Survey of Diophantine Geometry

Springer
Berlin
Heidelberg
New York
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo

Books of Related Interest by Serge Lang

Fundamentals of Diophantine Geometry
A systematic account of fundamentals, including the basic theory of heights, Roth and Siegel's theorems, the Néron-Tate quadratic form, the Mordell-Weil theorem, Weil and Néron functions, and the canonical form on a curve as it related to the Jacobian via the theta function.

Introduction to Complex Hyperbolic Spaces
Since its introduction by Kobayashi, the theory of complex hyperbolic spaces has progressed considerably. This book gives an account of some of the most important results, such as Brody's theorem, hyperbolic imbeddings, curvature properties, and some Nevanlinna theory. It also includes Cartan's proof for the Second Main Theorem, which was elegant and short.

Elliptic Curves: Diophantine Analysis
This systematic account of the basic diophantine theory on elliptic curves starts with the classical Weierstrass parametrization, complemented by the basic theory of Néron functions, and goes on to the formal group, heights and the Mordell-Weil theorem, and bounds for integral points. A second part gives an extensive account of Baker's method in diophantine approximation and diophantine inequalities which were applied to get the bounds for the integral points in the first part.

Other Books by Lang Published by Springer-Verlag

Introduction to Arakelov Theory • Riemann-Roch Algebra (with William Fulton) • Complex Multiplication • Introduction to Modular Forms • Modular Units (with Daniel Kubert) • Introduction to Algebraic and Abelian Functions • Cyclotomic Fields I and II • Elliptic Functions • Algebraic Number Theory • Topics in Cohomology of Groups • $SL_2(R)$ • Abelian Varieties • Differential and Riemannian Manifolds • Complex Analysis • Introduction to Diophantine Approximations • Undergraduate Analysis • Undergraduate Algebra • Linear Algebra • Introduction to Linear Algebra • Calculus of Several Variables • First Course in Calculus • Basic Mathematics • Geometry (with Gene Murrow) • Math! Encounters with High School Students • The Beauty of Doing Mathematics • THE FILE

Serge Lang

Survey of Diophantine Geometry

Springer

Title of the Russian edition:
Itogi nauki i tekhniki, Sovremennye problemy matematiki,
Fundamental'nye napravleniya, Vol. 60, Teoriya Chisel 3
Publisher VINITI, Moscow.

Corrected Second Printing 1997 of the First Edition 1991,
which was originally published as Number Theory III,
Volume 60 of the Encyclopaedia of Mathematical Sciences.

Mathematics Subject Classification (1991):
11Dxx, 11Gxx, 14Dxx, 14Gxx, 14Hxx, 14Kxx

ISBN 3-540-61223-8 Springer-Verlag Berlin Heidelberg New York

Die Deutsche Bibliothek - CIP-Einheitsaufnahme
Lang, Serge: Survey of diophantine geometry / Serge Lang. - Corr. 2. printing. - Berlin; Heidelberg; New York; Barcelona; Budapest; Hong Kong; London; Milan; Paris; Santa Clara; Singapore; Tokyo: Springer, 1997
1. Aufl. u. d. T.: Number theory
ISBN 3-540-61223-8

SPIN: 10535780
41/3143-5 4 3 2 1 0 – Printed on acid-free paper.

Contents

List of Editors and Authors

Editor-in-Chief

R.V. Gamkrelidze, Russian Academy of Sciences, Steklov Mathematical Institute, ul. Vavilova 42, 117966 Moscow, Institute for Scientific Information (VINITI), ul. Usievicha 20 a, 125219 Moscow, Russia; e-mail: gam@ipsun.ras.ru

Consulting Editor and Author

S. Lang, Department of Mathematics, Yale University, New Haven, CT 06520, USA

Preface

In 1988 Shafarevich asked me to write a volume for the Encyclopaedia of Mathematical Sciences on Diophantine Geometry. I said yes, and here is the volume.

By definition, diophantine problems concern the solutions of equations in integers, or rational numbers, or various generalizations, such as finitely generated rings over **Z** or finitely generated fields over **Q**. The word Geometry is tacked on to suggest geometric methods. This means that the present volume is not elementary. For a survey of some basic problems with a much more elementary approach, see [La 90c].

The field of diophantine geometry is now moving quite rapidly. Outstanding conjectures ranging from decades back are being proved. I have tried to give the book some sort of coherence and permanence by emphasizing structural conjectures as much as results, so that one has a clear picture of the field. On the whole, I omit proofs, according to the boundary conditions of the encyclopedia. On some occasions I do give some ideas for the proofs when these are especially important. In any case, a lengthy bibliography refers to papers and books where proofs may be found. I have also followed Shafarevich's suggestion to give examples, and I have especially chosen these examples which show how some classical problems do or do not get solved by contemporary insights. Fermat's last theorem occupies an intermediate position. Although it is not proved, it is not an isolated problem any more. It fits in two main approaches to certain diophantine questions, which will be found in Chapter II from the point of view of diophantine inequalities, and Chapter V from the point of view of modular curves and the Taniyama–Shimura conjecture. Some people might even see a race between the two approaches: which one will prove Fermat first? It is actually conceivable that diophantine inequalities might prove the Taniyama–Shimura conjecture, which would give a high to everybody. There are also two approaches to Mordell's conjecture that a curve of genus $\geqq 2$ over the rationals (or over a number field) has only a finite number of rational points: via l-adic representations in Chapter IV, and via diophantine approximations in Chapter IX. But in this case, Mordell's conjecture is now Faltings' theorem.

Parts of the subject are more accessible than others because they require less knowledge for their understanding. To increase accessibility of some parts, I have reproduced some definitions from basic algebraic geometry. This is especially true of the first chapter, dealing with qualitative questions. If substantially more knowledge was required for some results, then I did not try to reproduce such definitions, but I just used whatever language was necessary. Obviously decisions as to where to stop in the backward tree of definitions depend on personal judgments, influenced by several people who have commented on the manuscript before publication.

The question also arose where to stop in the direction of diophantine approximations. I decided not to include results of the last few years centering around the explicit Hilbert Nullstellensatz, notably by Brownawell, and related bounds for the degrees of polynomials vanishing on certain subsets of group varieties, as developed by those who needed such estimates in the theory of transcendental numbers. My not including these results does not imply that I regard them as less important than some results I have included. It simply means that at the moment, I feel they would fit more appropriately in a volume devoted to diophantine approximations or computational algebraic geometry.

I have included several connections of diophantine geometry with other parts of mathematics, such as PDE and Laplacians, complex analysis, and differential geometry. A grand unification is going on, with multiple connections between these fields.

New Haven Serge Lang
Summer 1990

Acknowledgment

I want to thank the numerous people who have made suggestions and corrections when I circulated the manuscript in draft, especially Chai, Coleman, Colliot-Thélène, Gross, Parshin and Vojta. I also thank Chai and Colliot-Thélène for their help with the proofreading.

S.L.

Notation

Some symbols will be used throughout systematically, and have a more or less universal meaning. I list a few of these.

F^{a} denotes the algebraic closure of a field F. I am trying to replace the older notation $\bar{F}$, since the bar is used for reduction mod a prime, for complex conjugates, and whatnot. Also the notation F^{a} is in line with F^{s} or F^{nr} for the separable closure, or the unramified closure, etc.

$\#$ denotes number of elements, so $\#(S)$ denotes the number of elements of a set S.

$\ll$ is used synonymously with the big Oh notation. If f, g are two real functions with g positive, then $f \ll g$ means that $f(x) = O(g(x))$. Then $f \gg\ll g$ means $f \ll g$ and $g \ll f$.

$A[\varphi]$ means the kernel of a homomorphism φ when A is an abelian group.

$A[m]$ is the kernel of multiplication by an integer m.

Line sheaf is what is sometimes called an invertible sheaf. The French have been using the expression "faisceau en droites" for quite some time, and there is no reason to lag behind in English.

Vector sheaf will, I hope, replace locally free sheaf of finite rank, both because it is shorter, and because the terminology becomes functorial with respect to the ideas. Also I object to using the same expression vector bundle for the bundle *and* for its sheaf of sections. I am fighting an uphill battle on this, but again the French have been using faisceau vectoriel, so why not use the expression in English, functorially with respect to linguistics?

CHAPTER I

Some Qualitative Diophantine Statements

The basic purpose of this chapter is to list systematically fundamental theorems concerning the nature of sets of rational points, as well as conjectures which make the theory more coherent. We use a fairly limited language from algebraic geometry, and hence for the convenience of those readers whose background is foreign to algebraic geometry, I have started with a section reproducing the basic definitions which we shall use.

Most cases treated in this chapter are those when the set of rational points is "as small as possible". One of the purposes is to describe what this means. "Small" may mean finite, it may mean thinly distributed, or if there is a group structure it may mean finitely generated. As much as possible, we try to characterize those situations when the set of rational points is small by algebraic geometric conditions. In Chapter VIII we relate these algebraic conditions to others which arise from one imbedding of the ground field into the complex numbers, and from complex analysis or differential geometry applied to the complex points of the variety after such an imbedding.

We shall also try to describe conjecturally qualitative conditions under which there exist many rational points. These conditions seem to have to do with group structures in various ways. The qualitative statements of this first chapter will be complemented by quantitative statements in the next chapter, both in the form of theorems and of conjectures.

The first section of Chapter II is extremely elementary, and many readers might want to read it first. It shows the sort of fundamental results one wishes to obtain, admitting very simple statements, but for which no known proofs are known today. The elaborate machinery being built up strives partly to prove such results.

I, §1. BASIC GEOMETRIC NOTIONS

For the convenience of the reader we shall give definitions of the simple, basic notions of algebraic geometry which we need for this chapter. A reader acquainted with these notions may skip this part. It just happens that we need very few notions, and so a totally uninformed reader might still benefit if provided with these basic definitions.

Let k be a field. Consider the polynomial ring in n variables $k[z_1, \dots, z_n]$. Let I be an ideal in this ring, generated by a finite number of polynomials $g_1, \dots, g_m$. Assume that $g_1, \dots, g_m$ generate a prime ideal in the ring $k^a[z_1, \dots, z_n]$ over the algebraic closure of k. The set of zeros of I is called an **affine variety** X. The variety defined by the zero ideal is all of affine space $\mathbf{A}^n$. If k' is a field containing k, the set of zeros of I with coordinates $z_1, \dots, z_n \in k'$ is called the set of **rational points of X in** k', and is denoted by $X(k')$. It is equal to the set of solutions of the finite number of equations

$$g_j(z_1, \dots, z_n) = 0 \qquad \text{with} \quad j = 1, \dots, m$$

and $z_i \in k'$ for all $i = 1, \dots, n$.

The condition that the polynomials generate a prime ideal is to insure what is called the irreducibility of the variety. Under our condition, it is not possible to express a variety as the finite union of proper subvarieties.

By pasting together a finite number of affine varieties in a suitable way one obtains the general notion of a variety. To avoid a foundational discussion here, we shall limit ourselves ad hoc to the three types of varieties which we shall consider: affine, projective, and quasi projective, defined below. But for those acquainted with the scheme foundations of algebraic geometry, a **variety** is a scheme over a field k, reduced, integral, separated and of finite type, and such that these properties are preserved under arbitrary extensions of the ground field k.

