Smith explained part II

Peter Koymans
Max Planck Institute for Mathematics

MAX-PLANCK-GESELLSCHAFT

Informal Seminar

22 October 2020

The Cohen-Lenstra heuristics

Let p be an odd prime and K be a quadratic field. The group $\mathrm{Cl}(K)[p^\infty]$ is believed to behave as a random finite, abelian p-group.

The Cohen-Lenstra heuristics

Let p be an odd prime and K be a quadratic field. The group $\mathrm{Cl}(K)[p^\infty]$ is believed to behave as a random finite, abelian p-group.

More formally, Cohen and Lenstra conjectured that

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X \text{ and } \mathrm{Cl}(K)[p^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1 - \frac{1}{p^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian p-group A.

The Cohen-Lenstra heuristics

Let p be an odd prime and K be a quadratic field. The group $\mathrm{Cl}(K)[p^\infty]$ is believed to behave as a random finite, abelian p-group.

More formally, Cohen and Lenstra conjectured that

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X \text{ and } \mathrm{Cl}(K)[p^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{p^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian p-group A.

For real quadratic fields

$$\lim_{X\to\infty} \frac{|\{K \text{ re. quadr.} : |D_K| < X \text{ and } \mathrm{Cl}(K)[p^\infty] \cong A\}|}{|\{K \text{ re. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=2}^{\infty}\left(1-\frac{1}{p^i}\right)}{|A||\mathrm{Aut}(A)|},$$

where $\mathrm{Cl}(K)[p^\infty]$ is now the quotient of a random abelian group.

Genus theory

Why is $p = 2$ excluded from the Cohen–Lenstra heuristics?

Genus theory

Why is $p = 2$ excluded from the Cohen–Lenstra heuristics?

The group $\mathrm{Cl}(K)[2]$ has a predictable behavior unlike $\mathrm{Cl}(K)[p]$ for p odd.

Genus theory

Why is $p = 2$ excluded from the Cohen–Lenstra heuristics?

The group $\mathrm{Cl}(K)[2]$ has a predictable behavior unlike $\mathrm{Cl}(K)[p]$ for p odd.

The description of $\mathrm{Cl}(K)[2]$ is due to Gauss and is known as genus theory. We have that

$$|\mathrm{Cl}(K)[2]| = 2^{\omega(D_K)-1}$$

and $\mathrm{Cl}(K)[2]$ is generated by the ramified prime ideals of $\mathcal{O}_K$.

Genus theory

Why is $p = 2$ excluded from the Cohen–Lenstra heuristics?

The group $\mathrm{Cl}(K)[2]$ has a predictable behavior unlike $\mathrm{Cl}(K)[p]$ for p odd.

The description of $\mathrm{Cl}(K)[2]$ is due to Gauss and is known as genus theory. We have that

$$|\mathrm{Cl}(K)[2]| = 2^{\omega(D_K)-1}$$

and $\mathrm{Cl}(K)[2]$ is generated by the ramified prime ideals of $\mathcal{O}_K$.

Indeed, if p divides the discriminant of $\mathbb{Q}(\sqrt{d})$, then p ramifies, so

$$\begin{array}{ccccc} \mathbb{Q}(\sqrt{d}) & \quad & \mathfrak{p} & \quad & \mathfrak{p}^2 = (p). \\ | & & | & & \\ \mathbb{Q} & & p & & \end{array}$$

There is precisely one relation between the ramified primes.

Gerth's modification

Instead of $\mathrm{Cl}(K)[2^\infty]$, it is the group $2\mathrm{Cl}(K)[2^\infty]$ that behaves randomly.

Gerth's modification

Instead of $\mathrm{Cl}(K)[2^\infty]$, it is the group $2\mathrm{Cl}(K)[2^\infty]$ that behaves randomly.

To be precise, Gerth conjectured the following

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{2^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian 2-group A, and similarly for real quadratics.

Gerth's modification

Instead of $\mathrm{Cl}(K)[2^\infty]$, it is the group $2\mathrm{Cl}(K)[2^\infty]$ that behaves randomly.

To be precise, Gerth conjectured the following

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{2^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian 2-group A, and similarly for real quadratics.

Fouvry and Klüners dealt with the distribution of $2\mathrm{Cl}(K)[4]$.

Gerth's modification

Instead of $\mathrm{Cl}(K)[2^\infty]$, it is the group $2\mathrm{Cl}(K)[2^\infty]$ that behaves randomly.

