



Treball de fi de grau
GRAU EN MATEMÀTIQUES

Facultat de Ciències
Universitat Autònoma de Barcelona

K-TEORIA ALGEBRAICA
Els grups K_0 i K_1

Autor: **Xavier LÓPEZ**

Supervisor: **Dr. Francesc PERERA**

26 de juny de 2017

Resum

K-TEORIA ALGEBRAICA

Els grups K_0 i K_1

La K -teoria algebraica és la branca de les matemàtiques que estudia el cas general de l'àlgebra lineal, usant anells en lloc de cossos. Associa a un anell R una seqüència de grups abelians $K_i(R)$. L'objectiu d'aquest treball és realitzar la construcció dels grups K_0 i K_1 , trobar casos (estructures algebraiques intermèdies entre cos i anell) que ens permetin calcular aquests grups i veure la relació entre ells.

Abstract

ALGEBRAIC K-THEORY

The groups K_0 and K_1

Algebraic K -theory is the branch of mathematics dealing with linear algebra over a general ring R instead of over a field F . It associates to a ring R a sequence of abelian groups $K_i(R)$. In this work the aim is to describe $K_0(R)$ and $K_1(R)$, find algebraic structures in the middle ground between fields and rings in which those groups are computable and find the relationship between those two groups.

Prefaci

El document que es presenta a continuació correspon al *Treball de fi de grau* del Grau en Matemàtiques de la Facultat de Ciències de la Universitat Autònoma de Barcelona realitzat per Xavier López Español.

Aquest treball està dedicat a l'estudi de K -teoria algebraica, la K -teoria alegraica és l'estudi de grups de classes d'objectes algebraics. De fet la lletra K va ser triada per Grothendieck, referint-se a ' K ' de "Klassen"(alemany per classes).

La K -teoria algebraica és centra en una cadena de grups abelians $K_n(R)$ associats a un anell R . En aquest treball ens basarem a construir els dos primers anells d'aquesta cadena, els grups K_0 i K_1 . El grup $K_0(R)$ permet definir un concepte proper a la dimensió sobre R -mòduls sense necessitat que tinguin una base. El grup $K_1(R)$ consisteix en classes d'equivalència sota transformacions per files de matrius invertibles sobre un anell R i és usat per a l'estudi de determinants.

El contingut del treball és nutreix essencialment de dos llibres fonamentals, *Algebraic K-Theory and Its Applications* amb l'autoria de Jonathan Rosenberg i *An Algebraic Introduction to K-theory* amb l'autoria de Bruce A. Magurn.

Rosenberg [1] realitza la construcció dels K -grups de forma molt eficient, tanmateix requereix certs prerequisits, com conceptes de mòduls, els quals són exposats en tot detall per Magurn [2]. També s'inclouen com a resultats algunes resolucions d'exercicis proposats per Rosenberg durant tot el treball, vull destacar en particular la construcció del grup K_1 sobre l'anell dels quaternions.

Estructura

El treball està estructurat en tres parts, en el primer capítol s'introdueixen els conceptes fonamentals sobre mòduls per a definir el grup K_0 i es planteja el problema de la impossibilitat de generalitzar el concepte de dimensió sobre R -mòduls, que donarà lloc al grup K_0 com a substitut viable d'aquest concepte.

En el segon capítol construïm el grup K_0 a partir de dues fonts: els mòduls projectius i els idempotents. Aquestes dues construccions equivalents ens permetran veure amb facilitat propietats d'aquest grup. Un cop definit, procedirem a calcular el grup K_0 per a diferents casos (estructures algebraiques intermitges entre cos i anell). Finalment definirem el grup relatiu $K_0(R, I)$ i trobarem una cadena exacta que el relaciona amb $K_0(R)$, també veurem que el grup relatiu $K_0(R, I)$ de fet és l'extensió del concepte de K_0 sobre anells sense unitat I .

El darrer capítol té una estructura semblant, comencem construint el grup K_1 , continuem amb el càlcul d'aquest grup per a estructures algebraiques entre cos i anell, definim el grup relatiu $K_1(R, I)$ i acabem extenent la cadena exacta del capítol anterior a una cadena que relaciona els grups K_0 i K_1 que usarem per a calcular K -grups.

Agraïments

En primer lloc vull agrair al meu tutor Francesc Perera per la seva tasca de direcció i suport que ha fet possible aquest treball.

També és imprescindible agrair el suport incansable proporcionat per la meua família durant tots aquests anys.

Finalment vull agrair a tots aquells que s'han interessat sobre aquest treball, inclosos els que no tenen cap interès en llegir-lo.

El treball de fi de grau representa el punt final d'una etapa, per acabar-la m'agradaria agrair a totes aquelles persones que m'han ajudat durant aquests anys a arribar fins aquí.

Vull mencionar especialment al Joan Gutiérrez, o Guti, que és l'excel·lent professor de l'institut públic Escola Industrial de Sabadell, ell és qui va despertar en mi l'interès per les matemàtiques.

També vull fer una menció especial a tots els companys de grau amb qui he col·laborat, però especialment amb els qui he tingut una col·laboració especialment intensa durant aquests anys, com el Gerard González, Guillem Miguel, Jordi Martínez, Dani Davidson amb els qui vam fer un excel·lent treball sobre el teorema de coloració de Pólya, a l'Alícia Sánchez, la Miriam Steinherr i Cristian Cisneros amb qui vaig col·laborar extensament, especialment a teoria de Galois, al Xavier Civit i el Jordi Lendínez que tot i ser companys em van fer de mentors en certa manera, a l'Edu Sándeiz i la Gemma Solera per deixar-me repetidament els seus magnífics apunts, i al Joshua Blöcker, amb qui vaig poder col·laborar a programació avançada i vam compartir sortides amb bicicleta després de classe.

Moltes Gràcies.

Contingut

Prefaci	vi
1 Introducció	1
1.1 Sumes directes i Idempotents	1
1.2 Producte tensorial	2
1.3 La propietat IBN	4
1.4 Mòduls projectius	6
2 Construcció del Grup K_0	9
2.1 K_0 a partir de mòduls projectius	9
2.2 K_0 a partir d'idempotents.	13
2.3 El cas d'un cos	15
2.4 El cas dels DIPs	15
2.5 El cas dels anells locals	16
2.6 El grup K_0 relatiu i el Teorema d'Excisió	20
3 Construcció del Grup K_1	25
3.1 Definició de K_1	25
3.2 El cas d'un cos	30
3.3 El cas dels anells de divisió	30
3.4 El cas dels anells locals	31
3.5 El cas dels Quaternions	36
3.6 El cas dels Dominis Euclidians.	40
3.7 El grup K_1 relatiu i la successió exacta	41
4 Conclusions	47
A Conceptes de Mòduls i Estructures Algebraiques	49
A.1 Recordatori	49
A.2 Definició de Mòduls	52
A.3 Submòduls i Quocients de Mòduls	56
A.4 Mòduls lliures i Bases	58
A.5 Mòduls finitament generats	61

Capítol 1

Introducció

L'objectiu d'aquest capítol és per una banda introduir els conceptes fonamentals per a la construcció dels grups K_0 i K_1 , en especial K_0 , i per l'altra exposar la propietat IBN com a plantejament del problema de la generalització del concepte de dimensió sobre R -mòduls. El contingut està basat en [2] per a les sumes directes, idempotents, producte tensorial i propietat IBN, i [1] per a la introducció a mòduls projectius, també hem usat [6] per a provar que els R -mòduls sobre anells commutatius compleixen la propietat IBN.

Inicialment l'annex A estava inclòs en aquesta secció, aquest annex té el fi de posar com a protagonista indiscutible del treball la K -teoria algebraica i al mateix temps permetre que el treball sigui autocontingut.

En aquest annex es recorden les definicions essencials que s'han vist durant el grau, i conceptes de mòduls, submòduls, mòduls quocients, mòduls lliures, bases i mòduls finitament generats, els quals un graduat recent no hi està necessàriament familiaritzat i que convé tenir presents durant la lectura del treball.

1.1 Sumes directes i Idempotents

En aquesta secció presentem els conceptes fonamentals de suma directa, interna i externa. Aquests conceptes tenen un rol fonamental al caracteritzar els mòduls projectius, els quals són la font de K_0 . També s'introdueix la relació entre els idempotents i la suma directa, que també usarem per a caracteritzar K_0 .

Definició 1.1.1. Diem que M és la **suma directa externa** $L \oplus N$ si M és el producte cartesià $L \times N = \{(x, y) : x \in L, y \in N\}$ amb suma component a component

$$(x_1, x_2) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

i producte escalar $r(x, y) = (rx, ry)$.

Diem que M és la suma directa interna $L \dot{\oplus} N$, si L i N són submòduls de M , $L + N = M$ i $L \cap N = 0_M$.

En qualsevol anell S , un **idempotent** és un element $e \in S$, amb $ee = e$.

Proposició 1.1.1. *Suposem que L i N són submòduls de M . Són equivalents:*

- i) $M = L \dot{\oplus} N$
- ii) Cada $m \in M$ té una i només una expressió de la forma $m = x + y$ amb $x \in L$ i $y \in N$.
- iii) Existeix un idempotent $e \in \text{End}_R(M)$ amb imatge L i nucli N .

Demostració. En les condicions de i), pel fet que $M = L + N$, tenim que tot $m \in M$ té una expressió $m = x + y$, amb $x \in L$ i $y \in N$. Suposem que existeix una expressió diferent

$m = x' + y'$ amb $x' \in L$ i $y' \in N$, aleshores $x - x' = y' - y \in L \cap N = \{0_M\}$, per tant $x = x'$ i $y = y'$ provant la unicitat de l'expressió.

En les condicions de ii), a d'existir una aplicació R -lineal $e : M \rightarrow M$, tal que $e(x + y) = x$ si $x \in L$ i $y \in N$. Observem que al complir-se que

$$(e \circ e)(x + y) = e(x) = e(x + 0) = x = e(x + y)$$

queda comprovat que e és un idempotent, amb imatge L i nucli N .

En les condicions de iii), per cada $m \in M$, $m = e(m) + m - e(m)$ amb $e(m) \in L$ i $m - e(m) \in \ker(e) = N$. Si $x \in L \cap N$, aleshores $x = e(y)$ per algun $y \in M$, i

$$0_M = e(x) = e(e(y)) = e(y) = x.$$

Per tant, $M = L \dot{\oplus} N$. □

Proposició 1.1.2. *Siguin L, M i N R -mòduls. Aleshores $M \cong L \oplus N$ si i només si $M = L' \dot{\oplus} N'$ per L', N' submòduls de M tals que $L' \cong L$ i $N' \cong N$.*

Demostració. Si $f : L \oplus N \rightarrow M$ és un isomorfisme, tenim que $L \cong L \oplus 0 \cong f(L \oplus 0)$, $N \cong 0 \oplus N \cong f(0 \oplus N)$, i

$$M = f(L \oplus 0) \dot{\oplus} f(0 \oplus N).$$

Recíprocament, si $\alpha : L \rightarrow L', \beta : N \rightarrow N'$ són isomorfismes i $M = L' \dot{\oplus} N'$, aleshores

$$\begin{aligned} f : L \oplus N &\rightarrow M \\ (x, y) &\mapsto \alpha(x) + \beta(y) \end{aligned}$$

és R -lineal i bijectiva per la proposició anterior. □

1.2 Producte tensorial

Si K és un cos, i J el conjunt de classes d'isomorfisme de K -espais vectorials, la dimensió sobre K defineix un isomorfisme de monoides

$$(J, \oplus) \cong (\mathbb{N}, +).$$

Tanmateix \mathbb{N} és un semianell sota les operacions suma i producte, usant l'isomorfisme de dimensió podem donar estructura de semianell a J , és a dir si V i W són K -espais vectorials de dimensió finita, ha d'existir un espai vectorial X amb $c(V)c(W) = c(X)$ a J amb $\dim_F X = (\dim_F V)(\dim_F W)$.

Per a la construcció de X a partir de V i W necessitem una forma de multiplicar elements d'un mòdul per elements d'un altre mòdul.

Definició 1.2.1. Si R és un anell, donats dos R -mòduls $M_R, {}_R N$ i un grup abelià additiu A , l'aplicació $f : M \times N \rightarrow A$ és **R -equilibrada** si compleix:

$$\begin{aligned} f((m + m', n)) &= f((m, n)) + f((m', n)) \\ f((m, n + n')) &= f((m, n)) + f((m, n')) \\ f((mr, n)) &= f((m, rn)) \end{aligned}$$

per a tot $m, m' \in M, n, n' \in N$ i $r \in R$.

Hi ha una aplicació universal R -equilibrada $M_r \times_R N \rightarrow A$ tal que el seu codomini A és el producte de mòduls que busquem, ara la construïm.

Definició 1.2.2. Si R és un anell, el **producte tensorial** dels mòduls M_R i ${}_R N$ sobre l'anell R és el grup quocient

$$M \otimes_R N := F_{\mathbb{Z}}(M \times N) / \langle D \rangle$$

on $F_{\mathbb{Z}}(M \times N) / \langle D \rangle$ és el \mathbb{Z} -mòdul lliure construït per tenir com a base el conjunt $M \times N$, i D el subgrup generat per elements que tinguin una de les següents tres formes:

$$\begin{aligned} (m + m', n) - (m, n) - (m', n), \\ (m, n + n') - (m, n) - (m, n'), \\ (mr, n) - (m, rn), \end{aligned}$$

per $m, m' \in M$, $n, n' \in N$, i $r \in R$. Si $m \in M$ i $n \in N$, denotem per $m \otimes n := (m, n) + \langle D \rangle$.

Per construcció $M \otimes_R N$ és un grup abelià additiu amb generadors $m \otimes n$ i relacions:

$$\begin{aligned} (m + m') \otimes n &= (m \otimes n) + (m' \otimes n), \\ m \otimes (n + n') &= (m \otimes n) + (m \otimes n'), \\ mr \otimes n &= m \otimes rn \end{aligned}$$

per $m, m' \in M$, $n, n' \in N$ i $r \in R$. L'aplicació natural

$$\begin{aligned} t : M \times N &\rightarrow M \otimes_R N \\ (m, n) &\mapsto m \otimes n \end{aligned}$$

és equilibrada, de fet, és l'aplicació amb codomini $M \otimes_R N$ que volíem construir.

Proposició 1.2.1. Si R és un anell amb mòduls M_R i ${}_R N$, aleshores per a cada funció R -equilibrada $f : M \times N \rightarrow A$, hi ha un i només un homomorfisme de grups additius:

$$\bar{f} : M \otimes_R N \rightarrow A \quad \text{amb} \quad \bar{f}(m \otimes n) = f((m, n))$$

per a tot $m \in M$ i $n \in N$; aquest és el únic homomorfisme de grups \bar{f} tal que fa commutar el triangle:

$$\begin{array}{ccc} M \times N & \xrightarrow{t} & M \otimes_R N \\ & \searrow f & \downarrow \bar{f} \\ & & A \end{array}$$

Demostració. El fet que f sigui R -equilibrada fa que la seva extensió \mathbb{Z} -lineal $F_{\mathbb{Z}}(M \times N)$ envii D a 0, per tant l'existència de \bar{f} ve induïda per $\bar{f}(m \otimes n) = f((m, n))$. La unicitat és conseqüència del fet que els elements de la forma $m \otimes n$ generen $M \otimes_R N$. \square

Definició 1.2.3. Sigui R i S anells. Diem que un grup abelià additiu M és un **bimòdul** si és un R -mòdul per l'esquerra i un S -mòdul per la dreta, i ha de complir $r(ms) = (rm)s$, el denotem ${}_R M_S$.

Proposició 1.2.2. Donats tres anells R, S, T i dos bimòduls ${}_R M_S$ i ${}_S N_T$, el producte tensorial sobre S és un bimòdul ${}_R M \otimes N_T$.

Demostració. Si $r \in R$, la funció

$$\begin{aligned} f_r : M \times N &\rightarrow M \otimes_S N \\ (m, n) &\mapsto (rm \otimes n) \end{aligned}$$

és S -equilibrada.

Observem que a la definició de bimòdul anterior, demanem per definició que un bimòdul compleixi $r(ms) = (rm)s$, aquesta propietat és necessària per a que la funció anterior sigui S -equilibrada, en particular, és necessària per a que compleixi $f_r((ms, n)) = f_r((m, sn))$.

Per tant, usant la proposició anterior hi ha un homomorfisme de grups \mathbb{Z} -lineal

$$\bar{f}_r : M \otimes_S N \rightarrow M \otimes_S N$$

amb $\bar{f}_r(m \otimes n) = (rm) \otimes n$, per $m \in M$ i $n \in N$. Observem que la funció

$$\begin{aligned} R \times (M \otimes_S N) &\rightarrow M \otimes_S N \\ (r, x) &\mapsto r \cdot x = \bar{f}_r(x) \end{aligned}$$

és el producte per escalars que dóna estructura de R -mòdul per l'esquerra a $M \otimes_S N$, ja que com que \bar{f}_r és \mathbb{Z} -lineal i

$$\begin{aligned} (r + r') \cdot (m \otimes n) &= ((r + r')m \otimes n) = (rm + r'm \otimes n) = (rm \otimes n) + (r'm \otimes n), \\ (rr') \cdot (m \otimes n) &= r \cdot (r' \cdot (m \otimes n)), \\ 1 \cdot (m \otimes n) &= m \otimes n \end{aligned}$$

Sota el producte per escalars, tenim

$$r \cdot \sum_{i=1}^k (m_i \otimes n_i) = \sum_{i=1}^k (rm_i) \otimes n_i$$

Similarment, $M \otimes_S N$ és un T -mòdul per la dreta via

$$\left(\sum_{i=1}^k (m_i \otimes n_i) \right) \cdot t = \sum_{i=1}^k m_i \otimes (n_i t)$$

Finalment per a provar que $M \otimes_S N$ és un R, T -bimòdul, només cal veure que

$$r \cdot \left(\sum (m_i \otimes n_i) \cdot t \right) = \sum (rm_i) \otimes (n_i t) = (r \cdot \sum (m_i \otimes n_i)) \cdot t.$$

□

1.3 La propietat IBN

Tot espai vectorial sobre un cos té una base, i dues bases del mateix espai vectorial tenen sempre el mateix nombre d'elements, per tant el concepte de dimensió d'un espai vectorial V està ben definit. A més la dimensió és un invariant que classifica els espais vectorials.

Hom podria pensar que aquest resultat es manté al generalitzar el concepte d'espai vectorial sobre un cos a espai vectorial sobre un anell, i.e., sobre R -mòduls, però no és així.

En un R -mòdul M , l'existència d'una base no està garantida, i en cas de tenir base, podem tenir bases amb diferent cardinal, i.e., el cardinal de la base no és un invariant. L'objectiu d'aquesta subsecció és comprovar aquests fets.

La millor forma de provar que l'existència de la base no està garantida és trobar un R -mòdul que no tingui base.

Proposició 1.3.1. *Els grup additiu format pels racionals \mathbb{Q} és un \mathbb{Z} -mòdul sense base.*

Demostració. En primer lloc observem \mathbb{Q} no és un \mathbb{Z} -mòdul cíclic, i.e., no pot estar generat per un únic element. D'altra banda, observem que dos elements qualsevols de \mathbb{Q} són \mathbb{Z} -linealment dependents, ja que donats $m, n \in \mathbb{Q}$, existeixen $a, b \in \mathbb{Z}$ tal que es forma una combinació \mathbb{Z} -lineal amb $am + bn = 0$.

Així doncs aquest \mathbb{Z} -mòdul no pot tenir una base formada per un element, ni una base formada per més d'un element. \square

Definició 1.3.1. Diem que un anell R compleix la propietat **IBN** (Invariant Basis Number) si per a tot R -mòdul M , tota parella de bases de M té el mateix cardinal, és a dir, el nombre d'elements bàsics és invariant.

Veiem ara que el cardinal de la base no és un invariant sobre R -mòduls, en particular trobarem un anell sense la propietat IBN, i.e. un R -mòdul amb dues bases de cardinal diferent.

Proposició 1.3.2. *El cardinal de la base no és un invariant sobre tot R -mòdul, amb R anell no necessàriament commutatiu.*

Demostració. Per a qualsevol R anell no trivial, considerem A com el conjunt de matrius definides sobre R amb infinites files i columnes, tals que cada columna tingui un nombre finit d'entrades diferents de zero.

Observem que la suma i producte habitual doten A amb l'estructura d'anell. A més, si considerem el conjunt de columnes d'elements de A , tenim un A -mòdul. En concret si $A \in A$, la columna j -èssima de A la denotarem per ae_j , al considerar A com a A -mòdul tenim que la suma i el producte són calculats per columnes:

$$\begin{aligned}(a + b)e_j &= ae_j + be_j \\ (ab)e_j &= a(be_j)\end{aligned}$$

Així doncs tenim que A és un A -mòdul. Per una banda observem que a la matriu identitat, denotada per

$$1_A = \begin{bmatrix} 1 & 0 & \dots \\ 0 & 1 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix},$$

és una base de A , i.e., A té una base formada per un element.

D'altra banda, per a cada $a \in A$, definim a', a'' de forma que les columnes de a' siguin les columnes senars de a , i les columnes de a'' siguin les columnes parells de a .

Aleshores la funció $f : A \rightarrow A \oplus A$ definida per $f(a) = (a', a'')$ és un isomorfisme A -lineal amb inversa formada per ajuntar les columnes de a' i a'' .

Usant el fet que la imatge d'elements bàsics és element bàsic, podem veure el resultat al Corol·lari A.4.1, tenim que A té una base formada per dos elements

$$f^{-1}(1_A, 0_A) = \begin{bmatrix} 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}, \quad f^{-1}(0_A, 1_A) = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

□

Finalment veurem que tot R anell commutatiu no trivial compleixen la propietat IBN, per a veure aquest resultat veiem el següent Lema.

Lema 1.3.1. *Sigui R un anell commutatiu i siguin m, n dos enters qualsevols tals que $m < n$, si hi ha una aplicació lineal exhaustiva $R^m \rightarrow R^n$. Aleshores $1_R = 0_R$.*

Demostració. Sigui φ l'aplicació exhaustiva que envia $R^m \rightarrow R^n$. L'exhaustivitat de φ garanteix l'existència d'una aplicació ψ (inversa per la dreta) tal que $\varphi \circ \psi = \text{id}$. Podem estendre φ a $R^n = R^m \oplus R^{n-m}$ de forma que $\varphi(R^{n-m}) = 0_R$, i considerar ψ com una aplicació sobre R^n .

Considerem ara les matrius A i B associades a les aplicacions φ i ψ respectivament. Per una banda tenim que $\det(AB) = 1_R$, d'altra banda tenim que $\det(B) = 0$ ja que la darrera fila de B és plena de 0_R 's per construcció.

Usant la propietat $\det(AB) = \det(A)\det(B)$ obtenim el resultat que buscàvem. □

Observem que a la prova anterior hem pogut usar l'existència del determinant gràcies al fet que A i B són matrius definides sobre un anell commutatiu.

Corol·lari 1.3.1. *Si R és un anell commutatiu no trivial, compleix la propietat IBN, i.e., els R -m.ll.f.g. tenen un nombre d'elements bàsics invariant.*¹

1.4 Mòduls projectius

Els mòduls projectius tenen un rol fonamental en la construcció de K_0 , en aquesta secció introduïm la definició dels mòduls projectius i provem la caracterització fonamental dels mòduls projectius usant la suma directa.

Definició 1.4.1. Donat un anell R , anomenem **mòdul projectiu sobre R** a un R -mòdul P si compleix que, per a tot homomorfisme de R -mòduls exhaustiu $\alpha : M \twoheadrightarrow P$ existeix un homomorfisme $\beta : P \rightarrow M$ tal que $\alpha \circ \beta = \text{id}_P$, és a dir, tot homomorfisme de R -mòduls exhaustiu té una inversa per la dreta.

Lema 1.4.1. *Un R -mòdul P és projectiu si i només si tot diagrama de R -mòduls com el de la Figura 1.1 amb ψ exhaustiva*

$$\begin{array}{ccc} & P & \\ & \downarrow \phi & \\ M & \xrightarrow{\psi} & N \end{array} \quad \begin{array}{l} \text{es pot completar fent-lo com-} \\ \text{mutatiu, i.e., existeix una} \\ \text{aplicació } \theta \text{ tal que} \end{array} \quad \begin{array}{ccc} & P & \\ & \downarrow \phi & \\ M & \xrightarrow{\psi} & N \end{array} \quad \begin{array}{l} \swarrow \theta \\ \end{array}$$

FIGURA 1.1

¹Usem l'abreviatura per R -mòdul lliure finitament generat (R -m.ll.f.g.).

Demostració. Suposem que es compleix la propietat de completació de diagrames, sigui α un homomorfisme exhaustiu de R -mòduls $\alpha : M \rightarrow P$, hem de veure que té una inversa per la dreta. podem prendre $N = P$, $\phi = id_P$, i $\psi = \alpha$. Aleshores el $\theta : P \rightarrow M$ resultant de la propietat de completació de diagrames compleix $\alpha \circ \theta = id_P$, i.e. β és la inversa per la dreta de α .