Let $\mathbf{P}^n$ denote projective n-space. If F is a field, then $\mathbf{P}^n(F)$ denotes the set of points of $\mathbf{P}^n$ over F. Thus $\mathbf{P}^n(F)$ consists of equivalence classes of $(n+1)$-tuples

$$P = (x_0, \dots, x_n) \qquad \text{with} \quad x_j \in F, \text{ not all } x_j = 0,$$

where two such $(n+1)$-tuples $(x_0, \dots, x_n)$ and $(y_0, \dots, y_n)$ are equivalent if and only if there exists $c \in F$, $c \neq 0$ such that

$$(y_0, \dots, y_n) = (cx_0, \dots, cx_n).$$

By a **projective variety** X over a field k we mean the set of solutions in a projective space $\mathbf{P}^n$ of a finite number of equations

$$f_j(T_0, \dots, T_n) = 0 \qquad (j = 1, \dots, m)$$

such that each f_j is a homogeneous polynomial in $n + 1$ variables with coefficients in k, and $f_1, \ldots, f_m$ generate a prime ideal in the polynomial ring $k^a[T_0, \ldots, T_n]$. If k' is a field containing k, by $X(k')$ we mean the set of such zeros having some projective coordinates $(x_0, \ldots, x_n)$ with $x_i \in k'$ for all $i = 0, \ldots, n$. We denote by $k(x)$ (the **residue class field of the point**) the field

$$k(x) = k(x_0, \ldots, x_n)$$

such that at least one of the projective coordinates is equal to 1. It does not matter which such coordinate is selected. If for instance $x_0 \neq 0$, then

$$k(x) = k(x_1/x_0, \ldots, x_n/x_0).$$

We shall give a more intrinsic definition of this field below. We say that $X(k')$ is the set of **rational points of** X **in** k'. The set of points in $X(k^a)$ is called the set of **algebraic points** (over k).

We can define the **Zariski topology on $\mathbf{P}^n$** by prescribing that a **closed set** is a finite union of varieties. A **Zariski open set** is defined to be the complement of a closed set. By a **quasi-projective variety**, we mean the open subset of a projective variety obtained by omitting a closed subset. A closed subset is simply the set of zeros of a finite number of polynomials, or equivalently of some ideal, which need not be a prime ideal. A projective variety is covered by a finite number of affine varieties, as follows.

Let, say, $z_i = T_i/T_0$ $(i = 1, \ldots, n)$ and let

$$g_j(z_1, \ldots, z_n) = f_j(1, z_1, \ldots, z_n).$$

Then the polynomials $g_1, \ldots, g_n$ generate a prime ideal in $k^a[z_1, \ldots, z_n]$, and the set of solutions of the equations

$$g_j(z_1, \ldots, z_n) = 0 \qquad (j = 1, \ldots, m)$$

is an affine variety, which is an open subset of X, denoted by U_0. It consists of those points $(x_0, \ldots, x_n) \in X$ such that $x_0 \neq 0$. Similarly, we could have picked any index instead of 0, say j, and let

$$z_i^{(j)} = T_i/T_j \qquad \text{for} \quad i = 0, \ldots, n \text{ and } i \neq j.$$

Thus the set of points $(x_0, \ldots, x_n)$ such that $x_j \neq 0$ is an affine open subset of X denoted by U_j. The projective variety X is covered by the open sets $U_0, \ldots, U_n$.

By a **subvariety** of a variety X we shall always means a closed subvariety unless otherwise specified. Consider a maximal chain of subvarieties

$$Y_0 \subset Y_1 \subset \cdots \subset Y_r = X,$$

where Y_0 is a point and $Y_i \neq Y_{i+1}$ for all i. Then all such chains have the same number of elements r, and r is called the **dimension** of X. If k is a subfield of the complex numbers, then $X(\mathbf{C})$ is a complex analytic space of complex analytic dimension r. A projective variety of dimension r is sometimes called an r-**fold**.

A **hypersurface** is a subvariety of $\mathbf{P}^n$ of codimension 1, defined by one equation $f(T_0, \ldots, T_n) = 0$. The degree of f is called the **degree** of the hypersurface. If X is a subvariety of $\mathbf{P}^n$ of dimension $n - r$, defined by r equations $f_j = 0$ $(j = 1, \ldots, r)$, then we say that X is a **complete intersection.**

A **curve** is a variety of dimension 1. A **surface** is a variety of dimension 2. In the course of a discussion, one may wish to assume that a curve or a surface is projective, or satisfies additional conditions such as being non-singular (to be defined below), in which case such conditions will be specified.

Let Z be an affine variety in affine space $\mathbf{A}^n$, with coordinates $(z_1, \ldots, z_n)$, and defined over a field k. Let $P = (a_1, \ldots, a_n)$ be a point of Z. Suppose k algebraically closed and $a_i \in k$ for all i. Let

$$g_j = 0 \qquad (j = 1, \ldots, m)$$

be a set of defining equations for Z. We say that the point P is **simple** if the matrix $(D_i g_j(P))$ has rank $n - r$, where r is the dimension of Z. We have used D_i for the partial derivative $\partial/\partial z_i$. We say that Z is **non-singular** if every point on Z is simple. A **projective variety** is called **non-singular** if all the affine open sets $U_0, \ldots, U_n$ above are non-singular. If X is a variety defined over the complex numbers, then X is non-singular if and only the set of complex points $X(\mathbf{C})$ is a complex manifold.

Let X be an affine variety, defined by an ideal I in $k[z_1, \ldots, z_n]$. The ring $R = k[z_1, \ldots, z_n]/I$ is called the **affine coordinate ring** of X, or simply the **affine ring** of X. This ring has no divisors of zero, and its quotient field is called the **function field** of X over k. An element of the function field is called a **rational function** on X. A rational function on X is therefore the quotient of two polynomial functions on X, such that the denominator does not vanish identically on X. The function field is denoted by $k(X)$.

Let X be a projective variety. Then the function fields $k(U_0), \ldots, k(U_n)$ are all equal, and are generated by the restrictions to X of the quotients T_i/T_j (for all i, j such that T_j is not identically 0 on X). The **function field** of X over k is defined to be $k(U_i)$ (for any i), and is denoted by $k(X)$. A rational function can also be expressed as a quotient of two homogeneous polynomial functions $f_1(T_0, \ldots, T_n)/f_2(T_0, \ldots, T_n)$ where f_1, f_2 have the same degree.

Let P be a point of X. We then have the **local ring of regular functions** $\mathcal{O}_P$ at P, which is defined to be the set of all rational functions φ, expressible as a quotient $\varphi = f/g$, where f, g are polynomial functions on X and $g(P) \neq 0$. This local ring has a unique maximal ideal $\mathcal{M}_P$, consisting of quotients as above such that $f(P) = 0$. The residue class field at P is defined to be

$$k(P) = \mathcal{O}_P/\mathcal{M}_P.$$

A variety is said to be **normal** if the local ring of every point is integrally closed. A non-singular variety is normal.

Let X, Y be varieties, defined over a field k. By a **morphism**

$$f: X \to Y$$

defined over k we mean a map which is given locally in the neighborhood of each point by polynomial functions. An **isomorphism** is a morphism which has an inverse, i.e. a morphism $g: Y \to X$ such that

$$f \circ g = \mathrm{id}_X \quad \text{and} \quad g \circ f = \mathrm{id}_Y.$$

We say that f is an **imbedding** if f induces an isomorphism of X with a subvariety of Y.

A **rational map** $f: X \to Y$ is a morphism on a non-empty Zariski open subset U of X. If V is a Zariski open subset of X, and $g: V \to Y$ is a morphism which is equal to f on $U \cap V$, then g is uniquely determined. Thus we think of a rational map as being extended to a morphism on a maximal Zariski open subset of X. A **birational map** is a rational map which has a rational inverse. If f is a birational map, then f induces an isomorphism of the function fields. Two varieties X, Y are said to be **birationally equivalent** if there exists a birational map between them. If needed, we specify the field over which rational maps or birational maps are defined. For instance, there may be a variety over a field k which is isomorphic or birationally equivalent to projective space $\mathbf{P}^m$ over an extension of k, but not over k itself. Example: the curve defined by the equation in $\mathbf{P}^2$

$$x_0^2 + x_1^2 + x_2^2 = 0.$$

Let $f: X \to Y$ be a rational map, defined over the field k. We say that f is **generically surjective** if the image of a non-empty Zariski open subset of X under f contains a Zariski open subset of Y. In this case, f induces an injection of function fields

$$k(Y) \hookrightarrow k(X).$$

A variety is said to be **rational** (resp. **unirational**) if it is birationally equivalent to (resp. a rational image of) projective space.

Next we describe divisors on a variety. There are two kinds.

A **Weil divisor** is an element of the free abelian group generated by the subvarieties of codimension 1. A Weil divisor can therefore be written as a linear combination

$$D = \sum n_i D_i$$

where D_i is a subvariety of codimension 1, and $n_i \in \mathbf{Z}$. If all $n_i \geqq 0$ then D is called **effective**.

A **Cartier divisor** is defined as follows. We consider pairs (U, φ) consisting of a Zariski open set U and a rational function φ on X. We say that two such pairs are equivalent, and write $(U, \varphi) \sim (V, \psi)$ if the rational function $\varphi\psi^{-1}$ is a unit in the local ring $\mathcal{O}_P$ for every $P \in U \cap V$. In other words, both $\varphi\psi^{-1}$ and $\varphi^{-1}\psi$ are regular functions at all points of $U \cap V$. A maximal family of equivalent pairs whose open sets cover X is defined to be a **Cartier divisor**. A pair (U, φ) is said to **represent the divisor locally**, or on the open set U. The Cartier divisor is said to be **effective** if for all representing pairs (U, φ) the rational function φ is regular at all points of U. We then view the Cartier divisor as a hypersurface on X, defined locally on U by the equation $\varphi = 0$. The Cartier divisors form a group. Indeed, if Cartier divisors are represented locally by (U, φ) and (U, φ') respectively, then their sum is represented by $(U, \varphi\varphi')$.

It is a basic fact that if X is non-singular then the groups of Weil divisors and Cartier divisors are isomorphic in a natural way.

Let φ be a non-zero rational function. Then φ defines a Cartier divisor denoted by (φ), represented by the pairs (U, φ) for all open sets U. Such Cartier divisors are said to be **rationally** or **linearly equivalent** to 0. The factor group of all Cartier divisors modulo the group of divisors of functions is called the **Cartier divisor class group** or the **Picard group** $\mathrm{Pic}(X)$. (See [Ha 77], Chapter II, Proposition 6.15.)

One can also define the notion of linearly equivalent to 0 for Weil divisors. Let W be a subvariety of X of codimension 1. Let $\mathcal{O}_W$ be the local ring of rational functions on X which are defined at W. If f is a rational function on X which lies in $\mathcal{O}_W$, $f \neq 0$, then we define the **order** of f at W to be

$$\mathrm{ord}_W(f) = \text{length of the } \mathcal{O}_W\text{-module } \mathcal{O}_W/f\mathcal{O}_W.$$

The order function extends to a homomorphism of the group of non-zero rational functions on X into $\mathbf{Z}$. To each rational function we can associate its **divisor**

$$(f) = \sum \mathrm{ord}_W(f)(W).$$

The subgroup of the Weil divisor group consisting of the divisors of rational functions defines the group of divisors **rationally equivalent** to 0, and the factor group is called the **Chow group** $\mathrm{CH}^1(X)$.

