On the arithmetic of 1–motives

Known in 2005: Classical arithmetic duality theorems for abelian varieties, and for tori and their character groups can be generalized and unified to duality theorems for 1–motives. If k is a number field and M a 1–motive over k with dual $M^\vee$ then there is a canonical pairing

$$Ш^i(k, M) \times Ш^{2-i}(k, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

This pairings are nondegenerate modulo divisible subgroups (provided the groups $Ш^0(k, -)$ are slightly modified).

Problem: This does not generalize duality theorems for finite Galois modules (e.g. the Poitou–Tate duality theorem), because finite Galois modules can not be interpreted as 1–motives in Deligne's sense.

Tamás's Question (2006): Is there a category of *1–motives with torsion* such that classical arithmetic duality theorems known for abelian varieties, for tori and their character groups, as well as for finite group schemes (Galois modules) can be generalized and unified to duality theorems for these new 1–motives with torsion?

Answer: Yes.

Duality Theorem. *Let M be a 1–motive with torsion over a number field k, with dual $M^\vee$. There are canonical pairings*

$$Ш^i(k, M) \times Ш^{2-i}(k, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

These are nondegenerate modulo divisible subgroups and trivial for $i \neq 0, 1, 2$.

This duality theorem generalizes and unifies all arithmetic duality theorems I mentioned so far by making suitable specializations. But for the proof I needed another duality theorem, a particular form of which is

Another duality theorem. *Let C be a bounded complex of fppf–sheaves on k with finite homology groups, and write $C^\vee := \mathbb{R}\mathcal{H}om(C, \mathbb{G}_m)$. There are canonical, perfect pairings finite groups*

$$Ш^i(k, C) \times Ш^{3-i}(k, C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

This theorem also generalizes the classical Poitou–Tate duality theorem for finite Galois modules, and is not a special case of the duality theorem for 1-motives with torsion.

Why such complexes? Because we need ℓ–adic Tate–modules and ℓ–adic Barsotti–Tate groups.

Theorem. *Let k be a number field with absolute Galois group Γ, and let M_1 and M_2 be torsion free 1–motives over k. The natural map*

$$\mathrm{Hom}_k(M_1, M_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_\Gamma(\mathrm{T}_\ell M_1, \mathrm{T}_\ell M_2)$$

is an isomorphism.

Ideas of Serre, Tate and Gabber. Let S be a set of places of k of density 1, not containing a finite list of "bad" places. Set $\Gamma := \mathrm{Gal}(\bar{k}|k)$ and let L^M be the image of Γ in $\mathrm{GL}(\mathrm{T}_\ell M)$. The following groups are canonically isomorphic

$$H^1_S(k, \mathrm{T}_\ell M) \;:=\; \ker\left(H^1(k, \mathrm{T}_\ell M) \longrightarrow \prod_{v \in S} H^1(k_v, \mathrm{T}_\ell M)\right)$$

$$H^1_*(L^M, \mathrm{T}_\ell M) \;:=\; \ker\left(H^1(L^M, \mathrm{T}_\ell M) \longrightarrow \prod_{\sigma \in L^M} H^1(\langle\sigma\rangle, \mathrm{T}_\ell M)\right)$$

The group $H^1_S(k, \mathrm{T}_\ell M)$ contains $\text{Ш}^1(k, \mathrm{T}_\ell M)$. The group $H^1_*(L^M, \mathrm{T}_\ell M)$ can be computed in terms of Lie group and Lie algebra cohomology.

Consequence. If $H^1_*(L^M, \mathrm{T}_\ell M)$ is finite, then the pairing

$$\text{Ш}^i(k, M) \times \text{Ш}^{2-i}(k, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite groups.

How to compute $H^1_*(L^M, \mathrm{T}_\ell M)$? We need to control L^M, the image of the absolute Galois group $\Gamma := \mathrm{Gal}\,\overline{k}|k$ in the group of $\mathbb{Z}_\ell$–linear automorphisms of $\mathrm{T}_\ell M$.

The action of an element $\sigma \in \Gamma$ acting on $\mathrm{T}_\ell M$ is given by a 3×3 upper triangular block matrix

$$\sigma = \left(\begin{array}{c|c|c} \sigma_T & * & * \\ \hline 0 & \sigma_A & * \\ \hline 0 & 0 & \sigma_Y \end{array}\right) \qquad\qquad * = \text{something}$$

On the diagonal blocks, we see the action of Γ on the pure parts of M. The extension data is encoded in the strictly upper triangular blocks.

Algebraicity Theorem. *Let $M = [u : \mathbb{Z}^r \longrightarrow A]$ be a 1–motive over k, where A is an abelian variety. Consider u as a rational point on the abelian variety $\mathcal{H}om(\mathbb{Z}^r, A) \cong A^r$, and let H^M_A be the smallest abelian subvariety of A^r containing a nonzero multiple of u. The image of the Kummer injection*

$$\vartheta : L^M_A \longrightarrow \mathrm{Hom}(\mathbb{Z}^r_\ell, \mathrm{T}_\ell A) \cong \mathrm{T}_\ell A^r \supseteq \mathrm{T}_\ell H^M_A$$

is contained and open in $\mathrm{T}_\ell H^M_A$. In particular, the Lie group L^M_A is algebraic and its dimension is independent of the prime ℓ.

