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

→ Ξ →



・ロト ・ 日 ト ・ ヨ ト ・ ヨ ト

1 Adeles and Ideles

(A bit of) Topology of ideles

・ロト ・聞ト ・ヨト ・ヨト

Adeles and Ideles

- (A bit of) Topology of ideles
- Field extensions and ideles

< ロ > < 同 > < 回 > < 回 > < 回 > < 回

Adeles and Ideles

- (A bit of) Topology of ideles
- 3 Field extensions and ideles
- 4 Tate Cohomology

Adeles and Ideles

- (A bit of) Topology of ideles
- Field extensions and ideles
- 4 Tate Cohomology
- 5 The First Inequality

• • • • • • • • • • • •

Adeles and Ideles

- (A bit of) Topology of ideles
- Field extensions and ideles
- 🗿 Tate Cohomology
- 5 The First Inequality
- 6 The Second Inequality

Adeles and Ideles

- (A bit of) Topology of ideles
- Field extensions and ideles
- 🗿 Tate Cohomology
- 5 The First Inequality
- 6 The Second Inequality

The BIG results

Image: A math a mat

Notation

Let k be a number field, 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.

(日) (同) (三) (三)

Notation

Let k be a number field, 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:

(日) (同) (三) (三)

Notation

Let k be a number field, 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_p , the completion (which must be **R**, **C** or a 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

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Adèles

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

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

・ロト ・聞 ト ・ ヨト ・ ヨト

Adèles

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

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

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).

< ロ > < 同 > < 回 > < 回 > < 回 > < 回

Adèles

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

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

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:

$$\mathsf{A}_{\mathsf{Q}} = \mathsf{R} imes \{(a_p) \mid a_p \in \mathsf{Q}_p ext{ and } a_p \in \mathsf{Z}_p ext{ for almost all } p\}$$
 .

(日) (同) (三) (三)

Idèles (I)

The idèles of k, noted I_k , is the unit group of A_k (which would usually be noted A_k^*).

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

Idèles (I)

The idèles of k, noted I_k , is the unit group of A_k (which would usually be noted A_k^*).

They may also be described as the restricted product of k_p^* w.r.t. U_p .

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

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

associating $a \in k^*$ with (α_p) which is a at each p-component

<ロト < 団ト < 団ト < 団ト

Idèles (I)

The idèles of k, noted I_k , is the unit group of A_k (which would usually be noted A_k^*).

They may also be described as the restricted product of k_p^* w.r.t. U_p .

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

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

associating $a \in k^*$ with (α_p) which is a at each 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

$$\mathsf{I}^{\mathcal{S}}_k = \prod_{\mathfrak{p} \in \mathcal{S}} k^*_\mathfrak{p} imes \prod_{\mathfrak{p} \notin \mathcal{S}} U_\mathfrak{p}$$

the group of S-idèles, which is obviously a subgroup of I_k .

Idèles (II)

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

$$\mathsf{I}^{\mathcal{S}}_{k} = \prod_{\mathfrak{p} \in \mathcal{S}} k^{*}_{\mathfrak{p}} imes \prod_{\mathfrak{p} \notin \mathcal{S}} U_{\mathfrak{p}}$$

the group of S-idèles, which is obviously a subgroup of 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

$$\mathsf{I}^{\mathcal{S}}_{k} = \prod_{\mathfrak{p} \in \mathcal{S}} k^{*}_{\mathfrak{p}} imes \prod_{\mathfrak{p} \notin \mathcal{S}} U_{\mathfrak{p}}$$

the group of S-idèles, which is obviously a subgroup of I_k .

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

$$\mathsf{I}_k^{\mathcal{S}_\infty} = \prod_{\mathfrak{p}\mid\infty} k_\mathfrak{p}^* imes \prod_{\mathfrak{p} \text{ finite}} U_\mathfrak{p},$$

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

Idèles and FId_k

Let Fld_k be the group of fractional ideals of k.

Idèles and FId_k

Let Fld_k be the group of fractional ideals of k.

We can define

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

Idèles and FId_k

Let Fld_k be the group of fractional ideals of k.

