Math 254 – Number Theory 2

Lectures by Joe Silverman
Notes by Zev Chonoles

Brown University, Spring 2011

Introduction

Math 254 is one of the courses offered for mathematics graduate students at Brown University. It is the second of two courses in the year-long number theory sequence. I took these notes while taking the course as a junior.

The notes are handwritten because this was before I started live-TeXing. I may eventually get around to typing these notes properly.

I am responsible for all faults in this document, mathematical or otherwise; any merits of the material here should be credited to the lecturer, not to me.

Please email any corrections or suggestions to chonoles@math.uchicago.edu.

Lecture 1 (2011-01-26)

2011-1-26 (1)

Topics
- Class field theory < Global, Local
- Group Cohomology (especially Galois cohomology)
- Elliptic Curves < Mordell-Weil theorem, CM

References: see web page
in particular Lang Algebraic Number Theory
Serre Local fields

No class April 27, 29, May 2, so make-up class during reading period, May 4, 6, 9

Class Field Theory

Study of abelian extensions L/K - describe them in terms of the arithmetic of K

Example: Kronecker-Weber theorem
Let $L/\mathbb{Q}$ be an abelian extension. Then
$L \subset \mathbb{Q}(\mu_N)$ for some N ($\mu_N = \{\text{roots of } x^N - 1\}$)

Review of Algebraic Number Theory (global)

$K/\mathbb{Q}$ a number field, $\mathcal{O}_K$ its ring of integers

Prop. $\mathcal{O}_K$ is a Dedekind domain

hence ideals have unique factorization

Given an ideal $\mathfrak{a} \subset \mathcal{O}_K$, $\mathfrak{a} = \prod \mathfrak{p}^{e_\mathfrak{p}}$

$e_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(\mathfrak{a}) = v_\mathfrak{p}(\mathfrak{a})$

$I_K = \{\text{fractional ideals}\} = \{\text{finitely generated } \mathcal{O}_K\text{-modules (whose } K\text{-span is } K) \text{ of } K\}$

(fractional ideals: implicitly non-zero)

$\mathfrak{a}^{-1} = \{x \in K^\times \mid x\mathfrak{a} \subset \mathcal{O}_K\}$

I_K is a group

$P_K = \{\text{principal fractional ideals}\} = \{a\mathcal{O}_K \mid a \in K^\times\}$

$C_K = I_K / P_K$ = ideal class group of K

Thm. C_K is finite. $h_K = |C_K|$ = class number of K

Thm (Dirichlet). $\mathcal{O}_K^\times$ is finitely generated.
In particular, $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r_1+r_2-1}$

(μ_K: roots of unity in K)

$r_1 = \#$ of real embeddings of K
$r_2 = \frac{1}{2}(\#$ of complex embeddings of $K)$

Galois group acts on $\mathcal{O}_K^\times$, and in particular $\mathbb{Z}^{r_1+r_2-1}$
choosing a basis, for each $\sigma \in G_{K/\mathbb{Q}}$ we get a matrix, hence a representation

$$1 \to \mathcal{O}_K^\times \to K^\times \to \mathcal{P}_K \to 1$$

$$1 \to \mathcal{P}_K \to I_K \to C_K \to 1$$

or $1 \to \mathcal{O}_K^\times \to K^\times \to I_K \to C_K \to 1$

$\alpha \mapsto \alpha\mathcal{O}_K$

Let $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ be a finite set of primes

(Silverman will occasionally abuse notation and use $\mathrm{Spec}(\mathcal{O}_K) = \{\text{non-zero prime ideals}\}$)

$\mathcal{O}_S = \mathcal{O}_{K,S}$ = ring of S-integers =
$\{\alpha \in K^\times \mid \mathrm{ord}_\mathfrak{p}(\alpha) \geq 0 \text{ for all } \mathfrak{p} \notin S\} \cup \{0\}$

