An introduction to global class field theory (Towards a p-adic Langlands correspondence)

José M. Tornero
tornero@us.es

Departamento de Álgebra
Universidad de Sevilla

October 2009

Contenido

Contenido

Contenido

Contenido

Contenido

Contenido

Contenido

Notation

Let k be a number field, $\mathcal{O}$ its ring of integers.

A place is an equivalence class of absolute values, called finite (whenever they are non–archimedean) or infinite (otherwise) Let P_k be the set of places of k.

Notation

Let k be a number field, $\mathcal{O}$ its ring of integers.

A place is an equivalence class of absolute values, called finite (whenever they are non–archimedean) or infinite (otherwise) Let P_k be the set of places of k.

Let $\mathfrak{p} \in P_k$ (either finite or infinite). We've got:

Notation

Let k be a number field, $\mathcal{O}$ its ring of integers.

A place is an equivalence class of absolute values, called finite (whenever they are non–archimedean) or infinite (otherwise) Let P_k be the set of places of k.

Let $\mathfrak{p} \in P_k$ (either finite or infinite). We've got:

a) $k_{\mathfrak{p}}$, the completion (which must be $\mathbf{R}$, $\mathbf{C}$ or a $\mathfrak{p}$–adic one).

b) $\mathcal{O}_{\mathfrak{p}} = \{\alpha \in k_{\mathfrak{p}}^* \mid |\alpha|_{\mathfrak{p}} \leq 1\}$, the ring of integers of $k_{\mathfrak{p}}$.

c) $U_{\mathfrak{p}} = \{\alpha \in k_{\mathfrak{p}}^* \mid |\alpha|_{\mathfrak{p}} = 1\}$, the group of units

Adèles

The ring of adèles of k, noted $\mathbf{A}_k$ is

$$\mathbf{A}_k = \left\{ (\alpha_{\mathfrak{p}})_{\mathfrak{p} \in P_k} \mid \alpha_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}} \text{ for almost all } \mathfrak{p} \in P_k \right\}$$

Adèles

The ring of adèles of k, noted $\mathbf{A}_k$ is

$$\mathbf{A}_k = \left\{ (\alpha_{\mathfrak{p}})_{\mathfrak{p} \in P_k} \mid \alpha_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}} \text{ for almost all } \mathfrak{p} \in P_k \right\}$$

This is also called the *restricted product* of the $k_{\mathfrak{p}}$ w.r.t $\mathcal{O}_{\mathfrak{p}} \subset k_{\mathfrak{p}}$.

It is a ring (adding and multiplying componentwise).

Adèles

The ring of adèles of k, noted $\mathbf{A}_k$ is

$$\mathbf{A}_k = \left\{ (\alpha_{\mathfrak{p}})_{\mathfrak{p} \in P_k} \mid \alpha_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}} \text{ for almost all } \mathfrak{p} \in P_k \right\}$$

This is also called the *restricted product* of the $k_{\mathfrak{p}}$ w.r.t $\mathcal{O}_{\mathfrak{p}} \subset k_{\mathfrak{p}}$.

It is a ring (adding and multiplying componentwise).

Easy example:

$$\mathbf{A}_{\mathbf{Q}} = \mathbf{R} \times \{(a_p) \mid a_p \in \mathbf{Q}_p \text{ and } a_p \in \mathbf{Z}_p \text{ for almost all } p\}.$$

Idèles (I)

The idèles of k, noted $\mathbf{I}_k$, is the unit group of $\mathbf{A}_k$ (which would usually be noted $\mathbf{A}_k^*$).

They may also be described as the restricted product of $k_{\mathfrak{p}}^*$ w.r.t. $U_{\mathfrak{p}}$.

Idèles (I)

The idèles of k, noted $\mathbf{I}_k$, is the unit group of $\mathbf{A}_k$ (which would usually be noted $\mathbf{A}_k^*$).

They may also be described as the restricted product of $k_\mathfrak{p}^*$ w.r.t. $U_\mathfrak{p}$.

$k \hookrightarrow k_\mathfrak{p}$ induces a diagonal embedding

$$K^* \hookrightarrow \mathbf{I}_k,$$

associating $a \in k^*$ with $(\alpha_\mathfrak{p})$ which is a at each $\mathfrak{p}$-component

Idèles (I)

The idèles of k, noted $\mathbf{I}_k$, is the unit group of $\mathbf{A}_k$ (which would usually be noted $\mathbf{A}_k^*$).

They may also be described as the restricted product of $k_{\mathfrak{p}}^*$ w.r.t. $U_{\mathfrak{p}}$.

$k \hookrightarrow k_{\mathfrak{p}}$ induces a diagonal embedding

$$K^* \hookrightarrow \mathbf{I}_k,$$

associating $a \in k^*$ with $(\alpha_{\mathfrak{p}})$ which is a at each $\mathfrak{p}$-component

Such elements are called *principal idèles*, they are a subgroup of $\mathbf{I}_k$ and the quotient

$$C_k = \mathbf{I}_k / k^*$$

is called the *idèle class group*. Its elements will be noted $[\alpha]$.

Idèles (II)

If $S \subset P_k$ is a finite set of places, we call

$$\mathbf{I}_k^S = \prod_{\mathfrak{p} \in S} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$$

the group of S–idèles, which is obviously a subgroup of $\mathbf{I}_k$.

Idèles (II)

If $S \subset P_k$ is a finite set of places, we call

$$\mathbf{I}_k^S = \prod_{\mathfrak{p} \in S} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$$

the group of S–idèles, which is obviously a subgroup of $\mathbf{I}_k$.

For instance, if S_∞ is the set of infinite places

Idèles (II)

If $S \subset P_k$ is a finite set of places, we call

$$\mathbf{I}_k^S = \prod_{\mathfrak{p}\in S} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}$$

the group of S–idèles, which is obviously a subgroup of $\mathbf{I}_k$.

For instance, if S_∞ is the set of infinite places

$$\mathbf{I}_k^{S_\infty} = \prod_{\mathfrak{p}|\infty} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\text{ finite}} U_{\mathfrak{p}},$$

where the first factors are either $\mathbf{R}^*$ or $\mathbf{C}^*$.

Idèles and FId_k

Let FId_k be the group of fractional ideals of k.

Idèles and FId_k

Let FId_k be the group of fractional ideals of k.

We can define

$$\begin{array}{ccc} \mathbf{I}_k & \longrightarrow & \mathrm{FId}_k \\ (\alpha_{\mathfrak{p}}) & \longmapsto & \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} \end{array}$$

Idèles and FId_k

Let FId_k be the group of fractional ideals of k.

We can define

$$\begin{array}{ccc} \mathbf{I}_k & \longrightarrow & \mathrm{FId}_k \\ (\alpha_{\mathfrak{p}}) & \longmapsto & \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} \end{array}$$

It is a surjective homomorphism, with kernel $\mathbf{I}_k^{S_\infty}$.

Idèles and Cl_k

Therefore we have an isomorphism

$$\mathbf{I}_k/\mathbf{I}_k^{S_\infty} \simeq \mathrm{FId}_k.$$

Idèles and Cl_k

Therefore we have an isomorphism

$$\mathbf{I}_k/\mathbf{I}_k^{S_\infty} \simeq \mathrm{FId}_k.$$

In this isomorphism principal idèles correspond to principal fractional ideals, and viceversa. Hence

Idèles and Cl_k

Therefore we have an isomorphism

$$\mathbf{I}_k / \mathbf{I}_k^{S_\infty} \simeq \mathrm{FId}_k.$$

In this isomorphism principal idèles correspond to principal fractional ideals, and viceversa. Hence

$$\mathbf{I}_k / \left(k^* \cdot \mathbf{I}_k^{S_\infty} \right) \simeq \mathrm{Cl}_k$$

Norm (I)

Let $\alpha = (\alpha_\mathfrak{p}) \in \mathbf{I}_k$. We define

$$|(\alpha_\mathfrak{p})|_\mathfrak{p} = |\alpha_\mathfrak{p}|_\mathfrak{p},$$

Norm (I)

Let $\alpha = (\alpha_{\mathfrak{p}}) \in \mathbf{I}_k$. We define

$$|(\alpha_{\mathfrak{p}})|_{\mathfrak{p}} = |\alpha_{\mathfrak{p}}|_{\mathfrak{p}},$$

and, subsequently,

$$|\alpha| = \prod_{\mathfrak{p}} |\alpha_{\mathfrak{p}}|_{\mathfrak{p}}.$$

We can assume
$$\begin{array}{lcl} \mathfrak{p} \text{ real} & \longrightarrow & |\cdot| \\ \mathfrak{p} \text{ complex} & \longrightarrow & |\cdot|^2 \\ \mathfrak{p} \text{ is over } p & \longrightarrow & |p|_{\mathfrak{p}} = 1/p \end{array}$$

Norm (I)

Let $\alpha = (\alpha_\mathfrak{p}) \in \mathbf{I}_k$. We define

$$|(\alpha_\mathfrak{p})|_\mathfrak{p} = |\alpha_\mathfrak{p}|_\mathfrak{p},$$

and, subsequently,

$$|\alpha| = \prod_\mathfrak{p} |\alpha_\mathfrak{p}|_\mathfrak{p}.$$

$$\text{We can assume} \quad \begin{array}{lcl} \mathfrak{p} \text{ real} & \longrightarrow & |\cdot| \\ \mathfrak{p} \text{ complex} & \longrightarrow & |\cdot|^2 \\ \mathfrak{p} \text{ is over } p & \longrightarrow & |p|_\mathfrak{p} = 1/p \end{array}$$

And, because of the product formula,

$$x \in k^* \implies |x| = 1.$$

Norm (II)

We have defined then a *norm* mapping

$$| \cdot | : \mathbf{I}_k \longrightarrow \mathbf{R}_+^*$$

which is a surjective group homomorphism (define an "inverse").