We can define

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

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

Idèles and Cl_k

Therefore we have an isomorphism

$$\mathsf{I}_k/\mathsf{I}_k^{\mathcal{S}_\infty}\simeq\mathsf{Fld}_k.$$

・ロト ・聞ト ・ヨト ・ヨト

Idèles and Cl_k

Therefore we have an isomorphism

$$\mathsf{I}_k/\mathsf{I}_k^{S_\infty}\simeq\mathsf{Fld}_k.$$

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

• • • • • • • • • • • •

Idèles and Cl_k

Therefore we have an isomorphism

$$\mathsf{I}_k/\mathsf{I}_k^{\mathcal{S}_\infty}\simeq\mathsf{Fld}_k.$$

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

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

• • • • • • • • • • • •

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,

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

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

・ロト ・聞ト ・ヨト ・ヨト

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,

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

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

And, because of the product formula,

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

3

イロト イポト イヨト イヨト

Norm (II)

We have defined then a norm mapping

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

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

(日) (同) (三) (三)

Norm (II)

We have defined then a norm mapping

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

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

We call its kernel

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

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

(日) (同) (三) (三)

October 2009

10 / 68

Norm (II)

We have defined then a *norm* mapping

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

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

We call its kernel

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

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

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

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

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

Topological groups

Topological groups are nice!

(日) (同) (三) (三)

3

11 / 68

October 2009

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.

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

11 / 68

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.

(日) (同) (三) (三)

Not really much choice

We want I_k^S to be open subsets (subgroups) of I_k (a good reason in a while).

3

(日) (同) (三) (三)
Not really much choice

We want I_k^S to be open subsets (subgroups) of I_k (a good reason in a while).

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

< □ > < 同 > < 回 > < 回 > < 回

October 2009

Not really much choice

We want I_k^S to be open subsets (subgroups) of I_k (a good reason in a while).

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

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

Definition via neighbourhoods of 1

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

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

Image: A marked and A marked

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_p is a basic system of neighbourhoods of $1 \in k_p$, 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_p is a basic system of neighbourhoods of $1 \in k_p$, and S is finite, $S_{\infty} \subset S$.

Equivalently we can take

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

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 $I_k^{S_{\infty}}$, therefore in 1, therefore in I_k).

(日) (同) (日) (日) (日)

October 2009

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 $I_k^{S_{\infty}}$, therefore in 1, therefore in I_k).

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

イロト イポト イヨト イヨト

- 3

14 / 68

October 2009

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 $I_k^{S_{\infty}}$, therefore in 1, therefore in I_k).

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

And hence so it is

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

イロト イポト イヨト イヨト

- 3

14 / 68

October 2009

Locally compactness

Let $\mathcal{S}_\infty \subset \mathcal{S}$ and consider

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

æ

< ロ > < 同 > < 回 > < 回 > < 回 >

Locally compactness

Let $S_\infty \subset S$ and consider

$$\mathsf{I}^{\mathcal{S}}_{k} = \prod_{\mathfrak{p}\in\mathcal{S}} k^*_{\mathfrak{p}} imes \prod_{\mathfrak{p}\notin\mathcal{S}} U_{\mathfrak{p}}.$$

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

(日) (同) (三) (三)

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 I_k^S is locally compact, and so it is I_k .

(日) (同) (三) (三)

So far, so good

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

< ロ > < 同 > < 回 > < 回 > < 回

3

16 / 68

October 2009

So far, so good

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

If S is finite, I_k^S is a closed subgroup.

Image: A marked and A marked

So far, so good

- \mathbf{I}_k is a locally compact topological group.
- If S is finite, I_k^S is a closed subgroup.
- If $S_{\infty} \subset S$, \mathbf{I}_k^S is an open subgroup.

< ロ > < 同 > < 回 > < 回 > < 回

A bit more of idèles and Fld_k

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

・ロト ・聞ト ・ヨト ・ヨト

A bit more of idèles and Fld_k

- ${\bf I}_k^{S_\infty}$ is open and closed, therefore $\{1\}$ is open and closed in the quotient space ${\bf I}_k/{\bf I}_k^{S_\infty}.$
- Then $\mathbf{I}_k / \mathbf{I}_k^{S_{\infty}}$ must be a discrete space.

A bit more of idèles and Fld_k

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

Then $I_k/I_k^{S_{\infty}}$ must be a discrete space.

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

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

イロト 不得下 イヨト イヨト 二日

October 2009

A bit more of norm

Remember that our norm homomorphism

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

was surjective.

