})$ para cada $k \geq 0$, veamos qué se deduce de estas igualdades, tenemos $a_m \sim a_{m+1}$, ver Ejercicio (13.42.), luego a_{m+1}' es invertible, lo que es una contradicción, y por tanto, necesariamente en este proceso tenemos que encontrar un factor irreducible de a.
(2). Vamos a probar que cada elemento no nulo y no invertible tiene una factorización en elementos irreducibles; sea a un elemento verificando estas propiedades, si a es irreducible, entonces tenemos el resultado; en caso contrario, aplicando el anterior resultado, existe un factor irreducible p_1 de a, esto es; existe una factorización $a = p_1 b_1$, si b_1 es irreducible, entonces tenemos el resultado, en caso contrario, aplicando el anterior resultado, existe una factor irreducible p_2 de b_1 y una factorización $b_1 = p_2 b_2$, si b_2 es irreducible, entonces tenemos el resultado, en caso contrario seguimos y

determinamos p_3 y b_3 ... Siguiendo el proceso tenemos una sucesión de factores $b_1, b_2, \ldots$ y si no encontramos un factor irreducible b_i, entonces esta sucesión se prolonga indefinidamente, tenemos que $b_i | b_{i-1}$ para cada i, obtenemos así una cadena de ideales:

$$(a) \subseteq (b_1) \subseteq (b_2) \subseteq \ldots$$

y aplicando la Proposición (13.33.), la cadena es estacionaria, existe m tal que $(b_m) = (b_{m+k})$ para cada $k \geq 0$, y de estas igualdades se deduce que $b_m \sim b_{m+1}$, entonces de la factorización $b_m = p_{m+1} b_{m+1}$ se deduce que p_{m+1} es invertible, lo que es una contradicción, por lo tanto algún b_i es irreducible y a tiene una factorización en elementos irreducibles.

(3). Vamos a probar que dos factorizaciones en elementos irreducibles son esencialmente iguales, supongamos dos factorizaciones de un elemento no nulo a que no es invertible, por ejemplo:

$$p_1 \cdots p_r = a = q_1 \cdots q_s,$$

con $p_1, \ldots, p_r, q_1, \ldots, q_s$ elementos irreducibles; vamos a hacer inducción sobre r; si $r = 1$, entonces $q_1 \ldots q_s$ es irreducible, luego $s = 1$ y tenemos $p_1 = q_1$; supongamos que $r > 1$, consideramos p_r, por el Corolario (13.32.) resulta que p_r es primo, y por tanto existe $j \in \{1, \ldots, s\}$ tal que $p_r | q_j$, sin pérdida de generalidad podemos suponer que $j = s$, entonces $p_r \sim q_s$, y existe $u \in \mathscr{U}(D)$ tal que $p_r = u q_s$, por tanto tenemos la igualdad

$$p_1 \cdots p_{r-1} u q_s = p_1 \cdots p_r = q_1 \cdots q_s,$$

simplificando por q_s llegamos a la igualdad

$$p_1 \cdots p_{r-1} u = q_1 \cdots q_{s-1},$$

es claro que el primer miembro es un producto de $r-1$ factores irreducibles, luego se verifica $r-1 = s-1$, y por tanto $r = s$, además por la hipótesis de inducción existe una permutación $\sigma \in S_{r-1}$ tal que $q_i \sim p_{\sigma(i)}$, si $\sigma(i) \neq r-1$ y $q_i \sim p_{\sigma(i)} u$, si $\sigma(i) = r-1$, de donde se deduce el resultado. □

Como consecuencia, ya que sabemos que cada ideal del anillo $\mathbb{Z}$ de los números enteros es principal, resulta que $\mathbb{Z}$ es un DFU. Un sencillo Corolario de este Teorema es:

Corolario. 13.35. (Teorema fundamental de la Aritmética)
Para cada número entero n, no nulo y distinto de ± 1, existe una factorización única en la forma

$$n = (\pm 1) p_1^{e_1} \cdots p_r^{e_r},$$

donde $p_1, \ldots, p_r$ son enteros primos positivos, y $e_1, \ldots, e_r$ y r son enteros positivos.

No todo DFU es un DIP.

Ejemplo. 13.36.
Consideramos el anillo de polinomios $\mathbb{Z}[X]$. Es un DFU, como veremos más adelante, y no es un DIP, ya que $(2, X)$ no es un ideal principal.

En los DIP existe una estrecha relación entre el mcd de dos elementos y estos, que generaliza los resultados conocidos para números enteros.

Proposición. 13.37.
Sea D un DIP y $a, b, d \in D$, son equivalentes:

(a) d es un mcd *de a y b.*
(b) $(d) = (a, b)$.

DEMOSTRACIÓN. Supongamos que $(e) = (a, b)$, entonces $a, b \in (e)$, luego $e \mid a$ y $e \mid b$, por lo tanto $e \mid d$ y como consecuencia $(a, b) \subseteq (d) \subseteq (e) \subseteq (a, b)$. Recíprocamente, supongamos que $(d) = (a, b)$, entonces $d \mid a$ y $d \mid b$, supongamos que existe $e \in D$ tal que $e \mid a$ y $e \mid b$, entonces existen $a', b' \in D$ tales que $a = ea'$ y $b = eb'$, y existen $u, v \in D$ tales que $d = ua + vb$, y sustituyendo los valores de a y b tenemos $d = uea' + veb'$, de donde se deduce que $e \mid d$, y d es un mcd de a y b. □

Corolario. 13.38. (Teorema de Bezout)
Sean D un DIP y $a, b \in D$, si d es un mcd *de a y b, entonces existen $u, v \in D$ verificando $ua + vb = d$.*

Dominios euclídeos

Aunque hemos ganado en eficacia a la hora de representar los ideales — en un DIP todos los ideales son principales — resulta que no es posible desarrollar la aritmética de forma satisfactoria en un DIP, como se hizo en el caso del anillo $\mathbb{Z}$. Por ejemplo, dados $a, b \in D$ sabemos que existe el mcd, y si d es un mcd, entonces existe una igualdad de ideales $(d) = (a) + (b)$, ó de elementos, $d = ua + vb$, para $u, v \in D$, sin embargo no conocemos ningún método para calcular u y v. Es por eso que nos vemos en la necesidad de introducir una nueva clase de anillos; probaremos que todos los elementos de esta nueva clase son ejemplos de DIP y por tanto también de DFU.
Dado el conjunto $\mathbb{N}$ de los números naturales, consideramos un nuevo elemento $\omega \notin \mathbb{N}$, y el conjunto $\mathbb{N} \cup \{\omega\}$. En él definimos una relación de orden mediante:

$$a \leq b \text{ si } \begin{cases} a \leq b, & \text{y } a, b \in \mathbb{N}, \\ b = \omega, & \text{y } a \in \mathbb{N} \cup \{\omega\}. \end{cases}$$

Con esta definición tenemos que $\mathbb{N} \cup \{\omega\}$ es un conjunto bien ordenado.

Llamamos **dominio euclídeo**, abreviadamente **DE**, a un anillo D que es un DI y en el que existe una función δ

$$\delta : D \longrightarrow \mathbb{N} \cup \{\omega\},$$

verificando:

(1) $\delta(0) = \text{Inf}\{\delta(a) \mid\ a \in D \setminus \{0\}\}$.
(2) $\delta(ab) \geq \delta(a)$, para todos $a, b \in D^*$.
(3) Para todos $a, b \in D$, existen $q, r \in D$ verificando:

   (I) $a = bq + r$

   (II) $r = 0$, ó $\delta(r) < \delta(b)$ si $r \neq 0$.

La aplicación δ se llama la **función euclídea** de D.

Ejemplos. 13.39.
(1) El principal ejemplo de DE es el anillo $\mathbb{Z}$ de los números enteros, donde podemos tomar como función δ la función **valor absoluto** en $\mathbb{Z} \setminus \{0\}$, y $\delta(0) = \omega$.

(2) En el anillo $\mathbb{Z}[i]$ de los enteros de Gauss, si consideramos la función

$$\delta : \mathbb{Z}[i]^* \longrightarrow \mathbb{N};\ \delta(a + bi) = a^2 + b^2,$$

y $\delta(0) = \omega$, tenemos también un DE. Equivalentemente podemos tomar la función δ definida mediante $\delta(a + bi) = \sqrt{a^2 + b^2}$, para $a + bi \neq 0$. De esta forma, tomando el módulo del número complejo, generalizamos la situación del anillo $\mathbb{Z}$ de los anillos enteros.

(3) También es un DE el anillo $\mathbb{Z}[\sqrt{2}]$ con la función

$$\delta : \mathbb{Z}[\sqrt{2}]^* \longrightarrow \mathbb{N};\ \delta(a + b\sqrt{2}) = \mid a^2 - 2b^2 \mid,\ \text{si } a + b\sqrt{2} \neq 0,$$

y $\delta(0) = \omega$.

(4) En cambio el anillo $\mathbb{Z}[\sqrt{-5}]$ no lo es, para probarlo nos remitimos el siguiente Lema y al hecho de que $\mathbb{Z}[\sqrt{-5}]$ no es un DFU.

(5) Todo cuerpo K es un DE, podemos definir $\delta : K^* \longrightarrow \mathbb{N}$ mediante $\delta(a) = \begin{cases} 0, & \text{si } a \neq 0, \\ 1, & \text{si } a = 0. \end{cases}$

Lema. 13.40.
Todo DE es un DIP.

DEMOSTRACIÓN. Sea D un DE con función euclídea δ, y $\mathfrak{a}$ un ideal de D; si $\mathfrak{a}=0$, entonces $\mathfrak{a}$ es principal; supongamos ahora que $\mathfrak{a}$ es no nulo y consideremos $0\neq a\in\mathfrak{a}$ de forma que $\delta(a)$ sea mínimo entre las imágenes por δ de los elementos de $\mathfrak{a}$. Para cada $x\in\mathfrak{a}$ podemos hacer la división por a y obtenemos elementos $q,r\in D$ tales que $x=aq+r$ verificando $r=0$ ó $\delta(r)<\delta(a)$; si $r\neq 0$, entonces se verifica $\delta(r)<\delta(a)$, y ya que $r=x-aq\in\mathfrak{a}$, llegamos a una contradicción, por lo tanto se verifica que $r=0$ y como consecuencia $x=aq$, esto es; $x\in(a)$, tenemos pues $(a)\subseteq\mathfrak{a}\subseteq(a)$, y $\mathfrak{a}$ es un ideal principal. □

No todo DIP es un DE. La demostración de este hecho no cae dentro de lo que podemos hacer en este curso; para un ejemplo remitimos a los ejercicios.
Veamos algunas propiedades aritméticas de los DE.

Proposición. 13.41.
Sea D un DE, y $a,b,u\in D$, se verifica:
(1) $\delta(1)\leq\delta(a)$.
(2) $\delta(1)=\delta(u)$ si, y sólo si, $u\in\mathscr{U}(D)$.
(3) Si $b\neq 0$, $a|b$ y $b\nmid a$, entonces $\delta(a)<\delta(b)$.

DEMOSTRACIÓN. (1). Es claro que $\delta(a)=\delta(1\times a)\geq\delta(1)$.
(2). Supongamos que $\delta(1)=\delta(u)$, entonces existen $q,r\in D$ tales que $1=uq+r$ con $r=0$ ó $\delta(r)<\delta(u)$, y ya que por la propiedad (1) se tiene $\delta(r)\geq\delta(1)=\delta(u)$, se verifica necesariamente $r=0$, y por tanto $1=uq$ y u es invertible. Por el contrario, supongamos que u sea invertible, entonces existe $v\in D$ tal que $1=uv$, y se verifica $\delta(1)=\delta(uv)\geq\delta(u)$, de donde se deduce $\delta(1)=\delta(u)$.
(3). Por hipótesis, $a|b$ y se tiene $\delta(b)\geq\delta(a)$; si $b\nmid a$, hacemos la división de a por b y encontramos $q,r\in D$ tales que $a=bq+r$ con $r=0$ ó $\delta(r)<\delta(b)$; ya que $b\nmid a$, ocurre que $r\neq 0$. Por otro lado existe $c\in D$ tal que $b=ac$, y entonces tenemos la igualdad $a=acq+r$, de donde se deduce que $a|r$, y entonces $\delta(r)\geq\delta(a)$. Uniendo estos resultados tenemos $\delta(b)>\delta(r)\geq\delta(a)$. □

Deseamos destacar aquí que los elementos q y r que aparecen en la definición de DE no están determinados de forma única, por ejemplo, si consideramos el anillo $\mathbb{Z}$ de los números enteros y los números 41 y 5, las posibles divisiones de 41 por 5 son dos:

$$41=5\times 8+1,\qquad 41=5\times 9-4,$$

Algoritmo extendido de Euclides

Como ya conocemos, el **algoritmo de Euclides** es un proceso para calcular un mcd de dos números enteros; vamos a desarrollarlo para un DE. Dados $a,b\in D$, si $a=0$, entonces $\mathrm{mcd}\{a,b\}=b$, igual ocurre si suponemos que $b=0$. Supongamos que $a\neq 0$ y $b\neq 0$, entonces existen $q_1,r_1\in D$ verificando:

$$a=bq_1+r_1,\quad \text{con } r_1=0 \text{ ó } \delta(r_1)<d(b) \text{ si } r_1\neq 0.$$

Si $r_1 = 0$, entonces $a \mid b$ y tenemos que $\mcd\{a,b\} = b$. En caso contrario tenemos: $\mcd\{a,b\} = \mcd\{b, r_1 = r - sq_1\}$. Entonces existen $q_2, r_2 \in D$ verificando:

$$b = r_1 q_2 + r_2, \quad \text{con } r_2 = 0 \text{ ó } \delta(r_2) < \delta(r_1) \text{ si } r_2 \neq 0.$$

Reiterando el proceso, en el caso en que todos los r_n son no nulos, obtenemos las siguientes sucesiones:

$$\begin{array}{ll} r_0 = b. & \\ a = r_0 q_1 + r_1, & \delta(r_1) < \delta(r_0). \\ r_0 = r_1 q_2 + r_2, & \delta(r_2) < \delta(r_1). \\ \dots & \\ r_{n-2} = r_{n-1} q_n + r_n, & \delta(r_n) < \delta(r_{n-1}). \\ r_{n-1} = r_n q_{n+1} + r_{n+1}, & \delta(r_{n+1}) < \delta(r_n). \\ \dots & \end{array}$$

y tenemos una sucesión estrictamente descendente de números naturales,

$$\delta(r_0) > \delta(r_1) > \ldots > \delta(r_n) > \ldots$$

esta sucesión debe ser finita, luego necesariamente algún $r_i = 0$. Supongamos que $r_{n+1} = 0$, entonces tenemos la cadena de igualdades

$$\mcd\{a,b\} = \mcd\{r_0, r_1\} = \ldots = \mcd\{r_{n-2}, r_{n-1}\} = \mcd\{r_{n-1}, r_n\} = r_n,$$

y r_n es el mcd de a y b.
También es posible ahora calcular el mcd como una combinación lineal de a y b; tenemos

$$r_1 = au_1 + bv_1, \qquad \text{con } u_1 = 1, v_1 = -q_1.$$

Supongamos que para $1 \leq j \leq i$ tenemos

$$r_j = au_j + bv_j,$$

entonces haciendo un pequeño cálculo tenemos

$$r_{i+1} = r_{i-1} - r_i q_{i+1} = (au_{i-1} + bv_{i-1}) - (au_i + bv_i)q_{i+1} = a(u_{i-1} - u_i q_{i+1}) + b(v_{i-1} - v_i q_{i+1}),$$

y se verifican las igualdades:

$$\begin{array}{l} u_{i+1} = u_{i-1} - u_i q_{i+1}, \text{ y} \\ v_{i+1} = v_{i-1} - v_i q_{i+1}. \end{array}$$

Veamos ahora algunas aplicaciones del algoritmo de Euclides. Supongamos que D es un DE.

(1) **Cálculo de inverso módulo un elemento**. Supongamos que $a, b \in D$ son elementos tales que $\mcd\{a,b\} = 1$, entonces existen $u, v \in D$ tales que $1 = ua + vb$, y tenemos $ua \equiv 1 \pmod{b}$, luego u es el inverso de a módulo b.

(2) **Resolución de ecuaciones lineales en un DE**. Sean $a, b, t \in D$, vamos a estudiar las raíces de la ecuación

$$aX + bY = t.$$

Llamamos d a un mcd de a y b. En el caso en que $d \nmid t$, tenemos que la ecuación

$$aX + bY = t$$

no tiene solución en D, ya que en caso de existir una solución $x, y \in D$, se verifica $ax + by = t$, luego $d \mid t$. Supongamos por tanto que $d \mid t$, entonces existe $t' \in D$ tal que $t = dt'$; por el algoritmo de Euclides, existen $u, v \in D$ tales que $d = ua + vb$, y las soluciones a la ecuación son de la forma:

$$X = ut' - k(b/d), \quad Y = vt' + k(a/d),$$

con $k \in D$.

(3) **Algoritmo chino del resto**. Supongamos que tenemos solamente dos congruencias. Para elementos $a, b, n, m \in D$ con m y n primos relativos, $(n, m) = 1$, el problema consiste en encontrar $x \in D$ tal que $x \equiv a \pmod{m}$ y $x \equiv b \pmod{n}$. El método para encontrar x lo dividimos en tres pasos:

(I) Hallar $\alpha \in D$ tal que $\alpha m \equiv 1 \pmod{n}$.
(II) Hallar $\beta \in D$ tal que $\beta \equiv (b - a)\alpha \pmod{n}$.
(III) Tomamos entonces como solución $x = a + \beta m$;

es claro que x es solución ya que

$$x - a = \beta m \equiv 0 \pmod{m}.$$
$$x - b = a + \beta m - b \equiv a + (b - a)\alpha m - b \equiv 0 \pmod{n}.$$

También son soluciones todos los elementos de la forma $a + \beta m + knm$, para $k \in D$. En el caso en que haya más de dos congruencias,

$$x \equiv a_i \pmod{m_i}, i = 1, \ldots, n,$$

con los m_i primos relativos dos a dos, para encontrar una solución procedemos como sigue:

(I) Definimos

$$M_k = \begin{cases} 1 & \text{si } k = 1 \\ \prod_{i=1}^{k-1} m_i & \text{si } k > 1 \end{cases} \quad \text{para } k = 1, \ldots, n.$$

Tenemos que M_i y m_i son primos relativos para $i = 1, \ldots, n$.
(II) Hallamos $\alpha_k \in D$ tal que $\alpha_k M_k \equiv 1 \pmod{m_k}$.
(III) Hallamos $\beta_k \in D$ tal que $\beta_k \equiv (a_k - b_{k-1})\alpha_k \pmod{m_k}$, donde $b_1 \equiv a_1 \pmod{m_1}$ y $b_k = b_{k-1} + \beta_k M_k$.
(IV) Finalmente tomamos como solución $x = b_n$.

Al igual que en el caso de dos congruencias, también son soluciones todos los elementos de la forma $b_n + km_1 \cdots m_n$ para $k \in D$.

Ejercicios

Dominios euclídeos

Ejercicio. 13.42.
Demuestra que en un DI se verifican las siguientes condiciones:

(1) $a|b$ *si, y sólo si,* $(b)\subseteq(a)$*. Para todos* $a,b\in D$*.*
(2) a *es un factor propio de* b *si, y sólo si,* $(b)\subsetneq(a)$*. Para todos* $a,b\in D$*.*
(3) $a\sim b$ *si, y sólo si,* $(a)=(b)$*. Para todos* $a,b\in D$*.*
(4) $u\in\mathscr{U}(A)$ *si, y sólo si,* $(u)=A$*. Para* $u\in D$*.*
(5) $a=0$ *si, y sólo si,* $(a)=0$*. Para* $a\in D$*.*

Ref.: 1103e_071 *SOLUCIÓN.*

Ejercicio. 13.43.
Sea D *un DI, y* $p,q\in D$ *dos elementos irreducibles, si* $p|q$*, demuestra que* $p\sim q$*.*

Ref.: 1103e_072 *SOLUCIÓN.*

Ejercicio. 13.44.
En el anillo $\mathbb{Z}[\sqrt{-5}]$ *definimos una aplicación* $N:\mathbb{Z}[\sqrt{-5}]^*\longrightarrow\mathbb{N}$ *mediante* $N(a+b\sqrt{-5})=a^2+5b^2$*.*

(1) Demuestra que $N(xy)=N(x)N(y)$*, para cada* $x,y\in\mathbb{Z}[\sqrt{-5}]^*$*.*
(2) Demuestra que u *es invertible si, y sólo si,* $N(u)=1$*.*
(3) Demuestra que si $x\sim y$*, entonces* $N(x)=N(y)$*.*
(4) Demuestra que si a *es un factor propio de* b*, entonces* $N(a)$ *es un factor propio de* $N(b)$*.*
(5) Demuestra que $2,3,1+\sqrt{-5}$ *y* $1-\sqrt{-5}$ *son elementos irreducibles.*
(6) Demuestra que $2,3,1+\sqrt{-5}$ *y* $1-\sqrt{-5}$ *no son primos.*
(7) Demuestra que un mcd *de* 2 *y* $1+\sqrt{-5}$ *es* 1*, y que no existe el* mcm*.*
(8) Demuestra que no existe el mcd *de los elementos* $2(1+\sqrt{-5})$ *y* 6*.*
(9) Demostrar que el ideal $\mathfrak{b}=(2,1+\sqrt{-5})$ *no es principal.*
(10) Demostrar que $\mathfrak{b}^2=(2)$*.*

Ref.: 1103e_073 *SOLUCIÓN.*

El Lema (13.8.) nos asegura que si en un dominio D dos elementos no nulos a y b tiene un mcm, también tienen un mcd. El resultado recíproco no es siempre cierto como el siguiente ejemplo prueba.

En el anillo $\mathbb{Z}[\sqrt{-5}]$ los elementos $1+\sqrt{-5}, 1-\sqrt{-5}, 2$ y 3 son irreducibles, y por tanto el mcd de cada par es igual a 1. Todos ellos tienen un múltiplo común, ya que verifican $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2\times 3$.

Si consideramos el elemento $x = 2(1+\sqrt{-5})$, resulta que es un múltiplo común de 2 y $1+\sqrt{-5}$, y no tiene divisores propios distintos de éstos y sus asociados, por lo que es un candidato a ser el mcm. Sin embargo no divide al múltiplo común 6. En consecuencia, no existe el mcm de 2 y $1+\sqrt{-5}$.

El siguiente ejercicio nos asegura la existencia de mcm cuando existe el mcd de cada par de elementos.

Ejercicio. 13.45.
Sea D un DI, si todo par de elementos de D tiene un mcd*, entonces todo par de elementos de D tiene un* mcm.
Ref.: 1103e_020 *SOLUCIÓN.*

Ejercicio. 13.46.
Estudia los siguientes enunciados:

(1) El anillo $\mathbb{Z}[\sqrt{5}]$ tiene un número infinito de elementos invertibles.
(2) Determina $a \in \mathbb{Z}$ para que $1-\sqrt{5}$ y $a+\sqrt{5}$ sean asociados.

Ref.: 1103e_065 *SOLUCIÓN.*

Ejercicio. 13.47.
Estudia los siguientes enunciados:

(1) Demuestra que el anillo $\mathbb{Z}[\sqrt{10}]$ no es un DFU.
(2) Demuestra que el anillo $\mathbb{Z}[\sqrt{5}]$ no es un DFU.

Ref.: 1103e_074 *SOLUCIÓN.*

Ejercicio. 13.48.
Estudia los siguientes enunciados:

(1) Determina los elementos invertibles de los anillos, $\mathbb{Z}[i]$ *y* $\mathbb{Z}[\sqrt{-3}]$.
(2) Demuestra que si $d \in \mathbb{Z}$ *es libre de cuadrados y verifica* $d < -1$, *entonces el anillo* $\mathbb{Z}[\sqrt{d}]$ *tiene únicamente dos elementos invertibles,* ± 1.
(3) Demuestra que los elementos $\pm(1+\sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]$ *son invertibles, y que por lo tanto este anillo tiene infinitos elementos invertibles.*

Ref.: 1103e_075 *SOLUCIÓN.*

Ejercicio. 13.49.
Demuestra que en un DFU para cada dos elementos a *y* b *se verifica:*

$$ab \sim (a,b)[a,b].$$

Ref.: 1103e_076 *SOLUCIÓN.*

Ejercicio. 13.50.
Sea D *un DFU, si* $d|x$ *y* $(d,x) = 1$, *prueba que* $d|y$.
Ref.: 1103e_021 *SOLUCIÓN.*

Ejercicio. 13.51.
Sea D *un DFU y* $a, b \in D$ *elementos no nulos. Si* $d = \operatorname{mcd}\{a,b\}$ *y se tienen las factorizaciones* $a = da'$, $b = db'$. *Prueba que* $\operatorname{mcd}\{a',b'\} = 1$.
Ref.: 1103e_022 *SOLUCIÓN.*

Ejercicio. 13.52.
En la demostración del Teorema (13.34.) hemos utilizado que todo DIP verifica las dos condiciones siguientes:

(I) *Todo elemento irreducible es primo. (Condición de primo).*
(II) *Toda cadena ascendente de ideales principales es estacionaria. (Condición de cadena de divisores).*

Probar los siguientes resultados:

(1) Un DI es un DFU si, y sólo si, verifica la condición de primo y la condición de cadena de divisores.
(2) Si un DI verifica la condición de cadena de divisores (CCD), entonces cada elemento no nulo que no es invertible tiene una factorización en elementos irreducibles. (Notar que esta factorización no ha de ser necesariamente esencialmente única).
(3) El anillo $\mathbb{Z}[\sqrt{-5}]$ verifica la condición de cadena de divisores.

Ref.: 1103e_077 *SOLUCIÓN.*

Ejercicio. 13.53.
Sea D un DI, demuestra que son equivalentes las siguientes condiciones:

(a) D es un DIP.
(b) D es un DFU, y cada ideal de la forma (a, b) es principal.

Ref.: 1103e_078 *SOLUCIÓN.*

Ejercicio. 13.54.
Sea D un DIP, demuestra las siguientes propiedades:

(1) Cada ideal propio de D es igual al producto de un número finito de ideales maximales, los cuales están determinados de forma única salvo en el orden.
*(2) Un ideal propio $\mathfrak{a}$ de D se llama **primario** si para cualesquiera elementos $a, b \in D$ se verifica:*

$$ab \in \mathfrak{a} \text{ y } a \notin \mathfrak{a} \text{ implica } b^n \in \mathfrak{a} \text{ para algún entero positivo } n.$$

Demuestra que un ideal $\mathfrak{a}$ de D es primario si, y sólo si, existe $p \in D$ primo y $n \in \mathbb{N}^*$ tal que $\mathfrak{a} = (p^n)$.

(3) *Sean* $\mathfrak{a}_i$, $1 \leq i \leq r$, *ideales primarios de* D *tales que* $\mathfrak{a}_i = (p_i^{e_i})$ *para cada* i *y además* $p_i \nsim p_j$ *si* $i \neq j$. *Demuestra que entonces se tiene* $\mathfrak{a}_1 \cdots \mathfrak{a}_r = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r$.
(4) *Demuestra que todo ideal* $\mathfrak{a}$ *de* D *se puede escribir, de forma única salvo en el orden, como una intersección de un número finito de ideales primarios*

Ref.: 1103e_079 *SOLUCIÓN.*

Ejercicio. 13.55.
Demuestra que el subanillo de $\mathbb{Q}$ *formado por todas las fracciones que se pueden escribir en la forma* $\frac{n}{m}$ *con* m *impar es un DIP.*
Ref.: 1103e_080 *SOLUCIÓN.*

Ejercicio. 13.56.
Estudia los siguientes enunciados:
(1) *Da un ejemplo de un DFU y de un ideal primo no nulo en él que no sea maximal.*
(2) *Demuestra que si* D *es un DIP, entonces todo ideal primo no nulo es maximal.*

Ref.: 1103e_081 *SOLUCIÓN.*

Ejercicio. 13.57. (Nivel avanzado)
Un entero a *se llama un* ***residuo cuadrático módulo el primo*** p *si la congruencia* $x^2 \equiv a \pmod{p}$ *tiene solución. Definimos el* ***símbolo de Legendre*** $\left(\frac{a}{p}\right)$ *mediante:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \pmod{p}. \\ 1 & \text{si } a \not\equiv 0 \pmod{p} \text{ y } a \text{ es un residuo cuadrático módulo } p. \\ -1 & \text{si } a \not\equiv 0 \pmod{p} \text{ y } a \text{ no es un residuo cuadrático módulo } p. \end{cases}$$

Es de destacar que $\left(\frac{a}{p}\right) = 1$ *si, y sólo si,* $a + p\mathbb{Z}$ *es un cuadrado en el anillo* $\mathbb{Z}_p$.
(1) *Demuestra que para cada par de números enteros* a *y* b *se verifica:*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

(2) Demuestra que si $p \neq 2$, entonces $\left(\frac{a}{p}\right) = 1$ si, y sólo si, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Ref.: 1103e_082 *SOLUCIÓN.*

Ejercicio. 13.58. (Nivel avanzado)
Sea p un entero primo positivo de la forma $4n+1$ y sea q un entero primo positivo tal que $\left(\frac{p}{q}\right) = -1$. Demuestra que $\mathbb{Z}[\sqrt{pq}]$ no es un DFU.
Ref.: 1103e_083 *SOLUCIÓN.*

Ejercicio. 13.59.
Resuelve los siguientes enunciados:

(1) Estudia si es un DFU el anillo $\mathbb{Z}[\sqrt{-3}]$.
(2) Estudia si es un DE el anillo

$$D = \left\{ a + bz \mid \ a, b \in \mathbb{Z}, z = \frac{1}{2}(-1 + \sqrt{-3}) \right\}.$$

(3) ¿Es 43 un número primo en estos anillos?

Ref.: 1103e_084 *SOLUCIÓN.*

Ejercicio. 13.60.
Demuestra que $\mathbb{Z}[\sqrt{-2}]$ es un DE.
Ref.: 1103e_085 *SOLUCIÓN.*

Ejercicio. 13.61.
Estudia los siguientes enunciados:

(1) *Haz la división de* $7+2i$ *y* $3-4i$ *en el anillo de los enteros de Gauss.*
(2) *Halla el* mcd *y el* mcm *de* $11+7i$ *y* $3+7i$ *en* $\mathbb{Z}[i]$.
(3) *Halla el* mcd *y el* mcm *de* $8+6i$ *y* $5-15i$ *en* $\mathbb{Z}[i]$.
(4) *Halla el* mcd *y el* mcm *de* $16+7i$ *y* $10-5i$ *en* $\mathbb{Z}[i]$.

Ref.: 1103e_086 *SOLUCIÓN.*

Ejercicio. 13.62.
Demuestra que $1-2i$ *es primo en* $\mathbb{Z}[i]$.
Ref.: 1103e_087 *SOLUCIÓN.*

Ejercicio. 13.63.
Sea D *un DE, demuestra que las únicas soluciones de la ecuación* $aX+bY=t$ *son las siguientes:*

$$x = ut' - k(b/d), \quad y = vt' + k(a/d),$$

donde $d = \mathrm{mcd}\{a,b\}$, $t = dt'$ *y* k *varía en* D.
Ref.: 1103e_088 *SOLUCIÓN.*

Ejercicio. 13.64.
Calcula todas la soluciones en $\mathbb{Z}$ *de las siguientes ecuaciones:*
(1) $35X-44Y=18$.
(2) $84X+54Y=-24$.

Calcula todas la soluciones en $\mathbb{Z}[i]$ *de las siguientes ecuaciones:*
(3) $(11+7i)X+(3+7i)Y=4$.
(4) $(8+6i)X+(5-15i)Y=-100$.

Ref.: 1103e_089 *SOLUCIÓN.*

Ejercicio. 13.65.
El número de páginas de un libro es mayor que 400 y menor que 500. Si se cuentan de 2 en 2 sobra 1. Si se cuentan de 3 en 3 sobran 2. Si se cuentan de 5 en 5 sobran 4. Si se cuentan de 7 en 7 sobran 6. ¿Cuantas páginas tiene el libro?
Ref.: 1103e_090 *SOLUCIÓN.*

Ejercicio. 13.66.
Resuelve en $\mathbb{Z}[i]$ el siguiente sistema de congruencias.

$$\begin{cases} x \equiv i & (\text{mod } 3) \\ x \equiv 2 & (\text{mod } 2+i) \\ x \equiv 1+i & (\text{mod } 3+2i) \\ x \equiv 3+2i & (\text{mod } 4+i) \end{cases}$$

Ref.: 1103e_091 *SOLUCIÓN.*

Ejercicio. 13.67.
Resuelve en $\mathbb{Z}$ el siguiente sistema de congruencias.

$$\begin{cases} x \equiv 1 & (\text{mod } 2) \\ x \equiv 2 & (\text{mod } 3) \\ x \equiv 2 & (\text{mod } 5) \\ x \equiv 10 & (\text{mod } 49) \end{cases}$$

Ref.: 1103e_092 *SOLUCIÓN.*

Ejercicio. 13.68.
Resuelve en $\mathbb{Z}$ el siguiente sistema de congruencias.

$$\begin{cases} x \equiv 1 & (\text{mod } 5) \\ x \equiv 3 & (\text{mod } 9) \\ x \equiv 5 & (\text{mod } 11) \\ x \equiv 2 & (\text{mod } 14) \end{cases}$$

Ref.: 1103e_093 *SOLUCIÓN.*

Ejercicio. 13.69.
¿Qué es incorrecto en la siguiente demostración de que en un DI todo elemento irreducible es primo?
Si $p \in D$ irreducible, y $a, b \in D$ tales que $p \mid ab$ y $p \nmid a$, $p \nmid b$, entonces, ya que $(p, a) = 1 = (p, b)$, aplicando el apartado (5) de la Proposición (13.4.), tenemos $(p, ab) = 1$, y por tanto $p \nmid ab$, lo que es una contradicción.
Ref.: 1103e_094 *SOLUCIÓN.*

Capítulo IV

Anillos de polinomios

Introducción

1104-00.tex

14. Anillos de polinomios

Sea A un anillo conmutativo y X una **indeterminada**, esto es; un símbolo que no pertenece a A, llamamos **polinomio** en X con coeficientes en A a una expresión formal del tipo

$$a_0 + a_1X + \cdots + a_nX^n,$$

con $a_0, a_1, \ldots, a_n \in A$, $n \in \mathbb{N}$ y donde $X^2, \ldots, X^n$ son nuevos símbolos que están relacionados con X. Representamos el conjunto de todos los polinomios en X con coeficientes en A por $A[X]$.

Sean, en lo que sigue, $p(X) = a_0 + a_1X + \cdots + a_nX^n$ y $q(X) = b_0 + b_1X + \cdots + b_mX^m$ dos elementos de $A[X]$.

Diremos que $p(X)$ y $q(X)$ son **iguales** si $a_i = b_i$, para $0 \leq i \leq \min\{n, m\}$ y $a_i = 0$ ó $b_j = 0$ si $i, j \geq \min\{n, m\}$.

Definimos a continuación dos operaciones binarias en el conjunto $A[X]$; sean $p(X)$ y $q(X)$ como antes, entonces definimos una operación suma mediante:

$$p(X) + q(X) = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_h + b_h)X^h,$$

y una operación producto:

$$p(X)q(X) = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + t_iX^i + \cdots + a_nb_mX^{n+m},$$

donde $a_k = 0$ si $k > n$ y $b_l = 0$ si $l > m$, $h = \max\{n, m\}$ y $t_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$.

Lema. 14.1.
En la situación anterior $A[X]$ es un anillo con elemento uno igual al polinomio 1.

Dado un polinomio $p(X) = a_0 + a_1X + \cdots + a_nX^n$, llamamos **coeficientes** de $p(X)$ a los elementos $a_0, \ldots, a_n$; si $a_n \neq 0$ se llama **coeficiente líder** de $p(X)$ y a_0 se llama **coeficiente** ó **término independiente** de $p(X)$.

El polinomio $p(X)$ es **constante** si $n = 0$. Si $a_n \neq 0$, entonces n se llama **grado** de $p(X)$, y lo notamos $\text{grad}(p(X))$. El polinomio constante $p(X) = 0$ diremos que tiene grado $-\infty$.

Si $X_1, \ldots, X_r$ son indeterminadas sobre A, definimos por recurrencia el anillo de polinomios en las indeterminadas $X_1, \ldots, X_r$ con coeficientes en A como $A[X_1, \ldots, X_r] = A[X_1, \ldots, X_{r-1}][X_r]$. Podemos definir el grado en cada una de las indeterminadas, ya que para cada $1 \leq i \leq r$ existe un isomorfismo

$$A[X_1, \ldots, X_r] \cong A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_r][X_i].$$

1104-01.tex

Como consecuencia cada elemento de $p(X_1,\dots,X_r)\in A[X_1,\dots,X_r]$ se expresa de forma única como una suma finita de la siguiente forma:

$$p(X_1,\dots,X_r)=\sum_{(e_1,\dots,e_r)\in\mathbb{N}^r} a_{(e_1,\dots,e_r)}X_1^{e_1}\cdots X_r^{e_r},$$

donde $a_{e_1\dots e_r}\in A$. A cada uno de los sumandos de esta suma lo llamamos un **término** de $p(X_1,\dots,X_r)$, y cada $X_1^{e_1}\cdots X_r^{e_r}$ lo llamamos un **monomio**. Definimos el grado del término $a_{(e_1,\dots,e_r)}X_1^{e_1}\cdots X_r^{e_r}$ o del monomio $X_1^{e_1}\cdots X_r^{e_r}$ simplemente como la suma $e_1+\cdots+e_r$ de los grados en cada una de las indeterminadas, y decimos que un polinomio es **homogéneo** si todos sus monomios tienen el mismo grado.

Volvamos ahora a la situación de polinomios en una indeterminada. Vamos a estudiar la aritmética del anillo $A[X]$.

Lema. 14.2.
Sea A un anillo y $p(X)$, $q(X)\in A[X]$, entonces se tiene que $\operatorname{grad}(p(X)q(X))\leq\operatorname{grad}(p(X))+\operatorname{grad}(q(X))$. *Y si A es un DI, y los polinomios son no nulos, se verifica la igualdad.*

DEMOSTRACIÓN. Tenemos que $p(X)q(X)=a_0b_0+\cdots+a_nb_mX^{n+m}$. Si $a_nb_m=0$, entonces se verifica: $\operatorname{grad}(p(X)q(X))<\operatorname{grad}(p(X))+\operatorname{grad}(q(X))$. Si A es un DI, entonces $a_nb_m\neq 0$ y $\operatorname{grad}(p(X)q(X))=\operatorname{grad}(p(X))+\operatorname{grad}(q(X))$. □

Corolario. 14.3.
Sea A un anillo, son equivalentes:

(a) A es un DI.
(b) $A[X]$ es un DI.

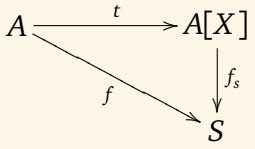
Sea A un anillo, definimos una aplicación $t:A\longrightarrow A[X]$ mediante $t(a)=a$ para cada $a\in A$.

Lema. 14.4.
En la situación anterior t es un homomorfismo inyectivo de anillos. Luego podemos identificar A con su imagen por t en $A[X]$.

Corolario. 14.5.
Si A es un DI, entonces los elementos invertibles de $A[X]$ coinciden con los de A.

DEMOSTRACIÓN. Es claro que todo elemento invertible de A es también invertible en $A[X]$. Supongamos que $p(X) \in A[X]$ es invertible, entonces existe $q(X) \in A[X]$ tal que $p(X)q(X) = 1$, entonces, aplicando el Lema (14.2.), tenemos que $0 = \text{grad}(1) = \text{grad}(p(X)q(X)) \leq \text{grad}(p(X)) + \text{grad}(q(X))$, por tanto $\text{grad}(p(X)) = 0$, y $p(X)$ es un polinomio constante, esto es; pertenece a A. □

Teorema. 14.6. (Propiedad universal del anillo de polinomios)
Sea A un anillo y $f : A \longrightarrow S$ un homomorfismo de anillos. Para cada $s \in S$ existe un único homomorfismo de anillos $f_s : A[X] \longrightarrow S$ tal que $f_s(X) = s$ y $f = f_s t$.



DEMOSTRACIÓN. Sea $p(X) = a_0 + a_1X + \cdots + a_nX^n$ un polinomio en $A[X]$. Definimos $f_s(p(X)) = f_s(a_0) + f_s(a_1)s + \cdots + f_s(a_n)s^n$. Así definido f_s es un morfismo de anillos y verifica $f_s(X) = s$ y $f = f_s t$. Para probar la unicidad, podemos aplicar que X y A generan el anillo $A[X]$. □

Como consecuencia, esta propiedad universal determina salvo isomorfismo el anillo de polinomios en una indeterminada X, esto es; si Y es otra indeterminada, entonces los anillos $A[X]$ y $A[Y]$ son isomorfos.

Otra consecuencia del Teorema (14.6.) es la siguiente: para cada elemento $r \in A$ existe pues un único homomorfismo de anillos $e_r : A[X] \longrightarrow A$ inducido por la identidad en A y el elemento $r \in A$. El homomorfismo e_r se llama **homomorfismo de evaluación en** r. La imagen del polinomio $p(X)$ por e_r la notaremos simplemente por $p(r)$.

