Ways of obtaining Local and Global Class Field Theory

November 30, 2008

1 Formulations

Let K be a local or a global field; that is, K is a finite degree extension field of either $\mathbb{Q}_p$ or $\mathbb{Q}$; set $G = G_K; = \mathrm{Gal}(\bar{K}/K$ (or if you wish to include the function field case where K is of transcendence degree one over a finite field, you would take $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$).

As in Tate's notation, let A_K designate K^* or $C_K = J_K/K^*$ in the local and global cases respectively. For finite Galois extensions L/K we put $\mathcal{H}^*(L/K) := \hat{H}^*(\mathrm{Gal}(L/K); A_L)$. Passing to the inductive limit we put:

$$\mathcal{H}^*(*/K) := \lim_{K \subset L \subset \bar{K}} \mathcal{H}^*(L/K).$$

We will be making use of the notes (*Notes For Cohomology Lecture[s]* $4, 5$) regarding Class Formations, and in particular the axiom schemes, but here—in the next few subsections—are some "titles" for subsets of these axioms.

1.1 Size axioms

Let L/K be a cyclic extension of prime degree. The following cluster of axioms (taken all together) I'll refer to simply as "size axioms" for they have only to do with the size of various $\mathcal{H}^*(L/K)$. (I also refer to their CF-label given in the notes.)

- The "First Inequality" (CF0): $|\mathcal{H}^2(L/K)| \;=\; [L:K] \cdot |\mathcal{H}^1(L/K)|.$
- The "HT90 Axiom" (CF1)': $|\mathcal{H}^1(L/K)| \;=\; 0.$
- The "Second Inequality" (CF2, $\leq$)': $|\mathcal{H}^2(L/K)| \;\leq\; [L:K].$

Visibly, these are not entirely independent; specifically, the First Inequality plus either of the other two size axioms implies all three size axioms, and also implies that $|\mathcal{H}^2(L/K)| \;=\; [L:K]$ for L/K finite abelian.

1.2 The Brauer invariant axiom

This is put in a stronger form than the corresponding axiom (CF6)* in the notes, but here goes: We have a functorial identification

$$\mathcal{H}^2(*/K) \simeq \mathrm{Q}/\mathrm{Z}$$

where for finite extension fields L/K the homomorphism $\mathrm{res}_K^L : \mathcal{H}^2(*/K) \to \mathcal{H}^2(*/L)$ is identified with multiplication by $[L : K]$.

1.3 The "Existence" axiom

Any open subgroup W of finite index in A_K is a *norm subgroup*, i.e., there is an extension L/K such that $N_{L/K}A_L = W \subset A_K$. We may take L/K to be an abelian extension.

1.4 Global Reciprocity

This will not play the role of an "axiom" in our discussion below, but rather is a consequence of the size and Brauer invariant axioms of subsections 1.1 and 1.2 above. We use the terminology of Thursday's lecture.

Global Reciprocity: Let $a \in K^*$, and L/K a finite abelian extension, then

$$\prod_v (a_v, L_w/K_v) \;=\; 1,$$

where the product is taken over all places v of K, w is any choice of place of L above v, and $(a_v, L_w/K_v)$ is the local Artin symbol of the element $a = a_v \in K_v^*$ relative to the finite abelian extension L_w. Thus, $(a_v, L_w/K_v) = 1$ if and only if a_v is a norm from L_w.

2 Implications

- The size axioms + The Brauer invariant axiom $\Longrightarrow$ $\{G_K, A_K\}_K$ is a Class Formation.
- The Global size axioms + The Global Brauer invariant axiom $\Longrightarrow$ Global Reciprocity.
- The Global Second inequality + Global Reciprocity (+ Krasner's lemma) $\Longrightarrow$ The Local Second Inequality.

