Classical Algebraic K-Theory (K_0, K_1)

A project submitted to
Department of Mathematics
University of Mumbai
by

Bhoris Dhanjal

Semester III

2024-2025

Certificate

This is to certify the Semester III Research Project titled 'Classical Algebraic K-Theory (K_0, K_1)' in partial fulfilment of the requirements for the degree of M.Sc. Mathematics submitted by Mr. Bhoris Dhanjal is approved for submission.

Dr. Anuradha Garge
(Project Guide)

Prof. B. S. Desale
(Head of Department)

Date:

Acknowledgements

I would like to express my deepest gratitude to my guide, Dr. Anuradha Garge, for her invaluable guidance, encouragement, and support throughout this research project. Her insights and expertise were instrumental in shaping this work.

I am also thankful to my family and friends for their unwavering support and encouragement, which have been a constant source of strength during this journey.

Abstract

This project explores key results in classical algebraic K-theory, focusing on the Grothendieck groups K_0, Whitehead groups K_1, and its various applications. Topics include the Quillen–Suslin theorem, and Suslin's work on unimodular vectors linear groups.

Contents

Chapter 1

Projective modules

We begin with with basic prerequisites in homological algebra. Introducing the concept of a projective module.

Unless otherwise specified, all rings considered are assumed to be commutative with unity.

1.1 Chain complexes and exact sequences

Definition 1.1.1 (Chain complex)**.** *A chain complex* $(A_\bullet, \varphi_\bullet)$ *is a collection of modules over a commutative ring and homomorphisms* $\varphi_i : A_i \to A_{i-1}$ *such that* $\varphi_i \varphi_{i+1} = 0$*.*

$$\cdots \xrightarrow{\varphi_{i+2}} A_{i+1} \xrightarrow{\varphi_{i+1}} A_i \xrightarrow{\varphi_i} A_{i-1} \xrightarrow{\varphi_{i-1}} \cdots$$

Definition 1.1.2 (Chain (Co)Homology)**.** *The homology of the complex at* F_i *is denoted as its* i^{th} *homology defined as follows,*

$$H_i A := \ker \varphi_i / \mathrm{im} \varphi_{i+1}.$$

Reversing the arrows gives us the analogous definitions for cochain complexes and cohomology.

The homomorphisms are often called ‘boundary operators’ or ‘differentials’. This nomenclature is motivated by de Rahm cohomology. Furthermore elements of $\ker \varphi_i$ are called ‘cycles’ and elements of $\mathrm{im}\varphi_{i+1}$ are called boundaries, this echoes the aphorism ‘cycles modulo boundaries’ often encountered in singular homology.

Definition 1.1.3 (Exact sequence)**.** *A chain complex is said to be exact if all its homologies are zero. In particular it is exact at one object if its homology there is zero.*

An exact sequence of the form

$$0 \to A \to B \to C \to 0$$

is referred to as short exact sequence. Note that due to the exactness conditions $A \to B$ is injective and $B \to C$ is surjective.

Proposition 1.1.4 (Splitting lemma)**.** *For a short exact sequence*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

the following are equivalent:

1. *The sequence splits, i.e.* $B \cong A \oplus C$.
2. *Left split: There is a morphism* $h : B \to A$*, such that* $hf = 1_A$.
3. *Right split: There is a module morphism* $i : C \to B$ *such that* $gi = 1_C$.

1.2 Projective modules

The category of finitely generated projective modules is the main object of study in algebraic K-theory. This is largely motivated by a theorem due to Swan's which we will prove in the next project.

Recall the definition of a free module.

Definition 1.2.1 (Free module of rank n)**.** *A module over a ring A is said to be free with rank n if it is isomorphism to a module of the form* A^n.

In particular this means that there exists a linearly independent spanning set of the module with n elements.

Note homomorphisms from free modules to other modules are determined by the image of their generators.

Definition 1.2.2 (Projective module)**.** *A module P is said to be projective if it satisfies the following lifting property, every morphism from P to N factors through an epimorphism into N. Note that the lift need not be unique.*

$$\begin{tikzcd}
 & M \arrow[d, two heads] \\
P \arrow[ur, dashed] \arrow[r] & N
\end{tikzcd}$$

Proposition 1.2.3 (Equivalent definitions of projectivity)**.** *The following are equivalent,*

1. *P is projective.*

2. *For all epimorphisms between $M \twoheadrightarrow N$, the induced map* $\mathrm{Hom}(P, g)$: $\mathrm{Hom}(P, M) \to \mathrm{Hom}(P, N)$ *sending $f \mapsto g \circ f$ for $g : M \to N$ and $f : P \to M$ is an epimorphism.*

3. *For some epimorphism from a free module F to P,* $\mathrm{Hom}(P, F) \to \mathrm{Hom}(P, P)$ *is an epimorphism.*

4. *There exists Q s.t. $P \oplus Q$ is free.*

5. *Short exact sequences of the form $0 \to A \to B \to P \to 0$ split, i.e. isomorphic to another short exact where middle term is $A \oplus P$.* [1]

Proof. $1 \iff 2$ is restatement of definitions.

$2 \implies 3$ is also just substitution.

$3 \implies 4$ consider a map in the preimage of identity in $\mathrm{Hom}(P, P)$ which is a splitting (inverse) of the epimorphism F into P,

$$\begin{tikzcd}
 & P \arrow[dl, "f"'] \arrow[dr, dashed, two heads, "\mathrm{Id}_P = g \circ f"] \arrow[d, phantom, "\Longrightarrow"] & \\
F \arrow[rr, two heads, "g"] & & P
\end{tikzcd}$$

Now we have a short exact sequence $0 \to \ker g \to F \to P \to 0$, and also $f \circ g$ is idempotent so it naturally admits a decomposition $F = \mathrm{Im}(f \circ g) \oplus$

[1] In general any epimorphisms into projective objects split (i.e. have an inverse).

$\mathrm{Ker}(f \circ g)$[2]$=\mathrm{Im}(g) \oplus \mathrm{Ker}(g)$ the first by the 1st isomorphism theorem and the second by f being a mono.

$4 \implies 2$ simply as $\mathrm{Hom}(P \oplus Q, -) = \mathrm{Hom}(P, -) \oplus \mathrm{Hom}(Q, -)$

$1 \iff 5$ To show that $0 \to A \to B \xrightarrow{\varphi} P$ splits we need to show that there exists a $\psi : P \to B$ such that $\varphi \circ \psi = 1_P$. This is just obtained by the definition of P being projective.

$$\begin{tikzcd}
 & M \arrow[d, "\varphi"] \\
P \arrow[ur, dashed, "\psi"] \arrow[r, "="] & P
\end{tikzcd}$$

$\square$

Lemma 1.2.4 (Free modules are projective)**.**

Proof. Consider the preimages of images of basis of P in N, that lie in M. Then map basis elements from P into these preimages. $\square$

Example 1.2.5 (Projective modules are not always free)**.** *Let R, S be two non-trivial commutative rings with unity, consider $R \oplus S$ as a (free) module over itself. Consider $R \oplus \{0\}$ as a submodule of $R \oplus S$, it is projective as it is a direct summand of $R \oplus S$. However, it cannot be free as $(R \oplus \{0\})^n \ncong R \oplus S$ for any n.*

Theorem 1.2.6. *Projective finitely generated modules over local rings are free.*

Proof. Pick a minimal set of generators and see its residue classes in $M/\mathfrak{m}M$ as the basis of it as a vector space over $R/\mathfrak{m}$.

Now as for some free module $F, F = \varphi(M) \oplus K$ for some K and some homomorphism $\varphi : M \to F$, (by definition of projective module), we get

$$M/\mathfrak{m}M \cong F/\mathfrak{m}F = (R/\mathfrak{m})^n \cong R^n \otimes R/\mathfrak{m} \cong F \otimes R/\mathfrak{m} \cong (\varphi(M) \oplus K) \otimes R/\mathfrak{m}$$

Finally we get $M/\mathfrak{m}M \cong M/\mathfrak{m}M \oplus K/\mathfrak{m}K \implies K = \mathfrak{m}K \implies K = 0$ by Nakayamas lemma. $\square$

[2] For some idempotent e, $1 - e$ is also an idempotent and images under these two mappings decompose any module, furthermore image of $1 - e$ is just kernel of e

This holds for not necessarily finitely generated modules too refer to [**?**, Theorem 2.5] .

Using the convention of [**?**] we define the rank of a projective module as such.

Definition 1.2.7 (Rank of a finitely generated projective module)**.** *For any finitely generated projective module P over commutative ring A the localization $P_{\mathfrak{p}} = P \otimes_A A_{\mathfrak{p}}$ is also a finitely generated $A_{\mathfrak{p}}$ module, but $P_{\mathfrak{p}}$ being local is free by Theorem 1.2.6. So the local rank of P is defined as the rank of the free $P_{\mathfrak{p}}$ module.*

This induces a map $\phi : \mathrm{Spec}(A) \to \mathbb{Z}$ sending each $\mathfrak{p}$ to the local rank of P. If ϕ is constant and the rank of P is the same for all localizations then we refer to that as the rank of P.

