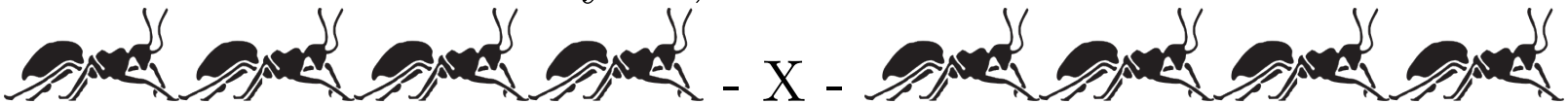
Imaginary Quadratic Fields With Isomorphic Abelian Galois Groups

A. Angelakis[♯♭], P. Stevenhagen[♯]

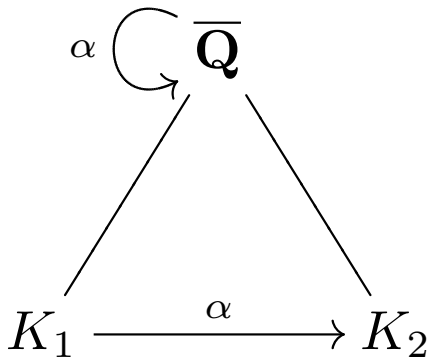
Universiteit Leiden[♯], Université Bordeaux 1[♭]

July 12, 2012 - UCSD



Let K be a number field and $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group.

- **Question**: Does G_K determine K?
  - meaning, if $G_{K_1} \cong G_{K_2}$ then $K_1 \cong K_2$?
- **Answer**: Yes!
  - Neukirch, Ikeda, Iwasawa & Uchida (around $1969 - 75$)
  - $\exists!\ \alpha \in \mathrm{Aut}(\overline{\mathbf{Q}}) :\ \alpha[K_1] = K_2$ inducing $G_{K_1} \cong G_{K_2}$



Let K be a number field and $G_K^{\mathrm{solv}} = \mathrm{Gal}(K^{\mathrm{solv}}/K)$ the maximal prosolvable quotient of G_K.

- **Question**: Does G_K^{solv} determine K?
  - meaning, if $G_{K_1}^{\mathrm{solv}} \cong G_{K_2}^{\mathrm{solv}}$ then $K_1 \cong K_2$?
- **Answer**: Yes!
  - Neukirch, Ikeda, Iwasawa & Uchida (around $1969 - 75$)

Let K be a number field and $A_K = G_K/\overline{[G_K, G_K]}$ the maximal *abelian* quotient of G_K.

- **Question**: Does A_K determine K?
  - meaning, if $A_{K_1} \cong A_{K_2}$ then $K_1 \cong K_2$?
- **Answer**: No!!!
  - First examples found by Onabe (1976)
  - Uses Kubota's (1957) description of the character group of G_K in terms of Ulm invariants
  - A_K is not **explicitly** given but characterized by the number of Ulm invariants

- K^{ab} is not "explicit", but A_K is explicit (class field theory)

Theorem

Many imaginary quadratic fields K have the same minimal absolute abelian Galois group

$$A_K \cong M = \widehat{\mathbf{Z}}^2 \times \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$$

- here $\widehat{\mathbf{Z}} = \varprojlim \mathbf{Z}/n\mathbf{Z}$, the profinite completion of $\mathbf{Z}$
- 2291 out of 2348, meaning, more than 97.5% of K of prime class number < 100 have this *minimal* group
- Conjecture: there are *infinitely many* such K

- The topological group A_K is a module over $\widehat{\mathbf{Z}}$:
- The exponentiation of elements of this group with ordinary integers extends to exponentiation with elements of $\widehat{\mathbf{Z}}$
- For any $\sigma \in A_K$, we have

