Bounding the kernel of the tame symbol on curves

Rob de Jeu

`http://www.few.vu.nl/~jeu`

Department of Mathematics

VU University Amsterdam

Amsterdam

The Netherlands

K_2 of a field

For a field F let $F^\flat = F \setminus \{0,1\}$. Then

$$K_2(F) = F^* \otimes_{\mathbb{Z}} F^* / \langle x \otimes (1-x) | x \in F^\flat \rangle$$

is an Abelian group written additively with

$$\begin{array}{lrl} \text{generators} & \{a,b\} = & \text{the class of } a \otimes b \\ \text{relations} & \{a_1a_2,b\} = & \{a_1,b\} + \{a_2,b\} \\ & \{a,b_1b_2\} = & \{a,b_1\} + \{a,b_2\} \\ & \{a,1-a\} = & 0 \text{ if } a \text{ is in } F^\flat \end{array}$$

Then also $\{a,b\} = -\{b,a\}$ and $\{c,-c\} = 0$ for a, b, c in F^*.

So if $A + B = C$ with A, B, C in F and A, $B \neq 0$, then

$$\{A,B\} = 0 \text{ if } C = 0 \qquad \{A/C, B/C\} = 0 \text{ if } C \neq 0.$$

$K_2(\mathbb{Q})$

$K_2(\mathbb{Q}) \overset{T}{\twoheadrightarrow} \oplus_{p \text{ prime}} \mathbb{F}_p^*$ with $\ker(T) = \langle\{-1,-1\}\rangle (\cong \mathbb{Z}/2\mathbb{Z})$

Here T is the tame symbol, defined by

$$T_p(\{a,b\}) = (-1)^{v_p(a)v_p(b)} \frac{a^{v_p(b)}}{b^{v_p(a)}} \text{ modulo } p$$

More precisely, for q prime or -1, let
$F_q = \langle\{a,b\} \text{ with } a,b \in \{-1,2,3,5,7,11,\ldots,q\}\rangle \subseteq K_2(\mathbb{Q})$

Then

$$F_q/F_{q'} \overset{\cong}{\to} \mathbb{F}_q^* \text{ via } T_q \qquad (q \geq 2)$$

with q' the subprime of q (= one prime smaller) ($2' = -1$)

Proof Let $q \geq 2$

- surjectivity: $\{i,q\} \mapsto \bar{i} \in \mathbb{F}_q^*$ ($i = 1,\ldots,q-1$)

- injectivity: the kernel of $F_q \overset{T_q}{\to} \mathbb{F}_q^*$ is $F_{q'}$: $F_{q'} \subseteq \ker(T_q)$: clear;

if $q = 2$ then $F_2 = F_{-1}$ as $\{2,2\} = \{2,-1\} = \{-1,2\} = 0$
if $q > 2$ then $F_q/F_{q'}$ is generated by the classes of
$\{a,q\} - \{b,q\}$ with $a, b \in M_q \overset{\text{def}}{=} \{-1, 1, 2, 3, 4, 5, \ldots, q-1\}$

If $a_1, a_2 \in M_q$ then $\{a_1, q\} + \{a_2, q\} \overset{F_{q'}}{\equiv} \{a_3, q\}$ for $a_3 \in M_q$:
division with remainder gives $a_1 a_2 - a_3 = qA$ with
$a_3 = 1, 2, \ldots, q-1 \in M_q$ and $A = -1, 0, 1, \ldots, q-2$, and
if $A = 0$: $a_1 a_2 = a_3$ so clear;

if $A \neq 0$: $0 = \{\frac{a_1 a_2}{qA}, \frac{a_3}{-qA}\} \overset{F_{q'}}{\equiv} \{a_3, q\} - \{a_1, q\} - \{a_2, q\}$.