3

(日) (同) (三) (三)

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 $I_k^{S_{\infty}}$, therefore in 1, therefore in 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 $I_k^{S_{\infty}}$, therefore in 1, therefore in I_k .

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

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

イロト イポト イヨト イヨト

A bit more of k^*

Remember that k^* could be viewed as a subgroup of I_k .

Proposition.– k^* is a discrete closed subgroup of I_k .

3

(日) (同) (三) (三)

A bit more of k^*

Remember that k^* could be viewed as a subgroup of I_k .

Proposition.– k^* is a discrete closed subgroup of I_k .

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

< ロ > < 同 > < 回 > < 回 > < 回 >

A bit more of k^*

Remember that k^* could be viewed as a subgroup of I_k .

Proposition.– k^* is a discrete closed subgroup of 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 .

< ロ > < 同 > < 回 > < 回 > < 回 >

A bit more of C_k^0

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

Proposition.– C_k^0 is compact.

<ロ> (日) (日) (日) (日) (日)

3

20 / 68

October 2009

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).

(日) (同) (三) (三)

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

$$|\mathbf{I}_k/\left(k^*\cdot\mathbf{I}_k^{\mathcal{S}_\infty}\right)\simeq\mathsf{Cl}_k$$

3

(日) (同) (三) (三)

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

Remember we had

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

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

< ロ > < 同 > < 回 > < 回 > < 回

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

Remember we had

$$|\mathbf{I}_k/\left(k^*\cdot\mathbf{I}_k^{\mathcal{S}_\infty}
ight)\simeq\mathsf{Cl}_k$$

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

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

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

which is surjective.

October 2009

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.

(日)

October 2009

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).

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

October 2009

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).

イロト 不得下 イヨト イヨト 二日

A word on open subgroups (I)

We will call a finite formal sum

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

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

3

(日) (同) (三) (三)

A word on open subgroups (I)

We will call a finite formal sum

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

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

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

(日) (同) (三) (三)

October 2009

A word on open subgroups (I)

We will call a finite formal sum

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

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

Let us write 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 $\mathfrak{m} = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$.

▲ロト ▲圖ト ▲画ト ▲画ト 三回 - のへで

October 2009

A word on open subgroups (II)

Let us define the following sets:

Image: A marked and A marked
A word on open subgroups (II)

Let us define the following sets:

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

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

(日)

A word on open subgroups (II)

Let us define the following sets:

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

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

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

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

October 2009

Yet another word on open subgroups

Define now the subset:

3

-

• • • • • • • • • • • •

Yet another word on open subgroups

Define now the subset:

$$\mathsf{I}_{\mathfrak{m}} = \left(\prod_{\mathfrak{p} \notin \mathsf{supp}(\mathfrak{m})} k_{\mathfrak{p}}^* imes \prod_{\mathfrak{p} \in \mathsf{supp}(\mathfrak{m})} \mathcal{W}_{\mathfrak{m}}(\mathfrak{p})
ight) \cap \mathsf{I}_k.$$

• • • • • • • • • • • •

-

October 2009

3

Yet another word on open subgroups

Define now the subset:

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

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

3

• • • • • • • • • • • •

A penultimate word on open subgroups

Then we consider the sets

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

< ロ > < 同 > < 回 > < 回 > < 回

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:

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

< ロ > < 同 > < 回 > < 回 > < 回

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:

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

That is, (\alpha) such that $\alpha_{\mathfrak{p}} \in k_{\mathfrak{p}}^*$ for all \mathfrak{p} infinte
 $\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}$ for all \mathfrak{p} finite
 $\alpha_{\mathfrak{p}} \in W_{\mathfrak{m}}(\mathfrak{p})$ for all $\mathfrak{p} \in \text{supp}(\mathfrak{m})$

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

A last word on open subgroups

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

- ∢ 🗇 እ

October 2009

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

Image: A math a mat

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 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

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

< □ > < 同 > < 回 > < Ξ > < Ξ

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 $I_{\mathcal{K}} \hookrightarrow I_{\mathcal{K}}.$

(日) (同) (三) (三)

The canonical embedding

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

$$\mathbf{A}_k \longrightarrow \mathbf{A}_K$$

 $(\alpha_p) \longmapsto (\alpha_p), \text{ where } \alpha_p = \alpha_p, \text{ whenever } \mathfrak{P}|\mathfrak{p}$

It is, in fact, an injective homomorphism which induces also an embedding $I_k \hookrightarrow I_{\mathcal{K}}.$

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

イロト 不得下 イヨト イヨト 二日

Idèles and field isomorphisms

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

< ロ > < 同 > < 回 > < 回 > < 回

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) $\sigma : L_{\mathfrak{P}} \longrightarrow \mathcal{K}_{\sigma \mathfrak{P}}$. Idea: Take \mathfrak{P} -limits to $\sigma \mathfrak{P}$ -limits.