Thm, $\mathcal{O}_{K,S}^\times \cong \mu_K \times \mathbb{Z}^{r_1+r_2+|S|-1}$

Example. $K = \mathbb{Q}$, $\mathbb{Z}^\times = \mu_\mathbb{Q} = \{\pm 1\}$, $\mathbb{Z}_{\{2,3\}}^\times = \mathbb{Z}\left[\frac{1}{2}, \frac{1}{3}\right]^\times =$
$\{\pm 2^i 3^j \mid i,j \in \mathbb{Z}\}$

Extension fields

L/K, $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$, $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$, $e_i \geq 1$
$n = [L:K]$ ← ramification index

we write $\mathfrak{P}_i \mid \mathfrak{p}$. Also, $e_\mathfrak{p} = e(\mathfrak{P}/\mathfrak{p}) = \mathrm{ord}_\mathfrak{P}(\mathfrak{p}\mathcal{O}_L)$.
$(\Leftrightarrow \mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}_i)$

Let $\mathfrak{P} \mid \mathfrak{p}$. $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induces $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$.

Silverman's notation: $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$, $\mathbb{F}_\mathfrak{P} = \mathcal{O}_L/\mathfrak{P}$

$f(\mathfrak{P}/\mathfrak{p}) = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_{\mathfrak{p}}]$ is the residue field degree.

Thm. Given $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, $\sum_{i=1}^{r} e_i f_i = n$

If L/K is Galois, $e(\mathfrak{P}_i/\mathfrak{p})$ all the same,
$f(\mathfrak{P}_i/\mathfrak{p})$ all the same,
hence $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$, $ref = n$

$\mathfrak{p}$ is unramified if all $e(\mathfrak{P}_i/\mathfrak{p}) = 1$, ramified otherwise

$\mathfrak{p}$ is totally ramified if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n$, i.e. there is a prime $\mathfrak{P} \mid \mathfrak{p}$ with $e(\mathfrak{P}/\mathfrak{p}) = n$ (hence $r = 1$, $f = 1$)

$\mathfrak{p}$ is inert if $\mathfrak{p}\mathcal{O}_L$ is prime, i.e. $e(\mathfrak{P}/\mathfrak{p}) = 1$, $f(\mathfrak{P}/\mathfrak{p}) = n$

$\mathfrak{p}$ is totally split if $e(\mathfrak{P}_i/\mathfrak{p}) = 1$, $f(\mathfrak{P}_i/\mathfrak{p}) = 1$,
$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r$

Thm. $\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) \mid \mathfrak{p}$ ramified in $L\}$ finite

Given $x_1, \ldots, x_n \in L$, $\mathrm{disc}(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j))$
$= \det(\sigma_i(x_j))^2$,

$\mathrm{Tr}_{L/K} = \sum_{\substack{\sigma : L \hookrightarrow \bar{K} \\ \sigma|_K = \mathrm{id}}} \sigma(x)$

$\mathfrak{p}$ ramified $\Leftrightarrow \mathfrak{p} \mid \mathrm{Disc}$

Lecture 2 (2011-01-28)

$\alpha \in \mathcal{O}_L$, or $\alpha \in I_L$,

2011-1-28

(2)

$\mathrm{Disc}(\alpha) = \langle \mathrm{Disc}(x_1, \dots, x_n) \rangle_{\alpha = (x_1, \dots, x_n)} \in I_L$

Thm. $\mathfrak{p}$ ramifies $\iff \mathfrak{p} \mid \underbrace{\mathrm{Disc}_{L/K}(\mathcal{O}_L)}_{d_{L/K}}$

$d_K = \mathrm{Disc}_{K/\mathbb{Q}}(\mathcal{O}_K)$

The Norm $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$

Extend to I_L, $N_{L/K}(\prod \mathfrak{P}_i^{a_i}) = \prod N_{L/K}(\mathfrak{P}_i)^{a_i}$

If L/K Galois, $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$

If $\alpha \in L$, $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$, $N_{L/K}((\alpha)) = (N_{L/K}(\alpha))$

