The Geometry of Gauss' Composition Law

by

Yelena Baishanski

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2010

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirements for the degree of Doctor of Philosophy.

June 14, 2010
Date

Lucien SZPIRO
Chair of Examining Committee

June 14, 2010
Date

Josef DODZIUK
Executive Officer

Kenneth KRAMER
Supervisory Committee Member

Clayton PETSCHE
Supervisory Committee Member

THE CITY UNIVERSITY OF NEW YORK

Abstract

The Geometry of Gauss' Composition Law

by

Yelena Baishanski

Advisor: Lucien Szpiro

We examine Gauss composition of quadratic forms from both an arithmetic and geometric perspective. Gauss' identification of a composition law for primitive integral binary quadratic forms of given discriminant D—which provides the set $\mathcal{F}_D$ of $SL_2(\mathbb{Z})$-equivalence classes of such forms with a group structure—essentially amounts to the discovery of the class group of an order in a quadratic number field. We consider quadratic extensions of the field of rational functions $k(u)$, where k is an algebraically closed field, and seek an analogue of Gauss composition in this context.

A quadratic extension of $k(u)$ corresponds to the function field of a curve C with affine model $t^2 = D(u)$ for some polynomial $D = D(u)$ in $k[u]$, which is of odd degree if C has a smooth ramified point at infinity. Focusing on this case—the analogue of quadratic number fields with one complex place at infinity—we extend the notion of the degree of a Weil divisor on a curve to Cartier divisors on C, and find a bijection between the set of $SL_2(k[u])$-equivalence classes of primitive forms with coefficients in $k[u]$ of discriminant D, and the group $Pic^0(C)$ of isomorphism classes of degree zero lines bundles on C.

In parallel fashion, we reinterpret the arithmetic case using Arakelov's invention of metrics associated to the infinite places of a number field. Given an invertible A-module L for an order A in a number field K, we have for each infinite place σ of K a corresponding one-dimensional $\mathbb{C}$-vector space L_σ with a positive non-degenerate hermitian metric $\| \ \|_\sigma$ (which is then determined by the length $\|x\|^2$ of any element x of L_σ). Using a notion of *degree* of an invertible metrized module—which mirrors the notion of degree used in

the geometric case, yielding in both cases a "product formula" $deg(f) = 0$ for a principal divisor (f)—we find for $D < 0$ a bijection between classes of positive definite forms in $\mathcal{F}_D$ and the compactified Picard group $Pic_c^0(A)$ of isometry classes of degree zero invertible A-modules.

Acknowledgements

I wish to take this opportunity to convey my heartfelt thanks to my advisor, professor Lucien Szpiro, for his always generous help and spirited engagement. He challenged and stimulated me at all levels of my graduate study, helping me develop mathematically and as a person, through animated discussions which I still feel privileged to have in memory: with his patient wisdom and profound humanity, they will continue to inspire and encourage me for many years to come. My deepest thanks also to professor Kenneth Kramer, whose Modern Algebra class at the onset of my studies first sparked my love of the subject, and whose exceptional and passionate pedagogy made it thrive; I am indebted and very grateful to him for the constant support he has provided me ever since, and for his invaluable time and input on many drafts of this thesis. The third member of my Defense Committee, professor Clayton Petsche, has always been more than willing to offer his help, whether it be to explain and simplify arguments or to listen to and comment on my

presentations; I have always greatly appreciated his ready availability and goodwill, for which he has my sincerest gratitude.

Without being able to list them all here, I thank all my friends and classmates at the Graduate Center for their conversation, solidarity, humor and generosity, which continue to enrich and brighten my life. I also want to express my gratitude to my parents, Jacqueline and Bogdan Baishanski, for their love, encouragement and support of all my pursuits, as well as to my siblings Ana, Vanya and Tatyana, for all together blessing me with the incredible family I have—loving, understanding, lively, argumentative and mirthful. I am especially grateful to my mother—who shied from no effort or sacrifice in so doing, and faced many—for *making* this family; and thank her particularly for setting for me in all things (including in the beautiful, unassailable logic and coherence of her argumentation) an example I strive to emulate.

Finally, I am immesurably grateful to my partner and treasure in life, Kevin P.Q. Phelan, for gifts which call for thanks apart—but I do want to mention here the unshakable confidence in me, and pride in my goals, with which he always counteracts any wavering of my own. It is my greatest fortune to be able to rely on him as a true better half... and I cannot thank him enough for being always such an irrepressibly, vigorously vocal one.

Contents

Introduction

We introduce the conventions and notations used in the following chapters. Rings are assumed to be commutative with unity. Prior to our discussion of the norm of an ideal in an order A of a number field K, we implicitly adopt the following definitions: the norm $N(M)$ of an A-submodule M of K refers to the absolute value of the determinant of a transition matrix from a $\mathbb{Z}$-basis for A to one for M; the norm $N_{L/F}(x)$ of an element x in a finite separable extension L of a field F refers to the product of its conjugates $\sigma(x)$, where the σ are the F-isomorphisms of L into $\overline{F}$. Throughout, k denotes an algebraically closed field of characteristic other than 2.

Chapter 1

The Picard Group

1.1 Invertible Ideals

We begin by establishing some vocabulary and notations for later use. Let R be a ring with fraction field K. An R-submodule M of K is an *fractional ideal* of R if there exists a nonzero $b \in R$ such that $bM \subset R$. Any finitely generated R-submodule of K is clearly fractional, and those generated by a single element $\alpha \in K$ are called *principal*. For any R-submodule M of K we define $(R : M) := \{\alpha \in K \mid \alpha M \subset R\}$, and define the *stabilizer of* M to be $Stab(M) := \{\alpha \in K \mid \alpha M \subset M\}$. An R-submodule M of K is an *invertible ideal* if there exists an R-submodule N of K such that $MN = R$. Then M is finitely generated, hence fractional: there exist elements x_i of M and y_i of N $(1 \leq i \leq n)$, such that $\sum x_i y_i = 1$, so any m in M can be written $m = \sum x_i(my_i)$ where the $my_i \in R$. Moreover the module N is unique and

equal to $(R : M)$, since

$$N \subset (R : M) = (R : M)MN \subset RN = N$$

It follows that invertible ideals of R form a group with identity R, which we denote $Inv(R)$.

Lemma 1.1. *If M is an invertible ideal of R, then $Stab(M) = R$.*

Proof. For any R-submodule M of K we have $R \subset Stab(M)$. Moreover $Stab(M) \subset RStab(M) \subset Stab(M)$, hence $Stab(M) = RStab(M)$. If M is invertible with inverse N, this yields $Stab(M) = NMStab(M) \subset NM = R$, hence $Stab(M) = R$. □

Lemma 1.2. *In a local ring, a fractional ideal is invertible if and only if it is principal.*

Proof. Let R be a local ring with maximal ideal $\mathfrak{m}$. Principal ideals are clearly invertible, so let I be an invertible fractional ideal of R. Then there exist elements x_i in I, y_i in $(R : I)$ $(1 \leq i \leq n)$, such that $\sum x_i y_i = 1 \in R$. Then for some j, $x_j y_j \notin \mathfrak{m}$, so $x_j y_j u = 1$ for some unit u of R. It follows that any element x of I can be written $x = x_j(y_j u x) \in Rx_j$, so $I = Rx_j$ is principal. □

1.2 Projective Finitely Generated Modules

We recapitulate some results formulated by Szpiro in his *Cours de Géometrie Arithmétique*, to be used in later proofs.

Proposition 1.3. *Let R be a ring, P an R-module. The following statement are equivalent:*

i) P is projective finitely generated over R

ii) P is locally free of finite rank for the Zariski topology

iii) the canonical R-homomorphism $\Phi : P^\vee \otimes_R P \to End_R(P)$ which maps $\varphi \otimes y$ to $x \mapsto y\varphi(x)$ is surjective.

Proof. Lemmas 1.4 and 1.5 below show $i) \Rightarrow ii)$. If P is locally free of finite rank, $Coker\ \Phi$ is locally zero since Φ is surjective for $P \simeq R^n$, hence $ii) \Rightarrow iii)$. Finally if $iii)$ holds, the identity id_P on P is in the image of $P \otimes P^\vee$, so there exists an integer n, elements (x_i) of P and (φ_i) of $P^\vee$ $(1 \leq i \leq n)$, such that for all y in P, $\sum x_i \varphi_i(y) = y$. Thus the x_i generate P, yielding a surjective homomorphism $R^n \to P$ mapping basis elements e_i to x_i. It splits though the map $\varphi : P \to R^n$ which sends $y \mapsto (\varphi_i(y))_{1 \leq i \leq n}$, so P is a direct summand of R^n, hence projective. □

Lemma 1.4. *Let R be a local ring with maximal ideal $\mathfrak{m}$, P a projective finitely generated R-module. Then P is free of rank $dim_{R/\mathfrak{m}}(P/\mathfrak{m}P)$.*

Proof. Let $(x_i)_{1\leq i\leq n}$ be elements of P forming a basis for $P/\mathfrak{m}P$ over $R/\mathfrak{m}$, and let $\varphi : R^n \to P$ be the R-module homomorphism mapping e_i the canonical basis element of R^n to x_i. By Nakayama's lemma φ is surjective, hence yields an exact sequence $0 \to M \to R^n \xrightarrow{\varphi} P \to 0$ which is split, hence remains exact after tensoring by $R/\mathfrak{m}$:

$$0 \to M \otimes R/\mathfrak{m} \to (R/\mathfrak{m})^n \xrightarrow{\overline{\varphi}} P/\mathfrak{m}P \to 0.$$

