Real abelian varieties with complex multiplication

VRIJE UNIVERSITEIT

Real abelian varieties with complex multiplication

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor aan
de Vrije Universiteit te Amsterdam,
op gezag van de rector magnificus
dr. C. Datema,
hoogleraar aan de faculteit der letteren,
in het openbaar te verdedigen
ten overstaan van de promotiecommissie
van de faculteit der wiskunde en informatica
op dinsdag 8 september 1992 te 13.30 uur
in het hoofdgebouw van de universiteit, De Boelelaan 1105

door

Johannes Huisman
geboren te Hellevoetsluis

Krips Repro Meppel
1992

Promotor:	prof.dr. J. Bochnak
Copromotor:	prof.dr. F. Oort
Referent:	prof.dr. E. Becker

Voorwoord

Dit proefschrift is voortgekomen uit het onderzoek dat ik als assistent in opleiding bij de faculteit der Wiskunde en Informatica van de Vrije Universiteit te Amsterdam onder leiding van J. Bochnak gedaan heb. Hij was het die mij meetkunde, in het bijzonder reële algebraïsche meetkunde, leerde. Ik wil hem daarvoor uitdrukkelijk bedanken. Verder denk ik met veel plezier terug aan de enthousiaste wijze waarop hij met mij discussiëerde over wiskunde en aan de vrijheid die hij mij gaf bij de keuze van het onderwerp van mijn onderzoek. Vooral dat laatste heeft er veel aan bijgedragen dat ik het, toen nog maagdelijke, terrein van de onderliggende reële algebraïsche structuur van algebraïsche variëteiten over $\mathbb{C}$ betrad.

Verder wil ik F. Oort bedanken voor de grote belangstelling die hij in mijn onderzoek heeft getoond. Onze plezierige gesprekken gingen, vooral in het begin, gepaard met hevige spraakverwarringen (wat die gesprekken overigens niet minder plezierig maakte) als gevolg van het feit dat er twee verwante èn totaal verschillende vakgebieden bij betrokken waren. De invloed op dit proefschrift die hiervan uitging is groot. Voorts bedank ik hem voor de suggestie, na het bestuderen van de onderliggende reële algebraïsche structuur van elliptische krommen over $\mathbb{C}$, die structuur van abelse variëteiten over $\mathbb{C}$ met voldoende veel complexe vermenigvuldigingen te bestuderen.

Ik wil E. Becker bedanken voor het feit dat hij referent van dit proefschrift wilde zijn en voor het geduld dat hij had bij de vertraging die ontstond tijdens de voltooiing van het manuscript.

Ik bedank de faculteit der Wiskunde en Informatica voor de aangename sfeer waarin ik heb kunnen werken, en daarbij denk ik ook aan het AIO-boekenbudget en de subsidieregeling voor de aanschaf van computer-apparatuur.

Voorts denk ik met veel plezier terug aan de animerende discussies die ik had met Ira Helsloot, en dan vooral de discussies ten tijde van ons 2-koppig seminarium.

Jeroen Warmerdam bedank ik voor de buitengewoon zorgvuldige wijze, die hem zo eigen is, waarop hij het manuscript doorgelezen heeft. Het is daarbij zeker niet beperkt gebleven tot “type-checking”!

Johan Huisman
Amsterdam, juli 1992

Contents

Introduction

In real algebraic geometry one essentially studies affine real algebraic varieties. (Projective real algebraic varieties are affine [2, Théorème 3.4.4].) An affine real algebraic variety is a subset V of $\mathbb{R}^n$ given by polynomial equations. An interesting problem is the question of realizability of $\mathbb{Z}/2\mathbb{Z}$-homology classes by real algebraic subvarieties. More precisely, let $V \subseteq \mathbb{R}^n$ be an affine real algebraic variety which is compact with respect to the strong topology (=Euclidean topology) and let

$$c \in H_i(V, \mathbb{Z}/2\mathbb{Z})$$

be an element of the i^{th} homology group of V with coefficients in $\mathbb{Z}/2\mathbb{Z}$. Then, c is realizable by a real algebraic subvariety of V if there exists an i-dimensional real algebraic subvariety W of V such that the $\mathbb{Z}/2\mathbb{Z}$-homology class

$$[W] \in H_i(V, \mathbb{Z}/2\mathbb{Z})$$

determined by W [2, p. 235] is equal to c. The subgroup of elements of $H_i(V, \mathbb{Z}/2\mathbb{Z})$ that are realizable by a real algebraic subvariety is denoted by

$$H_i^{alg}(V, \mathbb{Z}/2\mathbb{Z}).$$

The problem then is to determine this group.

We will solve this problem in the case $i = \dim V - 1$ (cf. Theorem 89) for a large class of affine real algebraic varieties, namely the class of real abelian varieties. (A real abelian variety is a real algebraic group admitting a complete complexification which is itself an algebraic group.) In particular, we will prove in Chapter 2, among other things, that

$$(0) \neq H_{d-1}^{alg}(V, \mathbb{Z}/2\mathbb{Z}) \neq H_{d-1}(V, \mathbb{Z}/2\mathbb{Z}),$$

for any real abelian variety V of dimension $d > 1$, which is not connected with respect to the strong topology (Corollary 93).

Other questions which we will study are concerned with the underlying real algebraic structure of algebraic varieties over $\mathbb{C}$. Briefly, if X is an algebraic variety over $\mathbb{C}$ then, using the identification of $\mathbb{C}^n$ with $\mathbb{R}^{2n}$, there exists a canonical structure of a real algebraic variety on X, called the underlying real algebraic structure of X and denoted by ${}_{\mathbb{R}}X$. Obviously, the dimension of the real algebraic variety ${}_{\mathbb{R}}X$ is twice the dimension of X, that is, $\dim {}_{\mathbb{R}}X = 2 \dim X$.

In the last section of Chapter 2 we will study realizability of $\mathbb{Z}/2\mathbb{Z}$-homology classes of the underlying real algebraic structure of elliptic curves over $\mathbb{C}$ with complex multiplication, i.e. we will study the group $H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z})$, where E is a elliptic curve over $\mathbb{C}$ such that its ring of endomorphisms $\mathrm{End}(E)$ is not equal to $\mathbb{Z}$. In [6] it has been proved that the $\mathbb{Z}/2\mathbb{Z}$-dimension of $H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z})$ is equal to 2 if and only if the discriminant $\mathfrak{d}$ of $\mathrm{End}(E)$ is odd, is equal to 1 if $\mathfrak{d}$ is even and $\mathfrak{d} \neq 8\mathfrak{d}$, with d odd, and is equal to 0 or 1 in the remaining cases (that is, $\mathfrak{d} = 8\mathfrak{d}$, with d odd). The question rose whether the $\mathbb{Z}/2\mathbb{Z}$-dimension of $H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z})$ is equal to 0 or to 1 in these remaining cases. In Section 2.7 we will answer this question and present a different proof of the results mentioned above. More precisely, we will show that

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z}) = \begin{cases} 2, & \text{if } \mathfrak{d} \text{ is odd}, \\ 1, & \text{if } \mathfrak{d} \text{ is even}, \end{cases}$$

whenever E is an elliptic curve over $\mathbb{C}$ with complex multiplication. Particularly interesting is the fact that in the case $\mathfrak{d} = 8\mathfrak{d}$, with d odd, the nonzero homology class in $H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z})$ is not realizable by a real elliptic curve, while in the other cases all nonzero homology classes in $H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z})$ are realizable by a real elliptic curve.

Another interesting problem is classification of the underlying real algebraic structure of algebraic varieties over $\mathbb{C}$. The case of elliptic curves over $\mathbb{C}$ has been solved [14]. In particular, for any elliptic curve E over $\mathbb{C}$ with complex multiplication the following is proved in [14]. The number $\rho({}_{\mathbb{R}}E)$ of (isomorphism classes of) algebraic varieties F over $\mathbb{C}$ such that ${}_{\mathbb{R}}F$ is isomorphic to ${}_{\mathbb{R}}E$ is equal to the class number $h(\mathrm{End}(E))$ of the ring $\mathrm{End}(E)$. In Chapter 3, this will be generalized to abelian varieties over $\mathbb{C}$ having sufficiently many complex multiplications (Theorem 137).

A related problem is the problem of the product structure of a simple abelian variety over $\mathbb{C}$. Let us explain this. It is well known that, for any abelian variety X over $\mathbb{C}$ of dimension n, the set of complex points $X(\mathbb{C})$ of X is topologically isomorphic to $(S^1)^{2n}$, where S^1 is the topological circle. Hence, at least topologically, X is the product of two real algebraic varieties. The problem of the product structure of a simple abelian variety X over $\mathbb{C}$ is the question whether there exist real algebraic varieties X_1 and X_2 of positive dimension, such that

$$_{\mathbb{R}}X \cong X_1 \times X_2,$$

as real algebraic varieties.

The problem of the product structure of elliptic curves over $\mathbb{C}$ has been solved in [5]. There, it is proved that an elliptic curve E over $\mathbb{C}$ has product structure if and only if E has complex multiplication and the discriminant of the ring $\mathrm{End}(E)$ of endomorphisms of E is odd (see Corollary 100). In Chapter 3, we will generalize this to a large class of simple abelian varieties over $\mathbb{C}$ having sufficiently many complex multiplications (Theorem 140).

An important notion in real algebraic geometry is that of a complexification. All our proofs of the statements mentioned above make use of this notion. Classically, a complexification of a real algebraic variety $V \subseteq \mathbb{R}^n$ (or $V \subseteq \mathbb{P}^n(\mathbb{R})$) is the algebraic variety over $\mathbb{C}$ in $\mathbb{C}^n$ (or $\mathbb{P}^n(\mathbb{C})$) given by the same equations as V. In terminology of schemes, a complexification of a real algebraic variety V is just a geometrically reduced separated scheme X over $\mathbb{R}$ of finite type such that the set of real points $X(\mathbb{R})$ of X is isomorphic to V, as a real algebraic variety. We will take the latter characterization as definition of a complexification (see Definition 11). Although a real algebraic variety does not have a canonical complexification in general, we will prove in Chapter 2 that every real algebraic group does have a canonical complexification (Theorem 79).

The fact that the Weil restriction of an irreducible algebraic variety X over $\mathbb{C}$ with respect to the field extension $\mathbb{C}/\mathbb{R}$ is a complexification of the underlying real algebraic structure $_{\mathbb{R}}X$ of X (Theorem 29) will play an important role in the study of the underlying real algebraic structure of algebraic varieties over $\mathbb{C}$.

The reader is refered to the book [2] for more details on real algebraic geometry and to [13] or [24] for more details on algebraic geometry in general.

Conventions and notation

If $\mathcal{C}$ is a category and X and Y are objects in $\mathcal{C}$ then the set of morphisms from X into Y will be denoted by $\mathrm{Hom}_{\mathcal{C}}(X, Y)$, or $\mathrm{Hom}(X, Y)$ when no confusion is likely to occur. If $X = Y$ then this set is denoted by $\mathrm{End}_{\mathcal{C}}(X)$ or $\mathrm{End}(X)$. Furthermore, $X \cong_{\mathcal{C}} Y$ or $X \cong Y$ means X is isomorphic to Y.

An action of a group G on a set X will always be a left action, unless stated otherwise. The set of fixed points of G is denoted by X^G, that is,

$$X^G = \{x \in X \mid \sigma x = x, \text{ for every } \sigma \in G\}.$$

If we also have an action of G on the set Y, then a mapping $f\colon X \to Y$ is called *G-equivariant* if

$$f(\sigma x) = \sigma f(x),$$

for every $x \in X$ and $\sigma \in G$.

A module over a ring will always be a left module, unless stated otherwise.

If $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are locally ringed spaces then, for every morphism $f\colon X \to Y$ of locally ringed spaces, the corresponding morphism of sheaves

$$\mathcal{O}_Y \longrightarrow f_\star \mathcal{O}_X$$

will be denoted by $f^\#$.

We will use the symbol $\restriction$ to denote restriction.

Chapter 1

Generalities

In this chapter we define the notion of a real algebraic variety. This definition is essentially the same as [2, Définition 3.2.11] and has the advantage that, whenever X is a geometrically reduced separated scheme over $\mathbb{R}$ of finite type such that the set of real points $X(\mathbb{R})$ of X is dense in X, the space $X(\mathbb{R})$ together with the restriction of the structure sheaf of X to $X(\mathbb{R})$ is a real algebraic variety (Proposition 8). In Section 1.2 we recall some facts concerning realizability of homology classes by real algebraic subvarieties and in Section 1.3 we recall the basic fact of the theory of descent, which we will need in Section 2.4 and in Section 1.4. The latter section is devoted to the Weil restriction. The last section of this chapter, Section 1.5, is concerned with the underlying real algebraic structure of algebraic varieties over $\mathbb{C}$. In this section it will be proved that the Weil restriction of an irreducible algebraic variety X over $\mathbb{C}$ is a complexification of the underlying real algebraic structure ${}_{\mathbb{R}}X$ of X (Theorem 29).

1.1 Real algebraic geometry vs. algebraic geometry over the reals

Let us define the notion of a real algebraic variety (cf. [2]).

A subset V of the n-fold cartesian product $\mathbb{R}^n$ of $\mathbb{R}$ is an *algebraic set* if there exist polynomials F_i, $i \in I$, in the polynomial ring $\mathbb{R}[X_1, \ldots, X_n]$ such that

$$V = \{x \in \mathbb{R}^n \mid \forall i \in I \colon F_i(x) = 0\}.$$

Clearly, the algebraic subsets of $\mathbb{R}^n$ determine a topology on $\mathbb{R}^n$ such that the closed sets are precisely the algebraic sets. This topology is called the *Zariski topology*. Any algebraic subset V of $\mathbb{R}^n$ will be given the induced topology. Again, this topology is called the Zariski topology.

Let U be an open subset of the algebraic subset V of $\mathbb{R}^n$. A real-valued function $f\colon U \to \mathbb{R}$ will be called *regular* on U if, for every $x \in U$, there exist polynomials $p, q \in \mathbb{R}[X_1, \ldots, X_n]$ such that q does not vanish on a neighbourhood $U' \subseteq U$ of x and

$$f(y) = \frac{p(y)}{q(y)},$$

for every $y \in U'$. Denote the $\mathbb{R}$-algebra of regular functions on U by $\mathcal{R}_V(U)$. Obviously, $\mathcal{R}_V$ is a sheaf on V, the *sheaf of regular functions* on V.

Remark 1. It follows from [2, Proposition 3.2.3] that, whenever $V \subseteq \mathbb{R}^n$ is an algebraic set and U is an open subset of V, for every regular function f on U there exist polynomials $p, q \in \mathbb{R}[X_1, \ldots, X_n]$ such that q does not vanish on U and

$$f(y) = \frac{p(y)}{q(y)},$$

for every $y \in U$. $\square$

Observe that $(V, \mathcal{R}_V)$ is a locally ringed space [13, p. 72] and $\mathcal{R}_V$ is a sheaf of $\mathbb{R}$-algebras. Let us call a locally ringed space $(X, \mathcal{O}_X)$, where $\mathcal{O}_X$ is a sheaf of $\mathbb{R}$-algebras, an $\mathbb{R}$-*space*. If X and Y are $\mathbb{R}$-spaces, a morphism $f\colon X \to Y$ of locally ringed spaces is a *morphism of* $\mathbb{R}$-*spaces* if

$$f^{\#}\colon \mathcal{O}_Y \longrightarrow f_\star \mathcal{O}_X$$

is a morphism of sheaves of $\mathbb{R}$-algebras on Y. With the obvious composition of morphisms, we get the category of $\mathbb{R}$-spaces.

Definition 2. *An* $\mathbb{R}$-*space* X *is an* affine real algebraic variety *if* X *is isomorphic to* $(V, \mathcal{R}_V)$*, for some algebraic set* V*. A* pre-real algebraic variety *is an* $\mathbb{R}$*-space* X *such that there exists a finite open covering* $\{U_i\}$ *of* X *such that the* $\mathbb{R}$*-spaces* $(U_i, \mathcal{O}_X\restriction_{U_i})$ *are affine real algebraic varieties.*

Observe that the category of pre-real algebraic varieties has finite products. Therefore we can define the *diagonal* $\Delta \subseteq X \times X$, if X is a pre-real algebraic variety. Namely, Δ is the image of X under the morphism $<\mathrm{id}_X, \mathrm{id}_X>: X \to X \times X$.

A pre-real algebraic variety X is called *separated* if Δ is closed in $X \times X$.

Definition 3. *A* real algebraic variety *is a separated pre-real algebraic variety. A morphism from a real algebraic variety* X *into a real algebraic variety* Y *is just a morphism from the* $\mathbb{R}$*-space* X *into the* $\mathbb{R}$*-space* Y*. The* dimension *of a real algebraic variety is the Krull dimension of the underlying topological space.*

This definition of a real algebraic variety is only slightly different from [2, Définition 3.2.11]. Fortunately, the two definitions give rise to equivalent categories, as can be seen easily. Moreover, definitions and properties from [2] concerning real algebraic varieties apply to our real algebraic varieties.

Observe that the dimension of a real algebraic variety in the sense of [2] is equal to the dimension in our sense. In particular, if X is an irreducible real algebraic variety, the dimension $\dim X$ of X is equal to the transcendence degree over $\mathbb{R}$ of the function field of X.

Remark 4. Let X be a real algebraic variety. Clearly, every open subset U of X has an induced structure of a real algebraic variety. Furthermore, every closed subset C of X has a unique structure of a real algebraic variety such that the inclusion $i: C \to X$ extends to a morphism of real algebraic varieties. Hence, every locally closed subset Y of X has an induced structure of a real algebraic variety. □

Example 5. An open subset U of an affine real algebraic variety $V \subseteq \mathbb{R}^n$ is affine. Indeed, $V - U$ is closed in $\mathbb{R}^n$. Hence, there is an ideal I of

$\mathbb{R}[X_1,\ldots,X_n]$ which has as vanishing set $V - U$. Since $\mathbb{R}[X_1,\ldots,X_n]$ is Noetherian, there exist $F_1,\ldots,F_m \in I$ which generate I. Put

$$F = \sum_{i=1}^{m} F_i^2.$$

Then,

$$V' = \{(x,t) \in \mathbb{R}^n \times \mathbb{R} \mid x \in V \quad \text{and} \quad tF(x) = 1\}$$

is an affine real algebraic variety isomorphic to U. □

Observe that, if V is an affine real algebraic variety, V has a topology induced by the Euclidean topology, called the *strong topology*. Of course, if X is an arbitrary real algebraic variety then X has a topology generated by the strong topologies on all open affine subsets. Again, this topology is called the strong topology. We will denote this topological space associated to the real algebraic variety X by X_s.

Definition 6. *An* algebraic variety over a field K *is a geometrically reduced, separated scheme over K, which is of finite type over K.*

Let us mention explicitly that, according to Definitions 3 and 6, we have made distinction between "real algebraic varieties" and "algebraic varieties over $\mathbb{R}$".

Remark 7. Suppose X is an algebraic variety over K. An open subset U of X becomes an algebraic variety over K by taking the restriction of the structure sheaf $\mathcal{O}_X$ of X to U. A closed subset of X will always be given the reduced induced closed subscheme structure, when considered as an algebraic variety over K.

Combining these facts, every locally closed subset Y of X has the structure of an algebraic variety over K. Moreover, the inclusion mapping $i\colon Y \to X$ extends to a morphism of algebraic varieties over K. □

If X is a scheme over a field K and L/K is a field extension, then an *L-rational point* of X is a morphism

$$x\colon \operatorname{Spec} L \longrightarrow X$$

of schemes over K. The set of L-rational points of X will be denoted by $X(L)$.

In the special case that $L = K$, the set $X(K)$ of K-rational points can be considered to be a subset of X in a canonical way. For, a K-rational point is a morphism $x\colon \operatorname{Spec} K \to X$ of schemes over K and the image of $(0) \in \operatorname{Spec} K$ is uniquely determined by x.

If X is a scheme over $\mathbb{R}$, let us denote the $\mathbb{R}$-space $(X(\mathbb{R}), \mathcal{O}_X\restriction_{X(\mathbb{R})})$ by $\mathcal{R}(X)$, called the *real part* of X.

Proposition 8. *If X is an algebraic variety over $\mathbb{R}$ with its set of real points $X(\mathbb{R})$ dense in X then the real part $\mathcal{R}(X)$ of X is a real algebraic variety.*

Proof. Let us first prove the statement for affine varieties. That is, we first prove that, if $X = \operatorname{Spec} A$, where $A = \mathbb{R}[X_1, \ldots, X_n]/I$ and I is an ideal of $\mathbb{R}[X_1, \ldots, X_n]$, the real part $\mathcal{R}(X)$ of X is a real algebraic variety.

Let V be the vanishing set of I in $\mathbb{R}^n$, that is,

$$V = \mathfrak{V}(\mathfrak{I}) = \{x \in \mathbb{R}^n \mid \forall F \in I\colon F(x) = 0\}$$

and let $I' \subseteq \mathbb{R}[X_1, \ldots, X_n]$ be the vanishing ideal of V, that is,

$$I' = \mathfrak{I}(\mathfrak{V}) = \{F \in \mathbb{R}[X_1, \ldots, X_n] \mid \forall x \in V\colon F(x) = 0\}.$$

We claim that $I' = I$.

Obviously, I is contained in I'. Put $A' = \mathbb{R}[X_1, \ldots, X_n]/I'$ and $X' = \operatorname{Spec} A'$ and let $\varphi\colon A \to A'$ be the canonical mapping. Then,

$$\operatorname{Spec} \varphi\colon X' \longrightarrow X$$

is a closed immersion and $X(\mathbb{R})$ is contained in the image of $\operatorname{Spec} \varphi$. Since $X(\mathbb{R})$ is dense, $\operatorname{Spec} \varphi$ is a homeomorphism. In particular, I' is the radical ideal of I [16, p. 23]. Since X is reduced, I is its own radical ideal. Therefore $I' = I$.

Now we will prove that the real part $\mathcal{R}(X)$ of X is isomorphic to $(V, \mathcal{R}_V)$. Define the mapping

$$\begin{aligned} f\colon V &\longrightarrow X(\mathbb{R}) \\ x &\longmapsto m_x, \end{aligned}$$

where m_x is the maximal ideal of A generated by $X_1 - x_1, \dots, X_n - x_n$ and $x = (x_1, \dots, x_n)$. Clearly, f is a homeomorphism. The local ring of m_x in $\mathcal{R}(X)$ is equal to the local ring of m_x in X and is A_{m_x}. Define a morphism of local rings

$$f_x^{\#} \colon A_{m_x} \longrightarrow \mathcal{R}_{V,x}$$

by considering an element of A_{m_x} as a regular real-valued function in a neighbourhood of x in V. This is well defined since every polynomial $F \in I$ vanishes on V and every element $a \in A - m_x$ is nonzero in x.

Let us prove that f is an isomorphism of $\mathbb{R}$-spaces. Since $f_x^{\#}$ is clearly surjective for every $x \in V$, it suffices to show injectivity of $f_x^{\#}$. Suppose $p \in A$, $q \in A - m_x$ and $f_x^{\#}(p/q) = 0$ in $\mathcal{R}_{V,x}$. In particular, p vanishes in a neigbourhood of x in V. Hence, there exists a polynomial $F \in \mathbb{R}[X_1, \dots, X_n]$ such that $F(x) \neq 0$ and Fp vanishes on V. This shows that Fp is an element of I. Furthermore, the image a of F in A is not contained in m_x and $ap = 0$ in A. Therefore, $p/q = 0$ in A_{m_x} and $f_x^{\#}$ is injective. This proves that f is an isomorphism.

To prove the theorem for an arbitrary algebraic variety X over $\mathbb{R}$, it suffices to show that the pre-algebraic variety $\mathcal{R}(X)$ is separated. Observe that

$$\mathcal{R}(X \times X) \cong \mathcal{R}(X) \times \mathcal{R}(X)$$

and, under this isomorphism, the diagonal $\Delta_{\mathcal{R}(X)} \subseteq \mathcal{R}(X) \times \mathcal{R}(X)$ corresponds to $\Delta_X \cap \mathcal{R}(X \times X)$. Since X is separated, Δ_X is closed in $X \times X$. Therefore, $\Delta_X \cap \mathcal{R}(X \times X)$ is closed in $\mathcal{R}(X \times X)$ and $\mathcal{R}(X)$ is separated. □

In categorical language, $\mathcal{R}$ is a functor from the category of algebraic varieties over $\mathbb{R}$ with dense sets of real points into the category of real algebraic varieties.

Observe that, the real part $\mathcal{R}(U)$ of U is canonically isomorphic to $\mathcal{R}(X)$, if U is an open subset of the algebraic variety X over $\mathbb{R}$ such that U contains the set of real points $X(\mathbb{R})$ of X.

We sometimes refer to the real part $\mathcal{R}(X)$ of X by just writing $X(\mathbb{R})$.

Example 9. As usual, the n-dimensional affine scheme

$$\operatorname{Spec} A[X_1, \dots, X_n]$$

over a ring A is denoted by $\mathbb{A}^n_A$, the n-dimensional projective space

$$\operatorname{Proj} A[X_0, \dots, X_n]$$

over a ring A is denoted by $\mathbb{P}^n_A$. If $A = \mathbb{Z}$, we write just $\mathbb{A}^n$ (resp. $\mathbb{P}^n$) instead of $\mathbb{A}^n_{\mathbb{Z}}$ (resp. $\mathbb{P}^n_{\mathbb{Z}}$).

Both $\mathbb{A}^n_{\mathbb{R}}$ and $\mathbb{P}^n_{\mathbb{R}}$ are algebraic varieties over $\mathbb{R}$. Their real parts $\mathbb{A}^n_{\mathbb{R}}(\mathbb{R}) = \mathbb{R}^n$ and $\mathbb{P}^n_{\mathbb{R}}(\mathbb{R}) = \mathbb{P}^n(\mathbb{R})$ are real algebraic varieties, by Theorem 8. Of course, these structures of real algebraic varieties on $\mathbb{R}^n$ and $\mathbb{P}^n(\mathbb{R})$ coincide with the usual structures. □

Remark 10. An important class of algebraic varieties X over $\mathbb{R}$, such that $X(\mathbb{R})$ is dense in X, is the class of nonsingular irreducible algebraic varieties X over $\mathbb{R}$ with $X(\mathbb{R})$ nonempty [31, p. 8]. □

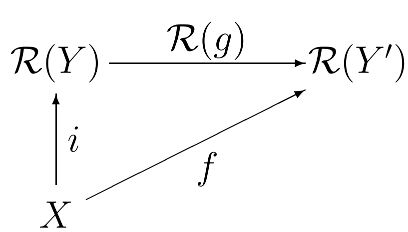
Definition 11. *A* complexification *of a real algebraic variety X is a pair (Y, i) consisting of an algebraic variety Y over $\mathbb{R}$, having its set of real points $Y(\mathbb{R})$ dense in Y, and an isomorphism $i\colon X \to \mathcal{R}(Y)$ of real algebraic varieties.*

It is clear that the dimension of X is equal to the dimension of Y, whenever Y is a complexification of X.

Observation 12. Complexifications play an important role in the study of real algebraic varieties because of the following property. Let X be a real algebraic variety and suppose (Y, i) is a complexification of X. Then, for every algebraic variety Y' over $\mathbb{R}$ and every morphism $f\colon X \to \mathcal{R}(Y')$ of $\mathbb{R}$-spaces, there exists a unique rational mapping

$$g\colon Y \dashrightarrow Y',$$

such that the domain $\operatorname{dom} g$ of g contains the set of real points $Y(\mathbb{R})$ of Y and the diagram



commutes.

To prove this, one may assume both Y and Y' affine. Then we have to extend the morphism

$$h = f \circ i^{-1} \colon \mathcal{R}(Y) \longrightarrow \mathcal{R}(Y')$$

to a morphism on some open subset U of Y.

Choose generators $a_1, \ldots, a_n$ of $\Gamma(Y', \mathcal{O}_{Y'})$ as an $\mathbb{R}$-algebra. Then, the image under $h^\#$ of the restriction of a_i to $Y'(\mathbb{R})$ is the restriction to $Y(\mathbb{R})$ of some $b_i \in \Gamma(U_i, \mathcal{O}_Y)$, for some open affine subset U_i of Y containing $Y(\mathbb{R})$. Then, U_i is dense in Y and every b_i can be considered as a rational function. Observe that, since $Y(\mathbb{R})$ is dense in Y, each b_i is uniquely determined as a rational map by a_i. Let U be the intersection of all U_i. Then, again since $Y(\mathbb{R})$ is dense in Y, the assignment $a_i \mapsto b_{i|U}$ extends to a morphism of $\mathbb{R}$-algebras

$$\varphi \colon \Gamma(U, \mathcal{O}_Y) \longrightarrow \Gamma(Y', \mathcal{O}_{Y'}).$$

Now, $g = \operatorname{Spec} \varphi \colon U \to Y'$ extends h and is uniquely determined as a rational mapping $Y \dashrightarrow Y'$. □

The preceding observation shows that complexifications are unique up to birational equivalence. That is, if Y and Y' are complexifications of the real algebraic variety X, then Y and Y' are birationally equivalent. In particular, if a real algebraic variety X has a complexification (Y, i), birational invariants of Y are, in fact, invariants of the real algebraic variety X.

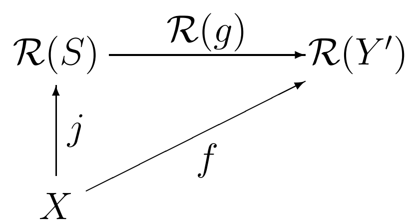
As an example, the genus of a nonsingular irreducible real algebraic curve C is defined and is an invariant of C. For, let D be a nonsingular complete complexification of C. Then, the genus $g(D)$ of D does not depend on D and will be called the *genus* of C. Clearly, if the nonsingular geometrically irreducible real algebraic curves C and C' are isomorphic then both genera are equal.

Remark 13. It is clear that a real algebraic variety X of positive dimension does not have a "minimal" complexification, that is, there does not exist an algebraic variety Y over $\mathbb{R}$ with $Y(\mathbb{R})$ dense in Y and $\mathcal{R}(Y)$ isomorphic to X such that for every algebraic variety Y'

over $\mathbb{R}$ and every morphism $f\colon X \to \mathcal{R}(Y')$ of $\mathbb{R}$-spaces, there exists a unique morphism g from Y into Y' which makes the diagram on page 17 commutative. However, if the real algebraic variety X has a complexification then one can construct a seperated reduced scheme S over $\mathbb{R}$, together with an isomorphism of $\mathbb{R}$-spaces

$$j\colon X \to \mathcal{R}(S)$$

such that for every algebraic variety Y' over $\mathbb{R}$ and every morphism $f\colon X \to \mathcal{R}(Y')$ of $\mathbb{R}$-spaces, there exists a unique morphism g of schemes over $\mathbb{R}$ from S into Y' which makes the diagram



commutative. For, if (Y, i) is a complexification of X then one defines

$$S = \{P \in Y \mid \overline{\{P\}} \cap Y(\mathbb{R}) \neq \emptyset\}.$$

One makes the subset S of Y into a scheme by taking as the structure sheaf on S the restriction of the structure sheaf of Y. Since $\mathcal{R}(S) = \mathcal{R}(Y)$, the mapping i from X into $\mathcal{R}(Y)$ is at the same time a mapping j from X into $\mathcal{R}(S)$. One can check that (S, j) has the required property. Moreover, (S, j) is unique up to isomorphism.

Let us call the scheme S over $\mathbb{R}$, when it exists, the *real scheme associated to* X. Of course, S is not of finite type over $\mathbb{R}$, in general.

In the case that X is an affine real algebraic variety, S is just the scheme over $\mathbb{R}$

$$S = \operatorname{Spec} \Gamma(X, \mathcal{R}_X),$$

where $\mathcal{R}_X$ is the sheaf of regular functions on X. □

Remark 14. Observe that, when Y is an algebraic variety over $\mathbb{R}$ and i is an isomorphism of $\mathbb{R}$-spaces from the real algebraic variety X to the $\mathbb{R}$-space $\mathcal{R}(Y)$, the closure Z in Y of the set of real points of Y is a complexification of X. For, i factors through $\mathcal{R}(j)\colon \mathcal{R}(Z) \to \mathcal{R}(Y)$, where $j\colon Z \to Y$ is the inclusion. Since j is a closed immersion,

$$j_x^\#\colon \mathcal{O}_{Y,x} \longrightarrow \mathcal{O}_{Z,x}$$

is surjective for every $x \in Z(\mathbb{R}) = Y(\mathbb{R})$. Therefore, X is isomorphic to $\mathcal{R}(Z)$, where Z has a dense set of real points. (It even follows that Z is the union of all irreducible components C of Y having $C(\mathbb{R})$ nonempty.) □

Definition 15. *A real algebraic variety X is* (quasi-)projective *if X is isomorphic to a (locally) closed subvariety Y of $\mathbb{P}^n(\mathbb{R})$. An algebraic variety X over $\mathbb{R}$ is* (quasi-)projective *if X is isomorphic to a (locally) closed subvariety Y of $\mathbb{P}^n_{\mathbb{R}}$.*

We have the following trivial, but important, fact.

Proposition 16. *Every quasi-projective (resp. projective) real algebraic variety has a quasi-projective (resp. projective) complexification.*

Proof. Suppose $X \subseteq \mathbb{P}^n(\mathbb{R})$ is locally closed (resp. closed). There exists a locally closed (resp. closed) subset Y of $\mathbb{P}^n_{\mathbb{R}}$ such that

$$X = Y(\mathbb{R}).$$

Let Z be the closure of X in Y. Then Z is a complexification of X and Z is quasi-projective (resp. projective). □

Of course, the complexification constructed in the proof of Proposition 16 depends on the embedding of the quasi-projective real algebraic variety in projective space.

We will see in Section 2.5 (Theorem 29) that real algebraic groups have canonical complexifications.