Norm (II)

We have defined then a *norm* mapping

$$|\cdot|: \mathbf{I}_k \longrightarrow \mathbf{R}_+^*$$

which is a surjective group homomorphism (define an "inverse").

We call its kernel

$$\mathbf{I}_k^0 = \{\alpha \in \mathbf{I}_k \mid |\alpha| = 1\}$$

which verifies $k^* \subset \mathbf{I}_k^0$.

Norm (II)

We have defined then a *norm* mapping

$$| \cdot | : \mathbf{I}_k \longrightarrow \mathbf{R}_+^*$$

which is a surjective group homomorphism (define an "inverse").

We call its kernel

$$\mathbf{I}_k^0 = \{\alpha \in \mathbf{I}_k \mid |\alpha| = 1\}$$

which verifies $k^* \subset \mathbf{I}_k^0$.

Therefore we can consider a norm (induced, and identically noted) on the idèle class group:

$$| \cdot | : C_k \longrightarrow \mathbf{R}_+^*$$

whose kernel, noted C_k^0 will be of some interest.

Topological groups

Topological groups are nice!

Topological groups

Topological groups are nice!

They consist of a group endowed with a topology, in such a way that product and inverse are continuous mappings.

Topological groups

Topological groups are nice!

They consist of a group endowed with a topology, in such a way that product and inverse are continuous mappings.

Big advantange: 1 is (almost) all that matters for local (and sometimes global) issues.

Not really much choice

We want $\mathbf{I}_k^S$ to be open subsets (subgroups) of $\mathbf{I}_k$ (a good reason in a while).

Not really much choice

We want $\mathbf{I}_k^S$ to be open subsets (subgroups) of $\mathbf{I}_k$ (a good reason in a while).

More specifically, we would like $\mathbf{I}_k^S$ to be open subgroups whenever $S_\infty \subset S$. But then

Not really much choice

We want $\mathbf{I}_k^S$ to be open subsets (subgroups) of $\mathbf{I}_k$ (a good reason in a while).

More specifically, we would like $\mathbf{I}_k^S$ to be open subgroups whenever $S_\infty \subset S$. But then

Theorem.– There exists a unique topology in $\mathbf{I}_k$ such that, if $S_\infty \subset S$ and S is finite, $\mathbf{I}_k^S$ is open.

Definition via neighbourhoods of 1

This topology, when defined by basic systems of neighbourhoods, is given (at 1) by

$$\prod_{\mathfrak{p}\in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}$$

Definition via neighbourhoods of 1

This topology, when defined by basic systems of neighbourhoods, is given (at 1) by

$$\prod_{\mathfrak{p}\in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}$$

where $W_{\mathfrak{p}}$ is a basic system of neighbourhoods of $1 \in k_{\mathfrak{p}}$, and S is finite, $S_\infty \subset S$.

Definition via neighbourhoods of 1

This topology, when defined by basic systems of neighbourhoods, is given (at 1) by

$$\prod_{\mathfrak{p}\in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}$$

where $W_{\mathfrak{p}}$ is a basic system of neighbourhoods of $1 \in k_{\mathfrak{p}}$, and S is finite, $S_\infty \subset S$.

Equivalently we can take

$$N(S,\epsilon) = \left\{ (\alpha_{\mathfrak{p}}) \mid |\alpha_{\mathfrak{p}}|_{\mathfrak{p}} = 1 \text{ if } \mathfrak{p} \notin S,\ |\alpha_{\mathfrak{p}} - 1|_{\mathfrak{p}} < \epsilon \text{ if } \mathfrak{p} \in S \right\}.$$

S–idèles are closed

Let $\mathfrak{p}$ be a place. Then the projection

$$\mathbf{I}_k \xrightarrow{\pi} k_{\mathfrak{p}}^*$$

is continuous (it is in $\mathbf{I}_k^{S_\infty}$, therefore in 1, therefore in $\mathbf{I}_k$).

S–idèles are closed

Let $\mathfrak{p}$ be a place. Then the projection

$$\mathbf{I}_k \xrightarrow{\pi} k_{\mathfrak{p}}^*$$

is continuous (it is in $\mathbf{I}_k^{S_\infty}$, therefore in 1, therefore in $\mathbf{I}_k$).

Then $\pi^{-1}(U_{\mathfrak{p}})$ is closed.

S–idèles are closed

Let $\mathfrak{p}$ be a place. Then the projection

$$\mathbf{I}_k \xrightarrow{\pi} k_{\mathfrak{p}}^*$$

is continuous (it is in $\mathbf{I}_k^{S_\infty}$, therefore in 1, therefore in $\mathbf{I}_k$).

Then $\pi^{-1}(U_{\mathfrak{p}})$ is closed.

And hence so it is

$$\mathbf{I}_k^S = \bigcap_{\mathfrak{p}\notin S} \pi^{-1}(U_{\mathfrak{p}}) .$$

Locally compactness

Let $S_\infty \subset S$ and consider

$$\mathbf{I}_k^S = \prod_{\mathfrak{p}\in S} k_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}.$$

Locally compactness

Let $S_\infty \subset S$ and consider

$$\mathbf{I}_k^S = \prod_{\mathfrak{p}\in S} k_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}.$$

The first factor is a finite product of locally compact spaces, while the second is a product of compact spaces.

Locally compactness

Let $S_\infty \subset S$ and consider

$$\mathbf{I}_k^S = \prod_{\mathfrak{p}\in S} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}.$$

The first factor is a finite product of locally compact spaces, while the second is a product of compact spaces.

Hence $\mathbf{I}_k^S$ is locally compact, and so it is $\mathbf{I}_k$.

So far, so good

$\mathbf{I}_k$ is a locally compact topological group.

So far, so good

$\mathbf{I}_k$ is a locally compact topological group.

If S is finite, $\mathbf{I}_k^S$ is a closed subgroup.

So far, so good

$\mathbf{I}_k$ is a locally compact topological group.

If S is finite, $\mathbf{I}_k^S$ is a closed subgroup.

If $S_\infty \subset S$, $\mathbf{I}_k^S$ is an open subgroup.

A bit more of idèles and FId_k

$\mathbf{I}_k^{S_\infty}$ is open and closed, therefore $\{1\}$ is open and closed in the quotient space $\mathbf{I}_k/\mathbf{I}_k^{S_\infty}$.

A bit more of idèles and FId_k

$\mathbf{I}_k^{S_\infty}$ is open and closed, therefore $\{1\}$ is open and closed in the quotient space $\mathbf{I}_k/\mathbf{I}_k^{S_\infty}$.

Then $\mathbf{I}_k/\mathbf{I}_k^{S_\infty}$ must be a discrete space.

A bit more of idèles and FId_k

$\mathbf{I}_k^{S_\infty}$ is open and closed, therefore $\{1\}$ is open and closed in the quotient space $\mathbf{I}_k/\mathbf{I}_k^{S_\infty}$.

Then $\mathbf{I}_k/\mathbf{I}_k^{S_\infty}$ must be a discrete space.

So, if we consider the discrete topology on FId_k, we have a homeomorphism

$$\mathbf{I}_k/\mathbf{I}_k^{S_\infty} \simeq \mathrm{FId}_k.$$

A bit more of norm

Remember that our norm homomorphism

$$| \cdot | : \mathbf{I}_k \longrightarrow \mathbf{R}_+^*$$

was surjective.

A bit more of norm

Remember that our norm homomorphism

$$| \cdot | : \mathbf{I}_k \longrightarrow \mathbf{R}_+^*$$

was surjective.

But it is also continuous. It is in $\mathbf{I}_k^{S_\infty}$, therefore in 1, therefore in $\mathbf{I}_k$.

A bit more of norm

Remember that our norm homomorphism

$$| \cdot | : \mathbf{I}_k \longrightarrow \mathbf{R}_+^*$$

was surjective.

But it is also continuous. It is in $\mathbf{I}_k^{S_\infty}$, therefore in 1, therefore in $\mathbf{I}_k$.

Its "inverse" is continuous as well, henceforth we have a homeomorphism

$$\mathbf{I}_k / \mathbf{I}_k^0 \simeq \mathbf{R}_+^*.$$

A bit more of k^*

Remember that k^* could be viewed as a subgroup of $\mathbf{I}_k$.

Proposition.– k^* is a discrete closed subgroup of $\mathbf{I}_k$.

A bit more of k^*

Remember that k^* could be viewed as a subgroup of $\mathbf{I}_k$.

Proposition.– k^* is a discrete closed subgroup of $\mathbf{I}_k$.

The proof basically consists of showing that $N(S_\infty, \epsilon) \cap k^* = \{1\}$, hence k^* is discrete.

A bit more of k^*

Remember that k^* could be viewed as a subgroup of $\mathbf{I}_k$.

Proposition.– k^* is a discrete closed subgroup of $\mathbf{I}_k$.

The proof basically consists of showing that $N(S_\infty, \epsilon) \cap k^* = \{1\}$, hence k^* is discrete.
As a corollary, we have a locally compact topology in C_k.

A bit more of C_k^0

$$C_k^0 = \{[\alpha] \in C_k \mid |[\alpha]| = 1\}$$

Proposition.– C_k^0 is compact.

A bit more of C_k^0

$$C_k^0 = \{[\alpha] \in C_k \mid \|[\alpha]\| = 1\}$$

Proposition.– C_k^0 is compact.

The proof chooses a big enough $\rho > 0$ such that any idèle of such norm is k^*–congruent to another whose components are all of smaller norm (yes, you can do that).