$N_{E/K} = N_{L/K} \circ N_{E/L}$

Galois extensions

L/K, $G_{L/K} = \mathrm{Gal}(L/K)$, $\mathfrak{P} \mid \mathfrak{p}$

Decomposition group: $D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G_{L/K} \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$

$\sigma \in D(\mathfrak{P}|\mathfrak{p})$ induces an automorphism of $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$

So we get a homomorphism $D(\mathfrak{P}|\mathfrak{p}) \to \underbrace{\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})}_{\text{cyclic}}$

The kernel of this map is the inertia group

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}/\mathfrak{p}) \mid \sigma(a) \equiv a \bmod \mathfrak{P} \text{ for all } a \in \mathcal{O}_L\}$$

$\mathfrak{P}/\mathfrak{p}$ unramified iff $I(\mathfrak{P}/\mathfrak{p}) = 1$, and

furthermore, $|I(\mathfrak{P}/\mathfrak{p})| = e(\mathfrak{P}/\mathfrak{p})$

Thm. $G_{L/K}$ acts transitively on the $\mathfrak{P}_i/\mathfrak{p}$.

$D(\mathfrak{P}_i/\mathfrak{p})$ and $D(\mathfrak{P}_j/\mathfrak{p})$ are all conjugate

$N\mathfrak{p} = |\mathbb{F}_\mathfrak{p}|$, $N\mathfrak{P} = |\mathbb{F}_\mathfrak{P}|$

N means norm down to $\mathbb{Q}$

$\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ is cyclic, generated by Frobenius

$a \longmapsto a^{N\mathfrak{p}}$

$\phi_\mathfrak{p}$ or $\mathrm{Frob}_\mathfrak{p}$

$|\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})| = f(\mathfrak{P}/\mathfrak{p})$

$D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p}) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$, so that

if $\mathfrak{p}$ is unramified, $I(\mathfrak{P}/\mathfrak{p}) = 1$, hence there is a unique element of $D(\mathfrak{P}/\mathfrak{p})$ that induces $\phi_\mathfrak{p}$ on $\mathbb{F}_\mathfrak{P}$. This is denoted $\left(\frac{\mathfrak{P}/\mathfrak{p}, L/K}{}\right) \in D(\mathfrak{P}/\mathfrak{p})$

Called the Artin symbol.

Lemma. $\mathfrak{P}_1, \mathfrak{P}_2 \mid \mathfrak{p} \Rightarrow (\mathfrak{P}_1/\mathfrak{p}, L/K)$ and $(\mathfrak{P}_2/\mathfrak{p}, L/K)$ one conjugate

So $\mathfrak{p}$ determines a conjugacy class $(\mathfrak{p}, L/K) \subset G_{L/K}$

If L/K abelian, $(\mathfrak{p}, L/K) \in G_{L/K}$ "Box that and put stars around it".

Artin Map (L/K abelian)

$$(\cdot, L/K): I_K^{unr} \longrightarrow G_{L/K}$$
$$(\textstyle\prod \mathfrak{p}_i, L/K) \to \prod (\mathfrak{p}_i, L/K)$$

Thm. (part of class field theory)

L/K abelian (and K is totally imaginary), then

$\exists$ an ideal $\mathfrak{C}$ (conductor) $\subset \mathcal{O}_K$ such that

Let $\alpha \in \mathcal{O}_K$, $\alpha \equiv 1 \bmod \mathfrak{C}$. Then $(\alpha\mathcal{O}_K, L/K) = 1$.

(Still not quite true.)

Example. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$(a\mathbb{Z}, K/\mathbb{Q}) = \prod (p_i\mathbb{Z}, K/\mathbb{Q})$

but $(p\mathbb{Z}, K/\mathbb{Q})$ needs to raise things to pth powers, so

$(p\mathbb{Z}, K/\mathbb{Q})(\zeta_n) \equiv \zeta_n^p \bmod \mathfrak{P}$

Prop. $\mu_n \to \mathcal{O}_K/\mathfrak{p} = \mathbb{Z}[\zeta_n]/\mathfrak{p}$ is injective iff $p \nmid n$.