$$\lim_{n\to\infty} \sigma^{n!} = \mathrm{id} \in A_K$$

- Describe infinite abelian Galois groups as modules over $\widehat{\mathbf{Z}}$

- Toy example: $K = \mathbf{Q}$
  By Kronecker-Weber theorem $\mathbf{Q}^{\mathrm{ab}} = \cup_{n=1}^{\infty} \mathbf{Q}(\zeta_n)$ is the maximal cyclotomic extension of $\mathbf{Q}$
- This yields the well-known isomorphism
  $A_{\mathbf{Q}} = \varprojlim (\mathbf{Z}/n\mathbf{Z})^* = \widehat{\mathbf{Z}}^*$
- $\widehat{\mathbf{Z}}^* = \prod_p \mathbf{Z}_p^*$, (Chinese Remainder Theorem)

$$\begin{aligned} \mathbf{Z}_p^* &\cong \mathbf{Z}/(p-1)\mathbf{Z} \times (1 + p\mathbf{Z}_p) \\ &\cong \mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}_p, \quad (p \neq 2) \end{aligned}$$

- $T_{\mathbf{Q}} \cong \prod_p (\mathbf{Z}/(p-1)\mathbf{Z}) \cong \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$
- This is "the" countable product of finite cyclic groups having infinitely many cyclic components of prime power order for every prime

- Taking the product over all p, we obtain

$$\begin{aligned} A_{\mathbf{Q}} &\cong \widehat{\mathbf{Z}} \times \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z} \\ &\cong \widehat{\mathbf{Z}} \times T_{\mathbf{Q}} \end{aligned}$$

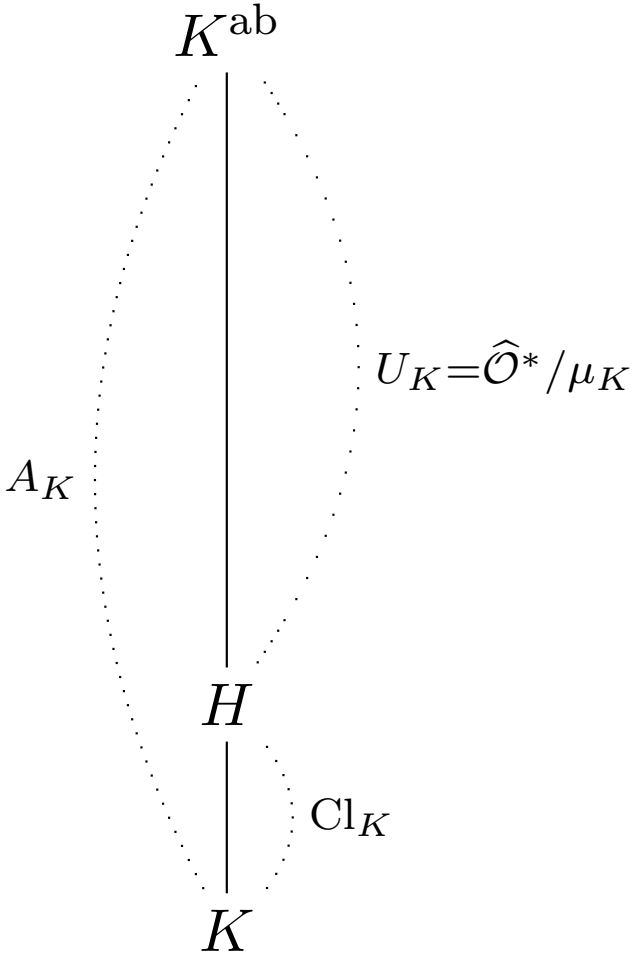
- $T_{\mathbf{Q}}$ is the *closure* of the torsion subgroup of $A_{\mathbf{Q}}$
- It is not a torsion group itself
- $A_{\mathbf{Q}}/T_{\mathbf{Q}}$ is a free $\widehat{\mathbf{Z}}$-module of rank 1
- The subfield of $\mathbf{Q}^{\mathrm{ab}}$ left invariant by the subgroup $T_{\mathbf{Q}} \subset A_{\mathbf{Q}} = \mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q})$ is the unique $\widehat{\mathbf{Z}}$-extension of $\mathbf{Q}$

- K^{ab} "unknown" for arbitrary K
- Class field theory: A_K for arbitrary K

$$A_K = [(\prod_{\mathfrak{p}\leq\infty}{}' K_{\mathfrak{p}}^*)/K^*]/(\text{conn. comp. of unit element})$$