Proposición. 14.7.
Sea $g : A \longrightarrow B$ un homomorfismo de anillos, y X una indeterminada, entonces g induce un único homomorfismo de anillos entre los anillos de polinomios $g' : A[X] \longrightarrow B[X]$ haciendo conmutativo el diagrama:

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ {\scriptstyle t_A}\downarrow & & \downarrow{\scriptstyle t_B} \\ A[X] & \xrightarrow[g']{} & B[X] \end{array}$$

Donde t_A y t_B son los homomorfismos canónicos de A en $A[X]$ y de B en $B[X]$ respectivamente.

DEMOSTRACIÓN. Es consecuencia directa de la Propiedad Universal del anillo de polinomios cuando tomamos $f = t_B g$ y $b = X \in B[X]$ □

Divisibilidad

Teorema. 14.8. (Algoritmo de Euclides)
Sea A un anillo y $p(X), q(X) \in A[X]$, con $q(X) \neq 0$ y coeficiente líder invertible en A. Entonces existen polinomios, únicos, $c(X), r(X) \in A[X]$ que verifican:
(1) $p(X) = q(X)c(X) + r(X)$ *y*
(2) $\operatorname{grad}(r(X)) < \operatorname{grad}(q(X))$.

DEMOSTRACIÓN. Demostración por inducción sobre el grado de $p(X)$. Si $\operatorname{grad}(p(X)) \leq \operatorname{grad}(q(X))$, basta tomar $c(X) = 0$ y $r(X) = p(X)$. Supongamos que $\operatorname{grad}(p(X)) \geq \operatorname{grad}(q(X))$. Si $\operatorname{grad}(q(X)) = 0$, entonces tomamos $c(X) = p(X)q(X)^{-1}$ y $r(X) = 0$. Supongamos ahora que el resultado es cierto para todos los polinomios de grado menor que el de $p(X)$, y fijando notación sean $n = \operatorname{grad}(p(X)) \geq \operatorname{grad}(q(X)) = m \geq 0$; definimos

$$p_1(X) = p(X) - (a_n b_m^{-1})X^{n-m}q(X),$$

es claro que $\operatorname{grad}(p_1(X)) < n$, y entonces, por la hipótesis de inducción tenemos

$$\left.\begin{array}{l} p_1(X) = q(X)c_1(X) + r_1(X) \\ \operatorname{grad}(r_1(X)) < \operatorname{grad}(q(X)) \end{array}\right\} \text{ con } c_1(X) \text{ y } r_1(X) \text{ únicos.}$$

Se tiene entonces la siguiente igualdad:

$$p(X) = q(X)\left[c_1(X) + (a_n b_m^{-1})X^{n-m}\right] + r_1(X).$$

Por tanto únicamente queda probar la unicidad de esta descomposición. Supongamos que tenemos dos descomposiciones

$$p(X) = q(X)c_1(X) + r_1(X) = q(X)c_2(X) + r_2(X),$$

con $\text{grad}(r_i(X)) < \text{grad}(q(X))$, $i = 1, 2$.
Entonces tenemos:

$$r_1(X) - r_2(X) = q(X)[c_1(X) - c_2(X)],$$

y si $c_1(X) - c_2(X) \neq 0$, entonces se verifica:

$$\text{grad}(r_1(X) - r_2(X)) = \text{grad}(q(X)[c_1(X) - c_2(X)] =$$

$$\text{grad}(q(X)) + \text{grad}(c_1(X) - c_2(X)) \geq \text{grad}(q(X)) > \text{grad}(r_1(X) - r_2(X)),$$

lo cual es una contradicción. Entonces ha de ser necesariamente $c_1(X) = c_2(X)$, y como consecuencia $r_1(X) = r_2(X)$. □

Vamos a dar nombre a los polinomios que nos aparecen en el anterior Teorema. El polinomio $c(X)$ se llama **cociente** de $p(X)$ por $q(X)$, y $r(X)$ se llama **resto**, estos polinomios no están determinados de forma única.

Corolario. 14.9.
Si K es un cuerpo, entonces $K[X]$ es un DE con función euclídea δ definida por $\delta(p(X)) = \text{grad}(p(X))$.

Tenemos pues perfectamente determinada la aritmética de los anillos de polinomios $K[X]$ con coeficientes en un cuerpo K. Más complicado es el estudio de la aritmética de otros anillos de polinomios, como por ejemplo el anillo $\mathbb{Z}[X]$. La técnica a emplear será reducir, en parte, el estudio del anillo $\mathbb{Z}[X]$ al estudio del anillo $\mathbb{Q}[X]$ del que conocemos perfectamente su aritmética. Ver Corolario (14.9.).

Sea A un anillo, y $p(X) \in A[X]$, un elemento $\alpha \in A$ se llama **raíz** ó un **cero** de $p(X)$ si $p(\alpha) = 0$. Vamos a traducir en términos de la aritmética del anillo $A[X]$ el hecho de que α sea una raíz de un polinomio.

Lema. 14.10.
Sea A un anillo y $p(X) \in A[X]$, para cada $a \in A$ existe un único polinomio $c(X) \in A[X]$ verificando: $p(X) = (X - a)c(X) + p(a)$.

DEMOSTRACIÓN. Aplicando el Algoritmo de Euclides a los polinomios $p(X)$ y $X-a$, resulta que existen polinomios $c(X)$ y $r(X)$ tales que $p(X)=(X-a)c(X)+r(X)$ y $\operatorname{grad}(r(X))<\operatorname{grad}(X-a)=1$, luego $r(X)$ es un polinomio constante; aplicando e_a tenemos:

$$p(a)=e_a(p(X))=e_a((X-a)c(X)+r(X))=(a-a)c(a)+r(a)=r(a),$$

entonces tenemos el resultado $p(X)=(X-a)c(X)+p(a)$. □

Corolario. 14.11.
Sea A un anillo, $p(X)\in A[X]$ y $\alpha\in A$. Son equivalentes:
(a) $p(X)$ es divisible por $X-\alpha$.
(b) α es una raíz de $p(X)$.

Una generalización de este resultado es el siguiente:

Proposición. 14.12.
Sea A un DI, $p(X)\in A[X]$ y $\alpha_1,\ldots,\alpha_k\in A$ raíces de $p(X)$ distintas dos a dos, entonces $(X-\alpha_1)\ldots(X-\alpha_k)\mid p(X)$.

DEMOSTRACIÓN. Para $k=1$ el resultado es exactamente el Corolario (14.11.). Supongamos que $k>1$ y que el resultado sea cierto para todo conjunto de menos de k raíces. Entonces $(X-\alpha_2)\ldots(X-\alpha_k)\mid p(X)$, luego existe un polinomio $q(X)$ tal que $p(X)=(X-\alpha_2)\ldots(X-\alpha_k)q(X)$; aplicando e_{α_1} tenemos:

$$0=p(\alpha_1)=(\alpha_1-\alpha_2)\ldots(\alpha_1-\alpha_k)q(\alpha_1),$$

y ya que $\alpha_1\neq\alpha_i$ para $i=2,\ldots,k$, resulta que ha de ser $q(\alpha_1)=0$. Como consecuencia $(X-\alpha_1)\mid q(X)$ y tenemos $q(X)=(X-\alpha_1)q_0(X)$, entonces $p(X)=(X-\alpha_2)\ldots(X-\alpha_k)(X-\alpha_1)q_0(X)$, de donde deducimos que $(X-\alpha_1)\ldots(X-\alpha_k)\mid p(X)$. □

La hipótesis de ser A un DI es necesaria como prueba el siguiente ejemplo.

Ejemplo. 14.13.
Tomamos $A=\mathbb{Z}_6$ y $p(X)=X^2+5X$, tenemos $p(X)=(X+3)(X+2)=X(X+5)$, entonces raíces de $p(X)$ son 0, 1, 2 y 3, sin embargo $X(X+5)(X+3)(X+2)$ no divide a $p(X)$.

Corolario. 14.14.
Sea A un DI, $p(X),q(X)\in A[X]$ polinomios de grado n; si existen $n+1$ elementos distintos $a_1,\ldots,a_{n+1}$ tales que $p(a_i)-q(a_i)=0$, para $1\leq i\leq n+1$, entonces $p(X)=q(X)$.

Corolario. 14.15.
Sea A un DI y $p(X) \in A[X]$; si $p(X)$ se anula en todos los elementos de un subconjunto infinito de A, entonces $p(X) = 0$.

Fórmula de interpolación de Lagrange

Sea A un DI. Vamos a determinar un polinomio $p(X) \in A[X]$ verificando que en elementos distintos $a_1, \ldots, a_n \in A$ tome los valores $b_1, \ldots, b_n \in A$, y cuyo grado sea como máximo $n-1$. Tal polinomio si existe es único, ya que si existen dos $p(X)$ y $q(X)$, como los grados son menores que n, y $p(X)-q(X)$ tiene n raíces, resulta que $p(X)-q(X)=0$. Para probar su existencia basta con definirlo; definimos polinomios $p_i(X)$ como:

$$p_i(X) = \frac{(X-a_1)\cdots(X-a_{i-1})(X-a_{i+1})\cdots(X-a_n)}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)}$$

y finalmente $p(X)$ se define como:

$$p(X) = b_1 p_1(X) + \cdots + b_n p_n(X).$$

El método de interpolación de Lagrange es un caso particular de la resolución de sistemas de congruencias, supongamos que queremos determinar un polinomio $p(X)$ tal que en el punto a_i tome el valor b_i, para i=1,...,n; entonces tenemos el sistema

$$p(X) \equiv b_i \pmod{X-a_i}\}_{i=1,\ldots,n}$$

El polinomio $p(X)$ es entonces una solución al anterior sistema.

Ejercicios

Homomorfismos

Ejercicio. 14.16.
Sea A un anillo, y $\varphi : A[X] \longrightarrow A[X]$ un homomorfismo tal que $\varphi_{|A} = id_A$. Supongamos que $\varphi(X) = f(X) \in A[X]$,

(1) Si A es un dominio de integridad (DI), ¿qué condición tiene que verificar $f(X)$ para que φ sea un isomorfismo?
(2) ¿Qué ocurre cuando A no es un DI?

Ref.: 1104e_026 *SOLUCIÓN.*

Módulos

Ejercicio. 14.17. (Ejemplo de un módulo que no es cíclico)
Sea $\mathbb{F}$ un cuerpo y X una indeterminada sobre $\mathbb{F}$. Se considera el anillo $A = \mathbb{F}[X^m]$ y el A–módulo $M = \mathbb{F}[X]$; se tiene que M no es un A–módulo cíclico, y que necesita al menos m elementos en un sistema de generadores.
Ref.: 1104e_030 *SOLUCIÓN.*

15. Factorización de polinomios

Sea A en esta sección un DFU y $p(X) \in A[X]$, definimos el **contenido** de $p(X) = a_0 + a_1X + \cdots + a_nX^n$ como

$$c(p(X)) = \text{mcd}\{a_0, a_1, \ldots, a_n\}.$$

Un polinomio $p(X)$ se llama **primitivo** si $c(p(X)) = 1$.

Lema. 15.1.
Sea A un DFU y $p(X) \in A[X]$ un polinomio no constante, entonces existe un polinomio primitivo $q(X) \in A[X]$ tal que $p(X) = cq(X)$, donde $c = c(p(X))$. Esta descomposición es única en el siguiente sentido: Si además $p(X) = c'q'(X)$, con $q'(X) \in A[X]$ primitivo y $c' \in A$, entonces c y c' son asociados en A y $q(X)$ y $q'(X)$ son asociados en $A[X]$.

Teorema. 15.2. (Lema de Gauss)
Sea A un DFU, el producto en $A[X]$ de dos polinomios primitivos es un polinomio primitivo.

DEMOSTRACIÓN. Supongamos que $p(X)$ y $q(X)$ son polinomios primitivos; si $p(X)q(X)$ no es un polinomio primitivo, entonces existe un elemento irreducible, y por tanto primo, $d \in A$ tal que d divide a todos los coeficientes de $p(X)q(X)$. Sabemos que existen coeficientes de $p(X)$ y de $q(X)$ que no son múltiplos de d, sean a_s y b_r los coeficientes con subíndice menor que no son múltiplos de d. El coeficiente de X^{s+r} en $p(X)q(X)$ es:

$$a_0b_{s+r} + \cdots + a_{s-1}b_{r+1} + a_sb_r + a_{s+1}b_{r-1} + \cdots + a_{s+r}b_0$$

es un múltiplo de d, así como todos los sumandos salvo posiblemente a_sb_r. Por tanto d también divide a a_sb_r, de donde se deduce que $d \mid a_s$ ó $d \mid b_r$, lo que es una contradicción. □

Corolario. 15.3.
Sea A un DFU, para cada par de polinomios $p(X), p'(X) \in A[X]$ se verifica: $c(p(X)p'(X)) \sim c(p(X))c(p'(X))$.

1104-02.tex

DEMOSTRACIÓN. Tenemos que $p(X) = cq(X)$ y $p'(X) = c'q'(X)$ con $c = c(p(X))$, $c' = c(p'(X))$ y $q(X)$, $q'(X)$ primitivos. Entonces tenemos $p(X)p'(X) = cc'q(X)q'(X)$ con $q(X)q'(X)$ un polinomio primitivo, por tanto

$$c(p(X)p'(X)) \sim cc' = c(p(X))c(p'(X)).$$

□

Sea K el cuerpo de fracciones de A.

Proposición. 15.4.
Sea A un DFU con cuerpo de fracciones K. Si $p(X) \in K[X]$ es un polinomio no constante, entonces existen $a, b \in A$ verificando que $p(X) = ab^{-1}q(X)$ con $q(X) \in A[X]$ un polinomio primitivo. Además $q(X)$ está unívocamente determinado salvo asociados (elementos invertibles de A).

DEMOSTRACIÓN. Ya que K es el cuerpo de fracciones de A, tenemos

$$p(X) = (a_0 b_0^{-1}) + (a_1 b_1^{-1})X + \cdots + (a_n b_n^{-1})X^n$$

para $a_i, b_i \in A$. Podemos tomar $b = \text{mcm}\{b_0, \ldots, b_n\}$, entonces $b \neq 0$, y todos los coeficientes del polinomio $bp(X)$ pertenecen a A, luego $bp(X) \in A[X]$. Además, ya que $p(X)$ no es constante, tampoco $bp(X)$ lo es. Calculamos el contenido de $bp(X)$ y lo llamamos a, entonces $bp(X) = aq(X)$ con $q(X)$ un polinomio primitivo en $A[X]$. Por tanto $p(X) = ab^{-1}q(X)$. Para estudiar la unicidad, supongamos que $p(X) = ab^{-1}q(X) = cd^{-1}q'(X)$ con $a, b, c, d \in A$ y $q(X), q'(X)$ polinomios primitivos en $A[X]$. Entonces $adq(X) = cbq'(X)$, y por ser $q(X)$ y $q'(X)$ primitivos resulta que ad y cb son asociados, luego $q(X)$ y $q'(X)$ son también asociados. □

Lema. 15.5.
Sea A un DFU con cuerpo de fracciones K, si $p(X) \in A[X]$ es un polinomio primitivo y para $a, b \in A$ el polinomio $ab^{-1}p(X)$ tiene todos sus coeficientes en A, entonces $b \mid a$.

DEMOSTRACIÓN. Ya que $ab^{-1}p(X) \in A[X]$, podemos escribirlo en $cq(X)$, con $c = c(ab^{-1}p(X))$ y $q(X)$ un polinomio primitivo en $A[X]$. Entonces $ap(X) = bcq(X)$, de donde se deduce que a y bc son asociados, luego $b \mid a$. □

Teorema. 15.6.
Sea A un DFU con cuerpo de fracciones K, si $p(X) \in A[X]$ es no constante e irreducible, entonces $p(X) \in K[X]$ es irreducible.

DEMOSTRACIÓN. Si $p(X) \in A[X]$ es no constante e irreducible, entonces es primitivo, ya que en caso contrario tendríamos una factorización propia $p(X) = c(p(X))q(X)$ con $q(X)$ un polinomio primitivo en $A[X]$. Supongamos ahora que $p(X) = p_1(X)p_2(X)$ es un factorización en $K[X]$ con los $p_i(X)$ no invertibles. Entonces existen polinomios primitivos $q_i(X) \in A[X]$ y elementos $a, b, c, d \in A$ tales que $p_1(X) = ab^{-1}q_1(X)$ y $p_2(X) = cd^{-1}q_2(X)$. Por tanto tenemos

$$p(X) = ac(bd)^{-1}q_1(X)q_2(X)$$

y

$$bdp(X) = acq_1(X)q_2(X).$$

Ya que $p(X)$, $q_1(X)$ y $q_2(X)$ son polinomios primitivos, tenemos que $p(X)$ y $q_1(X)q_2(X)$ son asociados en $A[X]$, y por ser $p(X)$ irreducible, resulta que $q_1(X)$ ó $q_2(X)$ es invertible, luego un polinomio constante, lo que es una contradicción. □

Como consecuencia los únicos elementos irreducibles en $A[X]$ son los elementos irreducibles de A y los polinomios primitivos irreducibles no constantes.

Teorema. 15.7.
Si A es un DFU, entonces $A[X]$ es un DFU.

DEMOSTRACIÓN. Supongamos que $0 \neq p(X) \in A[X]$ es no constante, y consideremos $p(X)$ como elemento de $K[X]$. Ya que K es un cuerpo, tenemos que $K[X]$ es un DE, y por tanto un DFU. Entonces existe una factorización de $p(X)$:

$$p(X) = p_1(X) \cdots p_r(X)$$

con los $p_i(X) \in K[X]$ irreducibles y por tanto primos en $K[X]$. Como ya conocemos, podemos escribir $p_i(X) = a_i b_i^{-1} q_i(X)$ con $a_i, b_i \in A$ y $q_i(X)$ polinomios primitivos en $A[X]$. Ya que $p_i(X)$ es irreducible en $K[X]$, entonces $q_i(X)$ es irreducible en $A[X]$, y tenemos la siguiente expresión para $p(X)$:

$$p(X) = (a_1 \cdots a_r)(b_1 \cdots b_r)^{-1} q_1(X) \cdots q_r(X).$$

Ya que el producto finito de polinomios primitivos es primitivo, resulta que $a_1 \cdots a_r \mid b_1 \cdots b_r$, entonces existe un elemento $d \in A$ tal que

$$p(X) = dq_1(X) \cdots q_r(X).$$

Por ser A un DFU, existe una factorización de d en elementos irreducibles; $d = d_1 \cdots d_s$. De esta forma llegamos a una factorización de $p(X)$ en irreducibles

$$p(X) = d_1 \cdots d_s q_1(X) \cdots q_r(X).$$

Para probar la unicidad supongamos que

$$p(X) = e_1 \cdots e_t h_1(X) \cdots h_v(X)$$

con los $e_m \in A$ irreducibles, $1 \leq m \leq t$, y los $h_u(X) \in A[X]$ irreducibles, $1 \leq u \leq v$. Aplicando el Lema de Gauss tenemos que $q_1(X)\cdots q_r(X)$ y $h_1(X)\cdots h_v(X)$ son polinomios primitivos en $A[X]$ y por tanto son asociados, de donde se deduce la unicidad. □

Corolario. 15.8.
Si A es un DFU, entonces para indeterminadas $X_1,\ldots,X_n$, el anillo $A[X_1,\ldots,X_n]$ es un DFU.

Criterios de irreducibilidad

Sea A un DI con cuerpo de fracciones K. Si $p(X)$ es un polinomio con coeficientes en A, decimos que $p(X)$ es **irreducible** (en $A[X]$) si no existen polinomios (que no son invertibles) $p_1(X)$, $p_2(X) \in A[X]$ tales que $p(X) = p_1(X)p_2(X)$. Esto es, es un elemento irreducible del anillo $A[X]$.

Vamos a estudiar en este apartado algunos criterios de irreducibilidad de polinomios.

Es necesario destacar que si un polinomio $p(X)$ tiene una raíz en A, entonces tiene un factor de grado uno, y por tanto es reducible en $A[X]$. El recíproco no es cierto, en general, salvo que el grado de $p(X)$ sea dos ó tres y A sea un cuerpo. Entonces para estudiar la reducibilidad de un polinomio lo primero que hay que hacer es estudiar si tiene ó no raíces.

El siguiente algoritmo que nos permite calcular las raíces de polinomios en $A[X]$ en K. Es aplicable cuando el número de elementos invertibles del anillo A es pequeño, y es útil para el cálculo de las raíces racionales de los polinomios con coeficientes enteros.

Lema. 15.9.
Sea A un DI con cuerpo de fracciones K. Si $a, b \in A$ son primos relativos, $b \neq 0$ y ab^{-1} es una raíz del polinomio $p(X) = a_0 + \cdots + a_nX^n \in A[X]$, entonces $a \mid a_0$ y $b \mid a_n$.

DEMOSTRACIÓN. Si ab^{-1} es una raíz de $p(X)$, entonces se verifica:

$$0 = p(ab^{-1}) = a_0 + a_1(ab^{-1}) + \cdots + a_n(ab^{-1})^n.$$

Multiplicando por b^n resulta

$$a_0b^n + a_1ab^{n-1} + \cdots + a_na^n = 0,$$

entonces b divide a a_n y a divide a a_0. □

Otro criterio de irreducibilidad para DI es el siguiente:

Teorema. 15.10. (Criterio de irreducibilidad por reducción)
Sean A y S dos DI y $f : A \longrightarrow S$ un homomorfismo de anillos. Si $p(X) \in A[X]$ verifica que $\text{grad}(f(p(X))) = \text{grad}(p(X))$ *y $f(p(X))$ es irreducible en $S[X]$, entonces $p(X)$ no se escribe como un producto de dos polinomios no constantes de $A[X]$.*

DEMOSTRACIÓN. Supongamos que $p(X)$ admite una descomposición del tipo anterior

$$p(X) = p_1(X)p_2(X)$$

en $A[X]$, aplicando f tenemos:

$$f(p(X)) = f(p_1(X)p_2(X)) = f(p_1(X))f(p_2(X)).$$

Ya que $\text{grad}(p(X)) = \text{grad}(f(p(X)))$, resulta que $\text{grad}(p_1(X)) = \text{grad}(f(p_i(X)))$, para $i = 1, 2$. Luego $f(p(X))$ no es irreducible en $S[X]$. □

Veamos a continuación algunas aplicaciones de este último criterio.

Ejemplo. 15.11.
El polinomio $p(X) = X^3 + X^2 + 15$ es irreducible en $\mathbb{Z}[X]$.
Consideramos la proyección canónica $\mathbb{Z} \longrightarrow \mathbb{Z}_2$ y el homomorfismo inducido entre los anillos de polinomios $f : \mathbb{Z}[X] \longrightarrow \mathbb{Z}_2[X]$. Entonces $f(p(X)) = X^3 + X^2 + 1$, ya que $f(p(X))$ es irreducible en $\mathbb{Z}_2[X]$, resulta que $p(X)$ no puede descomponerse en $\mathbb{Z}[X]$.

Ejemplo. 15.12.
El polinomio $p(X) = X^4 + 2X^3 + 7X^2 - 4X + 5$ es irreducible en $\mathbb{Z}[X]$.
Consideramos la proyección canónica $\mathbb{Z} \longrightarrow \mathbb{Z}_2$ y el homomorfismo inducido entre los anillos de polinomios $f : \mathbb{Z}[X] \longrightarrow \mathbb{Z}_2[X]$. Entonces $f(p(X)) = X^4 + X^2 + 1$, que admite la descomposición $(X^2 + X + 1)^2$, luego no es irreducible en $\mathbb{Z}_2[X]$. Consideramos la proyección canónica $\mathbb{Z} \longrightarrow \mathbb{Z}_3$ y el homomorfismo inducido entre los anillos de polinomios $g : \mathbb{Z}[X] \longrightarrow \mathbb{Z}_3[X]$. Entonces $g(p(X)) = X^4 + 2X^3 + X^2 + 2X + 2$, que admite la descomposición $(X + 1)(X^3 + X^2 + 2)$, luego no es irreducible en $\mathbb{Z}_3[X]$. Uniendo los dos resultados obtenidos tenemos que $p(X)$ es irreducible en $\mathbb{Z}[X]$. Ya que una posible descomposición en irreducibles en $\mathbb{Z}[X]$ induce una descomposición en $\mathbb{Z}_2[X]$, con lo cual la descomposición en $\mathbb{Z}[X]$ sería en producto de dos polinomios de grado dos. Y esa misma descomposición induce en $\mathbb{Z}_3[X]$ una descomposición en producto de polinomios de grado como máximo dos, lo que es una contradicción con la descomposición que hemos hallado en $\mathbb{Z}_3[X]$ como un producto de un polinomio de grado uno y un polinomio de grado tres.

Vamos a restringir nuevamente el anillo en consideración, vamos a imponer la condición de ser un DFU.

Teorema. 15.13. (Criterio de irreducibilidad de Eisenstein)
Sea A un DFU con cuerpo de fracciones K. Si $p(X) \in A[X]$ es no constante y existe un elemento primo $d \in A$ verificando:
(1) $d \nmid a_n$,
(2) $d^2 \nmid a_0$ y
(3) $d \mid a_i$, $0 \leq i \leq n-1$,

entonces $p(X)$ es irreducible en $K[X]$. Además si $p(X)$ es primitivo en $A[X]$, entonces también es irreducible en $A[X]$.

DEMOSTRACIÓN. Supongamos que $p(X) \in K[X]$ es reducible, entonces

$$p(X) = p_1(X)p_2(X)$$

con $p_1(X)$, $p_2(X) \in K[X]$ no invertible (no constantes). Existen pues elementos $a, b, c, e \in A$ y $q_1(X), q_2(X)$ polinomios primitivos en $A[X]$ tales que

$$p_1(X) = ab^{-1}q_1(X) \qquad p_2(X) = ce^{-1}q_2(X),$$

Tenemos por tanto

$$bep(X) = acq_1(X)q_2(X).$$

Simplificando por los factores comunes de be y ac podemos suponer que son primos relativos. Ya que $d \nmid a_n$, si $d \mid be$ entonces $d \mid c((ac)q_1(X)q_2(X)) = ac$, lo que es una contradicción, entonces $d \nmid be$. Por otro lado, si $d \mid ac$, entonces $d \mid c(p(X))$, y por tanto $d \mid a_n$, lo que es una contradicción. Supongamos que

$$q_1(X) = c_0 + \cdots + c_r X^r, \quad c_r \neq 0, r \geq 1,$$
$$q_2(X) = d_0 + \cdots + d_s X^s, \quad d_s \neq 0, s \geq 1,$$

entonces de $d \mid a_0$ y $d^2 \nmid a_0$ deducimos que d ó divide a c_0 ó a d_0 (solamente a uno de los dos). Supongamos que $d \mid d_0$, ya que d no divide a todos los coeficientes de $q_2(X)$ por ser este un polinomio primitivo, resulta que podemos encontrar un índice t tal que $d \nmid d_t$ y $d \mid d_j$ para todo $j \leq t$. Si consideramos ahora el coeficiente de índice t de $bep(X)$, resulta

$$bea_t = (ac)(c_0 d_t + c_1 d_{t-1} + \cdots + c_t d_0),$$

de donde deducimos que d divide a la última suma (por ser $t \leq s < n$) y a todos los sumandos menos al primero $c_0 d_t$, lo que es una contradicción. Como consecuencia $p(X)$ es un polinomio irreducible en $K[X]$. El resto se sigue de forma sencilla. □

DEMOSTRACIÓN. Supongamos que $p(X) \in K[X]$ es reducible, entonces

$$p(X) = p_1(X)p_2(X)$$

con $p_1(X), p_2(X) \in K[X]$ no invertible (no constantes). Existen pues elementos $a, b, c, e \in A$ y $q_1(X), q_2(X)$ polinomios primitivos en $A[X]$ tales que

$$p_1(X) = ab^{-1}q_1(X) \qquad p_2(X) = ce^{-1}q_2(X),$$

Tenemos por tanto

$$bep(X) = acq_1(X)q_2(X). \tag{IV.1}$$

Simplificando por los factores comunes de be y ac podemos suponer que son primos relativos. Ya que $d \nmid a_n$, si $d \mid be$ entonces $d \mid c((ac)q_1(X)q_2(X)) = ac$, lo que es una contradicción, entonces $d \nmid be$. Por otro lado, si $d \mid ac$, entonces $d \mid c(p(X))$, y por tanto $d \mid a_n$, lo que es una contradicción.
Los polinomios en la ecuación (IV.1) tienen coeficientes en A. Reducimos módulo d y tenemos

$$\overline{bea_n}X^n = \overline{ac}\,\overline{q_1(X)}\,\overline{q_2(X)}$$

Observa que el término de la izquierda es un monomio, luego es un producto de dos monomios, esto es, $\overline{q_1(X)}$ y $\overline{q_2(X)}$ son monomios; como son no constantes, resulta que los términos independientes de $q_1(X)$ y de $Q_2(X)$ son múltiplos de d. Esto es una contradicción, ya que entonces $d^2 \mid a_0$. □

Criterio de descomposición

Hasta ahora hemos tratado de determinar si un polinomio $p(X) \in A[X]$ es o no irreducible. Vamos ahora a tratar de encontrar, cuando es reducible, una descomposición en producto de polinomios no constantes.
En general los métodos de descomposición son más complicados que los criterios de irreducibilidad. Sin embargo, vamos a estudiar el método de descomposición de Kronecker que es particularmente sencillo cuando se aplica a polinomios, con coeficientes no excesivamente grandes, en el anillo $\mathbb{Z}[X]$.
Consideramos $p(X) \in \mathbb{Z}[X]$, un polinomio mónico no constante de grado n. Si $p(X)$ admite una factorización $p(X) = p_1(X)p_2(X)$ en $\mathbb{Z}[X]$, entonces, por ejemplo, $\operatorname{grad}(p_1(X)) \leq n/2$. Llamemos s a la parte entera de $n/2$. Si tomamos $s+1$ elementos distintos $a_0, \ldots, a_s$ de $\mathbb{Z}$, al valorar $p(X)$ en a_i tenemos:

$$p(a_i) = p_1(a_i)p_2(a_i), \quad 0 \leq i \leq s.$$

Luego $p_1(a_i)$ es un divisor de $p(a_i)$, y como $p(a_i)$ tiene un número finito de divisores, resulta que $p_1(a_i)$ toma valores en un conjunto finito. Por la fórmula de interpolación de Lagrange, existe un único polinomio $q(X)$ de grado menor ó igual que s tal que $q(a_i) = p_1(a_i)$, $0 \leq i \leq s$, entonces $q(X) = p_1(X)$ y tendríamos de esta forma determinado un factor de $p(X)$.
Entonces si no conocemos previamente la factorización de $p(X)$, consideramos todas las posibles elecciones de colecciones $d_0, \ldots, d_s$ con $d_i \mid p(a_i)$, $0 \leq i \leq s$. Si calculamos en cada caso el polinomio de interpolación de Lagrange, $q(X)$, tal que $q(a_i) = d_i$, $0 \leq i \leq s$, resulta que si $p(X)$ es reducible, alguno de estos polinomios debe ser un factor de $p(X)$; en cambio, si es irreducible evidentemente ninguno lo es.
Hemos encontrado pues un método de factorización de polinomios que también es un criterio de irreducibilidad. Finalmente destacar que este método puede ser aplicado también a cualquier DFU A que tenga un número finito (pequeño) de elementos invertibles y en el que tengamos algún método que permita calcular la descomposición en irreducibles.

Ejemplo. 15.14.
Estudiar si es reducible en $\mathbb{Z}[X]$ el polinomio $p(X) = X^7 - 2X^6 + 3X^5 - 2X^3 + 6X^2 - 4X + 4$ y, si lo es, encontrar una descomposición en irreducibles.

Ya que el grado es siete, resulta que $s = 3$. Consideramos esta vez tres elementos de $\mathbb{Z}$: $a_0 = -1$, $a_1 = 0$, $a_2 = 1$.
Valoramos $p(X)$ en a_i obteniendo: $p(a_0) = 10$, $p(a_1) = 4$, $p(a_2) = 6$.
Consideremos los divisores $d_0 = 2$, $d_1 = 1$, $d_2 = 2$.
Construimos el polinomio de interpolación de Lagrange

$$q(X) = 2\frac{X(X-1)}{(-1-0)(-1-1)} + 1\frac{(X+1)(X-1)}{(0+1)(0-1)} + 2\frac{(X+1)X}{(1+1)(1-0)} = X^2 + 1.$$

Y resulta que $X^2 + 1$ es irreducible y es un divisor de $p(X)$:

$$p(X) = (X^2 + 1)(X^5 - 2X^4 + 2X^3 + 2X^2 - 4X + 4)$$

Estudiamos ahora el polinomio $p_2(X) = X^5 - 2X^4 + 2X^3 + 2X^2 - 4X + 4$. Ya que su grado es cinco, resulta que $s = 2$. Consideramos tres elementos de $\mathbb{Z}$: $a_0 = -1$, $a_1 = 0$, $a_2 = 1$.
Valoramos $p_2(X)$ en a_i obteniendo: $p_2(a_0) = 5$, $p_2(a_1) = 4$, $p_2(a_2) = 3$.
Consideremos los divisores $d_0 = 5$, $d_1 = 2$, $d_2 = 1$.
Construimos el polinomio de interpolación de Lagrange

$$\begin{aligned} q(X) &= 5\frac{X(X-1)}{(-1-0)(-1-1)} + 2\frac{(X+1)(X-1)}{(0+1)(0-1)} + 1\frac{(X+1)X}{(1+1)(1-0)} \\ &= \frac{5}{2}X(X-1) - 2(x^2-1) + \frac{1}{2}(X^2+X) \\ &= \frac{1}{2}(2X^2 - 4X + 4) = X^2 - 2X + 2. \end{aligned}$$

Y resulta que $X^2 - 2X + 2$ es irreducible y es un divisor de $p_2(X)$:

$$p_2(X) = (X^2 - 2X + 2)(X^3 + 2).$$

Ya que el otro factor es irreducible, resulta que hemos obtenido una descomposición en irreducibles de $p(X)$ en la siguiente forma:

$$p(X) = (X^2 + 1)(X^2 - 2X + 2)(X^3 + 2).$$

Es conveniente destacar que en el ejemplo anterior, en el primer paso, hemos tomados menos elementos a_i de lo que indicaba el número s, esto puede ser arriesgado en casos generales, ya que estamos descartando a priori posibles factores de $p(X)$ de grado cuatro.

Ejercicios

HACER

16. Derivada de un polinomio. Raíces múltiples

Nos encaminamos ahora a estudiar las raíces múltiples de un polinomio. Para ello vamos a introducir la derivada de un polinomio de forma algebraica. Sean A un DI y X, T dos indeterminadas. Para cada $p(X) \in A[X]$ consideramos el polinomio $p(X+T) \in A[X,T]$. Este polinomio se puede escribir como un elemento de $A[X][T]$ en la forma

$$p(X+T) = p_0(X) + p_1(X)T + \cdots + p_m(X)T^m,$$

con $p_i(X) \in A[X]$, $0 \leq i \leq m$.

Es inmediato comprobar que $p_0(X) = p(X)$, y que $T \mid p(X+T) - p(X)$. Definimos la **derivada formal** del polinomio $p(X)$ como el único polinomio $Dp(X) \in A[X]$ que verifica $p(X+T) - p(X) \equiv Dp(X)T \pmod{T^2}$.

Vamos a comprobar que $Dp(X)$ está determinado de forma única. Supongamos que $q(X) \in A[X]$ verifica:

$$p(X+T) - p(X) \equiv q(X)T \pmod{T^2},$$

entonces $q(X)T \equiv Dp(X)T \pmod{T^2}$, y por tanto existe un polinomio $h(X,T) \in A[X,T]$ tal que $q(X)T - Dp(X)T = T^2 h(X,T)$, simplificando por T tenemos $q(X) - Dp(X) = Th(X,T)$, luego $q(X) = pD(X)$.

Es claro de lo anterior que $Dp(X) = p_1(X) = a_1 + a_2X + \cdots + a_nX^{n-1}$.

Lema. 16.1.
Sea A un DI, la derivada define una aplicación $D : A[X] \longrightarrow A[X]$ verificando:
(1) $D(p_1(X) + p_2(X)) = Dp_1(X) + Dp_2(X)$, para $p_1(X)$, $p_2(X) \in A[X]$.
(2) $D(ap(X)) = aDp(X)$, para $p(X) \in A[X]$ y $a \in A$.
(3) $D(p_1(X)p_2(X)) = Dp_1(X)p_2(X) + p_1(X)Dp_2(X)$, para $p_1(X)$, $p_2(X) \in A[X]$.

DEMOSTRACIÓN. (1) Tenemos $p_1(X+T) - p_1(X) \equiv Dp_1(X)T \pmod{T^2}$ y $p_2(X+T) - p_2(X) \equiv Dp_2(X)T \pmod{T^2}$, y sumando ambas expresiones

$$(p_1(X+T) + p_2(X+T)) - (p_1(X) + p_2(X)) \equiv (Dp_1(X) + Dp_2(X))T \pmod{T^2}.$$

Luego $D(p_1(X) + p_2(X)) = Dp_1(X) + Dp_2(X)$.
(2) Tenemos $p(X+T) - p(X) \equiv Dp(X)T \pmod{T^2}$ y multiplicando por a tenemos

$$ap(X+T) - ap(X) \equiv aDp(X)T \pmod{T^2}.$$

1104-03.tex

Luego $D(ap(X)) = aDp(X)$.
(3) Tenemos las expresiones $p_1(X+T) - p_1(X) \equiv Dp_1(X)T \pmod{T^2}$ y $p_2(X+T) - p_2(X) \equiv Dp_2(X)T \pmod{T^2}$. Multiplicando la primera por $p_2(X+T)$ y la segunda por $p_1(X)$ y sumando tenemos:

$$p_1(X+T)p_2(X+T) - p_1(X)p_2(X) \equiv (p_2(X+T)Dp_1(X) + p_1(X)Dp_2(X))T \pmod{T^2},$$

y ya que $p_2(X+T) \equiv p_2(X) + Dp_2(X)T \pmod{T^2}$, tenemos:

$$p_1(X+T)p_2(X+T) - p_1(X)p_2(X) \equiv (p_2(X)Dp_1(X) + p_1(X)Dp_2(X))T \pmod{T^2}.$$

Luego $D(p_1(X)p_2(X)) = p_1(X)Dp_2(X) + p_2(X)Dp_1(X)$. □

Si $p(X) \in A[X]$ y $\alpha \in A$ es una raíz de $p(X)$, llamamos **multiplicidad** de α al mayor número entero positivo k tal que $(X-\alpha)^k \mid p(X)$. Las raíces de multiplicidad uno se llaman **raíces simples**, las de multiplicidad mayor que uno se llaman **raíces múltiples**. Por extensión las raíces de multiplicidad cero son los elementos de A que no son raíces del polinomio.
Tenemos de forma inmediata que si $\alpha_1, \ldots, \alpha_r$ son raíces de $p(X)$ con multiplicidades $k_1, \ldots, k_r$, entonces $(X-\alpha_1)^{k_1} \cdots (X-\alpha_r)^{k_r} \mid p(X)$.

Proposición. 16.2.
Sea A un DI y $p(X) \in A[X]$ un polinomio, si $\alpha \in A$ entonces son equivalentes:
(a) α es una raíz múltiple de $p(X)$.
(b) $p(\alpha) = Dp(\alpha) = 0$.

DEMOSTRACIÓN. (a) ⇒ (b). Sea α una raíz múltiple de $p(X)$, entonces existe $k > 1$ tal que $p(X) = (X-\alpha)^k q(X)$ para algún polinomio $q(X) \in A[X]$. Aplicando D tenemos:

$$Dp(X) = k(X-\alpha)^{k-1}q(X) + (X-\alpha)^k Dq(X),$$

y valorando en α tenemos que $Dp(\alpha) = 0$.
(b) ⇒ (a). Ya que $p(\alpha) = 0$, resulta que α es una raíz de $p(X)$, y se tiene una factorización $p(X) = (X-\alpha)q(X)$. Aplicando D tenemos:

$$Dp(X) = q(X) + (X-\alpha)Dq(X),$$

y valorando en α tenemos

$$0 = Dp(\alpha) = q(\alpha),$$

por tanto $X - \alpha \mid q(X)$, y α es una raíz múltiple de $p(X)$. □

Corolario. 16.3.
Sea A un DI, $p(X) \in A[X]$ un polinomio y $\alpha \in A$, si α es una raíz de $p(X)$ de multiplicidad $k \geq 1$, entonces α es una raíz de multiplicidad $k-1$ de $Dp(X)$.

Vamos a tratar de afinar el resultado anterior, para ello necesitamos restringir el tipo de anillos al que se va a aplicar.

Si A es un anillo, existe un único homomorfismo de anillos $f : \mathbb{Z} \longrightarrow A$, definido por $f(n) = n1$, para cada $n \in \mathbb{Z}$. El núcleo de f es un ideal de $\mathbb{Z}$ generado por un entero positivo ó nulo m. El entero m se llama la **característica** del anillo A. Es claro que si A es un DI, entonces la característica de A es $cero$ ó un número primo; en este caso, el subanillo $\mathrm{Im}(f)$ se llama **subanillo primo** de A.

