On 1-dimensional Group Variety

Abstract

We discuss abelian variety and use it to generalize the concept of elliptic curve we discussed in the class. We state some of the basic properties of abelian variety and in particular 1-dimensional abelian variety. The main result of this report is to show that elliptic curve is that the only 1-dimensional abelian variety.

1. Introduction

The main purpose of this paper is to characterize elliptic curve. In the class, we discuss the properties of elliptic curves, especially rational points on elliptic curves where we define elliptic curves to be curves on projective spaces over complex numbers or finite fields which is the vanishing set of homogeneous polynomial of degree 3. The main tool we use to study elliptic curve is that we define a group structure on all the points of an non-singular elliptic curve of which rational points are a subset. We also show that the group is isomorphic to torus. We also see that on a singular elliptic curve, we can define a group structure on all points except the points of singularity. We see that the fact that non-singular elliptic curve have a everywhere defined group structure make it different from singular elliptic curves. For example, the rational points on non-singular elliptic curves are finitely generated but it is not true for singular elliptic curves. As a result, we would like to know if non-singular elliptic curves are the only curves with a group structure for all points on the curve. The purpose of this paper is to show that in fact, this characterized elliptic curves. In this paper, we study some property of group variety and generalize concept of curves to be 1-dimensional group variety. In this more generalized treatment, we give a new definition of elliptic curves which is equivalent to the old definition if we restrict ourselves to the special case we considered in the class. Then we end our paper with the main theorem that elliptic curves is the only complete 1-dimensional group variety, which if we restrict ourself to curve on complex numbers, will implies that torus is the only compact curve with (everywhere defined) group structure.

The organization of the paper is as follows. In the second section, we introduce the notion of variety following the approach of Hartshorne [2]. In third section, we discuss some basic properties of group variety which are varieties with a group structure following Serge Lang's book [1]. Afterward, we spend the rest of paper on curve, which is 1-dimensional group variety. In the fourth section, we introduce the divisors on a 1-dimensional variety and use it to define the genus of a curve which is a important invariant of curve. In the fifth section, we construct. the Jacobi variety for a curve. In the the last section, we use the universal property of Jacobi variety for a curve to prove that elliptic curve is the only 1-dimensional abelian variety.

Throughout the paper the underlying field K is assumed to be of characteristic zero and is algebraically closed. We will use the notation A^n_K for the direct sum of n copy of K.

2. Algebraic Variety

In this section, we define what is an algebraic variety. First, we consider the special case of affine variety. Roughly speaking, an affine variety is the space common roots of a collection of polynomials of n variables. However, to be precise, we need to specify what kind of topology we have one the space and what kind of maps we allow between the spaces.

Let R be the polynomial ring over K with n variable.

Definition 1. Given an ideal I of R, define the vanishing set $\mathbb{V}(I)$ to be

$$\mathbb{V}(I) = \{x \in A_K^n \| f(x) = 0 \forall f \in I\} \tag{1}$$

It is not hard to see that if we let I range from all ideals of R $\{\mathbb{V}(I)\}$ satisfies the axiom of closed subset for a topology and forms a topology on A_K^n. More precisely, we can show that:

(i) A_K^n and ϕ are of the form $\mathbb{V}(I)$ for some I

$$\mathbb{V}(\{0\}) = A_K^n \tag{2}$$

$$\mathbb{V}(R) = \emptyset \tag{3}$$

(ii)the collection is closed under finite union since

$$\mathbb{V}(I) \bigcup \mathbb{V}(I) = \mathbb{V}(IJ) \tag{4}$$

(iii) the collection is closed under arbitrary intersection since

$$\bigcap_{s \in S} \mathbb{V}(I_s) = \mathbb{V}(I) \tag{5}$$

where I is the ideal generated by $\{I_s\}$.

Definition 2. The Zariski topology of A_K^n is the topological space A_K^n with closed sets $\{\mathbb{V}(I)\}$

Definition 3. An affine variety is a subset $\mathbb{V}(I)$ of A_K^n whose topology is induced by Zariski topology of A_K^n.

Now that we define the topology of affine variety, we want to specify the maps between affine variety we want to consider. Notice that we define the variety and the topology on it by vanishing set of collection of polynomials. As a result, we would like to restrict maps between affine varieties to be polynomial maps.

