Why is an ideal class group a Tate-Schaferevich group?

Kevin Buzzard

February 7, 2012

Last modified 24/5/2005. Note in particular comment at the bottom of p3 saying "first three pages are making a meal of a triviality".

I have been asked the question in the title several times in my life and it's about time I wrote it up because for some reason not a lot of people seem to know it! I have no idea why not. Jan Nekovar told me it was true, but it's only now that I've bothered checking (some of) the details. I have also taken the trouble to construct the "Kummer sequence" for a number field—this was not logically necessary to show the analogy (and indeed took much longer than it did to show why the ideal class group was a Sha!), but it was an instructive exercise.

1 Abelian groups.

We say that an abelian group A is *divisible* if multiplication by n is a surjection $A \to A$ for all $n \in \mathbf{Z}_{\geq 1}$. We say that A is *uniquely divisible* if multiplication by n is an isomorphism $A \to A$ for all $n \in \mathbf{Z}_{\geq 1}$. One checks easily that being uniquely divisible is equivalent to being the underlying abelian group of a $\mathbf{Q}$-vector space (let $1/n$ act as the inverse of the isomorphism given by multiplication by n).

Lemma 1. *If A is a divisible abelian group then $A \otimes (\mathbf{Q}/\mathbf{Z}) = 0$.*

Proof. It suffices to prove that $a \otimes (m/n) = 0$ for any $a \in A$ and $m, n \in \mathbf{Z}$ with $n > 0$. But if $b \in A$ such that $nb = a$ then $a \otimes (m/n) = nb \otimes (m/n) = b \otimes m = 0$. □

If A is any abelian group then its torsion subgroup A_{tors} is the $a \in A$ such that there exists $n \in \mathbf{Z}_{\geq 1}$ such that $na = 0$.

Lemma 2. *If A is a divisible abelian group then A_{tors} is divisible and A/A_{tors} is uniquely divisible. Furthermore A/A_{tors} is canonically isomorphic to $A \otimes_{\mathbf{Z}} \mathbf{Q}$.*

Proof. If $n \in \mathbf{Z}_{\geq 1}$ and $a \in A_{\mathrm{tors}}$ then by divisibility of A there exists $b \in A$ such that $nb = a$; now b is easily checked to be in A_{tors}. This proves the first

part. The second follows easily from the first by applying the snake lemma to multiplication by n on the short exact sequence

$$0 \to A_{\mathrm{tors}} \to A \to A/A_{\mathrm{tors}} \to 0.$$

The last part can be checked using standard homological algebra: if one tensors $0 \to \mathbf{Z} \to \mathbf{Q} \to (\mathbf{Q}/\mathbf{Z}) \to 0$ with A then one gets a long exact sequence which ends

$$\mathrm{Tor}_1(\mathbf{Q}, A) \to \mathrm{Tor}_1(\mathbf{Q}/\mathbf{Z}, A) \to A \to A \otimes \mathbf{Q} \to A \otimes (\mathbf{Q}/\mathbf{Z}) \to 0.$$

Now $\mathbf{Q}$ is a flat $\mathbf{Z}$-module so $\mathrm{Tor}_1(\mathbf{Q}, A) = 0$, and $\mathrm{Tor}_1(\mathbf{Q}/\mathbf{Z}, A)$ is the torsion subgroup of A (see e.g. Weibel's homological algebra book, Proposition 3.1.3; this is the reason they're called Tor groups, so he says!), and $A \otimes (\mathbf{Q}/\mathbf{Z}) = 0$ by the above lemma, and this gives the result. Alternatively one can verify that the obvious maps $A/A_{\mathrm{tors}} \to A \otimes_{\mathbf{Z}} \mathbf{Q}$ and $A \otimes_{\mathbf{Z}} \mathbf{Q} \to A/A_{\mathrm{tors}}$ are well-defined and inverse to one another. □

2 Galois cohomology.

Now let K be a field and let G_K denote its absolute Galois group. Recall that a G_K-module M is said to be *discrete* if for all $m \in M$ there exists L/K finite and Galois such that G_L fixes m. Equivalently, $M = \lim_L M^{G_L}$ where the (direct) limit is over the finite Galois extensions L of K. Galois cohomology works well for such things—on the category of discrete G_K-modules, Galois cohomology is a derived functor and turns short exact sequences into long exact sequences (see for example Serre's "Cohomologie Galoisienne"). From now on, all Galois modules will be discrete.