To be precise, Gerth conjectured the following

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1 - \frac{1}{2^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian 2-group A, and similarly for real quadratics.

Fouvry and Klüners dealt with the distribution of $2\mathrm{Cl}(K)[4]$.

Theorem 1 (Smith, 2017)

Gerth's conjecture is true.

The dual class group

Theorem 2 (Class field theory)

We have an isomorphism

$$\mathrm{Cl}(K) \cong \mathrm{Gal}(H(K)/K)$$

given by sending a prime ideal $\mathfrak{p}$ *to* $\mathrm{Art}(\mathfrak{p})$. *Furthermore, if* K *is Galois, this isomorphism respects the natural Galois action of* $\mathrm{Gal}(K/\mathbb{Q})$.

The dual class group

Theorem 2 (Class field theory)

We have an isomorphism

$$\mathrm{Cl}(K) \cong \mathrm{Gal}(H(K)/K)$$

given by sending a prime ideal $\mathfrak{p}$ *to* $\mathrm{Art}(\mathfrak{p})$*. Furthermore, if* K *is Galois, this isomorphism respects the natural Galois action of* $\mathrm{Gal}(K/\mathbb{Q})$*.*

From this we get a bijection

$$\mathrm{Cl}^{\vee}(K)[2] \leftrightarrow \{\text{quadratic unramified extensions of } K\}.$$

The dual class group

Theorem 2 (Class field theory)

We have an isomorphism

$$\mathrm{Cl}(K) \cong \mathrm{Gal}(H(K)/K)$$

given by sending a prime ideal $\mathfrak{p}$ *to* $\mathrm{Art}(\mathfrak{p})$*. Furthermore, if* K *is Galois, this isomorphism respects the natural Galois action of* $\mathrm{Gal}(K/\mathbb{Q})$*.*

From this we get a bijection

$$\mathrm{Cl}^{\vee}(K)[2] \leftrightarrow \{\text{quadratic unramified extensions of } K\}.$$

Indeed,

$$\mathrm{Cl}^{\vee}(K)[2] = \mathrm{Hom}(\mathrm{Cl}(K), \mathbb{C}^*)[2] \cong \mathrm{Hom}(\mathrm{Gal}(H(K)/K), \{\pm 1\}).$$

Given $\chi \in \mathrm{Hom}(\mathrm{Gal}(H(K)/K), \{\pm 1\})$, look at $H(K)^{\ker(\chi)}$. The quadratic unramified characters are generated by χ_p with p dividing d.

The Artin pairing

Let A be a finite abelian 2-group. We have a natural pairing

$$\mathrm{Art}_m : 2^{m-1}A[2^m] \times 2^{m-1}A^\vee[2^m] \to \mathbb{F}_2$$

given by sending (a, χ) to $\psi(a)$, where ψ satisfies $2^{m-1}\psi = \chi$.

The Artin pairing

Let A be a finite abelian 2-group. We have a natural pairing

$$\mathrm{Art}_m : 2^{m-1}A[2^m] \times 2^{m-1}A^\vee[2^m] \to \mathbb{F}_2$$

given by sending (a, χ) to $\psi(a)$, where ψ satisfies $2^{m-1}\psi = \chi$.

Duality of finite abelian groups implies that the left kernel is $2^m A[2^{m+1}]$ and the right kernel is $2^m A^\vee[2^{m+1}]$.

The Artin pairing

Let A be a finite abelian 2-group. We have a natural pairing

$$\mathrm{Art}_m : 2^{m-1}A[2^m] \times 2^{m-1}A^\vee[2^m] \to \mathbb{F}_2$$

given by sending (a, χ) to $\psi(a)$, where ψ satisfies $2^{m-1}\psi = \chi$.

Duality of finite abelian groups implies that the left kernel is $2^m A[2^{m+1}]$ and the right kernel is $2^m A^\vee[2^{m+1}]$.

For $A = \mathrm{Cl}(K)$, we have that $A^\vee \cong \mathrm{Hom}(\mathrm{Gal}(H(K)/K), \mathbb{Q}/\mathbb{Z})$. Then the Artin pairing becomes

$$\mathrm{Art}_{m,K} : (\mathfrak{p}, \chi) \mapsto \psi(\mathrm{Frob}_{\mathfrak{p}}).$$

Smith essentially proves that the Artin pairing is random. This implies Cohen–Lenstra.