Definition 4. Given a affine variety V which is contained in A_K^n for some n, a map $G : V \mapsto K$ is regular if and only if it is restriction of a polynomial $F : A_K^n \mapsto K$

Definition 5. Given two affine variety U and V, a map $F : U \mapsto V$ is regular if and only if for every regular map $G : V \mapsto K$, the composition $F \cdot G$ is regular.

Notice that regular maps are continuous maps under Zariski topology.

Similarly, we can define regular maps.

Definition 6. Given a affine variety V which is contained in A_K^n for some n, a map $G : V \mapsto K$ is regular if and only if around every point p of V, the map is restriction of it is restriction of a map $F : U \mapsto K$, U open set of A_K^n contains p and F is f_1/f_2 where f_i are polynomials.

Definition 7. We say that a map F between two affine varieties X and Y is rational if and only for any ration for every rational map $G : V \mapsto K$, the composition $G \cdot F$ is rational.

We defined the affine varieties as above. Now we are ready to define algebraic varieties, which roughly speaking, are spaces that are locally the same as affine variety. The idea is similar to that of gluing Euclidean spaces together to get manifolds.

Definition 8. A topological space X is an algebraic variety if there exists an index set I and an open covering of X by $\{U_i\}$, $i \in I$ and affine varieties $\{V_i\}$ and homeomorphisms $\{\phi_i : V_i \mapsto U_i\}$ such that on intersection U_{ij} of U_i and U_j

$$\phi_j^{-1}\phi_i : \phi_i^{-1}(U_{ij}) \mapsto \phi_j^{-1}(U_{ij}) \tag{6}$$

are regular functions. We say that U_i are the open affine subset of X.

Definition 9. Given two algebraic varieties X and Y, a map $F : X \mapsto Y$ is a rational morphism if for every open affine U_i of X and U_j' of Y so that $F(U_i)$ is contained in U_j' the composition of ϕ_i, F and $\phi_j^{'-1}$ between affine variety V_i and V_j' is rational map of affine variety.

Example

(i)As an example, we may notice that the projective plane P_K^2 is an algebraic variety since it is covered by three copy of A_K^2 where the i-th copy is the subset of P_K^2 whose i-th coordinate is non-zero.

(ii) An elliptic curve on P_K^2 is an algebraic variety since it is covered by three subset that are affine variety defined by the vanishing point of a degree 3 polynomial of two variables.

Definition 10. An algebraic variety is irreducible if it cannot be expressed as union of proper closed subset of itself.

We will state the following lemma without proof:

Lemma 1. *Product of two algebraic varieties is an algebraic variety*

3. Group Variety and Abelian Variety

We show in class that we can define a group structure on non-singular elliptic curves. We see in the previous section that elliptic curves are special examples of algebraic variety. The purpose of this section is to generalize this idea to arbitrary algebraic variety.

Recall that a group is a set G with an associative operation $G \times G \mapsto G$ so that the unit and inverse element exists.

A group variety is an irreducible algebraic variety with a group structure such that the group structure is compatible with the structure of variety. Moreover, we have the following definition:

Definition 11. A group variety is an irreducible algebraic variety A with a rational map $F : A \times A \mapsto A$ such that F gives a group structure on A. In addition we require that the map

$$\psi : A \mapsto A \qquad x \mapsto x^{-1} \tag{7}$$

is an rational map from A to A

Lemma 2. *A group variety is non-singular.*

Proof. Given $g \in A$, define the map T_g from A to A to be multiplied by g from the left. T_g and $T_{g^{-1}}$ are isomorphism of an open set around the identity and an open set around g. Thus, if g is singular if and only if identity is. However, we can not have a algebraic variety which is everywhere singular. Thus A group variety is non-singular. □

Definition 12. We say that a group variety is commutative if the group is a commutative group

Example A non-singular elliptic curve (in the sense we discussed in class) is a example of a group variety of dimension 1 since we defined a group structure on the curve that is defined by quotient of polynomials. Notice that we defined similar structure on a singular elliptic curve but the product is defined only for non-singular points of the curve. Thus, non-singular points on a singular elliptic curve also form a group variety. The two examples here are distinguished by the fact that a non-singular elliptic curve is a complete space (under the induced topology of Zariski topology) but the non-singular points on a singular elliptic curve is not a complete space. We see in the class that the properties of non-singular elliptic curve and singular elliptic are very different. As a result, we have the following definition of abelian variety.