The last of these implications is a nice exercise for which here is a big hint: First use Krasner's Lemma to guarantee that any local (cyclic prime degree, say) extension comes from a global cyclic Galois extension L/K of the same degree in the sense that that there is a place v of K and a place w of L dividing v for which our initial local extension is isomorphic to L_w/K_v. Then consider the natural inclusion

$$K_v^* \stackrel{\iota_v}{\hookrightarrow} J_K$$

given by $\iota_v : a_v \mapsto (1, 1, \cdots, 1, a_v, 1 \cdots) \in J_K$. The question to ask is: what is the intersection of $K^* \cdot N_{L/K} J_L$ and $\iota_v(K_v^*)$ in J_K? The answer is that it is something of the form $b \cdot N_{L/K}(\beta)$ where $\beta \in J_L$ and where $b \in K^*$ is locally a norm from L/K for all places of K other than v. Global Reciprocity implies that it is also a a local norm at v giving us that

$$\iota_v : K_v^*/N_{L_w/K_v} L_w^* \hookrightarrow J_K/K^* \cdot N_{L/K} J_L = C_K/N_{L/K} C_L$$

is injective. Therefore the Global Second Inequality implies the Local Second Inequality.

3 The Local "Size Axioms"

3.1 The Local First Inequality

Here is a sketch of the proof of the Local First Inequality.

For any finite cyclic group Γ acting on any abelian group M put

$$h(\Gamma, M) = |\hat{H}^0(\Gamma, M)|/|\hat{H}^1(\Gamma, M)|$$

and recall that h is *exact* in the sense that the alternating product of the h's of a short exact sequence of Γ-modules is equal to 1; also if M is finite then $h(M) = 1$. The First inequality is the statement that if L/K is a finite cyclic extension of local fields (of prime degree), then $h(\mathrm{Gal}(L/K), L^*) = [L : K]$. Given the short exact sequence $0 \to \mathcal{O}_L^* \to L^* \to \mathrm{Z} \to 0$ and given that $h(\mathrm{Gal}(L/K), \mathrm{Z}) = [L : K]$ it suffices to show that $h(\mathrm{Gal}(L/K), \mathcal{O}_L^*) = 1$. For this, we show:

Lemma 1 *There is an open subgroup of finite index, $W \subset \mathcal{O}_L^*$, stable under the action of* $\mathrm{Gal}(L/K)$ *admitting a (*$\mathrm{Gal}(L/K)$*-equivariant) isomorphism*

$$W \simeq \mathcal{O}_K[\mathrm{Gal}(L/K)].$$

Proof. First find a $\mathrm{Gal}(L/K)$-stable subgroup W_1 of finite index in $\mathcal{O}_L*$ that is brought isomorphically via log to a $\mathrm{Gal}(L/K)$-stable $\mathcal{O}_K$-lattice in L^+ (which as $K[\mathrm{Gal}(L/K)]$-module is free of rank one, by the normal basis theorem). Argue then that the $\mathcal{O}_K[\mathrm{Gal}(L/K)]$-module W_1 contains a sub-$\mathcal{O}_K[\mathrm{Gal}(L/K)]$-module of finite index, $W \subset W_1$ such that $W \simeq \mathcal{O}_K[\mathrm{Gal}(L/K)]$.

Corollary 1 *Let $h(M)$ denote $h(\mathrm{Gal}(L/K), M)$. We have:*

$$h(\mathcal{O}_L^*) = h(W) = h(\mathcal{O}_K[\mathrm{Gal}(L/K)]) = 1.$$

Proof. Reading from left to right, the first two equalities come from Lemma 1 since the value of $h(M)$ is unchanged by modifications of M that are of finite index ; the last equality is because the $\mathcal{O}_K[\mathrm{Gal}(L/K)])$ module $\mathcal{O}_K[\mathrm{Gal}(L/K)])$ is cohomologically trivial.

3.2 Routes to the Local Size Axioms

- **Route 1:** Since we have the classical "Hilbert Theorem 90" the size axioms are verified by the discussion above, i.e., in subsection 3.1.
- **Route 2:** We might use the above discussion, forget that we ever knew anything about Hilbert's Theorem 90, but instead give a proof of the Second Inequality to establish the Local Size Axioms. For this there are two choices
  - **Route 2a:** Establish the Second inequality via a straightforward study of the local norm mapping.
  - **Route 2b:** A slightly more arduous (also more venerable[1]) road via Global Class Field Theory.
    * Recall that we have already established the *Global Second inequality.*
    * Prove Global Reciprocity.
    * Use the third bullet in the section *Implications* above to note that we therefore get the Local Second Inequality.