So $F_q/F_{q'} = \{\{a,q\} - \{b,q\} \text{ with } a, b \in M_q\}$

Finally, if $T_q(\{a,q\}) = T_q(\{b,q\})$ for $a, b \in M_q$ then
$a - b = 0, \pm q$ and $\{a,q\} \equiv \{b,q\}$ modulo F_q' as before

$K_2(k(x))$

If k is a field and x a variable then one can treat $K_2(k(x))$ similarly using division with remainder in $k[x]$:

if $d = \deg(f(x)) \geq d' = \deg(g(x))$ for $f(x), g(x) \neq 0$, then

$$\begin{aligned} \mathrm{Pol}_{\leq 0} \times \mathrm{Pol}_{\leq d-d'} \times \mathrm{Pol}_{\leq d'-1} &\to \mathrm{Pol}_{\leq d} \\ (c, q, r) &\mapsto cf - qg - r \end{aligned}$$

is a k-linear map with non-trivial kernel:
$1 + (d - d' + 1) + d' > d + 1$

If $(c, q, r) \neq 0$ is in this kernel then $c \neq 0$ because of degrees, so the kernel has basis $\{(1, q/c, r/c)\}$.

A useful lemma

The Euclidean algorithm in $\mathbb{Z}$ converges faster if we allow negative remainders: $a = qb + r$ with $|r| \le |b|/2$
So(?) in $k[x]$ it "converges faster" if we allow $a(x) = q(x)b(x) + r(x)$ with "$|\deg(r(x))| \le |\deg(b(x))|/2$"

This inspired the
VW-lemma Let K/k be a finite extension of fields, $V, W \subseteq K$ k-subspaces with $\dim_k(V) + \dim_k(W) > \dim_k(K) = [K : k]$. Then $K^* = \{vw^{-1} \text{ with } v \in V^*, w \in W^*\}$ where $V^* = V \setminus \{0\}$ and $W^* = W \setminus \{0\}$.

Example $\mathbb{Q}[\sqrt[3]{2}]^* = \left\{a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{2}^2\right\}^* = \left\{\frac{b_1+b_2\sqrt[3]{2}^2}{c_1+c_2\sqrt[3]{2}}\right\}$,
where all $a_i, b_j, c_l \in \mathbb{Q}$, and $b_1 + b_2\sqrt[3]{2}^2, c_1 + c_2\sqrt[3]{2} \neq 0$

A useful lemma

The Euclidean algorithm in $\mathbb{Z}$ converges faster if we allow negative remainders: $a = qb + r$ with $|r| \leq |b|/2$
So(?) in $k[x]$ it “converges faster” if we allow
$a(x) = q(x)b(x) + r(x)$ with “$|\deg(r(x))| \leq |\deg(b(x))|/2$”

This inspired the
VW-lemma Let K/k be a finite extension of fields, $V, W \subseteq K$ k-subspaces with $\dim_k(V) + \dim_k(W) > \dim_k(K) = [K : k]$.
Then $K^* = \{vw^{-1} \text{ with } v \in V^*, w \in W^*\}$ where $V^* = V \setminus \{0\}$ and $W^* = W \setminus \{0\}$.

Example $\mathbb{Q}[\sqrt[3]{2}]^* = \left\{a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{2}^2\right\}^* = \left\{\frac{b_1+b_2\sqrt[3]{2}^2}{c_1+c_2\sqrt[3]{2}}\right\}$,

where all $a_i, b_j, c_l \in \mathbb{Q}$, and $b_1 + b_2\sqrt[3]{2}^2, c_1 + c_2\sqrt[3]{2} \neq 0$

Proof of the VW-lemma
For $\beta \in K^*$ we have $V \cap \beta W \neq \{0\}$ because of dimensions.

