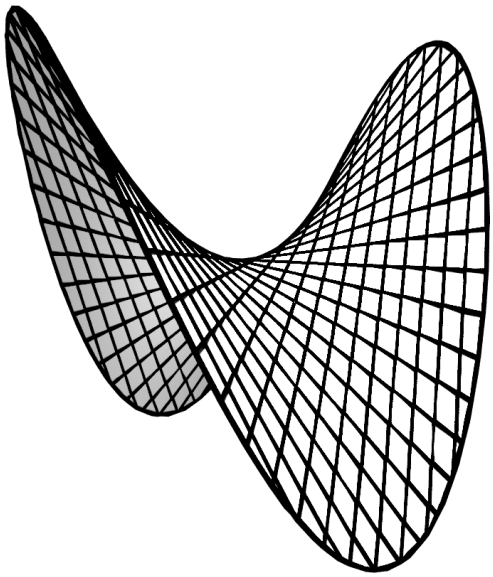
Strong Approximation for a Family of Quadratic Surfaces

Leer, Arnoud van der

Universiteit Leiden
Mathematisch Instituut

Strong Approximation for a Family of Quadratic Surfaces

Arnoud van der Leer



Advisors:
Prof. Dr. Bas Edixhoven
Dr. Martin Bright

Master's thesis
Exam Date: February 13, 2023

Contents

Acknowledgements

First and foremost, I would like to thank the Almighty God, without whom I would not be here, nor this thesis. He has given me the means to study, an aptitude for mathematics and inspiration for solutions to the countless obstacles I found along the way.

I am grateful for my supervisors, Bas and Martin, who guided me in the right direction through the jungle of mathematics that I did not yet understand, and who showed flexibility when I took a bit longer than eight months to finish my thesis. During my master's studies, I learned many bits of theory, but Bas and Martin allowed me to actually learn how it all fits together.

From the beginning, Bas had a clear idea of what we were going to do, and how we would achieve it. Whenever I had made a bit of progress, he always knew what would be the next step and what would be its core idea. He also strove to make sure that the resulting mathematics would provide intuition about what was actually happening.

Martin, thank you for providing me with literature that proved to be very useful, and that I should have read right when you suggested it. Thank you for comforting me when I was insecure about my progress. Thank you for answering my long stream of questions, even the ones that did not have anything to do with my thesis. And thank you for helping me to work through the nitty-gritty details that a lot of this high-level mathematics is composed of.

Then I would like to express my gratitude towards all the people in my life who have witnessed this process. I have a profound love for mathematics, but it would quickly lose its shine if I did not have people around me, who listened when I had to vent my frustration because I was stuck, or my excitement because I was starting to understand something.

Elise, at the time of writing my fiancée, thank you for patiently listening to my long stories about the things that I was working on, and for attempting to actually follow a bit of what I was talking about. And thank you for putting up with my sleepiness whenenever I had traded in an hour of sleep for an hour of working on another small 'breakthrough'.

To my parents: thank you for supporting me financially and for listening to many a story about my thesis at the kitchen table.

And to my friends: thank you for asking me, again and again, whether I had finished my thesis yet, and what it was about. To the mathematicians among you: thank you for easily understanding what I told you. To the non-mathematicians who asked what my thesis was about, and when I asked "are you sure?" always said yes: thank you for trying to understand. To all of you: thank you for allowing me to share my excitement, reflect on what my thesis was about, and practice on distilling this topic and explaining it in laymen's terms.

Soli Deo gloria

CHAPTER 0

Prologue

1. Diophantine equations

In this thesis we will consider problems in the domain of Diophantine equations (which belongs to the realm of number theory). The name "Diophantine equations" dates back to the third century AD, to Diophantus of Alexandria, who wrote a series of books on solving them. A Diophantine equation is a polynomial equation, potentially with multiple unknowns. For example:

$$a^2 + b^2 = c^2 \quad \text{and} \quad y^2 = x^3 - x + 1.$$

We are interested in integer or rational solutions to these equations: solutions where every number is, respectively, a whole number or a fraction. For example, for the two equations above, we have respectively an integer and a rational solution

$$3^2 + 4^2 = 5^2 \quad \text{and} \quad \left(\frac{7}{8}\right)^2 = \left(\frac{1}{4}\right)^3 - \left(\frac{1}{4}\right) + 1.$$

Note that for a homogeneous Diophantine equation (in which each term has the same degree), every integral solution gives rise to an infinitude of similar solutions by scaling. For example, for the first equation, $6^2 + 8^2 = 10^2$ and $9^2 + 12^2 = 15^2$ are also solutions. However, these additional solutions do not really provide any more information. Therefore, we are usually just interested in "primitive solutions", in which the variables do not have a common prime factor (so $3^2 + 4^2 = 5^2$ is a primitive solution, while $15^2 + 20^2 = 25^2$ is not, since the variables have a common factor 5).

2. p-adic numbers

Determining whether a Diophantine equation has integer or rational solutions is generally quite hard. However, sometimes there is a way to show that there are no integer solutions, by showing that the reduction modulo a prime power has no solutions.

For example, if $3x^{37} + 4y^{42} = 6$ were to have any integer solutions, it certainly would have solutions modulo 4. However, the equation modulo 4 becomes $3x^{37} \equiv 2 \mod 4$, and it is trivial to check that neither 0, 1, 2 or 3 satisfy this equation modulo 4. Therefore, $3x^{37} + 4y^{42} = 6$ has no integer solutions.

Now, if an equation has solutions in $\mathbb{Z}/p\mathbb{Z}$, we can try to 'lift' those solutions to $\mathbb{Z}/p^2\mathbb{Z}$ (the advantage of lifting solutions is that we only have to consider p options for each variable, instead of p^m). If we succeed in that, we can try lifting again, to higher and higher powers of p. If we continue doing this, we are constructing solutions over $\mathbb{Z}_p$, the ring of integers modulo p with lifts to higher and higher

powers of p. We can write this formally as

$$\mathbb{Z}_p = \{(x_m)_{m\geq 1} \mid \forall m, x_m \in \mathbb{Z}/p^m\mathbb{Z}, x_m \equiv x_{m+1} \mod p^m\},$$

Therefore, the statement that an equation has solutions over $\mathbb{Z}/p^m\mathbb{Z}$ for all m is equivalent to the statement that it has solutions over $\mathbb{Z}_p$ and if there exists an m such that no solutions can be lifted to $\mathbb{Z}/p^m\mathbb{Z}$, the equation has no solutions over $\mathbb{Z}_p$. We have 'bundled' all of our powers of p in this one object $\mathbb{Z}_p$.

We can now define an additional object $\hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p$, which bundles all powers of all prime numbers. An equation has a solution modulo every prime power (and therefore, by the Chinese Remainder Theorem, modulo every natural number) if and only if it has a solution over $\hat{\mathbb{Z}}$ and conversely, if it has no solution over $\hat{\mathbb{Z}}$, there exists a prime number p such that there exists no solution modulo p^m for some number m, and therefore the equation has no integer solutions.

For rational solutions, we can define a similar object, $\mathbf{A}_{\mathbb{Q},\{\infty\}} = \mathbb{Q} \otimes \hat{\mathbb{Z}}$, which has a similar property: if there exist no solutions over $\mathbf{A}_{\mathbb{Q},\{\infty\}}$, there exist no rational solutions.

3. Schemes

The theory of schemes gives us a different language to talk about solutions of equations. For one Diophantine equation f_1, or even multiple equations $f_1, \ldots, f_m$ with variables $X_1, \ldots, X_n$, we can define a scheme

$$X = V(f_1, \ldots, f_m) = \operatorname{Spec}\left(\mathbb{Z}[X_1, \ldots, X_n]/(f_1, \ldots, f_m)\right).$$

Then we can rephrase "integer solutions to the equations $f_1, \ldots, f_m$" as "$\mathbb{Z}$-points of X" (which we denote by the set $X(\mathbb{Z})$). More generally, for R any ring, $X(R)$ denotes the solutions to $f_1, \ldots, f_m$ over R.

If the equations $f_1, \ldots, f_m$ are homogeneous, we can define another scheme

$$X = C_n(f_1, \ldots, f_m) = V(f_1, \ldots, f_m) \setminus V(X_1, \ldots, X_n).$$

This allows us to rephrase "primitive solutions of $f_1, \ldots, f_m$ over R" as "R-points of X", or $X(R)$, which we will prove in Lemma 1.2. This means that if $X(\hat{\mathbb{Z}})$ is empty, the equations have no primitive integer solutions and if $X(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ is empty, the equations have no primitive rational solutions.

4. Strong Approximation

However, what if $X(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ is not empty? Then we cannot disprove the existence of rational solutions in this way. This does, however, give rise to another question: what information does $X(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ provide about $X(\mathbb{Q})$? This question is at the core of *strong approximation*. A scheme X is said to 'satisfy strong approximation away from infinity' if, for every solution $X(\mathbb{A}_{\mathbb{Q},\{\infty\}})$ there exist arbitrarily close solutions in $X(\mathbb{Q})$. In other words: an equation satisfies strong approximation away from infinity if for every solution x in $X(\mathbb{A}_{\mathbb{Q},\{\infty\}})$ and every distance $\varepsilon > 0$, we can find a solution y in $X(\mathbb{Q})$ such that the 'distance' between x and y is smaller than ε (for some definition of 'distance'). If this is true, $X(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ provides us with a lot of information about $X(\mathbb{Q})$.

5. The equation at hand

In this thesis, we will study the (homogeneous) Diophantine equation

$$q_1' : X_1^2 + 47X_2^2 - 103X_3^2 - 17 \cdot 47 \cdot 103X_4^2 = 0.$$

This equation has been studied before in [**BK19**]. They proved that the scheme $C_4(q_1')$ corresponding to this equation does not satisfy strong approximation away from infinity.

Furthermore, it has been shown in [**Pag20**] that the scheme *does* satisfy strong approximation away from infinity, 2, 17, 47 and 103. This means that we look at the solutions over

$$\mathbf{A}_{\mathbb{Q},\{\infty,2,17,47,103\}} = \mathbb{Q} \otimes \prod_{p \neq 2,17,47,103} \mathbb{Z}_p$$

instead of $\mathbf{A}_{\mathbb{Q},\{\infty\}}$.

6. Group schemes

In this thesis, we will prove a similar result, but this time we will use group schemes to get there. In particular, we will use the group scheme of linear automorphisms of $C_n(f_1, \ldots, f_m)$.

In the first chapter, we will define the schemes that we will work with in the rest of the thesis, and some maps between them.

In the second chapter, we will define the ring of adeles, adelic points, a topology on the set of adelic points, and we will prove some useful lemmas about this topology. Also, we actually define strong approximation, and show two schemes that do not satisfy strong approximation.

The third chapter is all about the 'easy' equation $q_0 : X_1X_4 - X_2X_3 = 0$. We will prove consecutively that the schemes SL_2, C_2 and $C_4(q_0)$ satisfy strong approximation away from infinity.

The fourth and fifth chapter are somewhat more theory-heavy, as they deal with models and twists. In chapter four, we will show how we can modify q_1' slightly, such that its behaviour with respect to the primes 2, 47 and 103 becomes nice. In chapter five, we will discuss the theory of twisting and show that we can define $C_4(q_1')$ (and a couple of related schemes) as a variant, or 'twist', of $C_4(q_0)$ (and its related schemes).

In the sixth and final chapter, we will use all of the above to prove that $\widetilde{\mathrm{SO}(q_1')}$, one of the schemes related to $C_4(q_1')$, satisfies strong approximation away from infinity. From that, we will deduce that $C_4(q_1')$ satisfies strong approximation away from infinity and 17.

CHAPTER 1

Setting the Stage: The Actors

In this chapter, we will cover some preliminaries, which we will use in the rest of this thesis.

In this thesis, we work with several schemes over $\mathbb{Z}$. We will introduce them in this section. Note that all of them can be embedded as locally closed subschemes into $\mathbb{A}^n$ for some n, can therefore be covered by distinguished opens of $\mathbb{A}^n$, and are therefore of finite type over $\mathbb{Z}$.

1. Notation

For $f : X \to Y$ a morphism of schemes and R a ring, we will also use f for the function on R-valued points $f : X(R) \to Y(R)$.

2. The Yoneda Lemma

The following lemma, based on the Yoneda lemma, can be found as Proposition VI-2 in [**EH00**]:

LEMMA 1.1. *If R is a commutative ring, a scheme over R is determined by the restriction of its functor of points to affine schemes over R; in fact*

$$h : (R\text{−Sch}) \to \mathrm{Fun}(R\text{−Alg}, \mathrm{Set})$$

is an equivalence of the category of R-schemes with a full subcategory of the category of functors.

We will usually use the following corollary:

COROLLARY 1.1. *Let R be a ring and let X and Y be R-schemes. Suppose that we have, for each R-algebra A, a function $\mathcal{F}(A) : X(A) \to Y(A)$, such that for each R-algebra morphism $\varphi : A \to B$, the following diagram commutes:*

$$\begin{array}{ccc} X(A) & \xrightarrow{\mathcal{F}(A)} & Y(A) \\ \downarrow{\scriptstyle X(\varphi)} & & \downarrow{\scriptstyle Y(\varphi)} \\ X(B) & \xrightarrow{\mathcal{F}(B)} & X(B) \end{array}.$$

Then there is a unique morphism of schemes $f : X \to Y$ that induces $\mathcal{F}$.

In this thesis we deal mostly with schemes X such that for some $n \in \mathbb{Z}$, for all R-algebras A, $X(A) \subseteq A^n$. Now, given two such schemes X and Y with $X(A) \subseteq A^n$ and $Y(A) \subseteq A^m$, given $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$ such that for all R-algebras A, if we define

$$\mathcal{F}(A) : X(A) \mapsto A^m, \quad (x_1, \ldots, x_n) \mapsto (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

the image lies within $Y(A)$, then the diagram is automatically commutative and $\mathcal{F}(A)$ is induced by a morphism $f : X \to Y$.

3. Algorithmic proofs

This thesis contains a handful of theorems that deal with groups G_l, G_r, sets $T \subseteq S$ and left and right group actions $G_l \times S \to S$, $S \times G_r \to S$ (note that G_l or G_r can be trivial). These theorems usually state something along the lines of "For all $s \in S$, there exist $g_l \in G_l$, $g_r \in G_r$ and a $t \in T$ such that $g_l t g_r = s$". Now, take $s \in S$. If we can find $g_{l1}, \dots, g_{lk} \in G_l$ and $g_{r1}, \dots, g_{rk'} \in G_r$ for some k and k', such that

$$g_{lk} \dots g_{l1} s g_{r1} \dots g_{rk'} \in T,$$

then if we take $g_l = (g_{lk} \dots g_{l1})^{-1}$, $g_r = (g_{r1} \dots g_{rk'})^{-1}$ and $t = g_l^{-1} s g_r^{-1}$, then

$$s = g_l t g_r,$$

which is what we are looking for.

Now, in almost all of the theorems, S is actually a group, and we have group homomorphisms $f_l : G_l \to S$ and $f_r : G_r \to S$, such that the left and right action are given by $(g, s) \mapsto f_l(g)s$ and $(s, g) \mapsto s f_r(g)$. Note that to show that a group homomorphism $f : G \to H$ is surjective, it suffices to show that for all $h \in H$, we can find $g_{l1}, \dots, g_{lk}, g_{r1}, \dots, g_{rk'} \in G$ such that $f(g_{lk}) \dots f(g_{l1}) h f(g_{r1}) \dots f(g_{rk'}) = e$, the identity element of H.

Also, in some cases, we actually have $G \subseteq S$, in which case the homomorphism is just the identity map.

The following is a proof that the map $r_n : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is surjective. In this case we have $G_l = G_r = \mathrm{SL}_2(\mathbb{Z})$, $S = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ and $T = \{I_2\}$.

There are a few things to remark about the form of the proof. First of all, we write the steps of the algorithm (the descriptions of the g_{li} and g_{ri}) on the left and the results of those steps ($g_{lj} \dots g_{l1} m g_{r1} \dots g_{rj'}$ for some j and j') on the right, as a reference for the state of the matrix and for the indices.

Secondly, the proof contains many references to coefficients of a matrix m, but after each step, this is a different matrix. We could call them m, m', m'' etc., but that would become hard to read very soon. This m is a variable and changes, sometimes even multiple times, during each step.

Thirdly, note that we can lift any number $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ to some $a \in \mathbb{Z}$. Also, note that $\mathrm{SL}_2(\mathbb{Z})$ contains (and is generated by) all matrices of the form

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

for $a \in \mathbb{Z}$. Now, multiplying m on the right by their images in $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ adds respectively $\bar{a}$ times the second column to the first, or the first column to the second. Multiplying on the left adds respectively $\bar{a}$ times the second row to the first, or the first to the second. These are the so-called 'elementary column and row operations'. This justifies steps like "We can add m_{21} times m_{12} to m_{11}" and "Then we add $-m_{21}$ times the first row to the second". In most algorithmic proofs, we will have at least one of $\mathrm{SL}_k(R) \subseteq G_l$ and $\mathrm{SL}_k(R) \subseteq G_r$.

Most of these algorithmic proofs have also been implemented in sagemath as jupyter notebooks and have been published at [**vdL23**]. If there is a sagemath implementation of a proof, this will be mentioned at the start of the proof.

THEOREM 1.1. *The map $r_n : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is surjective.*

PROOF. See also the corresponding code at [**vdL23**].

Step	**Outcome**
We start with a 2×2-matrix $m \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.	$\left(\begin{smallmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{smallmatrix}\right)$
We keep subtracting m_{11} and m_{12} from each other, whichever one has a greater lift $0 \leq \overline{m_{1i}} < n \in \mathbb{Z}$ at any point, until either one becomes 0.	$\left(\begin{smallmatrix} m_{11} & 0 \\ m_{21} & m_{22} \end{smallmatrix}\right)$
If $m_{12} = 0$, we can add m_{11} to it, and then subtract m_{12} from m_{11} to get $m_{11} = 0$.	$\left(\begin{smallmatrix} 0 & m_{12} \\ m_{21} & m_{22} \end{smallmatrix}\right)$
Since $m \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, we know that $m_{12}m_{21} = -1$. Therefore, we can add $-m_{21}$ times m_{12} to m_{11} to have $m_{11} = 1$.	$\left(\begin{smallmatrix} 1 & m_{12} \\ m_{21} & m_{22} \end{smallmatrix}\right)$
Then we add $-m_{12}$ times the first column to the second and $-m_{21}$ times the first row to the second to have $m_{12} = m_{21} = 0$.	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & m_{22} \end{smallmatrix}\right)$
Since $m \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, we have $m_{22} = 1$, which concludes the proof.	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$

□

4. GL_n and SL_n

Definition 1.1. For $n \in \mathbb{Z}_{>0}$, we define GL_n via the Yoneda lemma as

$$\mathrm{GL}_n(R) = \{m \in \mathrm{Mat}_{n\times n}(R) \mid \det(m) \in R^*\}.$$

and SL_2 as the subscheme

$$\mathrm{SL}_n(R) = \{m \in \mathrm{Mat}_{n\times n}(R) \mid \det(m) = 1\}.$$

They are representable since we have

$$\mathrm{GL}_n \cong \mathrm{Spec}\left(\mathbb{Z}[X_{11}, \ldots, X_{nn}, Y]/(|X_{ij}|_{ij}Y - 1)\right),$$

where $|X_{ij}|_{ij}$ denotes the determinant of the matrix with the X_{ij} as its coefficients, and

$$\mathrm{SL}_n \cong \mathrm{Spec}\left(\mathbb{Z}[X_{11}, \ldots, X_{nn}]/(|X_{ij}|_{ij} - 1)\right).$$

Since the multiplication of matrices is given by polynomial equations in the coefficients of the matrices, and since determinants are multiplicative, GL_n and SL_n become group schemes under matrix multiplication.

5. $C_n(f_1, \ldots, f_m)$

When studying 'primitive' solutions to a homogeneous Diophantine equation, the notion of a punctured affine cone arises quite naturally. Its definition generally looks as follows

Definition 1.2. For $n, m \in \mathbb{Z}_{>0}$ and $f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_n]$ all homogeneous of degree > 0, we define

$$C_n(f_1, \ldots, f_m) = \mathrm{Spec}\left(\mathbb{Z}[X_1, \ldots, X_n]/(f_1, \ldots, f_m)\right) \setminus V(X_1, \ldots, X_n),$$

the open subscheme obtained by 'removing the origin'. When $m = 0$, we will leave out the parentheses and just write C_n.