Note that if a group G acts on a uniquely divisible module A then the fixed points A^G are also uniquely divisible, as if $n \in \mathbf{Z}_{\geq 1}$ then multiplication by n is a G-invariant isomorphism $A \to A$ which hence induces an isomorphism $A^G \to A^G$.

Lemma 3. *If M is a discrete G_K-module then $H^1(K, M)$ is torsion (that is, every element has finite order). If furthermore M is uniquely divisible then $H^1(K, M) = 0$.*

Proof. By definition $H^1(K, M)$ is the direct limit of $H^1(\mathrm{Gal}(L/K), M^{G_L})$ as L runs over the finite Galois extensions of K, and each of these groups is torsion (indeed $H^1(\mathrm{Gal}(L/K), M^{G_L})$ is annihiliated by the order of $\mathrm{Gal}(L/K)$), so this does the first part. For the second part note that M^{G_L} is uniquely divisible and hence multiplication by the order of $\mathrm{Gal}(L/K)$ on $H^1(\mathrm{Gal}(L/K), M^{G_L})$ is both zero and an isomorphism, showing that $H^1(\mathrm{Gal}(L/K), M^{G_L}) = 0$ for all L/K finite Galois, and hence that $H^1(K, M) = 0$. □

3 Galois cohomology of divisible discrete G_K-modules.

People in general seem to see these arguments for $E(\overline{K})$ when E is an elliptic curve, but the arguments are quite general. Somehow it seems that people know more about the cohomological interpretation of Selmer groups of elliptic curves (because this is how they are introduced in the theory nowadays) than they do about units and class groups for number fields (because they are typically taught about these via more hands-on methods), even though they both boil down to very similar things from a cohomological point of view.

Let A be a discrete G_K-module which is also a divisible abelian group. We have seen that there is a canonical short exact sequence

$$0 \to A_{\rm tors} \to A \to A \otimes \mathbf{Q} \to 0$$

and we note that both $A_{\rm tors}$ and $A \otimes \mathbf{Q} = A/A_{\rm tors}$ are also discrete G_K-modules. Taking cohomology we get a long exact sequence

$$A^{G_K} \to (A \otimes \mathbf{Q})^{G_K} \to H^1(K, A_{\rm tors}) \to H^1(K, A) \to 0,$$

the zero on the right because $A \otimes \mathbf{Q}$ is uniquely divisible. Let's analyse the second term a little more.

Lemma 4. *If A is divisible then $(A \otimes \mathbf{Q})^{G_K} = (A^{G_K}) \otimes \mathbf{Q}$.*

Proof. There is an obvious map from the right hand side to the left hand side. Here is its inverse: $A \otimes \mathbf{Q} = A/A_{\rm tors}$ and given a G_K-invariant element of $A/A_{\rm tors}$, lift it to $a \in A$. We know a is G_L-invariant for some finite Galois extension L of K, as A is discrete. Now for $\sigma \in {\rm Gal}(L/K)$ we know that $\sigma a - a$ is torsion. Choose $M \in \mathbf{Z}_{>0}$ such that M annihilates $\sigma a - a$ for all $\sigma \in {\rm Gal}(L/K)$. Then Ma is G_K-invariant. Our map sends a to $(Ma) \otimes (1/M) \in A^{G_K} \otimes \mathbf{Q}$. □

Note that if M is any abelian group then tensoring $0 \to \mathbf{Z} \to \mathbf{Q} \to (\mathbf{Q}/\mathbf{Z}) \to 0$ with M we deduce that $M \to M \otimes \mathbf{Q} \to M \otimes (\mathbf{Q}/\mathbf{Z}) \to 0$ is exact, and hence that $M \otimes (\mathbf{Q}/\mathbf{Z}) = M \otimes \mathbf{Q}/({\rm im}(M))$, where ${\rm im}(M)$ denotes the image of M in $M \otimes \mathbf{Q}$. Applying this with $M = A^{G_K}$ we have proved the following proposition.