A bit more of C_k^0

$$C_k^0 = \{[\alpha] \in C_k \mid \|[\alpha]\| = 1\}$$

Proposition.– C_k^0 is compact.

The proof chooses a big enough $\rho > 0$ such that any idèle of such norm is k^*–congruent to another whose components are all of smaller norm (yes, you can do that).

The set of such idèles is compact, so the original set of idèles with norm ρ is also compact (closed subset) and it is homeomorphic to C_k^0.

Why is important that C_k^0 is compact? (I)

Remember we had

$$\mathbf{I}_k / \left(k^* \cdot \mathbf{I}_k^{S_\infty} \right) \simeq \mathrm{Cl}_k$$

Why is important that C_k^0 is compact? (I)

Remember we had

$$\mathbf{I}_k / \left(k^* \cdot \mathbf{I}_k^{S_\infty} \right) \simeq \mathrm{Cl}_k$$

Then, for an element in Cl_k we have a class $[\alpha] \in C_k$ modulo the projection of $\mathbf{I}_k^{S_\infty}$.

Why is important that C_k^0 is compact? (I)

Remember we had

$$\mathbf{I}_k / \left(k^* \cdot \mathbf{I}_k^{S_\infty} \right) \simeq \mathrm{Cl}_k$$

Then, for an element in Cl_k we have a class $[\alpha] \in C_k$ modulo the projection of $\mathbf{I}_k^{S_\infty}$.

This means we can pick an idèle α on it in such a way that $|\alpha| = 1$ (adjusting the norm at the infinite places). We have then a map

$$C_k^0 \longrightarrow \mathrm{Cl}_k$$

which is surjective.

Why is important that C_k^0 is compact? (II)

As C_k^0 is compact, so is Cl_k (for the discrete topology), hence it must be finite.

Why is important that C_k^0 is compact? (II)

As C_k^0 is compact, so is Cl_k (for the discrete topology), hence it must be finite.

Another corollary is:

Theorem (Dirichlet).– The group U_k has rank $r+s-1$ (where r is the number of real places and s is the number of complex places).

Why is important that C_k^0 is compact? (II)

As C_k^0 is compact, so is Cl_k (for the discrete topology), hence it must be finite.

Another corollary is:

Theorem (Dirichlet).– The group U_k has rank $r+s-1$ (where r is the number of real places and s is the number of complex places).

The proof is somehow more involved (lattices and so on).

A word on open subgroups (I)

We will call a finite formal sum

$$\mathfrak{m} = \sum_{\mathfrak{p} \in P_k} n_{\mathfrak{p}} \mathfrak{p},$$

$$\text{where} \quad \begin{array}{ll} n_{\mathfrak{p}} = 0 & \text{almost always} \\ n_{\mathfrak{p}} = 0, 1 & \text{if } \mathfrak{p} \text{ is real} \\ n_{\mathfrak{p}} = 0 & \text{if } \mathfrak{p} \text{ is complex} \end{array} \quad \text{a divisor.}$$

A word on open subgroups (I)

We will call a finite formal sum

$$\mathfrak{m} = \sum_{\mathfrak{p} \in P_k} n_{\mathfrak{p}} \mathfrak{p},$$

where $\begin{array}{ll} n_{\mathfrak{p}} = 0 & \text{almost always} \\ n_{\mathfrak{p}} = 0, 1 & \text{if } \mathfrak{p} \text{ is real} \\ n_{\mathfrak{p}} = 0 & \text{if } \mathfrak{p} \text{ is complex} \end{array}$ a divisor.

Let us write $\operatorname{supp}(\mathfrak{m}) = \{\mathfrak{p} \mid n_{\mathfrak{p}} \neq 0\}$.

A word on open subgroups (I)

We will call a finite formal sum

$$\mathfrak{m} = \sum_{\mathfrak{p}\in P_k} n_{\mathfrak{p}}\mathfrak{p},$$

where $\begin{array}{ll} n_{\mathfrak{p}} = 0 & \text{almost always} \\ n_{\mathfrak{p}} = 0,1 & \text{if } \mathfrak{p} \text{ is real} \\ n_{\mathfrak{p}} = 0 & \text{if } \mathfrak{p} \text{ is complex} \end{array}$ a divisor.

Let us write $\operatorname{supp}(\mathfrak{m}) = \{\mathfrak{p} \mid n_{\mathfrak{p}} \neq 0\}$.

Variants: modulus, module, formal product of places, replete divisor,...

Also (in fact, normally) written $\mathfrak{m} = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$.

A word on open subgroups (II)

Let us define the following sets:

A word on open subgroups (II)

Let us define the following sets:

If $\mathfrak{p} \in \operatorname{supp}(\mathfrak{m})$ and it is non–archimedian, then

$$W_{\mathfrak{m}}(\mathfrak{p}) = \left\{ \alpha \in k_{\mathfrak{p}}^{*} \mid \alpha \equiv 1 \mod \mathfrak{p}^{n_{\mathfrak{p}}} \right\} = 1 + \mathfrak{p}^{n_{\mathfrak{p}}}.$$

A word on open subgroups (II)

Let us define the following sets:

If $\mathfrak{p} \in \operatorname{supp}(\mathfrak{m})$ and it is non–archimedian, then

$$W_{\mathfrak{m}}(\mathfrak{p}) = \left\{ \alpha \in k_{\mathfrak{p}}^* \mid \alpha \equiv 1 \mod \mathfrak{p}^{n_{\mathfrak{p}}} \right\} = 1 + \mathfrak{p}^{n_{\mathfrak{p}}}.$$

If $\mathfrak{p} \in \operatorname{supp}(\mathfrak{m})$ and it is archimedian, then

$$W_{\mathfrak{m}}(\mathfrak{p}) = \mathbf{R}_+^*.$$

Yet another word on open subgroups

Define now the subset:

Yet another word on open subgroups

Define now the subset:

$$\mathbf{I}_{\mathfrak{m}} = \left(\prod_{\mathfrak{p} \notin \mathrm{supp}(\mathfrak{m})} k_{\mathfrak{p}}^{*} \times \prod_{\mathfrak{p} \in \mathrm{supp}(\mathfrak{m})} W_{\mathfrak{m}}(\mathfrak{p}) \right) \cap \mathbf{I}_{k}.$$

Yet another word on open subgroups

Define now the subset:

$$\mathbf{I}_{\mathfrak{m}} = \left(\prod_{\mathfrak{p} \notin \mathrm{supp}(\mathfrak{m})} k_{\mathfrak{p}}^{*} \times \prod_{\mathfrak{p} \in \mathrm{supp}(\mathfrak{m})} W_{\mathfrak{m}}(\mathfrak{p}) \right) \cap \mathbf{I}_{k}.$$

That is, (α) such that
$$\begin{array}{ll} \alpha_{\mathfrak{p}} \in k_{\mathfrak{p}}^{*} & \text{for all } \mathfrak{p} \\ \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}} & \text{for almost all } \mathfrak{p} \\ \alpha_{\mathfrak{p}} \in W_{\mathfrak{m}}(\mathfrak{p}) & \text{for all } \mathfrak{p} \in \mathrm{supp}(\mathfrak{m}) \end{array}$$

A penultimate word on open subgroups

Then we consider the sets

$$W_{\mathfrak{m}} = \{(\alpha_{\mathfrak{p}}) \in \mathbf{I}_m \mid \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}},\ \text{for all } \mathfrak{p} \text{ finite, } \mathfrak{p} \notin \operatorname{supp}(\mathfrak{m})\}$$

A penultimate word on open subgroups

Then we consider the sets

$$W_{\mathfrak{m}} = \{(\alpha_{\mathfrak{p}}) \in \mathbf{I}_m \mid \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}, \text{ for all } \mathfrak{p} \text{ finite}, \mathfrak{p} \notin \operatorname{supp}(\mathfrak{m})\}$$

In other words:

$$W_{\mathfrak{m}} = \prod_{\text{infinite } \mathfrak{p} \notin \operatorname{supp}(\mathfrak{m})} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \in \operatorname{supp}(\mathfrak{m})} W_{\mathfrak{m}}(\mathfrak{p}) \times \prod_{\text{finite } \mathfrak{p} \notin \operatorname{supp}(\mathfrak{m})} U_{\mathfrak{p}}$$

A penultimate word on open subgroups

Then we consider the sets

$$W_{\mathfrak{m}} = \{(\alpha_{\mathfrak{p}}) \in \mathbf{I}_m \mid \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}},\ \text{for all } \mathfrak{p} \text{ finite, } \mathfrak{p} \notin \operatorname{supp}(\mathfrak{m})\}$$

In other words:

$$W_{\mathfrak{m}} = \prod_{\text{infinite } \mathfrak{p} \notin \operatorname{supp}(\mathfrak{m})} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \in \operatorname{supp}(\mathfrak{m})} W_{\mathfrak{m}}(\mathfrak{p}) \times \prod_{\text{finite } \mathfrak{p} \notin \operatorname{supp}(\mathfrak{m})} U_{\mathfrak{p}}$$

That is, (α) such that
$$\begin{array}{ll} \alpha_{\mathfrak{p}} \in k_{\mathfrak{p}}^* & \text{for all } \mathfrak{p} \text{ infinte} \\ \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}} & \text{for all } \mathfrak{p} \text{ finite} \\ \alpha_{\mathfrak{p}} \in W_{\mathfrak{m}}(\mathfrak{p}) & \text{for all } \mathfrak{p} \in \operatorname{supp}(\mathfrak{m}) \end{array}$$

A last word on open subgroups

$W_{\mathfrak{m}}$ is called the congruence subgroup of $\mathfrak{m}$.