Random Artin pairings

What does it mean that the Artin pairing is random? How does one compare Artin pairings?

Random Artin pairings

What does it mean that the Artin pairing is random? How does one compare Artin pairings?

Take an integer d and let $p_1, \ldots, p_r$ be its prime divisors ordered by size. Then we have natural surjective maps

$$\mathbb{F}_2^r \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2], \quad \mathbb{F}_2^r \to \mathrm{Cl}^\vee(\mathbb{Q}(\sqrt{d}))[2].$$

This allows us to compare various Artin pairings if we fix the number of prime divisors r.

Random Artin pairings

What does it mean that the Artin pairing is random? How does one compare Artin pairings?

Take an integer d and let $p_1, \ldots, p_r$ be its prime divisors ordered by size. Then we have natural surjective maps

$$\mathbb{F}_2^r \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2], \quad \mathbb{F}_2^r \to \mathrm{Cl}^\vee(\mathbb{Q}(\sqrt{d}))[2].$$

This allows us to compare various Artin pairings if we fix the number of prime divisors r.

If d is negative, then $(1, \ldots, 1)$ is in the kernel of both maps. For d positive, this is no longer true!

Random Artin pairings

What does it mean that the Artin pairing is random? How does one compare Artin pairings?

Take an integer d and let $p_1, \ldots, p_r$ be its prime divisors ordered by size. Then we have natural surjective maps

$$\mathbb{F}_2^r \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2], \quad \mathbb{F}_2^r \to \mathrm{Cl}^\vee(\mathbb{Q}(\sqrt{d}))[2].$$

This allows us to compare various Artin pairings if we fix the number of prime divisors r.

If d is negative, then $(1, \ldots, 1)$ is in the kernel of both maps. For d positive, this is no longer true!

Real quadratic: random $N + 1$ by N matrices.
Imaginary quadratic: random N by N matrices.

The first Artin pairing

In matrix form Art_1 becomes

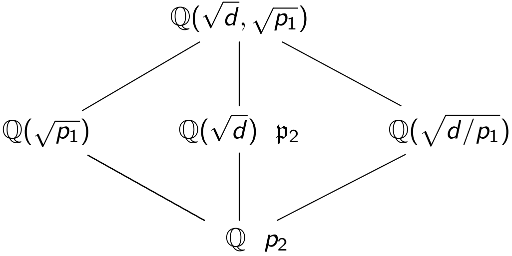
$$\begin{array}{ccccc} & \chi_{p_1} & \chi_{p_2} & \cdots & \chi_{p_r} \\ p_1 & * & \left(\frac{p_2}{p_1}\right) & \cdots & \left(\frac{p_r}{p_1}\right) \\ p_2 & \left(\frac{p_1}{p_2}\right) & * & \cdots & \left(\frac{p_r}{p_2}\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_r & \left(\frac{p_1}{p_r}\right) & \left(\frac{p_2}{p_r}\right) & \cdots & * \end{array}.$$

The first Artin pairing

In matrix form Art_1 becomes

$$\begin{array}{c|cccc} & \chi_{p_1} & \chi_{p_2} & \cdots & \chi_{p_r} \\ p_1 & * & \left(\frac{p_2}{p_1}\right) & \cdots & \left(\frac{p_r}{p_1}\right) \\ p_2 & \left(\frac{p_1}{p_2}\right) & * & \cdots & \left(\frac{p_r}{p_2}\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_r & \left(\frac{p_1}{p_r}\right) & \left(\frac{p_2}{p_r}\right) & \cdots & * \end{array}.$$

Indeed,



Prime divisors part I

This is an entirely analytic problem. To tackle this problem, our first aim is to gain a deeper understanding of the typical structure of the prime divisors of an integer.

Prime divisors part I

This is an entirely analytic problem. To tackle this problem, our first aim is to gain a deeper understanding of the typical structure of the prime divisors of an integer.

An integer n has typically $\log \log n$ prime divisors. More precisely, the set of integers n such that

$$|\omega(n) - \log \log n| > (\log \log n)^{2/3}$$

has density zero.

Prime divisors part I

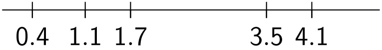
This is an entirely analytic problem. To tackle this problem, our first aim is to gain a deeper understanding of the typical structure of the prime divisors of an integer.