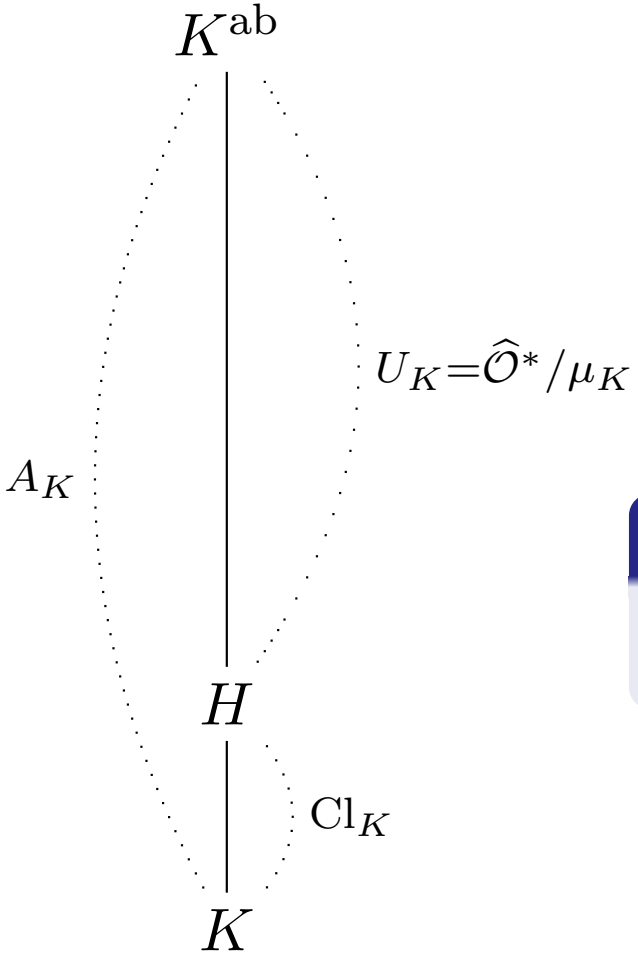
- **From now on** we take K to be imaginary quadratic. Then,

$$A_K = (\prod_{\mathfrak{p}<\infty}{}' K_{\mathfrak{p}}^*)/K^*$$



- H is the Hilbert class field
- Cl_K is the class group of K
- μ_K is the group of roots of unity in K (of order ≤ 6)
- $\widehat{\mathcal{O}}^* = \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*$ unit group of the profinite completion of the ring of integers $\mathcal{O} = \mathcal{O}_K$

$$\begin{aligned} A_K &= (\prod_{\mathfrak{p}<\infty}{}' K_{\mathfrak{p}}^*)/K^* \\ \cup & \\ U_K &= (\prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*)/\mathcal{O}^* = \widehat{\mathcal{O}}^*/\mu_K \end{aligned}$$



- $K_{\mathfrak{p}}^* \supset \mu_{\mathfrak{p}}$ local roots of unity
- $\widehat{\mathcal{O}}^* = \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^* \supset \prod_{\mathfrak{p}} \mu_{\mathfrak{p}} = T_K$
- T_K is the closure of the torsion subgroup of $\widehat{\mathcal{O}}^*$

Lemma (1)

$$\widehat{\mathcal{O}}^* \cong \widehat{\mathbf{Z}}^{[K:\mathbf{Q}]} \times T_K$$

- $\widehat{\mathcal{O}}^* \cong \widehat{\mathbf{Z}}^2 \times T_K$

Lemma (2)

Let w_K be the number of roots of unity in K. Then we have a non-canonical isomorphism of profinite groups

$$T_K \cong \prod_{n \geq 1} \mathbf{Z}/nw_K\mathbf{Z}$$

- If w_K is squarefree, then $T_K \cong T_{\mathbf{Q}}$

Lemma (3)