Teorema. 16.4.
Sea A un DI de característica cero. Si $\alpha \in A$ es una raíz de multiplicidad $k \geq 1$ de un polinomio $p(X) \in A[X]$, entonces α es una raíz de multiplicidad exactamente $k-1$ de $Dp(X)$.

DEMOSTRACIÓN. Supongamos que $p(X) = (X-\alpha)^k q(X)$, con $q(X) \in A[X]$, entonces tenemos:

$$Dp(X) = k(X-\alpha)^{k-1}q(X) + (X-\alpha)^k Dq(X) =$$

$$= (X-\alpha)^{k-1}(kq(X) + (X-\alpha)Dp(X)).$$

El segundo factor no se anula para α, luego la multiplicidad de α en $Dp(X)$ es exactamente $k-1$. □

Ejemplo. 16.5.
Consideramos $p(X) = X^5+1 \in \mathbb{Z}_5$, es claro que $p(X) = (X+1)^5$, luego -1 es una raíz de multiplicidad cinco de $p(X)$. Sin embargo $Dp(X) = 0$, y el Teorema (16.4.) no es aplicable.

Sin embargo, para característica distinta de cero tenemos el siguiente teorema.

Teorema. 16.6.
Sea A un DI y $p(X) \in A[X]$ un polinomio con $Dp(X) = 0$, se verifica:

(1) Si la característica de A es $cero$, entonces $p(X)$ es constante.
(2) Si la característica de A es $m \neq 0$, entonces $p(X) = q(X^p)$ para algún polinomio $q(X) \in A[X]$.

DEMOSTRACIÓN. Tenemos $Dp(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$, entonces la primera parte es inmediata. Para la segunda tenemos que $ia_i = 0$ para todo $i = 1, \ldots, n$, luego $a_i = 0$ si i no es un múltiplo de p, y por tanto el polinomio $p(X)$ tiene una expresión del tipo siguiente:

$$p(X) = a_0 + a_pX^p + a_{2p}X^{2p} + \cdots + a_{rp}X^{rp},$$

que es un polinomio del tipo indicado. □

Teorema. 16.7. (Fórmula de Taylor)
Sea A un DI de característica cero, si $p(X) \in A[X]$ es un polinomio de grado n, entonces $p(X)$ tiene una expresión del tipo

$$p(X) = p(a) + \frac{Dp(a)}{1!}(X-a) + \cdots + \frac{D^np(a)}{n!}(X-a)^n,$$

para todo $a \in A$.

DEMOSTRACIÓN. Tenemos la siguiente expresión para $p(X)$:

$$p(X) = p((X-a)+a) = b_0 + b_1(X-a) + \cdots + b_n(X-a)^n.$$

Se trata entonces de determinar los coeficientes b_i. Si denotamos por D^r aplicar r veces D, entonces tenemos:

$$D^r(b_i(X-a)^i) = \begin{cases} 0 & \text{si } r > i \\ i(i-1)\cdots(i-r+1)b_i(X-a)^{i-r} & \text{si } r \leq i \end{cases}$$

Por tanto, valorando en a tenemos:

$$D^r(b_i(X-a)^i)(a) = \begin{cases} 0 & \text{si } r > i \\ r!b_r & \text{si } r = i \\ 0 & \text{si } r < i \end{cases}$$

Entonces $D^rp(a) = r!b_r$ y como consecuencia podemos calcular el valor de cada b_r, esto es, $b_r = \frac{D^rp(a)}{r!}$. □

Para finalizar veamos una aplicación de este último resultado.

Corolario. 16.8.
Sea A un DI de característica cero, $p(X) \in A[X]$ y $\alpha \in A$, entonces son equivalentes:
(a) α es raíz de $p(X)$ de multiplicidad $k \geq 1$.
(b) $p(\alpha) = Dp(\alpha) = \ldots = D^{k-1}p(\alpha) = 0$ y $D^kp(\alpha) \neq 0$.

DEMOSTRACIÓN. (1) $\Rightarrow$ (2). Tenemos $(X-\alpha)^k \mid p(X)$, luego $p(X) = (X-\alpha)^k q(X)$, siendo $q(\alpha) \neq 0$. Se tienen entonces la igualdad:

$$Dp(X) = (X-\alpha)^{k-1}(kq(X) + (X-\alpha)Dq(X)) = (X-\alpha)^{k-1}q_1(X),$$

donde $q_1(X) = kq(X)+(X-\alpha)Dq(X)$, y α no es raíz de $q_1(X)$. Si continuamos de esta forma tenemos:

$$\begin{array}{ll} D^2p(X) & = (X-\alpha)^{k-2}((k-1)q_1(X) + (X-\alpha)Dq_1(X)) = (X-\alpha)^{k-2}q_2(X), \\ \dots & \dots\dots\dots, \\ D^{k-1}p(X) & = (X-\alpha)q_{k-1}(X), \\ D^kp(X) & = q_k(X), \end{array}$$

donde los polinomios $q_2(X), \dots, q_k(X)$ se han ido construyendo de la misma forma que $q_1(X)$, y para los cuales α no es raíz. Se tiene entonces el resultado.
(2) $\Rightarrow$ (1). Aplicando la fórmula de Taylor para $p(X)$ en $\alpha \in A$ tenemos:

$$p(X) = \frac{D^kp(\alpha)}{k!}(X-\alpha)^k + \cdots + \frac{D^np(\alpha)}{n!}(X-\alpha)^n = (X-\alpha)^kq(X),$$

donde $q(X) = \frac{D^kp(\alpha)}{k!} + \cdots + \frac{D^np(\alpha)}{n!}(X-\alpha)^{n-k} \in A[X]$ verifica $q(\alpha) \neq 0$, luego α es una raíz de exactamente multiplicidad k de $p(X)$. □

Ejercicios

Raíces múltiples

Ejercicio. 16.9.
Sea K un cuerpo de característica cero, $f(X) \in K[X]$ y $\alpha \neq 0$ una raíz de $f(X)$. Demuestra que α es una raíz doble de $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ si, y sólo si, es raíz de $a_{n-1}X^{n-1} + 2a_{n-2}X^{n-2} + \cdots + (n-1)a_1X + na_0$.
Ref.: 1104e_002 *SOLUCIÓN.*

Ejercicio. 16.10.
Se considera el polinomio $X^3 - 4X^2 + 5X + k \in \mathbb{Q}[X]$, halla $k \in \mathbb{Z}$ para que el polinomio admita una raíz doble, y en ese caso resolver la ecuación $X^3 - 4X^2 + 5X + k = 0$.
Ref.: 1104e_010 *SOLUCIÓN.*

Ejercicio. 16.11.
Estudia los siguientes enunciados:

(a) Demuestra que el polinomio $f(X) = X^3 + 2X^2 + 5X + k \in \mathbb{Z}$ es irreducible sobre $\mathbb{Q}$ si k es impar.
(b) Demuestra que $f(X)$ no tiene raíces múltiples sea cual sea el valor de k.
(c) Para k impar di si son ó no cuerpos los siguientes anillos cocientes:

$$\mathbb{Q}[X]/(f(X)), \quad \mathbb{R}[X]/(f(X)), \quad \mathbb{C}[X]/(f(X)).$$

Ref.: 1104e_011 *SOLUCIÓN.*

17. Polinomios simétricos

Consideramos $A[X_1,\dots,X_r]$, el anillo de polinomios en las indeterminadas $X_1,\dots,X_r$ con coeficientes en A.
Cada permutación $\sigma \in S_r$ define un homomorfismo de anillos

$$f_\sigma : A[X_1,\dots,X_r] \longrightarrow A[X_1,\dots,X_r] : \quad f_\sigma(X_i) = X_{\sigma(i)}, 1 \le i \le r.$$

Es claro que f_σ es un isomorfismo de anillos con inverso $f_{\sigma^{-1}}$.
Un polinomio $p(X) \in A[X_1,\dots,X_r]$ se llama **simétrico** si es invariante por f_σ, para cada $\sigma \in S_r$, esto es, $f_\sigma(p(X)) = p(X)$, para todo $\sigma \in S_r$.

Ejemplo. 17.1.
(1) Los polinomios $X_1^k + \cdots + X_r^k$ y $\prod\{X_i - X_j \mid \ i \neq j,\ 1 \le i,j \le r\}$ son polinomios simétricos en $A[X_1,\dots,X_r]$.
(2) Todo polinomio de $A[X]$ es simétrico en $A[X]$.
(3) El polinomio $X_1 + X_2$ no es simétrico en $A[X_1,X_2,X_3]$, aunque sí lo es en $A[X_1,X_2]$.

Lema. 17.2.
Sea A un anillo, el conjunto $\mathrm{Sim}(A[X_1,\dots,X_r])$ *de todos los polinomios simétricos de $A[X_1,\dots,X_r]$ es un subanillo de $A[X_1,\dots,X_r]$ que contiene a A.*

DEMOSTRACIÓN. Ya que todo polinomio constante es simétrico, tenemos una inclusión de anillos $A \subseteq \mathrm{Sim}(A[X_1,\dots,X_r])$. Supongamos que $p, q \in \mathrm{Sim}(A[X_1,\dots,X_r])$, entonces aplicando f_σ tenemos:

$$f_\sigma(p+q) = f_\sigma(p) + f_\sigma(q) = p + q,$$
$$f_\sigma(pq) = f_\sigma(p) f_\sigma(q) = pq.$$

□

Recordemos que un polinomio en $A[X_1,\dots,X_r]$ se llama **homogéneo** si todos sus monomios tienen el mismo grado. Todo polinomio de $A[X_1,\dots,X_r]$ se puede expresar de forma única como una suma de polinomios homogéneos. Para cada $0 \neq p \in A[X_1,\dots,X_r]$ tenemos pues una única expresión del tipo

$$p = p_0 + p_1 + \cdots + p_n,$$

con $p_i \in A[X_1,\dots,X_r]$ homogéneo de grado i, $0 \le i \le n$, para un cierto entero no negativo n, con $p_n \neq 0$. Los polinomios p_i se llaman las **componentes homogéneas** de p.

1104-04.tex

Proposición. 17.3.
Un polinomio $p \in A[X_1,\dots,X_r]$ es simétrico si, y sólo si, cada una de sus componentes homogéneas lo es.

Como consecuencia de esta Proposición podemos reducir el estudio de los polinomios simétricos al estudio de los polinomios simétricos homogéneos, ver Teorema (17.4.)
Vamos a determinar la estructura del anillo $\mathrm{Sim}(A[X_1,\dots,X_r])$. Para ello en primer lugar vamos a ver que existe un conjunto de r polinomios que genera $\mathrm{Sim}(A[X_1,\dots,X_r])$ como anillo.
Para ello consideramos el polinomio $p = p(X_1,\dots,X_r,T) \in A[X_1,\dots,X_r,T] = A[T][X_1,\dots,X_r]$, definido por:

$$p = (T-X_1)\cdots(T-X_r).$$

Tenemos que $p \in \mathrm{Sim}(A[T][X_1,\dots,X_r])$. Como elemento del anillo $A[X_1,\dots,X_r][T]$ el polinomio p se escribe en la forma

$$p = T^r + (-1)e_1T^{r-1} + (-1)^2e_2T^{r-2} + \cdots + (-1)^{r-1}e_{r-1}T + (-1)^re_r,$$

donde cada sumando es un polinomio de grado r en las indeterminadas $T, X_1, \dots, X_r$. Por lo tanto cada e_i es un polinomio homogéneo de grado i. Y es fácil comprobar que cada e_i es un polinomio simétrico en $A[X_1,\dots,X_r]$.
Los polinomios e_i se llaman **polinomios simétricos elementales** en las variables $X_1,\dots,X_r$, y tienen las siguientes expresiones:

$$\begin{aligned}
e_1 &= \textstyle\sum_{i=1}^{r} X_i = X_1 + \cdots + X_r,\\
e_2 &= \textstyle\sum_{i_1<i_2} X_{i_1}X_{i_2} = X_1X_2 + X_1X_3 + \cdots + X_{r-1}X_r,\\
&\cdots\\
e_r &= \textstyle\sum_{i_1<\dots<i_r} X_{i_1}\cdots X_{i_r} = X_1X_2\cdots X_r,
\end{aligned}$$

que se representan abreviadamente también por

$$(X_1),\ (X_1X_2),\ \dots,\ (X_1X_2\dots X_r),$$

ó por

$$\sum X_1,\ \sum X_1X_2,\ \dots,\ \sum X_1X_2\cdots X_n,$$

respectivamente.
El siguiente Teorema prueba que estos polinomios son un conjunto de generadores del subanillo $\mathrm{Sim}(A[X_1,\dots,X_r])$.

Teorema. 17.4. (Teorema fundamental de los polinomios simétricos)
El subanillo de $A[X_1,\dots,X_r]$ generado por A y los polinomios simétricos elementales $e_1, e_2, \dots, e_r$ coincide con $\mathrm{Sim}(A[X_1,\dots,X_r])$.

Un enunciado equivalente a éste, que es el que vamos a demostrar, es el siguiente:
Todo polinomio simétrico homogéneo del anillo $A[X_1,\dots,X_r]$ se puede expresar como un polinomio con coeficientes en A en las variables $e_1, e_2, \dots, e_r$.

DEMOSTRACIÓN. Definimos una relación de preorden entre los monomios, no nulos, de un polinomio simétrico homogéneo a partir de:

$$aX_1^{k_1}\cdots X_r^{k_r} > bX_1^{h_1}\cdots X_r^{h_r}, \quad a \text{ y } b \text{ no nulos},$$

si para el primer entero t tal que $k_t \neq h_t$ se tiene $k_t > h_t$ (orden lexicográfico). Por ejemplo, se tiene $X_1^2X_2^2 > X_1^2X_2X_3^3$. Supongamos que p es un polinomio simétrico homogéneo no nulo, agrupamos en un sólo monomio todos los monomios $aX_1^{k_1}\cdots X_r^{k_r}$ y $bX_1^{h_1}\cdots X_r^{h_r}$ que verifiquen $k_i = h_i$ para todo $1 \leq i \leq r$. De esta forma la relación definida anteriormente entre los monomios de p define ahora una relación de orden estricta. Consideramos el mayor monomio de p al que vamos a llamar $aX_1^{k_1}\cdots X_r^{k_r}$. Tenemos que $k_1 \geq k_2 \geq \cdots \geq k_r$, ya que si existen índices $i < j$ tales que $k_i \leq k_j$, entonces el monomio $aX_1^{k_1}\cdots X_i^{k_j}\cdots X_j^{k_i}\cdots X_r^{k_r}$ es mayor que $aX_1^{k_1}\cdots X_r^{k_r}$, lo que es una contradicción. Determinamos ahora un producto $e_1^{b_1}\cdots e_r^{b_r}$ tal que el monomio mayor sea precisamente $X_1^{k_1}\cdots X_r^{k_r}$, para ello observamos que deben de verificarse las siguientes relaciones:

$$\begin{aligned} k_1 + k_2 + \cdots + k_r &= b_1 + 2b_2 + \cdots + rb_r,\\ k_1 &= b_1 + b_2 + \cdots + b_r,\\ k_2 &= b_2 + \cdots + b_r,\\ k_3 &= b_3 + \cdots + b_r,\\ &\vdots\\ k_r &= b_r. \end{aligned}$$

Tenemos entonces que $b_i = k_i - k_{i+1}$, para $1 \leq i \leq r$, siendo $k_{r+1} = 0$.
La diferencia

$$q = p - ae_1^{b_1}\cdots e_r^{b_r},$$

es cero ó es un polinomio simétrico y homogéneo, del mismo grado que p, cuyo monomio mayor es más pequeño que el monomio mayor de p. En el primer caso tenemos la igualdad:

$$p = ae_1^{b_1}\cdots e_r^{b_r},$$

y en el segundo podemos aplicar a q el mismo proceso que a p. Obteniendo un nuevo polinomio simétrico y homogéneo que es cero ó es del mismo grado que q y cuyo monomio mayor es más pequeño que el monomio mayor que q.
Este proceso en algún momento ha de llegar a obtener un polinomio cero, y entonces tendremos una descomposición de p como una combinación de los polinomios simétricos elementales. □

Una propiedad de esta descomposición es que es única. Supongamos que tenemos dos expresiones $p = h(e_1,\dots,e_r) = k(e_1,\dots,e_r)$ de p como polinomio en los e_i con coeficientes en A, entonces se verifica:

$$0 = h(e_1,\dots,e_r) - k(e_1,\dots,e_r) = l(e_1,\dots,e_r) = q(X_1,\dots,X_r).$$

Vamos a ver que cada coeficiente de $l(e_1,\dots,e_r)$ es cero; en caso contrario existe algún monomio no nulo; supongamos que $l_1 = ae_1^{b_1}\cdots e_r^{b_r}$ es un monomio no nulo de $l(e_1,\dots,e_r)$ de grado máximo. Sea $aX_1^{k_1}\cdots X_r^{k_r}$ el mayor monomio de l_1, entonces tenemos la igualdades $b_i = k_i - k_{i+1}$, para $1 \le i \le r$ y $k_1 \ge \cdots \ge k_r$. Ya que $q(X_1,\dots,X_r)$ es nulo, debe de existir otro monomio de $l(e_1,\dots,e_r)$ que contenga un monomio no nulo del tipo $a'X_1^{k_1}\cdots X_r^{k_r}$. Si este monomio es $a'e_1^{c_1}\cdots e_r^{c_r}$, entonces también se verifica $c_i = k_i - k_{i+1} = b_i$, para $1 \le i \le n$, lo que implica la igualdad de los monomios $ae_1^{b_1}\cdots e_r^{b_r}$ y $a'e_1^{c_1}\cdots e_r^{c_r}$, y esto es una contradicción.
Podemos enunciar el resultado, así obtenido, en una forma más sencilla, y obtener, como consecuencia, una descripción completa del anillo $\mathrm{Sim}(A[X_1,\dots,X_r])$.

Corolario. 17.5.
Existe un isomorfismo de anillos

$$\omega : A[X_1,\dots,X_r] \longrightarrow \mathrm{Sim}(A[X_1,\dots,X_r]),$$

definido por $\omega(a) = a$ *para todo* $a \in A$ *y* $\omega(X_i) = e_i$, *para* $1 \le i \le r$.

Veamos a continuación cómo se utiliza el método seguido en la demostración del Teorema para expresar un polinomio simétrico homogéneo como una combinación lineal de los polinomios simétricos elementales.

Ejemplo. 17.6.
Sea p el polinomio simétrico $p = (X_1+X_2)(X_1+X_3)(X_2+X_3)$. Si desarrollamos p obtenemos

$$p = X_1^2X_2 + X^2X_3 + X_1X_2^2 + 2X_1X_2X_3 + X_3^2X_1 + X_2^2X_3 + X_2X_3^2.$$

Si ordenamos sus monomios en forma descendente, el mayor resulta ser $X_1^2X_2$, entonces $k_1 = 2$, $k_2 = 1$ y $k_3 = 0$. Tenemos, según la notación del Teorema, que $b_1 = 1$, $b_2 = 1$ y $b_3 = 0$. Llamamos q al nuevo polinomio:

$$q = p - e_1^1e_2^1e_3^0 = p - e_1e_2 = -X_1X_2X_3.$$

Finalmente resulta que $q = -e_3$, luego la expresión de p es:

$$p = e_1e_2 - e_3.$$

A continuación vamos a mostrar otro método más práctico, para calcular la expresión de p en función de los polinomios simétricos elementales, cuando el número de indeterminadas es pequeño.
Como ya conocemos por el Corolario (17.5.), p admite una expresión única en función de los polinomios e_i con coeficientes en A. Vamos a considerar una expresión general con coeficientes indeterminados, e intentar calcular cuales deben ser estos coeficientes.

Ya que p es un polinomio simétrico y homogéneo de grado 3, consideramos todos los polinomios de grado tres que podemos formar con los polinomios simétricos elementales. En este caso son: e_1^3, e_1e_2 y e_3. Y ahora se considera la combinación lineal en A

$$p = \alpha e_1^3 + \beta e_1e_2 + \gamma e_3.$$

La expresión anterior es una igualdad de polinomios en X_1, X_2 y X_3. Resulta que la igualdad se sigue manteniendo al evaluar las indeterminadas X_1, X_2 y X_3. Luego dando valores a X_1, X_2 y X_3, obtenemos relaciones que han de verificar α, β y γ. Veamos algunas de ellas:

$$X_1 = 1, \quad X_2 = 0 = X_3, \quad 0 = \alpha(1) + \beta(0) + \gamma(0),$$

de donde resulta que $\alpha = 0$. Tenemos la siguiente expresión de p:

$$p = \beta e_1e_2 + \gamma e_3.$$

Damos ahora los valores:

$$X_1 = 1 = X_2, \quad X_3 = 0, \quad 2 = \beta(2) + \gamma(0),$$

de donde resulta que $\beta = 1$. Tenemos la expresión de p

$$p = e_1e_2 + \gamma e_3.$$

Damos ahora los valores:

$$X_1 = 1 = X_2, X_3 = -2, \qquad 2 = 0 + \gamma(-2),$$

de donde resulta que $\gamma = -1$. La expresión definitiva de p es:

$$p = e_1e_2 - e_3.$$

Resultante

Veamos que el uso de los polinomios simétricos permite estudiar fácilmente cuando dos polinomios, con coeficientes en un DI, tienen raíces comunes. Conviene aclarar algo en este punto. Supongamos que A es un DI con cuerpo de fracciones K, y sean $p, q \in A[X]$. Puede ocurrir que alguno de estos polinomios no tenga sus raíces en K. Este problema lo solucionamos admitiendo el siguiente hecho: *Sea p un polinomio con coeficientes en un cuerpo K, entonces existe otro cuerpo F, que contiene a K como subcuerpo, tal que p tiene en $F[X]$ una descomposición en la siguiente forma:* $p(X) = a_n(X - \alpha_1)\cdots(X - \alpha_n)$. Podemos por tanto suponer que en F se tiene también una descomposición de q como $q(X) = b_m(X - \beta_1)\cdots(X - \beta_m)$.
Sea A un DI y sea K su cuerpo de fracciones. Sean $p(X), q(X) \in A[X]$ dos polinomios con expresiones:

$$p(X) = a_0 + a_1X + \ldots + a_nX^n, \;\; a_n \neq 0, n \geq 1,$$
$$q(X) = b_0 + b_1X + \ldots + b_mX^m, \;\; b_m \neq 0, m \geq 1.$$

Lema. 17.7.
En la situación anterior, si A es un DFU, son equivalentes:

(a) Los polinomios $p(X)$ y $q(X)$ tienen de mcd *un polinomio no constante. (¡No son primos relativos!).*

(b) Existen polinomios no nulos $p_1(X)$ y $q_1(X) \in A[X]$ tales que

$$\operatorname{grad}(p_1(X)) \leq n-1, \quad \operatorname{grad}(q_1(X)) \leq m-1 \quad y \quad p(X)q_1(X) = q(X)p_1(X).$$

DEMOSTRACIÓN. (a)⇒(b). Sea $d(X)$ un mcd de $p(X)$ y $q(X)$ en $K[X]$ no constante, entonces $p(X) = d(X)p_1(X)$ y $q(X) = d(X)q_1(X)$, de donde resulta que $p(X)q_1(X) = q(X)p_1(X)$. Además, se tiene que $\operatorname{grad}(p_1(X)) < \operatorname{grad}(p(X)) = n$ y $\operatorname{grad}(q_1(X)) < \operatorname{grad}(q(X)) = m$.

(b)⇒(a). Por la hipótesis (b) tenemos $p(X)q_1(X) = q(X)p_1(X)$. Factorizamos ambos miembros en factores irreducibles en $K[X]$. Al ser el grado de $p_1(X)$ estrictamente menor que el de $p(X)$, algún factor irreducible ha de dividir a $p(X)$ y no a $p_1(X)$, luego debe dividir a $q(X)$, y por tanto $p(X)$ y $q(X)$ tienen un mcd no constante. □

Supongamos que los polinomios $p_1(X)$ y $q_1(X)$ tienen las expresiones

$$\begin{aligned} p_1(X) &= c_0 + c_1X + \ldots + c_{n-1}X^{n-1}, \\ q_1(X) &= d_0 + d_1X + \ldots + d_{m-1}X^{m-1}, \end{aligned}$$

entonces de la igualdad del Lema se deduce $p(X)q_1(X) - q(X)p_1(X) = 0$, luego los $n+m$ coeficientes de este polinomio son iguales a cero, si escribimos esto en una lista tenemos las siguientes igualdades:

$$\left.\begin{array}{lllllll} a_0d_0 & & & -b_0c_0 & & & = 0 \\ a_1d_0 & +a_0d_1 & & -b_1c_0 & -b_0c_1 & & = 0 \\ a_2d_0 & +a_1d_1 & +a_0d_2 & -b_2c_0 & -b_1c_1 & -b_0c_2 & = 0 \\ \vdots & & & & & & \\ a_nd_{m-2} & +a_{n-1}d_{m-1} & & -b_mc_{n-2} & -b_{m-1}c_{n-1} & & = 0 \\ a_nd_{m-1} & & & -b_mc_{n-1} & & & = 0 \end{array}\right\}$$

Que es un sistema de ecuaciones lineales en las incógnitas $d_0, \ldots, d_{m-1}, -c_0, \ldots, -c_{n-1}$. (El considerar $-c_i$ es para que los coeficientes vayan afectados por el signo "+"). Es pues un sistema homogéneo de $n+m$ ecuaciones en $n+m$ incógnitas. Este sistema tiene solución (no trivial) si, y sólo si, el determinante del sistema es igual a cero.

El determinante de este sistema de llama la **resultante de Euler-Sylvester-Cayley** de $p(X)$ y $q(X)$.

Proposición. 17.8.
En la situación anterior los polinomios $p(X)$ y $q(X)$ tienen un mcd *no constante si, y sólo si, su resultante es igual a cero.*

La resultante de $p(X)$ y $q(X)$ se suele representar por $R(p(X),q(X))$, y tiene la expresión

$$R(p(X),q(X)) = \begin{vmatrix} a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n \\ b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m \end{vmatrix}$$

donde el determinante tiene $n+m$ filas, m filas para los a_i y n filas para los b_j.

Observación. 17.9.
En algunos textos la resultante aparece también descrita como

$$R(p(X),q(X)) = \begin{vmatrix} a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 \end{vmatrix}$$

Es fácil observar que ambas expresiones dan el mismo valor, y que esta expresión se tiene al trabajar por columnas.

Ejemplo. 17.10.
Se consideran los polinomios

$$p(X) = 2 + 3X + 4X^2,$$
$$q(X) = 1 + 5X + 6X^2 + 7X^3.$$

La resultante de $p(X)$ y $q(X)$ es:

$$R(p(X),q(X)) = \begin{vmatrix} 2 & 3 & 4 & 0 & 0 \\ 0 & 2 & 3 & 4 & 0 \\ 0 & 0 & 2 & 3 & 4 \\ 1 & 5 & 6 & 7 & 0 \\ 0 & 1 & 5 & 6 & 7 \end{vmatrix}$$

Llamamos **matriz resultante** de $p(X)$ y $q(X)$ a la matriz

$$MR(p(X),q(X)) = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n \\ b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m \end{pmatrix}$$

Observa que para los polinomios $p_1(X) = \sum_0^{m-1} c_i X^i$ y $q_1(X) = \sum_1^{n-1} d_i X^i$, de grados $m-1$ y $n-1$, respectivamente, se tiene

$$(c_0,\cdots,c_{m-1},d_0,\ldots,d_{n-1})MR(p(X),q(X)) = (e_0,\ldots,e_{m+n-1}),$$

siendo $p_1(X)p(X) + q_1(X)q(X) = \sum_{i=0}^{m+n-1} e_i X^i$.
Para los dos siguientes resultados, ver también el Teorema (17.13.).

Proposición. 17.11.
Dados dos polinomios $p(X)$ y $q(X)$, de grado n y m, respectivamente, existen polinomios $p_2(X)$ y $q_2(X)$, de grado menor que m y n, respectivamente, tales que $p_2(X)p(X) + q_2(X)q(X) = R(p(X),q(X))$.

DEMOSTRACIÓN. Ya que se tiene $\mathrm{adj}(MR(p(X),q(X)))MR(p(X),q(X)) = R(p(X),q(X))I_{m+n-1}$, basta considerar la primera fila de la matriz $\mathrm{adj}(MR(p(X),q(X)))$, y escribirla como

$$(c_0,\cdots,c_{m-1},d_0,\ldots,d_{n-1});$$

se tiene entonces

$$(c_0,\cdots,c_{m-1},d_0,\ldots,d_{n-1})MR(p(X),q(X)) = (R(p(X),q(X)),0,\ldots,0).$$

Basta definir $p_1(X) = \sum_{i=0}^{m-1} c_i X^i$ y $q_1(X) = \sum_{i=0}^{n-1} d_i X^i$. □

Corolario. 17.12.
En la situación anterior los polinomios $p_2(X)$ y $q_2(X)$ son únicos si $R(p(X),q(X)) \neq 0$.

DEMOSTRACIÓN. Supongamos que $R(p(X),q(X)) \neq 0$ y que existan polinomios $p_3(X)$ y $q_3(X)$, de grado menor que m y n, respectivamente, tales que $p_3(X)p(X)+q_3(X)q(X) = R(p(X),q(X))$, entonces se tiene $(p_2(X)-p_3(X))p(X)+(q_2(X)-q_3(X))q(X) = 0$. Conocemos que son equivalentes $R(p(X),q(X)) = 0$ y $p(X)$ y $q(X)$ no son primos relativos; por lo tanto, en nuestro caso $p(X)$ y $q(X)$ son primos relativos, y por tanto $q(X)|(p_2(X)-p_3(X))$, lo que implica $p_2(X) = p_3(X)$, ya que $\operatorname{grad}(p_i(X)) \leq \operatorname{grad}(q(X))$. Del mismo modo se prueba que $q_2(X) = q_3(X)$. □

Vamos a calcular otras expresiones más útiles de la resultante. Si $p(X) \in A[X]$, podemos suponer que $p(X)$ tiene n raíces, $\alpha_1,\ldots,\alpha_n$, en K, el cuerpo de fracciones de A. Tenemos

$$p(X) = a_n(X-\alpha_1)\cdots(X-\alpha_n),$$

los coeficientes de $p(X)$ están determinados por las raíces mediante las igualdades:

$$\begin{array}{ll} a_0/a_n & = (-1)^n \sum \alpha_1\cdots\alpha_n \qquad = (-1)^n\alpha_1\cdots\alpha_n, \\ a_1/a_n & = (-1)^{n-1}\sum \alpha_1\ldots\alpha_{n-1}, \\ \vdots & \\ a_{n-1}/a_n & = (-1)\sum \alpha_1 \qquad\qquad = -(\alpha_1+\cdots+\alpha_n), \end{array}$$

por tanto los a_i/a_n, $0 \leq i \leq n-1$, son polinomios simétricos en los α_j, $1 \leq j \leq n$.

Teorema. 17.13.
En la situación anterior se verifica:

(1) La resultante $R(p(X),q(X))$ es un polinomio homogéneo de grado m en los a_i, y de grado n en los b_j.
(2) Existen polinomios $P(X)$ y $Q(X)$, con coeficientes polinomios en los a_i y b_j y grados acotados por $n-1$ y $m-1$, respectivamente, verificando $R(p(X),q(X)) = p(X)Q(X)+q(X)P(X)$.
(3) Si $p(X)$ tiene raíces $\alpha_1,\ldots,\alpha_n$, y $q(X)$ tiene raíces $\beta_1,\ldots,\beta_m$, en $K[X]$, entonces

$$R(p(X),q(X)) = a_n^m \prod_{i=1}^{n} q(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} p(\beta_j)$$

$$= a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j).$$

DEMOSTRACIÓN. (1). Si calculamos la resultante de los polinomios $Tp(X)$ y $q(X)$, resulta que las m primeras filas del determinante están multiplicadas por T, y es claro que se tiene

$$R(Tp(X),q(X)) = T^m R(p(X),q(X)),$$

por tanto $R(p(X),q(X))$ es un polinomio homogéneo de grado m es los a_i. Análogamente se tiene para los b_j.

(2). Consideramos $R(p(X), q(X))$; multiplicamos la columna k por X^{n+m-k} y la sumamos a la columna $n+m$; hacemos esto para todo k verificando $1 \leq k \leq n+m-1$. El determinante $R(p(X), q(X))$ no cambia de valor, pero la columna $n+m$ es:

$$X^{m-1}p(X),\ X^{m-2}p(X),\ \ldots,\ p(X),\ X^{n-1}q(X),\ \ldots,\ q(X).$$

Desarrollando el determinante por esta columna tenemos:

$$R(p(X), q(X)) = p(X)(d'_0 + d'_1X + \cdots + d'_{m-1}X^{m-1}) + q(X)(c'_0 + c'_1X + \cdots + c'_{n-1}X^{n-1}),$$

siendo los coeficientes d'_h, c'_k polinomios en los a_i y b_j.
(3). Para una indeterminada T definimos $R(T) = R(p(X), q(X) - T)$. Para cada $1 \leq i \leq n$ llamamos $\gamma_i = q(\alpha_i)$. Se verifica $R(\gamma_i) = 0$ para cada i, ya que $p(X)$ y $q(X) - \gamma_i$ tienen a α_i como raíz común. Al hacer el desarrollo del determinante $R(T)$ obtenemos un polinomio de grado n en T cuyo coeficiente líder es: $(-1)^n a_n^m$. (Esto es consecuencia de que el sumando con mayor grado en T se obtiene multiplicando los elementos de la diagonal de $R(p(X), q(X) - T)$). Ya conocemos las raíces de este polinomio, que son: $\gamma_1, \ldots, \gamma_n$, entonces $R(T)$ tiene la siguiente expresión:

$$R(T) = (-1)^n a_n^m (T - \gamma_1)\cdots(T - \gamma_n) = a_n^m(\gamma_1 - T)\cdots(\gamma_n - T).$$

Además tenemos la igualdad:

$$\gamma_i = q(\alpha_i) = b_m \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

Ahora evaluando $R(T)$ en $T = 0$ tenemos:

$$R(p(X), q(X)) = R(0) = a_n^m \textstyle\prod_{i=1}^n \gamma_i = a_n^m \prod_{i=1}^n (b_m \prod_{j=1}^m (\alpha_i - \beta_j))$$

$$= a_n^m b_m^n \textstyle\prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j).$$

Para comprobar el resto basta considerar las igualdades

$$p(\beta_j) = a_n \prod_{i=1}^{n} (\beta_j - \alpha_i) = a_n (-1)^n \prod_{i=1}^{n} (\alpha_i - \beta_j)$$

y hacer los siguientes cálculos:

$$\begin{aligned}(-1)^{nm} b_m^n \textstyle\prod_{j=1}^m p(\beta_j) &= (-1)^{nm} b_m^n \prod_{j=1}^m (a_n (-1)^n \prod_{i=1}^n (\alpha_i - \beta_j)) \\ &= (-1)^{nm} b_m^n a_n^m (-1)^n m \textstyle\prod_{j=1}^m \prod_{i=1}^n (\alpha_i - \beta_j) = R(p(X), q(X)).\end{aligned}$$

□

Observa que la resultante de dos polinomios se obtiene como una expresión polinómica de los coeficientes, y también como un producto de las diferencias de las raíces, que sabemos que existen en algún cuerpo $F \supseteq K \supseteq A$, por tanto $p(X)$ y $q(X)$ tienen una raíz común si, y sólo si, su resultante es nula.
Vamos a estudiar un algoritmo para el cálculo de la resultante de dos polinomios basado en el algoritmo de Euclides, de forma que reduzcamos al mínimo el número de operaciones a hacer.

Lema. 17.14.
En la situación anterior se tiene:

$$R(p(X),q(X)) = (-1)^{nm}R(q(X),p(X)).$$

DEMOSTRACIÓN. Es consecuencia de que si en un determinante se permutan entre si dos filas, entonces el valor del determinante cambia de signo. □

Lema. 17.15.
Consideremos polinomios $p(X)$, $q(X) \in A[X]$ verificando:

$$q(X) = p(X)c(X) + r(X), \text{ con } c(X), r(X) \in A[X] \text{ y } \operatorname{grad}(r(X)) < \operatorname{grad}(p(X)),$$

entonces

$$R(p(X),q(X)) = a_n^{m-\operatorname{grad}(r(X))}R(p(X)),r(X)).$$

DEMOSTRACIÓN. Vamos a utilizar la nota anterior para suponer que las raíces de $p(X)$ están en K, tenemos entonces:

$$\begin{aligned} R(p(X),q(X)) &= a_n^m \textstyle\prod_{i=1}^n q(\alpha_i) = a_n^m \prod_{i=1}^n (p(\alpha_i)c(\alpha_i) + r(\alpha_i)) \\ &= a_n^m \textstyle\prod_{i=1}^n r(\alpha_i) = a_n^{m-\operatorname{grad}(r(X))} a_n^{\operatorname{grad}(r(X))} \prod_{i=1}^n r(\alpha_i) \\ &= a_n^{m-\operatorname{grad}(r(X))} R(p(X),r(X)). \end{aligned}$$

□

Vamos a aplicar los Lemas anteriores, para calcular la resultante de dos polinomios, $p(X)$ y $q(X)$. Supongamos que $\operatorname{grad}(p(X)) \leq \operatorname{grad}(q(X))$, entonces existen polinomios $c(X)$ y $r(X)$ verificando $q(X) = p(X)c(X) + r(X)$ y $\operatorname{grad}(r(X)) < \operatorname{grad}(p(X))$. Se tiene entonces:

$$R(p(X),q(X)) = a_n^{m-\operatorname{grad}(r(X))}R(p(X),r(X)) = (-1)^{n\operatorname{grad}(r(X))}a_n^{m-\operatorname{grad}(r(X))}R(r(X),p(X)).$$

Evidentemente este proceso podemos reiterarlo hasta llegar a que uno de los dos polinomios sea constante. En el siguiente Lema resolvemos este caso.

Lema. 17.16.
Si $a \in A$, entonces $R(p(X), a) = a^n$.

DEMOSTRACIÓN. Trivial. □

Podemos, en este punto, completar la definición de resultante definiendo para a, $b \in K$ no nulos $R(a, b) = 1$ y si alguno de ellos es cero, entonces $R(a, b) = 0$.

Ejercicio. 17.17.
Calcula la resultante de los polinomios

$$p(X) = X^4 + 10X^3 + 35X^2 + 50X + 24,$$
$$q(X) = X^5 + 30X^4 + 355X^3 + 2070X^2 + 5944X + 6720.$$

SOLUCIÓN. Tenemos las siguientes divisiones:

$$q(X) = p(X)c_1(X) + r_1(X), \quad \begin{cases} c_1(X) = X + 20, \\ r_1(X) = 120X^3 + 1320X^2 + 4920X + 6240, \end{cases}$$
$$p(X) = r_1(X)c_2(X) + r_2(X), \quad \begin{cases} c_2(X) = \frac{1}{120}X - \frac{1}{120}, \\ r_2(X) = 5X^2 + 39X + 76, \end{cases}$$
$$r_1(X) = r_2(X)c_3(X) + r_3(X), \quad \begin{cases} c_3(X) = 24X + \frac{384}{5}, \\ r_3(X) = \frac{504}{5}X + \frac{2016}{5}, \end{cases}$$
$$r_2(X) = r_3(X)c_4(X) + r_4(X), \quad \begin{cases} c_4(X) = \frac{25}{504}X + \frac{95}{504}, \\ r_4(X) = 0. \end{cases}$$

Luego la resultante de $p(X)$ y $q(X)$ es 0. □

Ejercicio. 17.18.
Calcula la resultante de los polinomios

$$p(X) = X^4 + 10X^3 + 35X^2 + 50X + 24,$$
$$q(X) = X^5 + 35X^4 + 485X^3 + 3325X^2 + 11274X + 15120.$$

SOLUCIÓN. Tenemos las siguientes divisiones:

$$\begin{aligned}
q(X) &= p(X)c_1(X) + r_1(X), & \begin{cases} c_1(X) = X + 25, \\ r_1(X) = 200X^3 + 2400X^2 + 10000X + 14520, \end{cases} \\
p(X) &= r_1(X)c_2(X) + r_2(X), & \begin{cases} c_2(X) = \frac{1}{200}X - \frac{1}{200}, \\ r_2(X) = 9X^2 + \frac{387}{5}X + \frac{846}{5}, \end{cases} \\
r_1(X) &= r_2(X)c_3(X) + r_3(X), & \begin{cases} c_3(X) = \frac{200}{9}X + \frac{680}{9}, \\ r_3(X) = 392X + 1736, \end{cases} \\
r_2(X) &= r_3(X)c_4(X) + r_4(X), & \begin{cases} c_4(X) = \frac{9}{392}X + \frac{657}{6860}, \\ r_4(X) = \frac{144}{49}. \end{cases}
\end{aligned}$$

Luego la resultante es:

$$\begin{aligned}
R(p(X), q(X)) &= R(p(X), r_1(X) \\
&= (-1)^{\operatorname{grad}(p(X))\operatorname{grad}(r_1(X))} R(r_1(X), p(X)) = R(r_1(X), p(X)) \\
&= R(r_1(X), p(X)) = 200^{3-\operatorname{grad}(r_2(X))} R(r_1(X), r_2(X)) \\
&= 200R(r_1(X), r_2(X)) = 200(-1)^{\operatorname{grad}(r_1(X))\operatorname{grad}(r_2(X))} R(r_2(X), r_1(X)) \\
&= 200R(r_2(X), r_1(X)) = 200 \times 9^{2-\operatorname{grad}(r_3(X))} R(r_2(X), r_3(X)) \\
&= 200 \times 9R(r_2(X), r_3(X)) \\
&= 200 \times 9(-1)^{\operatorname{grad}(r_2(X))\operatorname{grad}(r_3(X))} R(r_3(X), r_2(X)) \\
&= 200 \times 9R(r_3(X), r_2(X)) = 200 \times 9 \times 392^{1-\operatorname{grad}(r_4(X))} R(r_3(X), r_4(X)) \\
&= 200 \times 9 \times 392R(r_3(X), r_4(X)) \\
&= 200 \times 9 \times 392r_4(X) = 200 \times 9 \times 392\tfrac{144}{49} \\
&= 2073600.
\end{aligned}$$

□

Discriminante

Un caso particular de resultante es el discriminante de un polinomio. Si $p(X) \in K[X]$ tiene todas sus raíces $\alpha_1, \ldots, \alpha_n$ en un cuerpo $F \supseteq K$, definimos el **discriminante** de $p(X)$ como

$$\operatorname{Discr}(p(X)) = a_n^{2n-2} \prod_{i>j} (\alpha_i - \alpha_j)^2.$$

Ya que por la definición el discriminante de $p(X)$ es un polinomio simétrico en las raíces de $p(X)$, entonces admite una expresión en función de los coeficientes del polinomio. En particular es un elemento de K. Y podríamos dar una definición alternativa del mismo en función únicamente de los coeficientes de $p(X)$. Vamos a relacionarlo con la resultante de $p(X)$ y $Dp(X)$.