An integer n has typically $\log\log n$ prime divisors. More precisely, the set of integers n such that

$$|\omega(n) - \log\log n| > (\log\log n)^{2/3}$$

has density zero.

A good heuristic model is that $\log\log p_i$ is roughly equal to i.



Prime divisors part II

Hence to prove equidistribution of Art_1, restrict to integers n with $\omega(n) = r$, where

$$|r - \log\log n| \leq (\log\log n)^{2/3}.$$

Prime divisors part II

Hence to prove equidistribution of Art_1, restrict to integers n with $\omega(n) = r$, where

$$|r - \log\log n| \leq (\log\log n)^{2/3}.$$

We can cover the set of squarefree integers up to N with r prime divisors with product sets of the shape

$$X := X_1 \times \cdots \times X_r$$

where the X_i are suitable, disjoint intervals of primes. We view an element $x \in (x_1, \ldots, x_r)$ as a squarefree integer by multiplying out its coordinates.

Prime divisors part II

Hence to prove equidistribution of Art_1, restrict to integers n with $\omega(n) = r$, where

$$|r - \log\log n| \leq (\log\log n)^{2/3}.$$

We can cover the set of squarefree integers up to N with r prime divisors with product sets of the shape

$$X := X_1 \times \cdots \times X_r$$

where the X_i are suitable, disjoint intervals of primes. We view an element $x \in (x_1, \dots, x_r)$ as a squarefree integer by multiplying out its coordinates.

For this to work out, we need that most integers n satisfy

$$\log p_{i+1} - \log p_i \geq 1 \text{ for all } i.$$

We also need to shrink the intervals at the end.

Prime divisors part III

These boxes X are extremely useful. It will be the most natural way to set up our algebraic results later for the higher Artin pairings, while it also helps with analytic questions (allowing for inductive arguments).

Prime divisors part III

These boxes X are extremely useful. It will be the most natural way to set up our algebraic results later for the higher Artin pairings, while it also helps with analytic questions (allowing for inductive arguments).

Smith shows that a typical integer is regularly spaced, i.e.

$$|\log\log p_i - i| \leq (\log\log\log N)^{1/5} \max(i, \log\log\log N)^{4/5}$$

for all $i \leq r/3$.

Prime divisors part III

These boxes X are extremely useful. It will be the most natural way to set up our algebraic results later for the higher Artin pairings, while it also helps with analytic questions (allowing for inductive arguments).

Smith shows that a typical integer is regularly spaced, i.e.

$$|\log\log p_i - i| \leq (\log\log\log N)^{1/5} \max(i, \log\log\log N)^{4/5}$$

for all $i \leq r/3$.

Smith also shows that there is typically at least one big gap, i.e.

$$\log p_i > \log\log p_i \cdot \left(\sum_{j=1}^{i-1} \log p_j\right)$$

for some $i \in (0.5r^{1/4}, 0.5r^{1/2})$. It is then easy to show that this is also true for boxes (except for a negligible amount).

Equidistribution of the first Artin pairing

We now need to deal with nice boxes X. Suppose that k_{gap} is the index where the huge gap occurs.

Equidistribution of the first Artin pairing

We now need to deal with nice boxes X. Suppose that k_{gap} is the index where the huge gap occurs.

Pick any elements $x_1, \ldots, x_{k_{\text{gap}}}$ in $X_1, \ldots, X_{k_{\text{gap}}}$ respectively. For the X_i with $i > k_{\text{gap}}$ now apply Chebotarev with respect to the field obtained by adjoining the square roots of the x_i.

Equidistribution of the first Artin pairing

We now need to deal with nice boxes X. Suppose that k_{gap} is the index where the huge gap occurs.

Pick any elements $x_1, \ldots, x_{k_{\text{gap}}}$ in $X_1, \ldots, X_{k_{\text{gap}}}$ respectively. For the X_i with $i > k_{\text{gap}}$ now apply Chebotarev with respect to the field obtained by adjoining the square roots of the x_i.

By the regular spacing the remaining primes are of decent size and we can apply the large sieve.

Equidistribution of the first Artin pairing

We now need to deal with nice boxes X. Suppose that k_{gap} is the index where the huge gap occurs.

Pick any elements $x_1, \ldots, x_{k_{\text{gap}}}$ in $X_1, \ldots, X_{k_{\text{gap}}}$ respectively. For the X_i with $i > k_{\text{gap}}$ now apply Chebotarev with respect to the field obtained by adjoining the square roots of the x_i.