Proposition 1.2.8. *For a principal ideal domain A a submodule M of a free module of finite rank say A^n is free, and the submodule has rank $\leq n$.*

Proof. We prove this by induction on n. When $n = 0$ there is nothing to prove. For $n = 1$ due to the fact that A is a principal ideal domain the submodules of A (ideals) are one generated i.e. they are rank 1 free modules of A.

Proceed via induction. Now consider the case when $n = k$.

Let $M \subset A^k$ be non zero. Consider the componentwise projection maps $p_i : A^k \to A$ for each i. Then $\pi_i(M) \neq \{0\}$ for some i. Therefore $p_i(M)$ is a non-zero ideal in A, i.e. free with rank 1. Also, $\ker p_i \cap M$ is a submodule of $\ker p_i$ which is itself free of rank $n-1$. Therefore rank of $\ker p_i \cap M$ is $\leq n-1$. Let a be a generator for $p_i(M)$ consider some preimage of it as a_p.

Now $M = \ker p_i \cap M \oplus \langle a_p \rangle$. If $\{a_1, a_2, \cdots a_m\}$ is a basis of $\ker p_i \cap M$, then $\{a_1, a_2, \cdots a_m, a_p\}$ is a basis of M. Hence rank of M equals $m + 1 \leq n$. □

Proposition 1.2.9. *Projective finitely generated modules over principal ideal domains are free.*

Proof. Every finitely generated projective module P is a direct summand of a free module F meaning it is a submodule of F and by Proposition 1.2.8 it is free. □

Definition 1.2.10 (Stably isomorphic)**.** *Two $A-$modules M, N are said to be stably isomorphic if there exists r such that $M \oplus A^r \cong M \oplus A^r$.*

Definition 1.2.11 (Stably free module)**.** *An A module M is stably free if there exists a finitely generated free module F such that $M \oplus F$ is free, i.e. if M is stably isomorphic to a finitely generated free A module.*

1.3 Resolutions

Definition 1.3.1. *[Left resolution] Given a module M its left resolution is given by the data of a exact sequence $(A_\bullet, \varphi_\bullet)$ into M as such,*

$$\cdots \to A_1 \to A_0 \xrightarrow{\epsilon} M \to 0$$

where ϵ is called the augmentation map, if the exact sequence is free its a free resolution and such for projective.

If we have a cochain complex instead it forms a right resolution and if its elements are injective we call them injective resolutions.

We cover a result about stably free modules. We will revisit this in greater detail in further sections.

Lemma 1.3.2. *A projective module is stably free iff if has a finite free resolution.*

Proof. Say $M \in A-$Mod and is projective. Then M is stably free implies $M \oplus A^n \cong A^m$ for some n, m. So M has a finite free resolution given by

$$0 \to A^n \to A^m \to M \to 0$$

Conversely if M is a projective module with a finite free resolution.

$$0 \to F_n \to \cdots \to F_0 \to M \to 0$$

for F_i free modules over A.

We proceed via induction on n. If $n = 0$ then we are done as simply M is free. Let M_1 denote the kernel of $F_0 \to M$. Since M is projective, $F_0 = M \oplus M_1$. Now M_1 is projective and has a free resolution of length $< n$.

Thus, by the induction hypothesis, $M_1 \oplus F$ is free for some finite free module F, i.e. M_1 is stably free.

Consequently $F_0 \oplus F$ is trivially finitely free and so $F_0 \oplus F \cong (M \oplus M_1) \oplus F \cong M \oplus (M_1 \oplus F)$ is finite free, i.e. M is stably free. $\square$

Chapter 2

Grothendieck group K_0

The Grothendieck group K_0 arises from the natural idea of wanting to extending a commutative monoid to a group in a universal manner. This concept finds its roots in many naturally occurring mathematical structures, such as finitely generated projective modules or vector bundles.

Recall a monoid is an algebraic object consisting of a set of symbols A with a associative binary operation $+$ and an identity element e (where $a + e = e + a = a$ for all $a \in A$).

2.1 Definitions and basic results

The group completion of a monoid proceeds as such. We begin with a commutative monoid A to complete it into a group we formally add inverses for each symbol $[a] \in A$. Consider the free group on the set of symbols in the monoid labelled as $F(A)$. Now quotient away all the nontrivial monoidal relations $F(A)/\sim$ where $[a + b] \sim [a] + [b] \sim [b] + [a] \sim [b + a]$.

This gives us the group completion of a monoid, i.e. the smallest group which has A as a submonoid.

Proposition 2.1.1. *The group completion of the natural numbers* $\mathbb{N}$ *is* $\mathbb{Z}$*. Following the group completion procedure as described above we obtain a formal inverse symbol* $[b]$ *for each symbol* $[a] \in \mathbb{N}$*, i.e. a symbol* $[b]$ *such that* $[b] + [a] = [a] + [b] = [0]$ *for all* $[a] \in \mathbb{N}$*, but note that this is naturally isomorphic to* $\mathbb{Z}$ *as* $[b] \mapsto [-a]$*.*

Definition 2.1.2 (K_0 of a monoid (Group completion functor)). *For a commutative monoid A, the group completion of A is denoted as $K_0(A)$.*

Definition 2.1.3 (Reduced K_0 group of a commutative monoid A). *There is a canonical homomorphism $i : \mathbb{Z} \to K_0(A)$ given by $z \mapsto z[m] = \underbrace{[m] + \cdots + [m]}_{z \text{ times}}$ the reduced K group is defined as $\tilde{K}_0(A) := K_0(A)/\mathrm{Im}\ i$.*

We return now to the case of modules over a commutative ring A.

Recall the notion of stable isomorphisms and stably free modules Definitions 1.2.10 and 1.2.11.

Definition 2.1.4 (K_0 for a ring A). *Consider the stable isomorphism classes of finitely generated projective modules over A denoted as* $\mathrm{Proj}(A)$*. This forms a commutative monoid so $K_0(A)$ is defined as $K_0(\mathrm{Proj}(A))$.*

Definition 2.1.5 (G_0 for a ring A). *The group completion of $M(A)$ the monoid of all finitely generated modules over A is denoted as $G_0(A)$. There is a canonical inclusion map $K_0(A) \to G_0(A)$.*

The reason we require the caveat of finitely generated projective modules instead of simply considering the class of all projective modules is because for the non finitely generated case $K_0(A)$ becomes trivial as we see below.

Proposition 2.1.6 (Eilenberg Swindle). *If we consider R^∞ as a non finitely generated free module over a ring R if $P \oplus Q \equiv R^n$ then*

$$P \oplus R^\infty \cong P \oplus (Q \oplus P) \oplus (Q \oplus P) \oplus \cdots \equiv (P \oplus Q) \oplus (P \oplus Q) \oplus \cdots \equiv R^\infty$$

but this relation would imply $[P] = 0$ for all projectives.

2.2 Computing K_0 groups with idempotent matrices and Morita invariance

We now see a few examples of computations of K_0. We must first prove a result about the invariant basis property. Recall that a ring A has the invariant basis property if $A^n \cong A^m$ implies $n = m$.

A division ring (also called a skew field) is any nontrivial ring in which every non-zero element has a multiplicative inverse. Division rings need not be commutative, in fact commutative division ring is simply a field.

Example 2.2.1 (Non-commutative division ring). *The set of quaternions* $\mathbb{H}$ *forms a non-commutative division ring.*

Proposition 2.2.2. *Any division ring* A *has the invariant basis property.*

Proof. Consider a free A-module M with two finite bases $B = \{b_1, \ldots, b_n\}$ and $C = \{c_1, \ldots, c_m\}$, then if we prove $n = m$ we are done. We prove with induction on n.

If $n = 1$, then $B = \{b_1\}$. If $C = \{c_1, \ldots, c_m\}$ for some $m > 1$, we can express the c_i in terms of b_1 as, $c_1 = a_1 b_1$ and $c_2 = a_2 b_1$ where $a_1, a_2 \in A$ and $a_1, a_2 \neq 0$. Then $a_1^{-1} c_1 - a_2^{-1} c_2 = 0$, contradicting the linear independence of C. Therefore $m = 1 = n$.

Proceeding inductively assume the statement holds for $n = k$. Let M be a free A-module with a basis $B = \{b_1, \ldots, b_{k+1}\}$ and let $C = \{c_1, \ldots, c_m\}$ be another basis.

Since B spans M, we can write b_{k+1} as a linear combination of the c_i: $b_{k+1} = a_1 c_1 + \cdots + a_m c_m$ for some $a_i \in A$. Since $b_{k+1} \neq 0$, at least one $a_i \neq 0$. Without loss of generality, assume $a_m \neq 0$.