A last word on open subgroups

$W_{\mathfrak{m}}$ is called the congruence subgroup of $\mathfrak{m}$.

$W_{\mathfrak{m}}$ is an open subgroup of $\mathbf{I}_k$.

AND

A last word on open subgroups

$W_{\mathfrak{m}}$ is called the congruence subgroup of $\mathfrak{m}$.

$W_{\mathfrak{m}}$ is an open subgroup of $\mathbf{I}_k$.

AND

Every open subgroup of $\mathbf{I}_k$ must contain some congruence subgroup $W_{\mathfrak{m}}$.

The canonical embedding

Let $K|k$ be a finite extension of number fields. Then we have a canonical embedding

$$\begin{array}{ccc} \mathbf{A}_k & \longrightarrow & \mathbf{A}_K \\ (\alpha_{\mathfrak{p}}) & \longmapsto & (\alpha_{\mathfrak{P}}), \text{ where } \alpha_{\mathfrak{P}} = \alpha_{\mathfrak{p}}, \text{ whenever } \mathfrak{P}|\mathfrak{p} \end{array}$$

The canonical embedding

Let $K|k$ be a finite extension of number fields. Then we have a canonical embedding

$$\begin{array}{ccc} \mathbf{A}_k & \longrightarrow & \mathbf{A}_K \\ (\alpha_{\mathfrak{p}}) & \longmapsto & (\alpha_{\mathfrak{P}}),\ \text{where } \alpha_{\mathfrak{P}} = \alpha_{\mathfrak{p}},\ \text{whenever } \mathfrak{P}|\mathfrak{p} \end{array}$$

It is, in fact, an injective homomorphism which induces also an embedding $\mathbf{I}_k \hookrightarrow \mathbf{I}_K$.

The canonical embedding

Let $K|k$ be a finite extension of number fields. Then we have a canonical embedding

$$\begin{array}{rcl} \mathbf{A}_k & \longrightarrow & \mathbf{A}_K \\ (\alpha_{\mathfrak{p}}) & \longmapsto & (\alpha_{\mathfrak{P}}),\ \text{where } \alpha_{\mathfrak{P}} = \alpha_{\mathfrak{p}},\ \text{whenever } \mathfrak{P}|\mathfrak{p} \end{array}$$

It is, in fact, an injective homomorphism which induces also an embedding $\mathbf{I}_k \hookrightarrow \mathbf{I}_K$.

Remark.– If $\mathfrak{P}, \mathfrak{P}'|\mathfrak{p}$ then for all $\alpha \in \mathbf{I}_k$, $\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{P}'}$ (criterion for being in $\mathbf{I}_k$).

Idèles and field isomorphisms

Let $\sigma : L \longrightarrow K$ be a field isomorphism, $\mathfrak{P}$ a place in L.

Idèles and field isomorphisms

Let $\sigma : L \longrightarrow K$ be a field isomorphism, $\mathfrak{P}$ a place in L.

It induces an isomorphism (an isometry actually) $\sigma : L_{\mathfrak{P}} \longrightarrow K_{\sigma\mathfrak{P}}$.

Idea: Take $\mathfrak{P}$–limits to $\sigma\mathfrak{P}$–limits.

Idèles and field isomorphisms

Let $\sigma : L \longrightarrow K$ be a field isomorphism, $\mathfrak{P}$ a place in L.

It induces an isomorphism (an isometry actually) $\sigma : L_{\mathfrak{P}} \longrightarrow K_{\sigma\mathfrak{P}}$.

Idea: Take $\mathfrak{P}$–limits to $\sigma\mathfrak{P}$–limits.

As for idèles is concerned α goes to $\sigma\alpha$, where

$$\alpha_{\mathfrak{P}} \in L_{\mathfrak{P}} \implies (\sigma\alpha)_{\sigma\mathfrak{P}} = \sigma\left(\alpha_{\mathfrak{P}}\right) \in K_{\sigma\mathfrak{P}}.$$

Galois descent for idèles (I)

Let $K|k$ be a Galois extension with Galois group G.

Galois descent for idèles (I)

Let $K|k$ be a Galois extension with Galois group G.

$\sigma \in G$ is an automorphism of K, therefore induces an automorphism

$$\sigma : \mathbf{I}_K \longrightarrow \mathbf{I}_K,$$

making $\mathbf{I}_K$ a G–module.

Galois descent for idèles (I)

Let $K|k$ be a Galois extension with Galois group G.

$\sigma \in G$ is an automorphism of K, therefore induces an automorphism

$$\sigma : \mathbf{I}_K \longrightarrow \mathbf{I}_K,$$

making $\mathbf{I}_K$ a G–module.

As usual:

$$\mathbf{I}_K^G = \{\alpha \in \mathbf{I}_K \mid \sigma\alpha = \alpha,\ \forall \sigma \in G\}.$$

Galois descent for idèles (II)

Theorem.– $\mathbf{I}_K^G = \mathbf{I}_k$.

Galois descent for idèles (II)

Theorem.– $\mathbf{I}_K^G = \mathbf{I}_k$.

If $\alpha = (\alpha_{\mathfrak{P}}) \in \mathbf{I}_K^G$, then $\alpha_{\sigma\mathfrak{P}} = (\sigma\alpha)_{\sigma\mathfrak{P}}$.

Galois descent for idèles (II)

Theorem.– $\mathbf{I}_K^G = \mathbf{I}_k$.

If $\alpha = (\alpha_{\mathfrak{P}}) \in \mathbf{I}_K^G$, then $\alpha_{\sigma\mathfrak{P}} = (\sigma\alpha)_{\sigma\mathfrak{P}}$.

Then, if we take $\sigma \in \mathrm{Gal}\,(K_{\mathfrak{P}}|k_{\mathfrak{p}})$, $\sigma\mathfrak{P} = \mathfrak{P}$, and then $\alpha_{\mathfrak{P}} \in k_{\mathfrak{p}}^*$.

For an arbitrary σ, it takes $\mathfrak{P}$ into $\mathfrak{P}'$ which also divides $\mathfrak{p}$. Then α begin fixed implies $\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{P}'}$, hence $\alpha \in \mathbf{I}_k$.

Norm (revisited)

Take $\alpha \in \mathbf{I}_K$, $\mathfrak{P} \in P_K$ (a place in K).

Multiplication by $\alpha_{\mathfrak{P}}$ is a $k_{\mathfrak{p}}$–linear automorphism of $K_{\mathfrak{P}}$, and its determinant is set to be

$$N_{K_{\mathfrak{P}}|k_{\mathfrak{p}}}(\alpha_{\mathfrak{P}}) \in k_{\mathfrak{p}}.$$

Norm (revisited)

Take $\alpha \in \mathbf{I}_K$, $\mathfrak{P} \in P_K$ (a place in K).

Multiplication by $\alpha_{\mathfrak{P}}$ is a $k_{\mathfrak{p}}$–linear automorphism of $K_{\mathfrak{P}}$, and its determinant is set to be

$$N_{K_{\mathfrak{P}}|k_{\mathfrak{p}}}(\alpha_{\mathfrak{P}}) \in k_{\mathfrak{p}}.$$

In fact, these local norms induce a global norm $\mathbf{I}_K \longrightarrow \mathbf{I}_k$.

Let $\alpha \in \mathbf{I}_K$, then

$$N_{K|k}(\alpha)_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} N_{K_{\mathfrak{P}}|k_{\mathfrak{p}}}(\alpha_{\mathfrak{P}})$$

Norm (revisited)

Take $\alpha \in \mathbf{I}_K$, $\mathfrak{P} \in P_K$ (a place in K).

Multiplication by $\alpha_{\mathfrak{P}}$ is a $k_{\mathfrak{p}}$–linear automorphism of $K_{\mathfrak{P}}$, and its determinant is set to be

$$N_{K_{\mathfrak{P}}|k_{\mathfrak{p}}}(\alpha_{\mathfrak{P}}) \in k_{\mathfrak{p}}.$$

In fact, these local norms induce a global norm $\mathbf{I}_K \longrightarrow \mathbf{I}_k$.

Let $\alpha \in \mathbf{I}_K$, then

$$N_{K|k}(\alpha)_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} N_{K_{\mathfrak{P}}|k_{\mathfrak{p}}}(\alpha_{\mathfrak{P}})$$

Proposition.– The set $N_{K|k}\mathbf{I}_K$ is an open and closed subgroup of $\mathbf{I}_k$.

The embedding of the idèle class groups

The embedding $\mathbf{I}_k \hookrightarrow \mathbf{I}_K$ takes clearly principal idèles into principal idèles.

The embedding of the idèle class groups

The embedding $\mathbf{I}_k \hookrightarrow \mathbf{I}_K$ takes clearly principal idèles into principal idèles.

Proposition.– If $K|k$ is finite, then $\mathbf{I}_k \hookrightarrow \mathbf{I}_K$ induces an injection

$$C_k \hookrightarrow C_K.$$

The embedding of the idèle class groups

The embedding $\mathbf{I}_k \hookrightarrow \mathbf{I}_K$ takes clearly principal idèles into principal idèles.

Proposition.– If $K|k$ is finite, then $\mathbf{I}_k \hookrightarrow \mathbf{I}_K$ induces an injection

$$C_k \hookrightarrow C_K.$$

Mind that injectivity requires proving $\mathbf{I}_k \cap K^* = k^*$, which is not very difficult taking $L|k$ a Galois extension such that $k \subset K \subset L$.

Norm on the idèle class group

Remark.– If $x \in K^*$, then $N_{K|k}(x)$ has the same meaning as idèle in $\mathbf{I}_k$ and as element of k^* (therefore as idèle).