Remark 17. A typical feature of real algebraic geometry is that all quasi-projective real algebraic varieties are actually affine. For, if X is a quasi-projective real algebraic variety then, by Proposition 16, X has a quasi-projective complexification Y. Without loss of generality, we may assume that Y is a locally closed subvariety of $\mathbb{P}^n_{\mathbb{R}}$. Let H be the hypersurface in $\mathbb{P}^n_{\mathbb{R}}$ given by

$$\sum_{i=0}^{n} X_i^2 = 0.$$

One knows that $\mathbb{P}^n_{\mathbb{R}} - H$ is affine [13, Exercise I.3.5]. Now the set of real points $H(\mathbb{R})$ is empty. Therefore, the real parts of Y and $Y - H$ are isomorphic and the real part of $Y - H$ is quasi-affine. Hence, $Y - H$ is also a complexification of X. In particular, X is quasi-affine. By Example 5, X is affine. □

1.2 Algebraic cycles and line bundles

The i^{th} singular homology (resp. cohomology) group with coefficients in $\mathbb{Z}/2\mathbb{Z}$ will be denoted by

$$H_i(M, \mathbb{Z}/2\mathbb{Z}) \ \ (\text{resp. } H^i(M, \mathbb{Z}/2\mathbb{Z})).$$

Recall from [2, p. 235] that, if X is an affine real algebraic variety and *strongly compact*, i.e. X_s is compact, then every real algebraic subvariety Y of dimension i has a fundamental class

$$[Y] \in H_i(X_s, \mathbb{Z}/2\mathbb{Z}).$$

A cycle $c \in H_i(X_s, \mathbb{Z}/2\mathbb{Z})$ is said to be *realizable by a real algebraic subvariety* of X if there exists an i-dimensional real algebraic subvariety Y of X such that

$$[Y] = c.$$

The subset $H_i^{alg}(X, \mathbb{Z}/2\mathbb{Z})$, consisting of cycles that are realizable by real algebraic subvarieties of X, is clearly a subgroup of $H_i(X_s, \mathbb{Z}/2\mathbb{Z})$. Furthermore, if X is nonsingular and of dimension n then one defines the subgroup

$$H^i_{alg}(X, \mathbb{Z}/2\mathbb{Z})$$

of $H^i(X_s, \mathbb{Z}/2\mathbb{Z})$ as the image of $H^{alg}_{n-i}(X, \mathbb{Z}/2\mathbb{Z})$ under Poincaré duality.

Example 18. Let $T \subseteq \mathbb{R}^n$ be the real algebraic torus given by the equation

$$z^2 = 1 - (x^2 + y^2 - 2)^2.$$

Then, intersecting the torus T with the plane $z = 0$ gives us the reducible real algebraic subvariety

$$(x^2 + y^2 - 1)(x^2 + y^2 - 3) = 0$$

of T. Clearly, both subvarieties $x^2+y^2 = 1$ and $x^2+y^2 = 3$ represent the same nontrivial homology class in $H_1^{alg}(T, \mathbb{Z}/2\mathbb{Z})$. The reader may enjoy finding real algebraic subvarieties representing the other 2 nontrivial elements of $H_1^{alg}(T, \mathbb{Z}/2\mathbb{Z})$. (It can be shown that T is isomorphic to $S^1 \times S^1$.) □

Remark 19. The following facts are known [3]. Let M be a compact connected C^∞-manifold of dimension greater than 1. Let k be an integer satisfying

$$\begin{cases} 0 \leq k \leq \dim_{\mathbb{Z}/2\mathbb{Z}} H^1(M, \mathbb{Z}/2\mathbb{Z}), & \text{if } M \text{ is orientable,} \\ 1 \leq k \leq \dim_{\mathbb{Z}/2\mathbb{Z}} H^1(M, \mathbb{Z}/2\mathbb{Z}), & \text{if } M \text{ is nonorientable.} \end{cases}$$

Then there exists a nonsingular affine real algebraic variety X diffeomorphic to M, such that $\dim_{\mathbb{Z}/2\mathbb{Z}} H^1_{alg}(X, \mathbb{Z}/2\mathbb{Z}) = k$. □

In general, given a strongly compact affine real algebraic variety X, it is very difficult to compute the group $H_i^{alg}(X, \mathbb{Z}/2\mathbb{Z})$. However, in Section 2.6 we will be able to compute this group for a large class of real algebraic varieties in the case $i = \dim X - 1$. A crucial tool for this is the first Stiefel-Whitney class of a strongly algebraic line bundle.

Suppose X is real algebraic variety and S is a scheme over $\mathbb{R}$ such that $\mathcal{R}(S)$ is isomorphic to X. If $\mathcal{L}$ is an invertible sheaf on S then the restriction $\mathcal{L}\restriction_{\mathcal{R}(S)}$ of $\mathcal{L}$ to $\mathcal{R}(S)$ is an invertible sheaf on $\mathcal{R}(S)$. Clearly, there is, up to isomorphism, a unique real algebraic line bundle on $\mathcal{R}(S)$, denoted by $\mathcal{R}(\mathcal{L})$, such that the sheaf of sections of $\mathcal{R}(\mathcal{L})$ is isomorphic to $\mathcal{L}\restriction_{\mathcal{R}(S)}$. Then, if $i\colon X \to S$ is an isomorphism, $i^\star\mathcal{R}(\mathcal{L})$ is a real algebraic line bundle on X. Moreover, if X is affine and S is the associated real scheme of X, a real algebraic line bundle L on X is strongly algebraic if and only if there exists an invertible sheaf $\mathcal{L}$ on S such that

$$i^\star \mathcal{R}(\mathcal{L}) \cong L.$$

This follows immediately from the definition of strongly algebraic line bundles [2, p. 259].

The group of isomorphism classes of strongly algebraic line bundles on X is denoted by $V^1_{alg}(X)$. Hence, by what we have said above, the group $V^1_{alg}(X)$ is isomorphic to the group $\operatorname{Pic} S$ of invertible sheaves on S, where S is the associated real scheme of the affine real algebraic variety X.

If M is a topological manifold, the group of isomorphism classes of topological line bundles on M will be denoted by $V^1(M)$. It has been proved in [2, p. 265] that the canonical mapping

$$V^1_{alg}(X) \longrightarrow V^1(X_s)$$

is injective, whenever X is strongly compact nonsingular and affine. Hence, for such real algebraic varieties, $V^1_{alg}(X)$ can be considered as a subgroup of $V^1(X_s)$. The following theorem, proved in [2, p. 271], shows that if one wants to study the group $H^{alg}_{n-1}(X, \mathbb{Z}/2\mathbb{Z})$ or, equivalently, $H^1_{alg}(X, \mathbb{Z}/2\mathbb{Z})$, one could as well study the group $V^1_{alg}(X)$ of strongly algebraic line bundles on X. (For the definition of Stiefel-Whitney classes of a topological line bundle on a manifold, the reader is refered to [22, p. 37].)

Theorem 20. *Let X be a nonsingular affine real algebraic variety and strongly compact. Then, the first Stiefel-Whitney class defines a mapping*

$$w_1 \colon V^1_{alg}(X) \longrightarrow H^1(X_s, \mathbb{Z}/2\mathbb{Z})$$

which is an isomorphism onto $H^1_{alg}(X, \mathbb{Z}/2\mathbb{Z})$.

As a consequence, $H^1_{alg}(\,\cdot\,, \mathbb{Z}/2\mathbb{Z})$ is a contravariant functor from the category of strongly compact nonsingular affine real algebraic varieties into the category of abelian groups.

When studying strongly algebraic line bundles on an affine irreducible real algebraic variety X, we will need to know whether such a line bundle extends to a line bundle over a complexification (Y, i) of X. More precisely, we will need to know whether the mapping

$$l_Y\colon \operatorname{Pic} Y \longrightarrow V^1_{alg}(X),$$

defined by $l_Y(\mathcal{L}) = i^\star\mathcal{R}(\mathcal{L})$, is surjective, where $\operatorname{Pic} Y$ is the group of isomorphism classes of invertible sheaves on Y. We will prove that l_Y is surjective whenever X and Y are nonsingular.

Lemma 21. *If X is an irreducible nonsingular affine real algebraic variety and Y is a nonsingular complexification of X, then the mapping*

$$l_Y\colon \operatorname{Pic} Y \longrightarrow V^1_{alg}(X),$$

defined above, is surjective.

Proof. Let S be the associated real scheme of X. Then, S can be considered as a subscheme of Y (see Remark 13). Since

$$\operatorname{Pic} S \cong V^1_{alg}(X),$$

it suffices to show that the canonical mapping

$$\rho\colon \operatorname{Pic} Y \longrightarrow \operatorname{Pic} S,$$

defined by $\rho(\mathcal{L}) = \mathcal{L}\restriction_S$, is surjective.

Let $\operatorname{Cl} T$ denote the *class group* of a nonsingular integral scheme T. It is proved in [13, p. 145] that the class group of such a scheme is isomorphic to the Picard group. Clearly, the canonical mapping

$$\operatorname{Cl} Y \longrightarrow \operatorname{Cl} S$$

is surjective. Therefore, ρ is surjective. This proves the lemma. □

1.3 Field of definition of an algebraic variety

The object of this section is to recall a fundamental theorem from the theory of descent. A profound study of this subject was done by A. Weil [34], after which A. Grothendieck generalized this [12, Exp. 190].

Before we state this fundamental theorem, we need some preparation. Let L/K be a finite Galois extension with Galois group G. Suppose Y is an algebraic variety over L and G acts on Y, that is, for every $\sigma \in G$, we are given a morphism of schemes

$$\psi_\sigma : Y \longrightarrow Y$$

such that $\psi_1 = \mathrm{id}_Y$ and $\psi_\sigma \circ \psi_\tau = \psi_{\sigma\tau}$, for $\sigma, \tau \in G$. Let us call such an action a *descent datum* for Y with respect to the field extension L/K if the diagram

$$\begin{array}{ccc} Y & \xrightarrow{\psi_\sigma} & Y \\ \downarrow & & \downarrow \\ \operatorname{Spec} L & \xrightarrow{\operatorname{Spec} \sigma^{-1}} & \operatorname{Spec} L \end{array}$$

commutes for every $\sigma \in G$.

If X is an algebraic variety over K then $X \otimes_K L$ is an algebraic variety over L, denoted by X_L. Observe that G acts on X_L by letting $\sigma \in G$ act like

$$1 \otimes \sigma^{-1} : X_L \longrightarrow X_L.$$

Clearly, this action is a descent datum for X_L with respect to the field extension L/K.

The following theorem states that it is in fact equivalent to give a quasi-projective algebraic variety X over K or to give a descent datum for X_L. For a proof the reader should consult the above mentioned references.

Theorem 22. *Let L/K be a finite Galois extension with Galois group G. If Y is a quasi-projective algebraic variety over L endowed with a descent datum with respect to the field extension L/K, then there exists a unique, up to K-isomorphism, algebraic variety X over K such that X_L and Y are G-equivariantly isomorphic.*

1.4 The Weil restriction

In this section we recall the definition and construction of the Weil restriction (see [35, Section 1.3] or [12, Exp. 195, Section C2]), also called restriction of scalars, of an L-scheme with respect to a finite Galois extension L/K. Although we are mainly interested in the case $L = \mathbb{C}$, $K = \mathbb{R}$, we will treat this more general case here.

In this section, L/K will be a finite Galois extension and G its Galois group.

Definition 23. *If X is a scheme over L then the* Weil restriction *of X with respect to the field extension L/K is a K-scheme $\mathcal{N}_{L/K}(X)$ and a morphism of L-schemes $\varphi\colon \mathcal{N}_{L/K}(X) \otimes_K L \to X$ such that for every K-scheme Y and every morphism of L-schemes $\psi\colon Y \otimes_K L \to X$ there exists a unique morphism of K-schemes $\eta\colon Y \to \mathcal{N}_{L/K}(X)$ making the diagram*

$$\begin{array}{ccc} \mathcal{N}_{L/K}(X) \otimes_K L & \xrightarrow{\varphi} & X \\ {\scriptstyle \eta \otimes_K L}\uparrow & \nearrow_{\psi} & \\ Y \otimes_K L & & \end{array}$$

commutative.

The notation $\mathcal{N}_{L/K}(X)$ stems from [20]. Of course, if the Weil restriction of an L-scheme exists, it is unique up to an isomorphism. One could rephrase the condition on $\mathcal{N}_{L/K}(X)$ by requiring, for every K-scheme Y, the existence of a bijection

$$\mathrm{Hom}_{K\text{–}Sch}(Y, \mathcal{N}_{L/K}(X)) \longrightarrow \mathrm{Hom}_{L\text{–}Sch}(Y \otimes_K L, X),$$

which is natural in Y, where $K-Sch$ denotes the category of schemes over K. In the language of category theory (see [19]), the functor $\mathcal{N}_{L/K}$ is a right adjoint of the functor $Y \mapsto Y \otimes_K L$. Anyway, we have a bijection

$$\mathcal{N}_{L/K}(X)(K) \longrightarrow X(L).$$

In the special case $L = \mathbb{C}$, $K = \mathbb{R}$ and X is an algebraic variety over $\mathbb{C}$, the bijection $\mathcal{N}_{\mathbb{C}/\mathbb{R}}(X)(\mathbb{R}) \to X(\mathbb{C})$ will give rise to an isomorphism of the real algebraic varieties $\mathcal{R}(\mathcal{N}_{\mathbb{C}/\mathbb{R}}(X))$ and the underlying real algebraic structure ${}_{\mathbb{R}}X$ of X. In other words, if X is an irreducible algebraic variety over $\mathbb{C}$ then $\mathcal{N}_{\mathbb{C}/\mathbb{R}}(X)$ is a complexification of the underlying real algebraic structure ${}_{\mathbb{R}}X$ of X (Theorem 29).

Before we prove the existence of the Weil restriction for quasi-projective algebraic varieties, we need to fix some notation.

If X is a scheme over L and $\sigma \in G$ then the L-scheme X^σ is defined to be the composition

$$X \longrightarrow \operatorname{Spec} L \overset{\operatorname{Spec}\sigma^{-1}}{\longrightarrow} \operatorname{Spec} L.$$

The assignment $X \mapsto X^\sigma$ can be made into a functor from the category $L-Sch$ of L-schemes into itself. Although this notation is classical, it is a little bit awkward. For, if $\sigma, \tau \in G$, then the composition of functors $X \mapsto (X^\tau)^\sigma$ of $X \mapsto X^\sigma$ with $X \mapsto X^\tau$ is equivalent with the functor $X \mapsto X^{\sigma\tau}$. Nevertheless, we adopt the classical notation.

Forgetting the structures of an L-scheme on both X and X^σ, the schemes X and X^σ are identical, by definition of X^σ. Therefore, the identity on X is a morphism of schemes

$$\varphi_\sigma \colon X \longrightarrow X^\sigma.$$

Note that φ_σ is a morphism of K-schemes, not of L-schemes.

Theorem 24. *Let L/K be a finite Galois extension. Then, the Weil restriction with respect to the field extension L/K exists for quasi-projective algebraic varieties.*

Proof. Let X be a quasi-projective algebraic variety over L. We will give a construction of the Weil restriction $\mathcal{N}_{L/K}(X)$ of X with respect to the field extension L/K.

For any $\sigma, \tau \in G$ let

$$\varphi_{\tau,\sigma^{-1}} \colon X^\sigma \longrightarrow X^\tau$$

be the morphism of K-schemes $\varphi_\tau \circ \varphi_\sigma^{-1}$. Then, for every $\pi, \sigma, \tau \in G$, we have

$$\varphi_{\tau,\sigma^{-1}} \circ \varphi_{\sigma,\pi^{-1}} = \varphi_{\tau,\pi^{-1}}.$$

Put

$$X' = \prod_{\alpha \in G} X^\alpha,$$

and let, for $\alpha \in G$, $p_\alpha\colon X' \to X^\alpha$ be the projection on the α^{th} factor. We define a descent datum for X' with respect to L/K as follows. Define for any $\tau \in G$ a morphism $\psi_\tau\colon X' \to X'$ by requiring

$$p_\alpha \circ \psi_\tau = \varphi_{\alpha,\alpha^{-1}\tau} \circ p_{\tau^{-1}\alpha}, \text{ for every } \alpha \in G.$$

Indeed, this defines a descent datum for X'. We only have to check that $\psi_\sigma \circ \psi_\tau = \psi_{\sigma\tau}$, for every $\sigma, \tau \in G$. This holds since, for any $\alpha \in G$,

$$\begin{aligned} p_\alpha \circ \psi_\sigma \circ \psi_\tau &= \varphi_{\alpha,\alpha^{-1}\sigma} \circ p_{\sigma^{-1}\alpha} \circ \psi_\tau \\ &= \varphi_{\alpha,\alpha^{-1}\sigma} \circ \varphi_{\sigma^{-1}\alpha,\alpha^{-1}\sigma\tau} \circ p_{\tau^{-1}\sigma^{-1}\alpha} \\ &= \varphi_{\alpha,\alpha^{-1}\sigma\tau} \circ p_{(\sigma\tau)^{-1}\alpha} \\ &= p_\alpha \circ \psi_{\sigma\tau}. \end{aligned}$$

Now, it follows from Theorem 22 that, if X is a quasi-projective algebraic variety over L, there exist a unique quasi-projective algebraic variety $\mathcal{N}_{L/K}(X)$ over K and a G-equivariant isomorphism of L-schemes

$$\mathcal{N}_{L/K}(X) \otimes_K L \longrightarrow X'.$$

Identifying $\mathcal{N}_{L/K}(X) \otimes_K L$ and X' via this mapping, the pair

$$(\mathcal{N}_{L/K}(X), p_1)$$

is the Weil restriction of X with respect to the field extension L/K. We omit the easy proof of the latter statement. □

Example 25. Let $L = \mathbb{C}$, $K = \mathbb{R}$, and let $\mathbb{R}$ be embedded in $\mathbb{C}$ in the standard way. Then the Galois group consists of two elements, complex conjugation, denoted by σ, and the identity. If X is a quasi-projective algebraic variety over $\mathbb{C}$, then the algebraic variety X^σ over $\mathbb{C}$, also denoted by $\overline{X}$, is called the *conjugate variety.*

Furthermore, suppose we choose an embedding $i\colon X \to \mathbb{P}^n_{\mathbb{C}}$ of X in n-dimensional projective space over $\mathbb{C}$. Then the conjugate variety $\overline{X}$ is isomorphic to the image $\sigma_n(X)$ of X under the mapping $\sigma_n = 1 \otimes \sigma\colon \mathbb{P}^n_{\mathbb{C}} \to \mathbb{P}^n_{\mathbb{C}}$, where we have identified $\mathbb{P}^n_{\mathbb{C}}$ with $\mathbb{P}^n_{\mathbb{R}} \otimes \mathbb{C}$.

Moreover, the action of σ on $X' = X \times \overline{X}$ is the mapping ψ_σ. On the set of complex points of X', this is just the mapping

$$(x, y) \longmapsto (\sigma_n(y), \sigma_n(x)),$$

where $(x, y) \in X'(\mathbb{C})$. $\square$

Given a quasi-projective algebraic variety X over L, it is interesting to study the set of (isomorphism classes of) quasi-projective varieties Y over L, which have the property that $\mathcal{N}_{L/K}(Y)$ is isomorphic to $\mathcal{N}_{L/K}(X)$. Roughly speaking, one studies the fibers of $\mathcal{N}_{L/K}$.

Clearly, $\mathcal{N}_{L/K}(X^\sigma)$ is isomorphic to $\mathcal{N}_{L/K}(X)$, for every $\sigma \in G$. One might expect that, in general, these are the only varieties Y with $\mathcal{N}_{L/K}(Y) \cong \mathcal{N}_{L/K}(X)$. This is true for certain curves of genus $g > 1$.

Theorem 26. *Let L/K be a finite Galois extension of degree n and let X be a complete geometrically irreducible nonsingular algebraic curve over L of genus $g > 1$ such that $X(L)$ is nonempty. If Y is an algebraic curve over L with*

$$\mathcal{N}_{L/K}(Y) \cong \mathcal{N}_{L/K}(X)$$

then there exists an automorphism σ of L over K such that $Y \cong X^\sigma$. In particular, the number of (isomorphism classes of) algebraic curves Y over L having $\mathcal{N}_{L/K}(Y)$ isomorphic to $\mathcal{N}_{L/K}(X)$ divides n.

Proof. Suppose $\mathcal{N}_{L/K}(Y)$ is isomorphic to $\mathcal{N}_{L/K}(X)$, but Y is not isomorphic to any X^σ. Then, there exists an isomorphism

$$\varphi\colon \prod_{\alpha\in G} Y^\alpha \longrightarrow \prod_{\alpha\in G} X^\alpha.$$

In particular, Y is a complete geometrically irreducible nonsingular algebraic curve of genus g. Let $i\colon Y \to \prod Y^\alpha$ be an inclusion of Y as a factor (which exists since $Y^\alpha(L)$ is nonempty for all $\alpha \in G$), let $p_\sigma\colon \prod X^\alpha \to X^\sigma$ be the projection on the σ^{th} factor. Then, for all $\sigma \in G$,

$$p_\sigma \circ \varphi \circ i\colon Y \longrightarrow X^\sigma$$

is a separable morphism between curves of the same genus $g > 1$. Since Y is not isomorphic to X^σ, this morphism is constant, for any σ, by Hurwitz's Theorem [13, p. 301]. Contradiction. $\square$

The preceding result is not true for curves of genus 1. The following theorem, which follows easily from [14], illustrates this.

Theorem 27. *For every positive integer k, there exist mutually nonisomorphic complete geometrically irreducible nonsingular algebraic curves $E_1, \dots, E_k$ over $\mathbb{C}$ of genus 1 such that*

$$\mathcal{N}_{\mathbb{C}/\mathbb{R}}(E_i) \cong \mathcal{N}_{\mathbb{C}/\mathbb{R}}(E_j),$$

for all $i, j \leq k$.

1.5 The underlying real algebraic structure of algebraic varieties over $\mathbb{C}$

Let us recall the definition of the underlying real algebraic structure of an algebraic variety over $\mathbb{C}$. Taking the standard identification of $\mathbb{C}^n$ with $\mathbb{R}^{2n}$, one sees immediately that, given a quasi-affine algebraic variety $X \subseteq \mathbb{A}^n_{\mathbb{C}}$ over $\mathbb{C}$, the subset $X(\mathbb{C}) \subseteq \mathbb{C}^n$ gives rise to a quasi-affine real algebraic variety ${}_{\mathbb{R}}X \subseteq \mathbb{R}^{2n}$, called the underlying real algebraic structure of X.

Observe that the underlying real algebraic structure of a quasi-affine algebraic variety X over $\mathbb{C}$ does not depend on the embedding of X in affine space. To see this, observe that, if $X \subseteq \mathbb{A}^n_{\mathbb{C}}$ and $Y \subseteq \mathbb{A}^m_{\mathbb{C}}$ are quasi-affine subvarieties and $f\colon X \to Y$ is a morphism then the induced mapping ${}_{\mathbb{R}}f\colon {}_{\mathbb{R}}X \to {}_{\mathbb{R}}Y$ is a morphism of real algebraic varieties.

Now that we have defined the underlying real algebraic structure for quasi-affine algebraic varieties over $\mathbb{C}$, it is easy to extend this to arbitrary algebraic varieties over $\mathbb{C}$. For, if X is an algebraic variety over $\mathbb{C}$ then choose a covering $\{U_i\}$ of X by open affine subsets U_i. Choose embeddings $\varphi_i\colon U_i \to \mathbb{A}^{n_i}_{\mathbb{C}}$ and let V_i be the image of φ_i. Put $V_{ij} = \varphi_i(U_i \cap U_j)$, in particular, the varieties V_{ij} are affine, and let $\varphi_{ji}\colon V_{ij} \to V_{ji}$ be defined by

$$\varphi_{ji} = \varphi_j \circ \varphi_i^{-1}\restriction_{V_{ij}}.$$

By the preceding remark, the induced mappings ${}_{\mathbb{R}}\varphi_{ji}\colon {}_{\mathbb{R}}V_{ij} \to {}_{\mathbb{R}}V_{ji}$ are isomorphisms of real algebraic varieties. Furthermore, the variety ${}_{\mathbb{R}}V_{ij}$ is an open subvariety of ${}_{\mathbb{R}}V_i$. Hence, the real algebraic structures ${}_{\mathbb{R}}V_i$ on $V_i(\mathbb{C})$ can be glued together along the ${}_{\mathbb{R}}V_{ij}$ using the morphisms ${}_{\mathbb{R}}\varphi_{ji}$. Obviously, this defines the structure of a real algebraic variety ${}_{\mathbb{R}}X$ on the set of complex points $X(\mathbb{C})$ of X. Again, this structure is called the *underlying real algebraic structure* of X.

In [14] the underlying real algebraic structure of an algebraic variety X over $\mathbb{C}$ is denoted by $X_{\mathbb{R}}$. However, here we will use the notation ${}_{\mathbb{R}}X$.

Example 28. The underlying real algebraic structure of the projective line $\mathbb{P}^1_{\mathbb{C}}$ over $\mathbb{C}$ is isomorphic to the 2-sphere $S^2 \subseteq \mathbb{R}^3$, that is,

$$ {}_{\mathbb{R}}\mathbb{P}^1_{\mathbb{C}} \cong S^2. $$

To show this, it will be convenient to write $\mathbb{C} \times \mathbb{R}$ instead of $\mathbb{R}^3$, then

$$ S^2 = \{(z, x) \in \mathbb{C} \times \mathbb{R} \mid |z|^2 + x^2 = 1\}. $$

Define the real algebraic morphism $f\colon {}_{\mathbb{R}}\mathbb{P}^1_{\mathbb{C}} \to S^2$ by

$$ f\colon (z : w) \longmapsto \left(\frac{2z\overline{w}}{|z|^2 + |w|^2}, \frac{|z|^2 - |w|^2}{|z|^2 + |w|^2} \right). $$

This is just the inverse of stereographic projection and is an isomorphism. □

To ease notation, we will often write $\mathcal{N}(X)$ instead of $\mathcal{N}_{\mathbb{C}/\mathbb{R}}(X)$ for the Weil restriction of X with respect to the (standard) field extension $\mathbb{C}/\mathbb{R}$.

Theorem 29. *If X is a quasi-projective algebraic variety over $\mathbb{C}$ then the real part $\mathcal{R}(\mathcal{N}(X))$ of the Weil restriction $\mathcal{N}(X)$ of X with respect to the field extension $\mathbb{C}/\mathbb{R}$ is naturally isomorphic to ${}_{\mathbb{R}}X$ as $\mathbb{R}$-spaces. Moreover, if $X_1, \ldots, X_n$ are the irreducible components of X then the Weil restrictions $\mathcal{N}(X_i)$ are closed subvarieties of $\mathcal{N}(X)$ and the union*

$$ \bigcup_{i=1}^{n} \mathcal{N}(X_i) $$

is a complexification of the underlying real algebraic structure ${}_{\mathbb{R}}X$ of X.

Proof. The second statement follows from the first and from Remark 14. Let the pair $(\mathcal{N}(X), \varphi)$ be the Weil restriction of X. Let

$$\psi\colon X(\mathbb{C}) \longrightarrow \mathcal{N}(X)(\mathbb{R})$$

be the natural bijective mapping induced by φ. We will prove that ψ induces an isomorphism

$$\widetilde{\psi}\colon {}_{\mathbb{R}}X \longrightarrow \mathcal{R}(\mathcal{N}(X))$$

of $\mathbb{R}$-spaces.

It clearly suffices to prove this statement for affine algebraic varieties X over $\mathbb{C}$. Let X be an affine subvariety of $\mathbb{A}^n_{\mathbb{C}}$. Then, under the identification of $\mathbb{C}^n$ with $\mathbb{R}^{2n}$, the set of complex points $X(\mathbb{C}) \subseteq \mathbb{C}^n$ of X is the affine real algebraic variety ${}_{\mathbb{R}}X$ in $\mathbb{R}^{2n}$. Since $\mathcal{N}(X) = X \times \overline{X}$, which may be considered as a subvariety of $\mathbb{A}^n_{\mathbb{C}} \times \mathbb{A}^n_{\mathbb{C}}$, the set of real points of $\mathcal{N}(X)$ is the set

$$\mathcal{N}(X)(\mathbb{R}) = \{(z, \overline{z}) \mid z \in X(\mathbb{C})\} \subseteq \mathbb{C}^n \times \mathbb{C}^n.$$

Then the mapping ψ is given by

$$\begin{aligned}&\psi(x_1, y_1, \ldots, x_n, y_n) =\\ &((x_1 + iy_1, \ldots, x_n + iy_n), (x_1 - iy_1, \ldots, x_n - iy_n)),\end{aligned}$$

where $(x_1, y_1, \ldots, x_n, y_n) \in {}_{\mathbb{R}}X \subseteq \mathbb{R}^{2n}$. The inverse of ψ is given by

$$\begin{aligned}&\psi^{-1}((z_1, \ldots, z_n), (w_1, \ldots, w_n)) =\\ &(\tfrac{1}{2}(z_1 + w_1), \tfrac{1}{2i}(z_1 - w_1), \ldots, \tfrac{1}{2}(z_n + w_n), \tfrac{1}{2i}(z_n - w_n)),\end{aligned}$$

where $((z_1, \ldots, z_n), (w_1, \ldots, w_n)) \in \mathcal{N}(X)(\mathbb{R}) \subseteq \mathbb{C}^n \times \mathbb{C}^n$. Therefore, ψ is continuous and induces an isomorphism $\widetilde{\psi}$ from ${}_{\mathbb{R}}X$ into $\mathcal{R}(\mathcal{N}(X))$. □

Remark 30. The underlying real algebraic structure of a quasi-projective algebraic variety over $\mathbb{C}$ is an affine real algebraic variety. For, if X is a quasi-projective algebraic variety over $\mathbb{C}$, the Weil restriction $\mathcal{N}(X)$ of X is a quasi-projective algebraic variety over $\mathbb{R}$. By Theorem 29, the underlying real algebraic structure ${}_{\mathbb{R}}X$ of X is isomorphic to the real part $\mathcal{R}(\mathcal{N}(X))$ of X, which is a quasi-projective real algebraic variety. By Remark 17, ${}_{\mathbb{R}}X$ is an affine real algebraic variety. □

Proposition 31. *Let X be a nonsingular complete irreducible algebraic curve over $\mathbb{C}$ of genus g. Then, any irreducible real algebraic curve C embedded in the underlying real algebraic structure $_{\mathbb{R}}X$ of X has genus at least g.*

Proof. Let C' be any complexification of C. Since C is embedded in $_{\mathbb{R}}X$, there exists a nonconstant rational mapping $f\colon C' \dashrightarrow \mathcal{N}(X)$, by Theorem 29. Then, either $p_1 \circ f_{\mathbb{C}}$ or $p_2 \circ f_{\mathbb{C}}$ is a nonconstant rational mapping, where p_i is the projection from $\mathcal{N}(X)_{\mathbb{C}} = X \times \overline{X}$ onto the i^{th}-factor. By Hurwitz's Theorem [13, p. 301], the genus of C is at least g. □

Definition 32. *A real algebraic variety M is said to* admit a complex structure *if there exists an algebraic variety X over $\mathbb{C}$ such that the underlying real algebraic structure $_{\mathbb{R}}X$ of X is isomorphic to M.*

Of course, there are trivial examples of real algebraic varieties which do not admit complex structures. Odd dimensional real algebraic varieties are such examples, or nonsingular real algebraic varieties which are not orientable as smooth varieties. Other examples of real algebraic varieties which do not admit complex structures are real algebraic varieties M, having a singular point $x \in M$ with (algebraic) tangent space at x to M of odd dimension. For example, a singular real algebraic surface in $\mathbb{R}^3$ does not admit a complex structure. Less trivial examples will be discussed in Example 33.

Example 33. Let us construct, for any integer $g \geq 1$, a nonsingular strongly compact irreducible real algebraic surface $T_g \subseteq \mathbb{R}^3$ of (topological) genus g which does not admit a complex structure.

Choose g distinct real numbers $x_1, \ldots, x_g$. Put

$$f(x) = \prod_{i=1}^{g} (x - x_i)^2.$$

Let $a_1 < a_2$ be real numbers such that the equation $f(x) = a_1$ (resp. $f(x) = a_2$) has precisely $2g$ (resp. 2) distinct real solutions. One can check that

$$T_g = \left\{ (x, y, z) \in \mathbb{R}^3 \;\middle|\; \left(y^2 + f(x) - \frac{a_1 + a_2}{2} \right)^2 + z^2 = \left(\frac{a_1 - a_2}{2} \right)^2 \right\}$$

is a nonsingular compact irreducible real algebraic surface of (topological) genus g.

We claim that T_g does not admit a complex structure. For, if we intersect T_g with the plane $z = 0$, we get a reducible set which is the union of two real algebraic curves C_1, C_2, given by

$$C_i = \{(x, y) \in \mathbb{R}^2 \mid y^2 = a_i - f(x)\}, \text{ for } i = 1, 2.$$

It is well known that, since $\deg f = 2g$, the genus of such a curve is $g - 1$ (cf. [10, p. 253]). It follows from Proposition 31 that T_g does not admit a complex structure. □

It follows from [4, Theorem 4.12] that "almost all" (in the sense of [4]) nonsingular irreducible real algebraic surfaces $M \subseteq \mathbb{P}^3(\mathbb{R})$ do not admit a complex structure.

Definition 34. *If M is a real algebraic variety, the cardinality of the set of (isomorphism classes of) algebraic varieties X over $\mathbb{C}$ with ${}_{\mathbb{R}}X$ isomorphic to M is denoted by $\rho(M)$.*

Example 35. The number $\rho(S^2)$ of (isomorphism classes of) algebraic varieties X over $\mathbb{C}$ with ${}_{\mathbb{R}}X$ isomorphic to the 2-sphere S^2 is 1. For, if X is an algebraic curve over $\mathbb{C}$ with ${}_{\mathbb{R}}X$ isomorphic to S^2 then X is of genus 0. Hence, X is isomorphic to $\mathbb{P}^1_{\mathbb{C}}$. By Example 28, ${}_{\mathbb{R}}\mathbb{P}^1_{\mathbb{C}}$ is isomorphic to S^2. Therefore, $\rho(S^2) = 1$. □

Example 36. The $2n$-sphere S^{2n}, where n is an integer different from 1 and 3, does not admit a complex structure, i.e. $\rho(S^{2n}) = 0$. This follows from the fact that the smooth manifold S^{2n} does not admit an almost complex structure, for $n \neq 1, 3$ (see [7]). □

Theorem 37. *Let M be a nonsingular strongly compact strongly connected real algebraic surface of topological genus $g > 1$. Then the number $\rho(M)$ of nonisomorphic complex structures admitted by M is $0, 1$ or 2.*

Proof. Suppose $\rho(M) \neq 0$. Choose algebraic curves X and Y over $\mathbb{C}$ such that both ${}_{\mathbb{R}}X$ and ${}_{\mathbb{R}}Y$ are isomorphic to M. In particular, X and Y are complete nonsingular irreducible curves of genus g. Furthermore, the algebraic surfaces $\mathcal{N}(X)$ and $\mathcal{N}(Y)$ over $\mathbb{R}$ are birationally isomorphic. However, $\mathcal{N}(X)_{\mathbb{C}}$ and $\mathcal{N}(Y)_{\mathbb{C}}$ are minimal surfaces [26], since the genera of both X and Y are equal to $g > 0$. Hence, $\mathcal{N}(X)$ and $\mathcal{N}(Y)$ are isomorphic. By Theorem 26, Y is isomorphic to X or $\overline{X}$. □

Remark 38. It follows from Theorem 37 and [14] that any nonsingular strongly compact strongly connected real algebraic surface M admits, up to isomorphism, only finitely many complex structures, i.e. $\rho(M)$ is finite. No example of a real algebraic variety M is known with $\rho(M) = \infty$. □

Chapter 2

Abelian varieties

In the first section of this chapter we recall the basic facts of the theory of abelian varieties over a field. In the next section we specialize to the field of complex numbers and recall the analytic theory of complex tori and their line bundles. Section 2.3 is devoted to conjugate analytic varieties and complex tori with a real structure. This we will need in Section 2.4, when we study abelian varieties over $\mathbb{R}$ and invertible sheaves on abelian varieties over $\mathbb{R}$. Section 2.5 contains the definition of real abelian varieties. In Section 2.6 we will prove our results concerning realizability of codimension-1 homology classes of an arbitrary real abelian variety by real algebraic subvarieties (Theorem 89). Section 2.7 is concerned with the topology of the underlying real algebraic structure of elliptic curves over $\mathbb{C}$ with emphasis on the case of complex multiplication. In this section we will prove our results on realizability of $\mathbb{Z}/2\mathbb{Z}$-homology classes of these real algebraic tori by real algebraic subvarieties.

