Open problems:
CM-types acting on class groups

Gabor Wiese*

October 29, 2003

These are (modified) notes and slides of a talk given in the Leiden number theory seminar, whose general topic are Shimura varieties.

The aim of the talk is to formulate a purely number theoretic question (of Brauer-Siegel type), whose (partial) answer might lead to progress on the so-called André-Oort conjecture on special subvarieties of Shimura varieties (thus the link to the seminar).

The question ought to be considered as a special case of problem 14 in [EMO], which was proposed by Bas Edixhoven and which we recall now.

> Let g be a positive integer and let A_g be the moduli space of principally polarized abelian varieties of dimension g.
>
> Do there exist $C, \delta > 0$ such that for every CM-point x of A_g (i.e. the corresponding abelian variety has CM) one has
>
> $$|G_{\mathbb{Q}}.x| \geq C|\mathrm{discr}(R_x)|^{\delta},$$
>
> where R_x is the centre of the endomorphism ring of the abelian variety corresponding to x???

What we will call the Siegel question in the sequel, is obtained by restricting to simple abelian varieties.

In the talk I will prove everything that seems to be known on the question up to this moment, namely the case of dimension 2. This was worked out by Bas Edixhoven in [E].

The arguments used are quite "ad hoc" and I will try to point out, where obstacles to generalisations seem to lie.

The boxes correspond more or less to the slides I used.

*gabor@math.leidenuniv.nl

Open problems:
CM-types acting on class groups

Gabor Wiese
Leiden, 22/10/2003

Aims of the talk:

- Present a question supposed to imply higher dimensional cases of the André-Oort conjecture.
- Relate it to other questions.
- Present and prove known results.
- Try to show the problems.
- **ASK YOUR HELP!**

The result in dimension 2 is actually obtained by reducing to the image of multiplication by 4 on the class group of the CM field in question. Thus the "other question" I am referring to is to estimate the size of the image of multiplication by a (fixed) integer on the class group.

Let us start the talk by explaining all essential notions, although they are "generally well-known"...

A number field K is a **CM field** if

- K is a totally imaginary,
- $[K : K^+] = 2$ with K^+ the max. tot. real subfield.

Examples:

- $\mathbb{Q}(\zeta_n)$,
- imaginary quadratic fields.
- Produce more with prop. below.

Let $\alpha : K \hookrightarrow \mathbb{C}$ embedding. Then the map

$$c : x \mapsto \alpha^{-1}(\overline{\alpha(x)})$$

is in $G(K|K^+)$, indep. of α: the **complex conjugation.**

Over every real embedding $\alpha^+ : K^+ \hookrightarrow \mathbb{R}$ there are precisely two complex embeddings

$$\alpha, \alpha \circ c : K \hookrightarrow \mathbb{C}.$$

The thing of crucial importance for us will be the last point, namely that the embeddings of a CM field into $\mathbb{C}$ come in pairs.

I should remark that the complex conjugation is indeed well-defined, because $K|K^+$ is normal as it is of degree 2. Moreover, as K is totally imaginary, the map c will not be the identity. But it is an element in $G(K|K^+)$, which proves the independence of the chosen embedding α.

On the next slide we shall look at the "group theory" of a CM field that is Galois over $\mathbb{Q}$.

Proposition 1 *Let $K|\mathbb{Q}$ be CM and Galois, group $\widehat{G}$.*

(a) $c \in \widehat{G}$ is central of order 2.

(b) $K^+|\mathbb{Q}$ is Galois with $G = G(K^+|\mathbb{Q})$.

(c) Central extension $0 \to < c > \to \widehat{G} \to G \to 0$.

(d) If $H \leq \widehat{G}$ with $c \notin H$, then $< c > \times H \leq \widehat{G}$ and K^H is CM with totally real subfield $K^{<c>\times H}$

(e) If $L|\mathbb{Q}$ is totally real and Galois with group H, then LK is CM with totally real subfield LK^+. Moreover, LK is Galois with group contained in $\widehat{G} \times H$.

Moreover, composites and Galois closures of CM fields are CM fields.
Given K^+ totally real, **Kummer theory** gives:

$$\{K|K^+ \text{ CM }\} \overset{1-1}{\leftrightarrow}$$

$$\{< x, (K^+)^{*2} > \mid x \in (K^+)^* \text{ tot. negative }\}.$$

Some remarks on the proof. That complex conjugation is an involution is clear. That c is central is precisely the fact that c does not depend on the embedding into $\mathbb{C}$. So in the definition of c, one can replace α by αg, where g is an arbitrary element of $\widehat{G}$.

