0

Introduction

1. The method of infinite descent

1.1 One way of proving the irrationality of the square root of 2 is the following one, known as the *infinite descent* method [I]. Assume that x and y are non-zero positive integers such that

$$x^2 = 2y^2. \tag{1}$$

Then x^2 is even, hence x is even,

$$x = 2z, \tag{2}$$

say. Substituting in (1) and dividing by two we get

$$y^2 = 2z^2. \tag{3}$$

In other words, we have a new solution of (1). But this solution (y, z) is *smaller* than the previous one. For instance, the squared norm $y^2 + z^2$ of the vector (y, z) is smaller than $x^2 + y^2$.

We can repeat the argument starting from the solution (y, z) to get a new solution (z, t), and so on. Since a bounded set of integers is finite, this "descent" must end. We get a solution of (1) with either x or y equal to zero. But then, by (2), the original solution must also be the trivial one; a contradiction.

1.2 One may wonder whether this method of infinite descent, due to Fermat, can solve all diophantine equations, i.e., systems of polynomial

equations with integral coefficients and integral unknowns. It is very appropriate for showing that a diophantine equation has no nontrivial solution; for instance, $x^4 + y^4 = z^2$ or $x^3 + y^3 = z^3$ [W1].

It is also a good method for obtaining infinitely many solutions. One starts with a few small solutions; then, by running the descent argument backwards, these generate infinitely many others. This applies to Pell's equation and to the proof of the Mordell–Weil theorem.

But the argument we just made suggests that, when descent applies, there are either zero or infinitely many nontrivial solutions. Indeed, if there are finitely many solutions, when trying to show there are no more, we would have to be sure that the descent process avoids the nontrivial ones!

1.3 To overcome this difficulty, we describe the method of infinite descent in other terms. Forgetting the (fortuitous?) fact that equation (3) repeats equation (1), we may say that *infinite descent is a combination of congruence and height (= size) arguments.* In that sense, one may hope for a *geometry* which, instead of using these two kinds of arguments one after the other, would involve them simultaneously. Such a static version of infinite descent might prove finiteness theorems.

1.4 The Grothendieck theory of *schemes* gives an adequate geometric generalization of the congruence arguments in diophantine equations. Indeed, a scheme X over $\mathbb{Z}$ is viewed as a family of varieties over $\operatorname{Spec}\mathbb{Z}$, the fiber at a prime p being the reduction of X modulo p.

Given such a variety X, if we want to control the *height* of its points we have to consider the complex variety $X(\mathbb{C})$ (we assume it is smooth) from the point of view of *hermitian complex geometry.* This means that we endow holomorphic vector bundles on $X(\mathbb{C})$ with smooth hermitian metrics.

Arakelov geometry [A1][A2] is a combination of schemes and hermitian complex geometry. Its main achievement today is the proof of the Mordell conjecture [F1][V2][Bo]: a smooth projective curve of genus greater than one has only finitely many rational points.

1.5 As we said earlier, Arakelov geometry is a *static* generalization of infinite descent. For instance, when doing intersection theory on X (see Chapter I below) one is not allowed to move the cycles; no analog of Chow's Moving Lemma is known over $\mathbb{Z}$. A more dynamic approach would be an *adelic* variant of Arakelov geometry. The main object of

study in this theory would be a smooth variety V over $\mathbb{Q}$, and vector bundles on V equipped with metrics at archimedean places, and p-adic analogs of these at finite places. Such an *adelic geometry* is still to be built.

2. The analogy between function fields and number fields

2.1 Several authors, including A. Weil [W2], have emphasized the analogy between a number field, i.e., a finite extension of $\mathbb{Q}$, and the field $\mathbb{C}(S)$ of meromorphic functions on a smooth complete curve S.

For instance, for any function $f \in \mathbb{C}(S)$, $f \neq 0$, and any point $x \in S$, denote by $v_x(f) \in \mathbb{Z}$ the valuation of f at x, i.e., the order of vanishing of f at x or minus the order of the pole of f at x. From the Cauchy *residue formula* we get

$$\sum_{x \in S} v_x(f) = \sum_{x \in S} \mathrm{Res}_x\left(\frac{df}{f}\right) = 0, \tag{4}$$

where Res_x denotes the residue at x of differential forms.