2.1 Abelian varieties over a field

Definition 39. *Let K be a field and X a connected algebraic variety over K. Suppose*

$$\begin{aligned} O\colon \operatorname{Spec} K &\longrightarrow X \\ m\colon X \times X &\longrightarrow X \\ i\colon X &\longrightarrow X \end{aligned}$$

are morphisms of algebraic varieties over K. Then, (X, O, m, i), or X when no confusion is possible, is an algebraic group over K *if*

$$\begin{aligned} m \circ (m \times \mathrm{id}) &= m \circ (\mathrm{id} \times m) \\ m \circ (O \times \mathrm{id}) &= \mathrm{id} \\ m \circ (\mathrm{id} \times O) &= \mathrm{id} \\ m \circ <\mathrm{id}, i> &= O \circ s \\ m \circ <i, \mathrm{id}> &= O \circ s \end{aligned}$$

where id *is the identity on X and $s \colon X \to \operatorname{Spec} K$ is the K-structure on X. A* morphism of algebraic groups over K *from (X, O_X, m_X, i_X) to (Y, O_Y, m_Y, i_Y) is a morphism $f \colon X \to Y$ of algebraic varieties over K such that*

$$m_Y \circ (f \times f) = f \circ m_X.$$

Suppose X is an algebraic group over K. If P is a K-rational point of X, we have a morphism of algebraic varieties over K

$$\tau_P \colon X \longrightarrow X,$$

called *translation* with P, defined by $\tau_P = m \circ i_P$, where i_P is the mapping from X into $X \times X$, given by $i_P(Q) = (Q, P)$ on closed points $Q \in X$. It follows that, if X is an algebraic group over K, the algebraic variety $X_{\overline{K}}$ over the algebraic closure $\overline{K}$ of K is nonsingular. Therefore, X is nonsingular. Hence, X is irreducible and even geometrically irreducible. In particular, if L is a field extension of K and X is an algebraic group over K then X_L is an algebraic group over L.

Definition 40. *Let K be a field. An* abelian variety over K *is a complete algebraic group over K. An abelian variety over K of dimension 1 is called an* elliptic curve over K. *A* morphism of abelian varieties over K *is just a morphism of algebraic groups over K.*

Example 41. Let $C \subseteq \mathbb{P}^2_K$ be a nonsingular geometrically irreducible cubic curve with its set of K-rational points $C(K)$ nonempty. It is well known [32] that C can be made into an abelian variety over K, i.e. into an elliptic curve over K.

On the other hand, every elliptic curve X over K is isomorphic to some cubic curve $C \subseteq \mathbb{P}^2_K$. This follows easily from Riemann-Roch. □

More general, every abelian variety over K can be embedded as a closed subvariety into some projective space [21, p. 113]. In other words, every abelian variety over K is projective.

The geometry of abelian varieties over K is very rigid according to the following theorems.

Theorem 42. *If V is a nonsingular algebraic variety over K and X is an abelian variety over K then every rational mapping f from V into X is a morphism.*

Theorem 43. *If X and Y are abelian varieties over K and $f\colon X \to Y$ is a morphism of algebraic varieties over K then $\tau_{-P} \circ f\colon X \to Y$ is a morphism of abelian varieties over K, where $P = f(O)$.*

A proof of Theorem 42 is in [21, p. 106]. Theorem 43 is proved in [21, p. 105]. As a consequence of the latter theorem, every abelian variety X over K is commutative, i.e.

$$m \circ \varphi = m,$$

where $\varphi\colon X \times X \to X \times X$ exchanges the factors. For, the mapping $i\colon X \to X$ maps O into O. Hence, by Theorem 43, i is a morphism of abelian varieties over K. It follows that X is commutative.

If X and Y are abelian varieties over K then the group of morphisms of abelian varieties over K from X into Y is denoted by $\mathrm{Hom}(X, Y)$. It can be proved that $\mathrm{Hom}(X, Y)$ is a free $\mathbb{Z}$-module of finite rank [21, p. 122]. The ring of morphisms from the abelian variety X over K into itself is denoted by $\mathrm{End}(X)$, called the *endomorphism ring* of X. The *endomorphism algebra* of X is the $\mathbb{Q}$-algebra

$$\mathrm{End}^{\mathrm{o}} X = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(X).$$

Definition 44. *Let K be a field. A morphism $f\colon X \to Y$ of abelian varieties over K is called an* isogeny *if X and Y are of the same dimension and f has finite kernel. The abelian varieties X and Y over K are called* isogenous *whenever there exists an isogeny $f\colon X \to Y$.*

Example 45. If X is an abelian variety over K then, for every integer n, we have the multiplication-by-n mapping

$$[n]\colon X \longrightarrow X.$$

Since X is commutative, $[n]$ is a morphism of abelian varieties over K. If the characteristic of K is 0 and K is algebraically closed, the order of the kernel of $[n]$ is n^{2g}, where g is the dimension of X. It follows that, for any field K of characteristic 0, the morphism $[n]$ is an isogeny. □

It can be proved that "isogenous" is an equivalence relation [21, p. 115].

Definition 46. *Let K be a field. An abelian variety X over K is called* simple *if X does not contain nontrivial abelian subvarieties over K other than X.*

The following theorem is proved in [21, p. 122].

Theorem 47. (Poincaré-Weil) *Any abelian variety X over K is isogenous to a product $X_1^{n_1} \times \cdots \times X_k^{n_k}$, where the X_i are simple and not isogenous to each other. The isogeny type of the X_i and the integers n_i are uniquely determined by X.*

If L is a field extension of K and X is a simple abelian variety over K then it is not necessarily true that X_L is simple. Let us give an example of this in the case $K = \mathbb{R}$ and $L = \mathbb{C}$.

Example 48. Let Y be a simple abelian variety over $\mathbb{C}$ such that Y is not isogenous to its conjugate variety Y^σ. Many, not to say most, abelian varieties over $\mathbb{C}$ have this property. For example, the number of (isomorphism classes of) elliptic curves Y over $\mathbb{C}$ such that Y is not isogenous to its conjugate curve Y^σ is uncountable [14]. Let X be the Weil restriction $\mathcal{N}_{\mathbb{C}/\mathbb{R}}(Y)$ of Y with respect to the field extension $\mathbb{C}/\mathbb{R}$. Observe that X is an abelian variety over $\mathbb{R}$. Moreover, X is a simple abelian variety over $\mathbb{R}$ while $X_\mathbb{C}$ is nonsimple.

For, suppose there exists a nontrivial abelian subvariety Z over $\mathbb{R}$ of X. Then, $Z_{\mathbb{C}}$ is an abelian subvariety over $\mathbb{C}$ of

$$\big(\mathcal{N}_{\mathbb{C}/\mathbb{R}}(Y)\big)_{\mathbb{C}} \cong Y \times Y^{\sigma}.$$

Moreover, $Z_{\mathbb{C}}$ is stable under the action of the Galois group of $\mathbb{C}/\mathbb{R}$ on $Y \times Y^{\sigma}$. Therefore, the dimension of the projection of $Z_{\mathbb{C}}$ on Y is equal to the dimension of the projection of $Z_{\mathbb{C}}$ on Y^{σ}. Hence, if $Z \neq O$ then Y and Y^{σ} are both isogeny factors of $Z_{\mathbb{C}}$, according to Theorem 47. Since Y and Y^{σ} are not isogenous, the dimension of $Z_{\mathbb{C}}$ is at least $2 \dim Y$. This proves that $Z = X$. □

It is well known that, if X is a complete geometrically irreducible algebraic variety over K, the canonical mapping from the group $\operatorname{Pic} X$ of (isomorphism classes of) invertible sheaves on X into the group $\operatorname{Pic} X_{\overline{K}}$ is injective, where $\overline{K}$ is an algebraic closure of K.

If X is an abelian variety over K then $\operatorname{Pic}^{\circ} X$ is the subgroup of $\operatorname{Pic} X$ consisting of (isomorphism classes of) invertible sheaves $\mathcal{L}$ on X such that

$$\tau_P^{\star}\mathcal{L}_{\overline{K}} \cong \mathcal{L}_{\overline{K}},$$

for every $\overline{K}$-rational point P. The *Néron-Severi group* of X is, by definition, the quotient group of the group $\operatorname{Pic} X$ by $\operatorname{Pic}^{\circ} X$. It is denoted by $\operatorname{NS}(X)$. This group is free of finite rank [21, p. 124] and this rank is called the *base number* of X.

2.2 Abelian varieties over $\mathbb{C}$

Suppose K is a subfield of $\mathbb{C}$. If X is an algebraic variety over K then the set of complex points $X(\mathbb{C})$ of X has a natural structure of a complex analytic variety. In particular, if X is an abelian variety over K then $X(\mathbb{C})$ has a natural structure of a complex Lie group. In this section we study the relation between abelian varieties over $\mathbb{C}$ and complex Lie groups. A basic reference for this is [23, Chapter 1].

Recall from [23, p. 1] that, if M is a compact connected complex Lie group, one has a holomorphic mapping

$$\exp_M : V \longrightarrow M,$$

where V is the tangent space T_0M at the unit element 0 of M. This mapping is called the *exponential mapping* and is defined by

$$\exp_M(v) = \varphi_{M,v}(1),$$

where $\varphi_{M,v}\colon \mathbb{C} \to M$ is the unique holomorphic mapping such that

$$d_0\varphi_{M,v}(1) = v.$$

We will omit the subscript M from $\exp_M$ or $\varphi_{M,v}$ when there is no confusion possible.

If M and M' are compact connected complex Lie groups, $f\colon M \to M'$ is an analytic mapping with $f(0) = 0$ and V (resp. V') is the tangent space at the unit element 0 of M (resp. M'), then the diagram

$$\begin{array}{ccc} V & \xrightarrow{\;df\;} & V' \\ \Big\downarrow{\scriptstyle \exp_M} & & \Big\downarrow{\scriptstyle \exp_{M'}} \\ M & \xrightarrow{\;f\;} & M' \end{array}$$

commutes, where df denotes the derivative of f in 0. For, if $v \in V$ then

$$d(f \circ \varphi_{M,v})(1) = df \circ d\varphi_{M,v}(1) = df(v).$$

Hence, by uniqueness of $\varphi_{M',df(v)}$,

$$\varphi_{M',df(v)} = f \circ \varphi_{M,v}.$$

This proves the commutativity of the diagram above. As a direct consequence, the exponential mapping is a morphism of groups. Indeed, the derivative dm of the addition mapping $m\colon M \times M \to M$ is the addition mapping on the vector space V and the diagram

$$\begin{array}{ccc} V \times V & \xrightarrow{\;dm\;} & V \\ \Big\downarrow{\scriptstyle \exp_{M\times M}} & & \Big\downarrow{\scriptstyle \exp_M} \\ M \times M & \xrightarrow{\;m\;} & M \end{array}$$

commutes.

It follows easily from the definition of the exponential mapping that its derivative $d\exp$ is the identity on V. Therefore, the exponential mapping is a local homeomorphism and is surjective by connectedness of M. If $\Lambda \subseteq V$ is the kernel of exp, then Λ is a *lattice* in V, that is, Λ is a discrete subgroup of V which spans V as an $\mathbb{R}$-vector space. This follows from compactness of M. Hence, the exponential mapping induces an isomorphism of complex Lie groups from V/Λ onto M. A complex Lie group isomorphic to V/Λ, for some lattice Λ in some complex vector space V, is called a *complex torus*.

Definition 49. *Let $\mathcal{M}$ be the category of lattices in finite dimensional complex vector spaces, that is, the objects of $\mathcal{M}$ are pairs (V, Λ), where V is a finite dimensional $\mathbb{C}$-vector space and $\Lambda \subseteq V$ is a lattice. A morphism in $\mathcal{M}$ from (V, Λ) to (V', Λ') is a $\mathbb{C}$-linear mapping $L\colon V \to V'$ such that $L(\Lambda) \subseteq \Lambda'$.*

Clearly, every object (V, Λ) of $\mathcal{M}$ is isomorphic to an object of the form $(\mathbb{C}^n, \Lambda')$.

We have proven above the following known theorem.

Theorem 50. *The functor*

$$M \longmapsto (T_0 M, \ker \exp_M)$$

is an equivalence from the category of compact connected complex Lie groups into the category $\mathcal{M}$ of lattices. The functor

$$(V, \Lambda) \longmapsto V/\Lambda$$

from the category $\mathcal{M}$ into the category of compact connected complex Lie groups serves as an inverse.

Let us turn our attention to abelian varieties over $\mathbb{C}$. As observed earlier, if X is an abelian variety over $\mathbb{C}$ then $X(\mathbb{C})$ is a compact connected complex Lie group in a natural way. By the GAGA-principle [27], the functor $X \mapsto X(\mathbb{C})$ from the category of abelian varieties over $\mathbb{C}$ into the category of compact connected complex Lie groups is an equivalence from the former onto some full subcategory of the latter. According to Theorem 50, this subcategory should be equivalent to a subcategory of the category $\mathcal{M}$ of lattices. The following theorem describes this subcategory [23, p. 35].

Theorem 51. *The functor*

$$X \longmapsto (T_0X(\mathbb{C}), \ker \exp)$$

is an equivalence from the category of abelian varieties over $\mathbb{C}$ *onto the full subcategory of the category* $\mathcal{M}$ *consisting of pairs* (V, Λ) *such that there exists a positive definite Hermitian form*

$$H: V \times V \longrightarrow \mathbb{C}$$

with $E = \operatorname{Im} H$ *integral on* Λ*, that is* $E(\Lambda \times \Lambda) \subseteq \mathbb{Z}$*.*

Example 52. If Λ is a lattice in $\mathbb{C}$, we may assume that $\Lambda = \Lambda_\tau$, where

$$\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau,$$

for some $\tau \in \mathbb{C}$ with $\operatorname{Im} \tau$ positive. Then

$$H(z, w) = \frac{z\overline{w}}{\operatorname{Im} \tau}$$

defines a positive definite Hermitian form on $\mathbb{C}$ with $E = \operatorname{Im} H$ integral on Λ. Therefore, by Theorem 51, for all lattices Λ in $\mathbb{C}$ there exists an abelian variety X over $\mathbb{C}$ such that

$$X(\mathbb{C}) \cong \mathbb{C}/\Lambda.$$

Clearly, X is an elliptic curve over $\mathbb{C}$. □

Since we will study line bundles, we will need the Theorem of Appell-Humbert. Before we can state this theorem, we need to introduce the following notation.

Let us recall that a *Hermitian form* on a complex vector space V is a mapping

$$H: V \times V \longrightarrow \mathbb{C}$$

which is $\mathbb{C}$-linear in the first variable and

$$H(v', v) = \overline{H(v, v')},$$

for every $v, v' \in V$. In particular, if H is an Hermitian form on V then $E = \operatorname{Im} H$ is an alternating $\mathbb{R}$-bilinear form on V such that

$$E(iv, iv') = E(v, v'),$$

for every $v, v' \in V$.

Conversely, if E is an alternating $\mathbb{R}$-bilinear form on the complex vector space V such that $E(iv, iv') = E(v, v')$, for every $v, v' \in V$, then

$$H(v, v') = E(iv, v') + iE(v, v')$$

defines a Hermitian form on V.

If V is a finite-dimensional complex vector space and $\Lambda \subseteq V$ is a lattice, then an *Appell-Humbert datum* for (V, Λ) is a pair (α, H), where H is a Hermitian form on V, such that $E = \operatorname{Im} H$ is integral on Λ, and α is a mapping from Λ into the 1-sphere

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\},$$

such that

$$\alpha(\lambda + \mu) = \alpha(\lambda)\alpha(\mu)(-1)^{E(\lambda,\mu)},$$

for every $\lambda, \mu \in \Lambda$.

Given an Appell-Humbert datum (α, H) one defines, for every $\lambda \in \Lambda$, a holomorphic function $e_\lambda \colon V \to \mathbb{C}^\star$ by

$$e_\lambda(v) = \alpha(\lambda)e^{\pi H(v,\lambda) + \frac{1}{2}\pi H(\lambda,\lambda)}.$$

One can check that

$$\lambda(v, z) = (v + \lambda, e_\lambda(v)z)$$

defines an action of Λ on $V \times \mathbb{C}$. The quotient of $V \times \mathbb{C}$ under this action of Λ is a complex analytic line bundle, denoted by $L(\alpha, H)$, on the complex analytic variety V/Λ.

Clearly, the set $\mathrm{AH}(V, \Lambda)$ of Appell-Humbert data for (V, Λ) is a group if we define

$$(\alpha_1, H_1)(\alpha_2, H_2) = (\alpha_1\alpha_2, H_1 + H_2),$$

for any Appell-Humbert data (α_1, H_1) and (α_2, H_2) for (V, Λ). Moreover, the mapping L that assigns the line bundle $L(\alpha, H)$ to the Appell-Humbert datum (α, H), is a morphism from $\mathrm{AH}(V, \Lambda)$ into the group of (isomorphism classes of) complex analytic line bundles on V/Λ.

Then the Appell-Humbert Theorem reads as follows [23, p. 20].

Theorem 53. (Appell-Humbert) *If V is a complex vector space of finite dimension and $\Lambda \subseteq V$ is a lattice, then for every complex analytic line bundle L on the complex analytic variety V/Λ, there exists a unique Appell-Humbert datum (α, H) for (V, Λ) such that*

$$L \cong L(\alpha, H).$$

In other words, the mapping L from the group $\mathrm{AH}(V, \Lambda)$ into the group of (isomorphism classes of) complex analytic line bundles on V/Λ is an isomorphism.

Remark 54. (according to [15, p. 5]) Let V be a complex vector space of dimension n and let $\Lambda \subseteq V$ be a lattice. Suppose that we are given a Hermitian form H on V such that $E = \operatorname{Im} H$ is integral on Λ. Let us study the mappings α from Λ into the 1-sphere S^1 such that (α, H) is an Appell-Humbert datum. For this, choose a $\mathbb{Z}$-basis $\lambda_1, \ldots, \lambda_{2n}$ for Λ.

Clearly, a mapping α from Λ into the 1-sphere such that (α, H) is an Appell-Humbert datum is determined by the complex numbers

$$\alpha_i = \alpha(\lambda_i),\ i = 1, \ldots, 2n.$$

On the other hand, if we are given complex numbers

$$\alpha_i \in S^1,\ i = 1, \ldots, 2n,$$

then there exists a mapping α from Λ into the 1-sphere such that (α, H) is an Appell-Humbert datum and $\alpha(\lambda_i) = \alpha_i$, $i = 1, \ldots, 2n$. For, define

$\delta\colon \Lambda \to \mathbb{Z}$ by

$$\delta(\lambda) = \sum_{i<j} m_i m_j E(\lambda_i, \lambda_j),$$

where $\lambda = \sum m_i \lambda_i$. Then, for every $\lambda, \lambda' \in \Lambda$,

$$\begin{aligned} \delta(\lambda + \lambda') &= \sum_{i<j} (m_i + m_i')(m_j + m_j') E(\lambda_i, \lambda_j) \\ &\equiv \delta(\lambda) + \delta(\lambda') + \sum_{i<j} (m_i m_j' - m_j m_i') E(\lambda_i, \lambda_j) \pmod 2 \\ &= \delta(\lambda) + \delta(\lambda') + \sum_{i,j} m_i m_j' E(\lambda_i, \lambda_j) \\ &= \delta(\lambda) + \delta(\lambda') + E(\lambda, \lambda'), \end{aligned}$$

where $\lambda = \sum m_i \lambda_i$ and $\lambda' = \sum m_i' \lambda_i$. Hence,

$$\alpha(\lambda) = (-1)^{\delta(\lambda)} \prod_{i=1}^{2n} \alpha_i^{m_i},$$

where $\lambda = \sum m_i \lambda_i$, defines a mapping α from Λ into the 1-sphere such that (α, H) is an Appell-Humbert datum.

As a consequence we have an evident exact sequence

$$0 \longrightarrow \mathrm{Hom}(\Lambda, S^1) \longrightarrow \mathrm{AH}(V, \Lambda) \longrightarrow \mathcal{H}(V, \Lambda) \longrightarrow 0,$$

where $\mathcal{H}(V, \Lambda)$ is the group of Hermitian forms H on V with $E = \operatorname{Im} H$ integral on Λ. □

Let us turn our attention to invertible sheaves on abelian varieties over $\mathbb{C}$. If we have an invertible sheaf $\mathcal{L}$ on the abelian variety X over $\mathbb{C}$ then the associated *geometric line bundle* $V(\mathcal{L})$ [13, p. 128] is itself an algebraic variety over $\mathbb{C}$. In particular, the set of complex points $V(\mathcal{L})(\mathbb{C})$ is a complex analytic line bundle over $X(\mathbb{C})$. We will denote this line bundle by $\mathcal{L}(\mathbb{C})$. The following theorem is then a direct consequence of the GAGA-principle [27, p. 19] and Theorem 53.

Theorem 55. *Let X be an abelian variety over $\mathbb{C}$, (V, Λ) a lattice and $\pi\colon V \to X(\mathbb{C})$ a mapping which induces an isomorphism $\widetilde{\pi}$ from V/Λ*

onto $X(\mathbb{C})$. Then, the mapping from $\operatorname{Pic} X$ *into the group of (isomorphism classes of) complex analytic line bundles on V/Λ, given by*

$$\mathcal{L} \longmapsto \widetilde{\pi}^{\star}\mathcal{L}(\mathbb{C})$$

is an isomorphism. In particular, for every Appell-Humbert datum (α, H) for (V, Λ) there exists a unique invertible sheaf $\mathcal{L}$ on X such that

$$\widetilde{\pi}^{\star}\mathcal{L}(\mathbb{C}) \cong L(\alpha, H).$$

Remark 56. Let X be an abelian variety over $\mathbb{C}$, (V, Λ) a lattice and $\pi\colon V \to X(\mathbb{C})$ a mapping which induces an isomorphism $\widetilde{\pi}$ from V/Λ onto $X(\mathbb{C})$. One knows [23, p. 30] that $\mathcal{L}$ is ample if and only if H is positive definite, where $\mathcal{L}$ is an invertible sheaf on X and (α, H) is an Appell-Humbert datum for (V, Λ) such that

$$L(\alpha, H) \cong \widetilde{\pi}^{\star}\mathcal{L}(\mathbb{C}).$$

Moreover, it is proved in [23, p. 184] that $\mathcal{L}$ is an element of $\operatorname{Pic}^{\mathrm{o}} X$ if and only if $H = 0$. □

Remark 57. By Theorem 55 and Remark 56 we have a good knowledge of the group $\operatorname{Pic} X$ of the abelian variety X over $\mathbb{C}$. For, if (V, Λ) is a lattice such that $V/\Lambda \cong X(\mathbb{C})$ then we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Hom}(\Lambda, S^1) & \longrightarrow & \operatorname{AH}(V, \Lambda) & \longrightarrow & \mathcal{H}(V, \Lambda) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \operatorname{Pic}^{\mathrm{o}} X & \longrightarrow & \operatorname{Pic} X & \longrightarrow & \operatorname{NS}(X) & \longrightarrow & 0 \end{array}$$

where the vertical arrows are isomorphisms and the horizontal sequences are exact. □

2.3 Conjugate analytic varieties

In contrast with the existence of a conjugate algebraic variety X^{σ}, for every algebraic variety X over $\mathbb{C}$ and every automorphism σ of $\mathbb{C}$, there seems only to exist something like a conjugate variety M^{σ}, for a complex analytic variety M, if the automorphism σ of $\mathbb{C}$ is continuous, i.e. σ is either the identity or complex conjugation. Let us give the construction of the *conjugate complex analytic variety* M^σ of the complex analytic variety M in the case that σ is complex conjugation.

Since a complex analytic variety is a locally ringed space $(M, \mathcal{O}_M)$, where $\mathcal{O}_M$ is a sheaf of local $\mathbb{C}$-algebras, one can define the sheaf $\mathcal{O}_M^\sigma$ of local $\mathbb{C}$-algebras by letting $\Gamma(U, \mathcal{O}_M^\sigma)$ be the ring $\Gamma(U, \mathcal{O}_M)$ with the conjugate $\mathbb{C}$-algebra structure, i.e.

$$\lambda \cdot f = \sigma(\lambda) f,$$

for any $f \in \Gamma(U, \mathcal{O}_M^\sigma)$, U open in M and $\lambda \in \mathbb{C}$. The topological space M, equipped with the sheaf of local $\mathbb{C}$-algebras $\mathcal{O}_M^\sigma$, defines the locally ringed space M^σ.

There is an obvious morphism of locally ringed spaces

$$\varphi_M \colon M \longrightarrow M^\sigma,$$

such that φ_M is just the identity on the underlying topological space M and $\varphi_M^\#(f) = f$ for any $f \in \Gamma(U, \mathcal{O}_M^\sigma)$ and U open in M^σ. Observe that φ_M is not a morphism of complex analytic varieties. For, φ_M is not $\mathbb{C}$-linear (but anti-$\mathbb{C}$-linear).

One can check that M^σ is a complex analytic variety whenever M is one (here one will need continuity of the action of σ on $\mathbb{C}$). Moreover, the assignment $M \mapsto M^\sigma$ extends to a functor from the category of complex analytic varieties into itself. For, if $f \colon M \to N$ is a morphism of complex analytic varieties then

$$f^\sigma \colon M^\sigma \longrightarrow N^\sigma,$$

defined by $f^\sigma = \varphi_N \circ f \circ \varphi_M^{-1}$, is a morphism of complex analytic varieties.

Observe that, if V is a complex vector space, there is some ambiguity in the symbol V^σ. For, both the conjugate complex vector space structure on V and the conjugate complex analytic variety V^σ are denoted by V^σ. Fortunately, both objects are canonically isomorphic as complex analytic varieties. This justifies our notation.

Example 58. Let M be a complex torus and V its tangent space at the unit element. Then, the conjugate complex vector space structure

V^σ on V is the tangent space to M^σ at the unit element of M^σ and the holomorphic mapping

$$\exp_M^\sigma : V^\sigma \longrightarrow M^\sigma$$

is equal to the exponential mapping $\exp_{M^\sigma}$ of M^σ. This follows easily from the definition of the exponential mapping.

In particular, if $M = V/\Lambda$, for some lattice $\Lambda \subseteq V$, then $\Lambda^\sigma = \varphi_V(\Lambda)$ is a lattice in V^σ and M^σ is isomorphic to V^σ/Λ^σ.

In the special case that $V = \mathbb{C}^n$, one can identify V^σ with $\mathbb{C}^n$ via

$$\begin{array}{rcl} V^\sigma & \longrightarrow & \mathbb{C}^n \\ v & \longmapsto & \overline{\varphi_V^{-1}(v)}. \end{array}$$

Hence, if $M = \mathbb{C}^n/\Lambda$ then M^σ is isomorphic to $\mathbb{C}^n/\overline{\Lambda}$. □

If we have an algebraic variety X over $\mathbb{C}$ then, on the one hand, we can take the complex analytic variety $X^\sigma(\mathbb{C})$ associated to the conjugate algebraic variety X^σ and, on the other hand, we have just defined the conjugate analytic variety $X(\mathbb{C})^\sigma$ of the analytic variety $X(\mathbb{C})$ associated to X. It is easy to see that both constructions give rise to the same complex analytic variety. More precisely, the functors

$$X \longmapsto X^\sigma(\mathbb{C}) \quad \text{and} \quad X \longmapsto X(\mathbb{C})^\sigma$$

from the category of algebraic varieties over $\mathbb{C}$ into the category of complex analytic varieties are naturally isomorphic.

Furthermore, if $p: L \to M$ is a complex analytic line bundle on M then

$$p^\sigma : L^\sigma \longrightarrow M^\sigma$$

is a complex analytic line bundle on M^σ, called the *conjugate line bundle.*

In the particular case that $M = V/\Lambda$, where Λ is a lattice in the complex vector space V, and L is the Appell-Humbert line bundle $L(\alpha, H)$, for some Appell-Humbert datum (α, H) for (V, Λ), one can try to find an Appell-Humbert datum for $(V^\sigma, \Lambda^\sigma)$ that gives rise to a line bundle on V^σ/Λ^σ isomorphic to L^σ.

Define a Hermitian form H^σ on V^σ by

$$H^\sigma(v, v') = \overline{H(\varphi_V^{-1}(v), \varphi_V^{-1}(v'))},$$

for every $v, v' \in V^\sigma$, and define a mapping α^σ from Λ^σ into S^1 by

$$\alpha^\sigma(\lambda) = \overline{\alpha(\varphi_V^{-1}(\lambda))},$$

for every $\lambda \in \Lambda^\sigma$. Then, it is easy to check that $(\alpha^\sigma, H^\sigma)$ is an Appell-Humbert datum for $(V^\sigma, \Lambda^\sigma)$.

Lemma 59. *If $M = V/\Lambda$, where Λ is a lattice in the complex vector space V, and (α, H) is an Appell-Humbert datum for (V, Λ) then the conjugate line bundle $L(\alpha, H)^\sigma$ of $L(\alpha, H)$ is isomorphic to the line bundle $L(\alpha^\sigma, H^\sigma)$.*

Proof. The conjugate line bundle $L(\alpha, H)^\sigma$ is the quotient of $V^\sigma \times \mathbb{C}$ under the action of Λ^σ given by

$$\lambda(v, z) = (v + \lambda, \overline{e_{\varphi_V^{-1}(\lambda)}(\varphi_V^{-1}(v))}z),$$

where $v \in V^\sigma$, $z \in \mathbb{C}$, $\lambda \in \Lambda^\sigma$ and e_μ, for $\mu \in \Lambda$, is the holomorphic function on V associated with the Appell-Humbert datum (α, H). Put $\lambda' = \varphi_V^{-1}(\lambda)$ and $v' = \varphi_V^{-1}(v)$. Then

$$\overline{e_{\lambda'}(v')} = \overline{\alpha(\lambda')}\overline{e^{\pi H(v', \lambda') + \frac{1}{2}\pi H(\lambda', \lambda')}} = \alpha^\sigma(\lambda) e^{\pi H^\sigma(v, \lambda) + \frac{1}{2}\pi H^\sigma(\lambda, \lambda)}$$

is equal to the function e_λ, associated with the Appell-Humbert datum $(\alpha^\sigma, H^\sigma)$. Therefore, $L(\alpha, H)^\sigma$ is isomorphic to $L(\alpha^\sigma, H^\sigma)$. □

Let G denote the Galois group of $\mathbb{C}/\mathbb{R}$. If G acts on the complex analytic variety M such that the action of σ is anti-holomorphic then this action of G on M is called a *real structure* on M. Let M and N be complex analytic varieties with a real structure. A mapping f from M into N is a *morphism of complex analytic varieties with a real structure* if f is an analytic mapping and f is G-equivariant.

This notion of a real structure will be interesting for us since, if X is an abelian variety over $\mathbb{R}$ then the complex analytic variety $X(\mathbb{C})$ has a natural real structure.

Remark 60. If a complex analytic variety M has a real structure then the conjugate complex analytic variety M^σ can be canonically identified with M in the following way. The mapping

$$\begin{aligned} M^\sigma &\longrightarrow M \\ m &\longmapsto \sigma\varphi_M^{-1}(m) \end{aligned}$$

is an isomorphism of complex analytic varieties, moreover this isomorphism is natural in M. Clearly, the mapping φ_M from M into M^σ corresponds under this isomorphism to the action of σ on M. Therefore, if M is a complex analytic variety with a real structure we may identify M^σ with M through the isomorphism above. The mapping φ_M is then the action of σ on M. In particular, if M and N are complex analytic varieties with a real structure and f is just an analytic mapping from M into N then, under these identifications of M^σ with M and N^σ with N, f^σ is an analytic mapping from M into N satisfying

$$f^\sigma(m) = \sigma f(\sigma^{-1}m),$$

for $m \in M$.

Furthermore, if M is a complex analytic variety with a real structure and $p\colon L \to M$ is a complex analytic line bundle on M, then the conjugate line bundle L^σ is a line bundle on M, under the identification of M^σ with M. □

Assumption 61. Of course, in the special case that M is a complex torus, it might happen that a real structure on M does not have the unit element of M as a fixed point. However, since we will only meet such tori of the form $X(\mathbb{C})$, where X is an abelian variety over $\mathbb{R}$, we may as well assume that a real structure on a complex torus has the unit element as a fixed point. □

Suppose M is a complex torus with a real structure. Then, according to the above assumption, the unit element 0 of M is invariant under the action of G. Hence, we get an induced action of G on the tangent space V to M at 0. In fact, this action is a real structure on the complex analytic variety V. Hence, by Example 58 and Remark 60, the exponential mapping

$$\exp\colon V \to M$$

is G-equivariant. In particular, the kernel $\ker\exp$ is invariant under the G-action.