Veiem ara el recíproc, suposem que tot homomorfisme de R -mòduls exhaustiu $\alpha : M \rightarrow P$ té una inversa per la dreta $\beta : P \rightarrow M$. Donat un diagrama de R -mòduls com el de la Figura 1.1, canviant $M \xrightarrow{\psi} N$ per $M \oplus P \xrightarrow{\psi \oplus id_P} N \oplus P$ i $\phi : P \rightarrow N$ per $((\phi, id_P) : P \rightarrow N \oplus P)$, podem suposar que ϕ és injectiva (Figura 1.2). A més, si canviem N per la imatge de ϕ i M per $\psi^{-1}(\phi(P))$, podem suposar que ϕ és un isomorfisme (Figura 1.3). Aleshores, considerant β com la inversa per la dreta de $\alpha = \phi^{-1} \circ \psi$ tenim que $\beta : P \rightarrow M$ ens permet completar el diagrama.

$$\begin{array}{ccc} & P & \\ & \downarrow \phi & \\ M & \xrightarrow{\psi} & N \end{array} \quad \begin{array}{ccc} & P & \\ & \downarrow \phi \oplus id_P & \\ M \oplus P & \xrightarrow{\psi \oplus id_P} & N \oplus P \end{array}$$

FIGURA 1.2

$$\begin{array}{ccc} & P & \\ & \downarrow \phi \oplus id_P & \\ \psi^{-1}(\phi(P)) \oplus P & \xrightarrow{\psi \oplus id_P} & \phi(P) \oplus P \end{array}$$

FIGURA 1.3

□

Observació. Observem que si $\alpha : M \rightarrow P$ és exhaustiva i $\beta : P \rightarrow M$ és la seva inversa per la dreta, aleshores $p := \beta \circ \alpha$ és un endomorfisme idempotent de M ja que

$$\begin{aligned} (\beta \circ \alpha)^2 &= (\beta \circ \alpha) \circ (\beta \circ \alpha) \\ &= \beta \circ (\alpha \circ \beta) \circ \alpha \\ &= \beta \circ id_P \circ \alpha = \beta \circ \alpha \end{aligned} \tag{1.1}$$

A més, usant la Proposició 1.1.1 tenim que $M \cong P \oplus \text{Ker}(p) = P \oplus (1 - p)(M)$

Lema 1.4.2. *Sigui R un anell, tot R -mòdul lliure és projectiu.*

Demostració. Sigui F un R -mòdul lliure, al ser lliure ha de tenir una base B . Sigui $\alpha : M \rightarrow F$ un homomorfisme de mòduls exhaustiu, gràcies a l'exhaustivitat de α per a cada element bàsic $x_i \in B \subset F$ ha d'existir algun $y_i \in M$ tal que $\alpha(y_i) = x_i$. Definim l'aplicació β a partir de la imatge dels elements bàsics $\beta(x_i) = y_i$, usant la Proposició A.4.1 β és un morfisme $F \rightarrow M$ ben definit. A més, és inversa per la dreta de α . □

Teorema 1.4.3 (Caracterització fonamental dels mòduls projectius). *Sigui R un anell. Un R -mòdul és projectiu si i només si és isomorf a un sumand directe d'un R -mòdul lliure². És finitament generat i projectiu si i només si és isomorf a un sumand directe de R^n per algun n .*

Demostració. Si P és un mòdul projectiu, ha de tenir almenys un conjunt generador G (no és necessàriament una base de P). Triem un R -mòdul F amb base B que ens permeti definir una aplicació bijectiva entre elements de B i G . Usant de nou A.4.1 tenim que α té una extensió a una aplicació R -lineal $\hat{\alpha} : F \rightarrow P$. De fet, com que la imatge de B és P , $\hat{\alpha}$ és exhaustiva. Usant l'Observació anterior tenim que P és isomorf a una suma directa en un R -mòdul lliure, a més, si P és finitament generat, podem escollir que F sigui exactament

²i.e. existeix un R -mòdul Q i un R -mòdul lliure F tal que $F = P \oplus Q$.

R^n on n és el nombre d'elements de G .

Per a veure el recíproc, suposem que $F \cong P \oplus Q$, on F és un mòdul lliure. Donat un homomorfisme de R -mòduls exhaustiu $\alpha : M \rightarrow P$, observem que l'homomorfisme de R -mòduls $\alpha \oplus id_Q : (M \oplus Q) \rightarrow (P \oplus Q) = F$ també és exhaustiu. A més, com que F és lliure, ha de ser projectiu. Així doncs, usant la projectivitat de F tenim que $\alpha \oplus id_Q$ té una inversa per la dreta. Si restringim la inversa per la dreta a P i la projectem sobre M tenim una inversa per la dreta de α . Per acabar, si $F \cong R^n$ amb generadors $x_1, \dots, x_n \in F$, aleshores P ve generat pels n elements $p(x_i)$, on p és la identitat a P i 0 a Q . \square

Capítol 2

Construcció del Grup K_0

La dimensió és un invariant dels espais vectorials que els classifica, és a dir, dos espais vectorials sobre un cos K són isomorfs si i només si tenen la mateixa dimensió, en concret podem crear una bijecció entre la col·lecció de classes d'isomorfisme de K -espais vectorials i \mathbb{N} , a més, la suma directa ens permet sumar espais vectorials, de forma que $\dim(V \oplus W) = \dim(V) + \dim(W)$. Per afegit, podem completar el monoide \mathbb{N} a un grup abelià \mathbb{Z} que conté totes les diferències d'enters no negatius $m - n$. Similarment, podem completar el monoide de la col·lecció de les classes de isomorfia d'espais vectorials al grup $K_0(K)$, aquest grup és isomorf a \mathbb{Z} i consisteix en les diferències $c(V) - c(W)$ on c denota la classe d'isomorfisme dels espais vectorials.

Al generalitzar el cas d'un cos K a un anell arbitrari R tenim que els R -mòduls no tenen necessàriament una base, per tant el concepte de dimensió desapareix, però si restringim la nostra atenció a la classe dels R -mòduls projectius, tenim que el grup abelià $K_0(R)$ segueix intacte com el fantasma desaparegut de la dimensió. L'estructura de $K_0(R)$ reflecteix la generalització del concepte de dimensió dels espais vectorials sobre R -mòduls. En particular si R no és un cos, $K_0(R)$ no és necessàriament isomorf a \mathbb{Z} .

En aquest capítol presentarem $K_0(R)$, començarem definint-lo a partir de classes d'isomorfisme de mòduls projectius i després usarem la relació entre mòduls projectius i els idempotents per a presentar K_0 a partir de classes d'equivalència de matrius idempotents. Aquestes caracteritzacions ens permetran mostrar amb facilitat propietats del grup. Després estudiem K_0 per a cossos, dominis d'ideals principals i anells locals. A la darrera secció introduïrem el grup K_0 relatiu, aquest grup ens permetrà trobar una successió exacta que generalitzarem al següent capítol relacionant els grups K_0 i K_1 . Finalment veurem que K_0 també es pot definir per a anells sense unitat.

La referència bibliogràfica essencial d'aquest capítol és [1], a més s'ha usat [2] com a referència puntualment, també hem usat [7] per l'*Eilenberg swindle*, [9] per el Lema de Nakayama i el seu corol·lari, i un resultat puntual de [8] que no hem provat però està explícitament referenciat durant el capítol.

2.1 K_0 a partir de mòduls projectius

L'objectiu d'aquesta secció és definir K_0 a través de mòduls projectius, en primer lloc notarem la importància de considerar el conjunt de classes d'isomorfisme de mòduls projectius en lloc de prendre la col·lecció de tots els mòduls projectius, posteriorment presentem el grup de Grothendieck i finalment definim K_0 .

Definició 2.1.1. Donat un anell R , denotem per $\text{Proj } R$ a les classes d'isomorfisme de mòduls projectius finitament generats.

La següent Proposició justifica perquè prenem classes d'isomorfisme, però abans necessitem un Lema:

Lema 2.1.1. *La col·lecció de tots els singletons no és un conjunt. (Un singletó és un conjunt format per un únic element).*

Demostració. Si A és un conjunt que conté tots els singletons, per l'axioma de la unió (l'axioma de la unió afirma que per a un conjunt arbitrari A , existeix el conjunt $\bigcup A$ que consisteix en els elements dels elements del conjunt), $\bigcup A$ és un conjunt, però és el conjunt que conté tots els conjunts, per la paradoxa de Russell no pot ser un conjunt. Per tant A no és un conjunt. \square

Proposició 2.1.1. *Sigui P la col·lecció de tots els R -mòduls projectius finitament generats, llavors P no és un conjunt.*

Demostració. Observem que donats dos elements diferents $\bullet \neq \star$, el mòdul $(\{\bullet\}, +, \cdot)$ amb estructura $\bullet + \bullet = \bullet$ i $r \cdot \bullet = \bullet$ per a tot $r \in R$; és un mòdul diferent del mòdul $(\{\star\}, \oplus, \odot)$ amb estructura $\star \oplus \star = \star$ i $r \odot \star = \star$ per a tot $r \in R$.

Així doncs, per cada conjunt format per un únic element (singletó), podem crear un R -mòdul finitament generat, i com que la col·lecció de tots els singletons no és un conjunt, la col·lecció de tots els R -mòduls tampoc pot ser un conjunt. \square

Així doncs, hem de considerar $\text{Proj } R$ com el conjunt de classes d'isomorfia, és a dir, per a cada classe d'isomorfa escollim un, i només un, mòdul que la representi.

Proposició 2.1.2. *$\text{Proj } R$ amb l'operació binària \oplus té estructura de semigrup (un semigrup és un conjunt S junt amb una operació binària associativa $\cdot : S \times S \rightarrow S$).*

Demostració. Si $P, Q \in \text{Proj } R$, al ser R -mòduls projectius finitament generats existeixen dos R -mòduls P', Q' i dos enters positius n, m tal que $P \oplus P' \cong R^m$ i $Q \oplus Q' \cong R^n$. Aleshores usant que \oplus és associativa tenim

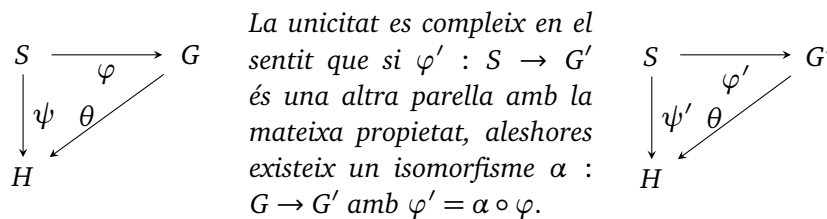
$$(P \oplus Q) \oplus (P' \oplus Q') \cong (P \oplus P') \oplus (Q \oplus Q') \cong R^m \oplus R^n \cong R^{n+m}$$

Observem que la suma directa està ben definida, ja que si $P \cong P'$ i $Q \cong Q'$, aleshores $P \oplus Q \cong P' \oplus Q'$.

De fet, $\text{Proj } R$ té estructura de monoide, ja que té per element identitat el mòdul 0. \square

Tenim doncs que $\text{Proj } R$ té estructura de semigrup, però en general no té estructura de grup. El següent Teorema ens permet forçar l'estructura de grup a $\text{Proj } R$. La idea que ens permetrà dotar d'estructura de grup és una generalització de la construcció del grup abelià additiu \mathbb{Z} a partir dels enters positius, o de la construcció de \mathbb{Q}^\times a partir dels enters no nuls, consisteix a introduir inverses formals per a certs elements.

Teorema 2.1.2. *Sigui S un semigrup commutatiu (sense necessitat de tenir element unitat). Existeix un grup abelià G , anomenat **grup de Grothendieck** o grup completat de S , junt amb un homomorfisme de semigrups $\varphi : S \rightarrow G$, tal que per a tot grup H i tot homomorfisme $\psi : S \rightarrow H$, hi ha un únic homomorfisme $\theta : G \rightarrow H$ amb $\psi = \theta \circ \varphi$.*



Demostració. Definim G com el conjunt de les classes d'equivalència de parelles (x, y) amb $x, y \in S$, on $(x, y) \sim (u, v)$ si i només si hi ha un $t \in S$ tal que

$$x + v + t = u + y + t \text{ a } S.$$

Denotem per $[(x, y)]$ a la classe d'equivalència de (x, y) . Aleshores definim la suma per

$$[(x, y)] + [(x', y')] = [(x + x', y + y')]$$

La suma de classes està ben definida, ja que si $(x, y) \sim (u, v)$, i $(x', y') \sim (u', v')$ aleshores existeixen $t, t' \in S$ tal que

$$\begin{cases} x + v + t = y + u + t \\ x' + v' + t' = y' + u' + t' \end{cases} \Rightarrow x + x' + v + v' + t + t' = y + y' + u + u' + t + t'$$

Al ser S un semigrup, $t + t' \in S$ i per tant

$$(x, y) + (x', y') = (x + x', y + y') \sim (u + u', v + v') = (u, v) + (u', v').$$

Com que l'associativitat se segueix complint, tenim que G amb la suma té estructura de semigrup. A més, com que S és commutatiu tenim que $x + y = y + x$ i per tant $[(x, x)] = [(y, y)]$, observem que aquest element és element neutre de G , i.e., 0_G . De fet aquest element dóna estructura de monoide a G . També es compleix que tot element de G té invers:

$$[(x, y)] + [(y, x)] = [(x + y, x + y)] = 0,$$

per tant G és un grup. Definim $\varphi : S \rightarrow G$ com

$$\varphi(x) = [(x + x, x)]$$

es compleix $\varphi(x) + \varphi(y) = \varphi(x + y)$, per tant és un homomorfisme de semigrups.

Observem que la imatge de φ genera G com a grup ja que

$$[(x, y)] = \varphi(x) - \varphi(y)$$

Donat un grup H i un homomorfisme $\psi : S \rightarrow H$, el homomorfisme $\theta : G \rightarrow H$ amb $\psi = \theta \circ \varphi$ es defineix per

$$\theta([(x, y)]) = \psi(x) - \psi(y).$$

Una manera alternativa de definir G és definir-lo com el grup generat per $[x]$, amb $x \in S$, sota la relació $[x] + [y] = [z]$ a G si $x + y = z$ a S . Observem que $[(x, y)]$ de la construcció anterior correspon a $[x] - [y]$ d'aquesta relació. L'aplicació φ és $x \mapsto [x]$, i tot homomorfisme de S a un grup H ha de factoritzar a través de G per construcció.

Per provar la unicitat, suposa que $\varphi' : S \rightarrow G'$ té la mateixa propietat universal. En primer lloc, $\varphi'(S)$ ha de generar G' ja que, en cas contrari, si G'' és el subgrup generat per la imatge de φ' , aleshores hi ha dos homomorfismes $\theta : G' \rightarrow G' \oplus G'/G''$ amb

$$(\varphi', 0) = \theta \circ \varphi'$$

aquests són $\theta = (id, 0)$ i $\theta = (id, q)$ on q és la projecció canònica.

Aplicant la propietat universal per a G i G' , han d'existir aplicacions $\alpha : G \rightarrow G'$ amb $\varphi' = \alpha \circ \varphi$ i $\beta : G' \rightarrow G$ amb $\varphi = \beta \circ \varphi'$. A més $\alpha \circ \beta = id$ a la imatge de φ' , i.e., a tot G' , i per tant té inversa per l'esquerra β . Similarment $\beta \circ \alpha = id$ a la imatge de φ , per tant

també tenim que α és inversa per la dreta de β . □

Observació. L'assignació $S \mapsto G = G(S)$ és de fet un functor de la categoria de semigrups abelians a la categoria de grups abelians, ja que si $\gamma : S \rightarrow S'$ és un homomorfisme de semigrups, indueix un diagrama commutatiu

$$\begin{array}{ccc} S & \xrightarrow{\quad} & S' \\ \downarrow \varphi & \gamma' & \downarrow \varphi' \\ G(S) & \longrightarrow & G(S') \end{array}$$

on l'aplicació $G(S) \rightarrow G(S')$ és unívocament determinada per la propietat universal de $G(S)$ que acabem de demostrar.

Observació. L'aplicació $\varphi : S \rightarrow G$ (en el context del Teorema 2.1.2) és injectiva si i només si la propietat cancel·lativa es compleix a S , i.e. $(x + z = y + z \Rightarrow x = y)$ per a tot $x, y, z \in S$ ¹. Els semigrups sense propietat cancel·lativa són generalment difícils de tractar, en canvi tractar el seus grup de Grothendieck pot ser més senzill.

Veiem ara un exemple de càlcul específic del grup de Grothendieck d'un semigrup específic.

Exemple. Sigui S el monoide abelià amb elements $a_{n,m}$, on $n \in \mathbb{N}$, i

$$\begin{cases} m = 0 & \text{si } n = 0 \text{ o } 1 \\ m \in \mathbb{Z} & \text{si } n = 2 \\ m \in \mathbb{Z}/2 & \text{si } n \geq 3 \end{cases}$$

amb l'operació de semigrup donada per la fórmula

$$a_{n,m} + a_{n',m'} = a_{n+n',m+m'}$$

on $m + m'$ es calcula a \mathbb{Z} si $n + n' \leq 2$ i a $\mathbb{Z}/2$ si $n + n' \geq 3$.

Per calcular el grup de Grothendieck $G(S)$ del monoide, nota primer que φ no és injectiva, ja que per $m, n \in \mathbb{Z}$ amb $m \equiv n \pmod{2}$ i $m \neq n$, compleix que $\varphi((2, n)) = \varphi((2, m))$. Així doncs usant l'observació anterior tenim que la propietat cancel·lativa a S no es compleix.

Usarem que $G(S)$ ve generat per $\varphi(S)$, per tant convé calcular

$$\begin{aligned} \varphi : \quad S &\rightarrow G(S) \\ (0, 0) &\mapsto [(0, 0), (0, 0)] \sim (0, 0) \\ (1, 0) &\mapsto [(2, 0), (1, 0)] \sim (1, 0) \\ (2, n) &\mapsto [(4, 2n), (2, n)] \sim (2, n \bmod 2) \\ (m, 0) &\mapsto [(2m, 0), (m, 0)] \sim (m, 0) \\ (m, 1) &\mapsto [(2m, 2), (m, 1)] \sim (m, 1) \end{aligned}$$

per $n, m \in \mathbb{Z}$ i $m \geq 3$. Tenim doncs que aquests elements formen el grup

$$G(S) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

¹ Si tenim $x, y \in S$ elements diferents tals que $[x + x, x] = [y + y, y]$, aleshores $x + x + y = y + y + x$, si prenem $z = x + y$ tenim $x + z = y + z$ però per hipòtesi $x \neq y$, per tant no es compleix la propietat cancel·lativa. Podem invertir el raonament per veure el recíproc.

Definició 2.1.2. Sigui R un anell amb unitat. Aleshores $K_0(R)$ és el **grup de Grothendieck** (en el mateix sentit que en el Teorema 2.1.2) del semigrup $\text{Proj } R$ (semigrup format per classes d'isomorfisme de R -mòduls projectius finitament generats).

Podríem provar que K_0 és un **functor**, en el sentit que si $\varphi : R \rightarrow R'$ és un homomorfisme d'anells, hi ha un homomorfisme induït $K_0(\varphi) = \varphi_* : K_0(R) \rightarrow K_0(R')$, aquest fet esdevindrà trivial a partir de la caracterització dels mòduls projectius a través de classes de matrius idempotents.

2.2 K_0 a partir d'idempotents.

L'objectiu d'aquesta secció és caracteritzar el grup K_0 a partir de les classes d'equivalència d'idempotents, en lloc de fer-ho a partir de les classes d'isomorfia de mòduls projectius com hem fet a la secció anterior. Aquesta caracterització ens facilitarà provar propietats rellevants per al càlcul de K -grups.

Si P és R -m.p.f.g.,² usant la caracterització dels mòduls projectius (Teorema 1.4.3) podem assumir sota isomorfisme que $P \oplus Q = R^n$ per algun n , a més per la Proposició 1.1.1 existeix automorfisme de R -mòduls idempotent sobre R^n que consisteix per ser la identitat sobre P i 0 sobre Q . Si a més tenim en compte que tot homomorfisme de R -mòduls $R^n \rightarrow R^n$ ve determinat per la imatge dels n vectors bàsics, aquest homomorfisme es correspon a una matriu $n \times n$ que actua per la dreta. Per tant, el mòdul projectiu P queda determinat per una matriu idempotent p de dimensions $n \times n$.

No obstant hi ha matrius idempotents diferents que poden donar lloc a la mateixa classe de mòduls projectius. Per exemple en el cas d'un cos l'únic invariant d'un mòdul projectiu és la seva dimensió, que es correspon amb el rang de p . Per tant, si pretenem caracteritzar $K_0(R)$ a partir de matrius idempotents, és indispensable descriure una relació d'equivalència entre les matrius idempotents de forma que cada classe de matrius idempotents es correspongui a una i només una classe de mòduls projectius.

Lema 2.2.1. Si p i q són matrius idempotents, possiblement de diferents mides, sobre un anell R ; els corresponents R -m.p.f.g. són isomorfs si i només si podem augmentar la mida de les matrius p i q afegint zeros a la cantonada inferior-dreta de forma que tinguin la mateixa mida $N \times N$ i siguin conjugades sota el grup $GL(N, R)$ de matrius $N \times N$ invertibles sobre R .

Demostració. Si $u \in GL(N, R)$ i $upu^{-1} = q$, aleshores el producte per la dreta induïx un isomorfisme de $R^N q$ a $R^N p$, per tant la condició és suficient. Per a provar que la condició és necessària suposem que p i q són matrius de mida $n \times n$ i $m \times m$ respectivament, i que $R^n p \cong R^m q$. Podem estendre aquest isomorfisme $\alpha : R^n p \rightarrow R^m q$ a un homomorfisme de R -mòduls $R^n \rightarrow R^m$ a partir de prendre $\alpha = 0$ en el complementari del mòdul $R^n(1-p)$, i veure la imatge de $R^m q$ incrustada a R^m . Similarment extenem α^{-1} a un homomorfisme de R -mòduls $\beta : R^m \rightarrow R^n$ el qual pren valors 0 sobre $R^m(1-q)$. Aleshores α ve donada per la multiplicació per la dreta per una matriu a de mida $n \times m$ i β ve donada per multiplicar per la dreta per una matriu b de mida $m \times n$. A més, tenim les relacions $ab = p$, $ba = q$, $a = pa = aq$, $b = qb = bp$. La gràcia de la prova consisteix en prendre $N = n + m$ i notar que

$$\begin{pmatrix} 1-p & a \\ b & 1-q \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

²Useu l'abreviatura R -m.p.f.g. per a referir-nos a R -mòduls projectius finitament generats.

complint la conjugació

$$\begin{pmatrix} 1-p & a \\ b & 1-q \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1-p & a \\ b & 1-q \end{pmatrix} = \begin{pmatrix} 1-p & a \\ b & 1-q \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & q \end{pmatrix}.$$

per tant $\begin{pmatrix} 1-p & a \\ b & 1-q \end{pmatrix}$ és una matriu de $GL(N, R)$ que conjuga $p \oplus 0$ amb $0 \oplus q$, finalment i per acabar observem que $0 \oplus q$ és conjugat de $q \oplus 0$ a partir de la matriu permutació. \square

Ara estem en condicions de descriure $\text{Proj } R$.

Definició 2.2.1. Sigui R un anell, deontem $M(n, R)$ a la col·lecció de matrius $n \times n$ sobre un anell R i $GL(n, R)$ al grup de matrius invertibles $n \times n$ sobre R . Incrustem $M(n, R)$ a $M(n+1, R)$ a partir de $a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ i incrustem $GL(n, R)$ a $GL(n+1, R)$ a partir de l'homomorfisme de grups $a \mapsto \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. Denotem per $M(R)$ i $GL(R)$ la unió infinita dels grups $M(n, R)$ i $GL(n, R)$ respectivament, observem que tota matriu d'aquests grups té una mida finita. Denotarem $\text{Idem } R$ al conjunt de matrius idempotents a $M(R)$, a més, observem que $GL(R)$ actua a $\text{Idem } R$ per conjugació com hem vist al Lema anterior.

Teorema 2.2.2. Per a tot anell R , podem identificar $\text{Proj } R$ com el conjunt d'òrbites de l'acció de $GL(R)$ a $\text{Idem } R$. L'operació de semigrup és induïda per $(p, q) \mapsto \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}$. Per tant $K_0(R)$ és el grup de Grothendieck d'aquest semigrup.

Per acabar veiem que K_0 és invariant sota el pas de R a $M_n(R)$ i un Corol·lari del Teorema anterior que ens serà molt útil per a calcular K -grups.

Teorema 2.2.3 (Invariància de Morita). Per a tot anell R i tot enter positiu n hi ha un isomorfisme natural

$$K_0(R) \longleftrightarrow K_0(M_n(R)).$$

Demostració. Usant la identificació $M_k(M_n(R))$ amb $M_{kn}(R)$, tenim que

$$\text{Idem}(M_n(R)) = \text{Idem}(R) \text{ i } GL(M_n(R)) = GL(R).$$

Per tant aquest resultat és un corol·lari del Lema anterior. \square

Corol·lari 2.2.1. Donats dos anells R_1 i R_2 ,

$$K_0(R_1 \times R_2) \cong K_0(R_1) \oplus K_0(R_2).$$

Demostració. Usant la identificació $M_{2n}(R)$ amb $M_n(R) \times M_n(R)$ tenim que

$$\text{Idem}(R_1 \times R_2) = (R_1) \times \text{Idem}(R_2)$$

, a més, $GL(R_1 \times R_2) = GL(R_1) \times GL(R_2)$ actua per conjugació sobre aquest semigrup, per tant $\text{Proj}(R_1 \times R_2) \cong \text{Proj } R_1 \times \text{Proj } R_2$, i per tant

$$K_0(R_1 \times R_2) \cong K_0(R_1) \oplus K_0(R_2).$$

Aquest raonament es pot generalitzar per a productes finits. \square

2.3 El cas d'un cos

En aquesta secció estudiarem K_0 sobre un cos i notarem el motiu pel qual restringim la definició de K_0 sobre mòduls projectius finitament generats.

Proposició 2.3.1. *Si R és un cos, $K_0(R) \cong \mathbb{Z}$.*

Demostració. Si R és un cos tot R -m.p.f.g. és un R -espai vectorial, i per tant té una base i una dimensió ben definides. De fet, la dimensió és l'únic isomorfisme invariant del mòdul, per tant tenim $\text{Proj } R \cong \mathbb{N}$, considerat com el monoide additiu dels nombres naturals. Com que la completió (grup de Grothendieck) del semigup \mathbb{N} és \mathbb{Z} , tenim $K_0(R) \cong \mathbb{Z}$. \square

Observació. El mateix argument de la prova anterior mostra que $K_0(R) \cong \mathbb{Z}$ si R és un anell de divisió.

Observació. Si R és un cos i en lloc de calcular el grup de Grothendieck de $\text{Proj } R$ calculem el grup de Grothendieck del monoide format per les classes d'isomorfisme dels mòduls projectius **numerablement generats**, amb el mateix argument que el de la prova anterior tenim que aquest monoide és isomorf a $\mathbb{N} \cup \infty$, amb la norma habitual $n + \infty = \infty$ per a tot n . Observem en aquest monoide no es compleix la propietat cancel·lativa, de fet dos elements qualsevols esdevenen isomorfs si sumem ∞ a cada banda. Per tant el grup de Grothendieck d'aquest monoide és trivial. Així doncs és raonable usar només mòduls **finitament generats** per definir K_0 .

De fet podem generalitzar l'observació anterior sobre un anell R qualsevol.

Proposició 2.3.2 ("Eilenberg swindle"). *Si R és un anell, el grup de Grothendieck del semi-grup de les classes d'isomorfia dels R -mòduls projectius numerablement generats desapareix, i.e., és trivial.*

Demostració. Si R^∞ és un mòdul lliure infinitament generat numerablement i P és un mòdul projectiu tal que $P \oplus Q \cong R^n$, per commutativitat de la suma directa es compleix $Q \oplus P \cong R^n$. Així doncs tenim

$$P \oplus R^\infty \cong P \oplus (Q \oplus P) \oplus (Q \oplus P) \dots \cong (P \oplus Q) \oplus (P \oplus Q) \dots \cong R^\infty.$$

A més si $P \oplus R^m \cong R^\infty$, amb $m \neq \infty$, aleshores $P \cong R^\infty$. També es compleix la propietat $R^\infty \cong R^\infty \oplus R^\infty$.

