LECTURE 1: GENERALITIES ON ENDOMORPHISMS (2/15/12)

NOTES BY I. BOREICO

In this lecture and the two that follow, we will summarize many facts about abelian varieties and their endomorphisms, with an emphasis on making statements over a general ground field (especially of characteristic 0, but we will later need to work over finite fields too). Many facts which we state without proofs will be proved in the lecture(s) by Tripathy that come next.

Our goal in these initial "overview" lectures is to reach precise formulations of several results which can be called the "Main Theorem" of Complex Multiplication, the proofs of which will be the focus of most of the rest of the seminar.

1. Endomorphism algebras

Let K be a field and A an abelian variety over K of dimension $g > 0$. The endomorphism ring $\mathrm{End}(A) := \mathrm{End}_K(A)$ is a finitely generated $\mathbf{Z}$-module. The proof is obtained just like in the case of elliptic curves, by using ℓ-adic Tate modules. The *endomorphism algebra* is $\mathrm{End}^0(A) := \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}(A)$. These are "endomorphisms in the isogeny category" (over K!).

Theorem 1.1 (Poincare reducibility/Complete reducibility)**.** *If $B \hookrightarrow A$ is an abelian subvariety over K then there exists an abelian subvariety $B' \hookrightarrow A$ over K such that the map $B \times B' \to A$ induced by addition is an isogeny.*

An abelian variety over K is called *simple* (or *K-simple* for emphasis) if it has no nontrivial proper abelian subvarieties over K. By using the above theorem in the role of Maschke's theorem for finite group representations in characteristic 0, the same formalism yields:

Corollary 1.2. *The abelian variety A is K-isogenous to a finite product $\prod B_i^{e_i}$ for $e_i \geq 1$, where the B_i are K-simple abelian varieties, pairwise non-isogenous over K. Moreover, the isogeny class of each B_i, and the multiplicities e_i, are uniquely determined.*

The above decomposition is called the "isotypic decomposition" for A over K (with the canonical images $C_i \subset A$ of the $B_i^{e_i}$ (namely, the abelian subvariety spanned by the images of *all* K-homomorphisms $B_i \to A$) are called the *isotypic parts* of A (though in practice these only matter up to abstract K-isogeny, so we usually can work with the actual product $B_i^{e_i}$ even though the C_i may not be such products). An abelian variety A is called *isotypic* (or *K-isotypic* for emphasis) if it is K-isogenous to B^e where B is K-simple and $e \geq 1$. Beware that isotypicity can be destroyed by extension of the ground field in general; see Example 1.4. This is analogous to the fact that an irreducible but not absolutely irreducible representation of a finite group on a finite-dimensional $\mathbf{Q}$-vector space may decompose into a direct sum of non-isomorphic irreducible representations after a finite extension of the ground field (and so loses isotypicity in the sense of finite group representations).

Isogenies induces isomorphisms between endomorphism algebras: if $f\colon A \to B$ is an isogeny then there exists $f'\colon B \to A$ such that $f \circ f' = [n]_B$, $f' \circ f = [n]_B$ for some integer $n \geq 1$ and hence

$\sigma \mapsto (1/n) f \circ \sigma \circ f'$, $\tau \mapsto (1/n) f' \circ \tau \circ f$ are inverse maps that provide isomorphism between $\mathrm{End}^0(A)$ and $\mathrm{End}^0(B)$ (here we use the fact that all elements of these endomorphism algebras can be written as fractions h/m for an actual endomorphism h and an integer $m \neq 0$). See Proposition 3.5.4. from Brian's notes on abelian varieties in the Mordell seminar. Beware that, unlike the case of elliptic curves, usually we *cannot* arrange that $n = \deg f$, nor that $\deg f' = \deg f$.

This argument provides a $\mathbf{Q}$-algebra isomorphism

$$\mathrm{End}^0(A) \simeq \mathrm{End}^0(\prod B_i^{e_i}) = \prod_i End(B_i^{e_i}) = \prod \mathrm{Mat}_{e_i}(\Delta_i)$$

where $\Delta_i = \mathrm{End}^0(B_i)$ is division algebra finitely-dimensional over $\mathbf{Q}$. (By Wedderburn's theorem, Δ_i and e_i are uniquely determined. (But Δ_i does not determine the isogeny class of B_i; for example in many cases it is just $\mathbf{Q}$.)

