THÉORIE DE LA MULTIPLICATION COMPLEXE

Table des matières

On se propose dans cette quatrième partie du cours d'étudier en détail une certaine classe de problèmes de module de type PEL qui est très remarquable à plus d'un titre :

(1) Les variétés abéliennes que l'on classifie sont distinguées dans la catégorie de toutes les variétés abéliennes par une propriété de maximalité : ce sont les variétés abéliennes de type CM.

(2) Les schémas qui classifient ces variétés abéliennes de type CM sont finis : ce sont les variétés de Shimura de dimension 0.

(3) Les groupes réductifs qui apparaissent dans la description des points complexes de ces variétés sont commutatifs : ce sont des tores.

Dans la cinquième partie du cours, nous verrons que la théorie des variétés de Shimura s'appuie de manière essentielle sur la théorie de la multiplication complexe.

1. Schémas abéliens à multiplications complexe

1.1. Complément sur la caractéristique d'Euler-Poincaré. Soit k un corps, X un schéma propre sur k, $\mathcal{C}(X)$ la catégorie exacte des faisceaux cohérents sur X, $\mathcal{C}_r(X)$ la sous-catégorie pleine épaisse des faisceaux dont le support est de dimension inférieure ou égale à r, $\mathbf{G}(X) = K_0(\mathcal{C}(X))$ le groupe de Grothendieck de $\mathcal{C}(X)$, $\mathbf{G}_r(X) \subset \mathbf{G}(X)$ le sous-groupe image de $K_0(\mathcal{C}_r(X))$, et $\chi : \mathbf{G}(X) \to \mathbb{Z}$ le morphisme de groupe induit par la caractéristique d'Euler-Poincaré. Pour $\mathcal{L} \in \mathrm{Pic}(X)$, on note $[\mathcal{L}] \in \mathrm{Aut}(\mathbf{G}(X))$ l'isomorphisme induit par $\mathcal{F} \mapsto \mathcal{F} \otimes \mathcal{L}$ et $c(\mathcal{L}) \in \mathrm{End}(\mathbf{G}(X))$ le morphisme définit par $c(\mathcal{L}) = \mathrm{Id} - [\mathcal{L}]^{-1}$, qui est induit par $\mathcal{F} \mapsto \mathcal{F} - \mathcal{L}^{-1} \otimes \mathcal{F}$.

Puisque $c(\mathcal{L})\,(\mathbf{G}_r(X)) \subset \mathbf{G}_{r-1}(X)$ pour tout $r \geq 0$ (avec $\mathbf{G}_{-1}(X) = \{0\}$), l'endomorphisme $c(\mathcal{L})$ de $\mathbf{G}(X) = \mathbf{G}_{\dim(X)}(X)$ est nilpotent, donc pour tout $m \in \mathbb{Z}$,

$$[\mathcal{L}]^m = (1 - c(\mathcal{L}))^{-m} = \left(1 + c(\mathcal{L}) + c(\mathcal{L})^2 + \cdots\right)^m = \sum_{i \geq 0} \binom{m+i-1}{i} c(\mathcal{L})^i$$

dans $\mathrm{End}(\mathbf{G}(X))$. Pour $\mathcal{L}_1, \cdots, \mathcal{L}_s$ dans $\mathrm{Pic}(X)$ et $m_1, \cdots, m_s \in \mathbb{Z}$, on a alors

$$[\mathcal{L}_1]^{m_1} \circ \cdots \circ [\mathcal{L}_s]^{m_s} = \sum_{i_1, \cdots, i_s \geq 0} \binom{m_1+i_1-1}{i_1} \cdots \binom{m_s+i_s-1}{i_s} c(\mathcal{L}_1)^{i_1} \cdots c(\mathcal{L}_s)^{i_s}$$

donc pour tout faisceau cohérent $\mathcal{F}$ sur X,

$$\mathcal{X}(\mathcal{F} \otimes \mathcal{L}_1^{m_1} \otimes \cdots \otimes \mathcal{L}_s^{m_s}) = \sum_{i_1, \cdots, i_s \geq 0} a_{i_1, \cdots, i_s}(\mathcal{F}) \binom{m_1+i_1-1}{i_1} \cdots \binom{m_s+i_s-1}{i_s}$$

où $a_{i_1, \cdots, i_s}(\mathcal{F}) = \chi\left(c(\mathcal{L}_1)^{i_1} \circ \cdots \circ c(\mathcal{L}_s)^{i_s}(\mathcal{F})\right) = 0$ si $\max(i_1, \cdots, i_s) > \dim(\mathcal{F})$. C'est une variante du lemme de Snapper, cf [3].

1.2. Compléments sur $\mathrm{Hom}^0_k(A, B)$. Soit k un corps (parfait).

Lemma 1. *La fonction $\phi \mapsto \deg \phi$ sur $\mathrm{End}_k(A)$ s'étend en une fonction*

$$\deg : \mathrm{End}^0_k(A) \to \mathbb{Q}$$

qui est polynomiale de degré $2g$ où $g = \dim A$.

Démonstration. [1, §19, Theorem 2] Puisque $\deg(n\alpha) = n^{2g}\alpha$, il suffit de voir que pour tout α et β dans $\mathrm{End}_k(A)$, la fonction $n \mapsto \deg(n\alpha + \beta)$ est polynomiale. Choisissant un faisceau inversible $\mathcal{L}$ ample sur A, on sait que

$$\chi(\mathcal{L}) \cdot \deg(n\alpha + \beta) = \chi((n\alpha + \beta)^* \mathcal{L}) \quad \text{et} \quad \chi(\mathcal{L}) = \dim_k H^0(A, \mathcal{L}) \neq 0.$$

Posant $\mathcal{L}_n = (n\alpha + \beta)^* \mathcal{L}$, il nous faut donc vérifier que $n \mapsto \chi(\mathcal{L}_n)$ est polynomiale. D'après le théorème du cube appliqué à $(n\alpha + \beta)$, α et $\alpha : A \to A$ (bis),

$$\mathcal{L}_{n+2} \otimes \mathcal{L}_n \otimes \alpha^* \mathcal{L}^2 = \mathcal{L}^2_{n+1} \otimes (2\alpha)^* \mathcal{L}.$$

On en déduit que $\mathcal{L}_n = \mathcal{X}_1^{\frac{n(n-1)}{2}} \otimes \mathcal{X}_2^n \otimes \mathcal{X}_3$ où $\mathcal{X}_1 = (2\alpha)^* \mathcal{L} \otimes \alpha^* \mathcal{L}^{-2} \sim \alpha^* \mathcal{L}^2$, $\mathcal{X}_2 = \mathcal{L}_1 \otimes \mathcal{L}_0^{-1}$ et $\mathcal{X}_3 = \mathcal{L}_0 = \beta^* \mathcal{L}$, donc

$$\chi(\mathcal{L}_n) = \sum_{i,j \geq 0} a_{i,j}(\mathcal{X}_3) \binom{\frac{n(n-1)}{2}+i-1}{i} \binom{n+j-1}{j}$$

avec $a_{i,j}(\mathcal{X}_3) = \chi(c(\mathcal{X}_1)^i \circ c(\mathcal{X}_2)^j (\mathcal{X}_3)) = 0$ si $\max(i,j) \geq g = \dim_k(A)$. $\square$

Corollary 2. *Pour tout sous-groupe M de $\mathrm{Hom}_k(A, B)$ de type fini sur $\mathbb{Z}$, l'intersection N de $\mathbb{Q}M$ et $\mathrm{Hom}_k(A, B)$ dans $\mathrm{Hom}^0_k(A, B)$ est de type fini sur $\mathbb{Z}$.*

Démonstration. On se ramène au cas où $A = B$. La fonction polynomiale $\phi \mapsto \deg \phi$ sur $\mathrm{End}_k^0(A)$ se restreint au $\mathbb{Q}$-espace vectoriel de dimension finie $\mathbb{Q}M$, puis s'étend au $\mathbb{R}$-espace vectoriel $V = \mathbb{Q}M \otimes_{\mathbb{Q}} \mathbb{R}$ en une application polynomiale, donc continue, que l'on note encore $\deg : V \to \mathbb{R}$. L'ensemble $U = \{v \in V : |\deg(v)| < 1\}$ est alors un voisinage ouvert de 0 dans V dont l'intersection avec $N = \mathbb{Q}M \cap \mathrm{End}_k(A)$ est réduite à 0. Donc N est un sous-groupe discret de V. Il est bien connu que de tels sous-groupes sont de type fini sur $\mathbb{Z}$. □

Proposition 3. *Pour tout $\ell \neq \mathrm{car} k$, le morphisme*

$$T_\ell : \mathrm{Hom}_k(A, B) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$$

est injectif.

Démonstration. Il suffit de montrer que pour tout sous-groupe M de $\mathrm{Hom}_k(A, B)$ qui est de type fini sur $\mathbb{Z}$, la restriction de T_ℓ à $M \otimes \mathbb{Z}_\ell$ est injective. On peut supposer d'après le corollaire précédent que M est saturé dans $\mathrm{Hom}_k(A, B)$, i.e. $M = \mathrm{Hom}_k(A, B) \cap \mathbb{Q}M$. Soit $\alpha_1, \cdots, \alpha_r$ une $\mathbb{Z}$-base de M, $\lambda_1, \cdots, \lambda_r \in \mathbb{Z}_\ell$ tels que $T_\ell(\alpha_1 \otimes \lambda_1 + \cdots + \alpha_r \otimes \lambda_r) = 0$, et $n_i(s) \in \mathbb{Z}$ avec $n_i(s) \equiv \lambda_i \bmod \ell^s$. Alors

$$\alpha(s) = n_1(s)\alpha_1 + \cdots + n_r(s)\alpha_r \in \mathrm{Hom}_k(A, B)$$

est nul sur $A[\ell^s]$, donc $\alpha(s) = \ell^s \cdot \beta(s)$ pour un $\beta(s) \in \mathrm{Hom}_k(A, B) \cap \mathbb{Q}M = M$, donc $\ell^s \mid n_i(s)$ pour tout i, donc $\lambda_i \equiv 0 \bmod \ell^s$ pour tout i et tout s, et $\lambda_i = 0$. □

Proposition 4. $\mathrm{Hom}_k(A, B) \simeq \mathbb{Z}^r$ *avec $r \leq 4 \dim A \cdot \dim B$.*

Démonstration. D'après le lemme précédent, $\mathrm{Hom}_k^0(A, B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \hookrightarrow \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell A, V_\ell B)$, donc $\mathrm{Hom}_k^0(A, B)$ est un $\mathbb{Q}$-espace vectoriel de dimension finie $r \leq 4 \dim A \cdot \dim B$. Soit $\alpha_1, \cdots, \alpha_r$ une $\mathbb{Q}$-base de $\mathrm{Hom}_k^0(A, B)$ contenue dans $\mathrm{Hom}_k(A, B)$, M le sous-module de $\mathrm{Hom}_k(A, B)$ engendré sur $\mathbb{Z}$ par cette base. Alors

$$\mathrm{Hom}_k(A, B) = \mathrm{Hom}_k^0(A, B) \cap \mathrm{Hom}_k(A, B) = \mathbb{Q}M \cap \mathrm{Hom}_k(A, B)$$

est encore un $\mathbb{Z}$-module de type fini, donc en fait un $\mathbb{Z}$-module libre de rang r. □

Corollary 5. $\mathrm{End}_k^0(A)$ *est une $\mathbb{Q}$-algèbre semi-simple* de dimension finie $\leq 4g^2$.

1.3. **Schémas abéliens à multiplication complexe.**

Proposition 6. *Soit S un schéma connexe, A un S-schéma abélien de dimension g et $E \subset \mathrm{End}_S^0(A)$ une sous-algèbre commutative réduite. Alors $[E : \mathbb{Q}] \leq 2g$ avec égalité si et seulement si pour un (resp. tout) point géométrique s de S, pour un (resp. tout) $\ell \neq \mathrm{car} s$, le $E \otimes \mathbb{Q}_\ell$-module $V_\ell(A, s)$ est libre de rang* 1.

Démonstration. Par rigidité, $E \subset \mathrm{End}_s^0(A_s)$, donc le $E \otimes \mathbb{Q}_\ell$-module $V_\ell = V_\ell(A, s)$ est fidèle d'après la proposition 3. Décomposons $E \otimes \mathbb{Q}_\ell = \prod E_i$ en produit de corps et $V_\ell = \prod V_i$ en produit de E_i-espaces vectoriels. Alors $\dim_{E_i} V_i > 0$ par fidélité et

$$2g = \dim_{\mathbb{Q}_\ell} V_\ell = \sum \dim_{\mathbb{Q}_\ell} V_i = \sum \dim_{\mathbb{Q}_\ell} E_i \cdot \dim_{E_i} V_i \geq \sum \dim_{\mathbb{Q}_\ell} E_i = [E : \mathbb{Q}]$$

donc $[E : \mathbb{Q}] \leq 2g$ avec égalité si et seulement si $\dim_{E_i} V_i = 1$ pour tout i, i.e. si et seulement si $V_\ell = V_\ell(A, s)$ est un $E \otimes \mathbb{Q}_\ell$-module libre de rang 1. □

Definition 7. On dit que le S-schéma abélien A a de la multiplication complexe s'il existe une sous-algèbre commutative réduite (= un produit de corps) $E \subset \mathrm{End}_S^0(A)$ telle que $[E : \mathbb{Q}] = 2g$, où g est la dimension relative de A sur S. On dit alors aussi que A a multiplication complexe par E.

Remark 8. Si A/S a multiplication complexe par E, alors E est une sous-algèbre commutative maximale de $\mathrm{End}^0_S(A)$. Si ℓ est inversible dans S et si s est un point géométrique de S, l'action de $\pi(S,s)$ sur $V_\ell(A,s)$ est E_ℓ-linéaire, donc donnée par un caractère $\chi_{A,\ell} : \pi(S,s) \to E_\ell^\times$. En particulier, cette action est abélienne.

Definition 9. Soit (A_i, ι_i) deux S-schémas abéliens à multiplication complexe par $\iota_i : E \hookrightarrow \mathrm{End}^0_S A_i$. On note $\mathrm{Hom}^0_S((A_1,\iota_1),(A_2,\iota_2))$ le sous-espace vectoriel de $\mathrm{Hom}^0_S(A_1,A_2)$ formé des éléments E-linéaires, i.e. des f tels que $f\circ\iota_1(e) = \iota_2(e)\circ f$ pour tout E. Une E-isogénie $(A_1,\iota_1) \to (A_2,\iota_2)$ est une isogénie qui est E-linéaire.

