R-equivalence and norm principles in algebraic groups

By

Nivedita Bhaskhar
Doctor of Philosophy

Mathematics

Raman Parimala
Advisor

Suresh Venapally
Committee Member

David Zureick-Brown
Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.
Dean of the James T. Laney School of Graduate Studies

Date

R-equivalence and norm principles in algebraic groups

By

Nivedita Bhaskhar
B.Sc., Chennai Mathematical Institute, 2009
M.Sc., Northeastern University, 2011

Advisor: Raman Parimala, Ph.D.

An abstract of
A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2016

Abstract

R-equivalence and norm principles in algebraic groups
By Nivedita Bhaskhar

We start by exploring the theme of R-equivalence in algebraic groups. First introduced by Manin to study cubic surfaces, this notion proves to be a fundamental tool in the study of rationality of algebraic group varieties. A k-variety is said to be rational if its function field is purely transcendental over k. We exploit Merkurjev's fundamental computations of the R-equivalence classes of adjoint classical groups and give a recursive construction to produce an infinite family of non-rational adjoint groups coming from quadratic forms living in various levels of the filtration of the Witt group. This extends the earlier results of Merkurjev and P. Gille where the forms considered live in the first and second level of the filtration.

In a different direction, we address Serre's injectivity question which asks whether a principal homogeneous space under a connected linear algebraic group admitting a zero cycle of degree one in fact has a rational point. We give a positive answer to this question for any smooth connected reductive k-group whose Dynkin diagram contains connected components only of type A_n, B_n or C_n. We also investigate Serre's question for reductive k-groups whose derived subgroups admit quasi-split simply connected covers. We do this by relating Serre's question to the norm principles previously proved by Barquero and Merkurjev.

The study of norm principles are interesting in their own right and we examine in detail the case of groups of the non-trialitarian D_n type and get a scalar obstruction defined up to spinor norms whose vanishing will imply the norm principle for these groups. This in turn will also yield a positive answer to Serre's question for all connected reductive k-groups of classical type.

R-equivalence and norm principles in algebraic groups

By

Nivedita Bhaskhar
B.Sc., Chennai Mathematical Institute, 2009
M.Sc., Northeastern University, 2011

Advisor: Raman Parimala, Ph.D.

A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Mathematics
2016

गुरोरधीतं गुरवे समर्पितम्

Acknowledgements

It is a truth universally acknowledged, that the most read section of a dissertation must be the one about acknowledgements. And it is with the greatest pleasure that I put pen to paper to try and thank the beautiful people who have made my journey thus far possible.

To Professor Parimala, I owe a debt of gratitude that can never be repayed. There are few other people in this world apart from my parents under whom I have felt so protected and sheltered. I had never imagined the existence of such a joyous mathematical world before and it is entirely due to her, that I now belong to one such. To Professor Suresh, I am indebted no less. Apart from teaching me patiently and many times over(!), almost all of the mathematics that I now do, their extraordinary kindness, sheer generosity and warm camaraderie have made each day at work a delight. I have spent many an enjoyable hour in Parimala's office discussing mathematics with them and in wonder, watching them ruthlessly attack and untangle problems, mathematical or otherwise and weave them back into neat solutions. Their '*Let's fight it out*' optimism has been so cheerfully contagious that no difficulty cropping up has seemed unsurmountable. I can never thank them enough and also Ram and Sunitha for the many delicious dinners, conversation and companionship. For making an extremely homesick girl feel at home. For making my life as a graduate student so pleasant that graduating and moving out seems more bitter than sweet.

This thesis revolves around the theme of R-equivalence and norm principles and fundamentally depends on two papers of Professor Merkurjev on the same topic. I am extremely grateful to have had the opportunity to listen to his spectacular talks on Suslin's conjecture and would like to thank him for his generous and patient help and valuable discussions which helped crystallize my thoughts into concrete papers.

To Eva, I would like to extend my heartfelt thanks for her beautiful talks on Hasse principles, her magnanimous and ungrudging help with my research and kind words of encouragement which have helped me a great deal to overcome my diffidence in the academic world. I would also like to thank her and Monique for an enjoyable visit to EPFL, Lausanne in the Fall of 2014.

I would like to thank Fields Institute and the wonderful organizers and participants of the thematic program on torsors and cohomological invariants in Spring 2013. It served as the spring board for my dive into mathematical research, equipping me with so many of the right tools in so short a time. I would like to especially thank Professor Chernousov, Professor Karpenko and Professor P.Gille for their beautiful foundational courses on algebraic groups, quadratic forms and reductive group schemes. The seminar series on cohomological invariants with Professor Chernousov has also played a vital role in my research life and I would like to thank him for his generous help, time and patience! I would also like to thank Professor Gille for carefully explaining to me his paper on non-rational adjoint groups which played such an integral part in my work.

I have learnt and benefitted immensely from various workshops on patching from the team of Harbater-Hartmann-Krashen and would like to thank them for some beautiful and illuminating lectures on this topic. My gratitude to Giri Dada, Santhi Akka and Lalitha Maami for my home away from home in Toronto and my love to Pari for brightening my weekends by being the best baby cousin one could ever wish for.

I've had a wonderful time as a graduate student at Emory, attending well thought out and satisfying courses by the faculty in all areas, algebraic and otherwise. Grateful thanks to DZB for his courses on class field theory and stacks and to Professor Ken Ono for making me read Cassel's wonderful book '*Lectures on elliptic curves*'.

I thank Professor Colliot Thélène for his beautiful lectures on Brauer-Manin obstructions (among other things!) and patient help explaining several confusing aspects about algebraic groups to me during his occasional visits to Emory and Professor Saltman for his many exciting talks on division algebras and kind help with my research. A special thank you again to Danny for graciously including us Emory students in his fun courses on Stacks and Brauer groups which motivated us to continue the struggle to learn the stacky language.

My thanks to Professor Vicky for introducing me to the Math 115 team in my first ever semester and to Bree for lots of helpful advice. I am immensely grateful to Professor Dwight for putting up with me as a TA, for his thoughtful and valuable opinions about teaching, for his calm and unperturbed advice during my occasionally turbulent teaching days and for kindly laughing at my carefully inserted and mostly unnoticed puns in conversation and in my website. My grateful thanks to Terry for being an angel and answering and resolving my innumerable SOS calls about administrative affairs.

A big thank you to Asher for his generous help in explaining away some of the many mysteries of class field theory and for his many insightful lectures and talks on Brauer groups and Azumaya algebras. My thanks to Fred for teaching me all about Lie algebras, with pictures! And for the very many conversations about British movies, the weather, elementary number theory and the French language. Wu has been my mathematical comrade and co-student in arms and I would like to thank him for all the times we spent learning class field theory, patching and galois cohomology together. I would also like to thank him for timely reminders about the various deadlines which kept whooshing by, which I would have missed otherwise.

Thanks to Hernando for his valuable discussions about algebraic groups and invariants and for helping me understand what a half-spin group is. And to Ting-Yu for patiently answering my questions about R-equivalence and rationality and to her and Caroline for the fun times I've had with them in Toronto, Banff and other places.

A shout out to Mckenzie for putting up with me as an officemate, for her gorgeous cookies, for insights about the Brauer group and for answering all my queries about how to do this or that or that ; to Reed, for telling me interesting things about zero cycles, not necessarily of degree one ; to Jackson, for sharing his precise and beautifully TeXed notes with me, and to Bastian for his beautiful lectures on étale cohomology, for exciting discussions about what BG is exactly, for sharing the joys and sorrows about the wonderfully weird behaviour of division algebras in bad characteristic and for his cheerful help with proofreading my essays and papers and making encouraging comments on the margins while highlighting my errors. It has been wonderful discussing mathematics with you!

A special thanks to my tumblr friends, especially to halfwaythruthedark, florencecraye, weeguttersnipe, memories-of-indian-cinema, dweemeister and the south-indian squad for so many fulfulling exchanges about cinema and literature, which kept me afloat even when sometimes research rocked the boat a bit. A grateful thanks to the baristas of Starbucks at 1380 Oxford Road for their coffee and their friendly greetings which always made my days start well.

I would like to thank my teachers and friends at Northeastern University for a wonderful two years during my Masters program. Especially Professor Martsinkovsky from whom I learnt group cohomology, a tool which has become my bread and butter so as to speak, Professor Lakshmibai who taught me algebraic geometry and Professor Zelevinsky, who's no longer with us, for his wonderful courses in Algebraic combinatorics. And a special thank you to Undine for baking some amazing bread, for sharing the daily journeys on the Red line, insightful conversation and for some of the most beautiful times I had in Boston.

To CMI, where my mathematical journey began in earnest, I owe a great deal. My first taste of real mathematics could not have tasted sweeter from elsewhere. To each and every one of my teachers, the CMI staff and my fellow-collegemates, a grateful thanks for educating me (and not just in mathematics!) and for giving me an opportunity to take flight into the world of research.

I would also like to thank CMI and ENS and especially Professor Olivier Wittenberg for giving me an opportunity to spend three months in Paris learning about the Riemann Hypothesis for function fields. That period represents one of the best times I have had during my mathematical (and cultural!) education.

I remember with joy and gratitude my wonderful formative years at P.S. Senior Secondary School and thank all my teachers for their classroom lessons which taught me discipline, their multiudinous exams which took away the edge of fear while appearing for one and their kind words of encouragement which stay with me even today, especially Mrs Indrabai, my middle school math teacher.

My classmates, with whom I spent several wonderful years, I remember with thanks for their friendly cheer and support. To Manas, a thank you for many soulful conversations on what to do and how not to do it and to Gouthami, a salute for inspiring me by being so effortlessly jovial and passionate about academia and music.

To Madhu, a thank you for being there for me and a bigger thank you for being .. all that's awesome, you! From giggling about fictional heroes to worrying about being thirty soon, it's been a fun journey. And one, I couldn't have done without you.

To Nandita, who has succesfully managed the transformation from an adorably naive little sister who believed everything I said to an independent, succesful graduate student who now gives me self-help lessons, a thank you for being one of the few people who seem to know me effortlessly. And for inspiring me, though I do not often say it aloud, by pursuing academia and life with a vigour and energy that is admirable to say the least.

To Amma, a thank you for being my first mathematics teacher. To Bapa, a thank you for making me finish my thesis. To both of you, a thank you for making me, moulding me and then letting me be. For knowing when to say yes and when to say no. For worrying about what I have for dinner and for not worrying about my future prospects. For putting family above all else and staying together in the same boat, through both calm and storm.

And finally to Professor Sridharan who has steered me gently through the seas like the gentle wind guiding the sailboat. His influence, seemingly invisible and yet so powerful has navigated me around rocky corners, ruthless whirlpools and more importantly, kept me from stale stagnation. With him, I have learnt to admire beauty, be it in algebra or literature or in people. Without him, indeed, I would have quit the world of mathematics for ever and perhaps lost the link binding me to art and hence to beauty.

Contents

List of Figures

Chapter 1

An introduction

'But I will begin at the beginning,' said the Sage.
'I see that you are all impatient to hear the full details.'
- P. G. Wodehouse, The Long Hole

1.1 The story

This dissertation explores the closely connected themes of R-equivalence and norm principles of algebraic groups. The former is an equivalence relation on the L points of a k-variety X for any extension L/k and was first introduced by Manin in his study of cubic surfaces. The same notion carried over to the varieties underlying algebraic groups provides a key obstruction to the rationality of the same.

Recall that an irreducible k-variety is said to be k-rational if its function field is purely transcendental over k. Basic examples consist of affine and projective spaces. It is a theorem of Chevalley that in characteristic 0 every connected linear algebraic group is rational over the algebraic closure of its field of definition. However, rationality over the field of definition itself becomes infinitely more tricky and subtle to handle as the early examples of Chevalley and Serre of non-rational tori and semisimple neither simply connected nor adjoint groups indicate.

Platonov's famous example of non-rational groups of the form $\mathrm{SL}_1(D)$ settled negatively the long standing question of whether simply-connected almost simple k groups were necessarily rational over k. His example does indeed construct a group with non-trivial R-equivalence classes, the so-called $\mathrm{SK}_1(D)$ in this case!

The focus then shifted to adjoint groups, with Platonov himself conjecturing ([PLR], pg 426) that adjoint simple algebraic k-groups were rational over any infinite field. Some evidence of the veracity of this conjecture is found in ([Chernousov]) where it is established that $\mathrm{PSO}(q)$ is a stably rational k variety for the special quadratic form $q = \langle 1, 1, \ldots 1\rangle$ where k is any infinite field of characteristic not 2.

However Merkurjev in ([Me96]) constructed a quadratic form q/k of low even rank lying in the fundamental ideal $\mathrm{I}(k)$ such that the adjoint projective special orthogonal group, $\mathrm{PSO}(q)$, is not a k-rational variety. This example is obtained as a consequence of his computations of *R-equivalence classes* of adjoint classical groups which relates to rationality via the following elementary fact :

If X is a k-rational variety, then $X(K)/R$ is trivial for any extension K/k.

It is to be noted that in Merkurjev's example, q has non-trivial discriminant and therefore does not lie in $\mathrm{I}^2(k)$, the second term in the filtration of the Witt ring. The example uses the non-triviality of the signed discriminant of the quadratic form in a crucial way and indeed fails as such if the discriminant is trivial.

In the following year, P. Gille constructed a quadratic form q/k of even rank with trivial discriminant (hence lying in $\mathrm{I}^2(k)$) such that the corresponding adjoint group, $\mathrm{PSO}(q)$, is not a k-rational variety. It is to be noted that in

Gille's example, q has non-trivial Clifford invariant and therefore does not lie in $\mathrm{I}^3(k)$, the third term in the filtration of the Witt ring, which fact is again crucially exploited in his paper.

One can therefore pose the obvious natural question of whether there are examples of quadratic forms q_n defined over fields k_n satisfying the following two properties :

1. $q_n \in \mathrm{I}^n(k_n)$, the n-th power of the fundamental ideal.

2. $\mathrm{PSO}(q_n)$ is not k_n-stably rational.

The answer is yes and is one of the main results of this dissertation (Thm 7.9).

In a slightly different direction, we examine the closely related subject of norm principles for algebraic groups. Let G be a k-algebraic group, T, a commutative k-group and let $f\colon G \to T$ be an algebraic homomorphism defined over k.

$$\begin{array}{ccc} G(L) & \xrightarrow{f(L)} & T(L) \\ & & \big\downarrow {\scriptstyle \mathrm{N}_{L/k}} \\ G(k) & \xrightarrow{f(k)} & T(k) \end{array}$$

We say that the norm principle holds for $f\colon G \to T$ if for all separable field extensions L/k,

$$\mathrm{N}_{L/k}(\mathrm{Image}\, f(L)) \subseteq \mathrm{Image}\, f(k).$$

Norm principles form an interesting topic in their own right and have been widely studied ([Gille93], [Me95], [BM] et al). They also turn out to be an extremely pliant and pleasant tool to handle the following question of Serre (open in general) for many classical reductive groups.

Question 1.1 (Serre, [Serre95], Pg 233). Let G be any connected linear algebraic group over a field k. Let $L_1, L_2, \ldots, L_r$ be finite field extensions of k of degrees $d_1, d_2, \ldots, d_r$ respectively such that $\gcd_i(d_i) = 1$. Then is the following sequence exact?

$$1 \to \mathrm{H}^1(k, G) \to \prod_{i=1}^{r} \mathrm{H}^1(L_i, G).$$

The classical result that the index of a central simple algebra divides the degrees of its splitting fields answers Serre's question affirmatively for the group PGL_n. Springer's theorem for quadratic forms answers it affirmatively for the (albeit sometimes disconnected) group $\mathrm{O}(q)$ and Bayer-Lenstra's theorem ([BL]), for the groups of isometries of algebras with involutions. Jodi Black ([Black]) answers Serre's question positively for absolutely simple simply connected and adjoint k-groups of classical type.

In this dissertation, we are able to affirmatively answer Serre's question for classical reductive group of type A_n, B_n or C_n (Thm 9.8) and for quasi-split reductive groups without E_8 components (Thm 9.11) using Merkurjev and Barquero's norm principles ([BM]). We also study norm principles for groups of type D_n and construct an obstruction to the same (Thm 10.4).

1.2 The plan

This dissertation is shaped as follows :

In Chapter 2, we start by studying the Clifford algebras of quadratic forms and in more generality, of central simple algebras with orthogonal involutions.

Chapter 3 is a very quick walk through the classification of linear algebraic groups where we spend a little more time sniffing the flowers (i.e. understanding some rather nice groups) of type D_n. Chapter 4 is a crash course on group cohomology and Chapter 5 is naturally a glimpse of Galois cohomology.

Chapter 6 introduces the notion of rationality and R-equivalence and showcases examples of some of the well known non-rational groups present in literature. In Chapter 7, we produce quadratic forms q_n/k_n in a recursive fashion and use Merkurjev's powerful formulae about R-equivalence to provide an infinite family of examples of non-rational adjoint groups.

Chapter 8 is a quick introduction to the idea of norm principles. In Chapter 9, we use and extend Jodi Black's result on Serre's question to connected reductive k-groups whose Dynkin diagrams contain connected components only of type A_n, B_n or C_n and also explore the question for quasi-split reductive groups. We do this by relating Serre's question for G with the norm principles of other closely related groups following a series of reductions previously used by Barquero and Merkurjev.

In Chapter 10, the tantalizing missing ingredient, i.e. norm principles for groups of type (non-trialitarian) D_n, is studied and a scalar obstruction defined up to spinor norms is given whose vanishing will imply the norm principles and also yield a positive answer to Serre's question for all classical connected reductive k-groups. And finally, in Chapter 11, you can find a short summary of the main results of this thesis.

1.3 The prerequisites

'It is a subject on which authors frequently lie, claiming that whoever can count up to ten and recognize a few greek letters will immensely profit from the purchase of their books.'

- Inta Bertuccioni

This thesis is written in rather a leisurely style in the hope that it is an easy read for anyone possessing some knowledge of commutative and homological algebra, a smattering of algebraic geometry/algebraic groups jargon, some basic theorems about central simple algebras and the will to chase diagrams. We also give adequate references which we hope will fill in the missing details sought for by the avid reader.

We also assume *some familiarity* with quadratic forms and involutions, which is a topic which might or might not be covered in a first year graduate course. So here, we give a very very rough framework with which we hope the reader, if uninitiated, can still proceed on with the rest of this document and progress fruitfully.

1.3.1 Quadratic form theory

An excellent reference for a quick introduction to this subject would be the notes of ([Parimala09]). Let k be a field of characteristic not 2 and V/k, a finite dimensional vector space. We say $q\colon V \to k$ is a *quadratic form* if

- q is a quadratic map, i.e. $q(\lambda v) = \lambda^2 q(v)$ for each $\lambda \in k$ and $v \in V$.
- The associated polar form $b_q\colon V \times V \to k$ sending $(v, w) \rightsquigarrow \frac{q(v+w)-q(v)-q(w)}{2}$ is bilinear. Note that b_q is clearly symmetric by definition.

Any quadratic form can be *diagonalized* and written as

$$q := \langle a_1, a_2, \ldots, a_n \rangle.$$

That is there exists a basis of vectors $e_i \in V$ such that $q\left(e_i\right) = a_i$ and $b_q\left(e_i, e_j\right) = 0$ for $i \neq j$.

The *orthogonal sum* of two quadratic forms (V, q) and (V', q') over k written $(V, q) \perp (V', q')$ is defined to be the qudratic form $q \perp q' \colon V \times V' \to k$ sending $(v, v') \rightsquigarrow q(v) + q'(v')$. For $a \in k$, the quadratic form $aq \colon V \to k$ sends $v \rightsquigarrow aq(v)$.

An *isometry* between quadratic spaces (V, q) and (V', q') is a k-linear isomorphism $f \colon V \to V'$ such that $q'\left(f(v)\right) = q(v)$ for each $v \in V$.

A quadratic form q is said to be *non-degenerate* (or *regular*) if $\widetilde{b_q} \colon V \to V^*$ induced by b_q is injective (and hence an isomorphism since V is finite dimensional). It is called *isotropic* if it represents 0 non-trivially and *anisotropic* otherwise.

We denote the two dimensional quadratic form $\langle 1, -1 \rangle$ by $\mathbb{H}$ and call it the *hyperbolic plane*. For $r \in \mathbb{N}$, the symbol $\mathbb{H}^r$ then denotes the orthogonal sum of r hyperbolic planes which we term a *hyperbolic space*.

Two regular quadratic forms q_1, q_2 are defined to be *Witt equivalent* if there exist $r, s \in \mathbb{Z}$ such that $q_1 \perp \mathbb{H}^r \simeq q_2 \perp \mathbb{H}^s$. Define $\mathrm{W}(k)$ to be the set of isomorphism classes of regular quadratic forms modulo Witt equivalence.

It turns out that $\mathrm{W}(k)$ is an abelian group under $\perp$ and can further be made into a ring (called the *Witt ring*) using the tensor product operation $\otimes$. For example, if $q_1 = \langle a_1, \ldots, a_n \rangle$, then $q_1 \otimes q_2 = a_1 q_2 \perp a_2 q_2 \perp \ldots \perp a_n q_2$.

Witt's decomposition theorem implies that each equivalence class in $\mathrm{W}(k)$ has a unique anisotropic quadratic form as a representative.

Let $\mathrm{I}(k)$ denote the ideal of classes of even dimensional quadratic forms in $\mathrm{W}(k)$. The ideal $\mathrm{I}(k)$ is called the *fundamental ideal.* Note that $\mathrm{I}(k)$ is additively generated by forms of the shape $\langle a, b\rangle$. And since

$$\langle a, b\rangle = \langle 1, a\rangle - \langle 1, -b\rangle \in \mathrm{W}(k),$$

$\mathrm{I}(k)$ is in fact additively generated by *1-fold Pfister forms* $\langle\langle c\rangle\rangle := \langle 1, c\rangle$. One can also check that $\frac{\mathrm{W}(k)}{\mathrm{I}(k)} \simeq \frac{Z}{2\mathbb{Z}}$ quite easily.

Define $\mathrm{I}^0(k) := \mathrm{W}(k)$. For $n > 0$, the symbol $\mathrm{I}^n(k)$ denotes the n^{th} power of the fundamental ideal. This is therefore additively generated by *n-fold Pfister forms*

$$\langle\langle c_1, c_2, \ldots, c_n\rangle\rangle := \otimes_{i=1}^{n}\langle\langle c_i\rangle\rangle.$$

Note that $\frac{\mathrm{I}^n(k)}{\mathrm{I}^{n+1}(k)}$ is an elementary abelian 2-group for each $n \geq 0$. Let's check this easy fact. It is abelian because $\mathrm{W}(k)$ is abelian. And since n-fold Pfister forms generate $\mathrm{I}^n(k)$ additively, it is enough to check that

$$2q \in \mathrm{I}^{n+1}(k) \text{ for } q = \langle\langle c_1, c_2, \ldots, c_n\rangle\rangle.$$

Let $q' = \langle\langle c_2, c_3, \ldots, c_n\rangle\rangle$ and by induction, assume $2q' \in \mathrm{I}^n(k)$ and hence is a sum of n-fold Pfister forms $\sum f_i$. Thus

$$\begin{aligned}2q &= (\langle\langle c_1\rangle\rangle \otimes q') + (\langle\langle c_1\rangle\rangle \otimes q') \\ &= \langle\langle c_1\rangle\rangle \otimes 2q' \\ &= \langle\langle c_1\rangle\rangle \otimes \left(\sum f_i\right) \\ &= \sum f_i'\end{aligned}$$

where $f_i' = \langle\langle c_1\rangle\rangle \otimes f_i$ is an $(n+1)$-fold Pfister form and hence in $\mathrm{I}^{n+1}(F)$.

The powers of the fundamental ideal give a filtration of the Witt ring

$$\mathrm{W}(k) = \mathrm{I}^0(k) \supseteq \mathrm{I}^1(k) \supseteq \mathrm{I}^2(k) \supseteq \dots,$$

which is rather useful because of the following theorem :

Theorem 1.2 (Arason-Pfister-Hauptsatz, '71)**.**

$$\bigcap_{n=0}^{\infty} \mathrm{I}^n(k) = 0.$$

The *graded Witt ring* $\overline{\mathrm{W}}(k) := \bigoplus_{n=0}^{\infty} \frac{\mathrm{I}^n(k)}{\mathrm{I}^{n+1}(k)}$ is an oft-studied object in quadratic form theory.

1.3.2 Algebras with involutions

We are going to be even more brief here, content with only giving the definitions and refering the interested reader to ([KMRT], Chapter I).

Let K be a field of characteristic not 2. Let A/K be a central simple algebra. An involution $\sigma\colon A \to A$ is a morphism such that for each $a, b \in A$, the following holds :

1. $\sigma(a+b) = \sigma(a) + \sigma(b)$,

2. $\sigma(ab) = \sigma(b)\sigma(a)$,

3. $\sigma^2(a) = a$.

Set $k := K^\sigma$. If $K = k$, then we say σ is of *the first kind* and else, we say it is of the *second kind*. Involutions of the first kind can further be subdivided into types because of the following :

Theorem 1.3 ([KMRT], Page 1)**.** *Let $A = \mathrm{M}_n(k)$. Then there is a $1-1$ correspondence between the set of k-linear involutions of A and equivalence classes of symmetric or skew-symmetric nondegenerate bilinear forms on V modulo multiplication by a factor in k^*.*

Thus if σ is an involution of the first kind on A/k, then we say σ is

- *orthogonal* if over some splitting field L/k of A, the involution $\sigma \otimes L$ corresponds to a symmetric bilinear form under the above correspondence.

- *symplectic* if over some splitting field L/k of A, the involution $\sigma \otimes L$ corresponds to a skew-symmetric bilinear form under the above correspondence.

If $A = \mathrm{M}_n(k)$, then the transpose is an example of an orthgonal involution. The canonical involution on the Hamiltonian quarternions $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}\, i \oplus \mathbb{R}\, j \oplus \mathbb{R}\, k$ sending $x \rightsquigarrow -x$ for $x \in \{i, j, k\}$ is a symplectic involution.

There is a notion of *hyperbolicity* for an involution. If K/k is a field extension, σ is *hyperbolic* if and only if there exists an idempotent $e \in A$ such that $\sigma(e) = 1 - e$. ([KMRT], Prop 6.7, Pg 74).

Chapter 2

Examining Clifford's algebras

'Structures are the weapons of the mathematician.'

- Bourbaki

Clifford algebras make their presence felt throughout this thesis by either showing up as themselves or helping define other crucial algebraic structures. Thus, we begin by examining Clifford algebras in earnest. The main sources of references for this chapter are the seminal paper of Professor Clifford ([Cliff]), the pleasant notes in ([Knus88], Chapter IV) and ([Tignol93], Chapter II) and of course ([KMRT], Chapter II, §8).

2.1 Generalizing quaternions

Named after British mathematician William Kingdon Clifford, they were first written down by the latter under the name *geometric algebras* in an attempt to generalize the quaternions and the biquaternions to higher dimensions.

The Hamiltonian quaternions is a four dimensional real vector space $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}\, i \oplus \mathbb{R}\, j \oplus \mathbb{R}\, k$ made into a non-commutative algebra by the relations $i^2 = j^2 = k^2 = -1$ and $k = ij = -ji$.

Instead imagine four points a_0, x_1, x_2 and x_3 in the three dimensional real space so that '*x_1, x_2 and x_3 are at an infinite distance from a_0 in three* *directions at right angles to one another'*. That is, imagine a_0 as the origin, x_1, x_2 and x_3 as the points at infinity on the X, Y and Z-axes respectively. Let a_0x_1 (or more generally xy) represent a unit length placed anywhere on the x-axis (or more generally on the line joining the points x and y) but measured in the positive direction. Thus $xy = -yx$. When generalizing to higher dimensions, the triple xyz represents a unit area on the plane through the points x, y and z etc.

One can view the quaternions as operators on the three dimensional real space also. For instance, view the Hamiltonian vector $i \in \mathbb{H}$ as the operator which rotates the line segment a_0x_2 into the line segment a_0x_3. Thus, remembering the right hand thumb rule, we have

$$i\left(a_0x_2\right) = a_0x_3,\ \ j\left(a_0x_3\right) = a_0x_1,\ \ k\left(a_0x_1\right) = a_0x_2$$

Thus i translates x_2 to x_3 and we write $i = x_2x_3$ and similarly $j = x_3x_1$ and $k = x_1x_2$. Rewriting the above relations, we get some multiplicative relations on the x_i. For instance,

$$\begin{aligned}
& i\left(a_0x_2\right) = a_0x_3 \\
\Longrightarrow\ & x_2\left(x_3a_0\right)x_2 = a_0x_3 \\
\Longrightarrow\ & x_2\left(-a_0x_3\right)x_2 = a_0x_3 \\
\Longrightarrow\ & x_2a_0\left(x_2x_3\right) = a_0x_3 \\
\Longrightarrow\ & -x_2^2a_0x_3 = a_0x_3 \\
\Longrightarrow\ & x_2^2 = -1.
\end{aligned}$$

Now abusing some notation meaningfully, let x_1 in fact represent x_2x_3 (which is how we are viewing i also), x_2 represent x_3x_1 (which represents j also) and

x_3 represent x_1x_2 (which represents k also). Then, we recover the Hamiltonian quaternion relations. As an example,

$$ij = (x_2x_3)(x_3x_1) = (x_1)(x_2) = x_1x_2 = k$$

Clifford's generalization leads to the construction of the *geometric n algebra* which is the real algebra generated by $x_1, x_2, \ldots, x_n$ satisfying the relations $x_r^2 = -1$ and $x_rx_s = -x_sx_r$ for all $s \neq r$. This, we will see in the next section is exactly the Clifford algebra defined for the quadratic form $\langle\underbrace{-1, -1, \ldots, -1}_{n}\rangle$

Note that $(x_1x_2\ldots x_m)^2 = (-1)^{\frac{m(m+1)}{2}}$. Thus the Hamiltonian quaternion algebra is simply the geometric 2 algebra on two generators $i = x_1$ and $j = x_2$. Clifford goes on to determine the dimension of the n-algebra and shows that such algebras are in fact tensor products of quaternion algebras if n is even. And if n is odd, the *even subalgebras* of the n-algebras are tensor products of quaternion algebras!

2.2 Clifford algebra of a quadratic form

For the rest of this chapter, let k be a field of characteristic not 2 and let (V, q) be a finite dimensional regular quadratic space of dimension n over k. We are looking for a unital k-algebra $\mathrm{C}(V, q)$ and a k-linear map $i : V \to \mathrm{C}(V, q)$ such that $i(v)^2 = q(v)$.

We define the Clifford algebra of the quadratic space (V, q) to be the one which is universal for this property. Namely, if A is another such algebra with $j : V \to A$ satisfying $j(v)^2 = q(v)$, then there exists a unique k-algebra morphism f making the following diagram commute.

$$\begin{tikzcd} V \arrow[rr, "i"] \arrow[dr, "j"'] & & \mathrm{C}(V,q) \arrow[dl, dashed, "\exists! f"] \\ & A & \end{tikzcd}$$

The universal property guarantees that the Clifford algebra is unique up to isomorphism if it exists. Let us now give the most obvious way of constructing an algebra which satisfies the universal property: by going modulo the tensor algebra via the neccesary relations. More precisely, let $T(V)$ stand for the tensor algebra

$$T(V) = k \oplus V \oplus V \otimes_k V \oplus \dots$$

There is a natural k-linear map $\tilde{i} : V \to T(V)$ sending $v \rightsquigarrow v$. Since we want v^2 to pinch down to the scalar $q(v)$, we set

$$\mathrm{C}(V,q) := \frac{T(V)}{J},$$

where J is the two sided ideal generated by $\{v \otimes v - q(v) \mid \forall v \in V\}$. The map $i : V \to \mathrm{C}(V,q)$ is the natural one induced by $\tilde{i}$.

This should remind you of the construction of the exterior algebra ΛV. In fact, it is nothing but the Clifford algebra construction if we considered the (highly singular!) trivial quadratic form $\langle 0, 0, \dots, 0\rangle$.

Using the universal property, one can check that the Clifford algebra construction behaves well under field extensions. That is if L/k is a field extension, then

$$\mathrm{C}(V, q_L) \simeq \mathrm{C}(V,q) \otimes_k L.$$

And just like the exterior algebra, the dimension of $\mathrm{C}(V,q)$ as a k-vector space is 2^n. In fact, we also have the stronger

Theorem 2.1 (Poincaré - Birkhoff - Witt)**.** *If $e_1, e_2, \ldots, e_n$ form a k-basis of V, then the following is a k-basis of* $\mathrm{C}(V,q)$

$$\{1, i(e_{j_1})\, i(e_{j_2}) \ldots i(e_{j_r}) \mid 1 \leq r \leq n, 1 \leq j_1 < j_2 \ldots < j_r \leq n\}.$$

Let us work out the case when $n = 1$. Let $q = \langle a \rangle$ for $a \in k^*$ and let $V = ke$ where e is a basis vector of V. Thus $T(V) \simeq k[t]$, the polynomial ring and we identify e with t and in general V with monomials of degree one $\{\beta t \mid \beta \in k\}$.

Then $\mathrm{C}(V,q) \simeq k[t]/(t^2 - a)$ which is a two dimensional vector space over k. And $\{1, \beta t\}$ for any $\beta \in k \setminus 0$ is a k-basis of $\mathrm{C}(V,q)$. For a complete proof, see ([Knus88], Chapter IV, Thm 5).

Note that the above theorem implies that the map $i : V \to \mathrm{C}(V,q)$ is injective. And therefore we identity V with $i(V)$ in $\mathrm{C}(V,q)$.