Norm on the idèle class group

Remark.– If $x \in K^*$, then $N_{K|k}(x)$ has the same meaning as idèle in $\mathbf{I}_k$ and as element of k^* (therefore as idèle).

Proposition.– The norm $N_{K|k}$ induces a norm map

$$N_{K|k} : C_K \longrightarrow C_k.$$

Norm on the idèle class group

Remark.– If $x \in K^*$, then $N_{K|k}(x)$ has the same meaning as idèle in $\mathbf{I}_k$ and as element of k^* (therefore as idèle).

Proposition.– The norm $N_{K|k}$ induces a norm map

$$N_{K|k} : C_K \longrightarrow C_k.$$

In fact, the set $N_{K|k} C_K$ is an open and closed subgroup of C_k (easy from the idèle case).

Galois descent for idèle class group

Proposition.– Let $K|k$ be Galois, G its Galois group. Then C_K is a G–module and $C_K^G = C_k$.

Galois descent for idèle class group

Proposition.– Let $K|k$ be Galois, G its Galois group. Then C_K is a G–module and $C_K^G = C_k$.

We begin with the following exact sequence

$$1 \to K^* \longrightarrow \mathbf{I}_K \longrightarrow C_K \to 1$$

Then take G–fixed elements

$$1 \to (K^*)^G \longrightarrow \mathbf{I}_K^G \longrightarrow C_K^G \longrightarrow H^1(G, K^*)$$

Galois descent for idèle class group

Proposition.– Let $K|k$ be Galois, G its Galois group. Then C_K is a G–module and $C_K^G = C_k$.

We begin with the following exact sequence

$$1 \to K^* \longrightarrow \mathbf{I}_K \longrightarrow C_K \to 1$$

Then take G–fixed elements

$$1 \to (K^*)^G \longrightarrow \mathbf{I}_K^G \longrightarrow C_K^G \longrightarrow H^1(G, K^*)$$

And then, by Hilbert–Noether's Theorem 90,

$$1 \to k^* \longrightarrow \mathbf{I}_k \longrightarrow C_K^G \to 1.$$

Here comes the cohomology!

Here comes the cohomology!

End of Part I

Here comes the cohomology!

End of Part I

Coffee? Anyone?

The set–up

Let M be a G–module (think of G a Galois group, M a number field).

The set–up

Let M be a G–module (think of G a Galois group, M a number field).

Define the G–norm:

$$N_G(m) = \prod_{g \in G} g(m), \quad m \in M.$$

The set–up

Let M be a G–module (think of G a Galois group, M a number field).

Define the G–norm:

$$N_G(m) = \prod_{g \in G} g(m), \quad m \in M.$$

And consider the groups

$$M^G = \{m \in M \mid g(m) = m, \ \forall g \in G\}$$

$$I_G(M) = \langle g(m) \cdot m^{-1} \mid m \in M, \ g \in G \rangle$$

The Tate cohomology

We define (actually, Tate did) the Tate cohomology groups as:

The Tate cohomology

We define (actually, Tate did) the Tate cohomology groups as:

$$H_T^r(G,M) = \begin{cases} H^r(G,M) & \text{for } r > 0 \\ M^G/N_G(M) & \text{for } r = 0 \\ \ker(N_G)/I_G(M) & \text{for } r = -1 \\ H_{-r-1}(G,M) & \text{for } r < -1 \end{cases}$$

The Tate cohomology

We define (actually, Tate did) the Tate cohomology groups as:

$$H_T^r(G,M) = \begin{cases} H^r(G,M) & \text{for } r > 0 \\ M^G/N_G(M) & \text{for } r = 0 \\ \ker(N_G)/I_G(M) & \text{for } r = -1 \\ H_{-r-1}(G,M) & \text{for } r < -1 \end{cases}$$

It fits together homology and cohomology groups, via the induced homomorphism

$$N_G : H_0 = M/I_G(M) \longrightarrow M^G$$

The Tate long sequence

One of the most useful tools related to Tate cohomology is the following:

The Tate long sequence

One of the most useful tools related to Tate cohomology is the following:

Proposition.– Let

$$1 \to M' \longrightarrow M \longrightarrow M'' \to 1$$

be a short exact sequence.

The Tate long sequence

One of the most useful tools related to Tate cohomology is the following:

Proposition.– Let

$$1 \to M' \longrightarrow M \longrightarrow M'' \to 1$$

be a short exact sequence.

There is a long exact sequence

$$\ldots \longrightarrow H_T^{i-1}(G, M'') \longrightarrow H_T^i(G, M') \longrightarrow H_T^i(G, M) \longrightarrow$$

$$\longrightarrow H_T^i(G, M'') \longrightarrow H_T^{i+1}(G, M') \longrightarrow \ldots$$

The Herbrand quotient (I)

When G is a cyclic group, we have a special feature.

The Herbrand quotient (I)

When G is a cyclic group, we have a special feature.

Proposition.– If G is cyclic and finite, then

$$H_T^i(G, M) \simeq H_T^{i+2}(G, M).$$

The Herbrand quotient (I)

When G is a cyclic group, we have a special feature.

Proposition.– If G is cyclic and finite, then

$$H_T^i(G, M) \simeq H_T^{i+2}(G, M).$$

Let $1 \to M' \longrightarrow M \longrightarrow M'' \to 1$ be a short exact sequence.

Then the following diagram is exact

$$\begin{array}{ccccc} H_T^{-1}(G, M') & \longrightarrow & H_T^{-1}(G, M) & \longrightarrow & H_T^{-1}(G, M'') \\ \uparrow & & & & \downarrow \\ H_T^{0}(G, M'') & \longleftarrow & H_T^{0}(G, M) & \longleftarrow & H_T^{0}(G, M') \end{array}$$

The Herbrand quotient (II)

When the groups $H^i_T(G,M)$ are finite, we define the Herbrand quotient as

$$h(M) = \frac{\sharp H^0_T(G,M)}{\sharp H^{-1}_T(G,M)}.$$

The Herbrand quotient (II)

When the groups $H^i_T(G, M)$ are finite, we define the Herbrand quotient as

$$h(M) = \frac{\sharp H^0_T(G, M)}{\sharp H^{-1}_T(G, M)}.$$

From the previous exact rectangle is clear than $h(M) = h(M')h(M'')$.

The Herbrand quotient (II)

When the groups $H^i_T(G,M)$ are finite, we define the Herbrand quotient as

$$h(M) = \frac{\sharp H^0_T(G,M)}{\sharp H^{-1}_T(G,M)}.$$

From the previous exact rectangle is clear than $h(M) = h(M')h(M'')$.

Some remarks:

1) If two of M, M', M'' have Herbrand quotient, so does the third.

2) If M is finite, then $h(M) = 1$.

3) $h(M)$ is usually much more easy to compute than the actual Tate groups.

The Goal

In the previous set up, let us consider $K|k$ a Galois extension with Galois group G, $M = C_K$.

Here $N_G = N_{K|k}$, as we (quickly) mentioned.

The Goal

In the previous set up, let us consider $K|k$ a Galois extension with Galois group G, $M = C_K$.

Here $N_G = N_{K|k}$, as we (quickly) mentioned.

Moreover,

$$H^0 = \frac{C_K^G}{N_G(C_K)} = \frac{C_k}{N_{K|k}C_K}.$$

The Goal

In the previous set up, let us consider $K|k$ a Galois extension with Galois group G, $M = C_K$.

Here $N_G = N_{K|k}$, as we (quickly) mentioned.

Moreover,

$$H^0 = \frac{C_K^G}{N_G(C_K)} = \frac{C_k}{N_{K|k}C_K}.$$

We want to prove

$$\left[C_k : N_{K|k}C_K\right] = [K : k]$$

and, to begin with, we will see

$$\left[C_k : N_{K|k}C_K\right] \geq [K : k]$$

Local $\to$ global works!

Let S be finite, $S_\infty \subset S \subset P_k$.

$$\overline{S} = \{\mathfrak{P} \in P_K \text{ above places in } S\}$$

Local $\to$ global works!

Let S be finite, $S_\infty \subset S \subset P_k$.

$$\overline{S} = \{\mathfrak{P} \in P_K \text{ above places in } S\}$$

Lazy notation: $\mathbf{I}_K^S = \mathbf{I}_K^{\overline{S}}$.

Local $\to$ global works!

Let S be finite, $S_\infty \subset S \subset P_k$.

$$\overline{S} = \{\mathfrak{P} \in P_K \text{ above places in } S\}$$

Lazy notation: $\mathbf{I}_K^S = \mathbf{I}_K^{\overline{S}}$.

Proposition.– If $K|k$ cyclic, and S contains all ramified primes, for $i = 1, 2$:

$$H^i\left(G, \mathbf{I}_K^S\right) = \oplus_{\mathfrak{p} \in S} H^i\left(G_{\mathfrak{P}}, K_{\mathfrak{P}}^*\right)$$

$$H^i\left(G, \mathbf{I}_K\right) = \oplus_{\mathfrak{p}} H^i\left(G_{\mathfrak{P}}, K_{\mathfrak{P}}^*\right)$$

where $G_{\mathfrak{P}}$ is the Galois group of $K_{\mathfrak{P}}|k_{\mathfrak{p}}$ and $\mathfrak{P}|\mathfrak{p}$.

First brick

The fact that the global Tate cohomology can be decomposed and recovered from local pieces has two interesting corollaries.

First brick

The fact that the global Tate cohomology can be decomposed and recovered from local pieces has two interesting corollaries.