Here we implicitly used a version of Schur's lemma: $\mathrm{End}(B, B') = 0$ for simple non-isogenous B and B', and $\mathrm{End}(B)$ is a division algebra for simple B. That's done by the usual argument with $\ker(f) \subset B_i$ and image $f(B) \subset B'$: although the structure of $\ker(f)$ may be rather delicate when K is imperfect (e.g., its underlying reduced scheme might not even be a subgroup scheme, let alone smooth), the image $f(B)$ is an abelian K-subvariety of B (as we can check over $\overline{K}$) and so by K-simplicity of B' either $f(B) = 0$ or $f(B) = B'$. In the former case $f = 0$ and in the latter case $\ker f$ is finite for dimension reasons, with f an isogeny.

The center Z_i of each Δ_i is clearly a number field, so Δ_i is a finite-dimensional central division algebra over Z_i. Global class field theory is an important tool in classifying and working with such division algebras, provided we can get a handle on the possibilities for these centers Z_i (as we will do later).

Remark 1.3. If $K = \mathbf{Q}$ and A is an elliptic curve which acquires complex multiplication over an extension field then $\mathrm{End}(A) = \mathbf{Z}$ (the CM structure cannot be defined over $\mathbf{Q}$). This is immediate from the fact that the action on the Lie algebra is faithful in characteristic 0, so $\mathrm{End}^0(A) \hookrightarrow \mathrm{End}_{\mathbf{Q}}(T_0(A)) = \mathbf{Q}$, forcing $\mathrm{End}^0(A) = \mathbf{Q}$ and hence $\mathrm{End}(A) = \mathbf{Z}$ by $\mathbf{Z}$-finiteness of the endomorphism ring.

In general A is isotypic over K if and only if $\mathrm{End}^0(A)$ is a central simple algebra over a number field. Indeed, if A has more than one isotypic component then the isotypic decomposition of A induces a nontrivial product decomposition of $\mathrm{End}^0(A)$, contradicting simplicity of the $\mathbf{Q}$-algebra. Conversely we know that the ring of matrices over a finite-dimensional central division algebra over a field is a central simple algebra.

Example 1.4 (Extension of scalars does not preserve isotypicity)**.** Let $L/\mathbf{Q}$ be a quadratic field with σ the nontrivial automorphism of L, and pick an elliptic curve E over L with $j(E) \notin \mathbf{Q}$ (so E cannot descend over $\mathbf{Q}$) such that E and its $L/\mathbf{Q}$-twist $\sigma^*(E)$ are not isogenous over L. (This is stronger than merely being non-isomorphic; it is a nontrivial exercise for the reader to make examples of such E for suitable L.)

Let $A = \mathrm{R}_{L/\mathbf{Q}}(E)$ be the Weil restriction of E. It can be produced by taking $E \times \sigma^*(E)$ and descending it to $\mathbf{Q}$ using a "twisted" Galois descent datum. We have $A_L \simeq E \times \sigma^*(E)$ with 1-dimensional isotypic parts (as E and $\sigma^*(E)$ are non-isogenous over L), so A_L is not isotypic. However,

A is $\mathbf{Q}$-simple and hence isotypic, since a nontrivial proper abelian subvariety of A over $\mathbf{Q}$ would have to be an elliptic curve E', yielding $E'_L \subset A_L$ that must map nontrivially to both E and $\sigma^*(E)$ (as otherwise it would map isomorphically to one of these factors, contradicing that neither E or $\sigma^*(E)$ can be descended to $\mathbf{Q}$). Hence, the isotypicity of A is destroyed by extension of the ground field to L.

2. Facts about central simple algebras over a field

We always understand central simple algebras to be finite-dimensional over the center. The ur-examples are the matrix algebras $\mathrm{Mat}_n(k)$ over any field k. Let D be a (finite-dimensional) central-simple algebra over a field F (CSA). That is, it has no non-trivial two-sided ideals and its center is F. Here are some basic results (not necessarily obvious):

(1) For any extension field F'/F, $D \otimes_F F'$ is a central simple algebra over F'.
(2) For a separable closure F_s/F, $D \otimes_F F_s \simeq \mathrm{Mat}_n(F_s)$ as F_s-algebras. (This slickest proof of this is via deformation theory if we wish to include imperfect F; we will only need F of characteristic 0.) In particular, $\dim_F D = \dim_{F_s} D_s = n^2$ is a perfect square.
(3) There exists a finite Galois extension F' for which $D \otimes_F F' \cong \mathrm{Mat}_n(F')$ as F'-algebras. In general an extension field F'/F is said to *split* D if $D \otimes_F F' \simeq \mathrm{Mat}_n(F')$ as F'-algebras, and are called *splitting fields* of D over F. (Thus, finite Galois splitting fields always exist.)