We have a non-canonical isomorphism

$$T_K/\mu_K \cong \prod_{n \geq 1} \mathbf{Z}/nw_K\mathbf{Z}$$

Theorem

$$U_K = \widehat{\mathcal{O}}^*/\mu_K \cong \widehat{\mathbf{Z}}^2 \times T_K/\mu_K \cong \begin{cases} \widehat{\mathbf{Z}}^2 \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}, & K \neq \mathbf{Q}(i) \\ \widehat{\mathbf{Z}}^2 \times \prod_{n=1}^{\infty} \mathbf{Z}/4n\mathbf{Z}, & K = \mathbf{Q}(i) \end{cases}$$

(isomorphisms of profinite groups)

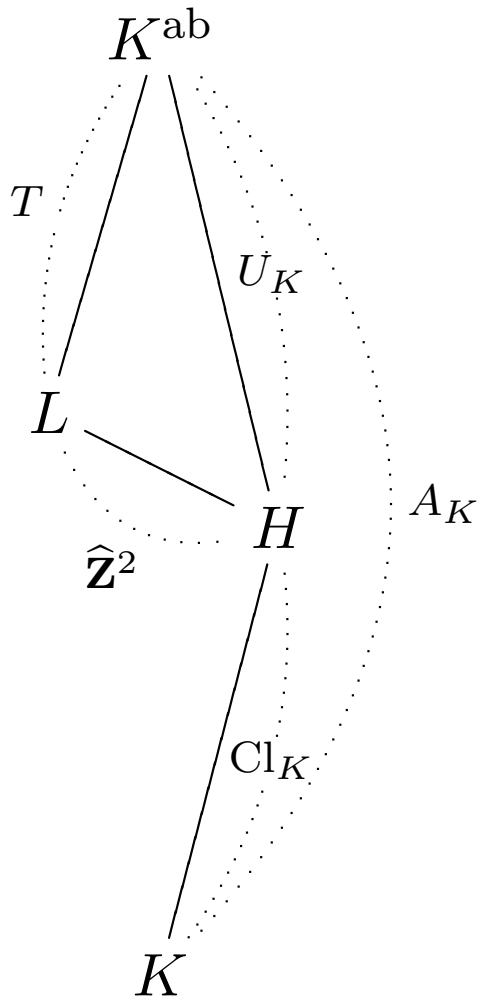
Corollary

All imaginary quadratic $K \neq \mathbf{Q}(i)$ of class number 1 have

$$A_K \cong \widehat{\mathbf{Z}}^2 \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}$$

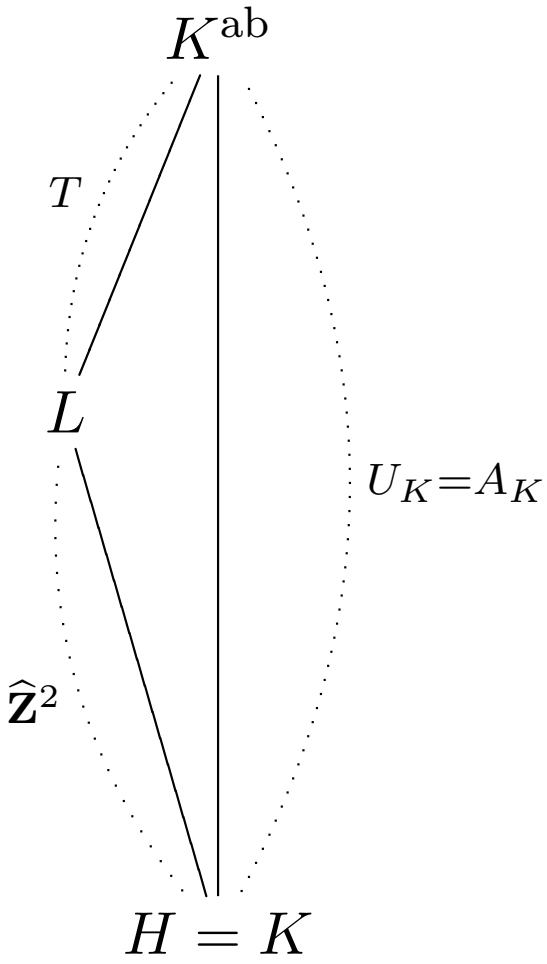
- This implies Onabe's observation: there are 8 such K!

diagrams 1/2



The invariant field L of the closure T of the torsion subgroup of U_K is an extension of H with group $\widehat{\mathbf{Z}}^2$

class number 1:



The invariant field L of the closure T of the torsion subgroup of U_K is an extension of K with group $\widehat{\mathbf{Z}}^2$

Question: $A_K \cong M$ for $h_K > 1$?