(HW #1) ↗

Thus we actually have $(p\mathbb{Z}, K/\mathbb{Q})(\zeta_n) = \zeta_n^p$

so $(a\mathbb{Z}, K/\mathbb{Q})(\zeta_n) = \zeta_n^a$, so $(a\mathbb{Z}, K/\mathbb{Q}) = 1$
$\Leftrightarrow a \equiv 1 \bmod n$

So n is the conductor of the cyclotomic extension

The roots of unity were helping us keep track of things

Dirichlet's Theorem

$$\{\text{primes } p \equiv 1 \bmod n\} = \{\text{primes } p \mid (p\mathbb{Z}, \mathbb{Q}(\zeta_n)/\mathbb{Q}) = 1\}$$

Lecture 3 (2009-01-31)

Office Hours (email in advance) 2011-1-31 (3)
Mon 2–3 Fri 9:30–10:30

$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$
$a \longmapsto (\sigma_a : \zeta_n \to \zeta_n^a)$ and $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) = \sigma_p$

So $\{p \mid p \equiv a \bmod n\} = \{p : (p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) = \sigma_a\}$

Generalize to arbitrary number fields L/K (Galois)

$\mathfrak{p} \in Spec(\mathcal{O}_K)$, unramified in L, then $(\mathfrak{p}, L/K)$ is a conjugacy class in $G_{L/K}$

So fix a conjugacy class $C \subset G_{L/K}$, and look at
$\{\mathfrak{p} \in Spec(\mathcal{O}_K) \mid (\mathfrak{p}, L/K) = C\}$

$$\pi_K(x, C) = \#\{\mathfrak{p} \in Spec(\mathcal{O}_K) \mid (\mathfrak{p}, L/K) = C, N_{\mathbb{Q}}^K(\mathfrak{p}) \le x\}$$

$$\pi_K(x) = \#\{\mathfrak{p} \in Spec(\mathcal{O}_K) \mid N_{\mathbb{Q}}^K(\mathfrak{p}) \le x\}$$

A subset $S \subset Spec(\mathcal{O}_K)$ has natural density

$$\delta(S) = \lim_{x \to \infty} \frac{\#\{\mathfrak{p} \in S \mid N\mathfrak{p} \le x\}}{\pi_K(x)} \quad \text{(if limit exists)}$$

Chebotarov Density Theorem

$$\delta(C) = \frac{\#C}{\#G_{L/K}}$$

Given some $\mathcal{P} \subset \mathrm{Spec}(\mathbb{Z})$

$$\sum_{p} \frac{1}{p^s} \sim -\log(s-1) \quad \text{as} \quad s \to 1^+$$

so analytic density of $\mathcal{P}$ is

$$\delta^{an}(\mathcal{P}) = \lim_{s \to 1} \frac{1}{-\log(s-1)} \sum_{p \in \mathcal{P}} \frac{1}{p^s}$$

Thm. If $\delta^{nat}(\mathcal{P})$ exists, then so does $\delta^{an}(\mathcal{P})$, and $\delta^{nat}(\mathcal{P}) = \delta^{an}(\mathcal{P})$.

New density: $\delta^{an-2}(\mathcal{P}) = \lim_{s \to 1^+} (s-1) \sum_{p \in \mathcal{P}} \frac{\log(p)}{p^s}$

HW 2: $\sum_{p} \frac{\log(p)}{p^s} \sim \frac{1}{s-1}$ as $s \to 1^+$

Hint: differentiate $\log(\zeta(s))$

Special case: Fix a prime q, and consider $\{p \mid p \equiv a \bmod q\}$

$$\sum_{p \equiv a \bmod q} \frac{\log(p)}{p^s} = \sum_{p} \begin{pmatrix} 1 \text{ if } p \equiv a \bmod q \\ 0 \text{ if } p \not\equiv a \bmod q \end{pmatrix} \frac{\log(p)}{p^s}$$

How can we define this non-step-function like?, Find a sum with this property - then we can switch the sums,