It is a pain to have to deal with both groups. When dealing with the Chow group, we shall usually assume that the variety is complete and non-singular in codimension 1. For simplicity, we shall now state some properties of divisor classes for the Cartier divisor class group. Analogous properties also apply to the Chow group. One reason why the Chow group is important for its own sake is that one can form similar groups with subvarieties of higher codimension, and these are interesting for their own sake. See Fulton's book *Intersection Theory.*

There is a natural homomorphism from Cartier divisors to Weil divisors, inducing a homomorphism

$$\mathrm{Pic}(X) \to \mathrm{CH}^1(X),$$

which is injective if X is normal, and an isomorphism if the variety X is non-singular.

Divisors also satisfy certain positivity properties. We have already defined effective divisors. A **divisor class** c is called **effective** if it contains an effective divisor. But there is a stronger property which is relevant. A **divisor** D on X is called **very ample** if there exists a projective imbedding

$$f\colon X \to \mathbf{P}^m$$

such that D is linearly equivalent to $f^{-1}(H)$ for some hyperplane H of $\mathbf{P}^m$. A **divisor class** c is called **very ample** if it contains a very ample divisor. We call a divisor D **ample** if there exists a positive integer q such that qD is very ample, and similarly for the definition of an ample divisor class. Equivalently, a divisor class c is ample if and only if there exists a positive integer q such that qc is very ample. We have a basic property:

Proposition 1.1. *Let X be a projective variety. Given a divisor D and an ample divisor E, there exists a positive integer n such that $D + nE$ is ample, or even very ample. In particular, every divisor D is linearly equivalent*

$$D \sim E_1 - E_2$$

where E_1, E_2 are very ample.

We view ampleness as a property of "positivity". We shall see in Chapter VIII that this property has an equivalent formulation in terms of differential geometry, and in Chapter II we shall see how it gives rise to positivity properties of heights.

By the **support** of a Cartier divisor D we mean the set of points P

such that if D is represented by (U, φ) in a neighborhood of P, then φ is not a unit in the local ring $\mathcal{O}_P$. The support of D is denoted by $\mathrm{supp}(D)$.

A morphism $f: X \to Y$ induces an inverse mapping

$$f^*: \mathrm{Pic}(Y) \to \mathrm{Pic}(X).$$

Indeed, let D be a Cartier divisor on Y, and suppose $f(X)$ is not contained in the support of D. Suppose D is represented by (V, ψ). Then $(f^{-1}(V), \psi \circ f)$ represents the inverse image $f^{-1}D$, which is a Cartier divisor on X. This inverse image defines the inverse image of the divisor class, and thus defines our mapping f^*.

Example. Let $X = \mathbf{P}^n$ be projective space, and let $T_0, \ldots, T_n$ be the projective variables. The equation $T_0 = 0$ defines a hyperplane in $\mathbf{P}^n$, and the complement of this hyperplane is the affine open set which we denoted by U_0. On U_i with $i \neq 0$, the hyperplane is represented by the rational function T_0/T_i. Instead of the index 0, we could have selected any other index, of course. More generally, let $a_0, \ldots, a_n$ be elements of k not all 0. The equation

$$f(T) = a_0 T_0 + \cdots + a_n T_n = 0$$

defines a hyperplane. On U_i, this hyperplane is represented by the rational function

$$\frac{f(T)}{T_i} = a_0(T_0/T_i) + \cdots + a_n(T_n/T_i).$$

Let X be a projective non-singular variety defined over an algebraically closed field k. Let D be a divisor on X. We let

$H^0(X, D) = k$-vector space of rational functions $\varphi \in k(X)$ such that

$$(\varphi) \geqq -D.$$

In other words, $(\varphi) = E - D$ where E is an effective divisor. Let $\{\varphi_0, \ldots, \varphi_N\}$ be a basis of $H^0(X, D)$. If $P \in X(k)$ is a point such that $\varphi_j \in \mathcal{O}_P$ for all j, and for some j we have $\varphi_j(P) \neq 0$ then

$$(\varphi_0(P), \ldots, \varphi_N(P))$$

is viewed as a point in projective space $\mathbf{P}^N(k)$, and we view the association

$$f: P \mapsto (\varphi_0(P), \ldots, \varphi_N(P))$$

as a map, which is defined on a non-empty Zariski open subset U of X.

Thus we obtain a morphism

$$f\colon U \to \mathbf{P}^N.$$

Similarly, for each positive multiple mD of D, using a basis for $H^0(X, mD)$, we obtain a morphism

$$f_m\colon \text{a non-empty Zariski open subset of } X \to \mathbf{P}^{N(m)}.$$

If there exists some positive integer m such that f_m is an imbedding of some non-empty Zariski open subset of X into a locally closed subset of $\mathbf{P}^{N(m)}$, then we say that D is **pseudo ample**. More generally, a divisor D_1 is defined to be **pseudo ample** if and only if D_1 is linear equivalent to a divisor D which is pseudo ample in the above sense. Thus the property of being pseudo ample is a property of divisor classes. It is a result of Kodaira (appendix to [KoO 71]) that:

On a non-singular projective variety, a divisor D is pseudo ample if and only if there exists some positive integer m such that

$$mD \sim E + Z$$

where E is ample and Z is effective.

I, §2. THE CANONICAL CLASS AND THE GENUS

We shall discuss a divisor class which plays a particularly important role. We first deal with varieties of dimension 1, and then we deal with the general case.

Curves

We define a **curve** to be a projective variety of dimension 1. Let X be a non-singular curve over k. Then divisors can be viewed as Weil divisors, and a subvariety of codimension 1 is a point. Hence a divisor D can be expressed as a linear combination of points

$$D = \sum_{i=1}^{r} m_i(P_i) \qquad \text{with} \quad m_i \in \mathbf{Z}, \quad \text{and} \quad P_i \in X(k^{\mathrm{a}}).$$

We define the **degree** of the divisor D to be

$$\deg D = \sum m_i.$$

Suppose for simplicity that k is algebraically closed. Let $y \in k(X)$ be a rational function, and $y \neq 0$. Let $P \in X(k)$. Let $\mathcal{O}_P$ be the local ring with maximal ideal P. Then $\mathcal{M}_P$ is a principal ideal, generated by one element t, which is called a **local parameter** at P. Every element $y \neq 0$ of $k(X)$ has an expression

$$y = t^r u \qquad \text{where } u \text{ is a unit in } \mathcal{O}_P.$$

We define $\operatorname{ord}_P(y) = r$. The function $y \mapsto v_p(y) = \operatorname{ord}_P(y)$ defines an absolute value on $k(X)$. The completion of $\mathcal{O}_P$ can be identified with the power series ring $k[[t]]$. Let $F = k(X)$. We may view F as a subfield of the quotient field of $k[[t]]$, denoted by $k((t))$. In this quotient field, y has a power series expansion

$$y = a_r t^r + \text{higher terms}, \qquad \text{with} \quad a_r \in k, \quad a_r \neq 0.$$

To each rational function y as above we can associate a Weil divisor

$$(y) = \sum_P \operatorname{ord}_P(y)(P).$$

It is a fact that

$$\deg(y) = 0.$$

Hence the degree is actually a function on divisor classes, i.e. on $\mathrm{CH}^1(X)$.

Let $x,\ y \in k(X)$. A differential form $y\,dx$ will be called a **rational differential form**. Let P be a point in $X(k)$. In terms of a local parameter t, we write

$$y\,dx = y(t)\frac{dx}{dt}\,dt,$$

where y, x are expressible as power series in t. Then we define

$$\operatorname{ord}_P(y\,dx) = \text{order of the power series } y(t)\frac{dx}{dt}.$$

We can associate a divisor to the differential form $y\,dx$ by letting

$$(y\,dx) = \sum_P \operatorname{ord}_P(y\,dx)(P).$$

Since every rational differential form is of type $uy\,dx$ for some rational function u, it follows that the degrees of non-zero differential forms are all equal. One possible definition of the **genus** of X is by the formula

$$\deg(y\,dx) = 2g - 2.$$

Furthermore, the divisors of rational differential forms constitute a class in $\mathrm{CH}^1(X)$, called the **canonical class**. Thus we may say that:

The degree of the canonical class is $2g - 2$.

A differential form ω is said to be of the **first kind** if $\mathrm{ord}_P(\omega) \geqq 0$ for all P. The differential forms of first kind form a vector space over k, denoted by $\Omega^1(X)$. The following property also characterizes the genus.

The dimension of $\Omega^1(X)$ *is equal to* g.

The genus can also be characterized topologically over the complex numbers. Suppose $k = \mathbf{C}$. Then $X(\mathbf{C})$ is a compact complex manifold of dimension 1, also called a compact Riemann surface. The genus g is equal to the number of holes in the surface. It also satisfies the formula

$$2g = \mathrm{rank}\, H_1(X(\mathbf{C}), \mathbf{Z}),$$

where $H_1(X(\mathbf{C}), \mathbf{Z})$ is the first topological homology group, which is a free abelian group over $\mathbf{Z}$.

Finally, we want to be able to compute the genus when the curve is given by an equation. We shall give the value only in the non-singular case. Let the curve X be defined by the homogeneous polynomial equation

$$f(T_0, T_1, T_2) = 0,$$

of degree n in the projective plane $\mathbf{P}^2$, over the algebraically closed field k. Suppose that X is non-singular. Then

$$\boxed{\text{genus of } X = \frac{(n-1)(n-2)}{2}.}$$

For instance, the Fermat curve

$$X_0^n + X_1^n + X_2^n = 0$$

over a field of characteristic p *with* $p \nmid n$ has genus $(n-1)(n-2)/2$. This genus is $\geqq 2$ when $n \geqq 4$.

In general, on a non-singular curve X, *a divisor class* c *is ample if and only if*

$$\deg(c) > 0.$$

Therefore, the canonical class is ample if and only if $g \geqq 2$.

For $g = 1$, the canonical class is 0. For $g = 0$, the canonical class has degree -2.

Examples. Let X be a projective non-singular curve of genus 0 over a field k, not necessarily algebraically closed. Then X is isomorphic to $\mathbf{P}^1$ over k if and only if X has a rational point in k.

Let X be a projective non-singular curve of genus 1 over a field k of characteristic $\neq 2$ or 3. Then X has a rational point in k if and only if X is isomorphic to a curve defined by an equation

$$y^2 = 4x^3 - g_2 x - g_3 \qquad \text{with} \quad g_2, g_3 \in k, \quad g_2^3 - 27g_3^2 \neq 0.$$

A curve of genus 1 with a rational point is called an **elliptic curve over** k.

We now have defined enough notions to pass to diophantine applications. We shall deal with the following kinds of fields:

A **number field**, which by definition is a finite extension of $\mathbf{Q}$.