- $K \neq \mathbf{Q}(i)$ imaginary quadratic

$$1 \to U_K \longrightarrow A_K \longrightarrow \mathrm{Cl}_K \to 1 \tag{1}$$

  - $U_K \cong \widehat{\mathbf{Z}}^2 \times T$
  - Does not depend on K
  - It is isomorphic to the "minimal" Galois group

$$M = \widehat{\mathbf{Z}}^2 \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}$$

- **Question**: Can A_K be isomorphic to M for $h_K > 1$?
  - If (1) splits, then A_K is isomorphic to M

Theorem

For every imaginary quadratic field K, the sequence

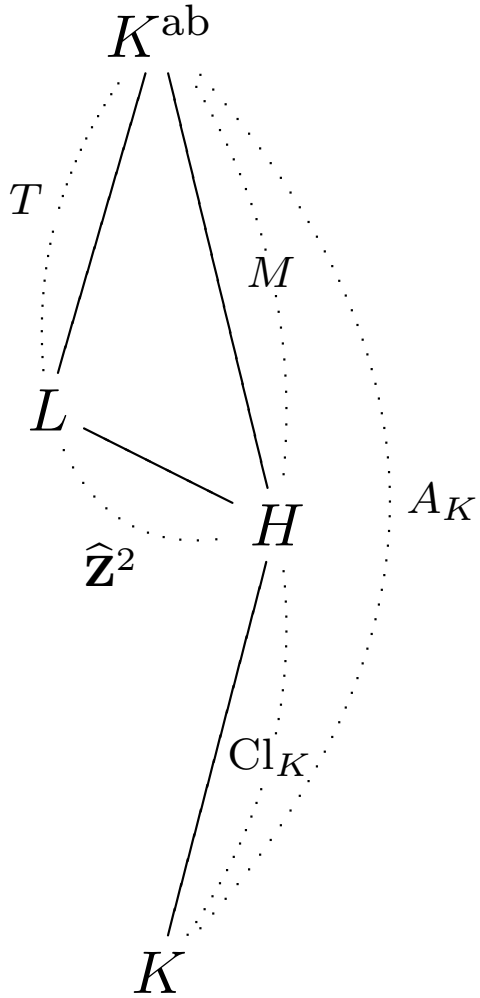
$$1 \to U_K \longrightarrow A_K \xrightarrow{\psi} \mathrm{Cl}_K \to 1$$

is totally non-split, i.e., there is no non-trivial subgroup $C \subset \mathrm{Cl}_K$ for which the associated subextension

$$1 \to U_K \to \psi^{-1}[C] \to C \to 1$$

is split

... still $A_K \cong M$



- We will show: even though

$$1 \to M \longrightarrow A_K \longrightarrow \mathrm{Cl}_K \to 1$$

is non-split, we may still have

$$A_K \cong M$$

$$\begin{array}{ccccccc} 1 & \to & U_K & \longrightarrow & A_K & \longrightarrow & \mathrm{Cl}_K \to 1 \\ & & || & & \wr & & \\ & & M & = & \widehat{\mathbf{Z}}^2 \times T & & \end{array}$$

is totally non-split, but the "quotient sequence"

