INTERSCIENCE TRACTS
IN PURE AND APPLIED MATHEMATICS
NUMBER 7

SERGE LANG

ABELIAN VARIETIES

ABELIAN VARIETIES

SERGE LANG

Columbia University, New York, New York

INTERSCIENCE PUBLISHERS, INC., NEW YORK

INTERSCIENCE PUBLISHERS LTD., LONDON

FOREWORD

Pour des simplifications plus substantielles, le développement futur de la géometrie algébrique ne saurait manquer sans doute d'en faire apparaitre.

It is with considerable pleasure that we have seen in recent years the simplifications expected by Weil realize themselves, and it has seemed timely to incorporate them into a new book.

We treat exclusively abelian varieties, and do not pretend to write a treatise on algebraic groups. Hence we have summarized in a first chapter all the general results on algebraic groups that are used in the sequel. They are all foundational results.

We then deal with the Jacobian variety of a curve, the Albanese variety of an arbitrary variety, and its Picard variety, i.e., the theory of cycles of dimension 0 and codimension 1. As we shall see, the numerical theory which gives the number of points of finite order on an abelian variety, and the properties of the trace of an endomorphism are simple formal consequences of the theory of the Picard variety and of numerical equivalence. The same thing holds for the Lefschetz fixed point formula for a curve, and hence for the Riemann hypothesis for curves.

Roughly speaking, it can be said that the theory of the Albanese and Picard variety incorporates in purely algebraic terms the theory which in the classical case would be that of the first homology group. It is far from giving a complete theory of abelian varieties, and a partial list of topics which we do not discuss includes the following:

The theory of differential forms and the cohomology theory.

The infinitesimal and global theory proper to characteristic p.

The theory of linear systems and the Riemann-Roch theorem.

The theory of moduli, i.e., the classification of algebraic families of abelian varieties, and the characterization of Jacobians among abelian varieties.

Various applications to arbitrary varieties, such as, for instance, the equivalence criteria and the theorem of Néron-Severi.

Arithmetic applications like class field theory (which actually belongs to the general theory of algebraic groups) or the theorem of Mordell-Weil.

To a large extent, these topics have not reached the same state of maturity as those with which we deal in this book. Many deserve to have a whole book devoted to them. In any case, we have included at least all the results of Weil's treatise [85] (and, of course, considerably many more).

We shall now make some remarks concerning the formal structure of the book. We begin by a list of prerequisites necessary for a rigorous understanding of the proofs given here. It should be understood, however, that much less is actually required for a general appreciation of the results stated and the methods of proofs. We hope that a good acquaintance with the language of algebraic geometry would suffice.

At the end of each chapter, we append a historical and bibliographical notice, one of whose purposes is to acquaint the reader with the current literature. We have also made comments concerning some of the directions in which the present research is leading. Further historical comments of a more general nature have been made preceding the bibliography given at the end of the book. The index includes all the terms defined here, and the table of notation includes the symbols used most frequently. Finally, we point out that the reader who wishes to get a more detailed summary account of the contents of this book can get it by reading through the brief introductions with which we begin each chapter.

S. Lang

New York, Fall 1958

PREREQUISITES

They are of order 4.

1. Elementary qualitative algebraic geometry, as it is treated for instance in *Introduction to Algebraic Geometry*, Interscience, New York, 1958. This book will be referred to as IAG. It treats of varieties, cycles, linear systems, topics in field theory, Zariski topology, and other topics of a heterogeneous nature.

2. The Riemann-Roch theorem for curves.

3. The elementary theory of algebraic groups: definitions, subgroups, factor groups, and the possibility of recovering a group starting with birational data. We have recalled all the results needed in Chapter I, without proofs. A complete self-contained exposition can be found in [90], [91], [92].

4. Intersection theory, of type F–X_y Th. Z. Occasionally we have given an argument in the language of specialization of cycles, for which we refer to Matsusaka [55].

In an appendix we have recalled certain theorems on correspondences properly belonging to the *Foundations of Algebraic Geometry*.

The terminology is that of *Foundations* [83] except for the following modifications.

Let $f: U \to V$ be a rational map. We say that f is *defined over a field* k if k is a field of definition for U, V and the graph of f, usually denoted by Γ_f. Let P be a point of U. We say that f is *holomorphic* at P, or *defined at* P, instead of saying (as in *Foundations*) that f is regular at P.