When $f \in \mathbb{Q}^*$ is a rational number we have the *product formula*

$$|f| = \prod_p p^{v_p(f)}, \tag{5}$$

where p runs over all integral primes and $v_p(f) \in \mathbb{Z}$ is the p-adic valuation of f. If we define

$$v_\infty(f) = -\log|f| \in \mathbb{R}, \tag{6}$$

we may rewrite (5) as

$$\sum_p v_p(f)\log(p) + v_\infty(f) = 0, \tag{7}$$

an analog for $\mathbb{Q}$ of equation (4) for $\mathbb{C}(S)$.

From this example we see that, in this analogy, the complete curve S is analogous to the affine scheme $\mathrm{Spec}\,\mathbb{Z}$ to which is added a point at infinity (at this point the archimedean norm is used instead of discrete valuations). This fits with the view expressed above that algebraic geometry has to be completed by hermitian complex geometry.

2.2 In general, let X be an *arithmetic variety*. By this we mean a regular scheme, projective and flat over $\mathbb{Z}$.

In other words, we consider a system of polynomial equations

$$f_1(x_0, \cdots, x_N) = f_2(x_0, \cdots, x_N) = \cdots = f_k(x_0, \cdots, x_N) = 0, \tag{8}$$

where $f_1, \cdots, f_k \in \mathbb{Z}[X_0, \cdots, X_N]$ are homogeneous polynomials with

integral coefficients. These define the projective scheme $X = \mathrm{Proj}(S)$, where S is the quotient of $\mathbb{Z}[X_0, \cdots, X_N]$ by the ideal generated by $f_1, \cdots, f_k$. The points of X are those homogeneous prime ideals $\mathcal{P}$ in S which do not contain the augmentation ideal ([H], II.2). The map $f : X \to \mathrm{Spec}\,\mathbb{Z}$ maps $\mathcal{P}$ to $\mathcal{P} \cap \mathbb{Z}$. The fiber of f over a prime integer (special fiber) is the variety $f^{-1}(p\mathbb{Z}) = X/p = \mathrm{Proj}(S/pS)$ over the field with p elements. The generic fiber is $f^{-1}((0)) = X_{\mathbb{Q}} = \mathrm{Proj}(S \otimes_{\mathbb{Z}} \mathbb{Q})$. We assume that X is regular and that f is flat, i.e. S is torsion free. It follows that X/p is smooth, except for finitely many values of p, like q in Figure 1, where it may not even be reduced.

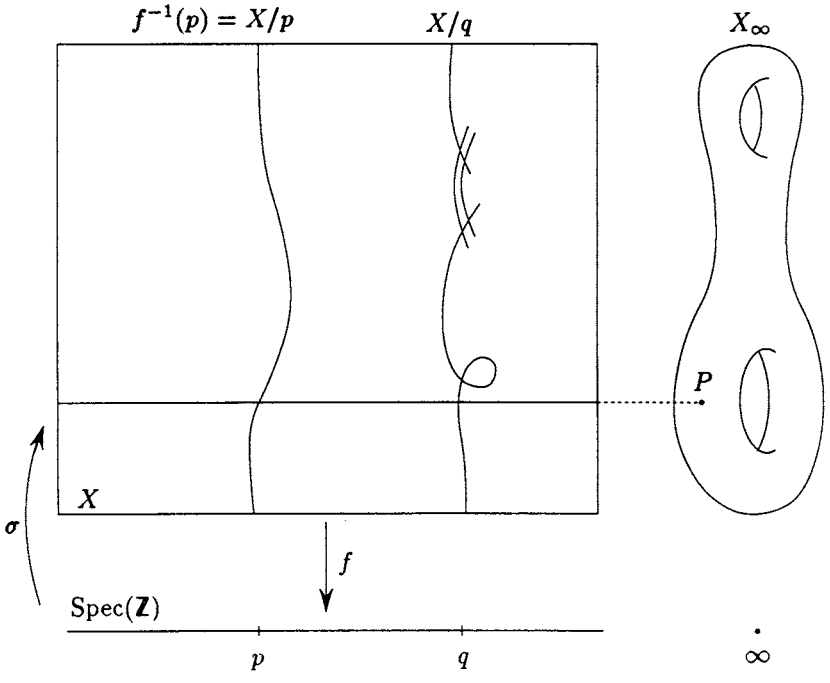

Figure 1: An arithmetic variety

In the same way that we completed $\mathrm{Spec}\,\mathbb{Z}$ by adding a point ∞ to it, we "complete" the family X of varieties over $\mathrm{Spec}\,\mathbb{Z}$ by adding to it the complex variety $X_\infty = X(\mathbb{C})$, i.e. the set of complex solutions of (8), viewed as the fiber at infinity. We think of the whole family as analogous to a complete smooth complex manifold Y fibered over a smooth complete curve S via a flat proper map $f : Y \to S$, and we

visualize the situation as in Figure 1. If the fibers of f have dimension one, X has Krull dimension two (we call it an *arithmetic surface*) and X_∞ is a complex curve (a *Riemann surface*). Notice that an integral solution of (8) is a (rational) point P in $X(\mathbb{Z}) = X(\mathbb{Q}) \subset X(\mathbb{C})$, i.e. a section σ of f.