Consider the quotient module $M/(b_{k+1})$. The set $\{b_1, \ldots, b_k\}$ forms a basis for $M/(b_{k+1})$. Similarly, $\{c_1, \ldots, c_{m-1}\}$ is a basis for $M/(b_{k+1})$. Applying the inductive hypothesis to $M/(b_{k+1})$, we have $k = m-1$. Therefore $k+1 = m$. $\square$

Corollary 2.2.3. *Nonzero commutative rings* A *have invariant basis property.*

Proof. For a free $A-$module M with basis $B = \{b_1, \ldots, b_n\}$, under the canonical surjection $A \to A/\mathfrak{m}$, $M/\mathfrak{m}M$ is also a free module over $A/\mathfrak{m}$ with basis $\{b_1 + \mathfrak{m}M, \ldots, b_n + \mathfrak{m}M\}$. Since every basis for $M/\mathfrak{m}M$ has n elements due to the fact that $A/\mathfrak{m}$ is a field, Proposition 2.2.2 shows it has invariant basis property. This implies any basis of M also has only n elements, i.e. A itself has the invariant basis property. $\square$

Proposition 2.2.4. *If* A *is a field/division ring/local ring/principal ideal domain then* $K_0(A) \cong \mathbb{Z}$.

Proof. For fields and division rings this is true due to all finitely generated modules being free, i.e. having a basis. We prove this directly for division rings for simplicity.

The similar linear algebraic proof extends to division rings for M a module over division ring A. Pick a maximally linearly independent subset B by Zorn's lemma. To show B is a generating set, the argument uses B's maximality. If $m \in M$ then, if $m \in B$ we are done. If $m \notin B$ then $B \cup \{m\}$ is linearly dependent by maximality of B therefore there exists $a \in A$ such that $am \in \text{span}(B)$ for some $a \neq 0$ and since a is invertible due to F being a division ring we have $m \in \text{span}(B)$. Therefore, B must span M, making it a basis and so $M \cong A^n$.

Similarly as seen in Theorem 1.2.6 and Proposition 1.2.9 finitely generated projective modules in a local ring/principal ideal domain are free.

So in each case $\text{Proj}(A) \cong \mathbb{N}$ so its group completion is $\mathbb{Z}$.

Throughout the proof we have implicitly assumed A has the invariant basis property which was proved above in Proposition 2.2.2 and Corollary 2.2.3 □

Lemma 2.2.5. *For commutative ring A, $K_0(A) \cong \mathbb{Z}$ implies projective modules over A are stably free.*

Proof. For a commutative ring A, $K_0(A) \cong \mathbb{Z}$ implies $\text{Spec}(A)$ is connected. For if not then there exists a non trivial idempotent in A which results in a splitting of A as a product which would contradict $\text{Spec}(A)$ being connected.

In light of Definition 1.2.7 we know that the rank of the projective modules must be constant due to the connectedness of $\text{Spec}(A)$ and the fact that the only connected components in $\mathbb{Z}$ are singletons.

So the rank map $\phi : K_0(A) \to \mathbb{Z}$ defined as $P \mapsto \text{Rank}(P)$ is well defined and surjective. A with rank 1 maps to 1, i.e. the generator of $\mathbb{Z}$. By our assumption, this is an isomorphism.

So any $[P] = n = [A]^n = [A^n]$ i.e. there exists Q projective such that $Q \oplus P \cong Q \oplus A^n$, i.e. P is stably free. □

We end this section with computing K_0 for semisimple rings. We first define what is means for a ring to be simple.

Definition 2.2.6 (Simple ring)**.** *A simple ring is a non-zero ring which have no non-trivial two-sided ideals.*

Example 2.2.7. *A commutative ring is simple iff it is a field.*

Example 2.2.8. *All division rings are simple rings.*

Example 2.2.9. *Not all division rings are simple consider $M_n(F)$ for some field F not all elements need be invertible.*

A simple module is naturally now any module which is non-zero and has no non-trivial submodules.

Lemma 2.2.10 (Schur's lemma)**.** *If A is any ring and M is a simple $R-$module then* $\mathrm{End}_A(M)$ *is a division ring.*

Proof. Let $f \in \mathrm{End}_A(M)$ be non-zero. Then $\mathrm{Im}(f) \neq 0, \ker(f) \neq M$, but since they are both submodules of M it follows due to simplicity that $\mathrm{Im}(f) = M, \ker(f) = 0$. That is to say all non-zero endomorphisms are invertible, i.e. it is a division ring. □

Now we move onto semisimple rings. There are various equivalent definitions of a semisimple ring.

Definition 2.2.11 (Semisimple ring)**.** *A ring A is called semisimple if*

- *A is Artinian with trivial Jacobson ideal.*
- *A is a finite product of simple Artinian rings.*
- *Every left/right $A-$module is projective.*

A useful characteristic of semisimple rings is the Wedderburn-Artin theorem (see [**?**][3.5] for a proof).

Theorem 2.2.12 (Wedderburn-Artin)**.** *A ring A is semisimple iff it is isomorphic to a direct product of $n_i \times n_i$ matrix rings over division rings D_i, i.e. $A \cong \prod_{i=1}^{r} M_{n_i}(D_i)$ where $D_i = \mathrm{Hom}_A(V_i, V_i), \dim_{D_i}(V_i) = n_i$ for V_i the simple A-modules components of A.*

We now discuss the role of idempotent matrices in computing K_0 following [**?**] this is presented in detail in [**?**]. We claim that idempotent matrices over A are in a one to one correspondence to finitely generated projective modules.

For a finitely generated projective module P over A, such that $P \oplus Q \cong A^n$ we can define a $R-$module homomorphism which is identity restricted to P and zero else. This is clearly an idempotent element in $M_n(A)$, i.e. P is represented by a $n \times n$ matrix over A.

Conversely any idempotent matrix $e \in M_n(A)$ determines a projective. Simply consider the associated module morphism induced by the matrix e and then the image under e is projective, i.e. eA^n. This is true because $A \cong eA^n \oplus (1-e)A^n$ [1].

[1]Idempotent property is used to show $eA^n \cap (1-e)A^n = 0$ since $e^2 = e \implies e(1)$

We must make a note of the fact that different idempotent matrices may induce projective modules in the same isomorphism class. This is made precise in the following result.

Proposition 2.2.13. *If e, f are idempotent matrices over A of possibly different sizes then the associated finitely generated projective modules are isomorphic iff e, f are conjugate over a larger common matrix group of order r (obtained by placing the matrices in the top left corner of a larger 0 matrix).*

Proof. Suppose we have two conjugate idempotent matrices $e, f \in M_n(A)$, i.e. there exists $u \in GL_n(A)$ such that $ueu^{-1} = f$ or $ue = fu$. If x lies in the image of e say $x = ey$ then ux lies in the image of f since $ux = uey = fuy = f(uy)$. By symmetry using u^{-1} we see also that, elements from fA^n belong to eA^n.

Now conversely, assume the projective modules corresponding to idempotent matrices e and f are isomorphic. Let $e \in M_n(A)$ and $f \in M_m(A)$. This isomorphism $\mathrm{Im}e \cong \mathrm{Im}f$, i.e. $eA^n \cong fA^m$, extends to an A-module homomorphism $\tilde{f} \colon A^n \to A^m$, similarly $\tilde{f}^{-1} = \tilde{g} \colon A^m \to A^n$.

We can represent $\tilde{f}$ and $\tilde{g}$ by right multiplication with matrices $\alpha \in M_{m,n}(A)$ and $\beta \in M_{n,m}(A)$ respectively. These obey the following relations $\alpha\beta = f, \beta\alpha = e, \alpha = \alpha e = f\alpha, \beta = \beta f = e\beta$.

Choose $r = n + m$, claim that the following block matrix is invertible

$$\varphi = \begin{bmatrix} 1-e & \beta \\ \alpha & 1-f \end{bmatrix}$$

and is conjugate to $\begin{bmatrix} e & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & f \end{bmatrix}$. This is true since $\varphi^2 = I_r$. A computation then shows that

$$\varphi \begin{bmatrix} e & 0 \\ 0 & 0 \end{bmatrix} \varphi = \varphi \begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & f \end{bmatrix}$$

A permutation matrix then conjugates $\begin{bmatrix} 0 & 0 \\ 0 & f \end{bmatrix}$ to $\begin{bmatrix} f & 0 \\ 0 & 0 \end{bmatrix}$. Thus e and f are conjugate after appropriate embedding into $GL_r(A)$ and therefore represent isomorphic modules. □

Consider $GL_n(A) \subset GL_{n+1}(A)$ by placing the $n \times n$ matrix in the top right. In this manner we have a filtered system and we can define $GL(A) =$

$\lim_{\to} GL_i(A)$ as the colimit. Similarly define $M(A)$. Denote the set of idempotent matrices in $M(A)$ as $\mathrm{Idem}(A)$ so we have that the group $GL(A)$ acts on the set $\mathrm{Idem}(A)$ by conjugation.

With the above discussion in mind we now have a alternate description for the monoid $\mathrm{Proj}(A)$ in terms of idempotent matrices. In particular $\mathrm{Proj}(A)$ corresponds to the conjugacy classes of the action of $GL(A)$ on $\mathrm{Idem}(A)$. The monoid operation $e + f$ is the block matrix $\begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$.