In this thesis, we will work extensively with C_2 and $C_4(q_0)$ for $q_0 = X_1X_4 - X_2X_3$.

For any ring R, we can describe the R-valued points of a punctured affine cone as follows:

LEMMA 1.2. *Let R be a ring. Then for $S = C_n(f_1, \ldots, f_m)$,*

$$S(R) = \{x \in R^n \mid x_1R + \cdots + x_nR = R \text{ and } f_i(x) = 0 \text{ for all } i\},$$

writing $x_1, \ldots, x_n$ for the coefficients of x.

PROOF. $C_n(f_1, \ldots, f_m)(R)$ can be identified with the set of $x \in R^n$ such that $f_i(x) = 0$ for all i, and such that for the morphism

$$\psi : \operatorname{Spec} R \to \operatorname{Spec} \left(\mathbb{Z}[X_1, \ldots, X_n]/(f_1, \ldots, f_m)\right),$$

given by $\psi^* : X_i \mapsto x_i$, for every prime $\mathfrak{p} \subseteq R$, $\psi(\mathfrak{p}) \notin V(X_1, \ldots, X_n)$

For $x \in R^n$, we have $(\psi^*)^{-1}(\mathfrak{p}) = \psi(\mathfrak{p}) \in V(X_1, \ldots, X_n)$ if and only if for all i, we have $X_i \in (\psi^*)^{-1}(\mathfrak{p})$. This is the case if and only if $x_i \in \mathfrak{p}$ for all i, or equivalently, $x_1R + \cdots + x_nR \subseteq \mathfrak{p}$.

We conclude that x is in $C_n(f_1, \ldots, f_m)(R)$ if and only if $f_i(x) = 0$ for all i and the ideal $x_1R + \cdots + x_nR$ is not contained in a prime ideal. Since maximal ideals are also prime ideals, this concludes the proof. □

EXAMPLE 1.1. For some rings R, we can state this primitivity condition more specifically:

(1) For $R = k$ for k a field, it means that some x_i is nonzero.
(2) For $R = \mathbb{Z}$, it means that $\gcd(x_1, \ldots, x_i) = 1$.
(3) For $R = \mathbb{Z}_p$ it means that some x_i is not divisible by p.

Now take

$$q_0 = X_0X_3 - X_1X_2.$$

We have a morphism $C_2 \times C_2 \to C_4(q_0)$, given (by the Yoneda Lemma) on R-points by sending $((x_1, x_2), (y_1, y_2))$ to $(x_1y_1, x_1y_2, x_2y_1, x_2y_2)$.

LEMMA 1.3. *The image of $(C_2 \times C_2)(R)$ is inside $C_4(q_0)(R)$.*

PROOF. Let R be a ring and let $((x_1, x_2), (y_1, y_2)) \in (C_2 \times C_2)(R)$. Let $\mathfrak{p} \subseteq R$ be a prime ideal. There exist $i, j \in \{1, 2\}$ such that we have $x_i, y_j \notin \mathfrak{p}$. Then $x_iy_j \notin \mathfrak{p}$. Therefore, $(x_1y_1, x_1y_2, x_2y_1, x_2y_2) \in C_4(q_0)(R)$. □

5.1. A better model for the quadratic form. The main theorem of this thesis proves that $C_4(q_1')$, with

$$q_1' = X_1^2 + 47X_2^2 - 103X_3^2 - 17 \cdot 47 \cdot 103X_4^2,$$

satisfies strong approximation away from infinity and 17. To accomplish this, we will work quite often in characteristic p for almost every prime p. However, the fibers of $C_4(q_1')$ over 2, 47 and 103 are given respectively by

$$(X_1 + X_2 + X_3 + X_4)^2, \quad X_1^2 - 103X_3^2 \quad \text{and} \quad X_1^2 + 47X_2^2.$$

So the fiber over 2 is not reduced, while the fibers over 47 and 103 are singular. This topic is covered more extensively in Chapter 4. In our case, we will just use Theorem 4.1, Lemma 4.7 and Lemma 4.8, to find a better model. We improve this model somewhat more with a $\mathbb{Z}$-isomorphism to obtain

$$q_1 = X_1X_4 + 2X_2^2 - 5X_2X_3 + X_3^2$$

with an isomorphism between q_1' and q_1 given by

$$\begin{pmatrix} -3 & -\frac{811141}{2} & 187191 & 2843673841 \\ -\frac{17}{47} & -\frac{4596505}{94} & \frac{1060758}{47} & \frac{16114425619}{47} \\ \frac{79}{206} & \frac{5340030}{103} & -\frac{2464690}{103} & -\frac{74883927657}{206} \\ -\frac{1}{9682} & -\frac{67624}{4841} & \frac{31196}{4841} & \frac{947907417}{9682} \end{pmatrix} \in \mathrm{GL}(\mathbb{Q}).$$

By Corollary 2.1, satisfying strong approximation is invariant under isomorphism over $\mathbb{Q}$, so we will work with q_1 instead of q_1' from now on.

Remark 1.1. "We improve this model somewhat more": We obtain this improvement on the obtained matrix m by first solving

$$\begin{pmatrix} 1 \\ a \\ b \\ c \end{pmatrix}^T m \begin{pmatrix} 1 \\ a \\ b \\ c \end{pmatrix} = 0.$$

Taking this as the first column of a (otherwise identity) matrix gives us a transformation $t \in \mathrm{SL}_4(\mathbb{Z})$ such that $(t^T m t)_{11} = 0$. Then we can do some (simultaneous) row and column reductions to obtain a matrix

$$\begin{pmatrix} 0 & 0 & 0 & \frac{1}{2} \\ 0 & a & b & 0 \\ 0 & c & d & 0 \\ \frac{1}{2} & 0 & 0 & 0 \end{pmatrix}$$

(for $a, b, c, d \in \frac{1}{2}\mathbb{Z}$ not necessarily the same as in the previous paragraph) such that $ad - bc = -\frac{17}{4}$. Then we can do some additional row and column reductions within this submatrix to finally obtain the quadratic form.

5.2. The group action of SL_n. We have a group action of GL_n (and therefore also of SL_n) on C_n, consisting of the morphism $\mathrm{GL}_n \times C_n \to C_n$, given on R-points by the usual matrix-vector multiplication

$$(m, x) \mapsto mx$$

where we view x as a column vector. Note that if for some prime ideal $\mathfrak{p} \subseteq R$, we have that $x_1, \ldots, x_n \in \mathfrak{p}$, we also have $(mx)_1, \ldots, (mx)_n \in \mathfrak{p}$, since these are R-linear combinations of $x_1, \ldots, x_n$. Multiplying by the inverse of m shows that if $(mx)_1, \ldots, (mx)_n \in \mathfrak{p}$, then also $x_1, \ldots, x_n \in \mathfrak{p}$. Therefore, the image of $(\mathrm{GL}_n \times C_n)(R)$ does indeed lie inside $C_n(R)$ and the map on R-points is induced by a morphism $\mathrm{GL}_n \times C_n \to C_n$.

6. Isom(q, q')

For $n \in \mathbb{Z}_{>0}$, two quadratic forms $q, q' \in \mathbb{Z}[Y_1, \ldots, Y_n]_2$, taking $Y = (Y_1, \ldots, Y_n)^T$, we define the scheme $\mathrm{Isom}(q, q')$ via the Yoneda lemma as

$$\mathrm{Isom}(q, q')(R) = \{m \in \mathrm{GL}_n(R) \mid \exists z \in R^* : q'(mY) = zq(Y)\},$$

where the equation $q'(mY) = zq(Y)$ must hold in $R[Y_1, \ldots, Y_n]$.

Note that the coefficients of $q'(mY)$ are polynomial equations in the m_{ij}, and that the coefficients of $zq(Y)$ are linear in z, so the equality $q'(mY) = zq(Y)$ is equivalent to a set of polynomial equations in z and in the entries of m, so the given functor is indeed representable by an (affine) scheme.

We define $\mathrm{GO}(q) = \mathrm{Isom}(q, q)$, which becomes a group scheme under matrix multiplication.

We also define

$$\mathrm{O}(q)(R) = \{m \in \mathrm{GL}_n(R) \mid q(mY) = q(Y)\},$$

We would want to define $\mathrm{SO}(q)(R) = \{g \in \mathrm{GO}(q)(R) \mid \det(g) = 1\}$, which makes $\mathrm{SO}(q)$ into an algebraic subgroup of $\mathrm{GO}(q)$. However, since 2 is not a unit in $\mathbb{Z}$, this is never smooth over $\mathbb{Z}$ if n is even (see Theorem C.1.5 from [**Con14**]). Therefore, we define $\mathrm{SO}(q_0)(R)$ in a better, more complicated way, and then define $\mathrm{SO}(q)(R)$ as a twist of this scheme where possible. Following Appendix A, we now define $\mathrm{SO}(q_0)(R)$ to be

$$\left\{ g \in \mathrm{O}(q_0) \mid 2 \begin{vmatrix} g_{12} & g_{13} \\ g_{22} & g_{23} \end{vmatrix} \begin{vmatrix} g_{31} & g_{34} \\ g_{41} & g_{44} \end{vmatrix} + 2 \left(\tfrac{1}{2} + \begin{vmatrix} g_{31} & g_{14} \\ g_{41} & g_{24} \end{vmatrix} \right) \left(\tfrac{1}{2} - \begin{vmatrix} g_{32} & g_{13} \\ g_{42} & g_{23} \end{vmatrix} \right) = \tfrac{1}{2} \right\}$$

In this thesis, we will mostly work with $\mathrm{Isom}(q, q_0)$, $\mathrm{SO}(q)$ and $\mathrm{SO}(q_0)$

6.0.1. *Morphism.* We can extend the group action of $\mathrm{GL}_2 \times \mathrm{GL}_2$ on $C_2 \times C_2$ to $C_4(q_0)$ via the morphism (of affine group schemes) $\gamma : \mathrm{GL}_2 \times \mathrm{GL}_2 \to \mathrm{GO}(q_0)$, given on R-points as

$$\gamma : \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right) \mapsto \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

γ restricts to a morphism $\gamma : \mathrm{SL}_2 \times \mathrm{SL}_2 \to \mathrm{SO}(q_0)$.

In particular, on R-points, it sends $(\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right), I)$ and $\left(I, \left(\begin{smallmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{smallmatrix}\right)\right)$ to respectively

$$\begin{pmatrix} a_{11} & 0 & a_{12} & 0 \\ 0 & a_{11} & 0 & a_{12} \\ a_{21} & 0 & a_{22} & 0 \\ 0 & a_{21} & 0 & a_{22} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} b_{11} & b_{12} & 0 & 0 \\ b_{21} & b_{22} & 0 & 0 \\ 0 & 0 & b_{11} & b_{12} \\ 0 & 0 & b_{21} & b_{22} \end{pmatrix},$$

both of which indeed lie in $\mathrm{SO}(q_0)(R)$ (and therefore, their product lies in $\mathrm{SO}(q_0)(R)$ as well).

7. Transporter

If we have a group G that acts on a space X, and if we have elements $a, b \in X$, the transporter from a to b is the set of elements of G that send a to b. There is a scheme-theoretic analogue to this:

For G a group scheme, with a group action $\varphi : G \times X \to X$ on a scheme X, and $a, b \in X(S)$ for a scheme S, we have a commutative diagram (a fiber product)

$$\begin{array}{ccccc} Y & \longrightarrow & & & S \\ \downarrow & & & & \downarrow{\scriptstyle b} \\ G_S & \longrightarrow & G_S \times S & \xrightarrow{(\mathrm{id}_G)_S \times a} & G_S \times X \xrightarrow{\varphi} X \end{array}.$$

Note that the composition of the arrows at the bottom is the morphism that sends m to $m \cdot a$. Also note that Y is the scheme theoretic inverse of b.

We define the *transporter* $G_{a,b}$ from a to b to be the scheme Y in the diagram. We write $G_a = G_{a,a}$, for the stabilizer of a.

CHAPTER 2

The Call to Adventure: Strong Approximation

As mentioned in the introduction, we want to know the relationship between (the geometry of) the p-adic points of a scheme, and the $\mathbb{Z}$-valued or $\mathbb{Q}$-valued points. This relationship is precisely what strong approximation is all about.

In this chapter, we will work towards defining strong approximation, and show two schemes that do not satisfy strong approximation, to get a feel one of the reasons why a scheme can fail to satisfy strong approximation.

1. The ring of adeles

Let k be a global field and Ω_k the set of places of k. For $v \in \Omega_k$, we will write k_v for the completion of k with respect to v and we will write

$$\mathcal{O}_v = \begin{cases} \{x \in k_v \mid v(x) \geq 0\} & v \text{ is nonarchimedean;} \\ k_v & v \text{ is archimedean.} \end{cases}$$

For finite $T \subseteq \Omega_k$, we will write $\mathbf{A}_{k,T} = \prod'_{v \in \Omega_k \setminus T}(k_v, \mathcal{O}_v)$ for the adeles away from T: the subring of $\prod_{v \in \Omega_k \setminus T} k_v$, consisting of the $(x_v)_v$ such that $x_v \in \mathcal{O}_v$ for all but finitely many v.

If we give k_v and $\mathcal{O}_v$ the v-adic topology, they become topological rings: rings with continuous addition and multiplication. We endow $\mathbf{A}_{k,T}$ with the restricted product topology, which makes it into a topological ring as well. A basis for this restricted product topology consists of opens

$$\prod_{v \in S} U_v \times \prod_{v \in \Omega_k \setminus (T \cup S)} \mathcal{O}_v$$

for $S \subseteq \Omega_k \setminus T$ finite and $U_v \subseteq k_v$ open.

In this thesis, we will study $k = \mathbb{Q}$, for which $\Omega_{\mathbb{Q}}$ consists of the prime numbers and ∞. For p prime we will write ord_p for the p-adic valuation, $\mathbb{Z}_p = \mathcal{O}_p$. We will write $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ for the profinite integers and we have the following equalities.

$$\mathbf{A}_{\mathbb{Q},\{\infty\}} = \mathbb{Q} \otimes \hat{\mathbb{Z}}, \quad \mathbf{A}_{\mathbb{Q}} = \mathbb{R} \times \mathbf{A}_{\mathbb{Q},\{\infty\}}.$$

The topology on $\mathbb{Q}_p$ has a basis consisting of opens $x + p^n\mathbb{Z}_p$ for $x \in \mathbb{Q}_p$ and $n \in \mathbb{Z}_{>0}$. For finite $T \subseteq \Omega_{\mathbb{Q}}$ with $\infty \in T$, the restricted product topology for $\mathbf{A}_{\mathbb{Q},T}$ has a basis consisting of opens $x + n\prod_{p \in \Omega_{\mathbb{Q}} \setminus T} \mathbb{Z}_p$ with $x \in \mathbf{A}_{\mathbb{Q},T}$ and $n \in \mathbb{Z} \setminus \{0\}$.

2. A topology on the adelic points

In this thesis we will show for some schemes that they satisfy strong approximation. To this end, we will first have to define strong approximation and this requires us to define a topology on $X(\mathbf{A}_{\mathbb{Q},T})$ for X a scheme of finite type over $\mathbf{A}_{\mathbb{Q},T}$.

For this section, we use Sections 2.6.2, 2.6.3 and Exercise 3.4 of [**Poo17**] as a reference. Let k be a global field with set of places Ω_k and let $T \subseteq \Omega_k$ be a finite subset. Let X be a scheme of finite type over $\mathcal{O}_k$.

Take $v \in \Omega_k$. If X is affine, we have $X = \operatorname{Spec}(\mathbb{Z}[X_1, \ldots, X_n]/I)$ for some ideal I, so $X(\mathcal{O}_v) \subseteq X(k_v) \subseteq k_v^n$ and we give $X(k_v)$ and $X(\mathcal{O}_v)$ the subspace topology. If X is not affine, it has an affine open cover $X = \bigcup_i U_i$. Then $X(k_v) = \bigcup_i U_i(k_v)$, so we give the $U_i(k_v)$ the topology for affine schemes, and we glue along the intersections. The resulting topology is independent of the choice of open affine covering. We give the open and closed subset $X(\mathcal{O}_v) \subseteq X(k_v)$ the subspace topology.

We have a bijection

$$X(\mathbf{A}_{k,T}) \xrightarrow{\sim} \prod_{v \in \Omega_k \setminus T}{}' (X(k_v), X(\mathcal{O}_v))$$

and we give $X(\mathbf{A}_{k,T})$ the restricted product topology.

We will now prove some useful lemmas about this topology.

Remark 2.1. By section 2.6.3 in [**Poo17**], based on [**Con12**], given a variety (separated k-scheme of finite type) X over k, there exists a finite set of places S and a finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$ such that $\mathcal{X}_k \cong X$. We can use this to give $X(\mathbf{A}_{k,T})$ a topology, which is independent of the chosen model $\mathcal{X}$, and functorial in X.

Lemma 2.1. *For $X = \operatorname{Spec}(\mathbb{Z}[X_1, \ldots, X_n]/I)$, $X(\mathbf{A}_{k,T})$ has the subspace topology from $\mathbf{A}_{k,T}^n$.*

Proof. The subspace topology has a basis consisting of elements

$$X(\mathbf{A}_{k,T}) \cap \left(\prod_{v \in S} U_v \times \prod_{v \in \Omega_k \setminus (T \cup S)} \mathcal{O}_v^n \right)$$

for $U_v \subseteq k_v^n$ open and $S \subseteq \Omega_k \setminus T$ finite. However, since X is affine, we have for all $v \in S$ that $U_v \cap X(k_v)$ is open in $X(k_v)$ (and every open of $X(k_v)$ is of this form), so this equals the basis element

$$\prod_{v \in S} X(k_v) \cap U_v \times \prod_{v \in \Omega_k \setminus (T \cup S)} X(\mathcal{O}_v),$$

and $X(\mathbf{A}_{k,T})$ has a basis where every element is of this form. □

Lemma 2.2. *For a morphism of schemes of finite type $f : X \to Y$, the morphism $X(\mathbf{A}_{k,T}) \to Y(\mathbf{A}_{k,T})$ induced by f is continuous.*

Proof. Note that for $v \in \Omega_k \setminus T$ and for the projection map $\pi_v : \mathbf{A}_{k,T} \to k_v$, we have a commutative diagram

$$\begin{array}{ccc} X(\mathbf{A}_{k,T}) & \xrightarrow{f_{\mathbf{A}_{k,T}}} & Y(\mathbf{A}_{k,T}) \\ \downarrow{\scriptstyle X(\pi_v)} & & \downarrow{\scriptstyle Y(\pi_v)} \\ X(k_v) & \xrightarrow{f_{k_v}} & Y(k_v) \end{array}$$

so the map is given separately on each coordinate. It is a remark in Section 2.6.2 of [**Poo17**] that $f(k_v) : X(k_v) \to Y(k_v)$ is continuous for all $v \in \Omega_k$. Therefore, given finite $S \subseteq \Omega_k \setminus T$ and given, for all $v \in S$, opens $U_v \subseteq Y(k_v)$, we have that

$$f^{-1}_{\mathbf{A}_{k,T}}\left(\prod_{v\in S} U_v \times \prod_{v\in\Omega_k\setminus(T\cup S)} Y(\mathcal{O}_v)\right) = \prod_{v\in S} f^{-1}_{k_v}(U_v) \times \prod_{v\in\Omega_k\setminus(T\cup S)} X(\mathcal{O}_v),$$

the preimage of a basis element, is open and since this holds for any basis element for the restricted product topology, $f(\mathbf{A}_{k,T})$ is continuous. □

LEMMA 2.3. *For schemes X, Y, $(X \times Y)(\mathbf{A}_{k,T})$ has the product topology from $X(\mathbf{A}_{k,T}) \times Y(\mathbf{A}_{k,T})$.*

PROOF. First of all, for all places $v \in \Omega_k \setminus T$, $(X \times Y)(k_v)$ has the product topology, according to Proposition 3.1 from [**Con12**]. Therefore, the topology on $(X \times Y)(\mathbf{A}_{k,T})$ has a basis consisting of sets

$$\prod_{v\in S} U_v \times V_v \times \prod_{v\in\Omega_k\setminus(S\cup T)} X(\mathcal{O}_v) \times Y(\mathcal{O}_v)$$

for $S \subseteq \Omega_k \setminus T$ finite and for all $v \in S$, $U_v \subseteq X(k_v)$ and $V_v \subseteq Y(k_v)$ open. Such basic open sets equal

$$\left(\prod_{v\in S} U_v \times \prod_{v\in\Omega_k\setminus(S\cup T)} X(\mathcal{O}_v)\right) \times \left(\prod_{v\in S} V_v \times \prod_{v\in\Omega_k\setminus(S\cup T)} Y(\mathcal{O}_v)\right)$$

which gives exactly a basis for the product topology on $X(\mathbf{A}_{k,T}) \times Y(\mathbf{A}_{k,T})$. □

3. Strong Approximation

Now, we are finally ready to define strong approximation. Furthermore, in this section, we will prove two additional lemmas that, for some schemes, show that they satisfy strong approximation.