2.2.1 The even Clifford algebra $\mathrm{C}_0(V,q)$

The tensor algebra $T(V)$ is clearly $\mathbb{Z}_{\geq 0}$ graded, i.e. elements in $V^{\otimes i}$ have degree i. Now $\mathrm{C}(V,q)$ is $T(V)$ modulo the ideal generated by $\{v \otimes v - q(v)\}$. Note that $v \otimes v - q(v)$, though not a homogeneous element, at least is of even degree. Thus $\mathrm{C}(V,q)$ is naturally $\mathbb{Z}/2\mathbb{Z}$ graded.

Separating out the elements of odd and even degree, we get the following decomposition

$$\mathrm{C}(V,q) = \mathrm{C}_0(V,q) \oplus \mathrm{C}_1(V,q),$$

where $\mathrm{C}_0(V,q)$ is a k-subalgebra consisting of elements of even degree. However $\mathrm{C}_1(V,q)$, the subset of elements of odd degree is no longer an algebra (squares of odd degree elements have even degree!) but simply a module over $\mathrm{C}_0(V,q)$. The dimensions of $\mathrm{C}_0(V,q)$ and $\mathrm{C}_1(V,q)$ as k-vector spaces are both 2^{n-1}.

Definition 2.2 ([Tignol93], Lemma 2.1)**.** *We can in fact alternatively also construct the even Clifford algebra as a quotient of the tensor algebra of $V \otimes V$ as follows :*

$$\mathrm{C}_0\,(V,q) = \frac{T(V \otimes V)}{I_1 + I_2},$$

where

- *I_1 is the two-sided ideal generated by elements of the form $v \otimes v - q(v)$ for $v \in V$,*
- *I_2 is the two-sided ideal generated by elements $u \otimes v \otimes v \otimes w - q(v) u \otimes w$ for $u, v, w \in V$.*

2.2.2 Structure theorem for Clifford algebras

Theorem 2.3. *Let (V,q) be a non-singular quadratic space of dimension equal to n over k.*

1. *If $n = 2m$, then $\mathrm{C}(V,q)$ is a central simple algebra of dimension 2^n over k. The center of the even Clifford algebra, $Z = \mathrm{Z}\,(C_0(V,q))$, is an étale quadratic extension of k which matches with the discriminant of q. And $\mathrm{C}_0(V,q)$ is a central simple algebra of dimension 2^{n-2} over Z.*

2. *If $n = 2m+1$, then* $\mathrm{C}(V,q)$ *is a central simple algebra of dimension* 2^{n-1} *over* $Z' = \mathrm{Z}(\mathrm{C}(V,q))$. *The even Clifford algebra,* $\mathrm{C}_0(V,q)$ *is a central simple algebra of dimension* 2^{n-1} *over* k. *Further*

$$\mathrm{C}_0(V,q) \otimes_k Z' \simeq \mathrm{C}(V,q).$$

We restrict ourselves to analyzing the low dimension cases and refer the reader to ([Knus88], Chapter IV, Section IV, Thm 8) for the complete proof.

When $n = 1$, we have already seen in the proof of Theorem 2.1 that $\mathrm{C}(V,q) = k[t]/(t^2 - a)$ when $q = \langle a \rangle$. Thus $\mathrm{C}(V,q)$ is itself commutative and hence $Z' = \mathrm{C}(V,q)$. Since $\operatorname{char} k \neq 2$, Z' is either a separable field extension of k (if a is not a square in k^*) or $k \times k$ (if a is a square in k^*). Hence $\mathrm{C}(V,q) \simeq k[t](t^2 - a) \simeq k.1 \oplus k.\bar{t} \simeq \mathrm{C}_0(V,q) \oplus \mathrm{C}_1(V,q)$. Thus $\mathrm{C}_0(V,q)$ is just k which finishes the proof in this case.

Let $n = 2$ and let $q = \langle a, b \rangle$. Let v, w be a k-basis of V such that $q(v) = a$, $q(w) = b$ and $b_q(v,w) = 0$. Thus in $\mathrm{C}(V,q)$,

$$\begin{aligned}
(v+w)^2 &= q(v+w) \\
&= q(v) + q(w) + 2b_q(v,w) \\
&= q(v) + q(w) \\
&= v^2 + w^2.
\end{aligned}$$

This implies $vw = -wv$. Thus $\mathrm{C}(V,q) = k.1 \oplus k.v \oplus k.w \oplus k.vw$ where $v^2 = a$, $v^2 = b$ and $vw = -wv$. Thus it is the generalized quaternion algebra (a,b), which is a central simple algebra of dimension 4 over k.

Since $(vw)^2 = (vw)(vw) = -v^2w^2 = -ab$,

$$\mathrm{C}_0(V,q) \simeq k.1 \oplus k.vw \simeq k[t]/(t^2+ab),$$

which is a two dimensional commutative étale algebra over k. Note that the discriminant of $q = \langle a, b\rangle$ is $(-1)^{\frac{(2)(2-1)}{2}} = -ab$. Hence we are done.

2.2.3 Involutions on Clifford algebras

Let us put the universal property satisfied by Clifford algebras to use to define involutions on them. Let $C = \mathrm{C}(V,q)$ and consider C^{op}, the opposite k-algebra along with the natural k-linear map $j : V \to C^{\mathrm{op}}$. Clearly $j(v)^2 = i(v)^2 = q(v)$ and hence by the universal property of Clifford algebras, we get a k-algebra map $\tau : C \to C^{\mathrm{op}}$ which sends $v \rightsquigarrow v$.

$$\begin{tikzcd} V \arrow[rr, "i"] \arrow[dr, "j"'] & & C \arrow[dl, dashed, "\exists!\tau"] \\ & C^{\mathrm{op}} & \end{tikzcd}$$

Interpreting τ as a map from C to itself, it becomes an anti-homomorphism.

$$\tau : C \to C, \ \tau(xy) = \tau(y)\tau(x).$$

Thus $\tau^2 = \tau \circ \tau$ is a legitimate homomorphism from C to itself which sends $v \in V$ to itself. It is an easy check to see that $\tau^2 = \mathrm{id}\,|_C$. Thus we have manufactured an involution $\tau : C \to C$ over k, which we will henceforth term the *canonical involution* of $\mathrm{C}(V,q)$.

The involution τ preserves the $\mathbb{Z}/2\mathbb{Z}$ grading of $\mathrm{C}(V,q)$ and hence restricts to an involution $\tau_0 : \mathrm{C}_0(V,q) \to \mathrm{C}_0(V,q)$ over k which we again call the canonical involution of $\mathrm{C}_0(V, q)$. It turns out that the dimension of V also determines the *type* of the involution τ_0 which we record below.

Theorem 2.4 ([KMRT], Prop 8.4, Pg 89)**.** *Let (V, q) be a non-singular quadratic space of dimension n over field k which is not of characteristic 2. Let τ_0 denote the canonical involution on the even Clifford algebra $\mathrm{C}_0 = \mathrm{C}_0(V, q)$. Then*

1. *If n is odd, then C_0 is a c.s.a over k and τ_0 is*

    $\rightarrow$ *orthogonal if $n = 8m \pm 1$.*

    $\rightarrow$ *symplectic if $n = 8m \pm 3$.*

2. *If n is even, then C_0 is a c.s.a over Z, the discriminant extension of q and τ_0 is*

    $\rightarrow$ *unitary if $n = 4m + 2$.*

    $\rightarrow$ *of the first kind if $n = 4m$, that is τ_0 fixes Z. Further τ_0 is*

    - *orthogonal if $n = 8m'$.*
    - *symplectic if $n = 8m' + 4$.*

The involutions τ and τ_0 give isomorphisms of $\mathrm{C}(V, q)$ and $\mathrm{C}_0(V, q)$ with their respective opposite algebras. Thus we immediately see that in the appropriate Brauer groups, these algebras are in fact of order at most two, or as we like to call it, two torsion. Of course, a little more work is needed to show the fact that they can be broken up into quaternions.

As a satisfying corollary, we get that isotropicity of a quadratic form implies hyperbolicity of the involutions on its Clifford and even Clifford algebra.

Corollary 2.5. *Let (V, q) be isotropic. Then τ and τ_0 are hyperbolic involutions.*

Proof. An involution σ is hyperbolic if we can find an idempotent e such that $\sigma(e) = 1 - e$. Since q is isotropic, there is a hyperbolic plane in V. That is, there are two vectors $v, w \in V$ such that $q(v) = 1$, $q(w) = -1$ and $b_q(v, w) = 0$. Thus $vw = -wv$ and $(v + w)^2 = (v - w)^2 = 0$. Then set

$$e = \frac{(v + w)(v - w)}{4} = \frac{v^2 + wv - vw - w^2}{4} = \frac{1 + wv}{2}.$$

Then we have $e^2 = e$ for

$$\frac{(1 + wv)^2}{4} = \frac{1 + (wv)^2 + 2wv}{4} = \frac{1 - w^2v^2 + 2wv}{4} = \frac{1 + wv}{2}.$$

Now $e \in \mathrm{C}_0(V, q)$ and $\tau(e) = \tau_0(e) = \frac{1+vw}{2} = \frac{1-wv}{2} = 1 - e$. $\square$

2.3 Clifford algebra of an algebra with orthogonal involution

A quadratic form or equivalently, a symmetric bilinear form $b : V \times V \to k$ induces an orthogonal involution $\sigma_b : \mathrm{End}_k(V) \to \mathrm{End}_k(V)$ by the relation

$$b(x, f(y)) = b(\sigma_b(f)(x), y),\ \forall f \in \mathrm{End}_k(V),\ \forall x, y \in V.$$

Note that this implies that the adjoint involutions of bilinear form b and a scaled version λb for $\lambda \in k^*$ are the same. i.e $\sigma_{\lambda b} = \sigma_b$.

In this section, we would like to define the notion of a Clifford algebra for an algebra with an orthogonal involution using the definition in the quadratic form case and recover similar structure theorems about its shape and its involutions.

The immediate stumbling block is that $\mathrm{C}(V, q)$ is not necessarily isomorphic to $\mathrm{C}(V, \lambda q)$ for $\lambda \in k^*$. For instance, compare the Clifford algebras of $q_1 = \langle 1 \rangle$ and $q_2 = \langle \lambda \rangle$ for $\lambda \in k^* \setminus k^{*2}$. Then $\mathrm{C}(V, q_1) = k \times k$ whereas $\mathrm{C}(V, q_2)$ is a field extension $k\left(\sqrt{\lambda}\right)$. However the even Clifford algebra behaves better and is therefore the right object to be generalized!

Before we write down the definition of a general Clifford algebra, let us translate Definition 2.2 from the language of quadratic forms into the language of algebras with involutions. If (V, q) is a non-singular quadratic space of dimension n over k, then $A = \mathrm{End}_k(V)$ is a central simple algebra of degree n and $\sigma = \sigma_q$, the adjoint involution of q. We go further and identify A with $V \otimes V$ as follows :

$$V \otimes V \xrightarrow{\quad \simeq \quad} V \otimes V^* \xrightarrow{\quad \simeq \quad} \mathrm{End}_k(V)$$

$$v \otimes w \longrightarrow v \otimes [x \mapsto b_q(w, x)] \longrightarrow [x \mapsto v b_q(w, x)] \,.$$

Under this identification, the trace map $\mathrm{Tr} : A \to k$ sends $v \otimes w \rightsquigarrow b_q(v, w)$. Thus $q(v) = \mathrm{Tr}(v \otimes v)$.

Let us calculate what $f = \sigma_q(v \otimes w)$ is where σ_q is the adjoint involution. We guess (correctly!) that it has to be $g = w \otimes v$ and show it as follows :

$$\begin{aligned} b_q(\sigma_q(v \otimes w)(x), y) &= b_q(x, v \otimes w(y)) \\ &= b_q(x, v b_q(w, y)) \\ &= b_q(w, y) b_q(x, v) \end{aligned}$$

$$\begin{aligned} b_q(w \otimes v(x), y) &= b_q(w b_q(v, x), y) \\ &= b_q(w, y) b_q(v, x). \end{aligned}$$

Thus $b_q(f(x), y) = b_q(g(x), y)$ for all $x, y \in V$ which implies $f(x) = g(x)$ for all $x \in V$ which implies $f = g$. This is because our quadratic form is non-singular. Also similarly one can check or at least believe with impunity that multiplication in A behaves as follows :

$$(v \otimes w)(v' \otimes w') = v b_q(w, v') \otimes w'. \qquad (*)$$

We would like to imitate Definition 2.2 in as straightforward a manner as possible. For the definition of the analogue of ideal I_1, we can replace elements of the shape $v \otimes v$ with the the elements of A fixed by the orthogonal involution σ and use the reduced trace of A instead of the quadratic form.

However for the analogue of ideal I_2, we need to work harder to understand what the elements of the shape $u \otimes v \otimes v \otimes w$ correspond to. But the other part is easy, namely the analogue of $q(v)u \otimes w$. Define the multiplication map $m : A \otimes A \to A$ which sends $a \otimes b \rightsquigarrow ab$. Using (*) above, it is clear that $q(v)u \otimes w = m(u \otimes v \otimes v \otimes w)$.

We now proceed to give the construction of a map $\sigma_2 : A \otimes A \to A \otimes A$ (without proof) such that when $\sigma = \sigma_q$, we have

$$\sigma_2(u \otimes v \otimes v' \otimes w) = u \otimes v' \otimes v \otimes w. \qquad (**)$$

Recall the Sandwich isomorphism $Sand : A \otimes A \to \mathrm{End}_k(A)$ which sends $a \otimes b \rightsquigarrow [x \mapsto axb]$. In a manner somewhat reminiscent of defining the adjoint involution, we define the map $\sigma_2 : A \otimes A \to A \otimes A$ via the following property : For all $u \in A \otimes A$ and $a \in A$

$$Sand(\sigma_2(u))(a) = Sand(u)(\sigma(a)).$$

For a proof that such a σ_2 satisfies (**), see ([Tignol93], Lem 2.3). We hope that the above discussion will aid in making the following definition of the Clifford algebra less of a mystery than it might seem at first glance.

Definition 2.6 ([Tignol93], Def 2.4)**.** *Let* (A, σ) *be a central simple algebra over* k *with an orthogonal involution and let* $T(A)$ *denote the tensor algebra on* A*. We define the Clifford algebra of* (A, σ) *(which generalizes the even Clifford algebra in the split case) to be*

$$\mathrm{C}\,(\mathrm{A}, \sigma) = \frac{T(A)}{J_1 + J_2},$$

where

- J_1 *is the ideal generated by elements of the form* $s - \mathrm{Trd}(s)$ *for* $s \in A$ *such that* $\sigma(s) = s$*.*
- J_2 *is the ideal generated by elements of the form* $u - m(u)$ *for* $u \in A \otimes A$ *such that* $\sigma_2(u) = u$*.*

The involution $\underline{\sigma} : T(A) \to T(A)$ which sends

$$a_1 \otimes a_2 \ldots \otimes a_r \rightsquigarrow \sigma(a_r) \otimes \ldots \otimes \sigma(a_2) \otimes \sigma(a_1),$$

descends to an involution on $\mathrm{C}\,(\mathrm{A}, \sigma)$ which we call its *canonical involution.* This exactly matches with τ_0 when $A = \mathrm{End}_k(V)$. And the structure theorems 2.3 and 2.4 pertinent to the even Clifford algebra and its canonical involution for even degree algebras (A, σ) in the split case go through in the general case without any change. Namely,

Theorem 2.7 ([KMRT], Thm 8.10, Prop 8.12, Pg 94-95)**.** *Let* (A, σ) *be a central simple algebra of degree* $n = 2m$ *with orthogonal involution over field* k *which is not of characteristic* 2*. Let* τ_0 *denote the canonical involution on its Clifford algebra* $\mathrm{C} = \mathrm{C}\,(\mathrm{A}, \sigma)$*. Then* C *is a c.s.a over* Z *of degree* 2^{m-1} *where* Z *is the discriminant extension of* (A, σ)*. The canonical involution* τ_0 *is*

- $\to$ *unitary if* $n = 4m' + 2$*.*
- $\to$ *of the first kind if* $n = 4m'$*, that is* τ_0 *fixes* Z*. Further* τ_0 *is*
  - *orthogonal if* $n = 8m''$*.*
  - *symplectic if* $n = 8m'' + 4$*.*

2.4 Examples serve better than description

- If $q = \langle a \rangle$, then $\mathrm{C}(V, q) = k[t]/(t^2 - a)$, the étale quadratic extension of k. The even Clifford algebra is simply k and τ_0 is the identity map on k.

- If $q = \langle a, b \rangle$, then $\mathrm{C}(V, q) = (a, b)$, the generalized quaternion algebra. The canonical involution τ of $\mathrm{C}(V, q)$ is the usual involution on the quaternions sending $i \rightsquigarrow -i$ and $j \rightsquigarrow -j$.

  The even Clifford algebra is $k[t]/(t^2 + ab)$, the discriminant extension and τ_0 is the non-trivial k-morphism of Z sending $\sqrt{-ab}$ to $-\sqrt{-ab}$.

- If $q = \langle \underbrace{-1, -1, \ldots, -1}_{m} \rangle$, then $\mathrm{C}(V, q)$ is the geometric m-algebra as defined by Clifford (c.f. Section 2.1).

- If q is the hyperbolic quadratic form of dimension $2n$, then $\mathrm{C}(V, q)$ is $\mathrm{M}_{2^n}(k)$.

- If $A = Q_1 \otimes Q_2$ where each Q_i is a quaternion algebra over k and $\sigma = \gamma_1 \otimes \gamma_2$ where γ_i is the canonical involution on Q_i, then by ([Tignol93], Ex 2.10) or ([KMRT], Ex 8.19)

$$\mathrm{C}\left(\mathrm{A}, \sigma\right) = Q_1 \times Q_2.$$

Chapter 3

A walk through the classification of linear algebraic groups

'I only went out for a walk, and finally concluded to stay out till sundown, for going out, I found, was really going in.'
- John Muir

In this chapter, we recall very briefly what it means for a (smooth) linear algebraic group to be reductive or semi-simple (simply connected or adjoint). We then present, in a rather terse manner, the classification due to Weil of *classical* absolutely simple simply connected and adjoint groups in terms of algebras with involutions. We concentrate on groups of type D_n and define some related groups like the Clifford group and the extended Clifford group for they will prove to be of use later on in this dissertation. For a reference, we suggest ([KMRT], Chapter VI, §26) or some parts of ([Me98], §4 - 9).

3.1 Some adjectives of linear algebraic groups

For the rest of this section, let G denote a smooth connected linear algebraic over perfect field k. It is said to be *unipotent* if all its elements are unipotent. An example would be the additive group $\mathbb{G}_a$.

G/k is said to be *reductive* if $G \times_k \overline{k}$ has no nontrivial, connected, unipotent, normal subgroups. An example would be GL_n. In general, the maximal connected unipotent normal subgroup of G is called its *unipotent radical*, denoted $\mathrm{R}_u(G)$. The quotient $G/\mathrm{R}_u(G)$ is reductive .

G/k is said to be *semisimple* if it is nontrivial and $G \times_k \overline{k}$ has no nontrivial, connected, solvable, normal subgroups. An example would be SL_n. In general, the maximal connected solvable normal subgroup of G is called its *radical*, denoted $\mathrm{R}(G)$. The quotient $G/\mathrm{R}(G)$ is semisimple.

The unipotent radical $\mathrm{R}_u(G)$ is also just the unipotent elements of $\mathrm{R}(G)$ and hence every semisimple group is immediately reductive.

A subtorus $T \subseteq G$ is said to be maximal if it is not contained in a larger subtorus. It is a theorem of Grothendieck that there always exists a maximal subtorus T defined over k. A semisimple group G/k is said to be *split* if it contains a maximal torus which is k-split. Every semisimple group G/k becomes split over k^{sep}.

For a split semisimple group G/k with split maximal torus T/k, one can define using the adjoint representation $ad : G \to \mathrm{Lie}(G)$, a root system which in turn defines the *root lattice* Λ_r and the weight lattice Λ sandwiching the character group T^* in between

$$\Lambda_r \subseteq T^* \subseteq \Lambda.$$

The split semisimple group G/k is called *simply connected* if $T^* = \Lambda$ and *adjoint* if $T^* = \Lambda_r$. Examples would be SL_n and PGL_n respectively. A semisimple group G/k is said to be simply connected (resp. adjoint) if the split group $G \times_k k^{sep}$ is so.

A surjective morphism of algebraic groups with finite kernel is called an *isogeny* of algebraic groups. An isogeny is called central if its kernel is central. Given any semisimple group G/k, there exists up to isomorphism, a unique simply connected group $\tilde{G}$ and a unique adjoint group $\overline{G}$ with central isogenies $\tilde{G} \to G$ and $G \to \overline{G}$. ([KMRT], Thm 26.7, Pg 364). The group $\tilde{G}$ is said to be the *simply connected cover* of G.

A semisimple group G is said to be *absolutely simple* if $G \times_k k^{sep}$ is simple (i.e no nontrivial connected normal subgroups). Any simply connected (resp. adjoint) semisimple group is a product of Weil restrictions of absolutely simple simply connected (resp. adjoint) groups. ([KMRT], Thm 26.8, Pg 365).

Let G/k be an absolutely simple semisimple group. Then it is of type A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4 or G_2. Groups of type A_n, B_n, C_n or (non-trialitarian) D_n are termed *classical* whereas groups of the remaining types are called *exceptional*.

3.2 Classical groups á la Weil

Let k be a field of characteristic not 2 and let K/k be such that $K = k$ or a quadratic étale extension. Let A be an Azumaya algebra over K with involution σ such that the fixed field $K^\sigma = k$. We define its *group of similitudes*, $\mathrm{Sim}\,(\mathrm{A}, \sigma)$ to be as follows

$$\mathrm{Sim}\,(\mathrm{A}, \sigma)(k) := \{a \in A \mid \sigma(a)a \in k^*\}.$$

The *group of isometries* $\mathrm{Iso}\,(\mathrm{A}, \sigma)$ is defined as follows :

$$\mathrm{Iso}\,(\mathrm{A}, \sigma)(k) := \{a \in A \mid \sigma(a)a = 1\}.$$

The multiplier map is defined to be the morphism $\mu : \mathrm{Sim}\,(\mathrm{A}, \sigma) \to \mathbb{G}_m$ sending $a \rightsquigarrow \sigma(a)a$. Now A is a central simple algebra over K and K^* is in the center of $\mathrm{Sim}\,(\mathrm{A}, \sigma)(k)^*$. Thus one can define the *group of projective similitudes*

$$\mathrm{PSim}\,(\mathrm{A}, \sigma) := \mathrm{Sim}\,(\mathrm{A}, \sigma)\,/R_{K/k}\mathbb{G}_m.$$

Since the torus $R_{K/k}\mathbb{G}_m$ is quasi-trivial, we have

$$\mathrm{PSim}\,(\mathrm{A}, \sigma)(k) = \mathrm{Sim}\,(\mathrm{A}, \sigma)(k)/K^*.$$

If f is an automorphism of A, Skolem-Noether implies f is an inner automorphism, say $\mathrm{Int}(g)$ for some $g \in A^*$. Then we have

$$\begin{aligned} f \circ \sigma = \sigma \circ f &\iff f\left(\sigma(a)\right) = \sigma\left(f(a)\right)\ \forall\ a \in A \\ &\iff g\sigma(a)g^{-1} = \sigma(g)^{-1}\sigma(a)\sigma(g)\ \forall\ a \in A \\ &\iff \sigma(g)g \in K^* \\ &\iff \sigma(g)g \in k^* \\ &\iff g \in \mathrm{Sim}\,(\mathrm{A}, \sigma)(k) \end{aligned}$$

Thus, we have an isomorphism $\mathrm{Int} : \mathrm{Sim}\,(\mathrm{A}, \sigma)(k)/K^* \to \mathrm{Aut}_K\left((\mathrm{A}, \sigma)\right)(k)$.

Denote the connected component containing the identity of $\mathrm{Sim}\,(\mathrm{A}, \sigma)$ by $\mathrm{Sim}_+\,(\mathrm{A}, \sigma)$. Similarly define $\mathrm{PSim}_+\,(\mathrm{A}, \sigma)$, $\mathrm{Iso}_+\,(\mathrm{A}, \sigma)$ and $\mathrm{Aut}_+\,(\mathrm{A}, \sigma)$. Then $\mathrm{PSim}_+\,(\mathrm{A}, \sigma) \simeq \mathrm{Aut}_+\,(\mathrm{A}, \sigma)$.

Just to make the reader feel at home, we recall what the above groups are when $A = \mathrm{End}_k(V)$ and $\sigma = \sigma_{b_q}$, the involution adjoint to a quadratic form q. We have $\mathrm{Iso}\,(\mathrm{A}, \sigma) = \mathrm{O}(q)$, the *group of isometries* and $\mathrm{Sim}\,(\mathrm{A}, \sigma)$ is simply the group $\mathrm{GO}(q)$ defined as follows :

$$\mathrm{GO}(q)(k) = \{f_\lambda \in \mathrm{End}(V) \mid q\left(f_\lambda(v)\right) = \lambda q(v)\ \forall\ v \in V\}.$$

If $a \in \mathrm{Sim}\,(\mathrm{A}, \sigma)(k)$ is a similitude, then $\sigma(a)a = \lambda$ for some $\lambda \in k^*$. Taking reduced norms, we see $\mathrm{Nrd}_k(a)^2 = \lambda^{2n}$ and hence $\mathrm{Nrd}_k(a) = \pm\lambda^n$. Then a is a *proper* similitude if $\mathrm{Nrd}_k(a) = \lambda^n$ and the *group of proper similitudes* coincides with $\mathrm{Sim}_+\,(\mathrm{A}, \sigma)$. Thus, we have also

$$\mathrm{Iso}_+\,(\mathrm{A}, \sigma)(k) = \mathrm{O}^+\,(\mathrm{A}, \sigma)(k) = \{a \in A \mid \sigma(a)a = 1\ \&\ \mathrm{Nrd}_k(a) = 1\}.$$

The classical result due to Weil asserts that classical adjoint groups can always be phrased in the language of algebras with involutions. More precisely,

Theorem 3.1 (Weil)**.** *Any adjoint absolutely simple classical algebraic group* G/k *is isomorphic to* $\mathrm{PSim}_+\,(\mathrm{A}, \sigma)$ *for suitable* (A, σ) *as above.*

3.3 Classification of classical groups

3.3.1 Case I : Simply connected

Let k be a field of characteristic different from 2. An absolutely simple, simply connected, classical k-group G has one of the following forms :

Type ${}^1A_n$: $G = \mathrm{SL}_1(A)$ where A/k is a central simple algebra of degree $n+1$.

Type ${}^2A_n$: $G = \mathrm{SU}\,(\mathrm{A}, \sigma)$ where A/K is a central simple algebra of degree $n+1$ where K/k is a quadratic étale extension and σ is a unitary involution on A with $K^\sigma = k$.

Type B_n : $G = \mathrm{Spin}(q)$ where q/k is a quadratic form of dimension $2n+1 \geq 3$.

Type C_n : $G = \mathrm{Sp}\,(\mathrm{A}, \sigma) := \mathrm{Iso}\,(\mathrm{A}, \sigma)$ where A/k is a central simple algebra of degree $2n \geq 2$ and σ is a symplectic involution.

Type D_n : $G = \mathrm{Spin}\,(\mathrm{A}, \sigma)$ where A/k is a central simple algebra of degree $2n \geq 4$ and σ is an orthogonal involution.

3.3.2 Case II : Adjoint

Let k be a field of characteristic different from 2. An absolutely simple, adjoint, classical k-group G has one of the following forms :

Type ${}^1A_n$: $G = \mathrm{PGL}_1(A)$ where A/k is a central simple algebra of degree $n+1$.

Type ${}^2A_n$: $G = \mathrm{PGU}\,(\mathrm{A}, \sigma) := \mathrm{PSim}\,(\mathrm{A}, \sigma)$ where A/K is a central simple algebra of degree $n+1$ where K/k is a quadratic étale extension and σ is a unitary involution on A with $K^\sigma = k$.

Type B_n : $G = \mathrm{O}^+(q)$ where q/k is a quadratic form of dimension $2n+1 \geq 3$.

Type C_n : $G = \mathrm{PGSp}\,(\mathrm{A}, \sigma) := \mathrm{PSim}\,(\mathrm{A}, \sigma)$ where A/k is a central simple algebra of degree $2n \geq 2$ and σ is a symplectic involution.

Type D_n : $G = \mathrm{PGO}^+\,(\mathrm{A}, \sigma) := \mathrm{PSim}_+\,(\mathrm{A}, \sigma)$ where A/k is a central simple algebra of degree $2n \geq 4$ and σ is an orthogonal involution.

3.4 Type D_n details

Let A be a central simple algebra of degree $2n$ over k with orthogonal involution σ. Let $\mathrm{C}(\mathrm{A}, \sigma)$ denote its Clifford algebra with center Z, the discriminant extension and let $\underline{\sigma}$ denote the canonical involution of $\mathrm{C}(\mathrm{A}, \sigma)$.

In this section, we would like to introduce the definitions of the Spin group, the Clifford group and the extended Clifford group which will play a very important role in Chapter 10. They will involve the Clifford algebras $\mathrm{C}(\mathrm{A}, \sigma)$, the group of proper similitudes $\mathrm{GO}^+(\mathrm{A}, \sigma)$ and the projective group of proper similitudes $\mathrm{PGO}^+(\mathrm{A}, \sigma)$, apart from a structure called the Clifford bimodule.

Since more than the definitions of these groups, the exact sequences into which they fit play a crucial role in our work, we do not give many details and only list some properties to give the reader a feel for these objects. For a thorough treatment, we refer her to ([KMRT], Chapter II, §9 and Chapter III).

3.4.1 The Clifford bimodule

We want to define a structure $\mathrm{B}(\mathrm{A}, \sigma)$ called the *Clifford bimodule* which should be a left A module and a bi- $\mathrm{C}(\mathrm{A}, \sigma)$ module.

Let us only define it for the case when $A = \mathrm{End}_k(V)$ and $\sigma = \sigma_q$ is the adjoint involution for a quadratic form q. Recall that the full Clifford algebra $\mathrm{C}(q) = \mathrm{C}_0(q) \oplus \mathrm{C}_1(q)$. Set the Clifford bimodule to be

$$\mathrm{B}(\mathrm{A}, \sigma) := V \otimes_k \mathrm{C}_1(q).$$

Then $A = \mathrm{End}_k(V)$ acts on $\mathrm{B}\,(\mathrm{A},\sigma)$ on the left by acting on V and $\mathrm{C}_0(q)$ acts on $\mathrm{B}\,(\mathrm{A},\sigma)$ by acting on both sides of $\mathrm{C}_1(q)$. Notice that the left action of $\mathrm{End}_k(V)$ and the bi-action of $\mathrm{C}_0(q)$ commute.

Identifying $V \otimes V$ with $A = \mathrm{End}_k(V)$ by identifying $v \otimes w$ with the endomorphism $[x \rightsquigarrow b_q(w,x)v]$, we can define an injective A-module map $b : A \hookrightarrow \mathrm{B}\,(\mathrm{A},\sigma)$ by identifying the second copy of V as the one sitting inside $\mathrm{C}_1(q)$. More precisely,

$$\begin{gathered} b : V \otimes V \hookrightarrow V \otimes \mathrm{C}_1(q) \\ v \otimes w \rightsquigarrow v \otimes w. \end{gathered}$$

Let $b(a) = a^b$ for $a \in A$ and let A^b denote the image of A in $\mathrm{B}\,(\mathrm{A},\sigma)$ under the map b. Note that $\dim_k \mathrm{B}\,(\mathrm{A},\sigma) = 2n(2^{2n-1}) = \deg A(2^{\deg A - 1})$.

The Clifford bimodule can be defined for a general (A,σ) ([KMRT], Chapter II, §9B) retaining the above properties such that the definition in the split case agrees with the one given above. We denote the left action of $\mathrm{C}\,(\mathrm{A},\sigma)$ on $\mathrm{B}\,(\mathrm{A},\sigma)$ by $\star$ and the right action by an invisible dot!

3.4.2 The Clifford group

We are now ready to define an interesting group $\Gamma\,(\mathrm{A},\sigma) \subseteq \mathrm{C}\,(\mathrm{A},\sigma)$ called the *Clifford group*. Set

$$\Gamma\,(\mathrm{A},\sigma) := \{c \in \mathrm{C}\,(\mathrm{A},\sigma)^* \mid c^{-1} \star A^b c \subseteq A^b\}.$$

Lemma 3.2.

$$\Gamma\left(\mathrm{A},\sigma\right) := \{c \in \mathrm{C}\left(\mathrm{A},\sigma\right)^{*} \ \mid c^{-1} \star 1^{b} c \subseteq A^{b}\}.$$

Proof. Clearly by definition $c \in \Gamma\left(\mathrm{A},\sigma\right)$ implies $c^{-1} \star 1^{b} c \subseteq A^{b}$ since $1 \in A$.