Corollary 2.2.14 (Morita invariance of K_0)**.** *Let A be a ring and $n \in \mathbb{N}$ arbitrary. Then $K_0(A) \cong K_0(M_n(A))$.*

Proof. Note that the infinite general linear matrices over $M_n(A)$ and A are canonically equivalent, i.e. $GL(M_n(A)) = GL(A)$ in particular their infinite idempotent matrices are also equivalent $\mathrm{Idem}(M_n(A)) = \mathrm{Idem}(A)$. Consequently by the correspondence between idempotent matrices and projective modules their monoid of finitely generated protectives are the same meaning their group completions are isomorphic. $\square$

Corollary 2.2.15. *For commutative ring A if $A \cong A_1 \times A_2$ for rings. Then $K_0(A) \cong K_0(A_1) \times K_0(A_2)$.*

Proof. Notice that $GL(A) \cong GL(A_1 \times A_2) \cong GL(A_1) \times GL(A_2)$ and $\mathrm{Idem}(A) \cong \mathrm{Idem}(A_1 \times A_2) \cong \mathrm{Idem}(A_1) \times \mathrm{Idem}(A_2)$. $\square$

Corollary 2.2.16. *If A is the direct limit of rings, i.e. $A \cong \lim_{\to i \in I} A_i$ then $K_0(A) \cong \lim_{\to i \in I} K_0(A_i)$.*

The below result is a generalization of Proposition 2.2.4 (since every division ring is a simple ring)

Lemma 2.2.17. *Let A be a simple ring then $K_0(A) \cong \mathbb{Z}$.*

Proof. By Morita invariance 2.2.14 we know that $K_0(A) \cong K_0(M_n(A)) \cong K_0(\mathrm{End}(A)) \cong K_0(D)$ for some division ring D. The last isomorphism is due to Schur's lemma 2.2.10. Now applying Proposition 2.2.4 we are done. $\square$

Theorem 2.2.18. *If A is a semisimple ring then $K_0(A) \cong \mathbb{Z}^r$.*

Proof. Due to Wedderburn-Artin 2.2.12, we know $A \cong \prod_{i=1}^{r} M_{n_i}(D_i)$ now applying Morita invariance 2.2.14, Corollary 2.2.15 (the result for n direct sums is obtained via induction).

$$K_0(A) \cong K_0\left(\prod_{i=1}^{r} M_{n_i} D_i\right) \cong \prod_{i=1}^{r} K_0\left(M_{n_i} D_i\right) \cong \prod_{i=1}^{r} K_0(D_i) \cong \mathbb{Z}^r.$$

□

2.3 Fundamental theorems for G_0, K_0

We state a few important results here without proof their detailed proofs can be seen in [**?**]. These will be covered in the next project. As they lend themselves to quick generalizations and motivate the introduction of higher K groups.

Theorem 2.3.1 (Fundamental theorem for G_0 for noetherian rings A)**.** $G_0[A] \cong G_0(A[t]) \cong G_0(A[t, t^{-1}])$.

Definition 2.3.2 (Regular ring)**.** *A ring is called regular if every finitely generated ideal has finite projective dimension (minimal length of resolution by projective modules).*

Example 2.3.3. *Any Dedekind domain is a regular ring in particular a principal ideal domain is a regular ring.*

Theorem 2.3.4 (Fundamental theorem for K_0 of regular rings)**.** *For a regular ring A, $K_0(A) \cong G_0(A)$ and by Theorem 2.3.1 we have,*

$$K_0(A) \cong K_0(A[t]) \cong K_0(A[t, t^{-1}]).$$

Chapter 3

Quillen-Suslin Theorem

We will now move towards a detailed proof of Horrock's theorem which will give us a concise proof of the famous Quillen-Suslin theorem which states that projective modules over polynomial rings over principal ideal domains are free.

We follow Lang's book for the first few results which recounts Vaserstein's proof of Quillen-Suslin [**?**].

3.1 Hilbert-Serre and stable freeness

Recall the definitions of stably free modules 1.2.11 and resolutions of chain complexes 1.3.1. We begin with a theorem due to Serre.

Theorem 3.1.1 (Hilbert-Serre). *Finitely generated module over $k[x_1, \dots x_n]$ are stably free where k is a principal ideal domain.*

Proof. Applying Theorem2.3.4 and then Theorem2.2.4 gives us a quick proof of this result since $k[x_1, \dots, x_n]$ is regular.

□

3.2 Unimodular rows

We now introduce an important concept of a unimodular row. This perspective helps greatly simplify the proof of Quillen-Suslin.

Definition 3.2.1 (Unimodular row)**.** *For a ring A, an element of A^n is said to be a unimodular row if its components generate A. We denote the set of all unimodular rows of length n in A as $\mathrm{Um}_n(A)$.*

In particular $v = (v_1, \cdots, v_n) \in \mathrm{Um}_n(A)$ if there exists $a = (a_1, \cdots a_n) \in A^n$ such that $v \cdot a = v^t a = \sum_{i=1}^n v_i a_i = 1$.

Definition 3.2.2 (Unimodular matrix)**.** *In general we say an arbitrary matrix over A not necessarily square is unimodular if it is right invertible (i.e. a surjective map).*

Alternatively it can be useful to view a unimodular row as as element of $M_{1\times n}(A)$ as such it represents a surjective linear map $A^n \to A$, or even an element in $M_{n\times 1}$ in which case it represents a injection from $A \to A^n$.

Recall the definition of a stably free projective module (Definition 1.2.11). Based on these definitions we can see that the kernel of the surjective $1 \times n$ matrix $A^n \to A$ (i.e. of a unimodular row) is precisely a stably free projective of the form $\underbrace{P}_{\ker v} \times A \cong A^n$.

Definition 3.2.3 (Equivalence of unimodular rows)**.** *For unimodular rows $v, w \in A^n$ we say $v \sim w$ if there exists $\alpha \in GL_n(A)$ such that $v\alpha = w$.*

Definition 3.2.4 (Unimodular completion property)**.** *Given a unimodular row $v = (v_1, \dots v_n) \in A^n$ if we can construct an invertible $n \times n$ matrix with v in the first column we say v has the unimodular completion property.*

Lemma 3.2.5. *A unimodular row $v \in A^n$ has the unimodular completion property iff $v \sim (1, 0, \dots, 0)$.*

Proof. If v can be extended to an invertible matrix $\alpha \in GL_n(A)$ then

$$v\alpha^{-1} = (1, 0, \dots, 0).$$

Conversely if $\alpha' \in GL_n(A)$ s.t. $v\alpha' = (1, 0, \dots, 0)$ then α'^{-1} has v in the first column. □

Corollary 3.2.6. *Based on the above lemma we can see that naturally any row of an invertible matrix (and column realized as a row of its transpose) is a unimodular row.*

Corollary 3.2.7. *A projective module P is free iff the unimodular row $v : A^n \to A$ such that $P = \ker v$ is completable to an invertible matrix (since we can adjoin the basis of P).*

Example 3.2.8 (Stably free projective module which is not free)**.** *Consider the ring R of polynomial functions on the sphere S^2, $R = \mathbb{R}[x, y, z]/\langle x^2 + y^2 + z^2 = 1\rangle$ the ring of real valued polynomials on S^2. Consider the unimodular row $v = (x, y, z)$. The associated projective module is $P = \ker v = \ker\{(p, q, r) \mapsto xp + yq + zr\}$. By definition $P \oplus R \cong R^3$.*

Every element (f, g, h) of R^3 yields a vector field in $\mathbb{R}^3$.

The unimodular row v is the vector field extending outward normal to the sphere. Therefore an element in P yields a vector field in tangent to the 2-sphere S^2.

*If P were free, i.e. $P \cong R^2$ a basis of P would yield two tangent vector fields on S^2 which are linearly independent at every point of S^2. This would mean we could construct a nowhere vanishing vector field on S^2 as a linear combination of these basis vector fields which is linearly independent at each point of S^2. This leads to a contradiction. The 'Hairy ball theorem' states that [**?**] any continuous vector field on S^2 must have at least one zero.*

Proposition 3.2.9. *Over a principal ideal domain A any two unimodular rows in A^n are equivalent.*

Proof. Let v be a unimodular row. So that we get a split sequence $0 \to A \xrightarrow{v} A^n \to P \to 0$ for some stably free P. We have that coker$v = A^n/\mathrm{Im}\{v\}$ is free as submodules of free finitely generated modules over a principal ideal domain are free (Proposition 1.2.8). So there exists a basis for A^n containing v, i.e. $v \sim (1, 0, \cdots, 0)$

$\square$

Using Theorem 1.2.6 which says that that projective finitely generated modules over local rings are free we obtain.

Proposition 3.2.10. *Over a local ring A any two unimodular rows are equivalent.*

3.3 Proof of Quillen-Suslin theorem

We begin with a useful theorem due to Horrocks.