Corollary 10. *Si l'ensemble des E-isogénies est non vide, c'est un espace homogène principal sous le groupe multiplicatif $E^\times$ de E.*

Démonstration. L'ensemble des isogénies $(A_1,\iota_1) \to (A_2,\iota_2)$ est l'ensemble des isomorphismes E-linéaires $(A_1,\iota_1) \to (A_2,\iota_2)$ dans une catégorie convenable. C'est donc vide, ou bien un espace homogène principal sous $\mathrm{End}^0_S(A_1,\iota_1)^\times$. Mais l'anneau $\mathrm{End}^0_S(A_1,\iota_1)$ est le commutant de $\iota_1(E)$ dans $\mathrm{End}^0_S(A_1)$, et c'est donc $\iota_1(E)$ puisque $\iota_1(E)$ est une sous-algèbre commutative maximale de $\mathrm{End}^0_S(A_1)$. □

Lemma 11. *Si $A \sim \oplus A_i$ dans $\mathbf{Ab}^0_S$ avec A_i simples, alors A a de la multiplication complexe $\iff$ pour tout i, A_i a de la multiplication complexe.*

Démonstration. On écrit $A \sim \oplus A_i^{n_i}$ où les A_i sont simples et deux à deux non-isogènes. Alors $\mathrm{End}^0_S A = \prod M_{n_i}(D_i)$ où $D_i = \mathrm{End}^0_S A_i$ est un corps gauche. Soit F_i le centre de D_i, $d_i^2 = [D_i : F_i]$, $f_i = [F_i : \mathbb{Q}]$ et $g_i = \dim A_i$. Les $\mathbb{Q}$-sous-algèbres commutatives maximales de D_i sont les F_i-sous-algèbres commutatives maximales de D_i, et elles ont donc une F_i-dimension égale à d_i (d'après le formule du bicommutant) et une $\mathbb{Q}$-dimension égale à $d_i f_i$. Donc $d_i f_i \le 2g_i$ avec égalité si et seulement si A_i a de la multiplication complexe. De même, les $\mathbb{Q}$-sous-algèbres commutatives maximales de $\mathrm{End}^0 A$ sont des produits $E = \prod E_i$ de F_i-sous-algèbres commutatives E_i de $M_{n_i}(D_i)$, lesquelles ont pour F_i-dimension $n_i d_i$ et pour $\mathbb{Q}$-dimension $n_i d_i f_i$. On trouve donc

$$[E:\mathbb{Q}] = \sum_i [E_i : \mathbb{Q}] = \sum_i n_i d_i f_i \le 2\sum_i n_i g_i = 2g$$

avec égalité si et seulement si $d_i f_i = 2g_i$ pour tout i, CQFD. □

Exercise 12. Si $S = \mathrm{Spec} k$ est le spectre d'un corps parfait, et A/k a multiplication complexe par un corps, alors $A \sim A_1^n$ pour une variété abélienne simple A_1 a multiplication complexe par un autre corps.

1.4. **Variétés abéliennes CM et points complexes.** On suppose toujours que S est connexe, et admet un point géométrique $s \in S(\mathbb{C})$. Le cas que l'on a en vue est celui où $S = \mathrm{Spec} k$ pour un sous-corps k de $\mathbb{C}$.

Lemma 13. *Soit A un S-schéma abélien de dimension relative g. On suppose que A est simple, i.e. $E = \mathrm{End}^0_S(A)$ est un corps, et admet de la multiplication complexe, i.e. E contient un corps commutatif C de $\mathbb{Q}$-dimension $2g$. Alors $C = E$ est un corps CM et toute polarisation $\lambda : A \to A^t$ est $(E,\star)$-linéaire, où $\star$ est l'involution canonique de E.*

Démonstration. Sur $\mathbb{C}$, $A_s(\mathbb{C}) = V_{\mathbb{R},I}/\Lambda$ correspond à un couple (polarisable) (Λ, I) où Λ est un réseau de dimension $2g$ et I une structure complexe sur $V_\mathbb{R}$, avec $V = \Lambda \otimes \mathbb{Q}$. On a donc $C \subset E \subset D$, où

$$D = \mathrm{End}^0_\mathbb{C}(A_s) = \{\alpha \in \mathrm{End}_\mathbb{Q}(V) : \alpha_\mathbb{R} \circ I = I \circ \alpha_\mathbb{R}\}$$

est à priori seulement une $\mathbb{Q}$-algèbre semi-simple de dimension finie. Décomposons $D \simeq \prod_i D_i$ et $V \simeq \prod V_i$ avec D_i simple et V_i un D_i-module, de sorte que chacun des V_i est aussi un E-espace vectoriel, qui est non nul puisque V est un D-module fidèle. Alors

$$2g = \dim_\mathbb{Q} V = \sum_i \dim_\mathbb{Q} V_i = [E : \mathbb{Q}] \cdot \sum_i \dim_E V_i = 2g \cdot [E : C] \cdot \sum_i \dim_E V_i.$$

Donc : $E = C$ est commutatif, D est simple, et V est un E-espace vectoriel de dimension 1. Par ailleurs, la structure complexe I induit un morphisme de $\mathbb{R}$-algèbres

$$\mathbb{C} \hookrightarrow \mathrm{End}_{E_\mathbb{R}}(E_\mathbb{R}) = E_\mathbb{R}$$

donc E est totalement imaginaire. Soit enfin $\lambda : A \to A^t$ une polarisation sur S. Alors λ induit une involution de Rosati $\star_E$ sur $E = \mathrm{End}^0_S A$ par la formule $\alpha^{\star_E} = \lambda^{-1}\alpha^t\lambda$, de sorte que $\lambda : A \to A^t$ est $(E, \star_E)$-linéaire par définition. De même, $\lambda_s : A_s \to A_s^t$ induit une involution $\star_D$ sur D, qui bien sûr fixe E et y induit $\star_E$. Mais la polarisation λ_s de A_s correspond à une polarisation $\psi_\mathbb{R}$ de la paire (Λ, I). Puisque $\psi_{\mathbb{R},I} > 0$, l'involution $\star_D$ est positive, donc $\star_E$ aussi. En particulier, le sous-corps F de E fixé par $\star_E$ est totalement réel, donc distinct de E. Mais alors E est un corps CM, F est son sous-corps totalement réel, et $\star_E$ est l'involution canonique de E. □

Corollary 14. *Toute variété abélienne CM sur $k \subset \mathbb{C}$ admet de la multiplication complexe par une $\mathbb{Q}$-algèbre CM.*

Remark 15. Le lemme est faux en caractéristique p : une courbe elliptique supersingulière E sur $k = \overline{\mathbb{F}}_p$ est simple et CM, mais $\mathrm{End}^0_k(E)$ n'est pas commutatif.

Mentionnons également une espèce de réciproque du corollaire ci-dessus :

Lemma 16. *Sur $k = \mathbb{C}$, tout tore complexe X de dimension g sur lequel agit fidèlement un produit de corps* CM *de dimension* $2g$ *est une variété abélienne CM.*

Démonstration. Nous verrons cela plus bas. □

Remark 17. Le lemme est faux si l'on ne suppose pas que E est CM.

1.5. **Propriétés de Bonne Réduction.** Soit S un schéma de Dedekind intègre, ξ le point générique de S, et x un point fermé de S. Soit A une variété abélienne sur ξ. On dit que A a bonne réduction en x si et seulement si A s'étend en un schéma abélien sur $S(x) = \mathrm{Spec}(\mathcal{O}_{S,x})$. En général, partant d'un modèle quelconque $\mathcal{A}$ de la variété A sur S, il existe un ouvert U de S au-dessus duquel $\mathcal{A}$ est un schéma abélien : donc A a bonne réduction en presque tous les points de S (i.e. tous sauf un nombre fini).

Cependant, il existe sur S un modèle qui est meilleur que les autres : le modèle de Néron $\mathcal{A}/S$. C'est un modèle qui est déjà lisse et qui vérifie la propriété universelle suivante : pour tout schéma X qui est lisse sur S, tout ξ-morphisme $X_\xi \to A$ s'étend en un S-morphisme $X \to \mathcal{A}$. En particulier, ce modèle de Néron est uniquement déterminé (à isomorphisme unique près) par cette propriété, et c'est canoniquement un S-schéma en groupes. Si A a bonne réduction en x et si $\mathcal{A}$ est un schéma abélien sur $S(x)$ tel que $\mathcal{A}_\xi = A$, alors $\mathcal{A}$ est le modèle de Néron de A sur $S(x)$. Les points de S où A a bonne réduction sont donc exactement ceux où le modèle de Néron est propre (donc propre et lisse à fibre *générique* géométriquement connexe, ce qui implique que toutes les fibres le sont, comme on voit par exemple en considérant la factorisation de Stein). L'existence du modèle de Néron permet de démontrer le critére suivant :

Proposition 18. *On fixe un point géométrique s au-dessus de ξ. Pour tout point fermé $x \in S$, les conditions suivantes sont équivalentes* (1) *A a bonne réduction en x, et* (2) *pour un (resp. tout) $\ell \neq \mathrm{car}k(x)$, l'action de $\pi(\xi, s)$ sur $T_\ell(A, s)$ est non-ramifiée en x, i.e. se factorise à travers $\pi(S(x), s)$.*

Dans un langage plus familier, cela s'énonce ainsi.

Proposition 19. *Soit R un anneau de valuation discrète de corps résiduel k, K le corps des fractions de R, K^s une clôture séparable de K, $I \subset \mathrm{Gal}(K^s/K)$ le groupe d'inertie d'une place de K^s au-dessus de R. Soit A une variété abélienne sur K. Alors A a bonne réduction sur R si et seulement si I agit trivialement sur $T_\ell(A, K^{sep})$ pour un (resp. tout) $\ell \neq \mathrm{car}k$.*

Démonstration. [2] Soit $\mathcal{A}$ le modèle de Néron de A sur $S = \mathrm{Spec}(R)$, $\widetilde{K}$ le sous-corps de K^s fixé par I, $\widetilde{R}$ l'anneau de sa valuation, $\widetilde{k}$ le corps résiduel de cet anneau. D'après la propriété universelle qui caractérise le modèle de Néron,

$$\mathcal{A}(\widetilde{R}) = \mathcal{A}(\widetilde{K}) = A(\widetilde{K}) = A(K^s)^I.$$

Si $\ell \neq \mathrm{car}k$, la multiplication $\ell : \mathcal{A} \to \mathcal{A}$ est étale (et quasi-finie, mais pas nécessairement propre, i.e. pas nécessairement finie). Donc $\mathcal{A}[\ell^n]$ est étale et $\mathcal{A}[\ell^n](\widetilde{R}) = \mathcal{A}[\ell^n](\widetilde{k})$. Finalement,

$$T_\ell(A, K^s)^I = T_\ell(\mathcal{A}_k, \widetilde{k}) \quad \text{et} \quad V_\ell(A, K^s)^I = V_\ell(\mathcal{A}_k, \widetilde{k})$$

Or $\mathcal{A}_{\widetilde{k}}$ admet une filtration $0 \subset \mathcal{A}^1_{\widetilde{k}} \subset \mathcal{A}^2_{\widetilde{k}} \subset \mathcal{A}^3_{\widetilde{k}} \subset \mathcal{A}_{\widetilde{k}}$ dont les quotients successifs sont respectivement un produit $\mathbb{G}_a^r$ de $\mathbb{G}_a$, un produit $\mathbb{G}_m^s$ de $\mathbb{G}_m$, une variété abélienne de dimension d, et un groupe fini. On a donc $r + s + d = g$ où g est la dimension de A. Chaque étape contribue à la $\mathbb{Q}_\ell$-dimension de $V_\ell(\mathcal{A}_k, \widetilde{k})$ pour respectivement 0, s, et $2d$. Donc I agit trivialement sur $V_\ell(A, K^s)$ si et seulement si $s + 2d = 2g$, i.e. $r = s = 0$, i.e. $\mathcal{A}_{\widetilde{k}}$ est propre, i.e. $\mathcal{A}$ est propre. □

Appliquons tout ceci au cas qui nous intéresse : K est un corps de nombre, $S = \mathrm{Spec}(\mathcal{O}_K)$ où $\mathcal{O}_K$ est l'anneau des entiers de K, et A est une variété abélienne sur K à multiplication complexe par E. On sait alors que l'action de $\mathrm{Gal}(K^s/K)$ sur $V_\ell(A, s)$ se factorise à travers un caractère continu $\chi_{A,\ell} : \mathrm{Gal}(K^{ab}/K) \to \mathcal{O}_{E_\ell}^\times$, où $\mathcal{O}_{E_\ell}$ est l'anneau des entiers de $E_\ell = E \otimes \mathbb{Q}_\ell$. D'autre part, si $I(P) \subset \mathrm{Gal}(K^{ab}/K)$ est le groupe d'inertie en un idéal premier $P \in \mathrm{Spec}(\mathcal{O}_K)$ de caractéristique résiduelle $p \neq \ell$, alors $I(P)$ est une extension d'un groupe fini par un pro-p-groupe. On en déduit facilement que $\chi_{A,\ell}(I(P))$ est fini. Donc : A a bonne réduction potentielle en P, et plus précisément, il existe une extension abélienne finie L de K telle que A_L a bonne réduction au-dessus de P. En travaillant un peu plus, on peut montrer qu'il existe même une extension cyclique finie L de K telle que A_L a bonne réduction *partout,* voir la remarque *49* ci-dessous.

1.6. **Groupes de Mumford-Tate.** Soit $A \simeq V_{\mathbb{R},I}/\Lambda$ une variété abélienne sur $\mathbb{C}$. Le groupe de Mumford-Tate $\mathbf{MT}(A)$ est le plus petit sous-groupe algébrique H de $G = GL(V)$ (sur $\mathbb{Q}$!) tel que le morphisme $h_I : \mathbb{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m \to G_{\mathbb{R}}$ défini par I se factorise par $H_{\mathbb{R}}$. Rappelons que ce morphisme envoie $z \in \mathbb{C}^\times = \mathbb{S}(\mathbb{R})$ sur la multiplication par z dans le $\mathbb{C}$-espace vectoriel $V_{\mathbb{R},I}$. Alors :

Lemma 20. *Pour toute variété abélienne A sur* $\mathbf{C}$,

$$A \text{ est CM} \iff \mathbf{MT}(A) \text{ est un tore.}$$

Démonstration. Si A a de la multiplication complexe par E, V est un E-module libre de rang 1 donc $T_E = \mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_{m,E} = GL_E(V)$ est un $\mathbb{Q}$-tore (maximal!) de $G = GL(V)$. Puisque E commute à l'action de I sur $V_{\mathbb{R}}$, $h_I : \mathbb{S} \to GL_{\mathbb{R}}(V_{\mathbb{R}})$ se factorise par T_E, donc $\mathbf{MT}(A) \subset T_E$ est un tore. Inversement, si $\mathbf{MT}(A) = T$ est un $\mathbb{Q}$-tore dans $G = GL(V)$, alors V est une représentation fidèle de T et l'anneau des endomorphismes de cette représentation contient une $\mathbb{Q}$-sous-algèbre commutative réduite E de $\mathrm{End}(V)$ de $\mathbb{Q}$-dimension $2g = \dim_{\mathbb{Q}} V$. Puisque l'action de E sur $V_{\mathbb{R}}$ commute à celle de I, $E \subset \mathrm{End}^0(A)$ et A a multiplication complexe par E. □

1.7. **Conclusion.** Tout cela suggère que les variétés CM sont très remarquables, qu'il conviendrait de les classifier, et qu'il suffit pour cela (sur $\mathbb{C}$) de classifier les variétés abéliennes à multiplication complexe par un produits de corps CM.

2. La Multiplication Complexe sur $\mathbb{C}$

2.1. **Les $\mathbb{Q}$-algèbres CM.** On note $\tau : \mathbb{C} \to \mathbb{C}$ la conjugaison complexe $\tau(z) = \overline{z}$.

Lemma 21. *Pour un corps de nombre E, les conditions suivantes sont équivalentes :* (1) *Il existe un automorphisme $\tau_E \neq 1$ de E tel que $\iota \circ \tau_E = \tau \circ \iota$ pour tout plongement $\iota : E \hookrightarrow \mathbb{C}$, et* (2)*$E = F(\sqrt{a})$ pour un corps F totalement réel et un élément a totalement négatif.*

Démonstration. Exercice. □

Definition 22. Un corps CM est un corps de nombre qui vérifie les conditions équivalentes ci-dessus. Une $\mathbb{Q}$-algèbre CM est un produit de corps CM.