Since $\overline{\varphi}$ was constructed to be an isomorphism $M \otimes R/\mathfrak{m} = 0$. Then since M is finitely generated (the splitting gives it n generators), Nakayama's lemma yields $M = 0$. □

Lemma 1.5. *Let R be a ring, P a projective finitely generated R-module, and ϕ an isomorphism $R_{\mathfrak{p}}^n \to P_{\mathfrak{p}}$ (which exists by 1.4). Then there exists $f \in R - \mathfrak{p}$ and an isomorphism $\varphi : R_f^n \to P_f$ extending ϕ.*

Proof. We use the fact that if M is a finitely generated R-module such that $M_{\mathfrak{p}} = 0$, then $M_f = 0$ for some $f \in R - \mathfrak{p}$: indeed if elements $(x_i)_{1\leq i\leq n}$ generate M, for each i there exists an $f_i \in R - \mathfrak{p}$ such that $f_i x_i = 0$ in M, so letting $f = \prod_{i=1}^n f_i$ we find $M_f = 0$. Let $\varphi : R^n \to P$ be an R-module homomorphism such that $\varphi_{\mathfrak{p}} = \phi$. *Coker* φ is finitely generated (since P is), hence $(Coker\ \varphi)_g = 0$ for some $g \in R - \mathfrak{p}$. Then since by hypothesis P_g is

a projective R_g-module, φ_g splits and $(Ker\ \varphi)_g$ is finitely generated. Thus $(Ker\ \varphi)_f = (Coker\ \varphi)_f = 0$ for some $f \in R - \mathfrak{p}$. □

Proposition 1.6. *Let R be a ring, L an R-module. Then the following statements are equivalent:*

i) L is projective rank 1

ii) The canonical "evaluation" map $L \otimes_R L^\vee \to R$ is an isomorphism

Proof. $(L \otimes_R L^\vee) \overset{eval}{\to} R$ is an isomorphism when $L \simeq R$, which proves $i) \Rightarrow ii)$. To show $ii) \Rightarrow i)$, we show L is isomorphic to R when R is local. Given condition $ii)$, we have elements $x_1, ..., x_n \in L$ and $\varphi_1, ..., \varphi_n \in L^\vee$ such that $\sum \varphi_i(x_i) = 1$. Since R is local, at least one of the summands must be invertible in R, so there exist $x \in L$, $\varphi \in L^\vee$ such that $\varphi(x) = 1$, yielding a factorization $L = R \oplus M$. We show $M = 0$. Since $L^\vee = R \oplus M^\vee$, we have $L \otimes L^\vee = R \oplus M \oplus M^\vee \oplus M \otimes M^\vee \overset{\sim}{\to} R$, where the induced map on R is the identity. Then if $m \in M$ has image a under the above isomorphism, $(-a, m)$ has image 0, whence $a = m = 0$. Thus $M = 0$. □

1.3 Invertible Modules

Definition 1.7. *Let R be a ring. We denote by $Div_+(R)$ the monoid (for the tensor product) of ideals of R which are projective of rank 1 R-modules. The*

group of Cartier divisors of *R, denoted $Div(R)$, is the free abelian group generated by $Div_+(R)$. The* ***group of principal divisors of*** *R, denoted $Pr(R)$, is the subgroup of $Div(R)$ generated by ideals aR where $a \in R$ is not a zero-divisor.*

Example 1.8. *If a ring R has fraction field K, $Pr(R)$ is canonically isomorphic to K^*/R^*.*

Projective R-modules of rank 1 are also called *invertible R-modules*. The following lemma clarifies the relation between invertible R-modules and invertible ideals of R.

Lemma 1.9. *If R is a domain, $Inv(R) \simeq Div(R)$.*

Proof. Let $I \in Div_+(R)$, so $I_\mathfrak{p}$ is a principal hence invertible $R_\mathfrak{p}$-ideal for all $\mathfrak{p} \in Spec(R)$. We show $(R : I)_\mathfrak{p} = (R_\mathfrak{p} : I_\mathfrak{p})$ for all $\mathfrak{p}$, whence $I(R : I) = R$ and I is invertible. Clearly $(R : I)_\mathfrak{p} \subset (R_\mathfrak{p} : I_\mathfrak{p})$. Let $\alpha \in (R_\mathfrak{p} : I_\mathfrak{p})$, and let $(x_i)_{1 \le i \le n}$ be a system of generators for I over R (which exists by 1.3). Then considering all the x_i as elements of $I_\mathfrak{p}$ we find $\alpha x_i = a_i/t_i$ for some $a_i \in R,\ t_i \in R - \mathfrak{p}$. Letting $t = \prod_{1 \le i \le n} t_i$ and using the fact that R is a domain, we find $\alpha t \in (R : I)$, hence $\alpha \in (R : I)_\mathfrak{p}$. If J is any other ideal in $Div_+(R)$, the morphism of monoids $I \otimes J \mapsto IJ$ induces a group homomorphism $Div(R) \to Inv(R)$ which is clearly injective. To establish

surjectivity, let $I \in Inv(R)$. Localizing $I(R : I) = R$ at any $\mathfrak{p} \in Spec\ R$ shows that $I_{\mathfrak{p}}$ is an invertible fractional ideal of $R_{\mathfrak{p}}$, hence generated by a nonzero element by 1.2. Then since R is a domain, $I_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$ for all $\mathfrak{p}$ so I is projective of rank 1. Since $aI \subset R$ for some nonzero $a \in R$, we then have $aI \in Div_+(R)$, and $I = aI \otimes (aR)^{\otimes -1}$ belongs to $Div(R)$. □

Definition 1.10. *Let R be a ring. The tensor product of R-modules induces a commutative group structure on the set of isomorphism classes of invertible R-modules. The class of R is the identity element, and the class of the dual module is the inverse element. This group is called the* ***Picard group of*** *R, and denoted $Pic(R)$.*

Proposition 1.11. *If R is an integral domain, we have an exact sequence*

$$0 \to Pr(R) \to Div(R) \to Pic(R) \to 0$$

Proof. For any ring R, $Pr(R)$ is the kernel of the map $Div(R) \to Pic(R)$ which maps $I \in Div_+(R)$ to the class of its dual. Since every element of $Div(R)$ is a "difference" $I \otimes J^{\otimes -1}$ of elements of $Div_+(R)$, it suffices to show that if $I, J \in Div_+(R)$ with $I^\vee \simeq J^\vee$, there exist a, b nonzero in R such that $aI = bJ$. Let K be the fraction field of R. Since $I \otimes K \simeq K \simeq J \otimes K$, we have $Isom(I, J) = \{f \in K | fI = J\}$, and our claim follows. The following lemma

shows that if R is a domain, for any $L \in Pic(R)$, there exists $I \in Div_+(R)$ such that $L \simeq I^\vee$. □

Lemma 1.12. *Let R be an integral domain, and L an invertible R-module. For any nonzero $s \in L$ we consider the map $\varphi_s : R \to L$ which maps 1 to s. Then the dual map $L^\vee \to R$ identifies $L^\vee$ to an ideal $\mathfrak{a}_s$ of R such that $\mathfrak{a}_s = Ann(L/Rs)$*

Proof. If R is a domain, any nonzero R-homomorphism $\varphi : L \to L'$ of invertible R-modules is injective: indeed $\varphi_\mathfrak{p} : L_\mathfrak{p} \to L'_\mathfrak{p}$ is then nonzero for all $\mathfrak{p}$, and any nonzero homomorphism $R_\mathfrak{p} \to R_\mathfrak{p}$ is clearly injective whence $Ker\ \varphi = 0$. Since $\varphi_s^\vee$ is nonzero (since $\varphi_s^{\vee\vee} = \varphi_s \neq 0$) it is thus injective and identifies $L^\vee$ to an ideal $\mathfrak{a}_s$ of R. To show that $\mathfrak{a}_s = Ann(L/Rs)$ it suffices to prove the equality locally: when L is isomorphic to R, φ_s corresponds to multiplication by an element $r \in R$. Then $\varphi_s^\vee$ also corresponds to multiplication by r, whence the result. □

Corollary 1.13. *Let R be a noetherian domain of dimension 1. Then if L is an invertible R-module, in the notation of 1.12 we have $L/Rs \simeq R/\mathfrak{a}_s$ for any nonzero s in L.*

Proof. Since L/Rs and $R/\mathfrak{a}_s$ are artinian hence of finite length, by lemma 1.14 below it suffices to prove the claim locally. When L is isomorphic to a

local ring R the result follows from 1.12. □

Lemma 1.14. *Let M be a module of finite length over a ring R. Then the set S of maximal ideals $\mathfrak{m}$ of R such that $M_{\mathfrak{m}} \neq 0$ is finite, and*

$$M \simeq \prod_{\mathfrak{m} \in S} M_{\mathfrak{m}}$$

Proof. First note that if M is a simple R-module (i.e., a nonzero module without any proper submodules), then $M \simeq R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset R$: any nonzero $x \in M$ generates M over R, so $M \simeq R/I$ where the ideal $I \subset R$ must be maximal for M to be simple. If M has length n, then M has a filtration $0 = M_0 \subset M_1 \subset ... \subset M_n = M$ such that the successive quotients M_{i+1}/M_i are simple, so isomorphic to $R/\mathfrak{m}_i$ for some maximal ideals $\mathfrak{m}_i \subset R$. Since $(R/\mathfrak{m}_i)_{\mathfrak{m}} = 0$ for any $\mathfrak{m} \neq \mathfrak{m}_i$, tensoring the above filtration by $R_{\mathfrak{m}}$ yields $M_{\mathfrak{m}} = 0$ for all $\mathfrak{m} \notin \{\mathfrak{m}_i\}_{0 \leq i < n}$. To establish the second statement, note that the canonical map $M \to \prod_{\mathfrak{m} \in S} M_{\mathfrak{m}}$ is injective: if $x \in M$ is in its kernel, then $Rx \subset M$ gives $(Rx)_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \subset R$, whence $Rx = 0$ and $x = 0$. Surjectivity follows from the additivity of the length function for modules of finite length. □

1.4 Invertible Sheaves

The notion of invertible sheaves over a scheme generalizes that of invertible modules over a ring.