By the regular spacing the remaining primes are of decent size and we can apply the large sieve.

	χ_{p_1}	χ_{p_2}	χ_{p_3}
p_1	?	Cheb	Cheb
p_2	Cheb	LarSie	LarSie
p_3	Cheb	LarSie	LarSie

This information is enough to recover for example the rank distribution as r goes to infinity, since there is only a ? in at most the top $0.5\sqrt{r}$ part of the matrix.

Recap: the Artin pairing

If A is a finite, abelian 2-group, we have a pairing

$$\mathrm{Art}_m : 2^{m-1}A[2^m] \times 2^{m-1}A^\vee[2^m] \to \mathbb{F}_2$$

given by sending (a, χ) to $\psi(a)$, where ψ satisfies $2^{m-1}\psi = \chi$.

Recap: the Artin pairing

If A is a finite, abelian 2-group, we have a pairing

$$\mathrm{Art}_m : 2^{m-1}A[2^m] \times 2^{m-1}A^\vee[2^m] \to \mathbb{F}_2$$

given by sending (a, χ) to $\psi(a)$, where ψ satisfies $2^{m-1}\psi = \chi$.

Duality of finite abelian groups implies that the left kernel is $2^m A[2^{m+1}]$ and the right kernel is $2^m A^\vee[2^{m+1}]$.

Recap: the Artin pairing

If A is a finite, abelian 2-group, we have a pairing

$$\mathrm{Art}_m : 2^{m-1}A[2^m] \times 2^{m-1}A^\vee[2^m] \to \mathbb{F}_2$$

given by sending (a, χ) to $\psi(a)$, where ψ satisfies $2^{m-1}\psi = \chi$.

Duality of finite abelian groups implies that the left kernel is $2^m A[2^{m+1}]$ and the right kernel is $2^m A^\vee[2^{m+1}]$.

For $A = \mathrm{Cl}(K)$, we have that $A^\vee \cong \mathrm{Hom}(\mathrm{Gal}(H(K)/K), \mathbb{Q}/\mathbb{Z})$. Then the Artin pairing becomes

$$\mathrm{Art}_{m,K} : (\mathfrak{p}, \chi) \mapsto \psi(\mathrm{Frob}_{\mathfrak{p}}).$$

Recap II: comparing Artin pairings

By genus theory we have a natural surjective map $\mathbb{F}_2^r \to \mathrm{Cl}(K)[2]$ and $\mathbb{F}_2^r \to \mathrm{Cl}^\vee(K)[2]$, where $r = \omega(\Delta_K)$.

Recap II: comparing Artin pairings

By genus theory we have a natural surjective map $\mathbb{F}_2^r \to \mathrm{Cl}(K)[2]$ and $\mathbb{F}_2^r \to \mathrm{Cl}^\vee(K)[2]$, where $r = \omega(\Delta_K)$.

Pulling back $\mathrm{Art}_{m,K}$ then induces a pairing $\mathbb{F}_2^r \times \mathbb{F}_2^r \to \mathbb{F}_2$. Concretely, if $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are the ramified prime ideals ordered by norm, then we are keeping track of the set of $(e_1, \dots, e_r) \in \mathbb{F}_2^r$ such that

$$\mathfrak{p}_1^{e_1} \cdot \dots \cdot \mathfrak{p}_r^{e_r} \in 2^m \mathrm{Cl}(K)[2^{m+1}]$$

for all $m \geq 1$.

Recap II: comparing Artin pairings

By genus theory we have a natural surjective map $\mathbb{F}_2^r \to \mathrm{Cl}(K)[2]$ and $\mathbb{F}_2^r \to \mathrm{Cl}^\vee(K)[2]$, where $r = \omega(\Delta_K)$.

Pulling back $\mathrm{Art}_{m,K}$ then induces a pairing $\mathbb{F}_2^r \times \mathbb{F}_2^r \to \mathbb{F}_2$. Concretely, if $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are the ramified prime ideals ordered by norm, then we are keeping track of the set of $(e_1, \dots, e_r) \in \mathbb{F}_2^r$ such that

$$\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r} \in 2^m \mathrm{Cl}(K)[2^{m+1}]$$

for all $m \geq 1$.