イロト イポト イヨト イヨト

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) $\sigma : L_{\mathfrak{P}} \longrightarrow \mathcal{K}_{\sigma \mathfrak{P}}$. Idea: Take \mathfrak{P} -limits to $\sigma \mathfrak{P}$ -limits.

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

$$\alpha_{\mathfrak{P}} \in \mathcal{L}_{\mathfrak{P}} \implies (\sigma \alpha)_{\sigma \mathfrak{P}} = \sigma (\alpha_{\mathfrak{P}}) \in \mathcal{K}_{\sigma \mathfrak{P}}.$$

・ロン ・四 ・ ・ ヨン

October 2009

Galois descent for idèles (I)

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

< ロ > < 同 > < 回 > < 回 > < 回

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 I_K a *G*-module.

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

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 I_K a *G*-module.

As usual:

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

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

Galois descent for idèles (II)

Theorem.–
$$I_{\mathcal{K}}^{\mathcal{G}} = I_{k}$$
.

イロト イ団ト イヨト イヨト

æ

31 / 68

October 2009

Galois descent for idèles (II)

Theorem.–
$$I_{\mathcal{K}}^{\mathcal{G}} = I_{k}$$
.

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

æ

イロト イ団ト イヨト イヨト

Galois descent for idèles (II)

Theorem.– $I_{\mathcal{K}}^{\mathcal{G}} = I_{k}$.

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

Then, if we take $\sigma \in \text{Gal}(K_{\mathfrak{P}}|k_{\mathfrak{p}}), \ \sigma \mathfrak{P} = \mathfrak{P}$, 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 $\alpha \in \mathbf{I}_k$.

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

October 2009

Norm (revisited)

Take $\alpha \in I_{\mathcal{K}}$, $\mathfrak{P} \in P_{\mathcal{K}}$ (a place in \mathcal{K}).

Multiplication by $\alpha_{\mathfrak{P}}$ is a $k_{\mathfrak{p}}$ -linear automorphism of $\mathcal{K}_{\mathfrak{P}}$, and its determinant is set to be

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

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Norm (revisited)

Take $\alpha \in I_{\mathcal{K}}$, $\mathfrak{P} \in P_{\mathcal{K}}$ (a place in \mathcal{K}).

Multiplication by $\alpha_{\mathfrak{P}}$ is a $k_{\mathfrak{p}}$ -linear automorphism of $\mathcal{K}_{\mathfrak{P}}$, 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 $I_K \longrightarrow I_k$. Let $\alpha \in I_K$, then

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

October 2009

Norm (revisited)

Take $\alpha \in I_{\mathcal{K}}$, $\mathfrak{P} \in P_{\mathcal{K}}$ (a place in \mathcal{K}).

Multiplication by $\alpha_{\mathfrak{P}}$ is a $k_{\mathfrak{p}}$ -linear automorphism of $\mathcal{K}_{\mathfrak{P}}$, 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 $I_K \longrightarrow I_k$.

Let $\alpha \in \mathbf{I}_{K}$, then

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

Proposition.– The set $N_{K|k}I_K$ is an open and closed subgroup of I_k .

イロト 不得下 イヨト イヨト 二日

The embedding of the idèle class groups

The embedding $I_k \hookrightarrow I_K$ takes clearly principal idèles into principal idèles.

< □ > < 同 > < 回 > < Ξ > < Ξ

The embedding of the idèle class groups

The embedding $I_k \hookrightarrow I_K$ takes clearly principal idèles into principal idèles.

Proposition.– If K|k is finite, then $I_k \hookrightarrow I_K$ induces an injection

 $C_k \hookrightarrow C_K$.