(b) is clear as $K^+ = K^{<c>}$ and $< c >$ is normal, as it is central.

(c) is only a reformulation. But let's remark that central extensions are well-understood. E.g. they are classified by the group cohomology group $H^2(G, \mathbb{Z}/2)$.

(d) and (e) follow from Galois theory.

That Galois closures of CM fields are CM follows from the fact that composites of CM fields are CM. That can be obtained from the fact that a totally imaginary field is CM if and only if it has a unique complex conjugation via embeddings into $\mathbb{C}$.

The remark on Kummer theory is supposed to suggest that in general one can obtain infinitely many CM fields with a fixed totally real subfield. In the sequel we shall be concerned with such infinite sets of CM fields.

On the next slide we shall introduce one of the words in the title, namely a CM type.

Given a CM field $K|\mathbb{Q}$. A **CM type** is a subset

$$\Phi_K \subseteq \mathrm{Hom}(K, \mathbb{C})$$

such that $\Phi_K \sqcup \Phi_K \circ c = \mathrm{Hom}(K, \mathbb{C})$.

If $K|\mathbb{Q}$ is Galois, then we consider Φ_K as a subset of $\widehat{G}$, resp. as a split (not nec. hom.) $G \to \widehat{G}$.
In this case we say that Φ_K is **essentially the same** as $\Phi_K \circ g$ (elementwise for fixed $g \in \widehat{G}$).

Let $M|K$ be CM fields and Φ_K a CM type. We define the **induced CM type** by

$$\Phi_M = \{\phi \in \mathrm{Hom}(M, \mathbb{C}) \mid \phi|_K \in \Phi_K \}.$$

A CM type that is not (non-trivially) induced is said to be **primitive**.

Let $K|\mathbb{Q}$ be a Galois CM field with group $\widehat{G}$. For every CM type Φ_K we define a **CM element**

$$t_{\Phi_K} := \sum_{g \in \Phi_K} g^{-1} \in \mathbb{Z}[\widehat{G}].$$

A CM type is thus a choice of one embedding out of each pair.

In the Galois case the identification of the set of embeddings with the Galois group does, of course, depend on the choice of one embedding. But for two different choices the resulting sets are essentially the same.

The fact that we take inverses in the definition of the CM element comes from the application (see [E]). It only makes a difference, when considering induced CM types (the elementwise inverse of a CM type is also a CM type).

On the next slide we shall consider low dimensional cases to illustrate the definitions. However, we will also use them in the proof to come.

- $d = 1$, K imaginary quadratic:
  CM types: $\Phi_K^1 = \{1\}$, $\Phi_K^2 = \{c\}$
  ("essentially the same": $\Phi_K^1 \circ c = \Phi_K^2$).
  So $t_1 = 1$ and $t_2 = c$.

- $d = 2$, $K|\mathbb{Q}$ Galois, $\widehat{G} = \mathbb{Z}/4 =< \sigma >$:
  Then $c = \sigma^2$. Only one essentially different CM type:

  $$\Phi_K = \{1, \sigma\}.$$

  It is primitive and $t = 1 + \sigma^3$.

- $d = 2$, $K|\mathbb{Q}$ Galois, $\widehat{G} = \mathbb{Z}/2 \times \mathbb{Z}/2$:
  Say $\widehat{G} =< c > \times < \sigma >$. Then essentially all CM types are:

  $$\Phi_K^1 = \{1, \sigma\}, \Phi_K^2 = \{1, c\sigma\}.$$

  They are induced from $K^{<\sigma>}$ resp. $K^{<c\sigma>}$.
  CM elements: $t_1 = 1 + \sigma$ and $t_2 = 1 + c\sigma$.

Here d denotes the degree of the totally real subfield over $\mathbb{Q}$. We want to consider all cases with $d = 2$. There is one more, namely the one of a non-Galois extension of degree 4.

- $d = 2$, $K|\mathbb{Q}$ not Galois of degree 4:
  $M|\mathbb{Q}$ Galois closure.
  $\widehat{G} = D_4 =< \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} >$.
  Then $c = \sigma^2$, $K = M^{<\tau>}$, $K^+ = M^{<\tau, c>}$.
  Essentially all CM types of K are

  $$\Phi_K^1 = \{1|_K, \sigma|_K\}, \Phi_K^2 = \{1|_K, \sigma^3|_K\}.$$

  The induced CM types are

  $$\Phi_M^1 = \{1, \tau, \sigma, \sigma\tau\}, \Phi_M^2 = \{1, \tau, \sigma^3, \tau\sigma\}.$$

  They are essentially the same.
  CM element: $t = 1 + \tau + \sigma^3 + \sigma\tau$. (Note $\tau\sigma = \sigma^3\tau$.)