Similarly, if $\chi_{p_1}, \dots, \chi_{p_r}$ are the unramified characters, then we bookkeep the set of $(e_1, \dots, e_r) \in \mathbb{F}_2^r$ with

$$e_1 \chi_{p_1} + \cdots + e_r \chi_{p_r} \in 2^m \mathrm{Cl}^\vee(K)[2^{m+1}].$$

Higher Artin pairings

The key idea for the higher Artin pairings is to use *reflection principles*.

Higher Artin pairings

The key idea for the higher Artin pairings is to use *reflection principles*.

In the literature there are many known results that compare different class groups. For example, we have

$$\dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) \leq \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{-3d})) \leq 1 + \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})),$$

which is known as Scholz's reflection principle.

Higher Artin pairings

The key idea for the higher Artin pairings is to use *reflection principles*.

In the literature there are many known results that compare different class groups. For example, we have

$$\dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) \leq \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{-3d})) \leq 1 + \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})),$$

which is known as Scholz's reflection principle.

The main algebraic result in Smith's work is in fact a reflection principle that compares the 2^m-torsion of 2^m quadratic fields.

Higher Artin pairings

The key idea for the higher Artin pairings is to use *reflection principles*.

In the literature there are many known results that compare different class groups. For example, we have

$$\dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) \leq \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{-3d})) \leq 1 + \dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{d})),$$

which is known as Scholz's reflection principle.

The main algebraic result in Smith's work is in fact a reflection principle that compares the 2^m-torsion of 2^m quadratic fields.

How can we find such reflection principles?

Reflection principles for the second Artin pairing

Suppose that we have four fields

$$\{p, p'\} \times \{q, q'\} \times \{d\}$$

such that χ_a is a double in the dual class group (with $a \mid d$), i.e. in the right kernel of the various Art_1.

Reflection principles for the second Artin pairing

Suppose that we have four fields

$$\{p, p'\} \times \{q, q'\} \times \{d\}$$

such that χ_a is a double in the dual class group (with $a \mid d$), i.e. in the right kernel of the various Art_1.

Inspecting Art_1, we see that χ_a is a double in $\mathrm{Cl}^\vee(\mathbb{Q}(\sqrt{m}))$ if and only if

$$x^2 = ay^2 + \frac{m}{a}z^2$$

is non-trivially soluble over $\mathbb{Q}$.

Reflection principles for the second Artin pairing

Suppose that we have four fields

$$\{p, p'\} \times \{q, q'\} \times \{d\}$$

such that χ_a is a double in the dual class group (with $a \mid d$), i.e. in the right kernel of the various Art_1.

Inspecting Art_1, we see that χ_a is a double in $\mathrm{Cl}^\vee(\mathbb{Q}(\sqrt{m}))$ if and only if

$$x^2 = ay^2 + \frac{m}{a} z^2$$

is non-trivially soluble over $\mathbb{Q}$.

To make a cyclic degree 4 unramified extension of $\mathbb{Q}(\sqrt{m})$ containing $\mathbb{Q}(\sqrt{a})$, one needs to pick a primitive point on the above equation and adjoin the square root of $x + y\sqrt{a}$.

Reflection principles for the second Artin pairing

Suppose that we have four fields

$$\{p, p'\} \times \{q, q'\} \times \{d\}$$

such that χ_a is a double in the dual class group (with $a \mid d$), i.e. in the right kernel of the various Art_1.

Inspecting Art_1, we see that χ_a is a double in $\mathrm{Cl}^\vee(\mathbb{Q}(\sqrt{m}))$ if and only if

$$x^2 = ay^2 + \frac{m}{a} z^2$$

is non-trivially soluble over $\mathbb{Q}$.

To make a cyclic degree 4 unramified extension of $\mathbb{Q}(\sqrt{m})$ containing $\mathbb{Q}(\sqrt{a})$, one needs to pick a primitive point on the above equation and adjoin the square root of $x + y\sqrt{a}$.

This is a Galois extension of $\mathbb{Q}$ (in fact a D_4).