DEFINITION 2.1 (Strong Approximation). For a global field k, a finite set $T \subseteq \Omega_k$ and a $\mathcal{O}_k$-scheme of finite type X, we say that X satisfies strong approximation away from T if $X(k)$ is dense in $X(\mathbf{A}_{k,T})$.

If we take $k = \mathbb{Q}$, $T = \{\infty\}$ and X affine (so a subscheme of $\mathbb{A}^n$), this definition boils down to: for all $(x_1, \ldots, x_n)^T \in X(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ and all $m \in \mathbb{Z}_{>0}$, there exists $(y_1, \ldots, y_n)^T \in X(\mathbb{Q})$ such that $x_i - y_i \in m\hat{\mathbb{Z}}$ for all i.

We have the following very useful lemma about strong approximation

LEMMA 2.4. *Let k be a global field and $T \subseteq \Omega_k$ finite. Let $f : X \to Y$ be a morphism of schemes of finite type over $\mathcal{O}_k$ such that the induced map $f_{\mathbf{A}_{k,T}} : X(\mathbf{A}_{k,T}) \to Y(\mathbf{A}_{k,T})$ is surjective. If X satisfies strong approximation away from T, then Y satisfies strong approximation away from T as well.*

PROOF. Let $V \subseteq Y(\mathbf{A}_{k,T})$ be a nonempty open. Then $f^{-1}_{\mathbf{A}_{k,T}}(V) \subseteq X(\mathbf{A}_{k,T})$ is a nonempty open, since $f_{\mathbf{A}_{k,T}}$ is surjective and continuous.

Because X satisfies strong approximation away from T, there exists $a \in {f_{\mathbf{A}_{k,T}}}^{-1}(V) \cap X(k)$. The fact that $f_{\mathbf{A}_{k,T}}(a) \in V \cap Y(k)$ concludes the proof. □

COROLLARY 2.1. *Let X and Y be separated schemes of finite type over $\mathcal{O}_k$ and let there be an isomorphism $f : X_k \xrightarrow{\sim} Y_k$. Then X satisfies strong approximation away from T if and only if Y satisfies strong approximation away from T.*

PROOF. Since f is an isomorphism, it has an inverse f^{-1}. We have $f \circ f^{-1} = \mathrm{id}_{Y_k}$ and this induces, using the diagonal map $k \hookrightarrow \mathbf{A}_{k,T}$, the equality $f_{\mathbf{A}_{k,T}} \circ f^{-1}_{\mathbf{A}_{k,T}} = \mathrm{id}_{Y(\mathbf{A}_{k,T})}$. Therefore, $f_{\mathbf{A}_{k,T}}$ (note that $\mathbf{A}_{k,T}$ is a k-algebra, so the function $f_{\mathbf{A}_{k,T}} : X(\mathbf{A}_{k,T}) \to Y(\mathbf{A}_{k,T})$ is defined) is surjective and in the same way, $f^{-1}_{\mathbf{A}_{k,T}}$ is surjective.

Applying in both directions an analogue to Lemma 2.4 for k-varieties, using Remark 2.1 for continuity, gives the result. □

Later on, we will use the following lemma to prove that SL_2 satisfies strong approximation away from infinity.

LEMMA 2.5. *For G a group scheme with an embedding (as a scheme) into $\mathbb{A}^n$, the following are equivalent:*

(1) $G(\mathbb{Q})$ is dense in $G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$;
(2) $G(\mathbb{Z})$ is dense in $G(\hat{\mathbb{Z}})$ and $G(\mathbb{Q}) \cdot G(\hat{\mathbb{Z}}) = G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$.

PROOF. Since G is a group scheme, it has inversion and multiplication morphisms. Then, by Lemma 2.2, these induce continuous morphisms on $G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$, which makes $G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ into a topological group.

Suppose that $G(\mathbb{Q})$ is dense in $G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$. Let $(x_1, \ldots, x_n) \in G(\hat{\mathbb{Z}})$ and $m \in \mathbb{Z} \setminus \{0\}$. Then there exists $(y_1, \ldots, y_n) \in G(\mathbb{Q})$ such that $x_i - y_i \in m\hat{\mathbb{Z}}$ for all i. However, then $y_i \in \hat{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Therefore $G(\mathbb{Z})$ is dense in $G(\hat{\mathbb{Z}})$.

Take $a \in G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$. Since $G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ is a topological group and $G(\hat{\mathbb{Z}})$ is open, $a \cdot G(\hat{\mathbb{Z}})$ is open. Since $G(\mathbb{Q})$ is dense in $G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$, there exists $b \in G(\mathbb{Q}) \cap (a \cdot G(\hat{\mathbb{Z}}))$. Then, take $c = a^{-1}b \in G(\hat{\mathbb{Z}})$, so $a = bc^{-1} \in G(\mathbb{Q}) \cdot G(\hat{\mathbb{Z}})$.

Conversely, suppose that $G(\mathbb{Z})$ is dense in $G(\hat{\mathbb{Z}})$ and $G(\mathbb{Q}) \cdot G(\hat{\mathbb{Z}}) = G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$. Let $U \subseteq G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ be a nonempty open. Then it contains an element $a = bc$ with $b \in G(\mathbb{Q})$ and $c \in G(\hat{\mathbb{Z}})$. Since $G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ is a topological group, $b^{-1}U$ is open and has a nonempty open intersection with $G(\hat{\mathbb{Z}})$ (since it contains c). Therefore, there exists $b' \in G(\mathbb{Z}) \cap (b^{-1}U)$. Then $bb' \in U$, but also $bb' \in G(\mathbb{Q}) \cdot G(\mathbb{Z}) = G(\mathbb{Q})$, so $G(\mathbb{Q})$ is dense in $G(\mathbf{A}_{\mathbb{Q},\{\infty\}})$. □

4. Two counterexamples to strong approximation

In this section, we take $k = \mathbb{Q}$, and we show two examples of schemes that do not satisfy strong approximation away from infinity.

A simple example is $\mathbb{G}_m = \mathrm{Spec}\,(\mathbb{Z}[X, Y]/(XY - 1))$.

EXAMPLE 2.1. $\mathbb{G}_m$ does not satisfy strong approximation away from infinity.

PROOF. Note that $\mathbb{G}_m(\hat{\mathbb{Z}})$ is an open subset of $\mathbb{G}_m(\mathbf{A}_{\mathbb{Q},\{\infty\}})$. Therefore, if $\mathbb{G}_m$ satisfies strong approximation, $\mathbb{G}_m(\mathbb{Q})$ must be dense in $\mathbb{G}_m(\hat{\mathbb{Z}})$. Since

$$\mathbb{G}_m(\mathbb{Q}) \cap \mathbb{G}_m(\hat{\mathbb{Z}}) = \mathbb{G}_m(\mathbb{Z}),$$

we must have that $\mathbb{G}_m(\mathbb{Z})$ is dense in $\mathbb{G}_m(\hat{\mathbb{Z}})$. Note in particular, this means that for every $n \in \mathbb{Z}_{>0}$ and every $x \in \mathbb{G}_m(\hat{\mathbb{Z}})$,

$$\mathbb{G}_m(\mathbb{Z}) \cap \left(\mathbb{G}_m(\hat{\mathbb{Z}}) \cap (x + (n\hat{\mathbb{Z}})^2)\right)$$

must not be empty. In other words, $\mathbb{G}_m(\mathbb{Z}) \to \mathbb{G}_m(\hat{\mathbb{Z}}/n\hat{\mathbb{Z}})$ must be surjective. Note that $\hat{\mathbb{Z}}/n\hat{\mathbb{Z}} = \mathbb{Z}/n\mathbb{Z}$, since scaling by n only affects the components $\mathbb{Z}_p$ for which $p \mid n$.

Now, if we take $n = 5$, then $\mathbb{G}_m(\mathbb{Z}/5\mathbb{Z})$ contains the point $(2, 3)$. However, $\mathbb{G}_m(\mathbb{Z}) = \{(1, 1), (-1, -1)\}$ and neither of these points reduce to $(2, 3)$. Therefore, $\mathbb{G}_m$ does not satisfy strong approximation away from infinity. □

A more sophisticated version of this principle is the scheme $\mathrm{SO}(q_0)$, with q_0 defined in Section 1.5 as $X_1X_4 - X_2X_3$. As established in Section 1.6, we have a map $\gamma : \mathrm{SL}_2 \times \mathrm{SL}_2 \to \mathrm{SO}(q_0)$. We use the lack of surjectivity of this map on $\mathbf{A}_{\mathbb{Q},\{\infty\}}$-points to show that $\mathrm{SO}(q_0)$ does not satisfy strong approximation away from infinity.

LEMMA 2.6. *Let k be a field. Then γ is surjective on k-points if and only if k is quadratically closed.*

PROOF. See also the corresponding code at [**vdL23**].

First of all, recall that γ is given on k-points by

$$\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\right) \mapsto \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

Now, suppose that k is not quadratically closed. Then there exists $\lambda \in k$ which is not a square. Now, suppose that there exists a preimage (a, b) of

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\lambda} & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then we must have $b_{11} = \frac{1}{a_{11}}$. Since $b_{11}a_{21} = b_{11}a_{12} = 0$, we must have $a_{21} = a_{12} = 0$. Since $a \in \mathrm{SL}_2(k)$, we have $a_{22} = \frac{1}{a_{11}} = b_{11}$. Then $\lambda = a_{22}b_{11} = b_{11}^2$, which is a contradiction. Therefore, the map is not surjective on k-points.

We will prove that the lack of square roots in k is the only obstruction to this map being surjective. Therefore, assume that k is quadratically closed. We will prove that the map is surjective on k-points by using 'elementary row operations on steroids': We let $(\mathrm{SL}_2 \times \mathrm{SL}_2)(k)$ act on the left of $\mathrm{SO}(q_0)(k)$. Our building blocks are

$$\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, I\right), \quad \left(\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, I\right), \quad \left(I, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right) \quad \text{and} \quad \left(I, \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}\right),$$

all elements of $(\mathrm{SL}_2 \times \mathrm{SL}_2)(k)$ which, respectively:

- add a times row 3 and 4 to row 1 and 2 respectively;
- add a times row 1 and 2 to row 3 and 4 respectively;
- add a times row 2 and 4 to row 1 and 3 respectively;
- add a times row 1 and 3 to row 2 and 4 respectively.

Most of the time, we will just mention one component, for example "We add 3 times m_{11} to m_{31}", leaving implicit that we then also add 3 times m_{21} to m_{41} (and that the same happens in the other columns).

Note that for every element $m \in \mathrm{SO}(q_0)(k)$, if we write m_{*i} for the ith column, we have $m_{*i}^T q_0 m_{*j} = (q_0)_{ij}$: the inner product (using q_0) between the ith and jth column, is the i,jth entry of q_0. Depending on the characteristic of k, we may need to multiply by 2 to actually let this make sense. For example, for $(i,j) = (1,1)$ and $(i,j) = (1,4)$, this gives respectively,

$$m_{11}m_{41} - m_{21}m_{31} = 0 \quad \text{and} \quad m_{11}m_{44} + m_{41}m_{14} - m_{21}m_{34} - m_{31}m_{24} = 1.$$

Step	**Outcome**
Take $m \in \mathrm{SO}(q_0)(k)$.	$\begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{pmatrix}$
First of all, if $m_{11} = 0$ and $m_{21} = 0$, we must have $m_{31} \neq 0$ or $m_{41} \neq 0$. We add m_{31} to m_{11} and m_{41} to m_{21} to have $m_{11} \neq 0$ or $m_{21} \neq 0$. If $m_{21} = 0$, we add m_{11} to m_{21} to have $m_{21} \neq 0$. We add $\frac{1-m_{11}}{m_{21}}$ times m_{21} to m_{11} to have $m_{11} = 1$.	$\begin{pmatrix} 1 & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{pmatrix}$
We now subtract m_{21} times m_{11} from m_{21}, and m_{31} times m_{11} from m_{31}. Then $m_{21} = m_{31} = 0$.	$\begin{pmatrix} 1 & m_{12} & m_{13} & m_{14} \\ 0 & m_{22} & m_{23} & m_{24} \\ 0 & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{pmatrix}$
Since $m \in \mathrm{SO}(q_0)(k)$, for $i \leq 3$, the inner product between columns 1 and i is 0, so $m_{4i} = 0$. Also, the inner product between columns 1 and 4 is $\frac{1}{2}$, so $m_{44} = 1$.	$\begin{pmatrix} 1 & m_{12} & m_{13} & m_{14} \\ 0 & m_{22} & m_{23} & m_{24} \\ 0 & m_{32} & m_{33} & m_{34} \\ 0 & 0 & 0 & 1 \end{pmatrix}$
We can now subtract m_{34} times m_{44} from m_{34} and m_{24} times m_{44} from m_{24} to make sure $m_{24} = m_{34} = 0$.	$\begin{pmatrix} 1 & m_{12} & m_{13} & m_{14} \\ 0 & m_{22} & m_{23} & 0 \\ 0 & m_{32} & m_{33} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
For $2 \leq i \leq 4$, the inner product between columns i and 4 is 0, so $m_{4i} = 0$.	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & m_{22} & m_{23} & 0 \\ 0 & m_{32} & m_{33} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
Then the equation, given at the end of Appendix A to cut out $\mathrm{SO}(q_0)$ inside $O(q_0)$, gives $m_{23}m_{32} = 0$. Also, since the inner product between the columns 2 and 3 is $\frac{1}{2}$, we have $m_{22}m_{33} = 1$. Now for $2 \leq i \leq 3$, since the inner product of column i with itself is 0 for all columns, we have $m_{2i}m_{3i} = 0$ and this gives $m_{23} = m_{32} = 0$. Then we have $m_{33} = \frac{1}{m_{22}}$.	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & m_{22} & 0 & 0 \\ 0 & 0 & \frac{1}{m_{22}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
Since k is quadratically closed, there exists $\mu \in k$ such that $\mu^2 = m_{22}$. Then we can lift m to $\left(\begin{pmatrix} \mu & 0 \\ 0 & \frac{1}{\mu} \end{pmatrix}, \begin{pmatrix} \frac{1}{\mu} & 0 \\ 0 & \mu \end{pmatrix}\right) \in (\mathrm{SL}_2 \times \mathrm{SL}_2)(k)$. Multiplying by its inverse concludes the proof.	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

□

EXAMPLE 2.2. $\mathrm{SO}(q_0)$ does not satisfy strong approximation away from infinity.

PROOF. The lemma shows that the map $\gamma : \mathrm{SL}_2 \times \mathrm{SL}_2 \to \mathrm{SO}(q_0)$ is a finite étale morphism of degree 2. Then Theorem 8.4.10 from [**Poo17**] tells us that the inclusion $\mathrm{SO}(q_0)(\mathbb{Q}) \to \mathrm{SO}(q_0)(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ is not dense. □

We can make things a lot more specific than the lemma does, since we don't have to worry about the general case.

Over $\mathbb{Z}\left[\frac{1}{2}\right]$, $\mathrm{SL}_2 \times \mathrm{SL}_2$ and $\mathrm{SO}(q_0)$ are separated with geometrically integral fibers. We have a matrix

$$m = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{SO}(q_0)(\mathbb{Z}_{17}).$$

Since γ is a finite étale morphism of degree 2, either 17 splits in $\kappa(\gamma^{-1}(m))$ and m has two inverse images, or it is inert and m has no inverse images.

As shown in Lemma 2.6, since 3 has no square root in $\mathbb{F}_{17}$ (and therefore not in $\mathbb{Z}_{17}$), 17 is inert in $\kappa(\gamma^{-1}(m))$.

By Krasner's Lemma (Proposition 3.5.74 from [**Poo17**]), we have an open subset

$$U_{17} = \{u \in \mathrm{SO}(q_0)(\mathbb{Z}_{17}) \mid 17 \text{ is inert in } \gamma^{-1}(u)\}.$$

We take $U_p = \mathrm{SO}(q_0)(\mathbb{Z}_p)$ for all primes $p \nmid 2 \cdot 17$. This gives an open

$$U = \prod_{p \nmid 2} U_p \subseteq \mathrm{SO}(q_0)(\mathbf{A}_{\mathbb{Q},\{2,\infty\}}).$$

Now, suppose that there exists $x \in \mathrm{SO}(q_0)(\mathbb{Q}) \cap U$. Then we have $x \in \mathrm{SO}(q_0)\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. We will show that this means that 17 is not inert in $\kappa(\gamma^{-1}(x))$, which contradicts the fact that $x \in U_{17}$.

Now, we take an arbitrary matrix $y \in \mathrm{SO}(q_0)\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ such that y can be obtained by multiplying x on the left by an element of $\mathrm{SL}_2 \times \mathrm{SL}_2\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. Note that this means that y has a preimage in $\mathrm{SL}_2 \times \mathrm{SL}_2\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ if and only if x has a preimage. We apply a reduction to y similar to the one in Lemma 2.6.

First, we add, if necessary, a row to the first and second row, to make sure the first two entries in first column are nonzero. Note that there exists $a \in \mathbb{Z}$ such that $2^a \cdot y_{11}, 2^a \cdot y_{21} \in \mathbb{Z}$.

If necessary, we apply the Euclidean algorithm (over $\mathbb{Z}$) to get $2^a \cdot y_{11} = 0$ and $2^a \cdot y_{21} = 1$ and we add 2^a (note that this is an element of $\mathbb{Z}\left[\frac{1}{2}\right]$) times the second row to the first. Therefore, we can assume that $y_{11} = 1$. After this, we follow the rest of the reduction steps of Lemma 2.6. Then we can assume that

$$y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \frac{1}{\lambda} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that λ is a unit in $\mathbb{Z}\left[\frac{1}{2}\right]$, so it is of the form $(-1)^b 2^c$ for $b, c \in \mathbb{Z}$. Then we have

$$\gamma\left(\begin{pmatrix} 4^b 6^c & 0 \\ 0 & \frac{1}{4^b 6^c} \end{pmatrix}, \begin{pmatrix} \frac{1}{4^b 6^c} & 0 \\ 0 & 4^b 6^c \end{pmatrix}\right) \equiv y \mod 17,$$

so 17 splits in $\kappa(\gamma^{-1}(y))$ and therefore in $\kappa(\gamma^{-1}(x))$. However, by construction, 17 was inert in $\kappa(\gamma^{-1}(x))$, which gives a contradiction.

Therefore, $\mathrm{SO}(q_0)(\mathbb{Q}) \cap U = \emptyset$ and we conclude that $\mathrm{SO}(q_0)$ does not satisfy strong approximation away from infinity.

CHAPTER 3

Fun and Games: The Simple Case

In this chapter, we will prove that $C_4(q_0)$ satisfies strong approximation away from infinity. To this end, we will first prove that SL_2 satisfies strong approximation away from infinity using Lemma 2.5, and then use Lemma 2.4 twice to transfer this property to C_2 and finally to $C_4(q_0)$.

1. SL_2

For S a scheme and $l \in \mathbb{Z}$, the map $\mathrm{Spec}\,(\mathbb{Z}/l\mathbb{Z}) \to \mathrm{Spec}\,(\mathbb{Z})$ induces a map $r_l : S(\mathbb{Z}) \to S(\mathbb{Z}/l\mathbb{Z})$ which, for affine schemes, corresponds to the usual reduction modulo l.