Remark 23. Les corps CM sont stables par composition, mais un sous-corps d'un corps CM n'est pas forcément CM. La clôture galoisienne d'un corps CM est encore CM. La réunion $\mathbb{Q}^{cm} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ de tous les corps CM est l'extension Galoisienne de $\mathbb{Q}$ qui est fixée par $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Definition 24. Soit E une $\mathbb{Q}$-algèbre CM de dimension $2g$ et S un schéma. Un S-schéma abélien à multiplication complexe par E est une paire (A, ι) où A est un S-schéma abélien de dimension relative g et $\iota : E \hookrightarrow \mathrm{End}^0_S(A)$ une action fidèle de E sur A. Une E-isogénie $\lambda : (A_1, \iota_1) \to (A_2, \iota_2)$ est un isomorphisme E-linéaire $A_1 \to A_2$ dans la catégorie des S-schémas abéliens à isogénie près, i.e. un élément inversible $\lambda \in \mathrm{Hom}^0_S(A_1, A_2)$ tel que $\lambda \circ \iota_1(e) = \iota_2(e) \circ \lambda$ pour tout $e \in E$. On note $\mathrm{Hom}^0_S((A_1, \iota_1), (A_2, \iota_2))$ l'ensemble de ces E-isogénies. En particulier, $\mathrm{End}^0_{E,S}(A, \iota)$ est le commutant de $\iota(E)$ dans $\mathrm{End}^0_S(A)$.

2.2. **Classification sur $\mathbb{C}$.** Soit E une $\mathbb{Q}$-algèbre CM de dimension $2g$. On se propose de décrire l'ensemble $\mathcal{H}(E)$ des classes d'isomorphismes de variétés abéliennes à multiplication complexe par E sur $S = \mathrm{Spec}(\mathbb{C})$. Il revient au même de décrire l'ensemble des classes d'isomorphismes de couples polarisables (Λ, I) où Λ est un réseau dans un E-module fidèle $V = \Lambda \otimes \mathbb{Q}$ de $\mathbb{Q}$-dimension $2g$, et I une structure complexe $E \otimes \mathbb{R}$-linéaire sur $V_{\mathbb{R}}$. La variété abélienne CM associée est alors $A = V_{\mathbb{R},I}/\Lambda$. Dans ce contexte, une E-isogénie $\lambda : (\Lambda_1, I_1) \to (\Lambda_2, I_2)$ est un isomorphisme E-linéaire $V_1 \to V_2$ tel que $\lambda_{\mathbb{R}} : V_{1,\mathbb{R}} \to V_{2,\mathbb{R}}$ est $\mathbb{C}$-linéaire, i.e. $\lambda_{\mathbb{R}} \circ I_1 = I_2 \circ \lambda_{\mathbb{R}}$.

2.2.1. *Le E-module V.*

Lemma 25. *V est un E-module libre de rang 1.*

Démonstration. C'est un E-module fidèle de $\mathbb{Q}$-dimension $2g$. Décomposant $E = \prod E_j$ en produit de corps et $V = \prod V_j$ en produit de E_j-espaces vectoriels non-nuls (puisque V est un E-module fidèle), on obtient

$$2g = \dim_{\mathbb{Q}} V = \sum_j \dim_{\mathbb{Q}} V_j = \sum_j [E_j : \mathbb{Q}] \cdot \dim_{E_j} V_j \geq \sum_j [E_j : \mathbb{Q}] = \dim_{\mathbb{Q}} E = 2g$$

donc $\dim_{E_j} V_j = 1$ pour tout j, ce qu'il fallait démontrer. □

Remark 26. On comparera utilement cette preuve à celle de la proposition 6.

On peut donc supposer que $V = E$.

2.2.2. *La structure complexe I.*

Definition 27. Si E est une $\mathbb{Q}$-algèbre CM, un type CM sur E est un sous-ensemble Φ de $\mathrm{Hom}_{\mathbb{Q}-alg}(E, \mathbb{C})$ tel que $\Phi \coprod \overline{\Phi} = \mathrm{Hom}_{\mathbb{Q}-alg}(E, \mathbb{C})$. Une paire CM est un couple (E, Φ) formé d'une $\mathbb{Q}$-algèbre CM E et d'un type CM Φ sur E.

Lemma 28. *Soit V un E-module libre de rang 1. Il revient au même de se donner* (1) *une structure complexe E-linéaire I sur $V_{\mathbb{R}}$,* (2) *un morphisme de $\mathbb{R}$-algèbre $\iota : \mathbb{C} \to E_{\mathbb{R}}$,* (3) *un type CM Φ sur E. Dans cette correspondance,*

$$(V_{\mathbb{R}}, I) \simeq \oplus_{\phi \in \Phi} \mathbb{C}(\phi) \quad \textit{comme module sur } E \otimes \mathbb{C} = \prod_{\phi \in \mathrm{Hom}_{\mathbb{Q}-alg}(E,\mathbb{C})} \mathbb{C}(\phi).$$

Démonstration. Une structure complexe E-linéaire I sur $V_{\mathbb{R}}$ est un morphisme de $\mathbb{R}$-algèbre $\iota : \mathbb{C} \to \mathrm{End}_{E_{\mathbb{R}}}(V_{\mathbb{R}}) = E_{\mathbb{R}}$ donc (1) $\iff$ (2). Pour le reste, on décompose

$$E = \prod E_j \quad \text{et} \quad E_{j,\mathbb{R}} = \textstyle\prod_{v : F_j \hookrightarrow \mathbb{R}} E_{j,v}$$

où F_j est le sous-corps totalement réel de E_j et $E_{j,v} = E_j \otimes_{F_j,v} \mathbb{R}$. Alors

$$\mathrm{Hom}_{\mathbb{R}-alg}(\mathbb{C}, E_{\mathbb{R}}) = \prod_{j, v : F_j \to \mathbb{R}} \mathrm{Hom}_{\mathbb{R}-alg}(\mathbb{C}, E_{j,v}) = \prod_{j,v} \mathrm{Aut}_{\mathbb{R}-alg}(\mathbb{C}, E_{j,v}).$$

Le choix d'un morphisme de $\mathbb{R}$-algèbre $\mathbb{C} \to E_{\mathbb{R}}$ est donc le choix pour tout j et tout v d'un isomorphisme $E_{j,v} \to \mathbb{C}$, i.e. d'une extension de $v : F_j \hookrightarrow \mathbb{R}$ à $\phi : E_j \hookrightarrow \mathbb{C}$, donc (2) $\iff$ (3). □

Definition 29. La donnée de Shimura associée à (E, Φ) est $(T_E, \{h_{\Phi}\})$ où T_E est le $\mathbb{Q}$-tore $T_E = \mathrm{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E}$ et $h_{\Phi} : \mathbb{S} \to T_{E,\mathbb{R}}$ est le morphisme qui envoie $z \in \mathbb{C}^{\times} = \mathbb{S}(\mathbb{R})$ sur $\iota_{\Phi}(z) \in (E \otimes \mathbb{R})^{\times} = T_{E,\mathbb{R}}(\mathbb{R})$, où $\iota_{\Phi} : \mathbb{C} \to E_{\mathbb{R}}$ est le morphisme de $\mathbb{R}$-algèbre associé à Φ.

2.2.3. *Les polarisations.* Soit F la sous-algèbre de E fixée par l'involution canonique $\star$ de E. C'est donc un produit de corps totalement réels. On note $F^\times_>$ le sous-groupe de $F^\times$ formé des éléments λ qui sont totalement positifs, i.e. tels que $\phi(\lambda) > 0$ pour tout morphisme de $\mathbb{Q}$-algèbre $\phi : F \to \mathbb{R}$. On note $N_{E/F} : E \to F$ la norme définie par $N_{E/F}(x) = x^\star x$, donc $N_{E/F}(E^\times) \subset F^\times_>$.

Soient Φ un type CM sur E, V un E-module libre de rang 1 et I la structure complexe sur $V_\mathbb{R}$ induite par Φ, i.e. I est la multiplication par $I = \iota_\Phi(i) \in (E\otimes\mathbb{R})^\times$. On se propose de décrire l'ensemble $\mathcal{P}(V, I)$ (resp. $\mathcal{P}[V, I]$) des polarisations de (V, I) (resp. des polarisations modulo les automorphismes $E^\times$ de (V, I)). On fixe pour cela un élément $\eta \in E^\times$ tel que

$$\forall\phi \in \Phi : \quad \phi(\eta) \in \mathbb{R}^\times_< i.$$

Exercise 30. L'ensemble de ces éléments est une $F^\times_>$-orbite non-vide dans $E^\times$.

En particulier, $\eta^\star = -\eta$ donc l'ensemble des formes symplectiques $\psi : V\times V \to \mathbb{Q}$ induisant $\star$ sur E est en bijection avec l'ensemble des formes $(E, \star)$-hermitiennes $\Psi : V \times V \to E$ par l'application qui à Ψ associe $\psi(x, y) = \mathrm{Tr}_{E/\mathbb{Q}}(\eta\Psi(x, y))$. Ces formes sont elles-mêmes classifiées par leur discriminant $d(\Psi)$, un élément de $\widehat{H}^0(\{1, \star\}, E^\times) = F^\times/NE^\times$ défini par $d(\Psi) = \Psi(v, v)$ où v est une E-base de V.

Lemma 31. *ψ est une polarisation de (V, I) $\iff d(\Psi) \in F^\times_>/NE^\times$.*

Démonstration. Soit $\phi(\eta) = -\lambda_\phi i$ avec donc $\lambda_\phi > 0$ pour $\phi \in \Phi$. Pour $x, y \in E\otimes\mathbb{R}$,

$$\psi_{\mathbb{R},I}(xv, yv) = \mathrm{Tr}_{E\otimes\mathbb{R}}(\eta Ixy^\star\Psi(v, v)) = \textstyle\sum_{\phi\in\Phi}\lambda_\phi\phi(x)\overline{\phi}(y)\phi(\Psi(v, v))$$

donc $\psi_{\mathbb{R},I} > 0$ si et seulement si $\phi(\Psi(v, v)) > 0$ pour tout $\phi \in \Phi$, i.e. $d(\Psi) \in F^\times_>$. □

Corollary 32. *L'action $(\lambda \cdot \psi)(x, y) = \psi(\lambda x, y)$ fait de $\mathcal{P}(V, I)$ un $F^\times$-espace homogène principal et de $\mathcal{P}[V, I]$ un $F^\times_>/N_{E/F}E^\times$-espace homogène principal.*

2.2.4. *Classifications.* Il résulte de ce qui précède que si $V_{\mathbb{R},I}/\Lambda$ est un tore complexe à multiplication complexe par E, alors $V_{\mathbb{R},I}/\Lambda$ est polarisable, i.e. c'est une variété abélienne. D'autre part, si (A, ι) est une variété abélienne à multiplication complexe par E, le $E\otimes\mathbb{C}$-module $\mathrm{Lie}(A) \simeq V_{\mathbb{R},I}$ est de la forme $\oplus_{\phi\in\Phi}\mathbb{C}(\phi)$ pour un unique type CM Φ de E. On dit alors que (A, ι) est de type CM (E, Φ). Deux variétés abéliennes (A, ι) et (A', ι') sont E-isogènes, i.e. liés par une E-isogénie, si et seulement si elles ont le même type CM.

Definition 33. On note $\mathcal{H}(E, \Phi) \subset \mathcal{H}(E)$ la classe de E-isogénie définie par Φ.

La classe d'isogénie $\mathcal{H}(E, \Phi)$ est en bijection avec l'ensemble des classes de réseaux Λ de V $(= E)$ modulo l'action du groupe des automorphismes $E^\times$ de V, i.e. avec l'ensemble des classes de $E^\times$-homothétie de réseaux Λ de V. La variété abélienne associée à Λ est $A = V_{\mathbb{R},I}/\Lambda$ où I est la structure complexe E-linéaire sur $V_\mathbb{R}$ déterminé par Φ, i.e. I est la multiplication par $I = \iota_\Phi(i) \in (E \otimes \mathbb{R})^\times$.

2.3. Le corps réflexe.

Lemma 34. *Avec les notations ci-dessus, le corps réflexe $E(\Phi)$ de (E, Φ) est*

1. *Le sous-corps de $\mathbb{C}$ fixé par $\{\sigma \in \mathrm{Aut}(\mathbb{C})|\sigma \circ \Phi = \Phi\}$,*
2. *Le sous-corps de $\mathbb{C}$ engendré par $\{\mathrm{Tr}_\Phi(e), e \in E\}$ où $\mathrm{Tr}_\Phi(e) = \sum_{\phi\in\Phi}\phi(e)$,*
3. *Le corps réflexe de la donnée de Shimura $(T_E, \{h_\Phi\})$,*

(4) *Le corps de définition de la représentation* $V(\Phi)_{\mathbb{C}} = \oplus_{\phi\in\Phi}\mathbb{C}(\phi)$ *de* $E\otimes\mathbb{C}$.

Démonstration. On note $E(\Phi)_i$ le sous-corps de $\mathbb{C}$ défini par la condition i. Il est clair que $E(\Phi)_2 \subset E(\Phi)_1$ et inversement $E(\Phi)_1 \subset E(\Phi)_2$ d'après le théorème sur l'indépendance linéaire des caractères. On a $X_\star(T_{E,\mathbf{C}}) = \mathbb{Z}[\mathrm{Hom}(E,\mathbb{C})]$ avec l'action évidente de $\mathrm{Aut}(\mathbb{C})$. Via cet isomorphisme, le caractère $\mu_\Phi : \mathbb{G}_{m,\mathbb{C}} \to T_{E,\mathbb{C}}$ associé à h_Φ est $\sum_{\phi\in\Phi}\phi$, donc $E(\Phi)_1 = E(\Phi)_3$. On a aussi $E(\Phi)_2 \subset E(\Phi)_4$ puisque

$$\forall e\in E: \qquad \mathrm{Tr}_\Phi(e) = \mathrm{Tr}_{\mathbb{C}}(e|V(\Phi)).$$

Soit enfin $k\subset\mathbb{C}$ une extension Galoisienne de $E(\phi)_1$ qui contient $\phi(E)$ pour tout $\phi\in\Phi$. Alors $V(\Phi)_k = \oplus_{\phi\in\Phi}k(\phi)$ est un $E\otimes k$-module et

$$V(\Phi)_{E(\Phi)_1} = \left\{\textstyle\sum_{\phi\in\Phi} w_\phi : \forall\gamma\in\mathrm{Gal}(k/E(\phi)_1),\ \gamma w_\phi = w_{\gamma\phi}\right\}$$

est un modèle sur $E(\phi)_1$ du $E\otimes\mathbb{C}$-module $V(\Phi)$, donc $E(\Phi)_4\subset E(\Phi)_1$. □

Example 35. Si $E = FE_0$ pour une extension quadratique imaginaire E_0 de $\mathbb{Q}$ et $\Phi = \{\phi : E\to\mathbb{C}$ tel que $\phi|E_0 = \phi_0\}$ où $\phi_0 : E_0\to\mathbb{C}$ est un plongement fixé, alors $E(\Phi) = \phi_0(E_0)$.

Exercise 36. Dans le cas général, $E(\Phi)$ est un corps CM.

Definition 37. Soit k un sous-corps de $\mathbb{C}$ et (A,ι) une k-variété abélienne à multiplication complexe par E. Le type CM Φ de (A,ι) est le type CM de $(A,\iota)_{\mathbb{C}}$, i.e. $(A,\iota)_{\mathbb{C}}\in\mathcal{H}(E,\Phi)$.