Higher dimensions become much more complicated!

We are now ready for the questions.

SQ (= strong question = Siegel question):
Fix an integer $d \geq 1$. Are there $\delta, C \in \mathbb{R}_{>0}$ such that the following holds?
For all CM fields $K|\mathbb{Q}$ of degree $2d$ and all primitive CM types Φ_K with Galois closure $M|\mathbb{Q}$, induced CM type Φ_M and CM element $t = \sum_{g \in \Phi_M} g^{-1}$ we have:

$$|\mathrm{Im}(\mathrm{CL}_M \xrightarrow{t\cdot} \mathrm{CL}_M)| \ \geq \ C|d_K|^{\delta}.$$

HQ (= weak question = Hilbert question):
The same, except that K^+ is fixed.

nSQ and nHQ:
The same as SQ resp. HQ, except that t is replaced by an integer n, i.e. we consider the image of
$\mathrm{CL}_M \xrightarrow{\cdot n} \mathrm{CL}_M$. Note: independent of CM type.

In the Siegel question the primitivity of the CM types is necessary as one sees from the following example. Consider the infinite series of CM fields for $d = 2$ obtained by $\mathbb{Q}(i, \sqrt{n})$ for n running through the positive square-free integers. The discriminants tend to infinity as n does. The group structure is $\mathbb{Z}/2 \times \mathbb{Z}/2 =< c > \times < \sigma >$ and as in the corresponding example above one can choose the CM type $\{1, \sigma\}$, hence $t = 1 + \sigma$. So the map given by applying $1 + \sigma$ factorises over the class group of $\mathbb{Q}(i)$, which is trivial. So the image is trivial, whereas the discriminants tend to infinity, contradicting the question.

Although this counter example does not work in the case of a fixed totally real subfield, it seems safer to assume primitivity in that case, too.

In his proof of the André-Oort conjecture for Hilbert modular surfaces Bas Edixhoven also treated the case of the induced CM types arising from the $\mathbb{Z}/2 \times \mathbb{Z}/2$-situation in order to avoid the general question how to deduce a lower bound for the Galois orbit of a CM point of a general abelian variety from the result on its simple factors (up to isogeny).

One might hope to treat SQ or HQ by reducing to some nSQ resp. nHQ. That's why I mention the last question, which in all generality certainly seems beyond reach at the moment. For powers of 2 it can be solved as we will see later in the talk. Maybe, one can often reduce HQ to a known case of nHQ?

Let us look at what is known.

Motivating hope:

- SQ $\stackrel{?}{\Rightarrow}$ André-Oort conj. for Siegel modular var.
- HQ $\stackrel{?}{\Rightarrow}$ André-Oort conj. for Hilbert modular var.

Results:

- $d = 1$: HQ = SQ. $t = 1$ or $t = c$. So image equals CL_K. Brauer-Siegel gives result.
- $d = 2$: HQ done by Bas Edixhoven by reducing to 4HQ, also for non-primitive CM types.

  He used this to show the André-Oort conjecture for Hilbert modular surfaces, assuming GRH.

  Here and now I give a proof, which actually shows SQ.
- $d > 2$: SQ, HQ seem **VERY DIFFICULT!**
- For $(d, n) = 1$, nHQ seems **VERY DIFFICULT!**

The hopeful implications above certainly require some work. As pointed out before the passage from simple abelian varieties to non-simple ones has to be worked out. Moreover, also on the Shimura variety side certain generalisations are required.

The state of the art is so bad (to my knowledge) that I can prove everything known (to me) in the remainder of this talk.

Following Bas Edixhoven we will first reduce HQ (resp. SQ) to 4HQ (resp. 4SQ). In a second step we will apply a corollary of the Brauer-Siegel theorem to give a positive answer to 4SQ.

Let's prepare the proof.