A **function field**, which is defined as the function field of a variety, over a field k. Such fields can be characterized as follows. An extension F of k is a function field over k if and only if F is finitely generated over k; every element of F algebraic over k lies in k; and there exist algebraically independent elements $t_1, \ldots, t_r$ in F over k such that F is a finite separable extension of $k(t_1, \ldots, t_r)$. Under these circumstances, we call k the **constant field**.

If F is a finitely generated field over the prime field, then F is a function field, whose constant field k is the set of elements in F which are algebraic over the prime field.

Let X_0 be a variety defined over k. Suppose F is the function field of a variety W over k. Then there is a natural bijection directly from the definitions between the set of rational points $X_0(F)$ and the rational maps $W \to X_0$ defined over k. We refer to this situation as the **split case** of a variety over F.

Mordell's conjecture made in 1922 [Mord 22] became **Faltings' theorem** in 1983 [Fa 83].

Theorem 2.1. *Let X be a curve defined over a number field F. Suppose X has genus $\geqq 2$. Then X has only a finite number of rational points in F, that is, $X(F)$ is finite.*

Using specialization techniques dating back to the earlier days of diophantine geometry, one then obtains the following corollary.

Corollary 2.2. *Let X be a curve defined over a field F finitely generated over the rational numbers. Then $X(F)$ is finite.*

Aside from this formulation in what we may call the **absolute case**, there is a **relative** formulation, in what is usually called the **function field case**.

In [La 60a] I conjectured the following analogue of Mordell's conjecture for a curve (assumed non-singular).

Theorem 2.3. *Let X be a curve defined over the function field F over k of characteristic 0, and of genus $\geqq 2$. Suppose that X has infinitely many rational points in $X(F)$. Then there exists a curve X_0 defined over k, such that X_0 is isomorphic to X over F, and all but a finite number of points in $X(F)$ are images under this isomorphism of points in $X_0(k)$.*

This formulation was proved by Manin [Man 63]. We shall describe certain features of Manin's proof, as well as several other proofs given since, in Chapter VI.

Note as in [La 60a] that the essential difficulty occurs when F has transcendence degree 1 over k, that is, when F is a finite extension of a rational field $k(t)$ with a variable t. Elementary reduction steps reduce the theorem to this case. Indeed, there exists a tower

$$k = F_0 \subset F_1 \subset \cdots \subset F_r = F$$

such that each F_i is a function field over F_{i-1}, of dimension 1. One can then apply induction to the case of dimension 1 to handle the general case.

Remark. If k is a finite field with q elements and X_0 is defined over k, and X_0 has a point in an extension F of k, then iterations of Frobenius on this point yield other points, so exceptional cases have to be excluded in characteristic p. See Chapter 6, §5.

The case of Theorem 2.3 when X is isomorphic to some curve X_0 over k is the split case in which the conclusion may be reformulated in the following geometric form. For a proof see [La 60a], p. 29, and [La 83a], p. 223.

Theorem of de Franchis. *Let X_0 be a curve in characteristic 0, of genus $\geqq 2$. Let W be an arbitrary variety. Then there is only a finite number of generically surjective rational maps of W onto X_0.*

Higher dimensions

Let X be a projective non-singular variety of dimension n, defined over an algebraically closed field k.

Let W be a subvariety of codimension 1. In particular, W is a divisor on X. Let $P \in X(k)$, and let $\mathcal{O}_P$ be the local ring of P on X, with maximal ideal $\mathcal{M}_P$. Then the hypothesis that X is non-singular implies that $\mathcal{O}_P$ is a unique factorization ring. There exists an element $\varphi \in \mathcal{O}_P$, well defined up to multiplication by a unit in $\mathcal{O}_P$, such that W is defined in a Zariski open neighborhood U of P by the equation $\varphi = 0$. If W does not pass through P, then φ is a unit, and $U \cap W$ is empty. If W passes through P, then φ is an irreducible (or prime) element in $\mathcal{O}_P$. The collection of pairs (U, φ) as above define the **Cartier divisor associated with** W.

Let $y, x_1, \ldots, x_n$ be rational functions on X, so in $k(X)$. A form of type $y\, dx_1 \wedge \cdots \wedge dx_n$ is called a **rational differential form** of top degree on X. Let ω be such a form. Let $t_1, \ldots, t_n$ be **local parameters** at P (that is, generators for the maximal ideal in the local ring at P). In a neighborhood U of P we may write

$$\omega = \psi\, dt_1 \wedge \cdots \wedge dt_n$$

for some rational function ψ. The collection of pairs (U, ψ) defines a Cartier divisor, which is called the **divisor associated with** ω, and is denoted by (ω). All such divisors are in the same linear equivalence class, and again this class is called the canonical class of X. A canonical divisor is sometimes denoted by K, as well as its class, or by K_X if we wish to emphasize the dependence on X.

A differential form of top degree is called **regular at** P if its divisor is represented in a neighborhood of P by a pair (U, ψ) where $\psi \in \mathcal{O}_P$. The differential form is called **regular** if it is regular at every point, or in other words, if its associated divisor is effective. The regular differential forms of top degree form a vector space over k, whose dimension is called the **geometric genus**, and is classically denoted by p_g.

Examples. The canonical class of $\mathbf{P}^m$ itself is given by

$$K_{\mathbf{P}^m} \sim -(m+1)H \text{ for any hyperplane } H \text{ on } \mathbf{P}^m.$$

In particular, for $m = 1$, any two points on $\mathbf{P}^1$ are linearly equivalent, and for any point P on $\mathbf{P}^1$ the canonical class on $\mathbf{P}^1$ is given by

$$K_{\mathbf{P}^1} \sim -2(P).$$

Suppose that X is a non-singular hypersurface in projective space $\mathbf{P}^m$, defined by the equation

$$f(T_0, \ldots, T_m) = 0$$

where f is a homogeneous polynomial of degree d. Let H_X be the restriction to X of a hyperplane which does not vanish identically on X. Then the canonical class on X is given by

$$K_X \sim (d - (m+1))H_X.$$

Thus the canonical class is ample if and only if $d \geqq m + 2$.

The class $-K_X$ is called the **co-canonical** or **anti-canonical class.**

A non-singular projective variety is defined to be:

canonical if the canonical class K_X is ample
very canonical if K_X is very ample
pseudo canonical if K_X is pseudo ample
anti-canonical if $-K_X$ is ample
and so on.

Instead of pseudo canonical, a variety has been called of **general type**, but *with the support of Griffiths*, I am trying to make the terminology functorial with respect to the ideas. (I know I am fighting an uphill battle on this.)

Finally, suppose that X is a projective variety, but possibly singular. We say that X is **pseudo canonical** if X is birationally equivalent to a projective non-singular pseudo canonical variety. In characteristic 0, **resolution of singularities** is known, and due to Hironaka. This means that given X a projective variety, there exists a birational morphism

$$f: X' \to X$$

such that X' is projective and non-singular and f is an isomorphism over the Zariski open subset subset of X consisting of the simple points.

It is an elementary fact of algebraic geometry that if $f: X \to Y$ is a birational map between non-singular projective varieties, then for every positive integer n, $f^*: H^0(Y, nK_Y) \to H^0(X, nK_X)$ is an isomorphism. In particular, K_Y is pseudo ample if and only if K_X is pseudo ample. In analogy with the case of curves, one defines the **geometric genus**

$$p_g(X) = \dim H^0(X, K_X).$$

It is a basic problem of algebraic geometry to determine under which conditions the canonical class is ample, or pseudo ample. We shall relate these conditions with diophantine conditions in the next section.

I, §3. THE SPECIAL SET

For simplicity let us now assume that our fields have characteristic 0.

I shall give a list of conjectures stemming from [La 74] and [La 86]. Let X be a variety defined over an algebraically closed field of characteristic 0. Then X can also be defined over a finitely generated field F_0 over the rational numbers. We say that X is **Mordellic** if $X(F)$ is finite for every finitely generated field F over $\mathbf{Q}$, containing F_0. We ask under what conditions can there be infinitely many rational points of X in some such field F? One can a priori describe such a situation. First, if there is a rational curve in X, i.e. a curve birationally equivalent to $\mathbf{P}^1$, then all the rational points of this curve give rise to rational points on X. Note that we are dealing here with curves (and later subvarieties) defined over some finitely generated extension, i.e. we are dealing with the "geometric" situation. A more general example is given by a **group variety**, that is a variety which is a group such that the composition law and the inverse map are morphisms. If G is a group variety, then from two random rational points in some field F we can construct lots of other points by using the law of composition. Roughly speaking, the conjecture is that these are the only examples. Let us make this conjecture more precise.

Let X be a projective variety. Let us define the **algebraic special set** $\mathrm{Sp}(X)$ to be the Zariski closure of the union of all images of non-constant rational maps $f: G \to X$ of group varieties into X. This special set may be empty, it may be part of X, or it may be the whole of X. Note that the maps f may be defined over finitely generated extensions, i.e. the special set is defined geometrically. I conjectured:

3.1. *The complement of the special set is Mordellic.*

3.2. *A projective variety is Mordellic if and only if the special set is empty, i.e. if and only if every rational map of a group variety into X is constant.*

Note that the affine line $\mathbf{A}^1$, or the multiplicative group $\mathbf{G}_m$, are birationally equivalent to $\mathbf{P}^1$, so the presence of rational curves in X can be viewed from the point of view that these lines are rational images of group varieties. A group variety which is projective is called an **abelian variety**. We shall study their diophantine properties more closely later. Other examples of group varieties are given by linear group varieties, i.e. subgroups of the general linear group which are Zariski closed subsets. A general structure theorem due to Chevalley states that the only group varieties are group extensions of an abelian variety by a linear group; and the function field of a linear group is unirational but rational over an algebraically closed field. Hence:

3.3. *The special set* $\mathrm{Sp}(X)$ *is the Zariski closure of the union of all images of non-constant rational maps of* $\mathbf{P}^1$ *and abelian varieties into X.*

Since $\mathbf{P}^1$ itself is a rational image of an abelian variety of dimension 1, we may also state:

3.4. *The special set* $\mathrm{Sp}(X)$ *is the Zariski closure of the union of the images of all non-constant rational maps of abelian varieties into X.*

We define a projective variety to be **algebraically hyperbolic** if and only if the special set is empty. We make this definition to fit conjecturally with the theory of hyperbolicity over the complex numbers. See Chapter V. Examples of hyperbolic projective varieties will be given in Chapter V. Analytic hyperbolicity implies algebraic hyperbolicity, so these examples are also examples of algebraically hyperbolic varieties, and hence conjecturally of Mordellic varieties.

We define a projective variety to be **special** if $\mathrm{Sp}(X) = X$, that is, if the special set is the whole variety. A variety which is not special can be called **general**. This fits older terminology (**general type**) in light of Conjecture 3.5 below.

There are the two extreme cases: when the special set is empty, i.e. the variety is algebraically hyperbolic, and when the special set is the whole variety, i.e. the variety is special. One wants a classification of both types of varieties, which amounts to problems principally in algebraic geometry, although already a diophantine flavor intervenes because one is led to consider generic fiber spaces, where there may not exist a rational section. We shall mention below some specific examples.