Definition 62. *Let us define the category* $\mathcal{M}_{\mathbb{R}}$ *of* lattices over $\mathbb{R}$ *by taking as objects pairs* (W, Λ)*, where* W *is a finite-dimensional* $\mathbb{R}$*-vector space and*

$$\Lambda \subseteq W \otimes_{\mathbb{R}} \mathbb{C}$$

is a lattice, stable under the canonical action of G *on* $W \otimes_{\mathbb{R}} \mathbb{C}$*, and as morphisms from* (W, Λ) *into* (W', Λ') $\mathbb{R}$*-linear mappings* $L\colon W \to W'$ *such that*

$$(L \otimes \mathbb{C})(\Lambda) \subseteq \Lambda'.$$

We see that, if M is a complex torus with a real structure, the pair

$$(V^G, \ker\exp)$$

is a lattice over $\mathbb{R}$. This proves, together with Theorem 50, the following proposition.

Proposition 63. *(under Assumption* 61*) The functor*

$$M \longmapsto ((T_0 M)^G, \ker\exp)$$

is an equivalence from the category of complex tori having a real structure into the category $\mathcal{M}_{\mathbb{R}}$ *of lattices over* $\mathbb{R}$*. The functor*

$$(W, \Lambda) \longmapsto W \otimes_{\mathbb{R}} \mathbb{C}/\Lambda$$

from the category $\mathcal{M}_{\mathbb{R}}$ *into the category of complex tori having a real structure serves as an inverse.* □

Let us turn our attention to real structures on line bundles. If M is a complex analytic variety with a real structure then a *real structure* on a complex analytic line bundle $p\colon L \to M$ is a real structure on the total space L such that p is a morphism of complex analytic varieties with a real structure and the action of G is $\mathbb{R}$-linear on each fibre.

Remark 64. If W is a real vector space and $V = W \otimes_{\mathbb{R}} \mathbb{C}$ then it is clear that, making the identification of V^σ with V as in Remark 60,

$$H^\sigma(v, v') = \overline{H(\sigma^{-1}v, \sigma^{-1}v')},$$

for any $v, v' \in V$. Moreover, if $\Lambda \subseteq V$ is a lattice, stable under the action of G and α is a mapping from Λ into S^1 then

$$\alpha^\sigma(\lambda) = \overline{\alpha(\sigma^{-1}\lambda)},$$

for any $\lambda \in \Lambda$. Hence, if (W, Λ) is a lattice over $\mathbb{R}$ and $M = V/\Lambda$, where $V = W \otimes_{\mathbb{R}} \mathbb{C}$, then the existence of a real structure on the complex line bundle $L(\alpha, H)$, for some Appell-Humbert datum (α, H) for (W, Λ), implies that

$$\alpha^\sigma = \alpha \quad \text{and} \quad H^\sigma = H,$$

by Lemma 59.

Conversely, if (α, H) is an Appell-Humbert datum for (V, Λ) such that $\alpha^\sigma = \alpha$ and $H^\sigma = H$, then there exists a real structure on the complex line bundle $L(\alpha, H)$ on V/Λ. For, G acts on the trivial line bundle $V \times \mathbb{C}$ by

$$\sigma(v, z) = (\sigma v, \overline{z}).$$

This action factorizes through the quotient of $V \times \mathbb{C}$ by the action of Λ, since

$$\begin{aligned}
\sigma(\lambda(v, z)) &= (\sigma v + \sigma\lambda, \overline{e_\lambda(v) z}) \\
&= (\sigma v + \sigma\lambda, e_{\sigma\lambda}(\sigma v)\overline{z}) \\
&= (\sigma\lambda)(\sigma v, \overline{z}) \\
&= (\sigma\lambda)(\sigma(v, z)),
\end{aligned}$$

where e_λ is the holomorphic function associated to (α, H). Therefore, $L(\alpha, H)$ has a real structure. □

Observe that, if W is a real vector space and F is a symmetric bilinear form on W, we can define a Hermitian form $F \otimes \mathbb{C}$ on $V = W \otimes \mathbb{C}$, determined by

$$(F \otimes \mathbb{C})(w \otimes \alpha, w' \otimes \alpha') = \alpha\overline{\alpha'} F(w, w'),$$

Conversely, if H is a Hermitian form on V such that $H^\sigma = H$ then there exists a symmetric bilinear form F on W such that $F \otimes \mathbb{C} = H$. Moreover, F is an inner product if and only if H is positive definite.

If (W, Λ) is a lattice over $\mathbb{R}$, let us call a pair (α, F), where α is a mapping from Λ into S^1 and F is a symmetric bilinear form on W, an *Appel-Humbert datum over* $\mathbb{R}$ for (W, Λ) if $\alpha^\sigma = \alpha$ and $(\alpha, F \otimes \mathbb{C})$ is an Appel-Humbert datum for $(W \otimes_{\mathbb{R}} \mathbb{C}, \Lambda)$. In such case, it is proved in Remark 64 that the complex analytic line bundle $L(\alpha, F \otimes \mathbb{C})$ over V/Λ, where $V = W \otimes_{\mathbb{R}} \mathbb{C}$, has a canonical real structure. Let us denote the complex analytic line bundle $L(\alpha, F \otimes \mathbb{C})$ over V/Λ together with this real structure by $L(\alpha, F)$.

We will denote the set of Appell-Humbert data over $\mathbb{R}$ for the lattice (W, Λ) over $\mathbb{R}$ by $\mathrm{AH}(W, \Lambda)$. This set is made into a group when we define the group structure by

$$(\alpha_1, F_1)(\alpha_2, F_2) = (\alpha_1\alpha_2, F_1 + F_2).$$

Clearly, the mapping L from the group $\mathrm{AH}(W, \Lambda)$ into the group of (isomorphism classes of) complex analytic line bundles on V/Λ having a real structure is a morphism of groups. Then, we have a real version of the Theorem of Appell-Humbert.

Lemma 65. *Let (W, Λ) be a lattice over $\mathbb{R}$ and put $V = W \otimes_{\mathbb{R}} \mathbb{C}$. If L is a complex analytic line bundle on V/Λ with a real structure, then there exists a unique Appel-Humbert datum (α, F) over $\mathbb{R}$ for (W, Λ) such that*

$$L(\alpha, F) \cong L,$$

as complex line bundles with a real structure. In other words, the mapping L from the group $\mathrm{AH}(W, \Lambda)$ into the group of (isomorphism classes of) complex analytic line bundles on V/Λ having a real structure is an isomorphism.

Proof. By Remark 64, if L is a complex analytic line bundle on V/Λ with a real structure then there exists an Appel-Humbert datum (α, H) for (V, Λ) such that $L(\alpha, H)$ is isomorphic to L as complex line bundles over V/Λ. Moreover, $\alpha^\sigma = \alpha$ and $H^\sigma = H$, hence there exists a unique Appel-Humbert datum (α, F) over $\mathbb{R}$ for (W, Λ) such that $L(\alpha, F)$ and

L are isomorphic as complex analytic line bundles. We have to show that this isomorphism can be chosen to be G-equivariant.

This can be shown most conveniently using the theory of forms [28, p. III-1]. For, L is a form of $L(\alpha, F)$ with respect to the field extension $\mathbb{C}/\mathbb{R}$. Hence, we would have proved the lemma if we show that the first cohomology group

$$H^1(G, \operatorname{Aut} L(\alpha, F \otimes \mathbb{C}))$$

is trivial. Indeed $\operatorname{Aut} L(\alpha, F \otimes \mathbb{C}) = \mathbb{C}^\star$, since V/Λ is compact, and this identity holds even G-equivariantly. One knows that $H^1(G, \mathbb{C}^\star)$ is trivial. The lemma follows. □

2.4 Abelian varieties over $\mathbb{R}$

If X is an abelian variety over $\mathbb{R}$ then, as mentioned in Section 2.2, the set of complex points $X(\mathbb{C})$ is a complex torus with a real structure. Hence, if we put $W = (T_0 X(\mathbb{C}))^G$ and $\Lambda = \ker \exp$ then (W, Λ) is a lattice over $\mathbb{R}$.

If $\mathcal{L}$ is an invertible sheaf on X, the *geometric line bundle* $V(\mathcal{L})$ associated to $\mathcal{L}$ [13, p. 128] is an algebraic variety over $\mathbb{R}$ itself. Therefore,

$$V(\mathcal{L})(\mathbb{C}) \longrightarrow X(\mathbb{C})$$

is a complex analytic line bundle on $X(\mathbb{C})$ with a real structure, denoted by $\mathcal{L}(\mathbb{C})$.

Theorem 66. *The functor*

$$X \longmapsto ((T_0 X(\mathbb{C}))^G, \ker \exp)$$

is an equivalence from the category of abelian varieties over $\mathbb{R}$ *onto the full subcategory of the category* $\mathcal{M}_\mathbb{R}$ *consisting of pairs* (W, Λ) *such that there exists an inner product* F *on* W *with* $E = \operatorname{Im}(F \otimes \mathbb{C})$ *integral on* Λ.

Proof. Suppose that X is an abelian variety over $\mathbb{R}$ and let (W, Λ) be the lattice $((T_0 X(\mathbb{C}))^G, \ker \exp)$ over $\mathbb{R}$. Since X is projective (see Section 2.1), there exists an ample invertible sheaf $\mathcal{L}$ on X. In particular,

$\mathcal{L}(\mathbb{C})$ is a complex analytic line bundle on $X(\mathbb{C})$ with a real structure. Hence, by Lemma 65, there exists an Appell-Humbert datum (α, F) over $\mathbb{R}$ for (W, Λ) such that

$$L(\alpha, F) \cong \mathcal{L}(\mathbb{C}).$$

Since $\mathcal{L}$ is ample, the Hermitian form $F \otimes \mathbb{C}$ is an inner product by Remark 56. Therefore, F is an inner product.

Conversely, if (W, Λ) is a lattice over $\mathbb{R}$ and F is an inner product on W with $E = \operatorname{Im}(F \otimes \mathbb{C})$ integral on Λ then we know from Theorem 51 that there exists an abelian variety Y over $\mathbb{C}$ such that $Y(\mathbb{C})$ is isomorphic to V/Λ, where $V = W \otimes_{\mathbb{R}} \mathbb{C}$. Using the GAGA-principle [27], the real structure on V/Λ gives rise to a descent datum for Y with respect to the field extension $\mathbb{C}/\mathbb{R}$. According to Theorem 22, there exists an algebraic variety X over $\mathbb{R}$ such that $X_{\mathbb{C}}$ and Y are G-equivariantly isomorphic. In particular, $X(\mathbb{C})$ and V/Λ are isomorphic as complex tori having a real structure. Of course, X is an abelian variety over $\mathbb{R}$.

The fact that the above functor is full follows from the GAGA-principle [27] and Proposition 63. Faithfulness is trivial. □

Remark 67. As a consequence of Theorem 66, if Λ is a lattice in $\mathbb{C}^n$, stable under the action of σ on $\mathbb{C}^n$ and such that there exists a positive definite Hermitian form H on $\mathbb{C}^n$ with $E = \operatorname{Im} H$ integral on Λ, then there exists an abelian variety X over $\mathbb{R}$ such that

$$X(\mathbb{C}) \cong \mathbb{C}^n/\Lambda$$

as complex tori with a real structure. For this, it is crucial that the action of the Galois group G of $\mathbb{C}/\mathbb{R}$ on $V = W \otimes_{\mathbb{R}} \mathbb{C}$ is continuous.

To illustrate this point, take instead of $\mathbb{R}$ the subfield

$$K = \mathbb{Q}\left(\sqrt{-5}\right)$$

of $\mathbb{C}$ and let G be the group of automorphisms of $\mathbb{C}$ over K. Let $\Lambda \subseteq \mathbb{C}$ be the lattice

$$\mathbb{Z} + \mathbb{Z}\sqrt{-5}.$$

Then, Λ is invariant under the action of G on $\mathbb{C}$ and there exists a positive definite Hermitian form H on $\mathbb{C}^n$ with $E = \operatorname{Im} H$ integral on Λ, according to Example 52. But, there does not exist an abelian variety X over K such that $X(\mathbb{C})$ is isomorphic to $\mathbb{C}/\Lambda$ as complex tori. Indeed, it is the theory of complex multiplication [29] which tells us that one has to enlarge the field K to its Hilbert class field L. More precisely, there exists an abelian variety X over L such that $X(\mathbb{C})$ is isomorphic to V/Λ as complex Lie groups. In our case $L = K(\sqrt{-1})$ will do. □

Theorem 68. *Let X be an abelian variety over $\mathbb{R}$, (W, Λ) a lattice over $\mathbb{R}$ and $\pi: V \to X(\mathbb{C})$ a mapping which induces an isomorphism of complex tori having a real structure $\widetilde{\pi}$ from V/Λ onto $X(\mathbb{C})$, where $V = W \otimes_{\mathbb{R}} \mathbb{C}$. Then, the mapping from $\operatorname{Pic} X$ into the group of (isomorphism classes of) complex analytic line bundles on V/Λ having a real structure, given by*

$$\mathcal{L} \longmapsto \widetilde{\pi}^{\star}\mathcal{L}(\mathbb{C})$$

is an isomorphism. In particular, for every Appell-Humbert datum (α, F) over $\mathbb{R}$ for (W, Λ) there exists a unique invertible sheaf $\mathcal{L}$ on X such that

$$\widetilde{\pi}^{\star}\mathcal{L}(\mathbb{C}) \cong L(\alpha, F),$$

as complex analytic line bundles having a real structure.

Proof. The first part follows from the GAGA-principle [27] and the Theorem of descent. The last part is then a direct consequence of the real version of the Appell-Humbert Theorem (Lemma 65). □

Theorem 68 will give us good insight in the group $\operatorname{Pic} X$ of isomorphism classes of invertible sheaves on the abelian variety X over $\mathbb{R}$ (see Remark 73).

Let $\mathcal{F}(W, \Lambda)$ be the group of symmetric bilinear forms F on W with $E = \operatorname{Im}(F \otimes \mathbb{C})$ integral on Λ. Then the projection

$$\mathrm{AH}(W, \Lambda) \longrightarrow \mathcal{F}(W, \Lambda)$$

is surjective. This is implied by the following lemma.

Lemma 69. *If (W, Λ) is a lattice over $\mathbb{R}$ and F is a symmetric bilinear form on W with $E = \mathrm{Im}\,(F \otimes \mathbb{C})$ integral on Λ, then there exists a mapping*

$$\alpha \colon \Lambda \longrightarrow S^1$$

such that (α, F) is an Appell-Humbert datum over $\mathbb{R}$ for (W, Λ).

Actually, this lemma is a consequence of Proposition 72. For the proof of this proposition we will need the following proposition, which describes the structure of lattices over $\mathbb{R}$. We will omit the proof of this proposition.

Let us first introduce the following notation. If the Galois group G of $\mathbb{C}/\mathbb{R}$ acts on a group H then we define

$$\mathrm{Re}\, H = \{h \in H \mid \sigma h = h\}$$

and

$$\mathrm{Im}\, H = \{h \in H \mid \sigma h = -h\},$$

where σ is the nontrivial element of G.

Proposition 70. *Let W be a real vector space of dimension n and let $\Lambda \subseteq V$ be a lattice, invariant under the action of G on $V = W \otimes_{\mathbb{R}} \mathbb{C}$. Then there exist a $\mathbb{Z}$-basis $x_1, \ldots, x_n$ for $\mathrm{Re}\,\Lambda$ and a $\mathbb{Z}$-basis $y_1, \ldots, y_n$ for $\mathrm{Im}\,\Lambda$ such that*

$$\tfrac{1}{2}(x_1 + y_1), \ldots, \tfrac{1}{2}(x_k + y_k), x_1, \ldots, x_n, y_{k+1}, \ldots, y_n$$

is a $\mathbb{Z}$-basis for Λ, for some uniquely determined integer k, $0 \leq k \leq n$.

We will call this integer k, which is uniquely determined by Λ, the *degree of connectedness* of Λ (or (W, Λ)). We will see (cf. Corollary 84) that the number of connected components of $(V/\Lambda)^G$ is precisely 2^{n-k}, if n is the dimension of W.

Remark 71. As a consequence of Proposition 70, if W is a n-dimensional real vector space, a lattice $\Lambda \subseteq V$ over $\mathbb{R}$ is completely determined by its degree of connectedness k and the nonsingular real $n \times n$-matrix M, defined by

$$y_l = \sum_{j=1}^{n} m_{lj} i x_j,$$

where $x_1, \ldots, x_n$ is a $\mathbb{Z}$-basis for $\operatorname{Re}\Lambda$ and $y_1, \ldots, y_n$ a $\mathbb{Z}$-basis for $\operatorname{Im}\Lambda$ as in Proposition 70. For, we can make a lattice $\Lambda' \subseteq V$ over $\mathbb{R}$ out of the nonsingular real $n \times n$-matrix M and the integer k as follows. Choose an $\mathbb{R}$-basis $w_1, \ldots, w_n$ for $\operatorname{Re} V$ and define

$$v_l = \sum_{j=1}^{n} m_{lj} i w_j.$$

Then $v_1, \ldots, v_n$ is an $\mathbb{R}$-basis for $\operatorname{Im} V$ and the $\mathbb{Z}$-module $\Lambda' \subseteq V$ generated by

$$\tfrac{1}{2}(w_1 + v_1), \ldots, \tfrac{1}{2}(w_k + v_k), w_1, \ldots, w_n, v_{k+1}, \ldots, v_n$$

is a lattice over $\mathbb{R}$. Clearly, (W, Λ') and (W, Λ) are isomorphic as lattices over $\mathbb{R}$. For, if L is a linear mapping from W into itself, such that $Lw_j = x_j$, for every j, then

$$(L \otimes \mathbb{C})(\Lambda') = \Lambda.$$

Hence, L is an isomorphism from (W, Λ') onto (W, Λ). □

Proposition 72. *Let (W, Λ) be a lattice over $\mathbb{R}$ and let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis for $\operatorname{Re}\Lambda$ and $y_1, \ldots, y_n$ a $\mathbb{Z}$-basis for $\operatorname{Im}\Lambda$ such that*

$$z_1, \ldots, z_k, x_1, \ldots, x_n, y_{k+1}, \ldots, y_n$$

is a $\mathbb{Z}$-basis for Λ, where $z_j = \frac{1}{2}(x_j + y_j)$, for $j = 1, \ldots, k$. Suppose we are given a symmetric bilinear form F on W, with $E = \operatorname{Im}(F \otimes \mathbb{C})$ integral on Λ, and complex numbers $\alpha_j \in S^1$, $j = 1, \ldots, n$. Then, there exists a mapping α from Λ into S^1 such that (α, F) is an Appell-Humbert datum over $\mathbb{R}$ for (W, Λ) and $\alpha(x_j) = \alpha_j$, for every j, if and only if all α_j are ± 1 and

$$\alpha_j = (-1)^{\frac{1}{2}E(x_j, y_j)}, \text{ for } j = 1, \ldots, k.$$

Proof. Suppose we have a mapping α from Λ into S^1 such that (α, F) is an Appell-Humbert datum over $\mathbb{R}$ for (W, Λ) and $\alpha(x_j) = \alpha_j$, for every j. Since α is G-equivariant, $\alpha(x_j) = \pm 1$, for every j. Therefore, $\alpha_j = \pm 1$, for every j. Moreover,

$$\begin{aligned}
\overline{\alpha(z_j)} &= \alpha(\overline{z_j}) \\
&= \alpha(x_j - z_j) \\
&= \alpha(x_j)\alpha(z_j)^{-1}(-1)^{\frac{1}{2}E(x_j,y_j)} \\
&= \alpha(x_j)\overline{\alpha(z_j)}(-1)^{\frac{1}{2}E(x_j,y_j)},
\end{aligned}$$

for $j = 1, \ldots, k$. Hence, $\alpha_j = (-1)^{\frac{1}{2}E(x_j,y_j)}$, for $j = 1, \ldots, k$.

Conversely, if all α_j are ± 1 and $\alpha_j = (-1)^{\frac{1}{2}E(x_j,y_j)}$, for $j = 1, \ldots, k$, then, according to Remark 54, there exists a mapping

$$\alpha \colon \Lambda \longrightarrow S^1$$

such that $(\alpha, F \otimes \mathbb{C})$ is an Appell-Humbert datum for (V, Λ) and $\alpha(x_j) = \alpha_j$ for every j. The above equation shows at the same time that α is G-equivariant. Hence, (α, F) is an Appell-Humbert datum over $\mathbb{R}$ for (W, Λ). □

As a consequence of Lemma 69 we have an exact sequence

$$0 \longrightarrow \operatorname{Hom}_G(\Lambda, S^1) \longrightarrow \operatorname{AH}(W, \Lambda) \longrightarrow \mathcal{F}(V, \Lambda) \longrightarrow 0,$$

where $\operatorname{Hom}_G(\Lambda, S^1)$ is the group of G-equivariant morphisms from Λ into S^1, whenever (W, Λ) is a lattice over $\mathbb{R}$.

Remark 73. Suppose X is an abelian variety over $\mathbb{R}$ and π is a mapping from $V = W \otimes \mathbb{C}$ into $X(\mathbb{C})$ such that π induces a G-equivariant mapping

$$\widetilde{\pi} \colon V/\Lambda \longrightarrow X(\mathbb{C}).$$

Then, by Theorem 68, the mapping

$$\begin{aligned}
\operatorname{AH}(W, \Lambda) &\longrightarrow \operatorname{Pic} X \\
(\alpha, F) &\longmapsto \mathcal{L},
\end{aligned}$$

where $\mathcal{L}$ is the unique invertible sheaf on X such that $\mathcal{L}(\mathbb{C})$ is G-equivariantly isomorphic to $L(\alpha, F)$, is an isomorphism. Moreover, by Remark 56, this isomorphism maps the subgroup of $\mathrm{AH}(W, \Lambda)$ consisting of (α, F), such that $F = 0$, onto $\mathrm{Pic}^{\mathrm{o}} X$. Therefore, we have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_G(\Lambda, S^1) & \longrightarrow & \mathrm{AH}(W, \Lambda) & \longrightarrow & \mathcal{F}(W, \Lambda) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Pic}^{\mathrm{o}} X & \longrightarrow & \mathrm{Pic}\, X & \longrightarrow & \mathrm{NS}(X) & \longrightarrow & 0 \end{array}$$

where the vertical arrows are isomorphisms and the horizontal sequences are exact. □

If X is an abelian variety over $\mathbb{R}$ then, recall from Section 2.1 that the base number of X, i.e. the rank of the Néron-Severi group of X is finite. Since the canonical mapping

$$\mathrm{Pic}\, X \to \mathrm{Pic}\, X_{\mathbb{C}}$$

is injective, the base number of X is smaller than or equal to the base number of $X_{\mathbb{C}}$. In particular, the base number of X is smaller than or equal to $n(2n-1)$, if n is the dimension of X. We will prove in Corollary 76 that this number is even smaller than or equal to $\frac{1}{2}n(n+1)$. For this we need some preparation.

If A is an $n \times n$-matrix, let us denote the transpose matrix of A by A^T.

Proposition 74. *Let (W, Λ) be a lattice over $\mathbb{R}$. Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis for $\mathrm{Re}\, \Lambda$ and $y_1, \ldots, y_n$ be a $\mathbb{Z}$-basis for $\mathrm{Im}\, \Lambda$ as in Proposition 70. In particular, k is the degree of connectedness of Λ. Then, there is a one-to-one correspondence between the set of symmetric bilinear forms F on W with $E = \mathrm{Im}\,(F \otimes \mathbb{C})$ integral on Λ and the set of $\mathbb{R}$-linear pairings*

$$e\colon \mathrm{Re}\, V \times \mathrm{Im}\, V \longrightarrow \mathbb{R}$$

such that

(i) *e is integral on $\mathrm{Re}\, \Lambda \times \mathrm{Im}\, \Lambda$,*

(ii) *$e(x_j, y_l) \equiv 0 \bmod 2$, if $j \leq k$ or $l \leq k$,*

(iii) *$e(x_j, y_l) \equiv e(x_l, y_j) \bmod 4$, if $j \leq k$ and $l \leq k$,*

(iv) $e(iv_2, iv_1) = -e(v_1, v_2)$, *for all* $v_1 \in \operatorname{Re} V$ *and* $v_2 \in \operatorname{Im} V$.
More precisely,

$$F \longmapsto e$$

where $e = E\restriction_{\operatorname{Re} V \times \operatorname{Im} V}$ *and* $E = \operatorname{Im}(F \otimes \mathbb{C})$, *defines such a correspondence. Moreover,* F *is an inner product if and only if* e *is nondegenerate and* $e(iv, v) > 0$, *for all nonzero* $v \in \operatorname{Im} V$.

Proof. If F is a symmetric bilinear form on W with $E = \operatorname{Im}(F \otimes \mathbb{C})$ integral on Λ then

$$e \colon \operatorname{Re} V \times \operatorname{Im} V \longrightarrow \mathbb{R},$$

defined by $e(v_1, v_2) = E(v_1, v_2)$, is indeed an $\mathbb{R}$-linear pairing and satisfies the properties above since $E(v, v') = 0$, whenever $v, v' \in \operatorname{Re} V$ or $v, v' \in \operatorname{Im} V$.

Conversely, suppose we are given an $\mathbb{R}$-linear pairing e on $\operatorname{Re} V \times \operatorname{Im} V$ which satisfies the properties above. Let σ be the nontrivial element of the Galois group G of $\mathbb{C}/\mathbb{R}$ and let $p_1 \colon V \to \operatorname{Re} V$ be defined by

$$p_1(v) = \tfrac{1}{2}(v + \sigma v)$$

and $p_2 \colon V \to \operatorname{Im} V$ defined by

$$p_2(v) = \tfrac{1}{2}(v - \sigma v),$$

then $E(v, v') = e(p_1(v), p_2(v')) - e(p_1(v'), p_2(v))$ defines an alternating bilinear form E on $V \times V$. Since $p_1(iv) = ip_2(v)$, we see that $E(iv, iv') = E(v, v')$. Hence, as explained in Section 2.2, there exists a unique Hermitian form H on V such that

$$\operatorname{Im} H = E.$$

It is also clear that $E(\sigma v, \sigma v') = -E(v, v')$. Therefore, there exists a unique symmetric bilinear form F on W such that $F \otimes \mathbb{C} = H$.

Hence, we would have finished the proof of the first assertion if we have shown that E, as defined above, is integral on Λ. This follows from the properties (i), (ii) and (iii) of e.

Finally, F is an inner product if and only if $E(iv, v) > 0$, for all nonzero $v \in V$. The latter statement is equivalent to $e(iv, v) > 0$, for all nonzero $v \in \operatorname{Im} V$. This proves the proposition. $\square$

Define, for a real $n \times n$-matrix M and for an integer k, the additive group $S_k(M)$ of integral $n \times n$-matrices $N = (n_{jl})$ such that

$$(MN)^T = MN$$

and $n_{jl} \equiv 0 \bmod 2$, if $j \leq k$ or $l \leq k$, and $n_{lj} \equiv n_{jl} \bmod 4$, if $j \leq k$ and $l \leq k$.

Proposition 75. *Let (W, Λ) be a lattice over $\mathbb{R}$ and let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis for $\operatorname{Re}\Lambda$ and $y_1, \ldots, y_n$ a $\mathbb{Z}$-basis for $\operatorname{Im}\Lambda$ such that as in Proposition 70. Let $M = (m_{lj})$ be the invertible real $n \times n$-matrix such that*

$$y_l = \sum_{j=1}^{n} m_{lj} i x_j.$$

Then the group of $\mathbb{R}$-linear pairings e on $\operatorname{Re}V \times \operatorname{Im}V$, such that e satisfies conditions (i), (ii), (iii) and (iv) of Proposition 74 is isomorphic to the group $S_k(M)$. An isomorphism is given by

$$e \longmapsto N,$$

where $N = (n_{jl})$ and $n_{jl} = e(x_j, y_l)$. Moreover, e is nodegenerate and $e(iv, v) > 0$, for all nonzero $v \in \operatorname{Im}V$, if and only if MN is negative definite, *i.e. $-MN$ is positive definite.*

Proof. Let us denote the element of the matrix A that is in the j^{th} row and the l^{th} column by A_{jl}. Then, if e is an $\mathbb{R}$-linear pairing on $\operatorname{Re}V \times \operatorname{Im}V$ and N is the matrix (n_{jl}), where $n_{jl} = e(x_j, y_l)$, the pairing e satisfies conditions (i), (ii) and (iii) of Proposition 74 if and only if N is an *integral matrix*, i.e.

$$N \in \mathbf{M}_n(\mathbb{Z}),$$

and $n_{jl} \equiv 0 \bmod 2$, if $j \leq k$ or $l \leq k$, and $n_{lj} \equiv n_{jl} \bmod 4$, if $j \leq k$ and $l \leq k$.

Let us denote the (j, l)-element of M^{-1} by m_{jl}^{-1}, by abuse of notation. Then

$$x_j = -\sum_{p=1}^{n} m_{jp}^{-1} i y_p$$

and

$$\begin{aligned}
-e(iy_l, ix_j) &= e\left(\sum_{q=1}^{n} m_{lq}x_q, \sum_{p=1}^{n} m_{jp}^{-1}y_p\right) \\
&= \sum_{p=1}^{n}\sum_{q=1}^{n} m_{jp}^{-1}m_{lq}n_{qp} \\
&= \sum_{p=1}^{n} m_{jp}^{-1}(MN)_{lp} \\
&= \sum_{p=1}^{n} m_{jp}^{-1}((MN)^T)_{pl} \\
&= (M^{-1}(MN)^T)_{jl}.
\end{aligned}$$

Hence, $e(iv_2, iv_1) = -e(v_1, v_2)$, for all $v_1 \in \operatorname{Re} V$ and $v_2 \in \operatorname{Im} V$, if and only if $(MN)^T = MN$. This shows the first statement.

To prove the second statement, choose $a_i \in \mathbb{R}$, $i = 1, \ldots, n$, and compute

$$\begin{aligned}
e(i\sum_{p=1}^{n} a_p y_p, \sum_{q=1}^{n} a_q y_q) &= \sum_{p,q=1}^{n} a_p a_q e(iy_p, y_q) \\
&= -\sum_{p,q=1}^{n} a_p a_q e(\sum_{j=1}^{n} m_{pj}x_j, y_q) \\
&= -\sum_{p,q=1}^{n} a_p (MN)_{pq} a_q \\
&= -a^T \cdot MN \cdot a.
\end{aligned}$$

Hence, $e(iv, v) > 0$, for all nonzero $v \in \operatorname{Im} V$, if and only if MN is negative definite. This proves the proposition. □

As a consequence of Theorem 66, Remark 73 and Propositions 74 and 75 we have the following corollary.

Corollary 76. *If (W, Λ) is a lattice over $\mathbb{R}$ then $\mathcal{F}(W, \Lambda)$ is isomorphic to the group $S_k(M)$, where k is the degree of connectedness of Λ and M*

is the real $n \times n$*-matrix associated to* Λ *as in Remark* 71*. Furthermore, there exists an abelian variety* X *over* $\mathbb{R}$ *such that* $X(\mathbb{C})$ *is isomorphic to* V/Λ*, as complex tori with a real structure, if and only if* $S_k(M)$ *contains a matrix* N *such that* MN *is negative definite. Moreover, then the Néron-Severi group* $\mathrm{NS}(X)$ *of* X *is isomorphic to* $S_k(M)$*. In particular, the base number of an* n*-dimensional abelian variety over* $\mathbb{R}$ *is smaller than or equal to* $\frac{1}{2}n(n+1)$*.*

Proof. Indeed, Proposition 74 and Proposition 75 imply that the group $\mathcal{F}(W, \Lambda)$ is isomorphic to the group $S_k(M)$. Moreover, it follows from Theorem 66 that there exists an abelian variety X over $\mathbb{R}$ such that $X(\mathbb{C})$ is isomorphic to V/Λ if and only if $S_k(M)$ contains a matrix N such that MN is negative definite. Hence, by Remark 73, $\mathrm{NS}(X)$ is isomorphic to $S_k(M)$.

Therefore, we only have to prove that the rank of $S_k(M)$ is smaller than or equal to $\frac{1}{2}n(n+1)$, for any nonsingular real $n \times n$-matrix M. For this, observe that the subgroup $\mathbf{M}_n(\mathbb{Z})$ of $\mathbf{M}_n(\mathbb{R})$ is a discrete subgroup. Moreover, the subspace

$$\{A \in \mathbf{M}_n(\mathbb{R}) \mid (MA)^T = MA\}$$

of $\mathbf{M}_n(\mathbb{R})$ has $\mathbb{R}$-dimension $\frac{1}{2}n(n+1)$, since M is nonsingular. Therefore, the rank of the group $S_k(M)$ is smaller than or equal to $\frac{1}{2}n(n+1)$. □

Remark 77. The upper bound on the base number of an abelian variety over $\mathbb{R}$ is sharp, as is shown by the following example.

Let $W = \mathbb{R}^n$, so that $V = \mathbb{C}^n$ and the action of G on $\mathbb{C}^n$ is the standard action. Choose an integral $n \times n$-matrix M with $d = \det M \neq 0$. Let $\Lambda \subseteq \mathbb{C}^n$ be the lattice generated by

$$e_1, \ldots, e_n, iM^T e_1, \ldots, iM^T e_n,$$

where $e_1, \ldots, e_n$ is the standard basis for $\mathbb{C}^n$. Since the group $S_0(M)$ contains the group

$$\{dM^{-1}A \mid A \text{ is a symmetric integral } n \times n\text{-matrix}\},$$

the rank of $S_0(M)$ is $\frac{1}{2}n(n+1)$. Moreover, this also proves that there exists a matrix $N \in S_0(M)$ such that MN is negative definite. Therefore, by Corollary 76, there exists an abelian variety X over $\mathbb{R}$ such that

$X(\mathbb{C})$ is isomorphic to $\mathbb{C}^n/\Lambda$, as complex tori with a real structure. By Corollary 76, the base number of X is $\frac{1}{2}n(n+1)$. □

2.5 Real abelian varieties

Definition 78. *A group* $(G, \cdot)$ *which is, at the same time, a connected real algebraic variety is a* real algebraic group *if*

$$\begin{aligned} m\colon G \times G &\longrightarrow G \\ (x,y) &\longmapsto xy \end{aligned}$$

and

$$\begin{aligned} i\colon G &\longrightarrow G \\ x &\longmapsto x^{-1} \end{aligned}$$

are morphisms of real algebraic varieties. A morphism of real algebraic groups *from* (G, m) *to* (G', m') *is a morphism* $f\colon G \to G'$ *of real algebraic varieties such that*

$$m' \circ (f \times f) = f \circ m.$$

Of course, "connected" in Definition 78 is with respect to the Zariski-topology. For example, the real elliptic curve $E \subseteq \mathbb{P}^2(\mathbb{R})$ defined by the equation

$$Y^2Z = X^3 - XZ^2$$

is a real algebraic group. However, E has two components with respect to the strong topology on E.