On the other hand, let f be defined over k, and let u be a generic point of U over k. Let $v = f(u)$. We shall say that f is respectively *regular*, *separable*, *primary*, *purely inseparable* if the extension $k(u)$ of $k(v)$ is of the corresponding type. If v is a generic point of V over k, we say that f is *generically surjective*. Suppose this is the case. Then one sees easily that the above four conditions are respectively equivalent to the following ones concerning the cycle

$$f^{-1}(v) = \mathrm{pr}_1 [\Gamma_f \cdot (U \times v)]:$$

It is a variety with multiplicity 1.

All the components of $f^{-1}(v)$ have multiplicity 1.

There is only one component having multiplicity p^m (where p is the characteristic).

It has only one component, which is a point with multiplicity p^m.

We observe that in the above notation, the support of $f^{-1}(v)$ is the locus of u over $k(v)$.

Let $f: U \to V$ be again a rational map of U into V, defined over k. Let W be a subvariety of U also defined over k. Let w be a generic point of W over k. We say that f is *defined at* W if f is defined at w. The locus of the point $f(w)$ over k will then be denoted by $f(W)$. It is in general distinct from the cycle $\mathrm{pr}_2 [\Gamma_f \cdot (W \times V)]$ even when this intersection is defined. We shall also use $f(W)$ to denote this cycle, and the context will usually make our meaning clear. To avoid confusion, we may also call the first the *set-theoretic image* $f(W)$, and the second the *cycle* $f(W)$, or $f(W)$ *in the sense of intersection theory.*

Finally (added in proof), to conform with the functorial terminology which is generally becoming accepted, we would like to recommend the use of the word "isomorphism" instead of the words "birational isomorphism." What we here call "isomorphism" should be called a "bijective homomorphism."

First Published 1959

Library of Congress Catalog Card Number 58-12725

Interscience Publishers, Inc.
250 Fifth Avenue, New York 1, N.Y.

For Great Britain and Northern Ireland:
Interscience Publishers Ltd.
88/90 Chancery Lane, London, W.C. 2, England

PRINTED IN THE NETHERLANDS
BY DRUKKERIJ VOORHEEN GEBRS. HOITSEMA, GRONINGEN

CONTENTS

CHAPTER VI

The Picard Variety of an Arbitrary Variety

CHAPTER VII

The l-Adic Representations

CHAPTER VIII

Algebraic Systems of Abelian Varieties

APPENDIX

Composition of Correspondences

CHAPTER I

Algebraic Groups

The purpose of this chapter is to recall briefly the fundamental notions of the theory of algebraic groups. In the sequel, we shall use only elementary properties of algebraic groups, and we shall not need structure theorems, for instance. All the results which we shall need are stated explicitly below. We give no proofs in § 1. Granting IAG, a complete self-contained exposition can be found in the papers of Weil and Rosenlicht.

The numerical theory in § 2, together with the Pontrjagin products requires intersection theory, and the proofs depend on *Foundations*.

Finally in § 3, we have stated the theorems concerning the field of definition of a variety, and indicated how they can be used to lower the field of definition of a group variety provided certain coherent isomorphisms are given. For the proof, we refer the reader to [92]. We shall use § 3 in the sequel only at the end of the theory of the Albanese variety, and in the last chapter, for the theory of algebraic systems of abelian varieties. The rest of this book is independent of § 3, and we advise the reader to skip § 2 and § 3 until he comes to a place where they are used.

§ 1. *Groups, subgroups, and factor groups*

An *algebraic group* is the union of a finite number of disjoint varieties (abstract) G_α called its components, on which a group structure is given by everywhere defined rational maps. More precisely, for each pair G_α, G_β of components of G, we are given a rational map $f_{\alpha\beta} : G_\alpha \times G_\beta \to G_\gamma$, everywhere defined into a third component G_γ determined by α and β, such that the group law $(x, y) \to xy$ for $x \in G_\alpha$ and $y \in G_\beta$ is given by $xy = f_{\alpha\beta}(x, y)$. In addition, for each G_α, we are given a birational biholomorphic map $\varphi_\alpha : G_\alpha \to G_\lambda$ into another component G_λ such that the inverse $x \to x^{-1}$ is given by $x^{-1} = \varphi_\alpha(x)$.

If there is only one component, the algebraic group is called a *group variety*, or a connected algebraic group. An algebraic group is defined over a field k if all the G_α are defined over k and the $f_{\alpha\beta}$, φ_α are also defined over k. One then sees that the identity e of G is rational over k.