Lema. 17.19.
En la situación anterior tenemos

$$R(p(X), Dp(X)) = (-1)^{\frac{n(n-1)}{2}} a_n \operatorname{Discr}(p(X)).$$

DEMOSTRACIÓN. Ya que tenemos

$$p(X) = a_n \prod_{i=1}^{n} (X - \alpha_i),$$

entonces

$$Dp(X) = a_n \sum_{i=1}^{n} (\prod_{j=1, j\neq i}^{n} (X - \alpha_j)),$$

y por tanto

$$Dp(\alpha_i) = a_n \prod_{j=1, j\neq i}^{n} (\alpha_i - \alpha_j).$$

Si tratamos de escribir ahora el discriminante en función de $Dp(\alpha_i)$, tenemos:

$$\text{Discr}(p(X)) = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 = a_n^{n-2} a_n^n \prod_{i<j} (\alpha_i - \alpha_j)^2 =$$

El número total de factores $(\alpha_i - \alpha_j)$ es $n(n-1)$, y necesitamos cambiar el signo de la mitad, esto es, de $\frac{n(n-1)}{2}$, entonces tenemos:

$$= a_n^{n-2} (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} Dp(\alpha_i).$$

Ahora bien, la siguiente expresión de la resultante de $p(X)$ y $Dp(X)$ se deduce del Teorema (17.13.).

$$R(p(X), Dp(X)) = a_n^{n-1} \prod_{i=1}^{n} Dp(\alpha_i),$$

luego tenemos la igualdad:

$$R(p(X), Dp(X)) = (-1)^{\frac{n(n-1)}{2}} a_n \text{Discr}(p(X)).$$

□

Lo habitual es que el coeficiente líder sea igual a 1, en este caso tenemos la fórmula:

$$R(p(X), Dp(X)) = (-1)^{\frac{n(n-1)}{2}} \text{Discr}(p(X)).$$

Veamos a continuación algunos ejemplos de cálculo del discriminante.

Ejercicio. 17.20.
Cálculo del discriminante del polinomio general de grado 2

$$p(X) = a_0 + a_1 X + a_2 X^2 \in K[X].$$

SOLUCIÓN. Vamos a calcular el discriminante usando las raíces. Supongamos que las raíces son α_1 y α_2, entonces tenemos:

$$\begin{aligned}\operatorname{Discr}(p(X)) &= a_2^2(\alpha_2-\alpha_1)^2 = a_2^2(\alpha_2^2+\alpha_1^2-2\alpha_1\alpha_2)\\ &= a_2^2((\alpha_2^2+\alpha_1^2+2\alpha_1\alpha_2)-4\alpha_1\alpha_2) = a_2^2((\alpha_1+\alpha_2)^2-4\alpha_1\alpha_2)\\ &= a_2^2((-a_1/a_2)^2-4(a_0/a_2) = a_1^2-4a_0a_2.\end{aligned}$$

Vamos ahora a calcularlo usando la resultante.

$$\operatorname{Discr}(p(X)) = (-1)^{\frac{n(n-1)}{2}}a_n^{-1}R(p(X),Dp(X)) = (-1)a_2^{-1}\begin{vmatrix} a_2 & a_1 & a_0\\ 2a_2 & a_1 & 0\\ 0 & 2a_2 & a_1\end{vmatrix}$$

$$= -a_2^{-1}(4a_0a_2^2+a_1^2a_2-2a_1^2a_2) = a_1^2-4a_0a_2.$$

Observa que hemos utilizado la nota que aparece en la página 191 sobre el cálculo de la resultante. □

Ejercicio. 17.21.
Cálculo del discriminante del polinomio general de grado 3

$$p(X) = a_0+a_1X+a_2X^2+a_3X^3 \in K[X].$$

SOLUCIÓN. Vamos a calcularlo usando la resultante.

$$\operatorname{Discr}(p(X)) = (-1)^{\frac{n(n-1)}{2}}a_n^{-1}R(p(X),Dp(X)) = -a_3^{-1}\begin{vmatrix} a_3 & a_2 & a_1 & a_0 & 0\\ 0 & a_3 & a_2 & a_1 & a_0\\ 3a_3 & 2a_2 & a_1 & 0 & 0\\ 0 & 3a_3 & 2a_2 & a_1 & 0\\ 0 & 0 & 3a_3 & 2a_2 & a_1\end{vmatrix}$$

$$= a_2^2a_1^2-4a_3a_1^3-4a_2^3a_0-27a_3^2a_0^2+18a_3a_2a_1a_0.$$

Como consecuencia el discriminante del polinomio

$$p(X) = a_0+a_1X+a_2X^2+X^3 \in K[X]$$

es: $a_2^2a_1^2-4a_1^3-4a_2^3a_0-27a_0^2+18a_2a_1a_0$. □

Ejercicio. 17.22.
Cálculo del discriminante del polinomio general de grado 4

$$p(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 \in K[X].$$

SOLUCIÓN. Vamos a calcularlo usando la resultante.

$$\operatorname{Discr}(p(X)) = (-1)^{\frac{n(n-1)}{2}} a_n^{-1} R(p(X), Dp(X)) = a_4^{-1} \begin{vmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & a_0 \\ 4a_4 & 3a_3 & 2a_2 & a_1 & 0 & 0 & 0 \\ 0 & 4a_4 & 3a_3 & 2a_2 & a_1 & 0 & 0 \\ 0 & 0 & 4a_4 & 3a_3 & 2a_2 & a_1 & 0 \\ 0 & 0 & 0 & 4a_4 & 3a_3 & 2a_2 & a_1 \end{vmatrix}$$

$$\begin{aligned} &= -4a_1^3a_3^3 - 27a_3^4a_0^2 - 128a_4^2a_2^2a_0^2 \\ &\quad -4a_4a_2^3a_1^2 + 16a_4a_2^4a_0 - 27a_4^2a_1^4 + 256a_4^3a_0^3 \\ &\quad +144a_4^2a_1^2a_0a_2 - 6a_4a_1^2a_0a_3^2 + 18a_4a_1^3a_2a_3 \\ &\quad -80a_4a_1a_2^2a_3a_0 + 18a_1a_2a_3^3a_0 - 192a_4^2a_1a_0^2a_3 \\ &\quad +a_2^2a_3^2a_1^2 - 4a_2^3a_3^2a_0 + 144a_4a_2a_3^2a_0^2. \end{aligned}$$

Como consecuencia el discriminante del polinomio

$$p(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + X^4 \in K[X].$$

es:

$$\begin{aligned} &-4a_1^3a_3^3 + 256a_0^3 - 27a_3^4a_0^2 + 144a_1^2a_0a_2 \\ &+18a_1a_2a_3^3a_0 + a_2^2a_3^2a_1^2 - 4a_2^3a_3^2a_0 \\ &-6a_1^2a_0a_3^2 + 18a_1^3a_2a_3 + 144a_2a_3^2a_0^2 \\ &-192a_1a_0^2a_3 - 128a_0^2a_2^2 + 16a_2^4a_0 \\ &-4a_2^3a_1^2 - 80a_1a_2^2a_3a_0 - 27a_1^4. \end{aligned}$$

□

Ejercicios

Polinomios simétricos

Ejercicio. 17.23.
Describe todos los polinomios simétricos elementales en cuatro variables.
Ref.: 1104e_001 *SOLUCIÓN.*

Ejercicio. 17.24.
Determina todos los polinomios simétricos de grado n engendrados por uno solo de sus monomios. Estudiar el caso $n = 5$.
Ref.: 1104e_003 *SOLUCIÓN.*

Ejercicio. 17.25.
Comprueba los siguientes desarrollos de los productos de los polinomios elementales para el número de variables que se indica.

Una variable:

(1.1) $e_1 = \sum X_1$.

Dos variables:

(2.1) $e_1^2 = \sum X_1^2 + 2\sum X_1X_2$,
(2.2) $e_2 = \sum X_1X_2$,

Tres variables:

(3.1) $e_1^3 = \sum X_1^3 + 3\sum X_1^2X_2 + 6\sum X_1X_2X_3$,
(3.2) $e_1e_2 = \sum X_1^2x_2 + 3\sum X_1X_2X_3$,
(3.3) $e_3 = \sum X_1X_2X_3$.

Cuatro variables:

(4.1) $e_1^4 = \sum X_1^4 + 6\sum X_1^3X_2 + 6\sum X_1^2X_2^2 + 12\sum X_1^2X_2X_3 + 24\sum X_1X_2X_3X_4$,
(4.2) $e_1^2e_2 = \sum X_1^3X_2 + 2\sum X_1^2X_2^2 + 5\sum X_1^2X_2X_3 + 12\sum X_1X_2X_3X_4$,
(4.3) $e_2^2 = \sum X_1^2X_2^2 + 2\sum X_1^2X_2X_3 + 6\sum X_1X_2X_3X_4$,
(4.4) $e_1e_3 = \sum X_1^2X_2X_3 + 4\sum X_1X_2X_3X_4$,
(4.5) $e_4 = \sum X_1X_2X_3X_4$.

Cinco variables:

(5.1) $e_1^5 = \sum X_1^5 + 5\sum X_1^4X_2 + 10\sum X_1^3X_2^2 + 20\sum X_1^3X_2X_3 + 30\sum X_1^2X_2^2X_3 + 40\sum X_1^2X_2X_3X_4 + 120\sum X_1X_2X_3X_4X_5$,

(5.2) $e_1^3e_2 = \sum X_1^4X_2 + 3\sum X_1^3X_2^2 + 7\sum X_1^3X_2X_3 + 12\sum X_1^2X_2^2X_3 + 27\sum X_1^2X_2X_3X_4 + 60\sum X_1X_2X_3X_4X_5$,

(5.3) $e_1e_2^2 = \sum X_1^3X_2^2 + 2\sum X_1^3X_2X_3 + 4\sum X_1^2X_2^2X_3 + 12\sum X_1^2X_2X_3X_4 + 30\sum X_1X_2X_3X_4X_5$,

(5.4) $e_1^2e_3 = \sum X_1^3X_2X_3 + 2\sum X_1^2X_2^2X_3 + 7\sum X_1^2X_2X_3X_4 + 20\sum X_1X_2X_3X_4X_5$,

(5.5) $e_2e_3 = \sum X_1^2X_2^2X_3 + 3\sum X_1^2X_2X_3X_4 + 10\sum X_1X_2X_3X_4X_5$,

(5.6) $e_1e_4 = \sum X_1^2X_2X_3X_4 + 5\sum X_1X_2X_3X_4X_5$,

(5.7) $e_5 = \sum X_1X_2X_3X_4X_5$.

Ref.: 1104e_004 *SOLUCIÓN.*

Ejercicio. 17.26.
Para n variables expresa $\sum X_1^2, \sum X_1^3, \sum X_1^4$ y $\sum X_1^5$ como una combinación de los polinomios simétricos elementales.

Ref.: 1104e_005 *SOLUCIÓN.*

Ejercicio. 17.27.
Estudia si son ó no simétricos los siguientes polinomios, y cuando lo sean, expresarlos en función de los polinomios simétricos elementales.

(1) $(X-Y)^2(X-2Y)(2Y-X)(X+Y)^2$, *en* $K[X,Y]$,
(2) $(X+Y-Z)(X-Y+Z)(X-Y-Z)$, *en* $K[X,Y,Z]$,
(3) $3X^4+2X-3$, *en* $K[X]$,
(4) $(X^2+X+1)(Y^2+Y+2)(Z^2+Z+3)$, *en* $K[X,Y,Z]$,
(5) $(X-Y)(Y-X)(X-Z)(Z-X)(Y-Z)(Z-Y)$, *en* $K[X,Y,Z]$,
(6) $(X+Y+Z)^3+(Y+X+T)^3+(X+Z+T)^3+(Y+Z+T)^3$, *en* $K[X,Y,Z,T]$.

Ref.: 1104e_006 *SOLUCIÓN.*

Ejercicio. 17.28.
Expresa como combinación de los polinomios simétricos elementales los siguientes polinomios simétricos:

(1) $(X+Y)(Y+Z)(Z+X)$, *en* $K[X,Y,Z]$,
(2) $(X+Y-Z)(Y+Z-X)(Z+X-Y)$, *en* $K[X,Y,Z]$,
(3) $(X+Y-Z)^3(Y+Z-X)^3(Z+X-Y)^3$, *en* $K[X,Y,Z]$,
(4) $(X+Y+Z)^3(X+Y+T)^3(X+Z+T)^3(Y+Z+T)^3$, *en* $K[X,Y,Z,T]$,
(5) $(X^2+Y^2)(Y^2+Z^2)(Z^2+X^2)$, *en* $K[X,Y,Z]$.

Ref.: 1104e_007 *SOLUCIÓN.*

Ejercicio. 17.29.
Expresa como combinación de los polinomios simétricos elementales los siguientes polinomios simétricos:

(1) $XY+X^2Y+Y^2X+XZ+ZY+Z^2Y+Z^2X+Y^2Z+X^2Z$, *en* $K[X,Y,Z]$,
(2) $XY+XYZ+XZ+YZ+Y+X+Z$, *en* $K[X,Y,Z]$,
(3) $X^2Y+X^2Z+Y^2X+Z^2Y+Y^2Z+Z^2Y+XYZ$, *en* $K[X,Y,Z]$,
(4) $(X-Y)^2(X-Z)^2+(Y-X)^2(Y-Z)^2+(Z-X)^2(Z-Y)^2$, *en* $K[X,Y,Z]$.

Ref.: 1104e_008 *SOLUCIÓN.*

Ejercicio. 17.30.
Determina el polinomio simétrico en tres variables más pequeño que sea múltiplo de $X-2Y$, *y exprésalo como combinación de los polinomios simétricos elementales.*
Ref.: 1104e_009 *SOLUCIÓN.*

Ejercicio. 17.31.
Se considera el polinomio $F=X^4+3X^3+2X^2+X-1$, *con raíces* $\alpha_1,\alpha_2,\alpha_3$ *y* α_4. *Determina, detalladamente, el valor de las siguientes expresiones simétricas en* $\alpha_1,\alpha_2,\alpha_3,\alpha_4$*:*

(1) $\sum \alpha_1^2\alpha_2$.
(2) *¿Cuantos sumandos tiene esta suma? Escribe todos los sumandos.*
(3) $\alpha_1^4+\alpha_2^4+\alpha_3^4+\alpha_4^4=:\sum\alpha_1^4$.

Ref.: 1104e_028 *SOLUCIÓN.*

Ejercicio. 17.32.
Expresa en función de los polinomios simétricos elementales los polinomios simétricos

(1) $p = X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2$.

(2) $q = X_1^3X_2^2X_3 + X_1^3X_2X_3^2 + X_1^2X_2^3X_3 + X_1^2X_2X_3^3 + X_1X_2^3X_3^2 + X_1X_2^2X_3^3$.

Ref.: 1104e_016 SOLUCIÓN.

Ejercicio. 17.33.
Dado un término $X_1^{e_1}\cdots X_n^{e_n}$, *con* $e_1 \geq \cdots \geq e_n$, *el polinomio simétrico mínimo que contiene a* $X_1^{e_1}\cdots X_n^{e_n}$ *lo representamos por* $(X_1^{e_1}\cdots X_n^{e_n})$, *y podemos escribirlo fácilmente como*

$$(X_1^{e_1}\cdots X_n^{e_n}) = \frac{1}{k}\sum_{\sigma\in S_n} X_{\sigma(1)}^{e_1}\cdots X_{\sigma(n)}^{e_n},$$

donde k *es el número de términos* $X_{\sigma(1)}^{e_1}\cdots X_{\sigma(n)}^{e_n}$ *que son iguales a* $X_1^{e_1}\cdots X_n^{e_n}$.
Calcula el valor de k, *y el número de monomios de* $(X_1^{e_1}\cdots X_n^{e_n})$.
Ref.: 1104e_021 SOLUCIÓN.

Ejercicio. 17.34.
Dado un polinomio $X^3 + bX^2 + cX + d$ *con raíces* $\alpha, \beta, \gamma \neq 0$, *calcula:*
(1) El valor de $\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma}$.
(2) Cuando $\alpha, \beta, \gamma \neq -1$, *el polinomio del que son raíces* $\frac{1}{\alpha+1}$, $\frac{1}{\beta+1}$ *y* $\frac{1}{\gamma+1}$.

Ref.: 1104e_023 SOLUCIÓN.

Ejercicio. 17.35.
Dado el polinomio $X^3 - 4X - 8$, *con raíces* α, β *y* γ, *calcula el valor de*

$$\frac{\alpha+1}{\alpha-1} + \frac{\beta+1}{\beta-1} + \frac{\gamma+1}{\gamma-1}.$$

Ref.: 1104e_024 SOLUCIÓN.

Ejercicio. 17.36.
Se considera el polinomio X^3-5X-5 *con raíces* α,β *y* γ. *Calcula el valor de* $\left(\frac{1}{\alpha+1}\right)^3+\left(\frac{1}{\beta+1}\right)^3+\left(\frac{1}{\gamma+1}\right)^3$.
Ref.: 1104e_025 SOLUCIÓN.

Ejercicio. 17.37.
Determina todas las ternas de números $\alpha_1,\alpha_2,\alpha_3$ *tales que su suma es* r, *la suma de sus cuadrados es* s, *y la suma de sus cubos es* t.
Estudiar el caso particular en el que $r=1$, $s=19$ *y* $t=1$.
Ref.: 1104e_018 SOLUCIÓN.

Ejercicio. 17.38.
Si las raíces del polinomio X^3+X^2-X-k *son* α_1,α_2 *y* α_3, *que verifican la relación* $\alpha_1^2-\alpha_2^2+\alpha_3^2=0$.
¿Cuáles son los posibles valores de k*?*
Ref.: 1104e_019 SOLUCIÓN.

Ejercicio. 17.39.
Sea $f(X)=X^3+bX^2+cX+d\in\mathbb{Q}[X]$. *Si el cuadrado de una de sus raíces es igual al producto de las otras dos, prueba que se verifica* $b^3d=c^3$.
Ref.: 1104e_020 SOLUCIÓN.

Resultante

El Teorema (17.13.) nos permite hacer automáticos algunos cálculos; veamos un ejemplo.

Ejercicio. 17.40.
Se considera polinomios $f(X)=\sum_{i=0}^{n} a_i X^i$ *y* $g(X)=\sum_{j=0}^{m} b_j X^j$, *con raíces* $\alpha_1,\dots,\alpha_n$ *y* $\beta_1,\dots,\beta_m$, *respectivamente, y coeficientes en un cuerpo* K. *Construye polinomios* f_i *de los que* $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ *y* β/α, *si* $\alpha\neq 0$, *respectivamente, son raíces.*
Aplícalo al caso en el que $f(X)=X^4+X+1$ *y* $g(X)=X^3+X+1$.
Ref.: 1104e_027 SOLUCIÓN.

Ejercicio. 17.41.
Sean $f,g\in\mathbb{Q}[X]$ *polinomios de grado* n *y* m *respectivamente. Llamemos* α_1 *a las raíces de* f *en* $\mathbb{C}$, *y* β_j *a las de* g.

(1) *Prueba que existe un polinomio* $h\in\mathbb{Q}[X]$ *cuyas raíces son de la forma* $\alpha_i-\beta_j$.
(2) *Prueba que existe un polinomio con coeficientes en* $\mathbb{Q}$ *que tiene por raíces a los elementos* $2\alpha_i-\beta_j$.
(3) *Si se considera* $f(X)=X^4+X^3+X^2+X+1$ *y* $g(X)=X^2+X+1$, *construye un polinomio que tenga como raíces a* $\alpha_i\beta_j$, *y un polinomio que tenga como raíces a* α_i/β_j.

Ref.: 1104e_029 SOLUCIÓN.

Ejercicio. 17.42.
Si $\alpha_1,\alpha_2,\alpha_3$ *son las raíces el polinomio* $X^3+bX^2+cX+d\in\mathbb{Q}[X]$, *determina los coeficientes de un polinomio cuyas raíces son las que se expresan en cada caso.*

(1) $\alpha_1+\alpha_2$, $\alpha_2+\alpha_3$ *y* $\alpha_3+\alpha_1$.

(2) $\alpha_1^2+\alpha_2^2$, $\alpha_2^2+\alpha_3^2$ *y* $\alpha_3^2+\alpha_1^2$.

Ref.: 1104e_017 SOLUCIÓN.

Discriminante

Ejercicio. 17.43.
Sean $f(X)=X^2+iX+2$ *y* $g(X)=X^3+(1-i)X^2+(2-i)X-2i$ *polinomios con coeficientes en* $\mathbb{C}$.

(1) ¿Son primos relativos $f(X)$ y $g(X)$?
(2) Halla el discriminante de $g(X)$.
(3) ¿Tiene $g(X)$ raíces dobles?

Ref.: 1104e_012 *SOLUCIÓN.*

Ejercicio. 17.44.
Halla el discriminante de $X^n + aX + b \in \mathbb{Z}[X]$.
Ref.: 1104e_013 *SOLUCIÓN.*

Ejercicio. 17.45.
Halla el discriminate de $X^5 + aX^4 + b \in \mathbb{Z}[X]$ sabiendo que el discriminante de $X^5 + aX + b$ es: $5^5b^4 + 4^4a^5$.
Ref.: 1104e_014 *SOLUCIÓN.*

Ejercicio. 17.46.
Halla el discriminante de $X^n + aX^{n-1} + b \in \mathbb{Z}[X]$.
Ref.: 1104e_015 *SOLUCIÓN.*

Ver Ejercicio (16.9.)
Ver Ejercicio (16.10.)
Ver Ejercicio (16.11.)

Ejercicio. 17.47.
Dado el polinomio $f(X) = X^3 + bX + c \in K[X]$, con $\mathrm{car}(K) \neq 2, 3$, da una condición para que $f(X)$ no tenga raíces múltiples.
Ref.: 1104e_022 *SOLUCIÓN.*

Ver Ejercicio (14.16.)

Capítulo V

Módulos

Introducción

En el moderno estudio de los anillos y las álgebras una herramienta esencial son las representaciones. La teoría general de representaciones se realiza a través del concepto de módulo, del que aquí vamos a dar su definición y propiedades elementales.

Haremos uso de las construcciones del módulo cociente y de la suma directa para construir módulos libres y probar que todo módulo es un cociente de un módulo libre.

1105-00.tex

18. Módulos y submódulos

Definición de módulo

En este capítulo A va a ser siempre un anillo conmutativo. Un A-**módulo** es un grupo abeliano M junto con una acción a la izquierda de A sobre M: $\alpha : A \times M \longrightarrow M$, tal que si representamos $\alpha(a,m) = am$, para $a \in A$ y $m \in M$, se verifican las propiedades.

(M-I) $a(m_1 + m_2) = am_1 + am_2$.
(M-II) $(a_1 + a_2)m = a_1m + a_2m$.
(M-III) $a_1(a_2m) = (a_1a_2)m$.
(M-IV) $1m = m$.

Para cualesquiera $a, a_1, a_2 \in A$ y $m, m_1, m_2 \in M$.

Lema. 18.1.
Sea M un grupo abeliano, entonces $\mathrm{End}(M)$ *es un anillo (no conmutativo), con las operaciones:*

suma: $(f+g)(m) = f(m) + g(m)$, *para cada* $m \in M$,

producto: $(fg)(m) = f(g(m))$, *para cada* $m \in M$,

elemento uno: *es* id_M,

para cada $f, g \in \mathrm{End}(M)$.

Las cuatro propiedades (M-i)–(M-iv) caracterizan también a los A-módulos en el siguiente sentido: *es equivalente que M sea un A-módulo con acción $\alpha : A \times M \longrightarrow M$ verificando las propiedades (M-i) a (M-iv) y que exista un homomorfismo de anillos $\beta : A \longrightarrow \mathrm{End}(M)$.*

Lema. 18.2.
Sea M un grupo abeliano. Son equivalentes:
(a) M es un A–módulo.
(b) Existe un homomorfismo de anillos $\beta : A \longrightarrow \mathrm{End}(M)$.

La aplicación α se llama una **acción** de A sobre M y β se llama el **homomorfismo de la acción**. Es claro que α y β están relacionados por la siguiente fórmula:

$$\alpha(a,m) = \beta(a)(m) \text{ para cualesquiera } a \in A \text{ y } m \in M.$$

1105-01.tex

Cambio de anillo

Sean A y B anillos conmutativos, $f : B \longrightarrow A$ un homomorfismo de anillos y M un A-módulo con homomorfismo $\beta : A \longrightarrow \mathrm{End}(M)$, entonces M también es un B-módulo con homomorfismo la composición $\beta \circ f : B \longrightarrow \mathrm{End}(M)$.

Aritmética de módulos

Los siguientes resultados señalan las propiedades básicas de la acción de un anillo sobre un módulo.

Lema. 18.3.
Sea M un A–módulo, para cada $a \in A$ y cada $m \in M$ se verifica:
(1) $a0 = 0$.
(2) $a(-m) = -(am)$.
(3) $0m = 0$.
(4) $(-a)m = -(am)$.

Lema. 18.4.
Sea M un A–módulo, para cualesquiera $a, a_i \in A$, $i \in I$ (finito) y $m, m_j \in M$, $j \in J$ (finito), se verifica:
(1) $a(\sum_{j\in J} m_j) = \sum_{j\in J} am_j$.
(2) $(\sum_{i\in I} a_i)m = \sum_{i\in I} a_i m$.

Ejercicios

Módulos y submódulos

Ejercicio. 18.5.
Estructuras imposibles.

(1) Razona que $\mathbb{Z}_{49}$ no es un $\mathbb{Z}_7$-módulo.
(2) Prueba que no todo $\mathbb{Z}$-módulo es un $\mathbb{Q}$-espacio vectorial.

Ref.: 1105e_005 *SOLUCIÓN.*

Ejercicio. 18.6.
Sea M un A-módulo. Para cada $m \in M$ definimos $Am = \{rm \mid r \in A\}$.

(1) Demuestra que Am es un submódulo de M.
(2) Demuestra que un A-módulo M es cíclico si, y sólo si, existe un ideal $\mathfrak{a}$ de A tal que $M \cong A/\mathfrak{a}$.

Ref.: 1105e_001 *SOLUCIÓN.*

19. Homomorfismos de A-módulos

Sean A un anillo, y M y M' dos A-módulos. Una aplicación $f : M \longrightarrow M'$ se llama un **homomorfismo de A–módulos** si verifica:
(HM-I) f es un homomorfismo de grupos abelianos.
(HM-II) $f(am) = af(m)$, para todo $a \in A$ y $m \in M$.

Esto es, el siguiente diagrama es conmutativo.

$$\begin{array}{ccc} A \times M & \xrightarrow{\alpha_M} & M \\ {\scriptstyle A\times f}\downarrow & & \downarrow{\scriptstyle f} \\ A \times M' & \xrightarrow{\alpha_{M'}} & M' \end{array}$$

Lema. 19.1.
Sean A un anillo, M y M' dos A-módulos y $f : M \longrightarrow M'$ una aplicación. Son equivalentes:
(a) f es un homomorfismo de A-módulos.
(b) Para cualesquiera $a_1, a_2 \in A$ y $m_1, m_2 \in M$ se tiene: $f(a_1m_1 + a_2m_2) = a_1f(m_1) + a_2f(m_2)$.

Lema. 19.2.
(1) Para cada A–módulo M la identidad, id_M, es un homomorfismo de A-módulos.

(2) La composición de homomorfismos de A-módulos, cuando está definida, es un homomorfismo de A-módulos.

Submódulos

Sean A un anillo y M un A-módulo. Un subgrupo abeliano N de M se llama un **submódulo** si para cada $a \in A$ y cada $n \in N$ se tiene $an \in N$.

Lema. 19.3.
Sean A un anillo, M un A-módulo y N un subconjunto de M, son equivalentes:
(a) N es un submódulo de M;
(b) Para todos $a_1, a_2 \in A$ y $n_1, n_2 \in N$ se tiene $a_1n_1 + a_2n_2 \in N$.

1105-02.tex

Lema. 19.4.
Si $N \subseteq M$ es un submódulo de M, entonces la inclusión $i : N \longrightarrow M$ es un homomorfismo de A-módulos. Lo llamamos homomorfismo inclusión.

Si M es un A-módulo, el propio M es un submódulo; los demás se llaman **submódulos propios** de M. El subconjunto $\{0\}$ se llama **submódulo trivial** y se representa simplemente por 0.
Dado un A-módulo M, el conjunto $\mathscr{L}(M) = \{N \mid N \text{ es un submódulo de } M\}$ se llama el **retículo de los submódulos** de M.

Lema. 19.5.
Sea M un A-módulo, en $\mathscr{L}(M)$ la relación

$$N_1 \leq N_2 \text{ si } N_1 \text{ está contenido en } N_2$$

es una relación de orden.

Utilizando lo anterior podemos representar por $N \subseteq M$, ó por $N \leq M$, cuando N es un submódulo de M.

Proposición. 19.6.
Sean A un anillo y M un A-módulo. Para cada familia de submódulos de M, por ejemplo $\{N_i \mid i \in I\}$, se tiene que $\cap\{N_i \mid i \in I\}$ es también un submódulo de M.
*Se tiene que en $\mathscr{L}(M)$ el **ínfimo** de la familia $\{N_i \mid i \in I\}$ es $\cap_i N_i$.*

Como consecuencia tenemos:

Corolario. 19.7.
Sea X un subconjunto de A-módulo M, existe un menor submódulo AX de M que contiene a X, y que se puede describir como

$$\begin{aligned} AX = \langle X \rangle = \cap\{N \mid N \text{ es un submódulo de } M \text{ y } X \subseteq N\} = \\ = \{\textstyle\sum_{i=1}^{n} r_i x_i \mid r_i \in A, x_i \in X\}. \end{aligned}$$

El submódulo $AX = \langle X \rangle$ se llama el submódulo de M **generado** por el conjunto X, y diremos que X es un **sistema de generadores** de AX.
Cuando $X = \{x\}$, tiene un sólo elemento, $Ax := AX$ se llama el **submódulo cíclico** generado por x.
Si X es un conjunto finito, entonces AX se llama un **submódulo finitamente generado**.

Teorema. 19.8.
*Sean A un anillo y M un A-módulo. Si $\{N_i \mid i \in I\}$ es una familia de submódulos de M, entonces existe un menor submódulo de M que contiene a cada elemento de la familia, que notaremos por $\sum\{N_i \mid i \in I\}$ y llamaremos **suma de la familia**; la descripción a través de sus elementos es:*

$$\left\{ \sum_j n_j \mid j \in F \subseteq I \text{ finito, } n_j \in N_j \text{ para todo } j \in F \right\}.$$

*Se tiene entonces que $\sum_i N_i$ es el **supremo** de la familia $\{N_i \mid i \in I\}$.*

Si $I = \{1, 2, \ldots, n\}$, entonces representamos $\sum_i N_i$ simplemente por $N_1 \cap N_2 \cap \cdots \cap N_n$

Lema. 19.9.
*El conjunto $\mathscr{L}(M)$ con la relación de orden "$\leq$" es un **retículo** con **ínfimo** la intersección y **supremo** la suma.*

El conjunto $\mathscr{L}(M)$ tiene pues dos operaciones: intersección o ínfimo, y suma o supremo. Las propiedades de estas operaciones son de interés; en particular no verifican la propiedad distributiva, pero sí un caso especial de la misma que se conoce como **ley modular**.

Proposición. 19.10. (Ley modular)
Para cada A–módulo M y submódulos $N, N_1, N_2 \subseteq M$ tales que $N_1 \subseteq N_2$, se verifica:

$$N_1 + (N \cap N_2) = (N_1 + N) \cap N_2.$$

Proposición. 19.11.
Sea A un anillo y $f : M \longrightarrow M'$ un homomorfismo de A-módulos. Se verifican las siguientes propiedades:

(1) Si N es un submódulo de M, entonces $f_*(N)$ es un submódulo de M'.
(2) Si N' es un submódulo de M', entonces $f^*(N')$ es un submódulo de M.
(3) Tanto f_* como f^* son homomorfismos de retículos.

Otras notaciones para f_* y f^* son f y f^{-1}, respectivamente.

El módulo de los homomorfismos

Sea A un anillo y M, M' dos A-módulos, el conjunto de los homomorfismos de A-módulos de M a M' se representa por $\mathrm{Hom}_A(M, M')$.

Lema. 19.12.
En la situación anterior $\mathrm{Hom}_A(M, M')$ *es un A-módulo con operaciones definidas mediante:*
(1) $(f+g)(m) = f(m) + g(m)$, para cualesquiera f, $g \in \mathrm{Hom}_A(M, M')$ y $m \in M$;
(2) $(af)(m) = a(f(m))$, para cualesquiera $a \in A$, $f \in \mathrm{Hom}_A(M, M')$ y $m \in M$.

Además, si X e Y son A-módulos y $h : X \longrightarrow M$, $k : M' \longrightarrow Y$, son homomorfismos de A-módulos, entonces para $f, g \in \mathrm{Hom}_A(M, M')$

$$X \xrightarrow{h} M \underset{g}{\overset{f}{\rightrightarrows}} M' \xrightarrow{k} Y$$

se verifica:

$$(f+g)\circ h = f\circ h + g\circ h \qquad \text{y} \qquad k\circ(f+g) = k\circ f + k\circ g.$$

En particular tenemos que $\mathrm{End}_A(M)$ es un anillo, no necesariamente conmutativo, que es un subanillo de $\mathrm{End}(M)$, (el anillo de los endomorfismos del grupo abeliano subyacente a M).
Observar que el anillo $\mathrm{End}_A(M)$ actúa a la derecha, por composición, sobre $\mathrm{Hom}_A(M, M')$ y que el anillo $\mathrm{End}_A(M')$ actúa a la izquierda sobre $\mathrm{Hom}_A(M, M')$, pero estas acciones no las vamos a utilizar en este texto.

Núcleo e imagen de un homomorfismo

Sea A un anillo, dado un homomorfismo de A-módulos $f : M \longrightarrow M'$, la **imagen** de f es:

$$\mathrm{Im}(f) = \{f(m) \mid m \in M\},$$

y el **núcleo** de f es:

$$\mathrm{Ker}(f) = \{m \in M \mid f(m) = 0\}.$$

Lema. 19.13.
En la situación anterior $\mathrm{Im}(f)$ *y* $\mathrm{Ker}(f)$ *son submódulos de* M' *y* M *respectivamente.*

El cero de $\mathrm{Hom}_A(M,M')$ se representa por 0 y verifica: $\mathrm{Im}(0)=\{0\}$, $\mathrm{Ker}(0)=M$.
Un homomorfismo $f : M \longrightarrow M'$ se llama un **monomorfismo** si es simplificable a la izquierda, esto es,

$$X \underset{h}{\overset{g}{\rightrightarrows}} M \xrightarrow{f} M'$$

si g y h son homomorfismo tales que $fg = fh$, entonces $g = h$.

Proposición. 19.14.
Si f *es un homomorfismo de módulos, son equivalentes:*
(a) f *es inyectiva.*
(b) $\mathrm{Ker}(f)=0$
(c) f *es un monomorfismo.*

Un homomorfismo $f : M \longrightarrow M'$ se llama un **epimorfismo** si es simplificable a derecha.

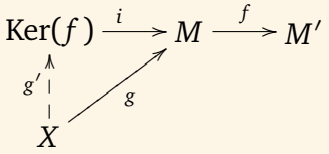
Proposición. 19.15.
Si f *es un homomorfismo de módulos, son equivalentes:*
(a) f *es sobreyectiva.*
(b) $\mathrm{Im}(f)=M'$.
(c) f *es un epimorfismo.*

Teorema. 19.16.
Sea $f : M \longrightarrow M'$ *un homomorfismo de módulos. Son equivalentes:*
(a) f *es una aplicación biyectiva.*
(b) f *es un monomorfismo y un epimorfismo.*
(c) Existe un homomorfismo de A-módulos $g : M' \longrightarrow M$ *tal que* $g \circ f = id_M$ *y* $f \circ g = id_{M'}$. *(Isomorfismo).*

Un homomorfismo de A-módulos verificando las condiciones del Teorema (19.16.) se llama un **isomorfismo**. Para un A-módulo M un isomorfismo $f : M \longrightarrow M$ se llama **automorfismo**. El conjunto de los automorfismos de un A-módulo M se representa por $\mathrm{Aut}_A(M)$, y tiene estructura de grupo respecto a la composición, ya que es el conjunto de los elementos invertibles del anillo $\mathrm{End}_A(M)$.

Proposición. 19.17. (Propiedad universal del núcleo.)
Sea A un anillo y $f : M \longrightarrow M'$ un homomorfismo de A-módulos. Si $i : \mathrm{Ker}(f) \longrightarrow M$ es la inclusión, entonces

(1) la composición $i \circ f$ es cero, y
(2) si $g : X \longrightarrow M$ es un homomorfismo de A-módulos verificando $g \circ f = 0$, entonces existe un único homomorfismo de A-módulos $g' : X \longrightarrow \mathrm{Ker}(f)$ tal que $g = i \circ g'$.



Módulo cociente

Sea N un submódulo de un A-módulo M. En M definimos la relación

$$m_1 \mathscr{R}_N m_2 \text{ si } m_1 - m_2 \in N.$$

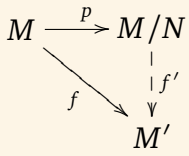
Es claro que $\mathscr{R}_N$ es una relación de equivalencia. Llamamos simplemente M/N al conjunto cociente $M/\mathscr{R}_N$. Sea $p : M \longrightarrow M/N$ la proyección canónica, esto es, para cada $m \in M$ se tiene que $p(m) = m + N$, la clase de equivalencia de m.

Lema. 19.18.
En la situación anterior existe una única estructura de A-módulo en M/N de forma que la proyección canónica $p : M \longrightarrow M/N$ sea un homomorfismo de A-módulos. Esta estructura está dada por las expresiones:

$$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N,$$
$$a(m + N) = (am) + N$$

El módulo M/N se llama **módulo cociente** de M por N.

Teorema. 19.19. (Propiedad universal del cociente.)
Sea A un anillo, $N \subseteq M$ un submódulo, y $f : M \longrightarrow M'$ un homomorfismo de A-módulos tal que $f(N) = 0$. Existe un único homomorfismo de A-módulos $f' : M/N \longrightarrow M'$ tal que $f = f' \circ p$.

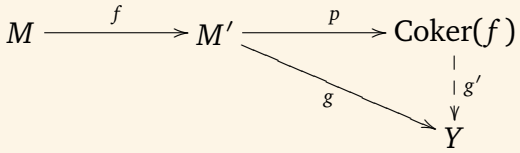


De forma dual a la construcción del núcleo de un homomorfismo tenemos la de conúcleo.

Sea A un anillo, y $f : M \longrightarrow M'$ un homomorfismo de A-módulos, llamamos **conúcleo** de f, y lo representamos por $\mathrm{Coker}(f)$, al módulo cociente $M'/\mathrm{Im}(f)$, junto con la proyección $p : M' \longrightarrow M'/\mathrm{Im}(f)$.

El conúcleo verifica la propiedad universal dual de la mencionada en la Proposición (19.17.).

Proposición. 19.20. (Propiedad universal del conúcleo.)
En la situación anterior, supongamos que $p : M \longrightarrow \mathrm{Coker}(f)$ es la proyección canónica, entonces $p \circ f = 0$ y si $g : M' \longrightarrow Y$ es un homomorfismo verificando $g \circ f = 0$, entonces existe un único homomorfismo de A-módulos $g' : \mathrm{Coker}(f) \longrightarrow Y$ tal que $g = g' \circ p$.



Cuando f es la inclusión de un submódulo N' de M', entonces el conúcleo es precisamente el cociente de M' por N'.

Un homomorfismo $f : M \longrightarrow M'$ con conúcleo igual a cero es un **epimorfismo**. Observa que ésta es otra posible caracterización de epimorfismo.