Note that a real algebraic group is nonsingular. It follows that every real algebraic group is irreducible.

Observe that, if X is an algebraic group over $\mathbb{R}$, the real part $\mathcal{R}(X)$ of X is a real algebraic group. For, the set of real points $X(\mathbb{R})$ is nonempty and X is nonsingular and irreducible hence, by Remark 10, $X(\mathbb{R})$ is dense in X. Therefore, the real part of X is an irreducible real algebraic variety (by Proposition 8). The morphisms $m\colon X \times X \to X$ and $i\colon X \to X$ induce morphisms

$$\begin{aligned} \mathcal{R}(m)\colon \mathcal{R}(X) \times \mathcal{R}(X) &\longrightarrow \mathcal{R}(X) \\ \mathcal{R}(i)\colon \mathcal{R}(X) &\longrightarrow \mathcal{R}(X) \end{aligned}$$

which turn $\mathcal{R}(X)$ into a real algebraic group.

The following theorem shows that every real algebraic group is the real part of a unique algebraic group over $\mathbb{R}$.

Theorem 79. *Every real algebraic group G has a complexification (G', i), such that G' is an algebraic group over $\mathbb{R}$ and $i\colon G \to \mathcal{R}(G')$ is an isomorphism of real algebraic groups. Furthermore, the algebraic group G' over $\mathbb{R}$ is unique up to isomorphism.*

Proof. Let $U \subseteq G$ be a nonempty affine open subset. Clearly, U has a complexification (V, j). Now, V has a rational group law, hence, by a theorem of A. Weil [1], there exist an algebraic group G' over $\mathbb{R}$ and a birational morphism $f\colon V \dashrightarrow G'$, which respects the group law. In particular, the birational mapping $i = \mathcal{R}(f) \circ j\colon G \dashrightarrow \mathcal{R}(G')$ respects the group law. Consequently, i is an isomorphism. □

We denote the complexification of a real algebraic group G by $\mathcal{C}(G)$. Observe that $\mathcal{C}$ extends to a functor from the category of real algebraic groups to the category of algebraic groups over $\mathbb{R}$. This establishes an equivalence between both categories.

Definition 80. *A* real abelian variety *is a real algebraic group G such that $\mathcal{C}(G)$ is an abelian variety over $\mathbb{R}$. A* real elliptic curve *is a real abelian variety of dimension* 1*. A* morphism of real abelian varieties *is just a morphism of real algebraic groups.*

In [14] real abelian varieties were called real algebraic groups of abelian type. However, we prefer the former name.

Since an abelian variety over $\mathbb{R}$ is commutative (Section 2.1), every real abelian variety is commutative. Furthermore, as a consequence of Theorem 42 and Theorem 43, real abelian varieties satisfy the following remarkable property.

Theorem 81. *If X and Y are real abelian varieties and*

$$f\colon X \dashrightarrow Y$$

is a rational mapping of real algebraic varieties then, up to translation, f is a morphism of real abelian varieties, i.e.

$$\tau_{-P} \circ f : X \longrightarrow Y$$

is a morphism of real abelian varieties, where $P = f(O)$ and τ_{-P} is translation with $-P$.

Corollary 82. *If X and Y are real abelian varieties then the following conditions are equivalent:*

(i) *X and Y are birationally isomorphic as real algebraic varieties,*
(ii) *X and Y are isomorphic as real algebraic varieties,*
(iii) *X and Y are isomorphic as real abelian varieties.*

Since abelian varieties over $\mathbb{R}$ are projective (see Section 2.1), real abelian varieties are affine, by Remark 17. As an example, we will prove that every real elliptic curve can be embedded into $\mathbb{R}^2$ as a closed subvariety.

Example 83. Let E be an elliptic curve over $\mathbb{R}$. We will prove that there exists an embedding of the real part $\mathcal{R}(E)$ of E into $\mathbb{R}^2$ as a closed subvariety.

Choose a closed point $P \in E$, such that the residue field at P is isomorphic to $\mathbb{C}$. Then, P has degree 2 as a divisor on E and, by Riemann-Roch,

$$\dim_{\mathbb{R}} \Gamma(E, \mathcal{L}(nP)) = 2n, \text{ for } n \geq 0,$$

where $\mathcal{L}(D)$ is the invertible subsheaf of the constant sheaf $\mathcal{K}_E = \mathbb{R}(E)$ of rational functions determined by the divisor D on E. Choose $x \in \Gamma(E, \mathcal{L}(P))$ such that $\{1, x\}$ is a basis. Then, there exists $y \in \Gamma(E, \mathcal{L}(2P))$ such that $\{1, x, x^2, y\}$ is a basis for $\Gamma(E, \mathcal{L}(2P))$. Now, $\{1, x, x^2, x^3, y, xy\}$ is linearly independent in $\Gamma(E, \mathcal{L}(3P))$. For, if there exist real numbers λ, μ such that $\lambda x^3 + \mu xy \in \Gamma(E, \mathcal{L}(2P))$, then $\lambda x^2 + \mu y$ is an element of $\Gamma(E, \mathcal{L}(P))$. This implies that $\lambda = \mu = 0$. Hence $\{1, x, x^2, x^3, y, xy\}$ is linearly independent. In the same way, one proves that

$$\{1, x, x^2, x^3, x^4, y, xy, x^2y\} \subseteq \Gamma(E, \mathcal{L}(4P))$$

is independent, hence this set is a basis for $\Gamma(E, \mathcal{L}(4P))$. But y^2 is in $\Gamma(E, \mathcal{L}(4P))$ too. Hence, modifying y if necessary,

$$y^2 = f(x),$$

for some real polynomial $f \in \mathbb{R}[X]$ of degree 4.

It is easy to see that f has no multiple factors in $\mathbb{R}[X]$. For, if f has multiple factors then there are two cases, f is a square or there exists a linear polynomial l such that l^2 divides f. In the latter case, y/l is a linear combination of $1, x$. Hence, y is a linear combination of $1, x, x^2$. In the former case, there exists a polynomial g of degree 2 such that $f = g^2$. But then, $y = \pm g$ and y is again a linear combination of $1, x, x^2$. Both cases lead to a contradiction since $\{1, x, x^2, y\}$ is linearly independent. It follows that the curve $F \subseteq \mathbb{P}^2_{\mathbb{R}}$ given by the equation

$$Y^2Z^2 = Z^4 f\left(\frac{X}{Z}\right)$$

has genus 1.

The rational functions x and y give rise to a morphism $\varphi\colon E \to F$, given by $\varphi = (x\colon y\colon 1)$. Since the mapping $x\colon E \to \mathbb{P}^1_{\mathbb{R}}$, of degree 2, factors through φ, the morphism φ is birational.

Now, F has only one singular point, namely the point $Q = (0\colon 1\colon 0)$. Since $\varphi^{-1}\{Q\} = \{P\}$,

$$\varphi_{|E-\{P\}}\colon E - \{P\} \longrightarrow F - \{Q\}$$

is an isomorphism. Clearly, $F - \{Q\}$ is contained in the affine open set $\{Z \neq 0\}$, which is isomorphic to $\mathbb{A}^2_{\mathbb{R}}$. Since $P \notin E(\mathbb{R})$, the real part $\mathcal{R}(E)$ of E is isomorphic to the real algebraic curve $y^2 = f(x)$ in $\mathbb{R}^2$.

As a concrete example, let us take for E the elliptic curve over $\mathbb{R}$ in $\mathbb{P}^2_{\mathbb{R}}$ defined by the equation $Y^2Z = X^3 + Z^3$. As usual, let O be the point at infinity, i.e. $O = (0\colon 1\colon 0)$, and let $x = X/Z$ and $y = Y/Z$ be rational functions on E.

The pair of conjugate complex points $(\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}\colon 0\colon 1)$ defines a closed point P of E. Put

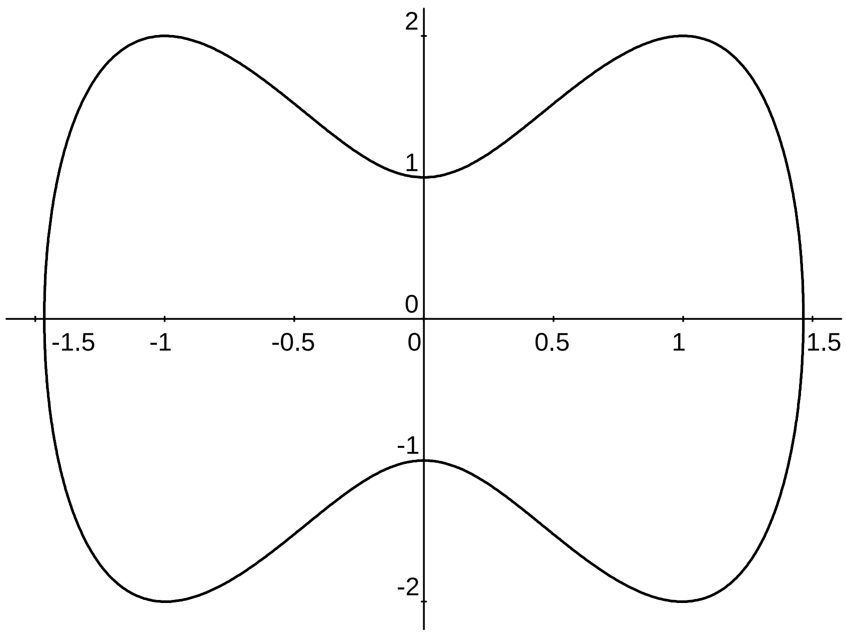
$$u = \frac{y}{x^2 - x + 1} \quad \text{and} \quad v = \frac{x^2 + 2x - 2}{x^2 - x + 1}.$$

Then, $\{1, u\}$ is a basis for $\Gamma(E, \mathcal{L}(P))$ and $\{1, u, u^2, v\}$ is a basis for $\Gamma(E, \mathcal{L}(2P))$. Furthermore,

$$3u^4 - 6u^2 + v^2 = 1.$$

It follows from the general discussion above that the morphism $\varphi = (u\colon v\colon 1)$ gives rise to an isomorphism between $E(\mathbb{R})$ and the real alge-

Figure 2.1: the real algebraic curve $3u^4 - 6u^2 + v^2 = 1$



braic curve $3u^4 - 6u^2 + v^2 = 1$ in $\mathbb{R}^2$ (Figure 2.1). □

2.6 The topology of real abelian varieties

In this section, X will be a real abelian variety, Y its complexification $\mathcal{C}(X)$ and M the complex Lie group $Y(\mathbb{C})$. We know from Section 2.4 that there exist a lattice (W, Λ) over $\mathbb{R}$ and a G-equivariant mapping

$$\pi\colon V \longrightarrow M,$$

where $V = W \otimes_{\mathbb{R}} \mathbb{C}$ and G is the Galois group of $\mathbb{C}/\mathbb{R}$, such that π induces an isomorphism

$$\widetilde{\pi}\colon V/\Lambda \longrightarrow M$$

of complex Lie groups. In particular, the restriction of $\widetilde{\pi}$ to $(V/\Lambda)^G$ is an isomorphism of real Lie groups from $(V/\Lambda)^G$ onto X_s (considered as a submanifold of M).

The following corollary is, in fact, a corollary of Proposition 70. Let us define the mapping $p_2\colon V \to \operatorname{Im} V$ by $p_2(z) = \frac{1}{2}(z - \sigma(z))$.

Corollary 84. *Let W be a real vector space of dimension n and let $\Lambda \subseteq V$, where $V = W \otimes_{\mathbb{R}} \mathbb{C}$, be a lattice, invariant under the action of G on V. Let k be the degree of connectedness of Λ. Denote the canonical mapping $V \to V/\Lambda$ by π. Then,*

$$\begin{array}{rcl} (\frac{1}{2}\operatorname{Im}\Lambda)/p_2(\Lambda) & \stackrel{\varphi}{\longrightarrow} & H \\ [z] & \longmapsto & \pi(z + \operatorname{Re} V) \end{array}$$

defines an isomorphism, where H is the group of connected components of $(V/\Lambda)^G$ and $[z]$ denotes the class of z modulo $p_2(\Lambda)$. In particular, H is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{n-k}$ and the number of connected components of $(V/\Lambda)^G$ is 2^{n-k}.

Proof. Observe that, for $z \in V$, $\pi(z)$ is in $(V/\Lambda)^G$ if and only if $z-\sigma(z)$ is in $\operatorname{Im}\Lambda$ or, equivalently, $p_2(z)$ is in $\frac{1}{2}\operatorname{Im}\Lambda$. Moreover, if $\pi(z)$ is in $(V/\Lambda)^G$ then the connected component of $(V/\Lambda)^G$ containing $\pi(z)$ is $\pi(z + \operatorname{Re} V)$. Hence, φ is surjective. Injectivity of φ follows from the fact that $\pi(z + \operatorname{Re} V) = \pi(\operatorname{Re} V)$ if and only if there exists $\lambda \in \Lambda$ such that $p_2(\lambda) = z$, for any $z \in \frac{1}{2}\operatorname{Im}\Lambda$. Therefore φ is an isomorphism. By Corollary 70, $(\frac{1}{2}\operatorname{Im}\Lambda)/p_2(\Lambda)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{n-k}$. □

As an immediate consequence, we have the following proposition (see [11] for a different proof).

Proposition 85. *If X is a real abelian variety of dimension n then the number of connected components of X with respect to the strong topology on X is a power of 2 and is smaller than, or equal to 2^n. Each component is homeomorphic to the n-fold cartesian product $(S^1)^n$ of the 1-sphere S^1.* □

Remark 86. Observe that for each nonnegative integer n and each integer i with $0 \le i \le n$ there exists a real abelian variety X of dimension n such that the number of connected components of X with respect to the strong topology is 2^i. □

We extend the definition of degree of connectedness to real abelian varieties. The *degree of connectedness* of a real abelian variety X is k, where $2^{\dim X - k}$ is the number of connected components of X with respect to the strong topology. According to Corollary 84, if (W, Λ) is a lattice over $\mathbb{R}$ such that

$$(V/\Lambda)^G \cong X_s,$$

as topological manifolds, then the degrees of connectedness of both Λ and X coincide.

We want to compute the group $H^{alg}_{n-1}(X, \mathbb{Z}/2\mathbb{Z})$ of codimension-1 cycles that are realizable by real algebraic subvarieties of X. As explained in Section 1.2, computing the subgroup

$$w_1(V^1_{alg}(X))$$

of $H^1_{alg}(X_s, \mathbb{Z}/2\mathbb{Z})$ amounts to the same. That is, we should compute first Stiefel-Whitney classes of all strongly algebraic line bundles on X.

For this, let $\{C_i\}_{i \in I}$ be the set of strongly connected components of X. Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis for $\operatorname{Re}\Lambda$ and $y_1, \ldots, y_n$ a $\mathbb{Z}$-basis for $\operatorname{Im}\Lambda$ such that

$$\tfrac{1}{2}(x_1 + y_1), \ldots, \tfrac{1}{2}(x_k + y_k), x_1, \ldots, x_n, y_{k+1}, \ldots, y_n$$

is a $\mathbb{Z}$-basis for Λ. By Corollary 84, there is a bijection between the set I and the set

$$I' = \{ \sum_{j=k+1}^{n} \varepsilon_j \tfrac{1}{2} y_j \mid \varepsilon_j \in \{0,1\},\ j = k+1, \ldots, n\},$$

the image of each element of I' belonging to precisely one component C_i. Therefore, we may as well assume that $I = I'$. Let $W' = I + \operatorname{Re} V$. Then, π maps W' onto X. Hence, the restriction ρ of π to W' induces a homeomorphism

$$\widetilde{\rho}\colon W'/\operatorname{Re}\Lambda \longrightarrow X_s$$

and is the universal covering of X_s. As a consequence, we have a natural isomorphism

$$h\colon H^1(X_s, \mathbb{Z}/2\mathbb{Z}) \longrightarrow {}^I\mathrm{Hom}(\mathrm{Re}\,\Lambda, \mathbb{Z}/2\mathbb{Z}),$$

where ${}^AB$ denotes the set of all mappings from the set A into the set B.

Recall that, if (α, F) is an Appell-Humbert datum over $\mathbb{R}$ for (W, Λ), the group G acts on the complex line bundle $L(\alpha, F)$. Clearly,

$$L(\alpha, F)^G$$

is a real line bundle over $M^G = X$.

In the next statement we shall use notation introduced above. In particular, X is a real abelian variety, (W, Λ) is a lattice over $\mathbb{R}$ and

$$\widetilde{\rho}\colon W'/\mathrm{Re}\,\Lambda \longrightarrow X_s$$

is an isomorphism.

Lemma 87. *For every strongly algebraic line bundle L on X there exists an Appell-Humbert datum (α, F) over $\mathbb{R}$ for (W, Λ) such that*

$$L(\alpha, F)^G \cong \widetilde{\rho}^\star L.$$

Conversely, if (α, F) is an Appell-Humbert datum over $\mathbb{R}$ for (W, Λ) then there exists a strongly algebraic line bundle L on X such that

$$\widetilde{\rho}^\star L \cong L(\alpha, F)^G.$$

Moreover, identifying $H^1(X_s, \mathbb{Z}/2\mathbb{Z})$ with ${}^I\mathrm{Hom}(\mathrm{Re}\,\Lambda, \mathbb{Z}/2\mathbb{Z})$ through h, the first Stiefel-Whitney class of such a line bundle on X is the element

$$w \in {}^I\mathrm{Hom}(\mathrm{Re}\,\Lambda, \mathbb{Z}/2\mathbb{Z}),$$

defined by

$$w(c)(\lambda) = \alpha(\lambda)(-1)^{E(\lambda, 2r(c))}$$

where $\lambda \in \mathrm{Re}\,\Lambda$, $c \in I$, $E = \mathrm{Im}\,(F \otimes \mathbb{C})$ and $\mathbb{Z}/2\mathbb{Z} = \{-1, 1\}$.

Before proving this theorem, let us draw some conclusions. Let

$$\omega\colon \mathrm{AH}(W,\Lambda) \longrightarrow {}^{I}\mathrm{Hom}(\mathrm{Re}\,\Lambda, \mathbb{Z}/2\mathbb{Z}),$$

be defined by $\omega(\alpha, F) = w$, where $w(c)(\lambda) = \alpha(\lambda)(-1)^{E(2c,\lambda)}$, for all $\lambda \in \mathrm{Re}\,\Lambda$ and $c \in I$.

Corollary 88. *One has*

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H^{alg}_{n-1}(X, \mathbb{Z}/2\mathbb{Z}) = \dim_{\mathbb{Z}/2\mathbb{Z}} \mathrm{im}\,\omega.$$

We shall now compute the dimension of $H^{alg}_{n-1}(X, \mathbb{Z}/2\mathbb{Z})$ in terms of the group $S_k(M)$ introduced in Section 2.4. Let M be the real $n \times n$-matrix associated to Λ as in Remark 71. Let $T_k(M)$ be the subgroup of $S_k(M)$ consisting of integral matrices $N = (n_{jl})$ such that

$$\begin{aligned} n_{jj} &\equiv 0 \bmod 4, \quad \text{for } j = 1, \ldots, k, \\ n_{jl} &\equiv 0 \bmod 2, \quad \text{for } j, l > k. \end{aligned}$$

Observe that $S_k(M)/T_k(M)$ is a $\mathbb{Z}/2\mathbb{Z}$-vector space.

Theorem 89. *There exists an exact sequence*

$$0 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{n-k} \longrightarrow \mathrm{im}\,\omega \longrightarrow S_k(M)/T_k(M) \longrightarrow 0.$$

In particular,

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H^{alg}_{n-1}(X, \mathbb{Z}/2\mathbb{Z}) = n - k + \dim_{\mathbb{Z}/2\mathbb{Z}} S_k(M)/T_k(M).$$

Proof. By Remark 73 and Corollary 76, we have an exact sequence

$$0 \longrightarrow \mathrm{Hom}_G(\Lambda, S^1) \longrightarrow \mathrm{AH}(W,\Lambda) \xrightarrow{\varphi} S_k(M) \longrightarrow 0$$

Consider $\mathrm{Hom}_G(\Lambda, S^1)$ as a subgroup of $\mathrm{AH}(W,\Lambda)$. It is clear from Proposition 72 that

$$\omega(\mathrm{Hom}_G(\Lambda, S^1)) \cong (\mathbb{Z}/2\mathbb{Z})^{n-k}.$$

Hence, to prove the statement it suffices to show that

$$\varphi^{-1}(T_k(M)) = \mathrm{Hom}_G(\Lambda, S^1) + \ker \omega.$$

This is equivalent to $\varphi(\ker\omega) = T_k(M)$, since $\ker\varphi = \mathrm{Hom}_G(\Lambda, S^1)$. Let us prove $\varphi(\ker\omega) = T_k(M)$.

Suppose (α, F) is an Appell-Humbert datum over $\mathbb{R}$ for (W, Λ) and $N = (n_{jl})$, where

$$n_{jl} = E(x_j, y_l)$$

and, as usual, $E = \mathrm{Im}\,(F \otimes \mathbb{C})$. We know from Proposition 72 that

$$\alpha(x_j) = (-1)^{\frac{1}{2}n_{jj}}, \text{ for } j = 1, \ldots, k. \tag{2.1}$$

By definition of ω, the Appell-Humbert datum (α, F) is in the kernel of ω if and only if

$$\alpha(x_j) = (-1)^{E(2r(c), x_j)}, \text{ for } j = 1, \ldots, n \text{ and } c \in I.$$

Then, $\omega(\alpha, F) = 0$ implies that $\alpha(x_j) = 1$, for every j, and n_{jl} is even, if $j, l > k$. By (2.1), the matrix N is an element of $T_k(M)$.

On the other hand, if N is an element of $T_k(M)$ then n_{jj} is divisible by 4, for $j = 1, \ldots, k$. Hence, by Proposition 72, there exists a G-equivariant mapping α from Λ into S^1 such that $\alpha(x_j) = 1$, for every j, and (α, F) is an Appell-Humbert datum over $\mathbb{R}$ for (W, Λ). Since

$$n_{jl} \equiv 0 \bmod 2,$$

for $j = 1, \ldots, n$ and $l > k$, we have that

$$w(c)(x_j) = \alpha(x_j)(-1)^{E(2r(c), x_j)} = 1,$$

for every j and $c \in I$. Therefore, N is an element of $\varphi(\ker\omega)$. This proves the proposition. □

Corollary 90. *If X is connected with respect to the strong topology then*

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_{n-1}^{alg}(X, \mathbb{Z}/2\mathbb{Z}) = \dim_{\mathbb{Z}/2\mathbb{Z}} S_n(M)/T_n(M).$$

Example 91. Let $W = \mathbb{R}^n$ and let $x_1, \ldots, x_n$ be the standard basis for W. Let $y_j = ix_j$, for every j. Then, for every permutation τ of the set $\{1, \ldots, n\}$,

$$\tfrac{1}{2}(x_1 + y_{\tau(1)}), \ldots, \tfrac{1}{2}(x_n + y_{\tau(n)}), x_1, \ldots, x_n$$

is a $\mathbb{Z}$-basis for a lattice Λ_τ in $\mathbb{C}^n$. Clearly, (W, Λ_τ) is a lattice over $\mathbb{R}$ and there exists, for every permutation τ, an abelian variety Y_τ over $\mathbb{R}$ such that

$$Y_\tau(\mathbb{C}) \cong \mathbb{C}^n/\Lambda_\tau,$$

G-equivariantly. Let X_τ be the real part $\mathcal{R}(Y_\tau)$ of Y_τ. Then, X_τ is a strongly connected real abelian variety of dimension n. We will prove that

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_{n-1}^{alg}(X_\tau, \mathbb{Z}/2\mathbb{Z}) = n - p, \tag{2.2}$$

where p is half of the number of elements of the set $\{1, \ldots, n\}$ that are fixed by τ^2 but not by τ. Equivalently, if we write the permutation τ as the product of disjoint cycles, p is the number of 2-cycles in this factorization of τ.

For example, taking $n = 2$, we have two real abelian varieties, $X_{(1)}$ and $X_{(12)}$, where (1) is the trivial permutation and (12) is the nontrivial permutation of $\{1, 2\}$. By (2.2), all homology cycles of $X_{(1)}$ are realizable by real algebraic subvarieties of $X_{(1)}$ (indeed, $X_{(1)}$ is isomorphic to the product of two strongly connected real algebraic curves), while

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_1^{alg}(X_{(12)}, \mathbb{Z}/2\mathbb{Z}) = 1.$$

For the proof of (2.2), observe that $x_1, \ldots, x_n$ is a $\mathbb{Z}$-basis for $\operatorname{Re}\Lambda_\tau$ and $y_{\tau(1)}, \ldots, y_{\tau(n)}$ is a $\mathbb{Z}$-basis for $\operatorname{Im}\Lambda_\tau$. Moreover, M is just the permutation matrix P_τ defined by

$$(P_\tau)_{jl} = \delta_{\tau(j)l},$$

where δ is the Kronecker delta function. Hence,

$$\begin{aligned} S_n(M) = \{N \in M_{n\times n}(\mathbb{Z}) \ \mid\ & N \equiv 0 \bmod 2, \\ & N \equiv N^T \bmod 4 \quad \text{and} \quad (P_\tau N)^T = P_\tau N\} \end{aligned}$$

and

$$T_n(M) = \{N \in S_n(M) \mid \forall j\colon N_{jj} \equiv 0 \bmod 4\}.$$

Therefore, the mapping ψ from $S_n(M)$ into $(\mathbb{Z}/2\mathbb{Z})^n$, which assigns to N the element

$$(\tfrac{1}{2}N_{11} \bmod 2, \ldots, \tfrac{1}{2}N_{nn} \bmod 2)$$

of $(\mathbb{Z}/2\mathbb{Z})^n$, has as kernel $T_n(M)$. Let us compute the image of ψ.

For an $n \times n$-matrix N, the condition $(P_\tau N)^T = P_\tau N$ is equivalent to

$$N_{\tau^{-1}(l)\tau(j)} = N_{jl}, \text{ for all } j, l.$$

Therefore, $(a_1, \ldots, a_n)$ is in the image of ψ if and only if $a_{\tau(j)} = a_j$, for every j fixed by τ^2. Hence, the $\mathbb{Z}/2\mathbb{Z}$-dimension of the image of ψ is equal to $n - p$, where p is half of the number of elements of the set $\{1, \ldots, n\}$ that are fixed by τ^2 but not by τ. By Theorem 89, this proves (2.2). □

Corollary 92. *If X is a real abelian variety of dimension n and with degree of connectedness k then*

$$n - k \leq \dim_{\mathbb{Z}/2\mathbb{Z}} H_{n-1}^{alg}(X, \mathbb{Z}/2\mathbb{Z}) \leq \min\{b + n - k, n + (n-k)^2\},$$

where b is the base number of X.

Proof. It follows from Corollary 76 and the definition of $T_k(M)$ that

$$0 \leq \dim_{\mathbb{Z}/2\mathbb{Z}} S_k(M)/T_k(M) \leq \min\{b, k + (n-k)^2\}.$$

The corollary follows now from Theorem 89. □

Corollary 93. *If X is a real abelian variety of dimension n then*

(i) $H_{n-1}^{alg}(X, \mathbb{Z}/2\mathbb{Z}) = 0$ *implies X is strongly connected, and*

(ii) $H_{n-1}^{alg}(X, \mathbb{Z}/2\mathbb{Z}) = H_{n-1}(X_s, \mathbb{Z}/2\mathbb{Z})$ *implies X is strongly connected or X is a real elliptic curve.*

Proof. The first assertion is clear from Corollary 92. For the proof of the second assertion, observe that

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_{n-1}(X_s, \mathbb{Z}/2\mathbb{Z}) = 2^{n-k} n,$$

where n is the dimension of X and k its degree of connectedness. By Corollary 92, if all codimension-1 homology classes are realizable by real algebraic subvarieties of X then

$$2^{n-k} n \leq n + (n-k)^2.$$

Assume $n \geq 2$. Then, $k \neq n-1$, for

$$2^{n-(n-1)}n = 2n \not\leq n+1 = n+(n-(n-1))^2.$$

At the same time, $k \not< n-1$, for if $n-k > 1$ then

$$\begin{aligned} 2^{n-k}n &> (1+n-k)n \\ &= n+(n-k)n \\ &\geq n+(n-k)^2. \end{aligned}$$

Hence, $k = n$ and X is strongly connected. □

Let us now turn to the proof of Lemma 87. The first part is easy to prove.

Proof of the first part of Lemma 87. On the one hand, given a strongly algebraic line bundle L on X, there exists, by Lemma 21, an invertible sheaf $\mathcal{L}$ on the abelian variety Y over $\mathbb{R}$ such that the real part $\mathcal{R}(\mathcal{L})$ of $\mathcal{L}$ is isomorphic to L. Then, by Theorem 66, there exists an Appell-Humbert datum (α, F) over $\mathbb{R}$ for (W, Λ) such that

$$L(\alpha, F) \cong \widetilde{\pi}^\star \mathcal{L}(\mathbb{C}),$$

G-equivariantly. Hence,

$$L(\alpha, F)^G \cong \widetilde{\rho}^\star L.$$

On the other hand, if (α, F) is an Appell-Humbert datum over $\mathbb{R}$ for (W, Λ) then we know from Theorem 66 that there exists an invertible sheaf $\mathcal{L}$ on Y such that

$$\widetilde{\pi}^\star \mathcal{L}(\mathbb{C}) \cong L(\alpha, F),$$

G-equivariantly. By Lemma 21, the real part $L = \mathcal{R}(\mathcal{L})$ is a strongly algebraic line bundle on X. Moreover,

$$\widetilde{\rho}^\star L \cong L(\alpha, F)^G.$$

This proves the first part of Lemma 87. □

For the proof of the second part of Lemma 87 it is convenient to consider a more general situation.

Suppose the topological manifold N is a disjoint union of finitely many copies of $\mathbb{R}^n$. Let the abelian group $A = \mathbb{Z}^n$ act on each connected component of N in the standard way. Then the quotient space M of N by the action of A is a compact topological manifold. Since the canonical mapping $\rho\colon N \to M$ is the universal covering of M, we have a natural isomorphism

$$h\colon H^1(M, \mathbb{Z}/2\mathbb{Z}) \longrightarrow {}^I\mathrm{Hom}(A, \mathbb{Z}/2\mathbb{Z}),$$

where $\{C_i\}_{i\in I}$ is the set of connected components of N.

If L is a topological line bundle on M, its first Stiefel-Whitney class (see Section 1.2) $w_1(L)$ is an element of the first cohomology group $H^1(M, \mathbb{Z}/2\mathbb{Z})$. We will compute $h(w_1(L))$.

Since N is the disjoint union of contractible spaces, $\rho^\star L$ is a trivial line bundle on N. If we choose an isomorphism

$$\rho^\star L \longrightarrow N \times \mathbb{R},$$

we get an action of A on $N \times \mathbb{R}$ such that the quotient of $N \times \mathbb{R}$ by this A-action is a line bundle on M, isomorphic to L. Clearly, there exist, for every $g \in A$, continuous mappings

$$e_g\colon N \longrightarrow \mathbb{R}^\star$$

such that the action of A on $N \times \mathbb{R}$ is

$$g \cdot (n, v) = (n + g, e_g(n)v),$$

for every $v \in \mathbb{R}$, $n \in N$ and $g \in A$. Since this should define an A-action,

$$e\colon A \longrightarrow C^\star$$

is a 1-cocycle, where $C^\star$ is the group of nonvanishing continuous real-valued functions on N and A acts on $C^\star$ as

$$(g \cdot f)(n) = f(n + g),$$

for every $n \in N$, $f \in C^\star$ and $g \in A$.

We define a mapping w from the group $V^1(M)$ of (isomorphism classes of) topological line bundles on M into ${}^I\mathrm{Hom}(A, \mathbb{Z}/2\mathbb{Z})$ by

$$w(L)(c)(g) = \mathrm{sign}(e_g(x)),$$

where x is an arbitrary element of the connected component c of N and g is an element of A. Indeed, one can check that $w(L)$, as defined above, is independent of the choice of the isomorphism between $\rho^\star L$ and $N \times \mathbb{R}$ and depends only on the isomorphism class of L. Moreover,

$$w \colon V^1(M) \longrightarrow {}^I\mathrm{Hom}(A, \mathbb{Z}/2\mathbb{Z})$$

is a morphism of groups and is natural with respect to N and A.

Lemma 94. *If L is a topological line bundle on M then*

$$w(L) = h(w_1(L)).$$

Proof. Both mappings w and $h \circ w_1$ are natural with respect to N and A. Hence, we may assume that N is connected, that is

$$N = \mathbb{R}^n \quad \text{and} \quad A = \mathbb{Z}^n.$$

Then, M is isomorphic to the n-fold product of the 1-sphere S^1. Since

$$V^1((S^1)^n) \cong (V^1(S^1))^n,$$

we have finished the proof if we show the statement for $n = 1$. But for this case the statement is trivial. □

Now we are ready to prove the last part of Lemma 87.

Proof of the second part of Lemma 87. Let (α, F) be an Appell-Humbert datum for (W, Λ). Then, identifying $W'/\mathrm{Re}\,\Lambda$ and X_s via $\widetilde{\rho}$, one sees that $L = L(\alpha, F)^G$ is a line bundle on X_s. According to Lemma 94, the first Stiefel-Whitney class $w_1(L)$ of L is $w(L)$, under the identification of $H^1(M, \mathbb{Z}/2\mathbb{Z})$ with ${}^I\mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z})$ through h. Let us compute $w(L)$.

Let e_λ be the holomorphic functions associated to the Appell-Humbert datum $(\alpha, F\otimes\mathbb{C})$. Then, by definition, $L(\alpha,F)$ is the quotient of $V\times\mathbb{C}$ by the action of Λ given by

$$\lambda(v,z) = (v+\lambda, e_\lambda(v)z),$$

where $z\in\mathbb{C}$, $v\in V = W\otimes\mathbb{C}$ and $\lambda\in\Lambda$. In particular, $L(\alpha,F)\restriction_{X_s}$ is the quotient of $W'\times\mathbb{C}$ by the restriction of this action to $\operatorname{Re}\Lambda$. Since L is a real sub-bundle of $L(\alpha,F)\restriction_{X_s}$, there should be a real sub-bundle of $W'\times\mathbb{C}$ that has L as a quotient. Let us compute this sub-bundle.