Theorem 3.3.1 (Horrocks' theorem)**.** *If $(A, \mathfrak{m})$ is a local ring then for any arbitrary unimodular row $v(x)$ in $A[x]^n$ such that one of its component elements has leading coefficient one implies that v has the unimodular completion property. Furthermore, any such v is equivalent to $v(0)$.*

Proof. Recall that for a local ring $x \notin \mathfrak{m}$ iff x is a unit.

When $n = 1$ there is nothing to prove. If $n = 2$ by unimodularity of $v(x)$ we have $v_1(x)w_1(x) + v_2(x)w_2(x) = 1$ simply consider the matrix

$$\begin{bmatrix} v_1(x) & -w_2(x) \\ v_2(x) & w_1(x) \end{bmatrix}.$$

We proceed with $n \geq 3$. Without loss of generality, we take $v_1(x)$ with degree d among components with leading coefficient 1 and $\deg v_i < d$, for $i \neq 1$ by repeated elementary row operations to move the components around. We proceed by inducting on d.

By unimodularity we know there exists $w(x) \in A[x]^n$ such that,

$$\sum_{i=1}^{n} w_i v_i = 1$$

Now we can say that not all of the coefficients of $v_2, \ldots v_n$ lie in $\mathfrak{m}$. For if it were the case, then reducing the above expression mod $\mathfrak{m}$ we arrive at a contradiction. Since after reducing mod $\mathfrak{m}$ all v_i for $i \geq 2$ go to 0. Note that we assumed v_1 has leading coefficient 1 which means that $w_1 v_1$ wouldn't have a constant residue but then since the rest of the $v_i \in \mathfrak{m}$ they are non units and cannot account for the right hand side of the expression either.

Therefore at least one of the other v_i contains a unit in its coefficients say this is $v_2(x)$ and and as such one of its coefficients is a unit. In particular

$$\begin{aligned} v_1(x) &= x^d + a_{d-1}x^{d-1} + \cdots + a_0 \\ v_2(x) &= b_s x^s + \cdots + b_0, \end{aligned}$$

with some b_j a unit.

Now consider the ideal I generated by the leading coefficients of polynomials of the form $z_1 v_1 + z_2 v_2$ with degree $< d$. Our claim is that I contains all of the coefficients of v_2.

This can be seen inductively. The trivial case is when we pick $z_1 = 0, z_2 = 1$ this gives us the coefficient of the x^s term, i.e. b_s. Since $0v_1 + 1v_2 = v_2$ and its leading coefficient is b_s.

For b_{s-1} consider $z_1 = -b_s$ and $z_2 = x^{d-s}$, then $z_1 v1 + z_2 v_2$ has leading coefficient b_{s-1} as we can see below.

$$\begin{aligned}
& -b_s v_1(x) + x^{d-s} v_2(x) \\
& = (b_s x^d + (-b_s a_{d-1} x^{d-1}) + \cdots + (-b_s a_0)) - (b_s x^d + b_{s-1} x^{d-1} \cdots + x^{d-s} b_0) \\
& = (-b_s a_{d-1} - b_{s-1}) x^{d-1} + \cdots
\end{aligned}$$

Note $b_s \in I$, so $-b_s a_{d-1} \in I$ and so we have $-b_{s-1} \in I$ too.

Continuing this process we find that all coefficients of v_2 are in I, a fortiori the unit coefficient is in I. Meaning I is a unit ideal, and so with a choice of z_1, z_2 we can construct any polynomial we require.

Consequently this means there exists some choice of polynomials $y_1 v_1 + y_2 v_2$ of degree $< d$ with leading coefficient 1, increasing exponentials in y_i appropriately we can adjust this to be of degree $d - 1$.

Now consider v_3 by our construction we know it has degree $< d$ if its leading coefficient is a unit then multiply by the inverse and get a component with leading coefficient one of smaller degree than v_1 and repeat the process. Else if the leading coefficient is not a unit and $c \in \mathfrak{m}$, adding the above choice of $y_1 v_1 + y_2 v_2$ to v_3 gives us a degree $d - 1$ polynomial with a unital leading term since $1 + c$ is a unit if $c \in \mathfrak{m}$ due to locality.

We keep repeating this process of reducing d until $d = 0$ leaving us with a unit component allowing us to cancel out the other components and be left with $v \sim (1, 0, \ldots, 0)$ as expected. □

We now extend the idea of Horrock's theorem.

Lemma 3.3.2. *For an integral domain A and a multiplicative subset S if $v(x) \sim v(0)$ unimodular over $A_S[x]^n$ then there exists $b \in S$ such that $v(x + by) \sim v(x)$ over $A[x, y]^n$.*

Proof. By the equivalence $v(x) \sim v(0)$ we know there exists a matrix $\alpha(x) \in GL_n(A_S[x])$ such that $\alpha(x) v(x) = v(0)$. Now consider

$$\beta(x, y) := \alpha(x)^{-1} \alpha(x + y)$$

Note that this gives us the relation,

$$\beta(x, y) v(x + y) = \alpha(x)^{-1} \alpha(x + y) v(x + y) = \alpha(x)^{-1} v(0) = v(x).$$

Under the mapping $y \mapsto by$ we have that $\beta(x, by) v(x + by) = v(x)$.

Now we have to show that indeed $\beta(x, by) \in A[x, y]$ for some choice of $b \in S$. Note this is true since $\beta(x, 0) = I_n$. This implies $\beta(x, y) = I + yP$ for some $P \in A_S[x, y]$, but this just means there is some appropriate choice of $b \in S$ that allow us to cancel out all the denominators in P so that $P[x, by] \in A[x, y]$. So with a choice of matrix $\beta(x, by) \in GL_A[x, y]$ we are done, as this forms an equivalence between $v(x + y)$ and $v(x)$. □

Lemma 3.3.3. *For an integral domain A and $v(x)$ unimodular row in $A[x]^n$ with at least one component having leading coefficient one implies $v(x) \sim v(0)$.*

Proof. Consider the set I containing all $b \in A$ such that $v(x + by) \sim v(x)$ as rows in $A[x, y]$. If the ideal contains 1, then sending $x \to 0$ would give us $v(y) \sim v(0)$ in $A[y]$. We proceed to show that the ideal I contains 1.

We can achieve this by first showing I is an ideal and then showing that its not contained in any maximal ideal. To do this last step we will localize at the maximals and use the previous result.

First prove that I is an ideal.

1. $I \neq \emptyset$ as $0 \in I$
2. If $b, c \in I$ then $b - c \in I$ as $v(x + (b - c)y) = v(x + by - cy) \sim v(x + by) \sim v(x)$ by a substitution $x \mapsto x + by$
3. For $a \in A, b \in I$ then simply $v(x + bay) \sim v(x)$ by the $y \mapsto ay$

Now to show I is not contained in any maximal ideal. Pick a maximal ideal $\mathfrak{m}$ and localize at it first due to Horrocks we know $v(x) \sim v(0)$ in $A_{\mathfrak{m}}[x]$ and then due to the previous Lemma 3.3.2 we find some $b \in A \setminus \mathfrak{m}$ such that $v(x + by) \sim v(x) \sim v(0)$. Note this just means that $b \in I$ and so $I \not\subset \mathfrak{m}$ this applies to any maximal and so we are done. □

Theorem 3.3.4. *For $A = k[x_1, \ldots, x_n]$ where k is a principal ideal domain, then $v \sim (1, 0, \ldots, 0)$ for any unimodular row $v \in A^n$.*

Proof. Proceed with induction on n. We proved $n = 0$ above Proposition 3.2.9.

Assume the result holds for $m - 1$ greater than 0.

Then $v \in k[x_1, \ldots, x_m] \cong k[x_1, \ldots, x_{m-1}][x_m]$ can be realized as $v(x_m)$ with coefficients in $k[x_1, \ldots, x_{m-1}]$. If $v(x_m)$ has some component with leading coefficient 1 then by Lemma 3.3.3 we now $v(x_m) \sim v(0) \in k[x_1, \ldots, x_{m-1}]$ and we can reduce by induction.

So if not by some appropriate change of variables as amongst $x_1, \dots, x_{m-1}$ in the form of $x_i \mapsto x_i - x_m^{p_i}$ for very large p_i's this allows us obtain the leading coefficient in terms of x_m to be 1 as needed. $\square$

Theorem 3.3.5 (Quillen-Suslin). *Finitely generated projective modules over $A = k[x_1, \dots, x_n]$ where k is a principal ideal domain are free.*

Proof. We know such finitely generated projective modules are stably free, and from above we know any unimodular row in A is equivalent to $(1, 0, \dots, 0)$.

That is to say given a finitely generated projective module P which is stably free, i.e. $P \oplus R^{m_1} \cong R^{m_2}$ then P is free.

When $m_1 = 1$ this is the split exact sequence (since P is projective see 1.2.3),

$$0 \to A \to A^{m_2} \to P \to 0$$

The injection $A \to A^{m_2}$ is precisely a unimodular row by definition which we know must correspond to the canonical embedding of $1 \mapsto (1, 0, \cdots, 0)$. So,

$$P = \operatorname{im}(A^{m_2} \to P) \cong A^{m_2} / \ker(A^{m_2} \to P) \cong A^{m_2} / \operatorname{im}(A \to A^{m_2}).$$

Note $A^{m_2}/\operatorname{im}(A \to A^{m_2})$ is free since $\operatorname{im}(A \to A^{m_2})$ is naturally free due to the embedding.