We want to prove that $\mathrm{SL}_2(\mathbb{Z})$ is dense in $\mathrm{SL}_2(\hat{\mathbb{Z}})$. Note that the topology on $\mathrm{SL}_2(\hat{\mathbb{Z}})$ has a basis consisting of opens $m + l\hat{\mathbb{Z}}^4$ for $l \in \mathbb{Z}$ and $m \in \mathrm{SL}_2(\hat{\mathbb{Z}})$. Saying that every one of these contains a $\mathbb{Z}$-point is equivalent to saying that the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\hat{\mathbb{Z}}/l\hat{\mathbb{Z}})$ is surjective for all l. Note that $\hat{\mathbb{Z}}/l\hat{\mathbb{Z}} \cong \mathbb{Z}/l\mathbb{Z}$. We prove that $\mathrm{SL}_2(\mathbb{Z})$ is dense in $\mathrm{SL}_2(\hat{\mathbb{Z}})$ with the following lemma.

LEMMA 3.1. *For the scheme SL_n, r_l is surjective for all l.*

PROOF. See also the corresponding code at [**vdL23**].

If $n = 1$, we have $\mathrm{SL}_1(\mathbb{Z}/l\mathbb{Z}) = \{(1)\}$, which can be lifted trivially.

Fix $l \in \mathbb{Z}$. We let $\mathrm{SL}_n(\mathbb{Z})$ act on $\mathrm{SL}_n(\mathbb{Z}/l\mathbb{Z})$ on the left and on the right. This gives us elementary row and column operations.

Step	**Outcome**
We start with a $n \times n$-matrix m.	$\begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ m_{21} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{pmatrix}$
Note that we can lift elements of $\mathbb{Z}/l\mathbb{Z}$ to $\mathbb{Z}$ such that they end up between 0 and $l-1$. Take i and j such that the lift of m_{1i} is less than or equal to m_{1j}. Then subtract m_{1i} from m_{1j}. This decreases the sum of their lifts. Since this sum is finite, if we do this repeatedly, all but one of the m_{1j} will become 0 in a finite number of steps.	$\begin{pmatrix} 0 & m_{12} & \dots & 0 \\ m_{21} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{pmatrix}$
Let m_{1i} be the nonzero value. If $i \neq n$, we add m_{1i} to m_{1n} and then subtract m_{1n} from m_{1i}.	$\begin{pmatrix} 0 & 0 & \dots & m_{1n} \\ m_{21} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{pmatrix}$

Let a be the determinant of the bottom left $(n-1)\times(n-1)$ submatrix. Note that $m_{1n}a = 1$. Add a times m_{1n} to m_{11}, which makes sure that $m_{11} = 1$. Then subtract m_{1n} times m_{11} from m_{1n}. Also, subtract m_{i1} times m_{11} from m_{i1} for all $i \geq 2$.

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & m_{n2} & \dots & m_{nn} \end{pmatrix}$$

Note that the bottom right $(n-1)\times(n-1)$ submatrix is an element of $\mathrm{SL}_{n-1}(\mathbb{Z}/l\mathbb{Z})$. Repeating the above for this submatrix (induction) gives the identity matrix.

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

□

In order to be able to use Lemma 2.5, we need the following lemma.

LEMMA 3.2. *We have*

$$\mathrm{SL}_n(\mathbb{Q}) \cdot \mathrm{SL}_n(\hat{\mathbb{Z}}) = \mathrm{SL}_n(\mathbf{A}_{\mathbb{Q},\{\infty\}}).$$

PROOF. If $n = 1$, we have $\mathrm{SL}_n(\mathbf{A}_{\mathbb{Q},\{\infty\}}) = \{(1)\}$, which is trivial.

We let $\mathrm{SL}_n(\mathbb{Q})$ act on the left and $\mathrm{SL}_n(\hat{\mathbb{Z}})$ on the right of $\mathrm{SL}_n(\mathbf{A}_{\mathbb{Q},\{\infty\}})$. Note that $\prod_{p \text{ prime}} \mathrm{SL}_n(\mathbb{Z}_p) = \mathrm{SL}_n(\hat{\mathbb{Z}})$, so we can give elements of $\mathrm{SL}_n(\hat{\mathbb{Z}})$ by giving an element of $\mathrm{SL}_n(\mathbb{Z}_p)$ for every prime p.

Step	**Outcome**
Take $m \in \mathrm{SL}_n(\mathbf{A}_{\mathbb{Q},\{\infty\}})$.	$\begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ m_{21} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{pmatrix}$
For all p simultaneously: Let ord_p be the p-adic valuation on the p-th component of elements of $\mathbf{A}_{\mathbb{Q},\{\infty\}}$. Take $i \geq 2$ such that $\mathrm{ord}_p(m_{1i})$ is minimal. If $\mathrm{ord}_p(m_{11}) > \mathrm{ord}_p(m_{1i})$, add m_{1i} to m_{11}. Then for all i, we have $\mathrm{ord}_p(m_{11}) \leq \mathrm{ord}_p(m_{1i})$.	
We have for all $i \geq 2$, and all primes p, $\mathrm{ord}_p\left(\frac{m_{1i}}{m_{11}}\right) \geq 0$, so $\frac{m_{1i}}{m_{11}} \in \hat{\mathbb{Z}}$. For all $i \geq 2$, add $-\frac{m_{1i}}{m_{11}}$ times m_{11} to m_{1i}, to make sure that $m_{1i} = 0$.	$\begin{pmatrix} m_{11} & 0 & \dots & 0 \\ m_{21} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{pmatrix}$
Note that the determinant of the bottom right $(n-1)\times(n-1)$ submatrix times m_{11} gives 1. Since both of these numbers are in $\mathbf{A}_{\mathbb{Q},\{\infty\}}$, we have for all but finitely many primes p that $\mathrm{ord}_p(m_{11}) = 0$. Therefore, the number $q = \prod_p p^{-\mathrm{ord}_p(m_{11})} \in \mathbb{Q}$ exists. We multiply the first row by q (and the second row by q^{-1}) to have $m_{11} = 1$.	$\begin{pmatrix} 1 & 0 & \dots & 0 \\ m_{21} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{pmatrix}$
Now, the bottom right $(n-1)\times(n-1)$ submatrix is an element of $\mathrm{SL}_{n-1}(\mathbf{A}_{\mathbb{Q},\{\infty\}})$. If we repeat the above for this submatrix (induction), we get $m_{ii} = 1$ and $m_{ij} = 0$ for all $i < j$.	$\begin{pmatrix} 1 & 0 & \dots & 0 \\ m_{21} & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & 1 \end{pmatrix}$
Because $\mathbb{Q}$ satisfies strong approximation away from ∞, there exists an element $m'_{21} \in \mathbb{Q}$ such that $m_{21} - m'_{21} \in \hat{\mathbb{Z}}$. We subtract m'_{21} times m_{11} from m_{21} such that the resulting $m_{21} \in \hat{\mathbb{Z}}$. Then we subtract m_{21} times m_{22} from m_{21} such that $m_{21} = 0$.	$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & 1 \end{pmatrix}$

Repeat this for $m_{31}, \ldots, m_{n1}$, then for $m_{32}, \ldots, m_{n2}$ and so on for $m_{43}, \ldots, m_{n,(n-1)}$. This completes the proof. $\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$

□

THEOREM 3.1. SL_n *satisfies strong approximation away from infinity.*

PROOF. We have proved that $\mathrm{SL}_n(\mathbb{Z})$ is dense in $\mathrm{SL}_n(\hat{\mathbb{Z}})$. By the previous lemma, we have that $\mathrm{SL}_n(\mathbb{Q}) \cdot \mathrm{SL}_n(\hat{\mathbb{Z}}) = \mathrm{SL}_n(\mathbf{A}_{\mathbb{Q},\{\infty\}})$. Then Lemma 2.5 gives that SL_n satisfies strong approximation away from infinity. □

2. C_2

We will now use Lemma 2.4 to prove that C_2 satisfies strong approximation away from infinity. To this end, we first need to establish surjectivity of a map $\mathrm{SL}_2 \to C_2$ on adelic points.

LEMMA 3.3. *For all rings* R, $\mathrm{SL}_2(R)$ *acts transitively on* $C_2(R)$.

PROOF. Let $x \in C_2(R)$. Then $x_1R + x_2R = R$, so there exist $y_1, y_2 \in R$ such that $x_1y_2 - x_2y_1 = 1$. Then we have

$$m = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \in \mathrm{SL}_2(R)$$

and $m(1,0)^T = x$. □

THEOREM 3.2. C_2 *satisfies strong approximation away from infinity.*

PROOF. If we compose the group scheme action $\mathrm{SL}_2 \times C_2 \to C_2$ with the embedding $\mathrm{SL}_2 \times \{(1,0)^T\} \to \mathrm{SL}_2 \times C_2$, we obtain a morphism $f : \mathrm{SL}_2 \to C_2$ (this is just the group action on the point $(1,0)^T$). We have already proved that the group action on R-points is transitive for any ring R, which means that in particular f is surjective on $\mathbf{A}_{\mathbb{Q},\{\infty\}}$-points.

Since we already proved that SL_2 satisfies strong approximation away from infinity, we use Lemma 2.4 to conclude that C_2 satisfies strong approximation away from infinity. □

3. $C_4(q_0)$

Now we do the same for the map $C_2 \times C_2 \to C_4(q_0)$, defined in Section 1.5.

LEMMA 3.4. *The map* $C_2 \times C_2 \to C_4(q_0)$ *is surjective on* R*-points for all local rings* R.

PROOF. Let R be a local ring with maximal ideal $\mathfrak{m}$. Note that $\mathfrak{m}$ contains every prime ideal of R. Take $x \in C_4(q_0)(R)$. Assume that $x_1 \notin \mathfrak{m}$. Then x_1 is invertible. Note that $x_1x_4 = x_2x_3$. Then $((1, \frac{x_3}{x_1})^T, (x_1, x_2)^T)$ is mapped to $(x_1, x_2, x_3, \frac{x_2x_3}{x_1})^T = x$. The cases where x_2, x_3 or x_4 is not in $\mathfrak{m}$ are completely analogous, which completes the proof. □

LEMMA 3.5. *For any* $T \subseteq \Omega_k$, *the map* $C_2 \times C_2 \to C_4(q_0)$ *is surjective on* $\mathbf{A}_{k,T}$*-points.*

PROOF. By Exercise 3.7 of [**Poo17**], for a $\mathcal{O}_k$-scheme X of finite type, we have a bijection $X(\mathbf{A}_{k,T}) \xrightarrow{\sim} \prod'_{v\in\Omega_k\setminus T}(X(k_v), X(\mathcal{O}_v))$.

Note that k_v and $\mathcal{O}_v$ are local rings. Therefore, given any element $(x_v)_{v\in\Omega_k\setminus T}$ of $C_4(q_0)(\mathbf{A}_{k,T})$ we can find by the previous Lemma, for every $v \in \Omega_k \setminus T$, a preimage $y_v \in (C_2 \times C_2)(k_v)$ of $x_v \in C_4(q_0)(k_v)$. Note that for almost all places v, $x_v \in C_4(q_0)(\mathcal{O}_v)$, in which case we can take $y_v \in (C_2 \times C_2)(\mathcal{O}_v)$. Then $(y_v)_{v\in\Omega_k\setminus T} \in (C_2 \times C_2)(\mathbf{A}_{k,T})$ and $(y_v)_{v\in\Omega_k\setminus T}$ is mapped to $(x_v)_{v\in\Omega_k\setminus T}$. □

THEOREM 3.3. *$C_4(q_0)$ satisfies strong approximation away from infinity.*

PROOF. Note that the topology of $(C_2 \times C_2)(\mathbf{A}_{\mathbb{Q},\{\infty\}})$ is the product topology (by Lemma 2.3), so, using 3.2, $(C_2 \times C_2)(\mathbb{Q})$ is dense in $(C_2 \times C_2)(\mathbf{A}_{\mathbb{Q},\{\infty\}})$. We have a morphism $C_2 \times C_2 \to C_4(q_0)$ that is surjective on $\mathbf{A}_{\mathbb{Q},\{\infty\}}$-points. Then by Lemma 2.4, $C_4(q_0)$ satisfies strong approximation from infinity. □

CHAPTER 4

Interlude: Finding a Better Model

In this thesis, we work with the quadratic form q_1' over $\mathbb{Z}$ which has a bad reduction modulo the primes 47 and 103, but is smooth over $\mathbb{Q}$. This is a problem that arises sometimes in algebraic geometry: we have a scheme X over a domain R (with fraction field K), in this case given by a single equation, with X_K smooth, but $X_{R/\mathfrak{p}}$ singular for one or more primes $\mathfrak{p} \subseteq R$. In that case, we can attempt to find a better model: a scheme X', with $X_K \cong X'_K$, but with less singular fibers. We will call this a better model for X.

We have a set of quadratic forms in n variables over R. If 2 is not zero in R, we can associate to these the set $Q_n(R)$ of symmetric matrices m in $\mathrm{Mat}_{n\times n}(K)$ with $m_{ij} + m_{ji} \in R$ and $m_{ii} \in R$ for all i and j, such that for every quadratic form q its associated matrix m satisfies $q(x) = x^T m x$ for all $x \in R^n$.

1. Better models

Now, suppose for $R = \mathbb{Z}$ or $R = \mathbb{Z}_p$, we have some quadratic form q with an associated matrix $m \in Q_n(R)$. Suppose that $\det(m) \neq 0$.

LEMMA 4.1. *The morphism $f : C_n(q)_{\mathbb{Z}_p} \to \mathrm{Spec}\,(\mathbb{Z}_p)$ is flat iff q is not divisible by p (i.e. if there exist i and j such that $p \nmid 2m_{ij}$).*

PROOF. Take $A = \mathbb{Z}_p[X_1, \ldots, X_n]/(q)$. By Example 3.3.2 in [**Poo17**], A is flat over $\mathbb{Z}_p$ iff it is a torsion-free $\mathbb{Z}_p$-module.

Now, suppose that $p \mid q$. Then for all i, $\frac{q}{p} \neq 0 \in A[Y]/(X_iY - 1)$, but $p \cdot \frac{q}{p} = q = 0 \in A[Y]/(X_iY - 1)$, so $A[Y]/(X_iY - 1)$ is not torsion-free. Therefore, $\mathbb{Z}_p \to A$, and thereby $\mathrm{Spec}\, A \to \mathrm{Spec}\,(\mathbb{Z}_p)$, is not flat, so the standard affine open subsets of $C_n(q)_{\mathbb{Z}_p}$ are not flat over $\mathbb{Z}_p$. Since flatness is a local property, this implies that f is not flat either.

For the converse, since $p \nmid q$, for q to be a reducible polynomial in $\mathbb{Z}_p[X_1, \ldots, X_n]$, we need

$$q = \left(\sum r_i X_i\right)\left(\sum r' i X_i\right)$$

for $r, r' \in \mathbb{Z}_p^n$. However, then $m = r(r')^T$, so $\det(m) = 0$, which we assumed not to be true. Therefore, q is irreducible. Since $\mathbb{Z}_p[X_1, \ldots, X_n]$ is a uniform factorization domain, q is prime, so (q) is a prime ideal and A is a domain. Especially, A is torsion-free as a $\mathbb{Z}_p$-module, the standard open subsets of $C_n(q)_{\mathbb{Z}_p}$ are flat over $\mathbb{Z}_p$ and f is flat. □

REMARK 4.1. Note that for $X_1, \dots, X_n \in \mathbb{Z}[X_1, \dots, X_n]$ and $x = (X_1, \dots, X_n)^T$, we have for all i,

$$\begin{aligned}\frac{\partial q}{\partial X_i} &= \frac{\partial}{\partial X_i} \sum_{j,k} m_{jk} X_j X_k \\ &= 2 \sum_j m_{ij} X_i \\ &= ((2m)x)_i .\end{aligned}$$

LEMMA 4.2. *If $p \nmid \det(2m)$, the morphism $f : C_n(q)_{\mathbb{Z}_p} \to \operatorname{Spec}(\mathbb{Z}_p)$ is smooth. For $p \neq 2$, the converse also holds.*

PROOF. By Definition 3.5.27 in [**Poo17**], since f is locally of finite presentation and by Lemma 4.1 it is flat, smoothness over $\mathbb{Z}_p$ is equivalent to smoothness over $\overline{\mathbb{Q}_p}$ and $\overline{\mathbb{F}_p}$.

Suppose that $p \nmid \det(2m)$. By Proposition 3.5.17 in [**Poo17**], we can just show smoothness on closed points. We will show that for both $k = \overline{\mathbb{F}_p}$ and $k = \overline{\mathbb{Q}_p}$, for

$$X = \operatorname{Spec}(k[X_1, \dots, X_n]/(q)),$$

$g : X \to \operatorname{Spec} k$ is smooth at all closed points, except $(X_1, \dots, X_n)$. Since $C_n(q)_k$ equals X, except for this point, and smoothness is a local condition, this shows that $C_n(q)_k$ is smooth.

Let

$$\mathfrak{m} = (X_1 - x_1, \dots, X_n - x_n)$$

be a closed point (note that we take the x_i in k). Take $x = (x_1, \dots, x_n)^T$. Suppose that X is not smooth at $\mathfrak{m}$. Then

$$\left(\frac{\partial q}{\partial X_1}(\mathfrak{m}), \frac{\partial q}{\partial X_2}(\mathfrak{m}), \dots, \frac{\partial q}{\partial X_n}(\mathfrak{m}) \right) \in \operatorname{Mat}_{1 \times n}(k)$$

has rank 0, so $\frac{\partial q}{\partial X_i}(\mathfrak{m}) = 0$ for all i. By Remark 4.1, $2mx = \mathbf{0}$. Note that $\det(2m) \in k^*$, so $2m$ is invertible over k and we have

$$x = (2m)^{-1}\mathbf{0} = \mathbf{0}.$$

Therefore, $C_n(q)_k$ is smooth.

On the other hand, suppose that $p \neq 2$ and $p \mid 2m$. Then over $\mathbb{F}_p$, the null space of $2m$ is nontrivial, so we have $x := (x_1, \dots, x_n)^T \in \mathbb{F}_p^n$ such that $x_i \neq 0$ for some x, and $2mx = \mathbf{0}$. Since $p \neq 2$, we have $x^T m x = x^T \mathbf{0} = 0$ and $\mathfrak{m} := (X_1 - x_1, \dots, X_n - x_n) \in C_n(q)_{\mathbb{F}_p}$. By Remark 4.1, we have

$$\left(\frac{\partial q}{\partial X_1}(\mathfrak{m}), \frac{\partial q}{\partial X_2}(\mathfrak{m}), \dots, \frac{\partial q}{\partial X_n}(\mathfrak{m}) \right) = (2mx)^T = \mathbf{0}^T$$

has rank 0 and $C_n(q)_{\mathbb{F}_p}$ is singular at $\mathfrak{m}$. □

In this chapter, we will only consider **linear** transformations between the models. To be more precise, we are looking for a matrix $t \in \mathrm{GL}_n(K)$ such that

MI1 $q \circ t$ is defined over R, or equivalently, $t^T m t \in Q_n(R)$;

MI2 $p \nmid \det(2t^T m t) = \det(t)^2 \cdot \det(2m)$.

We will call this a **model improvement** for q with respect to p.

We can immediately deduce from MI2 that it is impossible to find a model improvement with respect to a prime $p \neq 2$ if $\operatorname{ord}_p(\det(2m))$ is odd.

REMARK 4.2 (Transforming transformations). Suppose that R is a principal ideal domain, and we have a matrix $m \in Q_n(R)$ and a model improvement t for m with respect to a prime p.

We can embed S_n into $\mathrm{GL}_n(\mathbb{Z}) \subseteq \mathrm{GL}_n(R)$ by letting elements of S_n permute the standard basis vectors. Given such a $g \in S_n \subseteq \mathrm{GL}_n(R)$, $(g^{-1})^T m g^{-1}$ is m but with its rows and columns permuted (both in the same way). Then gt is a model improvement for it. Therefore, S_n acts on the left on 'the set of permutations of m, together with their model improvements with respect to p'.

If we take $g \in \mathrm{GL}_n(R)$, then tg transforms m to $g^T(t^T m t)g \in Q_n(R)$ and this has determinant $\det(g)^2 \det(t^T m t)$ with $\det(g)^2 \in R^*$, so tg is a model improvement with respect to the same primes as t. Therefore, $\mathrm{GL}_n(R)$ acts on the right on the set of 'model improvements for m with respect to p'. In particular, we can add $a \in R$ times one column to another, multiply a column by a factor $b \in R^*$ or interchange columns.

2. Assumptions about transformations

Suppose that R is a principal ideal domain, with fraction field K. For a vector v, and a prime p, let $\mathrm{ord}_p(v) = \min_i\{\mathrm{ord}_p(v_i)\}$. For an $n \times n$ matrix t, let t_{*i} denote its ith column.