Definition 1.15. *Let X be a scheme. A quasi-coherent sheaf $\mathcal{L}$ on X is* ***invertible*** *if there exists an open cover $(U_i)_{i\in I}$ of X such that $\mathcal{L}_{|U_i} \simeq \mathcal{O}_{|U_i}$.*

Example 1.16. *If $\mathcal{L}$ is invertible and $U = Spec\ R$ is an affine open of X, $\mathcal{L}_{|U}$ is the sheaf associated to an invertible R-module: indeed $\mathcal{L}_{|U} \simeq \tilde{L}$ for some R-module L, and for some open cover of U which we may take to consist of basic open affines $U_f = Spec\ R_f$, $\mathcal{L}_{|U_f} \simeq \tilde{R}_f$. Thus $L_f \simeq R_f$ for each f and L is invertible.*

Definition 1.17. *The tensor product of $\mathcal{O}_X$-modules induces a group structure on the set of isomorphism classes of invertible sheaves on X. The group is called the* ***Picard group of X*** *and denoted $Pic(X)$.*

Definition 1.18. *A closed subscheme of a scheme X is a* ***positive Cartier divisor*** *on X if it is locally defined by non zero divisors, i.e., if the ideal sheaf defining it is invertible. The set of all such is denoted $Div_+(X)$. A* ***Cartier divisor*** *on X is one that is locally a difference of two positive Cartier divisors, and the set of all such is denoted $Div(X)$.*

Example 1.19. *In light of 1.16, positive Cartier divisors on Spec R are in bijection with the ideals I in $Div_+(R)$. We thus obtain an isomorphism of groups $Div(Spec\ R) \simeq Div(R)$.*

By definition, a positive Cartier divisor D on a scheme X is given by a set $(U_i, a_i)_{i\in I}$, where $(U_i)_{i\in I}$ is an open cover of X, and where the a_i in $\Gamma(U_i, \mathcal{O}_{U_i})$ are not zero divisors in $\mathcal{O}_x$ for any x in U_i, and must locally generate the same ideal: that is, on any intersection $U_i \cap U_j$, we must have $a_i = u_{ij}\ a_j$ for some unit u_{ij} in $\Gamma(U_i \cap U_j, \mathcal{O}_{U_i\cap U_j})$. If $a_i = a_j$ in $\Gamma(U_i \cap U_j, \mathcal{O}_{U_i\cap U_j})$ for all i, j, there exists a global section a of the ideal sheaf $\mathcal{I}$ defining D such that $a_{|U_i} = a_i$, so $D = (X, a)$ is called *principal*. An arbitrary divisor is principal if it is locally a difference of positive principal divisors. The set $Pr(X)$ of all principal divisors is clearly a subgroup of the group $Div(X)$.

If a positive Cartier divisor D is defined by the invertible ideal sheaf $\mathcal{I}$ on X, the map which sends D to the isomorphism class of $\mathcal{I}^{-1}$ in $Pic(X)$ clearly extends to a group homomorphism $Div(X) \to Pic(X)$. Denoting the image of an arbitrary divisor D under this homomorphism by $\mathcal{L}_D$, we have the following generalization of lemma 1.11:

Lemma 1.20. *If X is an integral scheme, we have an exact sequence*

$$0 \to Pr(X) \to Div(X) \to Pic(X) \to 0$$

Proof. For any scheme X, the homomorphism $D \mapsto \mathcal{L}_D$ has kernel $Pr(X)$: if $D = (U_i, g_i)$ has image $\mathcal{L}_D \simeq \mathcal{O}_X$, and 1 in $\mathcal{O}_X(X)$ under this isomorphism has image f in $\mathcal{L}_D(X)$, then $f_{|U_i} = u_i g_i^{-1}$ for some unit u_i in $\Gamma(U_i, \mathcal{O}_{U_i})$. But (U_i, g_i) and $(U_i, u_i g_i)$ define the same divisor, so $D = (U_i, u_i g_i) = (X, f^{-1})$ is principal. To show $Div(X) \to Pic(X)$ is surjective for X integral, let $\mathcal{L}$ be an invertible sheaf on X. Then by lemma 1.12, for any open affine $Spec\ A$ of X we have $\mathcal{L}^{-1}_{|Spec\ A} \simeq \mathcal{I}_A$, where $\mathcal{I}_A$ is the invertible ideal sheaf associated to some ideal I in $Div_+(A)$. Since $\mathcal{L}$ is locally isomorphic to $\mathcal{O}_X$, there exists a cover of X by open affines $U = Spec\ A_i$ such that $\mathcal{L}_{|Spec\ A_i} \simeq \mathcal{O}_{Spec\ A_i}$, so we may assume $\mathcal{I}_{A_i} \simeq \mathcal{O}_{Spec\ A_i}$ is generated by a nonzero divisor a_i of A_i. The ideal sheaf I locally generated by the a_i is then invertible and isomorphic to $\mathcal{L}^{-1}$, so defines a divisor D in $Div_+(X)$ with image $\mathcal{L}$ in $Pic(X)$. □

1.5 The Degree of a Divisor

Definition 1.21. *A **prime divisor** on a scheme X is an integral closed subscheme Z of codimension 1. A **Weil divisor** on X is an element of the free abelian group $Z^1(X)$ generated by prime divisors, i.e., a sum*

$$\sum_{codim Z = 1} n_Z\ [Z]$$

where all but finitely many of the integers n_Z are zero. The ***degree of the Weil divisor*** *is then defined to be* $\sum_{codim Z=1} n_Z$.

Example 1.22. *If $X = Spec\ R$ is an affine scheme, a Weil divisor on X is an element of the free abelian group generated by primes $\mathfrak{p}$ in Spec R of codimension 1, i.e. a finite sum* $\sum_{dim\ R_\mathfrak{p}=1} n_\mathfrak{p}[\mathfrak{p}]$ *with $n_\mathfrak{p} \in \mathbb{Z}$. Thus we also denote the set of these* ***Weil divisors on R*** *by $Z^1(R)$.*

Lemma 1.23. *If R is a noetherian ring, associating I in $Div_+(R)$ to the sum*

$$cycle(R/I) := \sum_{dim\ R_\mathfrak{p}=1} l(R_\mathfrak{p}/I_\mathfrak{p})\ [\mathfrak{p}]$$

yields a map $Div(R) \to Z^1(R)$.

Proof. Since I is in $Div_+(R)$ (so $I_\mathfrak{p}$ is generated by a non zero divisor), $dim\ R_\mathfrak{p} \geq 1$ for all $\mathfrak{p}$ containing I. If $\mathfrak{p}$ is minimal containing I, $(R/I)_\mathfrak{p}$ is artinian, so the coefficients in the above sum are well-defined. Moreover the sum above is finite since the set of minimal primes of the noetherian ring R/I is finite. Thus $cycle(R/I)$ is an element of $Z^1(R)$. □

Definition 1.24. *Let R be a noetherian ring. Composing the map $Div(R) \to Z^1(R)$ with the degree map $Z^1(R) \to \mathbb{Z}$, we define the* ***degree of a divisor***

$I \otimes J^\nu$ of $Div(R)$ by

$$deg\ (I \otimes J^\nu) = \sum_{dim\ R_\mathfrak{p}=1} l(R_\mathfrak{p}/I_\mathfrak{p}) - l(R_\mathfrak{p}/J_\mathfrak{p})$$

Example 1.25. *Let C be a curve over an algebraically closed field k (i.e. an integral separated scheme of finite type over k of dimension one). Then prime divisors on C are just closed points of C, and we have a map $Div(C) \to Z^1(C)$ which maps the divisor D to $\sum_{codim\ P=1} l(\mathcal{O}_{D,P})\ [P]$. Indeed for D positive and defined on some open affine Spec R of C by the ideal I in $Div_+(R)$, $\mathcal{O}_{D,P}$ is of the form $(R/I)_\mathfrak{p}$ for some prime $\mathfrak{p}$ of R of codimension one. Then by 1.23 (and since C as a noetherian scheme admits a finite cover by open affines) the sum $\sum_{codim\ P=1} l(\mathcal{O}_{D,P})[P]$ is an element of $Z^1(C)$.*

