Notes for the talk about the reflex type and the type norm

Marco Streng

December 9 and 16, 2009

Abstract

We give the definitions of the reflex type and the type norm of a CM type. CM types occur in CM theory when diagonalizing the representation of the CM field on the tangent space.

For elliptic curves, the CM type and the type norm are the natural embedding of the CM field into the field of definition of the elliptic curve. The reflex type is then the partial inverse of this 'CM type'. This talk gives the appropriate generalizations for abelian varieties of higher dimension.

The definitions and main results are in number theory and Galois theory only.

These are notes for a talk in a seminar on complex multiplication. Please email any errors or suggestions to marco.streng@gmail.com

CM fields

Definition. A *CM field* is a totally imaginary quadratic extension K of a totally real number field K_0.

Here by "totally imaginary" we mean "with no embeddings into $\mathbf{R}$". In other words, a CM field is a field $K = K_0(\sqrt{r})$ for some totally real number field K_0 and some totally negative $r \in K_0$. Note that CM fields have even degree and that the CM fields of degree 2 are exactly the imaginary quadratic number fields.

Lemma 1. Let K be a number field. The following are equivalent.

(1) The field K is totally real or a CM field.

(2) There exists an automorphism ρ of K such that for every embedding of $K \to \mathbf{C}$, the automorphism ρ equals complex conjugation on K.

Moreover, the following holds:

(a) any composite of finitely many CM fields is a CM field,

(b) the normal closure of a CM field is a CM field,

(c) if ϕ is an embedding of CM fields $K_1 \to K_2$, then we have $\rho \circ \phi = \phi \circ \rho$ with ρ as in (2), and we denote $\rho \circ \phi$ by $\overline{\phi}$,

(d) any subfield of a CM field is totally real or a CM field.

Proof. (1) $\Rightarrow$ (2): If K is totally real, then $\rho = \mathrm{id}$ satisfies (2). If K is CM with totally real subfield K_0, then let ρ be the unique nontrivial element of $\mathrm{Gal}(K/K_0)$.
(2) $\Rightarrow$ (1): Conversely, suppose ρ is as in (2). Let K_0 be the fixed field of ρ, which is totally real. If $K_0 = K$ holds, then K is totally real. Otherwise, we see that K is a totally imaginary quadratic extension of the totally real field K_0.
(a): Now let $K, L \subset M$ be two CM fields and $M/\mathbf{Q}$ finite and normal. Choose an embedding of M into $\mathbf{C}$ and let τ be complex conjugation on M. Then τ maps K to K and L to L, hence maps KL to KL. Moreover, for every embedding of KL into $\mathbf{C}$, we have that τ equals complex conjugation on K and on L, hence on all of KL.
(b): Part (b) follows from part (a) since the normal closure is the composite of the conjugates.
(c): Let ψ be an embedding $K_2 \to \mathbf{C}$, so $\bar{\cdot} \circ \psi = \psi\rho$. We also have an embedding $\psi\phi : K_1 \to \mathbf{C}$, which yields $\bar{\cdot} \circ \psi\phi = \psi\phi\rho$, so $\psi\rho\phi = \psi\phi\rho$. As ψ is injective, we conclude $\rho\phi = \phi\rho$.
(d): Let K be a subfield of L, where L satisfies (2) for some ρ. By (b), we can assume without loss of generality that L is normal over $\mathbf{Q}$, so let $H = \mathrm{Gal}(L/K) \subset \mathrm{Gal}(L/\mathbf{Q})$. By (c), we have $\rho H = H\rho$, so ρ restricts to an automorphism of K.

Since every embedding $K \to \mathbf{C}$ extends to an embedding $L \to \mathbf{C}$, we find that ρ satisfies (2) also on K. □

Example. The cyclotomic field $\mathbf{Q}(\zeta_n)$ satisfies 2 for $\rho : \zeta_n \mapsto \zeta_n^{-1}$. The field is a CM field for $n > 2$ and equal to $\mathbf{Q}$ for $n \in \{1, 2\}$. Its totally real subfield is the fixed field of ρ, i.e., $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$.

CM fields occur naturally in CM theory because of the following result.