Characters for abelian groups

G finite abelian group, $\hat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$

Prop. a) $\hat{G} \cong G$ (non-canonical)
b) $\hat{\hat{G}} \cong G$ (canonical)

HW 3: G abelian, $\#G = \infty$, then $G \hookrightarrow \hat{\hat{G}}$

Pf in case G is cyclic (in particular $G = (\mathbb{Z}/q\mathbb{Z})^\times$)

$G \cong \mathbb{Z}/n\mathbb{Z}$, then define a map

$F: G \to \hat{G}$
$a \mapsto (k \mapsto \zeta_n^{ak})$

Injective: $F(a) = 1 \Rightarrow$ $\zeta_n^{ak} = 1$ for all k, hence $\zeta_n^a = 1$, hence $a \equiv 0 \bmod n$

Surjective $\chi \in \hat{G}$, then $\chi(1) = \zeta_n^b$ for some b,
so $\chi(k) = \zeta_n^{bk}$, so $\chi = F(b)$

b) $G \hookrightarrow \hat{\hat{G}} = \mathrm{Hom}(\hat{G}, \mathbb{C}^\times)$
$a \mapsto (\chi \mapsto \chi(a))$ and $\#G = \#\hat{G} = \#\hat{\hat{G}}$ by a) twice

Orthogonality

G a finite abelian group, χ_0 the trivial character

a) $\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} \#G & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases}$

b) $\sum_{a \in G} \chi(a) = \begin{cases} \#G & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0 \end{cases}$

Pf. a) $g \in G$, $g \neq 1$, then $\exists \gamma \in \hat{G}$ with $\gamma(g) \neq 1$

such a γ exists because $G \cong \hat{G}$

(if $\gamma(g) = 1$, then γ reduces to element of $\widehat{(G/\langle g \rangle)}$)

$$\gamma(g) \sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} (\gamma\chi)(g) = \sum_{\chi \in \hat{G}} \chi(g)$$

$\gamma(g) \neq 1$ hence $\sum_{\chi \in \hat{G}} \chi(g) = 0$

b) similar

So let $G_q = (\mathbb{Z}/q\mathbb{Z})^\times$ cyclic of order $q-1$

$$\sum_{\chi \in \hat{G}_q} \chi(b) = \begin{cases} q-1 & \text{if } b \equiv 1 \bmod q \\ 0 & \text{if } b \not\equiv 1 \bmod q \end{cases}$$

$$\frac{1}{q-1} \sum_{\chi \in \hat{G}_q} \chi(a^{-1}p) = \begin{cases} 1 & \text{if } p \equiv a \bmod q \\ 0 & \text{if } p \not\equiv a \bmod q \end{cases}$$

$\chi(a)^{-1}\chi(p) = \overline{\chi(a)}\,\chi(p)$

$$\sum_{p \equiv a \bmod q} \frac{\log(p)}{p^s} = \sum_p \left(\frac{1}{q-1} \sum_{\chi \in \hat{G}_q} \overline{\chi(a)}\,\chi(p) \right) \frac{\log(p)}{p^s}$$

absolutely convergent for $\mathrm{Re}(s) > 1$, so switch order

$$\frac{1}{q-1} \sum_{\chi \in \hat{G}_q} \overline{\chi(a)} \left(\sum_p \frac{\chi(p)\log(p)}{p^s} \right)$$

As $s \to 1^+$, this is $\sim \frac{1}{s-1}$ if $\chi = \chi_0$ (easy)

bounded if $\chi \neq \chi_0$ (hard)

Lecture 4 (2011-02-04)

$$\sum_{p \equiv a \bmod q} \frac{\log(p)}{p^s} = \sum_p \begin{pmatrix} 1 \text{ if } p \equiv a \bmod q \\ 0 \text{ otherwise} \end{pmatrix} \frac{\log(p)}{p^s} =$$

2011-2-4

(4)