Conversely, let $c^{-1} \star 1^{b} c = x \in A^{b}$ and let $a \in A$. Since b is an A module map, we have $a1^{b} = a^{b}$. Then since the left action of A on $\mathrm{B}\left(\mathrm{A},\sigma\right)$ commutes with the bi-$\mathrm{C}\left(\mathrm{A},\sigma\right)$ action, we have

$$c^{-1} \star a^{b} c = c^{-1}\left(a1^{b}\right) c = a\left[c^{-1} \star 1^{b} c\right] = ax \in A^{b}.$$

□

When $A = \mathrm{End}_{k}(V)$ and $\sigma = \sigma_{q}$, the group $\Gamma\left(\mathrm{A},\sigma\right)$ is called the *special Clifford group* $\Gamma^{+}(q)$. It has an easier description

$$\Gamma^{+}(q) := \{c \in \mathrm{C}_{0}(q)^{*} \mid c^{-1} V c \subseteq V\}.$$

This is because

$$\begin{aligned} c \in \Gamma\left(\mathrm{A},\sigma\right) &\iff c^{-1} \star \left(V \otimes V\right) c \subseteq V \otimes V \\ &\iff c^{-1} \star \left(v \otimes w\right) c \subseteq V \otimes V \ \forall\ v, w \in V \\ &\iff v \otimes \left(c^{-1} w c\right) \subseteq V \otimes V \ \forall\ v, w \in V \\ &\iff c^{-1} w c \in V \ \forall\ w \in V \\ &\iff c \in \Gamma^{+}(q). \end{aligned}$$

3.4.3 The vector representation

Since we have done all the hard work of defining $\Gamma(\mathrm{A}, \sigma)$ and $\mathrm{B}(\mathrm{A}, \sigma)$, the vector representation is easy to define. It is simply the morphism

$$\begin{aligned} \chi : \Gamma(\mathrm{A}, \sigma) &\to A^b \simeq A \\ c &\rightsquigarrow c^{-1} \star 1^b c \end{aligned}$$

Note that χ makes sense because of Lemma 3.2. When $A = \mathrm{End}_k(V)$ and $\sigma = \sigma_q$, then by ([KMRT], Prop 13.12, Pg 179), χ is the representation

$$\begin{aligned} \chi : \Gamma^+(q) &\to \mathrm{End}_k(V) \\ c &\rightsquigarrow \left[x \mapsto cvc^{-1}\right] \end{aligned}$$

It is an easy check that $\chi(c) \in \mathrm{O}(q)$. This is because for each $v \in V$,

$$q(cvc^{-1}) = (cvc^{-1})^2 = cv^2c^{-1} = q(v).$$

But in fact more is true, namely $\chi(c)$ is actually in $\mathrm{O}^+(q)$. Also we observe that $\Gamma^+(q) \subset \mathrm{Sim}\left(\mathrm{C}_0(q), \underline{\sigma}\right)$. This is because if $c \in \Gamma^+(q)$, then $cvc^{-1} = w \in V$. Let by abuse of notation, $\underline{\sigma}$ also denote the canonical involution on $\mathrm{C}(q)$. Thus for each v in V

$$w = cvc^{-1} = \underline{\sigma}(w) = \underline{\sigma}\left(cvc^{-1}\right) = \underline{\sigma}(c)^{-1} v \, \underline{\sigma}(c).$$

Thus $\underline{\sigma}(c)cv = v\,\underline{\sigma}(c)c$ for each $v \in V$. Thus $\underline{\sigma}(c)c \in \mathrm{Z}\left(\mathrm{C}(q)\right) = k$ and hence $c \in \mathrm{Sim}\left(\mathrm{C}_0(q), \underline{\sigma}\right)$.

Recall that the map Int induces an isomorphism $\mathrm{PGO}(\mathrm{A}, \sigma) \simeq \mathrm{Aut}_k(\mathrm{A}, \sigma)$. Every automorphism $\theta \in \mathrm{Aut}_k(\mathrm{A}, \sigma)$ induces an automorphism, which we will call $C(\theta) \in \mathrm{Aut}_k(\mathrm{C}(\mathrm{A}, \sigma), \underline{\sigma})$. Thus by composition, we get the following map (which we will continue calling C)

$$C : \mathrm{PGO}(\mathrm{A}, \sigma) \to \mathrm{Aut}_k(\mathrm{C}(\mathrm{A}, \sigma), \underline{\sigma}).$$

Note that $C(g)$ needn't be identity on Z for $g \in \mathrm{PGO}(\mathrm{A}, \sigma)$. However C restricted to $\mathrm{PGO}^+(\mathrm{A}, \sigma)$ does land in $\mathrm{Aut}_Z(\mathrm{C}(\mathrm{A}, \sigma), \underline{\sigma})$. Thus we get a morphism $C : \mathrm{PGO}^+(\mathrm{A}, \sigma) \to \mathrm{Aut}_Z(\mathrm{C}(\mathrm{A}, \sigma), \underline{\sigma})$ ([KMRT], Prop 13.2 & 13.4) and hence one from $\mathrm{O}^+(\mathrm{A}, \sigma)$ to $\mathrm{Aut}_Z(\mathrm{C}(\mathrm{A}, \sigma), \underline{\sigma})$.

All this with a little bit more work for the non-split case leads to the following proposition

Proposition 3.3 ([KMRT], Prop 13.15, Pg 179)**.** *The Clifford group* $\Gamma(\mathrm{A}, \sigma)$ *is contained in* $\mathrm{Sim}(\mathrm{C}(\mathrm{A}, \sigma), \underline{\sigma})$. *The map* χ *fits into the following commutative diagram with exact rows :*

$$\begin{tikzcd}
1 \arrow[r] & k^* \arrow[r] \arrow[d] & \Gamma(\mathrm{A}, \sigma) \arrow[r, "\chi"] \arrow[d] & \mathrm{O}^+(\mathrm{A}, \sigma) \arrow[r] \arrow[d, "C"] & 1 \\
1 \arrow[r] & Z^* \arrow[r] & \mathrm{Sim}(\mathrm{C}(\mathrm{A}, \sigma), \underline{\sigma}) \arrow[r, "\mathrm{Int}"] & \mathrm{Aut}_Z(\mathrm{C}(\mathrm{A}, \sigma), \underline{\sigma}) \arrow[r] & 1
\end{tikzcd}$$

3.4.4 The Spin group

Recall that in showing that $\Gamma(\mathrm{A},\sigma) \subseteq \mathrm{Sim}(\mathrm{C}(\mathrm{A},\sigma),\underline{\sigma})$, we showed (at least in the split case) that $\underline{\sigma}(c)c \in k^*$ for $c \in \Gamma(\mathrm{A},\sigma)$. Thus, one can define the Spinor norm map

$$\begin{aligned} \mathrm{Sn} : \Gamma(\mathrm{A},\sigma) &\to \mathbb{G}_m \\ c &\rightsquigarrow \underline{\sigma}(c)c \end{aligned}$$

The spin group $\mathrm{Spin}(\mathrm{A},\sigma)$ is defined to be the kernel of the Spinor norm map, namely

$$1 \to \mathrm{Spin}(\mathrm{A},\sigma) \to \Gamma(\mathrm{A},\sigma) \xrightarrow{\mathrm{Sn}} \mathbb{G}_m \to 1.$$

3.4.5 The extended Clifford group

Just for this subsection, we assume $\deg A = 2n \geq 4$. Recall the morphism $C : \mathrm{PGO}^+(\mathrm{A},\sigma) \to \mathrm{Aut}_Z(\mathrm{C}(\mathrm{A},\sigma),\underline{\sigma})$ ([KMRT], Prop 13.2 & 13.4). This is in fact injective as we have assumed $\deg A = 2n \geq 4$.

The group of similitudes of the Clifford algebra, $\mathrm{Sim}(\mathrm{C}(\mathrm{A},\sigma),\underline{\sigma})$, covers $\mathrm{Aut}_Z(\mathrm{C}(\mathrm{A},\sigma),\underline{\sigma})$ and the Clifford group, $\Gamma(\mathrm{A},\sigma)$ covers $\mathrm{O}^+(\mathrm{A},\sigma)$ by the vector representation. We would like to define an intermediate group called the *extended Clifford group* $\Omega(\mathrm{A},\sigma)$ which covers $\mathrm{PGO}^+(\mathrm{A},\sigma)$.

We now define $\Omega\,(\mathrm{A},\sigma)$ to be the inverse image of the image of $\mathrm{PGO}^+\,(\mathrm{A},\sigma)$ in $\mathrm{Sim}\,(\mathrm{C}\,(\mathrm{A},\sigma),\underline{\sigma})$. More precisely,

$$\Omega\,(\mathrm{A},\sigma) := \{c \in \mathrm{Sim}\,(\mathrm{C}\,(\mathrm{A},\sigma),\underline{\sigma})\ \mid \mathrm{Int}(c) \in C\left(\mathrm{PGO}^+\,(\mathrm{A},\sigma)\right)\}.$$

$$\begin{tikzcd}
1 \arrow[r] & k^* \arrow[r] \arrow[d, hook] & \Gamma\,(\mathrm{A},\sigma) \arrow[r, "\chi"] \arrow[d, hook] & \mathrm{O}^+\,(\mathrm{A},\sigma) \arrow[r] \arrow[d, "\pi"] & 1 \\
1 \arrow[r] & Z^* \arrow[r] \arrow[d, equal] & \Omega\,(\mathrm{A},\sigma) \arrow[r, "\chi'"] \arrow[d, hook] & \mathrm{PGO}^+\,(\mathrm{A},\sigma) \arrow[r] \arrow[d, hook, "C"] & 1 \\
1 \arrow[r] & Z^* \arrow[r] & \mathrm{Sim}\,(\mathrm{C}\,(\mathrm{A},\sigma),\underline{\sigma}) \arrow[r, "\mathrm{Int}"] & \mathrm{Aut}_Z\,(\mathrm{C}\,(\mathrm{A},\sigma),\underline{\sigma}) \arrow[r] & 1
\end{tikzcd}$$

Figure 3.1: The extended Clifford group

Chapter 4

A crash course on group cohomology

'Now, what I want is, Facts.'

- Charles Dickens, Hard Times

In this chapter, we introduce the language of finite group cohomology via a quick succesion of definitions, facts and more facts mostly without proof. For an extremely pleasant and elementary introduction to the subject via the *non-homogeneous cochains* route which walks through the works of Hilbert, Noether, Schreier, Baer et al in group theory, we refer to the excellent article by R. Sridharan ([Sridharan05]) which convinces the reader that cohomology theory is roughly the theory of obstructions. We redirect the reader interested in getting to the relevant algebraic nitty-gritties in as short a time as possible to Atiyah and Wall's exposition on the topic in ([CF67], Chapter IV). For the more topologically minded reader with time on her hands, we recommend ([Brown]) which covers a lot more theory and provides many more examples.

4.1 The Ext functor

Let G be a finite group and let $\mathbb{Z}\mathrm{G}$ denote the group ring on G. Thus,

$$\mathbb{Z}\mathrm{G} = \oplus_{g \in G} \mathbb{Z}\, g,$$

where the algebra mutliplication extends the group operation $\mathbb{Z}$ bilinearly. Let A be an abelian group which is also a $\mathbb{Z}\mathrm{G}$ module, which we term a G module. The integers, $\mathbb{Z}$, will always be a trivial G module unless otherwise specified. Thus $g.n = n$ for $g \in G$ and $n \in \mathbb{Z}$. We define the covariant left exact functor

$$\begin{aligned} (-)^G : (\text{G - Modules}) &\to (\text{Abelian groups}) \\ A &\rightsquigarrow \mathrm{Hom}_{\mathbb{Z}\mathrm{G}}(\mathbb{Z}, A) \end{aligned}$$

Let us examine what the abelian group $\mathrm{Hom}_{\mathbb{Z}\mathrm{G}}(\mathbb{Z}, A)$ is. If f is an element in this group, it is a homomorphism compatible with the action of G. Thus $f(g.1) = g.f(1)$ for $g \in G$. Since $\mathbb{Z}$ is a trivial G-module, $g.1 = 1$ and hence $g.f(1) = f(1)\ \forall\ g \in G$. Thus $f(1) \in A^G$, the subgroup of elements pointwise fixed by G. Since deciding where f takes 1 decides it completely, we can and do identify $\mathrm{Hom}_{\mathbb{Z}\mathrm{G}}(\mathbb{Z}, A)$ with A^G which justifies the name of the functor!

Left exactness simply means that if $0 \to A \to B \to C$ is an exact sequence of G-modules, then $0 \to A^G \to B^G \to C^G$ is an exact sequence of abelian groups. Then the cohomology groups $\mathrm{H}^q(G, A)$ are defined to be the right derived functors[1] of $(-)^G$ which correspond to the Ext groups $\mathrm{Ext}^q_{\mathbb{Z}\mathrm{G}}(\mathbb{Z}, A)$.

[1] Of course for derived functors to make sense, we need our category of $\mathbb{Z}\mathrm{G}$ modules to have *enough injectives* (Stacks Project : Tag 01D8)

4.1.1 Recipes for computing cohomology

To explain briefly what exactly a right derived functor is and how one can go about computing it, we need the notion of injective and projective modules which we introduce in the following propostions.

Proposition 4.1 ([Brown], Prop 8.1, 8.2)**.** *Let R be a unital ring and let P be a (left) R-module. We say P is projective if it satisfies the following equivalent conditions*

1. *If $M' \xrightarrow{i} M \xrightarrow{j} M''$ is an exact sequence of R-modules and there is a morphism $\phi : P \to M$ such that $j \circ \phi = 0$, then there exists a morphism $\psi : P \to M'$ such that $\psi \circ i = \phi$.*

$$\begin{tikzcd} & P \arrow[dl, dashed, "\psi"'] \arrow[d, "\phi"] \arrow[dr, "0"] & \\ M' \arrow[r, "i"] & M \arrow[r, "j"] & M'' \end{tikzcd}$$

2. *The functor* $\mathrm{Hom}_R(P, -)$ *is exact.*

3. *If $M \xrightarrow{\pi} \overline{M} \to 0$ is an exact sequence of R-modules and there is a morphism $\phi : P \to \overline{M}$, then there exists a lift morphism $\psi : P \to M$ such that $\pi \circ \psi = \phi$.*

$$\begin{tikzcd} & P \arrow[dl, dashed, "\psi"'] \arrow[d, "\phi"] & \\ M \arrow[r, "\pi"] & \overline{M} \arrow[r] & 0 \end{tikzcd}$$

4. *Every short exact sequence of R-modules $0 \to M' \to M \to P \to 0$ splits.*

5. *P is a direct summand of a free R-module.*

Proposition 4.2. *Let R be a unital ring and let Q be a (left) R-module. We say Q is injective if it satisfies the following equivalent conditions*

1. *The functor* $\mathrm{Hom}_R(-, Q)$ *is exact.*

2. *If* $0 \to M' \xrightarrow{i} M$ *is an exact sequence of R-modules and there is a morphism* $\phi : M' \to Q$*, then there exists a extension morphism* $\psi : M \to Q$ *such that* $\psi \circ i = \phi$.

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "i"] \arrow[d, "\phi"] & M \arrow[dl, dashed, "\psi"] \\ & Q & \end{tikzcd}$$

3. *Every short exact sequence of R-modules* $0 \to Q \to M \to M'' \to 0$ *splits.*

Now we are ready to define right derived functors and hence the cohomology or the Ext groups. Let $R = \mathbb{Z}\mathrm{G}$, let A be an R-module and let F be our left exact functor $(-)^G$. Pick an injective resolution[2] of A in the category of R-modules.

$$0 \to A \to Q_0 \xrightarrow{d_1} Q_1 \xrightarrow{d_2} Q_2 \to \dots$$

Applying F to the above sequence and deleting the term $F(A)$, we get a complex which need no longer be exact.

$$0 \to F(Q_0) \xrightarrow{F(d_1)} F(Q_1) \xrightarrow{F(d_2)} F(Q_3) \dots$$

[2]There always exists one in this category and the cohomology groups don't depend on the choice of the injective resolution.

However, since it is still a complex, the images are contained in their neighbouring kernels and one can compute the homology groups which we call right derived functors of F. More precisely,

$$\mathrm{R}F^q(A) := \frac{\text{Kernel } F\left(d_{q+1}\right)}{\text{Image } F\left(d_q\right)}.$$

For this particular functor $F = (-)^G$, the right derived functors define the cohomology groups.

$$\mathrm{Ext}^q_{\mathbb{Z}\mathrm{G}}\left(\mathbb{Z}, A\right) = \mathrm{H}^q\left(G, A\right) := \mathrm{R}F^q(A).$$

Another recipe for computing $\mathrm{H}^q(G, A)$

Step I : Pick a projective resolution[3] of $\mathbb{Z}$ as a $\mathbb{Z}$G module.

$$\ldots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to \mathbb{Z} \to 0.$$

Step II : Apply the contravariant functor $F'(-) = \mathrm{Hom}_{\mathbb{Z}\mathrm{G}}(-, A)$ and delete the term $F'(\mathbb{Z})$ to get the following complex

$$0 \to F'\left(P_0\right) \xrightarrow{F'(d_1)} F'\left(P_1\right) \xrightarrow{F'(d_2)} F'\left(P_2\right) \to \ldots$$

Step III : Take homology to get

$$\mathrm{H}^q\left(G, A\right) = \frac{\text{Kernel } F'\left(d_{q+1}\right)}{\text{Image } F'\left(d_q\right)}.$$

[3]This process doesn't depend on the choice of the projective resolution

4.1.2 Connecting maps

An important part of cohomology theory is the existence of functorial *connecting* maps which we summarize in the following proposition.

Proposition 4.3 ([CF67], Chapter IV, Thm 1)**.** *Let G be a finite group and let A, B be G-modules.*

1. *If $f : A \to B$ is a map of G-modules, then we get a canonical map $\mathrm{H}^q(G, A) \to \mathrm{H}^q(G, B)$ for each $q \geq 0$. The map at the zero-th level is simply the restriction of f to A^G, namely $f|_{A^G} : A^G \to B^G$.*

2. *For a short exact sequence of $0 \to A \to B \to C \to 0$ of G-modules, there exist functorial connecting maps $\delta_q : \mathrm{H}^q(G, C) \to \mathrm{H}^{q+1}(G, A)$ such that the following (very) long sequence is exact*

$$\ldots \to \mathrm{H}^q(G, A) \to \mathrm{H}^q(G, B) \to \mathrm{H}^q(G, C) \xrightarrow{\delta_q} \mathrm{H}^{q+1}(G, A) \to \ldots$$

4.2 A nice $\mathbb{Z}\mathrm{G}$ projective resolution of $\mathbb{Z}$

In this section we define the *standard resolution* of $\mathbb{Z}$ as a $\mathbb{Z}\mathrm{G}$ module which is extremely helpful in defining cochains and actually computing cohomologies. Let $G^i := \underbrace{G \times G \times \ldots \times G}_{i}$, the direct product of i-copies of G and let $\mathbb{Z}\mathrm{G}^i$ denote the free abelian group on G^i. This is a $\mathbb{Z}\mathrm{G}$ module as follows :

$$g\left(g_0, g_1, \ldots, g_{i-1}\right) = \left(gg_0, gg_1, \ldots, gg_{i-1}\right).$$

In fact, it is a free $\mathbb{Z}\mathrm{G}$ module. We have just found the terms of our nice projective resolution of $\mathbb{Z}$. Just set $P_{i-1} = \mathbb{Z}\mathrm{G}^i$. Now we only need to find maps between them.

The easiest map to define is probably the *augmentation* morphism $\epsilon : P_0 = \mathbb{Z}\mathrm{G} \to \mathbb{Z}$ which sends $g \rightsquigarrow 1$ for each $g \in G$. Define $d_i : P_i \to P_{i-1}$ for $i \geq 1$ to be the familiar map from algebraic topology as follows :

$$P_i = \mathbb{Z}\mathrm{G}^{i+1} \xrightarrow{\qquad d_i \qquad} P_{i-1} = \mathbb{Z}\mathrm{G}^i$$

$$(g_0, g_1, \ldots, g_i) \longrightarrow \textstyle\sum_{j=0}^{i} (-1)^j \, (g_0, g_1, \ldots, \hat{g}_j, \ldots, g_i)$$

It is an exercise in unravelling definitions (which everyone claims everyone else must do once in life!) that the following is a complex

$$\mathcal{P} := \ldots\ldots\ldots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0. \quad (***)$$

Proposition 4.4. *The complex $\mathcal{P}$ defined above (***) is in fact a resolution.*

Proof. We use a nice trick from homology ([Brown], Prop 0.1), namely that of constructing a *homotopy* between the identity map $\mathrm{id}\,|_{\mathcal{P}}$ on the complex $\mathcal{P}$ and the zero map $0|_{\mathcal{P}}$. This in turn forces that the homology groups of $\mathcal{P}$ are trivial and therefore, that $\mathcal{P}$ is in fact a resolution.

More explicitly, we would like to construct maps $h_i : P_i \to P_{i+1}$ such that $d_{i+1} \circ h_i + h_{i-1} \circ d_i = \mathrm{id}\,|_{P_i}$.

$$\begin{tikzcd}
\cdots \arrow[r] & P_{i+1} \arrow[r, "d_{i+1}"] \arrow[dl] & P_i \arrow[r, "d_i"] \arrow[dl, "h_i"] & P_{i-1} \arrow[r] \arrow[dl, "h_{i-1}"] & \cdots \\
\cdots \arrow[r] & P_{i+1} \arrow[r, "d_{i+1}"] & P_i \arrow[r, "d_i"] & P_{i-1} \arrow[r] & \cdots
\end{tikzcd}$$

Pretend that we have done so. Then let $x \in \text{Kernel } d_i \subseteq P_i$, i.e. $d_i(x) = 0$. Then $x = \text{id}(x) = (d_{i+1} \circ h_i + h_{i-1} \circ d_i)(x) = d_{i+1}(h_i(x))$, which shows that $x \in \text{Image } d_{i+1}$.

Fix an element $g \in G$. We leave you to check that the maps $h_i : P_i \to P_{i+1}$ defined below do indeed work.

$$h_i(g_0, g_1, \ldots, g_i) = (g, g_0, g_1, \ldots, g_i)$$

$\square$

4.2.1 Rewriting the complex $F'(P_i)$

The i^{th} term P_i of the standard resolution $\mathcal{P}$ of $\mathbb{Z}$ is $\mathbb{Z}\mathrm{G}^{i+1}$. Applying the functor $F'(-) = \mathrm{Hom}_{\mathbb{Z}\mathrm{G}}(-, A)$, we get

$$F'(P_i) = \mathrm{Hom}_{\mathbb{Z}\mathrm{G}}\left(\mathbb{Z}\mathrm{G}^{i+1}, A\right).$$

We can replace $F'(P_i)$ by $\text{Maps}(G^i, A)$ which we will call P_i^* by the following identification

$$\begin{gathered}\mathrm{Hom}_{\mathbb{Z}\mathrm{G}}\left(\mathbb{Z}\mathrm{G}^{i+1}, A\right) \cong \text{Maps}\left(G^i, A\right) \\ f : \mathbb{Z}\mathrm{G}^{i+1} \to A \rightsquigarrow \tilde{f} : G^i \to A\end{gathered}$$

where $\tilde{f}(g_1, \ldots, g_i) := f(1, g_1, g_1 g_2, \ldots, g_1 g_2 \ldots g_i)$.

Thus the new maps in the complex are

$$P_i^* = \text{Maps}\left(G^i, A\right) \xrightarrow{d_i'} P_{i+1}^* = \text{Maps}\left(G^{i+1}, A\right)$$

where $d_i'(\tilde{f}) : G^{i+1} \to A$ sends

$$
\begin{aligned}
(g_1, g_2, \ldots, g_{i+1}) \rightsquigarrow\ & g_1 \tilde{f}(g_2, \ldots, g_{i+1}) \\
& + \sum_{j=1}^{i} (-1)^j \tilde{f}\,(g_1, g_2, \ldots, g_{j-1}, g_j g_{j+1}, g_{j+2}, \ldots, g_{i+1}) \\
& + (-1)^{i+1} \tilde{f}\,(g_1, g_2, \ldots, g_i)\,.
\end{aligned}
$$

4.3 Cocycles and coboundaries in low dimensions

In this section, we give explicit formulae for low dimension cocycles and coboundaries (kernels and images of the d_i') for ease of reference later on. But first, let us write down the first few terms of the complex P_i^*.

$$
0 \longrightarrow P_0^* \xrightarrow{\quad d_0' \quad} P_1^* \xrightarrow{\quad d_1' \quad} P_2^* \xrightarrow{\quad d_2' \quad} P_3^* \ldots
$$

$$
0 \longrightarrow \mathrm{Maps}(G^0, A) \xrightarrow{d_0'} \mathrm{Maps}(G^1, A) \xrightarrow{d_1'} \mathrm{Maps}(G^2, A) \xrightarrow{d_2'} \mathrm{Maps}(G^3, A) \ldots
$$

Level zero

$P_0^* = \mathrm{Maps}(G^0, A)$ is simply the set A. And for $a \in A$, $d_0'(a) : G \to A$ is the map sending $g \rightsquigarrow ga - a$. The elements of the kernel of d_0' called *0-cocycles* are thus simply elements $a \in A^G$. And finally

$$
\mathrm{H}^0(G, A) = \frac{\{0 - \text{cocyles}\}}{0} = A^G.
$$

Level one

$P_1^* = \text{Maps}(G, A)$ and for $f : G \to A \in P_1^*$, we have

$$d_1'(f)(g,h) = gf(h) - f(gh) + f(g).$$

The elements of the kernel of d_1' called *1-cocycles* are therefore functions $f : G \to A$ such that $f(gh) = gf(h) + f(g)$. They are also sometimes referred to as *twisted* or *crossed* homomorphisms.

The elements of the image of d_0' called *1-coboundaries* are simply functions $f' : G \to A$ such that there exists $a \in A$ and $f'(g) = ga - a$ for each $g \in G$. Clearly 1-coboundaries are also 1-cocycles. And finally

$$\mathrm{H}^1(G, A) = \frac{\{1 - \text{cocyles}\}}{\{1 - \text{coboundaries}\}}.$$

Level two

$P_2^* = \text{Maps}(G \times G, A)$ and for $f : G \times G \to A \in P_1^*$, we have

$$d_1'(f)(x,y,z) = xf(y,z) - f(xy,z) + f(x,yz) - f(x,y).$$

The elements of the kernel of d_2' called *2-cocycles* are therefore functions $f : G \times G \to A$ such that $xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0 \; \forall \; x, y, z \in G$.

The elements of the image of d_1' called *2-coboundaries* are simply functions $f' : G \times G \to A$ such that there exists a function $\tilde{f} : G \to H$ such that $f'(g,h) = g\tilde{f}(h) - f(gh) + f(g)$. One can check that 2-coboundaries are also 2-cocycles directly. And finally

$$\mathrm{H}^2(G, A) = \frac{\{2 - \text{cocyles}\}}{\{2 - \text{coboundaries}\}}.$$

There is a beautiful correspondence between group extensions of G by A and the second cohomology group $\mathrm{H}^2(G, A)$ and we refer to ([Sridharan05]) for more details.

4.4 Special morphisms between cohomology groups

4.4.1 Restrictions and inflations

Let $f : H \to G$ be a group homomorphism and let A be a G-module. We can also consider A as an H-module by setting $h.a = f(h)a$ for $h \in H$ and $a \in A$. The morphism f clearly induces a homomorphism between the standard $\mathbb{Z}\mathrm{H}$ resolution of $\mathbb{Z}$ and the standard $\mathbb{Z}\mathrm{G}$ resolution of $\mathbb{Z}$. Thus we get a map of complexes $\mathrm{Hom}_{\mathbb{Z}\mathrm{G}}\left(\mathbb{Z}\mathrm{G}^i, A\right) \to \mathrm{Hom}_{\mathbb{Z}\mathrm{H}}\left(\mathbb{Z}\mathrm{H}^i, A\right)$ and hence between $P_H^* \to P_G^*$ as defined in Section 4.2.1. Thus f induces a morphism between the cohomology groups

$$f^* : \mathrm{H}^q(G, A) \to \mathrm{H}^q(H, A).$$

If $f : H \to G$ is the inclusion map of a subgroup H into G, then we call f^* to be the *restriction* morphism. This terminology is apt because at the cocycle level, f^* simply takes a function $j : G^i \to A$ in ${P_G}_i^*$ to its restriction $j|_{H^i} : H^i \to A$ in ${P_H}_i^*$.

$$\mathrm{Res} : \mathrm{H}^q\left(G, A\right) \to \mathrm{H}^q\left(H, A\right).$$

Let H be a normal subgroup of G and $f : G \to G/H$, the canonical quotient map. Let A be a G module. Now A needn't of course be a G/H module. However consider $A^H \subseteq A$. Firstly, it is a G-module (and hence also a G/H-module). This is because for $g \in G$ and $h \in H$, we have $hg = gh'$ for some $h' \in H$ and hence $h(ga) = g(h'a) = ga \ \forall\ a \in A^H$.

Thus we get $f^* : \mathrm{H}^q\left(G/H, A^H\right) \to \mathrm{H}^q\left(G, A^H\right)$. Using the G-module homomorphism $A^H \to A$ and part (1) of Prop 4.3, we get our *inflation* morphisms

$$\mathrm{Inf} : \mathrm{H}^q\left(G/H, A^H\right) \to \mathrm{H}^q\left(G, A\right).$$

There is a really nice proposition connecting the inflation and restriction morphisms which we state below in case it is of use later on.

Proposition 4.5 ([CF67], Chapter IV, Prop 4 & 5)**.** *Let H be a normal subgroup of G and let A be a G-module. Then*

1. *The sequence*

$$0 \to \mathrm{H}^1\left(G/H, A^H\right) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1\left(G, A\right) \xrightarrow{\mathrm{Res}} \mathrm{H}^1\left(H, A\right)$$

   is exact.

2. *Let $q > 1$ and suppose that $\mathrm{H}^i\left(H, A\right) = 0$ for $1 \le i \le q-1$. Then*

$$0 \to \mathrm{H}^q\left(G/H, A^H\right) \xrightarrow{\mathrm{Inf}} \mathrm{H}^q\left(G, A\right) \xrightarrow{\mathrm{Res}} \mathrm{H}^q\left(H, A\right)$$

   is exact and $\mathrm{H}^i\left(G/H, A^H\right) \simeq \mathrm{H}^i\left(G, A\right)$ for $1 \le i \le q-1$.

4.4.2 Coinduction and corestriction

Let H be a subgroup of G and let A be an H-module. We would like to construct a G-module out of A. If we were working with homology, the obvious candidate $\mathbb{Z}\mathrm{G} \otimes_{\mathbb{Z}\mathrm{H}} A$ called the *induced module* would be right. However, since we are dealing with *co*-homology, we need the *coinduced* module

$$M_G^H(A) := \mathrm{Hom}_{\mathbb{Z}\mathrm{H}}(\mathbb{Z}\mathrm{G}, A).$$

This has a G-module structure via the following G-action : For $g \in G$ and $f \in M_G^H(A)$,

$$gf : \mathbb{Z}\mathrm{G} \to A, \quad g' \rightsquigarrow f(g'g) \; \forall g' \in G.$$

The incredibly useful Shapiro's Lemma ([CF67], Chapter IV, Prop 2) relates the cohomology of A and its coinduced module $M_G^H(A)$.

Lemma 4.6 (Shapiro)**.**

$$\mathrm{H}^q\left(G, M_G^H(A)\right) \simeq \mathrm{H}^q(H, A) \;\; \forall \; q \geq 0.$$

We are now ready to define the *corestriction* morphism. Let H be a subgroup of finite index[4] of G and let A be a G-module. We want to define the corestriction to be a map Cores : $\mathrm{H}^q(H, A) \to \mathrm{H}^q(G, A)$.

We will use Shapiro's Lemma and define it via $\mathrm{H}^q\left(G, M_G^H(A)\right)$ as follows :

$$\begin{tikzcd}
\mathrm{H}^q(H,A) \arrow[rr, "\text{Cores}"] \arrow[dr, "\text{Shapiro}"'] & & \mathrm{H}^q(G,A) \\
& \mathrm{H}^q\left(G, M_G^H(A)\right) \arrow[ur, dashed] &
\end{tikzcd}$$

[4]Of course if G is finite, this is always true, but we emphasize this condition to remember to be careful while applying it to infinite groups later

The only thing left to do is to define the map $\mathrm{H}^q\left(G, M_G^H(A)\right) \to \mathrm{H}^q(G,A)$. We do this by defining a G-module morphism $X : M_G^H(A) \to A$ and using Part (1) of Proposition 4.3. Recall that $M_G^H(A) := \mathrm{Hom}_{\mathbb{Z}\mathrm{H}}(\mathbb{Z}\mathrm{G}, A)$ and define the G-module map X by sending

$$
\begin{aligned}
X : \mathrm{Hom}_{\mathbb{Z}\mathrm{H}}(\mathbb{Z}\mathrm{G}, A) &\longrightarrow A \\
f &\dashrightarrow \textstyle\sum_{y\in G/H} y f(y^{-1})
\end{aligned}
$$

This definition also tells us why we need to restrict ourselves to subgroups H of finite index.

An example

Let us see what Cores is explicitly at the zero-th level. $\mathrm{H}^0(H,A) = A^H$.

Let us first calculate what $\mathrm{H}^0(G, M_G^H(A)) = M_G^H(A)^G$ is. If $f \in M_G^H(A)^G$, then $gf = f$ for all $g \in G$. Thus $gf(g') = f(g')$ for each $g' \in G$. This implies that $f(g'g) = f(g')$ for all $g, g' \in G$ and hence $f(g) = a \ \forall\ g \in G$. Since f should also be a $\mathbb{Z}\mathrm{H}$ morphism, we see that $a \in A^H$.

Thus Shapiro's isomorphism simply sends $a \in A^H$ to the constant function $f(g) = a \ \forall\ g \in G$ in $\left(M_G^H(A)\right)^G$. The map X sends f to $\sum_{g\in G/H} ga$. Thus

$$
\begin{aligned}
\mathrm{Cores} : \mathrm{H}^0(H,A) &\to \mathrm{H}^0(G,A) \\
a &\rightsquigarrow \sum_{g\in G/H} ga
\end{aligned}
$$

Let L/k be a finite Galois extension and let $G = \mathrm{Gal}(L/k)$. Let E/k be a sub Galois-extension of L/k and $H = \mathrm{Gal}(L/E)$. Thus $G/H \simeq \mathrm{Gal}(E/k)$.