Abelian varieties and CM theory. *Let K be a number field of degree $2g$. The following are equivalent:*

(i) the field K is a CM field,

(ii) there exists an abelian variety $A/\mathbf{C}$ of dimension g and an embedding $K \to \mathrm{End}(A) \otimes \mathbf{Q}$ such that (for some polarization of A) the Rosati-involution maps K to K.

Actually, Jeroen will show that this equivalence is also true with $\mathbf{C}$ replaced by $\overline{\mathbf{Q}}$.

Proof. We have seen the construction of "$(i) \Rightarrow (ii)$" in David's talk. The proof "$(ii) \Rightarrow (i)$" was in Richard's talk. Here ρ equals the Rosati-involution on K and one can show that it satisfies (2) using its *positive definiteness* $\mathrm{tr}(\rho(x)x) > 0$ for all non-zero $x \in K$. □

CM types

Let K be a CM field of degree $2g$ and $L'/\mathbf{Q}$ a normal field that contains a subfield isomorphic to K.

Definition. A *CM type* of K with values in L' is a subset $\Phi \subset \mathrm{Hom}(K, L')$ consisting of exactly one element from each of the g *complex conjugate pairs* $\{\phi, \overline{\phi}\} \subset \mathrm{Hom}(K, L')$.

There are thus 2^g CM types of K with values in L'. A CM type of an imaginary quadratic K with values in L' is the same as an embedding of K into L'.

Definition. Let $K_1 \subset K_2$ be CM fields, and Φ a CM type of K_1 with values in L'. Assume L' is normal over $\mathbf{Q}$ and contains a subfield isomorphic to K_2. The CM type Φ_{K_2} of K_2 *induced* by Φ is

$$\Phi_{K_2} = \{\phi \in \mathrm{Hom}(K_1, L') : \phi_{|K_1} \in \Phi\}.$$

We say that a CM type is *primitive* if it is not induced from a CM type of a strict CM subfield.

Example. The cyclic CM field $K = \mathbf{Q}(\zeta_7)$ of degree 6 has subfields $K_0 = \mathbf{Q}(\zeta_7 + \zeta_7^{-1})$, $K_1 = \mathbf{Q}(\zeta_7)$, and $\mathbf{Q}$. Given a field L' that contains a copy of K, we see that K has $2^3 = 8$ CM types of which 2 are induced from K_1, hence has 6 primitive CM types.

Lemma 2. Let $K_1 \subset K_2$ be a pair of CM fields and Ψ a CM type of K_2 with values in L'. Let L be the normal closure of K_2 over $\mathbf{Q}$. If $\Psi = \Phi_{K_2}$ holds for some CM type Φ of K_1, then we have

$$\Phi = \Psi_{|K_1} := \{\psi_{|K_1} \mid \psi \in \Psi\}.$$

Moreover, the set $\Psi_{|K_1}$ is a CM type if and only if we have

$$\mathrm{Gal}(L/K_1) \subset H = \{\sigma \in \mathrm{Gal}(L/\mathbf{Q}) \mid \Phi\sigma = \Phi\}. \tag{1}$$

Proof. The first statement follows from the definition. For the 'if and only if' statement, note that $\Psi_{|K_1}$ contains at least one element from each complex conjugate pair, so it is a CM type if and only if there are no $\psi, \psi' \in \Psi$ with $\psi_{|K_1} = \overline{\psi'_{|K_1}}$. By extending ψ and ψ' to L and taking $\sigma = \psi^{-1}\psi'$, we see that this is equivalent to the non-existence of $\psi \in \Psi_L$ and $\sigma \in \mathrm{Gal}(L/K_1)$ with $\overline{\psi\sigma} \in \Psi_L$, i.e. with $\psi\sigma \notin \Phi_L$. In other words, this is equivalent to the non-existence of $\sigma \in \mathrm{Gal}(L/K_1) \setminus H$. □

Corollary. *With the notation as in the lemma, there is a unique pair* (K_0, Φ_0) *with* $K_0 \subset K_2$ *and* Φ_0 *a primitive CM type of* K_0 *such that* Ψ *is induced from* Φ_0*. Moreover, the field* K_0 *is the fixed field of* H*.*