When $m_1 \neq 1$ just take $(P \oplus A^{m_1-1}) \oplus A$. $\square$

Chapter 4

Whitehead group K_1

Definition 4.0.1 (Whitehead group for a ring)**.** *K_1 for a ring A is defined as the abelianization of its infinite general linear group.*

$$K_1 := \frac{GL(A)}{[GL(A) : GL(A)]},$$

Where $GL(A)$ the infinite general linear group is the colimit of $GL_n(A)$ with GL_n realized as a subgroup of GL_{n+1} by placing the matrix in the top left corner.

Note that $[GL(A) : GL(A)]$ denotes the derived/commutator subgroup of $GL(A)$, the subgroup generated by all commutators $[g : h] = g^{-1}h^{-1}gh$ for $g, h \in GL(A)$.

Definition 4.0.2 (Elementary matrices)**.** *We denote the $n \times n$ elementary matrices as $E_n(A)$ generated by standard elementary matrices of the form $e_{ij}(\lambda) := I_n + \lambda E_{ij}$ where E_{ij} is the matrix with 1 in the (i, j) entry and zero elsewhere.*

Lemma 4.0.3. *A nonsingular triangular matrix with 1's in the diagonal is a product of standard elementary matrices.*

Proof. Let $\alpha \in GL_n(A)$ then consider the following inductive procedure.

$$\alpha = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & & & \\ \vdots & & \alpha_{n-1} & \\ 0 & & & \end{bmatrix}$$

$$\alpha = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \alpha_{n-1} & \\ 0 & & & \end{bmatrix} e_{12}(a_{12})e_{13}(a_{13})\cdots e_{1n}(a_{1n})$$

Repeat the procedure for α_{n-1}, which is of the same form as α. We obtain

$$\alpha = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & \\ \vdots & 0 & & \alpha_{n-2} & \\ 0 & 0 & & & \end{bmatrix} \prod_{j=2}^{n} e_{2j}(a_{2j}) \prod_{i=1}^{n} e_{1i}(a_{1i}).$$

Continuing this process we obtain the required result. □

Proposition 4.0.4. *Let A be a ring and u be a unit in A, i.e. $u \in A^\times$. Then,*

$$\begin{bmatrix} u & 0 \\ 0 & u^{-1} \end{bmatrix} \equiv I_2 \mod E_2(A).$$

Proof. $\begin{bmatrix} u & 0 \\ 0 & u^{-1} \end{bmatrix} = e_{21}(u^{-1})e_{12}(1-u)e_{21}(-1)e_{12}(1-u^{-1}).$ □

Lemma 4.0.5 (Whitehead)**.** *For $\alpha, \beta \in GL_n(A)$,*

$$\begin{bmatrix} \alpha\beta & 0 \\ 0 & I_n \end{bmatrix} \equiv \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} \equiv \begin{bmatrix} \beta\alpha & 0 \\ 0 & I_n \end{bmatrix} \mod E_{2n}(A).$$

Proof. Let $A = M_n(A)$ and note $E_2(M_n(A)) \subset E_{2n}(A)$ in Proposition 4.0.4. □

Proposition 4.0.6.

$$[GL(A) : GL(A)] = E(A).$$

Proof. Using Lemma 4.0.5 we can see that

$$\begin{bmatrix} \alpha^{-1}\beta^{-1} & 0 \\ 0 & I_n \end{bmatrix} \equiv \begin{bmatrix} \beta^{-1}\alpha^{-1} & 0 \\ 0 & 1_n \end{bmatrix} \mod E_{2n}(A)$$

So the derived subgroup of $GL_n(A)$ is contained in $E_{2n}(A)$. Furthermore, every elementary matrix $e_{ij}(\lambda)$ is realized as a commutator since, $e_{ij}(\lambda) = [e_{ik}(1), e_{kj}(\lambda)]$. □

Lemma 4.0.7. *For a Euclidean domain A we have $SL_n(A) = EL_n(A)$ for all $n \in \mathbb{N}$.*

Proof. With elementary row and column operations arrange the matrix so that the element with the smallest norm is in the top right position. Using elementary row operations reduce it to a matrix with a unit in the top left and 0s in the rest of the first column and first row. Proceeding similarly for the remaining $(n-1) \times (n-1)$ matrix left we reduce it down to a matrix of the form.

$$\begin{bmatrix} u_1 & 0 & \dots & 0 \\ 0 & u_2 & \dots & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & 0 & \dots & u_n \end{bmatrix}$$

Now apply Whiteheads lemma □

Definition 4.0.8 (Relative K_1)**.** $SK_1(A) := \ker \det$,
where, $\det : K_1(A) \to A^\times$*. We have a split exact sequence*

$$0 \to SK_1(A) \to K_1(A) \to A^\times \to 0.$$

Chapter 5

Results on linear groups

5.1 Suslin's Normality theorem

We now consider a result due to Suslin about the normality of $E_n(A)$ in $GL_n(A)$. The following Lemma due to Vaserstein will be useful.

Lemma 5.1.1 (Vaserstein)**.** *Let $\alpha \in M_{m,n}(A)$ and $\beta \in M_{n,m}(A)$ then $I_m + \alpha\beta \in GL_m(A)$ implies that $I_n + \beta\alpha \in GL_n(A)$ and,*

$$\begin{bmatrix} I_m + \alpha\beta & 0 \\ 0 & (I_n + \beta\alpha)^{-1} \end{bmatrix} \in E_{m+n}(A).$$

Proof. Note that $(I_n + \beta\alpha)^{-1} = I_n - \beta(I_m + \alpha\beta)^{-1}\alpha$. Consider,

$$\begin{bmatrix} I_m + \alpha\beta & 0 \\ 0 & (I_n + \beta\alpha)^{-1} \end{bmatrix} =$$

$$\begin{bmatrix} I_m & 0 \\ (I_n + \beta\alpha)^{-1}\beta I_n & \end{bmatrix} \begin{bmatrix} I_m & -\alpha \\ 0 & I_n \end{bmatrix} \begin{bmatrix} I_m & 0 \\ -\beta & I_n \end{bmatrix} \begin{bmatrix} I_m & (I_n + \alpha\beta)^{-1}\alpha \\ 0 & I_n \end{bmatrix} \in E_{m+n}(A).$$

By Proposition 4.0.3, the triangular matrices here are indeed elementary. $\square$

Corollary 5.1.2. *Let $v = (v_1, \ldots, v_n)^t$ and $w = (w_1, \ldots, w_n)^t$ be column vectors in R^n such that $w^t v = 0$, and suppose $w_i = 0$ for some $i \leq n$. Then $I_n + vw^t \in E_n(R)$.*

Proof. When $w_i = 0$ for $i \neq n$ we have $\alpha(I_n + vw^t)\alpha^{-1} = I_n + (\alpha v)(w^t\alpha^{-1})$for $\alpha = e_{in}(-1)e_{ni}(1)e_{in}(-1)$, which acts as a permutation matrix making the nth term i.e. $(w^t\alpha^{-1})^t_n = 0$.

Therefore, without loss of generality we may assume that $w_n = 0$. Now define $w' = (w_1, \cdots, w_{n-1})^t, v' = (v_1, \cdots, v_{n-1}) \in R^{n-1}$. Since $w_n = 0$ and $w^t v = 0$ implies that $w'^t v' = 0$ also.

Proceeding inductively on n. We can say that $I_{n-1} + v'w'^t \in E_{n-1}(R)$. Note that the base case $n = 1$ is given by Lemma 5.1.1.

Therefore we have

$$I_n + vw^t = \left[\begin{array}{c|c} \multirow{3}{*}{$I_{n-1} + v'w'^t$} & 0 \\ & 0 \\ & \vdots \\ \hline * & 1 \end{array}\right],$$

We can make the last row zero using appropriate column transformations using the last column (which are all elementary matrices). Therefore, $I_n + vw^t \in E_n(R)$. □

Lemma 5.1.3. *For v unimodular row in R^n, and $f : R^n \to R$ a $R-$ linear map determined by $e_i \mapsto v_i$, where e_i is the standard basis element of R^n. We have,*

$$\ker(f) = \left\{ w = (w_1, \cdots w_n)^t \mid \sum_i^n w_i v_i = 0 \right\}$$

and it is generated by elements of the form $\{v_j e_i - v_i e_j\}$ for positive $1 \leq i < j \leq n$.