Theorem 2.1 (Noether-Skolem)**.** *All automorphisms of D as an F-algebra are inner (i.e., conjugation by some element of $D^\times$): $D^\times/F^\times = \mathrm{Aut}_F(D)$.*

A consequence of the Wedderburn–Artin structure theory is:

Proposition 2.2. *Up to F-isomorphism there is a unique central division algebra Δ over F and integer $e \geq 1$ such that $D \simeq \mathrm{Mat}_e(\Delta)$.*

By the Skolem–Noether theorem, the non-uniqueness of a choice of F_s-algebra isomorphism $D_{F_s} \simeq \mathrm{Mat}_n(F_s)$ is given by conjugation against $\mathrm{Mat}_n(F_s)^\times = \mathrm{GL}_n(F_s)$. Since the F_s-linear map $\mathrm{Tr} : \mathrm{Mat}_n(F_s) \to F_s$ and the homogeneous polynomial map $\det : \mathrm{Mat}_n(F_s) \to F_s$ of degree n are conjugation-invariant, if we transfer them to D_{F_s} via a choice of F_s-algebra isomorphism then the resulting maps $D_{F_s} \rightrightarrows F_s$ are intrinsic. Although the choice of isomorphism $D_{F_s} \simeq \mathrm{Mat}_n(F_s)$ is generally *not* Galois equivariant (indeed, such failure is the source of all interesting D!), this failure is again governed by $\mathrm{GL}_n(F_s)$-conjugations, so in fact the maps $D_{F_s} \rightrightarrows F_s$ are Galois-equivariant (!) and this descend to maps

$$\mathrm{Trd} : D \to F, \ \ \mathrm{Nrd} : D \to F$$

with the first one (*reduced trace*) actually F-linear and the second one (*reduced norm*) actually a multiplicative homogeneous polynomial map of degree $\sqrt{[D:F]}$. (This "polynomial map" condition uniquely determines the abstract degree-n polynomial form on D when F is infinite, and the only interesting case is infinite F since otherwise D is a matrix algebra!)

The reduced trace and reduced norm are compatible with arbitrary extension of the ground field F'/F in the sense that $\mathrm{Trd}_{D_{F'}/F'}$ restricts to $\mathrm{Trd}_{D/F}$ on $D \subset D_{F'}$, and similarly for reduced norms. Indeed, to check these claims we can pass to an extension F'_s/F_s between compatible separable

closures, where it becomes the obvious case of the behavior of trace and determinant on $\mathrm{Mat}_n(F'_s)$ and $\mathrm{Mat}_n(F_s)$.

Remark 2.3. The reason for the word "reduced" is that if we instead consider the intrinsic trace $\mathrm{Tr}_{D/F}$ and norm $\mathrm{N}_{D/F}$ for the F-algebra D (i.e., the trace and determinant of the F-linear multiplication map $x \mapsto d \cdot x$ for $d \in D$) then

$$\mathrm{Tr}_{D/F} = n\mathrm{Trd}_{D/F}, \;\; \mathrm{N}_{D/F} = \mathrm{Nrd}^n_{D/F}$$

for $n = \sqrt{[D:F]}$.

Proposition 2.4. *The maximal commutative semisimple F-subalgebras $F' \subset D$ have degree $n = \sqrt{[D:F]}$ over F, and are their own centralizers. Conversely, if a commutative semisimple F-subalgebra of D is its own centralizer then it is maximal and has F-degree n.*

An extension field F'/F of degree n occurs in D if and only if $D \otimes_F F' \simeq \mathrm{Mat}_n(F')$ as F'-algebras.

We now focus on the main case of interest, $\mathrm{End}^0(A)$ for a K-simple abelian variety A. Which central division algebras over number fields arise in this way? For instance, what are the constraints on the center Z? There are "positivity" conditions arising from the existence of polarizations, as follows.