Proposition 5. *If A is a divisible discrete G_K-module then there is an exact sequence*

$$0 \to A^{G_K} \otimes (\mathbf{Q}/\mathbf{Z}) \to H^1(K, A_{\rm tors}) \to H^1(K, A) \to 0.$$

I'll call this the *Kummer exact sequence* associated to A. The injection is usually called κ and the surjection λ. Note that the first and last terms are visibly torsion, and hence so is the middle term.

Note also that I have made a meal of deriving this! Jay Pottharst points out to me that direct limits are exact, so rather than typing out the last three pages

and thinking about divisible groups I could have just checked that the "usual" Kummer sequence

$$0 \to A^{G_K}/nA^{G_K} \to H^1(K, A[n]) \to H^1(K, A)[n] \to 0$$

was exact and then taken direct limits.

4 Elliptic curves.

If K is any field of characteristic zero (I haven't thought about to what extent these things work in characteristic p—there may or may not be problems) and E/K is an elliptic curve then $E(\overline{K})$ is a discrete G_K-module and it's also divisible (because multiplication is defined by polynomials and these have roots in $\overline{K}$). Hence the theory of the previous section applies and we deduce the standard Kummer sequence for an elliptic curve. Now assume K is a number field. Define $\mathrm{Sha}_E(K) \subseteq H^1(K, E(\overline{K}))$ to be the kernel of the natural restriction map $H^1(K, E(\overline{K})) \to \prod_v H^1(K_v, E(\overline{K}_v))$, the product over all places of K. Define $\mathrm{Sel}_E(K) \subseteq H^1(K, E(\overline{K})_{\mathrm{tors}})$ to be the pre-image of $\mathrm{Sha}_E(K)$ under the map $H^1(K, E(\overline{K})_{\mathrm{tors}}) \to H^1(K, E(\overline{K}))$. An easy diagram chase shows that $\mathrm{Sel}_E(K)$ is the kernel of the natural map

$$H^1(K, E(\overline{K}_{\mathrm{tors}})) \to \prod_v H^1(K_v, E(\overline{K}_v)_{\mathrm{tors}})/\operatorname{im}(\kappa_v)$$

where κ_v is the map from the local points $E(K_v) \otimes (\mathbf{Q}/\mathbf{Z})$ to $H^1(K_v, E(\overline{K}_v)_{\mathrm{tors}})$. We deduce that there is an exact sequence

$$0 \to E(K) \otimes (\mathbf{Q}/\mathbf{Z}) \to \mathrm{Sel}_E(K) \to \mathrm{Sha}_E(K) \to 0,$$

something which is very well-known to people working in elliptic curves.

5 Number fields.

Now let K be a number field, let $\overline{K}$ denote an algebraic closure, let $\overline{\mathcal{O}}$ denote the integers of $\overline{K}$, and let $A := \overline{\mathcal{O}}^\times$ denote the units in $\overline{\mathcal{O}}$, considered as a multiplicative group. Then A is a discrete G_K-module and a divisible group, as the nth root of a unit is a unit. Let μ denote the roots of unity in $\overline{\mathcal{O}}$. We deduce the existence of a short exact sequence

$$0 \to (\mathcal{O}_K^\times) \otimes (\mathbf{Q}/\mathbf{Z}) \to H^1(K, \mu) \to H^1(K, \overline{\mathcal{O}}^\times) \to 0.$$

An analogous short exact sequence exists if K is replaced by one of its completions at a finite place. Let's define $\mathrm{Sha}_{\mathcal{O}^\times}(K) \subseteq H^1(K, \overline{\mathcal{O}}^\times)$ to be the kernel of the natural restriction map $H^1(K, \overline{\mathcal{O}}^\times) \to \prod_{v<\infty} H^1(K_v, \overline{\mathcal{O}}_v^\times)$, where $\overline{\mathcal{O}}_v$ is the units in $\overline{K}_v$, and let's define $\mathrm{Sel}_{\mathcal{O}^\times}(K)$ to be $\lambda^{-1}(\mathrm{Sha}_{\mathcal{O}^\times}(K))$, where λ is the surjection in the above exact sequence. Then there is an exact sequence

$$0 \to (\mathcal{O}_K^\times) \otimes (\mathbf{Q}/\mathbf{Z}) \to \mathrm{Sel}_{\mathcal{O}^\times}(K) \to \mathrm{Sha}_{\mathcal{O}^\times}(K) \to 0.$$