Es de destacar que las propiedades universales del núcleo y el conúcleo están expresadas para los pares $(\mathrm{Ker}(f), i)$ y $(p, \mathrm{Coker}(f))$ respectivamente. Por lo que desde un punto de vista formal la definición de núcleo y conúcleo de un homomorfismo hay que realizarla para los pares anteriormente citados, y no solamente para los módulos que en ellos aparecen.

Siguiendo en esta línea, vamos a introducir en las siguientes secciones nuevas construcciones en módulos.

Teoremas de isomorfía

Vamos a hacer uso de los módulos cocientes en el estudio de módulos y homomorfismos de módulos.

Teorema. 19.21.
Dado un homomorfismo de A–módulos $f : M \longrightarrow M'$, se verifica:

(1) Existe una proyección $p : M \longrightarrow M/\mathrm{Ker}(f)$, definida por $p(m) = m + \mathrm{Ker}(f)$ para cada $m \in M$.
(2) Existe una inclusión $j : \mathrm{Im}(f) \longrightarrow M'$, definida por $j(f(m)) = f(m)$ para cada $m \in M$.
*(3) **Primer Teorema de Isomorfía.** Existe un isomorfismo $b : M/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$, definido por $b(m + \mathrm{Ker}(f)) = f(m)$ para cada $m \in M$.*

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & M' \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle j} \\ M/\mathrm{Ker}(f) & \overset{\cong}{\underset{b}{- - \succ}} & \mathrm{Im}(f) \end{array}$$

(4) Existe una biyección, que conserva el orden, entre las familias de submódulos

$$\mathscr{A} = \{N \subseteq M \mid \mathrm{Ker}(f) \subseteq N\} \; y$$

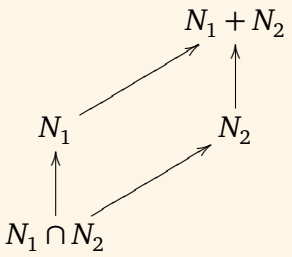
$$\mathscr{B} = \{N' \subseteq M' \mid N' \subseteq \mathrm{Im}(f)\}.$$

En esta biyección la imagen de $N \in \mathscr{A}$ es $f_*(N) \subseteq M'$ y la imagen de $N' \in \mathscr{B}$ es $f^*(N') \subseteq M$.

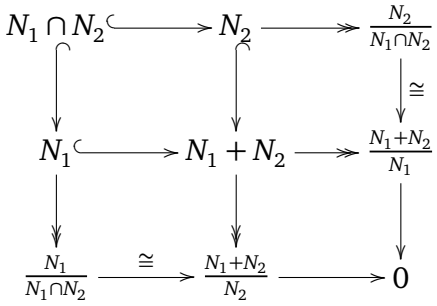
Teorema. 19.22. (Segundo Teorema de isomorfía o Teorema del paralelogramo)
Sea M un A-módulo y N_1, N_2 submódulos de M. Existe un isomorfismo

$$\frac{N_1}{N_1 \cap N_2} \cong \frac{N_1 + N_2}{N_2},$$

definido por $x + (N_1 \cap N_2) \mapsto x + N_2$.



Tenemos el siguiente diagrama conmutativo:



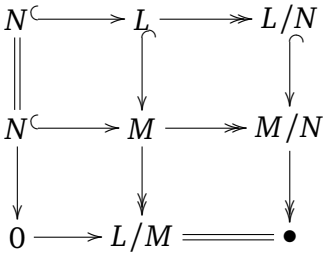
Para completar la teoría vamos a incluir el Tercer Teorema de Isomorfía o del Doble Cociente.

Teorema. 19.23. (Tercer Teorema de Isomorfía. o Teorema del Doble Cociente)
Sean M un A–módulo, y $N \subseteq L$ submódulos de M. Existe una biyección, que conserva el orden, entre los submódulos de M que contienen a N y los submódulos de M/N, dada por $L \mapsto \dfrac{L}{N}$. Además para cada $N \subseteq L \subseteq M$ existe un isomorfismo

$$\frac{M/N}{L/N} \cong \frac{M}{L},$$

que está definido por $(m+N)+\dfrac{L}{N} \mapsto m+L$.

Tenemos el siguiente diagrama conmutativo:



Los teoremas de isomorfía segundo y tercero se conocen como teoremas de **isomorfía de Noether**.

Módulos cíclicos

Si M es un A–módulo, para cada $m \in M$ podemos definir la aplicación $f_m : A \longrightarrow M$ mediante $f_m(a) = am$ para cada $a \in A$.

Lema. 19.24.
Sea M un A–módulo. Se verifica:
(1) Para cada $m \in M$ la aplicación $f_m : A \longrightarrow M$ es un homomorfismo A–módulos.
*(2) El núcleo de f_m es $\{a \in A \mid am = 0\}$ se llama el **anulador** de m, y se representa por $\mathrm{Ann}_A(m)$. Como consecuencia es un ideal de A.*
*(3) El **anulador** del módulo M se define como $\mathrm{Ann}_A(M) = \cap\{\mathrm{Ann}_A(m) \mid m \in M\}$.*

Ejercicio. 19.25.
Demuestra que cada A–módulo M tiene una estructura de módulo sobre el anillo $A/\mathrm{Ann}_A(M)$ de forma que la estructura de A–módulo, inducida por el cambio de anillo $A \longrightarrow A/\mathrm{Ann}_A(M)$, coincide con la estructura original en M.

Recordar que un A–módulo es **cíclico** si está generado por un elemento.

Proposición. 19.26.
Dado un A–módulo cíclico M con generador $g \in M$, se tiene:
(1) El homomorfismo $f_g : A \longrightarrow M$ es sobreyectivo.
(2) Existe un isomorfismo $A/\mathrm{Ann}_A(g) \cong M$.

Como consecuencia los A–módulos cíclicos son isomorfos a los cocientes del anillo A.

Módulos finitamente generados

Recordemos que un módulo M es **finitamente generado** si $\langle m_1, \ldots, m_t \rangle = M$, para $m_1, \ldots, m_t \in M$. Un submódulo $N \subseteq M$ es un **submódulo maximal** si $N \neq M$ y para cada submódulo H tal que $N \subseteq H \subsetneq M$ se tiene $N = H$.

Proposición. 19.27.
Sea M un módulo, y $N \subsetneq M$ un submódulo propio, son equivalentes:
(a) $N \subseteq M$ es maximal.
(b) Para cada $m \in M \setminus N$ se tiene $N + Am = M$.
(c) Para cada submódulo $H \subseteq M$ tal que $H \nsubseteq N$, se tiene $N + H = M$.

Proposición. 19.28.
Si M es un módulo finitamente generado, cada submódulo propio está contendido en un submódulo maximal.

DEMOSTRACIÓN. Consideramos el conjunto de submódulos $\Gamma = \{H \subseteq M \mid N \subseteq H \subsetneq M\}$, probamos que Γ es no vacío e inductivo; un elem,ento maximal de Γ es un submódulo maximal que contiene a N. □

Un módulo M es un **módulo simple** si es no nulo y los únicos submódulos de M son $\{0\}$ y el propio M.

Proposición. 19.29.
Sea M un módulo no nulo, son equivalentes:
(a) M es simple.
(b) Cada elemento no nulo es un generador.

Proposición. 19.30.
Sea M un módulo y $N \subsetneq M$ un submódulo propio, son equivalentes:
(a) $N \subseteq M$ es un submódulo maximal.
(b) El módulo cociente M/N es simple.

Proposición. 19.31.
Si $\mathfrak{a} \subseteq A$ es un ideal, son equivalentes:
(a) $\mathfrak{a}$ es un ideal maximal.
(b) $A/\mathfrak{a}$ es un módulo simple.
(c) $A/\mathfrak{a}$ es un cuerpo.

Corolario. 19.32.
Si $\mathfrak{m}$ *es un ideal maximal de* A*, entonces* $\mathfrak{m} \subseteq A$ *es un ideal primo.*

Ejercicios

Homomorfismos

Ejercicio. 19.33.
Sea $\{M_i \mid i \in I\}$ una familia de A-módulos y M un A-módulo. Demostrar que existen isomorfismos de A-módulos

(1) $\mathrm{Hom}_A(\oplus_i M_i, M) \cong \prod_i \mathrm{Hom}_A(M_i, M)$.
(2) $\mathrm{Hom}_A(M, \prod_i M_i) \cong \prod_i \mathrm{Hom}_A(M, M_i)$.

Ref.: 1105e_006 *SOLUCIÓN.*

Ejercicio. 19.34.
*Un A-módulo M se llama **simple** si es no nulo y sus únicos submódulos son 0 y el propio M.*

(1) Demuestra que si M es simple entonces es cíclico.
(2) Demuestra que un A-módulo no nulo es simple si, y sólo si, cada elemento no nulo genera M.
(3) Demuestra que un A-módulo es simple si, y sólo si, es isomorfo a un cociente $A/\mathfrak{m}$, para algún ideal maximal $\mathfrak{m}$ de A.
(4) Demuestra que si M es un A-módulo simple, entonces $\mathrm{End}_A(M)$ es un anillo de división (no necesariamente es conmutativo si A no lo es).

Ref.: 1105e_008 *SOLUCIÓN.*

Sea $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$, con f y g homomorfismos de A-módulos. Decimos que la anterior es una **sucesión exacta corta** si verifica:
(I) f es un monomorfismo,
(II) g es un epimorfismo y
(III) $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

Y lo representamos diciendo que $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ es exacta.

Ejercicio. 19.35.
Se considera un diagrama conmutativo de A-módulos y homomorfismos de A-módulos

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f} & M_2 & \xrightarrow{g} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{f'} & N_2 & \xrightarrow{g'} & N_3 & \longrightarrow & 0 \end{array}$$

tal que cada fila es una sucesión exacta. Demostrar que se verifica:

(1) Si α y γ son monomorfismos, entonces β es un monomorfismo.
(2) Si α y γ son epimorfismos, entonces β es un epimorfismo.
(3) Si α y γ son isomorfismos, entonces β es un isomorfismo.

Ref.: 1105e_009 *SOLUCIÓN.*

Ejercicio. 19.36.
Se consideran dos homomorfismos de A-módulos

$$f : L \longrightarrow M, \qquad g : K \longrightarrow M,$$

siendo g un monomorfismo. Demostrar que las siguientes condiciones son equivalentes:

(a) Existe un único homomorfismo de A-módulos $h : L \longrightarrow K$ tal que $gh = f$.
(b) $\mathrm{Im}(f) \subseteq \mathrm{Im}(g)$.

Ref.: 1105e_010 *SOLUCIÓN.*

Ejercicio. 19.37.
Sea M un A-módulo y $m \in M$, llamamos ***anulador*** *de m en A a $\mathrm{Ann}_A(m) = \{r \in A \mid rm = 0\}$.*

(1) Demostrar que $\mathrm{Ann}_A(m)$ es un ideal de A.
(2) Demostrar que $Am \cong A/\mathrm{Ann}_A(m)$.

Ref.: 1105e_002 *SOLUCIÓN.*

Ejercicio. 19.38.
Sea M un A-módulo, llamamos el ***anulador*** *de M en A a $\mathrm{Ann}_A(M) = \{r \in A \mid rm = 0$ para cada $m \in M\}$.*

(1) Demostrar que $\mathrm{Ann}_A(M)$ es un ideal de A y que se verifica la igualdad: $\mathrm{Ann}_A(M) = \cap\{\mathrm{Ann}_A(m) \mid m \in M\}$.

(2) Demostrar que M tiene una estructura de $A/\operatorname{Ann}_A(M)$-módulo que extiende la de A-módulo.
(3) Si llamamos $B = A/\operatorname{Ann}_A(M)$, demostrar que $\operatorname{Ann}_B(M) = 0$.

Un A-módulo de llama ***fiel*** *si $\operatorname{Ann}_A(M) = 0$.*
Ref.: 1105e_003 *SOLUCIÓN.*

Ejercicio. 19.39.
Considerar los grupos abelianos $A_1 = \mathbb{Z}_2 \times \mathbb{Z}_3$, $A_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, $A_3 = \mathbb{Z}_2 \times \mathbb{Z}_4$. Calcular $\operatorname{Ann}_{\mathbb{Z}}(A_i)$, para $i = 1, 2, 3$. Calcular el submódulo $\mathbb{Z}(1, 1)$ de A_i, $i = 1, 2, 3$.
Ref.: 1105e_004 *SOLUCIÓN.*

Ejercicio. 19.40.
Sean M_1 y M_2 dos A-módulos y N_1, N_2 submódulos de M_1 y M_2 respectivamente. Sea $f : M_1 \longrightarrow M_2$ un homomorfismo de A-módulos tal que $f(N_1) \subseteq N_2$. Si llamamos $p_i : M_i \longrightarrow M_i/N_i$ es la proyección canónica, demostrar que existe un único homomorfismo de A-módulos $f' : M_1/N_1 \longrightarrow M_2/N_2$, tal que $p_2 f = f' p_1$. ¿Bajo qué condiciones es f' un monomorfismo? ¿Cuando es f' un epimorfismo? ¿Cuando es f' un isomorfismo?
Ref.: 1105e_011 *SOLUCIÓN.*

20. Producto y suma directa de A-módulos

Producto directo

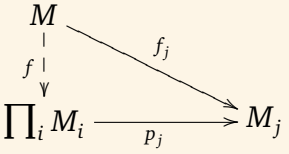
Sea $\{M_i \mid i \in I\}$ una familia de A-módulos, en $\prod\{M_i \mid i \in I\}$, el conjunto producto cartesiano de esta familia, definimos dos operaciones

$$(m_i)_i + (m_i')_i = (m_i + m_i')_i \text{ y}$$
$$a(m_i)_i = (am_i)_i$$

Lema. 20.1.
Sea $\{M_i \mid i \in I\}$ una familia de A-módulos, entonces el producto cartesiano $\prod\{M_i \mid i \in I\}$, con las operaciones definidas anteriormente, es un A-módulo, y las proyecciones canónicas $p_j : \prod\{M_i \mid i \in I\} \longrightarrow M_j$ son homomorfismos de A-módulos.

$\prod\{M_i \mid i \in I\}$ se llama el **módulo producto (directo)** de la familia, y cada A-módulo M_j se llama un **factor** de $\prod\{M_i \mid i \in I\}$.

Proposición. 20.2. (Propiedad universal del producto)
Si se considera una familia de A-módulos $\{M_i \mid i \in I\}$ y para cada $j \in I$ sea $f_j : M \longrightarrow M_j$ un homomorfismo de A-módulos, entonces existe un único homomorfismo de A-módulos $f : M \longrightarrow \prod\{M_i \mid i \in I\}$ tal que $f_j = p_j f$ para cada $j \in I$.



1105-03.tex

Lema. 20.3.
Sean $\{M_i \mid i \in I\}$ *y* $\{N_i \mid i \in I\}$ *dos familias de A-módulos y* $\{f_i : M_i \longrightarrow N_i \mid i \in I\}$ *una familia de homomorfismos de A-módulos,*

$$\begin{array}{ccc} \prod_i M_i & \xrightarrow{p_j} & M_j \\ {\scriptstyle \prod_i f_i}\downarrow & & \downarrow{\scriptstyle f} \\ \prod_i N_i & \xrightarrow[q_j]{} & N_j \end{array}$$

existe un único homomorfismo de A-módulos, al que representamos por $\prod_i f_i : \prod\{M_i \mid i \in I\} \longrightarrow \prod\{N_i \mid i \in I\}$ *verificando* $f_j p_j = q_j(\prod f_i)$ *para cada* $j \in I$*, siendo* q_j *las proyecciones canónicas del producto de la familia* $\{N_i \mid i \in I\}$*.*

La definición de $\prod_i f_i$ es como sigue:

$$\left(\prod_i f_i\right)((m_i)_i) = (f_i(m_i))_i.$$

Lema. 20.4.
Sea $\{M_i \mid i \in I\}$ *una familia de A-módulos, y para cada* $i \in I$*, sea* N_i *un submódulo de* M_i*. Se verifica entonces que* $\prod\{N_i \mid i \in I\}$ *es un submódulo de* $\prod\{M_i \mid i \in I\}$ *y se tiene el isomorfismo*

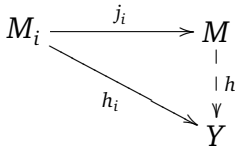
$$\frac{\prod\{M_i \mid i \in I\}}{\prod\{N_i \mid i \in I\}} \cong \prod\{M_i/N_i \mid i \in I\}.$$

Suma directa

Sea $\{M_i \mid i \in I\}$ una familia de A-módulos, se llama **suma directa** de la familia a un A-módulo M junto con una familia de homomorfismos de A-módulos $\{j_i : M_i \longrightarrow M \mid i \in I\}$ verificando: *para cada A-módulo* X *y cada familia de homomorfismos de A-módulos* $\{f_i : M_i \longrightarrow X \mid i \in I\}$*, existe un único homomorfismo de A-módulos* $f : M \longrightarrow X$ *tal que* $f_i = f \circ j_i$ *para cada índice* $i \in I$, esto es, los siguientes diagramas son conmutativos para todo $i \in I$.

$$\begin{array}{ccc} M_i & \xrightarrow{j_i} & M \\ & {\scriptstyle f_i}\searrow & \downarrow{\scriptstyle f} \\ & & X \end{array}$$

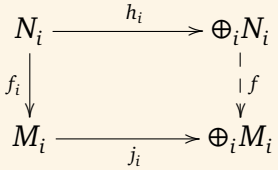
La suma directa, si existe, está definida de forma única salvo isomorfismo, esto es, si el par $(Y, \{h_i : M_i \longrightarrow Y \mid i \in I\})$ es otra suma directa de la misma familia, entonces existe un isomorfismo $h : M \longrightarrow Y$ tal que $h_i = h \circ j_i$ para cada $i \in I$. Esto es, los siguientes diagramas son conmutativos para todo $i \in I$.



Proposición. 20.5.
Para cada familia de A–módulos $\{M_i \mid i \in I\}$ se tiene:

(1) Para cada $i \in I$ el homomorfismo $j_i : M_i \longrightarrow \oplus_i M_i$ es un monomorfismo;

(2) Sean $\{M_i \mid i \in I\}$ y $\{N_i \mid i \in I\}$ familias de A–módulos de forma que para cada índice $i \in I$ existe un homomorfismo de A–módulos $f_i : N_i \longrightarrow M_i$. Existe un único homomorfismo $f : \oplus_i N_i \longrightarrow \oplus_i M_i$ tal que $j_i \circ f_i = f \circ h_i$ para cada $i \in I$, siendo $h_i : N_i \longrightarrow \oplus_i N_i$ la inclusión canónica de N_i en la suma directa;



(3) Si cada f_i es un monomorfismo, resp. epimorfismo, entonces f es un monomorfismo, resp. epimorfismo;

(4) $\oplus_i(M_i/N_i) \cong \dfrac{\oplus_i M_i}{\oplus_i N_i}$.

De forma dual tenemos el concepto de **producto directo** de una familia de A–módulos.

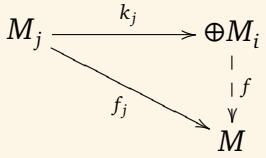
Ejercicio. 20.6.
Desarrolla el concepto de producto directo y sus propiedades de forma análoga a como hemos hecho con la suma directa.

Para cada familia de A-módulos $\{M_i \mid i \in I\}$ vamos a construir una suma directa. Dada una familia de A-módulos $\{M_i \mid i \in I\}$, para cada elemento $(m_i)_i \in \prod\{M_i \mid i \in I\}$ definimos el soporte de $(m_i)_i$ como el conjunto de todos los elementos $j \in I$ tales que $m_j \neq 0$. Se llama **suma directa** de la familia $\{M_i \mid i \in I\}$ al siguiente submódulo de $\prod\{M_i \mid i \in I\}$:

$$\oplus\{M_i \mid i \in I\} = \{(m_i)_i \in \prod_i M_i \mid \text{ soporte de } (m_i)_i \text{ es finito}\}.$$

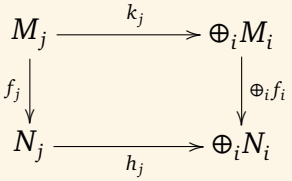
Para cada índice j definimos una aplicación $k_j : M_j \longrightarrow \oplus\{M_i \mid i \in I\}$ mediante $k_j(m) = (m_i)_i$, donde $m_i = \begin{cases} 0, \text{ si } i \neq j, \\ m, \text{ si } i = j. \end{cases}$ Los homomorfismos k_j se llaman **inclusiones canónicas**, y cada M_j se llama un **sumando directo** de $\oplus\{M_i \mid i \in I\}$.

Lema. 20.7. (Propiedad universal de la suma directa)
El par $(\oplus M_i, \{k_i \mid i \in I\})$ es una suma directa de la familia $\{M_i \mid i \in I\}$. Esto es, dada la familia de A–módulos $\{M_i \mid i \in I\}$ tal que para cada índice j existe un homomorfismo de A-módulos $f_j : M_j \longrightarrow M$, entonces existe un único homomorfismo de A-módulos $f : \oplus M_i \longrightarrow M$ tal que $f_j = g \circ k_j$ para cada índice $j \in I$.



Por abuso de lenguaje, al igual que en el caso del núcleo y el conúcleo, se llama **suma directa** de la familia al A-módulo $\oplus_i M_i$, sobre-entendiendo los homomorfismos k_i.

Lema. 20.8.
Sean $\{M_i \mid i \in I\}$ y $\{N_i \mid i \in I\}$ dos familias de A-módulos y $\{f_i : M_i \longrightarrow N_i \mid i \in I\}$ una familia de homomorfismos de A-módulos, entonces existe un único homomorfismo de A-módulos, al que representamos por $\oplus f_i : \oplus\{M_i \mid i \in I\} \longrightarrow \oplus\{N_i \mid i \in I\}$, verificando $h_j f_j = (\oplus f_i)k_j$ para cada $j \in I$, siendo h_j las inclusiones canónicas de la suma directa de la familia $\{N_i \mid i \in I\}$.



La definición de $\oplus_i f_i$ es la siguiente:

$$(\oplus_i f_i)((m_i)_i) = (f_i(m_i))_i.$$

Lema. 20.9.
Sea $\{M_i \mid i \in I\}$ una familia de A-módulos, y para cada $i \in I$ sea N_i un submódulo de M_i. Se verifica entonces que $\oplus\{N_i \mid i \in I\}$ es un submódulo de $\oplus\{M_i \mid i \in I\}$ y se tiene el isomorfismo

$$\frac{\oplus_i\{M_i \mid i \in I\}}{\oplus_i\{N_i \mid i \in I\}} \cong \oplus_i \{M_i/N_i \mid i \in I\}.$$

Sumas directas finitas

Sea $M_1, \ldots, M_t$ una familia finita de A–módulos. Podemos considerar la suma directa $\oplus\{M_i \mid i = 1, \ldots, t\} = M_1 \oplus \cdots \oplus M_t$. Observar que junto a los homomorfismos $k_i : M_i \longrightarrow \oplus_i M_i$ tenemos las proyecciones definidas por

$$p_j : \oplus_i M_i \longrightarrow M_j, \quad p_j(m_1, \ldots, m_t) = m_j.$$

Es fácil ver que $(\oplus_i M_i, \{p_i \mid i = 1, \ldots, t\})$ es un producto directo de la familia.
Los homomorfismos j_i y p_i verifican, entre otras, las siguientes relaciones:

$$\begin{array}{ll} p_i \circ j_i = \mathrm{id}_{M_i}, & \forall i = 1, \ldots, t \\ p_i \circ j_h = 0, & \text{si } i \neq h \\ j_1 p_1 + \cdots + j_t p_t = \mathrm{id}_M. & \end{array}$$

Podemos entonces enunciar y probar el siguiente teorema.

Teorema. 20.10.
Sea $M, M_1, \ldots, M_t$ una familia finita de A–módulos y $\{j_i : M_i \longrightarrow M \mid i = 1, \ldots, t\}$ una familia finita de homomorfismos. Son equivalentes

(a) $(M, \{j_i \mid i = 1, \ldots, t\})$ es una suma directa.
(b) Existe una familia de homomorfismos $\{p_i : M \longrightarrow M_i \mid i = 1, \ldots, t\}$ tal que $p_i \circ j_h = \delta_{i,h}\, id_{M_i}$ y $\sum_{i=1}^{t} j_i \circ p_i = id_M$.

De forma dual podemos enunciar este Teorema para productos directos.

Ejercicio. 20.11.
Enunciar y probar el Teorema (20.10.) para productos directos.

Una propiedad interesante de la suma directa de una familia finita ó infinita de A-módulos es que todo elemento no nulo se expresa, de forma única, como una suma finita de elementos no nulos de cada uno de los sumandos:

$$(m_i)_i = \sum \left\{ j_j(m_j) \mid \ j \text{ en el soporte de } (m_i)_i \right\}.$$

Suma directa interna

Se considera ahora un A–módulo M y una familia finita de submódulos: $N_1, \ldots, N_t$. Estamos interesados en relacionar $\oplus_{i=1}^t N_i$ y M.
Como consecuencia de la propiedad universal de la suma directa tenemos un homomorfismo, $f : \oplus_{i=1}^t N_i \longrightarrow M$, inducido por las inclusiones $N_i \subseteq M$ y definido por: $f((n_i)_i) = \sum_{i=1}^t n_i$.

Lema. 20.12.
Con la notación anterior se verifica:

(1) f es sobreyectivo si, y solo si, $\sum_{i=1}^t N_i = M$,
(2) f es inyectivo si, y solo si, $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_t) = 0$ para cada índice j, si, y solo si, $N_j \cap (N_1 + \cdots + N_{j-1}) = 0$ para cada índice j,
(3) f es un isomorfismo si, y sólo si, todo elemento no nulo de M se expresa de forma única como $m = m_1 + \cdots + m_r$, con $m_i \in N_{i_i}$, si, y sólo si, $M = \sum\{N_i \mid \ i \in I\}$ y para cada $j \in I$ se tiene $N_j \cap (\sum\{N_i \mid \ i \in I, i \neq j\} = 0$.

Cuando f es un isomorfismo decimos que M es la **suma directa interna** de los $N_1, \ldots, N_t$.
Una familia finita de submódulos $N_1, \ldots, N_t \subseteq M$ se dice **independiente** si verifica las condiciones equivalentes del apartado (2) del Lema (20.12.).

Homomorfismos

En el caso de tratar con homomorfismos entre dos sumas directas de familias finitas de módulos, el uso de matrices es muy útil como vamos a ver a continuación.

Proposición. 20.13.
Dadas dos familias finitas de A–módulos $\{M_i \mid \ i = 1, \ldots, t\}$ y $\{N_h \mid \ h = 1, \ldots, s\}$, existe un isomorfismo

$$\mathrm{Hom}_A(\oplus_{i=1}^t M_i, \oplus_{h=1}^s N_h) \cong \oplus_{i=1}^t \oplus_{h=1}^s \mathrm{Hom}_A(M_i, N_h),$$

que a cada homomorfismo $f : \oplus_{i=1}^t M_i \longrightarrow \oplus_{h=1}^s N_h$ hace corresponder $(f_{hi})_{hi}$, donde $f_{hi} : M_i \longrightarrow N_h$ está definido $f_{hi}(x) = (p_h \circ f \circ j_i)(x)$.

DEMOSTRACIÓN. Vamos a construir la aplicación inversa. Dado $(f_{hi})_{hi}$, para cada índice i consideramos $\{f_{hi} \mid h = 1, \ldots, s\}$, que inducen un homomorfismo $f_i : M_i \longrightarrow \prod_h N_h$. Ahora consideramos la familia $\{f_i \mid i = 1, \ldots, t\}$, que induce un homomorfismo $\oplus_i M_i \longrightarrow \prod_h N_h$, que es el morfismo f inicial. □

El homomorfismo $f : \oplus_{i=1}^t M_i \longrightarrow \oplus_{h=1}^s N_h$ puede ahora representarse por la matriz $(f_{hi})_{hi}$, y la imagen de un elemento $(m_1, \ldots, m_t) \in \oplus_i M_i$ se expresa:

$$\begin{pmatrix} f_{11} \cdots f_{1t} \\ \vdots \ \ddots \ \vdots \\ f_{s1} \cdots f_{st} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_t \end{pmatrix} = \begin{pmatrix} \sum_i f_{1i}(m_i) \\ \vdots \\ \sum_i f_{si}(m_i) \end{pmatrix} \in \oplus_{h=1}^s N_h.$$

Ejercicios

Producto y suma directa

Ejercicio. 20.14.
Sea $\{N_i \mid i \in I\}$ *una familia de submódulos de un A-módulo* M*, si* $\cap_i N_i = 0$*, demostrar que* M *es isomorfo a un submódulo de* $\prod_i M/N_i$*.*
Ref.: 1105e_007 SOLUCIÓN.

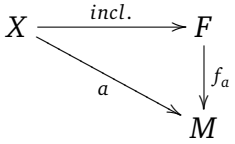
Ejercicio. 20.15.
Sea M *un A-módulo y* N_1*,* N_2 *submódulos de* M*. Si* $M = N_1 \oplus N_2$*, probar que* $M/N_1 \cong N_2$*. ¿Es cierta la afirmación recíproca?*
Ref.: 1105e_013 SOLUCIÓN.

Ejercicio. 20.16.
Sea M *un A-módulo y* $f : M \longrightarrow M$ *un endomorfismo de A-módulos, tal que* $f^2 = f$*. Demostrar que* $M = \mathrm{Im}(f) \oplus \mathrm{Ker}(f)$*.*
Ref.: 1105e_014 SOLUCIÓN.

Ejercicio. 20.17.
Un A-módulo M *se llama* ***indescomponible*** *si cuando* $M \cong N_1 \oplus N_2$ *entonces* $N_1 = 0$ *ó* $N_2 = 0$*. Demostrar que los siguientes* $\mathbb{Z}$*-módulos son indescomponibles:* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{Z}_{p^n}$*, para* $p \in \mathbb{Z}$ *primo.*
Ref.: 1105e_015 SOLUCIÓN.

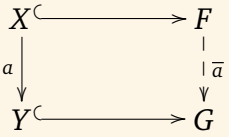
21. Módulos libres

Supongamos que F es un A-módulo y sea X un subconjunto de F, decimos que F es **libre** sobre X si para cualquier aplicación $a : X \longrightarrow M$, de X en un A-módulo M, existe un único homomorfismo de A-módulos $f_a : F \longrightarrow M$ tal que $f_a(x) = a(x)$ para cada $x \in X$.



El A-módulo cero es libre sobre el conjunto vacío. Si A es un cuerpo, entonces todo espacio vectorial es libre sobre un subconjunto.

Lema. 21.1.
Si F es libre sobre X, G es libre sobre Y, y existe una aplicación de $a : X \longrightarrow Y$, entonces a induce un homomorfismo de $\overline{a} : F \longrightarrow G$. Si a es una biyección, entonces $\overline{a}$ es un isomorfismo.



Como consecuencia, sobre cada conjunto X existe, salvo isomorfismo, un único módulo libre. Observar que módulos libres sobre conjuntos con el mismo cardinal son isomorfos.
Un subconjunto $\{x_h \mid h \in H\}$ de un A-módulo M se llama **linealmente independiente** si para todo subconjunto finito $K \subseteq H$ se tiene:

$$\sum\{r_k x_k \mid k \in K\} = 0 \text{ implica } r_k = 0 \text{ para cada } k \in K.$$

Un subconjunto de un A-módulo libre F se llama una **base** si es linealmente independiente y genera F.

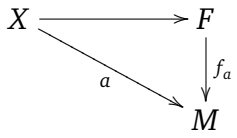
Lema. 21.2.
Sea F un A-módulo y $X = \{x_h \mid h \in H\}$ un subconjunto de F. Son equivalentes:
(a) F es un A-módulo libre con base X.
(b) F es un A-módulo libre sobre X.
(c) $F \cong \oplus\{Ax_h \mid h \in H\}$, con $Ax_h \cong A$ para todo $h \in H$, y X es una base de F.

1105-04.tex

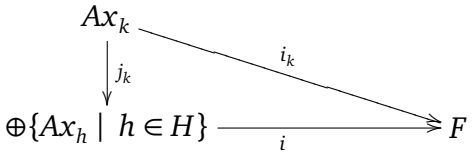
DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Dado un A-módulo M y una aplicación $a : X \longrightarrow M$, existe un homomorfismo de A-módulos $f_a : F \longrightarrow M$ definido por

$$f_a(\sum\{r_h x_h \mid h \in H\}) = \sum\{r_h a(x_h) \mid h \in H\}$$

con casi todos los r_h nulos. Es claro que f_a está bien definido y que es el único que hace conmutar el diagrama

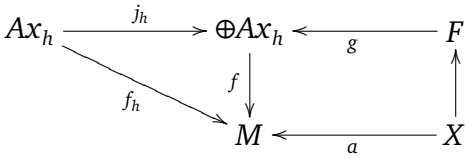


(b) $\Rightarrow$ (c). Dado $k \in H$, vamos a comprobar que Ax_k es isomorfo a A. Si existe $r \in A$ tal que $rx_k = 0$, entonces definimos $b : X \longrightarrow A$ mediante $b(x_h) = 0$ si $h \neq k$ y $b(x_k) = 1$, entonces $f_b : F \longrightarrow A$ verifica: $r = r1 = rf_b(x_k) = f_b(rx_k) = f_b(0) = 0$. Luego definiendo $a_k : A \longrightarrow Ax_k$, $a_k(r) = rx_k$, tenemos el isomorfismo pedido. Definimos ahora para cada $k \in H$ el homomorfismo inclusión $i_k : Ax_k \longrightarrow F$. Inducido por la familia $\{i_h \mid h \in H\}$, existe un único homomorfismo de A-módulos $i : \oplus\{Ax_h \mid h \in H\} \longrightarrow F$ tal que $i_k = ij_k$, donde j_k son las inclusiones canónicas a la suma directa.



Para comprobar que i es un isomorfismo, vamos a construir un inverso. Definimos $a : X \longrightarrow \oplus Ax_h$ mediante $a(x_h) = j_h(x_h)$, para todo $h \in H$; inducido por a existe un único homomorfismo $f_a : F \longrightarrow \oplus Ax_h$ tal que $f_a(x) = a(x)$ para cada $x \in X$. Es claro que f_a es un inverso de i.

(c) $\Rightarrow$ (a). Supongamos que tenemos un isomorfismo $g : F \longrightarrow \oplus Ax_h$ verificando $g(x_h) = x_h$ para cada $h \in H$. Para cada $h \in H$ llamamos $b_h : Ax_h \longrightarrow A$ al isomorfismo existente. Sea M un A-módulo, dada una aplicación $a : X \longrightarrow M$, definimos, para cada $h \in H$, un homomorfismo $f_h : Ax_h \longrightarrow M$ mediante $f_h(rx_h) = ra(x_h)$. Inducido por la familia $\{f_h \mid h \in H\}$ existe un único homomorfismo $f : \oplus Ax_h \longrightarrow M$ verificando $f_h = f j_h$ para cada $h \in H$



Entonces la composición fg es el único homomorfismo de F en M que verifica $fg(x) = a(x)$ para cada $x \in X$, luego F es sobre sobre X. Finalmente por el isomorfismo $g : F \longrightarrow \oplus Ax_h$ deducimos que X es una base de F. □

Dado un conjunto X existe siempre un A–módulo libre sobre X. Para construirlo definimos $F = \oplus\{A_x \mid x \in X,\ A_x = A,\ \text{para todo } x \in X\}$ e $i : X \longrightarrow F$ mediante $i(x) = e_x$, donde $e_x = (\delta_{x,y})_y$. De esta forma podemos identificar X con el conjunto $\{e_x \mid x \in X\}$.

Proposición. 21.3.
Con la notación anterior F es libre sobre X.

Tenemos un resultado de interés sobre bases de módulos libres.

Proposición. 21.4.
Sea F un módulo libre, y $\mathscr{B} = \{x_h \mid h \in H\} \subseteq F$ un subconjunto no vacío. Son equivalentes:
(a) $\mathscr{B}$ es una base de F.
(b) $\mathscr{B}$ es un subconjunto linealmente independiente maximal, y un sistema de generadores minimal.

DEMOSTRACIÓN. (b) $\Rightarrow$ (a). Es inmediato por la definición de base.
(a) $\Rightarrow$ (b). Para ver que es un conjunto linealmente independiente maximal, si $x \in F \subseteq \mathscr{B}$, y $\mathscr{B} \cup \{x\}$ es linealmente independiente, entonces $x \neq 0$, y por ser $\mathscr{B}$ un sistema de generadores, existe una expresión $x = \sum_h c_h x_h$, y por tanto $x - \sum_h c_h x_h = 0$, lo que es imposible pues $\lfloor \cup \{x\}$ es linealmente independiente.
Para ver que $\mathscr{B}$ es un sistema de generadores minimal, sea $\mathscr{D} \subsetneq \mathscr{B}$ un sistema de generadores de F, y sea $x \in \mathscr{B} \setminus \mathscr{D}$, por ser $\mathscr{D}$ un sistema de generadores existe una expresión $x = \sum_d c_d x_d$, con $x_d \in \mathscr{D}$, y por lo tanto una expresión $x - \sum_d c_d x_d = 0$, lo que es imposible, y que $\mathscr{B}$ es linealmente independiente. □

Lema. 21.5.
Todo A-módulo es un cociente de un A-módulo libre, y por tanto de una suma directa de copias de A.

Corolario. 21.6.
Todo A-módulo finitamente generado es un cociente de un A-módulo libre con base finita.

Proposición. 21.7.
Si A es un anillo y F es un módulo libre con una base infinita, entonces cada dos bases de F tienen el mismo cardinal. (El resultado también es cierto si A es no conmutativo.)

DEMOSTRACIÓN. Supongamos que $\mathscr{B} = \{x_h \mid h \in H\} \subseteq F$ es una base infinita de F.
Si $\mathscr{D} = \{y_1, \dots, y_t\}$ es una base finita, para cada y_k existe $\mathscr{B}_k \subseteq \mathscr{B}$, finito, tal que $y_k \in \langle \mathscr{B}_k \rangle$, por tanto $\cup_k \mathscr{B}_k$ es un sistema de generadores, y es finito, lo que es una contradicción.
Si $\mathscr{D} = \{y_k \mid k \in K\}$ es una base infinita, para cada y_k consideramos $\mathscr{B}_k \subseteq \mathscr{B}$, finito, tal que $y_k \in \langle \mathscr{B}_k \rangle$. Tenemos así una aplicación $\nu : \mathscr{D} \longrightarrow \mathscr{P}_F(\mathscr{B})$, el conjunto de las partes finitas de $\mathscr{B}$. Del mismo modo podemos construir una aplicación $\theta : \mathscr{B} \longrightarrow \mathscr{P}_F(\mathscr{D})$.
Para cada $S \in \mathscr{P}_F(\mathscr{B})$ el conjunto $\nu^{-1}(S) \subseteq \mathscr{D}$ es finito. En efecto, se tiene $\langle \nu^{-1}(S) \rangle \subseteq \langle S \rangle$. Por otro lado, $\langle S \rangle \subseteq \langle \theta(S) \rangle$, y juntando estas inclusiones tenemos:

$$\langle \nu^{-1}(S) \rangle \subseteq \langle S \rangle \subseteq \langle \theta(S) \rangle.$$

En consecuencia $\nu^{-1}(S) \subseteq \theta(S)$ y es un conjunto finito.
Consideramos en $\mathscr{D}$ la relación de equivalencia dada por $y_k \sim y_{k'}$ si $\nu(y_k) = \nu(y_{k'})$, como cada clase de equivalencia tiene un número finito de elementos, resulta que $\operatorname{card}(\mathscr{D}) = \operatorname{card}(\mathscr{D}/\sim)$. Por otro lado, existe una aplicación inyectiva $\mathscr{D}/\sim \xrightarrow{\nu} \mathscr{P}_F(\mathscr{B})$, y por tanto $\operatorname{card}(\mathscr{D}) = \operatorname{card}(\mathscr{D}/\sim) \leq \operatorname{card}(\mathscr{P}_F(\mathscr{B})) = \operatorname{card}(\mathscr{B})$. Del mismo modo tendríamos $\operatorname{card}(\mathscr{B}) \leq \operatorname{card}(\mathscr{D})$, y los dos cardinales coinciden. □

Corolario. 21.8.
Si K es un cuerpo (anillo de división), dos bases de un espacio vectorial tienen el mismo cardinal.

DEMOSTRACIÓN. Si una base tiene cardinal infinito, el resultado es cierto. Supongamos que las bases tienen cardinal finito, sean $\mathscr{B} = \{x_1, \dots, x_n\}$ y $\mathscr{D} = \{y_1, \dots, y_m\}$, con $n > m$. Dado x_1, lo expresamos en función de los y_k, sea $x_1 = \sum_k a_{1,k} y_k$, como algún $a_{1,k}$ es no nulo, sea $a_{1,1} \neq 0$, tendremos una expresión $y_{1,1} = \frac{1}{a_{1,1}}(x_1 - \sum_{k=2} a_{1,k} y_k)$, y $\{x_1, y_2, \dots, y_m\}$ es un sistema de generadores. Siguiendo el proceso podemos incluir en este conjunto a $x_2, x_3, \dots$, llegando a que el conjunto $\{x_1, x_2 \dots, x_m\}$ es un sistema de generadores, lo que es una contradicción. □

Corolario. 21.9.
Si A es un anillo (conmutativo) entonces cada dos bases de un mismo A-módulo libre tienen el mismo cardinal.