Proof. Let K_0 be the fixed field of H. Then $\Psi_{|K_0}$ is the unique CM type of K_0 that induces Ψ. If a CM type Φ of a field $K_1 \subset K$ also induces Ψ, then the lemma implies that K_1 contains K_0, so $\Psi_{|K_0}$ is primitive. Moreover, the type $\Psi_{|K_0}$ of K_0 induces $\Psi_{|K_1}$ on K_1, hence $\Psi_{|K_1}$ is only primitive if $(K_1, \Psi_{|K_1})$ equals $(K_0, \Psi_{|K_0})$ □

Abelian varieties and CM theory. *Let A be an abelian variety of dimension g over F with an embedding $\iota : \mathcal{O}_K \to \mathrm{End}(A)$, where K is a field of degree $2g$. Assume that the image of ι is stable under the Rosati involution.*

Richard showed in his talk that there is a basis $b_1, \ldots, b_g$ of the tangent space $T_0(A)(\overline{F})$ of A at 0 over the algebraic closure and a CM type Φ of K with values in $\overline{F}$ such that we have

$$D\iota(\alpha)b_i = \phi_i(\alpha)b_i.$$

This defines Φ uniquely and we say that (A, ι) is of type *Φ.*

If γ is an automorphism of K and (A, ι) has type Φ, then $(A, \iota \circ \gamma)$ has type

$$\Phi \circ \gamma = \{\phi \circ \gamma \mid \phi \in \Phi\}.$$

If σ is an automorphism of $\overline{k}$, then define $\sigma(\iota)$ by $\sigma(\iota)(\alpha) = \sigma(\iota(\alpha))$ for all $\alpha \in K$. We find that if (A, ι) has type Φ, then $(\sigma(A), \sigma(\iota))$ has type

$$\sigma \circ \Phi = \{\sigma \circ \phi \mid \phi \in \Phi\}.$$

The reflex of a CM type

Let K be a CM field and let Φ be a CM type of K with values in L'. Let $L \supset K$ be the normal closure of K. Then by making L' smaller, we can assume $L' \cong L$.

The *reflex* (K', Φ') of (K, Φ) is defined as follows. Let Φ_L be the CM type of L with values in L' induced by Φ. Note that Φ_L is a set of isomorphisms $L \to L'$, so we can take its set Φ_L^{-1} of inverses, which is a set of isomorphisms $L' \to L$.

We claim that Φ_L^{-1} is a CM type of L' with values in L. Indeed, if $\phi, \overline{\phi}$ is a pair of complex conjugate embeddings of L into L', then by Lemma 1c, we have $\overline{\phi^{-1}} = \phi^{-1} \circ \bar{\cdot} = (\bar{\cdot} \circ \phi)^{-1} = \overline{\phi}^{-1}$, hence $\phi^{-1}, \overline{\phi}^{-1}$ is also a pair of complex conjugate embeddings. As a CM type is a choice of exactly one element from each complex conjugate pair, this proves the claim.

Now let (K', Φ') be a pair consisting of a subfield $K' \subset L'$ and a primitive CM type Φ' of K' with values in L that induces Φ_L^{-1}. Existence and uniqueness of K' and Φ' hold by the corollary of Lemma 2.

Definition. The pair (K', Φ') is called the *reflex* of (K, Φ), the field K' is called the *reflex field* of (K, Φ), and the CM type Φ' is called the *reflex type* of (K, Φ).

Lemma 3. The CM type Φ' is a primitive CM type of K'. If (K'', Φ'') is the reflex of (K', Φ'), then K'' is a subfield of K and Φ is induced by Φ''. If Φ is primitive, then we have $K'' = K$ and $\Phi'' = \Phi$.

Proof. The first statement holds by definition. For the second, we apply the construction again, and see that $K'' \subset L$ and Φ'' are unique such that Φ'' is primitive and induces $(\Phi_L^{-1})^{-1} = \Phi_L$. As Φ also induces Φ_L, we find that Φ'' induces Φ, as seen in the proof of the corollary of Lemma 2. Finally, if Φ itself is primitive, then it equals Φ'' by definition of Φ''. □

Lemma 4. The reflex field K' satisfies

$$\mathrm{Gal}(L'/K') = \{\sigma \in \mathrm{Gal}(L'/\mathbf{Q}) \mid \sigma\Phi = \Phi\}.$$