Així doncs, $P \oplus R^\infty \cong R^\infty \oplus R^\infty$ implica que per a qualsevol parella d'elements del semi-grup existeix un element (R^∞) que els fa isomorfs, per tant el grup de Grothendieck ha de ser trivial. \square

2.4 El cas dels DIPs

En aquesta secció estudiarem K_0 sobre un domini d'ideals principals, en particular veurem que té sentit el concepte de dimensió en els R -mòduls sobre DIPs, i presentarem el grup K_0 reduït.

Definició 2.4.1. Un *DIP* (**domini d'ideals principals**) és un domini d'integritat (anell sense divisors de zero) commutatiu en el que tot ideal és generat per un únic element.

Teorema 2.4.1. *Si R és un DIP, tot submòdul d'un R -m.ll.f.g. és lliure, a més és isomorf a R^n per a un únic n , anomenarem a aquest N rang del mòdul.*

Demostració. Sigui M un R -m.l.f.g., podem assumir que existeix un enter n tal que M estigui inclòs a R^n .

Usarem inducció sobre n per a veure que si M està inclòs a R^n , M és isomorf a R^k per algun $k < n$. El cas $n = 0$ es compleix, assumim cert per a valors més petits que n , comprovem que és cert per a n .

Sigui $\pi : R^n \rightarrow R$ la projecció a la darrera coordenada, observem que π envia M a un R -submòdul de R , i.e., un ideal. Si $\pi(M) = 0$ podem veure M inclòs a $\ker \pi \cong R^{n-1}$ i usar la hipòtesi d'inducció. En cas contrari $\pi(M)$ és un ideal no nul, a més és principal, ja que R és un DIP i per tant és isomorf a R com a R -mòdul.³ Aleshores M és isomorf a $\ker \pi|_M \oplus R$. Com que $\ker \pi|_M$ ha d'estar inclòs a R^{n-1} podem aplicar la hipòtesi d'inducció per afirmar que és isomorf a $R^{k'}$ per $k' \leq n-1$. Per tant $M \cong R^k$ amb

$$k = k' + 1 \leq (n-1) + 1 = n.$$

D'altra banda, observem que si K és el cos de fraccions de R , podem caracteritzar n com la dimensió de l'espai vectorial format pel K -mòdul $K \otimes_R M$, d'aquí es dedueix la unicitat de n . □

Corol·lari 2.4.1. Si R és un DIP, tot R -m.p.f.g. és isomorf a R^n per a un únic n .

Observació. 2.4.1 Usant la functorialitat del grup de Grothendieck, tenim que si R és un DIP, el rang dels R -mòduls definit al Teorema 2.4.1 induïx un isomorfisme $K_0(R) \leftrightarrow \mathbb{Z}$.

$$\begin{array}{ccc} \mathbb{N} & \xleftarrow{\gamma} & \text{Proj } R \\ \downarrow \pi & & \downarrow \pi' \\ \mathbb{Z} & \xleftarrow{\quad} & K_0(R) \end{array}$$

Observació. Per a tot anell R podem definir l'homomorfisme d'anells $\iota : \mathbb{Z} \rightarrow R$ definit per enviar 1 a 1_R . Tenint en compte que \mathbb{Z} és un DIP i aplicant el Corol·lari 2.4.1 es dedueix $K_0(\mathbb{Z}) \cong \mathbb{Z}$. Usant la functorialitat de K_0 tenim que existeix una aplicació induïda $\iota_* : \mathbb{Z} \rightarrow K_0(R)$. La imatge de ι_* és el subgrup de $K_0(R)$ generat pels R -m.l.f.g.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\iota} & R \\ \downarrow \pi & & \downarrow \pi' \\ K_0(\mathbb{Z}) \cong \mathbb{Z} & \xrightarrow{\iota_*} & K_0(R) \end{array}$$

Definició 2.4.2. Donat un anell R definim el K_0 **grup reduït** per

$$\tilde{K}_0(R) := K_0(R) / \iota_*(\mathbb{Z})$$

En general $\tilde{K}_0(R)$ mesura la part no òbvia de $K_0(R)$, de moment hem vist que $\tilde{K}_0(R)$ desapareix si R és un anell de divisió o un DIP.

2.5 El cas dels anells locals

En aquesta secció presentem el concepte d'anell local amb alguns exemples i algunes de les seves propietats fonamentals que ens permetran calcular K_0 per aquesta estructura algebraica.

³Si α és un generador de l'ideal principal $\pi(M) = \{\alpha r; r \in R\}$, considera l'homomorfisme $f : R \rightarrow \pi(M)$ donat per $1 \mapsto \alpha$, és homomorfisme ja que $f(m+n) = \alpha(m+n) = \alpha m + \alpha n = f(m) + f(n)$, és injectiu gràcies a que R és un domini, i és exhaustiu per construcció.

Definició 2.5.1. Un anell R , no necessàriament commutatiu, és **local** si els elements no invertibles de R formen un ideal propi bilàter M de R .

Proposició 2.5.1. Un anell R és local si i només si R té un únic ideal maximal per l'esquerra, i un únic ideal maximal per la dreta, i aquests coincideixen.

Demostració. Veiem primer (\Rightarrow), si R és local i M és el seu ideal d'elements no invertibles, no pot existir cap ideal per l'esquerra (o dreta) propi que tingui algun element de $R \setminus M$, ja que l'ideal generat per un element invertible és tot l'anell R , per tant M és l'únic ideal maximal per l'esquerra (o dreta). Veiem ara (\Leftarrow), donat un $x \in R$, si x no té inversa per l'esquerra tenim que Rx és un ideal per l'esquerra propi, aquest ideal propi ha d'estar contingut en algun ideal maximal per l'esquerra, i per hipòtesi aquest ideal és únic. Similarment si x no té inversa per la dreta pertany a un ideal maximal únic per la dreta. La hipòtesi de coincidència ens permet afirmar que l'ideal d'elements invertibles és bilàter. \square

Corol·lari 2.5.1. En un anell local, si un element té inversa per un costat, és invertible.

Demostració. Suposem que en un anell local existeix un element x diferent de zero que té inversa per la dreta i no per l'esquerra, per una banda al tenir inversa per la dreta x no pot pertànyer a cap ideal propi per la dreta. D'altra banda, com que x té inversa per l'esquerra x pertany a un ideal propi per l'esquerra. Usant la Proposició 2.5.1, tenim que $x \in M$ i $x \notin M$. \square

Proposició 2.5.2. Sigui p un nombre primer i $k > 0$, aleshores l'anell $\mathbb{Z}/(p^k\mathbb{Z})$ és local.

Demostració. Un ideal és en particular un subgrup, els subgrups de $\mathbb{Z}/p^k\mathbb{Z}$ són de la forma $p^{k'}\mathbb{Z}/p^k\mathbb{Z}$ amb $0 \leq k' \leq k$. Per tant tots els ideals de $\mathbb{Z}/p^k\mathbb{Z}$ són principals, a més, el seu únic ideal maximal és $p\mathbb{Z}/p^k\mathbb{Z}$, usant la Proposició 2.5.1 tenim que és un anell local. \square

Proposició 2.5.3. Per a tot cos K , i tot $p(x) \in K[x]/(x^n)$, $p(x)$ és invertible si i només si $p(0) \neq 0$.

Demostració. En primer lloc observem que tots els elements de $K[x]/(x^n)$ són de la forma

$$a_0 + a_1y + a_2y^2 + \dots + a_ny^{n-1},$$

on $y = x + (x^n)$. A més, observem que per a tot $n_1, n_2 \in \mathbb{N}$, $y^{n_1}y^{n_2} = y^{n_1+n_2}$ si $n_1+n_2 < n$, i en cas contrari $y = (x^n)$. Observem que en particular, y és un element nilpotent, i.e. $y^n = 0 + (x^n)$. Feta aquesta observació, comencem la prova.

Donat un $p(x)$ tal que $p(0) \neq 0$, per l'observació anterior tenim que té inversa. D'altra banda, si $p(x)$ és invertible i $p(0) = 0$, existeix una expressió de la forma

$$p(x) = a_1y + \dots + a_{n-1}y^{n-1},$$

per tant podem expressar $p(x)$ com a combinació lineal d'elements nilpotents, i usant el Teorema del binomi tenim que $p(x)$ és nilpotent. Tanmateix si $p(x)$ és nilpotent no pot ser invertible, provant l'altra implicació. \square

Corol·lari 2.5.1. $p(x) \in K[x]/(x^n)$ és un anell local.

Demostració. Per la Proposició 2.5.3 tenim que els elements no invertibles són els que compleixen $p(0) = 0$, en particular formen un ideal bilàter. \square

Definició 2.5.2. Per a qualsevol anell R anomenem **radical** (o radical de Jacobson) de R a la intersecció dels ideals maximals per l'esquerra. Per la Proposició 2.5.1, en un anell local el radical coincideix amb l'ideal maximal, i.e., l'ideal format pels elements no invertibles de R .

Proposició 2.5.4. Per a qualsevol anell R el seu radical és un ideal bilàter.

Demostració. És suficient veure que $\text{rad } R = \bigcap_{I \text{ ideal max. per l'esquerra}} \text{Ann}_R(R/I)$ ⁴ ja que l'anul·lador és un ideal bilàter i intersecció d'ideals bilàters és un ideal bilàter. Per a veure (\supset) observem que donat un ideal maximal per l'esquerra I , l'anul·lador de R/I clarament està contingut a I , per tant

$$\bigcap_{I \text{ ideal max. per l'esquerra}} \text{Ann}_R(R/I) \subset \bigcap_I I = \text{rad } R$$

Per a veure (\subset) usem el fet que

$$\text{Ann}_R(R/I) = \bigcap_{\dot{x} \in R/I, \dot{x} \neq 0} \text{Ann}_R(\dot{x}),$$

i.e., l'anul·lador de R/I és intersecció d'ideals maximals per l'esquerra. \square

Observació. Tenint en compte la prova anterior i usant que tot R -mòdul simple és isomorf a un quocient R/m on m és un ideal maximal de R (es poden veure tots els detalls d'aquest resultat a [8]), tenim que $\text{rad } R$ és el conjunt d'elements que anul·len tots els R -mòduls simples. A més, com que tot mòdul simple per $M_n(R)$ és isomorf a un de la forma $R^n \otimes_R M$ on M és un R -mòdul simple, tota matriu amb entrades a $\text{rad } R$ ha d'anul·lar tots aquests mòduls, i per tant pertany al radical de $M_n(R)$.

Corol·lari 2.5.2. Si R és un anell local, $R/\text{rad } R$ és un anell de divisió⁵. Si R és commutatiu, $R/\text{rad } R$ és un cos.

Demostració. En primer lloc observem que l'anell quocient està ben definit gràcies a la Proposició 2.5.4. Usant la Proposició 2.5.1 tenim que $\text{rad } R$ és maximal, com que el quocient d'un anell per un ideal maximal ha de ser un anell simple, $R/\text{rad } R$ és simple (un anell és simple si és un anell no nul que no té més ideals bilàters que el zero i ell mateix), de fet en el cas commutatiu és un cos. A més, tot element no zero ha de tenir inversa gràcies al fet que $\text{rad } R$ en el cas dels anells locals és l'ideal format pels elements no invertibles de R . \square

Proposició 2.5.5. Per un anell R , $\text{rad } R = \{x \in R : \forall a \in R, 1 - ax \text{ té inversa per l'esquerra}\}$

Demostració. Veiem primer (\subset), si x pertany a tot ideal maximal per l'esquerra, aleshores Rx ha de pertànyer a tot ideal maximal per l'esquerra⁶. Suposem que existeix un $a \in R$ tal que $1 - ax$ no tingui inversa. Aleshores $1 - ax$ ha de pertànyer a un ideal propi, i per tant en un ideal maximal per l'esquerra. Com que $ax \in M$ tenim que $1_R \in M$, que contradiu que M sigui maximal⁷. Per a veure (\supset), suposem que per a tot $a \in R$, $1 - ax$ té inversa per l'esquerra. Sigui M un ideal maximal per l'esquerra, si $x \notin M$, aleshores $Rx + M = R$. Per tant per algun $a \in R$, $1 - a \in M$, fet que contradiu que $1 - a$ tingui inversa per l'esquerra. \square

⁴ $\text{Ann}_R(S) = \{r \in R \mid \forall s \in S, rs = 0\}$.

⁵ R és de divisió si és un anell no zero en que tot element diferent de zero és invertible, i.e., per a tot element $x \in R$ amb $x \neq 0_R$ existeix un $a \in R$ tal que $a \cdot x = x \cdot a = 1_R$.

⁶La intersecció d'ideals per l'esquerra és un ideal per l'esquerra.

⁷Un ideal maximal ha de ser propi.

Proposició 2.5.6. *Per un anell R el radical coincideix amb la intersecció dels ideals maximals per la drete.*

Demostració. Podem definir el radical per la drete de la següent forma:

$$r\text{-rad } R = \bigcap \text{ideals max. per la drete} = \{x \in R : \forall a \in R, 1 - xa \text{ té inversa per la drete}\}$$

Anem a provar que $\text{rad } R \subset r\text{-rad } R$, l'altre inclusió és simètrica. Usant la Proposició 2.5.4 tenim que $\text{rad } R$ és un ideal per la drete, per tant si $x \in \text{rad } R$, per a tot $a \in R$ tenim que $xa \in \text{rad } R$. Aplicant la Proposició 2.5.5 sobre xa i usant el fet que per a tot element $b \in R$ existeix un $c \in R$ tal que $(1 - c)b = 1$ ($c := 1 - b$) tenim que si $x \in \text{rad } R$ i $a \in R$, existeix un $c \in R$ tal que $(1 - c)(1 - xa) = 1$, d'aquí es dedueix $-c - xa = -cxa$, i aquesta igualtat dóna lloc a $(1 - xa)(1 - c) = 1 + xac - cxa$. Observem que $1 + xac - cxa$ ha de tenir una inversa per l'esquerra, ja que $x \in \text{rad } R$ i $xac - cxa \in \text{rad } R$. Per tant, $(1 - c)$ té una inversa per l'esquerra, a més, com que $(1 - xa)$ és una inversa per la drete, i les inverses han de coincidir⁸, $1 - xa$ també és inversa per l'esquerra, i per tant $1 - xa$ és invertible amb inversa $1 - c$. Així doncs $\text{rad } R \subset r\text{-rad } R$. \square

Teorema 2.5.1 (Lema de Nakayama). *Suposem que R és un anell i M és un R -m.f.g tal que $(\text{rad } R)M = M$. Aleshores $M = 0$.*

Demostració. Si $M \neq 0$, considerem un conjunt de generadors $x_1, \dots, x_m \in M$ amb m tan petit com sigui possible. Observem que per construcció s'ha de complir $x_j \neq 0$, ja que si existís algun $x_j = 0$, m no seria tan petita com seria possible. Per hipòtesi tenim que $(\text{rad } R)M = M$, usant aquesta hipòtesi i el conjunt generador x_1, \dots, x_m , tenim que existeixen $r_1, \dots, r_m \in \text{rad } R$, tal que $x_m = r_1x_1 + \dots + r_mx_m$. D'aquí es dedueix

$$(1 - r_m)x_m = r_1x_1 + \dots + r_{m-1}x_{m-1}.$$

Usant la Proposició 2.5.5 tenim que $(1 - r_m)$ és invertible i en conseqüència podem expressar x_m com a combinació lineal de x_1, \dots, x_{m-1} , i per tant m no és mínim, contradicció. \square

Corol·lari 2.5.3. *Si R és un anell, M un R -m.f.g. i $x_1, \dots, x_m \in M$, aleshores x_1, \dots, x_m generen M si i només si les imatges $\dot{x}_1 \dots \dot{x}_m$ generen $M/(\text{rad } R)M$ com a $R/\text{rad } R$ -mòdul.*

Demostració. Si x_1, \dots, x_m generen M és trivial veure que $\dot{x}_1, \dots, \dot{x}_m$ generen $M/\text{rad } R)M$. Veiem la implicació no trivial, sigui $N = M/(\sum_i Rx_i)$, tenim que

$$N/\text{rad } R)N = M/(\text{rad } RM + (\sum_i Rx_i)) = M/M = 0,$$

per tant $\text{rad } R)N = N$. Aplicant ara la proposició anterior tenim que $N = 0$, i en conseqüència $M = (\sum_i Rx_i)$. \square

Teorema 2.5.2. *Si R és un anell local, no necessàriament commutatiu, aleshores tot R -m.p.f.g. és lliure amb un rang unívocament determinat. En particular $K_0(R) \cong \mathbb{Z}$ i té per element generador la classe de mòduls de rang 1.*

⁸El fet que les inverses coincideixin és fruit de l'associativitat de R , sigui $x \in R$ un element que té $y \in R$ per inversa per l'esquerra i $z \in R$ per inversa per la drete, per una banda tenim $(yx)z = z$, d'altra banda $y(xz) = y$, per tant $y = z$, i.e., la inversa per la drete coincideix amb la inversa per l'esquerra.

Demostració. Pel Corol·lari 2.5.2 tenim que $D := R/\text{rad } R$ és un anell de divisió, recorda que tot anell de divisió és un DIP. Si M és un R -m.p.f.g podem assumir $M \oplus N = R^k$ per algun k . Aleshores $M/(\text{rad } R)M$ i $N/(\text{rad } R)N$ són D -mòduls, usant el Teorema 2.4.1 tenim que són lliures. Si denotem per m i n als seus respectius rangs cal que es compleixi $m + n = k$. Així doncs podem triar elements bàsics d'aquests mòduls i tiar-los enrere de forma que tinguem $x_1, \dots, x_m \in M$ i $x_{m+1}, \dots, x_k \in N$. Pel Corol·lari 2.5.3, aquests elements generen R^k . Falta veure que x_1, \dots, x_k són una base de R^k . Això mostrarà en particular que x_1, \dots, x_m són un conjunt generador de M linealment independent, per tant M és lliure amb un rang inequívocament determinat

$$\text{rank } M = \dim_D M/(\text{rad } R)M.$$

Sigui e_1, \dots, e_k una base estàndard de R^k . Com que tenim dos conjunts generadors de R^k , cada conjunt generador pot ser expressat en termes de l'altre, i.e., existeixen elements $a_{ij}, b_{ij} \in R$ amb

$$e_i = \sum_{j=1}^k a_{ij} x_j, \quad x_i = \sum_{j=1}^k b_{ij} e_j$$

Per tant tenim

$$e_i = \sum_{j=1}^k a_{ij} \sum_{l=1}^k b_{jl} e_l,$$

i consegüentment

$$\sum_{j=1}^k \sum_{l=1}^k (a_{ij} b_{jl} - \delta_{il}) e_l = 0,$$

i si $A = (a_{ij})$, $B = (b_{ij})$, significa que, com que els e_l són linealment independents, $AB = I$. Amb una substitució simètrica tenim

$$\sum_{j=1}^k \sum_{l=1}^k (b_{ij} a_{jl} - \delta_{il}) x_l = 0,$$

i com que els x_l són linealment independents mòdul el radical de R , usant l'observació que precedeix la Proposició 2.5.4 tenim que $BA - I \in M_n(\text{rad } R) \subset \text{rad } M_n(R)$. Per la proposició 2.5.5, BA és invertible, per tant B és invertible. Com que A era inversa per l'esquerra de B , això mostra que també és inversa per la dreta, i.e., $BA = I$. Provant que x_1, \dots, x_m és una base de R^k \square

2.6 El grup K_0 relatiu i el Teorema d'Excisió

El primer objectiu d'aquesta secció és definir el grup relatiu $K_0(R, I)$ i trobar la successió exacta que relaciona $K_0(R)$ amb $K_0(R/I)$, aquesta successió l'extendrem en el següent capítol i ens permetrà calcular K -grups. El segon objectiu d'aquesta secció és provar un anàleg de l'axioma de l'excisió de teoria de la homologia, de fet durant aquesta secció es pot veure que hi ha cert paral·lelisme entre la teoria de la homologia i K -teoria algebraica; aquest anàleg ens permetrà definir $K_0(I)$ on I és un anell sense necessitat de tenir element unitat, i veurem la relació entre $K_0(I)$ i el K_0 relatiu.

Per a trobar una successió exacta que relacioni $K_0(R/I)$ i $K_0(R)$ necessitem saber que és una successió exacta.

Definició 2.6.1. Diem que una successió de grups i homomorfismes de grups

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} \dots \xrightarrow{f_n} G_n$$

és **exacta** si la imatge de cada homomorfisme és igual al nucli del següent, i.e., $\text{im}(f_k) = \ker(f_{k+1})$. Aquesta successió d'homomorfismes i grups pot ser finita o infinita. En particular ens interessen les successions **exactes i curtes**, que són successions de la forma:

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0,$$

una successió exacta curta ha de complir que f sigui un *monomorfisme*⁹ i g un *epimorfisme*¹⁰. Una successió exacta és **escindida** si és curta i existeix un homomorfisme $h : C \rightarrow B$ tal que $g \circ h$ sigui la identitat sobre C .

Introduïm ara els conceptes necessaris per definir $K_0(R/I)$.

Definició 2.6.2. Sigui R un anell i $I \subset R$ un ideal (en aquesta secció els ideals sempre seran bilàters). El **doblet d'un anell** R sobre I és el subanell del producte cartesià $R \times R$ donat per

$$D(R, I) = \{(x, y) \in R \times R : x - y \in I\}$$

Observació. Si $p_1 : D(R, I) \rightarrow R$ és la projecció a la primera coordenada, podem identificar I com a $\ker p_1$, per tant existeix una successió exacta curta

$$0 \rightarrow I \rightarrow D(R, I) \xrightarrow{p_1} R \rightarrow 0,$$

a més si definim $h : R \rightarrow R \times R$ a l'assignació diagonal $x \mapsto (x, x)$, tenim que $p_1 \circ h$ és la identitat a C , i per tant la successió exacta escindeix.

Definició 2.6.3. El grup K_0 -relatiu d'un anell R i un ideal I ve definit per

$$K_0(R, I) = \ker((p_1)_*) : K_0(D(R, I)) \rightarrow K_0(R).$$

Un fenomen íntimament relacionat amb l'estudi de K-teoria relativa és el fet que tota matriu sobre R/I pot ser pujada a una matriu sobre R ; tanmateix una matriu invertible no sempre pot ser pujada a una matriu invertible.

Lema 2.6.1. Sigui R un anell i $I \subset R$ un ideal.

Aleshores si $A \in GL(n, R/I)$, $\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix} \in GL(2n, R/I)$ puja a una matriu $GL(2n, R)$.

Demostració. En primer lloc, observem que es compleix

$$\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix} = \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -A^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad (2.1)$$

La prova consisteix a constatar que cada matriu del producte de la factorització anterior puja a una matriu invertible. En concret la matriu $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ clarament puja a una matriu invertible. Siguin $B, C \in M_n(R)$ les preimatges de les matrius A i A^{-1} respectivament; B i C no són necessàriament invertibles, però les matrius

⁹Un monomorfisme és un homomorfisme injectiu.

¹⁰Els epimorfismes són homomorfismes exhaustius.

$$\begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix} i \begin{pmatrix} 1 & 0 \\ -C & 1 \end{pmatrix}$$

sí que ho són. □

Teorema 2.6.2. *Sigui R un anell i $I \subset R$ un ideal. Aleshores existeix una successió exacta curta*

$$K_0(R, I) \rightarrow K_0(R) \xrightarrow{q_*} K_0(R/I)$$

on q_* és induïda per l'aplicació quocient $q : R \rightarrow R/I$ i l'aplicació $K_0(R, I) \rightarrow K_0(R)$ és induïda per $p_2 : D(R, I) \rightarrow R$ (la projecció a la segona component).

Demostració. Per simplicitat si A és un element de R o una matriu amb entrades a R , sovint denotarem $q(A)$, la matriu corresponent amb entrades sobre R/I , per \dot{A} .

En primer lloc volem veure que la imatge de la primera aplicació està continguda en el nucli de la segona. Sigui $[e] - [f] \in K_0(R, I)$, on $e = (e_1, e_2)$, $f = (f_1, f_2) \in \text{Idem}(D(R, I))$. Usant el Corol·lari 2.2.1 tenim que $K_0(R \times R) \cong K_0(R) \times K_0(R)$, aleshores la imatge de $[e] - [f]$ és $([e_1] - [f_1], [e_2] - [f_2])$, per tant

$$q_* \circ (p_2)_*([e] - [f]) = q_*([e_2] - [f_2]) = [\dot{e}_2] - [\dot{f}_2],$$

mentre que $[e_1] - [f_1] = 0$, ja que per hipòtesi $[e] - [f] \in \ker(p_1)_*$. Però com que $e, f \in \text{Idem } D(R, I)$, $\dot{e}_1 = \dot{e}_2$ i $\dot{f}_1 = \dot{f}_2$. Per tant

$$[\dot{e}_2] - [\dot{f}_2] = [\dot{e}_1] - [\dot{f}_1] = q_*([e_1] - [f_1]) = 0$$

Per tant la imatge de la primera aplicació està continguda al nucli de la segona. Veiem ara el recíproc; siguin $e, f \in \text{Idem}(R)$ dels que $q_*([e] - [f]) = 0$. Aleshores existeix un r prou gran tal que

$$\dot{e} \oplus \dot{1}_r = q(e \oplus 1_r) \sim \dot{f} \oplus \dot{1}_r = q(f \oplus 1_r)$$

a $GL(R/I)$. Canviant e per $e \oplus 1_r$ i f per $f \oplus 1_r$, podem assumir que \dot{e} i \dot{f} són conjugades, i.e., existeix una matriu $\dot{g} \in GL(R)$ tal que $\dot{f} = \dot{g}\dot{e}(g)^{-1}$. Observem que la matriu $\dot{g} \oplus (\dot{g})^{-1}$ conjugua $\dot{e} \oplus \dot{0}$ a $\dot{f} \oplus \dot{0}$, i usant el Lema 2.6.1 puja a una matriu $h \in GL(R)$. Per tant podem canviar f per $f \oplus 0$ i e per $h(e \oplus 0)h^{-1}$ sense canviar $[e]$ i $[f]$, i reduir-nos al cas en que $\dot{e} = \dot{f}$. Així doncs $(e, f) \in \text{Idem}(D(R, I))$. Aleshores la imatge de la classe $[(e, e)] - [(e, f)] \in K_0(D(R, I))$ és 0 per $(p_1)_*$ i $[e] - [f]$ per $(p_2)_*$. □

Ara veurem que té sentit definir K_0 sobre un anell sense unitat, a més veurem que el grup relatiu $K_0(R, I)$ és isomorf a $K_0(I)$, on I és un anell sense unitat.