A small compositum

But from the equations

$$x^2 - ay^2 = \frac{dpq}{a}z^2, \quad x^2 - ay^2 = \frac{dpq'}{a}z^2, \quad x^2 - ay^2 = \frac{dp'q}{a}z^2$$

we get a solution to

$$x^2 - ay^2 = \frac{dp'q'}{a}z^2.$$

A small compositum

But from the equations

$$x^2 - ay^2 = \frac{dpq}{a}z^2, \quad x^2 - ay^2 = \frac{dpq'}{a}z^2, \quad x^2 - ay^2 = \frac{dp'q}{a}z^2$$

we get a solution to

$$x^2 - ay^2 = \frac{dp'q'}{a}z^2.$$

Concretely, a part of the Hilbert class field of $\mathbb{Q}(\sqrt{dp'q'})$ is already inside the compositum of the Hilbert class fields of $\mathbb{Q}(\sqrt{dpq})$, $\mathbb{Q}(\sqrt{dpq'})$ and $\mathbb{Q}(\sqrt{dp'q})$.

A small compositum

But from the equations

$$x^2 - ay^2 = \frac{dpq}{a} z^2, \quad x^2 - ay^2 = \frac{dpq'}{a} z^2, \quad x^2 - ay^2 = \frac{dp'q}{a} z^2$$

we get a solution to

$$x^2 - ay^2 = \frac{dp'q'}{a} z^2.$$

Concretely, a part of the Hilbert class field of $\mathbb{Q}(\sqrt{dp'q'})$ is already inside the compositum of the Hilbert class fields of $\mathbb{Q}(\sqrt{dpq})$, $\mathbb{Q}(\sqrt{dpq'})$ and $\mathbb{Q}(\sqrt{dp'q})$.

This implies for $b \mid d$ a common 4-rank ideal

$$\mathrm{Art}_{2,dpq}(\chi_a, b) + \mathrm{Art}_{2,dpq'}(\chi_a, b) + \mathrm{Art}_{2,dp'q}(\chi_a, b) + \mathrm{Art}_{2,dp'q'}(\chi_a, b) = 0.$$

Rephrasing in terms of cocycles

To generalize this, it turns out to be convenient to work with cocycles.

Rephrasing in terms of cocycles

To generalize this, it turns out to be convenient to work with cocycles.

We define $N = \mathbb{Q}_2/\mathbb{Z}_2$ with trivial $G_{\mathbb{Q}}$ action and the discrete topology.

Rephrasing in terms of cocycles

To generalize this, it turns out to be convenient to work with cocycles.

We define $N = \mathbb{Q}_2/\mathbb{Z}_2$ with trivial $G_\mathbb{Q}$ action and the discrete topology.

For a character $\chi : G_\mathbb{Q} \to \{\pm 1\}$ we define the twist $N(\chi)$ by $\sigma *_\chi n = \chi(\sigma) \cdot n$.

Rephrasing in terms of cocycles

To generalize this, it turns out to be convenient to work with cocycles.

We define $N = \mathbb{Q}_2/\mathbb{Z}_2$ with trivial $G_{\mathbb{Q}}$ action and the discrete topology.

For a character $\chi : G_{\mathbb{Q}} \to \{\pm 1\}$ we define the twist $N(\chi)$ by $\sigma *_\chi n = \chi(\sigma) \cdot n$.

We have a split exact sequence

$$0 \to \mathrm{Cocy}(\mathrm{Gal}(K/\mathbb{Q}), N(\chi))[2^k] \to \mathrm{Cocy}(\mathrm{Cl}(K) \rtimes \mathrm{Gal}(K/\mathbb{Q}), N(\chi))[2^k] \to \mathrm{Cl}(K)^\vee[2^k] \to 0,$$

where χ is the character corresponding to $\mathrm{Gal}(K/\mathbb{Q})$. Also note that $\mathrm{Cl}(K) \rtimes \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(H(K)/\mathbb{Q})$.

Rephrasing in terms of cocycles

To generalize this, it turns out to be convenient to work with cocycles.

We define $N = \mathbb{Q}_2/\mathbb{Z}_2$ with trivial $G_\mathbb{Q}$ action and the discrete topology.

For a character $\chi : G_\mathbb{Q} \to \{\pm 1\}$ we define the twist $N(\chi)$ by $\sigma *_\chi n = \chi(\sigma) \cdot n$.

We have a split exact sequence

$$0 \to \mathrm{Cocy}(\mathrm{Gal}(K/\mathbb{Q}), N(\chi))[2^k] \to \mathrm{Cocy}(\mathrm{Cl}(K) \rtimes \mathrm{Gal}(K/\mathbb{Q}), N(\chi))[2^k] \to \mathrm{Cl}(K)^\vee[2^k] \to 0,$$

where χ is the character corresponding to $\mathrm{Gal}(K/\mathbb{Q})$. Also note that $\mathrm{Cl}(K) \rtimes \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(H(K)/\mathbb{Q})$.