In fact, the mapping $Div(C) \to Z^1(C)$ is a group homomorphism, by the following:

Proposition 1.26. *If R is a noetherian domain of dimension 1, the mapping $Div(R) \to Z^1(R)$, which maps $I \in Div_+(R)$ to $\sum_{\mathfrak{p} \in Spec\ R} l(R_\mathfrak{p}/I_\mathfrak{p})\ [\mathfrak{p}]$ is a group homomorphism.*

The proof uses a lemma due to Szpiro (*Cours de Géométrie Arithmétique*, III.3.5):

Lemma 1.27. *Let I be an ideal of a ring R. If $x \in R$ is not a zero divisor, there is a short exact sequence*

$$0 \to R/I \to R/xI \to R/xR \to 0$$

Proof. Since the kernel of the canonical map $R/xI \to R/xR$ is xR/xI, it suffices to show that $R/I \simeq xR/xI$. Consider the map $R \to xR/xI$ which maps 1 to $[x]$. It is surjective with kernel $\{a \in R \mid ax \in xI\}$, which is exactly I since x is not a zero divisor. □

Proof. **1.26** Since $dim\ R_{\mathfrak{p}} = 1$ for every nonzero $\mathfrak{p}$ in $Spec\ R$ the map is well defined by lemma 1.23, and it only remains to show that it is a homomorphism of monoids. If I, J are in $Div_+(R)$, then for all $\mathfrak{p}$, $JR_{\mathfrak{p}} = xR_{\mathfrak{p}}$ for some x in R_p (which cannot be a zero divisor since R is a domain). Then by lemma 1.27 and the additivity of the length function for modules of finite length, we obtain $l(R/IJ)_{\mathfrak{p}} = l(R/I)_{\mathfrak{p}} + l(R/J)_{\mathfrak{p}}$ for all $\mathfrak{p}$, yielding $cycle(R/IJ) = cycle(R/I) + cycle(R/J)$. □

Chapter 2

Gauss Composition for Function Fields

2.1 Equivalent Quadratic Forms

We begin by defining an equivalence relation for binary quadratic forms with coefficients in a ring R, using the natural action of $GL_2(R)$ on binary forms $f(x,y)$: for $M = \begin{pmatrix} r & s \\ v & w \end{pmatrix}$ in $GL_2(R)$ we define $M(f) = f(rx+sy, vx+wy)$.

Definition 2.1. *Two binary quadratic forms $f(x,y)$ and $g(x,y)$ with coefficients in a ring R are **equivalent over** R if $g = M(f)$ for some M in $SL_2(R)$. We write $f \sim_R g$ to denote the equivalence of f and g over R.*

Definition 2.2. *A form $ax^2+bxy+cy^2$ with coefficients in a ring R is said to be **primitive** (over R) if the ideal (a,b,c) generated by its coefficients equals R.*

We denote by $F_{D,\ R}$ the set of primitive, binary quadratic forms with coeffi-

cients in R of discriminant D, and define $\mathcal{F}_{D,\,R} = F_{D,\,R}/\sim_R$. Throughout the remainder of this chapter, we consider only rings R which are domains with fraction field of characteristic other than 2.

Lemma 2.3. *If $ax^2 + bxy + cy^2 \sim_R Ax^2 + Bxy + Cy^2$, the two forms have same discriminant, and $(A, B, C) = (a, b, c)$. In particular, primitive forms remain so under the action of $SL_2(R)$.*

Proof. Since the forms are equivalent we may write (recalling that R has fraction field of characteristic not 2):

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} M^t \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M \begin{pmatrix} x \\ y \end{pmatrix}$$

where

$$M = \begin{pmatrix} r & s \\ v & w \end{pmatrix} \in SL_2(R)$$

Comparing determinants then yields $b^2 - 4ac = B^2 - 4AC$. We also obtain:

$$\begin{array}{rcc} A & = & f(r, v) \\ B & = & 2ars + b(rw + sv) + 2cvw \\ C & = & f(s, w) \end{array}$$

The above coefficient relations show $(A, B, C) \subset (a, b, c)$. By symmetry we obtain $(a, b, c) \subset (A, B, C)$. □

For $M = \begin{pmatrix} r & s \\ v & w \end{pmatrix}$ with entries in R we define $M^* = \begin{pmatrix} w & s \\ v & r \end{pmatrix}$. We then obtain the following relation between zeroes of equivalent forms:

Lemma 2.4. *Let* $f(x,y) = ax^2 + bxy + cy^2 = a(x + z_f y)(x + \overline{z}_f y)$ *have coefficients in* R *and nonsquare discriminant* D*, where*

$$z_f := \frac{b+\tau}{2a}\ , \quad \overline{z}_f := \frac{b-\tau}{2a}, \quad \textit{with } \tau^2 = D.$$

Then if $g = M(f)$ *for* $M = \begin{pmatrix} r & s \\ v & w \end{pmatrix}$ *in* $SL_2(R)$*, we have*

$$z_g = M^*(z_f) := \frac{wz_f + s}{vz_f + r}$$

Proof. Let K be the fraction field of R, and $N = N_{K(\tau)/K}$ denote the norm map, so we may write $f(x,y) = aN(x + z_f y)$. Then

$$\begin{aligned} g(x,y) &= f(rx+sy, vx+wy) \\ &= aN((rx+sy) + (vx+wy)z_f) \\ &= aN((vz_f+r)x + (wz_f+s)y) \\ &= aN(vz_f+r)\ N(x + \frac{wz_f+s}{vz_f+r}y) \end{aligned}$$

Thus z_g is equal to either $\frac{wz_f+s}{vz_f+r}$ or its conjugate. If $g(x,y) = Ax^2+Bxy+Cy^2$, the formulas for A, B, C in lemma 2.3 yield:

$$\frac{wz_f+s}{vz_f+r} = \frac{(wz_f+s)(v\overline{z}_f+r)}{(vz_f+r)(v\overline{z}_f+r)} = \frac{2a(wz_f+s)(v\overline{z}_f+r)}{2f(r,v)} = \frac{B+\tau}{2A} = z_g$$

□

2.2 Gauss Composition for Function Fields

Let k be an algebraically closed field of characteristic other than 2. We henceforth restrict our attention to the ring $R = k[u]$, and to *nonsquare* $D \in k[u]$. For any such D we let $R_D = k[u][t]/(t^2 - D)$, and for ease of notation write simply F_D for $F_{D,\ k[u]}$.

Lemma 2.5. *Given $f(x,y) = ax^2 + bxy + cy^2 \in F_D$, let z_f be as in lemma 2.4, and let I_f be the free rank 2 $k[u]$-module with $k[u]$-basis $(1, z_f)$. Then $I_f \in Div(R_D)$.*

Proof. Since $\tau^2 = D$, R_D has $k[u]$-basis $(1,\tau)$, and I_f is an R_D-submodule of the fraction field K of R_D since $\tau I_f \subset I_f$: indeed $\tau = -b + 2az_f \in I_f$, and $\tau z_f = -2c + bz_f \in I_f$. I_f is a fractional ideal of R_D since $aI_f \subset R_D$, and is invertible since $(1, z_f)(a, a\overline{z}_f) = R_D$. Thus $I_f \in Div(R_D)$ by lemma 1.9. □

Lemma 2.6. *Let $I \in Inv(R_D)$ have $k[u]$-basis $(1,\gamma)$, and let $a \in k[u]$ be of minimal degree such that $aTr(\gamma)$ and $aN(\gamma)$ belong to $k[u]$. Then we have $R_D = (1, a\gamma)$.*

Proof. By lemma 1.1, it suffices to show $Stab(I) = (1, a\gamma)$. For any α in $Stab(I)$ we have $\alpha(1,\gamma) \subset (1,\gamma)$, whence $\alpha = \alpha \cdot 1 = n + m\gamma$ for some

$n, m \in k[u]$. Then since γ satisfies $x^2 - Tr(\gamma)x + N(\gamma) = 0$, we also have

$$\alpha\gamma = (n + m\gamma)\gamma = (n + mTr(\gamma))\gamma - mN(\gamma)$$

whence $mTr(\gamma)$ and $mN(\gamma)$ belong to $k[u]$. But since by hypothesis a is of minimal degree such that $aTr(\gamma), aN(\gamma) \in k[u]$, it follows that $a|m$ and $Stab(I) = (1, a\gamma)$ as desired. □