Choose a point $v\in W'$ and let $\lambda\in\Lambda$ be such that $\sigma v - v = \lambda$. Then, for every $z\in\mathbb{C}$,

$$\begin{aligned}\sigma(v,z) &= (\sigma v, \overline{z})\\ &= (v+\lambda, \overline{z})\\ &= (v, e_\lambda(v)^{-1}\overline{z}).\end{aligned}$$

Hence, if we put

$$L' = \{(v,z)\in W'\times\mathbb{C} \mid e_\lambda(v)^{-1}\overline{z} = z,\ \text{where } \lambda = \sigma v - v\}$$

then the quotient of L' under the action of $\operatorname{Re}\Lambda$ is L.

To compute $w(L)$ we need to have L as a quotient of $W'\times\mathbb{R}$ under some action of $\operatorname{Re}\Lambda$. This can easily be arranged. Let, for $v\in W'$ and $\lambda = \sigma v - v$,

$$f_\lambda(v) = \alpha(\lambda)^{-\frac{1}{2}} e^{-\frac{1}{2}\pi H(v,\lambda) - \frac{1}{4}\pi H(\lambda,\lambda)},$$

for some choice of $\alpha(\lambda)^{-\frac{1}{2}}$, where $H = F\otimes\mathbb{C}$. Then,

$$f_\lambda(v)^2 = e_\lambda(v)^{-1}.$$

Hence, the mapping

$$\begin{aligned} W'\times\mathbb{R} &\longrightarrow W'\times\mathbb{C}\\ (v,x) &\longmapsto (v, f_\lambda(v)x),\end{aligned}$$

where $\lambda = \sigma v - v$, maps $W'\times\mathbb{R}$ onto L'. Via this isomorphism we get an action of $\operatorname{Re}\Lambda$ on $W'\times\mathbb{R}$ which has its quotient isomorphic to L. This action is

$$\mu(v,x) = (v, f_\lambda(v+\mu)^{-1} e_\mu(v) f_\lambda(v) x),$$

for every $x \in \mathbb{R}$, $v \in W'$ and $\mu \in \operatorname{Re}\Lambda$, where $\lambda = \sigma v - v$. Hence, to compute $w(L)$ we should compute the sign of

$$d_\mu(v) = f_\lambda(v+\mu)^{-1} e_\mu(v) f_\lambda(v).$$

Since

$$\begin{aligned} & \tfrac{1}{2}H(v+\mu,\lambda) + \tfrac{1}{4}H(\lambda,\lambda) + H(v,\mu) + \tfrac{1}{2}H(\mu,\mu) + \\ & \qquad -\tfrac{1}{2}H(v,\lambda) - \tfrac{1}{4}H(\lambda,\lambda) \ = \\ = \ & \tfrac{1}{2}H(\mu,\lambda) + H(v,\mu) + \tfrac{1}{2}H(\mu,\mu) \\ = \ & \tfrac{1}{2}H(\mu,\lambda) + \tfrac{1}{2}H(\mu,2\sigma v) + \tfrac{1}{2}H(\mu,\mu) \\ = \ & \tfrac{1}{2}H(\mu,\lambda) + \tfrac{1}{2}H(\mu,\sigma v + v + \lambda) + \tfrac{1}{2}H(\mu,\mu) \\ = \ & H(\mu,\lambda) + \tfrac{1}{2}H(\mu,\mu+\sigma v + v), \end{aligned}$$

where $v \in W'$, $\mu \in \operatorname{Re}\Lambda$ and $\lambda = \sigma v - v$, we have

$$d_\mu(v) = \alpha(\mu) e^{\pi H(\mu,\lambda) + \frac{1}{2}\pi H(\mu,\mu+\sigma v+v)}.$$

Since $\mu + \sigma v + v \in \operatorname{Re} V$, the number $H(\mu, \mu+\sigma v+v)$ is real, and, since $\mu \in \operatorname{Re}\Lambda$ and $\lambda \in \operatorname{Im}\Lambda$, the number $H(\mu,\lambda)$ is purely imaginary, i.e. $H(\mu,\lambda) = iE(\mu,\lambda)$, where $E = \operatorname{Im} H$. Therefore,

$$\operatorname{sign}(d_\mu(v)) = \alpha(\mu)(-1)^{E(\mu,\lambda)}.$$

Observe that, if $c \in I$ is the connected component of X_s containing $\rho(v)$, the component $\rho(-\frac{1}{2}\lambda + \operatorname{Re} V)$ is equal to c. Hence, there exists an $x \in \operatorname{Re} V$ such that $-\lambda + x = 2r(c)$. Then

$$E(\mu, 2r(c)) = E(\mu, -\lambda + x) = -E(\mu,\lambda).$$

Therefore,

$$w(c)(\lambda) = w_1(L)(c)(\lambda) = \alpha(\lambda)(-1)^{E(\lambda,2r(c))},$$

where $\lambda \in \operatorname{Re}\Lambda$ and $c \in I$. This finishes the proof of Lemma 87. $\square$

2.7 The topology of the underlying real algebraic structure of elliptic curves over $\mathbb{C}$

In this section we study the group

$$H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z}),$$

for an elliptic curve E over $\mathbb{C}$. Recall from Section 1.5 that ${}_{\mathbb{R}}E$ is the underlying real algebraic structure of the elliptic curve E over $\mathbb{C}$. Hence ${}_{\mathbb{R}}E$ is a real algebraic torus which is, moreover, an affine real algebraic variety, as observed in Section 2.5.

We start by studying the Weil restriction of an abelian variety over $\mathbb{C}$ with respect to the field extension $\mathbb{C}/\mathbb{R}$.

Suppose X is an abelian variety over $\mathbb{C}$. Then, by Theorem 51, there exists a lattice Λ in some complex vector space V such that

$$V/\Lambda \cong X(\mathbb{C}).$$

Then, by Example 58, V^σ/Λ^σ is isomorphic to $X^\sigma(\mathbb{C})$. Moreover, we have a commutative diagram

$$\begin{array}{ccc} V/\Lambda & \longrightarrow & X(\mathbb{C}) \\ \Big\downarrow \overline{\varphi_V} & & \Big\downarrow \varphi_\sigma(\mathbb{C}) \\ V^\sigma/\Lambda^\sigma & \longrightarrow & X^\sigma(\mathbb{C}) \end{array}$$

where $\overline{\varphi_V}$ is the mapping induced by

$$\varphi_V\colon V \longrightarrow V^\sigma.$$

Define an action of the Galois group G of $\mathbb{C}/\mathbb{R}$ on $V \oplus V^\sigma$ by

$$\sigma \cdot (v, v') = (\varphi_V^{-1}(v'), \varphi_V(v)), \tag{2.3}$$

for any $v \in V$ and $v' \in V^\sigma$. Then, the action of σ is anti-linear, hence, letting $W = (V \oplus V^\sigma)^G$, we have a lattice $(W, \Lambda \oplus \Lambda^\sigma)$ over $\mathbb{R}$. By construction of the Weil restriction (see Section 1.4)

$$(\mathbb{C} \otimes_{\mathbb{R}} W)/(\Lambda \oplus \Lambda^\sigma) \cong \mathcal{N}(X)(\mathbb{C}),$$

G-equivariantly. This proves the following proposition.

Proposition 95. *If X is an abelian variety over $\mathbb{C}$ and Λ a lattice in some complex vector space V such that V/Λ is isomorphic to $X(\mathbb{C})$ then*

$$(\mathbb{C} \otimes_{\mathbb{R}} W)/(\Lambda \oplus \Lambda^\sigma) \cong \mathcal{N}(X)(\mathbb{C}),$$

G-equivariantly, where $W = (V \oplus V^\sigma)^G$ with the action of G on $V \oplus V^\sigma$ given by (2.3). □

Example 96. As an example, let us show, using Proposition 95, that for every positive integer d such that $d \equiv 3 \bmod 4$, there exist real algebraic curves C_1, C_2 such that

$$C_1 \times C_2 \cong {}_{\mathbb{R}}E,$$

where E is the elliptic curve over $\mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$, and $\tau = \frac{1}{2}(1 + i\sqrt{d})$. As a consequence,

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z}) = 2,$$

whenever $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$, where $\tau = \frac{1}{2}(1 + i\sqrt{d})$, for some positive integer $d \equiv 3 \bmod 4$.

According to Proposition 95 and Example 58,

$$\mathcal{N}(E)(\mathbb{C}) \cong \mathbb{C}^2/\Lambda_\tau \oplus \overline{\Lambda_\tau},$$

G-equivariantly, where G acts on $\mathbb{C}^2$ by

$$\sigma \cdot (z, w) = (\overline{w}, \overline{z}),$$

for any $z, w \in \mathbb{C}$. Let L be the $\mathbb{C}$-linear endomorphism of $\mathbb{C}^2$ given by

$$L(z, w) = \left(\frac{z + w}{2}, \frac{z - w}{2i}\right).$$

Then, taking the domain of L equipped with the action of G defined above, and the codomain of L equipped with the standard action of G, the mapping L is G-equivariant. In particular,

$$\mathcal{N}(E)(\mathbb{C}) \cong \mathbb{C}^2/\Lambda,$$

where $\Lambda = L(\Lambda_\tau \oplus \overline{\Lambda_\tau}) \subseteq \mathbb{C}^2$ is the lattice generated by $x_1, x_2, \frac{1}{2}(x_1 + y_1), \frac{1}{2}(x_2 + y_2)$, where

$$x_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ x_2 = \tfrac{1}{2}\begin{pmatrix} 1 \\ \sqrt{d} \end{pmatrix}, \ y_1 = \begin{pmatrix} 0 \\ i \end{pmatrix}, \quad \text{and} \quad y_2 = \tfrac{1}{2}\begin{pmatrix} i\sqrt{d} \\ -i \end{pmatrix}.$$

Put $x_2' = \frac{1}{2}(d-1)x_1 + x_2$. Then, since d is odd, $x_2' \in \Lambda$. Moreover, x_1, x_2' is a $\mathbb{Z}$-basis for $\operatorname{Re}\Lambda$. One easily computes that

$$i\sqrt{d}x_1 = y_1 + 2y_2 \quad \text{and} \quad i\sqrt{d}x_2' = d(y_1 + y_2).$$

Since $y_1 + 2y_2, y_1 + y_2$ is a $\mathbb{Z}$-basis for $\operatorname{Im}\Lambda$ and

$$\tfrac{1}{2}(x_1 + (y_1 + 2y_2)) = \tfrac{1}{2}(x_1 + y_1) + y_2 \in \Lambda$$

and

$$\begin{aligned} \tfrac{1}{2}(x_2' + (y_1 + y_2)) &= \tfrac{1}{2}(\tfrac{1}{2}(d-1)x_1 + x_2 + y_1 + y_2) \\ &= \tfrac{1}{4}(d-3)x_1 + \tfrac{1}{2}(x_1 + y_1) + \tfrac{1}{2}(x_2 + y_2) \in \Lambda, \end{aligned}$$

we have an isomorphism

$$\alpha \colon \mathbb{C}/\Lambda_1 \times \mathbb{C}/\Lambda_2 \longrightarrow \mathbb{C}^2/\Lambda,$$

induced by the mapping from $\mathbb{C}^2$ into itself given by

$$(z, w) \longmapsto (zx_1, wx_2'),$$

where

$$\Lambda_1 = \mathbb{Z} + \mathbb{Z}\tfrac{1}{2}(1 + i\sqrt{d}) \quad \text{and} \quad \Lambda_2 = \mathbb{Z} + \mathbb{Z}\tfrac{1}{2}(1 + i(\sqrt{d})^{-1}).$$

Observe that both lattices Λ_1 and Λ_2 are stable under complex conjugation and, moreover, α is G-equivariant (taking on both domain and codomain of α the standard action of G). By Example 52 there exists algebraic curves X_1, X_2 over $\mathbb{R}$ such that

$$X_j(\mathbb{C}) \cong \mathbb{C}/\Lambda_j$$

G-equivariantly, for every j. In particular, $X_1 \times X_2$ is isomorphic to $\mathcal{N}(E)$. Therefore,

$$C_1 \times C_2 \cong_{\mathbb{R}} E,$$

where $C_j = \mathcal{R}(X_j)$, $j = 1, 2$. □

Example 97. Let us compute now the $\mathbb{Z}/2\mathbb{Z}$-dimension of the group $H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z})$ in the case E is an elliptic curve over $\mathbb{C}$ such that

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau,$$

where $\tau = i\sqrt{d}$, for some positive integer d.

As in Example 96,

$$\mathcal{N}(E)(\mathbb{C}) \cong \mathbb{C}^2/\Lambda,$$

where $\Lambda = L(\Lambda_\tau \oplus \overline{\Lambda_\tau})$. Clearly, Λ is generated by

$$x_1, x_2, \tfrac{1}{2}(x_1 + y_1), \tfrac{1}{2}(x_2 + y_2),$$

where

$$x_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ x_2 = \begin{pmatrix} 0 \\ \sqrt{d} \end{pmatrix}, \ y_1 = \begin{pmatrix} 0 \\ i \end{pmatrix}, \quad \text{and} \quad y_2 = \begin{pmatrix} i\sqrt{d} \\ 0 \end{pmatrix}.$$

Put

$$M = \begin{pmatrix} 0 & (\sqrt{d})^{-1} \\ \sqrt{d} & 0 \end{pmatrix}.$$

Then, according to Corollary 90,

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z}) = \dim_{\mathbb{Z}/2\mathbb{Z}} S_2(M)/T_2(M).$$

One easily computes that $S_2(M)$ is the group of integral 2×2-matrices

$$\begin{pmatrix} k & l \\ m & kd \end{pmatrix}$$

such that $l \equiv m \bmod 4$ and all k, l, m even. The subgroup $T_2(M)$ of $S_2(M)$ consists of the matrices

$$\begin{pmatrix} k & l \\ m & kd \end{pmatrix} \in S_2(M)$$

such that k is divisible by 4. We see that the quotient $S_2(M)/T_2(M)$ has $\mathbb{Z}/2\mathbb{Z}$-dimension 1. Therefore,

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z}) = 1,$$

whenever E is an elliptic curve over $\mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$, with $\tau = i\sqrt{d}$, for some positive integer d.

Observe that in the special case $d \equiv 2 \bmod 4$ every element $A \in S_2(M)$ which is nontrivial in the quotient $S_2(M)/T_2(M)$ has nonzero determinant. For, if

$$A = \begin{pmatrix} k & l \\ m & kd \end{pmatrix}$$

is not contained in $T_2(M)$ then k is even but not divisible by 4. Hence,

$$2^3 \mid k^2 d \quad \text{and} \quad 2^4 \not| \, k^2 d.$$

Since $l \equiv m \bmod 4$,

$$2^3 \mid lm \Rightarrow 2^4 \mid lm.$$

Hence, $k^2 d \neq lm$ and therefore $\det A$ is nonzero. This implies that the nonzero class in $H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z})$ cannot be represented by a real algebraic subgroup whenever $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_\tau$, $\tau = i\sqrt{d}$ and $d \equiv 2 \bmod 4$. For, let $C \subseteq {}_{\mathbb{R}}E$ be a real algebraic subgroup of dimension 1 and $\overline{C} \subseteq \mathcal{N}(E)$ its closure in $\mathcal{N}(E)$. Then $\overline{C}$ is an elliptic curve over $\mathbb{R}$. Let $\mathcal{L}$ be the invertible sheaf on $\mathcal{N}(E)$ corresponding to the divisor $\overline{C}$. Clearly, $\mathcal{L}$ is isomorphic to the pull-back of some invertible sheaf under the canonical morphism

$$\mathcal{N}(E) \longrightarrow \mathcal{N}(E)/\overline{C}.$$

Therefore, if (α, F) is an Appell-Humbert datum over $\mathbb{R}$ such that $L(\alpha, F) \cong \mathcal{L}$, the bilinear form F is degenerate. This implies that the matrix $A \in S_2(M)$ associated to F has zero determinant. It follows that

$$[C] = 0$$

in $H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z})$. □

Recall that an elliptic curve E over $\mathbb{C}$ is said to have *complex multiplication* if $\mathrm{End}(E) \neq \mathbb{Z}$ (cf. also Definition 102).

If E is an elliptic curve over $\mathbb{C}$ and $\tau \in \mathbb{C}$ such that

$$\mathbb{C}/\Lambda_\tau \cong E(\mathbb{C}),$$

then E has complex multiplication if and only if $[\mathbb{Q}(\tau):\mathbb{Q}] = 2$. Moreover, $\mathrm{End}(E)$ is then a subring of the field $L = \mathbb{Q}(\tau)$. Since L is a quadratic imaginary extension of $\mathbb{Q}$, there exists a square-free negative integer d such that

$$\mathbb{Q}(\sqrt{d}) \cong L.$$

Since L is the quotient field of $\mathrm{End}(E)$ and $\mathrm{End}(E)$ is finitely generated as a $\mathbb{Z}$-module, there exists a unique positive integer c such that

$$\mathrm{End}(E) = \begin{cases} \mathbb{Z}[c\sqrt{d}], & \text{if } d \not\equiv 1 \bmod 4 \\ \mathbb{Z}[c\frac{1}{2}(1+\sqrt{d})], & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

Then, the *discriminant* $\mathfrak{d}_{\mathfrak{E}}$ of $\mathrm{End}(E)$ is the ideal of $\mathbb{Z}$ generated by $4c^2d$ in the case $d \not\equiv 1 \bmod 4$ and c^2d in the case $d \equiv 1 \bmod 4$.

The following statement is proved in [14].

Theorem 98. *If E and F are elliptic curves over $\mathbb{C}$ with complex multiplication then*

$$_{\mathbb{R}}E \cong {}_{\mathbb{R}}F \iff \mathrm{End}(E) \cong \mathrm{End}(F).$$

This enables us to compute the $\mathbb{Z}/2\mathbb{Z}$-dimension of $H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z})$ in the case E has complex multiplication (see also [6]).

Theorem 99. *If E is an elliptic curve over $\mathbb{C}$ with complex multiplication then*

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z}) = 2$$

if and only if the discriminant $\mathfrak{d}_{\mathfrak{E}}$ of $\mathrm{End}(E)$ is not divisible by 2. Otherwise,

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_1^{alg}({}_{\mathbb{R}}E, \mathbb{Z}/2\mathbb{Z}) = 1.$$

Proof. Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication. Consider $\mathrm{End}(E)$ as a lattice Λ in $\mathbb{C}$. By Example 52, there exists an elliptic curve F over $\mathbb{C}$ such that

$$F(\mathbb{C}) \cong \mathbb{C}/\Lambda.$$

Clearly, $\mathrm{End}(F) \cong \mathrm{End}(E)$. Therefore, by Theorem 98, it suffices to compute

$$\dim_{\mathbb{Z}/2\mathbb{Z}} H_1^{alg}({}_{\mathbb{R}}F, \mathbb{Z}/2\mathbb{Z}).$$

The conclusion follows from Example 96 and Example 97. □

Corollary 100. [5] *Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication. Then the underlying real algebraic structure ${}_{\mathbb{R}}E$ of E is isomorphic to the product $C_1 \times C_2$ of two real algebraic curves C_1 and C_2 if and only if the discriminant $\mathfrak{d}_{\mathfrak{E}}$ of* $\mathrm{End}(E)$ *is not divisible by* 2*.*

Remark 101. The group $H_1^{alg}({}_{\mathbb{R}}X, \mathbb{Z}/2\mathbb{Z})$, where X is an arbitrary nonsingular projective curve over $\mathbb{C}$, has been studied in [6], where a slightly weaker version of Theorem 99 has been proved earlier by a different method. □

Chapter 3

Real abelian varieties with complex multiplication

In the first section of this chapter we introduce the notion of sufficiently many complex multiplications for abelian varieties over $\mathbb{C}$, as well as over $\mathbb{R}$. We prove some basic facts from which it becomes clear that classification of real abelian varieties X admitting sufficiently many complex multiplications is equivalent to classification of so-called Galois B-modules, where B is the center of the ring of endomorphisms $\mathrm{End}(X_{\mathbb{C}})$ of $X_{\mathbb{C}}$. Section 3.2 is devoted to classification of these modules. In the last section of this chapter, the results of Section 3.2 are used to prove the classification theorem about the underlying real algebraic structure of abelian varieties over $\mathbb{C}$ having sufficiently many complex multiplications (Theorem 136) and the theorem concerning the problem of the product structure of simple abelian varieties over $\mathbb{C}$ having sufficiently many complex multiplications (Theorem 140). Theorems 136 and 140 are the main theorems of this chapter.

3.1 Complex multiplication

Definition 102. *An abelian variety X over $\mathbb{C}$ is said to* have sufficiently many complex multiplications *if the endomorphism algebra $\mathrm{End}^{\mathrm{o}} X$ of X contains a field of degree $2 \dim X$ over $\mathbb{Q}$. In the case $\dim X = 1$ this is the same as "X* has complex multiplication*".*

Remark 103. This definition is different from that in [25, p. 399]. Both definitions coincide in the case of simple abelian varieties over $\mathbb{C}$. In [25] an arbitrary abelian variety X over $\mathbb{C}$ is said to have sufficiently many complex multiplications whenever X is isogenous to a product of simple abelian varieties over $\mathbb{C}$, each having sufficiently many complex multiplications (in either sense). For us, X has sufficiently many complex multiplications if and only if X is isogenous to Y^m, for some simple abelian variety Y over $\mathbb{C}$ having sufficiently many complex multiplications (Proposition 106). □

Example 104. If X is an elliptic curve over $\mathbb{C}$ then there exists $\tau \in \mathbb{C} - \mathbb{R}$ such that $\mathbb{C}/\Lambda_\tau \cong X(\mathbb{C})$, where

$$\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau.$$

It is easy to check that X has complex multiplication if and only if $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$. □

Remark 105. If X is a simple abelian variety over $\mathbb{C}$ of dimension n then it is proved in [23, p. 183] that

$$\operatorname{rank}_{\mathbb{Z}} \operatorname{End}(X) \leq 2n.$$

Moreover, X has sufficiently many complex multiplications if and only if

$$\operatorname{rank}_{\mathbb{Z}} \operatorname{End}(X) = 2n,$$

and then the endomorphism algebra $\operatorname{End}^{\circ} X$ of X is a field of degree $2n$ over $\mathbb{Q}$.

If a field L is isomorphic to $\operatorname{End}^{\circ} X$, for some simple abelian variety X over $\mathbb{C}$ having sufficiently many complex multiplications then L is called a *CM-field*. A CM-field has a unique totally real subfield K such that

$$[L : K] = 2$$

(cf. [23, p. 210]). Moreover, the extension L/K is totally imaginary. Conversely, we will see in Proposition 108 that every number field L which is a totally imaginary extension of degree 2 of a totally real field K, is a CM-field. □

Let us study more closely what it means for a (possibly nonsimple) abelian variety over $\mathbb{C}$ to have sufficiently many complex multiplications.

Proposition 106. *Let X be an abelian variety over $\mathbb{C}$. Then X has sufficiently many complex multiplications if and only if X is isogenous to Y^m, for some simple abelian variety Y over $\mathbb{C}$ with sufficiently many complex multiplications and some positive integer m.*

Proof. Of course, if Y is a simple abelian variety over $\mathbb{C}$ with sufficiently many complex multiplications then for every positive integer m, the abelian variety Y^m has sufficiently many complex multiplications. For, by Remark 105, $L = \mathrm{End}^{\mathrm{o}}\, Y$ is a field of degree $2 \dim Y$ over $\mathbb{Q}$. Hence,

$$\mathrm{End}^{\mathrm{o}}\,(Y^m) \cong \mathbf{M}_m(L),$$

the matrix algebra of order m over L. Clearly, $\mathrm{End}^{\mathrm{o}}\,(Y^m)$ contains a field of degree $2m \dim Y$ over $\mathbb{Q}$. Therefore, if X is isogenous to Y^m then X has sufficiently many complex multiplications.

Conversely, suppose X has sufficiently many complex multiplications. By Theorem 47, X is isogenous to

$$X_1^{m_1} \times \cdots \times X_k^{m_k},$$

where $X_1, \ldots, X_k$ are mutually nonisogenous simple abelian varieties over $\mathbb{C}$. If we put $D_i = \mathrm{End}^{\mathrm{o}}\, X_i$ then

$$\mathrm{End}^{\mathrm{o}}\, X \cong \prod_{i=1}^{k} \mathbf{M}_{m_i}(D_i).$$

Since $\mathrm{End}^{\mathrm{o}}\, X$ contains a field of degree $2n$ over $\mathbb{Q}$, where n is the dimension of X, there exists $j \leq k$ such that $\mathbf{M}_{m_j}(D_j)$ contains a field of degree $2n$ over $\mathbb{Q}$. Such a field has necessarily its degree over $\mathbb{Q}$ less than or equal to

$$m_j d_j e_j,$$

where e_j is the degree of the center K_j of D_j and d_j^2 is the K_j-dimension of D_j. Hence,

$$2n \leq m_j d_j e_j \leq m_j d_j^2 e_j \leq 2m_j \dim X_j,$$

by Remark 105. Therefore, X is isogenous to $X_j^{m_j}$ and $d_j = 1$, which implies that X_j has sufficiently many complex multiplications. $\square$

Suppose X is a simple abelian variety over $\mathbb{C}$ with sufficiently many complex multiplications. According to Remark 105,

$$L = \operatorname{End}^{\mathrm{o}} X$$

is a field. The subring $B = \operatorname{End}(X)$ of L is finitely generated as a $\mathbb{Z}$-module and has L as its field of fractions, i.e. B is an *order* in L. Let Λ be a lattice in some complex vector space V such that

$$V/\Lambda \cong X(\mathbb{C}).$$

As Λ is a lattice, the canonical mapping

$$\mathbb{R} \otimes_{\mathbb{Z}} \Lambda \longrightarrow V$$

is an isomorphism of real vector spaces, even of $\mathbb{R} \otimes_{\mathbb{Z}} B$-modules. This isomorphism induces a complex vector space structure on $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda$ which is compatible with the $\mathbb{R} \otimes_{\mathbb{Z}} B$-module structure since the action of B on V is $\mathbb{C}$-linear. Since Λ and B have the same $\mathbb{Z}$-rank, $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda$ is a free $\mathbb{R} \otimes_{\mathbb{Z}} B$-module of rank 1. Therefore $\mathbb{R} \otimes_{\mathbb{Z}} B$ has a complex vector space structure, which, moreover, does not depend on the isomorphism

$$\mathbb{R} \otimes_{\mathbb{Z}} B \longrightarrow \mathbb{R} \otimes_{\mathbb{Z}} \Lambda$$

chosen, since the action of B on $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda$ is $\mathbb{C}$-linear. Clearly this complex vector space structure turns the $\mathbb{R}$-algebra $\mathbb{R} \otimes_{\mathbb{Z}} B$ into a $\mathbb{C}$-algebra, that is, we are given a morphism of $\mathbb{R}$-algebras

$$\Phi \colon \mathbb{C} \longrightarrow \mathbb{R} \otimes_{\mathbb{Z}} B.$$

By construction, the complex vector space structure on

$$(\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes_B \Lambda$$

induced by Φ coincides with the complex vector space structure on $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda$ and

$$((\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes_B \Lambda)/\Lambda \cong X(\mathbb{C}),$$

as complex tori.

More general we have the following proposition.

Proposition 107. *If X is an abelian variety over $\mathbb{C}$ with sufficiently many complex multiplications and B is the center of the ring of endomorphisms* $\mathrm{End}(X)$ *of X then there exists a structure of a $\mathbb{C}$-algebra*

$$\Phi\colon \mathbb{C} \longrightarrow \mathbb{R} \otimes_{\mathbb{Z}} B$$

on the $\mathbb{R}$-algebra $\mathbb{R} \otimes_{\mathbb{Z}} B$ and there exists a B-module M such that

$$((\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes_B M)/M \cong X(\mathbb{C}),$$

as complex tori.

Proof. By Proposition 106, there exists a simple abelian variety Y over $\mathbb{C}$ having sufficiently many complex multiplications such that Y^m and X are isogenous. After chosing an isogeny, we may identify $\mathrm{End}^{\mathrm{o}} X$ with $\mathrm{End}^{\mathrm{o}}(Y^m)$. Of course, we may assume that

$$B \subseteq \mathrm{End}(Y^m).$$

By the discussion preceding this proposition, there exists a $\mathbb{C}$-algebra structure

$$\Phi\colon \mathbb{C} \longrightarrow \mathbb{R} \otimes_{\mathbb{Z}} B$$

on the $\mathbb{R}$-algebra $\mathbb{R} \otimes_{\mathbb{Z}} B$ and a B-module Λ such that

$$((\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes_B \Lambda)/\Lambda \cong Y(\mathbb{C}).$$

Let M be a lattice in some complex vector space V such that the complex tori V/M and $X(\mathbb{C})$ are isomorphic. The chosen isogeny gives us a mapping from Λ^m into M such that the induced mapping

$$(\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes_B \Lambda^m \longrightarrow V$$

is $\mathbb{C}$-linear. Therefore,

$$((\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes_B M)/M \cong X(\mathbb{C}),$$

as complex tori. □

One can reverse this construction. Suppose L is a number field which is a totally imaginary degree 2 extension of a totally real field K and B is an order in L. The canonical mapping

$$\mathbb{R} \otimes_{\mathbb{Z}} B \longrightarrow \mathbb{R} \otimes_{\mathbb{Q}} L$$

is an isomorphism of $\mathbb{R}$-algebras. Therefore, giving a $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Q}} L$ is equivalent to giving a $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Z}} B$. If $\sigma_1, \ldots, \sigma_n$ are the embeddings of K into $\mathbb{R}$ then

$$\mathbb{R} \otimes_{\mathbb{Q}} K \cong \prod_{i=1}^{n} \mathbb{R}_i,$$

as $\mathbb{R}$-algebras, where $\mathbb{R}_i$ is the K algebra

$$K \xrightarrow{\sigma_i} \mathbb{R}.$$

Hence,

$$\mathbb{R} \otimes_{\mathbb{Q}} L \cong \prod_{i=1}^{n} \mathbb{R}_i \otimes_K L,$$

Since L/K is totally imaginary, $\mathbb{R}_i \otimes_K L$ is isomorphic to $\mathbb{C}$, for every i. Therefore, there exists exactly 2^n structures of a $\mathbb{C}$-algebra on $\mathbb{R} \otimes_{\mathbb{Q}} L$, where n is the degree of K over $\mathbb{Q}$.

Now, let us take a $\mathbb{C}$-algebra structure Φ on $\mathbb{R} \otimes_{\mathbb{Z}} B$. If M is a torsion free finitely generated B-module then M can be considered as a subgroup of the complex vector space $(\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes_B M$. Clearly,

$$((\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes_B M)/M$$

is a complex torus. The following proposition states that this complex torus comes from an abelian variety over $\mathbb{C}$.

Proposition 108. *Let L be a totally imaginary degree 2 extension of a totally real field K and let B be an order in L. Let Φ be a structure of a $\mathbb{C}$-algebra on $\mathbb{R} \otimes_{\mathbb{Z}} B$. If M is a torsion free finitely generated B-module then there exists an abelian variety $X = X(M, \Phi)$ over $\mathbb{C}$ such that*

$$X(\mathbb{C}) \cong ((\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes_B M)/M,$$

as complex tori. In particular, X has sufficiently many complex multiplications and L is a CM-field.

Proof. It suffices to prove the statement for $M = B^m$ and then it reduces to the case $m = 1$, and B is the ring of integers in L. This case is proved in [23, p. 212]. □

Remark 109. Notice that the abelian variety $X(B, \Phi)$ over $\mathbb{C}$, with notation as in the preceding proposition, need not be simple. □

Example 110. If L is a quadratic imaginary extension of $\mathbb{Q}$, that is,

$$L = \mathbb{Q}(\sqrt{d}),$$

for some square-free negative integer d, then L is a CM-field. Let B be any order in L. Since

$$\mathbb{R} \otimes_{\mathbb{Z}} B \cong \mathbb{R} \otimes_{\mathbb{Q}} L \cong \mathbb{C},$$

a $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Z}} B$ corresponds to an embedding of L in $\mathbb{C}$. Therefore, there are exactly 2 $\mathbb{C}$-algebra structures Φ_1 and Φ_2 on $\mathbb{R} \otimes_{\mathbb{Z}} B$. If M is a torsion free finitely generated B-module then, clearly,

$$X(M, \Phi_1) \cong X(M^\sigma, \Phi_2),$$

where M^σ is the conjugate B-module structure on M. Therefore, in this case, one may fix an embedding of L in $\mathbb{C}$, or equivalently, one may fix a $\mathbb{C}$-algebra structure Φ on $\mathbb{R} \otimes_{\mathbb{Z}} B$, since every abelian variety X over $\mathbb{C}$ with sufficiently many complex multiplications and

$$\mathrm{Center}(\mathrm{End}^{\mathrm{o}} X) \cong L$$

is isomorphic to some $X(M, \Phi)$. □

Example 111. Let $m > 2$ be an integer and let ξ_m be a primitive m^{th} root of unity. Then

$$L = \mathbb{Q}(\xi_m)$$

is a CM-field. For, let

$$K = \mathbb{Q}(\xi_m + \xi_m^{-1}).$$

Then $[L : K] = 2$ and K is totally real and L is a totally imaginary extension of K. By Proposition 108, L is a CM-field. Let φ be the

Euler φ-function . Then, if B is any order in L and Φ is a $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Z}} B$,

$$\dim X(B, \Phi) = \frac{1}{2}\varphi(m),$$

since $[L : \mathbb{Q}] = \varphi(m)$. □

The construction of $X(M, \Phi)$ is functorial in the B-module M. Hence, $X(\cdot, \Phi)$ is a functor from the category of finitely generated torsion free B-modules into the category of abelian varieties over $\mathbb{C}$ with sufficiently many complex multiplications.

Proposition 112. *Let L be a CM-field and B an order in L. If Φ is a $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Z}} B$ such that $X(B, \Phi)$ is simple then the functor $X(\cdot, \Phi)$ is an equivalence onto some full subcategory of the category of abelian variety over $\mathbb{C}$ with sufficiently many complex multiplications, that is, for any finitely generated torsion free B-modules M and N, the mapping*

$$X(\cdot, \Phi)\colon \mathrm{Hom}_B(M, N) \longrightarrow \mathrm{Hom}(X(M, \Phi), X(N, \Phi))$$

is a bijection.

Proof. It is clear that this mapping is injective. Moreover, the cokernel of this mapping is torsion free. For, if φ is a morphism from $X(M, \Phi)$ into $X(N, \Phi)$ then, in particular, there exists a $\mathbb{Z}$-linear mapping ψ from M into N such that

$$X(\psi, \Phi) = \varphi.$$

Hence, if there exists an nonzero integer k such that $k\varphi$ is in the image of $X(\cdot, \Phi)$ then $k\psi$ is B-linear and then ψ is B-linear.