4 Route 2a: the Second Inequality via a detailed study of the norm mapping

4.1 The cokernel of the norm mapping

Here let K be local field, and for specificity, a field of finite degree over $\mathbb{Q}_p$. Let L/K be a finite extension, B/A the corresponding extension of rings of integers, and Let $B_n^* \subset B^*$, $A_n^* \subset A^*$ the n-th term in the corresponding standard filtrations ($B_n^* :=$ the elements of B^* congruent to 1 modulo the n-th power of a uniformizer of B and $A_n^* :=$ the elements of A^* congruent to 1 modulo the n-th power of a uniformizer of A.)

Let $N_{L/K} : L^* \to K^*$ and we must examine what this $N_{L/K}$ does to these filtrations.

4.2 The unramified case

Let L/K be a finite unramified (hence Galois, cyclic) extension of degree f. Let $G := \mathrm{Gal}(L/K)$. Choosing the same uniformizer $\pi \in A \subset K$ for L, we get splittings

$$K^* = A^* \times \mathbb{Z}; \qquad L^* = B^* \times \mathbb{Z}$$

and the Norm mapping $N_{L/K}$ preserves these splittings, and on the second factor is just multiplication by f. Once we show

[1] Also bewildering to me!

Lemma 2

$$N_{L/K}(B^*) = A^*$$

we would get:

Corollary 2 *$K^*/N_{L/K}L^*$ is cyclic of order f (in fact, it has a canonical generator: the image of any uniformizer of K, so is canonically $\mathrm{Z}/f\mathrm{Z}$). Identifying the image of any uniformizer in $K^*/N_{L/K}L^*$ with the Frobenius element in $\mathrm{Gal}(L/K)$ gives a canonical isomorphism*

$$K^*/N_{L/K}L^* \cong \mathrm{Gal}(L/K).$$

To show the above lemma, i.e., that $N_{L/K} : B^* \to A^*$ is surjective, we use the filtration, noting that $N_{\ell/k} : \ell^* \to k^*$ is surjective, and therefore it suffices to show that

1. $N_{L/K}$ preserves the standard filtrations of B^* and A^* so that it induces homomorphisms:

$$N_n : B^*_n/B^*_{n+1} \to A^*_n/A^*_{n+1}$$

(which, by the above, is an isomorphism for $n = 0$)

2. The homomorphisms N_n are all surjective ($n \geq 1$). (Actually, I suppose that if we know that they are surjective for $1 \leq n \leq n_0$ for n_0 sufficient large, this suffices, using Nakayama and our knowledge of the structure of these groups.)

Let $n \geq 1$. Note that, for $x \in B$, $N_{L/K}(1 + \pi^n x) = \prod_{g \in G}(1 + \pi^n g(x)) = 1 + \pi^n y$ for some $y \in A$, so the filtrations are indeed preserved; also y taken modulo π is the trace of x (modulo π) so surjectivity follows from surjectivity of $Tr_{\ell/k}$ (equivalently: from separability of the extension ℓ/k).

4.3 The case where L/K is a finite totally ramified extension

Here the strategy is to let $\Pi \in B$ be a uniformizer and put $\pi := N_{L/K}(\Pi) \in A$, using this π as our uniformizer for A. If we form our splittings

$$K^* \ = \ A^* \times \mathrm{Z}; \qquad L^* = B^* \times \mathrm{Z}$$

in terms of these uniformizers, we have that $N_{L/K}$ again respects the splittings but now is an isomorphism on the Z's, so we get

Lemma 3 *The natural homomorphism*

$$A^*/N_{L/K}B^* \to K^*/N_{L/K}L^*$$

is an isomorphism.