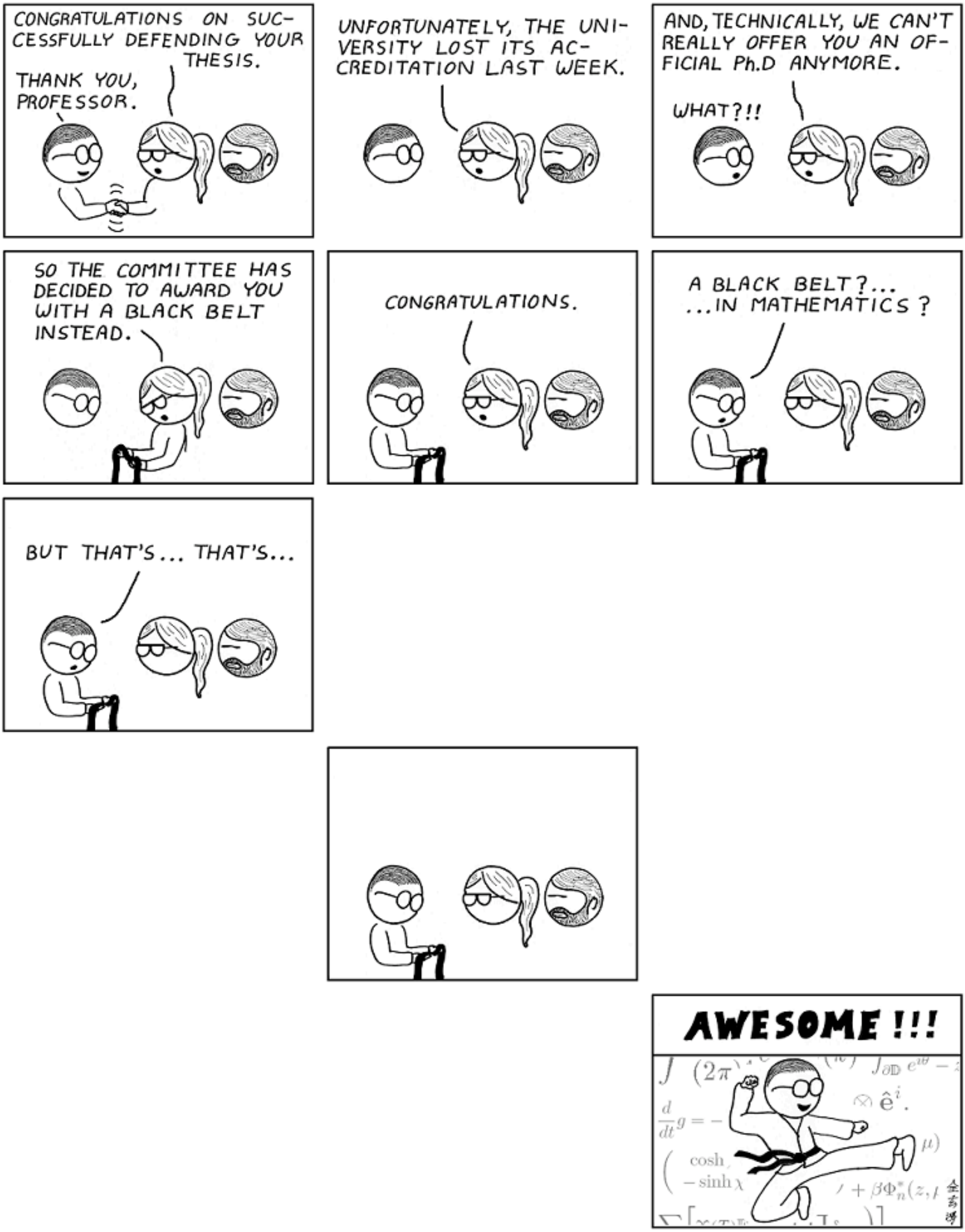
Theorem. *Let* $M = [Y \longrightarrow G]$ *be a 1–motive, where* G *is either a simple abelian variety or the multiplicative group. For every prime* ℓ*, the group* $H^1_*(L^M, \mathrm{T}_\ell M)$ *is finite. Hence the pairing*

$$Ш^0(k, M) \times Ш^2(k, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite groups.

Theorem. *Let* k *be a number field and let* G *be a simple abelian variety or the multiplicative group over* k*. Let* $X \subseteq G(k)$ *be a finitely generated subgroup and let* $P \in G(k)$ *be a point. The point* P *belongs to* X *if and only if for almost all primes* $\mathfrak{p}$ *of* k *the point* $(P \bmod \mathfrak{p})$ *belongs to* $(X \bmod \mathfrak{p})$*.*

For the multiplicative group this is a theorem of A. Schinzel (1975). For abelian varieties, and even for elliptic curves it is new! The statement is not true for nonsimple abelian varieties, together with Antonella Perucca I provide a counter example.


CONGRATULATIONS ON SUCCESSFULLY DEFENDING YOUR THESIS.
THANK YOU, PROFESSOR.
UNFORTUNATELY, THE UNIVERSITY LOST ITS ACCREDITATION LAST WEEK.
AND, TECHNICALLY, WE CAN'T REALLY OFFER YOU AN OFFICIAL Ph.D ANYMORE.
WHAT?!!
SO THE COMMITTEE HAS DECIDED TO AWARD YOU WITH A BLACK BELT INSTEAD.
CONGRATULATIONS.
A BLACK BELT?...
...IN MATHEMATICS?
BUT THAT'S... THAT'S...
AWESOME!!!