Proposition.– Let $K|k$ be a cyclic extension, $\alpha \in \mathbf{I}_k$. Then $\alpha \in N_{K|k} C_K$ if and only if $\alpha_\mathfrak{p} \in N_{K_\mathfrak{P}|k_\mathfrak{p}} K_\mathfrak{P}$, for all $\mathfrak{P}|\mathfrak{p}$.

First brick

The fact that the global Tate cohomology can be decomposed and recovered from local pieces has two interesting corollaries.

Proposition.– Let $K|k$ be a cyclic extension, $\alpha \in \mathbf{I}_k$. Then $\alpha \in N_{K|k} C_K$ if and only if $\alpha_{\mathfrak{p}} \in N_{K_{\mathfrak{P}}|k_{\mathfrak{p}}} K_{\mathfrak{P}}$, for all $\mathfrak{P}|\mathfrak{p}$.

Proposition.– If $K|k$ is cyclic, and S contains all ramified primes,

$$h\left(G, \mathbf{I}_K^S\right) = \prod_{\mathfrak{p}\in S} n_{\mathfrak{p}},$$

where $n_{\mathfrak{p}} = [K_{\mathfrak{P}} : k_{\mathfrak{p}}]$.

Second brick

For S finite, $S_\infty \subset S \subset P_k$, let

$$K^S = K \cap \mathbf{I}_K^S,$$

the group of $\overline{S}$–units.

Second brick

For S finite, $S_\infty \subset S \subset P_k$, let

$$K^S = K \cap \mathbf{I}_K^S,$$

the group of $\overline{S}$–units.

Proposition.– Assume $K|k$ is cyclic. Then

$$h\left(G, K^S\right) = \frac{1}{[K:k]} \prod_{\mathfrak{p}\in S} n_\mathfrak{p},$$

where $n_\mathfrak{p} = [K_\mathfrak{P} : k_\mathfrak{p}]$.

Second brick

For S finite, $S_\infty \subset S \subset P_k$, let

$$K^S = K \cap \mathbf{I}_K^S,$$

the group of $\overline{S}$–units.

Proposition.– Assume $K|k$ is cyclic. Then

$$h\left(G, K^S\right) = \frac{1}{[K:k]} \prod_{\mathfrak{p}\in S} n_\mathfrak{p},$$

where $n_\mathfrak{p} = [K_\mathfrak{P} : k_\mathfrak{p}]$.

The proof is based on local considerations, plus some (pretty technical) work on lattices.

Statement of the First Inequality

Theorem (First Inequality).– Let $K|k$ be cyclic, with Galois group G.

Statement of the First Inequality

Theorem (First Inequality).– Let $K|k$ be cyclic, with Galois group G.

Then

$$h(G, C_K) = \frac{\sharp H^0(G, C_K)}{\sharp H^{-1}(G, C_K)} = [K : k]$$

Statement of the First Inequality

Theorem (First Inequality).– Let $K|k$ be cyclic, with Galois group G.

Then

$$h(G, C_K) = \frac{\sharp H^0(G, C_K)}{\sharp H^{-1}(G, C_K)} = [K : k]$$

In particular,

$$\left[C_k : N_{K|k} C_K\right] \geq [K : k]$$

Proof of the First Inequality

Take, as previously, $S \subset P_k$ a set of places such that

-) $S_\infty \subset S$.

-) S contains all primes that split in K such that $\mathbf{I}_K^S \cdot K^* = \mathbf{I}_K$.

Proof of the First Inequality

Take, as previously, $S \subset P_k$ a set of places such that

-) $S_\infty \subset S$.

-) S contains all primes that split in K such that $\mathbf{I}_K^S \cdot K^* = \mathbf{I}_K$.

We have the following exact sequence

$$1 \to K^S \longrightarrow \mathbf{I}_K^S \longrightarrow (\mathbf{I}_K^S \cdot K^*)/K^* \simeq C_K \to 1$$

Proof of the First Inequality

Take, as previously, $S \subset P_k$ a set of places such that

-) $S_\infty \subset S$.

-) S contains all primes that split in K such that $\mathbf{I}_K^S \cdot K^* = \mathbf{I}_K$.

We have the following exact sequence

$$1 \to K^S \longrightarrow \mathbf{I}_K^S \longrightarrow (\mathbf{I}_K^S \cdot K^*)/K^* \simeq C_K \to 1$$

Then

$$h(G, C_K) = \frac{h\left(G, \mathbf{I}_K^S\right)}{h\left(G, K^S\right)} = [K : k]$$

Corollaries of the First Inequality

A pair of very interesting consequences:

Corollaries of the First Inequality

A pair of very interesting consequences:

Corollary 1.– Assume $K|k$ is cyclic of order p^{ν}, p prime. Then there are infinitely many places in P_k that do not split.

Corollaries of the First Inequality

A pair of very interesting consequences:

Corollary 1.– Assume $K|k$ is cyclic of order p^{ν}, p prime. Then there are infinitely many places in P_k that do not split.

Corollary 2.– Assume $K|k$ is finite. If almost all primes of k split completely in K, then $k = K$.

What are we proving (sort of)

Theorem.– Let $K|k$ be a Galois extension with Galois group G. Then:

1) $C_k / N_{K|k} C_K$ is finite, and its order divides $[K : k]$.

2) $H^1(G, C_K) = 1$.

3) $H^2(G, C_K)$ is finite, of order at most $[K : k]$.

What are we proving (sort of)

Theorem.– Let $K|k$ be a Galois extension with Galois group G. Then:

1) $C_k/N_{K|k}C_K$ is finite, and its order divides $[K:k]$.

2) $H^1(G, C_K) = 1$.

3) $H^2(G, C_K)$ is finite, of order at most $[K:k]$.

The First Inequality implies that, if G cyclic, all three are equivalent.

What are we proving (sort of)

Theorem.– Let $K|k$ be a Galois extension with Galois group G. Then:

1) $C_k / N_{K|k} C_K$ is finite, and its order divides $[K : k]$.

2) $H^1(G, C_K) = 1$.

3) $H^2(G, C_K)$ is finite, of order at most $[K : k]$.

The First Inequality implies that, if G cyclic, all three are equivalent.

Furthermore, in that case, $H^2(G, C_K)$ has order $[K : k]$.

Overview of an analytic proof

There is an analytic proof of this theorem, and it is shorter, but the techniques involved are rather different, so we will only sketch it.

Overview of an analytic proof

There is an analytic proof of this theorem, and it is shorter, but the techniques involved are rather different, so we will only sketch it.

Take $K|k$ finite, $L|k$ its Galois closure. Set

$$S = \{ \text{ primes of } k \text{ that split completely in } K \; \}$$

The set S has Dirichlet density $1/[L:k]$ (a special case of Chebotarev).

Overview of an analytic proof

There is an analytic proof of this theorem, and it is shorter, but the techniques involved are rather different, so we will only sketch it.

Take $K|k$ finite, $L|k$ its Galois closure. Set

$$S = \{ \text{ primes of } k \text{ that split completely in } K \text{ } \}$$

The set S has Dirichlet density $1/[L:k]$ (a special case of Chebotarev).

Via L–series and Fourier analysis this is related to a set

$$I_{\mathfrak{m}}/(P_{\mathfrak{m}}N_{L|k}J_{\mathfrak{m}})$$

which is an ideal version of $C_k/N_{K|k}C_K$, and has the same number of elements.

The reduction

The algebraic proof of our theorem relies at first on two very important reductions:

The reduction

The algebraic proof of our theorem relies at first on two very important reductions:

1) It is enough to consider the case where $K|k$ is cyclic of prime order

(We move from G to all of its Sylow p–subgroups, and prove that suffices)

The reduction

The algebraic proof of our theorem relies at first on two very important reductions:

1) It is enough to consider the case where $K|k$ is cyclic of prime order

(We move from G to all of its Sylow p–subgroups, and prove that suffices)

2) It is enough to consider the case where k contains a p-th root of unity.

(If not, we add ζ_p and prove, by diagram chasing, that things do not change a lot)

The key case: Set–up

Assume $K|k$ is cyclic of order p and k contains a p–th root of unity ζ_p.

The key case: Set–up

Assume $K|k$ is cyclic of order p and k contains a p–th root of unity ζ_p.

Let $S \subset P_k$ be a finite set such that:

1) $S_\infty \subset S$.

2) The primes that split in K are also in S.

3) $\mathbf{I}_k = \mathbf{I}_k^S \cdot k^*$.

The key case: Set–up

Assume $K|k$ is cyclic of order p and k contains a p–th root of unity ζ_p.

Let $S \subset P_k$ be a finite set such that:

1) $S_\infty \subset S$.

2) The primes that split in K are also in S.

3) $\mathbf{I}_k = \mathbf{I}_k^S \cdot k^*$.

And write, $k^S = \mathbf{I}_k^S \cap k^*$, $s = \sharp S$.

The key case: Auxiliary places

We want to construct a subgroup of C_k, of index $[K : k]$ which consists of norms from C_K.

The key case: Auxiliary places

We want to construct a subgroup of C_k, of index $[K : k]$ which consists of norms from C_K.

Let us take $T \subset P_k$, finite, such that $T \cap S = \emptyset$, and set

$$J = \prod_{\mathfrak{p}\in S} \left(k_{\mathfrak{p}}^*\right)^p \times \prod_{\mathfrak{p}\in T} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\notin S\cup T} U_{\mathfrak{p}}.$$

The key case: Auxiliary places

We want to construct a subgroup of C_k, of index $[K : k]$ which consists of norms from C_K.

Let us take $T \subset P_k$, finite, such that $T \cap S = \emptyset$, and set

$$J = \prod_{\mathfrak{p} \in S} \left(k_{\mathfrak{p}}^*\right)^p \times \prod_{\mathfrak{p} \in T} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S \cup T} U_{\mathfrak{p}}.$$

Let us also define $\Delta = (K^*)^p \cap k^S$.