The tame symbol on a curve

Let C/k be a smooth, proper, geometrically irreducible curve over a number field k, $F = k(C)$, and $g = \mathrm{genus}(C)$. According to Beilinson

$$K_2(F) \xrightarrow{T} \oplus_{P \in C^{(1)}} k(P)^* \xrightarrow{\mathrm{Nm}} k^*$$

should become exact after tensoring with $\mathbb{Q}$. Here

- $C^{(1)}$ = set of closed points in C • $\mathrm{Nm} = \prod_P \mathrm{Nm}_{k(P)/k}$
- T is the tame symbol, defined via

$$T_P(\{f_1, f_2\}) = (-1)^{\mathrm{ord}_P(f_1)\mathrm{ord}_P(f_2)} \frac{f_1^{\mathrm{ord}_P(f_2)}}{f_2^{\mathrm{ord}_P(f_1)}}|_P$$

Example $E : y^2 = x^3 + x - 1$, $P = \{x = 0\} \cap E \setminus \{O\}$, so $\mathbb{Q}(P) = \mathbb{Q}(i)$. For q a prime number with $q \equiv 1$ modulo 4 write $q = \alpha\overline{\alpha}$ in $\mathbb{Z}[i]$. Then for some $n > 0$, $\left(\frac{\overline{\alpha}}{\alpha}\right)^n_{|P} \in \mathrm{im}(T)$?

Beilinson(+Deligne+Bass) also expect: $\ker(T)/K_2(k)$ is a finitely generated group of rank $[k:\mathbb{Q}]\cdot g+\delta$
where δ depends on the primes of bad reduction of C

So it would be good to control $\operatorname{coker}(T)$ and $\ker(T)$

Assume k is an arbitrary field, and C/k is smooth, proper, geometrically irreducible with genus g.

Assume we have a rational point $O\in C(k)$ and let

$$RR_n = L(n(O)) = H^0(C,\mathcal{O}(n(O)))$$

$$RR_n^* = RR_n\setminus\{0\}$$

$$S = \{O\}\cup\{P\in C^{(1)} \text{ such that } f(P)=0 \text{ for some } f\in RR_{2g}^*\}$$

$$S' = \{O\}\cup\{P\in C^{(1)} \text{ such that } f(P)=0 \text{ for some } f\in RR_{3g}^*\}$$

The cokernel of T

Proposition The restriction of the tame symbol

$$K_2(F) \overset{T_S}{\to} \oplus_{P \in C^{(1)} \setminus S} \; k(P)^*$$

is surjective, so $\mathrm{coker}(T)$ is generated by $\oplus_{P \in S} k(P)^*$.

Idea of proof Induction on $\deg(P)$. For the initial step: if $P \notin S$, $\deg(P) \leq 2g$, and $\beta \in k(P)^*$, then $RR_{2g} \to k(P)$, $f \mapsto f(P)$ is injective, so there exist f_i in RR_{2g}^* with $f_1(P)/f_2(P) = \beta$ (VW-lemma!), and $T_S(\{f_1/f_2, f_P\}) = \beta_{|P}$ for a suitable f_P.

Example If E/k is an elliptic curve defined by a Weierstrass equation $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$, then $RR_2 = k \oplus kx$ and $S = \{O\} \cup \{\{x = c\} \text{ for } c \in k\}$

The kernel of T

Controlling the kernel of T is more involved (just as for $\mathbb{Q}$).

Division with remainder in $k[x]$ generalizes to the non-triviality of kernels of the form

$$\begin{aligned} L(D_1) \times L(D_2) \times L(D_3) &\to L(D_4) \\ (f_1, f_2, f_3) &\mapsto g_1 f_1 + g_2 f_2 + g_3 f_3 \end{aligned}$$

for suitable divisors D_i on C, where $L(D) = H^0(C, \mathcal{O}(D))$.

Let

$$C^{(1)}_{\leq d} = \{P \in C^{(1)} \text{ with } \deg(P) \leq d\}$$

and similarly for $C^{(1)}_d$.