The need to control the size of these points P leads us to take as our main object of study an algebraic vector bundle E on X, endowed with a smooth hermitian metric h on the corresponding holomorphic vector bundle E_∞ on X_∞ (we further assume that h is invariant under the complex conjugation F_∞ on X_∞). The pair $\overline{E} = (E, h)$ will be called an *hermitian vector bundle* on X.

3. The contents of this book

3.1 Let X be an arithmetic variety and $\overline{E}$ an hermitian vector bundle on X. We shall attach to $\overline{E}$ *characteristic classes* with values in *arithmetic Chow groups*.

More specifically, an *arithmetic cycle* is a pair (Z, g) consisting of an algebraic cycle on X, i.e. a finite sum $\sum_\alpha n_\alpha Z_\alpha$, $n_\alpha \in \mathbb{Z}$, where Z_α is a closed irreducible subscheme of X, of fixed codimension p, say, and a *Green current* g for Z. By this we mean that g is a real current on X_∞ which satisfies $F_\infty^*(g) = (-1)^{p-1} g$ and

$$dd^c g + \delta_Z = \omega, \tag{9}$$

where ω is (the current attached to) a smooth form on X_∞, and δ_Z is the current given by integration on Z_∞:

$$\delta_Z(\eta) = \sum_\alpha n_\alpha \int_{Z_\alpha(\mathbb{C})} \eta, \tag{10}$$

for any smooth form η of appropriate degree.

The arithmetic Chow group $\widehat{CH}^p(X)$ is the abelian group of arithmetic cycles, modulo the subgroup generated by pairs $(0, \partial u + \overline{\partial} v)$ and $(\mathrm{div} f, -\log |f|^2)$, where u and v are arbitrary currents of the appropriate degree and $\mathrm{div} f$ is the divisor of a non-zero rational function f on some irreducible closed subscheme of codimension $p-1$ in X.

3.2 In Chapter III we study the groups $\widehat{CH}^p(X)$, showing that they have functoriality properties and a graded product structure, at least after tensoring them by $\mathbb{Q}$. To prove these facts is rather difficult, for two reasons.

First, the intersection theory on a general regular scheme such as X cannot be defined in the usual way, since no Moving Lemma is available. We remedy this in Chapter I by using algebraic K-theory and Adams operations as in [GS1]. In particular, we give a proof of the vanishing of Serre's intersection multiplicities of two modules on a regular local ring, when the sum of the codimensions of their supports exceeds the dimension of the ring.

A second difficulty is that, given two arithmetic cycles (Z, g) and (Z', g'), we need a Green current for their intersection. The formula

$$g'' = \omega g' + g\delta_{Z'},$$

where ω is defined as in (9), is formally satisfactory, but involves a product of currents $g\delta_{Z'}$. To make sense of it in general we need to show that we can take for g a smooth form on $X_\infty - Z_\infty$, of *logarithmic type* along Z_∞. This is done in Chapter II.

3.3 After having set up arithmetic intersection theory, we define in Chapter IV characteristic classes for hermitian vector bundles $\overline{E}$ on X. For instance, we get a Chern character class

$$\widehat{\mathrm{ch}}(\overline{E}) \in \bigoplus_{p\geq 0} \widehat{CH}^p(X) \otimes_{\mathbf{Z}} \mathbf{Q}. \tag{11}$$

This class satisfies the usual axiomatic properties of a Chern character. But it does depend on the choice of a metric on E. Furthermore it is not additive for arbitrary exact sequences; it is additive, however, on orthogonal direct sums. Its failure to be additive on exact sequences is given by a *secondary characteristic class* first introduced by Bott and Chern [BC]. Similar results hold for the Chern classes $\widehat{c}_n(\overline{E})$ and the Todd class $\widehat{Td}(\overline{E})$.