Let $A = L$ and G acts on L via the Galois automorphisms. Thus $A^H = E$ and

$$\begin{aligned} \mathrm{Cores} : \mathrm{H}^0(H, A) &\to \mathrm{H}^0(G, A) \\ e &\rightsquigarrow \prod_{\sigma \in G/H} \sigma(a) = \mathrm{N}_{E/k}(e) \end{aligned}$$

Thus Cores is simply the Norm map in this case! What is the composition $\mathrm{Cores} \circ \mathrm{Res}$ in this case?

$$\begin{tikzcd} \mathrm{H}^0(G,A) \arrow[r, "\mathrm{Res}"] \arrow[d, equal] & \mathrm{H}^0(H,A) \arrow[r, "\mathrm{Cores}"] \arrow[d, equal] & \mathrm{H}^0(G,A) \arrow[d, equal] \\ k \arrow[r] & E \arrow[r] & k \\ \lambda \arrow[r, dashed] & \lambda \arrow[r, dashed] & \lambda^{[G:H]} \end{tikzcd}$$

This is a more general and incredibly powerful phenomenon termed *restriction-corestriction*.

Proposition 4.7 ([CF67], Chapter IV, Prop 8)**.**

$$\mathrm{Cores} \circ \mathrm{Res} = [G : H] \,.$$

4.4.3 Gratuities

The restriction-corestriction phenomenon yields immediately and almost for free several useful corollaries about the cardinality and torsion of the cohomology groups.

Corollary 4.8. *Let G be a group of size n. Then $n\,\mathrm{H}^q\,(G, A) = 0$ for each $q \geq 1$.*

Proof. Let $H = \{e\}$, the subgroup of order 1. Then $\mathrm{H}^q\,(H, B)$ is trivial for each $q \geq 1$ and abelian group B. This is because $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$ is a projective $\mathbb{Z}\mathrm{H}$ resolution of $\mathbb{Z}$. Thus $\mathrm{Res}(x) = 0$ for each $x \in \mathrm{H}^q\,(G, A)$ and hence so is $\mathrm{Cores} \circ \mathrm{Res}(x)$.

Now since $[G : H] = |G| = n$, Prop 4.7 gives us that $nx = \mathrm{Cores} \circ \mathrm{Res}(x) = 0$. □

Corollary 4.9. *If A is a finitely generated $\mathbb{Z}\mathrm{G}$ module, then $\mathrm{H}^q\,(G, A)$ is a finite abelian group for $q \geq 1$.*

Proof. The second recipe for calculating cohomology using the standard projective resolution of $\mathbb{Z}$ immediately implies that each $\mathrm{H}^q\,(G, A)$ is a quotient of a subgroup of $\mathrm{Hom}_{\mathbb{Z}\mathrm{G}}\,(\mathbb{Z}\mathrm{G}^q, A)$ and hence abelian and finitely generated. By the above Corollary 4.8, it has to be n-torsion and hence finite. □

Corollary 4.10. *Let H be a subgroup of G of index n and let A be a G-module. Let m be a positive integer coprime to n and let $X[m]$ denote the m-torsion subgroup of an abelian group X. Then for $q \geq 1$, the following restriction map restricted to the m-torsion of $\mathrm{H}^q\,(G, A)$ is injective*

$$\mathrm{Res} : \mathrm{H}^q(G, A)[m] \hookrightarrow \mathrm{H}^q\,(H, A)\,.$$

Proof. Let $x \in \mathrm{H}^q(G, A)[m]$ and in the kernel of Res. Thus $mx = 0$ and $\mathrm{Res}(x) = 0$. Now by Prop 4.7, $\mathrm{Cores} \circ \mathrm{Res}(x) = nx$. Thus, we see that $nx = 0$ too. Since $\gcd(m, n) = 1$, this implies $x = 0$. □

Corollary 4.11. *Let S be a p-Sylow subgroup of G and let A be a G-module. Then for $q \geq 1$, the following restriction map restricted to the p-primary component of* $\mathrm{H}^q(G, A)$ *is injective*

$$\mathrm{Res} : \mathrm{H}^q(G, A)[p^\infty] \hookrightarrow \mathrm{H}^q(S, A)\,.$$

Proof. Let $|G| = p^b m$ where m is coprime to p. Let $x \in \mathrm{H}^q(G, A)[p^\infty]$ and in the kernel of Res. Thus $\mathrm{Res}(x) = 0$. By Corollary 4.9, $\mathrm{H}^q(G, A)$ is finite and hence $p^d x = 0$ for some finite d . Now by Prop 4.7, $\mathrm{Cores} \circ \mathrm{Res}(x) = nx$. Thus, we see that $mx = 0$ too. Since $\gcd(p^d, n) = 1$, this implies $x = 0$. $\square$

Corollary 4.12. *Let $q \geq 1$. If $x \in \mathrm{H}^q(G, A)$ restricts to 0 in $\mathrm{H}^q(S, A)$ for all Sylow subgroups S of G, then $x = 0$.*

Proof. By Corollary 4.9, $x = \sum_p x_p \in \mathrm{H}^q(G, A)$ where $x_p \in \mathrm{H}^q(G, A)[p^\infty]$. If possible, let $x_p \neq 0$ for some prime p and let S be a p-Sylow subgroup of G.

Let $\mathrm{Res} : \mathrm{H}^q(G, A) \to \mathrm{H}^q(S, A)$. Thus $0 = \mathrm{Res}(x) = \mathrm{Res}\,(x_p) + \sum_{q \neq p} \mathrm{Res}\,(x_q)$. Note for $q \neq p$, $q^{n_q} x_q = 0$ by definition of x_q and by Corollary 4.8 $p^{m_q}\,\mathrm{Res}(x_q) = 0$. This implies $\mathrm{Res}(x_q) = 0$.

Thus $0 = \mathrm{Res}(x) = \mathrm{Res}\,(x_p)$. By Corollary 4.11, this implies $x_p = 0$, a contradiction. $\square$

4.5 A computation : Hilbert 90

Hilbert's theorem 90 gives a precise description of norm one elements of cyclic extensions.

Theorem 4.13 (Hilbert 90)**.** *Let K/F be a cyclic Galois extension with* $\mathrm{Gal}(K/F) = \langle \sigma \rangle$. *Then* $\mathrm{N}_{K/F}(x) = 1$ *if and only if $x = b^{-1}\sigma(b)$ for some $b \in K^*$.*

As $\mathrm{N}_{K/F}(b) = \prod_{i=0}^{[K:F]-1} \sigma^i(b)$ and $\sigma^{[K:F]} = \mathrm{id}_K$, it is clear that $\mathrm{N}_{K/F}(b^{-1}\sigma(b)) = 1$. To see some evidence for the converse implication, let us look at the simplest non-trivial case, namely $\mathbb{C}\,/\,\mathbb{R}$, the degree two cyclic extension. $\mathrm{N}(x) = x\overline{x}$ where $\overline{x}$ is the complex conjugate of x. Thus if $\mathrm{N}(x) = 1$, then $x\overline{x} = |x|^2 = 1$ and hence x lies on the unit circle and is $\cos\theta + i\sin\theta$ for $0 \leq \theta < 2\pi$.

Now, for $\theta \neq \pi$, some trignometric identities from a long time ago(!) give

$$\begin{aligned}\cos\theta &= \frac{1-\tan^2(\theta/2)}{1+\tan^2(\theta/2)},\\ \sin\theta &= \frac{2\tan(\theta/2)}{1+\tan^2(\theta/2)}.\end{aligned}$$

Then set $b = 1 - i\tan(\theta/2)$ and $x = b^{-1}\overline{b}$. If $\theta = \pi$, set $b = i$ and $x = -1 = b^{-1}\overline{b}$.

We will prove a more general form of Theorem 90 due to Emmy Noether which is expressed in terms of vanishing of certain cohomology groups.

Theorem 4.14 (Emmy Noether)**.** *Let K/F be a finite cyclic Galois extension and let $G = \mathrm{Gal}(L/K)$. Then $\mathrm{H}^1(G, K^*)$ is trivial*

Proof. Here G acts on K^* via Galois automorphisms. Let $f : G \to K^*$ be a 1-cocycle, that is $f(gh) = gf(h)f(h)$ for $g, h \in G$. We would like to prove f is a 1-coboundary.

Now, look at $\sum_{g\in G} f(g)g$. By Dedekind's lemma, the set $\{g \mid g \in G\}$ is a K-independent set. So the map $\sum_{g\in G} f(g)g$ is not the zero map. Hence there is a $b \in K^*$ such that $\sum_{g\in G} f(g)g(b) = a \neq 0$.

For any $h \in G$, we have

$$
\begin{aligned}
h(a) &= h\left(\sum_{g\in G} f(g)g(b)\right) \\
&= \sum_{g\in G} h(f(g))hg(b) \\
&= \sum_{g\in G} \frac{f(hg)}{f(h)} hg(b) \\
&= \frac{1}{f(h)} \sum_{hg\in G} f(hg)hg(b) \\
&= \frac{a}{f(h)}.
\end{aligned}
$$

This means $f(h) = h(a)^{-1}a$. Now let $c = a^{-1}$. Thus $h(c) = h\left(a^{-1}\right) = h(a)^{-1}$ and $c^{-1} = a$. So $f(h) = c^{-1}h(c)$ and hence f is a 1-coboundary. $\square$

Why does the above theorem imply Hilbert 90? Let $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ have order n and let $\mathrm{N}_{K/F}(a) = 1$. Define the function $f : \mathrm{Gal}(K/F) \to K^*$ which sends $\sigma^i \rightsquigarrow a\sigma(a)\sigma^2(a)\ldots\sigma^{i-1}(a)$ for $i \geq 1$. Note that $f(\mathrm{id}) = f(\sigma^n) = \mathrm{N}_{K/F}(a)$.

A little pleasant computation shows that f is a 1-cocycle. Thus by Noether's theorem, f is a 1-coboundary and hence there exists $b \in K^*$ such that $f\left(\sigma^i\right) = b^{-1}\sigma^i(b)$ for $1 \leq i \leq n$. Thus $f(\sigma) = a = b^{-1}\sigma(b)$.

Chapter 5

A glimpse of Galois cohomology

'Thus, the task is ... not so much to see what no one has yet seen; but to think what nobody has yet thought, about that which everybody sees.'
- Erwin Schrödinger

In this chapter, we understand what a profinite group is and its cohomology theory. We finally dive into non-abelian cohomology and end with three computations of the first cohomology group. For this chapter, of course we refer to the bible ([Serre97]). Another excellent reference is ([GS]).

5.1 Profinite groups

We would like to understand the cohomology of modules with a $\mathrm{Gal}\left(k^{sep}/k\right)$ action. The absolute Galois group is no longer a finite group and so the theory from the last chapter needs to be tweaked. However $\mathrm{Gal}\left(k^{sep}/k\right)$ has only finite quotients. This should bring to mind the notion (which we now recall) of a *profinite group* which is the inverse limit of discrete finite groups.

Let I be a directed set, i.e. a set with a partial order $\leq$ with the additional property that given $i, j \in I$, there exists $k \in I$ such that $i \leq k$ and $j \leq k$.

Given the following *inverse system* :

1. A finite group G_i with the discrete topology for each $i \in I$.
2. A (continuous) group homomorphism $\pi^i_j : G_j \to G_i$ every $i \leq j$ in I such that
   - $\pi^i_i = \mathrm{id}\,|_{G_i}$.
   - For $i \leq j \leq k$, we have $\pi^i_j \circ \pi^j_k = \pi^i_k$.

let $G = \varprojlim_{i \in I} G_i$ be the *inverse limit.* One can either define it via a universal property or more prosaically as the following subgroup of $\prod_{i \in I} G_i$, namely

$$G = \left\{ (g_i) \in \prod G_i \mid \pi^i_j(g_j) = g_i \ \forall \ i \leq j \right\}.$$

Equip $\prod G_i$ with the product topology and G, with the subspace topology to make G a profinite group. One can check G is closed in $\prod G_i$. Since $\prod G_i$ is compact by Tychonoff's theorem, we see that G is also compact.

Examples

- If p is a prime, then the p-adic integers $\mathbb{Z}_p$ is isomorphic to the inverse limit of $\mathbb{Z}/p^n\,\mathbb{Z}$.
- The absolute Galois group $\mathrm{Gal}\,(k^{sep}/k)$ is the inverse limit of the Galois groups $\mathrm{Gal}(L/k)$ for finite sub-Galois extensions L/k.
- More generally, let F/k be any (possibly infinite) Galois extension. Then $\mathrm{Gal}\,(F/k)$ is the inverse limit of the Galois groups $\mathrm{Gal}(L/k)$ for finite sub-Galois extensions L/k.

5.2 Profinite group cohomology

Let Γ be a profinite group and let A be an abelian group with the discrete topology. We term A to be a *discrete* Γ *module* if it is equipped with a continuous left action $\eta : \Gamma \times A \to A$.

If A is any $\mathbb{Z}\Gamma$ module and $U \subset \Gamma$, the symbol A^U stands for the set $\{a \in A \mid ua = a \; \forall \; u \in U\}$. A useful characterization of a continuous module is that A is continuous if and only if $A = \bigcup_U A^U$ where U runs over open subsets of Γ.

Let $\mathcal{A}$ denote the category of $\mathbb{Z}\Gamma$ modules and let $\mathcal{B}$ denote the category of discrete Γ modules. Clearly the forgetful functor $f : \mathcal{B} \to \mathcal{A}$ which forgets the topology of the Γ module is fully faithful.

One can define a functor $g : \mathcal{A} \to \mathcal{B}$ sending $A \rightsquigarrow \cup A^U$ where U runs over all open subsets of G. Then since $\mathcal{A}$ has enough injectives, so does $\mathcal{B}$ (Stacks Project : Tag 015Y, Tag 04JF).

The functor $(-)^\Gamma : \mathcal{B} \to$ (Abelian groups) sending $A \rightsquigarrow A^\Gamma$ is still left exact and we can then define the cohomology groups $\mathrm{H}^q(\Gamma, A)$ to be the right derived functors of $(-)^\Gamma$.

On the other hand, we could also look at open normal subgroups U of Γ. Since Γ is profinite, the quotient Γ/U is a finite group and A^U is a Γ/U module. Therefore $\mathrm{H}^q\left(\Gamma/U, A^U\right)$ makes sense for each such U. Varying over U, these in fact form an inverse system using inflation maps.

It is then a theorem that ([Shatz], Thm 7, Pg 24)

$$\varinjlim_{U} \mathrm{H}^q\left(\Gamma/U, A^U\right) \simeq \mathrm{H}^q(\Gamma, A).$$

We will always be interested in the case that $\Gamma = \mathrm{Gal}\left(k^{sep}/k\right)$ and $A = G\left(k^{sep}\right)$ where G is a linear algebraic group over k. However, then A is no longer abelian, which brings us to ...

5.3 Non-abelian cohomology

Let Γ be a profinite group and let A be a discrete (not necessarily abelian) group with a left Γ action. That is A (under the discrete topology) has a continuous left Γ action such that for each $\gamma \in \Gamma$ and $a, b \in A$, we have

$$^{\gamma}(ab) = {}^{\gamma}a\,{}^{\gamma}b.$$

We define the set of 1-*cocycles* to be the set

$$\mathrm{Z}^1\left(\Gamma, A\right) = \{f \in \mathrm{Maps}_{cont}\left(\Gamma, A\right) \mid f\left(\gamma_1\gamma_2\right) = f\left(\gamma_1\right)\,{}^{\gamma_1}f\left(\gamma_2\right).\}$$

Two 1-cocycles f and g are said to be *cohomologous* (denoted $f \sim g$) if there exists $a \in A$ such that for every $\gamma \in \Gamma$,

$$f\left(\gamma\right) = a^{-1}g\left(\gamma\right)\,{}^{\gamma}a.$$

Then we define the 0^{th} and 1^{st} cohomology groups as follows :

$$\mathrm{H}^0\left(\Gamma, A\right) := A^{\Gamma}.$$

$$\mathrm{H}^1\left(\Gamma, A\right) := \mathrm{Z}^1\left(\Gamma, A\right)/\sim.$$

Note that $\mathrm{H}^1(\Gamma, A)$ is just a pointed set where the special point corresponds to the equivalence class of the trivial cocycle $[\gamma \mapsto 1]$.

Further one can check that $\mathrm{H}^1(\Gamma, A) = \varinjlim_U \mathrm{H}^1\left(\Gamma/U, A^U\right)$ for U runing over the set of open normal subgroups of Γ. Moreover, the maps $\mathrm{H}^1\left(\Gamma/U, A^U\right) \to \mathrm{H}^1(\Gamma, A)$ are in fact injective.

In the case when A is abelian, A is a discrete Γ module and these cohomology groups coincide with the profinite cohomology groups discussed before. Further, higher profinite cohomology groups for A can be defined.

5.3.1 A principal homogeneous space

Let Γ be a profinite group and let A be a discrete group with a left Γ action. A non-empty set P is called a (Γ, A) set if it is a discrete left Γ set with a *compatible* right A-action. That is for each $p \in P, a \in A$ and $\gamma \in \Gamma$, we have

$$^{\gamma}(pa) = {}^{\gamma}p\, {}^{\gamma}a.$$

We say a (Γ, A) set P is a *principal homogeneous space under* A if the action of A is *simply transitive*. That is given $p, q \in P$, there is a unique $a \in A$ such that $pa = q$. The first Galois cohomology set turns out to classify principal homogeneous spaces!

Theorem 5.1 ([Serre97], Chapter I, Proposition 33)**.** *There is a one to one correspondence of pointed sets between the first cohomology group* $\mathrm{H}^1(\Gamma, A)$ *and isomorphism classes of principal homogeneous spaces under* A*.*

Under this bijection, the trivial class in $\mathrm{H}^1(\Gamma, A)$ *corresponds to the class of principal homogeneous spaces with a* Γ*-invariant point.*

Proof. We ony give the recipe to go from cocycles to principal homogeneous spaces and vice-versa and leave the checking of the other details to the reader.

Given a 1-cocycle $f : \Gamma \to A$, let us construct a principal homogeneous space P_f associated to it. Take P_f as a right A module to be just A itself (with the right action given by right multiplication). We vary the left Γ-action by *twisting it by the cocycle* f as follows :

$$\begin{aligned} \star : \Gamma \times P_f &\to P_f \\ \gamma \star a &= f(\gamma)\ {}^{\gamma}a \end{aligned}$$

Note that if you start with the trivial cocycle $[\gamma \to 1]$, you get back A as a principal homogeneous space under itself and it clearly has the Γ-invariant point 1.

Conversely, given a principal homogeneous space P under A, let us manufacture a 1-cocycle. Fix a point $p \in P$. Since A acts on P simply transitively, for each $\gamma \in \Gamma$, there exists a unique $f(\gamma) \in A$ such that ${}^{\gamma}p = pf(\gamma)$. Thus we have a map $f : \Gamma \to A$ depending on the base point $p \in P$. This is in fact a 1-cocycle. If you vary your base point, you will end up with a cohomologous 1-cocycle.

Note that if P has a Γ-invariant point p, then this process gives the trivial cocycle. $\square$

5.3.2 Two long exact sequences

If $f : A \to B$ is a Γ-morphism of discrete Γ groups A and B, then for $i = 0, 1$, we have canonical maps $\mathrm{H}^i(\Gamma, A) \xrightarrow{f} \mathrm{H}^i(\Gamma, B)$.

If $1 \to A \to B \to C \to 1$ is a short exact sequence in the category of discrete Γ groups, then we get a long exact sequence which becomes a little longer when A is central in B. These are listed in the propositions below and will be repeatedly used without mention in the final chapters of this dissertation.

Proposition 5.2 ([Serre97], Chapter I, §5, Prop 38). *Let $1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$ be a short exact sequence in the category of discrete Γ groups. Then there exists a connecting map of sets $\delta_0 : \mathrm{H}^0(\Gamma, C) \to \mathrm{H}^1(\Gamma, A)$ such that the following is an exact sequence of pointed sets.*

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{H}^0(\Gamma, A) \arrow[r, "f"] & \mathrm{H}^0(\Gamma, B) \arrow[r, "g"] & \mathrm{H}^0(\Gamma, C) \arrow[dll, rounded corners, "\delta_0"] \\
& \mathrm{H}^1(\Gamma, A) \arrow[r, "f"] & \mathrm{H}^1(\Gamma, B, "g") \arrow[r] & \mathrm{H}^1(\Gamma, C)
\end{tikzcd}$$

Proposition 5.3 ([Serre97], Chapter I, §5, Prop 43). *Let $1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$ be a short exact sequence in the category of discrete Γ groups such that $A \subseteq \mathrm{Z}(B)$. Then there exists a connecting map of sets $\delta_1 : \mathrm{H}^1(\Gamma, C) \to \mathrm{H}^2(\Gamma, A)$ which extends the previous long exact sequence.*

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{H}^0(\Gamma, A) \arrow[r, "f"] & \mathrm{H}^0(\Gamma, B) \arrow[r, "g"] & \mathrm{H}^0(\Gamma, C) \arrow[dll, rounded corners, "\delta_0"] & \\
& \mathrm{H}^1(\Gamma, A) \arrow[r, "f"] & \mathrm{H}^1(\Gamma, B) \arrow[r, "g"] & \mathrm{H}^1(\Gamma, C) \arrow[r, "\delta_1"] & \mathrm{H}^2(\Gamma, A)
\end{tikzcd}$$

We mention in passing how δ_0 and δ_1 are defined and leave the rest of the details to the tenacious reader.

δ_0 : Given $c \in \mathrm{H}^0(\Gamma, C) = C^\Gamma$, pick some lift $b \in B$ such that $g(b) = c$. Define $\delta_0(c) : \Gamma \to A$ to be the 1-cocycle which *measures* the failure of b from being a 0-cocycle. More precisely

$$\begin{aligned} \delta_0(c) : \Gamma &\to A \\ \gamma &\rightsquigarrow b^{-1}\, {}^{\gamma}b \end{aligned}$$

δ_1 : Let $h \in \mathrm{Z}^1(\Gamma, C)$. Thus $h : \Gamma \to C$. Pick some set map lift $\tilde{h} : \Gamma \to B$ such that $g \circ \tilde{h} = h$.

Define $\delta_1(h) : \Gamma \times \Gamma \to A$ to be the 2-cocycle which *measures* the failure of $\tilde{h}$ from being a 1-cocycle. More precisely,

$$\begin{aligned} \delta_1(h) : \Gamma \times \Gamma &\to A \\ (s,t) &\rightsquigarrow \tilde{h}(s)\, {}^{s}\left(\tilde{h}(t)\right) \tilde{h}(st)^{-1} \end{aligned}$$

5.3.3 Three computations

Let us compute the Galois cohomology of the following groups. The first two are the immensely useful but usual pedagogical examples but the last example is in fact one we will use in Chapter 10.

Example GL_n

Theorem 5.4 (Hilbert 90 for GL_n)**.**

$$\mathrm{H}^1(k, \mathrm{GL}_n(k^{sep})) = 1.$$

Proof. It is enough to check that $\mathrm{H}^1\left(G, \mathrm{GL}_n(L)\right)$ is trivial for finite Galois extensions L/k where $G = \mathrm{Gal}\left(L/K\right)$. Let $f : G \to \mathrm{GL}_n(L)$ be a 1-cocycle, that is $f(gh) = gf(h)f(h)$ for $g, h \in G$. We would like to prove f is cohomologous to the trivial cocycle $[g \mapsto \mathrm{id}]$.

We try to imitate the proof of Theorem 4.14 by looking at $B := \sum_{g \in G} f(g)g : \mathrm{M}_n(L) \to \mathrm{M}_n(L)$. If we can find a $b \in \mathrm{M}_n(L)$ such that $B(b) = a \in \mathrm{GL}_n(L)$, then as before we see that for any $h \in G$, we have

$$\begin{aligned} h(a) &= h\left(\sum_{g \in G} f(g)g(b)\right) \\ &= \sum_{g \in G} h(f(g))hg(b) \\ &= f(h)^{-1} \sum_{g \in G} f(hg)hg(b) \\ &= f(h)^{-1} \sum_{hg \in G} f(hg)hg(b) \\ &= f(h)^{-1} a. \end{aligned}$$

This means $f(h) = ah(a)^{-1}$ for each $h \in G$ and hence f is cohomologous to the trivial cocycle. So the problem reduces to finding a $b \in \mathrm{M}_n(L)$ such that $B(b) \in \mathrm{GL}_n(L)$

Look at the k-linear map $D : L^n \to L^n$ sending $\mathbf{x} \rightsquigarrow \sum_{g \in G} f(g) \circ g(\mathbf{x})$. Let the L-span of $\{D(\mathbf{x}) \mid \mathbf{x} \in L^n\} = V$. We claim that $V = L^n$. This can be checked showing that every L-functional $u \in \mathrm{Hom}_L\left(L^n, L\right)$ vanishing on V is actually zero. We leave this checking as an exercise.

Let us grant the claim and proceed by picking vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n \in L^n$ such that $\{D\left(\mathbf{x}_i\right)\}$ is an L-basis for L^n.

Define $b \in \mathrm{End}_L(L^n) \simeq \mathrm{M}_n(L)$ by sending the standard basis $e_i \rightsquigarrow \mathbf{x}_i$. We claim that $B(b) \in \mathrm{GL}_n(L)$ because $B(b) : L^n \to L^n$ sends L-basis e_i to another L-basis $D(\mathbf{x}_i)$.

Let us finally check that $B(b)(e_i) = D(\mathbf{x}_i)$. Note that $g(be_i) = g(b)g(e_i) = g(b)(e_i)$ as $e_i \in k^n$ in fact. Thus we have

$$\begin{aligned} B(b)(e_i) &= \sum_{g \in G} f(g)g(b)(e_i) \\ &= \sum_{g \in G} f(g)g(be_i) \\ &= \sum_{g \in G} f(g)g(\mathbf{x_i}) \\ &= D(\mathbf{x_i}). \end{aligned}$$

□

Example μ_n

Let $n \in \mathbb{N}$ be such that it is not divisible by the characteristic of k. The long exact sequence of cohomology for the Kummer sequence

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{x \rightsquigarrow x^n} \mathbb{G}_m \to 1,$$

along with Hilbert 90 for $\mathbb{G}_m$ (c.f. Thm 4.14) yields the fact that

$$\mathrm{H}^1(k, \mu_n) \simeq k^*/k^{*n}.$$

Example $\mu_{n[Z]}$

Let Z/k be an etale quadratic extension and $n \in \mathbb{N}$ which is not divisible by the characteristic of k. Define the group $\mu_{n[Z]}$ via the exact sequence :

$$1 \to \mu_{n[Z]} \to R_{Z/k}\left(\mu_{n,Z}\right) \xrightarrow{\mathrm{N}_{Z/k}} \mu_n .$$

Proposition 5.5 ([KMRT], Prop 30.13, Pg 418)**.**

$$\mathrm{H}^1\left(k, \mu_{n[Z]}\right) \simeq \frac{\{(x,y) \in k^* \times Z^* \mid x^n = \mathrm{N}_{Z/k}(y)\}}{\{\left(\mathrm{N}_{Z/k}(z), z^n\right) \; | z \in Z^* \;\}}.$$

Proof. If $Z = k \times k$, then $\mathrm{H}^1\left(k, \mu_{n[Z]}\right) = \mathrm{H}^1\left(k, \mu_n\right) \simeq k^*/k^{*n}$. The group on the right side of the equation becomes

$$\frac{\{(a, a^n c^{-1}, c) \in k^* \times k^* \times k^*\}}{\{(de, d^n, e^n)\}}.$$

Projection on the last coordinate gives the isomorphism to k^*/k^{*n}.

Assume now that Z is a field. Construct a k-group scheme $T \subset \mathbb{G}_m \times R_{Z/k}\mathbb{G}_m$ defined by $T(k) = \{(x,y) \in k^* \times Z^* \mid x^n = \mathrm{N}_{Z/k}(y)\}$.

Define the map $\theta : R_{Z/k}\mathbb{G}_m \to T$ sending $z \rightsquigarrow \left(\mathrm{N}_{Z/k}(z), z^n\right)$. The kernel of θ is precisely $\mu_{n[Z]}$ and hence we get the exact sequence

$$1 \to \mu_{n[Z]} \to R_{Z/k}\left(\mathbb{G}_{m,Z}\right) \xrightarrow{\theta} T \to 1.$$

Looking at the long exact sequence and using that $\mathrm{H}^1\left(k, R_{Z/k}\mathbb{G}_{m,Z}\right) = 1$, we see $\mathrm{H}^1\left(k, \mu_{n[Z]}\right)$ is just $T(k)/\theta(Z^*)$ which is precisely the group on the right hand side in the proposition. $\square$

Chapter 6

Reviewing R-equivalence and rationality

'There are many questions which fools can ask that wise men cannot answer.'

- George Polya

In this chapter, we recall what it means for the underlying variety of an algebraic group to be rational. We then review the notion of R-equivalence which serves as an extremely useful tool to detect non-rationality of group-varieties and proceed to present several important examples of non-rational group varieties collected from literature in this area. The discussion on adjoint groups will prompt a natural question which is explored in the next chapter leading to one of the principal results of this disseration.

For this chapter, we draw both material and inspiration from Gille's Bourbaki Seminar on the Kneser-Tits problem ([Gille07]), the notes from his lecture series on R-equivalence on linear algebraic groups ([Gille10]) and the first part of ([Me98]). The main technical references for this chapter are the powerful computations of R-equivalence classes of various algebraic groups in ([CTS], [Platonov76], [Me96], [CP], [Gille97] et al). Our base field for this chapter will be an infinite field k of characteristic not 2. By a k-variety, we will mean a geometrically integral k-variety and by a k-group, we will mean a smooth connected linear algebraic group over k unless mentioned otherwise.

6.1 What is being rational?

Let X, Y be k-varieties. They are said to be *k-birational* if there are dense open sets $U \subseteq X$ and $V \subseteq Y$ such that $U \simeq_k V$. Equivalently, their function fields $k(X)$ and $k(Y)$ are isomorphic over k.

X is said to be *k-rational* if it is k-birational to some projective space $\mathbb{P}^n_k$ (or affine space $\mathbb{A}^n_k$). Equivalently, its function field $k(X)$ is purely transcendental over k.

Consider the real unit circle $S = \operatorname{Spec}\left(\frac{\mathbb{R}[x,y]}{\langle x^2+y^2-1\rangle}\right)$. Note that $x^2 + y^2 - 1$ is an irreducible polynomial in $\mathbb{R}[x, y]$. For if not, it has a linear factor which will mean a straight line lying on the circle! Thus the coordinate ring $\mathbb{R}[S]$ is in fact a domain and S is an irreducible real variety. It is in fact also rational. The stereographic projection immediately gives an isomorphism between $S \setminus \{(0, -1)\}$ and the affine line.

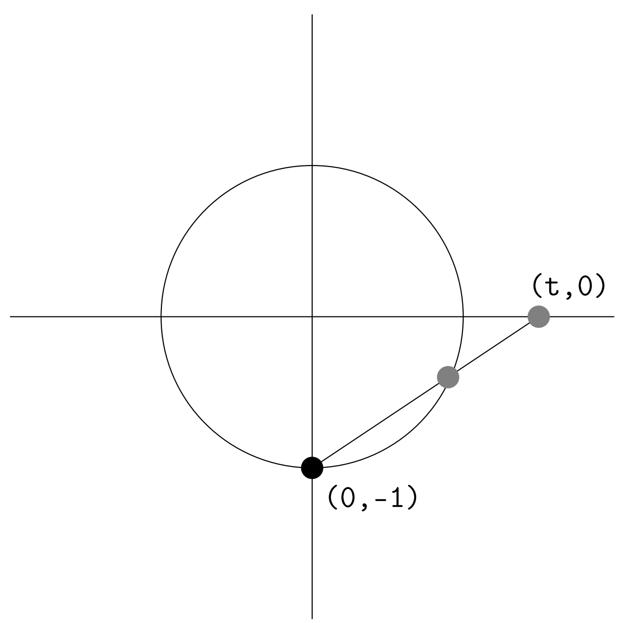

Figure 6.1: Stereographic projection

In coordinates, this gives a a nice parametrization of the circle with which we can check $\mathbb{R}(S) \simeq \mathbb{R}(t)$

$$\begin{aligned} \frac{\mathbb{R}[x,y]}{\langle x^2+y^2-1\rangle} &\to \mathbb{R}(t) \\ x &\rightsquigarrow \frac{2t}{1+t^2} \\ y &\rightsquigarrow \frac{1-t^2}{1+t^2} \end{aligned}$$

Consider the similar looking variety $T = \operatorname{Spec}\left(\frac{\mathbb{R}[x,y]}{\langle x^2+y^2+1\rangle}\right)$. Note that $x^2 + y^2 + 1$ is an irreducible polynomial in $\mathbb{R}[x,y]$ too. In fact, it has no zeroes over $\mathbb{R}$. Hence it cannot be birational to any affine space $\mathbb{A}^n_{\mathbb{R}}$ which has lots of $\mathbb{R}$-rational points.

The rationality question depends very fundamentally on the base field. For instance, the varieties S and T over $\mathbb{C}$ become isomorphic (and $\mathbb{C}$-rational).

$$\frac{\mathbb{C}[x,y]}{\langle x^2+y^2-1\rangle} \simeq \mathbb{C}\left[t,t^{-1}\right] \simeq \frac{\mathbb{C}[x,y]}{\langle x^2+y^2+1\rangle}.$$

This example generalizes to any anisotropic conic over k. It is a non-rational k-variety which becomes $\overline{k}$-rational.

A k-variety X is said to be *k-stably rational* if $X \times_k \mathbb{A}^n_k$ is k-rational for some $n \in \mathbb{N}$. Stable rationality is a strictly weaker notion than rationality ([BCTSSD]).

We are interested in rationality questions about the varieties underlying linear algebraic groups. Thus for G, a (smooth) connected linear algebraic group defined over k, we say G is k-(stably) rational if its underlying variety is k-(stably) rational.