Proof. We wish to show that $\ker(f)$ is generated by the elements

$$\{v_j e_i - v_i e_j \mid 1 \leq i < j \leq n\}.$$

By definition of unimodularity of v, there exist elements $r_1, \ldots, r_n \in R$ such that $\sum_{i=1}^n r_i v_i = 1$. Consider the R-module homomorphism $g : R \to R^n$ given by $g(1) = (r_1, \ldots, r_n)^t$. This provides a splitting on the right of the exact sequence

$$0 \to \ker(f) \to R^n \xrightarrow{f} R \to 0$$

since $f(g(1)) = \sum_i r_i v_i = 1$. So the sequence is split exact and $R^n \cong \ker(f) \oplus R$.

Now, consider a map $h : R^n \to \ker f$ defined as $h(x) = x - g(f(x))$. This creates a splitting on the left side of the exact sequence, since $h|_{\ker(f)} = 1_{\ker(f)}$. Since h is surjective, the elements $h(e_i)$ generate $\ker(f)$.

$$\begin{aligned} h(e_i) = e_i - g(f(e_i)) &= e_i - g(v_i) = e_i - v_i g(1) \\ &= e_i - (v_i r_1, v_i r_2, \ldots, v_i r_n) = e_i - v_i \sum_j r_j e_j \\ &= (\sum_j r_j v_j) e_i - \sum_j r_j v_i e_j = \sum_j r_j (v_j e_i - v_i e_j) \end{aligned}$$

This shows that $\ker(f)$ is indeed generated by the claimed elements. □

We finally generalize Corollary 5.1.2 to the following lemma which will be used in the proof of the normality theorem.

Proposition 5.1.4. *Let $n \geq 3$. If $v \in R^n$ is unimodular, and $w \in R^n$ such that $w^t v = 0$, then $I_n + vw^t \in E_n(R)$ and this is also true if w is unimodular and v is arbitrary by transposition.*

Proof. Consider the R-linear map $f : R^n \to R$ defined as $e_i \mapsto v_i$. The condition $w^t v = 0$ implies $w^t \in Ker(f)$. By Lemma 5.1.3, there exists $r_{ij} \in R$ such that we can decompose w^t as such

$$w^t = \sum_{i<j} r_{ij}(v_i e_j - v_j e_i).$$

Label $w_{ij}^t = v_i e_j - v_j e_i$ and decompose $I_n + vw^t$

$$I_n + vw^t = I_n + v \sum_{i<j} w_{ij}^t = \prod_{i<j} (I_n + vw_{ij}^t).$$

We have $w_{ij} v = 0$ and since $n \geq 3$, there exists a zero component and so we have from Corollary 5.1.2 that $I_n + vw_{ij}^t \in E_n(R)$ for all $i < j$. This completes the proof. □

Theorem 5.1.5 (Suslin's Normality theorem)**.** *For A, a commutative ring with unity, $E_n(A)$ normal in $GL_n(A)$ for $n \geq 3$.*

Proof. Since $E_n(R)$ is generated by $e_{ij}(\lambda)$ it suffices to check that $\alpha e_{ij}(\lambda)\alpha^{-1} \in E_n(R)$ for $\alpha \in GL_n(A)$.

Recall from 3.2.6 that the columns of α and the rows of α^{-1} are unimodular.

$$\alpha e_{ij}(\lambda)\alpha^{-1} = \alpha(I_n + \lambda E_{ij})\alpha^{-1} = I_n + \lambda c_i r_j$$

Where c_i is the i^{th} column of α and r_j is the j^{th} row of α^{-1}.

Furthermore since $\alpha^{-1}\alpha = I_n$ implies $r_j c_i = \delta_{ij}$ implies using Proposition 5.1.4 that $\alpha e_{ij}(\lambda)\alpha^{-1} = I_n + \lambda c_i r_j \in E_n(A)$. $\square$

5.2 Local-global principle for unimodular vectors

In this section, we establish an important result that plays a crucial role in proving Suslin's factorial theorem. Specifically, we prove a useful 'Local-global principle' for unimodular polynomial vectors.

Lemma 5.2.1. *Let S be a multiplicative set in A. For $f(x) \in GL_n(A_S[x])$ such that $f(0) = I_n$, there exists $\hat{f}(x) \in GL_n A[x])$ such that $\hat{f}(x)$ under the localization map maps to $f(sx)$ (for some $s \in S$), and $\hat{t}(0) = I_n$.*

Proof. Since $f(x) \in GL_n(A_S[x])$, there exists $g(x) \in GL_n(A_S[x])$ such that $f(x)g(x) = I_n$. The condition $f(0) = I_n$ implies $g(0) = I_n$.

In particular this means that the diagonal entries belong to $1 + xA_S[x]$ and off diagonal entries are of the form $xA_S[x]$.

Since only finitely many denominators appear in the entries of $f(x)$ and $g(x)$, there exists $s_1 \in S$ which is a common denominator. This allows us 'cancel' the denominators and to define matrices $f(s_1x)$ and $g(s_1x)$ with coefficients in A.

This means there exist $f_1(x)$ and $g_1(x)$ with polynomial entries in $A[x]$ with $f_1(0) = g_1(0) = I_n$ which map to $f(s_1x), g(s_1x)$ under the localization map.

Let $h(x) = f_1(x)g_1(x)$. Then $h(x)$ maps to $f(s_1x)g(s_1x) = I_n$ under the localization map. Since $h(0) = I_n$, there exists $s_2 \in S$ such that $h(s_2x) = I_n$. This implies that $f_1(s_2x)$ is invertible over $A[x]$ with inverse $g_1(s_2x)$.

Therefore, we define $\hat{f}(x) = f_1(s_2x)$. Then $\hat{f}(x) \in GL_n(A[x])$, $\hat{f}(0) = I_n$, and the image of $\hat{f}(x)$ under the localization map is $f(s_1s_2x)$. Thus, setting $s = s_1s_2$, the lemma is proved. $\square$

The below result is a generalization of Lemma 3.3.2.

Proposition 5.2.2. *Let A be a commutative ring and S a multiplicative subset of A. For $v = (v_1, \ldots, v_n) \in \mathrm{Um}_n(A[x])$, the following statements are equivalent:*

1. $v(x) \sim v(0)$ *over* $A_S[x]$.

2. *There exists* $b \in S$ *such that* $v(x + by) \sim v(x)$ *over* $A[x, y]$.

Proof. We first prove 2 implies 1. Consider a change of variable in $A_S[x, y]$ given by $x = 0, y = b^{-1}x$ so we have that under the localization map $v(0 + bb^{-1}x) = v(x) \sim v(0)$ over $A_S[x]$ as required.

For the other direction. There exists $\alpha(x) \in GL_n(A_S[x])$ such that $v(x) \cdot \alpha(x) = v(0)$. Define β as such $\beta(x, y) = \alpha(x + y)\alpha(x)^{-1} \in GL_n(A_S[x, y])$.

$$\begin{aligned} v(x + y)\beta(x, y) &= v(x + y)\alpha(x + y)\alpha(x)^{-1} \\ &= v(0)\alpha(x)^{-1} = v(x) \in A_S[x, y]. \end{aligned}$$

This shows $v(x + y) \sim v(x)$ over $A_s[x, y]$ now we lift it to $A[x, y]$.

Since $\beta(x, 0) = \alpha(x) \cdot \alpha(x)^{-1} = I_n$, we can apply Lemma 5.2.1 over $A[x]$ to obtain $\hat{\beta}(x, y) \in GL_n(A[x, y])$ such that under the localization map it goes to $\beta(x, sy) \in GL_n(A_S[x, y])$ for some $s \in S$, and $\hat{\beta}(x, 0) = I_n$.

With $y \mapsto sy$ in the above relation lifted to $A[x, y]^n$, we have

$$v(x + sy)\hat{\beta}(x, y) - v(x) = yg(x, y)$$

for some $g(x, y)$ that localizes to 0, so there exists $s' \in S$ such that

$$v(x + ss'y)\hat{\beta}(x, s'y) - v(x) = ys'g(x, s'y) = 0.$$

Choose $n = ss'$ and we are done. $\square$

Proposition 5.2.3. *Let $v(x) = (v_1(x), \ldots, v_n(x)) \in \mathrm{Um}_n(A[x])$. Define the ideals $\mathfrak{a}$ and $\mathfrak{b}$ as follows:*

$$\begin{aligned} \mathfrak{a} &= \{a \in A \mid v(x) \sim v(0) \text{ over } A_a[x]\} \\ \mathfrak{b} &= \{b \in A \mid v(x + by) \sim v(x) \text{ over } A[x, y]\} \end{aligned}$$

Then $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in A, with $\mathfrak{a} = rad(\mathfrak{b})$.

Proof. If $b \in \mathfrak{b}$, then $v(x+by) \sim v(x)$. With a substitution of variables for any $r \in A$, we have $v(x + bry) \sim v(x)$, so $br \in \mathfrak{b}$. If $b, b' \in \mathfrak{b}$, then the substitution $x \mapsto x+b'y$ shows that $\mathfrak{b}$ is an ideal. Since, $v(x+(b'+b)y) \sim v(x+b'y) \sim v(x)$.