Fact 38. *Si* (A,ι) *est de type CM* Φ*, le* $E\otimes k$*-module* $(\mathrm{Lie}A)(k)$ *est un modèle sur* k *du* $E\otimes\mathbb{C}$*-module* $(\mathrm{Lie}A)(\mathbb{C})\simeq\oplus_{\phi\in\Phi}\mathbb{C}(\phi)$*, donc* k *contient le corps réflexe* $E(\Phi)$ *de* Φ*. Si de plus* k *contient tous les* $\phi(E)$ *pour* $\phi\in\Phi$*, alors* $(\mathrm{Lie}A)(k)\simeq\oplus_{\phi\in\Phi}k(\phi)$ *comme* $E\otimes k$*-module.*

Remark 39. Si (A_1,ι_1) et (A_2,ι_2) sont deux k-variétés abéliennes à multiplication complexe par E, elles ont le même type CM (E,Φ) si et seulement si elles E-isogènes sur $\mathbb{C}$. Elles sont alors déjà E-isogènes sur la clôture algébrique de k dans $\mathbb{C}$, mais pas forcément E-isogènes sur k. Cependant :

Exercise 40. Si (A_1,ι_1) et (A_2,ι_2) sont E-isogènes sur k, alors

$$\mathrm{Hom}^0_k\left((A_1,\iota_1),(A_2,\iota_2)\right) = \mathrm{Hom}^0_{\mathbb{C}}\left((A_1,\iota_1)_{\mathbb{C}},(A_2,\iota_2)_{\mathbb{C}}\right).$$

En particulier, toute E-isogénie $(A_1,\iota_1)_{\mathbb{C}}\to(A_2,\iota_2)_{\mathbb{C}}$ est déjà définie sur k.

3. Le théorème principal de la multiplication complexe

3.1. **Les $\mathbb{Q}$-tores.** Pour toute $\mathbb{Q}$-algèbre réduite k de dimension finie, on note

$$T_k = \mathrm{Res}_{k/\mathbb{Q}}\mathbb{G}_{m,k}$$

le $\mathbb{Q}$-schéma en groupes dont les points sur une $\mathbb{Q}$-algèbre R sont donnés par

$$T_k(R) = (k\otimes R)^\times.$$

En particulier, $T_k|\overline{\mathbb{Q}}\simeq\prod_{\phi:k\hookrightarrow\Omega}\mathbb{G}_{m,\overline{\mathbb{Q}}}$ et T_k est un tore $\mathbb{Q}$-rationnel avec

$$X^*(T_k)\simeq\mathcal{F}\left(\mathrm{Hom}_{\mathbb{Q}-alg}(k,\overline{\mathbb{Q}}),\mathbb{Z}\right) \quad\text{et}\quad X_*(T_k)\simeq\mathbb{Z}\left[\mathrm{Hom}_{\mathbb{Q}-alg}(k,\overline{\mathbb{Q}})\right]$$

munis des actions évidentes de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Nous rencontrerons dans la suite divers sous-quotients des groupes $T_k(\mathbb{A}_f) = (k\otimes\mathbb{A}_f)^\times = \widehat{k}^\times$. Ces sous-quotients seront toujours munis de la topologie induite par la topologie adélique de $\widehat{k}^\times$.

On fixe dans toute la suite de cette section une paire CM (E, Φ). On note $\star$ l'involution canonique de E et $F = \{\lambda \in E : \lambda^\star = \lambda\}$, qui est un produit de corps totalement réels. On note $F_>^\times$ le sous-groupe de $F^\times$ formé des éléments totalement positifs. La norme $N_{E/F} : E \to F$ et l'inclusion $\mathbb{Q} \hookrightarrow F$ induisent des morphismes

$$N_{E/F} : T_E \to T_F \quad \text{et} \quad \mathbb{G}_{m,\mathbb{Q}} \hookrightarrow T_F.$$

On note T_E^1 le noyau de $N_{E/F}$ et $T_E^0 = N_{E/F}^{-1}(\mathbb{G}_{m,\mathbb{Q}})$, de sorte que $T_E^1 \subset T_E^0 \subset T_E$. On montre facilement que la norme $N_{E/F} : T_E(\mathbb{A}_f) \to T_F(\mathbb{A}_f)$ est un morphisme ouvert, de même que sa restriction $N_{E/F} : T_E^0(\mathbb{A}_f) \to \mathbb{A}_f^\times$. Pour se familiariser un peu avec ces différents groupes, montrons le lemme suivant.

Lemma 41. *Les lignes du diagramme commutatif suivant sont exactes*

$$\begin{array}{ccccccc} 0 & \to & T_E^1(\mathbb{A}_f)/T_E^1(\mathbb{Q}) & \to & T_E^0(\mathbb{A}_f)/T_E^0(\mathbb{Q}) & \xrightarrow{N} & \mathbb{A}_f^\times/\mathbb{Q}_>^\times \\ & & \| & & \downarrow & & \downarrow \\ 0 & \to & T_E^1(\mathbb{A}_f)/T_E^1(\mathbb{Q}) & \to & T_E(\mathbb{A}_f)/T_E(\mathbb{Q}) & \xrightarrow{N} & T_F(\mathbb{A}_f)/F_>^\times \end{array}$$

et les groupes topologiques de la première ligne sont compacts.

Démonstration. L'exactitude à gauche est immédiate. Pour l'exactitude au milieu, il suffit de le démontrer pour la seconde ligne. Soit donc $x \in T_E(\mathbb{A}_f)$ tel que $N(x) = \lambda \in F_>^\times$. Alors λ est un élément de $F^\times$ qui est dans l'image de la norme N_{E_v/F_v} : $E_v^\times \to F_v^\times$ pour toute place v de $\mathbb{Q}$, donc $\lambda = N_{E/F}\mu$ pour un $\mu \in E^\times = T_E(\mathbb{Q})$. Alors $N(x) = N(\mu)$ donc $x = \mu t^1$ avec $t^1 \in T^1(\mathbb{A}_f)$ et $\mu \in T_E(\mathbb{Q})$, ce qu'il fallait démontrer. Dans $T_E(\mathbb{A}_f) = \widehat{E}^\times$, on a

$$T_E^0(\mathbb{Q}) \cap \widehat{\mathcal{O}}_E^\times = \{\lambda \in \mathcal{O}_E^\times : \lambda\lambda^\star \in \mathbb{Q}^\times\} = \{\lambda \in \mathcal{O}_E^\times : \lambda\lambda^\star = 1\}.$$

Soit λ une telle unité. Puisque $[\mathcal{O}_E^\times : \mathcal{O}_F^\times]$ est fini, $\lambda^n \in \mathcal{O}_F^\times$ pour n assez grand, donc $\lambda^{2n} = \lambda^n(\lambda^n)^\star = (\lambda\lambda^\star)^n = 1$ et $\lambda \in \mu(E^\times)$, qui est fini. Donc $T_E^0(\mathbb{Q}) \cap \widehat{\mathcal{O}}_E^\times$ est fini et $T_E^0(\mathbb{Q})$ est discret, donc aussi fermé dans $T_E(\mathbb{A}_f)$. A fortiori, $T_E^1(\mathbb{Q})$ est discret donc aussi fermé dans $T_E^1(\mathbb{A}_f)$. D'après Hilbert 90, le morphisme h : $T_E(\mathbb{A}_f) \to T_E^1(\mathbb{A}_f)$ qui envoie z sur $h(z) = z/z^\star$ est surjectif. On montre facilement que ce morphisme est ouvert, donc $h(\widehat{\mathcal{O}}_E^\times)$ est un sous-groupe ouvert et compact de $T_E^1(\mathbb{A}_f)$. La surjectivité de

$$\operatorname{Pic}(\mathcal{O}_E) = T_E(\mathbb{A}_f)/T_E(\mathbb{Q}) \cdot \widehat{\mathcal{O}}_E^\times \twoheadrightarrow T_E^1(\mathbb{A}_f)/T_E^1(\mathbb{Q}) \cdot h(\widehat{\mathcal{O}}_E^\times)$$

implique par ailleurs que $T_E^1(\mathbb{A}_f)/T_E^1(\mathbb{Q}) \cdot h(\widehat{\mathcal{O}}_E^\times)$ est fini, donc $T_E^1(\mathbb{A}_f)/T_E^1(\mathbb{Q})$ est compact. Puisque tout idéal fractionnaire de $\mathbb{Z}$ est engendré par un élément de $\mathbb{Q}_>^\times$, $\mathbb{A}_f^\times = \widehat{\mathbb{Z}}^\times \times \mathbb{Q}_>^\times$ donc $\mathbb{A}_f^\times/\mathbb{Q}_>^\times$ est compact. Enfin, $T_E^0(\mathbb{A}_f)/T_E^0(\mathbb{Q})$ est compact comme extension séparée de deux groupes compacts. □

3.2. **L'action de** $\operatorname{Aut}(\mathbb{C})$ **sur** $\mathcal{H}(E)$**.** Le groupe $\operatorname{Aut}(\mathbb{C})$ des automorphismes de $\mathbb{C}$ agit sur $\mathcal{H}(\Phi)$ par $\sigma(A, \iota) = (\sigma A, \sigma\iota)$ où

$$\sigma A = (\operatorname{Spec}(\sigma))^* A \quad \text{et} \quad (\sigma\iota)(e) = (\operatorname{Spec}(\sigma))^*(\iota(e))$$

pour tout $e \in E$. Autrement dit, σA et $\sigma\iota(e)$ sont définis par le diagramme cartésien

$$\begin{array}{ccccc} \sigma A & \xrightarrow{(\sigma\iota)(e)} & \sigma A & \to & \operatorname{Spec}(\mathbb{C}) \\ \downarrow & & \downarrow & & \downarrow \\ A & \xrightarrow{\iota(e)} & A & \to & \operatorname{Spec}(\mathbb{C}) \end{array}$$

où la dernière flèche verticale est $\mathrm{Spec}(\sigma)$. C'est bien une action à gauche, puisque

$$(\mathrm{Spec}(\sigma_1\sigma_2))^* = (\mathrm{Spec}(\sigma_2) \circ \mathrm{Spec}(\sigma_1))^* = (\mathrm{Spec}(\sigma_1))^* \circ (\mathrm{Spec}(\sigma_2))^* .$$

L'action de $\mathrm{Aut}(\mathbb{C})$ sur l'ensemble des classes de E-isogénie se décrit aisément.

Lemma 42. *Pour tout $\sigma \in \mathrm{Aut}(\mathbb{C})$,*

$$\sigma \cdot \mathcal{H}(E, \Phi) = \mathcal{H}(E, \sigma\Phi).$$

Démonstration. Soit $(A, \iota) \in \mathcal{H}(E)$. Alors $\mathrm{Lie}(\sigma A) = \mathrm{Lie}(A) \otimes_{\mathbb{C},\sigma} \mathbb{C}$, donc

$$\mathrm{Lie}(A) \simeq \oplus_{\phi\in\Phi}\mathbb{C}(\phi) \quad \Rightarrow \quad \mathrm{Lie}(\sigma A) \simeq \oplus_{\phi\in\Phi}\mathbb{C}(\sigma \circ \phi)$$

comme $E \otimes \mathbb{C}$-module, ce qu'il fallait démontrer. □

3.3. Le morphisme $r_\Phi : \mathrm{Gal}^{ab}_{E(\Phi)} \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)$.

Proposition 43. *Il existe un unique morphisme de groupes topologiques*

$$r_\Phi : \mathrm{Gal}^{ab}_{E(\Phi)} \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)$$

tel que pour tout $(A, \iota) \in \mathcal{H}(E, \Phi)$, pour tout $\sigma \in \mathrm{Aut}(\mathbb{C}/E(\Phi))$ et $\widehat{t} \in T_E(\mathbb{A}_f)$ tel que $r_\Phi(\sigma) = T_E(\mathbb{Q})\widehat{t}$, il existe une E-isogénie $\lambda : (A, \iota) \to \sigma(A, \iota)$ telle que

$$\forall x \in V_f(A, \mathbb{C}) : \qquad \lambda(\widehat{t} \cdot x) = \sigma \cdot x \quad \textit{dans } V_f(\sigma A, \mathbb{C}).$$

Cette isogénie est alors unique.

Démonstration. Soit $(A, \iota) \in \mathcal{H}(E, \Phi)$ et $\sigma \in \mathrm{Aut}(\mathbb{C}/E(\Phi))$ comme dans l'énoncé. Puisque $\sigma(A, \iota) \in \mathcal{H}(E, \Phi)$, il existe une E-isogénie $\lambda : (A, \iota) \to \sigma(A, \iota)$, uniquement déterminée modulo $E^\times = T_E(\mathbb{Q})$. Les deux morphismes $V_f(A, \mathbb{C}) \to V_f(\sigma A, \mathbb{C})$ induits respectivement par σ et λ sont $\widehat{E}$-linéaires, et diffèrent donc d'un élément $\widehat{t} \in \widehat{E}^\times = T_E(\mathbb{A}_f)$ qui est uniquement déterminé par λ, i.e.

$$\forall x \in V_f(A, \mathbb{C}) : \qquad \lambda(\widehat{t} \cdot x) = \sigma \cdot x \quad \text{dans } V_f(\sigma A, \mathbb{C}).$$

On obtient ainsi une application bien définie

$$r_{(A,\iota)} : \mathrm{Aut}(\mathbb{C}/E(\Phi)) \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)$$

qui vérifie la conclusion du lemme pour notre (A, ι) : pour tout $\sigma \in \mathrm{Aut}(\mathbb{C}/E(\Phi))$ et tout $\widehat{t} \in T_E(\mathbb{A}_f)$ tel que $r_{(A,\iota)}(\sigma) = T_E(\mathbb{Q}) \cdot \widehat{t}$, il existe une unique E-isogénie $\lambda : (A, \iota) \to \sigma(A, \iota)$ telle que $\lambda(\widehat{t} \cdot x) = \sigma x$ dans $V_f(\sigma A, \mathbb{C})$ pour tout $x \in V_f(A, \mathbb{C})$. Il s'agit maintenant de vérifier que (1) cette application ne dépend pas du choix de (A, ι) dans $\mathcal{H}(E, \Phi)$, que (2) c'est un morphisme de groupes, que (3) ce morphisme de groupes se factorise par $\mathrm{Gal}(\overline{\mathbb{Q}}/E(\Phi))$, et que (4) le morphisme qui en résulte $r_\Phi : \mathrm{Gal}(\overline{\mathbb{Q}}/E(\Phi)) \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)$ est continu.

Pour (1) : soient (A, ι) et (A', ι') dans $\mathcal{H}(E, \Phi)$ et $\sigma \in \mathrm{Aut}(\mathbb{C}/E(\Phi))$. Choisissons des E-isogénies $\alpha : (A, \iota) \to (A', \iota')$ et $\lambda : (A, \iota) \to \sigma(A, \iota)$. Alors

$$\beta = (\sigma\alpha) \circ \lambda \circ \alpha^{-1} : (A', \iota') \to (A, \iota) \to \sigma(A, \iota) \to \sigma(A', \iota')$$

est une E-isogénie. Soit $\widehat{t} \in T_E(\mathbb{A}_f)$ tel que $\lambda(\widehat{t} \cdot x) = \sigma x$ pour $x \in V_f(A, \mathbb{C})$. Alors

$$\beta(\widehat{t} \cdot y) = \left((\sigma\alpha) \circ \lambda \circ \alpha^{-1}\right)(\widehat{t} \cdot y) = (\sigma\alpha)\left(\lambda(\widehat{t} \cdot \widehat{x})\right) = (\sigma\alpha)(\sigma \cdot \widehat{x}) = \sigma \cdot \alpha(x) = \sigma \cdot y$$

pour tout $x \in V_f(A, \mathbb{C})$ et $y \in V_f(A', \mathbb{C})$ avec $\alpha(x) = y$. Donc

$$r_{(A,\iota)}(\sigma) = T_E(\mathbb{Q}) \cdot \widehat{t} = r_{(A',\iota')}(\sigma)$$

i.e. $r_\Phi = r_{(A,\iota)}$ ne dépend pas du choix de $(A, \iota) \in \mathcal{H}(E, \Phi)$.