One basic conjecture states:

3.5. *The special set* $\mathrm{Sp}(X)$ *is a proper subset if and only if* X *is pseudo canonical.*

As a result, one gets the conjecture:

3.6. *The following conditions are equivalent for a projective variety* X:
X is algebraically hyperbolic, i.e. the special set is empty.
X is Mordellic.
Every subvariety of X is pseudo canonical.

In light of this conjecture, there are no other examples of Mordellic projective varieties besides hyperbolic ones.

In this context, it is natural to define a variety X to be **pseudo Mordellic** if there exists a proper Zariski closed subset Y of X such that $X - Y$ is Mordellic. Then I conjectured:

3.7. *A projective variety X is pseudo Mordellic if and only if X is pseudo canonical. The Zariski closed subset Y can be taken to be the special set* $\mathrm{Sp}(X)$.

As a consequence of the conjecture, we note that for any finitely generated field F over $\mathbf{Q}$, if X is pseudo Mordellic, then $X(F)$ is not Zariski dense in X. The converse is not true, however. For instance, let C be a curve of genus $\geqq 2$ and let

$$X = C \times \mathbf{P}^1.$$

We have $X = \mathrm{Sp}(X)$, and X is fibered by projective lines. By Faltings' theorem, for every finitely generated field F over $\mathbf{Q}$ the set $X(F)$ is not Zariski dense in X, but X is not pseudo canonical. However, conjecturally:

3.8. *If the special set is empty, then the canonical class is ample.*

The above discussion and conjectures give criteria for the special set to be empty or unequal to the whole projective variety. In the opposite direction, one is interested in those cases when X is special. This leads at first into problems of pure algebraic geometry, independently of diophantine applications, concerning the structure of the special set. Notably, we have the following problems.

Sp 1. If we omit taking the Zariski closure, do we still get the same set?

Sp 2. Are the irreducible components of the special set **generically fibered** by rational images of group varieties?

By this we mean the following. Let X be a special projective variety. The condition **Sp 2** means that there exists a generically surjective rational map $f: X \to Y$ such that the inverse image $f^{-1}(y)$ of a generic point of Y is a subvariety W_y for which there exist a group variety G and a generically surjective rational map $g: G \to W_y$ defined over some finite extension of the field $k(y)$. To get "fibrations" (in the strict sense, with disjoint fibers), one must of course allow for blow ups and the like, to turn rational maps into morphisms.

One can also formulate an alternative for the second question, namely:

Sp 3. Suppose $X = \text{Sp}(X)$ is special. Is there a generically finite rational map from a variety X' onto X such that X' is generically fibered by a rational image of a group variety?

It would still follow under this property that it is not necessary to take the Zariski closure in defining the special set. As a refinement of **Sp 3**, one can also ask for those conditions under which X' would be generically fibered by a group variety rather than a rational image.

Note that we are dealing here with rational fibrations, so only up to birational equivalence. In connection with **Sp 2**, suppose $f: X \to Y$ is a rational map whose generic fiber is a rational image of a group variety. Then one asks the general question:

Sp 4. When is there a rational section of f, so that the generic fiber has a rational point over the function field $k(y)$? If there is no rational section, over a number field k, how many fibers have one or more rational points?

We shall discuss several examples below and in Chapter X, §2.

As refinements of **Sp 2** and **Sp 3**, I would raise the possibility of finding "good" models, possibly not complete, for the complete X, whose fibers may be homogeneous spaces for linear groups, i.e. without generic sections. As we shall see later, such models can be found for abelian varieties (Néron models), and the question is to what extent there exists an analogous theory for non-complete special group varieties.

The question arises when the canonical class is 0 whether there exists a generic fibration as in **Sp 2** and **Sp 3** by rational images of abelian varieties, or abelian varieties themselves. Interesting cases when the canonical class K_X is not pseudo ample arise not only when $K_X = 0$ but also when $-K_X$ contains an effective divisor, or is pseudo ample, or ample. In these cases, Conjecture 3.5 implies that X is special. As $-K_X$ is assumed more and more ample, I would expect that there are more and more rational curves on the variety, where ultimately the special set is covered by rational curves and no abelian varieties are needed. The existence of rational curves has long been a subject of interest to algebraic geometers, and has received significant impetus through the work of Mori [Mori 82]. Such algebraic geometers work over an algebraically closed field, and there is of course the diophantine question whether rational curves are defined over a given field of definition for the variety or hypersurface. But still working geometrically we have the following theorem of [Mori 82], see also [ClKM 88], §1, Theorem 1.8.

Theorem 3.9a. *Let X be a projective non-singular variety and assume that $-K_X$ is ample. Then through every point of X there passes a rational curve in X.*

In particular, under the hypothesis of Theorem 3.9, X is special, but we note that only rational images of $\mathbf{P}^1$ are needed to fill out the special set. More generally I conjectured:

Theorem 3.9b. *Let X be a projective non-singular variety and assume that $-K_X$ is pseudo ample. Then X is special, and is equal to the union of rational curves in X.*

I asked Todorov if Mori's theorem would still be valid under the weaker hypothesis that the anti-canonical class is pseudo ample, and he told me that Mori's proof shows that in this case, there exists a rational curve passing through every point except possibly where the rational map defined by a large multiple of $-K_X$ is not an imbedding, which implies Theorem 3.9b as a corollary. These considerations fit well with those of Chapter X. In addition, **3.9a** and **3.9b** raise the question whether a generically finite covering of X is generically fibered by unirational varieties. Here the role of non-complete linear groups is not entirely clear. They intervene in the context of Chapter X, besides intervening in the Néron models of abelian varieties which will be defined later. In both cases, they reflect the existence of degenerate fibers. This suggests the existence of a theory of non-complete special models of special varieties which remains to be elaborated. In particular, the following questions also arise:

3.10. Suppose that $-K_X$ is pseudo ample. (a) Is **Sp 3** then necessarily satisfied with a linear group variety? (b) Suppose that X is defined over a field k and has a k-rational point. When is X unirational (resp. rational) over k?

In this direction, there is a condition which is much stronger than having $-K_X$ ample. Indeed one can define the notion of **ampleness** for a vector sheaf $\mathscr{E}$ as follows. Let $\mathbf{P}\mathscr{E}$ be the associated projective variety and let $\mathscr{L}$ be the corresponding line sheaf of hyperplanes. One possible characterization of $\mathscr{E}$ being **ample** is that $\mathscr{L}$ is ample. One of Mori's theorems proved a conjecture of Hartshorne:

Theorem 3.11. *Let X be a non-singular projective variety and assume that its tangent sheaf is ample. Then X is isomorphic to projective space.*

This result is valid over the algebraic closure of a field of definition of X. Over a given field of definition, a variety may not have any rational point, or may be only unirational. We shall discuss other examples in Chapter X.

There is another notion which has currently been used by algebraic geometers to describe when a variety is generically fibered by rational curves. Indeed, a variety X of dimension r over an algebraically closed field k is said to be **uniruled** if there exists an $(r-1)$-dimensional variety W over k and a generically surjective rational map $f: \mathbf{P}^1 \times W \to X$. For important results when threefolds are uniruled, having to do with negativity properties of the canonical class, in addition to Mori's paper already cited see Miyaoka–Mori [MiyM 86] and Miyaoka [Miy 88], Postscript Theorem, p. 332, which yield the following result among others.

Theorem 3.12. *Let X be a non-singular projective threefold (characteristic* 0). *The following three conditions are equivalent.* (a) *Through every point of X there passes a rational curve in X.* (b) *X is uniruled.* (c) *We have $H^0(X, mK_X) = 0$ for all $m > 0$.*

Note that $-K_X$ pseudo ample implies $H^0(X, mK_X) = 0$ for all $m > 0$, by the Kodaira criterion for pseudo ampleness. For further results see also Batyrev [Bat 90], and for a general exposition of Mori's program, see Kollár [Koll 89].

Extending the classical terminology of uniruled, I propose to define a variety X to be **unigrouped** if there exists a variety X' as in condition **Sp 3**. We shall now consider several significant examples illustrating the **Sp** conditions, among other things.

Example 1 (Subvarieties of abelian varieties). In this case the structure of the special set is known, and the answers to **Sp 1** and **Sp 2** are yes in both cases. This example will be discussed at length in §6. See also Chapter VIII, §1.

Example 2. Let X be a projective non-singular surface. One says that X is a **K3 surface** if $K_X = 0$ and if every rational map of X into an abelian variety is constant. If A is an abelian variety of dimension 2 and Z is the quotient of A by the group $\{\pm 1\}$, then a minimal desingularization of Z is a K3 surface, called a **Kummer surface**. If X is a K3 surface, then by a result of Green–Griffiths [GrG 80] and Bogomolov–Mumford completed by Mori–Mukai [MoM 83], Appendix, a generically finite covering X' of X has a generic fibration by curves of genus 1, so that X is unigrouped, and in particular X is special. Sometimes there exists a rational section and sometimes not. When such a section does not exist, over number fields, the problem arises how many fibers have rational points, or a point of infinite order on the fibral elliptic curve. We shall see an example with the Fermat surface below, and similar questions arise in the higher dimensional case of Fermat hypersurfaces, or in the case of the Châtelet surface of Chapter X, §2.

The next two cases deal with generic hypersurfaces.

Example 3. Let X be the **generic hypersurface** of degree d in $\mathbf{P}^n$, and suppose $d \geqq n + 2$, so that the canonical class is ample. By **generic** we mean that the polynomial defining X has algebraically independent coefficients over $\mathbf{Q}$. Then conjecturally the special set is empty.

The analogous conjecture goes for the generic complete intersection. These are algebraic formulations of a conjecture of Kobayashi in the complex analytic case. See Example 1.5 of Chapter VIII. Note that in light of Conjecture 3.6 these generic complete intersections would be Mordellic.

Example 4. Let X be the generic hypersurface of degree 5 in $\mathbf{P}^4$. One says that X is the **generic quintic threefold** in $\mathbf{P}^4$. Then $K_X = 0$. Following a construction of Griffiths, Clemens ([Cl 83], [Cl 84]) proved the existence of infinitely many rational curves which are Zariski dense, homologically equivalent, but which are linearly independent modulo algebraic equivalence. Hence in this case we have $\mathrm{Sp}(X) = X$, in other words X is special. It is then a problem to determine whether X satisfies conditions **Sp 2** or **Sp 3** above, especially whether a generically finite covering of X is generically fibered by elliptic curves, or K3 surfaces, or by rational images of abelian surfaces, if not by abelian surfaces themselves. In such a case, the Clemens curves might then be interpreted as sections over rational curves, thus explaining their independence in more geometric terms. The existence of such fibrations in the case of subvarieties of abelian varieties can be taken as an indication that a positive answer may exist in general, but the evidence at the moment is still too scarce to convince everyone that the answer will always be positive. For more on the quintic threefold, see [ClKM 88], §22 and Remark 5.5.

The above examples conjecturally illustrate some general principles on some generic hypersurfaces. Roughly speaking, as the degree increases (so the canonical class becomes more ample), the variety becomes less and less rational, and fibrations of the special set if they exist involve abelian varieties, whereas for lower degrees, these fibrations may involve only linear groups and rational or unirational fibers. Changes of behavior occur especially for $d = n + 2$, $n + 1$, and n. The less the canonical class is ample, the more a variety has a tendency to contain rational curves. For instance:

Let X be a hypersurface of degree d in $\mathbf{P}^n$. If $d \leqq n - 1$, then X contains a line through every point.