From now on, we will mostly work with $R = \mathbb{Z}$ and $K = \mathbb{Q}$, or $R = \mathbb{Z}_p$ and $K = \mathbb{Q}_p$. Take $m \in Q_n(\mathbb{Z})$.

First of all, it is easier to work with diagonal matrices than with general matrices. The following proof shows that for most purposes, we can restrict to the diagonal case.

LEMMA 4.3. *For $p \neq 2$, we can find $a \in \mathbb{Z}$ with $p \nmid a$, and $t \in \mathrm{SL}_n\left(\mathbb{Z}\left[\frac{1}{a}\right]\right)$ such that $t^T m t$ is diagonal.*

PROOF. See also the corresponding code at [**vdL23**].

Here we let $\mathrm{SL}_n\left(\mathbb{Z}\left[\frac{1}{a}\right]\right)$ act on $Q_n\left(\mathbb{Z}\left[\frac{1}{a}\right]\right)$ on the right with

$$(m, g) \mapsto g^T m g.$$

Step	**Outcome**
We start with m given, and $a = 1$.	$\begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ m_{12} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{1n} & m_{2n} & \dots & m_{nn} \end{pmatrix}$
If $\mathrm{ord}_p(m_{*1}) > \min_j\{\mathrm{ord}_p(m_{*j})\}$, there exists i such that $\mathrm{ord}_p(m_{*i}) = \min_j\{\mathrm{ord}_p(m_{*j})\}$. We switch the first and ith column (and row), such that the order of the first column is minimal.	
If $\mathrm{ord}_p(m_{11}) > \mathrm{ord}_p(m_{*1})$ (so $p \mid p^{-\mathrm{ord}_p(m_{*1})} m_{11}$), there exists i such that $\mathrm{ord}_p(m_{i1}) = \mathrm{ord}_p(m_{*1})$. Since $p \neq 2$, we can add 1 or 2 times the ith column and row to the first one, to make sure that $\mathrm{ord}_p(m_{11}) = \mathrm{ord}_p(m_{*1})$.	
If we take a to be the least common multiple of a and the numerator of $m_{11} p^{-\mathrm{ord}_p(m_{11})}$, we have for all $i > 1$ that $\frac{m_{1i}}{m_{11}} \in \mathbb{Z}\left[\frac{1}{a}\right]$, so we can add $-\frac{m_{1i}}{m_{11}}$ the first row and column to the ith one to make sure that in the first row and column, m_{11} is the only nonzero value.	$\begin{pmatrix} m_{11} & 0 & \dots & 0 \\ 0 & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & m_{2n} & \dots & m_{nn} \end{pmatrix}$

If we repeat this for m_{22} till m_{nn}, by induction, we get the required $a \in \mathbb{Z}$ and $t \in \mathrm{SL}_n\left(\mathbb{Z}\left[\frac{1}{a}\right]\right)$ such that $t^T m t$ is diagonal.

$$\begin{pmatrix} m_{11} & 0 & \dots & 0 \\ 0 & m_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & m_{nn} \end{pmatrix}$$

□

COROLLARY 4.1. *Since for all $a \in \mathbb{Z}$ such that $p \nmid a$, we have $\mathbb{Z}\left[\frac{1}{a}\right] \subseteq \mathbb{Z}_p$, any time we work over $\mathbb{Z}_p$ or $\mathbb{Z}/p^k\mathbb{Z}$, we can assume that m is diagonal if $p \neq 2$.*

Now, usually $\mathbb{Z}_p$ is much easier to deal with than $\mathbb{Z}$. The following lemma shows that if we can find a model improvement of a certain form over $\mathbb{Z}_p$, this will automatically give us a model improvement over $\mathbb{Z}$.

LEMMA 4.4. *Suppose that we have $r' \in \mathrm{SL}_n(\mathbb{Z}_p)$, $s_1, \dots, s_n \in \mathbb{Z}$ and $s = \mathrm{diag}(p^{s_1}, \dots, p^{s_n})$ such that $2\sum_i s_i = -\operatorname{ord}_p(\det(2m))$ and for all i and j,*

$$(r'_{*i})^T m r'_{*j} \equiv 0 \mod p^{-(s_i+s_j)}.$$

Take $s_{min} = \min_i\{s_i\}$. Then

(1) there exists $r \in \mathrm{SL}_n(\mathbb{Z})$ such that

$$r'_{ij} \equiv r_{ij} \mod p^{-(s_j+s_{min})} \qquad \text{for all } i \text{ and } j; \tag{1}$$

(2) for each $r \in \mathrm{SL}_n(\mathbb{Z})$ that satisfies 1, rs is a model improvement.

PROOF. (1) By Lemma 3.1, the reduction $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/a\mathbb{Z})$ is surjective for all $a \in \mathbb{Z}_{>0}$. Take $a = p^{-2s_{min}}$, which gives the result.

(2) Take $r \in \mathrm{SL}_n(\mathbb{Z})$ that satisfies 1. First of all, note that

$$\operatorname{ord}_p(\det(2(rs)^T m(rs))) = 2\operatorname{ord}_p(\det(s)) + \operatorname{ord}_p(2m) = 0,$$

so MI1 is satisfied. Secondly, note that the only denominators in rs are powers of p and for all i and j,

$$\begin{aligned} p^{-(s_i+s_j)}\left((rs)^T m(rs)\right)_{ij} &= p^{-(s_i+s_j)}(rs)^T_{*i} m(rs)_{*j} \\ &= p^{-(s_i+s_j)} p^{s_i+s_j} r^T_{*i} m r_{*j} \\ &= r^T_{*i} m r_{*j} \\ &\equiv (r'_{*i})^T m r'_{*j} \mod p^{-(s_i+s_j)} \\ &\equiv 0 \mod p^{-(s_i+s_j)}. \end{aligned}$$

so $(rs)^T m(rs)$ has neither denominators that are powers of p, nor other denominators (except possibly for a factor of 2). Therefore, $(rs)^T m(rs) \in Q_n(\mathbb{Z})$ so MI2 is satisfied and rs is a model improvement.

□

Now, it turns out that if we have a model improvement with respect to some prime, we can simplify it to get a sort of 'canonical' form:

LEMMA 4.5. *If there exists a model improvement t over $\mathbb{Z}_p$, there exist $s_1 \leq s_2 \leq \dots \leq s_n \in \mathbb{Z}$ for all i and there exists a lower triangular matrix $r \in \mathrm{SL}_n(\mathbb{Z})$ with $r_{ii} = 1$ for all i such that for $s = \mathrm{diag}(p^{s_1}, \dots, p^{s_n})$, rs is a model improvement for (a permuted version of) m, i.e.:*

(1) $\sum_i s_i = \operatorname{ord}_p(\det t)$;

(2) we can permute the rows and columns of m (with the same permutation for both) to get a matrix m', such that $(rs)^T m'(rs) \in Q_n(\mathbb{Z})$.

PROOF. See also the corresponding code at [**vdL23**].

In this proof, we will let S_n and $\mathrm{SL}_n(\mathbb{Z}_p)$ act on the left and right of t respectively.

Step	**Outcome**
By Remark 4.2, we can exchange the first column with another column (if necessary) such that $\mathrm{ord}_p(t_{*1}) \leq \mathrm{ord}_p(t_{*j})$ for all j. Take $s_1 = \mathrm{ord}_p(t_{*1})$. We can also exchange the first row with another row (if necessary) such that $\mathrm{ord}_p(t_{11}) = s_1$ (and perform the same exchange on these rows and columns of m).	$\begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & t_{nn} \end{pmatrix}$
Note that $p^{-s_1} t_{11} \in \mathbb{Z}_p^*$, so we can divide the first column by it, to obtain $t_{11} = p^{s_1}$.	$\begin{pmatrix} p^{s_1} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & t_{nn} \end{pmatrix}$
Since $s_1 = \mathrm{ord}_p(t_{*1}) \leq \mathrm{ord}_p(t_{*2}) \leq \mathrm{ord}_p(t_{12})$, we have $p^{-s_1} t_{12} \in \mathbb{Z}_p$. Therefore, we can subtract $p^{-s_1} t_{12}$ times t_{11} from t_{12} to get $t_{12} = 0$.	$\begin{pmatrix} p^{s_1} & 0 & \dots & t_{1n} \\ t_{21} & t_{22} & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & t_{nn} \end{pmatrix}$
In the same way, we can make sure that $t_{1j} = 0$ for all $j \geq 2$. Note that by doing this, the $\mathrm{ord}_p(t_{*j})$ can only increase, so they will stay larger than $\mathrm{ord}_p(t_{*1})$.	$\begin{pmatrix} p^{s_1} & 0 & \dots & 0 \\ t_{21} & t_{22} & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & t_{nn} \end{pmatrix}$
We can repeat the above for the second through nth columns (by induction), to make sure that for all $i < j$, $t_{ij} = 0$ and for all i, $t_{ii} = p^{s_i}$.	$\begin{pmatrix} p^{s_1} & 0 & \dots & 0 \\ t_{21} & p^{s_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & p^{s_n} \end{pmatrix}$

Note that ts^{-1} is a lower triangular matrix with entries in $\mathbb{Z}_p$ and all 1s on the diagonal. Taking $r' = ts^{-1}$, we can trivially find a matrix r as in the first part of Lemma 4.4 with all 1s on the diagonal. The second part of Lemma 4.4 gives us that r is indeed a model improvement on a permuted version of m with respect to p. □

COROLLARY 4.2. *Let m', the matrix $r \in \mathrm{SL}_n(\mathbb{Z})$ and $s_1 \leq \cdots \leq s_n \in \mathbb{Z}$ be given by the last lemma and assume that m is diagonal. If $s_1 + s_n \leq 1$, we have a nontrivial solution to the quadratic equation*

$$\sum_{i : p \mid m'_{ii}} x_{i1}^2 \frac{m'_{ii}}{p} \equiv 0 \mod p. \tag{2}$$

PROOF. Suppose that $s_1 + s_n \leq 1$. Then $s_1 + s_i \leq 1$ for all i. Recall that in order to satisfy MI1, we must have $(r_{*i})^T m' (r_{*j}) \equiv 0 \mod p^{-s_i - s_j}$ for all i and j. That means that

$$0 \equiv (r_{*1})^T m' r_{*n} = r_{n1} m'_{nn} 1 = r_{n1} m'_{nn} \mod p.$$

So either $p \mid m'_{nn}$ or $p \mid r_{n1}$. Continuing, we find

$$\begin{aligned} 0 &\equiv (r_{*1})^T m'(r_{*,(n-1)}) \\ &= r_{(n-1),1} m'_{(n-1),(n-1)} 1 + r_{n1} m'_{nn} r_{n,(n-1)} \\ &\equiv r_{(n-1),1} m'_{(n-1),(n-1)} \mod p. \end{aligned}$$

Therefore, either $p \mid m'_{(n-1),(n-1)}$ or $p \mid r_{(n-1),1}$. Doing this for all i yields that $p \nmid m'_{ii}$ implies that $p \mid r_{i1}$. Note that $s_1 \leq 1$ so $2s_1 \leq 2$. This gives

$$0 \equiv (r_{*1})^T m' r_{*1} = \sum_i r_{i1}^2 m'_{ii} \mod p^2.$$

However, since if $p \nmid m'_{ii}$, $p \mid r_{i1}$, so $p^2 \mid r_{i1}^2$, we have

$$\sum_{i:p|m'_{ii}} r_{i1}^2 m'_{ii} \equiv 0 \mod p^2$$

and

$$\sum_{i:p|m'_{ii}} r_{i1}^2 \frac{m'_{ii}}{p} \equiv 0 \mod p.$$

□

Conjecture 4.1. A (somewhat wishful) conjecture is that it is only possible to construct a model improvement with respect to a prime p if Equation (2) has a solution. In a small numerical search, no counterexamples were found for $n = 4$ and $(s_1, s_2, s_3, s_4) = (-1, -1, 0, 1)$.

If this conjecture holds, a model improvement exists iff it is possible to repeatedly construct partial model improvements (see section 4).

The last lemma shows that we only have to look for model improvements with a very specific form: we can restrict our search to matrices with determinant $p^{-\frac{1}{2}\operatorname{ord}_p(\det m)}$ that are (up to permutation of the rows) a lower triangular matrix in $\mathrm{SL}_n(\mathbb{Z})$ times a diagonal matrix that has the (positive and negative) powers of p.

It also shows that it is sufficient to construct a model improvement over $\mathbb{Z}_p$, because we can then always find a model improvement over $\mathbb{Z}$.

3. A counterexample

We already saw that if $\operatorname{ord}_p(\det(2m))$ is odd, finding a model improvement is impossible. Now, for

$$m = \operatorname{diag}(1, 1, 3, 3),$$

we have $\det(2m) = 16 \cdot 9$, so it would be nice if we could find a model improvement t with respect to 3. Since $\det(t) = \frac{1}{3}$, at least one of the entries of t must have 3 in the denominator and we must have $\operatorname{ord}_3(t_{*i}) \leq -1$ for some $i \leq 3$. We can assume without loss of generality that $i = 1$. Then $t'_{*1} = 3^{-\operatorname{ord}_3(t_{*i})} t_{*i}$ must satisfy ${t'_{11}}^2 + {t'_{21}}^2 + 3{t'_{31}}^2 + 3{t'_{41}}^2 \equiv 0 \mod 9$.

Reducing the equation modulo 3 gives ${t'_{11}}^2 + {t'_{21}}^2 \equiv 0 \mod 3$, which only has the solution $t'_{11} \equiv t'_{21} \equiv 0 \mod 3$ and ${t'_{11}}^2 \equiv {t'_{21}}^2 \equiv 0 \mod 9$. Therefore, we must have $3{t'_{31}}^2 + 3{t'_{41}}^2 \equiv 0 \mod 9$, so ${t'_{31}}^2 + {t'_{41}}^2 \equiv 0 \mod 3$, which only has the solution $t'_{31} \equiv t'_{41} \equiv 0 \mod 3$. This contradicts the fact that either t'_{11}, t'_{21}, t'_{31} or t'_{41} is nonzero modulo 3.

Therefore, we cannot find a better model with respect to 3 for this quadratic form.

We can do this for any prime p: We can find $a, b \in \mathbb{Z}$ such that a and b are not squares modulo p. Then, for all $c, d \in \mathbb{Z}$, both not divisible by p,

$$m = \operatorname{diag}(c, -ac, pd, -pbd)$$

has $\operatorname{ord}_p(\det(2m)) = 2$, but we cannot find a model improvement with respect to p.

4. Constructing a model improvement

4.1. The case $p \neq 2$. In this subsection, we will work over $\mathbb{Z}_p$ with $p \neq 2$. Therefore, we can assume that m is diagonal by Lemma 4.3. Now, by transforming by a diagonal matrix with powers of $\frac{1}{p}$ on the diagonal, where necessary, we can assume that for all i, $p^2 \nmid m_{ii}$.

Now, we will order the diagonal entries of m such that p divides the first k entries and doesn't divide the $n-k$ entries after that. Note that, to be able to find a model improvement, we need k to be even.

Definition 4.1. We define a **partial model improvement** to be a matrix $t \in \mathrm{GL}_n(\mathbb{Q}_p)$ such that

PMI1 $t^T m t \in Q_n(\mathbb{Z}_p)$;
PMI2 $\operatorname{ord}_p(\det(t^T m t)) = \operatorname{ord}_p(\det(2m)) - 2$.

Lemma 4.6. *If Equation* (2) *has a nontrivial solution, we can find a partial model improvement.*

Proof. Suppose that we can find a nontrivial solution $\bar{x_1}, \ldots, \bar{x_k} \in \mathbb{F}_p$ to Equation (2). We can lift the $\bar{x}_i$ to $x_1, \ldots, x_k \in \mathbb{Z}_p$ (we pick an arbitrary lift of the $\bar{x}_i$). By reordering $m_{11}, \ldots, m_{kk}$ and $x_1, \ldots, x_k$ correspondingly, we can assume that $p \nmid x_1$. Then, by dividing the x_i by x_1 (we can do that because Equation (2) is homogeneous), we can assume that $x_1 = 1$. Now, take

$$r = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ x_2 & 1 & 0 & \ldots & 0 \\ x_3 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \in \mathrm{SL}_n(\mathbb{Z}_p) \quad \text{and} \quad s = \operatorname{diag}\left(\frac{1}{p}, 1, 1, \ldots, 1\right).$$

If we take $t = rs$, we get $t^T m t \in Q_n(\mathbb{Z}_p)$ since $p^2 \mid \sum_i x_i^2 m_{ii}$ and $p \mid x_i m_{ii}$ for all $2 \leq i \leq k$. Also, $\det(t) = \frac{1}{p}$, so we remove two factors p from $\det(2m)$. □

We now have the following theorem:

Theorem 4.1. *For diagonal m, of which the first k diagonal entries are divisible by p, if $p \neq 2$ and*

$$(-1)^{\frac{k}{2}} \prod_{i \leq k} \frac{m_{ii}}{p}$$

is a square modulo p, then we can find a better model for m with respect to p.

PROOF. See also the corresponding code at [**vdL23**].

Suppose that $k = 2$. Then the equation tells us that $-\frac{m_{11}m_{22}}{p^2}$ is a square modulo p. Therefore, $-\frac{m_{11}}{m_{22}}$ is also a square modulo p. If we call the root λ, we have a solution to the equation

$$\frac{m_{11}}{p}1^2 + \frac{m_{22}}{p}\lambda^2 \equiv 0 \mod p.$$

Then, by Lemma 4.6 we get a partial model improvement t is, so $\operatorname{ord}_p(t^T m t) = \operatorname{ord}_p(m) - 2 = 0$, which means that t is actually a model improvement and we are done.

On the other hand, suppose that $k \geq 4$. By the Chevalley-Warning theorem, we have a solution to the equation $\frac{m_{11}}{p}x_1^2 + \frac{m_{22}}{p}x_2^2 + \frac{m_{33}}{p}x_3^2 \equiv 0 \mod p$. Then, by Lemma 4.6, we have (if we order the diagonal entries of m in a suitable way) a matrix

$$r = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ \lambda_2 & 1 & 0 & 0 & \dots & 0 \\ \lambda_3 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \quad \text{and} \quad s = \operatorname{diag}\left(\frac{1}{p}, 1, \dots, 1\right)$$

such that rs is a partial model improvement.

Now, take $m' = (rs)^T m r s$. If $p \mid m'_{11}$, we have $p \nmid m'_{1i}$ for some $i \in \{2, 3\}$. We can then add once or twice the ith row and column to the first one of m' to make sure that $p \nmid m'_{11}$. The result is the same as when we would have added p or $2p$ to λ_i in r. Therefore, we assume that $p \nmid m'_{11}$.

Now, since $p^2 \nmid m_{11}$, we must have either $p \nmid \lambda_2$ or $p \nmid \lambda_3$. By, if necessary, exchanging m_{22} and m_{33}, we can assume that $p \nmid \lambda_2$.

The following will only change the upper left 3×3 submatrix of our matrix, so we will only show what happens there. We have

$$(rs)^T m r s = \begin{pmatrix} \mu_1 & \lambda_2\frac{m_{22}}{p} & \lambda_3\frac{m_{33}}{p} & \dots \\ \lambda_2\frac{m_{22}}{p} & m_{22} & 0 & \dots \\ \lambda_3\frac{m_{33}}{p} & 0 & m_{33} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

with $\mu_1 = \frac{m_{11}+\lambda_2^2 m_{22}+\lambda_3^2 m_{33}}{p^2}$. If we then diagonalize with Lemma 4.3, we obtain

$$m' := \begin{pmatrix} \mu_1 & 0 & 0 & \dots \\ 0 & \mu_2 & 0 & \dots \\ 0 & 0 & \mu_3 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

for $\mu_2 = m_{22} - \frac{\lambda_2^2 m_{22}^2}{\mu_1 p^2}$, which is not divisible by p, and for some value of μ_3. Note that the determinant of the submatrix has only changed by a factor of $\frac{1}{p^2}$, so

$$\frac{m_{11}m_{22}m_{33}}{p^2} = \mu_1\mu_2\mu_3 = \mu_1\left(m_{22} - \frac{\lambda_2^2 m_{22}^2}{\mu_1 p^2}\right)\mu_3,$$

and μ_3 is divisible by p. Therefore,

$$\frac{\mu_3}{p} = \frac{\frac{m_{11}}{p}\frac{m_{22}}{p}\frac{m_{33}}{p}}{\mu_1 \frac{m_{22}}{p} p - \lambda_2^2 \left(\frac{m_{22}}{p}\right)^2} \equiv \frac{-\frac{m_{11}}{p}\frac{m_{22}}{p}\frac{m_{33}}{p}}{\lambda_2^2 \left(\frac{m_{22}}{p}\right)^2} \mod p.$$

Therefore,

$$(-1)^{\frac{k}{2}-1} \prod_{i,p|m'_{ii}} \frac{m'_{ii}}{p} \equiv \frac{(-1)^{\frac{k}{2}}}{\lambda_2^2 \left(\frac{m_{22}}{p}\right)^2} \prod_{i,p|m_{ii}} \frac{m_{ii}}{p} \mod p$$

Since the right-hand side is a square modulo p, the left-hand side is a square modulo p as well. By induction, we obtain a model improvement with respect to p, which completes the proof. □

REMARK 4.3. If $n = 4$, the only interesting case is $k = 2$. In that case, we can obtain a model improvement in the way described above if $-\frac{m_{11}}{m_{22}}$ is a square modulo p.