It is a theorem of Chevalley from the 1950s that when characteristic of k is 0, G is always $\overline{k}$-rational ([Chevalley]). Though the original proof was couched in the language of Lie algebras, we give a sketch below using the Bruhat decomposition machinery. Note that one can prove the rationality of smooth split groups over a more general field similarly.

Proposition 6.1 ([CT07], Prop 4.2)**.** *Let G be a connected algebraic group over an algebraically closed field k of char 0. Then G is k-rational.*

Proof. Let U be the unipotent radical of G. This is isomorphic to $\mathbb{G}_a^r$ for some r and hence rational. The quotient variety G/U is a reductive group and in fact $G \simeq U \times_k G/U$ as varieties. Thus we are reduced to looking at the case when G is reductive.

Let T be a maximal torus. Note that it is $\mathbb{G}_m^n$ and hence rational. Then there is an associated Borel subgroup B^+ with unipotent radical U^+. Let B^{-1} denote the opposite Borel subgroup and let its unipotent radical be U^-. The unipotent groups U^+ and U^- are rational being products of copies of $\mathbb{G}_a$.

The product map $m : U^+ \times T \times U^- \to G$ identifies the rational variety $U^+ \times T \times U^-$ with a non-empty dense open set V in G called the *big open cell.* Hence G is rational. $\square$

6.2 Detecting non-rationality

The notion of R-equivalence, first introduced by Manin in the 70s to study cubic hypersurfaces, is defined as follows :

Definition 6.2. *Let X be a k-variety and F/k, a field extension. Then $x, y \in X(F) = \mathrm{Hom}_{\mathrm{Spec}\, k}(\mathrm{Spec}\, F, X)$ are defined to be strictly R-equivalent if there exists an F-rational map $f : \mathbb{A}^1_F \dashrightarrow X$ defined at 0 and 1 sending*

$$0 \rightsquigarrow x,$$
$$1 \rightsquigarrow y.$$

Strict R-equivalence is reflexive and symmetric, but not neccesarily transitive and hence R-equivalence is defined to be the equivalence relation on $X(F)$ generated by strict R-equivalence. We let $X(F)/R$ denote the set of R-equivalence classes of $X(F)$.

Strict R-equivalence behaves well for algebraic groups. We expand on this in the following lemma.

Lemma 6.3. *Let G be a connected linear algebaic group over k and let F/k be a field extension of k. Then*

1. *R-equivalence is the same as strict R-equivalence for $G(F)$.*
2. *Let $RG(F)$ denote the subset of elements $x \in G(F)$ which are R-equivalent to the identity e. Then $RG(F)$ is a normal subgroup of $G(F)$.*
3. *There is a bijection of sets between $G(F)/R$ and $G(F)/RG(F)$.*

Proof.

1. We have to show strict R-equivalence is transitive. Let us denote $x \sim_{SR} y$ if $x, y \in G(F)$ are strictly R-equivalent. Let $x \sim_{SR} y$ and $y \sim_{SR} z$. We would like to show $x \sim_{SR} z$.

   Let $f : \mathbb{A}^1_F \dashrightarrow G$ such that $f(0) = x$, $f(1) = y$. Let h be the rational function got by composing f with right translation by y^{-1}.

That is $h : \mathbb{A}^1_F \dashrightarrow G \xrightarrow{*y^{-1}} G$. Thus $h(0) = xy^{-1}$ and $h(1) = e$. Since $y \sim_{SR} z$, let $g : \mathbb{A}^1_F \dashrightarrow G$ be such that $g(0) = y$ and $g(1) = z$.

Let $m : G \times G \to G$ denote the multiplication map. Define the rational function $w : \mathbb{A}^1_F \dashrightarrow^{(h,g)} G \times G \xrightarrow{m} G$. Thus $w(0) = m(xy^{-1}, y) = x$ and $w(1) = m(e, z) = z$. Hence $x \sim_{SR} z$.

2. We leave the proof that $RG(F)$ is a subgroup as an exercise to the interested reader and only check normality. Let $g \in G(F)$ and let $x \in RG(F)$. Thus $e \sim_{SR} x$ and let $f : \mathbb{A}^1_F \dashrightarrow G$ such that $f(0) = e$, $f(1) = x$.

   Let h be the rational function got by composing f with the conjugation map by $\mathrm{Int}(g)$. That is $h : \mathbb{A}^1_F \dashrightarrow G \xrightarrow{g-g^{-1}} G$. Thus $h(0) = geg^{-1} = e$ and $h(1) = gxg^{-1}$. Hence $e \sim_{SR} gxg^{-1}$ and hence $gxg^{-1} \in RG(F)$.

3. For $x \in G(F)$, let $[x]$ denote the subset of elements R-equivalent to x. We claim that $[x] = x.RG(F)$.

   To show the inclusion one way, let $z \in [x]$. That is $x \simeq_{SR} z$. Let $f : \mathbb{A}^1_F \dashrightarrow G$ be such that $f(0) = x$ and $f(1) = z$. Let h be the rational function got by composing f with the left translation by x^{-1}. That is $h : \mathbb{A}^1_F \dashrightarrow G \xrightarrow{x^{-1}*} G$. Thus $h(0) = e$ and $h(1) = x^{-1}z$. Hence $e \sim_{SR} x^{-1}z$ and hence $x^{-1}z \in RG(F)$. This implies $z = x(x^{-1}z) \in xRG(F)$.

   Conversely, let $z = xy \in xRG(F)$ where $y \in RG(F)$. Thus $e \simeq_{SR} y$ and let $f : \mathbb{A}^1_F \dashrightarrow G$ be such that $f(0) = e$ and $f(1) = y$. Let h be the rational function got by composing f with the left transation by x.

That is $h : \mathbb{A}^1_F \dashrightarrow G \xrightarrow{x*} G$. Thus $h(0) = x$ and $h(1) = xy = z$. Hence $x \sim_{SR} xy = z$ and hence $z \in [x]$.

$\square$

The bijection between $G(F)/R \leftrightarrow \frac{G(F)}{RG(F)}$ induces a group structure on the set of R-equivalence classes of $G(F)$. Thus, hereafter we shall consider $G(F)/R$ along with this transported group structure. There are many basic questions which have been asked (and remain unanswered!) about this group $G(F)/R$. For instance, the following question is still open.

Question 6.4. Is $G(F)/R$ abelian?

We pause to introduce a new terminology at this point. A k-algebraic group G is said to be *R-trivial* if $G(F)/R = \{0\}$ for all F/k. Our interest in $G(F)/R$ stems from the more or less immediate link to (non) stable rationality as evinced by the following lemma.

Lemma 6.5. *Any k-stably rational algebraic group G is R-trivial.*

Proof. If G is k-stably rational, then it is stably rational over any field. Thus it sufffices to show that $G(k)/R$ is trivial.

Let us first show that for the affine space $G = \mathbb{A}^n_k$. If $x = (x_1, \ldots, x_n) \in G(k)$, then define $f : \mathbb{A}^1_k \dashrightarrow G$ to be the function sending $t \rightsquigarrow (x_1 t, \ldots, x_n t)$.

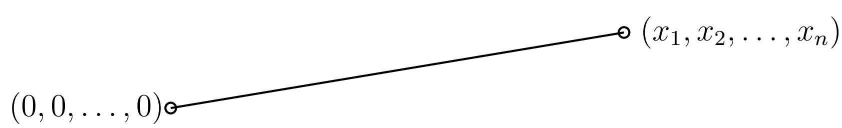

Figure 6.2: R-triviality of $\mathbb{A}^n_k$

Now if G were k-rational, it contains an open dense subset U which is k-isomorphic to a non-empty open set $V \subseteq \mathbb{A}_k^n$. Since k is an infinite field, $V(k) \neq \emptyset$ and hence $U(k) \neq \emptyset$ too. Let $u \in U(k)$ say. Let $x \in G(k)$ be an arbitrary rational point. Consider the open sets $U_1 = u^{-1}U$ and $U_2 = xu^{-1}U$ defined over k. Thus $e \in U_1(k)$ and $x \in U_2(k)$.

Now $U_1 \cap U_2$ is again open and defined over k and $U_1 \cap U_2(k) \neq \emptyset$ again. Let $y \in U_1 \cap U_2(k)$. Now we can connect e and y by a k-line in U_1 and y and x by a k-line in U_2. This shows that $e \sim_{SR} x$ in $G(k)$.

Finally if G is k-stably rational, then $H = G \times_k \mathbb{A}_k^n$ is k-rational. R-equivalence behaves well with respect to products and hence

$$0 = H(k)/R \simeq G(k)/R \times \mathbb{A}^n(k)/R \simeq G(k)/R.$$

□

The lemma is incredibly useful in its contrapositive form, namely

Lemma 6.6. *If there exists an F/k such that $G(F)/R \neq \{0\}$, then G is not k-stably rational.*

This will be the strategy mostly adopted to show the non-rationality of the various groups discussed in the following section.

6.3 Early examples of non-rational groups

6.3.1 Chevalley's example

Let us begin our search for non-rational groups by revisiting Chevalley's example of a non-rational torus in ([Chevalley]).

Let p be an odd prime and let k be the p-adic field $\mathbb{Q}_p$. Let F/k be the unique unramified extension of degree $p-1$. This is simply a lift of the cyclic extension $\mathbb{F}_{p^{p-1}}/\mathbb{F}_p$ of finite fields and hence F/k is cyclic as well with $\mathrm{Gal}(F/k) = \mathbb{Z}/(p-1)\,\mathbb{Z}$.

Let $K = \mathbb{Q}_p(\zeta_p)$ where ζ_p is a primitive p^{th} root of unity. This is a totally ramified extension of degree $p-1$. To see this, note that $K = \mathbb{Q}_p[t]/(f)$ where $f(t) = t^{p-1} + t^{p-2} + \ldots + t + 1$. Let $\eta = \zeta_p - 1$ whose minimal polynomial is the Eisenstein polynomial

$$\begin{aligned} g(t) &= f(t+1) \\ &= \frac{(t+1)^p - 1}{(t+1) - 1} \\ &= t^{p-1} + \left(\sum_{i=1}^{p-2} C(p,i) t^{p-i-1} \right) + p. \end{aligned}$$

Thus $K = \mathbb{Q}_p(\eta) = \mathbb{Q}_p[t]/(g)$ is a totally ramified extension of degree $p-1$ being obtained by attaching a root of an Eisenstein polynomial. Clearly K/k is cyclic Galois since it is the splitting field of $t^p - 1$ and $\mathrm{Gal}(K/k) = \mathbb{Z}/(p-1)\,\mathbb{Z}$.

$$\begin{array}{ccc} F & \longrightarrow & L \\ \uparrow & & \uparrow \\ k & \longrightarrow & K \end{array}$$

Thus K and F are disjoint over k. Let L denote their compositum. Thus L/k is a Galois extension with $\mathrm{Gal}(L/k) \cong \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$.

The Weil restriction $\mathrm{R}_{\mathrm{L/k}}\,\mathbb{G}_m$ is a rational torus over k of rank $(p-1)^2$. However the normic k-torus T of rank $(p-1)^2 - 1$ defined by the following exact sequence

$$1 \to T \to \mathrm{R}_{\mathrm{L/k}}\, \mathbb{G}_m \xrightarrow{\text{Norm}} \mathbb{G}_m \to 1,$$

is our candidate! Note that $T(k)$ is simply the norm one elements of L/k. Again, Chevalley's proof of the non-rationality is written down in the language of Lie algebras etc but a *modern* proof using R-equivalence is immediate if one appeals to the R-equivalence computations of Colliot-Thélène and Sansuc for tori.

Theorem 6.7 ([CTS], Prop 15 ; [Gille10], §2.1)**.** *Let L/k be a finite Galois extension and T, the kernel of $\mathrm{R}_{\mathrm{L/k}}\, \mathbb{G}_m \xrightarrow{\text{Norm}} \mathbb{G}_m$. Then T is R-trivial if and only if every Sylow subgroup of $Gal(L/k)$ is cyclic.*

Clearly Chevalley's torus is not R-trivial and hence not even k-stably rational. We note that taking $p = 3$ in the above discussion gives us a k-non rational torus of rank $(3-1)^2 - 1 = 3$. It turns out that tori of lesser rank are in fact rational!

6.3.2 Serre's example

The next example of a semisimple non-rational group comes from Serre. However, the strategy to showing non-rationality in this case is via failure of the *Hasse principle* for a certain algebraic group over a number field k. If Ω_k denotes the places of k, then,

Theorem 6.8 ([Serre97], Thm 8)**.** *There exists a connected semisimple algebraic group G defined over an algebraic number field k such that the kernel of the following canonical map of pointed sets is non-trivial*

$$\mathrm{H}^1(k, G) \to \prod_{v \in \Omega} \mathrm{H}^1(k_v, G).$$

For more details, the reader is encouraged to look at ([PLR], § 6.4).

Non-rationality of G

It is a deep theorem that both simply connected and adjoint groups over number fields satisfy the Hasse principle ([PLR], Thms 6.6 & 6.22). Thus G/k is necessarily neither simply connected nor adjoint.

A theorem of Sansuc and Voskresenskii ([Sansuc81], Corollary 9.7) asserts that if G/k is a rational group without an E_8 factor where k is a number field, then Hasse principle holds for principal homogeneous spaces under G over k. We note that the group G/k in Theorem 6.8 can be constructed to be a quotient of the semisimple group $\tilde{G} = \mathrm{R}_{\mathrm{L/k}} \mathrm{SL}_n$ for a suitable field extension L/k. Since G is a principal homogeneous space under itself over trivially, it would satisfy the Hasse principle if it were rational.

Thus the semisimple group G under consideration is non-rational.

6.4 The story for simply connected groups

Let us first look at G of type ${}^1A_{n-1}$. Thus if A/k is a central simple algebra, then $G = \mathrm{SL}_1(A)$, the group of reduced norm one elements.[1] The group of R-equivalence classes of $\mathrm{SL}_1(A)(k)$ has another neat description which the following lemma due to Voskresenskii gives.

Lemma 6.9 ([Vo77]). *Let A be a central simple algebra over k and let $[A^*, A^*]$ denote the commutator subgroup of A. Then*

$$\mathrm{SL}_1(A)(k)/R \simeq \mathrm{SL}_1(A)/[A^*, A^*].$$

Proof. We only give a sketch of the proof. Firstly, it can be shown by using Dieudonne determinants that one can without loss of generality assume A is a central division algebra over k. Thus, let $A = D$ be division over k.

[1]When the context is clear, by abuse of notation, sometimes we let $\mathrm{SL}_1(A)$ also denote its k-points, $\mathrm{SL}_1(A)(k)$.

Now base change to a purely transcendental extension behaves well. More precisely, let $k(t)$ be a purely transcendental extension of k in one variable and let $X = D \otimes_k k(t)$. Then the following two statements hold :

1. X is still division.
2. $\mathrm{SL}_1(X)/[X^*, X^*] \simeq \mathrm{SL}_1(D)/[D^*, D^*]$.

Granting these, let us show the lemma. Let $[1_D] = R\,\mathrm{SL}_1(D)(k)$. It is easy to see that the identity 1_D is R-equivalent to any element in the commutator subgroup. That is, it is (almost) clear that $[D^*, D^*] \subseteq [1_D]$.

Conversely, let $b \in \mathrm{SL}_1(D)(k) \in [1_D]$. So there exists $f : \mathbb{A}^1_k \dashrightarrow \mathrm{SL}_1(D)$ sending $0 \rightsquigarrow 1_D$ and $1 \rightsquigarrow b$. That is $f \in \mathrm{SL}_1(D)(k(t))$ is a *geometric point* such that $f(0) = 1_D$ and $f(1) = b$. We would like to show $b \in [D^*, D^*]$.

Since $\mathrm{SL}_1(X)/[X^*, X^*] \simeq \mathrm{SL}_1(D)/[D^*, D^*]$, we see that $f(t) = gu(t)$ where $g \in \mathrm{SL}_1(D)$ and $u(t) \in [X^*, X^*]$. Evaluating both sides at 0, we get

$$1_D = f(0) = gu(0).$$

Thus $g = u(0)^{-1} \in [D^*, D^*]$ since $u(t) \in [X^*, X^*]$. Now evaluating both sides at 1, we get

$$b = f(1) = gu(1) = u(0)^{-1}u(1) \in [D^*, D^*].$$

$\square$

Thus one way of showing the simply connected algebraic group $\mathrm{SL}_1(A)$ is not k-stably rational would be by finding some extension F/k such that $\mathrm{SL}_1(A \otimes_k F)/[(A \otimes_k F)^*, (A \otimes_k F)^*] \neq 1$.

6.4.1 The reduced Whitehead of an algebra

The abstract group $\mathrm{SL}_1(A)/[A^*, A^*]$, called the *reduced Whitehead group of* A or $\mathrm{SK}_1(A)$ has been an object of great interest since the early 40s after Tannaka and Artin independently questioned whether it was always trivial.

Question 6.10 (Tannaka-Artin,1943). Is $SK_1(A) = \{1\}$?

The theorems of Nakayamma and Wang proven in the 50s answering this question positively over local and global fields respectively, and also for algebras of square-free index, in general generated belief that $\mathrm{SK}_1(A)$ was always trivial. Thus, it came as quite a surprise when in 1976, Platonov gave his famous example of a biquarternion algebra D over a cohomological dimension 4 field[2] such that $SK_1(D) \neq \{1\}$.

Due to Voskresenskii's observation (c.f. Lemma 6.9), this also served as the first ever example of a non-stably rational simply connected group. Before we discuss Platonov's example, we would like to point out that reduced Whitehead groups $W(k, G)$ can be defined not just for $\mathrm{SL}_1(A)$ but for any semisimple simply connected isotropic[3] k-group G. And a generalization of the Tannaka-Artin problem, namely the *Kneser-Tits conjecture* asks whether reduced Whitehead groups are always trivial ([Tits78]).

Over global fields k, the Kneser Tits conjecture holds ([Gille07]). The isomorphism $W(k, G) \simeq G(k)/R$ proven in the same (ibid. Thm 7.2) therefore justifies terming the group of R-equivalence classes of $G(k)$, the correct analogue of the reduced Whitehead groups for non-isotropic groups.

[2] twice iterated Laurent series field over a global field

[3] contains a split torus

Platonov's example

Let k be a field and ℓ_1 and ℓ_2, two cyclic extensions of k such that $\ell = \ell_1 \otimes_k \ell_2$ is again a field. Let $\mathrm{Gal}(\ell_i/k) = \langle \sigma_i \rangle$ for $i = 1, 2$.

Set $K = k\,((t_1))\,((t_2))$ and $L_i = \ell_i\,((t_1))\,((t_2))$ for indeterminates t_1 and t_2. The automorphisms σ_i extend to L_i by acting trivially on t_i. Construct K-cyclic division algebras $D_1 = (L_1/K, \sigma_1, t_1)$ and $D_2 = (L_2/K, \sigma_1, t_2)$.

Platonov shows that $D = D_1 \otimes_K D_2$ is division still and calculates $\mathrm{SK}_1(D)$ as a quotient of $\mathrm{Br}(\ell/k)$. Now if $[\ell_1 : k] = [\ell_2 : k] = q$, a prime and k is a p-adic field, then $\mathrm{SK}_1(D)$ turns out to be $\mathbb{Z}\,/q\,\mathbb{Z}$ and hence is certainly non-trivial.

A similar example

To reiterate the importance the iterated Laurent series are going to play in this thesis, we present a similar example as above of a biquaternion algebra with non-trivial SK_1 ([Draxl], §24, Thm 1).

Let k be a field with a primitive 4^{th} root of unity ζ. Let t_1, t_2, t_3 and t_4 be indeterminates and let $K = k\,((t_1))\,((t_2))\,((t_3))\,((t_4))$. Set D to be the (division) biquaternion algebra $(t_1, t_2) \otimes_K (t_3, t_4)$.

Let $N = \mathbb{Z}^4_{\geq 0}$ denote the set of all non-negative integral 4-tuples with the usual lexicographic order. Then

$$D = \sum_{(i_1,i_2,i_3,i_4)\in N} k x_1^{i_1} x_2^{i_2} x_2^{i_3} x_4^{i_4} = \sum_{\bar{i}\in N} k\mathbf{x}^{\bar{i}},$$

where $x_i^2 = t_i$, $x_1x_2 = -x_2x_1$, $x_3x_4 = -x_4x_3$ and x_i and x_j commute if $i \in \{1, 2\}$ and $j \in \{3, 4\}$.

Define the function $v : D \setminus 0 \to N$ such that if $d = \sum_{\bar{i}\in N} a_{\bar{i}}\mathbf{x}^{\bar{i}}$, then

$$v(d) = \min\{\ \bar{j}\ \mid\ a_{\bar{j}} \neq 0\ \}.$$

This in fact is a valuation and hence $v(dd') = v(d) + v(d')$. Since $v(1) = 0$, we have $v(d^{-1}) = -v(d)$. Thus if $c = d_1 d_2 d_1^{-1} d_2^{-1}$ is a commutator, then $v(c) = 0$. In fact due to the relations on x_i, we see that

$$[D^*, D^*] \subseteq \left\{ \pm 1 + \sum_{\bar{i} \in N \setminus \bar{0}} a_{\bar{i}} \mathbf{x}^{\bar{i}} \right\} \qquad (*).$$

Now $\zeta \in k \subseteq D$ and $\mathrm{Nrd}_D(\zeta) = \zeta^4 = 1$. Hence $\zeta \in \mathrm{SL}_1(D)$. By (*), it is not in $[D^*, D^*]$ and hence $\mathrm{SK}_1(D) \neq 1$.

6.4.2 Positive rationality results for simply connected groups

We end the discussion on simply connected groups by listing some positive results about R-equivalence and rationality from ([Me98]). In the following, A is a central simple algebra over k, K/k is a quadratic étale field extension, B is a central simple algebra over K with unitary involution τ, q is a quadratic form over k, A' is a central simple algebra of even degree over k with symplectic involution σ'. Then,

- If index A is square-free, then $\mathrm{SL}_1(A)$ is R-trivial.
- If index B is square-free, then $\mathrm{SU}(B, \tau)$ is R-trivial.
- If q is isotropic, then $\mathrm{Spin}(q)$ is rational.
- If $\dim q \leq 5$, then $\mathrm{Spin}(q)$ is rational.
- Type C simply connected groups $\mathrm{Sp}(A', \sigma')$ are always rational due to Cayley parametrization.

6.5 The story for adjoint groups

After Platonov's example, it was still hoped for that semisimple adjoint groups were rational. Platonov himself conjectured ([PLR], pg 426) that adjoint simple algebraic k-groups were rational over any infinite field. Some evidence of the veracity of this conjecture is found in ([Chernousov]) where Chernousov establishes that $\mathrm{PSO}(q)$ is a stably rational k-variety for the special quadratic form $q = \langle 1, 1, \ldots 1\rangle$ where k is any infinite field of characteristic not 2. Note that the signed discriminant of the quadratic form in question is ± 1.

Here are some more positive results about rationality of absolutely simple adjoint groups from ([Me98]). In the following, A is a central simple algebra over k, K/k is a quadratic étale field extension, B is a central simple algebra over K with unitary involution τ, q is a quadratic form over k, A' is a central simple algebra of even degree over k with symplectic involution σ'. Then,

- $\mathrm{PGL}_1(A)$ is rational.
- If degree $B = 2$, then $\mathrm{PGU}(B, \tau)$ is rational.
- If degree B is odd, then $\mathrm{PGU}(B, \tau)$ is rational.
- Type B adjoint groups $\mathrm{O}^+(q)$ where $\dim q$ is odd are always rational due to Cayley parametrization.
- If degree $A' = 2$, then $\mathrm{PGSp}(A', \sigma')$ is rational.
- If degree $A' = 4$, then $\mathrm{PGSp}(A', \sigma')$ is rational.
- If degree $A' = 2(2n+1)$, then $\mathrm{PGSp}(A', \sigma')$ is stably rational.

6.5.1 Merkurjev's forumula

In 1996, Merkurjev in [Me96] computed the group of R-equivalence classes for adjoint semisimple classical groups. His powerful formula allowed him to find the first non-stably rational adjoint group of type D_n! In this section, we present the formula and examine it in detail in the case when $G = \mathrm{PSO}(q)$ which is of special importance to us and crucial for the next chapter.

Let $K = k$ or a quadratic étale extension of k and let A/K be a central simple algebra with an involution σ such that $K^\sigma = k$. Thus, if $K = k$, σ is of the first kind and if $K \neq k$, it is of the second kind.

Recall the *group of similitudes* $\mathrm{Sim}\,(\mathrm{A}, \sigma)$ which was defined as $\mathrm{Sim}\,(\mathrm{A}, \sigma)(k) = \{a \in A^* | \sigma(a)a \in k^*\}$. The similarity map $\mu : \mathrm{Sim}\,(\mathrm{A}, \sigma) \to \mathbb{G}_m$ sends $a \rightsquigarrow \sigma(a)(a)$. Let $\mathrm{Sim}_+\,(\mathrm{A}, \sigma)$ be the connected component of $\mathrm{Sim}\,(\mathrm{A}, \sigma)$. Let $\mathrm{PSim}_+\,(A, \sigma)$ denotes the connected component of the *group of projective similitudes*. Merkurjev's formula involves two subgroups $\mathrm{G}_+\,(\mathrm{A}, \sigma)$ and $\mathrm{Hyp}\,(\mathrm{A}, \sigma)$ of k^*. Let us first define what they are. The subgroup $\mathrm{G}_+\,(\mathrm{A}, \sigma) \subset k^*$ is defined as follows :

$$\mathrm{G}_+\,(\mathrm{A}, \sigma) := \mu(k)\,(\mathrm{Sim}_+\,(\mathrm{A}, \sigma)(k))\,.$$

The subgroup $\mathrm{Hyp}\,(\mathrm{A}, \sigma) \subseteq k^*$ is defined to be the subgroup generated by certain norms, namely look at all finite extensions E/k and set

$$\mathrm{Hyp}\,(\mathrm{A}, \sigma) := \langle \mathrm{N}_{E/k}\,(E^*) \ \mid \sigma_E \text{ hyperbolic}\rangle.$$

Let $\mathrm{NK}^* = \{\sigma(\lambda)\lambda \mid \lambda \in K^*\}$. Thus if σ is of the first kind, $\mathrm{NK}^* = k^{*2}$.

By the fundamental work of Weil, any adjoint absolutely simple classical algebraic group over k is isomorphic to $\mathrm{PSim}_+\,(A, \sigma)$ for a suitable (A, σ) as above. Then Merkurjev's formula for $\mathrm{PSim}_+\,(\mathrm{A}, \sigma)\,/R$ is the following

Theorem 6.11 (Merkurjev, [Me98])**.** *There is a natural isomorphism*

$$\mathrm{PSim}_+\,(\mathrm{A},\sigma)(k)/R \;\simeq\; \mathrm{G}_+\,(\mathrm{A},\sigma)\,/\,\mathrm{NK}^*\,\mathrm{Hyp}\,(\mathrm{A},\sigma)\,.$$

We are interested in the D_n case when A is a matrix algebra. Let (V, q) be a quadratic space of dimension $2n$. Then $K = k$, $A = \mathrm{End}_k(V)$ is the matrix algebra of degree $2n$ and $\sigma = \sigma_q$, the orthogonal involution adjoint to q. Then, we have

- $\mathrm{Sim}\,(\mathrm{A},\sigma) = \mathrm{GO}(q)$, the *group of similitudes* which is defined by the equation $\mathrm{GO}(q)(k) = \{f \in \mathrm{End}(V) \mid q(f(v)) = \alpha q(v)\ \forall\ v \in V\}$.
- $\mu : \mathrm{Sim}\,(\mathrm{A},\sigma) \to \mathbb{G}_m$ is the *multiplier map* sending $f \rightsquigarrow \alpha$.
- $\mathrm{Sim}_+\,(\mathrm{A},\sigma) = \mathrm{GO}^+(q)$, the *group of proper similitudes* which is defined by the equation $\mathrm{GO}^+(q)(k) = \{f \in \mathrm{GO}(q) | \det(f) = \mu(f)^n\}$.
- $\mathrm{PSim}_+\,(A,\sigma) = \mathrm{PGO}^+(q) = \mathrm{PSO}(q)$, the adjoint group of interest.
- $\mathrm{G}_+\,(\mathrm{A},\sigma) = \mathrm{G}(q)$, the *group of similarities* which is defined by the equation $\mathrm{G}(q) = \{\alpha \in k^* \mid \alpha q \simeq q\}$.
- The subgroup $\mathrm{Hyp}\,(\mathrm{A},\sigma) = \mathrm{Hyp}(q)$ which is $\langle \mathrm{N}_{E/k}\,(E^*)\ \mid q_E \simeq \mathbb{H}^r\rangle$.
- Finally $\mathrm{NK}^* = k^{*2}$.

Thus, the formula for $\mathrm{PSO}(q)/R$ is given by the following theorem.

Theorem 6.12 (Merkurjev, [Me98])**.** *Let q be a non-degenerate form of dim $2n$. Then there is a natural isomorphism*

$$\mathrm{PSO}(q)(k)/R \;\simeq\; \mathrm{G}(q)/k^{*2}\,\mathrm{Hyp}(q).$$

We do not present the proof here but offer a few lines of explanation about what induces the natural isomorphism in the formula in this case.

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & \mu_2 \arrow[r] \arrow[d] & \mathrm{SO}(q) \arrow[r] \arrow[d] & \mathrm{PSO}(q) \arrow[r] \arrow[d, "\simeq"] & 1 \\
1 \arrow[r] & \mathbb{G}_{\mathrm{m}} \arrow[r] \arrow[d, "\times 2"] & \mathrm{GO}^{+}(q) \arrow[r] \arrow[d, "\mu"] & \mathrm{PSO}(q) \arrow[r] & 1 \\
 & \mathbb{G}_{\mathrm{m}} \arrow[r, equal] \arrow[d] & \mathbb{G}_{\mathrm{m}} \arrow[d] & & \\
 & 1 & 1 & &
\end{tikzcd}$$

Figure 6.3: Relating $\mathrm{PSO}(q)/R$ and $\mathrm{G}(q)$

Look at the exact sequence $1 \to \mathbb{G}_{\mathrm{m}} \to \mathrm{GO}^{+}(q) \to \mathrm{PSO}(q) \to 1$. Since $\mathbb{G}_{\mathrm{m}}$ is H^1 trivial, $\mathrm{GO}^{+}(q)$ and $\mathrm{PSO}(q)$ are stably birational ([Me98], Lemma 1.1). Thus

$$\mathrm{PSO}(q)(k)/R \simeq \mathrm{GO}^{+}(q)(k)/R.$$

Now the multiplier map $\mu : \mathrm{GO}^{+}(q)(k) \to k^*$ induces the natural isomorphism in the formula.

6.5.2 Merkurjev's example

As one of the consequences of Theorem 6.12, the rationality of the absolutely simple adjoint group $\mathrm{PSO}\,(\mathrm{A}, \sigma)$ of type D_3 is investigated completely in ([Me96]). We only look at the case when A is split, namely when $G = \mathrm{PSO}(q)$

where q is a non-degenerate quadratic form of dim 6. By Theorem 2.4, its even Clifford algebra $\mathrm{C}_0(q)$ is a central simple algebra of degree 4 over Z, the discriminant extension of q.

Theorem 6.13 ([Me96], Thm 3)**.** *Let $G = \mathrm{PSO}(q)$ for q as above. Then*

1. *If* $\mathrm{disc}(q)$ *is trivial,* $\mathrm{PSO}(q)$ *is k-rational and hence R-trivial.*
2. *If* $\mathrm{disc}(q)$ *is not trivial,*
   (a) *If* $\mathrm{C}_0(q)$ *is not division,* $\mathrm{PSO}(q)$ *is k-stably rational and hence R-trivial.*
   (b) *If* $\mathrm{C}_0(q)$ *is division,* $\mathrm{PSO}(q)$ *is not R-trivial and hence not stably-rational.*

As this theorem indicates, the discriminant being non-trivial is a crucial assumption in manufacturing the non-rational adjoint group. Note that $q \in \mathrm{I}(k)$ as it has even dimension. Since q has non-trivial discriminant, we need $q \in \mathrm{I} \setminus \mathrm{I}^2$ to construct the non-rational group. And finally, the example is as follows :

- Let k be a field[4] such that it admits a quaternion algebra $Q = (a, b)$ which doesn't split over the bi-quadratic extension $L = k\left(\sqrt{c}, \sqrt{d}\right)$.
- Let $F = k(t)$.
- Define the quadratic form q over F to be $\langle ad, b, -ab, -c, -t, ct \rangle$.
- Then $\mathrm{PSO}(q)$ is not R-trivial and hence not F-stably rational.

A quick check shows that $\mathrm{disc}(q) = d$ is non-trivial. The Clifford algebra computation is less straight-forward but goes through and $\mathrm{C}_0(q)$ is indeed division.

[4] k could be a number field for instance

Gille's example

The next year, P. Gille in his paper ([Gille97]) investigated whether the triviality of discriminant was indeed necessary. And using Theorem 6.12, he produced a quadratic form q of dimension 8 and trivial discriminant over a characteristic 0 field k (of cohomological dimension 3) such that $\mathrm{PSO}(q)$ is not k-stably rational.

More precisely, he constructs a dimension 8, trivial discriminant quadatic form q as follows :

- D is a central division biquarternion algebra over k.
- ϕ is its associated Albert form[5] which represents -1.
- $a \in k^* \setminus k^{*2}$.
- q is the anisotropic part of $\phi \perp \langle\langle -a, t\rangle\rangle$ over the field $k((t))$.