Definition 13. A group variety A is an abelian variety if A is complete as a variety.

At first, the word "abelian" might seems to be confusing since we usually use abelian to mean that a group is commutative. However, this is somewhat justified by the following theorem:

Theorem 3. *(Theorem 1, Ch. 2* [1]*) An abelian variety A is a commutative group variety.*

We omit the proof of the theorem.

4. Divisors and genus of curves

We said previously that the main topics of interests is 1-dimensional group variety. In the following of the report, we call "a 1-dimensional group variety" a curve. Notice that if the underlying field is the complex number, then a curve is of complex dimension 1 or equivalently real dimension 2. In fact, we show in the class in the class that an elliptic curve over $\mathbb{C}$ is the torus. Moreover, we know that we can associate a bi-rational invariant number g, called the genus, to each affine curve over $\mathbb{C}$ which if visualized geometrically is the number if holes of the curves. For example, a torus is of genus 1. Genus is an important number associated to affine curve over $\mathbb{C}$ since we know that it classify the affine curve over $\mathbb{C}$. The purpose of this section is to generalize the definition of genus to all curves using divisors on curves.

First, we will state a theorem from [2] which allow us to consider only curves that are subset of projective spaces P^n.

Theorem 4. *(Corollary 3.6. Ch. 6* [2]*) Every curve can be embedded into P^3_K*

We will first define the a divisor on a curve C

Definition 14. A divisor D on a curve C is a formal sum of the form

$$\sum_{p_i \in C} n_i p_i$$

where all but finitely many n_i are zero. If we have two divisor

$$D_i = \sum_{pj \in C} n_{j,i} p_j, \qquad i = 1, 2$$

then we can naturally define the sum of the two divisors to be

$$D_1 + D_2 = \sum_{p_i \in C} (n_{i,1} + n_{i,2}) p_i \tag{8}$$

In this sense, the sets of all divisors D of C is the free abelian group generated by points of the curve C

In particular, 0 is a divisor. We can define the degree of an divisor to be:

Definition 15. The degree of a divisor $D$is defined by the following equation

$$deg(D) = \sum n_i \qquad D = \sum_{p_i \in C} n_i p_i \tag{9}$$

Definition 16. Given a rational function f on C, we want to associate a divisors of C to f. Notice that locally, f is defined by a quotient of two polynomials. Thus, locally, around a point $p \in C$, we have $f = g_1/g_2$ where g_i are polynomials. Thus, if $g_1(p) = 0$ we can define the multiplicity of f at p to be the multiplicity of the polynomial g_1 at p, if $g_2(p) = 0$ we define it to be negative of multiplicity of the polynomial g_2 at p and we define the multiplicity to be 0 otherwise. Denote by $v_p(f)$ the multiplicity of f at p.

We have the following lemma

Lemma 5. *For all but finitely many points $p \in C$, $v_p(f) = 0$ if f is not 0.*

Since only finite points have non-zero multiplicity for a given function f we can associate a divisor to f as follows.

Definition 17. Given a rational function f on C,

$$div(f) = \sum_{p \in C} v_p(f) p \tag{10}$$

We have the following lemma

Lemma 6. *Divisors correspond to a rational function is of degree 0. That is*

$$deg(div(f)) = 0 \tag{11}$$

Definition 18. We say that two divisors D_1 and D_2 are linear dependent if there exists a rational function f such that

$$D_1 - D_2 = div(f) \tag{12}$$

It follows that linear dependent divisors have the same degree

We can define an ordering on the set of divisor, by

Definition 19. $D_1 \geq D_2$ if $n_{p,1} \geq n_{p,2}$ for every $p \in C$. We say that a divisor D is positive if $D \geq 0$ and D is not 0.

Conversely, to every divisors D, we can associate a subspace of rational function on C denoted by $L(D)$.