Proof. By the corollary of Lemma 2, we have

$$\mathrm{Gal}(L'/K') = \{\sigma \in \mathrm{Gal}(L'/\mathbf{Q}) \mid \Phi_L^{-1}\sigma = \Phi_L^{-1}\}.$$

Now $\Phi_L^{-1}\sigma = \Phi_L^{-1}$ is equivalent to $\Phi_L = \sigma\Phi_L$ (by taking the inverse and multiplying by σ), which in turn is equivalent to $\Phi = \sigma\Phi$. □

Example. Let $K = \mathbf{Q}(\alpha)$ be a CM field of degree $2g$, let $\alpha_1 = \alpha, \overline{\alpha_1}, \ldots, \alpha_g, \overline{\alpha_g}$ be the conjugates of α and let $L = \mathbf{Q}(\alpha_i, \overline{\alpha_i} \mid i = 1, \ldots, g)$ be the normal closure of K. We denote $\rho \in G = \mathrm{Gal}(L/\mathbf{Q})$ simply by $\overline{\cdot}$. Let $\sigma \in G$ be any element. By Lemma 1c, we have

$$\sigma(\overline{\alpha_i}) = \overline{\sigma(\alpha_i)}. \qquad (2)$$

We interpret G as a subgroup of the symmetric group S on α_i and $\overline{\alpha_i}$.

Assume that we are in the "generic case", i.e. that G is the set of *all* elements of S that satisfy (2). Note that G contains $g!2^g$ elements: an element is a permutation of the i's, together with 2^g sign choices.

The group $H = \mathrm{Gal}(L/K)$ is the group of those elements that send α_1 to itself, which has $(g-1)!2^{g-1}$ elements, confirming the fact that K has degree $2g$. Consider the CM type $\Phi = \{(\alpha_1 \mapsto \alpha_i)\}$ of K with values in L. Note that Φ is primitive by Lemma 2.

Next, note that $H' = \mathrm{Gal}(L/K') = \{\sigma \in G \mid \sigma\Phi = \Phi\}$ consists of those $\sigma \in G$ such that for every $i \in \{1, \ldots, g\}$, there is a $j \in \{1, \ldots, g\}$ with $\sigma(\alpha_i) = \alpha_j$. This is a group of $g!$ elements, which shows that K' has degree 2^g.

We have thus found a CM field K of degree $2g$ with a primitive CM type Φ such that the reflex field K' has degree 2^g. At the same time, we have found a CM field K' of degree 2^g with a primitive CM type Φ' such that the reflex field K has degree $2g$.

Abelian varieties and CM theory. *Note that if (A, ι) over $\overline{\mathbf{Q}}$ is of type Φ, then for $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, we have that $(\sigma(A), \sigma(\iota))$ is of type Φ if and only if $\sigma\Phi = \Phi$ holds, i.e., if and only if σ fixes the reflex field K'.*

By what we have seen in the talks of David and Jeroen, there is then an isogeny $(A, \iota) \to (\sigma(A), \sigma(\iota))$ over $\overline{\mathbf{Q}}$ and this isogeny is in fact a $\mathfrak{b}$-multiplication for some $\mathfrak{b}$. One of our goals is to compute the ideal class $[\mathfrak{b}] \in \mathcal{CL}_K$ in terms of the ideal class $[\mathfrak{a}] \in \mathcal{CL}_{K'}$ corresponding to $\sigma_{|H_{K'}}$ via the Artin map. We will eventually prove $[\mathfrak{b}] = N_{\Phi'}([\mathfrak{a}])$, where Φ' is the reflex type.

The type norm

Definition. Let Φ be a CM type with values in L'. The *type norm* of Φ is the map

$$\begin{array}{rcl} N_\Phi : K & \to & K' \subset L' \\ x & \mapsto & \displaystyle\prod_{\phi \in \Phi} \phi(x). \end{array}$$

The image of the type norm lies in K' by Lemma 4.

The type norm is multiplicative and hence restricts to a homomorphism of unit groups $K^* \to K'^*$.

For any field M, let I_M denote the group of non-zero fractional ideals of $\mathcal{O}_M$.