Example 2.5. Choose a polarization $\phi\colon A \to A^\vee$. We recall that such maps are isogenies that are symmetric (i.e., $\phi^{\vee\vee}\colon A^{\vee\vee} \to A^\vee$ equals ϕ via double duality) and satisfy a "positivity" property:

• the map $A \xrightarrow{(id,\phi)} A \times A^\vee$ has pullback $(id,\phi)^*\mathscr{P}_A$ that is ample, where $\mathscr{P}_A$ is the Poincare line bundle.

To the choice of polarization we associate the Rosati involution of $D = \mathrm{End}^0(A)$ given by

$$f \mapsto \phi^{-1} f^\vee \phi =: f^\dagger$$

(recall that we can invert isogenies in the endomorphism algebra). It is anti-multiplicative in the sense that $(f_1 f_2)^\dagger = f_2^\dagger f_1^\dagger$, and the symmetry of ϕ yields the involution property $f^{\dagger\dagger} = f$. This involution is *positive* in the sense that the symmetric bilinear form $(f,g) \mapsto \mathrm{Tr}_{D/\mathbf{Q}}(fg^\dagger)$ has positive-definite associated quadratic form (i.e., $\mathrm{Tr}_{D/\mathbf{Q}}(ff^\dagger) > 0$ for $f \neq 0$). It is equivalent to work with $\mathrm{Tr}_{Z/\mathbf{Q}} \circ \mathrm{Trd}_{D/Z}$, due to Remark 2.3. Albert classified all pairs $(\Delta, *)$ consisting of a central division algebra over a number field equipped with a positive (anti-multiplicative) involution.

The involution must restriction to an automorphism of order 1 or 2 on the center Z, so one of two things can happen:

• if $*$ is the identity on Z then the quadratic form $x \mapsto \mathrm{Tr}_{Z/\mathbf{Q}}(x^2)$ is positive-definite, which forces Z to be a totally real number field.

• if $*$ is an involution σ of Z then the quadratic form $x \mapsto \mathrm{Tr}_{Z/\mathbf{Q}}(x\sigma(x))$ is positive-definite, and this forces Z to be a CM field: a totally imaginary quadratic extension of a totally real field. Equivalently, the fixed field of $*$ on Z is a totally real field Z^+ and $Z = Z^+(\sqrt{\alpha})$ where $\alpha \in Z^+$ is totally negative. In such cases $*$ is induced by complex conjugation (negation on $\sqrt{\alpha}$) for *every* embedding $Z \to \mathbf{C}$, so Z has an "intrinsic" complex conjugation (namely, its unique involution over its maximal totally real subfield).

CM fields are characterized in one of two equivalent ways:

Lemma 2.6. *Let Z be a number field. The following are equivalent:*

i) Z is a totally imaginary quadratic extension of Z^+ a totally real field.

ii) Z is not totally real, and complex conjugation is well-defined: for every embedding $Z \overset{j}{\hookrightarrow} \mathbf{C}$, $j(Z)$ is stable under complex conjugation and the map $\alpha \mapsto j^{-1}(\overline{j(\alpha)})$ is independent of j.

For example, the cyclotomic fields $\mathbf{Q}(\zeta_n)$ are CM for $n > 2$: the intrinsic complex conjugation is given by $\zeta \mapsto \zeta^{-1}$ on all roots of unity in such fields. Also, it is easy to check that every subfield of a CM field is either totally real of CM, so every subfield of a cyclotomic field is either totally real or CM. For any finite Galois extension of $\mathbf{Q}$, the effect of complex conjugations under embeddings into $\mathbf{C}$ constitute a single conjugacy class, so finite *abelian* extensions of $\mathbf{Q}$ are either totally real or CM. (One does not need to invoke Kronecker-Weber here.)

We can use weak approximation to construct examples of CM that extend finitely many chosen valuations in (almost) any way we want (i.e., induce pretty much any p-adic behavior we want for finitely many p, subject to degree conditions). For example, Let $f_\infty \in \mathbf{R}[t]$ be monic of degree g with g distinct real roots, and $f_p \in \mathbf{Q}_p[t]$ be monic irreducible degree g (e.g., Eisenstein). Choose monic $f \in \mathbf{Q}[t]$ of degree g close to f_∞ and f_p. By Krasner's Lemma, sufficient p-adic closeness implies that f is irreducible over $\mathbf{Q}_p$ also, hence f is irreducible over $\mathbf{Q}$. Thus, adjoining a root of f to $\mathbf{Q}$ yields a totally real field of degree g, to which we now add $\sqrt{-a}$ for any a that is totally positive at all archimedean places and is near to whatever we like at the p-adic place (i.e., near the negative of a square). We can do this for more than one p as well.