In simple words, we can lift dual class group elements to cocycles of $\mathrm{Gal}(H(K)/\mathbb{Q})$ valued in $N(\chi)$ (with an easily described kernel).

Cocycles surject to class group

On this slide we will prove that

$$\mathrm{Cocy}(\mathrm{Cl}(K) \rtimes \mathrm{Gal}(K/\mathbb{Q}), N(\chi))[2^k] \to \mathrm{Cl}(K)^\vee[2^k] \to 0.$$

Cocycles surject to class group

On this slide we will prove that

$$\mathrm{Cocy}(\mathrm{Cl}(K) \rtimes \mathrm{Gal}(K/\mathbb{Q}), N(\chi))[2^k] \to \mathrm{Cl}(K)^\vee[2^k] \to 0.$$

Take $\psi \in \mathrm{Cl}(K)^\vee[2^k] = \mathrm{Hom}(\mathrm{Cl}(K), N[2^k])$. Denote by σ a lift of the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$. Then a direct computation shows that $\sigma^2 = \mathrm{id}$.

Cocycles surject to class group

On this slide we will prove that

$$\mathrm{Cocy}(\mathrm{Cl}(K) \rtimes \mathrm{Gal}(K/\mathbb{Q}), N(\chi))[2^k] \to \mathrm{Cl}(K)^\vee[2^k] \to 0.$$

Take $\psi \in \mathrm{Cl}(K)^\vee[2^k] = \mathrm{Hom}(\mathrm{Cl}(K), N[2^k])$. Denote by σ a lift of the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$. Then a direct computation shows that $\sigma^2 = \mathrm{id}$.

We claim that we can send σ to any element of $N(\chi)[2^k]$ and this uniquely defines our cocycle lift $\widetilde{\psi}$. The cocycle rule forces

$$0 = \widetilde{\psi}(\sigma^2) \overset{\text{cocycle rule}}{=} \sigma * \widetilde{\psi}(\sigma) + \widetilde{\psi}(\sigma) = -\widetilde{\psi}(\sigma) + \widetilde{\psi}(\sigma) = 0,$$

since $\chi(\sigma) = -1$, so no conditions as claimed. Now check that this extends to a cocycle.

A common space

But now we can view our cocycles as elements in

$$\mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi)) \subseteq \mathrm{Map}(G_{\mathbb{Q}}, N),$$

so that everything lives in a common space.

A common space

But now we can view our cocycles as elements in

$$\mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi)) \subseteq \mathrm{Map}(G_{\mathbb{Q}}, N),$$

so that everything lives in a common space.

Now take elements $\mathrm{Cocy}(\mathrm{Gal}(H_K/\mathbb{Q}), N(\chi))[2^k]$ with $2\psi_K = \chi_a$.

A common space

But now we can view our cocycles as elements in

$$\mathrm{Cocy}(G_{\mathbb{Q}}, N(\chi)) \subseteq \mathrm{Map}(G_{\mathbb{Q}}, N),$$

so that everything lives in a common space.

Now take elements $\mathrm{Cocy}(\mathrm{Gal}(H_K/\mathbb{Q}), N(\chi))[2^k]$ with $2\psi_K = \chi_a$.

Look at

$$\begin{aligned} d\psi_{dpq}(\sigma, \tau) &:= \psi_{dpq}(\sigma\tau) - \psi_{dpq}(\sigma) - \psi_{dpq}(\tau) \\ &= \chi_{dpq}(\sigma) * \psi_{dpq}(\tau) - \psi_{dpq}(\tau) \\ &= (\chi_{dpq}(\sigma) - 1) \cdot \psi_{dpq}(\tau) \\ &= \iota(\chi_{dpq}(\sigma)) \cdot \chi_a(\tau), \end{aligned}$$

where $\iota : \{\pm 1\} \to \mathbb{F}_2$.

A small compositum: a cocycle perspective

We have

$$d\left(\psi_{dpq}+\psi_{dp'q}+\psi_{dpq'}+\psi_{dp'q'}\right)(\sigma,\tau)= \iota(\chi_{dpq}(\sigma)\cdot\chi_{dp'q}(\sigma)\cdot\chi_{dpq'}(\sigma)\cdot\chi_{dp'q'}(\sigma))\cdot\chi_a=0,$$

which recovers our previous computation.