The embedding of the idèle class groups

The embedding $I_k \hookrightarrow I_K$ takes clearly principal idèles into principal idèles.

Proposition.– If K|k is finite, then $I_k \hookrightarrow I_K$ induces an injection

$$C_k \hookrightarrow C_K.$$

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

イロト イポト イヨト イヨト 二日

October 2009

Norm on the idèle class group

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

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

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

・ロト ・同ト ・ヨト ・ヨ

October 2009

Norm on the idèle class group

Remark.– If $x \in K^*$, then $N_{K|k}(x)$ has the same meaning as idèle in 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).

イロト イポト イヨト イヨト 二日

October 2009

Galois descent for idèle class group

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

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

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

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

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

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

$$1 \to (K^*)^G \longrightarrow {\sf I}^G_K \longrightarrow C^G_K \longrightarrow H^1(G,K^*)$$

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

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

(日) (同) (三) (三)

October 2009

Here comes the cohomology!

3

・ロト ・聞 ト ・ ヨト ・ ヨト
Here comes the cohomology!

End of Part I

æ

・ロト ・聞ト ・ヨト ・ヨト

Here comes the cohomology!

End of Part I

Coffee? Anyone?

3

(日) (同) (三) (三)

The set-up

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

3

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

The set-up

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

Define the *G*-norm:

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

3

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

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

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

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

3

(日) (同) (三) (三)

The Tate cohomology

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

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

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

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

< ロ > < 同 > < 回 > < 回 > < 回 > < 回

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.

Image: Image:

October 2009

The Tate long sequence

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

Proposition.- Let

$$1 \rightarrow M' \longrightarrow M \longrightarrow M'' \rightarrow 1$$

be a short exact sequence.

There is a long exact sequence

$$\dots \longrightarrow H^{i-1}_{T}(G, M'') \longrightarrow H^{i}_{T}(G, M') \longrightarrow H^{i}_{T}(G, M) \longrightarrow$$
$$\longrightarrow H^{i}_{T}(G, M'') \longrightarrow H^{i+1}_{T}(G, M') \longrightarrow \dots$$

→ 3 → 4 3

The Herbrand quotient (I)

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

Image: A math a math

The Herbrand quotient (I)

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

Proposition.– If G is cyclic and finite, then

$$H^i_T(G,M)\simeq H^{i+2}_T(G,M).$$

(日)

October 2009

The Herbrand quotient (I)

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

Proposition.– If G is cyclic and finite, then

$$H^i_T(G,M)\simeq H^{i+2}_T(G,M).$$

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

Then the following diagram is exact

・ロン ・四 ・ ・ ヨン

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'').

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

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.

イロト イポト イヨト イヨト

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.

3

(日) (同) (三) (三)

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,

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

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

October 2009

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

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

and, to begin with, we will see

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

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Local \rightarrow global works!

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

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

◆□▶ ◆□▶ ◆ □▶ ◆ □▶ - □ - のへで

Local \rightarrow global works!

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

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

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

Local \rightarrow global works!

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

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

Lazy notation: $\mathbf{I}_{\mathcal{K}}^{S} = \mathbf{I}_{\mathcal{K}}^{\overline{S}}$.

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 $\mathfrak{P}|\mathfrak{p}$.

イロト 不得 とくまとう まし

First brick

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

(日) (同) (三) (三)

October 2009

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, $\alpha \in I_k$. 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 $\mathfrak{P}|\mathfrak{p}$.

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

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, $\alpha \in I_k$. 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,

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

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

イロト 不得下 イヨト イヨト 二日

October 2009

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.

3

イロト イポト イヨト イヨト

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

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

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

- 32

・ロン ・四 ・ ・ ヨン

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

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

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

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

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

October 2009

Statement of the First Inequality

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

< □ > < 同 > < 回 > < Ξ > < Ξ

Statement of the First Inequality

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

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

Statement of the First Inequality

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

Then

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

In particular,

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

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

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 $I_K^S \cdot K^* = I_K$.

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 $I_K^S \cdot K^* = I_K$.

We have the following exact sequence

$$1 \to {\mathcal K}^{\mathcal S} \longrightarrow {\mathbf I}_{{\mathcal K}}^{\mathcal S} \longrightarrow ({\mathbf I}_{{\mathcal K}}^{\mathcal S} \cdot {\mathcal K}^*)/{\mathcal K}^* \simeq {\mathcal C}_{{\mathcal K}} \to 1$$

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 $I_K^S \cdot K^* = I_K$.