- Given $L|K$, one has homomorphisms $\mathrm{CL}_K \to \mathrm{CL}_L$ (induced by $K \hookrightarrow L$) and $N_{L|K} : \mathrm{CL}_L \to \mathrm{CL}_K$ (induced by the norm $N_{L|K}$).
- If $L|K$ is Galois, the index $(\mathrm{CL}_K : N_{L|K}\mathrm{CL}_L)$ divides $|G(L|K)^{\mathrm{ab}}|$.
- If $K|K^+$ is CM, $|\mathrm{Ker}(\mathrm{CL}_{K^+} \to \mathrm{CL}_K)| \in \{1, 2\}$.
- If $K|K^+$ is CM, exact sequence

$$0 \to \mathrm{CL}_K^- \to \mathrm{CL}_K \xrightarrow{N_{K|K^+}} \mathrm{CL}_{K^+} \to 0$$

  and on CL_K^- we have $c\mathfrak{P} = -\mathfrak{P}$.
- **Relative class number** $h_K^- := |\mathrm{CL}_K^-| = h_K/h_{K^+}$.
- $L|K$ CM fields. Then homomorphisms $\mathrm{CL}_K^- \to \mathrm{CL}_L^-$ and $N_{L|K} : \mathrm{CL}_L^- \to \mathrm{CL}_K^-$.

Whenever we have a field extension $L|K$ we have two conceptual maps between the class groups, the first being induced by a chosen embedding $K \hookrightarrow L$ and the other one by the norm. In the case of CM fields these maps respect the minus class group.

For general number fields these maps will be neither surjective nor injective. But in the CM case one can say a little more.

The surjectivity in the exact sequence follows from [Wa], Thm. 10.1. In fact, that theorem is a result of global class field theory. It can be obtained by slightly extending the following argument that we give in order to prove the statement on the index of the image of the norm.

If C_K denotes the idèle class group of K, global reciprocity fits into the exact sequence

$$0 \to N_{L|K}C_L \to C_K \to G(L|K)^{\mathrm{ab}} \to 0,$$

whence $(C_K : N_{L|K}C_L)$ equals the order of $G(L|K)^{\mathrm{ab}}$. Now one only uses that one has compatible (w.r.t. the norm) surjections $C_K \twoheadrightarrow \mathrm{CL}_K$ and $C_L \twoheadrightarrow \mathrm{CL}_L$, to get that the index of $N_{L|K}\mathrm{CL}_L$ in CL_K divides the order of $G(L|K)^{\mathrm{ab}}$.

The statement on the kernel of $\mathrm{CL}_{K^+} \to \mathrm{CL}_K$ is [Wa], Thm. 10.3.

We continue with the reduction of the principal question to multiplication by 4.

Standard tricks:

- Reduce to (Galois) CM subfields (i.e. identify part of CM element as a norm)
- Look at CL_K^- and replace c by -1.

Proposition 2 *[Case $d = 2$] Let $K|\mathbb{Q}$ be a CM field of degree 4 and Φ_K a CM type of K. Let $M|\mathbb{Q}$ be a Galois closure of K with group $\widehat{G}$ and $t \in \mathbb{Z}[\widehat{G}]$ the CM element of the induced CM type Φ_M.*

(a) If $\widehat{G} = \mathbb{Z}/4$ or $\widehat{G} = D_4$, then

$$|\mathrm{Im}(\mathrm{CL}_M \xrightarrow{t\cdot} \mathrm{CL}_M)| \ \geq \ \frac{1}{2}|\mathrm{Im}(\mathrm{CL}_K^- \xrightarrow{\cdot 4} \mathrm{CL}_K^-)|.$$

(b) If $\widehat{G} = (\mathbb{Z}/2)^2 =< c > \times < \sigma >$, then

$$|\mathrm{Im}(\mathrm{CL}_M \xrightarrow{\cdot t} \mathrm{CL}_M)| \ \geq \ \frac{1}{2}|\mathrm{Im}(\mathrm{CL}_L^- \xrightarrow{\cdot 2} \mathrm{CL}_L^-)|$$

for some $L \subseteq M$ imaginary quadratic.

In this proposition we shall not assume that the CM type of K is primitive. However, as we have seen before in case (b) all CM types are induced.

I should maybe point out that in SQ the primitivity refers to the CM type of K and not to the one of M (which is necessarily induced). But it would already be a big step to prove SQ for all K of some degree that are Galois over $\mathbb{Q}$.

Now I will give a proof of the proposition. Since I would also like to point out where trouble can come from, I will not restrict to the three cases above, but discuss some more. These examples will illustrate the "standard tricks" mentioned on top of the slide.

- $\widehat{G} = \mathbb{Z}/4 =< \sigma >$:
  Then $c = \sigma^2$ and as seen above essentially the only CM element is $t = 1 + \sigma^3$.
  An ad hoc method is to compose t with $1 - \sigma^3$ in the group ring $\mathbb{Z}[\widehat{G}]$ to get $(1 + \sigma^3)(1 - \sigma^3) = 1 - \sigma^2$. The size of the image of a composition is less or equal the size of the image of a single map. Now we consider the commutative diagram

$$\begin{array}{ccc} \mathrm{CL}_K & \xrightarrow{(1-\sigma^2)\cdot} & \mathrm{CL}_K \\ \uparrow & & \uparrow \\ \mathrm{CL}_K^- & \xrightarrow{\cdot 2} & \mathrm{CL}_K^- \end{array}$$

  where the bottom arrow is multiplication by 2, as σ^2 acts as -1 on CL_K^-. In the sequel I will always implicitly use a similar diagram to reduce to the minus part of the class group.