The kernel and cokernel of T

Proposition Let $F_d = \langle \{f_1, f_2\} \text{ with } |(f_i)| \subseteq C^{(1)}_{\leq d} \rangle$. If $d \geq 3g+1$, then $F_d / F_{d-1} \cong \bigoplus_{O \neq P \in C^{(1)}_d} k(P)^*$, and the inclusions give a quasi-isomorphism

$$\begin{array}{c} F_{3g} \xrightarrow{T} \bigoplus_{P \in \{O\} \cup C^{(1)}_{\leq 3g}} k(P)^* \\ \downarrow \\ K_2(F) \stackrel{T}{\to} \bigoplus_{P \in C^{(1)}} k(P)^* \end{array}$$

The kernel and cokernel of T

Proposition Let $F_d = \langle \{f_1, f_2\} \text{ with } |(f_i)| \subseteq C^{(1)}_{\leq d} \rangle$. If $d \geq 3g+1$, then $F_d/F_{d-1} \cong \oplus_{O \neq P \in C^{(1)}_d} k(P)^*$, and the inclusions give a quasi-isomorphism

$$\begin{tikzcd}
F_{3g} \arrow[r, "T"] \arrow[d] & \oplus_{P \in \{O\} \cup C^{(1)}_{\leq 3g}} k(P)^* \\
K_2(F) \arrow[r, "T"] & \oplus_{P \in C^{(1)}} k(P)^*
\end{tikzcd}$$

Proposition If $g \geq 1$, and $L_{3g} = \langle \{f_1, f_2\} \text{ with } f_i \in RR^*_{3g} \rangle$. then the inclusions give a quasi-isomorphism

$$\begin{tikzcd}
L_{3g} \arrow[r, "T"] \arrow[d] & \oplus_{P \in S'} k(P)^* \\
K_2(F) \arrow[r, "T"] & \oplus_{P \in C^{(1)}} k(P)^*
\end{tikzcd}$$

A computational example

So for an ellipic curve E given by a Weierstrass equation,
$\ker(T) \subseteq \langle \{l, m\} \text{ with } l, m \text{ of the form } ax + by + c \ (a, b, c \in k) \rangle$

If $k = \mathbb{Q}$ we only need such $ax + by + c$ with a, b and c in $\mathbb{Z}$ and $\gcd(a, b, c) = 1$, or $a = b = 0$, $c = -1$ or a prime number.

Example $E : y^2 + xy + y = x^3 + x^2$
with conductor $286 = 2 \cdot 11 \cdot 13$ and $E(\mathbb{Q}) = \{O\}$

E has split multiplicative reduction at 2, 11 and 13 and conjecturally $\ker(T)/K_2(\mathbb{Q})$ is finitely generated of rank 4.

By imposing a boundary condition at the primes of split multiplicative reduction ("integrality conditions") we expect to get a subgroup of rank 1 ($\delta = 3$ here)

There is a regulator $R \in \mathbb{R}$ for this subgroup and Beilinson expects $R/L'(E, 0) \in \mathbb{Q}^*$

Using the "lines"

$l_1 = x$ $\quad l_2 = x - 1$ $\quad l_3 = x + 1$

$l_4 = y$ $\quad l_5 = y - 1$ $\quad l_6 = y + 1$

$l_7 = y + x$ $\quad l_8 = y - x$ $\quad l_9 = y - x - 1$

$l_{10} = y - x + 1$ $\quad l_{11} = y + x - 1$ $\quad l_{12} = y + x + 1$

$l_{13} = y - x - 2$ $\quad l_{14} = y - x + 2$ $\quad l_{15} = y + x - 2$

$l_{16} = y + x + 2$ $\quad l_{17} = y - 2x$ $\quad l_{18} = y + 2x$

$l_{19} = y - 2x - 1$ $\quad l_{20} = y - 2x + 1$ $\quad l_{21} = y + 2x - 1$

$l_{22} = y + 2x + 1$ $\quad l_{23} = 2$

all elements we get in $\ker(T)$ are "integral" at 11 and 13.

Using also 11, 13, and suitable lines one can hit all three "integrality obstructions", and $\ker(T)$ has rank at least 4.