A rigidity argument with Tate modules shows:

Theorem 2.7 (Chow)**.** *Let K'/K be an extension of fields with K separably closed in K' (e.g., $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$). The functor $A \rightsquigarrow A_{K'}$ from the category of abelian varieties over K to the category of abelian varieties over K' is fully faithful.*

For our purposes, the most important aspect of this result is that if an abelian variety A over $\mathbf{C}$ can be defined over $\overline{\mathbf{Q}}$ then such a descent to $\overline{\mathbf{Q}}$ is unique up to unique isomorphism, is functorial in A, and has the *same* endomorphism ring. In particular, when we construct CM abelian varieties over $\mathbf{C}$ by analytic methods, if it can be shown that our construction descends to $\overline{\mathbf{Q}}$ then the descent is also CM over $\overline{\mathbf{Q}}$.

3. The CM case

Let K be any field.

Theorem 3.1. *Let B be a K-simple abelian variety of dimension $g > 0$. A commutative $\mathbf{Q}$-subalgebra $L \subset End^0(B) =: \Delta$ satisfies $[L : \mathbf{Q}] \leq 2g$, and when equality holds, L is its own centralizer in Δ, so it is a maximal commutative subfield.*

Proof. We explain the case $K = \mathbf{C}$ vis analytic methods. The case of general K will be handled later (allowing K of characteristic > 0, such as finite fields) by an algebraic variant of the same idea (replacing rational homology below with Tate modules).

Consider the action of $\mathrm{End}(B)$ on $\mathrm{H}_1(B(\mathbf{C}), \mathbf{Z}) \simeq \mathbf{Z}^{2g}$, which induces an action of $\mathrm{End}^0(B)$ on the $2g$-dimensional $\mathbf{Q}$-vector space $V = \mathrm{H}_1(B(\mathbf{C}), \mathbf{Q})$. The faithfulness of the homology representation for complex tori implies that the homology is thereby a faithful module over L.

Considering the decomposition $L = \prod L_i$ into a product of finitely many number fields L_i, it follows that the associated decomposition $\prod V_i$ of V with L_i-vector spaces V_i has $V_i \neq 0$ for all i. Thus,

$$2g = \sum \dim_{\mathbf{Q}} V_i = \sum [L_i : \mathbf{Q}] \dim_{L_i} V_i \geq \sum [L_i : \mathbf{Q}] = [L : \mathbf{Q}],$$

with equality if and only if V_i is 1-dimensional over L_i for all i, which is to say that V is free of rank 1 over L. In such cases $\mathrm{End}_L(V) = L$, so L is its own centralizer in $\mathrm{End}^0(B)$. □

Example 3.2. Here is the key example for our purposes (see ă2 of Mumford's book *Abelian Varieties* for more details). Let L be a CM field of degree $2g$ over $\mathbf{Q}$, so

$$L \otimes_{\mathbf{Q}} \mathbf{R} = \prod_{v|\infty} L_v \simeq \mathbf{C}^g$$

where the product is taken over all places v above ∞ in L^+. Note that each L_v is isomorphic to $\mathbf{C}$ in two ways (over the *unique* isomorphism $L_v^+ = \mathbf{R}$). We have 2^g choices in total, and a choice $\Phi = \{\phi_v\}$ of these isomorphisms (i.e. embeddings $L \hookrightarrow \mathbf{C}$) is nothing more or less than a set of representatives for the quotient of the set of embeddings $\mathrm{Hom}(L, \mathbf{C})$ modulo the action of complex conjugation (on $\mathbf{C}$, or on L: these amount to the same thing since L is a CM field and hence has an intrinsic complex conjugations!). For such Φ, we write $(L \otimes_{\mathbf{Q}} \mathbf{R})_\Phi$ to denote $L \otimes_{\mathbf{Q}} \mathbf{R}$ equipped with its $\mathbf{C}$-linear structure via the isomorphisms $\varphi_v : L_v \simeq \mathbf{C}$ for all $v|\infty$.