Theorem 2.7. *(Gauss' Theorem for function fields)*
For $f(x, y) = ax^2 + bxy + cy^2 \in F_D$, let $I_f \in Div(R_D)$ be as in the previous lemma. Then the map $f \mapsto I_f$ induces a bijection

$$\mathcal{F}_D \to Pic(R_D)$$

$$[f] \mapsto [I_f^{\nu}]$$

Proof. The map is well-defined by lemma 2.4: indeed if $z_g = \dfrac{wz_f + s}{vz_f + r}$ where $rw - sv = 1$, then $(1, z_g) \simeq (vz_f + r, wz_f + s) = (1, z_f)$. To establish surjectivity, let $L \in Pic(R_D)$, so by lemma 1.12 $L \simeq I^{\nu}$ for some I in $Div(R_D)$, which we may assume has $k[u]$-basis $(1, \gamma)$ for $\gamma = p + q\tau,\ p,\ q$ in $k(u)$. Let $T = Tr(\gamma),\ N = N(\gamma)$, and let $a \in k[u]$ be of minimal degree such that $aT, aN \in k[u]$. Then by lemma 2.6, $R_D = (1, a\gamma) = (1, ap + aq\tau)$, so

$$\begin{pmatrix} 1 \\ \tau \end{pmatrix} = M \begin{pmatrix} 1 & 0 \\ ap & aq \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix}, \text{ where } M \in GL_2(k[u]),$$

whence $aq \in k^*$. Since a is defined up to a constant in k^*, we choose a such that $aq = 1/2$. Then $f(x,y) = ax^2 + aTxy + aNy^2$ is a form of discriminant $a^2(T^2 - 4N) = 4a^2q^2D = D$, which is primitive: indeed if $(a, aT, aN) \neq k[u]$, the ideal (a, aT, aN) is contained in some maximal ideal $(u - \alpha)$ of $k[u]$. But then $u - \alpha$ divides a, aT and aN, contradicting the minimality of the degree of a. Finally, we have

$$z_f = \frac{aT + \tau}{2a} = \frac{2apq + q\tau}{2aq} = p + q\tau.$$

Thus $I = (1, z_f)$, and L has antecedent $[f]$.

We now establish injectivity. First note that for $[f] \in \mathcal{F}_D$ we may always choose a representative $ax^2 + bxy + cy^2$ with a monic, since for any $\alpha \in k^*$, $f(x,y) \sim f(\alpha x, y/\alpha)$. Suppose $[I_f^\vee] = [I_g^\vee]$ for $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = Ax^2 + Bxy + Cy^2 \in F_D$, where a and A are assumed to be monic polynomials. Since $I_f \simeq I_g$, we have $(1, z_f) = (\mu, \mu z_g)$ for some $\mu \in K$. Replacing if necessary μ by $\alpha\mu$ for some $\alpha \in k^*$, we choose μ such that $N(\mu) \in k(u)$ is "monic", i.e. of the form

$$\frac{u^n + c_1u^{n-1} + \cdots + c_n}{u^m + c_1'u^{m-1} + \cdots + c_m'}$$

We have

$$\begin{pmatrix} 1 \\ z_f \end{pmatrix} = \begin{pmatrix} r & s \\ v & w \end{pmatrix} \begin{pmatrix} \mu \\ \mu z_g \end{pmatrix} \text{ for some } \begin{pmatrix} r & s \\ v & w \end{pmatrix} \in GL_2(k[u])$$

Hence

$$\begin{pmatrix} 1 & 0 \\ b/2a & 1/2a \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} r & s \\ v & w \end{pmatrix} \begin{pmatrix} M_\mu \end{pmatrix} \begin{pmatrix} 1 & 0 \\ B/2A & 1/2A \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix}$$

where M_μ denotes the matrix of multiplication by μ. Comparing determinants yields

$$1/2a = (rw - sv) \cdot N(\mu) \cdot (1/2A)$$

$$A = (rw - sv)\ aN(\mu)$$

Since a and A are monic polynomials and $N(\mu)$ is a quotient of monic polynomials, we find that $rw - sv = 1$, $A = aN(\mu)$, and hence

$$\begin{aligned} f(x,y) &= a\ N(x + z_f y) \\ &= a\ N(\mu)\ N((r + sz_g)x + (v + wz_g)y) \\ &= a\ N(\mu)\ N((rx + vy) + (sx + wy)z_g) \\ &= \frac{aN(\mu)}{A}\ g(rx + vy, sx + wy) \\ &= g(rx + vy, sx + wy) \end{aligned}$$

so indeed $f(x,y) \sim g(x,y)$ □

2.3 Geometric Interpretation of Gauss Composition

Lemma 2.8. *Let C be a curve, $f : C \to \mathbb{P}^1_k$ a degree 2 morphism with a smooth ramified point P_0. Then P_0 is ramified in the normalization $\tilde{C}$ of C.*

Proof. Writing $C - \{P_0\} = Spec\ A$ where A is a quadratic extension of the polynomial ring $k[u]$ and letting $z = 1/u$, we have that P_0 is ramified in $Spec\ B = f^{-1}(Spec\ k[z])$. If $B = k[z,T]/(T^2 - P)$ for $P = P(z)$ in $k[z]$, the singular points of $Spec\ B$ satisfy the system of equations

$$\begin{aligned} T^2 - P(z) &= 0 \\ 2T &= 0 \\ P'(z) &= 0 \end{aligned}$$

whence P_0 corresponds to a simple root of $P(z)$. Writing $P = \rho^2\delta$ where $\delta = \delta(z)$ is square-free, it is easily seen that the integral closure of B is $\tilde{B} = k[z,T]/(T^2 - \delta)$: any x in the fraction field K of B can be written $x = q_1 + q_2 t$, where $t^2 = P = \rho^2\delta$ and q_1, q_2 are in $k(z)$; if x is integral over $k[z]$, its trace $2q_1$ and norm $q_1^2 - q_2^2\rho^2\delta$ belong to $k[z]$, whence q_1 and $q_2\rho$ are in $k[z]$ and $x = q_1 + q_2 pT \in \tilde{B}$. Since the simple roots of $P(z)$ are necessarily roots of $\delta(z)$, P_0 ramifies in $Spec\ \tilde{B}$, hence in its projective closure $\tilde{C}$. $\square$

Lemma 2.9. *Let C be a curve over k that is a degree 2 covering of $\mathbb{P}^1_k$, with a smooth ramified point P_0. Then C is a projective closure of an affine curve $t^2 = D(u)$ where $D(u)$ is a polynomial of odd degree. Conversely, given an affine curve $t^2 = D(u)$ with $D(u)$ of odd degree, it has a projective closure C with a smooth ramified point at infinity.*

Proof. By lemma 2.8 P_0 is ramified in the normalization $\tilde{C}$ of C. We have $C - \{P_0\} = Spec\ A$, where $A = \dfrac{k[u,t]}{(t^2 - D)}$ for some polynomial $D = D(u)$, $D = m^2 d$ where d in $k[u]$ is square-free. Since $\tilde{C}$ is a projective closure of $Spec\ \dfrac{k[u,t]}{(t^2 - d)}$, it is ramified at the $deg\ d$ distinct zeroes of d in addition to P_0, for a total of $deg\ d + 1$ ramification points. We now apply Hurwitz's formula to the smooth curve $\tilde{C}$: if $g_{\tilde{C}}$ is the genus of $\tilde{C}$ and $e(P)$ is the ramification index at P of the covering $\tilde{C} \to \mathbb{P}^1_k$, we have

$$2g_{\tilde{C}} - 2 = -4 + \sum_{P \in \tilde{C}} (e(P) - 1)$$

It follows that the number of ramification points of $\tilde{C}$ is even. Thus d, and hence D, are of odd degree.

To prove the converse, note that if $D = D(u)$ has odd degree $2m + 1$, writing $D(u) = a \prod_{i=1}^{2m+1} (u - \alpha_i)$ and letting $z = 1/u$ and $T = t/u^{m+1}$, we obtain:

$$T^2 = az \prod_{i=1}^{2m+1} (1 - \alpha_i z) = a \prod_{\alpha_i \neq 0} \alpha_i \prod_{\alpha_i \neq 0} (\alpha_i^{-1} - z) =: P(z)$$

The affine curve $T^2 - P(z)$ is then clearly ramified and smooth at $z = 0$, giving us a projective closure C of $Spec\ A$ with a smooth ramified point at infinity. □

Lemma 2.10. *Let C be a curve that is a degree 2 covering of $\mathbb{P}^1_k$ with a smooth ramified point P_0, $C - \{P_0\} = Spec\ A$. Then we have an isomorphism of groups $Pic(A) \xrightarrow{\sim} Pic^0(C)$.*

Proof. We establish an isomorphism $Div(A) \xrightarrow{\sim} Div^0(C)$. Let $I \in Div_+(A)$, so $I_{f_i} \simeq A_{f_i}$ for some affine cover $X_i = Spec\ A_{f_i}$ of $Spec\ A$. Let $t_i \in I$ be generators for I_{f_i} as an A_{f_i}-module, let X_0 be an open neighborhood of P_0 where none of the t_i vanish, and let π be a local parameter at P_0, i.e., an element of $k(C)$ with $v_{P_0}(\pi) = 1$ where v_{P_0} is the valuation corresponding to the discrete valuation ring $\mathcal{O}_{P_0}$. We let $t_0 = \pi^l$ where $l = l(A/I)$. Then for all i, j nonzero, t_i/t_0 is invertible in $\mathcal{O}_C(X_i \bigcap X_0)$, and t_i/t_j is invertible in $\mathcal{O}_C(X_i \bigcap X_j) = A_{f_i f_j}$, since t_i and t_j both generate $I_{f_i f_j}$ as an $A_{f_i f_j}$-module. Thus I gives us a divisor D on C, which by example 1.25 has degree

$$degD = \sum_{P \in C} l(\mathcal{O}_{D,P}) = \sum_{\mathfrak{p} \in A} l(A_\mathfrak{p}/IA_\mathfrak{p}) + l(\mathcal{O}_{D,P_0}) = l(A/I) - v_{P_0}(\pi^l) = 0.$$