So this case reduces to finding a lower bound for the multiplication by 2 on CL_K^-, which is a little stronger than the claim in (a).

- $\widehat{G} = \mathbb{Z}/8 =< \sigma >$:
  Then $c = \sigma^4$. This case also reduces to multiplication by 2 on the minus part. However, now there are several essentially different CM types and each one seemed to require multiplication by an especially chosen element. It seems already significantly more difficult than the case $\mathbb{Z}/4$.

- $\widehat{G} = \mathbb{Z}/2 \times \mathbb{Z}/5 =< c > \times < \sigma >$:
  Here I'd like to illustrate a cyclic case, which is not of 2-power order, by looking only at two different CM elements, namely $t_1 = 1+c\sigma+\sigma^2+c\sigma^3+\sigma^4$ and $t_2 = c+\sigma+\sigma^2+\sigma^3+\sigma^4$.

  The first one can be treated as we have seen before, namely as

  $$t_1 \cdot (1 - c\sigma) = (1 + c\sigma + (c\sigma)^2 + (c\sigma)^3 + (c\sigma)^4)(1 - c\sigma) = 1 - (c\sigma)^5 = 1 - c.$$

  The element t_2 shows a different behaviour. Namely, it is not invertible in the group ring $\mathbb{Q}[\widehat{G}]$. So there does not exist any element $s \in \mathbb{Z}[\widehat{G}]$ such that $s \cdot t$ is multiplication by an integer.

  If we restrict to CL_K^-, the element acting is $-1 + \sigma + \sigma^2 + \sigma^3 + \sigma^4$. It is invertible in $\mathbb{Q}[< \sigma >]$ with inverse $\frac{1}{6}(-2 + \sigma + \sigma^2 + \sigma^3 + \sigma^4)$. So we necessarily get multiplication by 6, which is bad because it seems that one can only control multiplication by powers of 2 on the class group of a CM field.

  Alternatively, one could also consider the diagram

  $$\begin{array}{ccc} \mathrm{CL}_K^- & \xrightarrow{t_2 \cdot} & \mathrm{CL}_K^- \\ \downarrow{\scriptstyle N_{L|K}} & & \downarrow{\scriptstyle N_{L|K}} \\ \mathrm{CL}_L^- & \xrightarrow{\cdot 3} & \mathrm{CL}_L^-, \end{array}$$

  where L is the imaginary quadratic field $K^{<\sigma>}$. Let us recall that we can control the cokernel of the norm map (its size divides the degree of $K|L$). So we get that the image of multiplication by t_2 on CL_K is greater equal one fifth of the size of the image of multiplication by 3 on CL_L.

- $\widehat{G} = \mathbb{Z}/2 \times H =< c > \times H$:
  Here H is an arbitrary finite group. In this case I am unable to make any statement on invertibility of CM elements in $\mathbb{Q}[H]$, so the only thing I seem to have is to imitate the last approach in the previous point.

  In that way one can reduce to multiplication by n on CL_L^- for the imaginary quadratic field K^H. Here n is an integer in the range from $-|H|$ to $|H|$. If the order of H is even, it can happen that the integer is actually 0, and then this approach is, of course, useless.

- $\widehat{G} = \mathbb{Z}/2 \times \mathbb{Z}/2 =< c > \times < \sigma >$:
  That's part (b) of the proposition. The CM elements $t_1 = 1 + \sigma$ and $t_2 = 1 + c\sigma$ are not invertible. It seems that I have to use the previous point.

  So, one reduces to multiplication by 2 on CL_{K^σ} in the first and on $\mathrm{CL}_{K^{c\sigma}}$ in the second case. This gives the claim in (b).