Definition 20. $L(D)$ consists of function 0 alone with all functions f so that

$$div(f) + D \geq 0 \tag{13}$$

as divisors on C

It is straight-forward to see the following lemma:

Lemma 7. *L(D) is a K-vector space.*

Thus we can define

$$l(D) = dim_K(L(D)) \tag{14}$$

We have the following theorem:

Theorem 8. *(Ch. 3, theorem 5* [3]*) $L(D)$ is finite dimensional vector space, i.e, $l(D)$ is finite.*

We would like to relate differential 1-forms on C with divisors on C. Given a differential forms ω, locally in a affine open affine set U_i of C, it can be expressed as

$$\omega = g_i * dx_i \tag{15}$$

Moreover, on intersection of two sets U_i and U_j, g_i and g_j is related by the $det(x_i/dx_j)$ which is non-zero since this is the transformation function on the intersection. As a result, g_i and g_j have same multiplicity on points $p \in U_{ij}$. As a result, ω defines a divisor on C. There is one form ω that generates generates 1-form module exact 1-forms. We call the divisor K_C correspond to such ω to be canonical divisor of C . And we define the genus of C to be $l(K_C)$. which is finite since for every D, $l(D)$ is finite.

Example Although this definition of genus seems to be very different to what we had for real surfaces. However, they are in fact the same definition. For example, in chapter 6.4 [3] it is proved that a curve in projective plane defined by homogeneous polynomial of degree d has genus $(d-1)(d-2)/2$ in the new definition. In particular, elliptic (torus) is defined by homogeneous polynomial of degree 3 thus has genus 1 as we expected.

Since when they underlying field is $\mathbb{C}$, elliptic curve is the (unique) curve of genus 1 and we know that an elliptic curve is an abelian variety. Thus, it is reasonable for us to generalize elliptic curve in the following way:

Definition 21. An elliptic curve is an 1-dimensional abelian variety of genus 1.

We would like to show that, in fact, a 1-dimensional abelian variety is an elliptic curve. That is, we want to show that an 1-dimensional abelian variety always has genus 1.

Although this might seems to be redundant, this conclusion is useful. For example, this shows that there does not exist a everywhere defined group structure on double torus since it has genus 2. More generally, since the only complex curve of genus 1 is torus, thus the only complex curve with a everywhere defined group structure is a non-singular torus.

5. Jacobi variety for curves

We will construct the Jacobi variety for curves(group variety of dimension 1) in this section and use it to prove that a 1-dimensional abelian variety is an elliptic curve. We follow the construction in section 1 chapter 2 of [1]

Before we do the construction, let us first see the universal property that characterized the Jacobi variety for a curve.

Given a curve C, the Jacobi variety is an abelian variety J with a rational map $F : C \mapsto J$ having the universal property that for any ration map from C to abelian varieties factor through F, that is, for any abelian variety V and rational map $g : C \mapsto V$, there exists an unique homomorphism of abelian variety $h : J \mapsto V$ such that $g = h(F)$

Notice that given a curve C, the Jacobi variety of C, if exists will be unique, since if there are two abelian variety J_1 and J_2 with $F_i : C \mapsto J_i$ both have the universal property. Then using the universal property for the pair (F_1, J_1) to $F_2 : C \mapsto J_2$, we have a homomorphism from $\alpha_1 : J_2 \mapsto J_1$ with $F_2 = \alpha_1(F_1)$. Similarly there are $\alpha_2 : J_1 \mapsto J_2$ with $F_1 = \alpha_2(F_2)$. Then notice that

$$F_1 = \alpha_2(\alpha_1(F_1)) \tag{16}$$

However, apply universal property for the pair (F_1, J_1) to $F_1 : C \mapsto J_1$, we conclude that $\alpha_2(\alpha_1)$ is identity map on J_1. Similarly $\alpha_1(\alpha_2)$ is identity map on J_2. Thus α_2 and α_1 are inverse isomorphism to each other, so we have that J_1 is isomorphic to J_2. Thus we proved the uniqueness. As a result, given a curve C, we can, in fact just take the universal property as the definition of Jacobi variety. We want to show that Jacobi variety for any curve exists. We will construct it as follows.