Pour (2) : soient (A,ι) dans $\mathcal{H}(E,\Phi)$ et σ_1, $\sigma_2 \in \mathrm{Aut}(\mathbb{C}/E(\Phi))$. Choisissons des E-isogénies $\lambda_i : (A,\iota) \to \sigma_i(A,\iota)$. Soient $\widehat{t}_i \in T_E(\mathbb{A}_f)$ tels que $\lambda_i(\widehat{t}_i \cdot x) = \sigma_i \cdot x$ pour tout $x \in V_f(A,\mathbb{C})$. Alors

$$\beta = (\sigma_1\lambda_2) \circ \lambda_1 : (A,\iota) \to \sigma_1(A,\iota) \to \sigma_1\sigma_2(A,\iota)$$

est une E-isogénie et pour tout $x \in V_f(A,\mathbb{C})$,

$$\beta(\widehat{t}_1\widehat{t}_2 x) = (\sigma_1\lambda_2)\left(\lambda_1\left(\widehat{t}_1(\widehat{t}_2 x)\right)\right) = (\sigma_1\lambda_2)\left(\sigma_1 \cdot (\widehat{t}_2 x)\right) = \sigma_1 \cdot \left(\lambda_2(\widehat{t}_2 x)\right) = \sigma_1\sigma_2 \cdot x.$$

Donc $r_\Phi : \mathrm{Aut}(\mathbb{C}/E(\Phi)) \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)$ est un morphisme de groupes, car

$$r_\Phi(\sigma_1\sigma_2) = T_E(\mathbb{Q})\widehat{t}_1\widehat{t}_2 = T_E(\mathbb{Q})\widehat{t}_1 \cdot T_E(\mathbb{Q})\widehat{t}_2 = r_\Phi(\sigma_1) \cdot r_\Phi(\sigma_2).$$

Pour (3), nous montrerons ultérieurement que $\mathcal{H}(E,\Phi)$ contient un élément (A,ι) défini sur $\overline{\mathbb{Q}}$. Pour tout $\sigma \in \mathrm{Aut}(\mathbb{C}/\overline{\mathbb{Q}})$, on a alors $\sigma(A,\iota) = (A,\iota)$ et $\sigma = \mathrm{Id}$ sur $V_f(A,\mathbb{C})$, donc $\lambda = \mathrm{Id}$ et $\widehat{t} = 1$ donnent $\lambda(\widehat{t} \cdot x) = \sigma \cdot x$ pour tout $x \in V_f(A,\mathbb{C})$, i.e. $r_\Phi(\sigma) = T_E(\mathbb{Q}) \cdot 1$, donc r_Φ se factorise par $r_\Phi : \mathrm{Gal}(\overline{\mathbb{Q}}/E(\Phi)) \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)$.

Pour (4), on note que l'élément ci-dessus est même défini sur un corps de nombre $k \subset \overline{\mathbb{Q}}$, qui contient nécessairement $E(\Phi)$ d'après l'observation faite en 38. On peut supposer que $\mathcal{O}_E = \mathrm{End}_k(A) \cap E$. Pour tout $n \geq 1$, notons $K(n)$ le sous-groupe de $T_E(\mathbb{A}_f)$ formé des éléments $\widehat{t} \in \widehat{\mathcal{O}}_E^\times$ tels que $\widehat{t} \equiv 1 \bmod n$. Soient $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k(A[n]))$ et $\widehat{t} \in T_E(\mathbb{A}_f)$ tel que $\widehat{t}x = \sigma x$ pour tout $x \in V_f(A,\overline{\mathbb{Q}})$. Alors $\widehat{t} \in \widehat{\mathcal{O}}_E^\times$ puisque $\sigma T_f(A,\overline{\mathbb{Q}}) = T_f(A,\overline{\mathbb{Q}})$ et $\widehat{t} \in K(n)$ puisque $\sigma \equiv 1$ sur $T_f(A,\overline{\mathbb{Q}})/nT_f(A,\overline{\mathbb{Q}})$. Donc $r_\Phi^{-1}(T_E(\mathbb{Q}) \cdot K(n))$ contient le sous-groupe ouvert $\mathrm{Gal}(\overline{\mathbb{Q}}/k(A[n]))$ de $\mathrm{Gal}(\overline{\mathbb{Q}}/E(\Phi))$. Puisque les $K(n)$ forment une base de voisinages ouverts de $1 \in T_E(\mathbb{A}_f)$, le morphisme r_Φ est continu. □

Corollary 44. *L'action de* $\mathrm{Aut}(\mathbb{C}/E(\Phi))$ *sur* $\mathcal{H}(E,\Phi)$ *se factorise par*

$$r_\Phi : \mathrm{Gal}_{E(\Phi)}^{ab} \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)$$

et $\sigma[V_{\mathbb{R},I}/\Lambda] = [V_{\mathbb{R},I}/\Lambda']$ *pour* $\Lambda' \in r_\Phi(\sigma) \cdot \Lambda$.

Démonstration. Si $r_\Phi(\sigma) = T_E(\mathbb{Q})\widehat{t}$ et $(A,\iota) \simeq V_{\mathbb{R},I}/\Lambda$, il existe une E-isogénie $\lambda : (A,\iota) \to \sigma(A,\iota)$ telle que $\lambda(\widehat{t} \cdot x) = \sigma \cdot x$ pour tout $x \in V_f(A,\mathbb{C})$. Soit $(A',\iota') = V_{\mathbb{R},I}/\widehat{t} \cdot \Lambda$ et $\lambda_0 : V_{\mathbb{R},I}/\widehat{t} \cdot \Lambda \to V_{\mathbb{R},I}/\Lambda$ la E-isogénie qui correspond à l'identité de V. Alors λ_0 identifie $T_f(A',\iota')$ et $\widehat{t} \cdot T_f(A,\iota)$, donc

$$\lambda \circ \lambda_0 \left(T_f(A',\iota')\right) = \lambda\left(\widehat{t} \cdot T_f(A,\iota)\right) = \sigma T_f(A,\iota) = T_f(\sigma A, \sigma\iota)$$

donc $\lambda \circ \lambda_0 : V_{\mathbb{R},I}/\widehat{t} \cdot \Lambda \to \sigma(A,\iota)$ est un isomorphisme de variété abélienne à multiplication complexe par E, ce qu'il fallait démontrer. □

3.4. **La théorie du corps de classe.** Pour tout corps de nombres k, il existe un morphisme surjectif

$$\mathrm{Art}_k : T_k(\mathbb{Q})\backslash T_k(\mathbb{A}) \to \mathrm{Gal}_k^{ab}$$

tel que pour toute extension abélienne finie K/k, pour tout premier $\mathfrak{p}$ de k qui est non-ramifié dans K, si $s_\mathfrak{p} \in T_k(\mathbb{A}) = (k \otimes \mathbb{A})^\times = \prod' k_v^\times$ est l'idèle qui vaut 1 en $v \nmid p$ et une uniformisante en $v = v_\mathfrak{p}$, alors

$$\mathrm{Art}_k(s_\mathfrak{p}) = \mathrm{Frob}_\mathfrak{p}^{-1} \quad \text{dans } \mathrm{Gal}(K/k).$$

Le noyau de Art_k est la composante connexe de $1 \in T_k(\mathbb{Q})\backslash T_k(\mathbb{A})$. Si k est totalement imaginaire, ce noyau contient donc $T_k(\mathbb{R})$ et Art_k se factorise en

$$\mathrm{Art}_k : \overline{T_k(\mathbb{Q})}\backslash T_k(\mathbb{A}_f) \xrightarrow{\sim} \mathrm{Gal}_k^{ab}.$$

C'est le cas de tous les corps de nombres qui contiennent $E(\Phi)$. Le théorème principal de la multiplication complexe décrit le morphisme

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} : T_{E(\Phi)}(\mathbb{Q})\backslash T_{E(\Phi)}(\mathbb{A}_f) \to \mathrm{Gal}^{ab}_{E(\Phi)} \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f).$$

3.5. **La norme réflexe $N_\Phi : T_{E(\Phi)} \to T_E$.**

3.5.1. *Le morphisme algébrique.* Soit $k \subset \mathbb{C}$ un corps de nombre tel que

$$V(\Phi)_\mathbb{C} = \oplus_{\phi\in\Phi}\mathbb{C}(\phi)$$

admette un modèle $V(\Phi)_k$ sur k (donc $E(\Phi) \subset k$). Ce modèle est alors unique à isomorphisme près, et se décompose comme $E = \prod E_j$ en $V(\Phi)_k = \prod V(\Phi)^j_k$. Chacun des $V(\Phi)^j_k$ est un $E_j \otimes k$-module. Pour toute $\mathbb{Q}$-algèbre R, on peut donc considérer $V(\Phi)^j_k \otimes R$ comme un $E_j \otimes R$-module libre, et prendre sur ce module le déterminant des éléments de $(k \otimes R)^\times = T_k(R)$: on obtient ainsi un morphisme

$$N_{\Phi,k} : T_k \to \prod T_{E_j} = T_E$$

de $\mathbb{Q}$-tores. Si k contient tous les $\phi(E)$ pour $\phi \in \Phi$, alors

$$N_{\Phi,k}(\lambda) = \prod_{\phi\in\Phi} \phi^{-1}(N_{k/\phi(E)}\lambda).$$

Pour $k = E(\Phi)$, on note simplement $N_\Phi = N_{\Phi,E(\Phi)}$. C'est un morphisme

$$N_\Phi : T_{E(\Phi)} \to T_E.$$

On vérifie que $N_{\Phi,k} = N_\Phi \circ N_{k/E(\phi)}$ où $N_{k/E(\phi)} : T_k \to T_{E(\phi)}$ est la norme usuelle.

3.5.2. *Le morphisme adélique.* La norme réflexe $N_{\Phi,k}$ induit un morphisme

$$N_{\Phi,k} : T_k(\mathbb{A}_f) = \widehat{k}^\times \to T_E(\mathbb{A}_f) = \widehat{E}^\times$$

dont on vérifie qu'il envoie $\widehat{\mathcal{O}}^\times_k$ dans $\widehat{\mathcal{O}}^\times_E$. On obtient donc

$$N_{\Phi,k} : I(k) \to I(E)$$

où $I(k) = \widehat{k}^\times/\widehat{\mathcal{O}}^\times_k$ est le groupe des idéaux fractionaires de k (et idem pour E) qui vérifie à nouveau $N_{\Phi,k} = N_\Phi \circ N_{k/E(\Phi)}$. En particulier, si $\mathcal{I}$ est un idéal fractionnaire de $E(\phi)$, k une extension de $E(\phi)$ qui contient tous les $\phi(E)$ pour $\phi \in \Phi$, et si $\mathcal{O}_k\mathcal{I}$ est l'idéal fractionnaire de k induit par $\mathcal{I}$, alors

$$N_\Phi(\mathcal{I})^{[k:E(\Phi)]} = N_{\Phi,k}(\mathcal{O}_k\mathcal{I}) = \prod_{\phi\in\Phi} \phi^{-1}(N_{k/\phi(E)}(\mathcal{O}_k\mathcal{I})).$$

3.5.3. *Le morphisme $N_\Phi \cdot N^\star_\Phi : T_{E(\Phi)} \to T_E$.* On peut calculer le morphisme

$$N_{E/F} \circ N_\Phi = N_\Phi \cdot N^\star_\Phi : T_{E(\Phi)} \to T_E.$$

Puisque

$$V(\Phi) \oplus V(\Phi)^\star \simeq \oplus_{\phi:E\hookrightarrow\mathbb{C}}\mathbb{C}(\phi) \simeq E \otimes \mathbb{C}$$

comme $E \otimes \mathbb{C}$-module, pour toute $\mathbb{Q}$-algèbre R et tout $\lambda \in (E(\Phi) \otimes R)^\times$,

$$(N_\Phi \cdot N^\star_\Phi)(\lambda) = \det_{E\otimes R}(\lambda|E(\Phi) \otimes E \otimes R) = N_{E(\Phi)/\mathbb{Q}}(\lambda)$$

où $N_{E(\Phi)/\mathbb{Q}} : T_{E(\Phi)} \to T_\mathbb{Q} = \mathbb{G}_{m,\mathbb{Q}}$ est induit par la norme. En particulier,

$$N_\Phi : T_{E(\Phi)} \to T^0_E \subset T_E.$$

3.6. Le théorème principal de la multiplication complexe.

Theorem 45. *Avec les notations ci-dessus,*

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} = N_\Phi \quad : \quad T_{E(\Phi)}(\mathbb{Q})\backslash T_E(\mathbb{A}_f) \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f).$$

Corollary 46. *Pour tout* $(A,\iota) \in \mathcal{H}(E,\Phi)$, $\sigma \in \mathrm{Aut}(\mathbb{C}/E(\Phi))$ *et* $s \in T_{E(\Phi)}(\mathbb{A}_f)$ *tel que* $\mathrm{Art}_{E(\Phi)}(s) = \sigma | E(\Phi)^{ab}$, *il existe une unique* E*-isogénie* $\lambda : (A,\iota) \to \sigma(A,\iota)$ *telle que*

$$\forall x \in V_f(A,\mathbb{C}) : \qquad \lambda(N_\Phi(s)\cdot x) = \sigma x \quad \textit{dans } V_f(\sigma A, \mathbb{C}).$$

Démonstration. C'est immédiat. □

Corollary 47. *Avec ces notations, pour toute polarisation* $\alpha : A \to A^t$ *qui est* $(E,\star)$*-linéaire, l'isogénie* $\lambda : (A,\iota) \to \sigma(A,\iota)$ *envoie* $\mathbb{Q}\alpha$ *sur* $\mathbb{Q}\sigma\alpha$.