4.2. The case $p = 2$. Now, in the case of $p = 2$, we cannot just diagonalize, so we will assume that m is already diagonal.

LEMMA 4.7. *For m diagonal and $2 \nmid \det(m)$, we can find a model improvement with respect to 2 if the number of diagonal entries that are $1 \mod 4$ equals the number of diagonal entries that are $3 \mod 4$.*

PROOF. See also the corresponding code at [**vdL23**].

We reorder the diagonal entries of m such that we get a block matrix, with diagonal blocks $m_i = \left(\begin{smallmatrix} a_i & 0 \\ 0 & b_i \end{smallmatrix}\right)$ and $a_i \equiv 1 \mod 4$ and $b_i \equiv 3 \mod 4$ for all $i \leq \frac{n}{2}$. Then, we transform using a block matrix t, with diagonal blocks $t_i = \left(\begin{smallmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{smallmatrix}\right)$. Then we have $t_i^T m_i t_i = \left(\begin{smallmatrix} a_i & \frac{1}{2}a_i \\ \frac{1}{2}a_i & \frac{1}{4}(a_i+b_i) \end{smallmatrix}\right) \in Q(\mathbb{Z})$. Note that

$$\det(2t_i^T m_i t_i) = a^2 + \frac{a(a+b)}{2} \equiv 1 + 0 = 1 \mod 2,$$

so $\det(2t^T m t) \equiv 1 \mod 2$ and t is a model improvement with respect to 2. □

5. Combining model improvements with respect to different primes

In the last two sections, we described ways to construct a model improvement with respect to one prime. However, we would like to have a model improvement with respect to all the primes at once.

LEMMA 4.8. *Let $t_1, \ldots, t_k$ be model improvements with respect to primes $p_1, \ldots, p_k$. Then we can find a model improvement t with respect to $p_1, \ldots, p_k$.*

PROOF. See also the corresponding code at [**vdL23**].

Suppose that we have model improvements $t_1, \ldots, t_k$ with respect to primes $p_1, \ldots, p_k$.

Then Lemma 4.5 gives us lower triangular matrices $r_1, \ldots, r_k \in \mathrm{SL}_n(\mathbb{Z})$ and diagonal matrices $s_1, \ldots, s_k$ with $2\det(s_i) = -\operatorname{ord}_{p_i}(m)$ for all i. Note that these give transformations with respect to different permutations of (the rows and columns of) m. Therefore, we will reshuffle the rows of the r_i such that they correspond to the original matrix m again.

Now, let $l = -\min_{i,j}\{\mathrm{ord}_p((s_i)_{jj})\}$. Since SL_n satisfies strong approximation away from infinity, we have $r \in \mathrm{SL}_n(\mathbb{Z})$ such that for all i, $r \equiv r_i \mod p_i^{2l}$. We now take $s = \prod_i s_i$ and $t = rs$. By Lemma 4.4, t is a model improvement with respect to $p_1, \ldots, p_k$. $\square$

CHAPTER 5

The Twist

1. The theory of twisting

Suppose that we have a finite and faithfully flat morphism of schemes $p : S' \to S$.

In this chapter, we will look at fpqc descent of schemes and twists of schemes. The problem of descent is, given an S'-scheme X', finding an S-scheme X such that $X' \cong X \times_S S'$.

We define S'' and S''' as the following fiber products:

$$\begin{array}{ccccc} S''' & \longrightarrow & S'' & \longrightarrow & S' \\ \downarrow & & \downarrow & & \downarrow p \\ S' & \xrightarrow{p} & S' & \xrightarrow{p} & S \end{array}$$

Also, for a finite group G, we define

$$S' \times G = \coprod_{\sigma \in G} \operatorname{Spec} S'$$

Definition 5.1. A **Galois covering** with Galois group G is a finite and faithfully flat morphism of schemes $p : S' \to S$ with a right action of the finite group G on S' such that the morphism $S' \times G \to S''$, given by $(x, \sigma) \mapsto (x, \sigma x)$ is an isomorphism.

Galois coverings generalize finite Galois field extensions. In this thesis, we will only need affine Galois coverings $\operatorname{Spec} R \to \operatorname{Spec} S$ with group G such that we have inclusions into fields $R \subseteq L'$ and $S \subseteq L$ with $L \subseteq L'$ a finite Galois field extension with group G.

Example 5.1. An example of a Galois covering is

$$\operatorname{Spec}\left(\mathbb{Z}\left[\frac{1}{17}, \frac{1+\sqrt{17}}{2}\right]\right) \to \operatorname{Spec}\left(\mathbb{Z}\left[\frac{1}{17}\right]\right).$$

Its Galois group contains one nontrivial element: the ring automorphism that sends $\frac{1+\sqrt{17}}{2}$ to $\frac{1-\sqrt{17}}{2}$.

Example 5.2. Another example of a Galois covering is

$$\operatorname{Spec}\left(\mathbb{Z}\left[\frac{1}{2 \cdot d_1 \cdot d_2 \cdot \cdots \cdot d_n}, \sqrt{d_1}, \ldots, \sqrt{d_n}\right]\right) \to \operatorname{Spec}\left(\mathbb{Z}\left[\frac{1}{2 \cdot d_1 \cdot d_2 \cdot \cdots \cdot d_n}\right]\right)$$

with $\sqrt{d_i} \notin \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_{i-1}})$ for all i. Its Galois group contains 2^n elements and each of these elements is determined by the images of the $\sqrt{d_i}$ (either $\sqrt{d_i}$ or $-\sqrt{d_i}$).

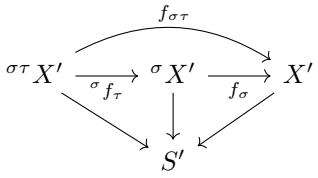
Note that if we have a morphism of schemes $X \to S'$ and an isomorphism $\sigma : S' \to S'$, we can take the fiber product

$$\begin{array}{ccc} Y & \longrightarrow & X \\ \downarrow & & \downarrow \\ S' & \xrightarrow{\sigma} & S' \end{array}.$$

We define ${}^{\sigma}X := Y$.

Now, let $p : S' \to S$ be a Galois covering with Galois group G.

DEFINITION 5.2. We define a **Galois descent datum** to be an S'-scheme X', together with S'-isomorphisms $f_\sigma : {}^{\sigma}X' \to X'$ for every $\sigma \in G$ such that for all $\sigma, \tau \in G$, we have that $f_{\sigma\tau} = f_\sigma \circ ({}^{\sigma}f_\tau)$ (the so-called *cocycle condition*), so the following diagram commutes:



Given two Galois descent data $(X', (f_\sigma)_{\sigma\in G})$ and $(Y', (g_\sigma)_{\sigma\in G})$, we define a **morphism of Galois descent data** to be a morphism $\varphi : X' \to Y'$ such that for all $\sigma \in G$, the following diagram commutes:

$$\begin{array}{ccc} {}^{\sigma}X' & \xrightarrow{f_\sigma} & X' \\ \downarrow{\scriptstyle {}^{\sigma}\varphi} & & \downarrow{\scriptstyle \varphi} \\ {}^{\sigma}Y' & \xrightarrow{g_\sigma} & Y' \end{array}$$

Galois descent data and their morphisms form a category.

Note that for an S-scheme X, we can identify ${}^{\sigma}X_{S'}$ with $X_{S'}$, intuitively because the S'/S-Galois action on a scheme defined over S does not change anything. Therefore, we can identify $f_\sigma : {}^{\sigma}X_{S'} \to X_{S'}$ with an element of $\operatorname{Aut} X_{S'}$, which we will call f_σ as well.

DEFINITION 5.3. A scheme is quasi-affine if it is an open subscheme of an affine scheme and is quasi-compact.

THEOREM 5.1. *If $p : S' \to S$ is fpqc and S is affine (by the definition of a finite Galois covering, p is finite, so S' is affine too), then*

(i) the functor $X \mapsto (X_{S'}, (\mathrm{Id}_{X_{S'}})_{\sigma\in G})$ from S-schemes to S'-schemes with descent data is fully faithful;

(ii) the functor $X \mapsto (X_{S'}, (\mathrm{Id}_{X_{S'}})_{\sigma\in G})$ from (quasi-)affine S-schemes to (quasi-)affine S'-schemes with descent data is an equivalence of categories.

PROOF. This follows from Theorem 4.3.5, Theorem 4.4.4 and Remark 4.4.7 in [**Poo17**]. □

The first part means that for S'-schemes with descent data $(X', (f_\sigma)_{\sigma\in G})$ and $(Y', (g_\sigma)_{\sigma\in G})$ that can be descended to S-schemes X and Y, giving a scheme morphism $X \to Y$ is equivalent to giving a morphism of Galois descent data $(X', (f_\sigma)_{\sigma\in G}) \to (Y', (g_\sigma)_{\sigma\in G})$.

The second part means that every descent datum on a (quasi-)affine S'-scheme can indeed be descended to a (quasi-)affine S-scheme.

Now, let X be an S-scheme.

DEFINITION 5.4. An **S'-twist** of X is an S-scheme Y such that $X_{S'} \cong Y_{S'}$.

Note that twisting X is equivalent to descending $X_{S'}$.

By Theorem 5.1 (ii) we have that for $p : S' \to S$ fpqc and S affine, twisting an S-scheme X is equivalent to giving $f_\sigma \in \operatorname{Aut} X_{S'}$ for all $\sigma \in G$ such that the f_σ satisfy the cocycle condition.

Remark 4.5.4 from [**Poo17**] gives us an explicit way of finding the $(f_\sigma)_{\sigma\in G}$ associated to a twist: for S-schemes X and X', if we choose an isomorphism $\varphi : X_{S'} \to X'_{S'}$, we can take $f_\sigma = \varphi^{-1}({}^\sigma\varphi)$.

EXAMPLE 5.3. To twist a group scheme G that has composition morphism $\varphi : G \times G \to G$, we want to twist not only G but also the morphism φ. Therefore, φ and the f_σ have to be compatible. This means that we want the following diagram to commute for all $\sigma \in G$:

$$\begin{array}{ccc} G \times G & \xrightarrow{(f_\sigma, f_\sigma)} & G \times G \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ G & \xrightarrow{f_\sigma} & G \end{array}$$

In other words, we want f_σ to be a group scheme automorphism.

Note that if f_σ is a group scheme automorphism, we know from group theory that the following diagrams commute on R-points

$$\begin{array}{ccc} G & \xrightarrow{f_\sigma} & G \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} \\ G & \xrightarrow{f_\sigma} & G \end{array} \quad \text{and} \quad \begin{array}{ccc} S & \xrightarrow{\mathrm{Id}} & S \\ \downarrow{\scriptstyle e} & & \downarrow{\scriptstyle e} \\ G & \xrightarrow{f_\sigma} & G \end{array}$$

for $i : G \to G$ the inverse and $e : S \to G$ identity point. Then it follows from the Yoneda Lemma that the diagrams themselves also commute. Therefore, to twist a group scheme, we only have to check whether the f_σ commute with φ for all σ.

2. Twisting for our specific quadratic form q_1

We want to twist the following structure that exists over our base quadratic form $q_0 = X_1X_4 - X_2X_3$, with all parts defined in Chapter 1:

(1) The scheme $C_4(q_0)$.
(2) The scheme $\mathrm{SO}(q_0)$.
(3) The scheme $\widetilde{\mathrm{SO}}(q_0)$.
(4) The group operation $\mathrm{SO}(q_0) \times \mathrm{SO}(q_0) \to \mathrm{SO}(q_0)$.
(5) The group operation $\widetilde{\mathrm{SO}}(q_0) \times \widetilde{\mathrm{SO}}(q_0) \to \widetilde{\mathrm{SO}}(q_0)$.
(6) The group action $\mathrm{SO}(q_0) \times C_4(q_0) \to C_4(q_0)$.
(7) The covering morphism (of group schemes) $\gamma : \widetilde{\mathrm{SO}}(q_0) \to \mathrm{SO}(q_0)$.

Roughy speaking, $C_4(q_0)$ encodes the primitive solutions of q_0. We then have $\mathrm{SO}(q_0)$, (a subgroup of) its symmetry group, defined in Appendix A. $\widetilde{\mathrm{SO}}(q_0)$ is the universal cover of this group, which we can conveniently define as $\mathrm{SL}_2 \times \mathrm{SL}_2$. Their relationships become clear in the following two cartesian diagrams:

$$\begin{array}{ccc} \widetilde{\mathrm{SO}(q_0)} \times \widetilde{\mathrm{SO}(q_0)} & \longrightarrow & \widetilde{\mathrm{SO}(q_0)} \\ \downarrow{\scriptstyle \gamma\times\gamma} & & \downarrow{\scriptstyle \gamma} \\ \mathrm{SO}(q_0) \times \mathrm{SO}(q_0) & \longrightarrow & \mathrm{SO}(q_0) \end{array} \qquad \begin{array}{ccc} \mathrm{SO}(q_0) \times \mathrm{SO}(q_0) \times C_4(q_0) & \longrightarrow & \mathrm{SO}(q_0) \times C_4(q_0) \\ \downarrow & & \downarrow \\ \mathrm{SO}(q_0) \times C_4(q_0) & \longrightarrow & C_4(q_0) \end{array}$$

The first diagram denotes that γ is compatible with the group operations of both group schemes. The second diagram denotes that first doing the group operation and then applying the group action is the same as applying the group action twice.

For the next lemma, we define

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

LEMMA 5.1. *Let* $\operatorname{Spec} A' \to \operatorname{Spec} A$ *be a Galois covering with group* G*. Let* $\varphi : C_4(q_0)_{A'} \xrightarrow{\sim} C_4(q)_{A'}$ *be a linear isomorphism, given by an element* $m \in \mathrm{Isom}(q_0, q)(A')$*. Suppose that*

- *for all* $\sigma \in G$*,* $a_\sigma := m^{-1}({}^\sigma m) \in \mathrm{GO}(q_0)(A')$ *is defined over* A *and commutes with* χ*;*
- *there exists, for every* $\sigma \in G$*, a matrix* $b_\sigma \in \mathrm{GL}_2(A)$ *such that* $\gamma(b_\sigma, b_\sigma) = \lambda a'_\sigma$ *for some* $\lambda \in A^*$*, for* $a'_\sigma = a_\sigma$ *if* $a_\sigma \in \mathrm{SO}(q_0)(A)$ *and* $a'_\sigma = a_\sigma\chi$ *if* $a_\sigma \notin \mathrm{SO}(q_0)(A)$*.*

Then we can twist the structure on $C_4(q_0)$*, given above as components (1)-(7), to a structure on* $C_4(q)$ *as schemes and morphisms over* A*.*

PROOF. We need to provide

(1) a cocycle $f : G \to \mathrm{Aut}(C_4(q_0)_{A'})$;
(2) a cocycle $g : G \to \mathrm{Aut}(\mathrm{SO}(q_0)_{A'})$;
(3) a cocycle $h : G \to \mathrm{Aut}(\widetilde{\mathrm{SO}(q_0)}_{A'})$.

Here, $\mathrm{Aut}(G)$ denotes the group of scheme automorphisms of the group scheme G.

We also need to prove that the following diagrams commute for all $\sigma \in G$, which shows that the f_σ, g_σ and h_σ are actually group scheme automorphisms, and that the g_σ and h_σ are compatible:

$$(4) \qquad \begin{array}{ccc} \mathrm{SO}(q_0) \times \mathrm{SO}(q_0) & \xrightarrow{g_\sigma\times g_\sigma} & \mathrm{SO}(q_0) \times \mathrm{SO}(q_0) \\ \downarrow & & \downarrow \\ \mathrm{SO}(q_0) & \xrightarrow{g_\sigma} & \mathrm{SO}(q_0) \end{array}$$

$$(5) \qquad \begin{array}{ccc} \widetilde{\mathrm{SO}(q_0)} \times \widetilde{\mathrm{SO}(q_0)} & \xrightarrow{h_\sigma\times h_\sigma} & \widetilde{\mathrm{SO}(q_0)} \times \widetilde{\mathrm{SO}(q_0)} \\ \downarrow & & \downarrow \\ \widetilde{\mathrm{SO}(q_0)} & \xrightarrow{h_\sigma} & \widetilde{\mathrm{SO}(q_0)} \end{array}$$

$$(6) \qquad \begin{array}{ccc} \mathrm{SO}(q_0) \times C_4(q_0) & \xrightarrow{g_\sigma\times f_\sigma} & \mathrm{SO}(q_0) \times C_4(q_0) \\ \downarrow & & \downarrow \\ C_4(q_0) & \xrightarrow{f_\sigma} & C_4(q_0) \end{array}$$

$$(7)\qquad \begin{array}{ccc} \widetilde{\mathrm{SO}(q_0)} & \xrightarrow{h_\sigma} & \widetilde{\mathrm{SO}(q_0)} \\ \downarrow & & \downarrow \\ \mathrm{SO}(q_0) & \xrightarrow{g_\sigma} & \mathrm{SO}(q_0) \end{array}$$

To this end, for all $\sigma \in G$, we define the following on R-points:

(1) We set $f_\sigma(x) = a_\sigma x$. This trivially satisfies the cocycle condition.
(2) We set $g_\sigma(m) = a_\sigma m a_\sigma^{-1}$. This trivially satisfies the cocycle condition.
(3) We set $h_\sigma(m_1, m_2) = \begin{cases} (b_\sigma m_1 b_\sigma^{-1}, b_\sigma m_2 b_\sigma^{-1}) & \text{if } a_\sigma \in \mathrm{SO}(q_0)(A) \\ (b_\sigma m_2 b_\sigma^{-1}, b_\sigma m_1 b_\sigma^{-1}) & \text{else} \end{cases}$

We still need to prove that h satisfies the cocycle condition. Therefore, note that the elements of $(\mathrm{GL}_2 \times \mathrm{GL}_2)(A)$ lying above $\lambda I_4 \in \mathrm{GO}(q_0)(A)$ for $\lambda \in A^*$ are exactly of the form $(\lambda\mu I_2, \frac{1}{\mu} I_2)$ for some $\mu \in A^*$. Also note that since the a_σ and b_σ are matrices over A, G acts trivially on the f_σ, g_σ and h_σ. Now, take $\sigma, \tau \in G$. Note that we have (since f is a cocycle and since a_τ commutes with χ)

$$\begin{aligned} I_4 &= a_\sigma a_\tau a_{\sigma\tau}^{-1} \\ &= a_\sigma a_\tau \chi \chi^{-1} a_{\sigma\tau}^{-1} \\ &= a_\sigma \chi a_\tau \chi^{-1} a_{\sigma\tau}^{-1} \\ &= a_\sigma \chi a_\tau \chi a_{\sigma\tau}^{-1} \end{aligned}$$

and therefore $a'_\sigma a'_\tau {a'_{\sigma\tau}}^{-1} = I_4$, regardless of whether a_σ and/or a_τ are in $\mathrm{SO}(q_0)(A)$ or not.