Let G be a group variety. Then G is non-singular. This comes from the fact that for each point $a \in G$ there is a birational biholomorphic transformation $T_a : G \to G$ of G onto itself such that $T_a(x) = ax$. We call it the *left translation*. On the whole, we shall deal only with commutative groups and thus do not need to distinguish our left from our right. If U is a subvariety of G, we denote by aU, or U_a, the left translation of U by a, i.e., $T_a(U)$.

Let H be an abstract subgroup of the group variety G, and assume that H is also an algebraic subset of G. Then H is an algebraic group, whose law of composition is induced by that of G. The components of H are all translations of the connected component (of identity) of H. If G is defined over k, and if H is k-closed, then the connected component of H is also k-closed, and is therefore defined over a purely inseparable extension of k. Indeed, every automorphism of the universal domain leaving k fixed leaves H fixed, permutes the components of H, and must leave the connected component of identity fixed because it leaves e fixed since e is rational over k.

Let G, G' be group varieties.

By a *rational homomorphism*, or simply *homomorphism* $\lambda : G \to G'$ we shall mean an everywhere defined rational map of G into G' which verifies the condition $\lambda(xy) = \lambda(x)\lambda(y)$, i.e., is an abstract homomorphism. We shall say that λ is an *isomorphism* if it is injective (i.e., one-one). As a rational map, λ is then purely inseparable, of finite degree. If this degree is equal to 1, we shall call λ a *birational isomorphism*.

We say that λ is *defined over k* if G, G', and the graph of λ are defined over k. This is compatible with our definition for rational maps.

Let $\lambda : G \to G'$ be a homomorphism defined over k. Then λ is continuous (for the k-topology of Zariski, of course) and its kernel is therefore an algebraic subgroup H of G, which is k-closed.

Let H be an algebraic subgroup of a group variety G and assume that H is a normal subgroup (in the abstract sense). *Then one can give the factor group the structure of a group variety.* More precisely, *there exists a group variety G' and a surjective homomorphism $\lambda : G \to G'$ such that:*

(i) *the kernel of λ is equal to H;*

(ii) *the map λ is separable;*

(iii) *the pair (G', λ) satisfies the universal mapping property for homomorphisms of G whose kernel contains H.*

More precisely, if $\alpha : G \to G''$ is a homomorphism of G whose kernel contains H, then there exists a homomorphism $\beta : G' \to G''$ such that $\alpha = \beta\lambda$. We shall call λ the *canonical homomorphism* on the factor group G'.

We shall say that the algebraic subgroup H of G is *rational* over k if the cycle consisting of the components of H taken with multiplicity 1 is rational over k. If G is defined over k, and if H is rational over k, then we may take the canonical homomorphism $\lambda : G \to G' = G/H$ also defined over k.

Suppose in addition that H is connected and both G, H are defined over k. Let b be a point of G'. Then $\lambda^{-1}(b) = H_a$ for any point $a \in G$ such that $\lambda(a) = b$. This is true both set-theoretically and in the sense of intersection theory i.e., $\lambda^{-1}(b)$ has exactly one component with multiplicity 1. Let u be a generic point of G over k, and put $v = \lambda(u)$. Then $\lambda^{-1}(v) = H_u$. Furthermore, H_u is a *homogeneous space* for H under left translation. The variety H_u is defined over $k(v)$, and is the locus of u over $k(v)$ according to the general theory of rational maps.

More generally, we shall say that a variety V is a *homogeneous space* of a group variety G if we are given an everywhere defined rational map $f : G \times V \to V$ such that if we write xP instead of $f(x, P)$, then $(xy)P = x(yP)$, and for any two points P, Q of V, there exists an element $x \in G$ such that $xP = Q$. In particular, if P is a generic point of V over a field of definition k for f, and if x is a generic point of G over $k(P)$, then xP is a generic point of V over $k(P)$. We shall almost never use homogeneous spaces in the sequel. The only point where a homogeneous space will occur will be in the proof of the complete reducibility theorem of Poincaré.

For the sake of completeness, recall that a homogeneous space V is said to be *principal* if the operation of G is simply transitive and is separable. In other words, if P is a point of V, and x is a generic point of G over $k(P)$ then the map $x \to xP$ establishes a birational biholomorphic correspondence between G and V. A homogeneous space V defined over k may of course not have a rational point over k. The search for conditions under which it has such points is an interesting diophantine problem.

In the example of the factor group above, the coset H_u is in fact a principal homogeneous space for H, defined over $k(v)$.

One can recover a group variety from birational data in the following manner.