This result is classical and easy. For the argument, see [La 86], p. 196.

In all the above, it is a problem to determine what happens on Zariski open subsets rather than generically. For some examples in other contexts, see Chapter VIII, §1 for the Brody–Green perturbation of the Fermat hypersurface, and Chapter X, §2 for the Châtelet surface. Here we now consider:

Example 5 (The Fermat hypersurface). Since this hypersurface

$$T_0^d + \cdots + T_n^d = 0 \qquad \text{or} \qquad T_1^d + \cdots + T_n^d = T_0^d$$

contains lines, we see that the condition that X has ample canonical class does not imply that X is Mordellic or that the special set is empty.

Euler was already concerned with the problem of finding rational curves, that is, solving the Fermat equation with polynomials. Swinnerton-Dyer [SWD 52] gives explicit examples of rational curves over the rationals, on

$$T_0^5 + \cdots + T_5^5 = 0.$$

Here X has degree $d = n = 5$, and so the anti-canonical class is very ample. Swinnerton-Dyer says: "It is very likely that there is a solution in four parameters, or at least that there are an infinity of solutions in three parameters, but I see no prospect of making further progress by the methods of this paper." In general, I conjectured:

3.13. *For the Fermat hypersurface if $d = n$, then the rational curves are Zariski dense, and the Fermat hypersurface is unirational over $\mathbf{Q}$.*

Of course one must take either d odd or express the Fermat equation in an indefinite form.

Example: When $d = n = 3$, the Fermat hypersurface has Ramanujan's taxicab rational point (1729 is the sum of two cubes in two different ways: 9, 10 and 12, 1). Furthermore, the conjecture is true in this case, i.e. for $d = n = 3$, the Fermat surface is a rational image of $\mathbf{P}^2$ over $\mathbf{Q}$, by using Theorem 12.11 of Manin's book [Man 74]. But so far there are no systematic results known for the general Fermat hypersurfaces from the present point of view of algebraic geometry, for the existence of rational curves, both geometrically and over $\mathbf{Q}$, and for the possibility of their being rational images of projective space for low degrees compared to n.

The Fermat equation is even more subtle for $d = n + 1$, when one expects fewer solutions. Euler had a false intuition when he guessed that there would be no non-trivial rational solutions. First, Lander and Parkin [LandP 66] found the solution in degree 5:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Then Elkies [El 88] found infinitely many solutions in degree 4, including

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

He was led to this solution by a mixture of theory and computer search. The point is that for the degree $d = n + 1$ there is no expectation that the Fermat hypersurface is unirational. Rather, *it is fibered by curves of genus* 1, *and the question is when a fiber has a rational point.* Elkies found theoretically that in many cases there could not be a rational point, and in one remaining case, he knew how to make the computer deliver. Furthermore, he proved that infinitely many fibers have at least two rational points; one of them can be taken as an origin, and the other one has infinite order on the fibral elliptic curve. This leaves open the problem of giving an asymptotic estimate for the number of rational points on the base curve of height bounded by $B \to \infty$, such that the fiber above those points is an elliptic curve with a rational point of infinite order.

The fibration of the Fermat surface by elliptic curves over $\mathbf{C}$ is classical, perhaps dating back to Gauss. Over $\mathbf{Q}$, as far as I know, a fibration comes from Demjanenko [Dem 74], and it is the one used by Elkies. When written in the form

$$x_0^4 + x_1^4 = x_2^4 + x_3^4,$$

there are other fibrations, related to modular curves. The Fermat surface can also be viewed as an example of a K3 surface. For various points of view, see also Mumford [Mu 83], p. 55 and Shioda [Shio 73], §4.

Let us now discuss the function field case, analogous to Theorem 2.3 for curves. The following analogue of de Franchis' theorem was proved by Kobayashi–Ochiai [KoO 75], motivated by my conjecture that a hyperbolic projective variety is Mordellic, see Chapter VIII, §4.

Theorem 3.14 (Kobayashi–Ochiai). *Let W be a variety, and let X_0 be a pseudo-canonical projective variety. Then there is only a finite number of generically surjective rational maps of W onto X_0.*

Theorem 3.14 is the **split** case. On this subject see also [DesM 78]. More generally, it has been conjectured that:

3.15. *Given a variety W, there is only a finite number of isomorphism classes of pseudo-canonical varieties X_0 for which there exists a generically surjective rational map of W onto X_0.*

For a partial result in this direction, see Maehara [Mae 83], who investigates algebraic families of pseudo-canonical varieties and rational maps.

In the non-split case, we only have a conjecture.

3.16. *Let X be a pseudo-canonical projective variety defined over a function field F with constant field k. Suppose that the set of rational points $X(F)$ is Zariski dense in X. Then there exists a variety X_0 defined over k such that X is birationally equivalent to X_0 over F. All the rational points in $X(F)$ outside some proper Zariski closed subset of X are images of points in $X_0(k)$ under the birational isomorphism.*

As in the case of curves, the problem is to bound the degrees of sections, so that they lie in a finite number of families. Again see [Mae 83]. It then follows that there exists a parameter variety T and a generically surjective rational map

$$f: T \times W \to X.$$

From this one wants to split X birationally. In [La 86] I stated the following self-contained version as a conjecture.

Theorem 3.17. *Let $\pi: X \to W$ be a generically surjective rational map, whose generic fiber is geometrically irreducible and pseudo canonical. Assume that there exists a variety T and a generically surjective rational map*

$$f: T \times W \to X.$$

Then X is birationally equivalent to a product $X_0 \times W$.

Viehweg pointed out to me that this statement is essentially proved in [Mae 83] over an algebraically closed field of characteristic 0.

The interplay between the diophantine problems and algebraic geometry is reflected in the history surrounding Theorem 3.14. My conjecture that hyperbolic projective varieties are Mordellic led Kobayashi–Ochiai to their theorem about pseudo-canonical varieties in the split case, and this theorem in turn made me conjecture that pseudo-canonical varieties are pseudo Mordellic, thus coming to the conjecture that a variety is Mordellic (or hyperbolic) if and only if every subvariety is pseudo canonical, and coming to the definition of the special set.

For more information on the topics of this section, readers might look up my survey [La 86]. For quantitative formulations, see Vojta's conjectures in Chapter II, §4.

I, §4. ABELIAN VARIETIES

An **abelian variety** is a projective non-singular variety which is at the same time a group such that the law of composition and inverse are morphisms. Over the complex numbers, abelian varieties are thus compact complex Lie groups, and are thus commutative groups. Weil originally developed the theory algebraically, although the fact that abelian varieties are commutative in all characteristics is due to Chevalley.

Example. Let A be an abelian variety of dimension 1, and suppose A is defined over a field k of characteristic $\neq 2, 3$. Then A can be defined by an affine equation in Weierstrass form

$$y^2 = 4x^3 - g_2 x - g_3 \qquad \text{with} \quad g_2, g_3 \in k$$

and $\Delta = g_2^3 - 27g_3^2 \neq 0$. The corresponding projective curve is (isomorphic to) A, whose points $A(k)$ consist of the solutions of the affine equation with $x, y \in k$ together with the point at infinity in $\mathbf{P}^2$. If $k = \mathbf{C}$ is the complex numbers, then $A(\mathbf{C})$ can be parametrized by the Weierstrass functions with respect to some lattice Λ. In other words, there exists a lattice, with basis ω_1, ω_2 over $\mathbf{Z}$, such that the map

$$z \mapsto (\wp(z), \wp'(z))$$

is an isomorphism of $\mathbf{C}/\Lambda$ with $A(\mathbf{C})$. The function $\wp$ is the Weierstrass function, defined by

$$\wp(z) = \sum_{\omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

The coefficients of the equation are given by

$$g_2 = 60 \sum_{\omega \neq 0} \omega^{-4} \qquad \text{and} \qquad g_3 = 140 \sum_{\omega \neq 0} \omega^{-6}.$$

The sums over $\omega \neq 0$ are taken over all elements of the lattice $\neq 0$. In the above parametrization, the lattice points map to the point at infinity on $\mathbf{P}^2$.

Abelian varieties of dimension 1 over a field k are precisely the curves of genus 1 together with a rational point, which is taken as the origin on the abelian variety for the group law.

In higher dimension, it is much more difficult to write down equations for abelian varieties. See Mumford [Mu 66] and Manin–Zarhin [MaZ 72].

Let A, B be abelian varieties over a field k. By $\mathrm{Hom}_k(A, B)$ we mean the **homomorphisms of** A into B which are algebraic, i.e. the morphisms of A into B which are also group homomorphisms, and are defined over k. A basic theorem states that $\mathrm{Hom}_k(A, B)$ is a free abelian group, finitely generated. We sometimes omit the reference to k in the notation, especially if k is algebraically closed.

Abelian varieties are of interest intrinsically, for themselves, and also because they affect the theory of other varieties in various ways. One of these ways is described in §5.

We are interested in the structure of the group of rational points of an abelian variety over various fields.

As usual, we consider the two important cases when F is a number field and F is a function field.

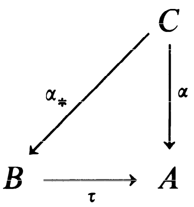
Theorem 4.1 (Mordell–Weil theorem). *Let A be an abelian variety defined over a number field F. Then $A(F)$ is a finitely generated abelian group.*

When $F = \mathbf{Q}$ and $\dim A = 1$, so when A is a curve of genus 1, the finite generation of $A(\mathbf{Q})$ was conjectured by Poincaré and proved by Mordell in 1921 [Mo 21]. Weil extended Mordell's theorem to number fields and arbitrary dimension [We 28]. Néron [Ne 52] extended the theorem to finitely generated fields over $\mathbf{Q}$.

Next we handle the function field case. Let k be a field and let F be a finitely generated extension of k, such that F is the function field of a variety defined over k. Let A be an abelian variety defined over F. By an **F/k-trace** of A we mean a pair (B, τ) consisting of an abelian variety B defined over k, and a homomorphism

$$\tau\colon B \to A$$

defined over F, such that (B, τ) satisfies the universal mapping property for such pairs. In other words, if (C, α) consists of an abelian variety C over k, and a homomorphism $\alpha: C \to A$ over F, then there exists a unique homomorphism $\alpha_*: C \to B$ over k such that the following diagram commutes.



Chow defined and proved the existence of the F/k-trace. He also proved that the homomorphism τ is injective. See [La 59].

The analogue of the Mordell–Weil theorem was then formulated and proved in the function field case as follows [LN 59].

Theorem 4.2 (Lang–Néron theorem). *Let F be the function field of a variety over k. Let A be an abelian variety defined over F, and let (B, τ) be its F/k-trace. Then $A(F)/\tau(B(k))$ is finitely generated.*

Example. Consider for example the case when $\dim A = 1$. Suppose A is defined by the Weierstrass equation as recalled at the beginning of this section. Let as usual

$$j = 1728 g_2^3/\Delta.$$

We assume the characteristic is $\neq 2, 3$. Suppose A is defined over the function field F with constant field k. Assume that the F/k-trace is 0. There may be two cases, when $j \in k$ or when j is transcendental over k. In both cases, the Lang–Néron theorem guarantees that $A(F)$ is finitely generated.