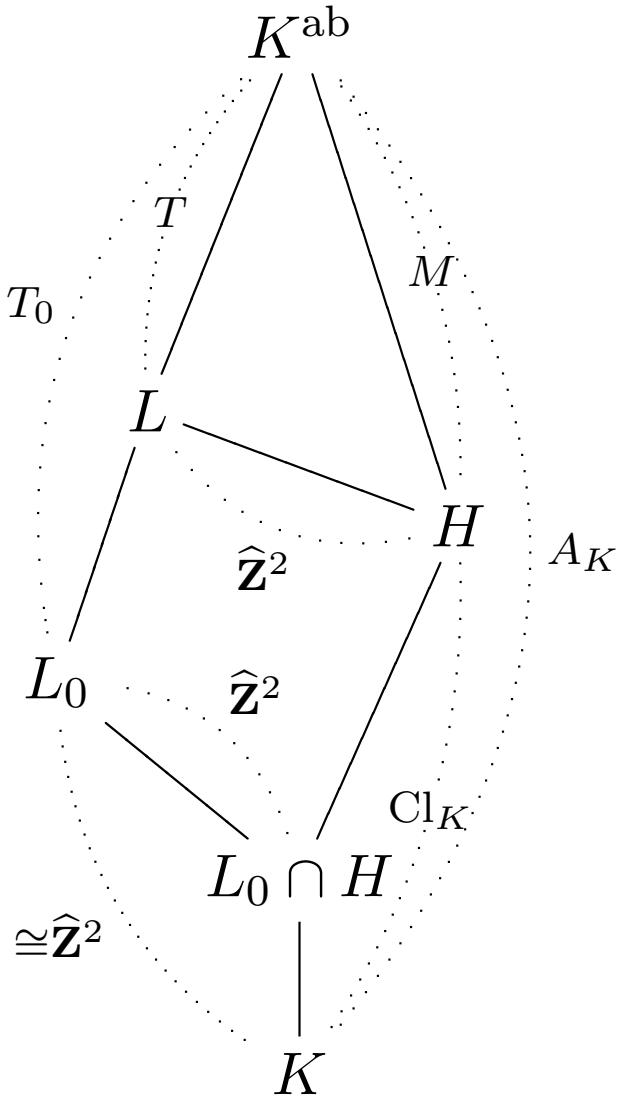
$$\begin{array}{ccccccc} 1 & \to & U_K/T & \longrightarrow & A_K/T & \longrightarrow & \mathrm{Cl}_K \to 1 \\ & & || & & \wr & & \\ & & \widehat{\mathbf{Z}}^2 & & & & \end{array}$$

can be split or non-split.

- If it is totally non-split, we have
$$A_K/T \cong \widehat{\mathbf{Z}}^2$$

and
$$A_K \cong \widehat{\mathbf{Z}}^2 \times T = M!$$

Galois diagram



Translation under Galois theory:

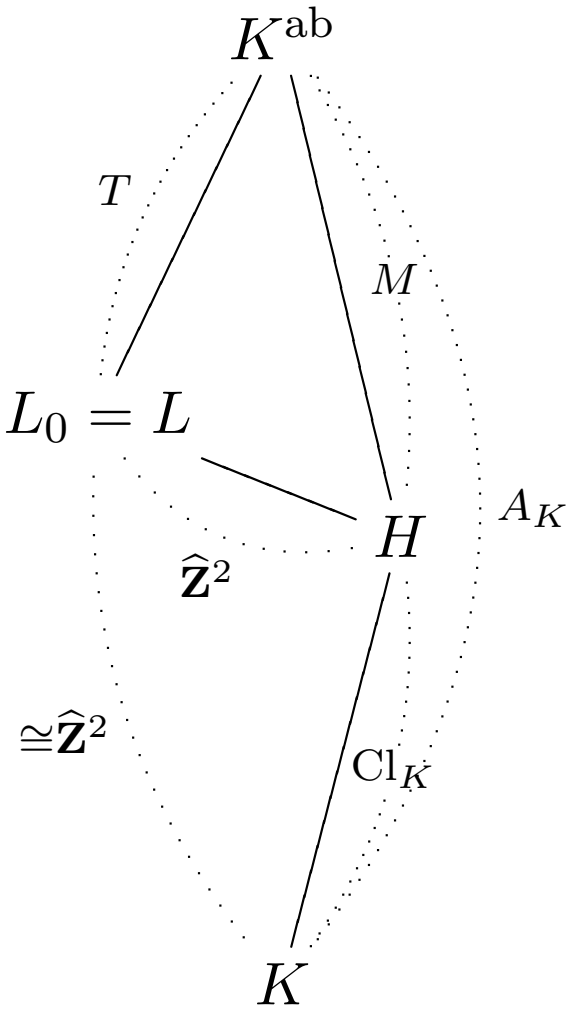
- $A_K/T = \mathrm{Gal}(L/K)$
- $L_0 =$ "maximal $\widehat{\mathbf{Z}}$-extension of K"
- the sequence