Any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_L$ of L, a $\mathbf{Z}$-lattice in $L \otimes_{\mathbf{Q}} \mathbf{R}$, but we will stick to the case $\mathfrak{a} = \mathcal{O}_L$ for simplicity. For each Φ as above, consider the g-dimensional complex torus

$$A_\Phi = (L \otimes_{\mathbf{Q}} \mathbf{R})_\Phi / \mathcal{O}_L$$

equipped with its natural action by $\mathcal{O}_L$. By a computation using the fact that L is a CM field, one can build a Riemann form on this complex torus and thereby prove it is *always* algebraic. In other words, we may and do regard A_Φ as an abelian variety, and by construction there is a specified embedding $\mathcal{O}_L \hookrightarrow End(A_\Phi)$, and hence $L \hookrightarrow End^0(A_\Phi)$.

We can reconstruct Φ from the embedding $L \hookrightarrow End^0(A_\Phi)$ as follows. The order

$$\mathcal{O} = L \bigcap End(A)$$

in $\mathcal{O}_L$ acts on $T_0(A)$ linearly over $\mathbf{C}$, and we extend this to an action of $\mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Q} = L$ and hence a module structure over $L \otimes \mathbf{QC}$. As an $L \otimes \mathbf{QC}$-module, $V := \mathrm{Tan}_0(A)$ them must decompose as a product $\prod_{\phi:\, L \to C} V_\phi$ where L acts on V_ϕ via ϕ (using the idempotents from the *canonical* $\mathbf{C}$-algebra decomposition $L \otimes_{\mathbf{Q}} \mathbf{C} \simeq \prod_{\phi: L \to \mathbf{C}} \mathbf{C} e_\phi$). The construction shows that each V_ϕ is at most 1-dimensional, with the set of $\{\phi\}$ for which $V_\phi \neq 0$ containing exactly one representative from each pair of conjugate embeddings $L \hookrightarrow \mathbf{C}$.

Next time we will use Hodge theory to show that this construction is exhaustive up to L-linear $\mathbf{C}$-isogeny in the following sense. First, for *any* degree-$2g$ CM field L occurring in $\mathrm{End}^0(A)$ for a g-dimensional abelian variety A over $\mathbf{C}$, necessarily the $L \otimes_{\mathbf{Q}} \mathbf{C}$-module structure on $\mathrm{Tan}_0(A)$ is given

by a set Φ of representatives for the quotient of $\mathrm{Hom}(L, \mathbf{C})$ modulo complex conjugation. Second, such an A is then L-linearly isogenous to A_Φ.

We will *use* these conclusions over $\mathbf{C}$ to deduce that something similar happens over *any* algebraically closed field of characteristic zero (especially $\overline{\mathbf{Q}}$).

Here is a more refined result:

Theorem 3.3. *Let A be an abelian variety of dimension $g > 0$ over an arbitrary field K. Let $P \subset \mathrm{End}^0(A)$ be a commutative semisimple $\mathbf{Q}$-algebra. Then $[P : \mathbf{Q}] \leq 2g$, and if equality holds then under the decomposition $P = \prod L_i$ as a product of fields there is a compatible isogeny $A \sim \prod A_i$ with A_i isotypic and $L_i \subset End^0(A_i)$ a maximal commutative semisimple $\mathbf{Q}$-subalgebra of degree $2\dim(A_i)$.*

Beware that we are *not* claiming that these A_i are the isotypic parts of A. Indeed, for some distinct i and j it may happen that the simple factors of A_i and A_j are K-isogenous.

Here is an important refinement:

Proposition 3.4 (Tate)**.** *When the equality $[P : \mathbf{Q}] = 2g$ holds above then there exists a commutative semisimple $\mathbf{Q}$-subalgebra $P' \subset \mathrm{End}^0(A)$ of $\mathbf{Q}$-degree $2g$ such that every factor field L'_j of P' is a CM field. Moreover, when A is isotypic then we can arrange that P' is itself a CM field.*

Example 3.5. Let $A = E \times E$, where E is a *CM* elliptic curve over a field F, with CM by an imaginary quadratic field K. Assume that $\mathrm{End}^0(E) = K$ (as happens except possibly with $\mathrm{char}(F) > 0$ and E is supersingular.) Clearly $\mathrm{End}^0(A) = \mathrm{Mat}_2(K)$, and this contains any quadratic extension of K. In particular, it contains any quadratic extension L/K that is not biquadratic (of which there are many examples for any K), and such L must have K as its unique quadratic subfield, yet that is not real quadratic, so L cannot be a CM field (since otherwise L^+ would be a real quadratic subfield). So one possibility for P is any such quartic field L. This is not CM.