He proved that $\mathrm{PSO}(q)$ is not R-trivial *provided that* $\mathrm{C}(V, q)$*, the full Clifford algebra of* q*, is still division.* Note that $q \in \mathrm{I}^2$ as it has trivial discriminant. Since the Clifford invariant of q is not trivial, $q \in \mathrm{I}^2 \setminus \mathrm{I}^3$.

We should also mention that questions about minimality of the dimension of q and cohomological dimension of k used in constructing the example are investigated thoroughly. For instance in the paper, Gille also showed that the dimension of the quadratic form has to be at least 8 and that the base field should have cohomological dimension at least 2 to be able to construct such an example.

[5] An Albert form associated to the biquaternion $(x, y) \otimes (z, w)$ is $\langle x, y, -xy, -z, -w, zw\rangle$

Year	Credits	Non-stably rational group
1954	Chevalley	Torus
1960s	Serre	Semisimple group (neither adjoint nor simply connected)
1976	Platonov	Simply connected group
1996	Merkurjev	Adjoint group $\mathrm{PSO}(q)$, $q \in \mathrm{I} \setminus \mathrm{I}^2$
1997	Gille	Adjoint group $\mathrm{PSO}(q)$, $q \in \mathrm{I}^2 \setminus \mathrm{I}^3$

Figure 6.4: A timeline

6.6 A natural question

The examples of non-rational adjoint groups discussed above yield quadratic forms q_1/k_1 and q_2/k_2 such that

> Merkurjev : $\dim(q_1)$ is even (i.e $q_1 \in \mathrm{I}(k_1)$) and $\mathrm{PSO}(q_1)$ is not k_1-stably rational.
>
> Gille : $\dim(q_2)$ is even, $\mathrm{disc}(q_2)$ is trivial (i.e $q_2 \in \mathrm{I}^2(k_2)$) and $\mathrm{PSO}(q_2)$ is not k_2-stably rational.

Recall that the dimension and discriminant are some of the *classical invariants* of quadratic forms taking values in the Galois cohomology groups $\mathrm{H}^i(k, \frac{\mathbb{Z}}{2\mathbb{Z}})$ for $0 \leq i \leq 2$. The Milnor conjectures give *successive* higher invariants for quadratic forms which determine the isomorphism class of a quadratic form in the Witt ring.

Thus one may be prompted to ask the following natural question.

Question 6.14. For each $n \in \mathbb{N}$, is there a quadratic form q_n defined over a field k_n such that $q_n \in \mathrm{I}^n(k_n)$, the n^{th} power of the fundamental ideal and $\mathrm{PSO}(q_n)$ is not k_n-stably rational?

Chapter 7

More examples of non-rational groups

'The central idea of poetry is the idea of guessing right, like a child.'

- G. K Chesterton, The Victorian Age in Literature

In this chapter we answer Question 6.14 and manufacture for each $n \in \mathbb{N}$, a quadratic form q_n defined over a field k_n (Theorem 7.9) such that

- $q_n \in \mathrm{I}^n(k_n)$, the n^{th} power of the fundamental ideal,
- $\mathrm{PSO}(q_n)$ is not k_n-stably rational.

In fact, we give a recursive construction to build q_{n+1}/k_{n+1} from q_n/k_n using Merkurjev's computations of the R-equivalence classes of adjoint classical groups (c.f. Theorem 6.12). Iterated Laurent-series fields come naturally into play and the fields k_n become very large in terms of cohomological dimension. The main reference is of course ([N1]) and ([Scharlau]) for facts from quadratic form theory.

7.1 Notations and Conventions

All fields considered in this chapter are assumed to have characteristic 0. Let $\mathrm{W}(k)$ denote the Witt ring of quadratic forms defined over k and $\mathrm{I}(k)$, the fundamental ideal of even dimensional forms. $P_n(k)$ is the set of isomorphism classes of anisotropic n-fold Pfister forms and $\mathrm{I}^n(k)$ denotes the n^{th} power of the fundamental ideal. Let us fix the convention that $\langle\langle a\rangle\rangle$ denotes the 1-fold Pfister form $\langle 1, a\rangle$. A generalized Pfister form is any scalar multiple of a Pfister form.

7.2 Strategy

We will in fact construct q_n/k_n such that $\mathrm{PSO}\,(q_n)\,(k_n)\,/R \neq \{1\}$. This will imply that these adjoint groups are not R-trivial and hence not k_n-stably rational. The recursive construction repeatedly uses Merkurjev's formula and is broadly as follows :

- Assume $q_n \in \mathrm{I}^n\,(k_n)$ and that $\mathrm{PSO}\,(q_n)\,(k_n)\,/R$ is non-trivial.
- Thus Theorem 6.12 implies there exists a $\lambda \in \mathrm{G}\,(q_n) \setminus \mathrm{Hyp}\,(q_n)\,k_n^{\times 2}$.
- Construct k_{n+1} to be a suitable iterated field of k_n.
- Construct $q_{n+1} \in \mathrm{I}^{n+1}\,(k_{n+1})$.
- Show $\lambda \in \mathrm{G}\,(q_{n+1})$.
- Show $\lambda \notin \mathrm{Hyp}\,(q_{n+1})\,k_{n+1}^{\times 2}$.
- Conclude by Theorem 6.12 again that $\mathrm{PSO}\,(q_{n+1})\,(k_{n+1})\,/R$ is non-trivial.

7.3 Lemmata

This section collects a list of lemmata which come in handy whilst constructing non-rational adjoint groups.

Lemma 7.1 (Odd extensions)**.** *Let q be a quadratic form over k. Let k'/k be an odd degree extension. Then,*

$$\mathrm{PSO}\left(q_{k'}\right)(k')/R = \{1\} \implies \mathrm{PSO}(q)(k)/R = \{1\}.$$

Proof. Suppose that $x \in \mathrm{G}(q)$.

Clearly $\mathrm{G}(q) \subseteq \mathrm{G}\left(q_{k'}\right) = \mathrm{Hyp}\left(q_{k'}\right) k'^{\times 2}$ as $\mathrm{PSO}\left(q_{k'}\right)(k')/R = \{1\}$.

The definition of Hyp groups and the transitivity of norms immediately yield the fact that $\mathrm{N}_{k'/k}\left(\mathrm{Hyp}\left(q_{k'}\right) k'^{\times 2}\right) \subseteq \mathrm{Hyp}(q)k^{\times 2}$.

If $2n+1$ is the degree of k' over k, it follows that $x^{2n+1} = \mathrm{N}_{k'/k}(x) \in \mathrm{Hyp}(q)k^{\times 2}$. Hence $x \in \mathrm{Hyp}(q)k^{\times 2}$. $\square$

Let p be a Pfister form over k. Its *pure-subform* $\tilde{p}$ is defined uniquely up to isometry via the property that $\tilde{p} \perp \langle 1 \rangle \simeq p$. The following useful result connects the values of pure-subforms and Pfister forms :

Lemma 7.2 ([Scharlau], Chap 4, Thm 1.4)**.** *If $\mathrm{D}(q)$ denotes the set of non-zero values represented by the quadratic form q, then, for $p \in P_n(k)$,*

$$b \in \mathrm{D}(\tilde{p}) \iff p \simeq \langle\langle b, b_2, \ldots, b_n \rangle\rangle,$$

for some $b_2, \ldots, b_n \in k^{\times}$.

The next lemma is a useful tool for converting an element which is a norm from two different quadratic extensions into a norm from a biquadratic extension of the base field up to squares.

Lemma 7.3 (Biquadratic-norm trick, [KLST], Lemma 1.4)**.** *If l_1 and l_2 are two quadratic extensions of a field l, then*

$$N_{l_1/l}\left(l_1^{\times}\right) \cap N_{l_2/l}\left(l_2^{\times}\right) = N_{l_1 \otimes_l l_2/l}\left((l_1 \otimes_l l_2)^{\times}\right) l^{\times 2}.$$

Lemma 7.4 (Folklore)**.** *Let $k(u)$ be a finite separable extension of k generated by u of degree $p^g h$ where p is a prime not dividing h and $g \geq 1$. Then there exist finite separable extensions $M_1/M_2/k$ such that the following conditions hold :*

1. *$k(u) \subset M_1$ and $M_1 = M_2(u)$.*
2. *$[M_1 : M_2] = p$ and $p \not| [M_1 : k(u)]$*

Proof. Let M/k be any finite Galois extension containing $k(u)$ and let S be any p-Sylow of $\mathrm{Gal}(M/k(u))$. Since $\mathrm{Gal}(M/k(u))$ is a subgroup of $\mathrm{Gal}(M/k)$, there is a p-Sylow subgroup T of $\mathrm{Gal}(M/k)$ containing S.

Let M^S and M^T denote the fixed fields of S and T in M respectively. Note that $M^S \supseteq M^T$ and since S and T are appropriate p-Sylow subgroups, we have $p \nmid [M^S : k(u)]$ and $p \nmid [M^T : k]$. Comparing degrees yields $[M^S : M^T] = p^g$. Also note that $u \notin M^T$ and $k(u) \subset M^S$.

In fact, $M^T(u) = M^S$ because $[M^S : M^T]$ and $[M^S : k(u)]$ are coprime.

S is a proper subgroup of its normalizer $N_T(S)$ because T is nilpotent and $S \neq T$. Thus, you can find a subgroup V such that $S \subseteq V \subseteq T$ and index of S in V is p. Set M_2 to be the fixed field of V in M and set $M_1 = M^S$.

Thus $M_1 = M_2(u)$ is of degree p over M_2 and satisfies the other conditions given in the Lemma.

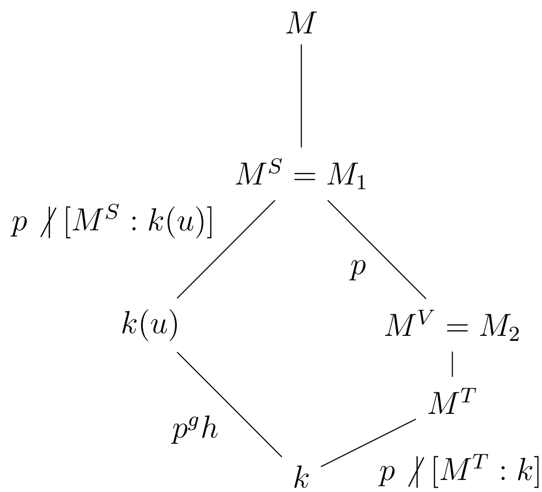

Figure 7.1: Diagram for the folklore lemma

$\square$

The following lemma tells us that Pfister forms yield R-trivial varieties. Note that in fact more is true, namely that $\mathrm{PSO}(q)$ is stably-rational for any generalized Pfister form q ([Me96], Prop 7).

Lemma 7.5. *If q is an n-fold Pfister form over a field k, then*

$$\mathrm{PSO}(q)(k)/R = \{1\}.$$

Proof. If q is isotropic, it is hyperbolic and hence $\mathrm{G}(q) = \mathrm{Hyp}(q) = k^{\times}$. Therefore assume without loss of generality that q is anisotropic.

Case $n = 1$ **:** Let $q = \langle 1, -a \rangle$. Then $\mathrm{G}(q) = N_{k(\sqrt{a})/k}(k(\sqrt{a})^{\times})$. Further, q splits over a finite field extension L of k if and only if a is a square in L. Therefore q_L splits if and only if $L \supseteq k(\sqrt{a}) \supseteq k$ and hence clearly $\mathrm{Hyp}(q) = \mathrm{G}(q)$.

General case : Recall that Pfister forms are round, that is $\mathrm{D}(q) = \mathrm{G}(q)$ for any Pfister form q. Let $\tilde{q}$ be the pure-subform of q. If $b \in \mathrm{D}(\tilde{q}) \subseteq \mathrm{D}(q)$, then by Lemma 7.2

$$b \in \mathrm{D}(\langle 1, b \rangle) = \mathrm{Hyp}(\langle 1, b \rangle)\, k^{\times 2} \subseteq \mathrm{Hyp}(q) k^{\times 2}.$$

Note that any $x \in \mathrm{G}(q) = \mathrm{D}(q)$ can be written (up to squares from $k^{\times}$) as either b or $1 + b$ for some $b \in \mathrm{D}(\tilde{q})$. Since $x = b \in \mathrm{D}(\tilde{q})$ has just been taken care of, it is enough to note that for $b \in \mathrm{D}(\tilde{q})$,

$$1 + b \in \mathrm{D}(\langle 1, b \rangle) \subseteq \mathrm{Hyp}(q) k^{\times 2}.$$

□

7.4 Comparison of some Hyp groups

Let q be an anisotropic quadratic form over a field k of characteristic 0. Let p be an anisotropic Pfister form defined over k and let $Q = q \perp tp$ over the field of Laurent series $K = k((t))$. Note that K is a complete discrete valued field with uniformizing parameter t and residue field k. Recall the exact sequence in Witt groups :

$$0 \to \mathrm{W}(k) \xrightarrow{Res} \mathrm{W}(K) \xrightarrow{\delta_{2,t}} \mathrm{W}(k) \to 0,$$

where Res is the restriction map and $\delta_{2,t}$ denotes the second residue homomorphism with respect to the parameter t.

Remark. Q is anisotropic and $\dim(Q) > \dim(p)$.

This can be shown with the aid of the above exact sequence. Let the anisotropic part of Q be $Q_{an} \simeq q_1 \perp tq_2$ for quadratic forms q_i defined over k. Then each q_i is anisotropic. The following equality in $\mathrm{W}(k)$ is in fact an isometry because the forms are anisotropic :

$$\delta_{2,t}(Q) = p = q_2.$$

This immediately implies $q \simeq q_1$. The inequality between dimensions of Q and p follows immediately.

Proposition 7.6. $\mathrm{Hyp}(Q)K^{\times 2} \subseteq \mathrm{Hyp}\,(q_K)\,K^{\times 2}$ *if* $\mathrm{PSO}(q)(k)/R \neq \{1\}$.

Proof. Let L/K be a finite field extension which splits Q. There is a unique extension of the discrete valuation on K to L which makes L into a complete discrete valued field. Let l denote the residue field of L. Since the characteristic of k is 0, $k \subseteq K$ and $l \subseteq L$. Let K_{nr} denote the maximal non-ramified extension of K in L and π be a uniformizing parameter of L. Let $f = [l : k]$, the degree of the residue field extensions and e be the ramification index of L/K. Let v_X denote the corresponding valuation on fields $X = K, K_{nr}, L$ and O_X, the corresponding discrete valuation rings.

Since L/K_{nr} is totally ramified, the minimal polynomial of π (which is also its characteristic polynomial) over K_{nr} is an *Eisenstein* polynomial $x^e + a_{e-1}x^{e-1}+\ldots+a_1x+a_0$ in $K_{nr}[x]$, where $v_{K_{nr}}(a_0) = 1$ and $v_{K_{nr}}(a_i) \geq 1 \; \forall \, 1 \leq i \leq e-1$ ([CF67], Chap 1, Sec 6, Thm 1). Note that $N_{L/K_{nr}}(\pi) = (-1)^e a_0$.

$K_{nr} = l((t))$ and $L = l((\pi))$ ([Serre95], Chap 2, Thm 2). Let $a_0 = -ut(1 + u_1t + \ldots)$ in $O_{K_{nr}} = l[[t]]$. By Hensel's lemma, $1 + u_1t + \ldots = w^2$ for some w in K_{nr}. The relation given by the Eisenstein polynomial can be rewritten by applying Hensel's lemma again as follows :

$$\pi^e = utv^2, u \in l^\times, v \in L^\times.$$

Hence the norm of π can be computed up to squares. That is,

$$N_{L/K}(\pi) = N_{K_{nr}/K}((-1)^e a_0) \in (-1)^{ef}(-t)^f N_{l/k}(u) K^{\times 2}.$$

The problem is subdivided into two cases depending on the parity of the ramification index e of L/K.

Case I : e is odd

We show that L also splits q in this case. Let $\delta_{2,\pi} : \mathrm{W}(L) \to \mathrm{W}(l)$ be the second Milnor residue map with respect to the uniformizing parameter π chosen above. Note that $Q_L = q + \pi up$ in $\mathrm{W}(L)$. Then

$$\begin{aligned} Q_L = 0 &\implies \delta_{2,\pi}(Q) = 0 \in \mathrm{W}(l) \\ &\implies up = 0 \in \mathrm{W}(L) \\ &\implies q = 0 \in \mathrm{W}(L). \end{aligned}$$

Case II : e is even

Now $Q_L = q + up = 0$ in $\mathrm{W}(L)$. Since any element of $L^\times$ is of the form $\alpha\pi b^2$ or αb^2 for some $\alpha \in l^\times$ and $b \in L$, the norm computation of π done before yields the following :

$$N_{L/K}\left(L^\times\right) \subseteq \langle N_{l/k}(u)(-t)^f\rangle K^{\times 2}.$$

So it is enough to show that f is even and $N_{l/k}(u)$ is in $\mathrm{Hyp}(q)\, k^{\times 2}$.

Claim : f is even.
If f is odd, then $\mathrm{PSO}(q_l)(l)/R \neq \{1\}$ by Lemma 7.1. But $q_l = -up$ is a form similar to a Pfister form. Hence by Lemma 7.5, $\mathrm{PSO}(q_l)(l)/R = \{1\}$ which is a contradiction.

Claim : $N_{l/k}(u) \in \mathrm{Hyp}(q)\, k^{\times 2}$.

Look at $l \supseteq k(u) \supseteq k$. If $[l : k(u)]$ is even, then $N_{l/k}(u) = N_{k(u)/k}\left(u^{[l:k(u)]}\right) \in k^{\times 2}$ which proves the claim.

Otherwise $r : \mathrm{W}(k(u)) \to \mathrm{W}(l)$ is injective and hence $q+up = 0$ in $\mathrm{W}(k(u))$. It remains to show that $N_{k(u)/k}(u) \in \mathrm{Hyp}(q)\, k^{\times 2}$.

Suppose that $[k(u) : k]$ is odd. Then Lemma 7.1 implies that $\mathrm{PSO}\left(q_{k(u)}\right)/R \neq \{1\}$. On the other hand, $q_{k(u)}$ is similar to Pfister form $p_{k(u)}$. This contradicts Lemma 7.5. Therefore $[k(u) : k]$ is even.

Let $[k(u) : k] = 2^g h$ where h is odd and $g \geq 1$. Lemma 7.4 gives us a quadratic extension $M_1 = M_2(u)$ over M_2 such that M_1 is an odd extension of $k(u)$.

Since $[M_1 : k(u)]$ is odd, there is a $w \in k^\times$ such that

$$N_{M_1/k}(u) = N_{k(u)/k}\left(N_{M_1/k(u)}(u)\right) = N_{k(u)/k}(u)w^2.$$

Hence it suffices to show that $N_{M_1/k}(u) \in \mathrm{Hyp}(q)k^{\times 2}$. Using transitivity of norms and the definition of Hyp groups, showing $N_{M_1/M_2}(u) \in \mathrm{Hyp}\left(q_{M_2}\right) {M_2}^{\times 2}$ proves the claim.

Let $\eta := N_{M_1/M_2}(u)$. By using Scharlau's transfer and Frobenius reciprocity ([Scharlau], Chap 2, Lemma 5.8 and Thm 5.6),

$$p \otimes \langle 1\rangle = -\langle u\rangle q \in \mathrm{W}\left(M_1\right) \implies p \otimes \langle 1, -\eta\rangle = 0 \in \mathrm{W}\left(M_2\right).$$

Hence $\eta \in \mathrm{G}\left(p_{M_2}\right) = \mathrm{D}\left(p_{M_2}\right)$ since p is a Pfister form.

Let s be the pure subform associated with p_{M_2}. We can assume (up to squares from M_2) that $\eta = b$ or $1 + b$ for some $b \in \mathrm{D}(s)$. In either case, $\eta \in N_{M_2\left(\sqrt{-b}\right)/M_2}\left(\left(M_2\left(\sqrt{-b}\right)\right)^{\times}\right)$. By Lemma 7.2, $p = \langle\langle b, \ldots\rangle\rangle$. Note that if $-b$ is already a square in M_2, then the above reasoning shows that q splits over M_1 which shows that $\eta \in \mathrm{Hyp}\left(q_{M_2}\right) M_2^{\times 2}$. If $-b$ is not a square, then p splits in $M_2\left(\sqrt{-b}\right)$ and hence $q = -up$ splits in $M_1\left(\sqrt{-b}\right)$.

The introduction of subfield M_2 is useful because the biquadratic norm trick can be used! More precisely, since

$$\eta \in N_{M_2\left(\sqrt{-b}\right)/M_2}\left(\left(M_2\left(\sqrt{-b}\right)\right)^{\times}\right) \cap N_{M_1/M_2}\left(M_1^{\times}\right),$$

Lemma 7.3 shows that η is up to squares a norm from $M_1\left(\sqrt{-b}\right)$ and $M_1\left(\sqrt{-b}\right)$ splits q. Thus $\eta \in \mathrm{Hyp}\left(q_{M_2}\right) M_2^{\times 2}$ as claimed. □

Proposition 7.7. $\mathrm{Hyp}\,(q_K)\,K^{\times 2} \subseteq \mathrm{Hyp}\,(q)\,K^{\times 2}$.

Proof. Again using the exact sequence of Witt groups, it is clear that if q is split by a finite field extension L of K, then it is also split by l, the residue field of L. Thus $\mathrm{Hyp}\,(q_K)$ is generated by $\mathrm{N}_{L/K}\,(L^{\times})$ where L runs over finite unramified extensions of K which split q. By Springer's theorem, $[l : k]$ has to be even. And characteristic of $k = 0$ implies that $L \simeq l((t))$. To conclude, it is enough to observe that

$$N_{l((t))/k((t))}\,(l((t)))^{\times} \subseteq N_{l/k}(l^{\times})K^{\times 2}.$$

□

7.5 A recursive procedure

We are ready to spell out our recursive procedure. We start with slightly stronger hypotheses than what was mentioned in the strategy in Section 7.2. Note that all fields discussed in this chapter henceforth will have characteristic 0. Let L be a field, $n \in \mathbb{N}$, $\lambda \in L$, and ϕ be a quadratic form over L. We say that (n, λ, L, ϕ) *has property* $\star$ if the following holds :

- ϕ is an anisotropic quadratic form over L in $\mathrm{I}^n\,(L)$,
- The scalar $\lambda \in L$ is in $\mathrm{G}\,(\phi)$ but not in $\mathrm{Hyp}\,(\phi)\,L^{\times 2}$,
- There exists a decomposition of ϕ into a sum of generalized n-fold Pfister forms in the Witt ring $\mathrm{W}\,(L)$, each of which is annihilated by $\langle 1, -\lambda\rangle$.

More precisely, in $\mathrm{W}(L)$,

$$\phi = \sum_{i=1}^{m} \alpha_i p_{i,n}, \text{where } \alpha_i \in L^\times, p_{i,n} \in P_n(L),$$

$$\langle 1, -\lambda \rangle \otimes p_{i,n} = 0 \ \forall \ i.$$

Assume that (n, λ, k_n, q_n) has property $\star$ with $q_n = \sum_{i=1}^{m} \alpha_i p_{i,n}$ for $p_{i,n} \in P_n(k_n)$ and $\alpha_i \in k_n^\times$ such that each $p_{i,n}$ is annihilated by $\langle 1, -\lambda \rangle$. Let K_0 denote the field k_n. Define the fields K_i recursively as follows :

$$K_i := K_{i-1}((t_i)) \ \forall \ 1 \leq i \leq m.$$

Let Q_0 denote the quadratic form q_n defined over K_0. Define the quadratic forms Q_i over fields K_i recursively as follows :

$$Q_i := Q_{i-1} \perp t_i p_{i,n} \ \forall \ 1 \leq i \leq m.$$

Note that $\lambda \in \mathrm{G}(Q_i)$ for each $1 \leq i \leq m$ since $\lambda \in \mathrm{G}(q_n)$ and $\mathrm{G}(p_{i,n})$ for each i.

Theorem 7.8. *Let (n, λ, k_n, q_n) have property $\star$. Then for (K_m, Q_m) as above, the following hold :*

1. $Q_m \in \mathrm{I}^{n+1}(K_m)$
2. $\lambda \in \mathrm{G}(Q_m) \setminus \mathrm{Hyp}(Q_m) {K_m}^{\times 2}$. *In particular,* $\mathrm{PSO}(Q_m)$ *is not K_m-stably rational.*
3. $(n+1, \lambda, K_m, Q_m)$ *has property $\star$.*

Proof. In the Witt ring $\mathrm{W}(K_m)$,

$$\begin{aligned} Q_m &= q_n + \sum_{i=1}^{m} t_i p_{i,n} \\ &= \sum_{i=1}^{m} \alpha_i p_{i,n} + t_i p_{i,n} \\ &= \sum_{i=1}^{m} p_{i,n} \otimes \langle \alpha_i, t_i \rangle \\ &\in \mathrm{I}^n \, \mathrm{I} \subseteq \mathrm{I}^{n+1}(K_m) \,. - - - (1) \end{aligned}$$

We now prove by induction that $\lambda \in \mathrm{G}(Q_i) \setminus \mathrm{Hyp}(Q_i) K_i^{\times 2}$ for each $i \leq m$.

The base case $i = 0$ is given, namely for the pair (k_n, q_n). Assume as induction hypothesis that this statement holds for all $i \leq j$. The proof of the statement for $i = j + 1$ follows :

The following notations are introduced for convenience.

$$\begin{aligned} (Q, K) &:= (Q_{j+1}, K_{j+1}) \,. \\ (q, k) &:= (Q_j, K_j) \,. \\ t &:= t_{j+1}. \\ p &:= p_{j+1,n} \in P_n(k) \,. \end{aligned}$$

Thus $Q = q + tp \in \mathrm{W}(K)$.

Since $\lambda \in k^{\times}$ and not in $\mathrm{Hyp}(q)k^{\times 2}$, it is not in $\mathrm{Hyp}(q)K^{\times 2}$. By Proposition 7.7, $\lambda \notin \mathrm{Hyp}(q_K)K^{\times 2}$ and by Proposition 7.6, $\lambda \notin \mathrm{Hyp}(Q)K^{\times 2}$. By construction, $\lambda \in \mathrm{G}(Q)$ as $\lambda \in \mathrm{G}(p) \cap \mathrm{G}(q)$. Hence $\lambda \in \mathrm{G}(Q) \setminus \mathrm{Hyp}(Q)K^{\times 2}$.

It is clear that $(n + 1, \lambda, K_m, Q_m)$ has property $\star$ by Equation 1. $\square$

7.6 Conclusion

Theorem 7.9. *For each n, there exists a quadratic form q_n defined over a field k_n such that $q_n \in \mathrm{I}^n(k_n)$ and $\mathrm{PSO}(q_n)$ is not k_n-stably rational.*

Proof. Let q be an anisotropic quadratic form of dimension 6 over a field F of characteristic 0. If the discriminant of q is not trivial and $\mathrm{C}_0(q)$ is a division algebra, then by ([Me96], Thm 3) there exists a field extension E of F such that

$$\mathrm{PSO}(q)(E)/R \neq \{1\}.$$

Define $k_1 := E$, $q_1 := q_E$ and pick a $\lambda \in \mathrm{G}(q_1) \setminus \mathrm{Hyp}(q_1)\, k_1^{\times 2}$.

We can write $q_1 = \sum_{i=1}^{r} \alpha_i f_i$ in the Witt ring $\mathrm{W}(k_1)$ for some scalars $\alpha_i \in k_1^{\times}$ and 1-fold Pfister forms f_i which are annihilated by $\langle 1, -\lambda \rangle$([Scharlau], Chap 2, Thm 10.13).

Therefore Theorem 7.8 can be applied repeatedly to produce pairs (k_n, q_n) such that

$$\mathrm{PSO}(q_n)(k_n)/R \neq \{1\}.$$

This implies that $\mathrm{PSO}(q_n)$ is not k_n-stably rational. □

Chapter 8

On norm principles

'Is that sort of stuff any use to you?'

- John Mortimer, Trials of Rumpole

Norm principles examine the behaviour of the images of group morphisms from an algebraic group into a commutative one with respect to the *norm* map. The classical norm principles attributed to Scharlau and Knebusch can be reformulated as a special case of norm principles for certain group homomorphisms. Further the Knebusch norm principle can be derived from Gille and Merkurjev's norm principle which is stated for more general R-trivial groups ([Gille93], [Me95]). Thus the study of norm principles is a close cousin to the study of rationality questions of group varieties. However as the paper of Merkurjev and Barquero shows, norm principles for certain classical groups hold without any condition whatsoever on their rationality ([BM]). In this chapter, we define what constitutes a norm principle for an algebraic group and examine some norm principles that have been shown to hold, which will prove a crucial ingredient in the second main result of this disseration.

8.1 What is a norm principle?

Let T be a commutative k-algebraic group and let L/k denote a finite separable field extension. Then one can define the *norm homomorphism* $\mathrm{N}_{L/k} : T(L) \to T(k)$ which sends $t \rightsquigarrow \prod_\gamma \gamma(t)$ where γ runs over cosets of $\mathrm{Gal}\,(k^{sep}/L)$ in $\mathrm{Gal}\,(k^{sep}/k)$.

If $T = \mathbb{G}_m$, then $\mathrm{N}_{L/k} : T(L) \to T(k)$ is precisely the usual norm $\mathrm{N}_{L/k} : L^* \to k^*$.

Now let G be a k-algebraic group and let $f : G \to T$ be an algebraic homomorphism defined over k.

$$\begin{array}{ccc} G(L) & \xrightarrow{f(L)} & T(L) \\ & & \Big\downarrow \mathrm{N}_{L/k} \\ G(k) & \xrightarrow{f(k)} & T(k) \end{array}$$

We say that the *norm principle* holds for $f : G \to T$ if for all separable field extensions L/k,

$$\mathrm{N}_{L/k}(\mathrm{Image}\, f(L)) \subseteq \mathrm{Image}\, f(k).$$

That is, we say that the norm principle holds for $f : G \to T$ if given any separable field extension L/k and any $t \in T(L)$ such that $t \in (\mathrm{Image}\, f(L) : G(L) \to T(L))$, then $\mathrm{N}_{L/k}(t) \in (\mathrm{Image}\, f(k) : G(k) \to T(k))$. Note that the norm principle holds for any algebraic group homomorphism between abelian groups.

We say that the *weak norm principle* holds for $f : G \to T$ if given any separable field extension L/k and any $t \in T(k)$ such that $t \in (\mathrm{Image}\, f(L) : G(L) \to T(L))$, then $t^{[L:k]} = \mathrm{N}_{L/k}(t) \in (\mathrm{Image}\, f(k) : G(k) \to T(k))$. It is clear that if the norm principle holds for f, then so does the weak norm principle.

8.2 Classical examples

Reduced norms

Let A/k be a central simple algebra and let L/k be a separable field extension. Further let $\lambda \in L^*$ such that $\lambda \in \mathrm{Nrd}_L\left((A \otimes_k L)^*\right)$. Then it is a classical result that $\mathrm{N}_{L/k}(\lambda)$ is again a reduced norm from A/k.

This can be easily seen from the following characterization of reduced norms of a central simple algebra

$$\mathrm{Nrd}_k(A^*) = \langle \mathrm{N}_{F/k}(F^*) \mid A \otimes_k F = 0 \in \mathrm{Br}(F) \rangle.$$

We can restate this in our context by saying that norm principle holds for the reduced norm morphism

$$\mathrm{Nrd} : \mathrm{GL}_1(A) \to \mathbb{G}_m.$$

Scharlau's norm principle

Let q be a regular quadratic form over k and let L/k be a separable field extension. Further let $\lambda \in L^*$ such that $\lambda \in \mathrm{G}(q_L)$, the group of similarities. Then Scharlau's norm principle states that that $\mathrm{N}_{L/k}(\lambda) \in \mathrm{G}(q)$ ([Lam], Thm 4.3).

One can see this as follows : Look at $F := k(\lambda) \subseteq L$. If $[L : F]$ is even, then $\mathrm{N}_{L/k}(\lambda) \in k^{*2}$ and hence clearly it is in $\mathrm{G}(q)$.

If $[L : F]$ is odd, then since $\mathrm{W}(F) \hookrightarrow \mathrm{W}(L)$, we have that $\lambda q_F \simeq q_F$. Also $\mathrm{N}_{k(\lambda)/k} \simeq \mathrm{N}_{L/k}(\lambda) \mod k^{*2}$. Hence we are reduced to showing the norm principle for the simple extension $L = k(\lambda)$, which can be done by using the so called *Scharlau transfer* and *Frobenius reciprocity*.

We can restate Scharlau's norm principle in our context by saying that norm principle holds for the multiplier map

$$\mu : \mathrm{GO}(q) \to \mathbb{G}_m.$$

Knebusch's norm principle

Let q be a regular quadratic form over k and let L/k be a separable field extension. Further let $\lambda \in L^*$ such that λ is a *spinor norm.* Then Knebusch's norm principle states that that $\mathrm{N}_{L/k}(\lambda)$ is a spinor norm as well ([Lam], Remark 5.13).

We can restate Knebusch's norm principle in our context by saying that norm principle holds for the spinor norm map

$$\underline{\mu} : \Gamma^+(q) \to \mathbb{G}_m.$$

8.3 More norm principles

The norm principles of Gille and Merkurjev are stated in general for R-trivial elements.