- $\widehat{G} = D_4 =< \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} >$.
We have $c = \sigma^2$ and $K = M^{<\tau>}$. The essentially only CM element is

$$t = 1 + \tau + \sigma^3 + \sigma\tau = (1 + \tau) + \sigma(\sigma^2 + \tau).$$

We consider the commutative diagram

$$\begin{array}{ccccc} \mathrm{CL}_M^- & \xrightarrow{(1+\tau)\cdot} & \mathrm{CL}_M^- & \xrightarrow{t\cdot} & \mathrm{CL}_M^- \\ \downarrow{\scriptstyle N_{M|K}} & & & & \downarrow{\scriptstyle N_{L|K}} \\ \mathrm{CL}_K^- & & \xrightarrow{\cdot 4} & & \mathrm{CL}_K^-. \end{array}$$

The top arrow is

$$((1 + \tau) + \sigma(\sigma^2 + \tau))(1 + \tau) = 2(1 + \tau) + \sigma(1 + \tau + \sigma^2 + \sigma^2\tau) = 2(1 + \tau),$$

where in the last step we used that σ^2 acts as -1 on CL_M^-. The claim in the proposition now follows because τ acts trivially on K and because the size of the cokernel of the norm is bounded by 2.

The arguments used above all seem very much "ad hoc". A conceptual generalisation seems essential for any progress.

We have now reduced to multiplication by 2 resp. 4 on class groups of CM fields. Now we will try to settle this question.

Using class field theory and Galois cohomology (Bas used étale cohomology), it is not difficult to show:

Proposition 3 *Let $K|F$ be a Galois extension of number fields of prime degree p. Let $r_{K|F}$ be the number of finite primes of F that ramify in K. Then*

$$\mathrm{rk}_p\mathrm{CL}_K \leq (p + 1)r_{K|F} + p + p \cdot \mathrm{rk}_p\mathrm{CL}_F.$$

Corollary 1 *(a) There is a $C > 0$ such that for all number fields $L|\mathbb{Q}$ of degree 2:*

$$|\mathrm{Ker}(\mathrm{CL}_L \xrightarrow{\cdot 2} \mathrm{CL}_L)| \leq C \cdot 8^{r_{L|\mathbb{Q}}}.$$

(b) There is a $C > 0$ such that for all number fields $K|\mathbb{Q}$ of degree 4 that have a quadratic subfield:

$$|\mathrm{Ker}(\mathrm{CL}_K \xrightarrow{\cdot 2} \mathrm{CL}_K)| \leq C \cdot 512^{r_{K|\mathbb{Q}}}.$$

Let us first note that the corollary is immediate from the proposition. It seems that one can get better constants than those above (with a different approach).

Now I give a proof of the proposition.

Let S a finite set of primes of F. By F_S^{ur} and F_S^{cs} we mean the maximal extension of F, which is unramified outside S, resp. everywhere unramified and completely split in S.

The S-ideal class group $\mathrm{CL}_S(K)$ can be defined as the abelian group generated by the prime ideals outside S modulo principal ideals.

Using the description above one obtains from class field theory that $\mathrm{CL}_S(K)$ is isomorphic to the Galois group of the maximal unramified abelian extension, which is completely split in S. Hence there is the isomorphism

$$\mathrm{CL}_S(K) \cong G(K_S^{\mathrm{cs}}|K)^{\mathrm{ab}}.$$

We denote by $G_{\mathfrak{p}} \leq G(K_S^{\mathrm{ur}}|K)$ a decomposition group of a prime $\mathfrak{p}$ and note that it is naturally isomorphic to the Galois group of a completion at $\mathfrak{p}$. Let H be the closed normal subgroup of $G(K_S^{\mathrm{ur}}|K)$ generated by the decomposition groups of the primes in S. Then there is the isomorphism $G(K_S^{\mathrm{ur}}|K)/H \cong G(K_S^{\mathrm{cs}}|K)$.

We have equalities

$$(\mathrm{CL}_S(K)/p)^\vee = \mathrm{Hom}(\mathrm{CL}_S(K), \mathbb{F}_p) = \mathrm{Hom}_{\mathrm{cts}}(G(K_S^{\mathrm{cs}}|K), \mathbb{F}_p) = \mathrm{Hom}_{\mathrm{cts}}(G(K_S^{\mathrm{ur}}|K)/H, \mathbb{F}_p),$$

where H is defined as above. They can be rewritten as follows

$$(\mathrm{CL}_S(K)/p)^\vee = \mathrm{sha}_S(K) := \mathrm{Ker}\Big(H^1(G(K_S^{\mathrm{ur}}|K), \mathbb{F}_p) \xrightarrow{\mathrm{res}} \prod_S H^1(G_{\mathfrak{p}}, \mathbb{F}_p) \Big).$$

The group $\mathrm{sha}_S(K)$ is called the *Tate-Shafarevich group*.