To approximate $\langle\{l_i, l_j\}\rangle \subseteq K_2(\mathbb{Q}(E))$ we use a free Abelian group Gen on generators $\{l_i, l_j\}$ ($i < j$) with relations the kernel Rel of

$$\mathrm{Gen} \to K_2(\mathbb{Q}(x,y)) \xrightarrow{\widetilde{T}} \oplus_C \mathbb{Q}(D)^*$$

(where D runs through the irreducible curves in $\mathbb{A}^2_{\mathbb{Q}}$) since $\ker(\widetilde{T}) = K_2(\mathbb{Q})$ is torsion. This gives

$$\mathrm{Gen}/\mathrm{Rel} \to K_2(F)/K_2(\mathbb{Q}) \xrightarrow{T} \oplus_{P\in E^{(1)}} \mathbb{Q}(P)^*$$

T+integrality conditions give a kernel in $\mathrm{Gen}/\mathrm{Rel}$ of rank 31 instead of 1 but numerically all regulators are integral multiples of $\frac{1}{12}L'(E,0)$.

We ignored torsion in the $\mathbb{Q}(P)^*$ that occur so may have to multiply everything by 12 to be in $\ker(T)$.

For example, the conjectures suggest that, modulo torsion,

- $2\{x,y\}+\{x+1,y\}+2\{x,x+y+1\}+\{x+1,x+y+1\}\overset{?}{=}0$
- $-2\{x,y+1\}-2\{x,y+x\}+\{x+1,x-1\}-\{x+1,y+1\}-\{x+1,y+x\}+\{x-1,y+1\}+\{x-1,y+x\}\overset{?}{=}0$

For example, the conjectures suggest that, modulo torsion,

- $2\{x,y\}+\{x+1,y\}+2\{x,x+y+1\}+\{x+1,x+y+1\}\overset{?}{=}0$
- $-2\{x,y+1\}-2\{x,y+x\}+\{x+1,x-1\}-\{x+1,y+1\}-\{x+1,y+x\}+\{x-1,y+1\}+\{x-1,y+x\}\overset{?}{=}0$

Herbert Gangl observed: many relations can be explained using Steinberg relations $\{u,1-u\}=0$ coming from linear triplet relations $A_1A_2A_3+B_1B_2B_3=C_1C_2C_3$ on E with each A_i, B_i and C_i a "line": $u=\frac{A_1A_2A_3}{C_1C_2C_3}$, $1-u=\frac{B_1B_2B_3}{C_1C_2C_3}$.

E.g., $x^2(x+1)-y(y+x+1)=1$ proves the first relation above (up to 2-torsion) since $\{x^2(x+1),-y(y+x+1)\}=0$.

For example, the conjectures suggest that, modulo torsion,

- $2\{x,y\}+\{x+1,y\}+2\{x,x+y+1\}+\{x+1,x+y+1\} \overset{?}{=} 0$
- $-2\{x,y+1\}-2\{x,y+x\}+\{x+1,x-1\}-\{x+1,y+1\}-\{x+1,y+x\}+\{x-1,y+1\}+\{x-1,y+x\} \overset{?}{=} 0$

Herbert Gangl observed: many relations can be explained using Steinberg relations $\{u,1-u\}=0$ coming from linear triplet relations $A_1A_2A_3+B_1B_2B_3=C_1C_2C_3$ on E with each A_i, B_i and C_i a "line": $u=\frac{A_1A_2A_3}{C_1C_2C_3}$, $1-u=\frac{B_1B_2B_3}{C_1C_2C_3}$.

E.g., $x^2(x+1)-y(y+x+1)=1$ proves the first relation above (up to 2-torsion) since $\{x^2(x+1),-y(y+x+1)\}=0$.

There are about 765 really different linear triplet relations. Replacing Rel with the resulting Steinberg relations then gives a kernel of rank 3 for $T+$integrality conditions.