We have the following exact sequence

$$1 \to {\mathcal K}^{\mathcal S} \longrightarrow {\mathbf I}_{{\mathcal K}}^{\mathcal S} \longrightarrow ({\mathbf I}_{{\mathcal K}}^{\mathcal S} \cdot {\mathcal K}^*)/{\mathcal K}^* \simeq {\mathcal C}_{{\mathcal K}} \to 1$$

Then

$$h(G, C_{\mathcal{K}}) = \frac{h(G, \mathbf{I}_{\mathcal{K}}^{S})}{h(G, \mathcal{K}^{S})} = [\mathcal{K} : k]$$

Corollaries of the First Inequality

A pair of very interesting consequences:

Image: A match a ma

October 2009
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.

イロト イヨト イヨト

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].

ヘロン 人間と 人間と 人間と

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.

→ 3 → 4 3

Image: Image:

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

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

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.

イロト 不得下 イヨト イヨト 二日

October 2009

The reduction

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

< ロ > < 同 > < 回 > < 回 > < 回

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)

イロト イポト イヨト イヨト 二日

The key case: Set-up

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

< ロ > < 同 > < 回 > < 回 > < 回 > < 回

3

52 / 68

October 2009

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

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

- 34

52 / 68

October 2009

```
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, $k^{S} = \mathbf{I}_{k}^{S} \cap k^{*}$, $s = \sharp S$.

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

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 .

< ロ > < 同 > < 回 > < 回 > < 回

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

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

< ロ > < 同 > < 回 > < 回 > < 回

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

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

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

< ロト < 同ト < ヨト < ヨト

October 2009

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

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

< ロ > < 同 > < 回 > < 回 > < 回

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

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

3) For such a *T*, set $C_k^{S,T} = (J \cdot K^*)/K^*$. Then $\begin{bmatrix} C_k/C_k^{S,T} \end{bmatrix} = [K:k] = p,$

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

J.M. Tornero (Universidad de Sevilla)

イロト イポト イヨト イヨト

October 2009

The Second Inequality and the Class Field Axiom

The construction of T finishes the proof of the Second Inequality

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

Image: Image:

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

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

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

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

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

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.

J.M. Tornero (Universidad de Sevilla)

October 2009

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

$$1 \to K^* \longrightarrow I_K \longrightarrow C_K \to 1$$

we get

$$1 = H^{-1}(G, C_{\mathcal{K}}) \longrightarrow H^{0}(G, \mathcal{K}^{*}) \longrightarrow H^{0}(G, \mathbf{I}_{\mathcal{K}})$$

(日) (同) (三) (三)

October 2009

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

$$1 \to K^* \longrightarrow I_K \longrightarrow C_K \to 1$$

we get

$$1 = H^{-1}(G, C_{\mathcal{K}}) \longrightarrow H^{0}(G, \mathcal{K}^{*}) \longrightarrow H^{0}(G, \mathbf{I}_{\mathcal{K}})$$

Therefore

$$H^{0}(G, K^{*}) = k^{*}/N_{K|k}K^{*} \hookrightarrow H^{0}(G, \mathbf{I}_{K}) = \oplus_{\mathfrak{p}}H^{0}(G_{\mathfrak{P}}, K_{\mathfrak{P}}^{*}),$$

which is the statement of the theorem, in a sophisticated way.

(日) (同) (三) (三)

October 2009

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

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

October 2009

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

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

The local Artin map is

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

October 2009

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

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

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

(日) (同) (三) (三)

October 2009

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

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

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

$$\begin{array}{ll} k_{\mathfrak{p}}^{*} & \stackrel{\phi_{\mathfrak{p}}}{\longrightarrow} & D\left(\mathfrak{P}\right) \simeq \mathsf{Gal}\left(\mathcal{K}_{\mathfrak{P}}|k_{\mathfrak{p}}\right) \\ \downarrow & & \downarrow \\ \mathbf{I}_{k} & \stackrel{\phi_{k}}{\longrightarrow} & \mathcal{G} \\ \alpha & \longmapsto & \phi_{k}(\alpha)_{|\mathcal{K}} \end{array}$$

commutes.

Artin Reciprocity Law: How to patch

The definition of ϕ_k can be seen as follows. Take $\alpha \in I_k$, 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).