From the idelic description one immediately obtains the exact sequence

$$\prod_{\mathfrak{p}\in S, \mathfrak{p}\nmid\infty} K_{\mathfrak{p}}^\times/\mathcal{O}_{K_{\mathfrak{p}}}^\times \to \mathrm{CL}_K \to \mathrm{CL}_S(K) \to 0.$$

Using the exact sequence $0 \to \mathcal{O}_{K_{\mathfrak{p}}}^\times \to K_{\mathfrak{p}}^\times \to \mathbb{Z} \to 0$ induced by the valuation, one gets the inequality

$$\mathrm{rk}_p\mathrm{CL}_K \leq \mathrm{rk}_p\mathrm{CL}_S(K) + \#S,$$

by tensoring the exact sequence above over $\mathbb{Z}$ with $\mathbb{F}_p$.

After these generalities let us now consider our Galois extension $K|F$ of prime degree p. We denote by S the finite set of finite primes of F that ramify in the extension. This choice of S implies that K_S^{ur} equals F_S^{ur}. If we now call $G = G(K_S^{\mathrm{ur}}|F)$ and $H = G(K_S^{\mathrm{ur}}|K)$, then clearly H is an open normal subgroup of G of index p. For simplicity we set $R = G/H$.

We note that the group $R = G/H$ acts trivially on the set S, as there is just one prime of K lying above a ramified prime of F.

From this it follows that we have an exact commutative diagramme

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & A_1 & \longrightarrow & A_2 & \longrightarrow & \prod_S A_{3,\mathfrak{p}} \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{sha}_S(F) & \longrightarrow & \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{F}_p) & \longrightarrow & \prod_S \mathrm{Hom}_{\mathrm{cts}}(G_{\mathfrak{p}}, \mathbb{F}_p) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{sha}_S(K)^R & \longrightarrow & \mathrm{Hom}_{\mathrm{cts}}(H, \mathbb{F}_p)^R & \longrightarrow & \prod_S \mathrm{Hom}_{\mathrm{cts}}(H_{\mathfrak{p}}, \mathbb{F}_p)^R \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & A_4 & \longrightarrow & A_5 & \longrightarrow & \prod_S A_{6,\mathfrak{p}} \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0,
\end{array}$$

in which the A_i are defined as the kernels resp. cokernels of the vertical maps in the centre.

The inflation-restriction sequence shows that $A_2 = A_{3,\mathfrak{p}} = \mathbb{F}_p$ and $A_5, A_{6,\mathfrak{p}} \in \{0, \mathbb{F}_p\}$, from which we see $\dim_p A_1 \leq 1$ and $\dim_p A_4 \leq 1 + \#S$. In conclusion, we get

$$\dim_p \mathrm{sha}_S(K)^R \leq 1 + \#S + \dim_p \mathrm{sha}_S(F) = 1 + \#S + \mathrm{rk}_p \mathrm{CL}_S(F).$$

Lemma 1 *Let $R =< \sigma > \cong \mathbb{Z}/p$ and consider an $\mathbb{F}_p[R]$-module M. Then*

$$\dim_p M \leq p \cdot \dim_p M^R.$$

Proof. Define submodules $M^i := (\sigma - 1)^i M$. Then clearly $M^0 = M$ and $M^p = 0$ as the characteristic is p. There are the exact sequences

$$0 \to (M^i)^R \to M^i \xrightarrow{\sigma - 1} M^{i+1} \to 0,$$

from which the result is immediate. □

Now it suffices to put the inequalities together to conclude the proposition. □

We have thus found upper bounds for the kernel of multiplication by 2, hence also for fixed powers of 2. Now we can proceed to statements on the size of the image.

Theorem 1 (Cor. of Brauer-Siegel) *Fix an integer $d \geq 1$. For all $\epsilon > 0$ there is a $C > 0$ such that for all CM-fields K of degree $2d$ one has*

$$h_K^- \geq C \cdot |d_K/d_{K^+}|^{1/2-\epsilon} \geq C \cdot |d_K|^{1/4-\epsilon}.$$

Corollary 2 *Let d be 1 or 2 and n an integer. For all $0 < \delta < 1/2d$ there exists a $C > 0$ such that for all CM fields $K|\mathbb{Q}$ of degree $2d$ one has*

$$|\mathrm{Im}(\mathrm{CL}_K^- \xrightarrow{\cdot 2^n} \mathrm{CL}_K^-)| \geq C \cdot |d_K|^{\delta}.$$

That follows because for all $\epsilon > 0$ the number

$$512^{r_{K|\mathbb{Q}}}/|d_K|^{\epsilon}$$

goes to 0, as $|d_K|$ tends to ∞.