Definició 2.6.4. Sigui I un anell que no tingui necessàriament element unitat. Anomenem **anell obtingut al afegir un element unitat a I** a el grup abelià $I \oplus \mathbb{Z}$ amb el producte definit per

$$(x, n) \cdot (y, m) = (xy + ny + mx, mn),$$

$x, y \in I$; $m, n \in \mathbb{Z}$. Aquest anell el denotarem I_+ . Notem que l'element $(0, 1) \in I_+$ és el seu element unitat.

Observació. Si $\alpha : I \rightarrow I'$ és un homomorfisme de la categoria d'anells sense unitat, llavors α estén a un únic homomorfisme d'anells amb unitat $I_+ \xrightarrow{\alpha_+} I'_+$. Observem que en el cas que I tingui element unitat, existeix un isomorfisme unitari¹¹ $\alpha : I_+ \rightarrow I \times \mathbb{Z}$ definit

¹¹Una aplicació es unitària si envia la imatge de l'element unitat és element unitat. En aquest cas $\alpha(0, 1) = (e, 1)$.

per

$$\alpha(x, n) = (x + ne, n),$$

ja que

$$\begin{aligned} \alpha((x, n) \cdot (y, m)) &= \alpha(xy + ny + mx, mn) \\ &= (xy + ny + mx + mne, mn) \\ &= (x + ne, n) \cdot (y + me, m) \\ &= \alpha(x, n) \cdot \alpha(y, m) \end{aligned}$$

Definició 2.6.5. Sigui I un anell el que no tingui necessàriament element unitat. Llavors existeix una successió exacta curta escindida

$$0 \rightarrow I \rightarrow I_+ \xrightarrow{\rho} \mathbb{Z} \rightarrow 0. \quad (2.2)$$

on ρ està definida per $\rho(x, n) = n$. En aquest context definim

$$K_0(I) := \ker(\rho_* : K_0(I_+) \rightarrow K_0(\mathbb{Z}) \cong \mathbb{Z}).$$

Pot semblar que la definició és ambigua, ja que si I té unitat hem donat dues definicions diferents de $K_0(I)$. En aquest cas veiem que les definicions són coincidents, ja que si I té unitat.

$$I_+ \cong I \times \mathbb{Z},$$

i usant l'observació anterior $K_0(I_+) \cong K_0(I) \oplus K_0(\mathbb{Z})$, i $\ker \rho_*$ només està format per elements del primer sumand. Per tant la nova definició coincideix amb l'anterior.

Teorema 2.6.3 (Excisió). Si I és un ideal bilàter en un anell R , aleshores $K(R, I) \cong K_0(I)$ (i per tant no depèn de R , només en l'estructura de I com a anell sense unitat).

Demostració. Definim l'homomorfisme unitari

$\gamma : I_+ \rightarrow D(R, I)$ per

$$(x, n) \mapsto (n \cdot 1, n \cdot 1 + x),$$

amb $x \in I$, $n \in \mathbb{Z}$, observem que el diagrama commuta.

Per tant $\gamma_* : K_0(I_+) \rightarrow K_0(D(R, I))$ envia $\ker \rho_*$ a $\ker(p_1)_*$, i.e., envia $K_0(I)$ a $K_0(R, I)$.

$$\begin{array}{ccc} I_+ & \xrightarrow{\gamma} & D(R, I) \\ \rho \downarrow & & \downarrow p_1 \\ \mathbb{Z} & \xrightarrow{\iota} & R \end{array}$$

. Per a veure que l'aplicació és exhaustiva considerem una classe classe $[e] - [f] \in K_0(R, I)$, on $e = (e_1, e_2)$, $f = (f_1, f_2) \in \text{Idem}(D(R, I))$ i $[e_1] = [f_1]$ a $K_0(R)$. A partir de canviar e i f per $e \oplus 1_r$ i $f \oplus 1_r$ respectivament per a una r prou gran, podem assumir que e_1 i f_1 són conjugats a $GL(R)$, i.e., existeix una matriu invertible g tal que $e_1 = gf_1g^{-1}$. Així doncs si canviem (f_1, f_2) per (gf_1g^{-1}, gf_2g^{-1}) podem assumir que $f_1 = e_1$. D'altra banda si e és una matriu $s \times s$, podem canviar e i f per $e \oplus (1_s - e_1, 1_s - e_1)$ i $f \oplus (1_s - e_1, 1_s - e_1)$ respectivament, obsevem que hi ha una matriu invertible h de mida $2s \times 2s$ amb entrades a R que conjugua $e_1 \oplus (1_s - e_1)$ i $1_s \oplus 0_s$. Conjugant-ho tot per h ens reduim en el cas on $e = (1_s \oplus 0_s, e_2)$, $f = (1_s \oplus 0_s, f_2)$, a més, com que e i f són matrius sobre $D(R, I)$, $e_2 - (1_s \oplus 0_s)$ i $f_2 - (1_s \oplus 0_s)$ tenen entrades a I . Així doncs observem que $[e] - [f]$ és la imatge de $K_0(I)$.

Falta veure que γ_* és injectiva, tot element de $K_0(I)$ pot ser expressat com $[e] - [f]$,

on $e, f \in \text{Idem}(I_+)$ i $\text{rank } \rho(e) = \text{rank } \rho(f)$. De la mateixa forma que a la prova de l'exhaustivitat, a partir de prendre suma directa amb $1_r - f$ i conjugar podem assumir que $f = 1_r$, $\text{rank } \rho(e) = r$. A més podem assumir que $g\rho(e)g^{-1} = 1_r$ per algún $g \in GL(\mathbb{Z})$. Considerant g com un element de $GL(I_+)$ via la successió exacta escindida (2.2) podem reemplaçar e per geg^{-1} i assumir que $\rho(e) = 1_r$. Ara si $\gamma_*([e] - [1_r]) = 0$ significa que

$$[(1_r, e)] = [(1_r, 1_r)] \text{ a } K_0(D(R, I)).$$

Si és necessari podem estabilitzar a través d'augmentar r i assumir que existeix una matriu $(g_1, g_2) \in GL(D(R, I))$ amb

$$g_1 1_r g_1^{-1} = 1_r, \quad g_2 e g_2^{-1} = 1_r.$$

Aleshores $(1, g_1^{-1} g_2) \in GL(D(R, I))$ i

$$((g_1^{-1} g_2) e (g_1^{-1} g_2)^{-1}) = g_1^{-1} (g_2 e g_2^{-1}) g_1 = g_1^{-1} 1_r g_1 = 1_r.$$

Com que $g_1^{-1} g_2 \cong 1 \pmod{I}$, $g_1^{-1} g_2$ pertany a $GL(I_+)$ i això significa que $[e] - [1_r] = 0$ a $K_0(I)$, i per tant el nucli γ_* és trivial. \square

Capítol 3

Construcció del Grup K_1

En àlgebra lineal es comença estudiant espais vectorials i la seva dimensió, i es procedeix amb l'estudi de les transformacions lineals i els seus invariants, com el determinant, les formes canòniques...

Similarment en K -teoria algebraica comencem estudiant mòduls projectius i la seva classificació a K_0 , i continuem estudiant la classificació d'automorfismes de mòduls lliures i projectius, i.e., invariants de matrius invertibles.

Així doncs, la relació entre K_0 i K_1 és la mateixa que hi ha entre transformacions lineals invertibles i els espais vectorials.

De la mateixa forma que un homomorfisme $K_0(R) \rightarrow G$ correspon a la generalització del concepte de rang, un homomorfisme de grups $K_1(R) \rightarrow G$ correspon a generalitzar el determinant de matrius invertibles sobre R .

L'objectiu d'aquest capítol és definir el grup K_1 a partir de matrius sobre un anell R i obtenir alguns resultats que ens facilitin el càlcul del grup $K_0(R)$, la construcció exposada segueix en gran part [1], també presentem resultats i observacions interessants de [2] i la resolució de part dels problemes plantejats a [1], com el càlcul de K_1 per a $\mathbb{Z}/(m)$, $K[x]$ i \mathbb{H} .

A la secció on estudiem el cas dels quaternions, cal mencionar que per a la introducció a l'anell dels quaternions hem usat [3], també hem usat [4] i [5] per a introduir el determinant de Dieudonné.

Començarem per definir K_1 a través de matrius invertibles sobre un anell R , estudiarem el cas d'un cos i intentarem generalitzar el mateix resultat per a anells de divisió, anells locals i dominis euclidiàns. També calculem K_1 d'alguns anells interessants, en particular hem dedicat una secció al càlcul de $K_1(\mathbb{H})$, ja que no només uso els resultats de les seccions anteriors, sinó que també presento el determinant de Dieudonné per al càlcul de $K_1(R)$. Finalment definirem el grup relatiu $K_1(R, I)$ que ens permetrà formular una successió exacta que relaciona K_0 i K_1 proveint-nos de més eines per al càlcul de K -grups.

3.1 Definició de K_1

Definició 3.1.1. Sigui R un anell (amb unitat), anomenarem **matriu elemental**, i la denotem per $e_{ij}(a)$, a la matriu $n \times n$ formada per 1_R 's a la diagonal, $a \in R$ a la posició (i, j) , on $i \neq j$, $1 \leq i, j \leq n$, i 0_R 's a la resta d'entrades.

Observació. Les matrius elementals són invertibles, en concret $e_{ij}(a)^{-1} = e_{ij}(-a)$, per tant són elements de $GL(n, R)$, i a més generen un subgrup que denotarem $E(n, R)$. A partir de la incrustació usual de $GL(n, R)$ a $GL(n+1, R)$ presentada a la Definició 2.2.1,

podem incrustar $E(n, R)$ a $E(n+1, R)$. La unió finita dels $E(n, R)$ és denotada per $E(R)$ i usualment s'anomena **grup de matrius elementals**.¹

Observació. Tota matriu elemental es pot expressar com $e_{ij}(r) = I_n + r\epsilon_{ij}$, on ϵ_{ij} és la matriu amb 1 a la posició (i, j) i zeros a la resta. Observem que el producte compleix

$$\epsilon_{ij}\epsilon_{kl} = \begin{cases} 0 & \text{si } j \neq k \\ \epsilon_{il} & \text{si } j = k. \end{cases}$$

Usant les matrius elementals podem causar una de les tres transformacions elementals usades en el mètode de reducció de Gauss, en concret

$$e_{ij}(r)(A) = (I + r\epsilon_{ij}) \sum_{k,l} a_{kl}\epsilon_{kl} = \sum_{k,l} a_{kl}\epsilon_{kl} + \sum_l r a_{jl}\epsilon_{il} = \sum_{k \neq i} \sum_l a_{kl}\epsilon_{kl} + \sum_l (a_{il} + r a_{jl})\epsilon_{il}$$

i.e., multiplicar $e_{ij}(r)$ per l'esquerra de A equival a sumar r vegades la fila j a la fila i de la matriu A . Les altres dues transformacions elementals usades en el mètode de Gauss també es poden expressar com a producte de matrius, en concret multiplicar $P_{i,j}$ per l'esquerra d' A

$$P_{i,j} = I_n - \epsilon_{ii} - \epsilon_{jj} + \epsilon_{ij} + \epsilon_{ji}$$

canvia de posició les files i i j de la matriu A , i finalment si $u \in R^x$, el producte de $d_i(u)$ per l'esquerra de A multiplica la fila i -èsima d' A per u .

$$d_i(u) = I_n + (u-1)\epsilon_{ii}$$

Així doncs, les tres transformacions usades en el mètode de Gauss es poden expressar com a producte de matrius invertibles, però només una d'aquestes tres pertany a $E(R)$, a més, només la primera deixa el determinant invariant, per aquest motiu $E(R)$ està íntimament relacionat amb $K_1(R)$.

Lema 3.1.1. *Les matrius triangulars superiors (i triangulars inferiors) sobre un anell R amb 1's a la diagonal pertanyen a $E(R)$.*

Demostració. Sigui $A = (a_{i,j}) \in GL(n, R)$ una matriu triangular superior amb zeros a la diagonal, aleshores

$$A' = (a'_{i,j}) = A_{12}(-a_{12})e_{23}(-a_{23}) \dots e_{n-1,n}(-a_{n-1,n})$$

és una matriu triangular superior amb 1's a la diagonal i zeros a la diagonal secundària superior. Similarment

$$A'' = (a''_{i,j}) = A' e_{13}(-a'_{13})e_{24}(-a'_{24}) \dots e_{n-2,n}(-a'_{n-2,n})$$

és triangular superior amb 1's a la diagonal i zeros a la primera i segona diagonals secundàries superiors. Continuant el procés per inducció construïm una successió

$$A, A', A'', \dots, A^{(n-1)}$$

de matrius a $GL(n, R)$, on per construcció la matriu $A^{(k)}$ és una matriu $(n \times n)$ triangular superior amb 1's a la diagonal i zeros a $a_{ij}^{(k)}$ amb $0 < j - i \leq k$. En particular $A^{(n-1)}$ és

¹Observem que el grup de matrius elementals és un abús de notació. Ens permetem aquest abús de notació, entenent que el grup de matrius elementals és la unió finita de tants $E(n, R)$ com ens convingui.

la matriu identitat $n \times n$, a més cada matriu de la successió s'obté multiplicant la matriu anterior per una matriu de $E(n, R)$. Per tant existeix una matriu $B \in E(n, R)$ tal que

$$A = A^{(n-1)}B = B \in E(n, R),$$

tal com volíem. Un raonament similar es pot usar per al cas diagonal inferior. \square

Corol·lari 3.1.1. *Segui $A \in GL(n, R)$, la matriu $2n \times 2n \begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix}$ pertany a $E(2n, R)$.*

Demostració. Recordant la prova del Lema 2.6.1 tenim

$$\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix} = \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -A^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad (3.1)$$

aplicant el Lema 3.1.1 tenim que les primeres tres matrius del costat dret de la igualtat anterior pertanyen a $E(2n, R)$. Per a veure que la darrera matriu també hi pertany, veiem que ve generada per matrius elementals:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

\square

Definició 3.1.2. Seguin x i y dos elements d'un grup G , definim el **commutador de la parella d'elements** com $[x, y] := xyx^{-1}y^{-1}$. Observem que $[x, y]^{-1} = [y, x]$, i per tant, el producte finit de commutadors $[x, y]$ amb $x, y \in G$ formen un subgrup de G , el denotem per $[G, G]$ i s'anomena **subgrup commutador** de G . A més es compleix $z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}]$ i per tant $[G, G]$ és un subgrup normal de G . Usant aquest fet podem definir el quocient

$$G_{ab} = G/[G, G],$$

que s'anomena grup abelianitzat de G .

Proposició 3.1.1. *Donat un grup G , el grup abelianitzat G_{ab} és abelià, de fet, és el quocient abelià maximal de G , i.e., si $H \triangleleft G$ i G/H és abelià aleshores H conté $[G, G]$.²*

Demostració. La commutativitat del grup és deguda a

$$[x[G, G], y[G, G]] = [x, y][G, G] = [G, G].$$

D'altra banda si $H \triangleleft G$ i G/H és abelià, aleshores per a tot $x, y \in G$, $[x, y]H = [xH, yH] = H$ a G/H . Per tant $[G, G] \subseteq H$. \square

Observació. Les matrius elementals sobre un anell R compleixen la propietat

$$e_{ik}(a)e_{kj}(b)e_{ik}(a)^{-1}e_{kj}(b)^{-1} = e_{ij}(ab), \quad (3.2)$$

per a i, j, k diferents entre si.

Proposició 3.1.2 (Lema de Whitehead). *Segui R un anell,*

$$[GL(R), GL(R)] = [E(R), E(R)] = E(R).$$

²De fet, el recíproc també és cert, [2] Proposició 9.2.

Demostració. En primer lloc observem que usant l'observació anterior tenim

$$e_{ij}(a) = [e_{ik}(a), e_{kj}(1)]$$

per i, j i k diferents, i.e., cada generador de $E(R)$ és el commutador de dos elements generadors, per tant $[E(R), E(R)] = E(R)$.

D'altra banda, com que $E(R) \subseteq GL(R)$, $[E(R), E(R)] \subseteq [GL(R), GL(R)]$. Veiem ara el recíproc, siguin $A, B \in GL(n, R)$. Podem incrustar $GL(n, R)$ a $GL(2n, R)$ i calcular

$$\begin{pmatrix} ABA^{-1}B^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & B^{-1}A^{-1} \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} B^{-1} & 0 \\ 0 & B \end{pmatrix}$$

Usant el Corol·lari 3.1.1, totes les matrius del costat dret de la igualtat pertanyen a $E(2n, R)$, per tant

$$ABA^{-1}B^{-1} \in E(R)$$

□

Definició 3.1.3. Sigui R un anell amb unitat, denotarem per $K_1(R)$ el **grup abelianitzat** $GL(R)_{\text{ab}} = GL(R)/E(R)$.

Observació. Si $\varphi : R \rightarrow S$ és un homomorfisme d'anells $\varphi : R \rightarrow S$, indueix una aplicació al grup de matrius invertibles de $GL(R)$ a $GL(S)$, i aquest indueix un homomorfisme de $K_1(R)$ a $K_1(S)$. Per tant $R \rightsquigarrow K_1(R)$ és un functor entre la categoria d'anells a la de grups abelians.

Podem identificar $K_1(R)$ com el grup de les formes canòniques, sota les transformacions elementals per files i columnes, de matrius invertibles sobre R . En particular, si $K_1(R)$ és trivial significa que tota matriu invertible pot ser reduïda per files i columnes a la matriu identitat.

Observació. Donades dues matrius invertibles sobre un anell $A, B \in GL(R)$, podem expressar el producte de les classes $[A], [B] \in R$ de la forma intuïtiva $[A] \cdot [B] = [AB]$, tanmateix aquest producte també es pot expressar com $A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ ja que aplicant el Corol·lari 3.1.1 sobre la igualtat

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} B^{-1} & 0 \\ 0 & B \end{pmatrix}$$

dóna lloc a la igualtat

$$[A \oplus B] = [AB \oplus 1] = [AB]$$

Proposició 3.1.3. Siguin R_1 i R_2 anells, aleshores

$$K_1(R) \cong K_1(R_1) \times K_2(R_2).$$

Demostració. Observem que existeix un isomorfisme $GL(R_1 \times R_2) \cong GL(R_1) \times GL(R_2)$ definit per

$$((a_{ij}, b_{ij})) \mapsto ((a_{ij}), (b_{ij})).$$

Aleshores

$$e_{ij}((r, s)) \mapsto (e_{ij}(r_1), e_{ij}(r_2)),$$

i per tant l'isomorfisme envia $E(R_1 \times R_2)$ a $E(R_1) \times E(R_2)$; a més $(e_{ij}(r_1), e_{ij}(r_2))$ generen $E(R_1) \times E(R_2)$ i per tant hi ha un isomorfisme induït

$$K_1(R_1 \times R_2) \cong \frac{GL(R_1) \times GL(R_2)}{E(R_1) \times E(R_2)} \cong K_1(R_1) \times K_1(R_2)$$

definit per

$$(a_{ij}, b_{ij})E(R_1 \times R_2) \mapsto ((a_{ij})E(R_1), (b_{ij})E(R_2)).$$

□

Proposició 3.1.4 (Invariància de Morita sobre K_1). *Per a tot anell R*

$$K_1(R) \cong K_1(M_n(R)).$$

Demostració. L'isomorfisme ve induït per l'isomorfisme $GL(R) \cong GL(M_n(R))$. □

En el cas que R sigui commutatiu, el concepte de determinant està ben definit, a més, ens interessaran particularment les matrius amb determinant unitari.

Definició 3.1.4. Si R és commutatiu, denotarem les matrius de $GL(n, R)$ amb determinant 1 per $SL(n, R)$, i a les de $GL(R)$ per $SL(R)$. Observem que tota matriu elemental té determinant 1, i per tant té sentit definir el quocient $SL(R)/E(R)$ que el denotarem $SK_1(R)$.

Observació. Si R és un anell commutatiu, els homomorfismes

$$\begin{aligned} \det : GL_n(R) &\rightarrow R^\times \\ \det : GL(R) &\rightarrow R^\times \\ \overline{\det} : K_1(R) &\rightarrow R^\times \end{aligned}$$

tenen per núclis $SL_n(R)$, $SL(R)$ i $SK_1(R)$ respectivament.

Proposició 3.1.5. *Si R és un anell commutatiu, existeix una successió exacta curta*

$$1 \rightarrow SK_1(R) \rightarrow K_1(R) \rightarrow R^\times \rightarrow 1$$

A més, existeix un homomorfisme $s_1 : R^\times \rightarrow K_1(R)$ de forma que la successió és escindida.

Demostració. Observem que $\det(A \oplus 1) = \det(A)$, per tant els determinants de $GL(n, R)$ són compatibles amb les incrustacions de $GL(n, R)$ dins $GL(m, R)$ amb $n < m$.

Com que $\det(AB) = \det(A)\det(B)$, obtenim un homomorfisme $GL(R) \rightarrow R^\times$ el qual ha de factoritzar a través de $GL(R)_{ab}$. Per tant el determinant i la incrustació $s : GL(1, R) \rightarrow R$ donen lloc a dues successions escindides:

$$\begin{array}{ccccccc} 1 & \longrightarrow & SL(R) & \xrightarrow{\subseteq} & GL(R) & \xrightarrow{\det} & R^\times \longrightarrow 1 \\ & & & & \downarrow \pi & \swarrow s & \parallel \\ 1 & \longrightarrow & SK_1(R) & \xrightarrow{\subseteq} & K_1(R) & \xrightarrow{\overline{\det}} & R^\times \longrightarrow 1 \\ & & & & & \nwarrow \bar{s} & \end{array}$$

□

Corol·lari 3.1.2. *Si R un anell commutatiu. Si $SK_1(R)$ és trivial, $\det : K_1(R) \rightarrow R^\times$ és un isomorfisme.*

3.2 El cas d'un cos

Proposició 3.2.1. *Si F és un cos, aleshores $SK_1(F)$ és trivial. És a dir, el determinant induïx un isomorfisme $\det : K_1(F) \rightarrow F^\times$.*

Demostració. La prova consisteix en explicitar un procés en el que tota matriu $A \in SL(n, F)$ sigui transformada a la matriu identitat usant transformacions elementals de $E(R)$.

Si l'entrada de la posició $(1, 1)$ de la matriu A és diferent de zero podem procedir al següent pas, si és nul·la necessitem col·locar un element no nul en aquesta posició. Sabem que a la primera fila de la matriu A ha d'existir un element no nul (ja que és invertible), suposem sense pèrdua de generalitat que $a_{i1} \neq 0$. Aleshores multiplicant A per $e_{1i}(1)e_{i1}(-1)e_{1i}(1)$ forcem que la matriu resultant tingui un element no nul a la posició $(1, 1)$.

Per tant podem assumir que $a_{11} \neq 0$. Sumant la primera fila multiplicada per $-a_{i1}a_{11}^{-1}$ a la fila i -èsima ($i = 2 \dots n$), podem forçar que la primera columna de la matriu A tingui zeros a totes les entrades excepte la primera.

Així doncs estem en el cas reduït en que A és de la forma $\begin{pmatrix} a_{11} & * \\ 0 & A' \end{pmatrix}$ on A' és una matriu $(n-1) \times (n-1)$ i $\det(A) = a_{11} \det(A')$. Repetint el mateix procediment per A' obtenim

$$\begin{pmatrix} a_{11} & * & * \\ 0 & a_{22} & * \\ 0 & 0 & A'' \end{pmatrix}$$

on A'' és una matriu $(n-2) \times (n-2)$. Repetint el procés per inducció tenim que A pot ser transformada a una matriu invertible triangular-superior.

Donada una matriu triangular superior A si afegim múltiples de la darrera fila a les altres podem forçar zeros a tots els elements de la darrera columna excepte a_{nn} , similarment afegint múltiples de la fila $(n-1)$ a les altres files podem forçar zeros a totes les entrades de la columna $(n-1)$ excepte $a_{n-1,n-1}$. Continuant per inducció podem reduir mitjançant transformacions elementals la matriu A en una matriu diagonal invertible D , amb determinant 1.

Usant el Corol·lari 3.1.1 tenim que la matriu

$$\text{diag}(1, \dots, 1, a, a^{-1}, 1, \dots, 1),$$

on $a \in R$, és una matriu elemental, multiplicant tantes vegades com sigui necessari (com a molt $n-1$ vegades) per aquest tipus de matrius transformem qualsevol matriu diagonal amb determinant 1 a la identitat.

Amb el mateix procediment si en lloc de prendre $A \in SL(n, F)$ prenem $A \in GL(n, F)$ tenim que tota matriu invertible es pot transformar en una matriu de la forma $\text{diag}(a, \dots, 1, \dots, 1)$ mitjançant transformacions elementals. \square

3.3 El cas dels anells de divisió

El problema que neix al intentar estendre el resultat de cossos a anells de divisió rau en que el determinant no està ben definit si R no és commutatiu.

Proposició 3.3.1. *Si R és un anell de divisió, la inclusió*

$$R^\times \rightarrow GL(1, R) \hookrightarrow GL(R)$$

indueix una aplicació exhaustiva $R_{ab}^\times \twoheadrightarrow K_1(R)$.