Lemma 5. The type norm induces homomorphisms

$$\begin{array}{rcl} N_\Phi : I_K & \to & I_{K'} \\ \mathfrak{a} & \mapsto & \mathfrak{a}' \quad \text{where} \quad \mathfrak{a}'\mathcal{O}_{L'} = \displaystyle\prod_{\phi\in\Phi} \phi(\mathfrak{a})\mathcal{O}_{L'}, \quad \text{and} \\ N_\Phi : \mathcal{CL}_K & \to & \mathcal{CL}_{K'}. \end{array}$$

Proof. It suffices to prove existence of $\mathfrak{a}'$ for $\mathfrak{a} \subset \mathcal{O}_K$. Let

$$\mathfrak{c} = \prod_{\phi\in\Phi} \phi(\mathfrak{a})\mathcal{O}_{L'}.$$

Take $\alpha \in \mathfrak{a}$ and then take $\gamma \in \mathfrak{a}$ such that $\gamma\mathfrak{a}^{-1}$ is coprime to $N_{K/\mathbf{Q}}(\alpha)$. Let $\beta = N_\Phi(\alpha)$, $\delta = N_\Phi(\gamma)$, and $\mathfrak{a}' = \beta\mathcal{O}_{K'} + \delta\mathcal{O}_{K'}$. We have that $\delta\mathfrak{c}^{-1}$ is coprime to β, hence we have

$$\mathfrak{c} = \delta\mathcal{O}_{L'} + \beta\mathcal{O}_{L'} = \mathfrak{a}'\mathcal{O}_{L'}. \qquad \square$$

Since N_Φ sends principal ideals to principal ideals via the original definition, we find an induced map on class groups.

It is easy to see that we have

$$\begin{array}{rcll} N_\Phi(x)\overline{N_\Phi(x)} & = & N_{K/\mathbf{Q}}(x) & \text{for all } x \in K^*, \text{ and} \\ N_\Phi(\mathfrak{a})\overline{N_\Phi(\mathfrak{a})} & = & N_{K/\mathbf{Q}}(\mathfrak{a}) & \text{for all } \mathfrak{a} \in I_K, \end{array}$$

where $N_{K/\mathbf{Q}}$ is the norm, taking positive values in $\mathbf{Q}^*$ and $\bar{\cdot}$ is complex conjugation on K' (which doesn't depend on a choice of complex embedding since K' is a CM field).

The reflex norm

The following lemma is how the reflex field will be used in the proof of "$[\mathfrak{b}] = N_{\Phi'}([\mathfrak{a}])$".

Lemma 6. Let K be a CM field and Φ a CM type with values in L'. Let K' be the reflex field of Φ. Let $\mathfrak{a}$ be a fractional ideal of L'. Then we have

$$\prod_{\phi\in\Phi} \phi^{-1}(N_{L'/\phi K}(\mathfrak{a})) = N_{\Phi'}(N_{L'/K'}(\mathfrak{a})).$$

Proof. Let L/K be isomorphic to L'. Both sides are (after multiplication by $\mathcal{O}_L$) equal to $N_{\Phi_L}(\mathfrak{a})$. For the right hand side, this uses the definition of Φ'. □

Alternative definition of the reflex field

Let K be a CM field and Φ a CM type of K with values in L'. The following lemma gives an alternative definition of the reflex field.

Lemma 7. The reflex field K' is generated over $\mathbf{Q}$ as a subfield of L' by the image of the type norm N_Φ.

Proof. Let M be the field generated by the image of the type norm. The inclusion $M \subset K'$ was shown below the definition of the type norm.

For the inclusion $K' \subset M$, let $h \in \mathrm{Gal}(L'/M)$ be any element and take $x \in K$ such that $K = \mathbf{Q}(x)$. Consider the polynomial

$$f = \prod_{\phi\in\Phi}(X - \phi(x)) \in L'[X].$$

For every $n \in \mathbf{Q}$, we have $f(n) = N_\Phi(n - x) \in K'$, hence we have $f(n) = hf(n)$ for all $n \in \mathbf{Q}$. Since $f(n)$ and $hf(n)$ take the same value for infinitely many $n \in \mathbf{Q}$, we find that the polynomials f and hf are equal, hence have the same set of roots $\{\phi(x) \mid \phi \in \Phi\} = \{h\phi(x) \mid \phi \in \Phi\}$. This shows $\Phi = h\Phi$, so $h \in \mathrm{Gal}(L'/K')$. □