$$1 \to U_K/T \longrightarrow A_K/T \longrightarrow \mathrm{Cl}_K \to 1$$

is totally non-split if and only if

$$L = L_0$$
$$\Updownarrow$$
$$A_K \cong M$$

Galois diagram: $L = L_0$



Totally non-split case:

$$H \subset L_0$$

- **Question:** How can we decide numerically whether this is the case?
- **Answer:** ...
  - do not use fields!
  - Class field theory suffices!

$$\begin{array}{ccccccc} 1 \to U_K/T & \longrightarrow & A_K/T & \longrightarrow & \mathrm{Cl}_K & \to & 1 \\ \| \wr & & \| \wr & & & & \\ \widehat{\mathcal{O}}^* / \prod_{\mathfrak{p}} \mu_{\mathfrak{p}} & & \widehat{K}^* / K^* \cdot \prod_{\mathfrak{p}} \mu_{\mathfrak{p}} & & & & \end{array}$$

Lemma

Suppose $\mathrm{Cl}_K = \langle [\mathfrak{a}] \rangle$ *is cyclic of prime order* p*. Then the above sequence is split iff every* $\alpha \in K^*$ *generating* $\mathfrak{a}^p$ *is locally everywhere "a* p^{th} *power up to roots of unity"*

- This means: for all primes $\mathfrak{p}$ we have
$$\alpha = \zeta_{\mathfrak{p}} \cdot x_{\mathfrak{p}}^p$$
with $\zeta_{\mathfrak{p}} \in \mu_{\mathfrak{p}}$ and $x_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$
- This condition is trivially satisfied at $\mathfrak{p} \nmid p$
- It is a local computation at $\mathfrak{p} \mid p$

Algorithm: to decide whether $A_K = M$

- **Input:** K imaginary quadratic
- **Checks:** for each prime $p \mid h_K$ whether

$$\phi_p : \mathrm{Cl}_K[p] \longrightarrow (\prod_{\mathfrak{p}|p} \mathcal{O}_{\mathfrak{p}}^*/\mu_{\mathfrak{p}})/(p^{\text{th}} \text{ powers})$$

$$\mathfrak{a} \longmapsto \overline{\alpha}, \qquad (\text{if } \mathfrak{a}^p = \alpha\mathcal{O})$$

  is injective
- **Output:** Yes, if for every prime $p \mid h_K$ the map ϕ_p is injective
  - Involves class group computation
  - local computation at $\mathfrak{p} \mid p$
  - and becomes linear algebra over $\mathbf{F}_p$
- **Remark:** For $p = 2$ we have a theorem, so no computation is necessary