Demostració. Usant el procediment de la prova anterior tenim que tota matriu $GL(n, R)$ pot ser transformada a partir de transformacions elementals per files en una matriu diagonal de la forma $\text{diag}(a, 1, \dots, 1)$. En altres paraules, pot ser transformada a la imatge de $GL(1, R)$ dins $GL(n, R)$. Com que $K_1(R)$ és abelià, l'aplicació exhaustiva $R^x \twoheadrightarrow K_1(R)$ factoritza a través de $R_{ab}^x = R^x / [R^x, R^x]$. \square

3.4 El cas dels anells locals

Proposició 3.4.1. *Si R és un anell local (no necessàriament commutatiu), la inclusió $R^x = GL(1, R) \hookrightarrow GL(R)$ induïx una aplicació exhaustiva $R_{ab}^x \rightarrow K_1(R)$.*

Demostració. A la prova anterior només usàvem que R es un anell de divisió al requerir que totes les files d'una matriu $A = (a_{ij}) \in GL(n, R)$ hagin de contenir almenys un element invertible, en el cas dels anells locals aquesta propietat no és trivial. Tanmateix es segueix complint, ja que si la fila i -èssima d'una matriu $A \in GL(n, R)$ té una fila on totes les seves entrades són elements no invertibles (i.e., pertanyen a l'ideal rad R), per a tota matriu $B \in GL(n, R)$ es compleix que totes les entrades de la fila i -èssima de la matriu AB són elements no invertibles, i per tant A no pot ser invertible, en contradicció amb el fet que $A \in GL(n, R)$. \square

Teorema 3.4.1. *Sigui R un anell local no necessàriament commutatiu, aleshores existeix una única aplicació "determinant": $GL(R) \rightarrow R_{ab}^x$ amb les següents propietats:*

- a) *El determinant és invariant sota operacions elementals per files, en altres paraules, si $A \in GL(n, R)$ i A' és la matriu resultant de A a través d'afegir un múltiple per l'esquerra d'una fila a una altra, aleshores $\det(A') = \det(A)$.*
- b) *El determinant de la matriu identitat és 1.*
- c) *Si $A \in GL(n, R)$, $a \in R^x$, i A' és la matriu obtinguda a partir de multiplicar per a una de les files de A , aleshores $(\bar{a})(\det A)$, on \bar{a} és la imatge de a a R_{ab}^x .*
- d) *Si $A, B \in GL(n, R)$, aleshores $\det(AB) = (\det A)(\det B)$.*
- e) *Si $A \in GL(n, R)$ i si A' es obtingut a partir de A intercanviant dues files, aleshores $\det A' = (-1)(\det A)$.*
- f) *El determinant d'una matriu i la seva transposta sempre és el mateix.*

Demostració. La prova consisteix en diferents parts, començarem per demostrar la unicitat. Després veurem que (d-f) són conseqüència de (a-c), i finalment definirem per inducció sobre n l'aplicació determinant, veurem que està ben definida i que compleix (a-c) per a tot n , també veurem que el determinant és compatible amb la incrustació de $GL(n, R)$ a $GL(R)$.

Així doncs comencem veient la unicitat, usant la prova de la Proposició 3.4.1 tenim que tota matriu de $GL(n, R)$ es pot diagonalitzar a través de transformacions elementals per files a una matriu de la forma $\text{diag}(a, 1, \dots, 1)$. Aleshores, usant (a) tenim que

$$\det A = \det(\text{diag}(a, 1, \dots, 1)),$$

a més, usant (b) i (c) respectivament tenim

$$\text{diag}(a, 1, \dots, 1) = \bar{a} \det 1 = \bar{a}.$$

Per tant les propietats (a)-(c) assignen el valor del determinant.

Veiem (d) com a conseqüència de (a-c), sigui $E \in E(n, R)$ la matriu elemental tal que $EA = \text{diag}(a, 1, \dots, 1)$, aleshores per (a) tenim que $\det(A) = \bar{a}$. D'altra banda si també usem (c) tenim

$$\det AB = \det((EA)B) = \bar{a}(\det B) = (\det A)(\det B)$$

la qual cosa prova (d). Per a veure (e) observem que per a tota matriu invertible $A \in GL(n, R)$ amb $i < j \leq n$, la permutació entre les files i - j es pot fer a partir de multiplicar per la matriu elemental $e_{ij}(1)e_{ji}(-1)e_{ij}(1)$ i després multiplicar la fila i -èsima per -1 . Per tant (e) és conseqüència de (a) i (c). Per a veure (f), en primer lloc observem que usant (b) i (a) tenim que les matrius elementals tenen determinant 1, i usant (d) tenim que tota matriu de $E(R)$ té determinant 1. D'altra banda considera l'aplicació $\det' : A \mapsto \det(A^t)$; aquesta aplicació clarament compleix (b), a més, la transposada d'una matriu elemental és elemental, i per tant \det' sobre les matrius elementals també és 1. Com que \det' pren valors sobre el grup abelianitzat, tenim que

$$\det'(AB) = \det((AB)^t) = \det(B^t A^t) = \det(B^t) \det(A^t) = \det'(B) \det'(A) = \det'(A) \det'(B),$$

i per tant (d) es compleix sobre \det' i en particular tota matriu de $E(R)$ té determinant 1.

$$\det(\text{diag}(1, \dots, 1, a, 1, \dots, 1)) = \bar{a}$$

Aleshores, com que \det' val 1 sobre $E(R)$ i \bar{a} sobre $\text{diag}(1, \dots, 1, a, 1, \dots, 1)$ tenim que \det' compleix les propietats (a) i (c). Usant la unicitat de l'aplicació determinant tenim que $\det' = \det$, provant (f).

Ara definirem el determinant $\det_n(A)$ per $A \in GL(n, R)$ per inducció sobre n , de tal manera que $\det_{n+m}(A \oplus 1_m) = \det_n A$, i per tant puguem estendre la definició a $GL(R)$. Si $n = 1$ definim $\det a := \bar{a}$, clarament es compleixen les propietats (a)-(c), suposem ara per hipòtesi d'inducció que el determinant \det_k existeix per a $k < n$ de tal manera que es segueixin complint les propietats (a)-(c). Hem de veure que \det_k està definit i compleix les propietats (a)-(c).

Sigui $A \in GL(n, R)$, denotarem les files de A per A_1, \dots, A_n , també denotarem per b_1, \dots, b_n a les entrades de la primera fila de la matriu A^{-1} . Aleshores com que $A^{-1}A = 1_n$ tenim la següent relació

$$b_1 A_1 + \dots + b_n A_n = (1 \ 0 \dots 0).$$

En particular, si denotem $A_j = (a_{j1} B_j)$, on $B_j \in R^{n-1}$, aleshores $\sum_j b_j B_j = 0$.

Pel mateix argument usat a la prova de la Proposició 3.4.1 no pot passar que la primera fila de A^{-1} no tingui cap element invertible; suposem sense pèrdua de generalitat que i és la posició on hi ha un d'aquests elements invertibles i aleshores es compleix

$$b_i^{-1} b_1 B_1 + \dots + b_i^{-1} b_{i-1} B_{i-1} + B_i + b_i^{-1} b_{i+1} B_{i+1} + \dots + b_i^{-1} b_n B_n = 0.$$

Per tant afegint múltiples de les altres files a A_i i usant la propietat:

$$a_{i1} + \sum_{j \neq i} b_i^{-1} b_j a_{j1} = b_i^{-1} \sum_j b_j a_{j1} = b_i^{-1}$$

podem reduir per files la matriu A a la següent forma:

$$\begin{pmatrix} a_{11} & B_1 \\ \vdots & \vdots \\ a_{i-1,1} & B_{i-1} \\ \bar{b}_i^{-1} & 0 \\ a_{i+1,1} & B_{i+1} \\ \vdots & \vdots \\ a_{nn} & B_n \end{pmatrix}$$

aleshores prenem com a definició

$$\det_n(A) := (-1)^{i-1} \bar{b}_i^{-1} \det_{n-1} \begin{pmatrix} B_1 \\ \vdots \\ \hat{B}_i \\ \vdots \\ B_n \end{pmatrix} \quad (3.3)$$

Cal veure que està ben definit, és a dir hem de veure que el determinant és independent de l'elecció de l'element invertible de la primera fila de A^{-1} que usem per a crear una fila de zeros, i.e.,

$$(-1)^i \bar{b}_i^{-1} \det_{n-1} C_i \stackrel{?}{=} (-1)^j \bar{b}_j^{-1} \det_{n-1} C_j, \quad (3.4)$$

on

$$C_i = \begin{pmatrix} B_1 \\ \vdots \\ \hat{B}_i \\ \vdots \\ B_n \end{pmatrix}, C_j = \begin{pmatrix} B_1 \\ \vdots \\ \hat{B}_j \\ \vdots \\ B_n \end{pmatrix}$$

Observem que a partir de C_i podem obtenir la matriu C_j aplicant permutacions per files i després canviar B_j per B_i . El procediment per a realitzar aquestes transformacions consisten en permutar les files (B_{i+1}, \dots, B_j) , i.e., requereix un total de $j - i - 1$ canvis de files, que dóna lloc a la següent matriu

$$C = \begin{pmatrix} B_1 \\ \vdots \\ B_{i-1} \\ B_j \\ B_{i+1} \\ \vdots \\ \hat{B}_j \\ \vdots \\ B_n \end{pmatrix}.$$

Usant el fet que $B_i = -\bar{b}_i^{-1} b_j B_j +$ (una combinació lineal de files) i aplicant les propietats (a) i (c) de la hipòtesi d'inducció tenim per una banda que

$$\det_{n-1} C_j = -\bar{b}_i^{-1} \bar{b}_j \det_{n-1} C$$

i per l'altra

$$\det_{n-1} C = (-1)^{j-i-1} \det_{n-1} C_i.$$

Aleshores usant aquests dos darrers resultats es comprova que (3.4) es satisfà, i per tant el determinant està ben definit.

Falta veure que el \det_n compleix les propietats (a)-(c). Per començar, (b) és certa per definició, per a veure (a) suposem que A' és friut d'una transformació elemental per files de la matriu A , i.e., té per files A'_1, \dots, A'_n amb $A'_j = A_j$ si $j \neq i$ i $A'_i = a_i + aA_k$, on $a \in R^\times$ i $i \neq k$. Aleshores existeix una matriu elemental tal que $A' = e_{ik}(a)A$, per tant $(A')^{-1} = A^{-1}e_{ik}(-a)$ i en particular els elements b'_1, \dots, b'_n de la primera fila de $(A')^{-1}$ són els mateixos que b_1, \dots, b_n excepte per $b'_k = b_k - b_i a$. Si $b_j \in R^\times$ per algun $j \neq k$ aleshores tenim

$$\det_n A' = (-1)^{j-1} \bar{b}_j^{-1} \det_{n-1} \begin{pmatrix} B_1 \\ \vdots \\ B_{i-1} \\ B_i + aB_k \\ B_{i+1} \\ \vdots \\ \hat{B}_j \\ \vdots \\ B_n \end{pmatrix}$$

i aplicant (a) per a \det_{n-1} tenim $\det_n A' = \det_n A$. Falta considerar el cas en què b_k i $b'_k = b_k - b_i a$ són ambdós invertibles i $b_i \in \text{rad } R$ per $i \neq k$. En aquest cas

$$\det_n A' = (-1)^{k-1} \bar{b}_k^{-1} \det_{n-1} \begin{pmatrix} B_1 \\ \vdots \\ \hat{B}_k \\ \vdots \\ B_n \end{pmatrix},$$

com que $\bar{b}'_k = \bar{b}_k$ (ja que $b_i a \in \text{rad } R$), i per tant $\det_n A' = \det_n A$.

Així doncs hem comprovat que (a) es compleix, veiem ara (c), sigui A' la matriu resultant de multiplicar la fila A_i de A per $a \in R$, i.e., A' és la matriu que té per files A'_1, \dots, A'_n amb $A'_j = A_j$ per a tot $j \neq i$ i $A'_i = aA_i$ per a $a \in R^\times$. Aleshores existeix una matriu diagonal $d_i(a)$ formada per 1's a la diagonal excepte a la posició (i, i) que té per valor a , tal que $A' = d_i(a)A$. Per tant $A^{-1} = A^{-1}d_i(a^{-1})$ i en particular els elements b_1, \dots, b_n de la primera fila de A^{-1} són els mateixos que $b_1 \dots b_n$ excepte per $b_i = b_i a^{-1}$. Així doncs tenim de nou dos casos a considerar.

Si $b_j \in R^\times$ per $j \neq i$, aleshores tenim

$$\det_n A' = (-1)^{j-1} \bar{b}_j^{-1} \det_{n-1} \begin{pmatrix} B_1 \\ \vdots \\ B_{i-1} \\ aB_i \\ B_{i+1} \\ \vdots \\ \hat{B}_j \\ \vdots \\ B_n \end{pmatrix},$$

i aplicant (c) per \det_{n-1} , tenim que $\det_n A' = \bar{a} \det_n A$. Falta doncs considerar el cas en que b_i és invertible i tots els altres b_j no ho són, i.e., $b_j \in \text{rad } R$ per $j \neq i$, en aquest com que $\bar{b}'_i = \bar{b}_i \bar{a}^{-1}$ tenim

$$\det_n A' = (-1)^{j-1} (\overline{b'_j a^{-1}})^{-1} \det_{n-1} \begin{pmatrix} B_1 \\ \vdots \\ \hat{B}_i \\ \vdots \\ B_n \end{pmatrix} = (-1)^{j-1} (\bar{b}'_j)^{-1} \det_{n-1} \begin{pmatrix} B_1 \\ \vdots \\ \hat{B}_i \\ \vdots \\ B_n \end{pmatrix} = \det_n A$$

i per tant (c) es compleix.

Per acabar la prova, observem que una matriu de la forma $B \oplus 1$ pot ser transformada a $1 \oplus B$ a partir de $2(n-1)$ permutacions per files i columnes, amb $B \in GL(n-1, R)$. Usant (e) tenim que $\det_n(B \oplus 1) = \det_n(1 \oplus B) = \det_{n-1} B$. \square

Corol·lari 3.4.1. Si R és un anell local, no necessàriament commutatiu, aleshores el determinant definit al Teorema 3.4.1 induïx un isomorfisme

$$K_1(R) \cong R_{ab}^\times$$

Demostració. El resultat és conseqüència de la Proposició 3.4.1 i el Teorema 3.4.1, ja que

$$GL(1, R) \hookrightarrow GL(R) \xrightarrow{\det} R_{ab}^\times$$

és l'aplicació quotient $R^\times \rightarrow R_{ab}^\times$. \square

Ara veurem exemples de càlcul del grup K_1 .

Proposició 3.4.2. Per a tot $m > 0$

$$K_1(\mathbb{Z}/(m)) \cong \left(\frac{\mathbb{Z}}{p_1^{k_1} \mathbb{Z}} \right)^\times \times \cdots \times \left(\frac{\mathbb{Z}}{p_n^{k_n} \mathbb{Z}} \right)^\times,$$

on els p_i són fruit de la descomposició en producte de factors primers de m usant el Teorema xinès del residu.

Demostració. Usant el Teorema xinès del residu tenim que

$$\frac{\mathbb{Z}}{m\mathbb{Z}} \cong \frac{\mathbb{Z}}{p_1^{k_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_n^{k_n}\mathbb{Z}}$$

Aleshores usant la Proposició 3.1.3 obtenim

$$K_1(\mathbb{Z}/(m)) \cong K_1(\mathbb{Z}/p_1^{k_1}) \times \cdots \times K_1(\mathbb{Z}/p_n^{k_n})$$

Usant la proposició 2.5.2 tenim que $\mathbb{Z}/m\mathbb{Z}$ descompon en producte cartesià d'anells locals, a més són abelians, i per tant aplicant el Corol·lari 3.4.1 tenim que

$$K_1(\mathbb{Z}/(m)) \cong \left(\frac{\mathbb{Z}}{p_1^{k_1}\mathbb{Z}} \right)^\times \times \cdots \times \left(\frac{\mathbb{Z}}{p_n^{k_n}\mathbb{Z}} \right)^\times$$

□

Veiem ara un altre exemple d'anell local i calculem el seu grup K_1 .

Proposició 3.4.3.

$$K_1(K[x]/(x^n)) \cong \{a_1y + \cdots + a_{n-1}y^{n-1} \in K[x]; y = x + (x^n)\}$$

Demostració. Conseqüència dels Corol·laris 3.4.1, 2.5.1 i del fet que $K[x]/(x^n)$ és abelià ja que K és un cos. □

3.5 El cas dels Quaternions

L'objectiu d'aquesta secció és calcular $K_1(\mathbb{H})$. Començarem per a definir els quaternions, descriure les propietats fonamentals i en particular la norma de quaternions.

Després introduïrem el concepte de matriu unitària i el grup $SU(2)$ per a veure que $\ker N = [\mathbb{H}, \mathbb{H}]$ (on N és la norma dels quaternions), aquest resultat ens permetrà deduir per factorització de N que $\mathbb{H}_{ab}^\times \cong \mathbb{R}_+^\times$.

Finalment, observarem que amb els resultats ja introduïts podríem computar $K_1(\mathbb{H})$, no obstant introduïrem el determinant de Dieudonné, que ens permetrà computar K_1 a través del fet que les matrius elementals sobre els quaternions $E(\mathbb{H})$ són exactament el grup de matrius (invertibles) amb determinant 1.

Definició 3.5.1. L'àlgebra dels **quaternions** \mathbb{H} és un espai vectorial real de dimensió quatre amb base $1, i, j, k$:

$$\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

on el producte compleix les relacions:

$$ij = k, jk = i, ki = j, i^2 = j^2 = k^2 = -1.$$

En particular, \mathbb{H} no és un cos, tot i que només falla la commutativitat, per exemple

$$ij = k \neq ji = -k$$

Donat un quaternió $z = (a + bi + cj + dk) \in \mathbb{H}$ definim el seu **conjugat** com

$$\bar{z} = a - bi - cj - dk,$$

Per tant, podem caracteritzar els reals com $\mathbb{R} = \{q \in \mathbb{H} : \bar{q} = q\}$, definim la **part real** d'un quaternió per $\text{Re}(z) = z - \bar{z}$. En interessaran en particular els quaternions amb part real nul·la, que anomenarem **quaternions purs**. Ens interessa el fet que tot quaternió pot ser escrit com a producte de dos quaternions purs, els conjunt dels quaternions purs formen el conjunt

$$\{z \in \mathbb{H} : \text{Re}(z) = 0\} = \{z \in \mathbb{H} : z = bi + cj + dk \ \forall b, c, d \in \mathbb{R}\} \cong \mathbb{R}^3$$

La conjugació compleix que per a tot $p, q \in \mathbb{H}$

$$\overline{pq} = \bar{q}\bar{p}.$$

Una aplicació que prendrà rellevància és la **norma** $N(z) = z\bar{z} \in \mathbb{R}$, es comprova que $N(z) = a^2 + b^2 + c^2 + d^2$, per tant $N(z) \geq 0$ on la igualtat es compleix si i només si $z = 0$. Es pot comprovar que per a tot $p, q \in \mathbb{H}$

$$N(pq) = N(p)N(q)$$

Per a tot $z \in \mathbb{H} \setminus \{0\}$ tenim que $N(z)^{-1}\bar{z}$ és el seu invers, i.e., $\mathbb{H}^\times = \mathbb{H} - \{0\}$, així doncs \mathbb{H} no és un cos però és un anell de divisió.

La norma

$$N : \mathbb{H} \rightarrow \mathbb{R}_+^\times$$

és un homomorfisme del grup \mathbb{H}^\times al grup \mathbb{R}_+^\times , prenen ambdós casos el producte com a operació.

A més

$$\ker N = \{q \in \mathbb{H}^\times : z\bar{z} = 1\} = \{z \in \mathbb{H} : a^2 + b^2 + c^2 + d^2 = 1\},$$

podem identificar $\ker N$ amb $S^3 \subset \mathbb{R}^4$, per tant existeix una successió exacta curta:

$$1 \rightarrow S^3 \hookrightarrow \mathbb{H}^\times \twoheadrightarrow \mathbb{R}_+^\times \rightarrow 1 \quad (3.5)$$

A partir de (3.5) tenim que $[\mathbb{H}^\times, \mathbb{H}^\times] \subset \ker N$, volem veure l'altra inclusió, és a dir, volem veure que el commutador de \mathbb{H}^\times és exactament $\ker N$. En veure aquest fet tindrem que $\mathbb{H}_{ab}^\times \cong \mathbb{R}_+^\times$

Definició 3.5.2. Diem que una matriu $U \in M_n(\mathbb{C})$ és **unitària** si

$$U^*U = UU^* = I$$

on I és la matriu identitat i U^* és la transposada conjugada de U , i.e., la matriu resultant de la transposició i de la conjugació de totes les entrades.

Anomenem **grup unitari** $U(n)$ a el grup de les matrius invertibles unitàries $n \times n$ amb entrades sobre \mathbb{C} , similarment definim el **grup unitari especial** $SU(n)$ el grup de les matrius invertibles unitàries amb determinant 1.

Observem que

$$SU(n) \subset U(n) \subset GL(n, \mathbb{C})$$

Lema 3.5.1. Si $A \in SU(2)$, existeix una matriu diagonal $D \in SU(2)$ i una matriu unitària $U \in SU(2)$ tal que $D = USU^*$.

Demostració. Aplicant el Teorema espectral tenim que tota matriu $A \in SU(2)$ és conjugada d'una matriu diagonal $D \in SU(2)$ per a una matriu unitària U , i.e., $D = USU^*$. Hem de veure que aquesta U pot ser escollida de forma que tingui determinant 1.

Com que U és unitària tenim que $UU^* = I$, per tant

$$1 = \det(UU^*) = \det(U)\det(U^*).$$

Com que el determinant és el producte dels valors propis, i al prendre el conjugat de la transposada transformem els valors propis als seus transposats, tenim que si $\det(U) = u$ aleshores $\det(U^*) = \bar{u}$. Per tant $u\bar{u} = 1$. Observem que la matriu $V := \sqrt{u}U$ compleix

$$\det(V) = \bar{u}\det(U) = u\bar{u} = 1$$

i per tant tenim $D' = VSV^*$ on la diferència entre D i D' és el producte per un escalar. \square

Lema 3.5.2. *Hi ha una correspondència bijectiva entre S^3 i $SU(2)$.*

Demostració. En primer lloc observem que per a tota $A \in SU(2)$, tenim $\det(A) = 1$ i $A^*A = I$, i per tant A ha de ser de la forma

$$A = \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix}$$

Considera el homomorfisme $\varphi : S^3 \rightarrow \mathbb{H}$ definit per

$$z = (a + bi + cj + dk) \mapsto \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix} = \varphi(z)$$

Observem que per a tot $z \in S^3$ tenim que $a^2 + b^2 + c^2 + d^2 = 1$, per tant $\det(\varphi(z)) = 1$, a més aquesta aplicació té una inversa definida per

$$\begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix} \mapsto a + ib + (c + id)j$$

a més es pot comprovar que és un homomorfisme de grups, on el producte de S^3 és l'heretat de \mathbb{H} . \square

Proposició 3.5.1. $S^3 \cong [\mathbb{H}^\times, \mathbb{H}^\times]$.

Demostració. Gràcies a (3.5) tenim que $[\mathbb{H}^\times, \mathbb{H}^\times] \subset S^3$. Hem de veure l'altra inclusió. Usant la correspondència bijectiva entre S^3 i $SU(2)$ tenim que per a tot $s \in S^3$ podem enviar-lo a $SU(2)$ usant l'isomorfisme φ definit al Lema 3.5.2. Com que $\varphi(s) \in SU(2)$, usant el Lema 3.5.1 tenim que existeix una matriu $U \in SU(2)$ tal que $\varphi(s) = UDU^*$, on D és una matriu diagonal. Com que $D \in SU(2)$ tenim que ha de ser de la forma

$$D = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}.$$

Aleshores aplicant l'antiimatge a $\varphi(s)$ tenim que

$$s = \varphi^{-1}(\varphi(s)) = \varphi^{-1}(UDU^*) = \varphi^{-1}(U)\varphi^{-1}(D)\varphi^{-1}(U^{-1}) = xyx^{-1},$$

on $x \in \mathbb{H}$ i $y \in \mathbb{C} \subset \mathbb{H}$. Com que $y \in \mathbb{C}$ podem trobar un $w \in \mathbb{C}$ tal que $y = w^2$. Usant el fet que tot quaternió es pot expressar com a producte de dos quaternions purs, tenim que existeixen $p, q \in S^3$ quaternions purs tals que $pq = w$, podem imposar que $|p| = |q| = 1$, a més, al ser quaternions purs han de complir $p^{-1} = -p$ i $q^{-1} = -q$. Aleshores

$$s = xppqpqx^{-1} = xppq(-p)(-q)x^{-1} = xppq^{-1}q^{-1}x^{-1} = (xpx^{-1})(xqx^{-1})(xpx^{-1})^{-1}(xqx^{-1})^{-1}.$$

□

Corol·lari 3.5.1. $\mathbb{H}_{ab}^\times \cong \mathbb{R}_+^\times$

Demostració. Observem que $\ker N = [\mathbb{H}, \mathbb{H}]$, aleshores la norma estesa a l'abelianitzat $\mathbb{H}_{ab}^\times = \mathbb{H}^\times / [\mathbb{H}^\times, \mathbb{H}^\times] \rightarrow \mathbb{R}_+^\times$ ha de ser un isomorfisme. □

$$\begin{array}{ccc} \mathbb{H}^\times & \xrightarrow{N} & \mathbb{R}_+^\times \\ \downarrow i & \nearrow & \\ \mathbb{H}_{ab}^\times & & \end{array}$$

Introduïrem ara el determinant de Dieudonné, notem però que usant el Corol·lari 3.4.1, ja tenim que $K_1(\mathbb{H}) \cong \mathbb{R}_+^\times$.

Definició 3.5.3. Per a tot $a \in \mathbb{H}^\times$ denotem $D(a, n)$ a la matriu invertible $n \times n$ la qual té totes les entrades iguals que la matriu identitat excepte l'entrada que ocupa la posició (n, n) que té per valor a . Observem que

$$D(a)D(b) = D(ab)$$

per a tot $a, b \in \mathbb{H}^\times$.

Teorema 3.5.3. Tota matriu invertible A es pot expressar de la forma $B \cdot D(\mu)$, on $B \in E(\mathbb{H})$ i $\mu \neq 0$.

Demostració. La prova consisteix en aplicar transformacions elementals, segueix un procediment semblant a la prova de la Proposició 3.2.1, tots els detalls de la prova explícita es troben a [4] Teorema 4.1. □

Definició 3.5.4. El **determinant de Dieudonné** és una aplicació

$$\det : GL(\mathbb{H}) \rightarrow \mathbb{H}_{ab}^\times,$$

definit a partir del Teorema anterior, $A = BD(\mu) \mapsto \bar{\mu}$.

A [4] s'explicita com el determinant de Dieudonné compleix (a-c) (i per tant també compleix (d-e) del Teorema 3.4.1 i per tant és la mateixa aplicació determinant que la descrita al Teorema 3.4.1.

Observem que el determinant de Dieudonné pren valors sobre els reals positius, de fet es comporta com el valor absolut del determinant usual de matrius reals o complexes des de tots els punts de vista (algebraic i analític).

Observació. Observem que a \mathbb{H}_{ab}^\times tenim que

$$\overline{ab} = \bar{a}\bar{b} = \bar{b}\bar{a} = \overline{ba}$$

en particular, $\bar{1} = \overline{-1}$.

Teorema 3.5.4. Si $a, b \in \mathbb{H}^\times$ i $c = aba^{-1}b^{-1}$, aleshores $D(c)$ és unimodal si $n \geq 2$.