We are led to study $A^*/N_{L/K}B^*$. Visibly

$$N_{L/K}(B_1^*) = N_{L/K}(1 + \Pi \cdot B) \subset 1 + \pi A$$

and therefore $N_{L/K}$ induces a homomorphism

$$N_0 : B^*/B_1^* = k^* \to A^*/A_1^* = k^*$$

that is simply raising to the power $e = [L : K]$.

4.4 The tame case: where L/K is a finite totally ramified abelian extension of order e prime to p; preliminary discussion

In this case we already know that $\mathrm{Gal}(L/K)$ is canonically a subgroup of k^*, and hence cyclic. From the previous paragraph, since

$$B^* = B_1^* \times k^*; \qquad A^* = A_1^* \times k^*$$

if we prove:

Lemma 4 *

$$N_{L/K} : B_1^* \to A_1^*$$

is surjective

we would get the corollary

Corollary 3 *There is a canonical isomorphism*

$$A^*/N_{L/K}B^* \cong k^*/(k^*)^e.$$

Corollary 4 *Let $q := |k|$. The homomorphism $k^* \to k^*$ given by $x \mapsto x^{\frac{q-1}{e}}$ induces an isomorphism between $k^*/(k^*)^e$ and the cyclic subgroup of order e in k^*. Using the canonical identifications described above, this gives a canonical isomorphism*

$$K^*/N_{L/K}L^* \cong \mathrm{Gal}(L/K).$$

4.5 The wild case: where L/K is a finite totally ramified abelian extension of order a power of p; preliminary discussion

In this case, by the above, the homomorphism $N_0 : B^*/B_1^* \to A^*/A_1^*$ is an isomorphism, and therefore we have that

Lemma 5 *Both natural homomorphisms*

$$A_1^*/N_{L/K}B_1^* \to A^*/N_{L/K}B^* \to K^*/N_{L/K}L^*$$

are isomorphisms.

So–in this case—we are left with the task of trying to find a canonical isomorphism

$$A_1^*/N_{L/K}B_1^* \cong \mathrm{Gal}(L/K);$$

in particular, if L/K is of degree p we will want to show that $A_1^*/N_{L/K}B_1^*$ is of order p.

4.6 The norm mapping from B_1^* to A_1^* in the ramified case, with L/K of prime order p

Let $G = \mathrm{Gal}(L/K)$ be cyclic of order ℓ. Let Π be a uniformizer of L as above, and define the *index* of this L/K to be the integer $i \geq 0$ such that

$$g(\Pi)/\Pi \equiv 1 + \Pi^i u$$

for g a generator of $\mathrm{Gal}(L/K)$ and $u \in B^*$. Of course, $i = 0$ if and only if we are in the tamely ramified case, so if $i > 0$ then $\ell = p$, which is the case we'll soon revert to, below. The index i is independent of the Π and g chosen.

Here are the the two workhorse theorems we are headed towards proving:

Theorem 5 *1. The norm mapping $N_{L/K}$ sends $B_n^* \subset B^*$ to $A_n^* \subset A*$ for all $n \leq i$ and (therefore) induces a homomorphism of k-vector spaces*

$$N_n : B_n^*/B_{n+1}^* \to A_n^*/A_{n+1}^*$$

for all $n < i$.

2. For $n \geq i$ put $\tilde{n} := i + \ell(n - i)$

The norm mapping $N_{L/K}$ sends $B_{\tilde{n}}^* \subset B^*$ to $A_n^* \subset A*$ for all $n \geq i$ and (therefore) induces a homomorphism of k-vector spaces

$$N_n : B_{\tilde{n}}^*/B_{\tilde{n}+1}^* \to A_n^*/A_{n+1}^*$$

for all $n \geq i$.

If $n > 0$ we can identify B_n^*/B_{n+1}^* with the 1-dimensional vector space k by sending $1 + \Pi^n b$ to b modulo Π, and ditto for A_n^*/A_{n+1}^* (i.e., we send $1 + \pi^n a$ to a modulo π).