Therefore, it suffices to prove that

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}_B(M, N) \quad \text{and} \quad \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(X(M, \Phi), X(N, \Phi))$$

have the same dimension over $\mathbb{Q}$. To prove this we may assume that $M = B^m$ and $N = B^n$. Since $X(B, \Phi)$ is simple,

$$\mathrm{End}(X(B, \Phi)) = B.$$

Moreover, $X(M,\Phi)$ is isomorphic to $X(B,\Phi)^m$ and $X(N,\Phi)$ is isomorphic to $X(B,\Phi)^n$. Therefore, both $\mathbb{Q}$-dimensions are equal. The proposition follows. □

Remark 113. For the functor $X(\cdot,\Phi)$ to be full it is necessary that $X(B,\Phi)$ is simple. For, if $X(B,\Phi)$ is not simple then, by Proposition 106, it is isogenous to Y^m, for some $m > 1$ and some simple abelian variety Y over $\mathbb{C}$ having sufficiently many complex multiplications. Then

$$\operatorname{rank}_{\mathbb{Z}} \operatorname{End}(X(B,\Phi)) = m^2 \operatorname{rank}_{\mathbb{Z}} \operatorname{End}(Y) = 2m \dim X,$$

while $\operatorname{rank}_{\mathbb{Z}} B = 2 \dim X$. □

Let us turn our attention to abelian varieties over $\mathbb{R}$.

Definition 114. *An abelian variety X over $\mathbb{R}$ is said to* admit sufficiently many complex multiplications *if $X_{\mathbb{C}}$ has sufficiently many complex multiplications. In the case X has dimension 1 this is the same as “X* admits complex multiplication *”.*

Let G be the Galois group of $\mathbb{C}/\mathbb{R}$ and let σ be the nontrivial element of G. If L is a CM-field and K its maximal totally real subfield then any embedding of L in $\mathbb{C}$ is stable under σ. For, if $L \subseteq \mathbb{C}$ then $K \subseteq \mathbb{R}$. Hence, $\sigma(K) = K$. As L/K is Galois, $\sigma(L) = L$. Moreover, this shows that there is a canonical isomorphism

$$G \longrightarrow \operatorname{Gal}(L/K).$$

Sometimes, the image of $\sigma \in G$ under this canonical mapping is again denoted by σ.

If B is an order in L then, since the degree of the extension L/K is 2, B is stable under the action of $\operatorname{Gal}(L/K)$. A B-module M, together with an action of the group $\operatorname{Gal}(L/K)$ will be called a *Galois B-module* if

$$\tau(bm) = \tau(b)\tau m,$$

for every $m \in M$, $b \in B$ and $\tau \in \operatorname{Gal}(L/K)$. With the obvious definition of a morphism of Galois B-modules, we have a category of Galois B-modules.

Now, if M is a Galois B-module which is a finitely generated torsion free B-module then we can construct an abelian variety over $\mathbb{R}$ out of M, denoted by $X_{\mathbb{R}}(M, \Phi)$, having sufficiently many complex multiplications, where Φ is some $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Z}} B$. This construction goes as follows.

As σ acts on B we have an induced $\mathbb{R}$-linear action of σ on $\mathbb{R} \otimes_{\mathbb{Z}} B$. Therefore we have an $\mathbb{R}$-linear action of σ on the complex vector space $V = (\mathbb{R} \otimes_{\mathbb{Z}} B) \otimes M$ determined by

$$\sigma \cdot \lambda \otimes b \otimes m = (\sigma \cdot \lambda \otimes b) \otimes \sigma m,$$

since M is a Galois B-module. Clearly,

$$\Phi \colon \mathbb{C} \longrightarrow \mathbb{R} \otimes_{\mathbb{Z}} B$$

is G-equivariant. Therefore σ acts anti-linear on V. Hence, (W, M) is a lattice over $\mathbb{R}$, where $W = V^G$, and, using Proposition 108, there exists an abelian variety $X_{\mathbb{R}}(M, \Phi)$ over $\mathbb{R}$ such that

$$X_{\mathbb{R}}(M, \Phi)(\mathbb{C}) \cong_G (\mathbb{C} \otimes_{\mathbb{R}} W)/M.$$

Clearly, $X_{\mathbb{R}}(M, \Phi)$ admits sufficiently many complex multiplications.

The following proposition shows that all abelian varieties over $\mathbb{R}$ admitting sufficiently many complex multiplications are of this form.

Proposition 115. *Let X be an abelian variety over $\mathbb{R}$ admitting sufficiently many complex multiplications and let B be the center of the ring* $\mathrm{End}(X_{\mathbb{C}})$. *Then there exist a $\mathbb{C}$-algebra structure Φ on $\mathbb{R} \otimes_{\mathbb{Z}} B$ and a Galois B-module M, which is finitely generated and torsion free as a B-module, such that*

$$X_{\mathbb{R}}(M, \Phi) \cong X.$$

Proof. By Proposition 107, there exists a $\mathbb{C}$-algebra structure Φ on $\mathbb{R} \otimes_{\mathbb{Z}} B$ and a finitely generated torsion free B-module M such that

$$X(M, \Phi) \cong X_{\mathbb{C}}.$$

Hence, using this isomorphism, we have an action of G on $X(M, \Phi)$. Since B is the center of $\mathrm{End}(X(M, \Phi))$, this gives rise to an action of σ on B given by

$$\sigma \cdot b = \sigma \circ b \circ \sigma^{-1}.$$

Then, there exists an automorphism τ of $L/\mathbb{Q}$, where L is the quotient field of B, such that

$$\tau(b) = \sigma \cdot b.$$

We will prove that τ is equal to the image of σ under the canonical mapping $G \to \operatorname{Gal}(L/K)$, where K is the maximal totally real subfield of L.

Let $L' \subseteq L$ be the fixed field of $\tau^{-1}\sigma$, where σ is considered to be an element of $\operatorname{Gal}(L/K)$. As the action of both σ and τ on the complex vector space $\mathbb{R} \otimes_{\mathbb{Z}} B$ is anti-linear, $\tau^{-1}\sigma$ acts $\mathbb{C}$-linear on $\mathbb{R} \otimes_{\mathbb{Z}} B$. In particular, Φ factorizes through the canonical mapping

$$\mathbb{R} \otimes_{\mathbb{Q}} L' \longrightarrow \mathbb{R} \otimes_{\mathbb{Q}} L.$$

It follows that L' is a CM-field and, since $X(B,\Phi)$ is simple, we have $L' = L$. Therefore, $\tau = \sigma$.

As a consequence M is a Galois B-module and $X_{\mathbb{R}}(M,\Phi) \cong X$. This finishes the proof. □

Clearly, the construction of $X_{\mathbb{R}}(M,\Phi)$ is canonical in M. Therefore, $X_{\mathbb{R}}(\cdot,\Phi)$ is a functor from the category of Galois B-modules into the category of abelian varieties over $\mathbb{R}$ admitting sufficiently many complex multiplications.

Proposition 116. *Let L be a CM-field and B an order in L. If Φ is a $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Z}} B$ such that $X(B,\Phi)$ is simple then the functor $X_{\mathbb{R}}(\cdot,\Phi)$ is an equivalence onto a full subcategory of the category of abelian varieties over $\mathbb{R}$ with sufficiently many complex multiplications, that is, the mapping*

$$X_{\mathbb{R}}(\cdot,\Phi)\colon \operatorname{Hom}_{B,G}(M,N) \longrightarrow \operatorname{Hom}(X_{\mathbb{R}}(M,\Phi), X_{\mathbb{R}}(N,\Phi))$$

is a bijection, for any Galois B-modules M and N that are finitely generated and B-torsion free.

Proof. This follows immediately from Proposition 112. □

As a last topic in this section, let us study the Weil restriction of an abelian variety over $\mathbb{C}$ with sufficiently many complex multiplications.

In virtue of Proposition 107, it suffices to study abelian varieties over $\mathbb{C}$ of the form $X(M,\Phi)$, where M is a B-module and Φ is a $\mathbb{C}$-algebra structure on $\mathbb{R}\otimes_{\mathbb{Z}} B$, for some order B in L.

Observe that if M is a B-module then $M\oplus M^\sigma$ can be made into a Galois B-module in the following way. Define the action of σ on $M\oplus M^\sigma$ by

$$\sigma\cdot(m,m')=(m',m),$$

for every $m\in M$ and $m'\in M^\sigma$. Here M^σ is again the conjugate B-module structure on M with respect to σ. Clearly, this Galois B-module depends in a functorial way on M. Hence, we get a functor from the category of B-modules into the category of Galois B-modules.

Proposition 117. *Let L be a CM-field and B an order in L. If Φ is a $\mathbb{C}$-algebra structure on $\mathbb{R}\otimes_{\mathbb{Z}} B$ and M is a finitely generated torsion free B-module then*

$$\mathcal{N}(X(M,\Phi))\cong X_{\mathbb{R}}(M\oplus M^\sigma,\Phi),$$

canonically. In particular, the Weil restriction of an abelian variety over $\mathbb{C}$ with sufficiently many complex multiplications is an abelian variety over $\mathbb{R}$ admitting sufficiently many complex multiplications.

Proof. If Φ is a $\mathbb{C}$-algebra structure on $\mathbb{R}\otimes_{\mathbb{Z}} B$ and M is a finitely generated torsion free B-module then the complex vector space structure on

$$(\mathbb{R}\otimes_{\mathbb{Z}} B)\otimes_B M^\sigma$$

is canonically isomorphic to the conjugate complex vector space structure on

$$(\mathbb{R}\otimes_{\mathbb{Z}} B)\otimes_B M.$$

Therefore, the first statement follows from Proposition 95. The last statement follows from the first and Proposition 107. □

3.2 Galois B-modules

In this section K will be a number field and $A\subseteq K$ a Dedekind ring having quotient field K. Furthermore, L/K will be a finite Galois extension with Galois group G and $B \subseteq L$ will be the integral closure of A in L. In particular, it follows that B is finitely generated as an A-module and B is a Dedekind ring [18, p. 6].

If $\mathfrak{p}$ is a nonzero prime ideal of A then

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}},$$

where the product is taken over the set of all prime ideals $\mathfrak{P}$ of B which lie over $\mathfrak{p}$. If moreover

$$f_{\mathfrak{P}} = [B/\mathfrak{P} : A/\mathfrak{p}],$$

then it is known [18, p. 24] that

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} = n,$$

where n is the degree of the extension L/K. Since the Galois group G acts transitively on the set of primes of B which lie over $\mathfrak{p}$ [18, p. 12], the integers $e_{\mathfrak{P}}$ and $f_{\mathfrak{P}}$ depend only on $\mathfrak{p}$. Henceforth, we will denote these integers by $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$, respectively. In particular, for every nonzero prime $\mathfrak{p}$ of A,

$$e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}} = n, \tag{3.1}$$

where $g_{\mathfrak{p}}$ is the number of primes of B which lie over $\mathfrak{p}$. The nonzero prime $\mathfrak{p}$ of A is called *ramified* in B if

$$e_{\mathfrak{p}} \neq 1.$$

Otherwise, the prime $\mathfrak{p}$ of A is called *unramified* in B.

Example 118. Since we will be primary interested in the case that the degree of the extension L/K is 2, let us see in this case what it means for a nonzero prime $\mathfrak{p}$ of A to be ramified in B. It follows immediately from formula (3.1) that $\mathfrak{p}$ is ramified in B if and only if $\mathfrak{p}B$ is not a prime ideal of B and there exists exactly one prime ideal of B which lies over $\mathfrak{p}$. $\square$

Let us recall the definition of the *discriminant* $\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}$ of B over A [30, p. 50]. If

$$T\colon L \times L \longrightarrow K$$

is the trace form with respect to L/K, i.e. $T(x,y) = \mathrm{Tr}_{L/K}(xy)$, then there is a canonical mapping

$$\bigwedge T\colon V \otimes_K V \longrightarrow K,$$

where V is the n-fold exterior power of L as a K-module and n is the degree of the extension L/K. The image in V of the n-fold exterior power of B as an A-module, is a finitely generated A-module M. The discriminant $\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}$ of B over A is by definition the image of M under $\bigwedge T$. In particular, the discriminant of B over A is a nonzero ideal of A. If B is a free A-module then, the discriminant of B over A is principal and generated by

$$\det(\mathrm{Tr}_{L/K}(x_i x_j)),$$

where $\{x_1, \ldots, x_n\}$ is a basis for B, which is equal to

$$\det(\sigma(x_i))^2,$$

where σ runs through the Galois group G.

It is well known [30, p. 53] that a nonzero prime ideal $\mathfrak{p}$ of A is ramified in B if and only if $\mathfrak{p}$ divides the discriminant $\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}$ of B over A.

Example 119. If $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$, for some nonzero square-free integer d, then the ring of integers $\mathcal{O}$ in L is $\mathbb{Z}[\omega]$, where

$$\omega = \begin{cases} \sqrt{d}, & \text{if } d \not\equiv 1 \bmod 4, \\ \frac{1}{2} + \frac{1}{2}\sqrt{d}, & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Taking $A = \mathbb{Z}$ and $B = \mathcal{O}$, the discriminant $\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}$ of B over A is the ideal of A generated by $4d$, if $d \not\equiv 1 \bmod 4$, and by d, if $d \equiv 1 \bmod 4$. $\square$

Recall that [30, p. 16], if A is a Dedekind ring and M is an A-module of finite length, $\chi_A(M)$ is the unique ideal of A characterized by the following conditions.

(i) $\chi_A(A/\mathfrak{p}) = \mathfrak{p}$, for every nonzero prime $\mathfrak{p}$ of A.

(ii) χ_A is additive, i.e.

$$\chi_A(M) = \chi_A(M')\chi_A(M''),$$

whenever $0 \to M' \to M \to M'' \to 0$ is an exact sequence of A-modules of finite length.

If M is a B-module of finite length then M is of finite length as an A-module and, as such, $\chi_A(M)$ is an ideal of A.

If M is a B-module and, moreover, G acts on M then we call M, as in Section 3.1, a *Galois B-module* if

$$\sigma \cdot (bm) = \sigma(b)\sigma m,$$

for every $m \in M$, $b \in B$ and $\sigma \in G$, which makes sense since B is stable under the action of G. With the evident definition of morphisms of Galois B-modules, the category of Galois B-modules turns out to be equivalent with the category of $B(G)$-modules, where the ring $B(G)$ is the smallest subring of the ring $\operatorname{End}_A(B)$ of A-linear endomorphisms of B, containing B as well as G. Since the subset G of $\operatorname{End}_A(B)$ is linearly independent over B [33, p. 90], it follows that the ring $B(G)$ is a free B-module generated by the elements of G. Then, if M is a Galois B-module, M is made into a $B(G)$-module by defining

$$\left(\sum_{\sigma\in G} b_\sigma \sigma\right) m = \sum_{\sigma\in G} b_\sigma(\sigma m),$$

where $m \in M$, $b_\sigma \in B$ and $\sigma \in G$. Clearly, this establishes an equivalence from the category of Galois B-modules into the category of $B(G)$-modules. Henceforth, we will use the notions "Galois B-module" and "$B(G)$-module" interchangeably.

If M is a $B(G)$-module and N an A-module then the tensor product

$$M \otimes_A N$$

of M and N as A-modules has the structure of a $B(G)$-module, since M is a $B(G)$-module. The special case $M = B$ will be important to us.

If M and N are $B(G)$-modules then the tensor product

$$M \otimes_B N$$

of M and N as B-modules has an action of G which turns it into a Galois B-module. This G-action is determined by

$$\sigma \cdot m \otimes n = (\sigma m) \otimes (\sigma n).$$

for any $m \in M$, $n \in N$ and $\sigma \in G$. Moreover, $\mathrm{Hom}_B(M, N)$, that is, the B-module of all B-linear mappings from M into N, is a Galois B-module if we define

$$(\sigma \cdot f)(m) = \sigma f(\sigma^{-1} m),$$

for any $m \in M$, $f \in \mathrm{Hom}_B(M, N)$ and $\sigma \in G$.

If M is a $B(G)$-module then G acts on M and M^G is an A-module. Since B is a $B(G)$-module, $B \otimes_A M^G$ is a $B(G)$-module and the canonical mapping

$$B \otimes_A (M^G) \longrightarrow M$$

is $B(G)$-linear. This mapping will be denoted by ι.

Lemma 120. *If M is a finitely generated $B(G)$-module, projective as a B-module then the canonical mapping*

$$\iota\colon B \otimes_A (M^G) \longrightarrow M$$

is injective. Moreover, the cokernel of ι has finite length as a B-module.

Proof. Let V be the L-vector space

$$L \otimes_B M.$$

Since M is B-torsion free, we can consider M as a B-submodule of V. Moreover, since both L and M are $B(G)$-modules, V is a $B(G)$-module and M is a $B(G)$-submodule of V.

Since V is finite-dimensional and [30, p. 151]

$$H^1(G, \mathbf{GL}_m(L)) = 0,$$

where m is the dimension of V, the L-vector space V is G-equivariantly isomorphic to L^m. In particular, identifying V with L^m, the A-module

M^G is contained in K^m. Since B is projective as an A-module, the canonical mapping

$$B \otimes_A M^G \longrightarrow L^m$$

is injective and has as image BM^G which is contained in M. Therefore, ι is injective. Moreover, since $KM^G = K^m$, we have

$$LM^G = L^m.$$

Hence, the cokernel of ι is a finitely generated B-torsion module. This implies that the cokernel of ι is of finite length as a B-module. □

Given a $B(G)$-module M, the cokernel of ι will be denoted by

$$\mathfrak{E}_{\mathfrak{B}/\mathfrak{A}}(M)$$

and will be called the *ramification module* of M. When there is no confusion possible we write just $\mathfrak{E}(M)$ for the ramification module of M. The ramification module of $B(G)$ will be denoted by $\mathfrak{E}$.

Remark 121. Observe that the ramification module of a finitely generated $B(G)$-module M which is B-projective contains only local information. That is, if $\mathfrak{p}$ is a nonzero prime ideal of A then

$$\mathfrak{E}_{\mathfrak{B}_\mathfrak{p}/\mathfrak{A}_\mathfrak{p}}(M_\mathfrak{p}) \cong \mathfrak{E}_{\mathfrak{B}/\mathfrak{A}}(M)_\mathfrak{p},$$

where $A_\mathfrak{p}$ is the localization of A in $\mathfrak{p}$ and, for any A-module M,

$$M_\mathfrak{p} = M \otimes_A A_\mathfrak{p}.$$

Moreover,

$$\mathfrak{E}_{\mathfrak{B}/\mathfrak{A}}(M) \cong \bigoplus_{\mathfrak{p}\in \operatorname{Spec} A} \mathfrak{E}_{\mathfrak{B}/\mathfrak{A}}(M)_\mathfrak{p},$$

since $\mathfrak{E}_{\mathfrak{B}/\mathfrak{A}}(M)$ is of finite length. □

Example 122. If the degree of the extension L/K is 2 and $\mathfrak{p}$ is a nonzero prime of A which is ramified in B then the unique prime ideal $\mathfrak{P}$ of B lying above $\mathfrak{p}$ (Example 118) is stable under the action of G. Hence, $\mathfrak{P}$ is a $B(G)$-submodule of B and

$$\mathfrak{P}^G = \mathfrak{p}.$$

Therefore,

$$\mathfrak{E}(\mathfrak{P}) \cong_B B/\mathfrak{P}.$$

If $\mathfrak{p}$ is a nonzero prime of A which is split in B then $\mathfrak{p}B = \mathfrak{P}_1\mathfrak{P}_2$, where $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are prime ideals of B. Since the Galois group of L/K acts transitively on $\{\mathfrak{P}_1, \mathfrak{P}_2\}$ [30, p. 20], neither $\mathfrak{P}_1$ nor $\mathfrak{P}_2$ are a $B(G)$-submodule of B. If $\mathfrak{p}$ is inert then $\mathfrak{P} = \mathfrak{p}B$ is a prime ideal of B and hence $\mathfrak{P}$ is G-stable. Clearly,

$$\mathfrak{E}(\mathfrak{P}) = 0.$$

If $\mathfrak{b} \subseteq L$ is a fractional ideal of B and G-stable then we can compute $\mathfrak{E}(\mathfrak{b})$ using the computations above. Let

$$\mathfrak{b} = \prod_{\mathfrak{P}} \mathfrak{P}^{\mathrm{ord}_{\mathfrak{P}}\mathfrak{b}}$$

be the unique prime factorization of $\mathfrak{b}$ [30, p. 12]. Then, since $\mathfrak{b}$ is G-stable

$$\mathrm{ord}_{\sigma\mathfrak{P}}\mathfrak{b} = \mathrm{ord}_{\mathfrak{P}}\mathfrak{b},$$

for every automorphism σ of L/K. Therefore,

$$\mathfrak{b} = \mathfrak{a} \prod_{\mathfrak{P}|\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}} \mathfrak{P}^{\mathrm{ord}_{\mathfrak{P}}\mathfrak{b}},$$

for some fractional ideal $\mathfrak{a}$ of A. Hence, by Remark 121

$$\mathfrak{E}(\mathfrak{b}) \cong_B \bigoplus_{\mathfrak{P}|\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}} (B/\mathfrak{P})^{\varepsilon_{\mathfrak{P}}},$$

where $\varepsilon_{\mathfrak{P}}$ is 0 or 1 according to $\mathrm{ord}_{\mathfrak{P}}\mathfrak{b}$ being even or odd (resp.). □

By Lemma 120, we have a short exact sequence

$$0 \longrightarrow B \otimes_A M^G \xrightarrow{\iota} M \longrightarrow \mathfrak{E}(M) \longrightarrow 0,$$

whenever M is a finitely generated $B(G)$-module which is B-projective. Clearly, this sequence depends in a functorial way on M. That is, if M and N are finitely generated $B(G)$-modules which are B-projective then, for every $B(G)$-linear mapping $f\colon M \to N$, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B \otimes_A M^G & \longrightarrow & M & \longrightarrow & \mathfrak{E}(M) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B \otimes_A N^G & \longrightarrow & N & \longrightarrow & \mathfrak{E}(N) & \longrightarrow & 0. \end{array}$$

In particular, if M and N are isomorphic then M^G and N^G are isomorphic as A-modules and $\mathfrak{E}(M)$ and $\mathfrak{E}(N)$ are isomorphic as $B(G)$-modules. In the case that the extension degree is 2 we will prove the converse below, under certain conditions. First we have to study ramification modules more thoroughly.

Define the element of $B(G)$

$$\mathrm{tr} = \sum_{\sigma \in G} \sigma.$$

Lemma 123. *If the degree of the extension L/K is n then*

$$\chi_A(\mathfrak{E})^2 = (\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}})^n.$$

In particular, the support of $\mathfrak{E}$ as a B-module is equal to the set of primes of B which are lying over ramified primes of A.

Proof. By Remark 121 we may assume that B is a free A-module. Clearly, the set G is a B-basis for $B(G)$. If $\{b_1, \ldots, b_n\}$ is an A-basis for B then

$$\{\mathrm{tr}\, b_1, \ldots, \mathrm{tr}\, b_n\}$$

is a B-basis for $B \otimes_A B(G)^G$, since

$$B(G)^G = \{\mathrm{tr}\, b \mid b \in B\}.$$

Hence, the ramification module of $B(G)$ is, as a B-module, isomorphic to the cokernel of the B-linear mapping $F\colon B(G) \to B(G)$ given by the matrix $(\sigma(b_i))$ with respect to the basis G for $B(G)$. Since A is Dedekind, $\chi_A(\mathfrak{E})$ is generated by the determinant of F as an A-linear mapping [30, p. 48]. However, this determinant is equal to

$$\mathrm{N}_{L/K}(\det F),$$

where $\mathrm{N}_{L/K}$ is the norm with respect to the field extension L/K. Since $(\det F)^2 = \mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}$, it follows that

$$\chi_A(\mathfrak{E})^2 = (\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}})^n.$$

This proves the lemma. □

Corollary 124. *If M is a $B(G)$-module then the support of $\mathfrak{E}(M)$ as a B-module is contained in the set of primes of B which are lying above ramified primes of A. In particular, the support of $\mathfrak{E}(M)$ is finite.*

Proof. There exists a surjective $B(G)$-linear mapping

$$F \longrightarrow M,$$

where F is a free $B(G)$-module. Then, the induced mapping

$$\mathfrak{E}(F) \longrightarrow \mathfrak{E}(M)$$

is surjective. As $\mathfrak{E}(F)$ is the direct sum of $\mathfrak{E}$, the statement follows from Lemma 123. □

If M is a finitely generated $B(G)$-module which is projective as a B-module then $B \otimes_A M^G$ is the biggest $B(G)$-submodule of M with trivial ramification module. We can also construct a smallest $B(G)$-module N containing M such that the ramification module of N is trivial. This construction goes as follows.

Let M be a finitely generated $B(G)$-module which is B-projective and let us denote the ring of A-linear endomorphisms of B by C, i.e.

$$C = \mathrm{End}_A(B).$$

Since M is B-torsion free, we may consider M as a $B(G)$-submodule of $V = L \otimes_B M$. Since

$$L \otimes_B C = L \otimes_B B(G),$$

there is a unique structure of a C-module on V extending the $B(G)$-module-structure. In particular, CM is a $B(G)$-module containing M.

Lemma 125. *The module CM is the smallest $B(G)$-submodule N of V containing M such that*

$$\mathfrak{E}(N) = 0.$$

Proof. Since $H^1(G, \mathbf{GL}_m(L)) = 0$, we may assume that $V = L^m$. Observe that, if $N \subseteq V$ is a $B(G)$-module containing M such that the ramification module of N is trivial, then

$$CM \subseteq N.$$

This will follow from the fact that $CN \subseteq N$. To prove this, it suffices to show that $CN^G \subseteq N$, since $BN^G = N$. If $x \in N^G$ and $c \in C$ then there exists $x_i \in K$ such that

$$x = (x_1, \ldots, x_m).$$

Then

$$\begin{aligned} cx &= (cx_1, \ldots, cx_m) \\ &= (c(x_1 \cdot 1), \ldots, c(x_n \cdot 1)) \\ &= (x_1 \cdot c(1), \ldots, x_n \cdot c(1)) \\ &= c(1)x. \end{aligned}$$

Therefore, $cx \in N$. This proves that $CM \subseteq N$.

On the other hand, $N = CM$ itself has a trivial ramification module. This follows from the fact that

$$C^G N = N^G \quad \text{and} \quad BC^G = C.$$

Indeed, the first statement is a direct consequence of the existence of an element c of C such that $c(1) = 1$, while the second statement is trivial. □

Remark 126. In general it is not true that CM is isomorphic as a C-module to

$$C \otimes_{B(G)} M.$$

The latter may have B-torsion, while CM is B-torsion free. □

Since $C/B(G)$ is of finite length as a B-module, the $B(G)$-module

$$\mathfrak{F}_{\mathfrak{B}/\mathfrak{A}}(M) = CM/M$$

is of finite length as a B-module, whenever M is a finitely generated $B(G)$-module which is B-projective. When no confusion is likely to occur we denote this $B(G)$-module by $\mathfrak{F}(M)$. We will call this $B(G)$-module the *dual ramification module* of M. If $M = B(G)$ then we define

$$\mathfrak{F} = \mathfrak{F}(M).$$

Clearly, one has a short exact sequence

$$0 \longrightarrow \mathfrak{E}(M) \longrightarrow CM/B \otimes_A M^G \longrightarrow \mathfrak{F}(M) \longrightarrow 0 \tag{3.2}$$

of $B(G)$-modules which are of finite length as B-modules.

If M is a $B(G)$-module, let us denote the $B(G)$-module

$$\mathrm{Hom}_B(M, B)$$

by $M^\star$. If M is a $B(G)$-module which is projective as a B-module then

$$(M^\star)^\star \cong M,$$

canonically. Moreover, if N is a $B(G)$-submodule of M such that M/N is of finite length as a B-module then $N^\star$ is a $B(G)$-submodule of $L \otimes_B M^\star$ containing $M^\star$.

Lemma 127. *If M is a $B(G)$-module which is projective as a B-module then*

$$(B \otimes_A M^G)^\star = C(M^\star) \quad \text{and} \quad (CM)^\star = B \otimes_A (M^\star)^G.$$

Moreover, $\mathfrak{E}(M)$ and $\mathfrak{F}(M)$ are isomorphic as B-modules.

Proof. Observe that, if N is a $B(G)$-module, finitely generated and B-projective, which has trivial ramification module, the $B(G)$-module $N^\star$ has trivial ramification module. Hence, since $(N^\star)^\star$ and N are canonically isomorphic as $B(G)$-modules, whenever N is B-projective, the assignment

$$N \longmapsto N^\star$$

is a bijection from the set of $B(G)$-submodules of M having trivial ramification module onto the set of $B(G)$-submodules of $L \otimes_B (M^\star)$ containing M and having trivial ramification module. In particular, since $B \otimes_A M^G$ is the biggest $B(G)$-submodule of M having trivial ramification module and, by Lemma 125, CM is the smallest $B(G)$-module containing M with trivial ramification module,

$$(B \otimes_A M^G)^\star = C(M^\star) \quad \text{and} \quad (CM)^\star = B \otimes_A (M^\star)^G.$$

To prove the last assertion, recall that we have an exact sequence

$$0 \longrightarrow B \otimes_A M^G \longrightarrow M \longrightarrow \mathfrak{E}(M) \longrightarrow 0.$$

Since M is projective as a B-module we have an exact sequence of B-modules

$$0 \longrightarrow M^\star \longrightarrow (B \otimes_A M^G)^\star \longrightarrow \operatorname{Ext}^1_B(\mathfrak{E}(M), B) \longrightarrow 0,$$

by definition of Ext^1_B (cf. [9, p. 107]). Hence, by what we have seen above,

$$\operatorname{Ext}^1_B(\mathfrak{E}(M), B) \cong \mathfrak{F}(M)$$

as B-modules. Since $\mathfrak{E}(M)$ is of finite length as a B-module, one easily verifies that

$$\operatorname{Ext}^1_B(\mathfrak{E}(M), B) \cong \mathfrak{E}(M),$$

as B-modules. This finishes the proof of the lemma. □

Let us turn our attention to the case that the extension degree of L/K is 2.

Lemma 128. *Suppose L/K is an extension of degree 2. If M is a $B(G)$-module then the nontrivial element σ of G acts on the ramification module $\mathfrak{E}(M)$ of M as multiplication by -1. Moreover, if M is B-projective then the canonical mapping*

$$\mu_M\colon (CM)^G/M^G \longrightarrow \mathfrak{F}(M)$$

is an isomorphism of A-modules. In particular, the nontrivial element σ of G acts on the dual ramification module $\mathfrak{F}(M)$ of M as multiplication by 1.

Proof. Reasoning as in the proof of Corollary 124, we may assume $M = B(G)$ for the first part of the lemma. Let φ be the B-linear mapping from $B(G)$ into B defined by

$$\varphi(b + b'\sigma) = b - b'.$$

Then, if we define a G-action on B by

$$\sigma \cdot b = -\sigma(b)$$

and if we denote the resulting $B(G)$-module by B', the mapping φ is in fact $B(G)$-linear. Thus

$$\mathfrak{E} \cong B'/\mathfrak{b},$$

where $\mathfrak{b}$ is the ideal of the ring B' generated by

$$\{b - \sigma(b) \mid b \in B\}.$$

Clearly, σ acts as multiplication by -1 on $B'/\mathfrak{b}$. This proves the first part of the lemma.

To prove the second part, observe that the canonical mapping μ_M is injective by definition of $\mathfrak{F}(M)$. Let N be the A-module

$$(CM)^G/M^G.$$

Then, by the exact sequence (3.2) and Lemma 127,

$$\chi_B(\mathfrak{F}(M))^2 = \chi_B(B \otimes_A N) = \chi_A(N)B.$$

Hence,

$$\chi_A(\mathfrak{F}(M)) = \chi_A(N).$$

Therefore, the mapping μ_M is an isomorphism of A-modules. □

As a consequence of Lemma 128, the A-module

$$(CM)^G/M^G$$

has a canonical structure of a B-module, if M is a B-projective $B(G)$-module. Moreover if N is also a B-projective $B(G)$-module and

$$\varphi\colon M \longrightarrow N$$

is an isomorphism then the A-linear mapping

$$(C\varphi)^G\colon (CM)^G \longrightarrow (CN)^G$$

induces a B-linear isomorphism from $(CM)^G/M^G$ onto $(CN)^G/N^G$. The converse is proven in the following lemma.

Lemma 129. *Suppose the degree of the extension L/K is 2. Let M and N be finitely generated B-projective $B(G)$-modules. If there exists an A-linear isomorphism ψ from $(CM)^G$ onto $(CN)^G$ such that ψ maps M^G into N^G and the induced mapping*

$$\overline{\psi}\colon (CM)^G/M^G \longrightarrow (CN)^G/N^G$$

is a B-linear isomorphism then there exists a $B(G)$-linear isomorphism

$$\varphi\colon M \longrightarrow N$$

such that $(C\varphi)^G = \psi$.

Proof. It suffices to prove that, given an A-linear mapping ψ from $(CM)^G$ into $(CN)^G$ such that ψ maps M^G into N^G and the induced mapping

$$\overline{\psi}\colon (CM)^G/M^G \longrightarrow (CN)^G/N^G$$

is B-linear, there exists a unique $B(G)$-linear mapping φ from M into N such that

$$(C\varphi)^G = \psi.$$

By assumption, the diagram

$$\begin{array}{ccc} CM/B \otimes_A M^G & \longrightarrow & \mathfrak{F}(M) \\ \big\downarrow{\scriptstyle B \otimes \overline{\psi}} & & \big\downarrow{\scriptstyle \mathfrak{F}(\overline{\psi})} \\ CN/B \otimes_A N^G & \longrightarrow & \mathfrak{F}(N) \end{array}$$

commutes, where we have identified $CM/B \otimes_A M^G$ with

$$B \otimes_A ((CM)^G/M^G)$$

for every B-projective $B(G)$-module M. Consequently, $B\otimes\overline{\psi}$ maps the ramification module of M, considered as a submodule of $CM/B\otimes_A M^G$, into the ramification module of N. Hence, $B\otimes\psi$, considered as a $B(G)$-linear mapping from $L\otimes_A M$ into $L\otimes_A N$ maps M into N. The restriction φ of $B\otimes\psi$ to M is therefore the desired $B(G)$-linear mapping. Since uniqueness of φ is trivial, the proof is finished. □

We are now ready to prove our first classification theorem. Using notation introduced earlier in this section, we have the following.