Demostració. Aquest Teorema de fet diu que si

$$\bar{c} = 1 \in \mathbb{H}_{ab}^\times,$$

aleshores $\det(D(c)) = \bar{1} \in \mathbb{H}_{ab}^\times$, la prova consisteix en constatar que a partir de transformacions elementals, i.e., multiplicant per matrius de $E(\mathbb{H})$ tenim

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &\rightarrow \begin{pmatrix} 1 & 0 \\ a^{-1} & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & -a \\ a^{-1} & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & -a \\ a^{-1} & b^{-1} \end{pmatrix} \rightarrow \begin{pmatrix} aba^{-1} & 0 \\ a^{-1} & b^{-1} \end{pmatrix} \\ &\rightarrow \begin{pmatrix} aba^{-1} & 0 \\ 1 & b^{-1} \end{pmatrix} \rightarrow \begin{pmatrix} 0 & -c \\ 1 & b^{-1} \end{pmatrix} \rightarrow \begin{pmatrix} 0 & -c \\ 1 & c \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 1 & c \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}. \end{aligned}$$

on cada fletxa correspon a multiplicar per una matriu de $E(\mathbb{H})$. \square

Proposició 3.5.2. $E(\mathbb{H}) = \{A \in GL(\mathbb{H}) ; \det(A) = 1\}$

Demostració. Està clar que tots els elements de $E(\mathbb{H})$ tenen determinant 1, veiem la implicació no trivial, per a tota $A \in GL(\mathbb{H})$ amb $\det A = 1$ tenim que, usant el Teorema 3.5.3 $A = BD(\mu)$ amb $B \in E(\mathbb{H})$ i per tant amb determinant unimodular. Així doncs $\det A = 1$ si i només si $\bar{\mu} = 1$, per tant $\mu \in [\mathbb{H}, \mathbb{H}]$, i.e., $D(\mu) \in E(\mathbb{H})$. \square

Teorema 3.5.5. $K_1(\mathbb{H}) \cong \mathbb{R}_+^\times$

Demostració. El determinant de Dieudonné, que de fet coincideix amb el determinant del Teorema 3.4.1, dóna lloc a una aplicació

$$\det : GL(\mathbb{H}) \rightarrow \mathbb{H}_+^\times$$

Per la proposició anterior, tenim que $\ker(\det) = E(\mathbb{H})$, i per tant, la factorització al abelianitzat dóna lloc a un isomorfisme $K_1(\mathbb{H}) = GL(\mathbb{H})/E(\mathbb{H}) \rightarrow \mathbb{H}_{ab}^\times$,

$$\begin{array}{ccc} GL(\mathbb{H}) & \xrightarrow{\det} & \mathbb{H}_{ab}^\times \\ \downarrow i & \nearrow & \\ K_1(\mathbb{H}) & & \end{array}$$

Usant el Corol·lari 3.5.1, on hem vist que $\mathbb{H}_{ab}^\times \cong \mathbb{R}_+^\times$, trobem el que buscàvem. \square

3.6 El cas dels Dominis Euclidians.

Al capítol anterior, en l'estudi de K_0 , estudiàvem el cas d'un cos, el d'un DIP i el dels anells locals. En aquest capítol, en l'estudi des K_1 hem vist el cas d'un cos i dels anells locals, ara ens centrarem en un tipus de DIP's, els dominis Euclidians.

Definició 3.6.1. Un domini d'integritat (anell no trivial sense divisors de zero) commutatiu R es diu **domini Euclidià** si hi ha una funció norma $|| : R \rightarrow \mathbb{N}$ amb les següents propietats:

- i) Si $a \in R$, $|a| = 0$ si i només si $a = 0$.
- ii) Si $a, b \in R$, $|ab| = |a||b|$.
- iii) Si $a, b \in R$, $b \neq 0$, aleshores existeix $q, r \in R$, que anomenarem quocient i residu respectivament, els quals compleixen $a = qb + r$ i $0 \leq |r| < |b|$.

Observació. Observem que \mathbb{Z} , $\mathbb{Z}[i]$, $\mathbb{Z}[\frac{-1+i\sqrt{3}}{2}]$ i $K[t]$ (on K és un cos) són dominis Euclidians, amb aplicacions norma definides per $|a+bi| = a^2+b^2$, $|a+b\frac{-1+i\sqrt{3}}{2}| = a^2-ab+b^2$, i per $|f(t)| = 2^{\text{grau } f}$ (amb el conveni que grau $0 = -\infty$), respectivament.

Proposició 3.6.1. *Tot domini Euclidià és un domini d'ideals principals.*

Demostració. Si R és un domini Euclidià, l'ideal $\{0\}$ és clarament principal. Si I és un ideal no nul i b un element no nul d'aquest ideal tal que

$$|b| = \min\{|x|, x \in I \setminus \{0\}\}.$$

Aleshores existeixen $q, r \in R$ tals que $a = qb + r \in I$, amb $0 \leq |r| < |b|$. Si $r \neq 0$ tenim contradicció gràcies a la tria de b , per tant $r = 0$, i en conseqüència I és un ideal principal generat per b . \square

Teorema 3.6.1. *Si R és un domini Euclidià, aleshores $SK_1(R)$ és trivial i $K_1(R) \cong R^\times$. De fet, per a tot n , $SL(n, R) = E(n, R)$.*

Demostració. Donada $A = (a_{ij}) \in GL(n, R)$, ens agradaria usar el mateix argument que a la Proposició 3.2.1, però tenim el problema que donada una columna de A , no és trivial que existeixi un element invertible en aquesta columna. Considerem la primera columna de A , no pot passar que tots els elements siguin zero, ja que és invertible, per tant ha d'existir almenys un element no nul, assumim sense pèrdua de generalitat que a_{i1} compleix la condició que és l'element amb norma mínima entre els elements no nuls d'aquesta columna. Aleshores si $|a_{i1}| = 1$, per (iii) existeix una expressió $1 = a_{i1}q + r$ amb $|r| < 1$, per tant $|r| = 0$ i tenim que a_{i1} és invertible. Altrament, si $|a_{i1}| > 1$, tenim que a_{i1} no és invertible, i per tant genera un ideal propi (a_{i1}) . D'altra banda com que A és invertible, l'ideal generat per tots els elements de la primera columna ha de ser tot R , i per tant ha d'existir algun $j \neq i$ tal que $a_{j1} \notin (a_{i1})$. Aleshores usant (iii) tenim que $a_{j1} = qa_{i1} + r$ amb $|r| < |a_{i1}|$, com que $a_{j1} \notin (a_{i1})$ tenim que $r \neq 0$. Aleshores a partir de restar $q \times$ (la fila i -èsima de A) la fila j -èsima estem fent decreixer la norma mínima dels elements no nuls de la primera columna. A partir d'iterar aquest procés, tenim una successió de valors naturals estrictament decreixent, i per tant ha de convergir a zero, i.e., aquest procediment ens permet reduir-nos al cas en que hi ha un element invertible a la primera columna.

Així doncs, podem transformar la matriu A a la forma

$$\begin{pmatrix} a_{11} & * \\ 0 & A' \end{pmatrix}$$

a través de transformacions elementals per files, on a_{11} és un element invertible i A' una matriu invertible $(n-1) \times (n-1)$. Podem repetir aquest procés per a A' , i acabar la prova amb el mateix argument usat a la Proposició 3.2.1. \square

Corol·lari 3.6.1. $K_1(\mathbb{Z}) \cong \{1, -1\}$, $K_1(\mathbb{Z}[i]) \cong \{1, i, -1, -i\}$, $K_1(K(x)) \cong K^\times$
i $K_1(\mathbb{Z}[\frac{-1+i\sqrt{3}}{2}]) \cong \{z \in \mathbb{C}; z^6 = 1\}$.

Demostració. Observem que per (ii) tenim que si R és un domini Euclidià, $a \in R$ és invertible si i només si $|a| = 1$, és fàcil comprovar quins elements tenen norma 1 dels dominis Euclidiàns donats. \square

3.7 El grup K_1 relatiu i la successió exacta

Definició 3.7.1. Sigui R un anell (amb unitat) i I un ideal bilàter de R . Definim el grup K_1 relatiu de l'anell R i l'ideal I com

$$K_1(R, I) = \ker((p_1)_* : K_1(D(R, I)) \rightarrow K_1(R))$$

Nota el paral·lelisme amb la definició 2.6.3.

Definició 3.7.2. Sigui R un anell (amb unitat) i I un ideal bilàter de R . Anomenarem $GL(R, I)$ al nucli de l'aplicació $GL(R) \rightarrow GL(R/I)$ induïda per l'aplicació quocient $R \rightarrow R/I$. Definim $E(R, I)$ com el subgrup normal de $E(R)$ més petit tal que contingui les matrius elementals $e_{ij}(a)$ amb $a \in I$.

Observació. Observem que totes les matrius elementals $e_{ij}(a)$ amb $a \in I$ són congruents a la identitat a $GL(R/I)$, i per tant, $E(R, I) \subset GL(R, I)$.

Teorema 3.7.1 (Lema de Whitehead Relatiu). *Sigui R un anell (amb unitat) i I un ideal bilàter de R . Aleshores $E(R, I)$ és un subgrup normal de $GL(R, I)$ i $GL(R)$,*

$$GL(R, I)/E(R, I) \cong K_1(R, I),$$

i $GL(R, I)/E(R, I)$ és el centre de $GL(R)/E(R, I)$. A més $E(R, I) = [E(R), E(R, I)] = [GL(R), E(R, I)]$.

Demostració. Comencem veient que $E(R, I)$ és normal de $GL(R, I)$ (que és normal de $GL(R)$ ja ho hem vist al Lema de Whitehead), siguin $A \in GL(n, R)$ i $B \in E(n, R, I)$, aleshores usant la igualtat ja vista a la demostració del Lema de Whitehead tenim per una banda

$$\begin{pmatrix} ABA^{-1}B^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & B^{-1}A^{-1} \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} B^{-1} & 0 \\ 0 & B \end{pmatrix}.$$

D'altra banda tenim que $\begin{pmatrix} A^{-1} & 0 \\ 0 & A \end{pmatrix}$ és una matriu elemental gràcies al Corol·lari 3.1.1, a més, per la definició de $E(R, I)$ tenim que és normal de $E(R)$, i per tant, la part dreta de la igualtat anterior pertany a $E(R, I)$, provant que $E(R, I)$ és normal de $GL(R, I)$.

Per a veure l'isomorfisme primer necessitem fer la següent observació, considerem $(A_1, A_2) \in GL(D(R, I)) \subset GL(R \times R)$ un element tal que pertany al nucli de $(p_1)_*$, i.e., aquesta aplicació l'envia a l'element identitat de $K_1(R)$ i per tant $A_1 \in E(R)$, però aleshores $(A_1, A_1) \in E(D(R, I))$ ja que si $A_1 = \prod_k e_{i_k j_k}(a_k)$,

$$(A_1, A_1) = \prod_k e_{i_k j_k}(a_k, a_k).$$

Així doncs, multiplicant (A_1, A_2) per $(A_1, A_1)^{-1}$ el podem transformar a la forma $(1, B)$ amb $B \in GL(R)$ sense canviar la seva classe a K_1 . Com que $(1, B) \in GL(D(R, I))$ tenim que $B \equiv 1 \pmod{I}$ i per tant $B \in GL(R, I)$. Recíprocament tot element $B \in GL(R, I)$ defineix una classe a $GL(D(R, I))$. Per tant, per a mostrar que $GL(R, I)/E(R, I) \cong K_1(R, I)$ només necessitem comprovar que si $B \in GL(R, I)$ aleshores $(1, B) \in E(D(R, I))$ si i només si $B \in E(R, I)$.

Per veure una implicació, observem que $E(R, I)$ ve generat per matrius de la forma $Se_{ij}(a)S^{-1}$ amb $a \in I$, i $S \in E(R)$. Tanmateix

$$(1, Se_{ij}(a)S^{-1}) = (S, S)e_{ij}(0, a)(S^{-1}, S^{-1})$$

i tots els tres factors de la part dreta pertanyen a $E(D(R, I))$. Per a veure el recíproc, suposem que

$$(1, B) = \prod_{k=1}^r e_{i_k j_k}(a_k, b_k) \in E(D(R, I)), \quad \prod_k e_{i_k j_k}(a_k) = 1 \in E(R).$$

Observem que per a cada k ,

$$e_{i_k j_k}(a_k, b_k) = e_{i_k j_k}(a_k, a_k)e_{i_k j_k}(0, b_k - a_k) = (S_k, S_k)(1, T_k)$$

on

$$S_k = e_{i_k j_k}(a) \in E(R), \quad T_k = e_{i_k j_k}(b_k - a_k), \quad b_k - a_k \in I.$$

Aleshores com que $S_1 S_2 \dots S_r = 1$ tenim

$$\begin{aligned} \prod_k e_{i_k j_k}(a_k, b_k) &= \\ \prod_k (S_k, S_k T_k) &= (S_1, S_1 T_1 S_1^{-1})(S_2, S_1 S_2 T_2 S_2^{-1} S_1^{-1}) \dots (S_r, S_1 S_2 \dots S_r T_r) \\ &= (1, (S_1 T_1 S_1^{-1}))(S_1 S_2 T_2 S_2^{-1} S_1^{-1}) \dots (S_1 S_2 \dots S_r T_r S_r^{-1} \dots S_2^{-1} S_1^{-1}), \end{aligned}$$

i per tant, hem escrit el nostre element B com a producte de generadors de $E(R, I)$. Així doncs això acaba la demostració de l'isomorfisme.

Veiem ara darrera igualtat, com que $E(R, I)$ és un subgrup normal de $GL(R, I)$ i de $GL(R)$, tenim que $[E(R), E(R, I)] = [GL(R), E(R, I)] \subset E(R, I)$. Per veure l'altra inclusió observem que, com que $E(R, I)$ ve generat per les matrius de la forma $Se_{ij}S^{-1}$ amb $a \in I$ i $S \in E(R)$, a més

$$Se_{ij}(a)S^{-1} = [S, e_{ij}(a)]e_{ij}(a) = [S, e_{ij}(a)][e_{ik}(1), e_{kj}(a)] \in [E(R), E(R, I)], \quad k \neq i, j.$$

Per acabar la prova hem de veure que $GL(R, I)/E(R, I)$ és el centre de $GL(R)/E(R, I)$. Veiem doncs la inclusió $G \subset Z(GL(R, I)/E(R, I))$, si $A \in GL(R, I)$ tenim que

$$\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix} = \begin{pmatrix} 1 & A-1 \\ 0 & 1 \end{pmatrix} \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -A^{-1}(A-1) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \right\} \begin{pmatrix} 1 & 0 \\ -(A-1) & 1 \end{pmatrix},$$

i com que les entrades de A^{-1} pertanyen a I , tenim que les matrius

$$\begin{pmatrix} 1 & A-1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -A^{-1}(A-1) \\ 0 & 1 \end{pmatrix}, \quad i \quad \begin{pmatrix} 1 & 0 \\ -(A-1) & 1 \end{pmatrix}$$

pertanyen a $E(R, I)$ i per tant el càlcul anterior mostra que $\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix}$ pertany a $E(R, I)$.

Per tant si $B \in GL(R)$,

$$\begin{pmatrix} ABA^{-1}B^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \left[\begin{pmatrix} A & 0 & 0 \\ 0 & A^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} B & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & B^{-1} \end{pmatrix} \right] \in [E(R, I), E(R)] = E(R, I).$$

per tant $GL(R, I)$ i $GL(R)$ commuten mòdul $E(R, I)$. Per a veure l'altra inclusió observem que la imatge sota el homomorfisme induït per l'aplicació quocient $R \twoheadrightarrow R/I$ del centre de $GL(R)/E(R, I)$ ha de ser el centre de $GL(R/I)$. A més, el centre de $GL(R/I)$ és trivial ja que una matriu del centre ha de ser diagonal amb elements iguals a la diagonal, i com que una matriu qualsevol de GL ha de tenir un nombre finit d'elements diferent de 1 a la diagonal, $Z(GL(S))$ és trivial. Per tant el centre de $GL(R)/E(R, I)$ està contingut en el nucli de l'aplicació a $GL(R/I)$, que és $GL(R, I)/E(R, I)$. \square

Veiem ara una extensió del Teorema 2.6.2.

Teorema 3.7.2. *Sigui R un anell i $I \subset R$ un ideal. Aleshores existeix una successió exacta*

$$K_1(R, I) \rightarrow K_1(R) \xrightarrow{q_*} K_1(R/I) \xrightarrow{\partial} K_0(R, I) \rightarrow K_0(R) \xrightarrow{q_*} K_0(R/I), \quad (3.6)$$

on q_* ve induïda per l'aplicació quocient $q : R \twoheadrightarrow R/I$ i les aplicacions $K_j(R, I) \rightarrow K_j(R)$ venen induïdes per $p_2 : D(R, I) \rightarrow R$.

Demostració. Usarem la mateixa notació que al Teorema 2.6.2 en el sentit que si A és una matriu amb entrades a R , denotarem per \dot{A} a la matriu $q(A)$, i.e. a la matriu corresponent amb entrades sobre R/I .

En primer lloc veurem que la subcadena

$$K_1(R, I) \rightarrow K_1(R) \xrightarrow{q_*} K_1(R/I)$$

és exacta. Per a veure-ho usarem la mateixa observació usada a la prova anterior, és a dir, usarem que tota classe de $K_1(R, I)$ es pot representar com

$$(1, B) \in GL(D(R, I)) \subset GL(R \times R)$$

amb $B \in GL(R, I)$. Aleshores tenim que $\dot{B} = \dot{1}$ i $q_*[B] = 1$ i per tant hem vist una inclusió. Per a veure l'altra inclusió considerem $B \in GL(R)$ i $q_*([B]) = 1$, aleshores $\dot{B} \in E(R/I)$. Ara si $\dot{a} \in R/I$, tenim que prové d'algun $a \in R$ i $e_{ij}(\dot{a}) = q(e_{ij}(a))$. Per tant tot generador de $E(R/I)$ pertany a la imatge de $E(R)$ i en conseqüència $E(R/I) = q(E(R))$. (Aquest argument l'hem usat en el Lema 2.6.1). Per tant \dot{B} ascendeix a una matriu $C \in E(R)$, i $q(BC^{-1}) = 1$. Aleshores $(1, BC^{-1}) \in GL(D(R, I))$ i $[B] = [BC^{-1}]$ a $K_1(R)$ prové de $[(1, BC^{-1})] \in K_1(R, I)$.

A continuació definirem l'aplicació frontera $K_1(R/I) \xrightarrow{\partial} K_0(R, I)$ i provarem l'exactitud de $K_1(R/I)$ i $K_0(R, I)$, un cop vist això el Teorema 2.6.2 completarà la prova. Donada una matriu $\dot{A} \in GL(n, R/I)$, on ara $A\dot{A}$ és la imatge d'una matriu $A \in M_n(R)$ no necessàriament invertible, definim

$$R^n \times_{\dot{A}} R^n := \{(x, y) \in R^n \times R^n : \dot{y} = \dot{x}\dot{A}\}$$

ensem pensar x i y com a matrius $1 \times n$. A la definició anterior té estructura de mòdul sobre $D(R, I)$ si imposem

$$(r_1, r_2) \cdot (x, y) = (r_1 x, r_2 y).$$

És compatible ja que, com que $r_1 = r_2$ tenim

$$q(r_2 y) = r_2 \dot{y} = r_1 (\dot{x}\dot{A}) = q(r_1 x)\dot{A}.$$

Aquesta estructura ens permet obtenir un mòdul projectiu sobre $D(R, I)$ a partir de dos mòduls lliures.

Observem que si $\dot{A} = q(A)$ amb $A \in GL(n, R)$, aleshores

$$(x, y) \mapsto (xA, y) \in R^n \times_i R^n \cong D(R, I)^n$$

dóna lloc a un isomorfisme de $R^n \times_{\dot{A}} R^n$ a un mòdul lliure de rang n . En particular, com que hem vist que $E(R/I) = q(E(R))$, tenim que $R^n \times_{\dot{A}} R^n$ és lliure de rang n si \dot{A} és elemental. Per a una matriu general $\dot{A} \in GL(n, R/I)$ sempre podem escollir $\dot{B} \in GL(n, R/I)$ de forma que $\dot{A} \oplus \dot{B}$ sigui elemental (per exemple, $\dot{B} = (\dot{A})^{-1}$ funciona pel Lema 2.6.1), i aleshores

$$(R^n \times_{\dot{A}} R^n) \oplus (R^n \times_{\dot{B}} R^n) \cong R^{2n} \times_{\dot{A} \oplus \dot{B}} R^{2n} \cong D(R, I)^{2n},$$

per tant $R^n \times_{\dot{A}} R^n$ és un sumand directe d'un mòdul lliure, i.e. d'un mòdul projectiu. Conseqüentment té sentit definir

$$\partial[\dot{A}] := [R^n \times_{\dot{A}} R^n] - [D(R, I)^n] \in K_0(D(R, I)).$$

Veurem que ∂ és de fet un homomorfisme $K_1(R/I) \rightarrow K_0(R, I)$. Té imatge a $K_0(R, I) = \ker(p_1)_*$ ja que

$$(p_1)_*(\partial[\dot{A}]) = (p_1)_*([R^n \times_{\dot{A}} R^n]) - (p_1)_*([D(R, I)]) = [R^n] - [R^n] = 0$$

És additiu sota la suma directa de matrius ja que

$$(R^n \times_{\dot{A}} R^n) \oplus (R^n \times_{\dot{B}} R^n) \cong R^{2n} \times_{\dot{A} \oplus \dot{B}} R^{2n},$$

i envia classes de matrius elementals al 0 ja que si \dot{A} és una matriu elemental,

$$\partial[\dot{A}] = [R^n \times_{\dot{A}} R^n] - [D(R, I)] \cong [D(R, I)^n] - [D(R, I)^n] = 0.$$

Més generalment, està ben definit sobre classes a K_1 , ja que si $\dot{A} = \dot{B}\dot{C}$ amb $B \in E(R)$, aleshores

$$(x, y) \mapsto (xB, y) \in R^n \times_{\dot{C}} R^n$$

dóna lloc a un isomorfisme de $R^n \times_{\dot{A}} R^n$ a $R^n \times_{\dot{C}} R^n$. Per tant obtenim un homomorfisme ben definit $K_1(R/I) \rightarrow K_0(R, I)$. A més ja hem vist que la composició

$$K_1(R) \xrightarrow{q_*} K_1(R/I) \xrightarrow{\partial} K_0(R, I)$$

és zero. La composició

$$K_1(R/I) \xrightarrow{\partial} K_0(R, I) \rightarrow K_0(R)$$

és zero ja que

$$(p_2)_*(\partial[\dot{A}]) = (p_2)_*([R^n \times_{\dot{A}} R^n]) - (p_2)_*([D(R, I)^n]) = [R^n] - [R^n] = 0.$$

Només falta comprovar que $\ker \partial \subset q_*(K_1(R))$ i que

$$\ker\{(p_2)_* : K_0(R, I) \rightarrow K_0(R)\} \subset \partial(K_1(R/I)).$$

Suposem $\partial([\dot{A}]) = 0$, això significa que $R^n \times_{\dot{A}} R^n$ és isomorf a un mòdul lliure de rang n , o que per alguna m ,

$$R^n \times_{\dot{A}} R^n \oplus D(R, I)^m \cong D(R, I)^{n+m}.$$

Després de canviar A per $A \oplus 1_m$, podem assumir que de fet

$$R^n \times_{\dot{A}} R^n \cong D(R, I)^n.$$

Escollim un isomorfisme

$$\varphi : D(R, I)^n = R^n \times_i R^n \rightarrow R^n \times_{\dot{A}} R^n.$$

Aleshores podem definir les matrius $B, C \in M_n(R)$ per $(e_j B, e_j C) = \varphi(e_j, e_j)$, on e_j és el j -èssim vector bàsic de R^n , en altres paraules prenem les files j -èssimes de B i C per a primera i segona coordenada de $\varphi(e_j, e_j)$. Aleshores per linealitat $\varphi(u, v) = (uB, vC)$ per a tot $(u, v) \in D(R, I)^n = R^n \times_i R^n$, i aleshores per a aquesta u i v , $\dot{u} = \dot{v}$, tenim $\dot{B}\dot{A} = \dot{C}$. Per tant φ és invertible, està clar que B i C són invertibles amb $\varphi(x, y) = (xB^{-1}, yC^{-1})$ per $(x, y) \in R^n \times_{\dot{A}} R^n$. Per tant $\dot{A} = q(B^{-1}C)$ i per tant $\ker \partial \subset q_*(K_1(R))$.

Finalment, suposem que tenim una classe de $K_0(R, I)$ que va a parar al 0 de $K_0(R)$. Això significa que tenim una classe a $K_0(D(R, I))$ que va a parar al 0 a partir de $(p_1)_*$ i de $(p_2)_*$. Representem la classe per $[P] - [D(R, I)^n]$, on P és un $D(R, I)$ -mòdul projectiu tal que $(p_1)_*(P)$ i $(p_2)_*(P)$ són isomorfs a R^n . Si és necessari, podem afegir-hi un mòdul de

rang k a P i canviar n per $n + k$ de forma que $(p_1)_*(P)$ i $(p_2)_*(P)$ siguin ambdós isomorfs a R^n . Aleshores està clar que P és de la forma $R^n \times_A R^n$, i per tant

$$[P] - [D(R, I)^n] = \partial([A]).$$

Això completa la prova. \square

Corol·lari 3.7.1. *Sigui R un anell, i $I \subset R$ un ideal tal que l'aplicació quocient $q : R \rightarrow R/I$ té una inversa per la dreta, i.e., existeix un homomorfisme d'anells $s : R/I \rightarrow R$ amb $q \circ s = \text{id}_{R/I}$. Aleshores*

$$0 \rightarrow K_0(I) \rightarrow K_0(R) \rightarrow K_0(R/I) \rightarrow 0$$

és una successió exacta escindida.

