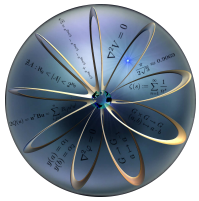

planetmath.org

Math for the people, by the people.

Selmer group

Canonical name	SelmerGroup
Date of creation	2013-03-22 13:50:55
Last modified on	2013-03-22 13:50:55
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	6
Author	alozano (2414)
Entry type	Definition
Classification	msc 14H52
Related topic	GroupCohomology
Related topic	RankOfAnEllipticCurve
Related topic	ArithmeticOfEllipticCurves
Defines	Selmer group
Defines	Tate-Shafarevich group

Given an elliptic curve E we can define two very interesting and important groups, the *Selmer group* and the *Tate-Shafarevich group*, which together provide a measure of the failure of the Hasse principle for elliptic curves, by measuring whether the curve is everywhere locally soluble. Here we present the construction of these groups.

Let E, E' be elliptic curves defined over $\mathbb{Q}$ and let $\bar{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Let $\phi\colon E \to E'$ be an non-constant isogeny (for example, we can let $E = E'$ and think of ϕ as being the "multiplication by n" map, $[n]\colon E \to E$). The following standard result asserts that ϕ is surjective over $\bar{\mathbb{Q}}$:

Theorem 1. *Let C_1, C_2 be curves defined over an algebraically closed field K and let*

$$\psi\colon C_1 \to C_2$$

be a morphism (or algebraic map) of curves. Then ψ is either constant or surjective.

Proof. See [**?**], Chapter II.6.8. □

Since $\phi\colon E(\bar{\mathbb{Q}}) \to E'(\bar{\mathbb{Q}})$ is non-constant, it must be surjective and we obtain the following exact sequence:

$$0 \to E(\bar{\mathbb{Q}})[\phi] \to E(\bar{\mathbb{Q}}) \to E'(\bar{\mathbb{Q}}) \to 0 \qquad (1)$$

where $E(\bar{\mathbb{Q}})[\phi] = \operatorname{Ker}\phi$. Let $G = \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, the absolute Galois group of $\mathbb{Q}$, and consider the i^{th}-cohomology group $H^i(G, E(\bar{\mathbb{Q}}))$ (we abbreviate by $H^i(G, E)$). Using equation (1) we obtain the following long exact sequence (see Proposition 1 in group cohomology):

$$0 \to H^0(G, E(\bar{\mathbb{Q}})[\phi]) \to H^0(G, E) \to H^0(G, E') \to H^1(G, E(\bar{\mathbb{Q}})[\phi]) \to H^1(G, E) \to H^1(G, E')$$

Note that

$$H^0(G, E(\bar{\mathbb{Q}})[\phi]) = (E(\bar{\mathbb{Q}})[\phi])^G = E(\mathbb{Q})[\phi]$$

and similarly

$$H^0(G, E) = E(\mathbb{Q}), \quad H^0(G, E') = E'(\mathbb{Q})$$

From (2) we can obtain an exact sequence:

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to H^1(G, E(\bar{\mathbb{Q}})[\phi]) \to H^1(G, E)[\phi] \to 0$$

We could repeat the same procedure but this time for E, E' defined over $\mathbb{Q}_p$,for some prime number p, and obtain a similar exact sequence but with coefficients in $\mathbb{Q}_p$ which relates to the original in the following commutative diagram (here $G_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$):

$$\begin{array}{ccccc} 0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to & H^1(G, E(\bar{\mathbb{Q}})[\phi]) & \to H^1(G,E)[\phi] \to 0 \\ \downarrow & \downarrow & \downarrow \\ 0 \to E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) \to & H^1(G_p, E(\bar{\mathbb{Q}}_p)[\phi]) & \to H^1(G_p,E)[\phi] \to 0 \end{array}$$

The goal here is to find a **finite** group containing $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$. Unfortunately $H^1(G, E(\bar{\mathbb{Q}})[\phi])$ is not necessarily finite. With this purpose in mind, we define the *ϕ-Selmer group*:

$$S^{\phi}(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(G, E(\bar{\mathbb{Q}})[\phi]) \to \prod_p H^1(G_p, E) \right)$$

Equivalently, the *ϕ-Selmer group* is the set of elements γ of $H^1(G, E(\bar{\mathbb{Q}})[\phi])$ whose image γ_p in $H^1(G_p, E(\bar{\mathbb{Q}}_\imath)[\phi])$ comes from some element in $E(\mathbb{Q}_p)$.

Finally, by imitation of the definition of the Selmer group, we define the *Tate-Shafarevich group*:

$$TS(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(G, E) \to \prod_p H^1(G_p, E) \right)$$

The Tate-Shafarevich group is precisely the group that measures the Hasse principle in the elliptic curve E. It is unknown if this group is finite.

References

[1] J.P. Serre, *Galois Cohomology*, Springer-Verlag, New York.

[2] James Milne, *Elliptic Curves*, `http://www.jmilne.org/math/CourseNotes/math679.html`onli course notes.

[3] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[4] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.