Theorem 8.1 (Gille, [Gille93]). *Let $1 \to \mu \to \tilde{G} \to G \to 1$ be an isogeny of semi-simple algebraic groups over a characteristic 0 field k and $\mathrm{N}_{L/k} : \mathrm{H}^1(L, \mu) \to \mathrm{H}^1(k, \mu)$ be the induced norm map for a field extension L/k.*

$$\begin{tikzcd} RG(L) \arrow[r, "\delta(L)"] & \mathrm{H}^1(L, \mu) \arrow[d, "\mathrm{N}_{L/k}"] \\ RG(k) \arrow[r, "\delta(k)"] & \mathrm{H}^1(k, \mu) \end{tikzcd}$$

Let $RG(L)$ (resp. $RG(k)$) denote the elements of $G(L)$ (resp $G(k)$) which are R-equivalent to the identity. Then

$$\mathrm{N}_{L/k}\left(\mathrm{Image}\,\delta(L) : RG(L) \to \mathrm{H}^1(L,\mu)\right) \subseteq \left(\mathrm{Image}\,\delta(k) : RG(k) \to \mathrm{H}^1(k,\mu)\right).$$

Theorem 8.2 (Merkurjev's norm principle, [Me95], Thm 3.9)**.** *Let G_1, G be connected reductive k-groups and let T be a k-torus which fit into the exact sequence $1 \to G_1 \to G \xrightarrow{f} T \to 1$. Then*

$$N_{L/k}\left(\mathrm{Image}\,f(L) : RG(L) \to T(L)\right) \subseteq \left(\mathrm{Image}\,f(k) : RG(k) \to T(k)\right).$$

Thus for instance if G is k-rational, then norm principle always holds for $f : G \to T$. The classical norm principle for reduced norms and Knebusch norm principle can therefore be recovered from the above theorem by noting that the group $\mathrm{GL}_1(A)$ and $\Gamma^+(q)$ are k-rational. Scharlau's norm principle is however not recovered since $\mathrm{GO}^+(q)$ needn't be rational always.

The most relevant norm principle for us is however the following one proved by Merkurjev and Barquero for classical reducive groups of certain types

Theorem 8.3 ([BM], Thm 1.1)**.** *Let G be a k-reductive group and T, a commutative k-group. Assume further that the Dynkin diagram of G does not contain connected components $D_n, n \geq 4$, E_6 or E_7. Then the norm principle holds for any k-group homomorphism $G \to T$.*

Note that any map $f : G \to T$ for G and T as above factors as follows :

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "f"'] & G/[G,G] \arrow[d, dashed] \\ & T \end{tikzcd}$$

Thus if the norm principle holds for the canonical map $\pi : G \to G/[G,G]$, it holds for f too. This is simply because $G/[G,G]$ is abelian and hence the norm principle trivially holds for $G/[G,G] \to T$. Thus their paper investigates norm principles for π.

Using several interesting algebraic group constructions, the authors manage to reduce the problem to norm principles of certain reductive groups called *envelopes* $\widehat{G}$ of $[G,G]$. These techniques are extremely useful to us for they can be adapted to answer a question of Serre for many connected reductive groups as shown in the next chapter.

Chapter 9

On a question of Serre

'Mathematics is letting the principles do the work for you so that you do not have to do the work for yourself.'
- George Polya

Let k be a field of characteristic not 2. In this chapter, we give a positive answer to Serre's injectivity question for any smooth connected reductive k-group whose Dynkin diagram contains connected components only of type A_n, B_n or C_n (Theorem 9.8). We do this by relating Serre's question to the norm principles proved by Barquero and Merkurjev ([BM]) and use and extend Jodi Black's result on Serre's question for adjoint classical groups ([Black]). We also investigate Serre's question for quasi-split reductive k-groups (Theorem 9.11). The main reference is ([N2])

9.1 Serre's question

Let k be a field and let G be smooth connected linear algebraic group over k. Let X denote a *principal homogeneous space* under G over k, i.e. a k-variety with a G-action such that $X_{k^{sep}}$ equipped with its $G_{k^{sep}}$-action is isomorphic to $G_{k^{sep}}$. Note that then $X\left(k^{sep}\right)$ is a principal homogeneous space under $G\left(k^{sep}\right)$ as defined in Section 5.3.1.

A *zero cycle* on X is any element of the free abelian group on closed points of X. We may associate to any zero cycle $z = \sum n_i x_i$ (where $n \in \mathbb{Z}$ and x_i are closed points of X), its *degree* which is defined to be

$$\deg(z) = \sum n_i \left[k(x_i) : k\right],$$

where $k\,(x_i)$ denotes the residue field of x_i.

A k-rational point z of X is simply a point in $X(k)$ (i.e. a closed point with residue field k). Clearly k-rational points are zero cycles of degree one. Serre's question, which is open in general, asks whether the converse is true, namely

Question 9.1 (Serre, [Serre95], p. 233). Let G be any connected linear algebraic group over a field k and let X be a principal homogeneous space under G over k. If X admits a zero cycle of degree one, does X have a k-rational point?

There is a one-to-one correspondence between the first cohomology group $\mathrm{H}^1(k, G)$ and the set of isomorphism classes of principal homogeneous spaces under G over k. Under this bijection, the trivial class in $\mathrm{H}^1(k, G)$ corresponds to the class of principal homogeneous spaces under G over k with rational points. (Thm 5.1 or [Serre97], Chapter I, Proposition 33).

Now if $z = \sum n_i x_i$ is a zero cycle of degree one on a principal homogeneous space X under G over k, then $[X] = 1 \in \mathrm{H}^1\left(k(x_i), G\right)$. Since $\deg(z) = 1$, we have that $\gcd\left[k(x_i) : k\right] = 1$.

The question whether X admits a k-rational point is equivalent to asking whether $[X] = 1 \in \mathrm{H}^1\left(k, G\right)$. Thus Serre's question can be restated in the language of Galois cohomology as follows :

Question 9.2. Let G be any connected linear algebraic group over a field k. Let $L_1, L_2, \ldots, L_r$ be finite field extensions of k of degrees $d_1, d_2, \ldots, d_r$ respectively such that $\gcd_i(d_i) = 1$. Then is the following sequence exact?

$$1 \to \mathrm{H}^1(k, G) \to \prod_{i=1}^{r} \mathrm{H}^1(L_i, G).$$

9.1.1 Known results

Let us look at $G = \mathrm{PGL}_n$. The first cohomology group $\mathrm{H}^1(k, G)$ classifies central simple algebras of degree n. The classical result that the index of a central simple algebra divides the degrees of its splitting fields answers Serre's question affirmatively for this group PGL_n.

Let q be a regular quadratic form over k and let $G = \mathrm{O}(q)$. The first cohomology group $\mathrm{H}^1(k, G)$ classifies regular quadratic forms q' with dimension equal to $\dim(q)$. Then Springer's theorem for quadratic forms answers it affirmatively for this (albeit sometimes disconnected) group.

This is because if $z = \sum n_i x_i$ is a zero cycle of degree one corresponding to a quadratic form q', then necessarily some $[k(x_i) : k]$ is odd. Thus we are given that q' becomes hyperbolic over $k(x_i)$. Springer's theorem asserts that therefore q' itself is hyperbolic.

More generally, let A/K be a central simple algebra with involution σ such that $K^\sigma = k$. That is $K = k$ if σ is of the first kind and K/k is a quadratic extension if σ is of the second kind. Bayer-Lenstra's theorem ([BL]) asserts that for any odd extension L/k, the following morphism between cohomology sets of the group of isometeries of (A, σ) is exact

$$1 \to \mathrm{H}^1(k, \mathrm{U}(\mathrm{A}, \sigma)) \to \mathrm{H}^1(L, \mathrm{U}(\mathrm{A}, \sigma)).$$

This immediately implies that Serre's question has a positive answer for $G = \mathrm{U}(\mathrm{A}, \sigma)$.

Jodi Black answers Serre's question positively for absolutely simple simply connected and adjoint k-groups of classical type.

Theorem 9.3 ([Black], Thm 0.2)**.** *Let k be a field of characteristic different from 2 and let J be an absolutely simple algebraic k-group which is not of type E_8 and which is either a simply connected or adjoint classical group or a quasi-split exceptional group. Then Serre's question has a positive answer for J.*

9.2 Preliminaries

We work over the base field k of characteristic not 2. By a k-group, we mean a smooth connected linear algebraic group defined over k. And mostly, we will restrict ourselves to reductive groups. We say that a k-group G satisfies SQ if Serre's question has a positive answer for G. In this section, we recall the reduction to the characteristic 0 case and list a few useful lemmata.

9.2.1 Reduction to characteristic 0

Let G be a connected reductive k-group whose Dynkin diagram contains connected components only of type A_n, B_n, C_n or (non-trialitarian) D_n. Without loss of generality we may assume that k has characteristic 0 ([Gille10(2)], Pg 47). We give a sketch of the reduction argument for the sake of completeness.

Suppose that the characteristic of k is $p > 0$. Let $L_1, L_2, \ldots, L_r$ be finite field extensions of k of degrees $d_1, d_2, \ldots, d_r$ respectively such that $\gcd_i(d_i) = 1$.

Let ξ be an element in the kernel of

$$\mathrm{H}^1(k, G) \to \prod_{i=1}^{r} \mathrm{H}^1(L_i, G).$$

By a theorem of Gabber, Liu and Lorenzini ([GLL], Thm 9.2) which was pointed out to us by O. Wittenberg, we note that any torsor under a smooth group scheme G/k which admits a zero-cycle of degree 1 also admits a zero-cycle of degree 1 whose support is étale over k. Thus without loss of generality we can assume that the given coprime extensions L_i/k are in fact separable.

By ([Maclane], Thm 1 & 2), there exists a complete discrete valuation ring R with residue field k and fraction field K of characteristic zero. Let S_i denote the corresponding étale extensions of R with residue fields L_i and fraction fields K_i.

There exists a smooth R-group scheme $\tilde{G}$ with special fiber G and connected reductive generic fiber $\tilde{G}_K$. Now given any torsor $t \in \mathrm{H}^1(k, G)$, there exists a torsor $\tilde{t} \in \mathrm{H}^1_{\text{ét}}(R, \tilde{G})$ specializing to t which is unique up to isomorphism. This in turn gives a torsor $\tilde{t}_K$ in $\mathrm{H}^1(K, \tilde{G}_K)$ by base change, thus defining a map $i_k : \mathrm{H}^1(k, G) \to \mathrm{H}^1(K, \tilde{G}_K)$ ([GMS], Pg 29). It clearly sends the trivial element to the trivial element. The map i also behaves well with the natural restriction maps, i.e., it fits into the following commutative diagram :

$$\begin{array}{ccc}
\mathrm{H}^1(k, G) & \xrightarrow{i_k} & \mathrm{H}^1(K, \tilde{G}_K) \\
\downarrow & & \downarrow \\
\prod \mathrm{H}^1(L_i, G) & \xrightarrow{\prod i_{L_i}} & \prod \mathrm{H}^1(K_i, \tilde{G}_K).
\end{array}$$

Let $\tilde{\xi}$ denote the torsor in $\mathrm{H}^1_{\text{ét}}(R, \tilde{G})$ corresponding to ξ as above. Therefore $\tilde{\xi}_K := i_k(\xi)$ is in the kernel of

$$\mathrm{H}^1(K, \tilde{G}_K) \to \prod_{i=1}^{r} \mathrm{H}^1(K_i, \tilde{G}_K).$$

Suppose that $\tilde{G}_K$ satisfies SQ. Then $\tilde{\xi}_K$ is trivial. However by ([Nisnevich]), the natural map $\mathrm{H}^1_{\text{ét}}(R, \tilde{G}) \to \mathrm{H}^1(K, \tilde{G}_K)$ is injective and hence $\tilde{\xi}$ is trivial in $\mathrm{H}^1_{\text{ét}}(R, \tilde{G})$. This implies that its specialization, ξ, is trivial in $\mathrm{H}^1(k, G)$.

Thus from here on, we assume that the base field k has characteristic 0.

9.2.2 Lemmata

Lemma 9.4. *Let k-groups G and H satisfy SQ. Then $G \times_k H$ also satisfies SQ.*

Proof. Let L_i/k be a field extension. Then the map $\mathrm{H}^1(k, G \times_k H) \to \mathrm{H}^1(L_i, G \times_k H)$ is precisely the product of the maps $\mathrm{H}^1(k, G) \to \mathrm{H}^1(L_i, G)$ and $\mathrm{H}^1(k, H) \to \mathrm{H}^1(L_i, H)$. This immediately shows that if G and H satisfy SQ, so does $G \times_k H$. $\square$

Lemma 9.5. *Let $1 \to Q \to H \to G \to 1$ be a central extension of a k-group G by a quasi-trivial torus Q. Then H satisfies SQ if and only if G satisfies SQ.*

Proof. Since Q is quasi-trivial, $\mathrm{H}^1(L, Q) = \{1\}\ \forall\ L/k$. From the long exact sequence in cohomology, we have the following commutative diagram.

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{H}^1(k, H) \arrow[r] \arrow[d] & \mathrm{H}^1(k, G) \arrow[r, "\delta_k"] \arrow[d] & \mathrm{H}^2(k, Q) \arrow[d] \\
1 \arrow[r] & \prod \mathrm{H}^1(L_i, H) \arrow[r] & \prod \mathrm{H}^1(L_i, G) \arrow[r, "\prod \delta_{L_i}"] & \prod \mathrm{H}^2(L_i, Q)
\end{tikzcd}$$

From the above diagram, it is clear that if G satisfies SQ, so does H.

Conversely, assume that H satisfies SQ. Let $a \in \mathrm{H}^1(k,G)$ become trivial in $\prod \mathrm{H}^1(L_i,G)$. Then $\delta_k(a)$ becomes trivial in each $\mathrm{H}^2(L_i,Q)$. Hence the corestriction $\mathrm{Cor}_{L_i/k}(\delta_k(a)) = \delta_k(a)^{d_i}$ becomes trivial in $\mathrm{H}^2(k,Q)$ where $d_i = [L_i : k]$. Since $\gcd_i(d_i) = 1$, this implies that $\delta_k(a)$ is itself trivial in $\mathrm{H}^2(k,Q)$. Therefore a comes from an element $b \in \mathrm{H}^1(k,H)$ which is trivial in $\prod \mathrm{H}^1(L_i,H)$. (The fact that $\mathrm{H}^1(L_i,Q) = \{1\}$ guarantees that b is trivial in $\mathrm{H}^1(L_i,H)$). Since H satisfies SQ by assumption, b is trivial in $\mathrm{H}^1(k,H)$ which implies the triviality of a in $\mathrm{H}^1(k,G)$. $\square$

Lemma 9.6. *Let E be a finite separable field extension of k and let H be an E-group satisfying SQ. Then the k-group $R_{E/k}(H)$ also satisfies SQ.*

Proof. Set $G = R_{E/k}(H)$ and let ξ be an element in the kernel of $\mathrm{H}^1(k,G) \to \prod_{i=1}^r \mathrm{H}^1(L_i,G)$ where $\gcd_i [L_i : k] = 1$.

Since $\mathrm{char}(k) = 0$, $L_i \otimes_k E$ is an étale E-algebra and hence isomorphic to $E_{1,i} \times E_{2,i} \times \ldots \times E_{n_i,i}$ where each $E_{j,i}$ is a separable field extension of E. Thus $\sum_{j=1}^{n_i} [E_{j,i} : E] = [L_i : k]$ and therefore $\gcd [E_{j,i} : E] = 1$ where $1 \le i \le r$ and $1 \le j \le n_i$.

By Eckmann-Faddeev-Shapiro, we have a natural bijection of pointed sets

$$\mathrm{H}^1(k,G) \simeq \mathrm{H}^1(E,H),$$
$$\mathrm{H}^1(L_i,G) \simeq \prod_{j=1}^{n_i} \mathrm{H}^1(E_{j,i},H).$$

Thus we have that ξ is in the kernel of $\mathrm{H}^1(E,H) \to \prod_{i\le r,\ j\le n_i} \mathrm{H}^1(E_{j,i},H)$. Since H satisfies SQ, we see that ξ is trivial. $\square$

9.3 Serre's question and norm principles

9.3.1 Pushouts

([CGP], Remark 1.4.5) Consider groups A, B, C such that C acts on the left on groups A, B. It acts on itself on the left by conjugation. Let $f : A \to B$ and $g : A \to C$ be C-homomorphisms. Assume further that for each $a \in A$ and $b \in B$, we have

$$g(a)b = f(a)bf(a)^{-1}.$$

Let X be the semi-direct product $B \rtimes C$. So for $x = (b, c), y = (b', c') \in X$, we have $xy = (b(cb'), cc')$. Define $h : A \to X$ sending $a \rightsquigarrow (f(a)^{-1}, g(a))$. Then h is a group homomorphism as

$$\begin{aligned} h(a)h(a') &= \left(f(a)^{-1}, g(a)\right)\left(f(a')^{-1}, g(a')\right) \\ &= \left(f(a)^{-1}g(a)f(a')^{-1}, g(a)g(a')\right) \\ &= \left(f(a)^{-1}f(a)f(a')^{-1}f(a)^{-1}, g(aa')\right) \\ &= \left(f(aa')^{-1}, g(aa')\right) \\ &= h(aa'). \end{aligned}$$

Also $h(A)$ is normal in X. This is because for $a \in A$ and $(b, c) \in X$, we have

$$\begin{aligned}
(b,c)h(a)(b,c)^{-1} &= (b,c)h(a)\big(c^{-1}b^{-1},c^{-1}\big) \\
&= (b,c)\big(f(a)^{-1},g(a)\big)\left(c^{-1}b^{-1},c^{-1}\right) \\
&= \left(bcf(a)^{-1},cg(a)\right)\left(c^{-1}b^{-1},c^{-1}\right) \\
&= \left(bcf(a)^{-1}cg(a)c^{-1}b^{-1},cg(a)c^{-1}\right) \\
&= \left(bcf(a)^{-1}g(ca)b^{-1},g(ca)\right) \\
&= \left(bf(ca^{-1})f(ca)b^{-1}f(ca)^{-1},g(ca)\right) \\
&= \left(bf\left(e_A\right)b^{-1}f(ca)^{-1},g(ca)\right) \\
&= \left(f(ca)^{-1},g(ca)\right) \\
&\in h(A).
\end{aligned}$$

Then we define the pushout or the cofibre product

$$\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\Big\downarrow{\scriptstyle g} & & \Big\downarrow \\
C & \longrightarrow & Q
\end{array}$$

to be $Q \simeq X/h(A)$.

Note that

- When A, C are abelian and C acts trivially on A and B, then $Q = B \times C/A$ where you identify $A \subseteq B \times C$ via the diagonal embedding. If further B is abelian, then Q is abelian also.

- When A is a normal subgroup of C and f is a C-equivariant quotient then B is a normal subgroup of the pushout Q, with $Q/B \simeq C/A$.

9.3.2 Intermediate groups $\hat{G}$ and $\tilde{G}$

Notations are as in Section 5 of ([BM]).

In this section, we introduce new groups $\hat{G}$ and $\tilde{G}$ related to G and deduce a positive answer to Serre's question for them.

Let G be our given connected reductive k-group whose Dynkin diagram contains connected components only of type A_n, B_n, C_n or (non-trialitarian) D_n and let G' denote its derived subgroup. Let $Z(G) = T$ and $Z(G') = \mu$.

Let $\rho : \mu \hookrightarrow S$ be an embedding of μ into a quasi-trivial torus S. We can always do this! This is because of the following :

Let $\Gamma = \mathrm{Gal}\,(k^{sep}/k)$, the absolute Galois group of k. The character group $X(\mu)$ is a continuous Γ module and hence the action makes it a Γ/N module for some open normal subgroup $N \lhd \Gamma$.

Notice that Γ/N is a finite group and $\mathbb{Z}\left[\Gamma/N\right]^n$ is a $\mathbb{Z}$ module of finite rank which is a Γ-permutation module for any $n \geq 1$. And these correspond to quasi-trivial tori!

Thus there exists $n \geq 1$ such that $f : \mathbb{Z}\left[\Gamma/N\right]^n \to X(\mu)$ is a surjective Γ module map. This implies $\mu \hookrightarrow S$ is a closed immersion of μ into corresponding quasi-trivial torus S.

We denote the cofibre product $e(G', \rho) = \frac{G' \times S}{\mu}$ by $\hat{G}$. This k-group is called an *envelope* of G'.

$$\begin{array}{ccc} \mu & \xrightarrow{\delta} & G' \\ \downarrow{\scriptstyle \rho} & & \downarrow \\ S & \xrightarrow{\gamma} & \hat{G} \end{array}$$

Now the quasi-trivial torus $S = Z(\hat{G})$ and $\hat{G}$ fit into an exact sequence as follows :

$$1 \to S \to \hat{G} \to G'^{\ ad} \to 1. \qquad (*)$$

where $G'^{\ ad}$ corresponds to the adjoint group of G'.

Since every adjoint group of classical type is a product of Weil restrictions of absolutely simple adjoint groups, Jodi's result (Theorem 9.3), along with Lemmata 9.4 and 9.6, implies that $G'^{\ ad}$ satisfies SQ. Applying Lemma 9.5 to the exact sequence (*) above, we see that $\hat{G}$ satisfies SQ. *Let us choose such an envelope $\hat{G}$ of G' which satisfies SQ.*

Define an intermediate abelian group $\tilde{T}$ to be the cofibre product $\frac{T \times S}{\mu}$.

$$\begin{tikzcd} \mu \arrow[r] \arrow[d, "\rho"] & T \arrow[d, "\alpha"] \\ S \arrow[r, "\nu"] & \tilde{T} \end{tikzcd}$$

Let the algebraic group $\tilde{G}$ be the cofibre product defined by the following diagram :

$$\begin{tikzcd} G' \times T \arrow[r, "m"] \arrow[d, "id \times \alpha"] & G \arrow[d, "\beta"] \\ G' \times \tilde{T} \arrow[r, "\epsilon"] & \tilde{G} \end{tikzcd}$$

Here $G' \times \tilde{T}$ acts on $G' \times T$ by $\left(g', \tilde{t}\right)(g, t) = (g'gg'^{-1}, t)$. And it acts on G by $\left(g', \tilde{t}\right)(g) = g'gg'^{-1}$. Thus by the discussion in the previous section about pushouts, we have $\tilde{G}/G \simeq \tilde{T}/T \simeq S/\mu$ which is a torus.

Then we have the following commutative diagram with exact rows ([BM], Prop 5.1) . Note that each row is a central extension of $\tilde{G}$.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu & \xrightarrow{\delta,\nu\rho} & G' \times \tilde{T} & \xrightarrow{\epsilon} & \tilde{G} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \rho} & & \downarrow & & \downarrow{\scriptstyle id} & & \\
1 & \longrightarrow & S & \xrightarrow{\gamma,\nu} & \hat{G} \times \tilde{T} & \longrightarrow & \tilde{G} & \longrightarrow & 1
\end{array}
\qquad \begin{array}{c}(**) \\ \\ (***)\end{array}$$

Since $\tilde{T}$ is abelian, the existence of the co-restriction map shows that $\tilde{T}$ satisfies SQ. Since $\hat{G}$ satisfies SQ, we can apply Lemmata 9.4 and 9.5 to (***) to see that $\tilde{G}$ *satisfies* SQ.

9.3.3 Relating Serre's question and norm principle

The deduction of SQ for G from $\hat{G}$ and $\tilde{G}$ follows via the (weak) norm principles.

Let $\beta : G \to \tilde{G}$ be the embedding of k-groups with the cokernel P isomorphic to the torus $\frac{S}{\mu}$ where $\tilde{G}$ and G are as in Section 9.3.2. Thus we have the following exact sequence :

$$1 \to G \xrightarrow{\beta} \tilde{G} \xrightarrow{\pi} P \to 1.$$

Lemma 9.7. *If the weak norm principle holds for* $\pi : \tilde{G} \to P$*, then* G *satisfies* SQ*.*

Proof. From the long exact sequence of cohomology, we have the following commutative diagram :

$$\begin{array}{ccccccccccc}
1 \to & G(k) & \to & \tilde{G}(k) & \xrightarrow{\pi_k} & P(k) & \xrightarrow{\delta_k} & \mathrm{H}^1(k,G) & \xrightarrow{\beta_k} & \mathrm{H}^1(k,\tilde{G}) \\
 & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 \to & \prod G(L_i) & \to & \prod \tilde{G}(L_i) & \xrightarrow{\prod \pi_{L_i}} & \prod P(L_i) & \xrightarrow{\prod \delta_{L_i}} & \prod \mathrm{H}^1(L_i,G) & \to & \prod \mathrm{H}^1(L_i,\tilde{G}).
\end{array}$$

Let $a \in \mathrm{H}^1(k,G)$ become trivial in $\prod \mathrm{H}^1(L_i,G)$. As $\tilde{G}$ satisfies SQ, $\beta_k(a)$ becomes trivial in $\mathrm{H}^1(k,\tilde{G})$. Hence $a = \delta_k(b)$ for some $b \in P(k)$ and $\delta_{L_i}(b)$ is trivial in $\mathrm{H}^1(L_i,G)$. Therefore, there exist $c_i \in \tilde{G}(L_i)$ such that $\pi_{L_i}(c_i) = b$.

Showing that G satisfies SQ, i.e. that a is trivial, is equivalent to showing

$$b \in \left(\mathrm{Image}\,\pi_k : \tilde{G}(k) \to P(k)\right).$$

However $b \in \left(\mathrm{Image}\,\pi_{L_i} : \tilde{G}(L_i) \to P(L_i)\right)$. Since the weak norm principle holds for $\pi : \tilde{G} \to P$, $b^{d_i} \in \mathrm{Image}\left(\pi_k : \tilde{G}(k) \to P(k)\right)$ where $[L_i : k] = d_i$ for each i. As $\gcd_i(d_i) = 1$, this means $b \in \mathrm{Image}\left(\pi_k : \tilde{G}(k) \to P(k)\right)$. □

The norm principle of Merkurjev and Barquero (Theorem 8.3) for reductive groups shows that the norm principle and hence the weak norm principle holds for the map $\pi : \tilde{G} \to P$ for reductive k-groups G as in the following theorem (Theorem 9.8). Thus we have

Theorem 9.8. *Let k be a field of characteristic not 2. Let G be a connected reductive k-group whose Dynkin diagram contains connected components only of type A_n, B_n or C_n. Then Serre's question has a positive answer for G.*

9.4 Quasi-split groups

Let G be a connected quasi-split reductive k-group whose Dynkin diagram does not contain connected components of type E_8 and let G' denote its derived subgroup. Let G^{sc} denote the simply connected cover of G'. Then one has the exact sequence $1 \to C \to G^{sc} \to G' \to 1$, where C is a finite k-group of multiplicative type, central in G^{sc}.

Using a remark made by Gopal Prasad that G^{sc} is quasi-split if and only if G is quasi-split, we can therefore assume that G^{sc} is quasi-split. Under this condition, we would like to show that G satisfies SQ by following the reduction techniques used in Sections 9.2 and 9.3.

Lemma 9.9. *Let G be a connected reductive k-group. If G^{sc} is quasi-split, then there exists an extension $1 \to Q \to H \xrightarrow{\psi} G \to 1$, where Q is a quasi-trivial k-torus, central in reductive k-group H with H' simply connected and quasi-split.*

Proof. Recall that there is a central extension (called a z-extension) of G by a quasi-trivial torus Q such that H' is semisimple and simply connected ([MS], Prop 3.1 and [BK], Lemma 1.1.4).

$$1 \to Q \to H \xrightarrow{\psi} G \to 1.$$

The restriction $\psi|_{H'} : H' \to G$ yields the fact that H' is the simply connected cover of G' and hence is quasi-split. □

Lemmata 9.5 and 9.9 imply that we can restrict ourselves to connected reductive k-groups G such that G' is simply connected and quasi-split.

Lemma 9.10. *Let H be any reductive k-group such that its derived subgroup H' is semi-simple simply connected and quasi-split. Let T denote the k-torus H/H'. Then the natural exact sequence $1 \to H' \to H \xrightarrow{\phi} T \to 1$ induces surjective maps $\phi(L) : H(L) \to T(L)$ for all field extensions L/k. In particular, the norm principle holds for $\phi : H \to T$.*

Proof. There exists a quasi-trivial maximal torus Q_1 of H' defined over k ([HS], Lem 6.7). Let $Q_1 \subset Q_2$, where Q_2 is a maximal torus of H defined over k. The proof of ([HS], Lem 6.6) shows that $\phi|_{Q_2} : Q_2 \to T$ is surjective and that $Q_2 \cap H'$ is a maximal torus of H'. Since $Q_2 \cap H' \subseteq Q_1$, we get the following extension of k-tori

$$1 \to Q_1 \to Q_2 \to T \to 1.$$

Since Q_1 is quasitrivial, $\mathrm{H}^1(L, Q_1) = 0$ for any field extension L/k which gives the surjectivity of $\phi(L) : Q_2(L) \to T(L)$ and hence of $\phi(L) : H(L) \to T(L)$. $\square$

Let $\hat{G}$ be an envelope of G' defined using an embedding of $\mu = Z(G')$ into a quasi-trivial torus S. Note that G' is assumed to be simply connected and quasi-split and is also the derived subgroup of $\hat{G}$ by construction.

$$\begin{array}{ccc} \mu & \xrightarrow{\delta} & G' \\ \Big\downarrow{\scriptstyle\rho} & & \Big\downarrow \\ S & \xrightarrow{\gamma} & \hat{G} \end{array}$$

Thus, we get an exact sequence $1 \to G' \to \hat{G} \to \hat{G}/G' \to 1$ to which we can apply Lemma 9.10 to conclude that the norm principle holds for the canonical map $\hat{G} \to \frac{\hat{G}}{[\hat{G},\hat{G}]}$.

Constructing the intermediate group $\tilde{G}$ as in Section 9.3.2, we see that the norm principle also holds for the natural map $\tilde{G} \to \tilde{G}/G$ ([BM], Prop 5.1). Then using Theorem 9.3 ([Black]) and Lemma 9.7, we can conclude that following theorem holds.

Theorem 9.11. *Let k be a field of characteristic not 2. Let G be a connected quasi-split reductive k-group whose Dynkin diagram does not contain connected components of type E_8. Then Serre's question has a positive answer for G.*

Chapter 10

Obstruction to norm principles for groups of type D_n

'So it's quite a necessary step, you see?' said the Tortoise
'I see,' said Achilles; and there was a touch of sadness in his tone.
- Lewis Caroll

Let k be a field of characteristic not 2. In this chapter, we investigate norm principles for (non-trialitarian) D_n groups and give a scalar obstruction defined up to spinor norms (Theorem 10.4) whose vanishing will imply the norm principles and yield a positive answer to Serre's question for connected reductive k-groups whose Dynkin diagrams contain components of this type also. The main references are ([N2]) and ([KMRT]).

10.1 Preliminaries

Let (A, σ) be a central simple algebra of degree $2n$ over k and let σ be an orthogonal involution. Let $\mathrm{C}(\mathrm{A}, \sigma)$ denote its Clifford algebra which is a central simple algebra over its center, Z/k, the discriminant extension. Let i denote the non-trivial automorphism of Z/k and let $\underline{\sigma}$ denote the canonical involution of $\mathrm{C}(\mathrm{A}, \sigma)$.

Recall from Theorem 2.7 that depending on the parity of n, $\underline{\sigma}$ is either an involution of the second kind (when n is odd) or of the first kind (when n is even). Let $\underline{\mu} : \mathrm{Sim}\,(\mathrm{C}\,(\mathrm{A},\sigma),\underline{\sigma}) \to R_{Z/k}\mathbb{G}_m$ denote the multiplier map sending similitude c to $\underline{\sigma}(c)c$.

Let $\Omega\,(\mathrm{A},\sigma)$ be the *extended Clifford group*. Note that this has center $R_{Z/k}\mathbb{G}_m$ and is an *envelope* of $\mathrm{Spin}\,(\mathrm{A},\sigma)$ ([BM], Ex 4.4). We recall below the map $\varkappa : \Omega\,(\mathrm{A},\sigma)(k) \to Z^*/k^*$ as defined in ([KMRT], Pg 182).

Given $\omega \in \Omega\,(\mathrm{A},\sigma)(k)$, let $g \in \mathrm{GO}^+\,(\mathrm{A},\sigma)(k)$ be some similitude such that $\omega \rightsquigarrow gk^*$ under the natural surjection $\Omega\,(\mathrm{A},\sigma)(k) \to \mathrm{PGO}^+\,(\mathrm{A},\sigma)(k)$.

Let $h = \mu(g)^{-1}g^2 \in \mathrm{O}^+\,(\mathrm{A},\sigma)(k)$ and let $\gamma \in \Gamma\,(\mathrm{A},\sigma)(k)$ be some element in the *special Clifford group* which maps to h under the vector representation $\chi : \Gamma\,(\mathrm{A},\sigma)(k) \to \mathrm{O}^+\,(\mathrm{A},\sigma)(k)$.

Note that by Section 3.4.5, we have $\mathrm{Int}\,(\omega) = C([g])$ and $\mathrm{Int}\,(\omega^2) = C([g^2]) = C([h]) = \mathrm{Int}(\gamma)$. Thus ω^2 and γ differ by an element in Z^*. Hence $\omega^2 = \gamma z$ for some $z \in Z^*$. Then $\varkappa\,(\omega) = zk^*$.

Note that the map $\varkappa$ has $\Gamma\,(\mathrm{A},\sigma)(k)$ as kernel. Also if $z \in Z^*$, then $\varkappa(z) = z^2k^*$.

By following the reductions in ([BM]), it is easy to see that one needs to investigate whether the norm principle holds for the canonical map

$$\Omega\,(\mathrm{A},\sigma) \to \frac{\Omega\,(\mathrm{A},\sigma)}{[\Omega\,(\mathrm{A},\sigma), \Omega\,(\mathrm{A},\sigma)]}.$$

We will need to investigate the norm principle for two different maps depending on the parity of n.