An optimistic conjecture

One of the two still unexplained relations is

$$\begin{aligned}&10\{x,y\}+5\{x+1,y\}\overset{?}{=}3\{x,y\}+6\{x,y+1\}-9\{x,y+x+1\}\\&+\{x,y-2x\}-6\{x+1,y\}-3\{x+1,y-1\}+3\{x+1,y+1\}\\&-3\{x-1,y\}+3\{x-1,y-1\}-3\{x-1,y+1\}\\&-6\{y-1,y+x+1\}+3\{y-1,y-2x\}-3\{x+y+1,y-2x\}\end{aligned}$$

An optimistic conjecture

One of the two still unexplained relations is

$$\begin{aligned}10\{x,y\}+5\{x+1,y\} &\overset{?}{=} 3\{x,y\}+6\{x,y+1\}-9\{x,y+x+1\}\\ &+\{x,y-2x\}-6\{x+1,y\}-3\{x+1,y-1\}+3\{x+1,y+1\}\\ &-3\{x-1,y\}+3\{x-1,y-1\}-3\{x-1,y+1\}\\ &-6\{y-1,y+x+1\}+3\{y-1,y-2x\}-3\{x+y+1,y-2x\}\end{aligned}$$

The calculations suggests the

Optimistic conjecture

Let k be any field, E/k an elliptic curve, $O \in E(k)$, $F = k(E)$, and $LF^* = \langle RR_3^* \rangle \subseteq F^*$ ($RR_3 = H^0(E, \mathcal{O}(3(O)))$) (so the image of $LF^* \otimes_{\mathbb{Z}} LF^*$ in $K_2(F)$ is L_3).

Then (perhaps up to torsion or so)

$$L_3 \overset{?}{=} \frac{LF^* \otimes_{\mathbb{Z}} LF^*}{\langle u \otimes (1-u) \text{ with } u, 1-u \text{ from a linear triplet relation} \rangle}$$

Some theoretical evidence

Proposition If E/k is elliptic with k algebraically closed (so $LF^* = F^*$ and $L_3 = K_2(F)$) then we only need relations $u \otimes (1-u)$ with $\deg(u) \leq 3$, and those come from linear triplet relations:

- if $\deg(u) = 0$ then $u + (1-u) = 1$;
- if $\deg(u) = 2$ then from some $l + m = n$;
- if $\deg(u) = 3$ then from some $l_1 l_2 n_2 + m_1 m_2 n_1 = n_1 n_2 N$.

Here all l_i, etc., are in RR_3^* for O the neutral element.

In the last case we have $u = \frac{l_1 l_2}{n_1 N}$ and $1 - u = \frac{m_1 m_2}{n_2 N}$.

For $* \in \{0, 1, \infty\}$ write $u^{-1}(*) = (A_{*,1}) + (A_{*,2}) + (A_{*,3})$. Then explicitly

$$(l_1) = (A_{0,1}) + (A_{0,2}) + (-A_{0,1} - A_{0,2}) - 3(O)$$

$$(l_2) = (A_{0,3}) + (-A_{\infty,1} - A_{\infty,2}) + (A_{\infty,1} + A_{\infty,2} - A_{0,3}) - 3(O)$$

$$(m_1) = (A_{1,1}) + (A_{1,2}) + (-A_{1,1} - A_{1,2}) - 3(O)$$

$$(m_2) = (A_{1,3}) + (-A_{\infty,1} - A_{\infty,2}) + (A_{\infty,1} + A_{\infty,2} - A_{1,3}) - 3(O)$$

$$(n_1) = (-A_{0,1} - A_{0,2}) + (A_{\infty,3}) + (A_{0,1} + A_{0,2} - A_{\infty,3}) - 3(O)$$

$$(n_2) = (-A_{1,1} - A_{1,2}) + (A_{\infty,3}) + (A_{1,1} + A_{1,2} - A_{\infty,3}) - 3(O)$$

$$(N) = (A_{\infty,1}) + (A_{\infty,2}) + (-A_{\infty,1} - A_{\infty,2}) - 3(O)$$