Let V be an arbitrary variety, and suppose we are given a *normal law of composition*. By this we mean a rational map $f: V \times V \to V$ which is generically surjective, and such that if u, v are two independent generic points of V over a field of definition k for f, then $w = f(u, v)$ is a generic point of V over k, and $k(u, v) = k(v, w) = k(u, w)$. In addition, f is assumed to be generically associative, i.e., if u, v, w are three independent generic points of V over k, then

$$f(u, f(v, w)) = f(f(u, v), w).$$

We denote $f(u, v)$ by uv. If U is a variety birationally equivalent to V, and if $T: V \to U$ is a birational transformation, then we can obviously define a law of composition on U by the formula

$$T(v)T(u) = T(w).$$

We say that this law is obtained by *transferring* that of V. A fundamental theorem then asserts that *if V and its normal law f are defined over k, there exists a group variety G also defined over*

k, such that the law of composition on G is obtained by transferring that of V. This group G is uniquely determined up to a birational isomorphism.

This uniqueness property is an immediate consequence of the following remarks which are extremely useful in handling group varieties.

Let $\lambda : G \to G'$ be a rational map of a group variety into another one, and assume that λ satisfies

$$\lambda(xy) = \lambda(x)\lambda(y)$$

whenever x, y are independent generic points of G. We shall then say that λ is a *generic homomorphism. It then follows that λ is everywhere defined, is a homomorphism, and that $\lambda(G)$ is a group subvariety of G'.* Indeed, we can write $\lambda(x) = \lambda(xy)\lambda(y)^{-1}$. For any x, we take y generic. Then xy and y are generic, and this shows that λ is defined at x. From this we conclude that λ is a homomorphism. Let H' be the closure of $\lambda(G)$ in G' for the Zariski topology. Then $\lambda(G)$ contains a non-empty open subset of H'. Since H' is the closure of an abstract subgroup of G', it is a subgroup of G', and the cosets of $\lambda(G)$ contain a non-empty open subset of H'. This can happen only if $\lambda(G) = H'$.

We finish this paragraph by stating an important property of commutative groups.

Let G be a commutative group variety. Let $\mathfrak{a}$ be a cycle of dimension 0 on G. It is a formal sum of points, which we write

$$\mathfrak{a} = \sum n_i(x_i).$$

Writing the law of composition on G additively, we can take the sum of the points x_i on G, each one taken n_i times. We thus obtain a point of G which will be denoted by $S(\mathfrak{a})$. This sum will be written without parentheses, to distinguish it from the formal sum above. Thus we have

$$S(\mathfrak{a}) = \sum n_i \cdot x_i = \sum n_i x_i.$$

In this notation, if x, y are two points of G, then $(x) + (y)$ is the 0-cycle of degree 2 having x, y as components with multiplicity 1, while $x + y$ is the sum on G of x and y.

Let k be a field of definition for G. The *fundamental theorem on symmetric functions* then asserts that *if* $\mathfrak{a}$ *is a 0-cycle of* G, *rational over* k, *then the point* $S(\mathfrak{a})$ *is rational over* k.

Of course, this is a special case of a more general theorem concerning arbitrary symmetric functions ([85] Th. 1), but the above statement will suffice for this book. It is obvious in the case where all the points of $\mathfrak{a}$ are rational over a separable extension of k. Indeed, the composition law of G being defined over k, for every automorphism σ of the algebraic closure of k leaving k fixed, we have

$$(S(\mathfrak{a}))^\sigma = S(\mathfrak{a}^\sigma) = S(\mathfrak{a}).$$

This shows that in general, $S(\mathfrak{a})$ is purely inseparable over k. The proof in this case is pure technique in characteristic p.

Left $f: U \to G$ be a rational map of a variety into the commutative group variety G. Let $\mathfrak{a}$ be a 0-cycle on U, and assume that f is defined at all the points of $\mathfrak{a}$. Then $f(\mathfrak{a})$ is a cycle on G: If $\mathfrak{a} = \sum n_i(P_i)$, then $f(\mathfrak{a}) = \sum n_i(f(P_i))$. Furthermore, if f is defined over k, and if $\mathfrak{a}$ is rational over k, then $f(\mathfrak{a})$ is rational over k, because

$$f(\mathfrak{a}) = \mathrm{pr}_2[\Gamma_f \cdot (\mathfrak{a} \times G)].$$

It follows that $S(f(\mathfrak{a}))$ is a point of G, rational over k. We shall denote it by $S_f(\mathfrak{a})$.

§ 2. *Intersections and Pontrjagin products*

We shall give here special formulas concerning intersections on group varieties. They show how certain operations can be defined in terms of intersection theory.