The key case: Three steps

With these notations, we can prove (with some work):

1) $K = k\left(\sqrt[p]{\Delta}\right)$.

The key case: Three steps

With these notations, we can prove (with some work):

1) $K = k\left(\sqrt[p]{\Delta}\right)$.

2) There exists T such that $\sharp T = s - 1$ and

$$\Delta = \ker\left(k^S \longrightarrow \prod_{\mathfrak{p}\in T} k_{\mathfrak{p}}^* / \left(k_{\mathfrak{p}}^*\right)^p\right)$$

The key case: Three steps

With these notations, we can prove (with some work):

1) $K = k\left(\sqrt[p]{\Delta}\right)$.

2) There exists T such that $\sharp T = s-1$ and

$$\Delta = \ker\left(k^S \longrightarrow \prod_{\mathfrak{p}\in T} k_{\mathfrak{p}}^*/\left(k_{\mathfrak{p}}^*\right)^p\right)$$

3) For such a T, set $C_k^{S,T} = (J\cdot K^*)/K^*$. Then

$$\left[C_k/C_k^{S,T}\right] = [K:k] = p,$$

and $C_k^{S,T} \subset N_{K|k}C_K$.

The Second Inequality and the Class Field Axiom

The construction of T finishes the proof of the Second Inequality

$$\left[C_k : N_{K|k} C_K\right] \leq p.$$

The Second Inequality and the Class Field Axiom

The construction of T finishes the proof of the Second Inequality

$$\left[C_k : N_{K|k} C_K\right] \leq p.$$

In Neukirch's terminology, we have

Theorem (The Global Class Field Axiom).– Let $K|k$ be cyclic. Then

$$\sharp H^i\left(G, C_K\right) = \begin{cases} [K : k] & i = 0 \\ 1 & i = -1 \end{cases}$$

The Second Inequality and the Class Field Axiom

The construction of T finishes the proof of the Second Inequality

$$\left[C_k : N_{K|k} C_K\right] \leq p.$$

In Neukirch's terminology, we have

Theorem (The Global Class Field Axiom).– Let $K|k$ be cyclic. Then

$$\sharp H^i\left(G, C_K\right) = \begin{cases} [K : k] & i = 0 \\ 1 & i = -1 \end{cases}$$

Remark.– We knew that x *as principal idèle* is a norm if and only if it is a norm locally everywhere, but it does *not* necessarily have to be the norm of a principal idèle if $K|k$ is not cyclic.

Hasse's Norm Theorem

Corollary (Hasse's Norm Theorem).– Let $K|k$ be a cyclic extension. Then $x \in k^*$ is the norm of an element of K^* if and only if x is a norm in every $K_{\mathfrak{P}}|k_{\mathfrak{p}}$.

Hasse's Norm Theorem

Corollary (Hasse's Norm Theorem).– Let $K|k$ be a cyclic extension. Then $x \in k^*$ is the norm of an element of K^* if and only if x is a norm in every $K_{\mathfrak{P}}|k_{\mathfrak{p}}$.

From

$$1 \to K^* \longrightarrow \mathbf{I}_K \longrightarrow C_K \to 1$$

we get

$$1 = H^{-1}(G, C_K) \longrightarrow H^0(G, K^*) \longrightarrow H^0(G, \mathbf{I}_K)$$

Hasse's Norm Theorem

Corollary (Hasse's Norm Theorem).– Let $K|k$ be a cyclic extension. Then $x \in k^*$ is the norm of an element of K^* if and only if x is a norm in every $K_{\mathfrak{P}}|k_{\mathfrak{p}}$.

From
$$1 \to K^* \longrightarrow \mathbf{I}_K \longrightarrow C_K \to 1$$
we get
$$1 = H^{-1}(G, C_K) \longrightarrow H^0(G, K^*) \longrightarrow H^0(G, \mathbf{I}_K)$$

Therefore
$$H^0(G, K^*) = k^*/N_{K|k}K^* \hookrightarrow H^0(G, \mathbf{I}_K) = \oplus_{\mathfrak{p}} H^0\left(G_{\mathfrak{P}}, K_{\mathfrak{P}}^*\right),$$
which is the statement of the theorem, in a sophisticated way.

Artin Reciprocity Law: The local map

Let $K|k$ be abelian, with Galois group G. Let $\mathfrak{p} \in P_k$, $\mathfrak{P} \in P_K$ such that $\mathfrak{P}|\mathfrak{p}$.

Artin Reciprocity Law: The local map

Let $K|k$ be abelian, with Galois group G. Let $\mathfrak{p} \in P_k$, $\mathfrak{P} \in P_K$ such that $\mathfrak{P}|\mathfrak{p}$.

We recall this set from LCFT

$$D(\mathfrak{P}) = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\} \simeq \mathrm{Gal}\left(K_{\mathfrak{P}}|k_{\mathfrak{p}}\right).$$

Artin Reciprocity Law: The local map

Let $K|k$ be abelian, with Galois group G. Let $\mathfrak{p} \in P_k$, $\mathfrak{P} \in P_K$ such that $\mathfrak{P}|\mathfrak{p}$.

We recall this set from LCFT

$$D(\mathfrak{P}) = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\} \simeq \mathrm{Gal}\left(K_{\mathfrak{P}}|k_{\mathfrak{p}}\right).$$

The local Artin map is

$$\phi_{\mathfrak{p}} : k_{\mathfrak{p}} \longrightarrow D(\mathfrak{P}) \subset G.$$

Artin Reciprocity Law: Patching local maps

We can fit together local Artin maps by means of the following result.

Artin Reciprocity Law: Patching local maps

We can fit together local Artin maps by means of the following result.

Proposition.– There exists a unique homeomorphism

$$\phi_k : \mathbf{I}_k \longrightarrow \mathrm{Gal}\left(k^{ab}|k\right)$$

such that, for all $K \subset k^{ab}$ finite, and every $\mathfrak{p} \in P_k$, $\mathfrak{P} \in P_K$ with $\mathfrak{P}|\mathfrak{p}$, the following diagram

Artin Reciprocity Law: Patching local maps

We can fit together local Artin maps by means of the following result.

Proposition.– There exists a unique homeomorphism

$$\phi_k : \mathbf{I}_k \longrightarrow \mathrm{Gal}\left(k^{ab}|k\right)$$

such that, for all $K \subset k^{ab}$ finite, and every $\mathfrak{p} \in P_k$, $\mathfrak{P} \in P_K$ with $\mathfrak{P}|\mathfrak{p}$, the following diagram

$$\begin{array}{ccc} k_{\mathfrak{p}}^* & \xrightarrow{\phi_{\mathfrak{p}}} & D\left(\mathfrak{P}\right) \simeq \mathrm{Gal}\left(K_{\mathfrak{P}}|k_{\mathfrak{p}}\right) \\ \downarrow & & \downarrow \\ \mathbf{I}_k & \xrightarrow{\phi_k} & G \\ \alpha & \longmapsto & \phi_k(\alpha)_{|K} \end{array}$$

commutes.

Artin Reciprocity Law: How to patch

The definition of ϕ_k can be seen as follows. Take $\alpha \in \mathbf{I}_k$, and $K \subset K^{ab}$ such that $K|k$ is finite. Then:

1) $\phi_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = 1$ except for finitely many $\mathfrak{p}$ (it is 1 when $\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}$ and $K_{\mathfrak{P}}|k_{\mathfrak{p}}$ is unramified).

Artin Reciprocity Law: How to patch

The definition of ϕ_k can be seen as follows. Take $\alpha \in \mathbf{I}_k$, and $K \subset K^{ab}$ such that $K|k$ is finite. Then:

1) $\phi_{\mathfrak{p}}\left(\alpha_{\mathfrak{p}}\right) = 1$ except for finitely many $\mathfrak{p}$ (it is 1 when $\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}$ and $K_{\mathfrak{P}}|k_{\mathfrak{p}}$ is unramified).

2) The unique choice is then (for a fixed K)

$$\phi_{K|k}(\alpha) = \prod_{\mathfrak{p}} \phi_{\mathfrak{p}}\left(\alpha_{\mathfrak{p}}\right).$$

Artin Reciprocity Law: How to patch

The definition of ϕ_k can be seen as follows. Take $\alpha \in \mathbf{I}_k$, and $K \subset K^{ab}$ such that $K|k$ is finite. Then:

1) $\phi_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = 1$ except for finitely many $\mathfrak{p}$ (it is 1 when $\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}$ and $K_{\mathfrak{P}}|k_{\mathfrak{p}}$ is unramified).

2) The unique choice is then (for a fixed K)

$$\phi_{K|k}(\alpha) = \prod_{\mathfrak{p}} \phi_{\mathfrak{p}}(\alpha_{\mathfrak{p}}).$$

3) A field extension corresponds to a unique extension of ϕ_k (because of the local properties of the Artin maps).

Artin Reciprocity Law: The statement

Theorem (Artin Reciprocity Law).– The homeomorphism

$$\phi_k : \mathbf{I}_k \longrightarrow \mathrm{Gal}\left(k^{ab}|k\right)$$

verifies:

Artin Reciprocity Law: The statement

Theorem (Artin Reciprocity Law).– The homeomorphism

$$\phi_k : \mathbf{I}_k \longrightarrow \mathrm{Gal}\left(k^{ab}|k\right)$$

verifies:

1) $\phi_k(k^*) = 1$.