10.1.1 The map μ_* for n odd

Let $U \subset \mathbb{G}_m \times R_{Z/k}\mathbb{G}_m$ be the algebraic subgroup defined by

$$U(k) = \{(f, z) \in k^* \times Z^* | f^4 = \mathrm{N}_{Z/k}(z)\}.$$

Recall the map $\mu_* : \Omega\,(\mathrm{A}, \sigma) \to U$ defined in ([KMRT], Pg 188) which sends

$$\omega \rightsquigarrow \left(\underline{\mu}(\omega), ai(a)^{-1}\,\underline{\mu}(\omega)^2\right),$$

where $\omega \in \Omega\,(\mathrm{A}, \sigma)(k)$ and $\varkappa(\omega) = a \quad k^*$. This induces the following exact sequence ([KMRT], Pg 190)

$$1 \to \mathrm{Spin}\,(\mathrm{A}, \sigma) \to \Omega\,(\mathrm{A}, \sigma) \xrightarrow{\mu_*} U \to 1.$$

Since the semisimple part of $\Omega\,(\mathrm{A}, \sigma)$ is $\mathrm{Spin}\,(\mathrm{A}, \sigma)$, the above exact sequence shows that it suffices to check the norm principle for the map μ_*.

10.1.2 The map $\underline{\mu}$ for n even

Recall the following exact sequence induced by restricting $\underline{\mu}$ to $\Omega\,(\mathrm{A}, \sigma)$ ([KMRT], Pg 187)

$$1 \to \mathrm{Spin}\,(\mathrm{A}, \sigma) \to \Omega\,(\mathrm{A}, \sigma) \xrightarrow{\underline{\mu}} R_{Z/k}\mathbb{G}_m \to 1.$$

Since the semisimple part of $\Omega\,(\mathrm{A}, \sigma)$ is $\mathrm{Spin}\,(\mathrm{A}, \sigma)$, the above exact sequence shows that it suffices to check the norm principle for the map $\underline{\mu}$.

10.2 An obstruction to being in the image of μ_* for n odd

Given $(f, z) \in U(k)$, we would like to formulate an obstruction which prevents (f, z) from being in the image $\mu_*(\Omega(\mathrm{A}, \sigma)(k))$. Note that for $z \in Z^*$, $\mu_*(z) = (\mathrm{N}_{Z/k}(z), z^4)$ and hence the algebraic subgroup $U_0 \subseteq U$ defined by

$$U_0(k) = \{(N_{Z/k}(z), z^4) | z \in Z^*\}.$$

has its k-points in the image $\mu_*(\Omega(\mathrm{A}, \sigma)(k))$.

Let $\mu_{n[K]}$ denote the kernel of the norm map $R_{K/k}\mu_n \xrightarrow{N} \mu_n$ where K/k is a quadratic extension. Note that $\mu_{4[Z]}$ is the center of $\mathrm{Spin}(\mathrm{A}, \sigma)$ as n is odd. Also recall that (Prop 5.5 or [KMRT], Prop 30.13, Pg 418)

$$\mathrm{H}^1\left(k, \mu_{4[Z]}\right) \cong \frac{U(k)}{U_0(k)}.$$

Thus, we can construct the map $S : \mathrm{PGO}^+(\mathrm{A}, \sigma)(k) \to \mathrm{H}^1\left(k, \mu_{4[Z]}\right)$ induced by the following commutative diagram with exact rows :

$$\begin{tikzcd}
1 \arrow[r] & Z^* \arrow[r] \arrow[d, "\mu_*"] & \Omega(\mathrm{A}, \sigma)(k) \arrow[r, "\chi'"] \arrow[d, "\mu_*"] & \mathrm{PGO}^+(\mathrm{A}, \sigma)(k) \arrow[r] \arrow[d, "S"] & 1 \\
1 \arrow[r] & U_0(k) \arrow[r] & U(k) \arrow[r] & \mathrm{H}^1\left(k, \mu_{4[Z]}\right) \arrow[r] & 1
\end{tikzcd}$$

The map S also turns out to be the connecting map from $\mathrm{PGO}^+(\mathrm{A}, \sigma)(k) \to \mathrm{H}^1\left(k, \mu_{4[Z]}\right)$ ([KMRT], Prop 13.37, Pg 190) in the long exact sequence of cohomology corresponding to the exact sequence

$$1 \to \mu_{4[Z]} \to \mathrm{Spin}\,(\mathrm{A}, \sigma) \to \mathrm{PGO}^{+}\,(\mathrm{A}, \sigma) \to 1.$$

Since the maps $\mu_* : Z^* \to U_0(k)$ and $\chi' : \Omega\,(\mathrm{A}, \sigma)(k) \to \mathrm{PGO}^{+}\,(\mathrm{A}, \sigma)(k)$ are surjective, an element $(f, z) \in U(k)$ is in the image $\mu_*\,(\Omega\,(\mathrm{A}, \sigma)(k))$ if and only if its image $[f, z] \in \mathrm{H}^1\left(k, \mu_{4[Z]}\right)$ is in the image $S\left(\mathrm{PGO}^{+}\,(\mathrm{A}, \sigma)(k)\right)$.

Therefore we look for an obstruction preventing $[f, z]$ from being in the image $S(\mathrm{PGO}^{+}\,(\mathrm{A}, \sigma)(k))$. Recall the following commutative diagram with exact rows and columns :

$$\begin{tikzcd}
 & & & 1 \arrow[d] & \\
 & & & \mu_2 \arrow[d] & \\
1 \arrow[r] & \mu_2 \arrow[r] \arrow[d] & \mathrm{Spin}\,(\mathrm{A}, \sigma) \arrow[r, "\chi"] \arrow[d, "id"] & \mathrm{O}^{+}\,(\mathrm{A}, \sigma) \arrow[r] \arrow[d, "\pi"] & 1 \\
1 \arrow[r] & \mu_{4[Z]} \arrow[r] & \mathrm{Spin}\,(\mathrm{A}, \sigma) \arrow[r, "\chi'"] & \mathrm{PGO}^{+}\,(\mathrm{A}, \sigma) \arrow[r] \arrow[d] & 1 \\
 & & & 1 &
\end{tikzcd}$$

Figure 10.1: Diagram relating $\mathrm{Spin}, \mathrm{PGO}^{+}$, and O^{+}

The long exact sequence of cohomology induces the following commutative diagram (Figure 10.2) with exact columns ([KMRT], Prop 13.36, Pg 189), where

$$\begin{tikzcd}
\mathrm{O}^{+}(\mathrm{A},\sigma)(k) \arrow[r, "Sn"] \arrow[d, "\pi"] & \frac{k^*}{k^{*2}} \arrow[d, "i"] \\
\mathrm{PGO}^{+}(\mathrm{A},\sigma)(k) \arrow[r, "\mathrm{S}"] \arrow[d, "\mu"] & \mathrm{H}^1\left(k, \mu_{4[Z]}\right) \arrow[d, "j"] \\
\frac{k^*}{k^{*2}} \arrow[r, phantom, "="] & \frac{k^*}{k^{*2}}
\end{tikzcd}$$

Figure 10.2: Spinor norms and S for n odd

$\mu : \mathrm{PGO}^{+}(\mathrm{A},\sigma)(k) \to \frac{k^*}{k^{*2}}$ is induced by the multiplier map

$$\mu : \mathrm{GO}^{+}(\mathrm{A},\sigma) \to \mathbb{G}_m,$$

$i : \frac{k^*}{k^{*2}} \to \mathrm{H}^1\left(k, \mu_{4[Z]}\right) = \frac{U(k)}{U_0(k)}$ is the map sending $fk^{*2} \rightsquigarrow [f, f^2]$,

$j : \frac{U(k)}{U_0(k)} = \mathrm{H}^1\left(k, \mu_{4[Z]}\right) \to \frac{k^*}{k^{*2}}$ is the map sending $[f, z] \rightsquigarrow \mathrm{N}(z_0)k^{*2}$ where $z_0 \in Z^*$ is such that $z_0 i(z_0)^{-1} = f^{-2}z$.

Definition 10.1. *We call an element $(f, z) \in U(k)$ to be special if there exists a $[g] \in \mathrm{PGO}^{+}(\mathrm{A},\sigma)(k)$ such that $j([f, z]) = \mu([g])$.*

Let $(f, z) \in U(k)$ be a special element and let $[g] \in \mathrm{PGO}^{+}(\mathrm{A},\sigma)(k)$ be such that $j([f, z]) = \mu([g])$. From the discussion above, it is clear that (f, z) is in the image $\mu_*(\Omega(\mathrm{A},\sigma)(k))$ if and only if $[f, z]$ is in the image $S\left(\mathrm{PGO}^{+}(\mathrm{A},\sigma)(k)\right)$.

Thus $S([g])[f, z]^{-1}$ is in kernel j = Image i and hence there exists some $\alpha \in k^*$ such that

$$[f,z] = S([g])[\alpha,\alpha^2] \in \frac{U(k)}{U_0(k)}.$$

Note that if g is changed by an element in $\mathrm{O}^+(\mathrm{A},\sigma)(k)$, then α changes by a spinor norm by Figure 10.2 above. *Thus given a special element, we have produced a scalar $\alpha \in k^*$ which is well defined up to spinor norms.*

$$\begin{aligned}[f,z] \in S\left(\mathrm{PGO}^+(\mathrm{A},\sigma)(k)\right) &\iff [\alpha,\alpha^2] \in S\left(\mathrm{PGO}^+(\mathrm{A},\sigma)(k)\right) \\ &\iff (\alpha,\alpha^2) \in \mu_*\left(\Omega\left(\mathrm{A},\sigma\right)(k)\right).\end{aligned}$$

This happens if and only if there exists $w \in \Omega(\mathrm{A},\sigma)(k)$ such that

$$\begin{aligned}\alpha &= \underline{\mu}(w), \\ \alpha^2 &= \varkappa(w)i(\varkappa(w))^{-1}\,\underline{\mu}(w)^2.\end{aligned}$$

This implies $\varkappa(w) \in k^*$ and hence $w \in \Gamma(\mathrm{A},\sigma)(k)$. Thus α is a spinor norm, being the similarity of an element in the special Clifford group. Also note if α is a spinor norm, then $\alpha = \underline{\mu}(\gamma)$ for some $\gamma \in \Gamma(\mathrm{A},\sigma)(k)$ and $\mu_*(\gamma) = \left(\underline{\mu}(\gamma), \underline{\mu}(\gamma)^2\right)$.

Thus a special element (f,z) is in the image of μ_* if and only if the produced scalar α is a spinor norm. We call the class of α in $\frac{k^*}{\mathrm{Sn}(\mathrm{A},\sigma)}$ to be the scalar obstruction preventing the *special* element $(f,z) \in U(k)$ from being in the image $\mu_*\left(\Omega\left(\mathrm{A},\sigma\right)(k)\right)$.

10.3 An obstruction to being in the image of $\underline{\mu}$ for n even

Given $z \in Z^*$, we would like to formulate an obstruction which prevents z from being in the image $\underline{\mu}\left(\Omega\left(\mathrm{A}, \sigma\right)(k)\right)$. Note that for $z \in Z^*$, $\underline{\mu}(z) = z^2$ and hence the subgroup Z^{*2} is in the image $\underline{\mu}\left(\Omega\left(\mathrm{A}, \sigma\right)(k)\right)$.

Like in the case of odd n, we can construct the map $S : \mathrm{PGO}^+\left(\mathrm{A}, \sigma\right)(k) \to \frac{Z^*}{Z^{*2}}$ induced by the following commutative diagram with exact rows :

$$\begin{tikzcd}
1 \arrow[r] & Z^* \arrow[r] \arrow[d, "\underline{\mu}"] & \Omega\left(\mathrm{A}, \sigma\right)(k) \arrow[r, "\chi'"] \arrow[d, "\underline{\mu}"] & \mathrm{PGO}^+\left(\mathrm{A}, \sigma\right)(k) \arrow[r] \arrow[d, "S"] & 1 \\
1 \arrow[r] & Z^{*2} \arrow[r] & Z^* \arrow[r] & \frac{Z^*}{Z^{*2}} \arrow[r] & 1
\end{tikzcd}$$

Figure 10.3: Diagram from ([KMRT], Definition 13.32, Pg 187)

Again by the surjectivity of the maps, $\underline{\mu} : Z^* \to Z^{*2}$ and $\chi' : \Omega\left(\mathrm{A}, \sigma\right)(k) \to \mathrm{PGO}^+\left(\mathrm{A}, \sigma\right)(k)$, an element $z \in Z^*$ is in the image $\underline{\mu}\left(\Omega\left(\mathrm{A}, \sigma\right)(k)\right)$ if and only if its image $[z] \in \frac{Z^*}{Z^{*2}}$ is in the image $S\left(\mathrm{PGO}^+\left(\mathrm{A}, \sigma\right)(k)\right)$. Therefore we look for an obstruction preventing $[z]$ from being in the image $S(\mathrm{PGO}^+\left(\mathrm{A}, \sigma\right)(k))$. And as before, we arrive at the the following commutative diagram (Figure 10.4) with exact rows and columns ([KMRT], Prop 13.33, Pg 188), where

$$\begin{tikzcd}
\mathrm{O}^{+}(\mathrm{A},\sigma)(k) \arrow[r, "Sn"] \arrow[d, "\pi"] & \frac{k^*}{k^{*2}} \arrow[d, "i"] \\
\mathrm{PGO}^{+}(\mathrm{A},\sigma)(k) \arrow[r, "\mathrm{S}"] \arrow[d, "\mu"] & \frac{Z^*}{Z^{*2}} \arrow[d, "j"] \\
\frac{k^*}{k^{*2}} \arrow[r, phantom, "="] & \frac{k^*}{k^{*2}}
\end{tikzcd}$$

Figure 10.4: Spinor norms and S for n even

$\mu : \mathrm{PGO}^{+}(\mathrm{A},\sigma)(k) \to \frac{k^*}{k^{*2}}$ is induced by the multiplier map

$$\mu : \mathrm{GO}^{+}(\mathrm{A},\sigma) \to \mathbb{G}_m,$$

$i : \frac{k^*}{k^{*2}} \to \frac{Z^*}{Z^{*2}}$ is the inclusion map,

$j : \frac{Z^*}{Z^{*2}} \to \frac{k^*}{k^{*2}}$ is induced by the norm map from $Z^* \to k^*$.

Definition 10.2. *We call an element $z \in Z^*$ to be special if there exists a $[g] \in \mathrm{PGO}^{+}(\mathrm{A},\sigma)(k)$ such that $j([z]) = \mu([g])$.*

Let $z \in Z^*$ be a special element and let $[g] \in \mathrm{PGO}^{+}(\mathrm{A},\sigma)(k)$ be such that $j([z]) = \mu([g])$. As before a *special* element $z \in Z^*$ is in the image $\underline{\mu}(\Omega(\mathrm{A},\sigma)(k))$ if and only if $[z]$ is in the image $S\left(\mathrm{PGO}^{+}(\mathrm{A},\sigma)(k)\right)$.

Thus $S([g])[z]^{-1}$ is in kernel $j = \mathrm{Image}\, i$ and hence there exists some $\alpha \in k^*$ such that

$$[z] = S([g])[\alpha] \in \frac{Z^*}{Z^{*2}}.$$

Note that if g is changed by an element in $\mathrm{O}^+(\mathrm{A},\sigma)(k)$, then α changes by a spinor norm by Figure 10.4 above. *Thus given a special element, we have produced a scalar $\alpha \in k^*$ which is well defined up to spinor norms.*

$$\begin{aligned}[z] \in S\left(\mathrm{PGO}^+(\mathrm{A},\sigma)(k)\right) &\iff [\alpha] \in S\left(\mathrm{PGO}^+(\mathrm{A},\sigma)(k)\right)\\ &\iff (\alpha) \in \underline{\mu}\left(\Omega(\mathrm{A},\sigma)(k)\right).\end{aligned}$$

Since $\alpha \in k^*$ also, this is equivalent to α being a spinor norm ([KMRT], Prop 13.25, Pg 184).

We call the class of α in $\frac{k^*}{\mathrm{Sn}(\mathrm{A},\sigma)}$ to be the scalar obstruction preventing the *special* element $z \in Z^*$ from being in the image $\underline{\mu}(\Omega(\mathrm{A},\sigma)(k))$.

10.4 Scharlau's norm principle revisited

Let $\mu : \mathrm{GO}^+(\mathrm{A},\sigma) \to \mathbb{G}_m$ denote the multiplier map. We would like to show that the norm principle holds for μ. So let L/k be a separable field extension of finite degree and let $g_1 \in GO^+(\mathrm{A},\sigma)(L)$ be such that $\mu(g_1) = f_1 \in L^*$. Let f denote $\mathrm{N}_{L/k}(f_1)$. We would like to show that f is in the image $\mu\left(\mathrm{GO}^+(\mathrm{A},\sigma)(k)\right)$.

Note that by a generalization of Scharlau's norm principle ([KMRT], Prop 12.21; [Black], Lemma 4.3) there exists a $\tilde{g} \in \mathrm{GO}(\mathrm{A},\sigma)(k)$ such that $f = \mu(\tilde{g})$. However we would like to find a *proper* similitude $g \in \mathrm{GO}^+(\mathrm{A},\sigma)(k)$ such that $\mu(g) = f$.

We investigate the cases when the algebra A is non-split and split separately.

Case I : A is non-split

Note that $g_1 \in \mathrm{GO}^+(\mathrm{A},\sigma)(L)$. If $\tilde{g} \in \mathrm{GO}^+(\mathrm{A},\sigma)(k)$, we are done. Hence assume $\tilde{g} \notin \mathrm{GO}^+(\mathrm{A},\sigma)(k)$. By a generalization of Dieudonné's theorem ([KMRT], Thm 13.38, Pg 190), we see that the quaternion algebras

$$B_1 = (Z, f_1) = 0 \in \mathrm{Br}(L),$$
$$B_2 = (Z, f) = A \in Br(k).$$

Since A is non-split, $B_2 \neq 0 \in \mathrm{Br}(k)$. However co-restriction of B_1 from L to k gives a contradiction, because

$$0 = \mathrm{Cor}\, B_1 = \big(Z, \mathrm{N}_{L/k}(f_1)\big) = B_2 \in \mathrm{Br}(k).$$

Hence $\tilde{g} \in \mathrm{GO}^+(\mathrm{A},\sigma)(k)$.

Case II : A is split

Since A is split, $A = \mathrm{End}\, V$ where (V, q) is a quadratic space and σ is the adjoint involution for the quadratic form q. Again, if $\tilde{g} \in \mathrm{GO}^+(\mathrm{A},\sigma)(k)$, we are done. Hence assume $\tilde{g} \notin \mathrm{GO}^+(\mathrm{A},\sigma)(k)$. That is

$$\det(\tilde{g}) = -f^{2n/2} = -(f^n).$$

Since A is of even degree ($2n$) and split, there exists an isometry[1] h of determinant -1. Set $g = \tilde{g}h$. Then $\det(g) = f^n$ where $\mu(g) = f$. Thus we have found a suitable $g \in \mathrm{GO}^+(\mathrm{A}, \sigma)(k)$ which concludes the proof of the following :

Theorem 10.3. *The norm principle holds for the map*

$$\mu : \mathrm{GO}^+(\mathrm{A}, \sigma) \to \mathbb{G}_m.$$

10.5 Spinor obstruction to norm principle for non-trialitarian D_n

Let L/k be a separable field extension of finite degree. And let $w_1 \in \Omega(\mathrm{A}, \sigma)(L)$ be such that for

$$n \text{ odd} : \mu_*(w_1) = \theta \text{ which is equal to } (f_1, z_1) \in U(L),$$

$$n \text{ even} : \underline{\mu}(w_1) = \theta \text{ which is equal to } z_1 \in \left(R_{Z/k}\mathbb{G}_m\right)(L).$$

We would like to investigate whether $\mathrm{N}_{L/k}(\theta)$ is in the image of $\mu_*(\Omega(\mathrm{A}, \sigma)(k))$ (resp $\underline{\mu}(\Omega(\mathrm{A}, \sigma)(k))$) when n is odd (resp. even) in order to check if the norm principle holds for the map $\mu_* : \Omega(\mathrm{A}, \sigma) \to U$ (resp. $\underline{\mu} : \Omega(\mathrm{A}, \sigma) \to R_{Z/k}\mathbb{G}_m$).

Let $[g_1] \in \mathrm{PGO}^+(\mathrm{A}, \sigma)(L)$ be the image of w_1 under the canonical map $\chi' : \Omega(\mathrm{A}, \sigma)(L) \to \mathrm{PGO}^+(\mathrm{A}, \sigma)(L)$. Clearly θ is *special* and let $g_1 \in \mathrm{GO}^+(\mathrm{A}, \sigma)(L)$ be such that $\mu([g_1]) = j([\theta])$.

[1]Since V is of even dimension $2n$, h can be chosen to be a hyperplane reflection for instance

By Theorem 10.3, there exists a $g \in \mathrm{GO}^+(\mathrm{A},\sigma)(k)$ such that[2]

$$\mu([g]) = \mathrm{N}_{L/k}(j[\theta]) = j\left([\mathrm{N}_{L/k}\,\theta]\right).$$

Hence $\mathrm{N}_{L/k}(\theta)$ is *special.*

By Subsection 10.2 (resp. 10.3) , $\mathrm{N}_{L/k}(\theta)$ is in the image of μ_* (resp $\underline{\mu}$) if and only if the scalar obstruction $\alpha \in \frac{k^*}{\mathrm{Sn}(\mathrm{A},\sigma)}$ defined for $\mathrm{N}_{L/k}(\theta)$ vanishes. Thus we have a spinor norm obstruction given below.

Theorem 10.4 (Spinor norm obstruction)**.** *Let L/k be a finite separable extension of fields. Let f denote the map μ_* (resp $\underline{\mu}$) in the case when n is odd (resp. even). Given $\theta \in f(\Omega(\mathrm{A},\sigma)(L))$, there exists scalar obstruction $\alpha \in k^*$ such that*

$$N_{L/k}(\theta) \in f(\Omega(\mathrm{A},\sigma)(k)) \iff \alpha = 1 \in \frac{k^*}{\mathrm{Sn}(\mathrm{A},\sigma)}.$$

Thus the norm principle for the canonical map

$$\Omega(\mathrm{A},\sigma) \to \frac{\Omega(\mathrm{A},\sigma)}{[\Omega(\mathrm{A},\sigma),\Omega(\mathrm{A},\sigma)]},$$

and hence for non-trialitarian D_n holds if and only if the scalar obstructions are spinor norms.

[2] The map j commutes with $\mathrm{N}_{L/k}$ in both cases.

Chapter 11

A summary

'You know what the poet Shakespeare said, Jeeves?'
'Exit hurriedly, pursued by a bear.'
- P.G. Wodehouse, Very good Jeeves

We conclude with a short note summarizing this dissertation and highlighting its main results.

A k-variety X is said to be k-rational if its function field $k(X)$ is a purely transcendental extension of k. X is said to be k-stably rational if $X \times_k \mathbb{A}_k^m$ is k-rational for some $m \geq 0$. The rationality of group varieties was studied using the machinery of R-equivalence.

Motivated by the examples of non-rational adjoint groups of the form $\mathrm{PSO}(q)$ of Merkurjev and Gille for quadratic forms q living in the first couple of terms of the filtration of the Witt ring, we gave a recursive construction producing an infinite family of examples of non-rational adjoint groups. More precisely, we proved the following:

Theorem (7.9)*.* For each n, there exists a quadratic form q_n defined over a field k_n such that $q_n \in \mathrm{I}^n(k_n)$ and $\mathrm{PSO}(q_n)$ is not k_n-stably rational.

The closely related theme of norm principles for algebraic groups was explored. The norm principles proved by Merkurjev and Barquero ([BM]) and the techniques used therein were adapted to study the following question of Serre for classical reductive groups.

Question. Let G be any connected linear algebraic group over a field k and let X be a principal homogeneous space under G over k. If X admits a zero cycle of degree one, does X have a k-rational point?

Using Jodi Black's result ([Black]), we were able to affirmatively answer Serre's question for many of the classical reductive groups as in the following:

Theorem (9.8). Let k be a field of characteristic not 2. Let G be a connected reductive k-group whose Dynkin diagram contains connected components only of type A_n, B_n or C_n. Then Serre's question has a positive answer for G.

The case of quasi-split reductive groups was also studied and a uniform proof answering Serre's question positively was given by the following

Theorem (9.11). Let k be a field of characteristic not 2. Let G be a connected quasi-split reductive k-group whose Dynkin diagram does not contain connected components of type E_8. Then Serre's question has a positive answer for G.

Finally, the missing ingredient, i.e. norm principles for groups of type (non-trialitarian) D_n, was studied and and a scalar obstruction defined up to spinor norms was given whose vanishing will imply the norm principles and yield a positive answer to Serre's question for connected reductive k-groups whose Dynkin diagrams contain components of this type also.

Theorem (10.4)*.* Let L/k be a finite separable extension of fields. Let f denote the map μ_* (resp $\underline{\mu}$) in the case when n is odd (resp. even). Given $\theta \in f\left(\Omega\left(\mathrm{A}, \sigma\right)(L)\right)$, there exists scalar obstruction $\alpha \in k^*$ such that

$$N_{L/k}(\theta) \in f\left(\Omega\left(\mathrm{A}, \sigma\right)(k)\right) \iff \alpha = 1 \in \frac{k*}{\mathrm{Sn}(\mathrm{A}, \sigma)}.$$

It is tantalizingly unclear whether such obstructions to norm principles for the non-trialitarian D_n case exist at all. It seems to be expected that norm principle holds, at least in this context and hence we would like to continue studying this scalar obstruction with greater vigour.

It has been an extremely pleasant journey compiling these results in the form of this dissertation and we hope, you the reader, have enjoyed it, if not as much, at least a little. And we end with the hopeful thought that maybe

पिक्चर अभी बाकी है मेरे दोस्त

Bibliography

[BM] P. Barquero and A. Merkurjev, Norm Principle for Reductive Algebraic Groups, *J. Proceedings of the International Colloquium on Algebra, Arithmetic and Geometry TIFR, Mumbai* (2000).

[BL] E. Bayer-Fluckiger and H. W. Lenstra Jr., Forms in odd degree extensions and self-dual normal bases, *Amer. J. Math.* **112 (3)** (1990) : pgs 359-373.

[BCTSSD] A. Beauville, J.-L. Colliot-Thélène, J. J. Sansuc & P. Swinnerton-Dyer, Variétés stablement rationnelles non rationnelles, *Annals of Mathematics* **121** (1985) : pgs 283-318.

[BK] M. Borovoi and B. Kunyavskiĭ, Formulas for the unramified Brauer group of a principal homogeneous space of a linear algebraic group, *Journal of Algebra* **225(2)** (2000) : pgs 804-821.

[Black] J. Black, Zero cycles of degree one on principal homogeneous spaces, *Journal of Algebra* **334** (2011) : pgs 232-246.

[Brown] K. S. Brown, Cohomology of groups, *Springer Science and Business Media* **(87)** (2012).

[CF67] J. W. S. Cassels & A. Fröhlich, Algebraic Number Theory, *Academic Press London/New York* (1967).

[Chernousov] V. Chernousov, The group of similarity ratios of a canonical quadratic form, and the stable rationality of the variety PSO, *Math. Zametki* **55** No. 4 (1994) : pgs 114-119; *Math. Notes* **55** Nos. 3-4 (1994) : pgs 413-416.

[CP] V. Chernousov & V. P. Platonov, The rationality problem for semisimple group varieties, *Journal fur die Reine und Angewandte Mathematik* (1998) : pgs 1-28.

[Chevalley] C. Chevalley, On algebraic group varieties, *J. Math. Soc. Jap.* **6** (1954) : pgs 303-324.

[Cliff] Professor Clifford, Applications of Grassmann's extensive algebra, *American Journal of Mathematics* **1(4)** (1878) : pgs 350-358.

[CTS] J.-L. Colliot-Thélène & J. J. Sansuc, La R-équivalence sur les tores, *Annales Scientifiques de l'École Normale Supérieure* **10** (1977) : pgs 175-229.

[CT07] J.-L. Colliot-Thélène, Lectures on linear algebraic groups, *Beijing* (2007) : `http://www.math.u-psud.fr/~colliot/BeijingLectures2Juin07.pdf`

[CGP] B. Conrad, O. Gabber & G. Prasad, Pseudo-reductive groups, **26** *Cambridge University Press* (2015).

[Draxl] P. K. Draxl, Skew fields, *Cambridge University Press* **81** (1983).

[GLL] O. Gabber, Q. Liu, & D. Lorenzini, The index of an algebraic variety, *Inventiones mathematicae* **192(3)** (2013) : pgs 567-626.

[GMS] S. Garibaldi, A. Merkurjev & J.-P. Serre, Cohomological invariants in Galois cohomology, *University Lecture Series* **28** (2003), American Mathematical Society, Providence, RI.

[Gille93] P. Gille, R-équivalence et principe de norme en cohomologie galoisienne, *Comptes rendus de l'Académie des sciences* **316 (4)** (1993) : pgs 315-320.

[Gille97] P. Gille, Examples of non-rational varieties of adjoint groups, *Journal of Algebra* **193** (1997) : pgs 728-747.

[Gille07] P. Gille, Le probleme de Kneser-Tits, *Séminarie Bourbaki* **983** (2009) : pgs 39-81.

[Gille10] P. Gille, Lectures on R-equivalence on linear algebraic groups, *Grenoble* (2010) : `http://math.univ-lyon1.fr/homes-www/gille/prenotes/grenoble.pdf`

[Gille10(2)] P. Gille, Serre's conjecture II: a survey, *Quadratic forms, linear algebraic groups, and cohomology, Springer New York* (2010) : pgs 41-56.

[GS] P. Gille & T. Szamuely, Central simple algebras and Galois cohomology, *Cambridge University Press* **101** (2006).

[HS] D. Harari & T. Szamuely, Local-global questions for tori over p-adic function fields, arXiv preprint arXiv:1307.4782 (2013).

[Knus88] M. A. Knus, Quadratic Forms, Clifford Algebras and Spinors, `https://people.math.ethz.ch/~knus/papers/campinas.pdf`.

[KLST] M.-A. Knus, T. Y. Lam, D. B. Shapiro & J.-P. Tignol, Discriminants of involutions on biquaternion algebras, *Proc. Sympos. Pure Math.* **58** (1995) : pgs 279-303.

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost & J.-P. Tignol, The book of involutions, American Mathematical Society Colloquium Publications **44** (1998), AMS.

[Lam] T. Y. Lam, Introduction to quadratic forms over fields, *American Mathematical Soc.* **67** (2005).

[Maclane] S. MacLane, Subfields and automorphism groups of p-adic fields, *Annals of Mathematics* (1939) : pgs 423-442.

[Me95] A. Merkurjev, The norm principle for algebraic groups, *Algebra i Analiz* **7** (1995) : pgs 77-105.

[Me96] A. Merkurjev, R-equivalence and rationality problem for semisimple adjoint classical groups, *Publications Mathématiques de l'IHÉS* **84** (1996) : pgs 189-213.

[Me98] A. Merkurjev, K-theory and algebraic groups, *European Congress of Mathematics, Birkhäuser Basel* (1998) : pgs 43-72.

[MS] J. S. Milne & K. Y. Shih, Conjugates of Shimura varieties, *Hodge cycles, motives, and Shimura varieties, Springer Berlin Heidelberg* (1981) : pgs 280-356.

[Nisnevich] Y. Nisnevich, Rationally Trivial Principal Homogeneous Spaces and Arithmetic of Reductive Group Schemes Over Dedekind Rings, *C. R. Acad. Sci. Paris*, Série I **299** (1984) : pgs 5-8.

[N1] Nivedita Bhaskhar, More examples of non-rational adjoint groups, *Journal of Algebra* **397** (2014) : pgs 39-46.

[N2] Nivedita Bhaskhar, On Serre's injectivity question and norm principle, *Commentarii Mathematici Helvetici* **91** (2016) : pgs 145-161.

[Parimala09] R. Parimala, Some aspects of the algebraic theory of quadratic forms, *Arizona Winter School* (2009) : `http://swc.math.arizona.edu/aws/2009/09ParimalaNotes.pdf`.

[PSr85] R. Parimala & R. Sridharan, 2-Torsion in Brauer Groups : A Theorem of Merkurjev, *ETHZ* (1985) : `www.math.ethz.ch/~knus/sridharan/merkurjev84.pdf`.

[Platonov76] V. P. Platonov, The Tannaka-Artin problem and reduced K-theory, *Mathematics of the USSR-Izvestiya* **10** (1976) : pgs 211-243.

[Platonov78] V. P. Platonov, Algebraic groups and reduced K-theory, *Proc. Internat. Congress Math., Helsinki* (1978) : pgs 311-317.

[PLR] V. P. Platonov & A.S. Rapinchuk, Algebraic Groups and Number Theory, Academic Press Inc. (1994).

[Sansuc81] J. J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, *Journal für die reine und angewandte Mathematik* **327** (1981) : pgs 12-80.

[Scharlau] W. Scharlau, Quadratic and Hermitian Forms, *Springer-Verlag* (1985).

[Serre79] J.-P. Serre, Local Fields, Springer-Verlag (1979).

[Serre95] J.-P. Serre, Cohomologie galoisienne: progrès et problèmes, *Séminaire Bourbaki* (1993/94), *Astérisque* **227 (783(4))** (1995) : pgs 229-257.

[Serre97] J.-P. Serre, Galois cohomology, Springer-Verlag (1997).

[Shatz] S. S. Shatz, Profinite groups, arithmetic, and geometry, *Princeton university press* **67** (1972).

[Sridharan05] R. Sridharan, Beginnings of group cohomology, *Resonance*, **10(9)** (2005) : pgs 37-52.

[Tignol93] J.-P. Tignol, Central simple algebras, involutions, and quadratic forms, *Lecture notes, National Taiwan University, Taiwan*, (1993).

[Tits78] J. Tits, Groupes de whitehead de groupes algébriques simples sur un corps. *Séminaire Bourbaki* **489-506** (1978) : pgs 218-236.

[Vo77] V. E. Voskresenskii, Algebraic tori, *Nauka. Moscow* (1977).