3.4 Our next construction is some *direct image* map for hermitian vector bundles. Let $f : X \to Y$ be a proper flat map between arithmetic varieties, smooth on the generic fiber $X_{\mathbf{Q}}$. According to [KM], there is a canonical line bundle $\lambda(E)$ on Y whose fiber at every point $y \in Y$ is the determinant of the cohomology of $X_y = f^{-1}(y)$ with coefficients in E:

$$\lambda(E)_y = \bigotimes_{q\geq 0} \Lambda^{\max}(H^q(X_y, E))^{(-1)^q}, \tag{12}$$

where $\Lambda^{\max}$ denotes the maximal exterior power, and L^{-1} the dual of a line bundle L.

To get a metric on $\lambda(E)$ let us fix a Kähler metric on X_∞, hence on each fiber X_y, $y \in Y_\infty$. According to Quillen [Q2] we may then

a smooth metric h_Q on $\lambda(E)_\infty$ by multiplying its L^2-metric (given by integration along the fibers) by the square of the Ray–Singer *analytic torsion* [RS]:

$$h_Q = h_{L^2} \cdot \exp(T(E)), \tag{13}$$

with

$$T(E) = \sum_{q \geq 0} (-1)^{q+1} q \, \zeta_q'(0). \tag{14}$$

Here $\zeta_q'(0)$ is the derivative at the origin of the zeta function $\zeta_q(s)$, $s \in \mathbb{C}$, of the Laplace operator $\Delta^q = \overline{\partial}\overline{\partial}^* + \overline{\partial}^*\overline{\partial}$ acting upon forms of type $(0,q)$ on X_y, $y \in Y_\infty$, with coefficients in E_∞.

In Chapters V and VI we study $\zeta_q(s)$ and the Quillen metric. Following [BGS1] we show that h_Q is smooth and we compute in Chapter VII the curvature on Y_∞ of the hermitian line bundle $\lambda(E)_Q = (\lambda(E), h_Q)$. It is given by a Riemann–Roch–Grothendieck formula at the level of forms.

3.5 When combining the above results with the Riemann–Roch–Grothendieck theorem for algebraic Chow groups, we get in Chapter VIII a Riemann–Roch–Grothendieck theorem for arithmetic Chow groups. Given a proper map $f : X \to Y$ between arithmetic varieties, smooth on $X_\mathbb{Q}$, and an hermitian vector bundle $\overline{E}$ on X, this theorem states that

$$\delta(E) = \widehat{c}_1(\lambda(E)_Q) - f_*(\widehat{\mathrm{ch}}(\overline{E})\widehat{Td}(f))^{(1)} \tag{15}$$

depends only on the class of E in the Grothendieck group $K_0(X_\mathbb{Q})$ of the generic fiber of X; here $\alpha^{(1)}$ is the degree one component of $\alpha \in \bigoplus_{p \geq 0} \widehat{CH}^p(X) \otimes_\mathbb{Z} \mathbb{Q}$.

3.6 An application of this is the following existence theorem of small sections for powers of ample line bundles [GS4]. Let $\overline{L}$ be an hermitian line bundle on some arithmetic variety X, of relative dimension d over $\operatorname{Spec} \mathbb{Z}$. Assume that L is ample, the metric on L_∞ is positive, and the arithmetic self-intersection $\overline{L}^{d+1} \in \mathbb{R}$ of $\overline{L}$ is positive. Let $\overline{E}$ be any holomorphic vector bundle on X, and r the rank of E. Call $h^0(X, \overline{E} \otimes \overline{L}^n) \in \mathbb{R}$ the logarithm of the number of sections $s \in H^0(X, E \otimes L^n)$ of $E \otimes L^n$ such that

$$\|s(x)\| \leq 1 \quad \text{for every } x \in X_\infty; \tag{16}$$

compare with (6).

Then, as n goes to infinity, we have

$$h^0(X, \overline{E} \otimes \overline{L}^n) \geq \frac{r}{(d+1)!} \overline{L}^{d+1} n^{d+1} + O(n^d \log\, n). \tag{17}$$

The proof of this result combines the arithmetic (relative) Riemann–Roch–Grothendieck theorem for the map $X \to \operatorname{Spec} \mathbb{Z}$ with the Minkowski theorem for the lattice $H^0(X, E \otimes L^n)$, endowed with the appropriate metrics. This fits well with the view of Weil [W2] that Minkowski's theorem is an arithmetic analog of the (absolute) Riemann–Roch theorem for complex curves; see also [GS6]. Notice that the base point over which such a curve is defined has no obvious arithmetic counterpart!