The divisor D is clearly independent of the open cover chosen for $C - \{P_0\}$ and the local generators chosen for I: if $\{U_j, s_j\}_{j=1,2,\ldots}$ is another such cover and set of local generators, then for some neighborhood U_0 of P_0 and $s_0 = \pi^l$,

we find that for all i, j, s_j and t_i differ by a unit in $\mathcal{O}_C(X_i \bigcap U_j)$, hence $(U_j, s_j) = (X_i, t_i)$ as elements of $Div^0(C)$. Thus we have a well-defined map $\varphi : Div_+(A) \to Div^0(C)$, and since $\varphi(IJ) = \varphi(I) + \varphi(J)$ for all $I, J \in Div_+(A)$, setting $\varphi(I^\nu) = -\varphi(I)$ gives us a homomorphism of groups $Div(A) \to Div^0(C)$. It is surjective: for any divisor D of degree zero on C, its restriction to $C - \{P_0\}$ corresponds to an element $I \otimes J^\nu$ of $Div(A)$ by example 1.19, and $\varphi(I \otimes J^\nu) = D$. If $\varphi(I) - \varphi(J) = (C, 1) = id_{Div^0(C)}$ for $I, J \in Div_+(A)$, local generators for I and J differ by units, so $I = J$ and φ is injective. Finally since φ maps $Pr(A)$ to principal divisors on C, the result follows from lemma 1.20. □

Theorem 2.11. *(Gauss' Theorem, Geometric version) Let C be a curve that is a degree 2 covering of $\mathbb{P}^1_k$ with a smooth ramified point P_0, and let $C - \{P_0\} = Spec\ A$. If $A = k[u,t]/(t^2 - D)$ for $D = D(u)$ in $k[u]$, we have a bijection $Pic^0(C) \to \mathcal{F}_D$.*

Proof. Immediate from lemmas 2.10 and 2.7. □

Chapter 3

Number Fields, Arakelov Theory

3.1 The Compactified Picard Group

We recall the necessary vocabulary to understand Arakelov's introduction of metrics at the infinite places of a number field.

Definition 3.1. *A* ***hermitian product*** *on a $\mathbb{C}$-vector space V is a bi-additive map $(\ ,\ ) : V \times V \to \mathbb{C}$, linear in the first variable, such that $(x, y) = \overline{(y, x)}$ for any $x, y \in V$. The product is* ***positive*** *if $(x, x) = \|x\|^2 \geq 0$ for all x in V, and is* ***nondegenerate*** *if $\|x\| = 0$ implies $x = 0$.*

If V is a one-dimensional $\mathbb{C}$-vector space, giving a positive nondegenerate hermitian product on V amounts to giving the length $\|x\| \neq 0$ of a nonzero element of V: indeed for $y, z \in V$, we have $y = \lambda x, z = \mu x$ for some $\lambda, \mu \in \mathbb{C}$ and hence $(y, z) = (\lambda x, \mu x) = \lambda\overline{\mu}\|x\|^2$. Accordingly, we will simply say that

V has a *hermitian metric* if V is a one-dimensional $\mathbb{C}$-vector space with a positive nondegenerate hermitian product.

Definition 3.2. *If a one-dimensional $\mathbb{C}$-vector space V has a hermitian metric $\| \ \|$, its dual $V^\vee$ has a canonical hermitian metric given by $\|\varphi\| = \frac{|\varphi(x)|}{\|x\|}$ for all nonzero x in V. The product $V_1 \otimes_{\mathbb{C}} V_2$ of two such vector spaces V_1, V_2 with hermitian metrics $\| \ \|_1, \| \ \|_2$, likewise has a canonical hermitian metric given by $\|x_1 \otimes x_2\| = \|x_1\|_1 \|x_2\|_2$.*

Now let K be a number field of degree n, with r_1 real places and $2r_2$ complex places. *We henceforth fix* a set Φ of r_1 real places and r_2 non-conjugate complex places, as well as an order A of K. Then if L is an invertible A-module, for every $\sigma \in \Phi$ we have a one-dimensional $\mathbb{C}$-vector space $L_\sigma := (L \otimes_A \sigma(A)) \otimes_{\sigma(A)} \mathbb{C}$, which can be provided with a hermitian metric $\| \ \|_\sigma$. This justifies the following:

Definition 3.3. *An invertible module L of an order A, together with a hermitian metric $\| \ \|_\sigma$ on L_σ for each $\sigma \in \Phi$, is called a* ***metrized invertible module*** *and denoted $(L, \| \ \|_\sigma)$.*

Since a metrized invertible module carries more information than its underlying module, a notion of 'isomorphism' for these objects necesarily refines that of an isomorphism of invertible modules:

Definition 3.4. *An **isometry** between two metrized invertible A-modules $(L_1, \| \ \|_{1,\sigma})$ and $(L_2, \| \ \|_{2,\sigma})$ is an A-module isomorphism $\varphi : L_1 \xrightarrow{\sim} L_2$, such that $\|\varphi(x)\|_{2,\sigma} = \|x\|_{1,\sigma}$ for every x in L_1.*

It immediately follows from the definition that:

Lemma 3.5. *Let $(L, \| \ \|_{1,\sigma})$ and $(L, \| \ \|_{2,\sigma})$ be metrized invertible A-modules having the same underlying module L. They are isometric if and only if $\| \ \|_{2,\sigma} = |\sigma(u)| \ \| \ \|_{1,\sigma}$ for some u in A^*.*

Definition 3.6. *The tensor product of metrized invertible A-modules induces a product on the set of isometry classes of such modules, which turns this set into a group called the **compactified Picard group of A** and denoted $Pic_c(A)$. Its identity element is the isometry class of $(A, \| \ \|_\sigma)$ where $\|1\|_\sigma = 1$ for all σ. Inverses are given by (the class of) the dual module together with the dual metric.*

For ease of notation, we shall henceforth write simply $(L, \| \ \|_\sigma)$ or L to refer to the isometry class of $(L, \| \ \|_\sigma)$ in $Pic_c(A)$ when no confusion is possible. We also denote by $(A, (x_\sigma))$ the metrized module $(A, \| \ \|_\sigma)$, where x_σ in $\mathbb{R}_+^*$ denotes the value $\|1\|_\sigma$.

Lemma 3.7. *If A is an order of a number field K, ϕ is the cardinal of the*

set Φ of real and nonconjugate complex places σ of K, and $\mu(A)$ is the set of roots of unity in A, we have the exact sequence:

$$0 \to \mu(A) \to A^* \to \mathbb{R}^\phi \to Pic_c(A) \to Pic(A) \to 0$$

where the homomorphism $A^* \to \mathbb{R}^\phi$ maps $u \mapsto (log\ |\sigma(u)|)_{\sigma\in\Phi}$

Proof. We clearly have a surjective homomorphism $Pic_c(A) \to Pic(A)$ which "forgets metrics", and whose kernel is the set $(A, (x_\sigma))$ for (x_σ) in $(\mathbb{R}_{>0})^\phi$, i.e., precisely the image of the homomorphism $\mathbb{R}^\phi \to Pic_c(A)$ mapping (λ_σ) to $(A, (e^{\lambda_\sigma}))$. By the previous lemma, we know that $(A, (e^{\lambda_\sigma}))$ is isometric to $(A, (1)_\sigma)$ if and only if there exists $u \in A^*$ such that $e^{\lambda_\sigma} = |\sigma(u)|$ for all σ, i.e., if $(\lambda_\sigma) = (log\ |\sigma(u)|)$. Finally, since $u \in A^*$ is a root of 1 if and only if $|\sigma(u)| = 1$ for all σ, we obtain the result. □

3.2 The Norm of an Ideal

In the following section we relate the norm of an ideal I in an order A of a number field to its degree as an element of $Div(A)$. The results will allow us to extend the notion of degree to classes of metrized invertible modules.

Lemma 3.8. *If $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$ is an injective homomorphism of free $\mathbb{Z}$-modules, then $|Coker\ \varphi| = |Coker\ (det\ \varphi)| = |\mathbb{Z}/(det\ \varphi)\mathbb{Z}|$.*

Proof. Since φ can be put in Smith normal form the result is immediate (note that if $a_1, a_2, ..., a_n$ are the diagonal entries of φ for appropriately chosen bases of $\mathbb{Z}^n$, they are all nonzero since φ is injective). □

Lemma 3.9. *Let I be a nonzero ideal of an order A of a number field K. Then $N(I) = |A/I|$.*

Proof. Immediate from lemma 3.8 and the definition of $N(I)$ adopted in the introduction (the absolute value of *det* T for T a transition matrix from a $\mathbb{Z}$-basis of A to a $\mathbb{Z}$-basis of I). □

Lemma 3.10. *Let x be an element of a number field K, let m_x denote a matrix of multiplication by x in K. Then*

$$det\ m_x = \prod_{\sigma: K \to \mathbb{C}} \sigma(x)$$

where the σ run through all $\mathbb{Q}$-homomorphisms of K into $\mathbb{C}$. From the definition of $N(x)$ adopted in the introduction we thus have $N(x) = det\ m_x$.