We have that

$$\gamma(b_\sigma b_\tau b_{\sigma\tau}^{-1}, b_\sigma b_\tau b_{\sigma\tau}^{-1}) = \lambda a'_\sigma a'_\tau {a'_{\sigma\tau}}^{-1} = \lambda I_4$$

for some $\lambda \in A^*$. Therefore, $b_\sigma b_\tau b_{\sigma\tau}^{-1} = \mu I_2$ for some $\mu \in A^*$. Then

$$h_\sigma h_\tau h_{\sigma\tau}^{-1}(m_1, m_2) = (b_\sigma b_\tau b_{\sigma\tau}^{-1} m_1 (b_\sigma b_\tau b_{\sigma\tau}^{-1})^{-1}, b_\sigma b_\tau b_{\sigma\tau}^{-1} m_2 (b_\sigma b_\tau b_{\sigma\tau}^{-1})^{-1}) = (m_1, m_2).$$

Since this holds for all $\sigma, \tau \in G$, h satisfies the cocycle condition.

We then have for all σ, the following equalities on R-points, which gives the commutativity of the diagrams by the Yoneda Lemma:

(4) For all $m_1, m_2 \in \mathrm{SO}(q_0)(R)$,

$$a_\sigma^{-1} m_1 a_\sigma \cdot a_\sigma^{-1} m_2 a_\sigma = a_\sigma^{-1} m_1 m_2 a_\sigma.$$

(5) For all $(m_{11}, m_{21}), (m_{12}, m_{22}) \in (\mathrm{SL}_2 \times \mathrm{SL}_2)(R)$, we have, if $a_\sigma \in \mathrm{SO}(q_0)(A)$,

$$(b_\sigma m_{11} b_\sigma^{-1}, b_\sigma m_{21} b_\sigma^{-1}) \cdot (b_\sigma m_{12} b_\sigma^{-1}, b_\sigma m_{22} b_\sigma^{-1}) = (b_\sigma m_{11} m_{12} b_\sigma^{-1}, b_\sigma m_{21} m_{22} b_\sigma^{-1})$$

and else,

$$(b_\sigma m_{21} b_\sigma^{-1}, b_\sigma m_{11} b_\sigma^{-1}) \cdot (b_\sigma m_{22} b_\sigma^{-1}, b_\sigma m_{12} b_\sigma^{-1}) = (b_\sigma m_{21} m_{22} b_\sigma^{-1}, b_\sigma m_{11} m_{12} b_\sigma^{-1}).$$

(6) We have for all $x \in C_4(q_0)(R)$ and $m \in \mathrm{SO}(q_0)(R)$,

$$a_\sigma m a_\sigma^{-1} \cdot a_\sigma x = a_\sigma m x.$$

(7) We have for all $(m_1, m_2) \in (\mathrm{SL}_2 \times \mathrm{SL}_2)(R)$ that if $a_\sigma \in \mathrm{SO}(q_0)(A)$,

$$\gamma(h_\sigma(m_1, m_2)) = \gamma(b_\sigma, b_\sigma)\gamma(m_1, m_2)\gamma(b_\sigma^{-1}, b_\sigma^{-1}) = a_\sigma \gamma(m_1, m_2) a_\sigma^{-1} = g_\sigma(\gamma(m_1, m_2))$$

and else, noting that $\chi\gamma(m_1, m_2)\chi = \gamma(m_2, m_1)$,

$$\gamma(h_\sigma(m_1, m_2)) = \gamma(b_\sigma, b_\sigma)\gamma(m_2, m_1)\gamma(b_\sigma^{-1}, b_\sigma^{-1}) = a_\sigma \chi \gamma(m_2, m_1) \chi a_\sigma^{-1} = g_\sigma(\gamma(m_1, m_2)).$$

This concludes the proof. □

COROLLARY 5.1. *For*

$$q_1 = X_1X_4 + 2X_2^2 - 5X_2X_3 + X_3^2,$$

we can twist the structure on $C_4(q_0)$ to a structure on $C_4(q_1)$ as schemes and morphisms over $A = \mathbb{Z}\left[\frac{1}{17}\right]$.

PROOF. Take the ring

$$A' = \mathbb{Z}\left[\frac{1}{17}, \frac{1+\sqrt{17}}{2}\right].$$

Note that we have a Galois covering $\operatorname{Spec} A' \to \operatorname{Spec}\left(\mathbb{Z}\left[\frac{1}{17}\right]\right)$ with Galois group $\{\mathrm{id}, \sigma\}$. We have an isomorphism $\varphi : C_4(q_0)_{A'} \xrightarrow{\sim} C_4(q_1)_{A'}$, given on R-points by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{17}}{17} & \frac{\sqrt{17}}{17} & 0 \\ 0 & 11\frac{\sqrt{17}}{17} - \frac{\sqrt{17}+1}{2} & -6\frac{\sqrt{17}}{17} + \frac{\sqrt{17}+1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Then we have

$$a_\sigma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad b_\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

Note that a_σ is defined over $\mathbb{Z}$ and commutes with χ. The result follows. □

3. Twisting for a generic quadratic form q

COROLLARY 5.2. *For*

$$q = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$$

for $a_1, \ldots, a_4 \in \mathbb{Z}$, we can twist the structure on $C_4(q_0)$ to a structure on $C_4(q)$ as schemes and morphisms over $A = \mathbb{Z}\left[\frac{1}{2a_1a_2a_3a_4}\right]$.

PROOF. Take $a_0 = -1$ and

$$A' = \mathbb{Z}\left[\frac{1}{2a_1a_2a_3a_4}, \alpha_0, \ldots, \alpha_4\right]$$

for $\alpha_j^2 = a_j$, so $\alpha_0 = i$. Remember from Section 1 that we have a Galois covering $\operatorname{Spec} A' \to \operatorname{Spec} A$ with a Galois group G, with order a power of 2.

Then we have an isomorphism $\varphi : C_4(q_0)_{A'} \to C_4(q)_{A'}$ given on R-points by the matrix

$$\frac{1}{2}\begin{pmatrix} \frac{1}{\alpha_1} & 0 & 0 & 0 \\ 0 & \frac{1}{\alpha_2} & 0 & 0 \\ 0 & 0 & \frac{1}{\alpha_3} & 0 \\ 0 & 0 & 0 & \frac{1}{\alpha_4} \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & -\alpha_0 & -\alpha_0 & 0 \\ -\alpha_0 & 0 & 0 & \alpha_0 \end{pmatrix}.$$

Now, every $\sigma \in G$ is determined by its action on the α_j: for all j, we have $\sigma(\alpha_j) = s_j\alpha_j$ for some $s_j \in \{-1, 1\}$ and σ is determined by the $s_0, \ldots, s_4$. Note that every combination of $s_0, \ldots, s_4$ gives an element $\sigma \in G$ if and only if we have $\alpha_j \notin \mathbb{Q}(\alpha_0, \ldots, \alpha_{j-1})$ for all j.

Then we have

$$a_\sigma = \frac{1}{2}\begin{pmatrix} s_1+s_0s_4 & 0 & 0 & s_1-s_0s_4 \\ 0 & s_2+s_0s_3 & -s_2+s_0s_3 & 0 \\ 0 & -s_2+s_0s_3 & s_2+s_0s_3 & 0 \\ s_1-s_0s_4 & 0 & 0 & s_1+s_0s_4 \end{pmatrix}.$$

For example, if $s_j = 1$ for all j, this evaluates to the identity matrix. Note that the a_σ are all defined over $\mathbb{Z}$ and all commute with χ. In the following table, we list the a_σ, a'_σ and b_σ for a set of generators $\sigma \in G$ (given by their values of s_j).

(s_0,s_1,s_2,s_3,s_4)	a_σ	a'_σ	b_σ
$(-1,1,1,1,1)$	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
$(1,-1,1,1,1)$	$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
$(1,1,-1,1,1)$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$(1,1,1,-1,1)$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$(1,1,1,1,-1)$	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Since the a_σ correspond to $\varphi^{-1}({}^\sigma\varphi)$, we have for all $\sigma,\tau \in G$ that $a_\sigma a_\tau = a_{\sigma\tau}$. Now, for all $\sigma \in G$, choose a decomposition $\sigma = \sigma_1\sigma_2\ldots\sigma_m$ in terms of the generators given in the table. Then set

$$b_\sigma = b_{\sigma_1} b_{\sigma_2} \ldots b_{\sigma_n}.$$

Then we have

$$\gamma(b_\sigma, b_\sigma) = \gamma(b_{\sigma_1}, b_{\sigma_1})\gamma(b_{\sigma_2}, b_{\sigma_2})\ldots\gamma(b_{\sigma_n}, b_{\sigma_n}) = a_\sigma$$

and the result follows. □

3.1. Glueing twists. In this thesis, we only work with our particular quadratic form, and with generic quadratic forms given by diagonal matrices. However, in future work it would be interesting to twist the structure over $C_4(q_0)$ to a structure on $C_4(q)$ for q not necessarily given by a diagonal matrix. This would go roughly as follows:

By Lemma 4.3, if we have a quadratic form q given by a matrix m, we can, for every prime $p \neq 2$, diagonalize q over $\mathbb{Z}\left[\frac{1}{a}\right]$ for some a with $p \nmid a$. Then we can

define $C_4(q)$, $\mathrm{SO}(q)$ and $\widetilde{\mathrm{SO}(q)}$ over $\mathbb{Z}\left[\frac{1}{2\det m}, \frac{1}{a}\right]$ as twists of $C_4(q_0)$, $\mathrm{SO}(q_0)$ and $\widetilde{\mathrm{SO}(q_0)}$. However, we want to define these over $\mathbb{Z}\left[\frac{1}{2\det m}\right]$.

To that end, we have to glue these twists together. Glueing schemes and morphisms is described in Exercise II.2.12 from [**Har77**] and step 3 in Theorem II.3.3 of [**Har77**]. To glue schemes $\{X_i\}$ together, one needs to provide opens $U_{ij} \subseteq X_i$ and isomorphisms $\varphi_{ij} : U_{ij} \xrightarrow{\sim} U_{ji}$ for all $i \neq j$ that satisfy some compatibility conditions.

So, as mentioned, for all primes p, we can diagonalize m over $\mathbb{Z}\left[\frac{1}{a_i}\right]$ for some a_i with $p \nmid a_i$ and then twist with Galois descent datum

$$(C_4(q_0)_{A_i}, (f_{i,\sigma} \in \mathrm{Aut}(C_4(q_0)_{A_i'}))_{\sigma \in G_i})$$

with $A_i = \mathbb{Z}\left[\frac{1}{2\det m}, \frac{1}{a_i}\right]$ and A_i' an extension of A_i by a couple of square roots. This twist is then $X_i = C_4(q)_{A_i}$.

The opens U_{ij} to glue along would then be $U_{ij} = C_4(q)_{A_{ij}}$ for $A_{ij} = A_i\left[\frac{1}{a_j}\right]$, which correspond to the twists given by the Galois descent data

$$(C_4(q_0)_{A_{ij}}, ((f_{i,\sigma})_{A_{ij}'} \in \mathrm{Aut}(C_4(q_0)_{A_{ij}'}))_{\sigma \in G_{ij}})$$

for (the 'compositum') A_{ij}' a ring containing A_i' and A_j' such that $\operatorname{Spec} A_{ij}' \to \operatorname{Spec} A_{ij}$ is a Galois covering.

Note that for all i there exists a matrix m_i such that for all σ, $f_{i,\sigma}$ is given on R-points by $m_i^{-1}({}^\sigma m_i)$. Define $c_{ij} = m_j^{-1} m_i$ and let $\varphi_{ij}' : C_4(q_0)_{A_{ij}} \to C_4(q_0)_{A_{ji}}$ be defined on R-points by $x \mapsto c_{ij} x$. Then, for all $\sigma \in G_{ij}$, for all A_{ij}-algebras R and for all $x \in C_4(q_0)(R)$,

$$f_{j,\sigma}({}^\sigma \varphi_{ij}'(x)) = m_j^{-1}({}^\sigma m_j)({}^\sigma m_j^{-1})({}^\sigma m_i)x = m_j^{-1} m_i m_i^{-1}({}^\sigma m_i) = \varphi_{ij}'(f_{i,\sigma}(x)),$$

so φ_{ij}' is an (iso)morphism of Galois descent data and induces an (iso)morphism $U_{ij} \xrightarrow{\sim} U_{ji}$.

Now, to get an isomorphism ψ_{ij} from $V_{ij} := \mathrm{SO}(q)_{A_{ij}} \subseteq \mathrm{SO}(q)_{A_i}$ to $V_{ji} := \mathrm{SO}(q)_{A_{ji}} \subseteq \mathrm{SO}(q)_{A_j}$ that is compatible with φ_{ij}, one can take, on R-points for $m \in \mathrm{SO}(q_0)_{A_{ij}}(R)$,

$$\psi_{ij}'(m) = c_{ij} m c_{ij}^{-1}.$$

However, to get an isomorphism ρ_{ij} from $W_{ij} := \widetilde{\mathrm{SO}(q)}_{A_{ij}} \subseteq \widetilde{\mathrm{SO}(q)}_{A_i}$ to $W_{ji} := \widetilde{\mathrm{SO}(q)}_{A_{ji}} \subseteq \widetilde{\mathrm{SO}(q)}_{A_j}$ that is compatible with ψ_{ij}, one needs to lift $c_{ij} \in \mathrm{GL}_4(A_{ij}')$ to $d_{ij} \in (\mathrm{GL}_2 \times \mathrm{GL}_2)(A_{ij}')$ such that $\gamma(d_{ij}, d_{ij}) = \lambda c_{ij}$ for some $\lambda \in A_{ij}'^*$. It would take quite some work to prove that such a d_{ij} actually exists and is defined over A_{ij}' or some Galois extension of A_{ij}'. Maybe it would be possible to adapt the algorithm in Lemma 2.6 to work for arbitrary rings, but this is beyond the scope of this thesis.

When we have these isomorphisms, the proof that they indeed yield the desired structure over $C_4(q)_{\mathbb{Z}\left[\frac{1}{2\det m}\right]}$ will probably be similar to Lemma 5.1.

CHAPTER 6

Apotheosis: The Interesting Case

DEFINITION 6.1. Note that every nondegenerate quadratic form over $\mathbb{Q}$ becomes equal, after a linear change of basis over $\mathbb{R}$, to

$$\sum_{i=1}^{k} X_i - \sum_{i=k+1}^{n} X_i.$$

for some k and n. We call $(k, n-k)$ the **signature** of this quadratic form.

Let q be a a quadratic form with signature $(2,2)$, for which Lemma 5.1 or Lemma 5.2 gives a ring $A = \mathbb{Z}\left[\frac{1}{p_1,\ldots,p_n}\right]$ and a ring A' such that the structure on $C_4(q)$ is given by A-schemes and A-morphisms, and over A' this structure becomes isomorphic to the structure over $C_4(q_0)$. We take $S = \{p_1, \ldots, p_n\}$.

EXAMPLE 6.1. This is satisfied by $q = q_1$, with $A = \mathbb{Z}\left[\frac{1}{17}\right]$, $S = \{17\}$ and $A' = A\left[\frac{1+\sqrt{17}}{2}\right]$.

EXAMPLE 6.2. This is also satisfied by a generic quadratic form

$$q = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$$

which has signature $(2,2)$ (i.e. with exactly two of the a_i positive), with

$$A = \mathbb{Z}\left[\frac{1}{2a_1a_2a_3a_4}\right],\ S = \{p : p \mid 2a_1a_2a_3a_4\} \text{ and } A' = A'\left[\sqrt{-1}, \sqrt{a_1}, \ldots, \sqrt{a_4}\right].$$

In this chapter we will prove that $C_4(q)$ satisfies strong approximation away from $S \cup \{\infty\}$. To this end, we first prove that $\widetilde{\mathrm{SO}(q)}$, defined in the previous chapter, satisfies strong approximation away from infinity, using Theorem 7.12 from [**PR94**], transferring some properties from $\widetilde{\mathrm{SO}(q_0)}$ (which equals $\mathrm{SL}_2 \times \mathrm{SL}_2$) to $\widetilde{\mathrm{SO}(q)}$, via the A'-isomorphisms. After this, we will use a morphism $\widetilde{\mathrm{SO}(q)} \to C_4(q)$, together with a proof of surjectivity, to show using Lemma 2.4 that $C_4(q)$ satisfies strong approximation away from $S \cup \{\infty\}$.

1. Isomorphisms

Note that the definition of $C_4(q)$ as a twist of $C_4(q_0)$ starts with giving an A'-point of $\mathrm{Isom}(q_0, q)$. This A' equals A, with some roots of quadratic polynomials adjoined.

REMARK 6.1. Now, given a field k with characteristic not in S (for example, $k = \mathbb{F}_p$, $k = \mathbb{Q}$ or $k = \mathbb{Q}_p$), take $L = k$. For each of the quadratic polynomials f of which we adjoined a root to A to obtain A', if f is irreducible over L, replace L by $L[X]/(f)$, so adjoin a root of f to L. Then $k \subseteq L$ is a finite field extension such

that $\mathrm{Isom}(q_0, q)$ has an L-point, since we have a (canonical) morphism $A' \to L$. Since the structure on $C_4(q)$ is an A'-twist of the structure on $C_4(q_0)$, we have that after base change to L, these structures become isomorphic.

REMARK 6.2. For any prime $p \notin S$, take $k = \mathbb{Q}_p$. Then let L as in remark 6.1 and take $B = \mathcal{O}_L$ the valuation ring of L. Note that $\operatorname{Spec} B \to \operatorname{Spec}(\mathbb{Z}_p)$ is flat by Example 3.3.2 from [**Poo17**] since B is a subring of a field and therefore torsion free, and of finite presentation by proposition 23 in [**Lan94**] and Proposition 5.4.5 in [**Gou97**]. Therefore, it is fppf, so especially it is fpqc. Since the $\sqrt{a_i}$ are integral over $\mathbb{Z}_p$, we have a (canonical) morphism $A' \to B$ and $\mathrm{Isom}(q_0, q)$ has a B-point.

2. Strong approximation of $\widetilde{\mathrm{SO}(q)}$

In this section, we show that $\widetilde{\mathrm{SO}(q)}$ satisfies strong approximation away from infinity, using Theorem 7.12 from [**PR94**]:

THEOREM 6.1. *Let G be a reductive algebraic group, over an algebraic number field K, and let S be a finite subset of V^K. Then G has the strong approximation property with respect to S if and only if*

(1) G is simply connected (in particular, G is semisimple);
(2) G does not contain any K-simple component G^i with G^i_S compact.

We will prove these properties one by one:

LEMMA 6.1. $\widetilde{\mathrm{SO}(q)}_{\mathbb{Q}}$ *is reductive.*

PROOF. $\widetilde{\mathrm{SO}(q)}_{\mathbb{Q}}$ is reductive if and only if its unipotent radical $(\widetilde{\mathrm{SO}(q)}_{\mathbb{Q}})_{\mathrm{unip}}$ is trivial. By Remark 6.1 there exists a finite field extension $\mathbb{Q} \subseteq L$ such that $\widetilde{\mathrm{SO}(q)}_L \cong (\mathrm{SL}_2 \times \mathrm{SL}_2)_L$. By Proposition 5.9.2 from [**Poo17**], we have

$$(\widetilde{\mathrm{SO}(q)}_{\mathbb{Q}})_{\mathrm{unip}})_L = (\widetilde{\mathrm{SO}(q)}_L)_{\mathrm{unip}} \cong ((\mathrm{SL}_2 \times \mathrm{SL}_2)_L)_{\mathrm{unip}} = (((\mathrm{SL}_2 \times \mathrm{SL}_2)_{\mathbb{Q}})_{\mathrm{unip}})_L.$$

$(\mathrm{SL}_2 \times \mathrm{SL}_2)_{\mathbb{Q}}$ has a faithful semisimple representation, since it is a product of the simple algebraic group $(\mathrm{SL}_2)_{\mathbb{Q}}$ with itself. This makes $(\mathrm{SL}_2 \times \mathrm{SL}_2)_{\mathbb{Q}}$ into a reductive algebraic group: [**Mil17**], Corollary 22.20 and Example 22.21. Therefore, $((\widetilde{\mathrm{SO}(q)}_{\mathbb{Q}})_{\mathrm{unip}})_L \cong (((\mathrm{SL}_2 \times \mathrm{SL}_2)_{\mathbb{Q}})_{\mathrm{unip}})_L$ is trivial, and $(\widetilde{\mathrm{SO}(q)}_{\mathbb{Q}})_{\mathrm{unip}}$ must be trivial as well so $\widetilde{\mathrm{SO}(q)}_{\mathbb{Q}}$ is reductive. □

LEMMA 6.2. $\widetilde{\mathrm{SO}(q)}_{\mathbb{Q}}$ *is geometrically simply connected.*

PROOF. There exists a finite field extension $\mathbb{Q} \subseteq L$ such that $\widetilde{\mathrm{SO}(q)}_L \cong (\mathrm{SL}_2 \times \mathrm{SL}_2)_L$. Simply connectedness is preserved under base extension and descent (Section C.3 in [**Poo17**]) and because $(\mathrm{SL}_2 \times \mathrm{SL}_2)_{\mathbb{Q}}$ is reductive and satisfies strong approximation away from infinity, we know by Theorem 6.1 that it is simply connected. Therefore, we have that $(\mathrm{SL}_2 \times \mathrm{SL}_2)_L$ is simply connected, so $\widetilde{\mathrm{SO}(q)}_L$ is simply connected and therefore $\widetilde{\mathrm{SO}(q)}$ is simply connected. □

LEMMA 6.3. $\widetilde{\mathrm{SO}(q)}$ *has no $\mathbb{Q}$-simple component G with $G_{\{\infty\}} = G(\mathbb{R})$ compact.*

PROOF. Note that both q and q_0 have signature $(2,2)$, so they are equal up to a change of basis over $\mathbb{R}$. Then, $\widetilde{\mathrm{SO}(q)}_{\mathbb{R}} \cong \widetilde{\mathrm{SO}(q_0)}_{\mathbb{R}} = (\mathrm{SL}_2 \times \mathrm{SL}_2)_{\mathbb{R}}$. Note that the simple components of $(\mathrm{SL}_2 \times \mathrm{SL}_2)_{\mathbb{R}}$ are both $(\mathrm{SL}_2)_{\mathbb{R}}$. Therefore, any $\mathbb{Q}$-simple component G of $\widetilde{\mathrm{SO}(q)}$ has either $G_{\mathbb{R}} \cong (\mathrm{SL}_2)_{\mathbb{R}}$ or $G_{\mathbb{R}} \cong (\mathrm{SL}_2 \times \mathrm{SL}_2)_{\mathbb{R}}$.