Theorem 130. *Suppose the degree of the extension L/K is 2. Let M and N be finitely generated B-projective $B(G)$-modules such that both ramification modules $\mathfrak{E}(M)$ and $\mathfrak{E}(N)$ are semi-simple as B-modules. Then*

$$M\cong_{B(G)}N \quad\Longleftrightarrow\quad \bigl(M^G\cong_A N^G \quad\text{and}\quad \mathfrak{E}(M)\cong_B\mathfrak{E}(N)\bigr)\,.$$

Proof. It suffices to prove that M and N are isomorphic, whenever M^G and N^G are isomorphic and $\mathfrak{E}(M)$ and $\mathfrak{E}(N)$ are isomorphic.

If M is a finitely generated B-projective $B(G)$-module then, by Lemma 128

$$\mu_M\colon (CM)^G/M^G\longrightarrow\mathfrak{F}(M),$$

is an A-linear isomorphism. Moreover, by Lemma 127, $\mathfrak{F}(M)$ and $\mathfrak{E}(M)$ are isomorphic as B-modules. Therefore, $(CM)^G/M^G$ is semi-simple and, by Corollary 124, its support consists of primes of B which are lying over ramified primes of A. In particular, the radical ideal

$$\mathfrak{b}=\mathfrak{r}\left(\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}\mathfrak{B}\right)$$

of $\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}B$ is contained in the annihilator of the B-module $(CM)^G/M^G$. Hence, $(CM)^G/M^G$ is a $B/\mathfrak{b}$-module. Since the canonical mapping

$$A\longrightarrow B/\mathfrak{b}$$

is surjective, it follows that every A-linear mapping

$$\overline{\psi}\colon (CM)^G/M^G\longrightarrow (CN)^G/N^G$$

is B-linear, whenever M and N are finitely generated B-projective $B(G)$-modules with $\mathfrak{E}(M)$ and $\mathfrak{E}(N)$ are B-semi-simple.

Now we are ready to prove the theorem. Let M and N be finitely generated B-projective $B(G)$-modules such that M^G and N^G are isomorphic and $\mathfrak{E}(M)$ and $\mathfrak{E}(N)$ are isomorphic. In particular,

$$(CM)^G/M^G \cong (CN)^G/N^G,$$

as A-modules. Hence, it follows from well known properties of projective modules over Dedekind rings (see [8, Proposition 16, p. 531] and [8, Proposition 24, p. 544]) that $(CM)^G$ and $(CN)^G$ are isomorphic. Then, by Lemma 132 below, there exists an isomorphism

$$\psi\colon (CM)^G \longrightarrow (CN)^G$$

which maps M^G onto N^G. We have seen above that the induced mapping $\overline{\psi}$ is B-linear. Hence, M and N are isomorphic as $B(G)$-modules by Lemma 129. □

Remark 131. If $[L : K] = 2$ and B is *tamely ramified* over A, that is,

$$\mathrm{ord}_{\mathfrak{p}} \mathfrak{d}_{\mathfrak{B}/\mathfrak{A}} \leq 1,$$

for every nonzero prime $\mathfrak{p}$ of A, then every B-projective $B(G)$-module M has a B-semi-simple ramification module $\mathfrak{E}(M)$. For, let

$$F \longrightarrow M$$

be a surjective $B(G)$-linear mapping, with F a free $B(G)$-module. Then

$$\mathfrak{E}(F) \longrightarrow \mathfrak{E}(M)$$

is surjective. Since $\mathfrak{E}(F)$ is isomorphic to the direct sum of a number of copies of $\mathfrak{E}$, the B-module $\mathfrak{E}(F)$ and hence the B-module $\mathfrak{E}(M)$ is semi-simple by Lemma 123.

If B is not tamely ramified over A then $\mathfrak{E}$ itself is not semi-simple as a B-module. One can check that

$$\mathfrak{E} \cong_B B/\mathfrak{D}_{B/A},$$

where $\mathfrak{D}_{B/A}$ is the *different* of B/A [30, p. 50]. □

Lemma 132. *Let A be a Dedekind ring and M and N isomorphic finitely generated projective A-modules. Suppose $M' \subseteq M$ and $N' \subseteq N$ are submodules such that M/M' and N/N' are isomorphic A-modules of finite length. Then there exists an isomorphism ψ from M into N such that*

$$\psi(M') = N'.$$

Proof. Of course, we may assume $N = M$. Let $\mathfrak{a} \subseteq A$ be a nonzero ideal such that

$$\mathfrak{a}M \subseteq M' \quad \text{and} \quad \mathfrak{a}M \subseteq N'.$$

Since M/M' and M/N' are isomorphic, there exists an $A/\mathfrak{a}$-linear automorphism $\overline{\psi}$ of $M/\mathfrak{a}M$ such that

$$\overline{\psi}(M'/\mathfrak{a}M) \subseteq N'/\mathfrak{a}M.$$

Moreover, $M/\mathfrak{a}M$ is a free $A/\mathfrak{a}$-module and we may assume that the determinant of $\overline{\psi}$ is equal to 1. By Lemma 133, there exists an A-linear automorphism ψ of M which induces $\overline{\psi}$. Clearly, ψ maps M' onto N'. □

Let us introduce the following notation. If A is a ring and M is a finitely generated projective A-module then

$$\mathbf{SL}(M) = \{\psi \in \mathrm{End}_A(M) \mid \det \psi = 1\}.$$

Furthermore, for a prime ideal $\mathfrak{p}$ of A, let us denote the completion of the local ring $A_\mathfrak{p}$ by $\widehat{A_\mathfrak{p}}$. The topological ring

$$\prod_{\mathfrak{p}\neq 0} \widehat{A_\mathfrak{p}}$$

is denoted by $\mathcal{A}_0$. If A is a Dedekind ring and K its function field then $\widehat{K_\mathfrak{p}}$ will denote the completion of K at $\mathfrak{p}$ and the subring of

$$\prod_{\mathfrak{p}\neq 0} \widehat{K_\mathfrak{p}}$$

consisting of $(x_\mathfrak{p})$ such that

$$x_\mathfrak{p} \in \widehat{A_\mathfrak{p}}$$

except for a finite number of prime ideals $\mathfrak{p}$ will be denoted by $\mathcal{A}$. This ring turns into a topological ring by taking as a fundamental system of neighbourhoods of 0 in $\mathcal{A}$ the system of neighbourhoods of 0 in $\mathcal{A}_0$. The topological ring $\mathcal{A}$ is called the *ring of restricted adèles* [8, p. 497].

Lemma 133. *If M is a finitely generated projective module over the Dedekind ring A and $\mathfrak{a}$ is a nonzero ideal of A then the canonical mapping*

$$\mathbf{SL}(M) \longrightarrow \mathbf{SL}(M/\mathfrak{a}M)$$

is surjective.

Proof. Suppose $\overline{\psi}$ is an element of $\mathbf{SL}(M/\mathfrak{a}M)$. Since $\widehat{A_\mathfrak{p}}$ is a discrete valuation ring,

$$\widehat{M_\mathfrak{p}} = M \otimes_A \widehat{A_\mathfrak{p}}$$

is a free $\widehat{A_\mathfrak{p}}$-module of finite rank. Hence, there exists, for any nonzero prime ideal $\mathfrak{p}$ of A

$$\psi_\mathfrak{p} \in \mathbf{SL}(\widehat{M_\mathfrak{p}})$$

such that the mapping

$$\widehat{M_\mathfrak{p}}/\mathfrak{a}\widehat{A_\mathfrak{p}}\widehat{M_\mathfrak{p}} \longrightarrow \widehat{M_\mathfrak{p}}/\mathfrak{a}\widehat{A_\mathfrak{p}}\widehat{M_\mathfrak{p}}$$

induced by $\psi_\mathfrak{p}$ is equal to $\overline{\psi} \otimes \widehat{A_\mathfrak{p}}$, when we identify $(M/\mathfrak{a}M) \otimes_A \widehat{A_\mathfrak{p}}$ with $\widehat{M_\mathfrak{p}}/\mathfrak{a}\widehat{A_\mathfrak{p}}\widehat{M_\mathfrak{p}}$.

We have the following commutative diagram

$$\begin{array}{ccc}
\mathbf{SL}(M) & \longrightarrow & \mathbf{SL}(M \otimes_A K) \\
\downarrow & & \downarrow \\
\mathbf{SL}(M \otimes_A \mathcal{A}_0) & \longrightarrow & \mathbf{SL}(M \otimes_A \mathcal{A})
\end{array}$$

where all arrows are injective and, moreover,

$$\mathbf{SL}(M) = \mathbf{SL}(M \otimes_A \mathcal{A}_0) \cap \mathbf{SL}(M \otimes_A K).$$

Since $\mathbf{SL}(M \otimes_A K)$ is dense in $\mathbf{SL}(M \otimes_A \mathcal{A})$ (cf. [8, Proposition 4, p. 498]) and $\mathbf{SL}(M \otimes_A \mathcal{A}_0)$ is an open subgroup of $\mathbf{SL}(M \otimes_A \mathcal{A})$, the group $\mathbf{SL}(M)$ is dense in $\mathbf{SL}(M \otimes_A \mathcal{A}_0)$. Therefore, there exists an element ψ of $\mathbf{SL}(M)$ such that

$$\psi \otimes_A \widehat{A_\mathfrak{p}} \equiv \psi_\mathfrak{p} \bmod (\mathfrak{p}\widehat{A_\mathfrak{p}})^{n_\mathfrak{p}},$$

for every nonzero prime ideal $\mathfrak{p}$ of A, where $n_\mathfrak{p}$ is the unique integer such that

$$\mathfrak{a} = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{n_\mathfrak{p}}.$$

Hence, the mapping from $M/\mathfrak{a}$ into itself induced by ψ is equal to $\overline{\psi}$. This proves surjectivity. □

Our second classification theorem, which we are now going to state and prove, is a corollary of Theorem 130.

Theorem 134. *Suppose the degree of the extension L/K is 2. If B is tamely ramified over A then, for all finitely generated projective B-modules M and N,*

$$B(G) \otimes_B M \cong_{B(G)} B(G) \otimes_B N \iff M \cong_A N.$$

Proof. By Remark 131, every ramification module with respect to B/A is semi-simple as a B-module.

Since the ramification module can be computed locally (cf. Remark 121) and since a projective module is locally free, we see that, for any finitely generated projective B-modules M and N,

$$\mathfrak{E}(B(G) \otimes_B M) \cong_B \mathfrak{E}(B(G) \otimes_B N)$$

if and only if M and N have the same rank over B. Moreover,

$$(B(G) \otimes_B M)^G \cong_A M.$$

Therefore, the theorem follows from Theorem 130. □

3.3 Real abelian varieties with complex multiplication

Definition 135. *A real abelian variety X is said to* admit sufficiently many complex multiplications *if the complexification $\mathcal{C}(X)$ of X admits sufficiently many complex multiplications. If the dimension of X is 1 then this is abbreviated to "X* admits complex multiplication*".*

If X is an abelian variety over $\mathbb{C}$ with sufficiently many complex multiplications then the underlying real algebraic structure ${}_{\mathbb{R}}X$ of X is a real abelian variety admitting sufficiently many complex multiplications, by Proposition 117.

The following theorem is a partial generalization of Theorem 98.

Theorem 136. *Let L be a CM-field and $B \subseteq L$ the ring of integers, such that B is tamely ramified over A, where $A = B \cap K$ and K is the maximal totally real subfield of L. Let M and N be finitely generated projective B-modules and let Φ be a $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Z}} B$ such that $X(B, \Phi)$ is simple. Let*

$$X = X(M, \Phi) \quad \text{and} \quad Y = X(N, \Phi)$$

be the associated abelian varieties over $\mathbb{C}$. Then,

$${}_{\mathbb{R}}X \cong {}_{\mathbb{R}}Y \iff M \cong_A N.$$

Proof. From Proposition 117 it follows that

$$\mathcal{N}(X) \cong X_{\mathbb{R}}(B(G) \otimes_B M, \Phi).$$

Therefore, the conclusion follows from Proposition 116 and Theorem 134. □

Observe that, by Corollary 82, the result still holds if we read "${}_{\mathbb{R}}X \cong {}_{\mathbb{R}}Y$ as real algebraic varieties" instead of "${}_{\mathbb{R}}X \cong {}_{\mathbb{R}}Y$".

As a consequence of Theorem 136 we are able determine the number $\rho({}_{\mathbb{R}}X)$ of (isomorphism classes of) algebraic varieties Y over $\mathbb{C}$ such that

$${}_{\mathbb{R}}Y \cong {}_{\mathbb{R}}X,$$

where X is the abelian variety $X(M, \Phi)$ associated to the finitely generated projective B-module M under the conditions of Theorem 136.

For this, let

$$\eta\colon \mathrm{Cl}\, B \longrightarrow \mathrm{Cl}\, A$$

be induced by the *norm mapping* $\mathrm{N}_{L/K}$ which assigns to any fractional ideal $\mathfrak{b}$ of B the fractional

$$\mathrm{N}_{L/K}(\mathfrak{b}) = \mathfrak{b}\sigma(\mathfrak{b}).$$

Then η is a morphism from the class group of B into the class group of A. Since the *class number* $h(B)$, i.e. $h(B) = \#\mathrm{Cl}\, B$, is finite [18, Chapter V], the kernel $\ker \eta$ of η is finite.

Theorem 137. *The number of (isomorphism classes of) algebraic varieties Y over $\mathbb{C}$ such that ${}_{\mathbb{R}}Y \cong {}_{\mathbb{R}}X$ is equal to the order of* $\ker \eta$*, i.e.*

$$\rho({}_{\mathbb{R}}X) = \# \ker \eta.$$

In particular, $\rho({}_{\mathbb{R}}X)$ is finite.

For the proof we will need the following lemma.

Lemma 138. *Let X be an abelian variety over $\mathbb{C}$. If Y is an algebraic variety over $\mathbb{C}$ such that*

$${}_{\mathbb{R}}Y \cong {}_{\mathbb{R}}X$$

then Y is isomorphic to an abelian variety over $\mathbb{C}$.

Proof. It is clear that Y is a nonsingular irreducible complete algebraic variety over $\mathbb{C}$. Let

$$g\colon Y \dashrightarrow A$$

be its *Albanese variety* [17, p. 41]. Then

$$\mathcal{N}(g)\colon \mathcal{N}(Y) \dashrightarrow \mathcal{N}(A)$$

is the Albanese variety of the algebraic variety $\mathcal{N}(Y)$ over $\mathbb{R}$. Actually, by Theorem 42, both g and $\mathcal{N}(g)$ are morphisms.

Since the underlying real algebraic structure ${}_{\mathbb{R}}Y$ of Y is isomorphic to the underlying real algebraic structure ${}_{\mathbb{R}}X$ of X, there exists, by Theorem 42 a birational morphism

$$f\colon \mathcal{N}(Y) \longrightarrow \mathcal{N}(X),$$

with the property that $\mathcal{R}(f)$ is an isomorphism from $\mathcal{R}(\mathcal{N}(Y))$ onto $\mathcal{R}(\mathcal{N}(X))$. Since f is birational and $\mathcal{N}(X)$ is an abelian variety over $\mathbb{R}$, this is also an Albanese variety of $\mathcal{N}(Y)$. Hence there exists, changing f by a translation if necessary, an isomorphism h from $\mathcal{N}(A)$ onto $\mathcal{N}(X)$ such that

$$\begin{array}{ccc} \mathcal{N}(Y) & \xrightarrow{\mathcal{N}(g)} & \mathcal{N}(A) \\ & \searrow^{f} & \downarrow h \\ & & \mathcal{N}(X) \end{array}$$

commutes. It follows that

$$g\colon Y \longrightarrow A$$

is a birational morphism with the property that ${}_{\mathbb{R}}g$ is an isomorphism of real algebraic varieties. Obviously, this implies that g is an isomorphism. This proves the lemma. □

Proof of Theorem 137. Suppose Y is an algebraic variety over $\mathbb{C}$ such that the underlying real algebraic structure ${}_{\mathbb{R}}Y$ of Y is isomorphic to ${}_{\mathbb{R}}X$. By Lemma 138, we may assume that Y is an abelian variety over $\mathbb{C}$. It follows that $\mathcal{N}(Y)$ and $\mathcal{N}(X)$ are isomorphic as abelian variety over $\mathbb{R}$. In particular,

$$\mathrm{Center}(\mathrm{End}(Y \times \overline{Y})) \cong \mathrm{Center}(\mathrm{End}(X \times \overline{X})) = B.$$

Therefore, there exists a finitely generated projective B-module N such that

$$X(N, \Phi) \cong Y.$$

Hence, by Theorem 136, N is isomorphic to M as an A-module.

Conversely, every finitely generated projective B-module N which is isomorphic to M as an A-module gives rise to an abelian variety $Y = X(N, \Phi)$ such that

$$_{\mathbb{R}}Y \cong {}_{\mathbb{R}}X,$$

by Theorem 136.

It follows from Proposition 116 that the number $\rho({}_{\mathbb{R}}X)$ of (isomorphism classes of) algebraic varieties Y over $\mathbb{C}$ such that $_{\mathbb{R}}Y$ is isomorphic to $_{\mathbb{R}}X$ is equal to the number of (B-isomorphism classes of) projective B-modules N such that N is isomorphic as an A-module to M. The latter number is equal to $\#\ker\eta$ (this follows from [8, Proposition 24, p. 544]). This finishes the proof of the theorem. $\square$

Example 139. Let K be a totally real field such that $h(A) = 1$, where A the ring of integers of K. Let L be a totally imaginary degree 2 extension of K such that B is tamely ramified over A, where B is the ring of integers of L. Let Φ be a $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Z}} B$ such that $X = X(B, \Phi)$ is simple. Then

$$\rho({}_{\mathbb{R}}X) = h(B).$$

In the special case $K = \mathbb{Q}$, this was proved in [14, Corollary 1.4]. $\square$

We also have a partial generalization of Corollary 100.

Theorem 140. *Let X be a simple abelian variety over $\mathbb{C}$ with sufficiently many complex multiplications such that its ring B of endomorphisms is the ring of integers of the field $L = \operatorname{End}^{\circ} X$. Let $A = B \cap K$, where K is the maximal totally real subfield of L. Then the underlying real algebraic structure $_{\mathbb{R}}X$ of X is isomorphic to the product $X_1 \times X_2$ of two real algebraic varieties X_1 and X_2 of positive dimension if and only if the ring B is tamely ramified over A. Moreover, in that case the number of (isomorphism classes of) ordered pairs (X_1, X_2) such that $X_1 \times X_2$ is isomorphic to $_{\mathbb{R}}X$ is equal to*

$$2^g h(A),$$

where g is the number of nonzero prime ideals of A dividing the discriminant $\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}$ of B over A.

Proof. By Proposition 107, there exist a $\mathbb{C}$-algebra structure Φ on $\mathbb{R}\otimes_{\mathbb{Z}} B$ and a B-module M such that

$$X(M, \Phi) \cong X.$$

In particular, M is B-projective of rank 1.

Suppose B is tamely ramified over A. Then, by Lemma 123, the B-module $\mathfrak{E}$ is semi-simple and

$$\mathfrak{E} \cong_B \bigoplus_{i=1}^{g} B/\mathfrak{P}_{\mathfrak{i}},$$

where $\mathfrak{P}_{\mathfrak{1}}, \ldots, \mathfrak{P}_{\mathfrak{g}}$ are the nonzero prime ideals of B dividing $\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}$. Choose $\varepsilon_i = 0, 1$, for $i = 1, \ldots, g$, and choose a fractional ideal $\mathfrak{a}$ of A. Let

$$M_1 = \mathfrak{a} \prod_{\mathfrak{i}=\mathfrak{1}}^{\mathfrak{g}} \mathfrak{P}_{\mathfrak{i}}^{\varepsilon_{\mathfrak{i}}} \quad \text{and} \quad \mathfrak{M}_{\mathfrak{2}} = \mathfrak{a}' \prod_{\mathfrak{i}=\mathfrak{1}}^{\mathfrak{g}} \mathfrak{P}_{\mathfrak{i}}^{\mathfrak{1}-\varepsilon_{\mathfrak{i}}},$$

where $\mathfrak{a}'$ is a fractional ideal of A such that

$$\mathfrak{a}\mathfrak{a}'\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}} \cong_{\mathfrak{A}} \wedge^{\mathfrak{2}}_{\mathfrak{A}}\mathfrak{M}.$$

Observe that we get in this way $2^g h(A)$ different (isomorphism classes of) ordered pairs (M_1, M_2) of $B(G)$-modules. Then M_1 and M_2 are $B(G)$-submodules of L and, by Example 122,

$$\mathfrak{E}(M_1) \cong_B \bigoplus_{i=1}^{g} B/\mathfrak{P}_{\mathfrak{i}}^{\varepsilon_{\mathfrak{i}}} \quad \text{and} \quad \mathfrak{E}(\mathfrak{M}_{\mathfrak{2}}) \cong_{\mathfrak{B}} \bigoplus_{\mathfrak{i}=\mathfrak{1}}^{\mathfrak{g}} \mathfrak{B}/\mathfrak{P}_{\mathfrak{i}}^{\mathfrak{1}-\varepsilon_{\mathfrak{i}}}.$$

Hence,

$$\mathfrak{E}(M_1 \oplus M_2) \cong_B \mathfrak{E}(M) \quad \text{and} \quad (M_1 \oplus M_2)^G \cong_A M \cong_A (B(G) \otimes_B M)^G.$$

Therefore, by Theorem 130,

$$M_1 \oplus M_2 \cong_{B(G)} M.$$

This implies, with use of Proposition 116,

$$X_1 \times X_2 \cong_{\mathbb{R}} X,$$

where X_i is the real abelian variety $\mathcal{R}(X_{\mathbb{R}}(M_i, \Phi))$, for $i = 1, 2$.

Conversely, suppose ${}_{\mathbb{R}}X$ is isomorphic to the product $X_1 \times X_2$ of two real algebraic varieties X_1 and X_2. One proves in much the same way as Lemma 138 that both X_1 and X_2 are isomorphic to real abelian varieties. Hence we may assume that X_1 and X_2 are real abelian subvarieties of ${}_{\mathbb{R}}X$. Clearly, there exists B-projective $B(G)$-modules M_1 and M_2, both of rank 1 as B-modules, such that

$$X_{\mathbb{R}}(M_1 \oplus M_2, \Phi) \cong \mathcal{N}(X) \quad \text{and} \quad \mathcal{R}(X_{\mathbb{R}}(M_i, \Phi)) \cong X_i, \text{ for } i = 1, 2.$$

Hence, $M_1 \oplus M_2$ and $B(G) \otimes_B M$ are isomorphic $B(G)$-modules. Since both M_1 and M_2 are of rank 1 as B-modules, their ramification modules are semi-simple by Example 122. Therefore, the ramification module of $B(G) \otimes_B M$ is B-semi-simple and so is $\mathfrak{E}$. This proves that B is tamely ramified over A. Moreover, by Theorem 130 and Example 122, there exist $\varepsilon_i = 0, 1$, for $i = 1, \ldots, g$, and a fractional ideal $\mathfrak{a}$ of A such that

$$M_1 \cong_{B(G)} \mathfrak{a} \prod_{\mathfrak{i}=1}^{\mathfrak{g}} \mathfrak{P}_{\mathfrak{i}}^{\varepsilon_{\mathfrak{i}}}.$$

Then necessarily

$$M_2 \cong_{B(G)} \mathfrak{a}' \prod_{\mathfrak{i}=1}^{\mathfrak{g}} \mathfrak{P}_{\mathfrak{i}}^{1-\varepsilon_{\mathfrak{i}}},$$

where $\mathfrak{a}'$ is a fractional ideal of A such that

$$\mathfrak{a}\mathfrak{a}'\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}} \cong_{\mathfrak{A}} \wedge^2_{\mathfrak{A}} \mathfrak{M}.$$

This proves the theorem. □

Example 141. Let K be a totally real field such that $h(A) = 1$, where A the ring of integers of K. Let L be a totally imaginary degree 2 extension of K such that B is tamely ramified over A, where B is the ring of integers of L. Let Φ be a $\mathbb{C}$-algebra structure on $\mathbb{R} \otimes_{\mathbb{Z}} B$ such that $X = X(B, \Phi)$ is simple. Then the number of (isomorphism classes of) ordered pairs (X_1, X_2) such that $X_1 \times X_2$ is isomorphic to ${}_{\mathbb{R}}X$ is equal to

$$2^g,$$

where g is the number of nonzero prime ideals of A dividing the discriminant $\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}}$ of B over A. In the special case $K = \mathbb{Q}$, this has been proved in [5]. □

Remark 142. It has been proved in [5, Theorem 1.3] that for any elliptic curve E over $\mathbb{C}$ there does not exist a real algebraic variety C such that

$$C^2 \cong {}_{\mathbb{R}}E.$$

Simple abelian varieties over $\mathbb{C}$ of dimension greater than 1 do not have this property, as is shown by the following example.

Let K be a totally real field such that $h(A) = 1$, where A is the ring of integers of K. Suppose L is a totally imaginary degree 2 extension of K such that B/A is unramified, where B is the ring of integers of L. (Such a situation exists, take $K = \mathbb{Q}(\sqrt{3})$ and $L = K(\sqrt{-1})$.) In particular, $\mathfrak{d}_{\mathfrak{B}/\mathfrak{A}} = A$. Let

$$X = X(B, \Phi),$$

for some $\mathbb{C}$-algebra structure Φ on $\mathbb{R} \otimes_{\mathbb{Z}} B$ such that X is simple. Then, according to Theorem 140, there is (up to isomorphism) a unique ordered pair (X_1, X_2) of real algebraic varieties such that

$$X_1 \times X_2 \cong {}_{\mathbb{R}}X.$$

Since $X_2 \times X_1$ is also isomorphic to ${}_{\mathbb{R}}X$, it follows that $X_1 \cong X_2$. Hence, there exists a real algebraic variety Y such that

$$Y^2 \cong {}_{\mathbb{R}}X$$

as real algebraic varieties. □

References

[1] Artin, M.: Théorème de Weil sur la construction d'un groupe à partir d'une loi rationelle. In: *SGA 3, Vol. II.* Lecture Notes in Mathematics, Vol. 152. Springer Verlag, Berlin Heidelberg New York, 1962/64.

[2] Bochnak, J., Coste, M., Roy, M.-F.: *Géométrie algébrique réelle.* Ergeb. Math. Springer Verlag, Berlin Heidelberg New York, 1987.

[3] Bochnak, J., Kucharz, W.: Algebraic models of smooth manifolds. *Invent. Math.* **97**, 585–611 (1989).

[4] Bochnak, J., Buchner, M., Kucharz, W.: Vector bundles over real algebraic varieties. *K-Theory* **3**, 271–298 (1990).

[5] Bochnak, J., Huisman, J.: When is a complex elliptic curve the product of two real algebraic curves? *Math. Ann.* (1992).

[6] Bochnak, J., Kucharz, W.: Real algebraic hypersurfaces in complex projective varieties, preprint 1990.

[7] Borel, A., Serre, J.-P.: Détermination des p-puissances réduites de Steenrod dans la cohomologie des groupes classiques. Applications. *C. R. Acad. Sci. Paris* **233**, 680–682 (1951).

[8] Bourbaki, N.: *Commutative algebra. Chapters 1–7.* 2nd ed. Springer Verlag, Berlin Heidelberg New York, 1989.

[9] Cartan, H., Eilenberg, S.: *Homological algebra.* 7th ed. Princeton Mathematical Series, Vol. 19. Princeton University Press, Princeton, 1973.

[10] Griffiths, P., Harris, J.: *Principles of algebraic geometry.* John Wiley & Sons, New York Chichester Brisbane Toronto, 1978.

[11] Gross, B.H., Harris, J.: Real algebraic curves. *Ann. scient. Éc. Norm. Sup.* **14**, 157–182 (1981).

[12] Grothendieck, A.: Fondements de la géométrie algébrique (extraits du Séminaire Bourbaki 1957-1962).

[13] Hartshorne, R.: *Algebraic geometry.* Springer Verlag, Berlin Heidelberg New York, 1977.

[14] Huisman, J.: The underlying real algebraic structure of complex elliptic curves. *Math. Ann.* (1992).

[15] Kempf, G.R.: *Complex abelian varieties and theta functions.* Springer Verlag, Berlin Heidelberg New York, 1990.

[16] Kunz, E.: *Introduction to commutative algebra and algebraic geometry.* Birkhäuser, Boston-Basel-Stuttgart, 1981.

[17] Lang, S.: *Abelian varieties.* Springer Verlag, Berlin Heidelberg New York, 1983.

[18] Lang, S.: *Algebraic number theory.* Springer Verlag, Berlin Heidelberg New York, 1986.

[19] Mac Lane, S.: *Categories for the working mathematician.* Springer Verlag, Berlin Heidelberg New York, 1971.

[20] Milne, J.S.: On the arithmetic of abelian varieties. *Invent. Math.* **17**, 177–190 (1972).

[21] Milne, J.S.: Abelian varieties. In: Cornell, G., Silverman, J.H. (eds.) *Arithmetic geometry.* Springer Verlag, Berlin Heidelberg New York, 1986, 103–150.

[22] Milnor, J.W., Stasheff, J.D.: *Characteristic classes.* Annals of Mathematics Studies, Vol. 76. Princeton University Press, New Jersey, 1974.

[23] Mumford, D.: *Abelian varieties.* Oxford University Press, London, 1970.

[24] Mumford, D.: *The red book of varieties and schemes.* Springer Verlag, Berlin Heidelberg New York, 1988.

[25] Oort, F.: The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field. *J. Pure Appl. Algebra* **3**, 399–408 (1973).

[26] Šafarevič, I. R.: *Algebraic surfaces.* Amer. Math. Soc., Providence, Rhode Island, 1967.

[27] Serre, J.-P.: Géométrie algébrique et géométrie analytique. *Ann. Inst. Fourier* **6**, 1–42 (1956).

[28] Serre, J.-P.: *Cohomologie galoisienne.* Lect. Notes Math., Vol. 5. Springer Verlag, Berlin Heidelberg New York, 1965.

[29] Serre, J.-P.: Complex multiplication. In: Cassels, J.W., Fröhlich, A. (eds.) *Algebraic number theory.* Academic Press, 1967, 292–296.

[30] Serre, J.-P.: *Local fields.* Springer Verlag, Berlin Heidelberg New York, 1979.

[31] Silhol, R.: *Real algebraic surfaces.* Lect. Notes Math., Vol. 1392. Springer Verlag, Berlin Heidelberg New York, 1989.

[32] Silverman, J. H.: *The arithmetic of elliptic curves.* Springer Verlag, Berlin Heidelberg New York, 1986.

[33] Stewart, I.: *Galois theory.* 2nd ed. Chapman and Hall, London, New York, 1989.

[34] Weil, A.: The field of definition of a variety. *Am. J. of Math.* **78**, 509–524 (1956).

[35] Weil, A.: *Adeles and algebraic groups.* Progress in Mathematics, Vol. 23. Birkhäuser, Boston-Basel-Stuttgart, 1982.

List of symbols

Index

Samenvatting

In dit proefschrift bestuderen we reële abelse variëteiten, waarbij de nadruk ligt op die reële abelse variëteiten die voldoende veel complexe vermenigvuldigingen toelaten. In het bijzonder zijn we geïnteresseerd in

(i) realiseerbaarheid van $\mathbb{Z}/2\mathbb{Z}$-homologieklassen van reële abelse variëteiten door reële algebraïsche deelvariëteiten,
(ii) klassificatie van de onderliggende reële algebraïsche structuur van abelse variëteiten over $\mathbb{C}$ die voldoende veel complexe vermenigvuldigingen hebben, en
(iii) de produktstructuur van simpele abelse variëteiten over $\mathbb{C}$ die voldoende veel complexe vermenigvuldigingen hebben.

We bestuderen (i) in Hoofdstuk 2. Daar wordt, voor een willekeurige reële abelse variëteit V, de groep $H_{d-1}^{alg}(V, \mathbb{Z}/2\mathbb{Z})$ van codimensie-1 $\mathbb{Z}/2\mathbb{Z}$-homologieklassen die realiseerbaar zijn door reële algebraïsche deelvariëteiten bepaald. In het bijzonder bewijzen we in Hoofdstuk 2 dat, zodra V niet samenhangend is met betrekking tot de sterke topologie en de dimensie d van V groter dan 1 is,

$$(0) \neq H_{d-1}^{alg}(V, \mathbb{Z}/2\mathbb{Z}) \neq H_{d-1}(V, \mathbb{Z}/2\mathbb{Z}).$$

In Hoofdstuk 3 bestuderen we (ii) en (iii). We generaliseren in dat hoofdstuk resultaten uit [5] en [14], waar het 1-dimensionale geval bestudeerd is. Zo is in [14] het volgende bewezen. Laat E een elliptische kromme over $\mathbb{C}$ zijn met complexe vermenigvuldiging, dat wil zeggen, de ring $\mathrm{End}(E)$ van endomorfismen van E is ongelijk aan $\mathbb{Z}$. Zij T de onderliggende reële algebraïsche structuur van E. (In het bijzonder geldt dan dat T een reële algebraïsche torus is.) Dan is het aantal (isomorfieklassen van) algebraïsche variëteiten X over $\mathbb{C}$ zodat de onderliggende reële algebraïsche structuur van X isomorf is met T, gelijk aan het klassegetal van de ring End(E). Stelling 137, die we in Paragraaf 3.3 bewijzen, is hier een generalisatie van.

In [5] is bewezen dat de onderliggende reële algebraïsche structuur van een elliptische kromme E over $\mathbb{C}$ isomorf is met het produkt van 2 reële algebraïsche krommen als en slechts als E complexe vermenigvuldiging heeft en de discriminant van de ring End(E) oneven is. Stelling 140 generaliseert deze uitspraak.

Curriculum vitae

De schrijver van dit proefschrift werd geboren op 31 januari 1964 te Hellevoetsluis. Aldaar bezocht hij de Rijksscholengemeenschap en behaalde in 1983 het VWO-diploma. In september 1983 begon hij de studie wiskunde aan de Vrije Universiteit te Amsterdam. Een jaar later slaagde hij voor het propedeutisch examen en in maart 1988 voor het doktoraal examen. Van april 1988 tot april 1992 was hij werkzaam als assistent in opleiding bij de faculteit der Wiskunde en Informatica van de Vrije Universiteit te Amsterdam. In deze periode verrichtte hij, onder leiding van prof. dr. J. Bochnak, het onderzoek dat in dit proefschrift zijn neerslag heeft gevonden. Vanaf 1 september 1992 is hij werkzaam op het Mathematisch Instituut van de Rijksuniversiteit te Utrecht.