Démonstration. Pour tout $x, y \in V_f(A,\mathbb{C})$,

$$\langle x,y\rangle_f^{\lambda^t\circ\sigma\alpha\circ\lambda} = \left\langle x, \lambda^t\circ\sigma\alpha\circ\lambda(y)\right\rangle_f^A = \langle \lambda(x), \sigma\alpha\circ\lambda(y)\rangle_f^{\sigma A} = \langle\lambda(x),\lambda(y)\rangle_f^{\sigma\alpha}$$

donc si $\widehat{t} = N_\Phi(s)$,

$$\left\langle \widehat{t}x, \widehat{t}y\right\rangle_f^{\lambda^t\circ\sigma\alpha\circ\lambda} = \left\langle \lambda(\widehat{t}x), \lambda(\widehat{t}y)\right\rangle_f^{\sigma\alpha} = \langle \sigma\cdot x, \sigma\cdot y)\rangle_f^{\sigma\alpha} = \chi_{cyl}(\sigma)\cdot\langle x,y\rangle_f^{\alpha}.$$

Mais la théorie du corps de classe fournit un $c \in \mathbb{Q}_>^\times$ tel que

$$\chi_{cyc}(\sigma) = \chi_{cyc}\circ\mathrm{Art}_{E(\Phi)}(s) = c\cdot N_{E(\Phi)/\mathbb{Q}}(s) = c\cdot N_\Phi(s)\cdot N_\Phi(s)^\star = c\cdot\widehat{tt^\star}$$

Puisque $\left\langle \widehat{t}x, \widehat{t}y\right\rangle_f^{\lambda^t\circ\sigma\alpha\circ\lambda} = \left\langle x, \widehat{t}^\star\widehat{t}y\right\rangle_f^{\lambda^t\circ\sigma\alpha\circ\lambda} = c^{-1}\chi_{cyc}(\sigma)\,\langle x,y\rangle_f^{\lambda^t\circ\sigma\alpha\circ\lambda}$, on obtient

$$\forall x,y \in V_f(A,\mathbb{C}) : \qquad \langle x,y\rangle_f^{\lambda^t\circ\sigma\alpha\circ\lambda} = c\,\langle x,y\rangle_f^\alpha = \langle x,y\rangle_f^{c\alpha}$$

donc $c\alpha = \lambda^*(\sigma\alpha)$, ce qu'il fallait démontrer. □

Corollary 48. *Soit* $(A,\iota) \in \mathcal{H}(E,\Phi)$ *défini sur un corps de nombre* $k \subset \overline{\mathbb{Q}}$ *et*

$$\chi_A : \mathrm{Gal}_k^{ab} \to \widehat{E}^\times = T_E(\mathbb{A}_f)$$

le caractère qui donne l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ *sur* $V_f(A,\overline{\mathbb{Q}})$, *i.e.*

$$\forall x \in V_f(A,\overline{\mathbb{Q}}) \textit{ et } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/k) : \qquad \sigma\cdot x = \chi_A(\sigma)\cdot x \quad \textit{dans } V_f(A,\overline{\mathbb{Q}}).$$

Alors : il existe un (unique) caractère $\epsilon_k : T_k(\mathbb{A}_f) \to E^\times$ *tel que*

$$\chi_A\circ\mathrm{Art}_k = \epsilon_k\cdot N_{\Phi,k} \quad : \quad T_k(\mathbb{A}_f) \to T_E(\mathbb{A}_f).$$

Démonstration. D'après le théorème, pour tout $s \in T_k(\mathbb{A}_f)$ donnant $s' = N_{k/E(\Phi)}(s)$ dans $T_{E(\Phi)}(\mathbb{A}_f)$ et $\sigma' = \mathrm{Art}_{E(\Phi}(s')$ dans $\mathrm{Gal}_{E(\Phi)}^{ab}$ relevé en $\widetilde{\sigma}'$ dans $\mathrm{Gal}(\overline{\mathbb{Q}}/E(\Phi))$, il existe une unique E-isogénie $\lambda : (A,\iota) \to \widetilde{\sigma}'(A,\iota)$ telle que

$$\forall x \in V_f(A,\overline{\mathbb{Q}}) : \qquad \lambda(N_\Phi(s')\cdot x) = \widetilde{\sigma}'\cdot x.$$

Mais $\sigma' = \sigma|E(\Phi)^{ab}$ où $\sigma = \mathrm{Art}_k(s)$. Si l'on choisit $\widetilde{\sigma}'$ tel que $\widetilde{\sigma}'|k^{ab} = \sigma$, on a donc $\widetilde{\sigma}'(A,\iota) = (A,\iota)$, i.e. $\lambda : (A,\iota) \to (A,\iota)$ est un élément $\lambda(s) \in E^\times$, et

$$\forall x \in V_f(A,\overline{\mathbb{Q}}) : \qquad \lambda(s)N_\Phi(s')\cdot x = \chi_A(\sigma)\cdot x$$

i.e. $\chi_A\circ\mathrm{Art}_k(s) = \lambda(s)\cdot N_{\Phi,k}(s)$. Alors $s \mapsto \lambda(s)$ est le caractère recherché. □

Remark 49. Si K est une extension finie de k, $\epsilon_K = \epsilon_k \circ N_{K/k}$. D'autre part, puisque χ_A et N_Φ sont continus et atterrissent dans $T_E^0(\mathbb{A}_f)$, ϵ_k atterrit en fait dans $T_E^0(\mathbb{Q}) \subset E^\times$, et est un morphisme continu si l'on met sur $T_E^0(\mathbb{Q})$ la topologie induite par celle de $T_E^0(\mathbb{A}_f)$, i.e. la topologie discrète (c.f. la preuve du lemme 41). En particulier, $\epsilon_k(\widehat{\mathcal{O}}_k^\times)$ est un sous-groupe fini de $E^\times$, donc de $\mu(E^\times)$. D'après la théorie du corps de classe, on peut donc bricoler une extension cyclique K de k, de degré divisant l'ordre de $\mu(E^\times)$, telle que $\epsilon_K(\widehat{\mathcal{O}}_K^\times) = 1$. Mais alors pour tout nombre premier p,

$$\chi_A \circ \mathrm{Art}_K(\mathcal{O}_{K,p}^\times) = N_{K,\Phi}(\mathcal{O}_{K,p}^\times) \subset T_E(\mathbb{Q}_p) \subset T_E(\mathbb{A}_f)$$

et en particulier $\mathrm{Art}_K(\mathcal{O}_{K,p}^\times)$ agit trivialement sur $V_\ell(A, \overline{\mathbb{Q}})$ pour tout $\ell \neq p$, donc A_K a bonne réduction partout.

4. La preuve du Théorème Principal

4.1. **Le formalisme des "$\mathfrak{a}$-transforms".**

4.1.1. *Généralités.* Soit $\mathcal{O}$ un anneau noethérien et A un S-schéma abélien muni d'une action de $\mathcal{O}$. Pour tout $\mathcal{O}$-module M de type fini, on note

$$A^M : (\mathbf{Sch}/S)^0 \to \mathbf{Ab} \qquad A^M(T) = \mathrm{Hom}_{\mathcal{O}}(M, A(T)) .$$

Cette construction est compatible au changement de base sur S, covariante en A, contravariante en M et exacte d'un côté : si

$$M_1 \to M_2 \to M_3 \to 0$$

est une suite exacte de $\mathcal{O}$-module, alors la suite de préfaisceau abélien

$$0 \to A^{M_3} \to A^{M_2} \to A^{M_1}$$

est exacte. En particulier, A^{M_3} est représentable si A^{M_2} et A^{M_1} le sont, donc A^M est représentable pour tout M (de type fini) puisque $A^M \simeq A^n$ l'est pour $M = \mathcal{O}^n$. On obtient ainsi un foncteur contravariant $M \mapsto A^M$ de la catégorie des $\mathcal{O}$-modules de type fini dans celle des S-schémas en groupes commutatifs. Puisque A est propre sur S, tous les A^M le sont aussi. De plus :

Exercise 50. Si M est un $\mathcal{O}$-module projectif, alors A^M est un S-schéma abélien.

4.1.2. *Le cas CM.*

Lemma 51. *Soit A un S-schéma abélien à multiplication complexe par l'anneau des entiers $\mathcal{O}_E$ d'une $\mathbb{Q}$-algèbre réduite E, i.e. $\mathcal{O}_E \subset \mathrm{End}_S(A)$ et $\dim_{\mathbb{Q}} E = 2\dim_S A$. Alors pour tout idéal inversible I de $\mathcal{O}_E$, l'inclusion $I \hookrightarrow \mathcal{O}_E$ induit une isogénie $\alpha_A^I : A \to A^I$ de degré $[\mathcal{O}_E : I]$.*

Démonstration. On suppose pour simplifier que E est un corps. Tout idéal non nul est alors inversible, donc projectif, et A^I est un S-schéma abélien de même dimension que A, comme on voit par exemple en calculant un module de Tate. Le noyau de $\alpha_A^I : A \to A^I$ est $A^{\mathcal{O}/I} = A[I]$, qui est fini, donc α_A^I est une isogénie (en particulier, elle est surjective : il résulte alors du critère de Baer que pour tout point géométrique s de S, $A(s)$ est un $\mathcal{O}$-module injectif). Pour $I = (\lambda)$ principal, $A[I] = \ker \lambda$ donc

$$\deg \alpha_A^I = \deg \lambda = \mathrm{nr}\lambda = [\mathcal{O}_E : I].$$

On le vérifie en effet directement pour $\alpha = [n]$, puis pour tout α en utilisant le fait que les deux fonctions deg et nr sur $\mathrm{End}^0_s(A_s)$ sont polynomiales, voir plus bas. Pour $I = I_1 I_2$ le produit de deux idéaux, on a

$$(\alpha_A^{I_1 I_2} : A \to A^{I_1 I_2}) = (\alpha^{I_2}_{A^{I_1}} \circ \alpha^{I_1}_A A \to A^{I_1} \to (A^{I_1})^{I_2})$$

et $A^{I_1}[I_2] \simeq A[I_2]$, donc $I \mapsto \deg \alpha_A^I$ est une fonction multiplicative sur l'ensemble des idéaux. On conclut en utilisant la finitude de $\mathrm{Pic}(\mathcal{O})$. □

Remark 52. Lorsque S est connexe et admet un point complexe $s \in S(\mathbb{C})$, on peut vérifier la formule $\deg \alpha_A^I = [\mathcal{O}_E : I]$ directement sur les points complexes. En effet, si $A_s(\mathbb{C}) \simeq V_{\mathbb{R},I}/\Lambda$, alors Λ est un $\mathcal{O}_E$-réseau dans $V = \Lambda \otimes E$. On montre comme dans le cas CM que V est un E-module libre de rang 1, donc Λ un $\mathcal{O}_E$-module inversible, et on vérifie facilement que $A_s^I(\mathbb{C}) \simeq V_{\mathbb{R},I}/I^{-1}\Lambda$. Donc $A_s[I](\mathbb{C}) \simeq I^{-1}\Lambda/\Lambda \simeq \mathcal{O}_E/I$ comme $\mathcal{O}_E$-module.

4.2. **La formule de Giraud.**

4.2.1. *Préliminaires sur les algèbres de Lie.* Soit $k = \mathbb{F}_q$, $\alpha : A \to B$ un morphisme entre deux variétés abéliennes, $\alpha_0^{\#} : \mathcal{O}_{B,0} \to \mathcal{O}_{A,0}$ le morphisme déduit de α entre les anneaux locaux de B en $\alpha(0) = 0$ et A en 0. C'est un morphisme de k-algèbres locales régulières augmentées qui permet de retrouver le morphisme induit par α sur les espaces cotangents en 0, $\alpha_0^{\#} : \mathcal{I}_{B,0}/\mathcal{I}^2_{B,0} \to \mathcal{I}_{A,0}/\mathcal{I}^2_{A,0}$, et donc aussi le morphisme $\mathrm{Lie}\alpha : \mathrm{Lie}A \to \mathrm{Lie}B$, qui est le dual du précédent. Ce morphisme induit aussi un morphisme entre les complétions de ces deux k-algèbres en leur idéal d'augmentation : $\alpha_0^{\#} : \widehat{\mathcal{O}}_{B,0} \to \widehat{\mathcal{O}}_{A,0}$. Le choix d'une k-base $y_1, \cdots, y_{g'}$ de $\mathcal{I}_{B,0}/\mathcal{I}^2_{B,0}$ (resp. $(x_1, \cdots, x_g)$ de $\mathcal{I}_{A,0}/\mathcal{I}^2_{A,0}$), où $g = \dim A$ et $g' = \dim B$ fournit des identifications de ces k-algèbres augmentées complètes avec des algèbres de séries formelles,

$$\alpha_0^{\#} : k[[y_1, \cdots, y_{g'}]] \to k[[x_1, \cdots, x_g]].$$

Si α est une isogénie, $\alpha_0^{\#}$ est un morphisme fidèlement plat et fini, qui fait donc de $\mathcal{O}_{A,0}$ une $\mathcal{O}_{B,0}$-algèbre qui est un $\mathcal{O}_{B,0}$-module libre de rang fini. L'anneau local en 0 du k-schéma en groupe fini $\ker \alpha$ est alors

$$\begin{aligned} \mathcal{O}_{\ker \alpha, 0} &= \mathcal{O}_{A,0}/\alpha_0^{\#}(\mathcal{I}_{B,0})\mathcal{O}_{A,0} \\ &= \widehat{\mathcal{O}}_{A,0}/\alpha_0^{\#}(\mathcal{I}_{B,0})\widehat{\mathcal{O}}_{A,0} \\ &= k[[x_1, \cdots, x_g]]/(\alpha_0^{\#}(y_1), \cdots \alpha_0^{\#}(y_{g'})). \end{aligned}$$

Prenons pour α le Frobénius $\pi : A \to A$. Alors

$$\alpha_0^{\#} : k[[x_1, \cdots, x_g]] \to k[[x_1, \cdots, x_g]] \qquad x_i \mapsto x_i^q$$

Puisque $(\ker \pi)(k^{alg}) = 0$, le k-schéma fini $\ker \pi$ est local, et c'est le Spec de

$$\mathcal{O}_{\ker \pi, 0} = k[[x_1, \cdots, x_g]]/(x_1^q, \cdots, x_g^q) = k[x_1, \cdots, x_g]/(x_1^q, \cdots, x_g^q).$$

On en déduit que

$$\mathrm{rang}(\ker \pi) = q^g = |\mathrm{Lie}(\ker \pi)| = |\mathrm{Lie}(A)|.$$

Prenons ensuite pour $\alpha : A \to B$ un morphisme qui factorise π, i.e. $\ker \alpha \subset \ker \pi$. Choisissons les bases $(y_1, \cdots, y_g)$ et $(x_1, \cdots, x_g)$ des espaces cotangents de sorte que $y_j \mapsto x_{g-j}$ pour $j \leq g - s$ et $y_j \mapsto 0$ pour $j > g - s$, donc s est la dimension du conoyau du morphisme cotangent, c'est-à-dire la dimension du noyau $\mathrm{Lie}(\ker\alpha)$ de $\alpha : \mathrm{Lie}A \to \mathrm{Lie}B$. D'autre part,

$$\mathcal{O}_{\ker\alpha,0} = k[x_1, \cdots, x_g]/I$$

pour un idéal $(x_1^q, \cdots, x_g^q) \subset I \subset (x_1, \cdots, x_g)$ contenant $x_{g-s+1}, \cdots, x_g$, donc $\mathcal{O}_{\ker\alpha,0}$ est un quotient de l'anneau $k[x_1, \cdots, x_s]/(x_1^q, \cdots, x_s^q)$, donc

$$\mathrm{rang}(\ker\alpha) \leq q^s = |\mathrm{Lie}(\ker\alpha)|.$$

On en déduit que

Lemma 53. *Pour tout sous-schéma en groupe K de $\ker\pi$,*

$$\mathrm{rang}K \leq |\mathrm{Lie}(K)|.$$

4.2.2. *La formule de Giraud.* Soit $k = \mathbb{F}_q$ un corps fini et A/k une variété abélienne à multiplication complexe par l'anneau des entiers $\mathcal{O}_E$ d'une $\mathbb{Q}$-algèbre réduite E, i.e. $\mathcal{O}_E \subset \mathrm{End}_k A$. Soit $\pi : A \to A$ le Frobenius. C'est une isogénie inséparable de degré q^g qui commute à tout le monde, qui est donc dans le commutant de $\mathcal{O}_E$ dans $\mathrm{End}_k A$, c'est-à-dire dans $\mathcal{O}_E$. Soit $(\pi) = P_1^{n_1} \cdots P_r^{n_r}$ la décomposition de l'idéal principal engendré par π dans $\mathcal{O}_E$ en produit d'idéaux premiers, avec $P_i \neq P_j$. Puisque $\pi = 0$ sur le $\mathcal{O}_E \otimes k$-module $\mathrm{Lie}A$,

$$\mathrm{Lie}A = \mathrm{Lie}A[P_1^{n_1}] \times \cdots \times \mathrm{Lie}A[P_r^{n_r}].$$

D'après le lemme 53,

$$q^g = |\mathrm{Lie}A| = \textstyle\prod_j \left|\mathrm{Lie}A[P_j^{n_j}]\right| \geq \prod_j \deg A[P_j^{n_j}] = \deg\pi = q^g$$

donc $\left|\mathrm{Lie}A[P_j^{n_j}]\right| = \deg A[P_j^{n_j}] = \left|\mathcal{O}_E/P_j^{n_j}\right|$. On en déduit la formule de Giraud :

Proposition 54. $[\mathrm{Lie}A] = [\mathcal{O}_E/(\pi)]$ *dans le groupe de Grothendieck $K_0(\mathcal{O}_E)$.*

4.3. **La formule de Shimura-Taniyama.**

Proposition 55. *Soit A une variété abélienne de type CM (E, Φ) sur un corps de nombres k contenu dans $\mathbb{C}$. On suppose que k contient $\phi(E)$ pour tout $\phi \in \Phi$ et que $\mathcal{O}_E \subset \mathrm{End}_k(A)$ où $\mathcal{O}_E$ est l'anneau des entiers de E. Soit P un idéal premier de $\mathcal{O}_k$ où A a bonne réduction. Alors le Frobenius de la réduction $\overline{A}$ de A sur $k(P)$ se relève en un endomorphisme π de $\mathcal{O}_E \subset \mathrm{End}_k(A)$, et l'idéal principal qu'il engendre dans $\mathcal{O}_E$ est*

$$(\pi) = N_{k,\Phi}(P) = \prod_{\phi\in\Phi} \phi^{-1}(N_{k/\phi(E)}P)$$

où $N_{k,\Phi} : \mathcal{I}(k) \to \mathcal{I}(E)$ est la norme réflexe au niveau des idéaux.