DEMOSTRACIÓN. Si F es un A–módulo libre sobre un conjunto X y $\mathfrak{m}$ es un ideal maximal de A, en $F \cong A^{(X)}$ podemos considerar el submódulo $\mathfrak{m}A^{(X)}$; es claro que tenemos

$$\frac{A^{(X)}}{\mathfrak{m}A^{(X)}} = \frac{A^{(X)}}{\mathfrak{m}^{(X)}} \cong \left(\frac{A}{\mathfrak{m}}\right)^{(X)},$$

que es un $A/\mathfrak{m}$–espacio vectorial de dimensión $\mathrm{card}(X)$. Como consecuencia si F es A–módulo libre sobre un conjunto X resulta que $\mathrm{card}(X)$ es un invariante de F. □

Si A es un anillo conmutativo y F es un A–módulo libre sobre un conjunto X, el cardinal de X es un invariante de F al que llamamos el **rango** de F.

Esto completa la teoría de módulos libres, de forma que, sobre un anillo conmutativo, a cada número cardinal podemos asociar una única clase de isomorfía de módulos libres de forma que esta correspondencia sea biyectiva.

Proposición. 21.10.
Sea F un A-módulo libre y $f : M \longrightarrow F$ un epimorfismo de A-módulos, entonces existe un homomorfismo de A-módulos $g : F \longrightarrow M$ tal que $f \circ g = id_F$. Además M es la suma directa interna de $\mathrm{Im}(g)$ *y* $\mathrm{Ker}(f)$.

DEMOSTRACIÓN. Ya que F es libre, supongamos que lo es sobre un subconjunto X. Para cada $x \in X$ consideramos $m_x \in M$ tal que $f(m_x) = x$, y definimos $a : F \longrightarrow M$ mediante $a(x) = m_x$, entonces a define un homomorfismos de A-módulos $g : F \longrightarrow M$ verificando $g(x) = m_x$ para cada $x \in X$. Para ver que $f \circ g = \mathrm{id}_F$ basta comprobar que para cada cada $x \in X$ se verifica $f \circ g(x) = x$, lo cual es inmediato. Para la segunda parte supongamos que $x \in \mathrm{Im}(g) \cap \mathrm{Ker}(f)$, entonces tenemos que existe $y \in F$ tal que $g(y) = x$ y $f(x) = 0$; uniendo ambos hechos tenemos $0 = f(x) = f \circ g(y) = y$, luego $x = g(y) = 0$. Sea ahora $m \in M$, consideramos la diferencia $m - g \circ f(m)$, ya que $f(m - g \circ f(m)) = 0$, resulta que $m \in \mathrm{Im}(g) + \mathrm{Ker}(f)$. Entonces M es la suma directa interna de $\mathrm{Im}(g)$ y $\mathrm{Ker}(f)$. □

Dado un A–módulo M una **presentación libre** de M es dar un módulo libre F y un submódulo K tal que $F/K \cong M$, o equivalentemente dar un homomorfismo sobreyectivo de un módulo libre a M.

El módulo M se llama **finitamente presentado** cuando tanto F con K son finitamente generados. En este caso si F está generado por $\{f_1, \ldots, f_t\}$ y K está generado por $\{k_1, \ldots, k_s\}$, siendo $k_j = \sum_i a_i f_i$, representamos el módulo M como $M = \langle f_1, \ldots, f_t \mid \sum_i a_i f_i = 0 \rangle$.

En particular un A–módulo es finitamente generado si, y sólo si, es un cociente de una suma directa finita de copias de A y hay que advertir que un módulo finitamente generado no tiene que ser finitamente presentado.

Bases

Un anillo tiene la **propiedad IBN** (Invariant Basis Number) si cada módulo libre tiene rango, esto es, todas las bases tienen la misma cardinalidad. Como dos bases infinitas tiene la misma cardinalidad,

sólo hay que fijarse en módulos libres con bases finitas. Según hemos visto, todo anillo conmutativo tiene la propiedad IBN.
(1) Existen anillo no conmutativos que no tienen la propiedad IBN.
(2) Todo anillo noetheriano tiene la propiedad IBN.

Un anillo R tiene la **propiedad SBN** (Single Basis Number) si $R \cong R^t$ para cada $t \in \mathbb{N} \setminus \{0\}$.
(1) Anderson-Fuller [2, pag. 113–114]

Un anillo se llama un **anillo de Steinitz** si en cada módulo libre todo subconjunto linealmente independiente se puede extender a una base.
(1) Brodskii, G. M.; Endomorphism rings of free modules over perfect rings. Mat. Sbornik **88** (1972), 138–147.
(2) Chwe, B.-S.; Neggers, J.; On the extension of linearly independent subsets of free modules to bases. Proc. Amer. Math. Soc. **24** (1970), 466–470.
(3) Mahdou, N.; Mouanis, H.; On Steinitz-like conditions. J. Taibah Univ. Sci. **9** (2015), 340–345.
(4) mathoverflow núm. 140535: "A class of rings related to rings with IBN property".

Homomorfismos entre módulos libres finitamente generados

Cada A–módulo libre finitamente generado F es isomorfo a una suma directa A^n de copias del anillo A, por lo que el estudio de los homomorfismos entre dos A–módulos libres finitamente generados se reduce al estudio de homomorfismos entre sumas directas finitas de copias de A. Observar que el isomorfismo $F \cong A^n$ se establece fijando una base de F, por lo que tomando bases distintas podemos tener isomorfismos $F \cong A^n$ distintos.

Como cada endomorfismo de A está definido por un elemento $a \in A$, en virtud de la Proposición (20.13.) el estudio de los endomorfismos entre módulos libres finitamente generados se reduce al estudio de matrices con coeficientes en A.

Representamos por $\mathscr{M}_{nm}(A)$ el conjunto de las matrices con coeficientes en A con n filas y m columnas. Por simplicidad el conjunto $\mathscr{M}_{nn}(A)$ se representa por $\mathscr{M}_n(A)$. Un elemento de $\mathscr{M}_{nm}(A)$ se representa por

$$\begin{pmatrix} a_{11} \cdots a_{1m} \\ \vdots \ \ddots \ \vdots \\ a_{n1} \cdots a_{nm} \end{pmatrix}$$

El conjunto $\mathscr{M}_{nm}(A)$ tiene estructura de A–módulo y el conjunto $\mathscr{M}_n(A)$ tiene estructura de A–álgebra, aunque no conmutativa.

Al considerar la estructura multiplicativa de $\mathscr{M}_n(A)$ aparece de forma natural el **grupo lineal general**, $\mathrm{GL}_n(A)$, que es el grupo de las matrices invertibles.

Lema. 21.11.
Dadas dos matrices X e Y en $\mathscr{M}_{nm}(A)$ que representan el mismo homomorfismo respecto a distintas bases, existen matrices invertibles $P \in \mathscr{M}_n(A)$ y $Q \in \mathscr{M}_m(A)$ tales que $X = PYQ$.

Dos matrices X e Y en la situación del lema se llaman matrices **equivalentes**. Es claro que la relación "equivalente a" es una relación de equivalencia en $\mathscr{M}_{nm}(A)$.

Lema. 21.12.
Dadas dos matrices X e Y en $\mathscr{M}_n(A)$, que representan el mismo endomorfismo respecto a distintas bases, existe una matriz invertible P tal que $Y = PXP^{-1}$.

Dos matrices X e Y en la situación del lema se llaman matrices **semejantes**. Es claro que la relación "semejante a" es una relación de equivalencia en $\mathscr{M}_n(A)$.
Dada una matriz $X = (x_{ij})_{ij} \in \mathscr{M}_n(A)$, el **determinante** de X se define

$$\det(X) = \sum_{\sigma \in S_n} (-1)^{s(\sigma)} a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

El determinante de una matriz X verifica algunas propiedades geométricas que son de interés. Dada la matriz X, el **elemento adjunto** o **cofactor** de x_{ij} es el determinante de la matriz obtenida de X eliminando la fila i y la columna j, es pues el determinante de una matriz $(n-1) \times (n-1)$, afectado por el signo $(-1)^{i+j}$; se representa por X_{ij}. La **matriz adjunta** de la matriz X es la matriz $\operatorname{adj}(X) = (X_{ij})_{ji}$, esto es, la matriz traspuesta de la matriz formada por los elementos adjuntos.

Lema. 21.13. (Teorema de Laplace)
Dada una matriz $X = (x_{ij})_{ij} \in \mathscr{M}_n(A)$, se verifica:
(1) $\det(X) = x_{i1}X_{i1} + \cdots + x_{in}X_{in}$ *para cada índice* $i = 1, \ldots, n$.
(2) $\det(X) = x_{1j}X_{1j} + \cdots + x_{nj}X_{nj}$ *para cada índice* $j = 1, \ldots, n$.
(3) $X \operatorname{adj}(X) = \det(X)\, I = \operatorname{adj}(X)\, X$.

Corolario. 21.14.
Una matriz $X \in \mathscr{M}_n(A)$ es invertible si, y solo si, $\det(X)$ *es un elemento invertible en A.*

Ejercicios

Módulos libres

Ejercicio. 21.15.
Sean M un A-módulo finitamente generado, F un A-módulo libre y $f : M \longrightarrow F$ un epimorfismo. Demostrar que $\mathrm{Ker}(f)$ es también finitamente generado.
Ref.: 1105e_012 SOLUCIÓN.

Ejercicio. 21.16.
Sea A un anillo, demostrar que $A[X]$ es un A-módulo libre y no es finitamente generado.
Ref.: 1105e_016 SOLUCIÓN.

Ejercicio. 21.17.
Demostrar que $\mathbb{Q}$ no es un grupo abeliano finitamente generado. ¿Es un grupo abeliano libre?
Ref.: 1105e_017 SOLUCIÓN.

Ejercicio. 21.18.
Sea $x = (a, b) \in \mathbb{Z}^2$, demostrar que x puede completarse a una base del grupo abeliano $\mathbb{Z}^2$ si, y sólo si, a y b son primos relativos. Aplicarlo al caso en que $(a, b) = (3, 7)$.
Ref.: 1105e_019 SOLUCIÓN.

Ejercicio. 21.19.
¿Es libre el grupo abeliano $\mathbb{Z}[X]/(X^2 - 1)$?
Ref.: 1105e_020 SOLUCIÓN.

Ejercicio. 21.20.
¿Es libre el $\mathbb{Q}[X]$-módulo $\mathbb{Q}[X]/(X^2-1)$?
Ref.: 1105e_021 *SOLUCIÓN.*

Módulos finitamente generados

Ejercicio. 21.21.
Se considera el conjunto A de las aplicaciones de $\mathbb{R}$ en $\mathbb{R}$ con las operaciones

Suma: $(f+g)(x) = f(x)+g(x)$,

Producto: $(fg)(x) = f(x)g(x)$.

Demostrar que A es un anillo y que existe un A-submódulo (ideal) de A que no es finitamente generado.
Ref.: 1105e_018 *SOLUCIÓN.*

Ejercicio. 21.22.
Sea $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ una sucesión exacta.
(1) Demostrar que si M_2 es finitamente generado, entonces M_3 lo es.
(2) Demostrar que si M_1 y M_3 son finitamente generados, entonces M_2 lo es.

Ref.: 1105e_022 *SOLUCIÓN.*

Capítulo VI

Módulos sobre un DIP

Introducción

La estructura de los módulos sobre un DIP es muy rica y generaliza, en una primera etapa, la teoría de espacios vectoriales. Además, como veremos, tiene aplicaciones de interés: la primera es referida a la estructura de los grupos abelianos finitamente generados, y la segunda a la forma canónica de matrices con coeficientes en un cuerpo.

22. Módulos finitamente generados sobre DIP

Recordemos que un A-módulo M es finitamente generado si existe un subconjunto finito $m_1, \ldots, m_s \in M$ que es un sistema de generadores, esto es,

$$M = Am_1 + \cdots + Am_s.$$

Lema. 22.1.
Para un A–módulo M se tiene:

(1) Si M es finitamente generado, todo cociente de M es finitamente generado.
(2) M es un A-módulo finitamente generado si, y sólo si, es un cociente de un A-módulo libre con una base con un número finito de elementos.

Salvo que se indique lo contrario, suponemos, en lo que sigue, que A es un DIP.
Vamos a estudiar con más detalle módulos libres sobre un DIP. Llamamos **rango** de un A-módulo libre finitamente generado F al número de elementos de una base de F.

Teorema. 22.2.
Si F es un A-módulo libre finitamente generado, entonces todo submódulo N de F es un A-módulo libre y su rango es menor ó igual que el de F.

DEMOSTRACIÓN. Supongamos que el rango de F es n. Si $n = 1$, entonces $F \cong A$, y todo submódulo N de F es un ideal de A, luego está generado por un elemento; supongamos que $N = Aa$. Si $a = 0$, entonces N es libre de rango cero. Si $a \neq 0$, entonces definimos un homomorfismo $f : A \longrightarrow Aa$ mediante $f(r) = ra$, resulta que f es un isomorfismo, luego N es libre de rango uno.
Hagamos ahora la siguiente hipótesis de inducción: si L es un A-módulo libre de rango menor que rango de F, entonces todo submódulo N de L es libre de rango número ó igual que rango de L. Supongamos que $e_1, \ldots, e_n$ es una base de F, definimos una aplicación $\alpha : \{e_1, \ldots, e_n\} \longrightarrow A$ mediante $\alpha(e_1) = \cdots = \alpha(e_{n-1}) = 0$, $\alpha(e_n) = 1$; α define un homomorfismo sobreyectivo de A-módulos $f = f_\alpha : F \longrightarrow A$ con núcleo $\mathrm{Ker}(f) = Ae_1 + \cdots Ae_{n-1}$. Tenemos que $\mathrm{Ker}(f)$ es libre de rango $n-1$. Dado un submódulo N de F consideramos el siguiente diagrama conmutativo:

$$\begin{array}{ccccc} \mathrm{Ker}(f_{|N}) & \longrightarrow & N & \xrightarrow{f_{|N}} & f(N) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Ker}(f) & \longrightarrow & F & \xrightarrow[f]{} & A \end{array}$$

1106-06.tex

Tenemos que $f(N)$ es un submódulo de A, y por tanto es libre de rango menor ó igual que uno. Tenemos $\mathrm{Ker}(f_{|N}) = \mathrm{Ker}(f) \cap N$, luego es un submódulo libre de rango menor ó igual que $n-1$. Además $f_{|N}$ es sobreyectiva, luego existe un isomorfismo $N \cong \mathrm{Ker}(f_{|N}) \oplus f(N)$, esto es, N es la suma directa de dos A-módulos libres de rangos acotados por $n-1$ y 1 respectivamente, luego N es un A-módulo libre de rango menor ó igual que n. □

Sea M un A-módulo, un elemento $m \in M$ se llama de **torsión** si existe $0 \neq r \in A$ tal que $rm = 0$.

Lema. 22.3.
Sea A un DI, si M es un A-módulo, entonces el subconjunto

$$T(M) = \{m \in M \mid m \text{ es de torsión}\}$$

*es un submódulo de M. Se llama el **submódulo de torsión** de M.*

DEMOSTRACIÓN. Es evidente que $0 \in T(M)$, luego $T(M)$ es no vacío. Sean ahora m_1, $m_2 \in T(M)$, existen $0 \neq r_1, r_2 \in A$ tales que $r_1 m_1 = r_2 m_2 = 0$, luego $r_1 r_2 \neq 0$ y se tiene $(r_1 r_2)(m_1 + m_2) = 0$, entonces $m_1 + m_2 \in T(M)$. Por otro lado, sean $s \in A$ y $m \in T(M)$, entonces existe $0 \neq r \in A$ tal que $rm = 0$, y se verifica $r(sm) = 0$, luego $sm \in T(M)$. □

Lema. 22.4.
Sea A un DI y $f : M_1 \longrightarrow M_2$ un homomorfismo de A-módulos, entonces $f(T(M_1)) \subseteq T(M_2)$.

Lema. 22.5.
Sea A in DI y $\{M_i \mid i \in I\}$ una familia de A-módulos, se verifica:

$$T(\oplus_i M_i) = \oplus_i T(M_i).$$

Un A-módulo M se llama de **torsión** si $T(M) = M$ y **libre de torsión** si $T(M) = 0$.

Lema. 22.6.
Sea A un DI y M un A-módulo, se verifica que $M/T(M)$ es libre de torsión.

Ejemplo. 22.7.
Si A es un DI, entonces $T(A) = 0$, y A es un módulo libre de torsión; lo mismo ocurre con todo módulo libre, ya que si $M = A^{(I)}$ es libre, entonces $T(M) = T(A^{(I)}) = T(A)^{(I)} = 0$.

No todo módulo libre de torsión es libre como los siguientes ejemplos muestran.

Ejemplo. 22.8.
(1) $\mathbb{Z}$ es un DIP, y $\mathbb{Q}$ es un grupo abeliano libre de torsión, pero no es libre.
(2) $(2,X)$ es un $\mathbb{Z}[X]$–módulo libre de torsión, ya que $(2,X) \subseteq \mathbb{Z}[X]$, pero no es libre, ya que no puede ser generado por un sólo elemento, por lo que su rango es mayor que uno y $\mathbb{Z}[X]$ tiene rango uno.
(3) (X,Y) es un $\mathbb{Q}[X,Y]$–módulo libre de torsión, pero no es libre.

Aplicamos ahora esta teoría al estudio de módulos finitamente generados sobre un DIP.

Teorema. 22.9.
Sea A un DIP, para cada A-módulo finitamente generado M, son equivalentes:
(a) M es un A-módulo libre.
(b) M es un A-módulo libre de torsión.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Es evidente.

(b) $\Rightarrow$ (a). El caso $M = 0$ es inmediato. Para el caso no nulo, dado M finitamente generado y libre de torsión, consideramos t el menor entero positivo tal que existe un sistema de generadores $\{m_1, \ldots, m_t\}$ de M. Vamos a hacer inducción sobre t. Si $t = 1$, entonces $M \cong A$ es libre.

Supongamos M es libre si es libre torsión y puede ser generado por menos de t elementos, y sea M un módulo libre de torsión con un sistema de generadores $\{m_1, \ldots, m_t\}$, con t mínimo. Definimos Γ la familia de los subconjuntos de $\{m_1, \ldots, m_t\}$ que son linealmente independientes. En Γ la inclusión es una relación de orden. Además Γ es no vacío, ya que $M \neq 0$ y por tanto cada conjunto unitario $\{m\}$, con $m \neq 0$, es linealmente independiente.

Por ser Γ finito, en Γ existen elementos maximales. Tras una reordenación, sea $X = \{m_1, \ldots, m_s\} \in \Gamma$ maximal. Si X no es un sistema de generadores, $\langle X \rangle \subsetneq M$, y para cada índice $s < j \leq t$ se tiene $m_j \in M \setminus \langle X \rangle$, y existe una combinación lineal $x_j m_j + a_{j_1} m_1 + \cdots + a_{j_s} m_s = 0$ con $x_j \neq 0$; definimos $x = x_{s+1} \cdots x_t$.

Tenemos $M \cong xM \subseteq \langle X \rangle$, ya que para cada $m \in M$, que se expresa $m = \sum_{i=1}^{t} c_i m_i$, se verifica: $xm = x \sum_{i=1}^{t} c_i m_i = \sum_{i=1}^{t} (xc_i) m_i \in \langle X \rangle$. En consecuencia xM es un submódulo de un módulo libre, y es libre. Por el isomorfismo, $M \cong xM$, también M es un módulo libre. □

Corolario. 22.10.
Sea A un DIP y M un A-módulo finitamente generado, entonces M es isomorfo a $N \oplus F$, con N un submódulo de M de torsión y F un A-módulo libre de torsión, ambos finitamente generados.
Además, si M es isomorfo a $N' \oplus F'$ con N' y F' verificando las condiciones anteriores, entonces $N \cong N'$ y $F \cong F'$.

Lema. 22.11.
Sea A un DIP, M un A-módulo finitamente generado, y N un submódulo de M, entonces N es finitamente generado.

DEMOSTRACIÓN. Dado el submódulo $N \subseteq M$, existe un módulo libre A^t y un homomorfismo sobreyectivo $f : A^t \longrightarrow M$; si llamamos $S = f^{-1}(N)$, entonces S es un módulo libre de rango menor o igual que t, y por tanto N, que es un cociente de un módulo libre finitamente generado, es finitamente generado.

$$\begin{array}{ccccc} \mathrm{Ker} & \longrightarrow & S = f^{-1}(N) & \longrightarrow & A^t \\ \| & & \downarrow & & \downarrow \\ \mathrm{Ker} & \longrightarrow & N & \longrightarrow & M \end{array}$$

□

Apéndice

Ya conocemos que cada submódulo de un módulo libre finitamente generado sobre un DIP es libre; la condición finitamente generado no es necesaria como el siguiente teorema prueba.

Teorema. 22.12. (Teorema de Kaplansky)
Sea D un DIP, todo submódulo de un módulo libre es libre.

DEMOSTRACIÓN. Sea $N \subseteq F = D^{(I)}$ un submódulo de un módulo libre. Consideramos $\mathscr{B} = \{e_i \mid i \in I\}$, donde $e_i = (\delta_{i,j})_j$, base de F. En I consideramos un buen orden, y para cada $j \in I$ se define $F_j = \sum\{Ae_i \mid i \leq j\}$ y $N_j = N \cap F_j$.
Para cada $j \in I$ definimos un ideal $\mathfrak{a}_j \subseteq D$ como $p_j(N_j)$, siendo $p_j : F \longrightarrow D$ la j–ésima proyección. Como D es un DIP, sea $\mathfrak{a}_j = (d_j) = Dd_j$. Si $d_j \neq 0$, consideramos $n_j \in N_j$ tal que $p_j(n_j) = d_j$; si $d_j = 0$ no elegimos ningún elemento n_j.

Vamos a ver que $\mathscr{N} = \{n_i \mid i \in I, d_i \neq 0\}$ es linealmente independiente. En efecto, si $\sum_i c_i n_i = 0$ es una combinación lineal finita, consideramos el mayor de los i tal que $c_i \neq 0$; entonces n_i se aplica en d_i por p_i, y los demás se aplican en 0; por tanto $c_i = 0$, y $\mathscr{N}$ es linealmente independiente.

Vamos a ver que $\mathscr{N}$ es un sistema de generadores. Sea $x \in N \setminus D\mathscr{N}$. Como $N = \cup N_i$, existe $j \in I$ tal que $x \in N_j$, y, por la hipótesis, no está generado por los $\{n_i \mid i \leq j\}$. La componente j–ésima de x es $0 \neq x_j$, donde $x = \sum_i c_i e_i$, Por tanto $d_j(x) = x_j$, y existe $d \in D$ tal que $x_j = dd_j$. Por lo tanto el elemento $y = x - dn_j$ pertenece a N_j, y $p_j(y) = p(x - dn_j) = 0$, esto es, $y \in N_{j_2}$ para un $j_2 \leq j$. En consecuencia, repitiendo el proceso tenemos una sucesión decreciente de ordinales $j = j_1 > j_2 > \cdots$, que necesariamente es finita, y entonces x es una combinación de los n_i con $i \leq j$.

Tenemos entonces que $\mathscr{N} = \{n_i \mid i \in I, d_i \neq 0\}$ es una base de N, que por lo tanto es libre, de rango menor o igual que el rango de F. □

Ejercicios

Módulos finitamente generados sobre DIP

Ejercicio. 22.13.
Prueba que si A es un DIP, y M es un A–módulo generado por t elementos, todo submódulo de M está generado, a lo más, por t elementos
Ref.: 1106e_001 *SOLUCIÓN.*

Ejercicio. 22.14.
Si D es un DI, prueba que si cada D–módulo cíclico es libre de torsión, entonces D es un cuerpo.
Ref.: 1106e_006 *SOLUCIÓN.*

Ejercicio. 22.15.
Si D es un DI, prueba que si cada D–módulo finitamente generado es libre, entonces D es un cuerpo.
Ref.: 1106e_007 *SOLUCIÓN.*

23. Matrices con coeficientes en un DIP

En esta sección A será un DIP.
Llamamos $\mathscr{M}_{mn}(A)$ al conjunto de matrices de n columnas y m filas. Vamos a relacionar las matrices de $\mathscr{M}_{mn}(A)$ y los homomorfismos de $\mathrm{Hom}_A(A^n,A^m)$.
Si fijamos bases $\{e_i\}_{i=1}^n$ y $\{h_j\}_{j=1}^m$ de A^n y A^m respectivamente, y si tomamos $f \in \mathrm{Hom}_A(A^n,A^m)$, entonces tenemos:

$$\begin{cases} f(e_1) = x_{11}h_1 + \cdots + x_{1m}h_m \\ \cdots \quad \cdots\cdots \\ f(e_n) = x_{n1}h_1 + \cdots + x_{nm}h_m \end{cases}$$

Si llamamos $X = \begin{pmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{12} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & & \vdots \\ x_{1m} & x_{2m} & \cdots & x_{nm} \end{pmatrix}$, resulta que la imagen $f(y)$ de $y \in A^n$ de expresión $y = y_1e_1 + \cdots + y_ne_n$ se puede calcular como el elemento de A^m con coordenadas dadas por la siguiente fórmula;

$$\begin{pmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{12} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & & \vdots \\ x_{1m} & x_{2m} & \cdots & x_{nm} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

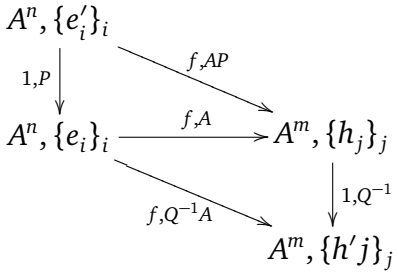
Decimos entonces que la matriz X representa al homomorfismo f respecto a las bases $\{e_i\}_i$ y $\{h_j\}_j$.
Consideremos ahora otro homomorfismo $g : A^m \longrightarrow A^r$, y sea $\{l_k\}_{k=1}^r$ una base de A^r, supongamos que Y es la matriz que representa a g respecto a las bases $\{h_j\}_j$ y $\{l_k\}_k$, entonces la matriz de la composición gf, respecto a las bases $\{e_i\}_i$ y $\{l_k\}_k$, es justamente el producto YX.
Vamos ahora a determinar todas las matrices que representan a un homomorfismo $f : A^n \longrightarrow A^m$ respecto a las distintas bases de A^n y A^m.
Consideremos primero dos bases $\{e_i\}_{i=1}^n$ y $\{e_i'\}_{i=1}^n$ de A^n, si la expresión de los e_i' en función de los e_i es:

$$\begin{cases} e_1' = p_{11}e_1 + \cdots + p_{1n}e_n \\ \cdots\cdots\cdots \\ e_n' = p_{n1}e_1 + \cdots + p_{nn}e_m \end{cases}$$

Entonces la aplicación identidad de A^n en sí mismo, respecto a las bases $\{e_i'\}_i$ y $\{e_i\}_i$, está dada por la matriz $P = \begin{pmatrix} p_{11} & p_{21} & \cdots & p_{n1} \\ p_{12} & p_{22} & \cdots & p_{n2} \\ \vdots & \vdots & & \vdots \\ p_{1n} & p_{2n} & \cdots & p_{nn} \end{pmatrix}$. Por supuesto que P es una matriz invertible, se llama **matriz del cambio de base** de $\{e_i\}_i$ a $\{e_i'\}_i$. Si queremos representar la aplicación identidad de A^n, respecto a las bases $\{e_i\}_i$ y $\{e_i'\}_i$, por una matriz, obtenemos que ésta es justamente P^{-1}.

1106-07.tex

Consideremos $\{e_i\}_i$, $\{e'_i\}_i$ bases de A^n y $\{h_j\}_j$, $\{h'_j\}_j$ bases de A^m, si $X \in \mathscr{M}_{mn}(A)$ representa a f respecto a las bases $\{e_i\}_i$ y $\{h_j\}_j$, entonces el cálculo de la matriz que representa a f respecto a las bases $\{e'_i\}_i$ y $\{h'_j\}_j$ es como sigue: si P es la matriz del cambio de base de A^n de $\{e_i\}_i$ a $\{e'_i\}_i$ y Q es la matriz de cambio de base de A_m de $\{h_j\}_j$ a $\{h'_j\}_j$, entonces la matriz buscada es: $Q^{-1}XP$.



Sean $X, Y \in \mathscr{M}_{mn}(A)$, decimos que X e Y son **equivalentes** si existen matrices invertibles P y Q tales que $Q^{-1}XP = Y$. En el conjunto $\mathscr{M}_{mn}(A)$ la relación "*ser equivalentes*" es una relación de equivalencia. Todos los elementos de una clase representan al mismo homomorfismo respecto a distintas bases.

Vamos a elegir en cada clase de equivalencia de $\mathscr{M}_{mn}(A)$ un elemento que sea suficientemente sencillo. Llamamos **forma normal** de una matriz $X \in \mathscr{M}_{mn}(A)$ a una matriz $D \in \mathscr{M}_{mn}(A)$ que es equivalente a X y que verifica $d_{ij} = 0$ si $i \neq j$, y si llamamos $d_i = d_{ii}$, entonces $d_i \mid d_{i+1}$.

$$D = \begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \\ & & & & & & & \ddots \end{pmatrix}$$

Los elementos d_i se llaman **factores invariantes** de X. Llamamos **rango** de D al índice i tal que $d_i \neq 0$ y $d_{i+1} = 0$. Donde suponemos que $d_{ii} = 0$ si $i > n$ ó $i > m$. Resulta que el rango de D es justamente el rango (dimensión) de la imagen de un homomorfismo f que es representado por X ó por D, ya que ambas representan al mismo homomorfismo respecto a distintas bases.

Vamos a probar que cada matriz tiene una única forma normal.

Primero vamos a introducir elementos para la demostración de este resultado.

Sea $X \in \mathscr{M}_{mn}(A)$, una **transformación elemental (de tipo I)** de X es cambiar la fila j por el resultado de multiplicar la fila i de X por $b \in A$ y sumarla a la fila j. La matriz así obtenida resulta ser equivalente a la matriz X. Podemos comprobar que la matriz obtenida es el resultado de la siguiente

multiplicación:

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & \vdots & \ddots & \\ & & b & \cdots & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} X$$

Donde b ocupa el lugar (i,j) (columna i y fila j). Llamamos $T_{ij}(b) \in \mathscr{M}_m(A)$ a la matriz antes descrita. Es claro que se tiene $T_{ij}(b)T_{ij}(-b) = 1 = T_{ij}(-b)T_{ij}(b)$, luego la matrices X y $T_{ij}(b)X$ son equivalentes.

Otra **transformación elemental (de tipo I')** de X es hacer la multiplicación $XT_{ij}(b)$, donde ahora $T_{ij}(b) \in \mathscr{M}_n(A)$. En este caso resulta que la matriz $XT_{ij}(b)$ se obtiene de la matriz X cambiando la columna i por el resultado de sumar a la columna i la columna j multiplicada por b.

Así pues las transformaciones elementales de tipo I ó I' se pueden obtener multiplicando a la derecha por matrices invertibles (transformaciones elementales por columnas) ó a la izquierda por matrices invertibles (transformaciones elementales por filas).

Vamos a introducir otro tipo de **transformaciones elementales (de tipo II)**. Multiplicar la fila i por un elemento invertible $u \in A$, la matriz así obtenida es el producto de las matrices:

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & u & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} X$$

Donde u ocupa el lugar (i,i). Llamamos $D(u) \in \mathscr{M}_m(A)$ a la matriz antes descrita. Es claro que se tiene $D(u)D(u^{-1}) = 1 = D(u^{-1})D(u)$. Luego la matriz $D(u)X$ es equivalente a la matriz X.

Otra **transformación elemental (de tipo II')** es hacer el producto $XD(u)$, donde ahora $D(u) \in \mathscr{M}_n(A)$. En este caso resulta que la matriz $XD(u)$ se obtiene de la matriz X multiplicando la columna i por el elemento u.

Así pues las transformaciones elementales de tipo II ó II' se pueden obtener multiplicando a la derecha por matrices invertibles (transformaciones elementales por columnas) ó a la izquierda por matrices invertibles (transformaciones elementales por filas).

Vamos a introducir otro tipo de **transformaciones elementales (de tipo III)**. Permutar las filas i y

j. La matriz así obtenida puede también obtenerse como el producto de las siguientes matrices:

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 0 \cdots 1 & & \\ & & \vdots \ddots \vdots & & \\ & & 1 \cdots 0 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} X$$

Donde ahora los elementos 1 fuera de la diagonal ocupan los lugares (i,j) y (j,i). Llamamos $P_{ij} \in \mathscr{M}_m(A)$ a la matriz así definida. Es claro que $P_{ij}P_{ij} = 1$, luego P_{ij} es una matriz invertible.

Otra **transformación elemental (de tipo III')** es hacer el producto XP_{ij}, donde ahora $P_{ij} \in \mathscr{M}_n(A)$. Esta matriz se obtiene de la matriz X permutando las columnas i y j.

Así pues las transformaciones elementales de tipo III ó III' se pueden obtener multiplicando a la derecha por matrices invertibles (transformaciones elementales por columnas) ó a la izquierda por matrices invertibles (transformaciones elementales por filas).

Las matrices $T_{ij}(b)$, $D(u)$ y P_{ij} se llaman **matrices elementales**, y como se ha podido comprobar son representaciones genéricas de matrices cuadradas en los distintos $\mathscr{M}_n(A)$.

Teorema. 23.1.
Sea A un DE, para cada matriz $X \in \mathscr{M}_{mn}(A)$ existe una forma normal.

DEMOSTRACIÓN. Supongamos que la función euclídea es δ. Sea $X \in \mathscr{M}_{mn}(A)$, si $X = 0$, entonces X está en la forma normal. Si $X \neq 0$, tomamos $a_{ij} \neq 0$ con $\delta(a_{ij})$ mínimo. Haciendo transformaciones elementales de filas y columnas llevamos a_{ij} al lugar $(1,1)$. Supongamos que ésta es la situación. Estudiamos la columna 1. Para cada $k > 1$ tenemos la división euclídea $a_{1k} = a_{11}b_k + b_{1k}$ con $b_{1k} = 0$ ó $\delta(b_{1k}) < \delta(a_{11})$. Hacemos pues la siguiente transformación elemental: multiplicamos la fila 1 por b_k y la restamos a la fila k; obtenemos en la posición $(1,k)$ el elemento b_{1k}; si $b_{1k} \neq 0$, obtenemos una matriz, equivalente a la matriz X, en la que el mínimo de los δ, para los elementos no nulos, es menor que el mínimo de X. Repetimos el proceso para esta nueva matriz. Este mismo proceso podemos también hacerlo para la fila 1. Ya que el mínimo de los δ, para los elementos no nulos, es un entero no negativo, después de un número finito de repeticiones del proceso, llegamos a una matriz equivalente a A, por ejemplo $S = (b_{ij})_{ij}$, tal que $b_{11} \mid b_{1k}$, para todo $1 \leq k \leq m$, y $b_{11} \mid b_{h1}$, para todo $1 \leq h \leq n$. Haciendo ahora transformaciones elementales por filas anulamos todos los elementos de la primera columna, y haciendo transformaciones elementales por columnas anulamos todos los elementos de la primera fila (todos menos el b_{11}). Obtenemos pues una matriz

equivalente a la matriz X que tiene la forma

$$\begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{n2} \\ \vdots & \vdots & & \vdots \\ 0 & c_{2m} & \cdots & c_{nm} \end{pmatrix}$$

Podemos suponer que $b_{11} \mid c_{ij}$ para todo i, j, ya que si $b_{11} \nmid c_{ij}$, entonces sumamos la columna i a la columna 1 obteniendo la columna $b_{11}, c_{i2}, \ldots, c_{im}$. Aplicando el algoritmo de la división a b_{11} y c_{ij}, obtenemos, en la primero columna, un elemento con δ menor que el del b_{11}. En cualquier caso, después de un número finito de pasos, obtenemos una matriz como la anterior con $b_{11} \mid c_{ij}$. Aplicando ahora el mismo proceso a la submatriz $(c_{ij})_{ij}$, obtenemos una matriz equivalente a la matriz X que tiene la forma

$$\begin{pmatrix} b_{11} & 0 & 0 & \cdots & 0 \\ 0 & c_{22} & 0 & \cdots & 0 \\ 0 & 0 & d_{33} & \cdots & d_{n3} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & d_{3m} & \cdots & d_{nm} \end{pmatrix}$$

con $c_{22} \mid d_{ij}$ para todos i, j, (ya teníamos de antes que $b_{11} \mid c_{22}$). Continuando el proceso llegamos a una matriz diagonal, que es una forma normal de X. □

EL proceso de cálculo de la forma normal de una matriz es claro en el caso de DE, pero si A es un DIP, también podemos realizar, de forma teórica, este proceso, ya que esencialmente se trata de determinar el mcd de dos elementos, y éste siempre existe en el caso de un DIP.

Teorema. 23.2.
Sea A un DIP, para cada matriz $X \in \mathscr{M}_{mn}(A)$ existe una forma normal.

DEMOSTRACIÓN. En este caso no podemos utilizar la función euclídea, sin embargo, vamos a introducir un nuevo el concepto, el de longitud de un elemento no nulo $a \in A$. Llamamos $\text{long}(a)$ al número de factores primos en una factorización en primos de a, y suponemos que $\text{long}(a) = 0$ si a es invertible. Introducimos también un nuevo tipo de transformaciones elementales definidas por matrices de la forma

$$\left(\begin{array}{cc|c} x & y & \\ z & t & 0 \\ \hline 0 & & I \end{array}\right)$$

Con $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ una matriz invertible. Dada una matriz A podemos suponer que $\text{long}(a_{11}) < \text{long}(a_{ij})$ para cada elemento $a_{ij} \neq 0$. Si $a_{11} \nmid a_{1k}$, entonces intercambiamos las columnas 2 y k y obtenemos que $a_{11} \nmid a_{12}$. Llamamos $a = a_{11}$ y $b = a_{12}$; si $d = \text{mcd}\{a, b\}$, tenemos $\text{long}(d) < \text{long}(a)$ y existen x,

$y \in A$ tales que $ax + by = d$. Si llamamos $z = bd^{-1}$ y $t = -ad^{-1}$, tenemos la siguiente igualdad de matrices:

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix}\begin{pmatrix} -t & y \\ z & -x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Por lo tanto son matrices invertibles. Resulta que la primera columna de SX es $d, 0, b_{13}, \ldots, b_{1m}$ con $\text{long}(d) < \text{long}(a_{11})$.

Análogamente hacemos si $a_{11} \nmid a_{h1}$.

De esta forma, repitiendo el proceso y haciendo las transformaciones elementales necesarias, llegamos a una matriz con $a_{11} \mid a_{1k}$ y $a_{11} \mid a_{h1}$ para todos h y k. Por tanto llegamos a una matriz del tipo

$$\begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{n2} \\ \vdots & \vdots & & \vdots \\ 0 & c_{2m} & \cdots & c_{nm} \end{pmatrix}$$

Haciendo ahora un razonamiento sobre la longitud análogo al realizado sobre δ, llegamos a que $b_{11} \mid c_{ij}$ para todos i y j. Después no tenemos más que repetir el proceso las veces que sean necesarias. □

Vamos a probar ahora la unicidad de la forma normal, para ello probamos la siguiente proposición.