The proof of (17) was used by Vojta in one of the steps of his proof of Mordell's conjecture. We refer the reader to his paper [V2], and to Faltings' paper [F3] for the use of arithmetic intersection theory in the study of rational points on abelian varieties.

3.7 Finally, a word of warning. Several proofs in this book are only sketched. Furthermore, we shall quote without proofs results from algebraic K-theory ([Q1], [S1], [GS1]) and the family index theorem ([B1], [BV], [BGV]). Generally speaking, we assume more knowledge of algebra, especially in Chapter I, than of differential geometry, but it might help to consult other books for the basic material, for instance [BGV] when reading Chapters V, VI and VII.

The book contains several remarks and open problems. These range from precise assertions and references to vague conjectures. We have not censored them too much, rather hoping that they will stimulate the reader's own research.

I

Intersection Theory on Regular Schemes

In this chapter, we shall follow [GS1] and define an intersection theory on an arbitrary regular noetherian finite-dimensional scheme X, i.e. a graded pairing between the Chow groups $CH^p(X)$ of cycles of codimension p on X, modulo linear equivalence. However, in general, this pairing is defined only up to torsion.

When X is of finite type over a field, the usual method to get an intersection theory for cycles on X is to use the Moving Lemma [RJ], which asserts that, given two cycles, one can change one of them by linear equivalence and make their intersection proper. Unfortunately this Lemma is not known on a general base. When X is smooth over a Dedekind ring, Fulton's method of the normal cone can be applied instead of the Moving Lemma [Fu]. But in general no geometric method is available (see however [RP] and [KT] for an extension of Fulton's method, up to torsion).

The tool we shall be using here is an isomorphism between $CH^p(X)_{\mathbb{Q}}$ and $K_0(X)^{(p)}$, the weight p-part, for the Adams operations, of the Grothendieck K-group of locally free coherent $\mathcal{O}_X$-modules. The pairing between $K_0(X)^{(p)}$ and $K_0(X)^{(q)}$ is then just given by the tensor product of $\mathcal{O}_X$-modules.

The plan of this chapter is as follows. In §1 and §2 we state the main results (see Theorem 2). In §3 we introduce Grothendieck groups. In Theorem 3(i) we state that their filtration by codimension is multiplicative up to torsion, and in Theorem 3(ii) we compare it with the Chow groups. In Corollary 1 we deduce from Theorem 3 a conjecture of Serre

on the vanishing of some intersection multiplicities; another proof was given by Roberts [RP], using Fulton's theory. In §4 we define λ-rings and we state the existence of such a structure on the Grothendieck groups (with supports). This result is proved in §5. In §6 we prove Theorem 3(i), thus completing the proof of Serre's conjecture. Finally, we describe how the λ-ring structure on Quillen higher K-theory [Kr] [S1] leads to the comparison of Chow groups and Grothendieck groups stated in Theorem 3(ii). However, at this point, we do not give any details.

We shall use the following convention (valid for the whole book): given an abelian group A, we denote by $A_{\mathbb{Q}}$ the vector space $A \otimes_{\mathbb{Z}} \mathbb{Q}$.

1. Length and order

1.1 Let R be a noetherian ring and M a finitely generated R-module. There exists a chain of submodules

$$M = M_0 \supset M_1 \supset \cdots \supset M_\ell = 0 \tag{1}$$

with $M_{i-1}/M_i \cong R/\wp_i$, where $\wp_i$ is a prime ideal of R [Se2].

Definition 1 *M is said to have finite length, if all $\wp_i$ occurring in (1) are maximal ideals.*

A module M has finite length if and only if its support $\mathrm{Supp}\ M = \{\wp \in \mathrm{Spec} R : M_\wp = M \otimes_R R_\wp \neq 0\}$ consists of maximal ideals. If M has finite length, it can be shown that any two chains (1) have the same length; we denote it by $\ell_R(M)$ and call it the *length* of M. The function $\ell_R(\cdot)$ is additive on exact sequences.

1.2 Let now R be a one-dimensional integral domain and K its fraction field.

Definition 2 *For $f \in K^*$, $f = a \cdot b^{-1}$ with $a, b \in R$ we put*

$$\mathrm{ord}_R(f) := \ell_R(R/aR) - \ell_R(R/bR)$$

and call it the order of f.

Then $\mathrm{ord}_R : K^* \to \mathbb{Z}$ is a homomorphism from the multiplicative group K^* to the additive group $\mathbb{Z}$. If R is a one-dimensional regular local ring, then the order of any $f \in R$ coincides with the valuation of f; note that R is then a discrete valuation ring.