Corollary 4.3. *Let F be finitely generated over the prime field. Let A be an abelian variety defined over F. Then $A(F)$ is finitely generated.*

This corollary is the absolute version of Theorem 4.2, and follows since the set of points of a variety in a finite field (the constant field) is finite, no matter what the variety, or in characteristic 0, by using Theorem 4.1.

Questions arise as to the rank and torsion of the group $A(F)$. First consider the generic case. Abelian varieties distribute themselves in algebraic families, of which the generic members are defined over a function field F over the complex numbers. Shioda in dimension 1 (for elliptic curves) [Shio 72] and Silverberg in higher dimension [Slbg 85] have shown that if A is the generic member of such families, then $A(F)$ is finite. Torsion for elliptic curves over a base of dimension 1 has been studied extensively, and I mention only the latest paper known to me giving fairly general results by Miranda–Persson [MirP 89].

Over the rational numbers, or over number fields, the situation involves a great deal of arithmetic, some of which will be mentioned in other chapters. Here, we mention only two qualitative conjectures, in line with the general topics which have been discussed.

Conjecture 4.4. *Over the rational numbers* $\mathbf{Q}$, *there exist elliptic curves* A *(abelian varieties of dimension* 1) *such that* $A(\mathbf{Q})$ *has arbitrarily high rank.*

No example of such elliptic curves is known today. Shafarevich–Tate have given such examples for elliptic curves defined over function fields over a finite field [ShT 67]. For rank 10 see [Ne 52] and rank 14 see [Me 86]. One problem is to give a quantitative measure, or probabilistic description, of those which have one rank or the other, and an asymptotic estimate of how many have a given positive integer as rank. The problem is also connected with the Birch–Swinnerton-Dyer conjecture, which relates the rank to certain aspects of a zeta function associated with the curve, and which we shall discuss in Chapter III. For some current partial results on the rank, see Goldfeld [Go 79], and for computations giving relatively high frequency of rank > 1, see Zagier–Kramarz [ZaK 87] and Brumer–McGuinness [BruM 90].

Aside from the rank, one also wants to describe the torsion group, for individual abelian varieties, and also uniformly for families. The general expectation lies in:

Conjecture 4.5. *Given a number field* F, *and a positive integer* d, *there exists a constant* $C(F, d)$ *such that for all abelian varieties* A *of dimension* d *defined over* F, *the order* $\# A(F)_{\mathrm{tor}}$ *of the torsion group is bounded by* $C(F, d)$.

Furthermore, Kamienny [Kam 90] has shown for $d = 1$ and $n = 2$ that the following stronger uniformity is true: *There exists a constant* $C(n, d)$ *such that for all abelian varieties* A *of dimension* d *over a number field* F *of degree* n *the order of the torsion group* $\# A(F)_{\mathrm{tor}}$ *is bounded by* $C(n, d)$.

For elliptic curves over the rationals, Mazur has proved that the order of the torsion group is bounded by 16, developing in the process an extensive theory on modular curves [Maz 77] and [Maz 78] which we shall mention in Chapter V. Over number fields, some results have been obtained by Kubert [Ku 76], [Ku 79]. Mazur has conjectured, or more cautiously, raised the question whether the following is true.

Question 4.6. *Given a number field* F, *there is an integer* $N_1(F)$ *and a finite number of values* $j_1, \ldots, j_{c(F)}$ *such that if* A *is an elliptic curve over* F *with a cyclic subgroup* C *of order* $N \geqq N_1(F)$, *and* C *is stable under the Galois group* G_F, *then* $j(A)$ *is equal to one of the* $j_1, \ldots, j_{c(F)}$.

We mention here that a certain diophantine conjecture, the *abc* conjecture (stated in Chapter II, §1) implies Conjecture 4.5 by an argument due to Frey (see [Fr 87a, b], [La 90], and also [HiS 88]). It also has something to do, but less clearly, with the above question of Mazur.

Questions also arise as to the behavior of the rank and torsion in infinite extensions. For instance:

Theorem 4.7. *Let A be an abelian variety defined over a number field F. Let $\boldsymbol{\mu}$ denote the group of all roots of unity in the algebraic numbers. Then the group of torsion points $A(F(\boldsymbol{\mu}))_{\mathrm{tor}}$ is finite.*

This was proved by Ribet (see the appendix of [KaL 82]). We also have:

Theorem 4.8 (Zarhin [Zar 87]). *Let A be a simple abelian variety over a number field F. Then $A(F^{\mathrm{ab}})_{\mathrm{tor}}$ is finite if and only if A does not have complex multiplication over F.*

For the convenience of the reader, we recall the definition that A has **complex multiplication**, or has **CM type** over a field F, if and only if $\mathrm{End}_F(A)$ contains a semisimple commutative $\mathbf{Q}$-algebra of dimension $2 \dim A$. The above theorem of Zarhin comes from other theorems concerned with non-abelian representations of the Galois group, for which I refer to his paper. Zarhin also has results for the finiteness of torsion points in non-abelian extensions, for instance:

Theorem 4.9 ([Zar 89]). *Let l be a prime number and let L be an infinite Galois extension of F such that* $\mathrm{Gal}(L/F)$ *is a compact l-adic Lie group. Let A be an abelian variety over F. If $A[p] \cap A(L)$ is $\neq 0$ for infinitely many primes p, and A is simple over L, then A has* CM *type over L.*

Mazur [Maz 72] has related the question of points of abelian varieties in certain cyclotomic extensions with the arithmetic of such extensions, and we shall state his main conjecture. Let F be a number field. Let p be an odd prime (for simplicity). Let F_n be the cyclic extension of F consisting of the largest subfield of $F(\boldsymbol{\mu}_{p^n})$ of p-power degree. Let

$$F_\infty = \bigcup F_n.$$

Then F_∞ is called the **cyclotomic $\mathbf{Z}_p$-extension** of F. Mazur raises the possibility that the following statement is true:

Let A be an abelian variety over F. Then $A(F_\infty)$ is finitely generated.

Rohrlich [Roh 84] proved: If A is an elliptic curve with complex multiplication, P is a finite set of primes where E has good reduction, L the maximal abelian extension of $\mathbf{Q}$ unramified outside P and infinity, then $A(L)$ is finitely generated.

For a survey of results and conjectures connecting the rank behavior of the Mordell–Weil group in towers of number fields with Iwasawa type theory and modular curves, see Mazur [Maz 83]. For other results concerning points in extensions whose Galois group is isomorphic to the p-adic integers $\mathbf{Z}_p$, see for instance Wingberg [Win 87].

I, §5. ALGEBRAIC EQUIVALENCE AND THE NÉRON–SEVERI GROUP

There is still another important possible relation between divisor classes. Let X be a projective variety, non-singular in codimension 1, and let Y be a non-singular variety. Let c be a divisor class on $X \times Y$. If x is a simple point of X we write

$$c(x) = \text{restriction of } c \text{ to } \{x\} \times Y \text{ identified with } Y.$$

Similarly, for a point y of Y we write

$${}^tc(y) = \text{restriction of } c \text{ to } X \times \{y\} \text{ identified with } X.$$

The superscript t indicates a transpose, namely ${}^tc$ is the transpose of c on $Y \times X$. The group generated by all classes of the form ${}^tc(y_1) - {}^tc(y_2)$ for all pairs of points $y_1, y_2 \in Y$, and all classes c on products $X \times Y$, will be said to be the group of classes **algebraically equivalent to** 0. This subgroup of $\mathrm{CH}^1(X)$ is denoted by $\mathrm{CH}^1_0(X)$, and is also called the **connected component** of $\mathrm{CH}^1(X)$, for reasons which we shall explain later in this section. The factor group

$$\mathrm{NS}(X) = \mathrm{CH}^1(X)/\mathrm{CH}^1_0(X)$$

is called the **Néron–Severi group**.

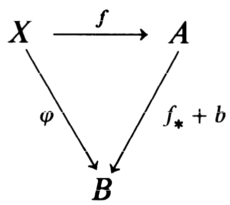
Theorem 5.1 (Néron [Ne 52]). *The Néron–Severi group is finitely generated.*

The history of this theorem is interesting. Severi had the intuition that there was some similarity between his conjecture that $\mathrm{NS}(X)$ is finitely generated, and the Mordell–Weil theorem that $A(F)$ is finitely generated for number field F. Néron made this similarity more precise when he proved the theorem, and an even clearer connection was established by Lang–Néron, who showed how to inject the Néron–Severi group in a group of rational points of an abelian variety over a function field. To do this we have to give some definitions.

Let X be any non-singular variety, defined say over a field k, and with a rational point $P \in X(k)$. There exists an abelian variety A over k and a morphism

$$f: X \to A$$

such that $f(P) = 0$, satisfying the universal mapping property for morphisms of X into abelian varieties. In other words, if $\varphi: X \to B$ is a morphism of X into an abelian variety B, then there exists a unique homomorphism $f_*: A \to B$ and a point $b \in B$ such that the following diagram commutes.



Of course, if $\varphi(P) = 0$ then $b = 0$. The abelian variety A is uniquely determined up to an isomorphism, and is called the **Albanese variety** of X. If k' is an extension of k, then A is also the Albanese variety of X over k', so one usually does not need to mention a field of definition for the Albanese variety. Note that the existence of a simple rational point, or some sort of condition is needed on the variety X. For instance, there may be a projective curve of genus 1, defined over a field k and having no rational point. Over any extension of k where this curve acquires a rational point, we may identify the curve with its Albanese variety, but over the field k itself, the curve does not admit an isomorphism with an abelian variety.

The morphism $f: X \to A$ can be extended. For any field k' containing k, define the group of **0-cycles** $\mathscr{Z}(X(k'))$ to be the free abelian group generated by the points in $X(k')$. A zero cycle $\mathfrak{a}$ can then be expressed as a formal linear combination

$$\mathfrak{a} = \sum n_i(P_i) \qquad \text{with} \quad P_i \in X(k') \quad \text{and} \quad n_i \in \mathbf{Z}.$$

We define

$$S_f(\mathfrak{a}) = \sum n_i f(P_i),$$

where the sum on the right-hand side is taken on A. Then

$$S_f: \mathscr{Z}(X) \to A$$

is a homomorphism. Let $\mathscr{Z}_0(X)$ be the subgroup of 0-cycles of degree 0, that is those cycles such that $\sum n_i = 0$. Then the image $S_f(\mathfrak{a})$ is independent of the map f, which was determined only up to a translation, whenever $\mathfrak{a}$ is of degree 0. As a result, one can show that even if X does not admit a rational point over k, there still exists an abelian variety A

over k and a homomorphism (the sum)

$$S\colon \mathscr{Z}_0(X(k')) \to A(k')$$

for every field k' containing k, such that over any field k' where X has a rational point, $A_{k'}$ is the Albanese variety of X, and $S = S_f$. We again call A the **Albanese variety** of X, and we call S the **Albanese homomorphism on the 0-cycles of degree 0**.