We have already treated N_0 which is simply given as the endomorphism of k^* that raises elements to the ℓ-th power. So assume that $n > 0$ and $\ell = p$.

In the statement of the theorem below we will make use of these identifications to give alternate formulations of the Norm mappings N_n viewed as $\mathbf{F}_p$-linear homomorphisms $N_n : k \to k$. Also, we use the same symbol to denote an element in B_n^* (resp., A_n^*) as its reduction in B_n^*/B_{n+1}^* (resp., A_n^*/A_{n+1}^*).

Theorem 6 *1. Let $n > i$.*

If $1 + x \in B_n^*$ we have

$$N_n(1 + x) = 1 + Tr_{L/K}(x) \in A_n^*/A_{n+1}^*.$$

In terms of the identifications signaled above, we may also say that $N_n : k \to k$ is a (k-linear) isomorphism of vector spaces (equivalently: there is a nonzero constant $a \in k$ such that $N_n(x) = ax$ for $x \in k$).

2. If $1 \le n < i$ and $1 + x \in B_n^*$ then

$$N_n(1 + x) = 1 + N_{L/k}(x) \in A_n^*/A_{n+1}^*.$$

In terms of the identifications signaled above, we may also say that $N_n : k \to k$ is an ($\mathbf{F}_p$-linear) isomorphism of vector spaces $N_n : k \to k$ of the form $N_n(x) = cx^p$ for all $x \in k$ where $c \in k$ is some nonzero constant.

3. If $1 \le n = i$ and $1 + x \in B_n^*$ then

$$N_n(1 + x) = 1 + Tr_{L/K}(x) + N_{L/k}(x) \in A_n^*/A_{n+1}^*.$$

In terms of the identifications signaled above, we may also say that $N_n : k \to k$ is a homomorphism of the form $N_n(x) = ax + bx^p$ for all $x \in k$, where $a, b \in k$ are nonzero constants.

A consequence of these theorems is the surjectivity of the norm mapping $N_{L/K} : B_1^* \to A_1^*$ in the tamely ramified case, i.e., Lemma 3 of section 4.3 of the previous handout and also therefore Corollaries 5 and 6 of that section.

Slithering around, using the snake lemma, gets you the following corollary out of our workhorse theorems.

Corollary 7 *Let L/K be a cyclic, ramified extension of degree p, and index i. The group $K^*/N_{L/K}L^*$ is canonically isomorphic to the cokernel of the homomorphism*

$$N_{i-1} : B_i^*/B_{i+1}^* \to A_i^*/A_{i+1}^*.$$

Let $n = i - 1$. Consider the mapping $G = \mathrm{Gal}(L/K) \to B_i^*/B_{i+1}^*$ given by $g \mapsto \frac{g(\Pi)}{\Pi}$. A simple argument shows this to be a homomorphism.

Proposition 1 *The above homomorphism fits into an exact sequence*

$$0 \to G \to B_i^*/B_{i+1}^* \to A_i^*/A_{i+1}^*$$

where the second homomorphism is our N_{i-1}.

Proof 1 *The mapping* $G \to B_i^*/B_{i+1}^*$ *is injective, since* i *is the index, as defined above. Since, after identification of* $N_{i-1} : B_i^*/B_{i+1}^* \to A_i^*/A_{i+1}^*$ *with the polynomial mapping from* k *to* k *given by the equation* $x \mapsto P(x) := ax + bx^p$ *we see that since* $P(X)$ *is of degree* p *it can have no more that* p *roots; on the other hand the image of* G *under the above injective homomorphism constitute* p *roots of* $P(X)$ *in* k *already, that's it: there are no more, and therefore the sequence is exact at its second station.*

Corollary 8 *The group* $K^*/N_{L/K}L^*$ *is cyclic of order* p*; i.e., isomorphic to* G*.*

Proof 2 *This follows since* B_i^*/B_{i+1}^* *and* A_i^*/A_{i+1}^* *are of the same cardinality.*