The corollary of Brauer-Siegel is proved as Lemma 4 in [HH]. In his article [E] Bas Edixhoven used a result by Stark apparently to avoid the use of GRH. With the above corollary it seems that we can also do without invoking GRH.

Let us now put things together.

Proposition 4 *In case $d = 2$, the question SQ is true for any exponent $0 < \delta < 1/4$. If we allow non-primitive CM types, HQ is still true for the same exponents.*

Proof.

- If $\widehat{G} = D_4$ or $\widehat{G} = \mathbb{Z}/4$, it suffices to combine corollary 2 and proposition 2 (a).

  If one restricts to this case, the constants do not depend on K^+.

- If $\widehat{G} = \mathbb{Z}/2 \times \mathbb{Z}/2$, proceeding as above gives

  $$|\mathrm{Im}(\mathrm{CL}_K \xrightarrow{\cdot t} \mathrm{CL}_K)| > C \cdot |d_L|^{1/2-\epsilon}$$

  with $L \subset K$ quadratic imaginary. Now we use

  $$|d_K| \leq |d_{K^+}|^2 \cdot |d_L|^2$$

  and get the result, but also a dependence on K^+. □

We just need to recall that in the case $\widehat{G} = (\mathbb{Z}/2)^2$ there are no non-induced CM types. The rest is immediate from proposition 2 and corollary 2.

On the next slide, I'd like to quickly come back to the question nSQ.

On the question nSQ:

Theorem 2 (Loubotin, Okazaki) *Assume GRH. Fix d. There exists a $C > 0$ such that for all CM fields $K|\mathbb{Q}$ of degree $2d$ the exponent e_K of CL_K satisfies*

$$e_K \geq C \frac{\log |d_K|}{\log \log |d_K|}.$$

This gives the best result on nSQ known to me. Fix some integer n. Then

$$|\mathrm{Im}(\mathrm{CL}_K \xrightarrow{\cdot n} \mathrm{CL}_K)| \geq C \frac{\log |d_K|}{\log \log |d_K|}.$$

Other approaches:

- Bloch-Kato conjecture??
- Cohen-Lenstra heuristics??

The theorem above is [LO], Thm. 1.

If the exponent of an abelian group is e, then we know that there is an element of order e in the group. So the image of multiplication by a fixed n will be a group containing an element of order greater equal e/n.

So assuming GRH one can get logarithmic growth, but one would like (and probably expect) exponential growth. There is thus a big gap.

Recent results by Andrei Yafaev seem to suggest that one can get arbitrary (fixed) powers of the logarithm of the discriminant.

The Bloch-Kato conjecture suggests that the class group ought to decompose into pieces, according to the irreducible representations of the Galois group. It would suffice to obtain a big image on one of the pieces.

Let's now come to an end...

Concluding remarks:

- Fix d. Does nHQ imply HQ for a finite collection of n's?

  I considered the non-trivial central extension

  $$0 \to < c > \to \widehat{A_5} \to A_5 \to 0.$$

  I generated random CM types Φ_K and looked at $t_{\Phi_K} \in \mathbb{Q}[\widehat{A_5}]/(c+1)$. Every such t_{Φ_K} was invertible! So image of multiplication by t is greater equal the image of multiplication by n, some n.

- I mostly took a group theoretic point of view (computations in the group ring). More number theoretically?

It seems that good ideas are necessary!

I have quickly tried to prove that one cannot always reduce to multiplication by an integer. To my surprise I obtained the result stated on the slide.

If we take non-simple groups, actually any one of those discussed in this talk will do, one finds non-invertible CM elements. But we were always able to conclude by passing to CM subfields, which I want to exclude (at least normal ones).

Let's finish this talk by reading aloud, everyone for himself, the last line on the slide.

References

[E] Edixhoven, S. J.: *On the André-Oort conjecture for Hilbert modular surfaces*, Moduli of abelian varieties (Texel Island, 1999), 133-155, Progr. Math. **195**, Birkhäuser, 2001.

[EMO] Edixhoven, S. J., Moonen, B. J. J., Oort, F.: *Open problems in algebraic geometry*, Bull. Sci. math. **125**, 1 (2001), 1-22

[HH] Horie, M., Horie, M.: *CM-fields and exponents of their ideal class groups*, Acta arithmetica **55** (1990), 157-170

[LO] Louboutin, S., Okazaki, R.: *Exponents of the ideal class groups of CM number fields,* Mathematische Zeitschrift **243** (2003), 155-159

[Wa] Washington, L. C.: *Introduction to Cyclotomic Fields*, GTM 83, Springer-Verlag