Proof. First suppose $K = \mathbb{Q}[x]$ is a degree d vector-space over $\mathbb{Q}$. The characteristic polynomial for m_x has constant term $(-1)^d det\ m_x$, while the minimal polynomial of x has constant term $(-1)^d \prod \sigma(x)$ where the σ run through all $\mathbb{Q}$-homomorphisms of $\mathbb{Q}(x)$ into $\mathbb{C}$. Since in this case the characteristic polynomial is equal to the minimal polynomial we obtain the result. Now

suppose x is an element of K such that $[K : \mathbb{Q}(x)] = m$, $[\mathbb{Q}(x) : \mathbb{Q}] = d$. The matrix m_x of multiplication by x in K can be written with m blocks equal to the matrix of m_x restricted to $\mathbb{Q}(x)$, whence

$$det\ m_x = \prod_{\sigma:\mathbb{Q}(x)\to\mathbb{C}} \sigma(x)^m$$

Since there are exactly m distinct extensions of $\sigma : \mathbb{Q}(x) \to \mathbb{C}$ to a $\mathbb{Q}$-homomorphism of K into $\mathbb{C}$, the result follows. □

Proposition 3.11. *Let I be a nonzero ideal of an order A of a number field K. Then*

$$|A/I| = \prod_{\mathfrak{p}\in Spec\ A} |A_\mathfrak{p}/IA_\mathfrak{p}|$$

and for all $\mathfrak{p} \in Spec\ A$,

$$\log|A_\mathfrak{p}/IA_\mathfrak{p}| = l(A_\mathfrak{p}/IA_\mathfrak{p})\ \log|A/\mathfrak{p}|.$$

Proof. Since A is a domain of dimension 1 and $I \neq (0)$, A/I is artinian so by lemma 1.14 $|A/I| = \prod_{\mathfrak{p}\supset I} |A_\mathfrak{p}/IA_\mathfrak{p}|$. Since $IA_\mathfrak{p} = A_\mathfrak{p}$ for all $\mathfrak{p} \not\supseteq I$, the first part of our claim follows. For the same reason, the second equation holds when $\mathfrak{p} \not\supseteq I$. When $\mathfrak{p} \supset I$, the only simple module on the artinian local ring $A_\mathfrak{p}/IA_\mathfrak{p}$ is the residual field $A/\mathfrak{p}$, whence $|A_\mathfrak{p}/IA_\mathfrak{p}| = |A/\mathfrak{p}|^{l(A_\mathfrak{p}/IA_\mathfrak{p})}$. □

Lemma 3.12. *(product formula) If x is an element of an order A of a number field K, $|N(x)| = N(Ax)$.*

Proof. Immediate from the definitions and 3.10: indeed the matrix of multiplication by x in A also represents multiplication by x in K. However as remarked by Szpiro (*Cours de Géometrie Arithmétique*, proposition 4.4), the above equality in light of 3.10 and 3.11 reads

$$\prod_{\sigma:K\to\mathbb{C}} |\sigma(x)| \quad = \prod_{\mathfrak{p}\in Spec\ A} N(\mathfrak{p})^{l(A_\mathfrak{p}/I_\mathfrak{p})} \tag{3.1}$$

and as such generalizes the classical product formula: any prime $\mathfrak{p}$ of the ring of integers $\tilde{A}$ of a number field K gives rise to a valuation $v = v_\mathfrak{p}$ on K, defined by $v_\mathfrak{p}(a) = sup\ \{n|\ a \in \mathfrak{p}^n\tilde{A}_\mathfrak{p}\}$ for a in $\tilde{A}$, and $v_\mathfrak{p}(x) = v_\mathfrak{p}(a) - v_\mathfrak{p}(b)$ for $x = a/b \in K$. The valuation $v_\mathfrak{p}$ is called a *finite place* of K, while the $\mathbb{Q}$-homomorphisms σ of K into $\mathbb{C}$ are called *infinite places* of K. For each place v we may define a norm $|\ |_v$ on K by

$$|x|_v = \begin{cases} N(\mathfrak{p})^{-v_\mathfrak{p}(x)} & \text{if } v = v_\mathfrak{p} \text{ is finite} \\ |\sigma_v(x)| & \text{if } v = \sigma_v \text{ is infinite} \end{cases}$$

Denoting by μ the set of all places of K, for any x in K the classical product formula then reads

$$\prod_{v\in\mu} |x|_v = 1$$

which is easily deduced from (3.1). □

Lemma 3.13. *For A an order of a number field, the norm map gives a group homomorphism $N : Div(A) \to \mathbb{Z}$.*

Proof. It suffices to show that the norm map $Div_+(A) \to \mathbb{N}$ is multiplicative. If I, J are elements of $Div_+(A)$, for any prime ideal $\mathfrak{p}$ of A we have $l(A_\mathfrak{p}/IJA_\mathfrak{p}) = l(A_\mathfrak{p}/I_\mathfrak{p}) + l(A_\mathfrak{p}/J_\mathfrak{p})$ by lemma 1.26 and the additivity of the length for modules of finite length. Then proposition 3.11 yields $|A/IJ| = |A/I|\ |A/J|$. □

3.3 The Degree of a Metrized Invertible Module

We begin by defining the degree of a compactified divisor:

Definition 3.14. *We define $Div_c(A)$ as $Div(A) \times \mathbb{R}^\phi$, and $Z^1_c(A)$ as $Z^1(A) \times \mathbb{R}^\phi$. Denoting a generic element of $Z^1_c(A)$ by*

$$\sum_{\mathfrak{p} \in SpecA} n_\mathfrak{p}[\mathfrak{p}] + \sum_{\sigma \in \Phi} \lambda_\sigma[\sigma]$$

we define its degree to be the real number $\sum n_\mathfrak{p}\ logN(\mathfrak{p}) + \sum \varepsilon_\sigma \lambda_\sigma$, where ε_σ is 1 or 2 acccording to whether σ is real or complex. Since we clearly have a group homomorphism $Div_c(A) \to Z^1_c(A)$ which extends the homomorphism $Div(A) \to Z^1(A)$ of 1.26 and "keeps the infinite components", by composition with the map $Z^1_c(A) \to \mathbb{R}$ we have thus defined the ***degree of a compactified divisor****.*

Proposition 3.15. *The degree map deg : $Div_c(A) \to \mathbb{R}$ is a group homo-*

morphism. If I is an ideal in $Div(A)$, considering it as a compactified divisor without any infinite components yields $deg(I) = logN(I)$.

Proof. The first claim is immediate from the definition of the degree map, while the second follows from proposition 3.11. □

Proposition 3.16. *For an order A of a number field K, we have the commutative diagram of exact sequences*

$$\begin{array}{ccccc} \mathbb{R}^{\phi} & \to & Div_c(A) & \to & Div(A) \to 0 \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{R}^{\phi} & \to & Pic_c(A) & \to & Pic(A) \to 0 \end{array}$$

Proof. The kernel of the map $Div_c(A) \to Div(A)$ which "forgets metrics" is precisely $\mathbb{R}^{\phi}$, and the bottom row of the diagram is exact by 3.7. We have a natural group homomorphism $Div_c(A) \to Pic_c(A)$ extending the homomorphism $Div(A) \to Pic(A)$ of 1.11: given $(I, (\lambda_\sigma))$ in $Div_c(A)$ for I an ideal of A, dualizing the inclusion $I \hookrightarrow A$ gives us a morphism $A \xrightarrow{\varphi} I^{\vee}$, and we map $(I, (\lambda_\sigma))$ to the isometry class of $(I^{\vee}, \| \ \|_\sigma)$ where $\|\varphi(1)\|_\sigma = e^{-\lambda_\sigma}$. (Thus if $L \in Pic_c(A)$ and s is any nonzero element of L, in the notation of lemma 1.12, L has antecedent $(\mathfrak{a}_s, -log\|s\|_\sigma)$ in $Div_c(A)$). The map $\mathbb{R}^{\phi} \to \mathbb{R}^{\phi}$ maps (λ_σ) to $(-\lambda_\sigma)$, and commutativity is then clear. □

Definition 3.17. *If a is an element of A, we associate to it the compactified divisor $(Aa, log|\sigma(a)|)$ which we denote simply (a). The induced homomorphism of semigroups $A - \{0\} \to Div_c(A)$ extends to a homomorphism of groups $K^* \to Div_c(A)$, the elements of whose image are called* ***principal compactified divisors****. These form a group of denoted $Pr_c(A)$.*

Proposition 3.18. *The degree map $Div_c(A) \to \mathbb{R}$ vanishes on $Pr_c(A)$. It thus defines a group homomorphism we continue to call deg: $Pic_c(A) \to \mathbb{R}$, which maps L in $Pic_c(A)$ to*

$$deg\ L = log\frac{|L/As|}{\prod_{\sigma\in\phi}\|s\|_\sigma^{\varepsilon_\sigma}} \tag{3.2}$$

where s is any nonzero element of L.