The equality $\mathfrak{a} = \mathrm{rad}(\mathfrak{b})$ follows from the above proposition. $\square$

Theorem 5.2.4 (Local-global principle)**.** *Let $v = (v_1, \dots, v_n) \in \mathrm{Um}_n(A[x])$. If $v(x) \sim v(0)$ over $A_{\mathfrak{m}}[x]$ for all maximal $\mathfrak{m} \in A$, then $v(x) \sim v(0)$ over $A[x]$.*

Proof. Define $\mathfrak{a}$ and $\mathfrak{b}$ as above. Suppose $v(x) \sim v(0)$ over $A_{\mathfrak{m}}[x]$ Proposition 5.2.2 implies that there exist $b \in A \setminus \mathfrak{m}$ such that $v(x+by) \sim v(x)$ over $A[x,y]$.

i.e $A \setminus \mathfrak{m}$ contains an element of $\mathfrak{b}$ this implies $\mathfrak{b} = A$. Since $\mathrm{rad}(\mathfrak{b}) = \mathrm{rad}(A) = A$, we have $\mathfrak{a} = A$, which implies $v(x) \sim v(0)$ over $A[x]$. □

5.3 Suslin's factorial theorem

In this section we will prove a celebrated theorem due to Suslin.

Theorem 5.3.1 (Suslin's factorial theorem)**.** *Given $(v_0, \dots, v_n) \in \mathrm{Um}_{n+1}(A)$ then $n! | \prod_{i=0}^{n} m_i$, then $(v_0^{m_1}, \dots, v_n^{m_n}) \in \mathrm{Um}_{n+1}(A)$.*

The proof of the theorem in this section can be seen in detail in the papers by Suslin [?] and the expository book by Lam [?].

The converse of this result is also true as proved by Suslin in [?].

Proposition 5.3.2. *If there exists $v = (v_0, v_1, \cdots v_n) \in \mathrm{Um}_{n+1}(A)$ such that $\bar{v} = (\bar{v}_0, \cdots, \bar{v}_{n-1})$ is completable over the ring $\bar{A} = A/Av_n$ then,*

$$(v_0, \cdots, v_{n-1}, v_n^n) \in \mathrm{Um}_{n+1}(A)$$

and it is completable in A.

Proof. Let $\alpha \in M_n(A)$ be some matrix with first row $(v_0 \cdots, v_{n-1})$ such that $\bar{\alpha} \in GL_n(\bar{A})$ (which we know exists due to v being completable) let $\beta \in M_n(A)$ be the lift of $\bar{\alpha}^{-1}$, i.e., $\bar{\alpha}\bar{\beta} = I_n$. Then

$$\alpha\beta = I_n + v_n\gamma, \quad \beta\alpha = I_n + v_n\delta$$

for some $\gamma, \delta \in M_n(A)$.

The matrix $\begin{bmatrix} \alpha & v_n I_n \\ \delta & \beta \end{bmatrix} \in GL_{2n}(A)$ since

$$\begin{bmatrix} \alpha & v_n I_n \\ \delta & \beta \end{bmatrix} \cdot \begin{bmatrix} \beta & -v_n I_n \\ -\gamma & \alpha \end{bmatrix} = \begin{bmatrix} I_n & 0 \\ * & I_n \end{bmatrix} \in GL_{2n}(A).$$

Note that $\det(\alpha)$ is a unit in $\bar{A}$ using Lemma 4.0.5 on $\bar{A}$ and pulling back through the surjection $E_n(A) \to E_n(\bar{A})$ we have

$$\begin{bmatrix} v_n^n & 0 \\ 0 & I_{n-1} \end{bmatrix} = (v_n I_n)\epsilon + \det(a)\zeta$$

for some $\epsilon \in E_n(A)$ and $\zeta \in M_n(A)$.

Let $\alpha' = \mathrm{adj}(\alpha)$ be the adjoint of α. Recall that $\alpha \cdot \mathrm{adj}(\alpha) = \det(\alpha) I_n$, define a matrix φ as such

$$\begin{aligned} \varphi = \begin{bmatrix} \alpha & v_n I_n \\ \delta & \beta \end{bmatrix} \begin{bmatrix} I_n & \alpha' t \\ 0 & \epsilon \end{bmatrix} &= \begin{bmatrix} \alpha & \alpha\alpha'\zeta + v_n\epsilon \\ \delta & * \end{bmatrix} \\ &= \begin{bmatrix} \alpha & \det(\alpha)\zeta + v_n\epsilon \\ \delta & * \end{bmatrix} \\ &= \left[\begin{array}{c|cc} \alpha & \begin{matrix} v_n^n & 0 \\ 0 & I_{n-1} \end{matrix} \\ \hline \delta & * \end{array}\right] \in GL_{2n}(R) \end{aligned}$$

We now rewrite φ in the following adjusted block form

$$\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix},$$

where a_1 is $n \times (n+1)$ comprising of a along with the column $(v_n^n, 0, \ldots, 0)^t)$ adjoined at the right, $a_2 = \begin{bmatrix} 0 \\ I_{n-1} \end{bmatrix}$.

With appropriate elementary transformations on the last n rows of φ, we obtain a matrix of the form

$$\varphi' = \begin{bmatrix} a_1 & a_2 \\ a_3' & 0 \end{bmatrix}$$

Now consider the submatrix of φ' formally complementary to I_{n-1} which we obtain by deleting the 2nd up to the nth rows and the last $n-1$ columns. This is the required invertible $(n+1)\times(n+1)$ matrix with top row $(v_0, \ldots, v_{n-1}, v_n^n)$. $\square$

By induction on n, we obtain the following corollary.

Corollary 5.3.3. *For $(v_0, \cdots, v_n) \in \mathrm{Um}_{n+1}(A)$ the row $(v_0, v_1, v_2^2, \cdots, v_n^n)$ is completable.*

We now prove a result involving moving powers of coefficients in a unimodular row. Which in conjunction with the above corollary will prove the forward direction of Theorem 5.3.1.

Proposition 5.3.4. *For* $(v_0, \cdots, v_n) \in \mathrm{Um}_{n+1}(A)$ *and any* $r \in \mathbb{N}, i \neq j$

$$(v_0, \cdots, v_i^r, \cdots, v_n) \sim (v_0, \cdots, v_j^r, \cdots, v_n).$$

Proof. Begin with the case of $i = 0, j = 1$. Define $f(t) = (v_0^r, v_1 + v_0 t, \cdots, v_n) \in \mathrm{Um}_{n+1}(A[t])$.

Claim that $f(t) \sim f(0)$ over $A[t]$. Using Theorem 5.2.4 local-global principle to check this equivalence in $A_{\mathfrak{m}}$ for some arbitrary $\mathfrak{m}$ maximal in A.

Assume that $v_0, v_2, \cdots, v_n \in \mathfrak{m}$ else the claim is naturally true as they will be invertible if not, so $v_1 \in A \setminus \mathfrak{m}$ is a unit.

Note that $(v_0^r, v_1 + v_0 t) \in \mathrm{Um}_2(A[t])$ since, which is naturally completable, unimodularity is due to the fact that not both v_0^r and $v_1 + v_0 t \in \mathfrak{m}$ for if that is the case then $v_0, v_1 \in \mathfrak{m}$ which is a contradiction. Since this is true for all $\mathfrak{m}$. We have by the local-global principle that $(v_0^r, v_1 + v_0 t) \in \mathrm{Um}_2(A[t])$ this is also completable as all length 2 unimodular rows are naturally completable. In particular if $v_0^r b_0 + (v_1 + v_0 t) b_1 = 1$ then consider the matrix $\alpha \in GL_2(A[t])$ defined as

$$\alpha = \begin{bmatrix} v_0^r & v_1 + v_0 t \\ -b_1 & b_0 \end{bmatrix}$$

Therefore over $A[t]$ we have $f(t)$ is also completable with the block matrix

$$\beta = \begin{bmatrix} \alpha & \beta \\ 0 & I_{n-2} \end{bmatrix} \in GL_n(A)$$

where the first row of β equals $(v_2, \cdots, v_n)$. Therefore we have

$$f(t) \sim (1, 0, \ldots, 0) \sim f(0)$$

as claimed.

Now note that $f(t) \sim f(0)$ over $A[t]$ implies that $f(-1) \sim f(0)$ over A

$$(v_0^r, v_1, v_2, \cdots, v_n) \sim (v_0^r, v_1 - v_0, v_2, \cdots, v_n).$$

With the substitution $v_0 \mapsto v_1$ and $v_1 \mapsto v_1 - v_0$

$$\begin{aligned} &\sim (v_1^r, -v_0, v_2, \ldots, v_n) \\ &\sim (v_0, v_1^r, v_2, \ldots, v_n). \end{aligned}$$

The last equivalence is true since the block matrix $\begin{bmatrix} -I & 0 \\ 0 & I \end{bmatrix}$ is elementary (with column transformations it is equivalent to the block matrix with I in both diagonal places).

Repeating this procedure for other $i \neq j$ completes the proof. $\square$

Combining Corollary 5.3.3 and Proposition 5.3.4 we obtain the proof of Theorem 5.3.1 as required.