Prime $h_K = p < 100$. $A_K = M$ for more than 97.5% of all K

p	$\#K : h_K = p$	non-split	split
2	18	8	$\mathbb{Q}(\sqrt{-35}), \mathbb{Q}(\sqrt{-51}), \mathbb{Q}(\sqrt{-91}),$ $\mathbb{Q}(\sqrt{-115}), \mathbb{Q}(\sqrt{-123}), \mathbb{Q}(\sqrt{-187}),$ $\mathbb{Q}(\sqrt{-235}), \mathbb{Q}(\sqrt{-267}), \mathbb{Q}(\sqrt{-403}),$ $\mathbb{Q}(\sqrt{-427})$
3	16	13	$\mathbb{Q}(\sqrt{-643}), \mathbb{Q}(\sqrt{-331}), \mathbb{Q}(\sqrt{-107})$
5	25	19	$\mathbb{Q}(\sqrt{-1723}), \mathbb{Q}(\sqrt{-1123}), \mathbb{Q}(\sqrt{-1051}),$ $\mathbb{Q}(\sqrt{-739}), \mathbb{Q}(\sqrt{-443}), \mathbb{Q}(\sqrt{-347})$
7	31	27	$\mathbb{Q}(\sqrt{-5107}), \mathbb{Q}(\sqrt{-2707}), \mathbb{Q}(\sqrt{-1163}),$ $\mathbb{Q}(\sqrt{-859})$
11	41	36	$\mathbb{Q}(\sqrt{-9403}), \mathbb{Q}(\sqrt{-5179}), \mathbb{Q}(\sqrt{-2027}),$ $\mathbb{Q}(\sqrt{-10987}), \mathbb{Q}(\sqrt{-13267})$
13	37	34	$\mathbb{Q}(\sqrt{-11923}), \mathbb{Q}(\sqrt{-2963}), \mathbb{Q}(\sqrt{-1667})$
17	45	41	$\mathbb{Q}(\sqrt{-25243}), \mathbb{Q}(\sqrt{-16699}), \mathbb{Q}(\sqrt{-8539}),$ $\mathbb{Q}(\sqrt{-383})$
19	47	43	$\mathbb{Q}(\sqrt{-17683}), \mathbb{Q}(\sqrt{-17539}), \mathbb{Q}(\sqrt{-17299}),$ $\mathbb{Q}(\sqrt{-4327})$
23	68	65	$\mathbb{Q}(\sqrt{-21163}), \mathbb{Q}(\sqrt{-9587}), \mathbb{Q}(\sqrt{-2411})$
29	83	80	$\mathbb{Q}(\sqrt{-110947}), \mathbb{Q}(\sqrt{-74827}), \mathbb{Q}(\sqrt{-47563})$
31	73	70	$\mathbb{Q}(\sqrt{-46867}), \mathbb{Q}(\sqrt{-12923}), \mathbb{Q}(\sqrt{-9203})$
37	85	83	$\mathbb{Q}(\sqrt{-28283}), \mathbb{Q}(\sqrt{-20011})$
41	109	106	$\mathbb{Q}(\sqrt{-96763}), \mathbb{Q}(\sqrt{-21487}), \mathbb{Q}(\sqrt{-14887})$
43	106	105	$\mathbb{Q}(\sqrt{-42683})$
47	107	107	$\varnothing$
53	114	114	$\varnothing$
59	128	126	$\mathbb{Q}(\sqrt{-166363}), \mathbb{Q}(\sqrt{-125731})$
61	132	131	$\mathbb{Q}(\sqrt{-101483})$
67	120	119	$\mathbb{Q}(\sqrt{-652723})$
71	150	150	$\varnothing$
73	119	117	$\mathbb{Q}(\sqrt{-597403}), \mathbb{Q}(\sqrt{-358747})$
79	175	174	$\mathbb{Q}(\sqrt{-64303})$
83	150	150	$\varnothing$
89	192	189	$\mathbb{Q}(\sqrt{-348883}), \mathbb{Q}(\sqrt{-165587}), \mathbb{Q}(\sqrt{-48779})$
97	185	184	$\mathbb{Q}(\sqrt{-130051})$

- Numerical observation: for $h_K = p$, we have $A_K = M$ for a fraction $1 - 1/p$ of fields

Conjecture

There are infinitely many imaginary quadratic fields K for which the absolute abelian Galois group is isomorphic to

$$M = \widehat{\mathbf{Z}}^2 \times \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$$

- The numerical evidence may be strong, but we do not even have a **theorem** that there are infinitely many prime numbers that occur as the class number of an imaginary quadratic field
- And even if we had, we have no **theorem** telling us what the distribution between split and non-split will be

checked already

We checked numerically:

- For $p \parallel h_K$, splitting at p occurs with frequency $1/p$
- Splitting at different primes $p, q \parallel h_K$ is "independent"
- No influence of the splitting over the three kinds of local behavior in K of the prime p
- Splitting at p, where $p^2 \parallel h_K$ and $\mathrm{Cl}_K \cong C_p \times C_p \times C_m,\ p \nmid m$, occurs with frequency $1/p^2$

Future work:

- Cohen-Lenstra should yield asymptotic number of K with $A_K = M$
- Extend the theory to Real quadratic fields!
- Go further ... to any number field!!

229 ·  - X -

 + ...

Thank You
for Your Attention!