Proposición. 23.3.
Sea A un DIP, y $X \in \mathscr{M}_{mn}(A)$ de rango r. Si para cada $1 \leq i \leq r$ llamamos Δ_i al mcd *de los menores de orden i de A, entonces los factores invariantes de X se diferencian de los siguientes sólo en elementos invertibles.*

$$d_1 = \Delta_1,\ d_2 = \Delta_2\Delta_1^{-1},\ \ldots,\ d_r = \Delta_r\Delta_{r-1}^{-1}.$$

DEMOSTRACIÓN. Dadas dos matrices X e $Y \in \mathscr{M}_{mn}(A)$ y una matriz invertible $P \in \mathscr{M}_m(A)$ tal que $Y = PX$, tenemos que las filas de la matriz Y son combinaciones lineales de las filas de la matriz X con coeficientes en A, y por tanto los menores de orden i de Y son combinación lineal de los menores de orden i de X. Luego el mcd de los primeros es un múltiplo del mcd de los segundos. Análogamente se hace para $X = P^{-1}Y$, por lo que ambos coinciden. Este proceso podemos hacerlo también con matrices verificando $X = YQ$ e $Y = XQ^{-1}$. Consideramos ahora las matrices equivalentes X e D, resulta que

$$d_1 = \Delta_1,\ d_1d_2 = \Delta_2,\ \ldots,\ d_1d_2\cdots d_r = \Delta_r.$$

De donde se obtienen las igualdades del enunciado. □

Ejemplo. 23.4.
Obtener la forma normal de la matriz X con coeficientes en $\mathbb{Q}[x]$.

$$X = \begin{pmatrix} 2-x & 3 & 4 \\ 1 & -x & 0 \\ 2 & 0 & 1-x \end{pmatrix}.$$

SOLUCIÓN. Hacemos transformaciones elementales de filas y columnas hasta obtener la forma normal de la matriz X:

$\begin{matrix}1&0&0\\0&1&0\\0&0&1\end{matrix}$	$\begin{matrix}2-x&3&4\\1&-x&0\\2&0&1-x\end{matrix}$	
$\begin{matrix}0&1&0\\1&0&0\\0&0&1\end{matrix}$	$\begin{matrix}1&-x&0\\2-x&3&4\\2&0&1-x\end{matrix}$	
	$\begin{matrix}1&0&0\\2-x&2x-x^2+3&4\\2&2x&1-x\end{matrix}$	$\begin{matrix}1&x&0\\0&1&0\\0&0&1\end{matrix}$
$\begin{matrix}0&1&0\\1&x-2&0\\0&0&1\end{matrix}$	$\begin{matrix}1&0&0\\0&2x-x^2+3&4\\2&2x&1-x\end{matrix}$	
$\begin{matrix}0&1&0\\1&x-2&0\\0&-2&1\end{matrix}$	$\begin{matrix}1&0&0\\0&2x-x^2+3&4\\0&2x&1-x\end{matrix}$	
	$\begin{matrix}1&0&0\\0&4&2x-x^2+3\\0&1-x&2x\end{matrix}$	$\begin{matrix}1&0&x\\0&0&1\\0&1&0\end{matrix}$
$\begin{matrix}0&1&0\\1&x-2&0\\\frac{x}{4}-1/4&\frac{x^2}{4}-\frac{3x}{4}-3/2&1\end{matrix}$	$\begin{matrix}1&0&0\\0&4&2x-x^2+3\\0&0&\frac{3x^2}{4}-\frac{x^3}{4}+\frac{9x}{4}-3/4\end{matrix}$	
	$\begin{matrix}1&0&0\\0&4&0\\0&0&\frac{3x^2}{4}-\frac{x^3}{4}+\frac{9x}{4}-3/4\end{matrix}$	$\begin{matrix}1&0&x\\0&0&1\\0&1&-3/4-\frac{x}{2}+\frac{x^2}{4}\end{matrix}$
	$\begin{matrix}1&0&0\\0&1&0\\0&0&\frac{3x^2}{4}-\frac{x^3}{4}+\frac{9x}{4}-3/4\end{matrix}$	$\begin{matrix}1&0&x\\0&0&1\\0&1/4&-3/4-\frac{x}{2}+\frac{x^2}{4}\end{matrix}$
$\begin{matrix}0&1&0\\1&x-2&0\\x-1&x^2-3x-6&4\end{matrix}$	$\begin{matrix}1&0&0\\0&1&0\\0&0&3x^2-x^3+9x-3\end{matrix}$	

La matriz central se obtiene en cada paso de la siguiente forma:

$$
\begin{gathered}
X \\
P_{12}X \\
P_{12}XT_{21}(x) \\
T_{12}(x-2)P_{12}XT_{21}(x) \\
T_{13}(-2)T_{12}(x-2)P_{12}XT_{21}(x) \\
T_{13}(-2)T_{12}(x-2)P_{12}XT_{21}(x)P_{23} \\
T_{23}(1/4(x-1))T_{13}(-2)T_{12}(x-2)P_{12}XT_{21}(x)P_{23} \\
T_{23}(1/4(x-1))T_{13}(-2)T_{12}(x-2)P_{12}XT_{21}(x)P_{23}T_{32}(1/4(x^2-3-2x)) \\
T_{23}(1/4(x-1))T_{13}(-2)T_{12}(x-2)P_{12}XT_{21}(x)P_{23}T_{32}(1/4(x^2-3-2x))D_2(1/4) \\
D_3(4)T_{23}(1/4(x-1))T_{13}(-2)T_{12}(x-2)P_{12}XT_{21}(x)P_{23}T_{32}(1/4(x^2-3-2x))D_2(1/4)
\end{gathered}
$$

La forma normal del X es: $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3x^2-x^3+9x-3 \end{pmatrix}$, y existen matrices invertibles Q y P tales que $D = Q^{-1}XP$, se verifica: $Q^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & x-2 & 0 \\ x-1 & x^2-3x-6 & 4 \end{pmatrix}$ y $P = \begin{pmatrix} 1 & 0 & x \\ 0 & 0 & 1 \\ 0 & 1/4 & -3/4-\frac{x}{2}+\frac{x^2}{4} \end{pmatrix}$.

Las matrices P y Q son las matrices del cambio de base en el dominio y el codominio, respectivamente.

Si f es un $\mathbb{Q}[x]$-homomorfismo representado por X, entonces podemos calcular las bases respecto a a las cuales f está representado por la forma normal D. Para ello tenemos simplemente que calcular la inversa de Q^{-1}.

Vamos a calcular la inversa de Q^{-1} usando también transformaciones elementales.

$$
\begin{array}{c|c}
\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} & \begin{matrix} 0 & 1 & 0 \\ 1 & x-2 & 0 \\ x-1 & x^2-3x-6 & 4 \end{matrix} \\ \hline
\begin{matrix} 1 & 0 & 0 \\ 2-x & 1 & 0 \\ 0 & 0 & 1 \end{matrix} & \begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ x-1 & x^2-3x-6 & 4 \end{matrix} \\ \hline
\begin{matrix} 1 & 0 & 0 \\ 2-x & 1 & 0 \\ 3x+6-x^2 & 0 & 1 \end{matrix} & \begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ x-1 & 0 & 4 \end{matrix} \\ \hline
\begin{matrix} 1 & 0 & 0 \\ 2-x & 1 & 0 \\ 8 & 1-x & 1 \end{matrix} & \begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 4 \end{matrix} \\ \hline
\begin{matrix} 1 & 0 & 0 \\ 2-x & 1 & 0 \\ 2 & 1/4(1-x) & 1/4 \end{matrix} & \begin{matrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{matrix} \\ \hline
\begin{matrix} 2-x & 1 & 0 \\ 1 & 0 & 0 \\ 2 & 1/4(1-x) & 1/4 \end{matrix} & \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}
\end{array}
$$

Así pues la matriz Q es: $\begin{pmatrix} 2-x & 1 & 0 \\ 1 & 0 & 0 \\ 2 & 1/4(1-x) & 1/4 \end{pmatrix}$

Las bases de $\mathbb{Q}[x]^3$ respecto a las que f está representado por la forma normal D son:
Dominio:

$$\left\{e_1,\ \frac{1}{4}e_3,\ xe_1+e_2+(-\frac{3}{4}-\frac{x}{2}+\frac{x^2}{4})e_3\right\}.$$

Codominio:

$$\left\{(2-x)h_1+h_2+2h_3,\ h_1+\frac{1}{4}(1-x)h_3,\ \frac{1}{4}h_3\right\}.$$

□

Ejercicios

HACER

24. Estructura de los módulos f. g. sobre un DIP

Sea A un DIP y M un A-módulo, recordemos que el **anulador** de M es el conjunto

$$\mathrm{Ann}(M) = \{r \in A \mid \ rm = 0 \text{ para todo } m \in M\}.$$

Lema. 24.1.
$\mathrm{Ann}(M)$ *es un ideal de* A.

Lema. 24.2.
Sea M *un* A*-módulo de torsión y finitamente generado, entonces* $\mathrm{Ann}(M)$ *es un ideal de* A *no nulo.*

DEMOSTRACIÓN. Sea $y_1, \ldots, y_m$ un sistema de generadores de M, para cada índice i existe $0 \neq r_i \in A$ tal que $r_i y_i = 0$. Definimos $r = r_1 \cdots r_m$, como A es un dominio tenemos que $r \neq 0$, y por ser $y_1, \ldots, y_m$un sistema de generadores, se verifica $rx = 0$ para cada elemento $x \in M$. □

Como A es in DIP, para un A-módulo de torsion y finitamente generado M se tiene que $\mathrm{Ann}(M)$ está generado por un elemento no nulo $d \in A$. El generador d se llama el **anulador minimal** de M, y está determinado de forma única salvo asociados.

Veamos a continuación algunas definiciones y resultados técnicos.

Sea M un A-módulo, para $a \in A$ definimos $aM = \{am \in M \mid \ m \in M\}$. Existe pues un homomorfismo $f : M \longrightarrow aM$ definido por $f(m) = am$. Es claro que f es sobreyectivo y su núcleo es:

$$\mathrm{Ker}(f) = \{m \in M \mid \ am = 0\} = \mathrm{Ann}_M(a).$$

Lema. 24.3.
Sean N_1 *y* N_2 *submódulos de un* A*-módulo* M *tales que* $N_1 \cap N_2 = 0$*, entonces se verifica:*
(1) $a(N_1 \oplus N_2) = aN_1 \oplus aN_2$.
(2) $\mathrm{Ann}_{N_1 \oplus N_2}(a) = \mathrm{Ann}_{N_1}(a) \oplus \mathrm{Ann}_{N_2}(a)$.

1106-08.tex

Lema. 24.4.
Sean $d \in A$ *y* $M \cong \dfrac{A}{(d)}$. *Si* $(a,d) = 1$, *entonces* $\mathrm{Ann}_M(a) = 0$ *y* $aM = M$.

Lema. 24.5.
Sean $d \in A$ *y* $M \cong \dfrac{A}{(d)}$. *Si* $d = ab$, *entonces* $\mathrm{Ann}_M(a) \cong \frac{A}{(a)}$ *y* $aM \cong \frac{A}{(b)}$.

DEMOSTRACIÓN. Tenemos $\overline{b} \in \mathrm{Ann}_M(a)$, definimos entonces $A \xrightarrow{g} \mathrm{Ann}_M(a)$ mediante $g(1) = \overline{b}$. Se verifica $a \in \mathrm{Ker}(g)$ y si $x \in \mathrm{Ker}(g)$, entonces $0 = x\overline{b} = \overline{xb}$, luego existe $y \in A$ tal que $xb = yd = yab$, y por tanto $x = ya$, esto es, $x \in (a)$. Tenemos pues que $\mathrm{Ker}(g) = (a)$, y por tanto $\mathrm{Ann}_M(a) = \mathrm{Im}(g) \cong \dfrac{A}{\mathrm{Ker}(f)} = \dfrac{A}{(a)}$.

Por otro lado definimos $M \xrightarrow{f} aM$ mediante $f(m) = am$. Se tiene claramente que $\overline{b} \in \mathrm{Ker}(f)$. Sea ahora $\overline{x} \in \mathrm{Ker}(f)$, entonces $\overline{ax} = 0$, y existe $y \in A$ tal que $ax = dy = aby$, y por tanto $x = by$, luego $\overline{x} \in \overline{b}A = \dfrac{(b)}{(d)}$. Tenemos pues $aM = \mathrm{Im}(f) \cong \dfrac{A/(d)}{(b)/(d)} \cong \dfrac{A}{(b)}$. □

Corolario. 24.6.
Sean $a, d \in A$ *y* $M \cong \dfrac{A}{(d)}$, *entonces* $aM = eM$, *siendo* $e = \mathrm{mcd}\{a,d\}$.

Vamos ahora a estudiar la estructura de un A-módulo de torsión finitamente generado M. Supongamos que $y_1, \ldots, y_m \in M$ es un sistema de generadores de M, entonces existe un homomorfismo sobreyectivo $A^m \xrightarrow{f} M$. Sea $\mathrm{Ker}(f)$ el núcleo de f y $\mathrm{Ker}(f) \xrightarrow{g} A^m$ la inclusión. Ya que A es un DIP, resulta que $\mathrm{Ker}(f)$ es un A-módulo libre de rango $n = \mathrm{rng}(\mathrm{Ker}(f)) \leq \mathrm{rng}(A^m) = m$, existe pues un isomorfismo $A^n \cong \mathrm{Ker}(f)$. Por comodidad vamos a seguir llamando g a la composición $A^n \cong \mathrm{Ker}(f) \xrightarrow{g} A^m$. Sea $\{z_j\}_{j=1}^n$ una base de A^n y $\{e_i\}_{i=1}^m$ una base de A^m, si para cada z_j tenemos:

$$g(z_j) = a_{j1}e_1 + \cdots + a_{jm}e_m,$$

entonces la matriz de g respecto a estas bases es:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1m} & \cdots & a_{nm} \end{pmatrix}$$

Si calculamos una forma normal de A, esta forma normal también representará a g respecto otras bases. Supongamos que

$$D = \begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$$

es una forma normal de A respecto a las bases $\{z'_j\}_{j=1}^n$ y $\{e'_i\}_{i=1}^m$ de A^n y A^m respectivamente. Se tiene entonces:

$$g(z'_j) = d_j e'_j, \text{ para } 1 \leq i \leq r$$
$$g(z'_j) = 0, \quad \text{para } r+1 \leq i \leq n.$$

Y por ser g un homomorfismo inyectivo, resulta que ha de ser $n = r$.
Pasemos ahora a M, un sistema de generadores de M está formado por los elementos:

$$\{f(e'_1), \ldots, f(e'_r), f(e'_{r+1}), \ldots, f(e'_m)\}.$$

Para $r+1 \leq i \leq m$ resulta que $f(e'_i) \in M$ y por tanto es de torsión, pero si existe algún $a \in A$ tal que $af(e'_i) = 0$, entonces tenemos $f(ae'_i) = 0$, luego $ae'_i \in \mathrm{Ker}(f) = \mathrm{Im}(g)$, y existe $\sum_{j=1}^r a_j z'_j \in A^n$ tal que $g(\sum_{j=1}^r a_j z'_j) = ae'_i$, de donde se deduce que $\sum_{j=1}^r a_j d_j e'_j = ae'_i$ y como $\{e'_i\}_i$ es una base de A^m, resulta que $a = 0$. Esto implica que $f(e'_i)$ es también libre de torsión, esto es, $f(e'_i) = 0$ para $r+1 \leq i \leq m$. Se verifica pues la igualdad:

$$M = f(e'_1)A + \cdots + f(e'_r)A.$$

Vamos a ver que esta suma es directa. Sea $m \in f(e'_j)A \cap (\sum_{i \neq j} f(e'_i)A)$, entonces existen $a_1, \ldots, a_r \in A$ tales que $m = -a_j f(e'_j) = a_1 f(e'_1) + \cdots + a_{j-1} f(e'_{j-1}) + a_{j+1} f(e'_{j+1}) + \cdots + a_r f(e'_r)$, obteniendo entonces la igualdad $0 = a_1 f(e'_j) + \cdots + a_r f(e'_r)$. Siendo entonces $a_1 e'_1 + \cdots + a_r e'_r \in \mathrm{Ker}(f) = \mathrm{Im}(g)$. Existe pues $\sum_{i=1}^r b_i z'_i \in A^n$ tal que $g(\sum_{i=1}^r b_i z'_i) = a_1 e'_1 + \cdots + a_r e'_r$ y desarrollando obtenemos: $\sum_{i=1}^r b_i d_i e'_i = a_1 e'_1 + \cdots + a_r e'_r$, o equivalentemente $\sum_{i=1}^r (b_i d_i - a_i) e'_i = 0$, y como los $\{e_i\}_i$ son una base de A^m, resulta que $a_i = b_i d_i$. Es fácil ver entonces que se tiene

$$m = -a_j f(e'_j) = -b_j d_j f(e'_j) = -b_j f(d_j e_j) = -b_j f(g(z'_j)) = 0.$$

Tenemos entonces la igualdad $M = f(e'_1)A \oplus \cdots \oplus f(e'_r)A$. El siguiente paso es estudiar cada uno de los sumandos. Como ya hemos visto, se verifica $d_i f(e'_i) = 0$, para $1 \leq i \leq r$. Sea ahora $a \in A$ tal que $af(e'_i) = 0$, entonces $ae'_i \in \mathrm{Ker}(f) = \mathrm{Im}(g)$, y existe $\sum_{j=1}^r a_j z'_j \in A^n$ tal que $g(\sum_{j=1}^r a_j z'_j) = ae'_i$, de aquí obtenemos $\sum_{j=1}^r a_j d_j e'_j = ae'_i$, luego $a = a_i d_i$, y por tanto $\mathrm{Ann}(f(e'_i)) = (d_i)$, entonces tenemos un isomorfismo:

$$M \cong \frac{A}{(d_1)} \oplus \cdots \oplus \frac{A}{(d_r)}.$$

Si d_1 es invertible entonces $\frac{A}{(d_1)} = 0$, y en la descomposición anterior podemos suprimir este factor. Igual hacemos si $d_2, \ldots$ son invertibles. De forma que finalmente obtenemos una descomposición

$$M \cong \frac{A}{(d_1)} \oplus \cdots \oplus \frac{A}{(d_s)}$$

de M con los d_j no nulos, no invertibles y verificando $d_j \mid d_{j+1}$ para $1 \leq j \leq s-1$ y siendo d_s el anulador minimal de M.
Vamos a reunir el desarrollo hecho hasta ahora en el siguiente Teorema:

Teorema. 24.7.
Sea A un DIP y M un A-módulo de torsión y finitamente generado, entonces existen elementos $d_1, \ldots, d_s \in A$ no nulos, no invertibles, con $d_j \mid d_{j+1}$ para $1 \leq j \leq s-1$, d_s el anulador minimal de M y verificando:

$$M \cong \frac{A}{(d_1)} \oplus \cdots \oplus \frac{A}{(d_s)}.$$

Además una descomposición de M verificando estas condiciones es única.

Los elementos $d_1, \ldots, d_s$ se llaman los **factores invariantes** de M.

DEMOSTRACIÓN. El razonamiento previo al enunciado nos asegura la existencia de una descomposición como la anunciada en el Teorema. Vamos a probar la unicidad. Supongamos que

$$M \cong \frac{A}{(f_1)} \oplus \cdots \oplus \frac{A}{(f_t)}$$

es otra descomposición de M verificando las condiciones del enunciado, entonces por no ser d_1 un elemento invertible, existe un elemento $p \in A$ primo tal que $p \mid d_1$; como consecuencia p divide a todos los d_j y se verifica:

$$\mathrm{Ann}_M(p) \cong \mathrm{Ann}_{\frac{A}{(d_1)}}(p) \oplus \cdots \oplus \mathrm{Ann}_{\frac{A}{(d_s)}}(p) \cong \frac{A}{(p)} \oplus \cdots \oplus \frac{A}{(p)}$$

es una suma de s sumandos. Como d_s y f_t son anuladores minimales de M, resulta que $p \mid f_t$; supongamos que $p \mid f_{k+1}$ y $p \nmid f_1, \ldots, f_k$, entonces otra forma de calcular $\mathrm{Ann}_M(p)$ es la siguiente:

$$\mathrm{Ann}_M(p) \cong \mathrm{Ann}_{\frac{A}{(f_1)}}(p) \oplus \cdots \oplus \mathrm{Ann}_{\frac{A}{(f_t)}}(p) \cong \frac{A}{(p)} \oplus \cdots \oplus \frac{A}{(p)}$$

es una suma de $t-k$ sumandos. Tenemos que $\mathrm{Ann}_M(p)$ es un $A/(p)$-módulo (libre), luego $s = t-k$, y por tanto $s \geq t$. De igual modo llegamos a que $t \geq r$, luego ambos coinciden, $s = t$.
Por otro lado, tenemos que d_r y f_r son asociados por ser anuladores minimales de M. Vamos a demostrar que también lo son el resto. Supongamos que $d_j, d_{j+1}, \ldots, f_r$ y $f_j, f_{j+1}, \ldots, f_r$ son asociados dos a dos, y que d_{j-1} y f_{j-1} no lo son, sin pérdida de generalidad podemos suponer que $f_{i-1} \nmid d_{i-1}$, entonces d_{i-1} no anula a $A/(f_{i-1})$, tenemos que d_{i-1} anula a $\dfrac{A}{(d_1)} \oplus \cdots \oplus \dfrac{A}{(d_{i-1})}$, luego

$$d_{i-1}M \cong d_{i-1}\frac{A}{(d_i)} \oplus \cdots \oplus d_{i-1}\frac{A}{(d_r)} \cong d_{i-1}\frac{A}{(f_1)} \oplus \cdots \oplus d_{i-1}\frac{A}{(f_r)}.$$

Vamos a ver como es cada uno de los sumandos. Para $i \leq j \leq r$, si $d_j = d_{i-1}a_j$, se verifica:

$$d_{i-1}\frac{A}{(d_i)} \oplus \cdots \oplus d_{i-1}\frac{A}{(d_r)} \cong \frac{A}{(a_i)} \oplus \cdots \oplus \frac{A}{(a_r)}.$$

Para $1 \leq j \leq i-1$, sea $e_j = \text{mcd}\{d_{i-1}, f_j\}$, entonces $d_{i-1}\frac{A}{(f_j)} = e_j\frac{A}{(f_j)}$, y si $f_j = e_j b_j$, entonces se tiene: $e_j\frac{A}{(f_j)} \cong \frac{A}{(b_j)}$. Así pues

$$d_{i-1}M \cong \left(\frac{A}{(b_1)} \oplus \cdots \oplus \frac{A}{(b_{i-1})}\right) \oplus \left(\frac{A}{(a_i)} \oplus \cdots \oplus \frac{A}{(a_r)}\right).$$

Es claro que $b_1 \mid b_2, \ldots, b_{i-2} \mid b_{i-1}$ y $a_i \mid a_{i+1}, \ldots, a_{r-1} \mid a_r$. Vamos a probar que $b_{i-1} \mid a_i$. Tenemos las siguientes relaciones:

$$\begin{aligned} f_{i-1} &= e_{i-1}b_{i-1}, \\ f_i &= d_{i-1}a_i = f_{i-1}\beta, \\ d_{i-1} &= e_{i-1}\alpha, \end{aligned}$$

entonces resulta:

$$\begin{aligned} f_i = d_{i-1}a_i &= (e_{i-1}\alpha)a_i \\ &= f_{i-1}\beta = (e_{i-1}b_{i-1})\beta, \end{aligned}$$

de donde deducimos $\alpha a_i = b_{i-1}\beta$. Por otro lado, ya que $f_{i-1} \nmid d_{i-1}$, tenemos

$$e_{i-1}b_{i-1} \nmid e_{i-1}\alpha,$$

de donde deducimos que $b_{i-1} \nmid \alpha$, luego ha de ser $b_{i-1} \mid a_i$.
Así pues $d_{i-1}M$ tiene dos expresiones verificando las condiciones del enunciado, por lo probado anteriormente estas dos expresiones han de tener el mismo número de sumandos no nulos, y ya que $b_{i-1}\frac{A}{(b_{i-1})}$ es no nulo, llegamos a una contradicción, por lo tanto ha de ser $f_{i-1} \mid d_{i-1}$. De la misma forma llegamos a que $d_{i-1} \mid f_{i-1}$ y entonces son asociados. □

Llamamos **descomposición cíclica** de un A-módulo de torsión M a una descomposición verificando las condiciones del Teorema.

Descomposición primaria

Sea M un A-módulo y $p \in A$ un elemento primo. Un elemento $m \in M$ se llama de p-**torsión** si existe $n \in \mathbb{N}$ tal que $p^n m = 0$.

Lema. 24.8.
Sea A un DI. El subconjunto

$$T_p(M) = \{m \in M \mid m \text{ es un elemento de } p\text{-torsión}\}$$

es un submódulo de M. Este submódulo $T_p(M)$ se llama la ***componente p–primaria*** *de M.*

Lema. 24.9.
Sea A un DI, $f : M \longrightarrow N$ un homomorfismo de A-módulos y $p \in A$ un elemento primo, entonces $f(T_p(M)) \subseteq T_p(N)$.

Lema. 24.10.
Sea A un DI, $\{M_i \mid i \in I\}$ una familia de A-módulos y $p \in A$ un elemento primo, entonces se verifica: $T_p(\oplus_i M_i) = \oplus_i T_p(M_i)$.

Un A-módulo M se llama p-**primario** si $M = T_p(M)$. Además se verifica que $T_p(M)$ es el mayor submódulo p-primario de M.

Proposición. 24.11.
Sea A un DI, M un A-módulo finitamente generado y $p \in A$ un elemento primo, son equivalentes:
(a) M es p-primario.
(b) $\mathrm{Ann}(M) = (p^e)$ para algún $e \in \mathbb{N}$.

DEMOSTRACIÓN. Sea $m_1, \ldots, m_t$ un sistema de generadores de M, para cada índice $1 \leq j \leq t$ existe un entero positivo $f_j \in \mathbb{N}$ tal que $p^{f_j} m_j = 0$. Si llamamos $f = \text{máx}\{m_1, \ldots, m_t\}$, entonces $p^f \in \mathrm{Ann}(M)$. Sea $(d) = \mathrm{Ann}(M)$, ya que $p^f \in (d)$, resulta que $d \mid p^f$, luego d es una potencia de p. La otra implicación es inmediata. □

Lema. 24.12.
Sea A in DI, M un A-módulo y $N_1, \ldots, N_t$ una familia de submódulos de M tales que $M = \sum_{i=1}^t N_i$. se verifica:
(1) Si $\mathrm{Ann}(M) = (d)$ y $p \in A$ es un elemento primo verificando $(d, p) = 1$, entonces $T_p(M) = 0$.
(2) Si $\mathrm{Ann}(N_i) = (d_i)$ y $(d_i, d_j) = 1$ si $i \neq j$, entonces $M = \oplus_{i=1}^t N_i$.
(3) Si $m \in M$ y $\mathrm{Ann}(m) = (d) = (d_1 \cdots d_s)$ con $(d_i, d_j) = 1$ si $i \neq j$, entonces $m = m_1 + \cdots + m_s$ con $d_i m_i = 0$ para cada $1 \leq i \leq s$.

DEMOSTRACIÓN. (1). Tenemos que $T_p(M)$ es p-primario, luego $\mathrm{Ann}(T_p(M)) = (p^e)$, para alguna potencia de p y $(d) = \mathrm{Ann}(M) \subseteq \mathrm{Ann}(T_p(M)) = (P^e)$, implica que $p^e \mid d$, lo que es una contradicción.
(2). Podemos suponer que $n = 2$. Sea $m \in N_i \cap N_2$, existe a, $b \in A$ tales que $d_1a + d_2b = 1$, luego $m = (d_1a + d_2b)m = 0$.
(3). Podemos suponer que $s = 2$. Sea $d = d_1d_2$, existen a, $b \in A$ tales que $d_1a + d_2b = 1$, entonces

$$m = (d_1a + d_2b)m = d_1am + d_2bm,$$

y tenemos $d_2(d_1am) = 0 = d_1(d_2bm)$. □

Teorema. 24.13.
Sea A un DI, M un A-módulo de torsión y finitamente generado, entonces existen $p_1, \ldots, p_r$ elementos primos de A y submódulos p_i-primarios no nulos $N_1, \ldots, N_r$ tales que

$$M \cong N_1 \oplus \cdots \oplus N_r.$$

Además esta descomposición es única salvo isomorfismo. Los N_i son las componentes p_i-primarias de M y $T_p(M) = 0$ para cada elemento primo $p \in A$ no asociado a ningún p_i. Los elementos primos p_i son los que aparecen en la descomposición en factores primos de d el anulador minimal de M, por lo tanto son únicos salvo asociados.

DEMOSTRACIÓN. Supongamos que $\mathrm{Ann}(M) = (d) = (p_1^{e_1} \cdots p_r^{e_r})$ con los e_i enteros positivos no nulos, entonces por el Lema (24.12.) resulta que $T_p(M) = 0$ para todo elemento primo $p \in A$ no asociado a algún p_i. Sea $0 \neq m \in M$, entonces $0 \neq \mathrm{Ann}(m) = (d') = (p_1^{f_1} \cdots p_r^{f_r})$, siendo $0 \leq f_i \leq e_i$. Utilizando otra vez el Lema (24.12.), existe una descomposición de m de la siguiente forma: $m = m_1 + \cdots + m_r$, con $p_i^{f_i} m_i = 0$. Tenemos pues que $m_i \in T_{p_i}(M)$, y por tanto resulta que $M = \sum\{T_{p_i}(M) \mid 1 \leq i \leq r\}$. Utilizando nuevamente el Lema (24.12.), resulta que esta suma es directa. Supongamos que para algún índice i se verifica $T_{p_i}(M) = 0$, llamamos $d'' = d/p_i^{e_i}$, para cada $m \in M$ se verifica $d''m = 0$, luego $d'' \in \mathrm{Ann}(M) = (d)$, por tanto d y d'' son asociados, lo que implica que $e_i = 0$, y esto es una contradicción. Supongamos que tenemos otra descomposición

$$M \cong M_1 \oplus \cdots \oplus M_t,$$

verificando las condiciones del enunciado, esto es, M_j es un A-módulo q_j-primario no nulo para elementos primos $q_j \in A$. Ya que cada q_j divide a d, tenemos que q_j está asociado a algún p_i, podemos suponer que es exactamente p_i; de esta forma tenemos una inclusión entre los conjuntos

$$\{q_1, \ldots, q_t\} \subseteq \{p_1, \ldots, p_r\}.$$

Por un razonamiento análogo tenemos la otra inclusión, y por tanto la igualdad. El resto se sigue de que cada N_i es exactamente la componente p_i-primaria de M. □

Descomposición cíclica primaria

Vamos ahora a aplicar de forma simultánea las dos descomposiciones estudiadas.

Teorema. 24.14.
Sea A un DIP, M un A-módulo de torsión y finitamente generado, entonces existen $p_1, \dots, p_r$ elementos primos de A y números naturales $e_1, \dots, e_r$ tales que se verifica:
(1) $\operatorname{Ann}(M) = (d) = (p_1^{e_1} \cdots p_r^{e_r})$.
(2) $M \cong \oplus\{\oplus\{\frac{A}{(p_i^{e_{ij}})} \mid e_{i1} \leq \cdots \leq e_{ik_i}\} \mid 1 \leq i \leq r\}$.

*Además los e_{ij} están determinados unívocamente. Los elementos $p_i^{e_{ij}}$ se llaman los **divisores elementales** de M.*

DEMOSTRACIÓN. Consideramos la descomposición primaria del A-módulo M:

$$M \cong N_1 \oplus \cdots \oplus N_r,$$

siendo N_i un A-módulo p_i-primario no nulo. Ahora, para cada A-módulo N_i consideramos su descomposición cíclica:

$$N_i \cong \oplus \left\{ \frac{A}{(d_{ij})} \mid 1 \leq j \leq k_i \right\}.$$

Tenemos que $d_{ij} \mid d_{ij+1}$ para cada $1 \leq j \leq k_i - 1$. Y como se verifica que $(d_{ik_i}) = \operatorname{Ann}(N_i) = (p_i^{e_i})$, entonces existen números enteros positivos $e_{i1}, \dots, e_{ik_i}$ verificando:

$$\begin{aligned} &d_{ij} = p_i^{e_{ij}} \text{ y} \\ &e_{i1} \leq \cdots \leq e_{ik_i} = p_i^{e_i}. \end{aligned}$$

El resultado se sigue ahora de forma inmediata. □

Aplicación a los grupos abelianos

Teorema. 24.15.
Sea M un grupo abeliano finitamente generado, se verifica:
(1) Existe una descomposición, esencialmente única, del tipo

$$M \cong \mathbb{Z}^n \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r},$$

siendo n el rango de M y n_i los factores invariantes de M.

(2) Existe una descomposición, esencialmente única, del tipo

$$M \cong \mathbb{Z}^n \oplus (\oplus\{\frac{\mathbb{Z}}{(p_i^{e_{ij}})} \mid e_{i1} \leq \cdots \leq e_{ik_i}\} \mid 1 \leq i \leq r\}),$$

siendo n el rango y $p_i^{e_{ij}}$ los divisores elementales de M.

Como aplicación podemos calcular, salvo isomorfismo, todos los grupos abelianos de orden 48.

Desc. Cíclica	Desc. Cíclica Prim.	Fact. Inv.	Div. Elem.
$\mathbb{Z}_{48}$	$\mathbb{Z}_{16} \oplus \mathbb{Z}_3$	48	$16, 3$
$\mathbb{Z}_2 \oplus \mathbb{Z}_{24}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3$	$2, 24$	$2, 8, 3$
$\mathbb{Z}_4 \oplus \mathbb{Z}_{12}$	$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$	$4, 12$	$4, 4, 3$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$	$2, 2, 12$	$2, 2, 4, 3$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$	$2, 2, 2, 6$	$2, 2, 2, 2, 3$

Podemos ahora estudiar la estructura de cualquier A-módulo M generado por elementos $m_1, \ldots, m_t$ verificando las relaciones

$$\begin{aligned} &a_{11}m_1 + \cdots + a_{1t}m_t = 0 \\ &\cdots\cdots\cdots \\ &a_{n1}m_1 + \cdots + a_{nt}m_t = 0 \end{aligned}$$

En este caso consideramos un tenemos un homomorfismo sobreyectivo $f : A^t \longrightarrow M$ definido $f(l_j) = m_j$, para $1 \leq j \leq t$. El núcleo de f está generado por los elementos $\{a_{i1}l_1 + \cdots + a_{it}l_t = 0\}_{i=1}^n$. Existe pues un A-módulo libre A^n y un homomorfismo sobreyectivo $g : A^n \longrightarrow \mathrm{Ker}(f)$ que lleva una base de A^n en los elementos $a_{i1}l_1 + \cdots + a_{it}l_t$. La matriz de g es pues:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1m} & \cdots & a_{nm} \end{pmatrix}$$

Podemos obtener la forma normal de A respecto a bases $\{e_i\}_{i=1}^n$ y $\{h_j\}_{j=1}^t$. Sea

$$D = \begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$$

entonces los generadores de M son $\{f(h_j)\}_{j=1}^t$ y verifican:

$$\begin{aligned} &d_1 f(h_1) = 0 \\ &\cdots \\ &d_r f(h_r) = 0 \end{aligned}$$

¿Qué ocurre con el resto?. Esto ya depende de los valores de r, n y t. Veamos todas las posibilidades. Las dos situaciones que se pueden presentar son:

A. $r \leq n \leq t$.

En este caso la matriz D es de la forma:

$$\left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & \\ & & d_{r_{r\times r}} & \\ \hline & & & 0 \\ & & & \ddots \\ & & & 0_{n\times n} \\ \hline 0 & \cdots & \cdots & \cdots\cdots\ 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & \cdots\cdots\ 0 \end{array}\right)$$

Se verifica

$$\begin{array}{lll} d_i f(h_j) = 0 & 1 \leq j \leq r & \text{parte de torsión} \\ f(h_j) & r+1 \leq j \leq n & \text{parte libre de torsión} \\ f(h_j) & n+1 \leq j \leq t & \text{parte libre de torsión} \end{array}$$

Entonces M es isomorfo a la suma directa

$$\left(\frac{A}{(d_1)} \oplus \cdots \oplus \frac{A}{(d_r)}\right) \oplus A^{n-r} \oplus A^{t-n}$$

bf B. $r \leq t \leq n$.

En este caso la matriz D es de la forma:

$$\left(\begin{array}{ccc|ccc} d_1 & & & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ & & d_{r_{r\times r}} & \vdots & & \vdots \\ \hline & & & \vdots & & \vdots \\ & & 0 & \vdots & & \vdots \\ & & \ddots & \vdots & & \vdots \\ & & 0_{t\times t} & 0 & \cdots & 0 \end{array}\right)$$

Se verifica:

$$\begin{array}{lll} d_i f(h_j) = 0 & 1 \leq j \leq r & \text{parte de torsión} \\ f(h_j) = 0 & r+1 \leq j \leq t & \text{parte libre de torsión} \end{array}$$

Entonces M es isomorfo a la suma directa

$$\left(\frac{A}{(d_1)} \oplus \cdots \oplus \frac{A}{(d_r)}\right) \oplus A^{t-r}.$$

Es claro que las únicas relaciones que verifican ahora los generadores de M están dadas por los d_i, y que el resto de los generadores son una base de la parte libre de torsión del módulo.

Como aplicación calcular la descomposición cíclica del grupo abeliano M generado por tres elementos a, b y c verificando las relaciones: $2a = b+c = 0$. Es fácil comprobar que M es isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}$. En este caso los tres nuevos generadores $f(h_1)$, $f(h_2)$ y $f(h_3)$ verifican las relaciones:

$$\begin{array}{l} f(h_1) = 0 \\ 2f(h_2) = 0 \\ f(h_3) \text{ no verifica ninguna.} \end{array}$$

Una vez calculada la descomposición cíclica del A-módulo M, para calcular la descomposición cíclica primaria, basta calcular la descomposición primaria de cada componente cíclica, lo cual es muy sencillo. Veamos como hacerlo. Si queremos calcular la descomposición primaria de $\frac{A}{(d)}$, tenemos que calcular las componentes primarias. Para esto, lo primero es descomponer d en factores primos, supongamos que $(d) = (p_1^{e_1} \cdots p_r^{e_r})$. Llamamos $N_i = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p_{i+1}^{e_{i+1}} \cdots p_r^{e_r} \frac{A}{(d)}$, entonces N_i es la componente p_i-primaria de $\frac{A}{(d)}$.

Ejercicios

HACER

25. Formas canónicas de matrices

Sea K un cuerpo y V un espacio vectorial sobre K, si $f : V \longrightarrow V$ es un endomorfismo de V, podemos definir sobre V un estructura de $K[X]$-módulo vía el homomorfismo de anillos

$$K[X] \longrightarrow \mathrm{End}_K(V),$$

definido por $X \mapsto f$. Esto es, la imagen de un polinomio $p(X) = \sum_{i=1}^{n} a_i X^i$ es $\sum_{i=1}^{i} a_i f^i$. El $K[X]$-módulo V lo representamos por el par (V, f), ya que depende del endomorfismo f, y por simplicidad también se suele representar por M. Es necesario destacar que los elementos de M y de V son los mismos, únicamente cambia la estructura del anillo sobre el que son módulo, en el caso de M es $K[X]$ y en el de V es el cuerpo K.

El proceso anterior podemos invertirlo, esto es, si M' es un $K[X]$-módulo, podemos considerar M' como espacio vectorial sobre K definiendo km' en la forma obvia, para cada $k \in K$ y cada $m' \in M'$. Además existe un K-endomorfismo g de M' definido por $g(m') = Xm'$ para cada $m' \in M'$. Finalmente es sencillo comprobar que el $K[X]$-módulo M' se obtiene como el par (M', g) de la construcción anterior.

Vamos a estudiar los submódulos de M. Si $N \subseteq M$ es un $K[X]$-submódulo de M, entonces consideramos el espacio vectorial ${}_KN$, los elementos de ${}_KN$ son los de N y la multiplicación kn es la obvia, para $k \in K$ y $n \in N$. Resulta que ${}_KN$ es un subespacio vectorial de V. Además, para cada $n \in N$ se verifica $f(n) = Xn \in N$, luego resulta que ${}_KN$ es **estable** para f (f**–estable**).

Lema. 25.1.
Los submódulos de M corresponden con los subespacios de V que son f–estables.

El siguiente paso es estudiar los submódulos cíclicos. Sea $m \in M$, llamamos N al submódulo cíclico generado por m, esto es, $N = K[X]m$. Al calcular el espacio vectorial ${}_KN$ tenemos que los elementos $f^i(m) = X^i m$ pertenecen a N, y además cada elemento de ${}_KN$ es una combinación K-lineal de estos elementos, luego resulta que $\{f^i(m) \mid i \in \mathbb{N}\}$ es un sistema de generadores de ${}_KN$.

Lema. 25.2.
Sea $m \in M$, son equivalentes:
(a) N es el submódulo cíclico generado por m,
(b) $\{f^i(m) \mid i \in \mathbb{N}\}$ es un sistema de generadores de ${}_KN$.

1106-09.tex

Ya conocemos la equivalencia entre submódulos y submódulos cíclicos de M y subespacios de V, ahora queda estudiar los submódulos cíclicos de torsión.

Proposición. 25.3.
Sea $m \in M$, son equivalentes:

(a) $N = K[X]m$, el submódulo cíclico generado por m, es de torsión y $\mathrm{Ann}(N) = \mathrm{Ann}(m) = (p(X))$, con $p(X) = a_0 + a_1X + \cdots + a_t - 1X^{t-1} + X^t \neq 0$,

(b) $\{m, f(m), \ldots, f^{t-1}(m)\}$ es una base de ${}_KN$ y la matriz de $f_{|_KN}$ es:

$$M_{p(X)} = \begin{pmatrix} 0 & 0 \cdots 0 & -a_0 \\ 1 & 0 \cdots 0 & -a_1 \\ \vdots & \ddots \ddots & \vdots \\ 0 & 0 \cdots 1 & -a_{t-1} \end{pmatrix}$$

La matriz $M_{p(X)}$ se llama **matriz asociada** a $p(X)$. Y el subespacio ${}_KN$ se llama un subespacio f-cíclico. Cuando $V =_K N$, entonces f se llama un **endomorfismo cíclico**.

Tenemos así una correspondencia biunívoca entre submódulos cíclicos y de torsión de M y subespacios f-cíclicos de V.

Proposición. 25.4.
Son equivalentes:

(a) M es un $K[X]$-módulo finitamente generado y de torsión,

(b) V es un espacio vectorial de dimensión finita.