Note that for all $a \in \mathbb{R}$, we have $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$, so $(\mathrm{SL}_2)_{\mathbb{R}}(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})$ is unbounded as a subset of $\mathbb{R}^4$ and therefore noncompact. Since topological spaces of $\mathbb{R}$-points of isomorphic schemes are homeomorphic, $G(\mathbb{R}) = G_{\mathbb{R}}(\mathbb{R})$ is noncompact as well. □

LEMMA 6.4. *$\widetilde{\mathrm{SO}(q)}$ satisfies strong approximation away from ∞.*

PROOF. We use [**PR94**], Theorem 7.12. We conclude the proof by remarking that we have already shown that

(1) $\widetilde{\mathrm{SO}(q)}$ is reductive: this is Lemma 6.1;
(2) $\widetilde{\mathrm{SO}(q)}$ is simply connected: this is Lemma 6.2;
(3) $\widetilde{\mathrm{SO}(q)}$ has no $\mathbb{Q}$-simple component G^i with $G^i_{\{\infty\}} = G^i(\mathbb{R})$ compact: this is Lemma 6.3.

□

3. Transitivity of the $\widetilde{\mathrm{SO}(q)}$-action

We want to prove that $\widetilde{\mathrm{SO}(q)}$ acts transitively on $\mathbb{Z}_p$-points of $C_4(q)$ for all primes $p \notin S$.

In this section, we fix such a prime and fix $a, b \in C_4(q)(\mathbb{Z}_p)$. We want to show that the transporter $\widetilde{\mathrm{SO}(q)}_{a,b}$ has a $\mathbb{Z}_p$-point.

LEMMA 6.5. *Let R be a local ring and let $x, y \in C_4(q_0)(R)$. Then $(\mathrm{SL}_2 \times \mathrm{SL}_2)_{x,y}$ has an R-point.*

PROOF. Take R a local ring and $x, y \in C_4(q_0)(R)$.

Then, by Lemma 3.4 there exist $\bar{x}, \bar{y} \in (C_2 \times C_2)(R)$ such that $\bar{x}$ is mapped to x and $\bar{y}$ to y.

By the transitivity of the SL_2-action, we have $g \in (\mathrm{SL}_2 \times \mathrm{SL}_2)(R)$ such that $g\bar{x} = \bar{y}$, so by definition of the $\mathrm{SL}_2 \times \mathrm{SL}_2$-action on $C_4(q_0)$, $gx = y$. □

Note that $\widetilde{\mathrm{SO}(q)}_{a,b}$ has a right action of $\widetilde{\mathrm{SO}(q)}_a$. In this section, we want to use Lang's theorem, for which we need to show that $\widetilde{\mathrm{SO}(q)}_{a,b}$ is a $\widetilde{\mathrm{SO}(q)}_a$-torsor.

DEFINITION 6.2. For a smooth algebraic group G over a perfect field k, a **G-torsor** is a k-variety X with a right G-action such that $X_{\bar{k}} \cong G_{\bar{k}}$, respecting the $G_{\bar{k}}$-action.

LEMMA 6.6. *For the ring B as in Remark 6.2, we have*

$$(\widetilde{\mathrm{SO}(q)}_{a,b})_B \cong (\widetilde{\mathrm{SO}(q)}_a)_B \cong ((\mathrm{SL}_2 \times \mathrm{SL}_2)_{(1,0,0,0)})_B$$

and the first isomorphism respects the $(\widetilde{\mathrm{SO}(q)}_a)_A$-action

PROOF. We have an isomorphism $\varphi : C_4(q)_B \xrightarrow{\sim} C_4(q_0)_B$ and isomorphisms

$$(\widetilde{\mathrm{SO}(q)}_{a,b})_B \cong ((\mathrm{SL}_2 \times \mathrm{SL}_2)_{\varphi(a),\varphi(b)})_B \quad \text{and} \quad (\widetilde{\mathrm{SO}(q)}_a)_B \cong ((\mathrm{SL}_2 \times \mathrm{SL}_2)_{\varphi(a)})_B.$$

Note that, by transitivity of the $\mathrm{SL}_2 \times \mathrm{SL}_2$-action on ring-valued points, $(\mathrm{SL}_2 \times \mathrm{SL}_2)_{\varphi(a),\varphi(b)}$ has a B-point g_0 and therefore $\widetilde{\mathrm{SO}(q)}_{a,b}$ has a B-point g, which gives an isomorphism, given on ring-valued points (for R a B-algebra) as

$$\widetilde{\mathrm{SO}(q)}_{a,b}(R) \xrightarrow{\sim} \widetilde{\mathrm{SO}(q)}_a(R), \quad h \mapsto g^{-1}h$$

and this (trivially) respects the right $\widetilde{\mathrm{SO}(q)}_a$-action.

Furthermore, since B is a local ring, the action of $\mathrm{SL}_2 \times \mathrm{SL}_2$ on C_2 is transitive on B-points. Therefore,

$$(\widetilde{\mathrm{SO}(q)}_a)_B \cong ((\mathrm{SL}_2 \times \mathrm{SL}_2)_{\varphi(a)})_B \cong ((\mathrm{SL}_2 \times \mathrm{SL}_2)_{(1,0,0,0)})_B,$$

with the second isomorphism given on R-points by

$$m \mapsto g^{-1}mg$$

for $g \in \mathrm{SL}_2(B)$ such that $g \cdot (1,0,0,0)^T = \varphi(a)$. □

LEMMA 6.7. *$(\widetilde{\mathrm{SO}(q)}_a)_{\mathbb{Z}_p}$ is smooth over $\mathbb{Z}_p$ and connected.*

PROOF. First of all, for the ring B as in Remark 6.2, we have

$$(\widetilde{\mathrm{SO}(q)}_a)_B \cong ((\mathrm{SL}_2 \times \mathrm{SL}_2)_{(1,0,0,0)})_B.$$

There also is an isomorphism of schemes, given on ring-valued points by

$$(\mathbb{G}_m \times \mathbb{A}^2)(R) \xrightarrow{\sim} (\mathrm{SL}_2 \times \mathrm{SL}_2)_{(1,0,0,0)}(R), \quad (\lambda,\mu,\nu) \mapsto \left(\begin{pmatrix} \lambda & \mu \\ 0 & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} \lambda^{-1} & \nu \\ 0 & \lambda \end{pmatrix}\right).$$

Therefore, $(\widetilde{\mathrm{SO}(q)}_a)_B \cong ((\mathrm{SL}_2 \times \mathrm{SL}_2)_{(1,0,0,0)})_B$ is connected and smooth over B. Since the image of a connected topological space is connected and the base change by an fpqc (surjective) morphism gives a surjection of topological spaces $(\widetilde{\mathrm{SO}(q)}_a)_B \to (\widetilde{\mathrm{SO}(q)}_a)_{\mathbb{Z}_p}$, connectedness is preserved under fpqc descent. By Appendix C.1 in [**Poo17**], smoothness is also preserved under fpqc descent. Now, since $\operatorname{Spec} B \to \operatorname{Spec}(\mathbb{Z}_p)$ is fpqc, $(\widetilde{\mathrm{SO}(q)}_a)_{\mathbb{Z}_p}$ is connected and smooth over $\mathbb{Z}_p$. □

LEMMA 6.8. *$\widetilde{\mathrm{SO}(q)}_{a,b}$ has a $\mathbb{Z}_p$-point.*

PROOF. Since $(\widetilde{\mathrm{SO}(q)}_a)_{\mathbb{F}_p}$ is a smooth connected algebraic group and $\widetilde{\mathrm{SO}(q)}_{a,b}$ is a $\widetilde{\mathrm{SO}(q)}_a$-torsor, Lang's Theorem (Theorem 5.12.19 from [**Poo17**]) tells us that we have an $\mathbb{F}_p$-point $\bar{g} \in \widetilde{\mathrm{SO}(q)}_{a,b}(\mathbb{F}_p)$.

Since $(\widetilde{\mathrm{SO}(q)}_{a,b})_{\mathbb{Z}_p}$ is smooth, Hensel's Lemma (Theorem 3.5.63a from [**Poo17**]) tells us that the function of sets $\widetilde{\mathrm{SO}(q)}_{a,b}(\mathbb{Z}_p) \to \widetilde{\mathrm{SO}(q)}_{a,b}(\mathbb{F}_p)$ is surjective, so we have $g \in \widetilde{\mathrm{SO}(q)}_{a,b}(\mathbb{Z}_p)$ (such that $g \equiv \bar{g} \mod p$). □

COROLLARY 6.1. *For all $a, b \in C_4(q)$, we have $g \in \widetilde{\mathrm{SO}(q)}(\mathbb{Z}_p)$ such that $g \cdot a = b$. Therefore, $\widetilde{\mathrm{SO}(q)}(\mathbb{Z}_p)$ acts transitively on $C_4(q)(\mathbb{Z}_p)$ for all $p \notin S$.*

4. Strong approximation of $C_4(q)$

Now we are finally ready to prove the theorem that we have been working towards in this thesis.

THEOREM 6.2. *$C_4(q)$ satisfies strong approximation away from $S \cup \{\infty\}$.*

PROOF. Take $U \subseteq C_4(q)(\mathbf{A}_{\mathbb{Q},S\cup\{\infty\}})$ a nonempty open. Then we have a point $x \in U$. There exists $a \in \mathbb{Q}^*$ such that $a^{-1}x \in C_4(q)(\prod_{p\notin S} \mathbb{Z}_p)$. Then $a^{-1}U$ is also nonempty open.

We have a morphism $f : \widetilde{\mathrm{SO}(q)} \to C_4(q)_A$, given on ring-valued points by $g \mapsto g(1,0,0,0)$. It is actually the composition of the morphisms

$$\widetilde{\mathrm{SO}(q)} \times \{(1,0,0,0)\} \to \mathrm{SO}(q) \times C_4(q) \to C_4(q).$$

By Lemma 2.2, f is continuous on $\mathbf{A}_{\mathbb{Q},S\cup\{\infty\}}$-points and by Lemma 6.8, its restriction to $\prod_{p\notin S} \mathbb{Z}_p$-points is surjective.

Therefore, $f^{-1}(a^{-1}U)$ is open, and contains a preimage of $a^{-1}x$, so it is nonempty.

Since, by Lemma 6.4, $\widetilde{\mathrm{SO}(q)}$ satisfies strong approximation away from ∞, we have a point $y \in f^{-1}(a^{-1}U) \cap \widetilde{\mathrm{SO}(q)}(\mathbb{Q})$. This gives a point

$$f(y) \in a^{-1}U \cap C_4(q)(\mathbb{Q}).$$

Note that multiplication by a sends $C_4(q)(\mathbb{Q})$ to itself. Therefore, $af(y) \in U \cap C_4(q)(\mathbb{Q})$, which concludes the proof. □

APPENDIX A

Clifford Algebras

This appendix summarizes the relevant parts of section C.2 from [**Con14**].

Given a domain R and a quadratic form $q \in R[X_1, \ldots, X_n]$, and defining $V = R^n$ and $e_i = (0, \ldots, 1, \ldots, 0) \in V$ the standard generators for V as a R-module, we define the Tensor Algebra

$$T(V) = \bigoplus_{n \geq 0} \underbrace{V \otimes \cdots \otimes V}_{n \text{ times}}.$$

This is an R-algebra with a $\mathbb{Z}$-grading.

We then define the Clifford algebra $C(q, V)$ to be the quotient of $T(V)$ by the relations $v \otimes v = q(V)$ for all $v \in V$. This gives an R-algebra with a $\mathbb{Z}/2\mathbb{Z}$-grading.

We have the relations $e_i^2 = q(e_i)$ and

$$q(e_i + e_j) = (e_i + e_j)^2 = e_i^2 + e_i e_j + e_j e_i + e_j^2 = q(e_i) + e_i e_j + e_j e_i + q(e_j),$$

so $e_i e_j = q(e_i + e_j) - q(e_i) - q(e_j) - e_j e_i$. Therefore, $C(q, V)$ is generated as an R-module by elements of $T(V)$ of degree at most n.

We define $C_0(q, V)$, the "even" part of $C(q, V)$, to be the subalgebra of $C(q, V)$, consisting of elements of degree $0 \in \mathbb{Z}/2\mathbb{Z}$. We then define $Z_q \subseteq C_0(q, V)$ to be the center of $C_0(q, V)$.

We have a $\mathrm{O}(q)$-action on $C(q, V)$, which preserves the $\mathbb{Z}/2\mathbb{Z}$-grading, so it preserves $C_0(q, V)$ and therefore Z_q. Therefore, we have a group homomorphism $\mathrm{O}(q) \to \mathrm{Aut}_{Z_q/R}$.

The automorphism group of Z_q consists of two elements, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. We therefore have an homomorphism

$$D_q : \mathrm{O}(q) \to \mathbb{Z}/2\mathbb{Z}.$$

If n is even, we define

$$\mathrm{SO}(q) = \ker D_q.$$

We have by Theorem C.2.11 in [**Con14**] that $\mathrm{SO}(q)$ is smooth with connected fibers.

Now, for $n = 2m$ even and $q = -X_1 X_{2m} + X_2 X_{2m-1} - \cdots + (-1)^m X_m X_{m+1}$, we have for all i and j, $e_i^2 = q(e_i) = 0$ and

$$e_i e_j = \begin{cases} (-1)^i - e_j e_i & j = n - i \\ -e_j e_i & j \neq n - i \end{cases}$$

Define

$$v_k = (1 - (-1)^k 2 e_k e_{n-k})$$

and $\mathbf{v} = \prod_{k=1}^{m} v_k$

Note that for all i and j with $j \notin \{i, n - i\}$, $v_i^2 = 1$ and $v_i v_j = v_j v_i$. so

$$\mathbf{v}^2 = 1.$$

We have, for all i, j, that

$$v_j e_i = \begin{cases} -e_i v_j & i \in \{j, n-j\} \\ e_i v_j & i \notin \{j, n-j\} \end{cases}$$

Therefore, $e_i \mathbf{v} = -\mathbf{v} e_i$, so for all i and j, we have $e_i e_j \mathbf{v} = \mathbf{v} e_i e_j$, so $\mathbf{v} \in Z_q$. Now, we define $\mathbf{v}' = \frac{1-\mathbf{v}}{2} \in Z_q$. This results in an expression over $\mathbb{Z}$, so this is also defined in characteristic 2. We have $(\mathbf{v}')^2 = \mathbf{v}'$.

We have that $Z_q \cong R \times R$, and is generated as an R-module by $1 \in R$ and $\mathbf{v}'$.

Now, suppose that we have some $\varphi \in \mathrm{Aut}_{Z_q/R}$, given by $\varphi(\mathbf{v}') = b_0 + b_1 \mathbf{v}'$. Then we have

$$b_0 + b_1 \mathbf{v}' = \varphi((\mathbf{v}')^2) = \varphi(\mathbf{v}')^2 = b_0^2 + (2b_0 b_1 + b_1^2)\mathbf{v}',$$

so we have $b_0(b_0 - 1) = 0$ and $(2b_0 + b_1 - 1)b_1 = 0$. Note that $b_1 \neq 0$, since φ is an automorphism. This gives either $(b_0, b_1) = (0, 1)$ or $(b_0, b_1) = (1, -1)$, so $\varphi(\mathbf{v}') = \mathbf{v}'$ or $\varphi(\mathbf{v}') = 1 - \mathbf{v}'$.

Now, note that in characteristic 2, the constraints $b_1 = 1$ and $b_1 = -1$ become the same, however, the constraints $b_0 = 0$ and $b_0 = 1$ stay distinct.

For $n = 4$, we have $q = -X_1 X_4 + X_2 X_3$ and $\mathbf{v}' = 2e_1 e_2 e_3 e_4 - e_1 e_4 + e_2 e_3$. Then we have, for $g \in \mathrm{O}(q)(R)$,

$$D_q(g)(\mathbf{v}') = \det(g)\mathbf{v}' - 2\begin{vmatrix} g_{12} & g_{13} \\ g_{22} & g_{23} \end{vmatrix}\begin{vmatrix} g_{31} & g_{34} \\ g_{41} & g_{44} \end{vmatrix} - 2\left(\tfrac{1}{2} + \begin{vmatrix} g_{31} & g_{14} \\ g_{41} & g_{24} \end{vmatrix}\right)\left(\tfrac{1}{2} - \begin{vmatrix} g_{32} & g_{13} \\ g_{42} & g_{23} \end{vmatrix}\right) + \tfrac{1}{2}$$

We now define $\mathrm{SO}(q_0)(R)$ to be

$$\left\{ g \in \mathrm{O}(q_0) \mid 2\begin{vmatrix} g_{12} & g_{13} \\ g_{22} & g_{23} \end{vmatrix}\begin{vmatrix} g_{31} & g_{34} \\ g_{41} & g_{44} \end{vmatrix} + 2\left(\tfrac{1}{2} + \begin{vmatrix} g_{31} & g_{14} \\ g_{41} & g_{24} \end{vmatrix}\right)\left(\tfrac{1}{2} - \begin{vmatrix} g_{32} & g_{13} \\ g_{42} & g_{23} \end{vmatrix}\right) = \tfrac{1}{2} \right\}$$

as a closed subscheme (given by a polynomial equation) of $\mathrm{SO}(q_0)$.

Note that $\frac{1}{2}$ is not defined in characteristic 2, but when expanding the equation, the $\frac{1}{2}$'s on the left side cancel with the $\frac{1}{2}$ on the right hand side and the multiplication by 2 to give an equation over $\mathbb{Z}$.

Bibliography

[BK19] Martin Bright and Ivo Kok. Failure of strong approximation on an affine cone. *Involve*, 12(2):321–327, 2019.

[Con12] Brian Conrad. Weil and Grothendieck approaches to adelic points. *Enseign. Math. (2)*, 58(1-2):61–97, 2012.

[Con14] Brian Conrad. Reductive group schemes. In *Autour des schémas en groupes. Vol. I*, volume 42/43 of *Panor. Synthèses*, pages 93–444. Soc. Math. France, Paris, 2014.

[EH00] David Eisenbud and Joe Harris. *The geometry of schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Gou97] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Mil17] J. S. Milne. *Algebraic groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field.

[Pag20] Margherita Pagano. Strong approximation on some punctured affine cones. Master's thesis, Leiden University, the Netherlands, 2020.

[Poo17] Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017.

[PR94] Vladimir Platonov and Andrei Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.

[vdL23] A. van der Leer. Accompanying sage code for my master's thesis. `https://github.com/arnoudvanderleer/strong-approximation-sage`, 2023.