PROPOSITION 1. *Let* G *be a group variety,* V *a subvariety of* G, *both defined over* k. *Let* (u, x) *be independent generic points of* G, V *over* k. *Let* $\bar{V}$ *be the locus of* (u, ux) *over* k, $((u, u + x)$ *if* G *is commutative*). *Then we have*

$$\bar{V} \cdot (u \times G) = u \times V_u.$$

Proof: We need but to apply F—VII$_6$ Th. 12.

We shall denote by $s_n : G \times \ldots \times G \to G$ the rational map of the product of G with itself n times obtained by the formula $s_n(u_1, \ldots, u_n) = u_1 \ldots u_n$. If G is commutative, then s_n is a homomorphism, which will be called the *sum*. In the non-commutative case, we say it is the *product*. Its graph will be denoted by S_n.

PROPOSITION 2. *Let $s_2 : G \times G \to G$ be the product, and V a subvariety of G. Let (u, x) be as in Proposition 1. Then the cycle*

$$s_2^{-1}(V) = \mathrm{pr}_{12}[S_2 \cdot (G \times G \times V)]$$

is a variety, which is the locus of $(u, u^{-1}x)$ over k, and we have

$$s_2^{-1}(V) \cdot (u \times G) = u \times u^{-1}V$$

or in the additive case, $u \times V_{-u}$.

Proof: Every point (a, b, c) of $S_2 \cap (G \times G \times V)$ is such that $ab = c$ and c is in V. We see therefore that the support of $s_2^{-1}(V)$ is a variety, locus of the point $(u, u^{-1}x)$. The single component of $S_2 \cdot (G \times G \times V)$ has multiplicity 1, according to F—VII_6 Th. 17. Since s_2 is everywhere defined on $G \times G$, the projection on the first two factors conserves this multiplicity.

Note particularly the sign — in the intersection

$$s_2^{-1}(V) \cdot (u \times G) = u \times V_{-u}.$$

We shall now define the Pontrjagin products. Let V, W be two subvarieties of G. We denote by $V \otimes W$ their set-theoretic product on G, or if G is commutative, by $V \oplus W$ or $V + W$. If x, y are two independent generic points of V, W over a field k, then by definition, $V \otimes W$ is the locus of xy over k. We have a rational map $F : V \times W \to V \otimes W$ induced by s_2, and we shall denote the degree of F by $d(V, W)$ if it is finite, and by 0 otherwise. We thus have $d(V, W) = \nu(F)$.

PROPOSITION 3. *Let V, W be two subvarieties of G. Then*

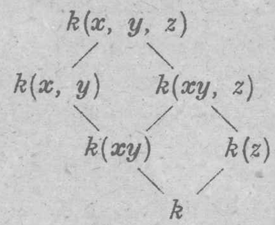
$$\mathrm{pr}_3[S_2 \cdot (V \times W \times G)] = d(V, W)(V \otimes W).$$

Proof: Since s_2 is everywhere defined, $S_2 \cdot (V \times W \times G)$ has one component with multiplicity 1 by F—VII_6 Th. 17. Our proposition is then a consequence of the definition of the projection.

The cycle $d(V, W)(V \otimes W)$ will be denoted by $V * W$. We have $V * W = 0$ if and only if the dimension of $V \otimes W$ is smaller than $\dim V + \dim W$. We shall say that $V \otimes W$, or $V * W$, is the *Pontrjagin product* of V and W. It will always be clear from the context whether we mean the set theoretic product, or the cycle.

If V is a point $a \in G$, then $V \otimes W = W_a$ is the translation of W by a.

The Pontrjagin product is associative. In order to see this, let U, V, W be three subvarieties of G, defined over k, and let x, y, z be three independent generic points of U, V, W over k. It is clear that $(U \otimes V) \otimes W = U \otimes (V \otimes W)$, this variety being the locus of xyz over k. On the other hand, if we put $d = d(U, V)$ and $e = d(U \otimes V, W)$, then $de = [k(x, y, z) : k(xyz)]$ if this degree is finite, and 0 otherwise.



Indeed, $k(x, y)$ and $k(z)$ are linearly disjoint over k, and hence $[k(x, y) : k(xy)] = [k(x, y, z) : k(xy, z)]$. Our assertion is then obvious, taking into account the inclusion

$$k(xyz) \subset k(xy, z) \subset k(x, y, z).$$

We have thus shown that

$$U * (V * W) = (U * V) * W,$$

and that the Pontrjagin product is associative from the point of view of intersection theory.

Of course, we can define the symbol $d(V_1, \ldots, V_m)$ for several subvarieties of G: It is the degree of the rational map of the