Remark 56. Puisque $\deg\pi = q^g$, la formule ci-dessus est équivalente à

$$v_{\mathfrak{p}}(\pi) = \sum_{\phi\in\Phi} v_{\phi(\mathfrak{p})}(N_{k/\phi(E)}P) = \sum_{\phi\in\Phi\cap H(\mathfrak{p})} f(P : \phi(\mathfrak{p}))$$

pour tout $\mathfrak{p} \mid p$ de $\mathcal{O}_E$, où

$$H(\mathfrak{p}) = \{\phi : E \to k | \phi^{-1}(P) = \mathfrak{p}\}.$$

Multipliant tout par $f(\mathfrak{p} : p) = f(\phi(\mathfrak{p}) : p)$, on obtient

$$v_{\mathfrak{p}}(\pi) \cdot f(\mathfrak{p} : p) = f(P : p) \cdot |H(\mathfrak{p}) \cap \Phi|.$$

Multipliant encore tout par $e(\mathfrak{p}, p)$, on obtient finalement

$$v_{\mathfrak{p}}(\pi) \cdot |H(\mathfrak{p})| = v_{\mathfrak{p}}(q) \cdot |H(\mathfrak{p}) \cap \Phi|$$

puisque

$$v_{\mathfrak{p}}(q) = f(P:p)\cdot e(\mathfrak{p}:p) \quad \text{et} \quad |H(\mathfrak{p})| = [E_{\mathfrak{p}}:\mathbb{Q}_p] = f(\mathfrak{p}:p)\cdot e(\mathfrak{p}:p)$$

La formule de Shimura-Tanyiama est donc équivalente à

$$\forall \mathfrak{p} \mid p \text{ de } \mathcal{O}_E : \qquad \frac{v_{\mathfrak{p}}(\pi)}{v_{\mathfrak{p}}(q)} = \frac{|H(\mathfrak{p})\cap\Phi|}{|H(\mathfrak{p})|}.$$

Démonstration. Soit $\mathcal{A}$ le modèle de Néron de A sur $\mathcal{O}_k$ et $L = \mathrm{Lie}(\mathcal{A})$. C'est un $\mathcal{O}_E \otimes \mathcal{O}_k$-module qui est un $\mathcal{O}_k$-module localement libre de rang g. Soit

$$\det_L : \mathcal{O}_E \to \mathcal{O}_k$$

le déterminant qui en résulte. Puisque A est de type CM (E,Φ) et $\phi(E) \subset k$ pour tout $\phi \in \Phi$, on sait que $L \otimes k \simeq \prod_{\phi\in\Phi} k(\phi)$ comme $E \otimes k$-module, donc

$$\forall e \in \mathcal{O}_E : \quad \det_L(e) = \textstyle\prod_{\phi\in\Phi}\phi(e).$$

Considérons d'autre part le $\mathcal{O}_E \otimes k(P)$-module $L \otimes_{\mathcal{O}_k} k(P)$. C'est un module de longueur finie sur $\mathcal{O}_E/p\mathcal{O}_E \otimes_{\mathbb{F}_p} k(P)$, et il admet donc une suite de composition (de Jordan-Holder) dont les quotients sont des $\mathcal{O}_E/p\mathcal{O}_E \otimes k(P)$-modules simples, lesquels sont des quotients de $\mathcal{O}_E/\mathfrak{p} \otimes_{\mathbb{F}_p} k(P)$ pour des idéaux premiers $\mathfrak{p} \mid p$ de $\mathcal{O}_E$, donc de la forme $k(P)(\phi)$ pour un morphisme $\phi \in H(\mathfrak{p})$. La formule qui donne le déterminant montre que ces facteurs simples sont exactement les $k(P)(\phi)$ pour $\phi \in \Phi$, sans multiplicité. Si $\phi \in H(\mathfrak{p})$ (i.e. $\phi^{-1}(P) = \mathfrak{p}$), le $\mathcal{O}_E/\mathfrak{p}$-espace vectoriel $k(P)$ est de $\mathbb{F}_p$-dimension $f(P:p) = f(P:\phi(\mathfrak{p}))\cdot f(\mathfrak{p}:p)$, donc de $\mathcal{O}_E/\mathfrak{p}$-dimension $f(P:\phi(\mathfrak{p}))$. On en déduit que la multiplicité du $\mathcal{O}_E$-module simple $\mathcal{O}_E/\mathfrak{p}$ dans $L \otimes_{\mathcal{O}_k} k(P)$ est la somme sur tous les $\phi \in H(\mathfrak{p}) \cap \Phi$ de $f(P:\phi(\mathfrak{p}))$. Mais puisque $L \otimes_{\mathcal{O}_k} k(P) = \mathrm{Lie}(A_{k(P)})$, cette multiplicité est aussi celle de $\mathcal{O}_E/\mathfrak{p}$ dans $\mathcal{O}_E/(\pi)$, d'après la formule de Giraud, proposition 54. On a donc

$$v_{\mathfrak{p}}(\pi) = \sum_{\phi\in H(\mathfrak{p})\cap\Phi} f(P:\phi(\mathfrak{p}))$$

pour tout $\mathfrak{p} \mid p$ de $\mathcal{O}_E$, ce qui est précisément la formule de Shimura-Taniyama. $\square$

4.4. **Preuve du théorème principal.** On veut montrer que

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} = N_\Phi \quad : \quad T_{E(\Phi)}(\mathbb{Q})\backslash T_{E(\Phi)}(\mathbb{A}_f) \to T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f).$$

4.4.1. *Niveau fini.* Pour tout n entier, notons

$$K(n) = \{\lambda \in \widehat{\mathcal{O}}_E^\times : \lambda \equiv 1 \bmod n\}.$$

C'est un sous-groupe ouvert et compact de $T_E(\mathbb{A}_f)$. Puisque $r_\Phi \circ \mathrm{Art}_{E(\Phi)}$ et N_Φ sont continus, il existe un idéal $\mathcal{N}$ de $\mathcal{O}_{E(\Phi)}$ tels que les deux applications

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} \bmod K(n) \qquad \text{et} \qquad N_\Phi \bmod K(n)$$

se factorisent en un diagramme

$$\begin{array}{lccc} r_\Phi \circ \mathrm{Art}_{E(\Phi)} \text{ ou } N_\Phi : & T_{E(\Phi)}(\mathbb{Q})\backslash T_{E(\Phi)}(\mathbb{A}_f) & \to & T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f) \\ & \downarrow & & \downarrow \\ r_\Phi \circ \mathrm{Art}_{E(\Phi)} \text{ ou } N_\Phi : & T_{E(\Phi)}(\mathbb{Q})\backslash T_{E(\Phi)}(\mathbb{A}_f)/K(\mathcal{N}) & \to & T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)/K(n) \end{array}$$

où $K(\mathcal{N}) = \{\lambda \in \widehat{\mathcal{O}}_{E(\Phi)}^\times : \lambda \equiv 1 \bmod \mathcal{N}\}$. Or

$$T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)/K(n) = E^\times \backslash \left(\widehat{E}^{(n)\times}/K(n)^{(n)} \times \textstyle\prod_{\mathfrak{q}\mid n} E_{\mathfrak{q}}^\times/K(n)_{\mathfrak{q}}\right)$$

avec des notations évidentes, et $E^\times$ est dense dans $\prod_{\mathfrak{q}|n} E_{\mathfrak{q}}^\times$, donc

$$T_E(\mathbb{Q})\backslash T_E(\mathbb{A}_f)/K(n) \simeq \Gamma(E^\times, n)\backslash \widehat{E}^{(n)\times}/K(n)^{(n)} \simeq i(\Gamma(E^\times, n))\backslash I^n(E) = C(E, n)$$

où $I^n(E)$ est l'ensemble des idéaux fractionnaires de E qui sont premiers à n,

$$\Gamma(E^\times, n) = \{\lambda \in E^\times : \forall \mathfrak{q} \mid n,\, v_{\mathfrak{q}}(\lambda - 1) \geq v_{\mathfrak{q}}(n)\}$$

et i est l'application qui à un élément de $E^\times$ associe le $\mathcal{O}_E$-idéal engendré par cet élément. De même et avec des notations similaires,

$$T_{E(\Phi)}(\mathbb{Q})\backslash T_{E(\Phi)}(\mathbb{A}_f)/K(\mathcal{N}) \simeq i(\Gamma(E(\Phi)^\times, \mathcal{N}))\backslash I^{\mathcal{N}}(E(\Phi)) = C(E(\Phi), \mathcal{N}).$$

Les morphismes ainsi obtenus sont

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} \text{ et } N_\Phi \quad : \quad C(E(\Phi), \mathcal{N}) \to C(E, n).$$

Le morphisme N_Φ se décrit aisément : il est induit par le morphisme N_Φ sur les idéaux. Quant au morphisme $r_\Phi \circ \mathrm{Art}_{E(\Phi)}$, il se décrit de la manière suivante.

4.4.2. *Description de* $r_\Phi \circ \mathrm{Art}_{E(\Phi)}$ *en niveau fini.* Soit $E(\Phi, \mathcal{N})$ l'extension abélienne de $E(\Phi)$ qui est fixée par $\mathrm{Art}_{E(\Phi)}(K(\mathcal{N}))$. C'est une extension non-ramifiée en dehors de $\mathcal{N}$, et les isomorphismes ci-dessus induisent un isomorphisme

$$\mathrm{Art}_{E(\Phi)} : C(E(\Phi), \mathcal{N}) \xrightarrow{\simeq} \mathrm{Gal}\,(E(\Phi, \mathcal{N})/E(\Phi))$$

qui envoient la classe d'un idéal premier $\mathfrak{p} \nmid \mathcal{N}$ de $E(\Phi)$ sur l'inverse $\mathrm{Frob}_{\mathfrak{p}}^{-1}$ du Frobénius arithmétique $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(E(\Phi, \mathcal{N})/E(\Phi))$.

Soit $\mathcal{X} \in C(E(\Phi), \mathcal{N})$. Choisissons $\sigma \in \mathrm{Aut}(\mathbb{C}/E(\Phi))$ tel que

$$\sigma | E(\Phi, \mathcal{N}) = \mathrm{Art}_{E(\Phi)}(X) \quad \text{dans} \quad \mathrm{Gal}\,(E(\Phi, \mathcal{N})/E(\Phi)).$$

Soient $(A, \iota) \in \mathcal{H}(E, \Phi)$, λ une E-isogénie $(A, \iota) \to \sigma(A, \iota)$ et $\widehat{t} \in T_E(\mathbb{A}_f)$ tel que

$$\forall x \in V_f(A, \mathbb{C}) : \qquad \lambda(\widehat{t} \cdot x) = \sigma \cdot x \quad \text{dans } V_f(\sigma A, \mathbb{C}).$$

Quitte à modifier λ par un élément convenable de $E^\times$, on peut supposer que pour tout $\mathfrak{p} \mid n$, la composante $\widehat{t}_{\mathfrak{p}}$ de $\widehat{t}$ est dans le sous-groupe ouvert compact $K(n)_{\mathfrak{p}}$ de $E_{\mathfrak{p}}^\times$. Si $\mathcal{O}_E = \mathrm{End}(A) \cap \iota(E)$, cette condition est équivalente à une condition sur λ, à savoir : $\lambda(a) = \sigma a$ pour tout $a \in A[n]$. Soit enfin $J = \widehat{t} \cdot \mathcal{O}_E \in I^n(E)$ et $\mathcal{Y}$ la classe de Y dans $C(E, n)$. Alors

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)}(\mathcal{X}) = \mathcal{Y}.$$

Nous allons montrer que pour de bons choix de

$$\mathfrak{p} \in \mathcal{X}, \quad \sigma \in \mathrm{Aut}(\mathbb{C}/E(\Phi)), \quad (A, \iota) \in \mathcal{H}(E, \Phi) \quad \text{et} \quad \lambda : (A, \iota) \to \sigma(A, \iota)$$

vérifiant toutes les conditions ci-dessus, on obtient $J = N_\Phi(\mathfrak{p})$.

4.4.3. *Choix de* (A, ι). Choisissons une extension galoisienne finie k de $E(\Phi)$ telle que (1) $E(\Phi, \mathcal{N}) \subset k$, et (2) il existe une variété abélienne $(A, \iota) \in \mathcal{H}(E, \Phi)$ qui est définie sur k et telle que $\mathcal{O}_E = \mathrm{End}_k(A) \cap \iota(E)$. Quitte à agrandir encore k, on peut supposer que (3) $\phi(E) \subset k$ pour tout $\phi \in \Phi$, et (4) pour tout $\sigma \in \mathrm{Gal}(k/E(\Phi))$, il existe une $\mathcal{O}_E$-isogénie $A \to \sigma A$ qui est définie sur k.

Exercise 57. Toute $\mathcal{O}_E$-isogénie $A \to \sigma A$ est alors également définie sur k.