4.7 Back to general finite Galois extensions L/K; with $K/\mathbb{Q}_p$ of finite degree

Theorem 9 *Let* L/K *be an arbitrary finite Galois extension. We have the Second Inequality:*

$$\#\{K^*/N_{L/K}L^*\} \leq [L : K].$$

Proof 3 *:*

Lemma 6 *Let* $K \subset M \subset L$ *be finite field extensions where* L/K *and* M/K *are Galois. Suppose that we have the inequalities:*

$$\#\{K^*/N_{M/K}M^*\} \leq [M : K],$$

and

$$\#\{M^*/N_{L/M}L^*\} \leq [L : M].$$

It then follows that

$$\#\{K^*/N_{L/K}L^*\} \leq [L : K].$$

Proof 4 *Since*

$$[L : K] = [L : M] \cdot [M : K],$$

it suffices to prove sub-multiplicativity for the cokernel of the norms, which follows from the exact sequence

$$M^*/N_{L/M}L^* \to K^*/N_{L/K}L^* \to K^*/N_{M/K}M^* \to 0$$

where the first mapping is $N_{M/K}$*.*

To prove the theorem, note that the Galois group of any finite Galois extension L/K *is solvable, so has a Jordan Holder filtration, corresponding to a tower of fields* $K = K_1 \subset K_2 \subset \ldots \subset K_N = L$ *each of the successive extensions being Galois of prime order. For each of the* $K_{\nu+1}/K_\nu$*,*

then, we have shown—modulo the proof of our workhorse theorems—the equality:

$$\#\{K_\nu^*/N_{K_{\nu+1}/K_\nu}K_{\nu+1}^*\} \quad = \quad [K_{\nu+1} : K_\nu]$$

so the lemma implies the theorem.

4.8 Sketch of proofs of the workhorse theorems

We will reduce the proof to the following

Lemma 7 *

For $n \geq 1$ *we have that* $Tr_{L/K}(m_B^n) = m_A^{i+[\frac{n-i}{p}]}$.

Of course, the parallel statement for $N_{L/K}$ is a triviality:

Lemma 8 *For* $n \geq 1$ *we have that* $N_{L/K}(m_B^n) = m_A^n$.

Assume Lemma 7 for the moment.

Lemma 9 *Let* $n \geq 1$ *and* $1 + x \in B_n*$. *Then*

$$N_{L/K}(1+x) \equiv 1 + Tr_{L/K}(x) + N_{L/K}(x) \quad \mod \quad Tr_{L/K}(m_B^{2n}).$$

The idea of the proof of this is to expand $N_{L/K}(1+x) = \prod_{g \in G}(1+g(x))$ to get the above formuala plus intermediate terms and then note that the intermediate terms can be expressed as a sum of traces of certain "monomials" given as products of conjugates of x—more than one conjugate appearing.

We have now assembled all the equipment to prove the theorems. Here is the swing computation. Let $1 \leq n = i - 1$. We have these things going for us:

- If $1 + x \in B_n*$ we have $Tr_{L/K}(x) \in m_A^n$ *and* if $1 + x$ generates B_n^*/B_{n+1}^* then $Tr_{L/K}(x)$ generates m_A^n/m_A^{n+1}.
- If $1+x \in B_n*$ we have $N_{L/K}(x) \in m_A^n$ *and* if $1+x$ generates B_n^*/B_{n+1}^* then $N_{L/K}(x)$ generates m_A^n/m_A^{n+1}.

So our norm mapping brings B_n^*/B_{n+1}^* to A_n^*/A_{n+1}^* and in the formula of Lemma 9 both trace and norm terms play a role, since neither of them get absorbed when taken modulo A_{n+1}^*.

If, on the other hand, $1 \leq n < i - 1$ the trace term does get absorbed, leaving only the norm term, which doesn't.

If $n > i - 1$ it is a computation ....

5 The First Inequality; global case

Not Yet Written = NYW

6 The Local Brauer Invariant Axiom; local and global case

NYW

7 Paths to Existence

NYW, but let's at least mention that in the global case Kummer theory is the way to proceed, and in the local case there are two routes:

- Via Kummer Theory
- Via Lubin-Tate Formal groups