If X is a curve, then its Albanese variety is called the **Jacobian**. A canonical map of X into its Jacobian is an imbedding. If X and J are defined over a field k, then one way to approach the study of the rational points $X(k)$ is via its imbedding in $J(k)$.

It will now be important to deal with fields of rationality, so suppose the projective variety X is defined over a field k. By $\mathrm{CH}^1(X, k)$ we mean the group of divisor classes on X, defined over k.

Theorem 5.2 (Lang–Néron [LN 59]). *Let X be a projective variety, non-singular in codimension 1, and defined over an algebraically closed field k. Let L_u be a linear variety defined by linear polynomials with algebraically independent coefficients u, and of dimension such that the intersection $X . L_u$ is a non-singular curve C_u defined over the function field $k(u)$ (purely transcendental over k). Let J_u be the Jacobian of C_u, defined over $k(u)$, and let*

$$S\colon \mathscr{Z}_0(C_u) \to J_u$$

be the Albanese homomorphism. Let (B, τ) be the $k(u)/k$-trace of J_u. Let $\mathscr{C}$ be the subgroup of $\mathrm{CH}^1(X, k)$ consisting of those divisor classes c whose restrictions $c . C_u$ to C_u have degree 0. Then

$$\mathscr{C} \supset \mathrm{CH}^1_0(X, k) \qquad \textit{and} \qquad \mathrm{CH}^1(X, k)/\mathscr{C} \approx \mathbf{Z}.$$

The projective imbedding of X can be chosen originally so that the map

$$c \mapsto S(c . C_u) \qquad \textit{for} \quad c \in \mathscr{C}$$

induces an injective homomorphism $\mathscr{C} \hookrightarrow J_u(k(u))$, and also an injective homomorphism

$$\mathscr{C}/\mathrm{CH}^1_0(X, k) \hookrightarrow J_u(k(u))/\tau B(k).$$

That $\mathrm{NS}(X, k)$ is finitely generated is then a consequence of the Lang–Néron Theorem 4.2.

Observe how a geometric object, the Néron-Severi group, is reduced to a diophantine object, the rational points of an abelian variety in some function field. Conversely, we shall see instances when geometric objects are associated to rational points, in the case of curves.

Remark. In the statement of the theorem, after a suitable choice of projective imbedding, we get an injection of $\mathrm{NS}(X, k)$ into $J_u(k(u))$. Actually, *given* a projective imbedding, the kernel of the homomorphism $c \mapsto S(c \,.\, C_u)$ is always finitely generated, according to basic criteria of algebraic equivalence [We 54]. This suffices for the proof that $\mathrm{NS}(X, k)$ is finitely generated, which proceeds in the same way.

Having described the Néron–Severi group, we next describe the subgroup $\mathrm{CH}_0^1(X)$ by showing how it can be given the structure of an algebraic group, and in fact an abelian variety. This explains why we call it a **connected component**.

Theorem 5.3. *Let X be a projective variety, non-singular in codimension 1, and defined over a field k. Let $P \in X(k)$ be a simple rational point. Then there exists an abelian variety $A' = A'(X)$, and a class $c \in \mathrm{CH}^1(X \times A')$ such that*

$$^t c(0) = 0, \qquad c(P) = 0,$$

and for any field k' containing k the map

$$a' \mapsto {}^t c(a') \qquad \text{for} \quad a' \in A'(k')$$

gives an isomorphism $A'(k') \xrightarrow{\approx} \mathrm{CH}_0^1(X, k')$. The abelian variety and c are uniquely determined up to an isomorphism over k.

We call the pair (A', c) the **Picard variety** of X over k. It is a theorem that for every extension k' of k, the base change $(A'_{k'}, c_{k'})$ is also the Picard variety of X over k'. The class c is called the **Poincaré class**.

Let A be the Albanese variety of X and let $f: X \to A$ be a canonical map, determined up to a translation. If (A', δ) is the Picard variety of A, then we can form its pull back to get the Picard variety of X. Indeed, we have a morphism

$$f \times \mathrm{id}: X \times A' \to A \times A',$$

and the pull back $(f \times \mathrm{id})^*(\delta)$ is the Poincaré class making A' also the Picard variety of X.

The Picard variety of an abelian variety is also called the **dual variety**.

It is a theorem that if (A', δ) is the dual of A then $(A, {}^t\delta)$ is the dual of A'. This property is called the **biduality** of abelian varieties.

Putting together the finite generation of the Néron–Severi group and the finite generation of the Mordell–Weil group, we find:

Theorem 5.4. *Let X be a projective variety, non-singular in codimension 1, defined over a field F finitely generated over the prime field. Then $\mathrm{CH}^1(X, F)$ is finitely generated.*

Remark 5.5. One can define **Chow groups** $\mathrm{CH}^m(X, k)$ for higher codimension m, and one can define the notion of algebraic equivalence, as well as cohomological equivalence. Thus one obtains factor groups analogous to the Néron–Severi group. The example of Clemens ([Cl 83], [Cl 84] and Example 4 of §3) shows that over an algebraically closed field, this group is not necessarily finitely generated. It is still conjectured that $\mathrm{CH}^m(X, F)$ is finitely generated if F is finitely generated over $\mathbf{Q}$. In fact there are even much deeper conjectures of Beilinson and Bloch connecting the rank with orders of poles of zeta functions in the manner of the Birch–Swinnerton-Dyer conjecture and the theory of heights. See for instance Beilinson [Be 85] and Bloch [Bl 84], [Bl 85]. For more on the Griffiths group of cycles, especially in connection with the Beilenson-Bloch conjectures, see [Ze 91].

We shall use other properties of the Picard variety later in several contexts, so we recall them there. By a **polarized abelian variety**, we mean an abelian variety A and an algebraic equivalence class $c \in \mathrm{NS}(A)$ which contains an ample divisor. Such a class is called a **polarization**. A **homomorphism of polarized abelian varieties**

$$f\colon (A, c) \to (A_1, c_1)$$

is a homomorphism of abelian varieties $f\colon A \to A_1$ such that $f^*c_1 = c$. To each polarization we shall associate a special kind of homomorphism of A. We define an **isogeny** $\varphi\colon A \to B$ of abelian varieties to be a homomorphism which is surjective and has finite kernel. Then A, B have the same dimension.

Proposition 5.6. *Given a class $c \in \mathrm{CH}^1(A)$ and $a \in A$, let c_a be the translation of c by a. Let A' be the dual variety. The map*

$$\varphi_c\colon A \to A' \quad \textit{satisfying } \varphi_c(a) = \textit{element } a' \textit{ such that } \ {}^t\delta(a') = c_a - c$$

is a homomorphism of A into A', depending only on the algebraic equivalence class of c. The association $c \mapsto \varphi_c$ induces an injective homomorphism

$$\mathrm{NS}(A) \hookrightarrow \mathrm{Hom}(A, A').$$

If c is ample, then φ_c is an isogeny.

By abuse of notation, one sometimes writes

$$\varphi_c(a) = c_a - c.$$

In general, let $\varphi: A \to B$ be an isogeny. Then φ is a finite covering, whose degree is called the **degree of the isogeny**. If c is a polarization, then the degree of φ_c is called the **degree of the polarization.** A polarization of degree 1 is a polarization c such that φ_c is an isomorphism, and is called a **principal polarization.**

I, §6. SUBVARIETIES OF ABELIAN AND SEMIABELIAN VARIETIES

Such varieties provide a class of examples for diophantine problems holding special interest, since all curves of genus $\geqq 1$ belong to this class. A basic theorem describes their algebraic structure. An important characterization was given by Ueno [Ue 73], see also Iitaka ([Ii 76], [Ii 77]), who proved:

Let X be a subvariety of an abelian variety over an algebraically closed field. Then X is pseudo canonical if and only if the group of translations which preserve X is finite.

Then we have quite generally, [Ue 73], Theorem 3.10:

Ueno's theorem. *Let X be a subvariety of an abelian variety A, and let B be the connected component of the group of translations preserving X. Then the quotient $f: X \to X/B = Y$ is a morphism, whose image is a pseudo-canonical subvariety of the abelian quotient A/B, and whose fibers are translations of B. In particular, if X does not contain any translates of abelian subvarieties of dimension $\geqq 1$, then X is pseudo canonical.*

For a proof, see also Iitaka [Ii 82], Theorem 10.13, and [Mori 87], Theorem 3.7. We call f the **Ueno fibration of** X.

The variety Y in Ueno's theorem is also a subvariety of an abelian variety. Hence to study the full structure of subvarieties of A and their rational points, we are reduced to pseudo-canonical subvarieties, in which case we have:

Kawamata's structure theorem ([Kaw 80]). *Let X be a pseudo-canonical subvariety of an abelian variety A in characteristic 0. Then there exists a finite number of proper subvarieties Z_i with Ueno fibrations $f_i: Z_i \to Y_i$ whose fibers have dimension $\geqq 1$, such that every translate of an abelian subvariety of A of dimension $\geqq 1$ contained in X is actually contained in the union of the subvarieties Z_i.*

Note that the set of Z_i is empty if and only if X does not contain any translation of an abelian subvariety of dimension $\geqq 1$.

Although the above version of Kawamata's theorem is not stated that way in the given references, I am indebted to Lu for pointing out that these references actually prove the structure theorem as stated. Ochiai [Och 77] made a substantial contribution besides Ueno, but it was actually Kawamata who finally proved the existence of the fibrations by abelian subvarieties, so we call the union of the subvarieties Z_i the **Ueno–Kawamata fibrations in** X when X is pseudo canonical. We now see:

For every subvariety X of an abelian variety A, the Ueno–Kawamata fibrations in X constitute the special set defined in §3.

So in the case of subvarieties of abelian varieties, we have a clear description of this special set.

For an extension of the above results to semiabelian varieties, see Noguchi [No 81a]. The structure theorems constitute the geometric analogue of my conjecture over finitely generated fields [La 60a]:

Conjecture 6.1. *Let X be a subvariety of an abelian variety over a field F finitely generated over* $\mathbf{Q}$. *Then X contains a finite number of translations of abelian subvarieties which contain all but a finite number of points of $X(F)$.*

In light of the determination of the exceptional set, this conjecture corresponds to the general conjecture of §4 applied to subvarieties of abelian varieties. By Kawamata's structure theorem, to prove Conjecture 6.1 it suffices to prove that if X is not the translate of an abelian subvariety of dimension $\geqq 1$, then the set of rational points $X(F)$ is not Zariski dense. The following especially important case from [La 60b] has now been proved.

Theorem 6.2 (Faltings [Fa 90]). *Let X be a subvariety of an abelian variety, and suppose that X does not contain any translation of an abelian subvariety of dimension* > 0. *Then X is Mordellic.*

In particular, let C be a projective non-singular curve, imbedded in its Jacobian J. In the early days of the theory, I formulated Mordell's conjecture as follows.

Suppose that the genus of C is $\geqq 2$. *Let Γ_0 be a finitely generated subgroup of J. Then $C \cap \Gamma_0$ is finite.*

No direct proof has been found, and the statement is today a consequence of Faltings' theorem over number fields, combined with the Mordell–Weil and Lang–Néron theorems, as they imply Corollary 4.3. Chabauty [Chab 41] proved the statement when the rank of Γ_0 is smal-