Fix a curve C with genus g We will have state the following lemma that is important to the construction:

Lemma 9. *(Lemma 5 Ch. 2* [1]*) Suppose we have a curve C of genus g and a divisor D of degree 0 on C. For any positive divisor p of degree g, that is*

$$p = \sum_{i=1}^{g} P_i \tag{17}$$

There is an unique positive divisor q such that q is linear dependent to $a + p$ In particular, since q is also positive divisor of degree g, we have

$$q = \sum_{i=1}^{g} Q_i \tag{18}$$

The proof of the above lemma use the following equation for a divisor b on C

$$l(b) = deg(b) + 1 - g + \delta(b) \tag{19}$$

where

$$\delta(b) = l(K_c - b) \tag{20}$$

The equation is resulted from Riemann-Roch Theorem but we will not prove the lemma or Riemann-Roch Theorem here.

However, we will use the lemma to construct a group structure on the set J of positive divisor of C with degree g, which as a set is C^g, the ordinary product of g copies of C.

Fix an element $\mathfrak{O} \in J$. For two elements p and q of J, applying Lemma (9) where p is a positive divisor with degree g and $q - \mathfrak{O}$ is an divisor of degree 0, we conclude that there is a unique divisor m of degree g linear dependent to $p + q - \mathfrak{O}$. By definition, we have $m \in J$. Thus since m is unique, we define the product of p and q to be m. Thus we define a operation

$$\oplus : J \times J \mapsto J \tag{21}$$

we use the notation $\oplus$ so that we do not confuse it with the ordinary addition of divisors.

We claim that $(J, \oplus)$ is a commutative group.

First, clearly, $\mathfrak{O}$ is the identity since $p + \mathfrak{O} - \mathfrak{O}$ is p for any p and thus

$$p \oplus \mathfrak{O} = p$$

Given three elements of J, p_1, p_2 and p_3, notice that both $(p_1 \oplus p_2) \oplus p_3$ and $p_1 \oplus (p_2 \oplus p_3)$ are linearly dependent to

$$p_1 + p_2 + p_3 - 2\mathfrak{O}$$

and thus we have the associativity that

$$(p_1 \oplus p_2) \oplus p_3 = p_1 \oplus (p_2 \oplus p_3)$$

The inverse of an element p exists since by Lemma (9), there is unique element q of J linear dependent to

$$(\mathfrak{O} - p) + \mathfrak{O}$$

thus $(p - \mathfrak{O}) + q$ is linearly dependent to $\mathfrak{O}$. Thus

$$p \oplus q = \mathfrak{O}$$

$\oplus$ is commutative since given p and q, both $p \oplus q$ and $q \oplus p$ are linear dependent to $p + q - \mathfrak{O}$, and thus

$$p \oplus q = q \oplus p$$

Also, we have the map $F : C \mapsto V$ defined by

$$F = id \times id \times \cdots \times id$$

where id is the identity map from C to C.

In fact, J is a abelian variety of dimension g and that the map F from C to J satisfy the universal property of Jacobi variety. We do not prove it in this report and refer the reader to chapter 2 of [1]. By the uniqueness of Jacobi variety variety of curve, this is the Jacobi variety of C and we conclude the following theorem:

Theorem 10. *Given a curve C of genus g, the Jacobi variety J of C is of dimension g.*

6. Main Theorem of Elliptic Curve

Now, it is very easy for us prove the following theorem

Theorem 11. *Every 1-dimensional abelian variety is of genus* 1*, that is, an elliptic curve.*

Proof. Given a 1-dimensional abelian variety V of genus g, V is a curve with genus g and thus we conclude from Theorem (10) that the Jacobi variety of V is g-dimensional. However, since V is itself abelian, we can easily see that the identity map $id : V \mapsto V$ has the universal property, i.e. V with identity map is the Jacobi variety of V and by definition, V is 1-dimensional. Thus $g = 1$ and V is an elliptic curve. □

References

[1] Abelian Varieties, Serge Lang, New York, Springer-Verlag, 1983.

[2] Algebraic Geometry. Hartshorne, New York, Springer-Verlag, c1977

[3] Basic Algebraic Geometry, Shafarevich, Now York, Spinger-Verlag, c1994