4.4.4. *Choix de $\mathfrak{p}$ et σ.* On choisit dans $\mathcal{X} \in C(E(\Phi), \mathcal{N})$ l'inverse $\mathfrak{p}^{-1}$ d'un idéal premier $\mathfrak{p} \nmid \mathcal{N}$ tel que la variété abélienne A sur k a bonne réduction en tous les idéaux premiers $P \mid \mathfrak{p}$ de k. On fixe un tel idéal premier $P \mid \mathfrak{p}$ de $\mathcal{O}_k$, de sorte que σA a bonne réduction en P pour tout $\sigma \in \mathrm{Gal}(k/E(\Phi))$. On choisit $\sigma \in \mathrm{Aut}(\mathbb{C}/E(\Phi))$ de sorte que

$$\sigma|k = \mathrm{Frob}_P \in \mathrm{Gal}(k/E(\Phi)).$$

4.4.5. *Calcul de $r_\Phi \circ \mathrm{Art}_{E(\Phi)}(\mathcal{X})$.*

Lemma 58. *Il existe $J \in I(E)$ et un k-isomorphisme $\mathcal{O}_E$-linéaire $\beta : A^J \simeq \sigma A$.*

Démonstration. D'après l'hypothèse (4) sur (A, ι), tout isomorphisme $\mathcal{O}_E$-linéaire $A^J(\mathbb{C}) \simeq (\sigma A)(\mathbb{C})$ est défini sur k, cf Exercice 57. Si

$$A(\mathbb{C}) \simeq V_{\mathbb{R},I}/\Lambda \qquad \text{et} \qquad (\sigma A)(\mathbb{C}) \simeq V_{\mathbb{R},I}/\Lambda',$$

il existe un idéal fractionnaire J de E tel que $\Lambda' = J^{-1}\Lambda$. Les isomorphismes

$$\mathrm{Hom}_{\mathcal{O}_E}(J, V_{\mathbb{R},I}) \simeq \mathrm{Hom}_E(E, V_{\mathbb{R},I}) \simeq V_{\mathbb{R},I}$$

induisent un isomorphisme

$$\mathrm{Hom}_{\mathcal{O}_E}(J, \Lambda) \simeq \{f : E \to V_{\mathbb{R},I} : f(J) = Jf(1) \subset \Lambda\} \simeq J^{-1}\Lambda$$

d'où l'on déduit que

$$\mathrm{Hom}_{\mathcal{O}_E}(J, V_{\mathbb{R},I}/\Lambda) \simeq V_{\mathbb{R},I}/J^{-1}\Lambda$$

i.e. $A^J(\mathbb{C}) \simeq (\sigma A)(\mathbb{C})$, cqfd. □

Soit $\overline{A}/k(P)$ la réduction de A en P. Alors $\overline{A}^{(q^i)}$ est celle de $\sigma^i A$. En particulier, le composé des Frobenius "absolus"

$$\overline{A} \to \overline{A}^{(q)} \to \overline{A}^{(q^2)} \to \cdots \to \overline{A}^{(q^f)} = \overline{A}$$

est le Frobénius $\pi \in \mathcal{O}_E$ de la variété abélienne $\overline{A}$ sur $k(P)$. Notons que tous ces morphismes sont $\mathcal{O}_E$-linéaires, et se déduisent de $F : \overline{A} \to \overline{A}^{(q)}$ par application itérée de $-^{(q)}$.

Lemma 59. *Il existe $J \subset \mathcal{O}_E$ et un isomorphisme $\mathcal{O}_E$-linéaire $\beta : A^J \xrightarrow{\simeq} \sigma A$ tel que $\beta \circ \alpha_J^A : A \to A^J \to \sigma A$ se réduise sur $F : \overline{A} \to \overline{A}^{(q)}$.*

Démonstration. Soit J un idéal fractionnaire de E tel qu'il existe un k-isomorphisme $\mathcal{O}_E$-linéaire $\beta : A^J \xrightarrow{\simeq} \sigma A$. La réduction de cet isomorphisme est un isomorphisme $\overline{\beta} : \overline{A}^J \xrightarrow{\simeq} \overline{A}^{(q)}$. Alors $\overline{\beta}^{-1} \circ F : \overline{A} \to \overline{A}^J$ est un élément de

$$\begin{aligned}
\mathrm{Hom}_{\mathcal{O}_E}(\overline{A}, \overline{A}^J) &= \mathrm{Hom}_{\mathcal{O}_E}(\overline{A}, \mathrm{Hom}_{\mathcal{O}_E}(J, \overline{A})) \\
&= \mathrm{Hom}_{\mathcal{O}_E}(\overline{A} \otimes J, \overline{A}) \\
&= \mathrm{Hom}_{\mathcal{O}_E}(J, \mathrm{Hom}_{\mathcal{O}_E}(\overline{A}, \overline{A})) \\
&= \mathrm{Hom}_{\mathcal{O}_E}(J, \mathcal{O}_E)
\end{aligned}$$

i.e., provient d'un $f : J \to \mathcal{O}_E$, qui est injectif puisque $\overline{\alpha} \circ F$ est une isogénie. Remplaçant J par $f(J)$, on peut donc supposer que $J \subset \mathcal{O}_E$ et

$$\overline{\beta}^{-1} \circ F = \overline{\alpha}_J^A : \overline{A} \to \overline{A}^J.$$

Alors $\beta \circ \alpha_J^A : A \to A^J \xrightarrow{\simeq} \sigma A$ se réduit bien sur $F : \overline{A} \to \overline{A}^{(q)}$. □

Soit $\lambda = \beta \circ \alpha_J^A : A \to A^J \xrightarrow{\simeq} \sigma A$. C'est une isogénie $\mathcal{O}_E$-linéaire de degré $[\mathcal{O}_E : J] = \deg F = (\deg \mathfrak{p})^g$ premier à n, et puisque λ se réduit sur F, $\lambda(a) = \sigma a$ pour tout $a \in A[n]$. Donc si $\widehat{t}$ est l'élément de $T_E(\mathbb{A}_f)$ tel que

$$\forall x \in V_f(A, \overline{\mathbb{Q}}) : \qquad \lambda(\widehat{t} \cdot x) = \sigma \cdot x \quad \text{dans } V_f(\sigma A, \overline{\mathbb{Q}})$$

alors $\widehat{t}_\mathfrak{q} \in K(n)_\mathfrak{q}$ pour tout $\mathfrak{q} \mid n$ et $r_\Phi \circ \mathrm{Art}(\mathcal{X}) \in C(E, n)$ est représenté par l'idéal $\widehat{t} \cdot \mathcal{O}_E \in I^n(E)$. Pour calculer cet idéal, on note que $\alpha_J^A : V_f(A, \overline{\mathbb{Q}}) \to V_f(A^J, \overline{\mathbb{Q}})$ envoie $\widehat{t} \cdot T_f(A, \overline{\mathbb{Q}})$ sur $T_f(A^J, \overline{\mathbb{Q}})$, et que les isomorphismes

$$V_f(A^J, \overline{\mathbb{Q}}) \simeq \mathrm{Hom}_{\mathcal{O}_E}\big(J, V_f(A, \overline{\mathbb{Q}})\big) \simeq \mathrm{Hom}_E\big(E, V_f(A, \overline{\mathbb{Q}})\big) \simeq V_f(A, \overline{\mathbb{Q}})$$

identifient $T_f(A^J, \overline{\mathbb{Q}})$ à $J^{-1} \cdot T_f(A, \overline{\mathbb{Q}})$ et α_J^A à l'identité, donc

$$\widehat{t} \cdot T_f(A, \overline{\mathbb{Q}}) = J^{-1} \cdot T_f(A, \overline{\mathbb{Q}}).$$

On en déduit que $\widehat{t} \cdot \mathcal{O}_E = J^{-1}$, donc

$$r_\Phi \circ \mathrm{Art}(\mathcal{X}) = [J^{-1}] \in C(E, n).$$

Posant $\beta_\ell = (\sigma^{\ell-1}\beta) \circ (\sigma^{\ell-2}\beta^J) \circ \cdots \circ (\sigma\beta^{J^{\ell-2}}) \circ \beta^{J^{\ell-1}}$, un isomorphisme $\mathcal{O}_E$-linéaire

$$\beta_\ell : A^{J^\ell} \to \sigma A^{J^{\ell-1}} \to \sigma^2 A^{J^{\ell-2}} \to \cdots \to \sigma^\ell A$$

on obtient un diagramme commutatif

$$\begin{array}{ccccccccc} A & \to & A^J & \to & A^{J^2} & \to & \cdots & \to & A^{J^f} \\ \| & & \beta_1 \downarrow & & \beta_2 \downarrow & & & & \beta_f \downarrow \\ A & \to & \sigma A & \to & \sigma^2 A & \to & \cdots & \to & \sigma^f A = A \end{array}$$

dont la deuxième ligne se réduit sur le Frobenius $\pi : \overline{A} \to \overline{A}$. On a donc

$$J^f = (\pi) = N_{\Phi,k}(P) = N_\Phi(\mathfrak{p}^f) = N_\Phi(\mathfrak{p})^f$$

d'après la formule de Shimura-Taniyama, donc $J = N_\Phi(\mathfrak{p})$ puisque $I^n(E)$ est sans torsion. Ainsi $J^{-1} = N_\Phi(\mathfrak{p}^{-1})$, et puisque $\mathcal{X} = [\mathfrak{p}^{-1}]$ dans $C(E(\Phi), \mathcal{N})$, on a bien

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} = N_\Phi \quad : \quad C(E(\phi), \mathcal{N}) \to C(E, n).$$

4.4.6. *Fin de la preuve.* On a donc vu que pour tout $n \geq 1$,

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} \equiv N_\Phi \bmod K(n).$$

Cela montre déjà que $\theta = r_\Phi \circ \mathrm{Art}_{E(\Phi)} / N_\Phi^{-1}$ est un morphisme

$$\theta : T_{E(\Phi)}(\mathbb{Q}) \backslash T_{E(\Phi)}(\mathbb{A}_f) \to T_E(\mathbb{Q}) \backslash \overline{T_E(\mathbb{Q})}$$

où $\overline{T_E(\mathbb{Q})} = \cap_n T_E(\mathbb{Q}) \cdot K(n)$ est l'adhérence de $T_E(\mathbb{Q})$ dans $T_E(\mathbb{A}_f)$. On conclut grâce aux deux lemmes suivants, où $\star$ est l'involution de $T_E(\mathbb{A}_f)$ induite par l'involution canonique $\star$ de E :

Lemma 60. *Avec les notations ci-dessus,* $\theta \cdot \theta^\star = 1$.

Démonstration. Soient $s \in T_{E(\Phi)}(\mathbb{A}_f)$, $\sigma \in \mathrm{Aut}(\mathbb{C})$ tel que $\sigma | E(\Phi)^{ab} = \mathrm{Art}_{E(\Phi)}(s)$, $(A, \iota) \in \mathcal{H}(E, \Phi)$, λ une E-isogénie $(A, \iota) \to \sigma(A, \iota)$, et $\widehat{t} \in T_E(\mathbb{A}_f)$ tel que

$$\forall x \in V_f(A, \mathbb{C}) : \quad \lambda(\widehat{t} \cdot x) = \sigma x \text{ dans } V_f(\sigma A, \mathbb{C}).$$

Soit $\alpha : A \to A^t$ une polarisation $(E, \star)$-linéaire de A. Alors

$$\sigma\alpha : \sigma A \to \sigma(A^t) \simeq (\sigma A)^t$$

est une polarisation $(E,\star)$-linéaire de σA et

$$\lambda^*(\sigma\alpha) = \lambda^t \circ \sigma\alpha \circ \lambda : A \to A^t$$

est à nouveau une polarisation de A. D'après le corollaire 32, il existe donc une constante $c \in F_>^\times$ telle que $c\alpha = \lambda^t \circ \sigma\alpha \circ \lambda$. Pour tout $x, y \in V_f(A, \mathbb{C})$, on a alors

$$\begin{aligned}\left\langle \widehat{t} \cdot x, c\widehat{t} \cdot y \right\rangle_f^\alpha &= \left\langle \widehat{t} \cdot x, \widehat{t} \cdot y \right\rangle_f^{\lambda^t\circ\sigma\alpha\circ\lambda} = \left\langle \lambda(\widehat{t}\cdot x), \lambda(\widehat{t}\cdot y)\right\rangle_f^{\sigma\alpha} \\ &= \langle \sigma x, \sigma y\rangle\rangle_f^{\sigma\alpha} = \sigma\,\langle x,y\rangle_f^\alpha = \chi_{cyc}(\sigma)\,\langle x,y\rangle_f^\alpha\end{aligned}$$

donc $\left\langle x, c\widehat{t\widehat{t}^\star} \cdot y\right\rangle_f^\alpha = \langle x, \chi_{cyc}(\sigma) y\rangle_f^\alpha$, de sorte que $c\widehat{t\widehat{t}^\star} = \chi_{cyc}(\sigma)$ et

$$(\theta\cdot\theta^\star)(s) = \frac{r_\Phi(\sigma)\cdot r_\Phi(\sigma)^\star}{N_\Phi(s)\cdot N_\Phi(s)^\star} = \frac{\widehat{t}\cdot\widehat{t}^\star}{N_\Phi(s)\cdot N_\Phi(s)^\star} \in T_E(\mathbb{Q}),$$

puisque $\chi_{cyc}(\sigma) \equiv N_\Phi(s)\cdot N_\phi(s)^\star \bmod T_E(\mathbb{Q})$. □

Lemma 61. *Le groupe $\overline{T_E(\mathbb{Q})}/T_E(\mathbb{Q})$ est un $\mathbb{Q}$-espace vectoriel sur lequel $\star = 1$.*

Démonstration. On admet le résultat suivant : la topologie de $T_E(\mathbb{A}_f)$ induit sur $\mathcal{O}_E^\times$ la topologie profinie, i.e. celle dont une base de voisinage ouvert (et fermé) de 1 est formé des sous-groupes U qui sont d'indice fini dans $\mathcal{O}_E^\times$. Pour un tel sous-groupe U, l'adhérence $\overline{U}$ de U dans $T_E(\mathbb{A}_f)$ s'identifie donc à la complétion profinie $\widehat{U}$ de U. D'autre part,

$$\left(T_E(\mathbb{Q})\cdot\overline{U}\right) \cap \widehat{\mathcal{O}}_E^\times = \mathcal{O}_E^\times \cdot \overline{U} = \cup_{x\in\mathcal{O}_E^\times/U}\, x\cdot\overline{U}$$

est fermé dans $\widehat{\mathcal{O}}_E^\times$, donc $T_E(\mathbb{Q})\cdot\overline{U}$ est un sous-groupe localement fermé, donc fermé, de $T_E(\mathbb{A}_f)$. Il en résulte que $T_E(\mathbb{Q})\cdot\overline{U} = \overline{T_E(\mathbb{Q})}$, et l'on obtient donc une suite exacte

$$1 \to \overline{U}\cap T_E(\mathbb{Q})/U \to \widehat{U}/U \simeq \overline{U}/U \to \overline{T_E(\mathbb{Q})}/T_E(\mathbb{Q}) \to 1$$

avec un noyau fini puisque $\overline{U}\cap T_E(\mathbb{Q}) \subset \mathcal{O}_E^\times$. Puisque $\mathcal{O}_F^\times$ et $\mathcal{O}_E^\times$ sont des groupes abéliens de type fini et de même rang $r = [F:\mathbb{Q}] - |\mathrm{Spec}F|$, on peut choisir pour U un sous-groupe de $\mathcal{O}_F^\times$ qui est sans torsion (et de rang r). Alors $\overline{U}/U \simeq \widehat{U}/U \simeq (\widehat{\mathbb{Z}}/\mathbb{Z})^r$. Mais $\widehat{\mathbb{Q}} = \widehat{\mathbb{Z}} + \mathbb{Q}$ avec $\widehat{\mathbb{Z}}\cap\mathbb{Q} = \mathbb{Z}$. On obtient alors

$$\overline{T_E(\mathbb{Q})}/T_E(\mathbb{Q}) \simeq \overline{U}/U \simeq \widehat{U}/U \simeq (\widehat{\mathbb{Z}}/\mathbb{Z})^r \simeq (\widehat{\mathbb{Q}}/\mathbb{Q})^r$$

et le lemme en résulte immédiatement. □

Références

[1] D. Mumford, *Abelian Varieties.*

[2] J-P. Serre et J. Tate, *Good Reduction of Abelian Varieties.* Annals of Math., Second Series, **88.3** (1968).

[3] E. Snapper, *Polynomials associated with divisors.* J. Math. Mech. **9** (1960) 123–139.