Artin Reciprocity Law: The statement

Theorem (Artin Reciprocity Law).– The homeomorphism

$$\phi_k : \mathbf{I}_k \longrightarrow \mathrm{Gal}\left(k^{ab}|k\right)$$

verifies:

1) $\phi_k(k^*) = 1$.

2) For all abelian finite extensions $K|k$, ϕ_k induces an isomorphism:

$$\phi_{K|k} : \mathbf{I}_k/(k^* \cdot N_{K|k}\mathbf{I}_K) \longrightarrow \mathrm{Gal}\,(K|k)$$

Artin Reciprocity Law: In terms of C_k

Artin Reciprocity Law can be restated in terms of the idèle class group as follows:

Artin Reciprocity Law: In terms of C_k

Artin Reciprocity Law can be restated in terms of the idèle class group as follows:

1) ϕ_k induces a homomorphism $C_k \longrightarrow \mathrm{Gal}\left(k^{ab}|k\right)$

Artin Reciprocity Law: In terms of C_k

Artin Reciprocity Law can be restated in terms of the idèle class group as follows:

1) ϕ_k induces a homomorphism $C_k \longrightarrow \mathrm{Gal}\left(k^{ab}|k\right)$

2) ϕ_k induces an isomorphism $\phi_{K|k} : C_k/N_{K|k}C_K \simeq \mathrm{Gal}\,(K|k)$

Artin Reciprocity Law: Frobenius elements

A brief recall from LCFT. Let us consider $K|k$.

Take $\mathfrak{p} \in P_k$ and $\mathfrak{P} \in P_K$ such that $\mathfrak{P}|\mathfrak{p}$ and $\mathfrak{P}$ is unramified over $\mathfrak{p}$.

Artin Reciprocity Law: Frobenius elements

A brief recall from LCFT. Let us consider $K|k$.

Take $\mathfrak{p} \in P_k$ and $\mathfrak{P} \in P_K$ such that $\mathfrak{P}|\mathfrak{p}$ and $\mathfrak{P}$ is unramified over $\mathfrak{p}$.

We have

$$\mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_k/\mathfrak{p}\right) \simeq \mathrm{Gal}\left(K_{\mathfrak{P}}|k_{\mathfrak{p}}\right)$$

and hence $D(\mathfrak{P})$ is cyclic

Remember $\mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_k/\mathfrak{p}\right)$ is generated by the Frobenius element $x \mapsto x^q$.

Artin Reciprocity Law: Frobenius elements

A brief recall from LCFT. Let us consider $K|k$.

Take $\mathfrak{p} \in P_k$ and $\mathfrak{P} \in P_K$ such that $\mathfrak{P}|\mathfrak{p}$ and $\mathfrak{P}$ is unramified over $\mathfrak{p}$.

We have

$$\mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_k/\mathfrak{p}\right) \simeq \mathrm{Gal}\left(K_{\mathfrak{P}}|k_{\mathfrak{p}}\right)$$

and hence $D(\mathfrak{P})$ is cyclic

Remember $\mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_k/\mathfrak{p}\right)$ is generated by the Frobenius element $x \mapsto x^q$.

The Frobenius element $(\mathfrak{P}, K|k)$ is the element of $D(\mathfrak{P})$ corresponding to the Frobenius element.

Artin Reciprocity Law: Properties of the Frobenius element

The Frobenius element can alternatively be described as the only element $\sigma \in G$ such that:

1) $\sigma\mathfrak{P} = \mathfrak{P}$.

Artin Reciprocity Law: Properties of the Frobenius element

The Frobenius element can alternatively be described as the only element $\sigma \in G$ such that:

1) $\sigma\mathfrak{P} = \mathfrak{P}$.

2) For all $\alpha \in \mathcal{O}_k$, $\sigma\alpha = \alpha^q \mod \mathfrak{P}$, where $q = \sharp(\mathcal{O}_k/\mathfrak{p})$.

Artin Reciprocity Law: Properties of the Frobenius element

The Frobenius element can alternatively be described as the only element $\sigma \in G$ such that:

1) $\sigma\mathfrak{P} = \mathfrak{P}$.

2) For all $\alpha \in \mathcal{O}_k$, $\sigma\alpha = \alpha^q \mod \mathfrak{P}$, where $q = \sharp(\mathcal{O}_k/\mathfrak{p})$.

Another interesting property is that, as G acts transitively on the set of primes dividing $\mathfrak{p}$,

$$\{(\mathfrak{P}, K|k) \mid \mathfrak{P}|\mathfrak{p}\}$$

is a conjugacy class in G, noted $(\mathfrak{p}, K|k)$.

The Frobenius elements $(\mathfrak{P}, K|k)$, for the primes $\mathfrak{P}$ which do not ramify generate the Galois group of $K|k$.

Artin Reciprocity Law: Proof (I)

To prove Artin Reciprocity Law it suffices proving:

Artin Reciprocity Law: Proof (I)

To prove Artin Reciprocity Law it suffices proving:

Key Theorem.– Let $K|k$ be a finite abelian extension with Galois group G. Then $\phi_{K|k} : \mathbf{I}_K \longrightarrow G$ is trivial on the principal idèles.

Artin Reciprocity Law: Proof (I)

To prove Artin Reciprocity Law it suffices proving:

Key Theorem.– Let $K|k$ be a finite abelian extension with Galois group G. Then $\phi_{K|k} : \mathbf{I}_K \longrightarrow G$ is trivial on the principal idèles.

It is the most delicate part of the proof because:

1) The norm subgroup $N_{K|k}\mathbf{I}_K$ is contained in the kernel of $\phi_{K|k}$ because it is locally.

Artin Reciprocity Law: Proof (II)

2) Once we assume the Key Theorem, we have a homomorphism

$$\mathbf{I}_k/(k^* \cdot N_{K|k}\mathbf{I}_K) \longrightarrow \mathrm{Gal}\,(K|k)$$

which is surjective because we can explicitly construct an idèle α such that $\phi_{K|k}(\alpha)$ is a Frobenius element for an unramified prime, and these elements generate G.

Artin Reciprocity Law: Proof (II)

2) Once we assume the Key Theorem, we have a homomorphism

$$\mathbf{I}_k/(k^* \cdot N_{K|k}\mathbf{I}_K) \longrightarrow \mathrm{Gal}\,(K|k)$$

which is surjective because we can explicitly construct an idèle α such that $\phi_{K|k}(\alpha)$ is a Frobenius element for an unramified prime, and these elements generate G.

3) From the Second Inequality

$$\left[\mathbf{I}_k : k^* \cdot N_{K|k}\mathbf{I}_K\right] \leq [K : k].$$

Artin Reciprocity Law: Proof (II)

2) Once we assume the Key Theorem, we have a homomorphism

$$\mathbf{I}_k/(k^* \cdot N_{K|k}\mathbf{I}_K) \longrightarrow \mathrm{Gal}\,(K|k)$$

which is surjective because we can explicitly construct an idèle α such that $\phi_{K|k}(\alpha)$ is a Frobenius element for an unramified prime, and these elements generate G.

3) From the Second Inequality

$$\left[\mathbf{I}_k : k^* \cdot N_{K|k}\mathbf{I}_K\right] \leq [K : k].$$

Then 2) and 3) (together with the Key Theorem) prove Artin Reciprocity Law.

Artin Reciprocity Law: Strategy for the Key Theorem

We will not go into detail, but the steps to prove the Key Theorem are:

1) Prove that, if it works for $K|k$, it works for any subextension, and also for joint extensions (given $K'|k$, considering $K' \cdot K|K'$) (technical, not difficult).

Artin Reciprocity Law: Strategy for the Key Theorem

We will not go into detail, but the steps to prove the Key Theorem are:

1) Prove that, if it works for $K|k$, it works for any subextension, and also for joint extensions (given $K'|k$, considering $K' \cdot K|K'$) (technical, not difficult).

2) Prove that it suffices to consider cyclic cyclotomic extensions (complicated).

Artin Reciprocity Law: Strategy for the Key Theorem

We will not go into detail, but the steps to prove the Key Theorem are:

1) Prove that, if it works for $K|k$, it works for any subextension, and also for joint extensions (given $K'|k$, considering $K' \cdot K|K'$) (technical, not difficult).

2) Prove that it suffices to consider cyclic cyclotomic extensions (complicated).

3) Check that it is true for cyclotomic extensions (fairly easy).

The Existence Theorem

We finish our presentation with a outstanding result, based on Artin Reciprocity Law.

Theorem (Existence Theorem).– Let k be a number field. The finite abelian extensions $K|k$ are in one–to–one correspondence with the open subgroups of C_k of finite index

$$K \longmapsto N_{K|k} C_K$$

The Existence Theorem

We finish our presentation with a outstanding result, based on Artin Reciprocity Law.

Theorem (Existence Theorem).– Let k be a number field. The finite abelian extensions $K|k$ are in one–to–one correspondence with the open subgroups of C_k of finite index

$$K \longmapsto N_{K|k} C_K$$

Thanks to the Reciprocity Law, it suffices to prove that every subgroup of finite index *contains* a norm subgroup.

The Existence Theorem

We finish our presentation with a outstanding result, based on Artin Reciprocity Law.

Theorem (Existence Theorem).– Let k be a number field. The finite abelian extensions $K|k$ are in one–to–one correspondence with the open subgroups of C_k of finite index

$$K \longmapsto N_{K|k} C_K$$

Thanks to the Reciprocity Law, it suffices to prove that every subgroup of finite index *contains* a norm subgroup.

Definition.– The field corresponding to an open subgroup $N \subset C_k$ is called the *class field* of N.

Thanks a lot!

Thanks a lot!

Any questions?

Thanks a lot!

Any questions?

Well, thanks again, you've been a wonderful audience!