DEMOSTRACIÓN. Si $\{m_1, \ldots, m_r\}$ es un sistema de generadores de M, entonces $\{f^j(m_i) \mid 0 \leq j \leq t_i - 1,\ 1 \leq i \leq r\}$ es un sistema finito de generadores de V. La otra inclusión es inmediata, ya que una base de V es un sistema de generadores de M. □

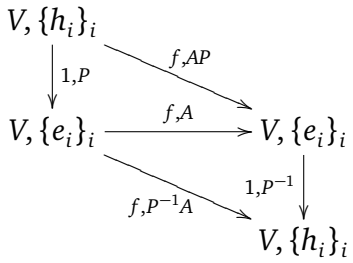
Como consecuencia, si queremos estudiar endomorfismos de un espacio vectorial de dimensión finita, pasando a los $K[X]$-módulos correspondientes obtenemos módulos finitamente generados y de torsión, luego podemos aplicar los teoremas de estructura de módulo finitamente generados de torsión sobre un DIP. Se trata ahora de traducir los resultados que se deducen de la descomposición cíclica, de la primaria y de la cíclica primaria.

Veamos previamente alguna notación útil en lo que sigue.

Sea V un espacio vectorial de dimensión finita sobre el cuerpo K, y sea $f : V \longrightarrow V$ un endomorfismo de V, si $\{e_1, \ldots, e_n\}$ es una base de V, entonces f se puede representar por una matriz

$$\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}$$

Donde $f(e_i) = \sum_{j=1}^{n} a_{ij} e_j$. Si cambiamos de base, de la base $\{e_i\}_i$ a la base $\{h_i\}_i$, y la matriz del cambio de base es P, entonces resulta que la matriz de f referida a la nueva base $\{h_i\}_i$ es exactamente $P^{-1}AP$, como muestra el siguiente gráfico.



Dos matrices A y B tales que existe una matriz invertible P verificando $B = P^{-1}AP$ se llaman **semejantes**.

Sea V un espacio vectorial de dimensión finita con base $\{e_i\}_{i=1}^n$ y sea f un endomorfismo de V con matriz A respecto a la base $\{e_i\}_i$. Consideramos el $K[X]$-módulo asociado M (que es finitamente generado y torsión) y calculamos una descomposición cíclica de M:

$$M \cong \frac{K[X]}{(p_1(X))} \oplus \cdots \oplus \frac{K[X]}{(p_s(X))},$$

con $p_i(X) \mid p_{i+1}(X)$ $(1 \leq i \leq s-1)$ y $p_i(X)$ no nulo y no invertible $(1 \leq i \leq s)$. Ya que cada cociente $\frac{K[X]}{(p_i(X))}$ es un módulo cíclico, podemos suponer que $\frac{K[X]}{(p_i(X))} = K[X]m_i$ para algún $m_i \in M$, entonces tenemos:

$$M \cong K[X]m_1 \oplus \cdots \oplus K[X]m_s,$$

con $\mathrm{Ann}(m_i) = (p_i(X))$ $(1 \leq i \leq s)$. Sea $p_i(X) = a_{i0} + a_{i1}X + \cdots + a_{it_i-1}X^{t_i-1} + X^{t_i}$, entonces

$$\{m_i, f(m_i), \ldots, f^{t_i-1}(m_i)\} = \{f^j(m_i) \mid 0 \leq j \leq t_i - 1\}$$

es una base de ${}_K(K[X]m_i)$, y como consecuencia

$$\{\{f^j(m_i) \mid 0 \leq j \leq t_i - 1\} : 1 \leq i \leq s\}$$

es una base de V. Si calculamos ahora la matriz de f respecto a esta base, resulta que es del tipo:

$$A' = \left(\begin{array}{c|c|c} M_{p_1(X)} & & \\ \hline & \ddots & \\ \hline & & M_{p_s(X)} \end{array}\right) = M_{p_1(X)} \oplus \cdots \oplus M_{p_s(X)}.$$

La matriz A' se llama la **forma canónica racional** del endomorfismo f, y si A es una matriz que representa a f respecto a una base de V, entonces A y A' son matrices semejantes. La matriz A' se llama también forma canónica racional de la matriz A. Los polinomios $p_i(X)$ se llaman **factores invariantes** de f ó de A. La matriz A' es además la única para la cual los polinomios mónicos $p_1((X), \ldots, p_s(X)$ verifican $p_i(X) \mid p_{i+1}(X)$, son no nulos y no invertibles.
Como consecuencia podemos enunciar:

Corolario. 25.5.
Dos matrices son semejantes si, y sólo si, tienen los mismos factores invariantes.

Lema. 25.6.
Se tiene que $p_s(X)$ es el anulador minimal de M, resulta que $p_s(f) = 0$ ó equivalentemente $p_s(A) = 0$. Y para cada $p(X) \in K[X]$ tal que $p(f) = 0$, se tiene $p_s(X) \mid p(X)$.

DEMOSTRACIÓN. Para $v \in V$ tenemos $p_s(f)(v) = p_s(X)v = 0$ ya que $p_s(X)$ es el anulador minimal de M, luego tenemos el resultado. Además si $p(X) \in K[X]$ verifica $p(f) = 0$, entonces para cada $v \in V$ se tiene $0 = p(f)(v) = p(X)v$, luego $p_s(X) \mid p(X)$. □

El polinomio $p_s(X)$ se llama en **polinomio mínimo** de f ó de A.
Veamos algunos resultados que se deducen fácilmente de los anteriores.

Lema. 25.7.
El espacio vectorial V es f-cíclico si, y sólo si, el grado del polinomio mínimo es igual a la dimensión de V.

Lema. 25.8.
Sea $p(X) \in K[X]$ un polinomio mónico no constante. El polinomio mínimo de $M_{p(X)}$ es $p(X)$, y por tanto es su único factor invariante.

Lema. 25.9.
La suma de los grados de los factores invariantes es igual a la dimensión de V.

Corolario. 25.10.
V es f-cíclico si, y sólo si, tiene un único factor invariante.

Vamos ahora a calcular los factores invariantes de un endomorfismo f ó equivalentemente de una representación matricial suya A. Supongamos que $\{m_1,\dots,m_n\}$ es una base de V y que la matriz de f respecto a esta base es A, entonces tomamos un $K[X]$-módulo libre de rango n y un homomorfismo sobreyectivo $\alpha : K[X]^n \longrightarrow M$ definido $\alpha(e_i) = m_i$, siendo $\{e_i\}_i$ una base de $K[X]^n$. Consideramos el núcleo de α y el homomorfismo inclusión $\beta : \mathrm{Ker}(\alpha) \longrightarrow K[X]^n$. Ya conocemos que $\mathrm{Ker}(\alpha)$ es un $K[X]$-módulo libre de rango menor ó igual que n. Vamos a probar que el rango de $\mathrm{Ker}(\alpha)$ es exactamente n y vamos a calcular una base de $\mathrm{Ker}(\alpha)$.

Proposición. 25.11.
Para cada índice i definimos $h_i = Xe_i - \sum_{j=1}^n a_{ij}e_j$, entonces $\{h_1,\dots,h_n\}$ es una base de $\mathrm{Ker}(\alpha)$.

Si consideramos en $\mathrm{Ker}(\alpha)$ la base $\{h_i\}_i$ y en $K[X]^n$ la base $\{e_i\}_i$, entonces la matriz de β es:

$$XI - A = \begin{pmatrix} X-a_{11} & -a_{21} & \cdots & -a_{n1} \\ -a_{12} & X-a_{22} & \cdots & -a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{1n} & -a_{2n} & \cdots & X-a_{nn} \end{pmatrix}$$

Al calcular la forma normal de la matriz $XI - A$ obtenemos una matriz del tipo

$$D = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & p_1(X) & \\ & & & & \ddots \\ & & & & & p_s(X) \end{pmatrix}$$

con los polinomios $p_1(X),\dots,p_s(X)$ no constantes en $K[X]$. Además, según sabemos, los $p_1(X)$, …, $p_s(X)$ son los factores invariantes de f y $p_s(X)$ es el polinomio mínimo de f.
El determinante de $XI-A$ se llama el **polinomio característico** de la matriz A. Vamos a ver que este es un invariante de f.

Lema. 25.12.
Sean $A, B \in \mathscr{M}_n(K)$ dos matrices cuadradas, son equivalentes:
(a) A y B son matrices semejantes,
(b) $XI-A$ y $XI-B$ son matrices equivalentes.

Además en este caso se tiene $|XI-A| = |XI-B|$.

Como consecuencia de los resultados previos tenemos:
(1) $|XI-A|$ es el producto de los factores invariantes de la matriz A,
(2) $p_s(X)$ divide a $|XI-A|$ y $|XI-A|$ divide a $(p_s(X))^s$.
(3) Toda matriz $A \in \mathscr{M}_n(K)$ es raíz de su polinomio característico (Teorema de Hamilton–Cayley).
(4) $p_s(X)$ y $|XI-A|$ tienen el mismo conjunto de factores invariantes.
(5) $p_s(X) = \frac{|XI-A|}{\Delta_{n-1}}$, donde Δ_{n-1} es el mcd de los menores de orden $n-1$ de la matriz $XI-A$.

Finalmente queda calcular las base de V respecto a las cuales se adopta la forma racional A'. Sabemos que existen matrices invertibles P y Q verificando $D = Q^{-1}AP$, entonces las matrices P y Q dan los cambios de base en $\mathrm{Ker}(\alpha)$ y $K[X]^n$, respectivamente. Sea $\{e'_i\}_i$ la nueva base de $K[X]^n$, entonces la base inducida en V es:

$$\mathscr{B}' = \{f^j(\alpha(e'_i)) \mid 0 \le j \le t_i - 1,\ 1 \le i \le n\} \setminus \{0\}.$$

Vamos a aplicarlo a un ejemplo. Consideramos el endomorfismo de $f : \mathbb{Q}^3 \longrightarrow \mathbb{Q}^3$ definido respecto a una base de $\mathbb{Q}^3$ por la matriz:

$$A = \begin{pmatrix} 2 & 3 & 4 \\ 1 & 0 & 0 \\ 2 & 0 & 1 \end{pmatrix}.$$

La matriz $XI-A$ es:

$$XI-A = \begin{pmatrix} X-2 & -3 & -4 \\ -1 & -X & 0 \\ -2 & 0 & X-1 \end{pmatrix}.$$

Al calcular la forma normal tenemos:

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & X^3-3X^2-9X+3 \end{pmatrix} = Q^{-1}AP,$$

donde las matrices P y Q son las matrices del cambio de base, la única que nos interesa es la matriz Q que lleva la información del cambio de base en $\mathbb{Q}^3$. Como se verifica

$$Q^{-1} = \begin{pmatrix} 0 & 1\,0 \\ 1 & X-2\,0 \\ X-1 & X^2-3X-6\,4 \end{pmatrix},$$

entonces tenemos

$$Q = \begin{pmatrix} 2-X & 1 & 0 \\ 1 & 0 & 0 \\ 2 & 1/4(1-X) & 1/4 \end{pmatrix}.$$

La base de $\mathbb{Q}^3$ es: $\{(2-X)e_1 + e_2 + 2e_3, e_1 + 1/4(1-X)e_3, 1/4e_3\}$, entonces la base de V respecto a la que se adopta la forma canónica racional es:

$$\{f^0(1/4e_3), f^1(1/4e_3), f^2(1/4e_3)\} = \{(0,0,1/4),(1,0,1/4),(3,1,9/4)\}.$$

Y la forma canónica racional es:

$$\begin{pmatrix} 0\,0 & -3 \\ 1\,0 & 9 \\ 0\,1 & 3 \end{pmatrix}$$

Para comprobarlo simplemente basta ver que se verifica

$$\begin{pmatrix} 2\,3\,4 \\ 1\,0\,0 \\ 2\,0\,1 \end{pmatrix}\begin{pmatrix} 3 \\ 1 \\ 9/4 \end{pmatrix} = -3\begin{pmatrix} 0 \\ 0 \\ 1/4 \end{pmatrix} + 9\begin{pmatrix} 1 \\ 0 \\ 1/4 \end{pmatrix} + 3\begin{pmatrix} 3 \\ 1 \\ 9/4 \end{pmatrix}.$$

Ya que el único factor invariante coincide con el polinomio minimal, resulta que V es f-cíclico.

Si en vez de aplicar el teorema de descomposición cíclica aplicamos el teorema de descomposición cíclica primaria, entonces obtenemos una nueva matriz semejante a la de partida, y a la que vamos a llamar **forma canónica de Weierstrass** de la matriz A ó del endomorfismo f.

Consideramos la descomposición cíclica primaria de M obtenida a partir de la descomposición cíclica

$$M \cong \frac{K[X]}{(p_1(X))} \oplus \cdots \oplus \frac{K[X]}{(p_s(X))},$$

con $p_i(X) \mid p_{i+1}(X)$ $(1 \leq i \leq s-1)$ y $p_i(X)$ no nulo y invertible $(1 \leq i \leq s)$. Ya que cada cociente $\frac{K[X]}{(p_i(X))}$ es un módulo cíclico, podemos suponer que $\frac{K[X]}{(p_i(X))} = K[X]m_i$ para algún $m_i \in M$, entonces tenemos:

$$M \cong K[X]m_1 \oplus \cdots \oplus K[X]m_s,$$

con $\mathrm{Ann}(m_i) = (p_i(X))$ $(1 \leq i \leq s)$. Consideremos uno de los sumandos y sea $p_i(X) = q_1^{e_{i1}} \cdots q_r^{e_{ir}}$, donde los q_j son polinomios irreducibles y los e_{ij} son los exponentes que pueden tomar valores positivos ó nulos. Como consecuencia de la definición de los factores invariantes, se tiene que $e_{1j} \leq$

$e_{2j} \leq \cdots \leq e_{sr}$. La descomposición cíclica primaria se obtiene de la siguiente forma: si llamamos $p_{ij} = p_i(X)/q_j^{e_{ij}}$ y $m_{ij} = p_{ij}m_i$, entonces tenemos:

$$M \cong K[X]m_1 \oplus \cdots \oplus K[X]m_s \cong$$

$$(K[X]m_{11} \oplus \cdots \oplus K[X]m_{1r}) \oplus \cdots \oplus (K[X]m_{s1} \oplus \cdots \oplus K[X]m_{sr}).$$

Eliminamos aquellos sumandos que son nulos, y tenemos una descomposición de M como una suma de $K[X]$-módulos cíclicos primarios.

La forma de conseguir ahora una base de V como espacio vectorial sobre K es una imitación de la hecha en la obtención de la forma canónica racional, esto es, una base es:

$$\mathscr{B}'' = \{f^k(m_{ij}) \mid 1 \leq i \leq s,\ 1 \leq j \leq r,\ 0 \leq k < gr(q_j^{e_{ij}})\}$$

En este conjunto no existen elementos nulos, ya que si $m_{ij} = 0$, entonces $q_j^{e_{ij}} = 1$, y por tanto en este caso k no está definido.

Respecto a la base $\mathscr{B}''$ el endomorfismo f tiene por matriz

$$A'' = \begin{pmatrix} M_{11} & & & \\ & M_{12} & & \\ & & \ddots & \\ & & & M_{sr} \end{pmatrix}$$

a la que se llama **forma canónica de Weierstrass** de f ó de A. En la matriz A'' la matriz M_{ij} es la asociada al polinomio $q_j^{e_{ij}}$. Los polinomios $q_j^{e_{ij}}$ se llaman **divisores elementales** de f ó A.

Vamos a hacer una lista de los resultados que se deducen de este desarrollo:

(1) Dos matrices son semejantes si, y sólo si, tiene los mismos divisores elementales.
(2) Si $p = q_1^{e_1} \cdots q_r^{e_r}$, con los $q_j \in K[X]$ irreducibles y distintos dos a dos, entonces los divisores elementales de M_p son los $q_1^{e_1}, \ldots, q_r^{e_r}$.
(3) Si $p \in K[X]$ es irreducible, entonces M_{p^e} tiene un único divisor elemental.
(4) Si conocemos los factores invariantes de un matriz conocemos también los divisores elementales y viceversa.

El método de calcular base de V respecto a la cual se adopta la forma canónica de Weierstrass (fcW) se hace a partir de lo ya realizado en el cálculo de la forma canónica racional. Si $\{e_i'\}_i$ es la nueva base de $K[X]^n$, entonces la base de V respecto a la cual se adopta la fcW es

$$\mathscr{B}'' = \{f^k(\alpha(p_{ij}e_i)) \mid 1 \leq i \leq s-1,\ 1 \leq j \leq r,\ 1 \leq k < gr(p_j^{e_{ij}})\} \setminus \{0\}.$$

En la forma canónica de Weierstrass, a cada divisor elemental le hacemos corresponder su matriz asociada, con lo cual complicamos sobre manera el cálculo de estas matrices, vamos a buscar un nuevo método de asociar otra matriz de forma que no sea necesario calcular explícitamente el divisor elemental. Para ello vamos a introducir la **forma canónica de Jacobson**.

Supongamos que tenemos un divisor elemental de la forma q^e, donde $q = b_0 + b_1X + \cdots + b_{t-1}X^{t-1} + X^t \in K[X]$ es irreducible y $0 \neq e \in \mathbb{N}$. Resulta que $K[X]/(q^e)$ es isomorfo a un submódulo de M,

luego existe un elemento $m \in M$ tal que $K[X]/(q^e) \cong K[X]m$, este submódulo cíclico determina un subespacio f-estable W de V de dimensión et con una base formada por los elementos

$$\{f^i(m) \mid 0 \leq i \leq et-1\}.$$

La matriz de f respecto a esta base es la matriz asociada a f. Vamos a cambiar la base de W para obtener una matriz más sencilla. Consideramos el conjunto $\mathscr{B}'''$

$$\begin{array}{l} v_0 = m,\ v_1 = f(m),\ \ldots,\ v_{t-1} = f^{t-1}(m), \\ v_t = q(f)(m),\ v_{t+1} = f(q(f)(m)),\ \ldots,\ v_{2t-1} = f^{t-1}(q(f)(m)), \\ \cdots\cdots\cdots \end{array}$$

En general se tiene $v_{\epsilon t+r} = f^r(q^\epsilon(f)(m))$, para $0 \leq \epsilon \leq e$ y $0 \leq r < t$.

Lema. 25.13.
El conjunto $\mathscr{B}''' = \{v_j \mid 0 \leq j \leq et-1\}$ *es una base de* W.

DEMOSTRACIÓN. Ya que $\mathscr{B}'''$ tiene et elementos, basta probar que es un sistema de generadores, y para esto consideramos $v_r = q(f)(m) = b_0 m + b_1 f(m) + \cdots + b_{t-1} f^{t-1}(m) + f^t(m)$, luego $\{m, f(m), \ldots, f^t(m)\}$ y $\{v_0, v_1, \ldots, v_t\}$ generan el mismo subespacio. El resto es inmediato. □

Vamos a calcular la matriz que representa a f respecto a la base $\mathscr{B}'''$. Se verifica:

$$\begin{array}{l} f(v_0) = v_1, \\ \cdots \\ f(v_{t-1}) = -b_0 v_0 + b_1 v_1 + \cdots + b_{t-1} v_{t-1} + v_t, \\ f(v_t) = v_{t+1}, \\ \cdots \end{array}$$

En general se tiene:

$$\begin{array}{ll} f(v_{\epsilon t+r}) = v_{\epsilon t+r+1}, & \text{si } 0 \leq r < t-1, \\ f(v_{\epsilon t+r-1}) = -b_0 v_{\epsilon t} - \cdots - b_{t-1} v_{\epsilon t+t-1} + v_{(\epsilon+1)t}, & \end{array}$$

Así pues la matriz es:

$$J_{q^e} = \left(\begin{array}{c|c|c|c|c|c} M_q & & & & & \\ \hline N & M_q & & & & \\ \hline & N & \ddots & & & \\ \hline & & & \ddots & & \\ \hline & & & & M_q & \\ \hline & & & & N & M_q \end{array}\right)$$

Donde M_q es la matriz asociada a q y N es la matriz $t \times t$ con cero en todos los lugares menos en $(t,1)$ que tiene un uno.
La matriz J_q se llama el **bloque de Jacobson** de q^e. Cuando $t = 1$, el bloque de Jacobson se llama **bloque de Jordan**, y en este caso tenemos si $q = X - a$, entonces:

$$J_{q^e} = \begin{pmatrix} a & 0 & 0 & \cdots & 0 & 0 \\ 1 & a & 0 & \cdots & 0 & 0 \\ 0 & 1 & a & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a & 0 \\ 0 & 0 & 0 & \cdots & 1 & a \end{pmatrix}$$

En cualquier caso el único factor invariante y el único divisor elemental es q^e.
Ya que no todos los polinomios irreducibles son de grado uno, resulta que no todas las matrices tienen forma canónica de Jordan, esto ocurre si $K = \mathbb{Q}$ ó $\mathbb{R}$. En cambio, si K es un cuerpo algebraicamente cerrado, por ejemplo $\mathbb{C}$, entonces toda matriz tiene una forma canónica de Jordan.

Ejemplo. 25.14.
Considerar el endomorfismo $f : \mathbb{Q}^4 \longrightarrow \mathbb{Q}^4$ definido

$$\begin{aligned} f(m_1) &= 3m_1 + m_2 \\ f(m_2) &= -4m_1 - m_2 \\ f(m_3) &= 6m_1 + m_2 + 2m_3 + m_4 \\ f(m_4) &= -14m_1 - 5m_2 - m_3 \end{aligned}$$

Calcular las formas canónicas de f y las bases respecto a las cuales las adopta.

La matriz de f respecto a la base $\{m_1, m_2, m_3, m_4\}$ es:

$$A = \begin{pmatrix} 3 & 1 & 0 & 0 \\ -4 & -1 & 0 & 0 \\ 6 & 1 & 2 & 1 \\ -14 & -5 & -1 & 0 \end{pmatrix}$$

Consideramos la matriz de las relaciones $XI - A$, y calculamos su forma normal D, en este caso

$$D = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & X^2 - 2X + 1 & \\ & & & X^2 - 2X + 1 \end{pmatrix}$$

Las matrices de cambio son

$$Q^{-1} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & X - 3 & 1 - 5X & 0 \\ 0 & 0 & X & 1 \end{pmatrix}$$

y

$$P=\begin{pmatrix}1 & 5X+1 & 1 & 4\\ 0 & 0 & 1 & 5\\ 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 2-X\end{pmatrix}$$

y verifican $D=Q^{-1}AP$. La inversa de Q^{-1} es:

$$Q=\begin{pmatrix}X-3 & 5X-1 & 1 & 0\\ -1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & X & 0 & 1\end{pmatrix}$$

La nueva base de $\mathbb{Q}[X]^4$ es:

$$\begin{aligned}e_1' &= (X-3)e_1 - e_2,\\ e_2' &= (5X-1)e_1 + e_3 + Xe_4,\\ e_3' &= e_1,\\ e_4' &= e_4.\end{aligned}$$

Y la base de $V=\mathbb{Q}^4$ respecto a la cual f tiene la forma canónica racional es $\mathbb{B}'=\{n_1,n_2,n_3,n_4\}$:

$$\begin{aligned}n_1 &= \alpha(e_3') = m_1,\\ n_2 &= f(\alpha(e_3')) = 3m_1 + m_2,\\ n_3 &= \alpha(e_4') = m_4,\\ n_4 &= f(\alpha(e_4')) = -14m_1 - 5m_2 - m_3,\end{aligned}$$

Y la forma canónica racional es:

$$A'=\left(\begin{array}{cc|cc}0 & -1 & & \\ 1 & 2 & & \\ \hline & & 0 & -1\\ & & 1 & 2\end{array}\right)$$

La matriz del cambio de base es: $T=\begin{pmatrix}1 & 3 & 0 & -14\\ 0 & 1 & 0 & -5\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$ y su inversa es: $T^{-1}=\begin{pmatrix}1 & -3 & 1 & 0\\ 0 & 1 & -5 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\end{pmatrix}$ y se verifica:

$A'=T^{-1}AT$.

Ya que los factores invariantes coinciden con los divisores elementales, entonces la forma canónica de Weierstrass coincide con la racional.

Los divisores elementales son: $(X-1)^2$ y $(X-1)^2$, entonces el bloque da Jacobson coincide con el de Jordan, y la forma canónica de Jacobson ó de Jordan es:

$$A'''=\left(\begin{array}{cc|cc}1 & 0 & & \\ 1 & 1 & & \\ \hline & & 1 & \\ & & 1 & 1\end{array}\right)$$

La base de V respecto a la cual se adopta esta forma canónica es justamente $\mathbb{B}''' = \{n_1''', n_2''', n_3''', n_4'''\}$ definida por:

$$\begin{aligned}
n_1''' &= m_1 \\
n_1''' &= (f-1)(m_1) = 2m_1 + m_2, \\
n_1''' &= m_4 \\
n_1''' &= (f-1)(m_4) = -14m_1 - 5m_2 - m_3 - m_4.
\end{aligned}$$

Ejercicio. 25.15.
Calcular las formas canónicas, y las bases respecto a las cuales las adoptan, del endomorfismo $f : \mathbb{Q}^4 \longrightarrow \mathbb{Q}^4$ definido, respecto a una base canónica, por la matriz

$$A = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 4 & 2 & 3 & 0 \\ -6 & -2 & -3 & -2 \\ -3 & -1 & -1 & -2 \end{pmatrix}$$

SOLUCIÓN. Calculamos la forma normal de la matriz $XI - A$ haciendo transformaciones elementales.

$$
\begin{array}{|r|l|l|}
\hline
 & \begin{matrix} X-2 & -1 & -1 & -1 \\ -4X-2 & -3 & 0 \\ 6 & 2X+3 & 2 \\ 3 & 1 & 1X+2 \end{matrix} & \\
\hline
 & \begin{matrix} -1 & -1 & -1X-2 \\ 0X-2 & -3 & -4 \\ 2 & 2X+3 & 6 \\ X+2 & 1 & 1 & 3 \end{matrix} & \begin{matrix} 0001 \\ 0100 \\ 0010 \\ 1000 \end{matrix} \\
\hline
\begin{matrix} 1000 \\ 0100 \\ 2010 \\ 0001 \end{matrix} & \begin{matrix} -1 & -1 & -1 & X-2 \\ 0X-2 & -3 & -4 \\ 0 & 0X+1 & 2X+2 \\ X+2 & 1 & 1 & 3 \end{matrix} & \\
\hline
\begin{matrix} 1000 \\ 0100 \\ 2010 \\ X+2001 \end{matrix} & \begin{matrix} -1 & -1 & -1 & X-2 \\ 0 & X-2 & -3 & -4 \\ 0 & 0 & X+1 & 2X+2 \\ 0 & -X-1 & -X-1 & X^2-1 \end{matrix} & \\
\hline
\end{array}
$$

$$\left(\begin{array}{cccc} -1 & 0 & -1 & X-2 \\ 0 & X-2 & -3 & -4 \\ 0 & 0 & X+1 & 2X+2 \\ 0 & -X-1 & -X-1 & X^2-1 \end{array}\right) \quad \left(\begin{array}{cccc} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 0 \end{array}\right)$$

$$\left(\begin{array}{cccc} -1 & 0 & 0 & X-2 \\ 0 & X-2 & -3 & -4 \\ 0 & 0 & X+1 & 2X+2 \\ 0 & -X-1 & -X-1 & X^2-1 \end{array}\right) \quad \left(\begin{array}{cccc} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & -1 & 0 \end{array}\right)$$

$$\left(\begin{array}{cccc} -1 & 0 & 0 & 0 \\ 0 & X-2 & -3 & -4 \\ 0 & 0 & X+1 & 2X+2 \\ 0 & -X-1 & -X-1 & X^2-1 \end{array}\right) \quad \left(\begin{array}{cccc} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & -1 & X-2 \end{array}\right)$$

$$\left(\begin{array}{cccc} -1 & 0 & 0 & 0 \\ 0 & X-2 & 1 & -4 \\ 0 & 0 & -X-1 & 2X+2 \\ 0 & -X-1 & -X^2-X & X^2-1 \end{array}\right) \quad \left(\begin{array}{cccc} 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & -X+1 & X-2 \end{array}\right)$$

$$\left(\begin{array}{cccc} -1 & 0 & 0 & 0 \\ 0 & 1 & X-2 & -4 \\ 0 & -X-1 & 0 & 2X+2 \\ 0 & -X^2-X & -X-1 & X^2-1 \end{array}\right) \quad \left(\begin{array}{cccc} 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -X+1 & -1 & X-2 \end{array}\right)$$

$$\left(\begin{array}{cccc} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -4 \\ 0 & -X-1 & X^2-X-2 & 2X+2 \\ 0 & -X^2-X & X^3-X^2-3X-1 & X^2-1 \end{array}\right) \quad \left(\begin{array}{cccc} 0 & -1 & X-2 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 2-X & 0 \\ 1 & -X+1 & X^2-3X+1 & X-2 \end{array}\right)$$

$$\left(\begin{array}{cccc} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -X-1 & X^2-X-2 & -2X-2 \\ 0 & -X^2-X & X^3-X^2-3X-1 & -3X^2-4X-1 \end{array}\right) \quad \left(\begin{array}{cccc} 0 & -1 & X-2 & -3 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 2-X & 4 \\ 1 & -X+1 & X^2-3X+1 & -3X+2 \end{array}\right)$$

$$\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2X+1 & 1 & 0 & 0 \\ X+2 & 0 & 0 & 1 \end{array}\right) \quad \left(\begin{array}{cccc} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X^2-X-2 & -2X-2 \\ 0 & -X^2-X & X^3-X^2-3X-1 & -3X^2-4X-1 \end{array}\right)$$

$$\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & X+1 & 1 & 0 \\ X+2 & X^2+X & 0 & 1 \end{array}\right) \quad \left(\begin{array}{cccc} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X^2-X-2 & -2X-2 \\ 0 & 0 & X^3-X^2-3X-1 & -3X^2-4X-1 \end{array}\right)$$

$$\left(\begin{array}{cccc|cccc}
-1 & 0 & 0 & 0 & 0 & -1 & -\frac{1}{2}(X+1) & -3 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & -X-1 & -2X-2 & 0 & 1 & X & 4 \\
0 & 0 & \frac{1}{2}(-X^3-3X^2-3X-1) & -3X^2-4X-1 & 1 & -X+1 & -\frac{1}{2}(X^2+X) & -3X+2
\end{array}\right)$$

$$\left(\begin{array}{cccc|cccc}
-1 & 0 & 0 & 0 & 0 & -1 & -\frac{1}{2}(X+1) & X-2 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & -2 \\
0 & 0 & -X-1 & 0 & 0 & 1 & X & -2X+4 \\
0 & 0 & \frac{1}{2}(-X^3-3X^2-3X-1) & X^3-X & 1 & -X+1 & -\frac{1}{2}(X^2+X) & X^2-2X+2
\end{array}\right)$$

$$\left(\begin{array}{cccc|cccc}
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
2 & X+1 & 1 & 0 & 0 & 0 & -X-1 & 0 \\
-X^2-X+1 & \frac{1}{2}(-X^3-X^2-X-1) & -\frac{1}{2}(X^2+2X+1) & 1 & 0 & 0 & 0 & X^3-X
\end{array}\right)$$

$$\left(\begin{array}{cccc|cccc}
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
2 & X+1 & 1 & 0 & 0 & 0 & -X-1 & 0 \\
2X^2+2X+2 & X^3+X^2+X+1 & X^2+2X+1 & -2 & 0 & 0 & 0 & -2X^3+2X
\end{array}\right)$$

$$\left(\begin{array}{cccc|cccc}
1 & 0 & 0 & 0 & 0 & -1 & \frac{1}{2}(X+1) & -\frac{1}{2}(X-2) \\
0 & 1 & 0 & 0 & 0 & 0 & -1 & 1 \\
0 & 0 & X+1 & 0 & 0 & 1 & -X & X-2 \\
0 & 0 & 0 & X^3-X & -1 & -X+1 & \frac{1}{2}(X^2+X) & -\frac{1}{2}(X^2-2X+2)
\end{array}\right)$$

Los factores invariantes son: $X+1$ y X^3-X.

Los divisores elementales son: $X+1, X+1, X, X-1$.

Entonces la forma canónica racional es:

$$\left(\begin{array}{c|ccc}
-1 & & & \\
\hline
 & 0 & 0 & 0 \\
 & 1 & 0 & 1 \\
 & 0 & 1 & 0
\end{array}\right)$$

La forma canónica de Weierstrass, la de Jacobson y la de Jordan es:

$$\left(\begin{array}{c|c|c|c}
-1 & & & \\
\hline
 & -1 & & \\
\hline
 & & 0 & \\
\hline
 & & & 1
\end{array}\right)$$

Cálculo de las bases. La matriz Q^{-1} es:

$$Q^{-1} = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
2 & X+1 & 1 & 0 \\
2X^2+2X+2 & X^3+X^2+X+1 & X^2+2X+1 & -2
\end{pmatrix}$$

y su inversa es:

$$Q=\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ -2 & -X-1 & 1 & 0\\ -X-2, & -X^2-X, & \frac{1}{2}(X^2+2X+1), & -\frac{1}{2}\end{pmatrix}$$

La base de $\mathbb{Q}[X]^4$ es:

$$\begin{array}{rrrr} e_1' = e_1 & & -2e_3 & -(X+2)e_4\\ e_2' = & e_2 & -(X+1)e_3 & -(X^2+X)e_4\\ e_3' = & & e_3 & +\frac{1}{2}(X^2+2X+1)e_4\\ e_4' = & & & -\frac{1}{2}e_4 \end{array}$$

Descomposición cíclica de M:

$$M\cong \frac{\mathbb{Q}[X]}{(X+1)}\oplus\frac{\mathbb{Q}[X]}{(X^3-X)}\cong \mathbb{Q}[X]\alpha(e_3')\oplus\mathbb{Q}[X]\alpha(e_4')$$

ya que e_1' y e_2' pertenecen al núcleo de α.
Base respecto a la cual adopta la forma canónica racional

$$\mathscr{B}'=\{\alpha(e_3'),\alpha(e_4'),f(\alpha(e_4')),f^2(\alpha(e_4'))\},$$

donde

$$\begin{array}{ll} \alpha(e_3') & = m_3+\frac{1}{2}(f^2+2f+1)(m_4)=-m_2+m_3,\\ \alpha(e_4') & = -\frac{1}{2}m_4,\\ f(\alpha(e_4')) & = -\frac{1}{2}m_1+m_3+m_4,\\ f^2(\alpha(e_4')) & = m_1+m_2-2m_3-\frac{3}{2}m_4. \end{array}$$

La matriz del cambio de base es:

$$T=\begin{pmatrix} 0 & 0 & -\frac{1}{2} & 1\\ -1 & 0 & 0 & 1\\ 1 & 0 & 1 & -2\\ 0 & -\frac{1}{2} & 1 & -\frac{3}{2}\end{pmatrix}$$

su inversa es:

$$T^{-1}=\begin{pmatrix} 2 & 0 & 1 & 0\\ -2 & 1 & 1 & -2\\ 2 & 2 & 2 & 0\\ 2 & 1 & 1 & 0\end{pmatrix}$$

La matriz de f respecto a la base $\mathscr{B}'$ es:

$$T^{-1}AT=\left(\begin{array}{c|ccc} -1 & 0 & 0 & 0\\ \hline 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0\end{array}\right).$$

La descomposición cíclica primaria de M es:

$$M \cong \frac{\mathbb{Q}[X]}{(X+1)} \oplus (\frac{\mathbb{Q}[X]}{(X+1)} \oplus \frac{\mathbb{Q}[X]}{(X)} \oplus \frac{\mathbb{Q}[X]}{(X-1)}) \cong$$

$$\mathbb{Q}[X]\alpha(e_3') \oplus \mathbb{Q}[X]X(X-1)\alpha(e_4') \oplus \mathbb{Q}[X](X+1)(X-1)\alpha(e_4') \oplus \mathbb{Q}[X](X+1)X\alpha(e_4').$$

La base respecto a la cual adopta la forma canónica de Weierstrass es:

$$\mathbb{B}'' = \{\alpha(e_3'), f(f-1)\alpha(e_4'), (f+1)(f-1)\alpha(e_4'), (f+1)f\alpha(e_4')\},$$

donde

$$\begin{array}{lrl} \alpha(e_3') & = & -m_2+m_3, \\ f(f-1)\alpha(e_4') & = & \frac{3}{2}m_1+m_2-3m_3-\frac{5}{2}m_4, \\ (f+1)(f-1)\alpha(e_4') & = & m_1+m_2-2m_3-m_4, \\ (f+1)f\alpha(e_4') & = & \frac{1}{2}m_1+m_2-m_3-\frac{1}{2}m_4. \end{array}$$

La matriz del cambio de base es:

$$S = \begin{pmatrix} 0 & \frac{3}{2} & 1 & \frac{1}{2} \\ -1 & 1 & 1 & 1 \\ 1 & -3 & -2 & -1 \\ 0 & -\frac{5}{2} & -1 & -\frac{1}{2} \end{pmatrix}$$

y su inversa es:

$$S^{-1} = \begin{pmatrix} 2 & 0 & 1 & 0 \\ -1 & 0 & 0 & -1 \\ 2 & -1 & -1 & 2 \\ 1 & 2 & 2 & -1 \end{pmatrix}$$

La matriz de f respecto a la base $\mathscr{B}''$ es:

$$S^{-1}AS = \left(\begin{array}{c|c|c|c} -1 & & & \\ \hline & -1 & & \\ \hline & & 0 & \\ \hline & & & 1 \end{array}\right)$$

□

Ejercicios

Formas canónicas de matrices

Ejercicio. 25.16.
Calcular las formas canónicas, y las bases respecto a las cuales las adoptan, del endomorfismo $f : \mathbb{Q}^4 \longrightarrow \mathbb{Q}^4$ *definido, respecto a una base canónica, por la matriz*

$$A = \begin{pmatrix} 6 & -1 & -1 & 2 \\ 4 & 2 & -2 & 4 \\ -4 & 2 & 6 & -4 \\ -2 & 1 & 1 & 2 \end{pmatrix}$$

Ref.: 1106e_002 *SOLUCIÓN.*

Ejercicio. 25.17.
Calcular las formas canónicas, y las bases respecto a las cuales las adoptan, del endomorfismo $f : \mathbb{Q}^4 \longrightarrow \mathbb{Q}^4$ *definido, respecto a una base canónica, por la matriz*

$$A = \begin{pmatrix} 12 & -1 & 2 & 2 \\ 8 & 2 & 0 & 4 \\ -16 & 2 & 0 & -4 \\ -12 & 1 & -4 & 2 \end{pmatrix}$$

Ref.: 1106e_003 *SOLUCIÓN.*

Ejercicio. 25.18.
Calcular las formas canónicas, y las bases respecto a las cuales las adoptan, del endomorfismo $f : \mathbb{Q}^4 \longrightarrow \mathbb{Q}^4$ *definido, respecto a una base canónica, por la matriz*

$$A = \begin{pmatrix} 4 & -1 & -1 & 0 \\ 2 & 2 & -2 & 2 \\ 0 & 2 & 6 & 0 \\ 0 & 1 & 1 & 4 \end{pmatrix}$$

Ref.: 1106e_004 *SOLUCIÓN.*

Ejercicio. 25.19.
Calcular las formas canónicas, y las bases respecto a las cuales las adoptan, del endomorfismo $f : \mathbb{Q}^4 \longrightarrow \mathbb{Q}^4$ *definido, respecto a una base canónica, por la matriz*

$$A = \begin{pmatrix} 10 & -1 & 2 & 0 \\ 6 & 2 & 0 & 2 \\ -12 & 2 & 0 & 0 \\ -10 & 1 & -4 & 4 \end{pmatrix}$$

Ref.: 1106e_000 *SOLUCIÓN.*

Bibliografía

[1] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, 3, American Mathematical Society, 1994.

[2] F. W. Anderson and K. R. Fuller, *Rings and categories of modules*, Graduate Texts in Math., 13, Springer–Verlag, 1974. 1

[3] M. F. Atiyah and I. G. Macdonald, *Introducción al álgebra conmutativa*, Reverté, Barcelona, 1973.

[4] Celine Carstensen, Benjamin Fine, and Rosenberger, *Abstract algebra. Applications to Galois Theory, Algebraic Geometry and Cryptography*, De Gruyter, 2011.

[5] I. S. Cohen, *Rings with restricted minimum condition*, Duke Math. J. **17** (1950), 27–42.

[6] P. M. Cohn, *Basic algebra*, Springer, 2003.

[7] D. Cox, J. J. Little, and D. O'Shea, *Ideals, varieties and algorithms*, Undergraduate Texts in Math., Springer–Verlag, 1992.

[8] D. S. Dummit and R. M. Foote, *Abstract algebra. 3rd ed.*, Wiley, 2004.

[9] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate texts in mathematics, 150, Springer–Verlag, 1995.

[10] M. Halmos, *Teoría intuitiva de los conjuntos*, Compañía Editorial Continental, 1982. I

[11] N. Jacobson, *Basic algebra II. 2nd ed.*, Freeman, 1989.

[12] G. J. Janusz, *Algebraic number theory*, Academic Press, 1973.

[13] I. Kaplansky, *Commutative rings*, Chicago Univ. Press, 1974. 13.15.

[14] E. Kunz, *Introduction to commutative algebra and algebraic geometry (Second edition corrected)*, Birkhauser, 1991.

[15] S. Lang, *Algebra 3rd. ed.*, Springer, 2002.

[16] H. Matsumura, *Commutative algebra*, Benjamin, 1980.

[17] N. Nagata, *Local rings*, R. E. Krieger Publ. Co., 1975.

[18] M. Reid, *Undergraduate commutative algebra*, London Math. Soc. Student Texts, 29, Cambridge Univ. Press, 1995.

[19] J. J. Watkins, *Topics in commutative algebra*, Princeton University Press, 2007.

Índice alfabético