Proposition 6. $\mathrm{Sha}_{\mathcal{O}^\times}(K)$ *is canonically isomorphic to the class group of* K*.*

Proof. Given a fractional ideal I of K, there exists a finite Galois extension L of K such that $I\mathcal{O}_L$ is principal (indeed L can be taken to be the class group of K—this was a conjecture of Hilbert, proved by Artin and Furtwängler). Let J denote the fractional ideal $I\mathcal{O}_L$. Then J is invariant under $\mathrm{Gal}(L/K)$ (which acts naturally on fractional ideals of L). Choose a generator t of J; then for all $\sigma \in \mathrm{Gal}(L/K)$ we deduce that $\sigma(t)$ and t generate the same fractional ideal, so $\sigma(t)/t \in \mathcal{O}_L^\times$. It is readily checked that this gives rise in the usual way to an element of $H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)$ and hence an element of $H^1(K, \overline{\mathcal{O}}^\times)$. Next one has to check that this construction is independent of choice of t (easy: this just changes the cocycle by a coboundary), of L (easy: all one has to do is check that if one makes L bigger then nothing changes, and this is clear because one doesn't have to change ones choice of t) and furthermore only depends on the ideal class of I (easy: changing t by an element of $K^\times$ doesn't change the cocycle). We deduce the existence of a natural map $\mathrm{Cl}(K) \to H^1(K, \overline{\mathcal{O}}^\times)$. We next claim that the image lies in $\mathrm{Sha}_{\mathcal{O}^\times}(K)$. In fact this is clear because the completion I_v of I at any finite place v of K is a principal fractional ideal of K_v (as all fractional ideals are principal) and localising the entire construction at v we see that we may choose $L = K_v$.

We now need to construct a map in the other direction. Say we have an element s of $\mathrm{Sha}_{\mathcal{O}^\times}(K)$. Let us choose a continuous cocycle $c : G_K \to \overline{\mathcal{O}}^\times$ representing s. Recall that $H^1(K, \overline{K}^\times) = 0$ by Hilbert 90, hence c represents a coboundary in this cohomology group and so there exists a finite Galois extension L of K and $t \in L^\times$ such that $c(\sigma) = \sigma(t)/t \in \mathcal{O}_L^\times$ for all $\sigma \in \mathrm{Gal}(L/K)$. This means that the fractional ideal $J = (t)$ of L is invariant under $\mathrm{Gal}(L/K)$. Of course this is not enough to descend it to K; for example the fractional ideal $(\sqrt{p})$ of $\mathbf{Q}(\sqrt{p})$ is Galois-invariant and doesn't come from $\mathbf{Q}$. However we can conclude that if v is a finite place of K then all places of L above v occur equally often in the factorization of J; hence J gives rise to an element $\sum a_v v \in I_K \otimes \mathbf{Q}$, where I_K denotes the fractional ideals of K. Here the a_v can be thought of as rational numbers, almost all of which are zero. This "rational" fractional ideal of K is well-defined modulo the image of $K^\times$ in $I_K \otimes \mathbf{Q}$, as it does not depend on t (easy: any two choices of t differ by an element of $K^\times$) or L (easy: take the same t) or the choice of cocycle (easy: bump up L so that the coboundary comes from $\mathcal{O}_L^\times$ and this doesn't change J). In particular the a_v give well-defined elements of $\mathbf{Q}/\mathbf{Z}$.

Finally we use the fact that $s \in \mathrm{Sha}_{\mathcal{O}^\times}(K)$ to deduce that our element of $I_K \otimes \mathbf{Q}$ is actually in I_K. This is an easy exercise because the local cohomology groups are easy to understand: the same construction as above but with K_v instead of K gives a finite extension L of K_v and a fractional ideal of L, thought of as an element of $I_{K_v} \otimes \mathbf{Q}/I_{K_v} = \mathbf{Q}/\mathbf{Z}$, the rational number so obtained being exactly a_v. So our local condition is that $a_v \in \mathbf{Z}$, which is exactly what we need to deduce that our rational fractional ideal is a fractional ideal. □

I should probably have broken up this last proof into easier-to-digest chunks

but I'm running out of energy and time for this now I can see my way through the argument.