Demostració. Per la functorialitat de K_0 tenim que existeix una s_* tal que $q_* \circ s_* = \text{id}_{K_0(R/I)}$. Així doncs només necessitem veure que $K_0(I) \rightarrow K_0(R)$ és injectiva. La injectivitat es veu a partir de que $s_* : K_1(R/I) \rightarrow K_1(R)$ és inversa per la dreta de $q_* : K_1(R) \rightarrow K_1(R/I)$, per tant $\partial = 0$ a la cadena exacta (3.6). \square

Exemples 3.7.1. *Aquests darrers resultats ens proporcionen eines per a calcular K -grups. Veiem alguns exemples.*

Sigui $R = \mathbb{Z}$ i $I = (m)$, amb $m > 0$. Recordem que al Corol·lari 3.6.1 vem veure $K_1(R) \cong \{\pm 1\}$, i a la Proposició 3.4.2 hem calculat $K_1(R/I)$. Aleshores és possible calcular $K_0(I)$ a partir de la cadena exacta. Per exemple suposem $m = 2$, aleshores R/I és el cos format per dos elements i $(R/I)^\times = \{1\}$. La cadena exacta és

$$K_1(R, I) \rightarrow \{\pm 1\} \rightarrow \{1\} \xrightarrow{\partial} K_0(I) \rightarrow \mathbb{Z} \xrightarrow{\cong} \mathbb{Z},$$

i $K_0(I) = 0$. Al mateix temps, tenim que $K_1(R, I)$ ha de ser exhaustiu a $\{\pm 1\}$.

Suposem ara que $m = p$ per a p primer senar. Aleshores R/I és un cos \mathbb{F}_p de p elements i $(R/I)^\times$ és cíclic d'ordre $p - 1$. Per tant la successió exacta esdevé

$$K_1(R, I) \rightarrow \{\pm 1\} \rightarrow \mathbb{F}_p^\times \xrightarrow{\partial} K_0(I) \rightarrow \mathbb{Z} \xrightarrow{\cong} \mathbb{Z},$$

i $K_0(I) \cong \mathbb{F}_p^\times \setminus \{\pm 1\}$, que és cíclic d'ordre $\frac{p-1}{2}$. En aquest cas, l'aplicació $K_1(R, I) \rightarrow \{\pm 1\}$ és trivial.

Suposem ara que $m = 2^r$ amb $r > 1$. Aleshores R/I és un anell local i $(R/I)^\times$ és un grup abelià d'ordre 2^{r-1} . Aleshores tenim la cadena exacta

$$K_1(R, I) \rightarrow \{\pm 1\} \rightarrow (R/I)^\times \xrightarrow{\partial} K_0(I) \rightarrow \mathbb{Z} \xrightarrow{\cong} \mathbb{Z},$$

i $K_0(I) \cong (R/I)^\times$ és un grup abelià d'ordre 2^{r-2} no necessàriament cíclic. Per exemple si $m = 8$ tenim que $(R/I)^\times \cong (\mathbb{Z}/(2) \cong \mathbb{Z}/(2))$ és el 4-grup de Klein.

Capítol 4

Conclusions

El contingut d'aquest treball és només una petita part del que es coneix per K -teoria algebraica. Hem introduït els dos primers grups, els quals formen part del que es coneix per K -teoria algebraica clàssica.

Per ampliar aquest treball en el sentit algebraic podríem haver estudiat K_0 i K_1 per dominis de Dedekind, aquesta estructura algebraica permet mostrar resultats interessants sobre K -grups. També podríem haver estudiat K_0 i K_1 per a categories en lloc d'anells, i introduir la K -teoria negativa. O fins i tot seria interessant estudiar el grup K_2 .

D'altra banda, és molt usual parlar de K -teoria en sentits no algebraics, cal destacar la K -teoria topològica, que és la branca de la topologia que es dedica a estudiar fibrats vectorials sobre espais topològics. Ampliacions d'aquest treball en el sentit topològic poden ser interessants.

Molts problemes profunds en àlgebra, com la classificació de subgrups normal de grups lineals, o la descripció del grup de Brauer d'un cos en termes d'àlgebres cícliques han estat resolts a través de K -teoria algebraica. Possibles ampliacions d'aquest treball podrien estar enfocades a estudiar aquests resultats en detall.

Però més enllà d'això, la K -teoria algebraica ha aportat tècniques de resolució de problemes importants en topologia, geometria, teoria de nombres i anàlisi funcional. En aquest treball ens hem dedicat a introduir els fonaments bàsics d'aquestes tècniques, la punta del iceberg.

Apèndix A

Conceptes de Mòduls i Estructures Algebraiques

L'objectiu d'aquest annex és introduir un bagatge de resultats que convé tenir presents durant la lectura del treball. El lector familiaritzat amb conceptes de mòduls pot prescindir d'aquest annex. Aquest annex permet que el treball sigui essencialment autocontingut, en el sentit que qualsevol recent graduat, estigui familiaritzat o no amb la teoria de mòduls, podrà seguir tots els conceptes exposats amb detall.

Per la redacció de l'annex ens hem basat en [10] i [2].

A.1 Recordatori

Definició A.1.1. Un **semigrup** (S, \cdot) és un conjunt amb una operació binària $\cdot : S \times S \rightarrow S$ tal que satisfà la propietat associativa, és a dir, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ per a tot $a, b, c \in S$.

Definició A.1.2. Un **grup** $(G, +)$ és un conjunt G amb una operació binària $+: G \times G \rightarrow G$ tal que satisfà:

- Associativitat: $(a + b) + c = a + (b + c)$ per a tot $a, b, c \in G$.
- Té un element neutre: existeix $e \in G$ tal que $e + a = a + e = a$ per tot $a \in G$.
- Per tot $a \in G$ existeix un element invers $b \in G$ tal que $a + b = b + a = e$.¹

Diem que $(G, +)$ és un grup (o un semigrup) **commutatiu** (o abelià) si l'operació és commutativa, i.e., $a + b = b + a$ per tot $a, b \in G$.

Definició A.1.3. Diem que $H \subset G$ és un **subgrup** de G si H amb l'operació binària de G és un grup. Un subgrup N d'un grup (G, \cdot) és **normal**, i ho denotarem $N \trianglelefteq G$, si és invariant sota conjugació, és a dir, la conjugació d'un element de N per un element de G pertany a N :

$$N \trianglelefteq G \Leftrightarrow \forall n \in N, \forall g \in G : gng^{-1} \in N$$

Definició A.1.4. Sigui N un subgrup normal d'un grup (G, \cdot) , $G/N := \{aN : a \in G\}$. Com que N és normal, si $a, b \in G$ s'ha de complir

$$(aN)(bN) = a(Nb)N = a(bN)N = (ab)NN = ab(N)$$

Per tant podem estendre l'operació del grup G a G/N usant aquest fet, així doncs G/N és un grup, que anomenem **grup quocient**.

¹Si a l'operació binària que defineix el grup la denotem \cdot , a l'invers de a el denotarem a^{-1} , de forma que $aa^{-1} = a^{-1}a = e$, en aquest cas a l'element neutre també el podem denotar per 1. Si el context permet entendre que $*$ és l'operació tal que $(G, *)$ sigui un grup, denotarem a G a aquest grup.

Definició A.1.5. Un **anell** $(R, +, \cdot)$ és un conjunt R amb dues operacions binàries $+$: $R \times R \rightarrow R$ (suma) i \cdot : $R \times R \rightarrow R$ (producte) tals que satisfan:

- a) $(R, +)$ és un grup abelià. (denotem per $0 \in R$ l'element neutre).
- b) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per a tot $a, b, c \in R$ (el producte és associatiu i.e. (R, \cdot) és un semigrup).
- c) Té un element identitat: existeix $1 \in R$ tal que $r \cdot 1 = 1 \cdot r = r$ per tot $r \in R$.
- d) $a \cdot (b + c) = a \cdot b + a \cdot c$ i $(b + c) \cdot a = b \cdot a + c \cdot a$ per a tot $a, b, c \in R$ (el producte és distributiu respecte la suma).

Diem que $(R, +, \cdot)$ és un anell **commutatiu** si $ab = ba$ per a tot $a, b \in R$.

Definició A.1.6. Un **subanell** S d'un anell R és un subconjunt S de R tal que sota les operacions suma i producte de R , és un anell.

Per tant, S és un subanell de R si i només si S és un subgrup additiu de R tancat sota el producte.

Definició A.1.7. Una funció $f : R \rightarrow S$, on R i S són anells, és un **morfisme d'anells** si

- (1) $f(a + b) = f(a) + f(b)$ i $f(ab) = f(a)f(b)$ per a tot $a, b \in R$.
- (2) $f(1_R) = 1_S$ on 1_R és la identitat de R i 1_S la identitat de S .

De (1) es dedueix que $f(-r) = -f(r)$ i $f(0_R) = 0_S$.

Donat un morfisme f , definim el **nucli** de f com $\text{Ker}(f) = \{r \in R : f(r) = 0\}$ i la **imatge** com $\text{Im}f = \{x \in S : x = f(r) \text{ per algun } r \in R\}$. Observem que $\text{Ker}f$ i $\text{Im}f$ són subanells de R i és un subanell de S respectivament.

Si f és invertible (i.e. existeix un morfisme d'anells $g : S \rightarrow R$ tal que $f \circ g = 1_S$ i $g \circ f = 1_R$), aleshores diem que f és un **isomorfisme** d'anells, per tant f és un isomorfisme d'anells si i només si és un morfisme d'anells bijectiu.

A més, f és injectiu si i només si $\text{Ker}f = 0$, i tautològicament, f és exhaustiu si i només si $\text{Im}f = S$.

Definició A.1.8. Sigui R un anell, diem que $I \subset R$ és un ideal de R si i només si

- (1) I és un subgrup additiu de R .
- (2) $rI \subset I$ per a tot $r \in R$
- (3) $Ir \subset I$ per a tot $r \in R$

Un subconjunt $I \subset R$ tal que satisfaci (1) i (2) s'anomena **ideal per l'esquerra** de R , i similarment, si I satisfà (1) i (3) s'anomena **ideal per la dreta** de R . Per tant un ideal de R és un ideal per l'esquerra i per la dreta.

Diem que el ideal I és **propi** si $a \in R$ amb $a \neq R$ i $a \neq \{0\}$.

Si R és commutatiu els conceptes de ideal per l'esquerra, d'ideal per la dreta i ideal són el mateix, però per anells no commutatius generalment són conceptes diferents.

Motivació de la definició d'ideal: De teoria de grups, sabem que no tot subgrup d'un grup pot ser el nucli d'un morfisme de grups, cal que el subgrup sigui normal. En el cas de un morfisme d'anells $f : R \rightarrow S$, $\text{Ker}(f) = \{a \in R : f(a) = 0\}$ és normal ja que és subgrup respecte la suma del grup abelià $(R, +)$.

Observem que l'estructura multiplicativa imposa sobre l'anell $\text{Ker}(f)$ una condició més

forta que la ser anell, que és la de ser ideal, és a dir, es compleix que si $a \in \text{Ker}(f)$ i $r \in R$, aleshores $f(ar) = f(a)f(r) = 0f(r) = 0$ i $f(ra) = f(r)f(a) = f(r)0 = 0$, per tant $ar \in \text{Ker}(f)$ i $ra \in \text{Ker}(f)$ per a qualsevols $a \in \text{Ker}(f)$ i $r \in R$.

Suma d'ideals. Observem que si I i J són ideals (ideal per l'esquerra, o dreta), la seva suma $I + J = \{a + b : a \in I, b \in J\}$ és també un ideal (ideal per l'esquerra o dreta) de R .

Definició A.1.9. Donat un ideal I de R , diem que $r, s \in R$ són congruents mòdul R si $r - a \in I$ (també es denota com $r \equiv s \pmod{I}$). La relació de congruència és una relació d'equivalència sobre R . La classe de congruència es denota $\bar{r} = \{r + x : x \in I\}$, R/I és el conjunt de totes aquestes classes, definim una suma i un producte sobre R/I de la forma següent:

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

Aleshores R/I és un anell amb element neutre $\bar{0}$ i identitat $\bar{1}$. Aquest anell s'anomena **anell quocient de R respecte I** .

Exemple. Un exemple bàsic d'anell residu, que justifica el nom és quan considerem R l'anell dels enters \mathbb{Z} i $I = n\mathbb{Z}$ per algun $n > 0$. Qualsevol enter a pot ser escrit de la forma $a = qn + r$ amb $0 \leq r < n$. L'enter r és el residu i q el quocient, per tant l'anell residu $\mathbb{Z}/n\mathbb{Z}$ consisteix en totes les classes de residus: $\bar{0}, \bar{1}, \dots, \bar{n-1}$.

Teorema A.1.1 (Primer teorema d'isomorfia). Sigui $f : R \rightarrow S$ un morfisme d'anells. Aleshores $R/\text{Ker}(f) \cong \text{Im}(f)$.

Teorema A.1.2 (Segon teorema d'isomorfia). Sigui R un anell, $I \subset R$ un ideal i $S \subset R$ un subanell. Aleshores $S + I$ és un subanell de R , I és un ideal de $S + I$, $S \cap I$ és un ideal de S , i hi ha un isomorfisme d'anells

$$(S + I)/I \cong S/(S \cap I)$$

Teorema A.1.3 (Tercer teorema d'isomorfia). Sigui R un anell, siguin I i J ideals de R tals que $I \subset J$. Aleshores J/I és un ideal de R/I i

$$R/J \cong (R/I)/(J/I)$$

Teorema A.1.4 (Teorema de correspondència). Sigui R un anell, $I \subset R$ un ideal de R i $\pi : R \rightarrow R/I$ l'aplicació natural ($r \mapsto \bar{r}$). Aleshores la funció $S \rightarrow S/I$ defineix una correspondència bijectiva entre el conjunt de tots els subanells de R que contenen I i el conjunt de tots els subanells de R/I . Sota aquesta correspondència, els ideals de R que contenen I corresponen a ideals de R/I .

Lema A.1.5. Sigui R un anell i $\{S_\alpha\}_{\alpha \in A}$ una família de subanells (resp. ideals) de R . Aleshores $S = \bigcap_{\alpha \in A} S_\alpha$ és un subanell (resp. ideal) de R .

Demostració. Sigui $a, b \in S$, aleshores existeix $a, b \in S_\alpha$ per algun $\alpha \in A$, per tant $a - b$ i $ab \in S_\alpha$, per tant S és un subanell de R .

Si cada S_α és un ideal i $r \in R$, aleshores ar i $ra \in S_\alpha$ per tot $\alpha \in A$, per tant $ar, ra \in S$ i en conseqüència S és un ideal. \square

Definició A.1.10. Sigui R un anell i X un subconjunt de R , definim el **subanell generat per X** com el subanell més petit de R que conte X , similarment definim com a **ideal**

generat per X com el ideal més petit de R que contingui X .

Pel Lema anterior, aquest anell (resp. ideal) és la intersecció de totes els subanells (resp. ideals) que contenen X .

Usarem la notació $\langle X \rangle$ per denotar el ideal generat per X .

Lema A.1.6. *Sigui $X \subset R$ un conjunt no buit de R .*

(1) *Si R és un anell amb identitat, aleshores el ideal de R generat per X és el conjunt*

$$XRX = \left\{ \sum_{i=1}^n r_i x_i s_i : r_i, s_i \in R, x_i \in X, n \geq 1 \right\}$$

(2) *Si R és un anell commutatiu amb identitat, aleshores el ideal de R generat per X és el conjunt*

$$RX = \left\{ \sum_{i=1}^n r_i x_i : r_i \in R, x_i \in X, n \geq 1 \right\}$$

Demostració. (1) tot ideal que contingui X clarament ha de contenir RXR , només cal observar que RXR és un ideal de R , i per tant és el ideal més petit de R que conté X . (2) és conseqüència directa de la commutativitat de R . \square

Teorema A.1.7 (Teorema de l'aplicació induïda (per anells)). *Sigui $f : R \rightarrow S$ un morfisme d'anells. Aleshores existeix un únic morfisme d'anells injectiu $\bar{f} : R/\text{Ker } f \rightarrow S$ tal que $\bar{f} \circ \pi = f$, on π és el morfisme natural $R \rightarrow R/\text{Ker}(f)$ definit per $r \mapsto \bar{r}$.*

Demostració. Aquest morfisme és $\bar{f}(\bar{r}) = f(r)$. El morfisme \bar{f} sovint és anomenat **morfisme induït**. \square

Definició A.1.11. Siguin $a \neq 0$ i $b \neq 0$ elements d'un anell R tal que $ab = 0$, aleshores a i b s'anomenen **divisors de zero** de l'anell R .

Definició A.1.12. Sigui R un anell, un element $a \in R$ és diu **element unitari** si té una inversa multiplicativa, és a dir, existeix $b \in R$ tal que $ab = 1 = ba$. Denotem per R^* al conjunt d'elements unitaris de R .

Definició A.1.13. Definició. Un anell R és un **domini de integritat** si és un anell commutatiu tal que no té divisors de zero.

Definició A.1.14. Definició. Un anell R amb identitat és un **anell de divisió** si $R^* = R \setminus \{0\}$, i.e., tot element no zero de R té un invers multiplicatiu.

Definició A.1.15. Definició. Un **cos** és un anell de divisió commutatiu.

Definició A.1.16. Definició. Un grup unitari que juga un rol fonamental en K -teoria és el següent, donat un anell R i un nombre natural n , el grup unitari $M_n(R)^*$ de l'anell de matrius $M_n(R)$ s'anomena grup lineal general de grau n , i s'escriu $GL_n(R)$.

A.2 Definició de Mòduls

Els mòduls són una generalització dels espais vectorials d'àlgebra lineal, on els *escalars* poden ser d'un anell arbitrari en lloc d'un cos.

Definició A.2.1. Sigui R un anell.

1. Un **R -mòdul per l'esquerra** és un grup abelià additiu M amb una operació binària $\cdot : R \times M \rightarrow M$, $(r, m) \rightarrow rm$, tal que

$$a_l) \quad r(m + n) = rm + rn$$

$$b_l) \quad (r + s)m = rm + sm$$

$$c_l) \quad (rs)m = r(sm)$$

$$d_l) \quad 1m = m$$

Per tot $r, s \in R$ i $m, n \in M$, per a un $1 \in R$.

2. Un **R -mòdul per la dreta** és un grup abelià additiu M amb una operació binària $\cdot : M \times R \rightarrow M$, $(m, r) \rightarrow mr$, tal que

$$a_l) \quad (m + n)r = mr + nr$$

$$b_l) \quad m(r + s) = mr + ms$$

$$c_l) \quad m(rs) = (mr)s$$

$$d_l) \quad m1 = m$$

Per tot $r, s \in R$ i $m, n \in M$, per a un $1 \in R$.

Observació. Si R és un anell conmutatiu, aleshores qualsevol ${}_R M$ mòdul també té estructura de M_R mòdul definint $mr = rm$.

Sigui R un anell arbitrari, considerem R^{op} , que és l'anell format pels elements de R , amb la mateixa suma que R però amb multiplicació \cdot donada per $a \cdot b = ba$.

Aleshores qualsevol ${}_R M$ mòdul és un $M_{R^{\text{op}}}$ mòdul.

Notació. Els resultats per mòduls per la dreta i per l'esquerra són paral·lels, per tant per evitar repetir els resultats, treballarem generalment amb R -mòduls per l'esquerra, que els denotarem **R -mòduls** o **mòduls sobre R** .

Si necessitem indicar per quina banda volem considerar el mòdul, denotarem per M_R un R -mòdul per la dreta i ${}_R M$ un mòdul per l'esquerra.

Definició A.2.2. Sigui R un anell i M, N R -mòduls. Una aplicació $f : M \rightarrow N$ és un **homomorfisme de R -mòduls** si compleix

$$(1) \quad f(m_1 + m_2) = f(m_1) + f(m_2) \text{ per a tot } m_1, m_2 \in M$$

$$(2) \quad f(rm) = rf(m) \text{ per a tot } r \in R \text{ i } m \in M.$$

Denotem per $\text{Hom}_R(M, N)$ a el conjunt de tots els homeomorfismes de R -mòduls de M a N , si $M = N$ en lloc de homeomorfismes els podem denotar **endomorfismes**, i al conjunt d'endomorfismes d'un R -mòdul el denotem per $\text{End}_R(M)$.

Si $f \in \text{End}_R(M)$ és invertible, aleshores s'anomena **automorfisme** de M . El grup de tots els automorfismes de R -mòduls de M es denota per $\text{Aut}_R(M)$.

Definició A.2.3. (1) Sigui K un cos, aleshores un K -mòdul V s'anomena **espai vectorial sobre K** .

(2) Si V i W són espais vectorials sobre un cos F , aleshores una transformació lineal de V a W és un **homomorfisme de F -mòduls de V a W** .

Exemples.

- (1) Un anell R pot ser vist com un R -mòdul per la dreta (esquerra), usant la seva suma i producte d'anell com a suma i producte de mòdul per la dreta (esquerra). De forma més general, qualsevol ideal per la dreta (esquerra) de R és un R -mòdul per la dreta (esquerra).
- (2) Sigui G un grup abelià i $g \in G$. Si $n \in \mathbb{Z}$ definim el producte per escalars ng com

$$ng = \begin{cases} g + \dots + g & (n \text{ sumands si } n > 0) \\ 0 & \text{si } n = 0. \\ (-g) + \dots + (-g) & (-n \text{ sumands si } n < 0) \end{cases}$$

Usant aquest producte per escalars G és un \mathbb{Z} -mòdul.

A més, si G i H són grups abelians i $f : G \rightarrow H$ és un homomorfisme, aleshores f també és un homomorfisme de \mathbb{Z} -mòduls ja que per a $n > 0$

$$f(ng) = f(g + \dots + g) = f(g) + \dots + f(g) = nf(g)$$

$$\text{i } f(-g) = -f(g)$$

- (3) Sigui R un anell arbitrari. Aleshores R^n és un R -mòdul, tant per la dreta com per l'esquerra, considerant el producte per escalars

$$\begin{aligned} a(b_1, \dots, b_n) &= (ab_1, \dots, ab_n) \\ (b_1, \dots, b_n)a &= (b_1a, \dots, b_na) \end{aligned}$$

- (4) Sigui R un anell, aleshores el conjunt de les matrius $M_{m,n}(R)$ és un R -mòdul, tant per la dreta com per l'esquerra, considerant el producte per escalars

$$\begin{aligned} (aA)_{i,j} &= a(A)_{i,j} \\ (Aa)_{i,j} &= (A)_{i,j}a \end{aligned}$$

- (5) L'aplicació producte de matrius

$$\begin{aligned} M_m(R) \times M_{m,n}(R) &\rightarrow M_{m,n}(R) \\ (A, B) &\mapsto AB \end{aligned}$$

permet considerar $M_{m,n}$ com un $M_m(R)$ -mòdul per l'esquerra, i similarment, la següent aplicació producte de matrius

$$\begin{aligned} M_{m,n}(R) \times M_n(R) &\rightarrow M_{m,n}(R) \\ (A, B) &\mapsto AB \end{aligned}$$

permet considerar $M_{m,n}$ com un $M_n(R)$ -mòdul per la dreta.

- (6) Si R és un anell i $I \subset R$ un ideal, aleshores l'anell quocient R/I és un R -mòdul tant per la dreta i per l'esquerra considerant les aplicacions producte

$$\begin{aligned} R \times R/I &\rightarrow R/I \\ (a, b + I) &\mapsto ab + I \end{aligned}$$

$$\begin{aligned} R/I \times R &\rightarrow R/I \\ (a + I, b) &\mapsto ab + I \end{aligned}$$

- (7) Diem que M és una R -àlgebra si M és un R -mòdul i un anell, tals que la seva suma com a anell és la mateixa que com a mòdul, i la multiplicació a M i la multiplicació escalar per R satisfà:

$$r(m_1 m_2) = (r m_1) m_2 = m_1 (r m_2)$$

Per a cada $r \in R$, $m_1, m_2 \in M$.

- (a) Tot anell és una \mathbb{Z} -àlgebra.
 - (b) Si R és un anell abelià, R és una R -àlgebra.
 - (c) Si R és una anell commutatiu, aleshores l'anell de polinomis $R[X]$ i l'anell de matrius $M_n(R)$ són R -àlgebres.
 - (d) Donats dos anells R i S , i un homomorfisme d'anells $\phi : R \rightarrow S$ amb $\text{Im}(\phi) \subset Z(S) := \{a \in S : ab = ba \text{ per a tot } b \in S\}$, el centre de S . Si M és un S -mòdul, aleshores M també és un R -mòdul usant la multiplicació escalar $am = (\phi(a))m$. Com que S és un S -mòdul, tenim que S és un R -mòdul, a més, com que $\text{Im}(\phi) \subset C(S)$, podem concloure que S és una R -àlgebra.
- (8) Si M i N són R -mòduls, aleshores $\text{Hom}_R(M, N)$ és un grup abelià amb la suma $(f + g)(m) = f(m) + g(m)$.
 Si R és commutatiu, podem considerar $\text{Hom}_R(M, N)$ com un R -mòdul definint el producte $(af)(m) = a(f(m))$.
 Observem que imposar que R sigui commutatiu és necessari per a garantir que af sigui un homomorfisme de R -mòduls, ja que

$$(af)(rm) = a(f(rm)) = a(r(f(m))) = ar(f(m))$$

Només si R és commutatiu podem continuar: $ar(f(m)) = ra(f(m)) = r(af(m))$.

Observa també que $\text{End}_R(M)$ és a més un anell, usant la composició de homomorfismes de R -mòduls com a producte, i com que hi ha un homomorfisme d'anells $\phi : R \rightarrow \text{End}_R(M)$ induït per $\phi(a) = a1_M$, on 1_M denota el homomorfisme identitat de M , per l'exemple anterior (7) es dedueix que $\text{End}_r(M)$ és una R -àlgebra si R és un anell commutatiu.

- (9) Si G és un grup abelià, aleshores $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}, G) \cong G$. Per a veure-ho definim $\Phi : \text{Hom}_{\mathbb{Z}} \rightarrow G$ per $\Phi(f) = f(1)$.
 Veiem que Φ és un isomorfisme de \mathbb{Z} -mòduls: Hem de veure doncs que $\text{Ker}(\Phi) = 0_M$ i que $\text{Im}(\Phi(f)) = G$.
 El nucli només pot tenir un element, que és l'aplicació que envia tots els elements de \mathbb{Z} a 0 ja que si $f \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, G)$ es compleix per definició que $f(1) = 0$, i per tant $f(n) = f(1n) = f(1)f(n) = 0f(n) = 0$. D'altra banda $\text{Im}(\Phi) = G$ ja que per a tot $g \in G$ existeix un homomorfisme f induït per $f(1) = g$. Hem vist que Φ és bijectiu, falta veure que és un homomorfisme de \mathbb{Z} -mòduls. Per una banda

$$\Phi(f) + \Phi(g) = f(1) + g(1) = (f + g)(1) = \Phi(f + g)$$

D'altra banda

$$\Phi(nf) = \Phi(f + \dots + f) = (f + \dots + f)(1) = nf(1) = n\Phi(f)$$

Per tant, Φ és un isomorfisme de \mathbb{Z} -mòduls.