Tate's refinement is illustrated by the fact that $\mathrm{Mat}_2(K)$ also contains any biquadratic field $L' \supset K$, as any such L' is necessarily CM (being the compositum of an imaginary quadratic and real quadratic field). (As a more extreme example, we can also take the split K-algebra $P'' = K \times K$ whose factor fields K are CM, but it is much more interesting that for the isotypic A we can choose P' to be a CM field rather than just a product of CM fields.)

Definition 3.6. An abelian variety A of dimension $g > 0$ over a field K is *of CM type* if there exists a commutative semisimple $\mathbf{Q}$-subalgebra $P \subset \mathrm{End}^0(A)$ of $\mathbf{Q}$-degree $2g$. A *CM structure* on A is a choice of $P \hookrightarrow \mathrm{End}^0(A)$ (which is best considered as an abstract P equipped with a specified embedding into $\mathrm{End}^0(A)$).

In general, if A is a CM abelian variety then its isotypic parts and simple isogeny factors over K are also CM abelian varieties. For a choice of CM structure $P = \prod L_i$ with number fields L_i, the intersection $P \bigcap \mathrm{End}(A)$ in P is a subring of finite index in $\mathcal{O}_P = \prod \mathcal{O}_{L_i}$ because $\mathrm{End}(A)$ is a $\mathbf{Z}$-lattice in $\mathrm{End}^0(A)$; it is called the *CM order*.

Example 3.7. Let C be the smooth projective (geometrically connected) curve over $\mathbf{Q}$ associated to the affine plane curve $y^p = x(1-x)$ for a prime $p \rangle 2$. Its genus is $(p-1)/2$. For $L = \mathbf{Q}(\zeta_p)$ there is

a natural action by $\mu_p(L)$ on C_L by $\zeta(x,y) = (x, \zeta y)$, and hence we get an action of $\mathbf{Z}[\zeta_p] = \mathcal{O}_L$ acts on $J = Jac(C_L)$. This defines a CM structure. Next time we will work out the set Φ of embeddings of L into $\mathbf{C}$ that occur on $\mathrm{Tan}_0(J_{\mathbf{C}})$ (for a choice of realization of $\mathbf{C}$ as an extension of L).

Remark 3.8. The possibility that the CM order is not maximal can create some headaches, and the desire to avoid this is one reason that we try as much as possible to work in the isogeny category. More specifically, if A has CM structure P over a field K and $\mathcal{O} = P \bigcap \mathrm{End}(A)$ is the CM order then one can make sense of a "scalar extension" $\mathcal{O}_P \otimes_{\mathcal{O}} A$ in the sense of fppf abelian sheaves on the category of K-schemes (exercise to make sense of this; we will come back to it later), with this being another abelian variety over K of the same dimension and admitting a canonical isogeny $A \to \mathcal{O}_P \otimes_{\mathcal{O}} A$ linear over $\mathcal{O} \to \mathcal{O}_P$. Explicitly, if $K = \mathbf{C}$ and $A = V/\Lambda$ then $\mathcal{O}_P \otimes_{\mathcal{O}} A = V/(\mathcal{O}_P \cdot \Lambda)$. In this way, we can always naturally "increase" the CM order to be maximal in P (without changing the ground field!).

This trick will be useful in some steps within the proof of the Main Theorem(s) of Complex Multiplication, at places where we need to harness torsion-level information while keeping track of the CM structure. (For example, if $\mathcal{O} = \mathcal{O}_P$ then in characteristic 0 $T_\ell(A)$ is free of rank 1 over $\mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathcal{O}_P$, so $A[N](\overline{K})$ is free of rank 1 over $\mathcal{O}_P/(N)$ for all $N \geq 1$. It is the need to pass to CM order $\mathcal{O}_P$ that forces us to maintain an "isogeny invariant" viewpoint in the formulation of the main results about complex multiplication in the higher-dimensional case (as it is much too restrictive in practice to only prove the main results when the CM order is $\mathcal{O}_P$, since this property tends to be destroyed by most P-linear isogenies).

The case of elliptic curves is extremely anamolous in the following sense. By the quirk that quadratic orders $\mathcal{O}$ are *always* monogenic, even when $\mathcal{O}$ is not maximal, the above module-freeness results at torsion level always hold for elliptic curves. Hence, the trick of passing to a maximal CM order is not important in the case of elliptic curves. But this breaks down in higher dimensions when $\mathcal{O}$ is not maximal.