< ロ > < 同 > < 回 > < 回 > < 回

Artin Reciprocity Law: How to patch

The definition of ϕ_k can be seen as follows. Take $\alpha \in I_k$, 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)

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

< ロ > < 同 > < 回 > < 回 > < 回

October 2009

Artin Reciprocity Law: How to patch

The definition of ϕ_k can be seen as follows. Take $\alpha \in I_k$, 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)

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

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

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

verifies:

・ロト ・聞ト ・ヨト ・ヨト

October 2009
Artin Reciprocity Law: The statement

Theorem (Artin Reciprocity Law).- The homeomorphism

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

verifies:

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

October 2009

Artin Reciprocity Law: The statement

Theorem (Artin Reciprocity Law).- The homeomorphism

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

verifies:

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

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

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

Artin Reciprocity Law: In terms of C_k

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

< □ > < 同 > < 回 > < 回 > < 回

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 $C_k \longrightarrow \text{Gal}(k^{ab}|k)$

(日) (同) (三) (三)

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 $C_k \longrightarrow \text{Gal}(k^{ab}|k)$
- 2) ϕ_k induces an isomorphism $\phi_{K|k} : C_k / N_{K|k} C_K \simeq \text{Gal}(K|k)$

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

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

$$\operatorname{\mathsf{Gal}}\left(\mathcal{O}_{\mathcal{K}}/\mathfrak{P}:\mathcal{O}_k/\mathfrak{p}
ight)\simeq\operatorname{\mathsf{Gal}}\left(\mathcal{K}_{\mathfrak{P}}|k_\mathfrak{p}
ight)$$

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

Remember $\operatorname{Gal}(\mathcal{O}_{\mathcal{K}}/\mathfrak{P}:\mathcal{O}_k/\mathfrak{p})$ is generated by the Frobenius element $x\mapsto x^q$.

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

October 2009

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

$$\operatorname{\mathsf{Gal}}\left(\mathcal{O}_{\mathcal{K}}/\mathfrak{P}:\mathcal{O}_k/\mathfrak{p}
ight)\simeq\operatorname{\mathsf{Gal}}\left(\mathcal{K}_{\mathfrak{P}}|k_\mathfrak{p}
ight)$$

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

Remember $\operatorname{Gal}(\mathcal{O}_{\mathcal{K}}/\mathfrak{P}:\mathcal{O}_k/\mathfrak{p})$ is generated by the Frobenius element $x\mapsto x^q$.

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

▲ロト ▲圖ト ▲画ト ▲画ト 三回 - のへで

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 $q = \sharp(\mathcal{O}_k/\mathfrak{p})$.

< ロ > < 同 > < 回 > < 回 > < 回

Artin Reciprocity Law: Properties of the Frobenius element

The Frobenius element can alternatively be described as the only element $\sigma \in {\cal G}$ 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 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.

▲ロト ▲圖ト ▲画ト ▲画ト 三回 - のへで

Artin Reciprocity Law: Proof (I)

To prove Artin Reciprocity Law it suffices proving:

• • • • • • • • • • • •

October 2009

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.

(日) (同) (三) (三)

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.

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Artin Reciprocity Law: Proof (II)

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

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

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.

(日) (同) (三) (三)

Artin Reciprocity Law: Proof (II)

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

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

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

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

October 2009

Artin Reciprocity Law: Proof (II)

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

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

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.

イロト 人間ト イヨト イヨト

October 2009

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).

< ロ > < 同 > < 回 > < 回 > < 回 > < 回

October 2009

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).

(日) (同) (三) (三)

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).

イロト イポト イヨト イヨト

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

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

< ロ > < 同 > < 回 > < 回 > < 回

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.

・ロン ・四 ・ ・ ヨン ・ ヨン

October 2009

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.

イロト 不得下 イヨト イヨト 二日

October 2009

Thanks a lot!

・ロト ・ 日 ト ・ ヨ ト ・ ヨ ト

æ

68 / 68

October 2009

Thanks a lot!

Any questions?

3

・ロト ・聞 ト ・ ヨト ・ ヨト

Thanks a lot!

Any questions?

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

• • • • • • • • • • • •

October 2009