- (10) Generalitzant l'exemple anterior, si M és un R -mòdul, aleshores $\text{Hom}_R(R, M) \cong M$ com a \mathbb{Z} -mòduls per l'aplicació $\Phi : \text{Hom}_R(R, M) \rightarrow M$ on $\Phi(f) = f(1)$.

- (11) Sigui R un anell commutatiu, sigui M un R -mòdul, sigui $S \subset \text{End}_R(M)$ un subanell. Aleshores M és un S -mòdul per la multiplicació escalar $S \times M \rightarrow M$ definida per $(f, m) \mapsto f(m)$.
- (12) Sigui $T \in \text{End}_R(M)$, definim un homomorfisme d'anells $\phi : R[X] \rightarrow \text{End}_R(M)$ enviant X a T i $a \in R$ a $a1_M$. Per tant si

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

aleshores

$$\phi(f(X)) = a_01_M + a_1T + \cdots + a_nT^n$$

Denotarem $\phi(f(X))$ per $f(T)$ i $\text{Im}(\phi) = R[T]$, és a dir, $R[T]$ és el subanell de $\text{End}_R(M)$ format pels polinomis en T .

Aleshores M és un $R[T]$ -mòdul per la multiplicació $f(T)m = f(T)(m)$. Similarment, usant el homomorfisme $\phi : R[X] \rightarrow R[T]$ tenim que M és un $R[X]$ -mòdul usant la multiplicació $f(X)m = f(T)(m)$.

Aquest exemple és important, dona la base per aplicar la teoria de mòduls sobre dominis de ideals principals per a l'estudi de transformacions lineals.

- (13) Ara introduïrem un exemple concret a l'exemple anterior, sigui K un cos, i $T : K^2 \rightarrow K^2$ una transformació lineal definida per $T(u_1, u_2) = (0, u_1)$. Tenim que $T^2 = 0$, per tant, si $f(X) = a_0 + a_1X + \cdots + a_mX^m \in K[X]$ tenim $f(T) = a_01_{K^2} + a_1T$. Per tant, l'operació producte $f(X)u$ per $u \in K^2$ ve donada per

$$f(X) \cdot (u_1, u_2) = f(T)(u_1, u_2) = (a_01_{K^2} + a_1T)(u_1, u_2) = (a_0u_1, a_0u_2 + a_1u_1)$$

A.3 Submòduls i Quocients de Mòduls

Definició A.3.1. Sigui R un anell i M un R -mòdul. Diem que un subconjunt $N \subset M$ és un **submòdul** (o R -submòdul) de M si N és un subgrup del grup additiu M i també és un R -mòdul usant la multiplicació escalar a M , és a dir, N és un submòdul de M si és un subgrup de M tancat sota la multiplicació escalar.

Lema A.3.1 (Criteri de Submòdul). Si M és un R -mòdul i N és un subconjunt de M no buit, aleshores N és un submòdul si i només si $x + ry \in N$ per a tot $x, y \in N$ i tot $r \in R$.

Definició A.3.2. Si K és un cos i V un espai vectorial sobre K , un K -submòdul de V s'anomena **subespai vectorial** de V .

Exemples.

- (1) Si R és un anell, aleshores els R -submòduls del R -mòdul R són els ideals per l'esquerra de l'anell R .
- (2) Si G és un grup abelià, aleshores G és un \mathbb{Z} -mòdul i els \mathbb{Z} -submòduls de G són els subgrups de G .
- (3) Sigui $f : M \rightarrow N$ un homomorfisme de R -mòduls, aleshores $\text{Ker}(f) \subset M$ i $\text{Im}(f) \subset N$ són R -submòduls.

Es verifica usant el criteri de submòdul, en primer lloc observem que $\text{Ker}(f)$ i $\text{Im}(f)$ són conjunts no buits ja que $f(0) = 0$. Si $x, y \in \text{Ker}(f)$ i $r \in R$, es compleix $f(x + ry) = f(x) + rf(y) = 0$, per tant $x + ry \in \text{Ker}(f)$ i per tant $\text{Ker}(f)$ és un R -submòdul de M . D'altra banda si $x, y \in M$ i $r \in R$, tenim que $f(x) + rf(y) = f(x + ry)$ on $f(x)$ i $f(y)$ són elements arbitraris de $\text{Im}(f)$ i aplicant el criteri de submòdul queda verificat.

- (4) Sigui V un espai vectorial sobre un cos K i $T \in \text{End}_K(V)$ una transformació lineal fixada. Denotem per V_T a V amb l'estructura de $K[X]$ -mòdul determinada per la transformació lineal T .

Aleshores un subconjunt $W \subset V$ és un $K[X]$ -submòdul del mòdul V_T si i nomé si W és un subespai vectorial de V i $T(W) \subset W$, és a dir, W ha de ser un **T -subespai invariant** de V .

Per verificar-ho, observem que $X \cdot w = T(w)$ i si $a \in K$, tenim que $a \cdot w = aw$, és a dir, l'acció del polinomi constant $a \in K[X]$ sobre V és la multiplicació escalar ordinària, mentre que la acció del polinomi X sobre V és l'acció de T sobre V . Per tant, un $K[X]$ -submòdul de V_T ha de ser un T -subespai invariant de V .

Recíprocament, si W és un subespai vectorial de V tal que $T(W) \subset W$, tenim que $T^m(W) \subset W$ per a tot $m \geq 1$. Per tant si $f(X) \in F(X)$ i $w \in W$ tenim $f(X) \cdot w = f(T)(w) \in W$ per tant W és tancat sota la multiplicació escalar i per tant, W és un $K[X]$ -submòdul de V .

Definició A.3.3. Sigui M un R -mòdul i $N \subset M$ un submòdul, aleshores N és un subgrup d'un grup abelià M , per tant podem formar el quocient de grups M/N . Definim la multiplicació escalar del grup abelià M/N per $a(m + N) = am + N$ per a tot $a \in R$ i $m + N \in M/N$.

Com que N és un R -submòdul de M , aquesta operació està ben definida, ja que si $m + N = m' + N$ tenim que $m - m' \in N$ i per tant $am - am' = a(m - m') \in N$ de forma que $am + N = am' + N$.

El R -mòdul M/N considerat amb aquesta operació l'anomenem **mòdul quocient** de M respecte N .

Ara introduïrem els teoremes d'isomorfia de Noether per a mòduls, que són anàlegs als que hem vist per grups i anells (són conseqüència del Teorema de l'aplicació induïda).

Teorema A.3.2 (Primer Teorema d'isomorfia). *Sigui M i N mòduls sobre R i $f : M \rightarrow N$ un homomorfisme de R -mòduls. Aleshores*

$$M/\text{Ker}(f) \cong \text{Im}(f)$$

Demostració. pel primer Teorema d'isomorfia per a grups, tenim que existeix un isomorfisme de grups abelians $\bar{f} : M/K \rightarrow \text{Im}(f)$ definit per $\bar{f}(m + K) = f(m)$, ens falta veure que \bar{f} és un homomorfisme de R -mòduls. Observem que $\bar{f}(a(m + K)) = \bar{f}(am + K) = f(am) = af(m) = a\bar{f}(m + K)$ per a tot $m \in M$ i $a \in R$, que és el que ens faltava veure. \square

Teorema A.3.3 (Segon Teorema d'isomorfia). *Sigui M un R -mòdul i N i P submòduls. Aleshores hi ha un isomorfisme de R -mòduls:*

$$(N + P)/P \cong N/(N \cap P)$$

Demostració. Recorda que per definició $N + P = \{n + p : n \in N, p \in P\}$.

Sigui $\pi : M \rightarrow M/P$ la projecció natural i π_0 la restricció de π sobre N . Aleshores π_0 és un homomorfisme de R -mòduls amb $\text{Ker}(\pi_0) = N \cap P$ i $\text{Im}(\pi_0) = (N + P)/P$. Aplicant el primer Teorema d'isomorfia veiem el que volíem. \square

Teorema A.3.4 (Tercer Teorema d'isomorfia). *Sigui M un R -mòdul i N i P submòduls de M amb $P \subset N$. Aleshores*

$$M/N \cong (M/P)/(N/P)$$

Demostració. Definim $f : M/P \rightarrow M/N$ per $f(m+P) = m+N$, aquest homomorfisme de R -mòduls està ben definit i compleix

$$\text{Ker}(f) = \{m+P : m+N = N\} = \{m+P : m \in N\} = N/P$$

Aplicant el primer Teorema d'isomorfia queda provat. \square

Teorema A.3.5 (Teorema de correspondència). *Sigui M un R -mòdul, N un submòdul i $\pi : M \rightarrow M/N$ la projecció natural. Aleshores la funció $P \rightarrow P/N$ és una correspondència bijectiva entre el conjunt de tots els submòduls de M que contenen N i el conjunt de tots els submòduls de M/N .*

A.4 Mòduls lliures i Bases

Definició A.4.1. Sigui R un anell i S un subconjunt d'un R -mòdul M . Anomenem **combinació R -lineal** d'elements de S a qualsevol element que s'expressi de la forma

$$r_1s_1 + \cdots + r_ns_n$$

on n és un enter positiu, $r_1, \dots, r_n \in R$ i $s_1, \dots, s_n \in S$.

Denotem per a $\langle S \rangle$ al conjunt de totes les combinacions R -lineals d'elements de S , (considerem $0_M \in \langle S \rangle$ en tots els casos, encara que $S = \emptyset$). Una altra forma equivalent de pensar $\langle S \rangle$ és com la intersecció de tots els submòduls de M que contenen S .

En conseqüència diem que S **genera** M si $\langle S \rangle = M$

Definició A.4.2. Sigui R un anell i S un subconjunt d'un R -mòdul M , una **relació R -lineal** de S és qualsevol equació

$$r_1s_1 + \cdots + r_ns_n = 0_M$$

definida a M , on n és un enter positiu, s_1, \dots, s_n són n elements diferents de S i r_1, \dots, r_n són elements no nuls de R .

Diem que el **conjunt S és R -linealment independent** si no existeix cap relació R -lineal a S .

Anomenem per a **R -base** de M a qualsevol conjunt $B \subset M$ R -linealment independent que generi M .

Definició A.4.3. Diem que un R -mòdul M és **lliure** si té una R -base.

Exemples.

- (1) Sobre qualsevol anell R , el mòdul zero $\{0\}$ és lliure amb el conjunt buit \emptyset com a base.
- (2) Si R és un anell no trivial, l'anell de polinomis $R[x]$ és un R -mòdul lliure prenent com a base d'infinit elements $\{1, x, x^2, \dots\}$.
- (3) Si R és un anell no trivial i n un enter positiu, la suma directa

$$R^n := R \oplus \cdots \oplus R$$

és un R -mòdul lliure amb base $\{e_1, \dots, e_n\}$ on

$$e_i = (0, \dots, 0, 1, 0, \dots, 0)$$

té un 1 a la coordenada i -èssima i 0 a les altres.

Observem que e_1, \dots, e_n generen R^n ja que $(r_1, \dots, r_n) = r_1 e_1 + \dots + r_n e_n$, i trobar una combinació R -lineal entre els elements e_1, \dots, e_n és impossible ja que si es compleix $(r_1, \dots, r_n) = (0, \dots, 0)$ tenim necessàriament que $r_i = 0$ per a cada i .

- (4) Sigui R un anell no trivial i S un conjunt no buit. Una funció $f : S \rightarrow R$ diem que té **suport finit** si $f(s) = 0_R$ per a tots excepte un nombre finit de $s \in S$. Denotem per $\oplus_S R$ al conjunt de totes les funcions $f : S \rightarrow R$ amb suport finit. Sota la suma component a component i la multiplicació escalar, $\oplus_S R$ és un R -mòdul. Si $s \in S$, denotem per $\hat{s} : S \rightarrow R$ la funció característica de s definida per

$$\hat{s}(t) = \begin{cases} 1_R & \text{si } t = s \\ 0_R & \text{si } t \neq s \end{cases}$$

El conjunt $\hat{S} = \{\hat{s} : s \in S\}$ és una base de $\oplus_S R$ ja que si $f \in \oplus_S R$, aleshores

$$f = \sum_{s \in S} f(s) \hat{s}$$

i una combinació R -lineal

$$\sum_{s \in S} f(s) \hat{s}$$

és l'aplicació zero (= l'element zero de $\oplus_S R$) si i només si $f(s) = 0_R$ per a tot s .

Observem que si $S = \{s_1, \dots, s_n\}$ té n elements, existeix un isomorfisme

$$\begin{aligned} \oplus_S R &\rightarrow R^n \\ f &\mapsto (f(s_1), \dots, f(s_n)) \end{aligned}$$

on la base $\hat{s}_1, \dots, \hat{s}_n$, correspon a la base e_1, \dots, e_n .

En el següent Teorema veurem que qualsevol R -mòdul lliure és isomorf a un de la forma $\oplus_S R$.

Teorema A.4.1. *Sigui R un anell i B un subconjunt no buit d'un R -mòdul M . Són equivalents:*

(i) B és una R -base de M .

(ii) L'aplicació R -lineal $\phi : \oplus_B R \rightarrow M$, definida per

$$\phi(f) = \sum_{b \in B} f(b)b$$

és un isomorfisme.

(iii) Cada $m \in M$ es pot expressar de la forma

$$m = \sum_{b \in B} f(b)b$$

per un i només un $f \in \oplus_B R$.

Demostració. El fet que B generi M equival a l'existència de l'expressió (iii) i equival a l'exhaustivitat de ϕ .

El fet que B sigui R -linealment independent, equival a la unicitat de l'expressió (iii) i equival a la injectivitat de ϕ .

Els següent resultat mostra que per a definir un homomorfisme de R -mòduls sortint d'un mòdul lliure, és necessari i suficient especificar la imatge dels generadors. \square

Proposició A.4.1. (*Propietat universal dels R -mòduls lliures*). *Sigui M un R -mòdul i B un subconjunt no buit de M . Els següents afirmacions són equivalents:*

- (i) B és una base de M .
- (ii) Cada funció $\phi : B \rightarrow N$, de B cap a un R -mòdul N , té una i només una extensió a una aplicació R -lineal $\hat{\phi} : M \rightarrow N$.

Diem que una aplicació és R lineal si compleix:

- $\hat{\phi}(x + y) = \hat{\phi}(x) + \hat{\phi}(y)$ per a qualsevol $x, y \in M$.
- $\hat{\phi}(ax) = a\hat{\phi}(x)$ per a tot $a \in R$ i $x \in M$.

Demostració. • (i) \Rightarrow (ii): Sigui M i N R -mòduls, B una base de M i $\phi : B \rightarrow N$ una aplicació. Si $\hat{\phi} : M \rightarrow N$ és una aplicació R -lineal que exten ϕ , cal que

$$\hat{\phi}\left(\sum_{b \in B} f(b)b\right) = \sum_{b \in B} f(b)\phi(b) \quad \forall f \in \oplus_B R \quad (\text{A.1})$$

per tant, la unicitat de l'extensió queda garantida.

- (i) \Leftarrow (ii): Considerem en particular la funció $\phi : B \rightarrow \oplus_B R$ definida per $b \mapsto \hat{b}$ per a tot $b \in B$, on \hat{b} és la funció característica de l'element bàsic b .
Aplicant $\hat{\phi}$ a l'equació

$$\sum_{b \in B} f(b)b = 0_M$$

tenim que $f = 0 \in \oplus_B R$, i en conseqüència no existeix cap relació R -lineal a B .

Veiem ara que $M = \langle B \rangle$: Observem que les aplicacions f i la projecció $\bar{\pi} : M \rightarrow M/\langle B \rangle$ (definida per $m \mapsto \bar{m}$) envien tot $b \in B$ a $0 + \langle B \rangle$.

Si es compleix (ii), per unicitat d'extensió $f = \bar{\pi}$ són la mateixa aplicació, per tant $M/\langle B \rangle = 0$ i $M = \langle B \rangle$. \square

Corol·lari A.4.1. (I) Si $\psi : M \rightarrow N$ és un isomorfisme de R -mòduls i M és lliure amb base B , aleshores N és lliure amb base $\psi(B)$.

(II) Si M és un R -mòdul i n és un enter positiu, M té una base de n elements si i només si $M \cong R^n$.

(III) Si M és un R -mòdul i n és un enter positiu, hi ha una bijecció entre el conjunt d'isomorfismes $R^n \cong M$ cap al conjunt ordenat de bases de n elements de M , donat per

$$\psi \mapsto (\psi(e_1), \dots, \psi(e_n))$$

Demostració. • Observem que en les condicions de la proposició anterior, una extensió R -lineal $\hat{\phi} : M \rightarrow N$ és exhaustiva si i només si $\phi(B)$ genera N , i injectiva si i només si ϕ és injectiva i $\phi(B)$ és linealment independent.

(I) és conseqüència d'aquesta constatació, considerant ψ com una extensió R -lineal de la seva restricció a B .

- (II) és conseqüència de (III).
- (III) Denotem per e_1, \dots, e_n una base de R^n . Si $\phi : R^n \rightarrow M$ és un isomorfisme, per (I) tenim que $(\psi(e_1), \dots, \psi(e_n))$ és una base ordenada de M .
Sigui $\theta : R^n \rightarrow M$ un altre isomorfisme amb $\theta(e_i) = \psi(e_i)$ per a tot i , aleshores constatem que són iguals:

$$\theta \left(\sum_{i=1}^n r_i e_i \right) = \sum_{i=1}^n r_i \theta(e_i) = \sum_{i=1}^n r_i \psi(e_i) = \psi \left(\sum_{i=1}^n r_i e_i \right)$$

L'exhaustivitat ve donada per (A.1) i (III), ja que si considerem una base ordenada de M formada per n elements (b_1, \dots, b_n) , aleshores existeix un isomorfisme $\psi : R^n \rightarrow M$ amb $\psi(e_i) = b_i$ per a cada i .

□

El següent resultat ens permet construir a partir d'un conjunt S i un anell R , un R -mòdul lliure que tingui S com a base.

Proposició A.4.2. Si R és un anell no trivial, tot conjunt S és base d'un R -mòdul lliure $F_R(S)$.

Demostració. Si S és buit, és suficient $F_R(S) = \{0_R\}$. Si S és no buit, considerem el R -mòdul $\oplus_S R$, a l'exemple anterior hem vist que \hat{S} és una base. Al ser R no trivial tenim que $1_R \neq 0_R$, per tant la funció $S \rightarrow \hat{S}$ definida per $s \mapsto \hat{s}$ per cada $s \in S$ és bijectiva. Usant bijectivitat podem reemplaçar \hat{S} per S a $\oplus_S R$. Considerem $T := \oplus_S R - \hat{S}$, es compleix $S \cap T = \emptyset$ i per tant $h : S \cup T \rightarrow \oplus_S R$ definida per

$$h(x) = \begin{cases} x & \text{si } x \in T \\ \hat{x} & \text{si } x \in S \end{cases}$$

és una bijecció. Observem que $S \cup T$ és un R -mòdul sota les operacions

$$\begin{aligned} x + y &= h^{-1}(h(x) + h(y)) \\ rx &= h^{-1}(rh(x)) \end{aligned}$$

per $x, y \in S \cup T$ i $r \in R$. Aleshores definim $F_R(S)$ pel conjunt $S \cup T$ amb aquesta estructura de R -mòdul. Observem que h és un isomorfisme R -lineal de $F_R(S)$ a $\oplus_S R$, per tant, h^{-1} també és un isomorfisme R -lineal, i pel Corol·lari anterior (i) tenim que la base de $F_R(S)$ és $h^{-1}(\hat{S}) = S$ □

Observació. Donat un conjunt S , podem definir un mòdul lliure que tingui S com a base $(F_S(R))$, i donada una funció $\phi : S \rightarrow N$ de S cap a un R -mòdul N qualsevol, existeix una i només una extensió a una aplicació R -lineal $\hat{\phi} : F_S(R) \rightarrow N$.

Corol·lari A.4.1. Tot R -mòdul M és R -linealment isomorf a un quocient d'un R -mòdul. Per a tot enter n , tot R -mòdul generat per a un conjunt de n elements és R -linealment isomorf a un quocient de R^n .

A.5 Mòduls finitament generats

Definició A.5.1. Un R -mòdul és **cíclic** si està generat per un element. Si M és un R -mòdul i $m \in M$, el submòdul cíclic generat per m és $\langle \{m\} \rangle = \{rm : r \in R\}$, el denotem per Rm .

Un R -mòdul M és **finitament generat** (f.g) si és generat per a un conjunt finit $\{m_1, \dots, m_n\}$, o equivalentment, si M és la suma finita de submòduls cíclics:

$$M = Rm_1 + \dots + Rm_n$$

és a dir

$$M = \langle m_1, \dots, m_n \rangle = \text{Span}\{m_1, \dots, m_n\} = \{0 + r_1 m_1 + \dots + r_n m_n : r_1, \dots, r_n \in R\}$$

Lema A.5.1. Donat un R -mòdul M i $a_1, \dots, a_n \in M$ amb $n \in \mathbb{N}$. Tenim que $\langle a_1, \dots, a_n \rangle$ és un submòdul de M .

Demostració. Aplicarem el criteri de submòdul, primer observem que $\langle a_1, \dots, a_n \rangle$ no és buit, ja que $0 \in \langle a_1, \dots, a_n \rangle$.

Ara considerem $a, b \in \langle a_1, \dots, a_n \rangle$, per definició tenim que $a = r_1 a_1 + \dots + r_n a_n$ i $b = s_1 a_1 + \dots + s_n a_n$, on r_i i s_i són elements de R per a $i = 1, \dots, n$. Aleshores $a + b = (r_1 + s_1)a_1 + \dots + (r_n + s_n)a_n \in \langle a_1, \dots, a_n \rangle$.

Similarment si $b \in \langle a_1, \dots, a_n \rangle$ i $r \in R$, tenim que $rb = (rs_1)a_1 + \dots + (rs_n)a_n \in \langle a_1, \dots, a_n \rangle$. Per tant, com que $a + rb \in R$, podem aplicar el criteri de submòdul i veiem el que volíem. \square

Definició A.5.2. Sigui S un subconjunt d'un R -mòdul M , aleshores $\langle S \rangle$ denota la intersecció de tots els submòduls de M que contenen S . L'anomenem el **submòdul de M generat per S** , i els elements de S els anomenem **generadors** de $\langle S \rangle$ com a exemple de generació de mòdul per conjunts.

És a dir, $\langle S \rangle$ és el submòdul de M que conté S i està contingut a tot submòdul M que conté S , en altres paraules, és el submòdul més petit de M que conté S .

Exemples.

- (1) Sigui R un anell, si considerem R com un R -mòdul, tenim que R com a mòdul és cíclic, i per tant finitament generat: $\langle 1 \rangle = R$.
- (2) Si considerem $R \oplus R$ com a R -mòdul veiem que és finitament generat per $\{(1, 0), (0, 1)\}$.
- (3) Tot mòdul finit és finitament generat.
- (4) \mathbb{Q} no és finitament generat com a \mathbb{Z} -mòdul, veiem-ho, suposem que $\{p_1/q_1, \dots, p_n/q_n\}$ és un conjunt generador de \mathbb{Q} , sigui q el mínim comú múltiple dels generadors ($q = \text{mcm}(q_1, \dots, q_n)$). Considerem ara $1/(q+1)$, com que $q+1$ no divideix q , $1/(q+1) \notin \langle p_1/q_1, \dots, p_n/q_n \rangle$ i per tant, els nombres racionals no són f.g. com a \mathbb{Z} -mòdul.
- (5) El concepte de R -mòdul generalitza el concepte de grup cíclic. De forma que, un grup abelià G és cíclic (com a grup abelià) si i només si és cíclic com a \mathbb{Z} -mòdul.
- (6) Com que els R -submòduls N de R són ideals, tenim que si aquest R és un *DIP*, qualsevol R -submòdul N ha de ser cíclic.

En un espai vectorial sobre un cos, dues bases qualsevols d'un mateix espai vectorial tenen el mateix cardinal, en un mòdul sobre un anell, de moment podem afirmar el següent:

Proposició A.5.1. Si M és un R -mòdul lliure no finitament generat, dues bases qualsevols de M tenen el mateix cardinal.

Si M és un mòdul lliure f.g., aleshores tota base de M és finita.

Demostració. Sigui M un R -mòdul generat pel conjunt T , i amb base B ; per a cada $t \in T$ existeix un subconjunt finit $B(t) \subset B$, tal que $t \in \langle B(t) \rangle$.

Com que T genera M , $U := \cup_{t \in T} B(t)$ també genera M ja que per construcció $\langle T \rangle \subset \langle U \rangle \subset M$.

Observem que tot element de $B - U$, pertany a M , i $M = \langle U \rangle$, per tant, $B = U$.

- Si M no és finitament generat, T és infinit; com que cada $B(t)$ està contingut en un conjunt numerable $\text{card}(U) \leq \text{card}(T)$, i per construcció $(U) \geq \text{card}(T)$, per tant es compleix la igualtat.
- Si M és f.g, T és finit, per tant cada $B(t)$ és finit i la base $B = U$ està formada per unió finita de conjunts finits.

□

Bibliografia

- [1] Jonathan Rosenberg, *Algebraic K-Theory and Its Applications*, Springer-Verlag New York, Graduate Texts in Mathematics Vol. 147 1st edition, 1994.
- [2] Bruce A. Magurn, *An Algebraic Introduction to K-Theory*, Cambridge University Press; 1 edition, Encyclopedia of Mathematics and its Applications (Book 87) 1st edition, 2002.
- [3] Mark Reeder, *Introduction to Lie Groups*, Department of Mathematics Boston College <https://www2.bc.edu/mark-reeder/LieGroups.pdf> 2016.
- [4] Emil Artin, *Geometric Algebra*, Interscience Publishers 1957.
- [5] Helmer Aslaksen, *Quaternionic Determinants*, Department of Mathematics National University of Singapore <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.877&rep=rep1&type=pdf>.
- [6] Fred Richman, *Non Trivial Uses of Trivial Rings*, Proceedings of the American Mathematical Society. Vol 103, Number 4 <http://www.ams.org/journals/proc/1988-103-04/S0002-9939-1988-0954974-5/S0002-9939-1988-0954974-5.pdf>. August 1988.
- [7] Charles A. Weibel, *The K-book, An introduction to Algebraic K-theory*, American Mathematical Society Graduate Studies in Mathematics Volume 145.
- [8] I. N. Herstein, *Non-commutative Ring Theory*, Mathematical Association of America Textbooks University of Chicago September 2005 Lemma 1.1.3.
- [9] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag New York, Graduate Texts in Mathematics Vol. 150 1995
- [10] William A. Adkins, Steven H. Weintraub *Algebra*, Springer-Verlag, Graduate Texts in Mathematics Vol. 136 1992