Proof. If a is in A,

$$deg(a) = logN(Aa) - \sum \varepsilon_\sigma log|\sigma(a)| = logN(Aa) - log|N(a)| = 0$$

by the product formula of 3.12. To establish the formula for the degree of L in $Pic_c(A)$ we consider the ideal $\mathfrak{a}_s$ corresponding to a nonzero s in L as in 1.12. By corollary 1.13 we have $L/As \simeq A/\mathfrak{a}_s$, and thus

$$deg\ L = deg\ (\mathfrak{a}_s, (-log\|s\|_\sigma))$$

by the antecedent for L given in 3.16. The formula above follows. □

3.4 Arakelovian Interpretation of Gauss Composition

Let A be an order of an imaginary quadratic field K. The degree formula above shows that if $L \in Pic_c(A)$ has degree 0, the metric for L is determined and given by $\|s\|_L^2 = |L/As|$. Denoting by $Pic_c^0(A)$ the kernel of the *deg* homomorphism, we have the following

Proposition 3.19. *For an order A of an imaginary quadratic field K, the map $Pic_c^0(A) \to Pic(A)$ which "forgets metrics" is an isomorphism of groups.*

Proof. We clearly have a surjective group homomorphism which is injective: if $\varphi : L \to L'$ is an A-isomorphism, then

$$\|\varphi(x)\|_{L'}^2 =\mid L'/A\varphi(x) \mid=\mid L/Ax \mid= \|x\|_L^2 \quad \text{for all } x \text{ in } L$$

whence $(L, \| \ \|_L)$ is isometric to $(L', \| \ \|_{L'})$. □

Lemma 3.20. *Let A be an order of a number field K, L an invertible A-submodule of K and s a nonzero element of L. Then $|L/As| = N(s)/N(L)$*

Proof. Supposing first that $L \subset A$, we have a split exact sequence

$$0 \to L/As \to A/As \leftrightarrows A/L \to 0$$

whence $|A/As| = |A/L| \ |L/As|$, so $N(s) = N(L)|L/As|$ by lemmas 3.9 and 3.12. If L is not contained in A, since L is invertible there exists a $b \in A$ such

that $bL \subset A$, so $|L/As| = |bL/Abs| = \dfrac{N(bs)}{N(bL)}$ by the above, and the result follows from the multiplicativity of the norm for invertible modules. □

Theorem 3.21. *(Gauss' Theorem in Arakelov's Theory) Let A be an order of discriminant D in an imaginary quadratic number field K. The set $\mathcal{F}_D^+$ of $SL_2(\mathbb{Z})$-equivalence classes of positive definite, primitive binary quadratic forms of discriminant D is in bijection with the group $Pic_c^0(A)$ of degree zero isometry classes of invertible A-modules.*

Proof. Since A has discriminant congruent to 0 or 1 (mod 4), it has $\mathbb{Z}$-basis $(1, t)$ where multiplication is given by

$$t^2 = \begin{cases} D/4 & if \quad D \equiv 0 \pmod 4 \\ t + \frac{D-1}{4} & if \quad D \equiv 1 \pmod 4 \end{cases}$$

Choosing τ such that $\tau^2 = D$ we may then choose t so that

$$t = \begin{cases} \tau/2 & if \quad D \equiv 0 \pmod 4 \\ \frac{\tau+1}{2} & if \quad D \equiv 1 \pmod 4 \end{cases}$$

If $f(x, y) = ax^2 + bxy + cy^2$ is in F_D^+, denoting by z_f the element $(b+\tau)/2a$ of K we write $f(x, y) = aN(x + z_f y)$, and claim that the free $\mathbb{Z}$-submodule I_f of K with basis $(1, z_f)$ is an A-module: indeed, $tI_f \subset I_f$ since if D is divisible by 4, b is even, and

$$\begin{array}{llll} t & = \tau/2 & = az_f - b/2 & \in (1, z_f) \\ tz_f & = \tau z_f/2 & = bz_f/2 - c & \in (1, z_f) \end{array}$$

Similarly, if $D \equiv 1 \pmod 4$, b is odd, and

$$\begin{array}{lll} t & = (\tau+1)/2 & = (1-b)/2 + az_f \quad \in (1, z_f) \\ tz_f & = (\tau+1)z_f/2 & = -c + (b+1)z_f/2 \quad \in (1, z_f) \end{array}$$

Moreover I_f is invertible: since $f(x,y)$ is primitive, we have in all cases

$$(1, z_f)(a, a\overline{z}_f) = (a, b, c, az_f) = (1, az_f) = (1, \frac{b+\tau}{2}) = A$$

whence I_f is in $Div(A)$ by 1.9. Finally if $f(x,y) \sim g(x,y)$, I_f is isomorphic to I_g as an A-module by 2.4, hence isometric by 3.19. Thus we have a well-defined map $\mathcal{F}_D^+ \to Pic_c^0(A)$, mapping the equivalence class of $f(x,y)$ to the isometry class of I_f.

We establish surjectivity: For any L in $Pic_c^0(A)$, identifying $L^\vee$ with an ideal $\mathfrak{a}_s$ of A as in 1.12—and noting that $\mathfrak{a}_s^\vee \simeq (A : \mathfrak{a}_s)$ by lemma 1.9—allows us to identify L with an A-submodule of K which we continue to call L, and which we may assume to have $\mathbb{Z}$-basis $(1, \gamma)$. Replacing if necessary γ by $-\gamma$ we moreover suppose $\gamma = p + qt$, where p, q are rational with $q > 0$. Letting $T = Tr(\gamma)$, $N = N(\gamma)$, and letting a be the smallest positive integer such that $aT, aN \in \mathbb{Z}$, by analogy with 2.6 we have $A = (1, a\gamma)$: for any α in $Stab(I)$ we have $\alpha = \alpha \cdot 1 = n + m\gamma$ for some $n, m \in \mathbb{Z}$, so since γ satisfies $x^2 - Tx + N = 0$, we also have

$$\alpha\gamma = (n + m\gamma)\gamma = (n + mT)\gamma - mN$$

whence mT and mN belong to $\mathbb{Z}$. Since a is minimal such that $aT, aN \in \mathbb{Z}$, it follows that $a|m$ and $Stab(I) = (1, a\gamma)$. Thus $A = (1, a\gamma)$ by 1.1, and $f(x,y) = aN(x + \gamma y)$ is a primitive positive definite form of discriminant $a^2(Tr(\gamma)^2 - 4N(\gamma)) = 4a^2q^2D$ equal to the discriminant of the basis $(1, a\gamma)$ of A, i.e. equal to D. Clearly $z_f = \gamma$ by our choice of γ, whence L has antecedent f in $\mathcal{F}_D^+$.

To see injectivity, suppose that $I_f \simeq I_g$ for $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = Ax^2 + Bxy + Cy^2$ in $\mathcal{F}_D^+$: then for some μ in K and some invertible $\begin{pmatrix} r & s \\ v & w \end{pmatrix}$ in $GL_2(\mathbb{Z})$, we have

$$\begin{pmatrix} r & s \\ v & w \end{pmatrix} \begin{pmatrix} 1 \\ z_f \end{pmatrix} = \begin{pmatrix} \mu \\ \mu z_g \end{pmatrix}$$

whence $\dfrac{\mu}{\mu z_g} = \dfrac{r + sz_f}{v + wz_f}$ and $z_g = \dfrac{v + wz_f}{r + sz_f}$. Expanding yields:

$$\begin{aligned} \frac{B + \tau}{2A} &= \frac{(v + wz_f)(r + s\overline{z}_f)}{(r + sz_f)(r + s\overline{z}_f)} \\ &= \frac{2a(v + wz_f)(r + s\overline{z}_f)}{2f(r,s)} \\ &= \frac{2arv + (rw + sv)b + 2csw + (rw - sv)\tau}{2f(r,s)} \end{aligned}$$

Then comparing coefficients for τ on the left and right, since A and $f(r,s)$

are both positive we obtain $rw - sv = 1$, hence $A = f(r, s)$ and

$$\begin{aligned} g(x,y) &= A\ N(x + z_g y) \\ &= A\ N(x + \frac{v + wz_f}{r + sz_f} y) \\ &= \frac{A}{N(r + sz_f)}\ N((r + sz_f)x + (v + wz_f)y) \\ &= a\ N((rx + vy) + (sx + wy)z_f) \\ &\sim f(x,y) \end{aligned}$$

Thus the map is injective. □

Bibliography

[1] M. Bharghava. *Higher composition laws I: a new view on Gauss composition, and quadratic generalizations*. Annals of Mathematics, vol. 159, 2004, pp. 217-250.

[2] Z. Borevich, I. Shafarevich. *Number Theory*. Pure and Applied Mathematics, No. 20, Academic Press, New York, 1966.

[3] G. van der Geer, R. Schoof. *Effectivity of Arakelov Divisors and the Theta Divisor of a Number Field*. http://arxiv.org/abs/math/9802121v3.

[4] A. Grothendieck, J.Dieudonné. *Eléments de Géométrie Algébrique I*. Springer-Verlag, Berlin Heidelberg, 1966.

[5] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York, 1977.

[6] Yves Hellegouarch. *Positive binary quadratic forms over k[X]*. Lect. Notes Math., No. 1380, Springer-Verlag, Berlin Heidelberg, 1989, pp. 93-119.

[7] P. Samuel. *Théorie Algébrique des Nombres*. Hermann, Paris, 1967.

[8] J.P. Serre. *Cours d'Arithmétique*. P.U.F., Paris, 1970.