$G_q = (\mathbb{Z}/q\mathbb{Z})^\times$ $\qquad \sum_p \frac{1}{q-1} \sum_{\chi \in \widehat{G}_q} \overline{\chi(a)} \chi(p) \frac{\log(p)}{p^s} =$

$$\frac{1}{q-1} \sum_{\chi \in \widehat{G}_q} \bar{\chi}(a) \sum_p \frac{\chi(p)\log(p)}{p^s}$$

L-Series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

If $\chi = \chi_0 \in \widehat{G}_q$, $L(s,\chi_0)$ is almost $\zeta(s)$, but

$\chi_0 : (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$

$\chi_0(a) = 1$ for all a

but $\chi_0(b) = 0$ if $b \notin (\mathbb{Z}/q\mathbb{Z})^\times$

So $L(s,\chi_0) = \underbrace{\left(1 - \frac{1}{q^s}\right)}_{\text{bounded from 0 if } \mathrm{Re}(s) > 0} \zeta(s)$

$$\frac{d}{ds} \log(L(s,\chi)) = \frac{1}{ds}\left(\sum_p -\log\left(1 - \frac{\chi(p)}{p^s}\right)\right) \qquad \mathrm{Re}(s) > 1$$

$$\frac{d}{ds}\left(\sum_p \sum_{u=1}^{\infty} \frac{1}{u}\left(\frac{\chi(p)}{p^s}\right)^u\right) = \sum_{u=1}^{\infty} \sum_p \frac{1}{u} \frac{\chi(p)^u (-u\log(p))}{p^{us}} =$$

$$-\sum_p \frac{\chi(p)\log(p)}{p^s} - \left(\sum_{u \geq 2} \sum_p \frac{\chi(p)^u \log(p)}{p^{us}}\right)$$

HW – analytic for $\mathrm{Re}(s) > \frac{1}{2}$

$$\operatorname*{Res}_{s=1}\left(\sum_{p\equiv a \bmod q}\frac{\log(p)}{p^s}\right)=\frac{1}{q-1}\sum_{\chi\in\widehat{G_q}}\overline{\chi}(a)\operatorname*{Res}_{s=1}\left(\sum_p\frac{\chi(p)\log(p)}{p^s}\right)=$$

$$\frac{1}{q-1}\sum_{\chi\in\widehat{G_q}}\overline{\chi}(a)\operatorname*{Res}_{s=1}\left(-\frac{d}{ds}(\log(L(s,\chi)))\right)$$

↑ equal because remainder term analytic for $\mathrm{Re}(s)>1$

$$\operatorname*{Res}_{s=a}\frac{d}{ds}\log(F(s))=\operatorname*{Res}_{s=a}\frac{F'(s)}{F(s)}=\operatorname*{ord}_{s=a}F(s)$$

$$F(s)=(s-a)^e G(s),\quad G(a)\neq 0,\infty$$

$$\frac{F'(s)}{F(s)}=\frac{e}{s-a}+\frac{G'}{G}$$

$$\zeta(s)-\frac{1}{s-1}=\sum_{n=1}^{\infty}\frac{1}{n^s}-\int_1^{\infty}\frac{dx}{x^s}\qquad \mathrm{Re}(s)>1$$

$$=\sum_{n=1}^{\infty}\frac{1}{n^s}-\sum_{n=1}^{\infty}\int_n^{n+1}\frac{dx}{x^s}=\sum_{n=1}^{\infty}\int_0^1\frac{1}{n^s}dx-\sum_{n=1}^{\infty}\int_0^1\frac{dx}{(x+n)^s}$$

$$=\int_0^1\sum_{n=1}^{\infty}\left(\frac{1}{n^s}-\frac{1}{(n+x)^s}\right)dx$$

$$\frac{1}{n^s}\left(1-\frac{1}{(1+\frac{x}{n})^s}\right)\qquad \sum_{n=1}^{\infty}\int_0^1\frac{sx}{n^{s+1}}dx\approx s\,c\,\zeta(s+1)$$

HW: Try to figure out $\lim_{s\to 1}\zeta(s)-\frac{1}{s-1}$ using

$\lim_{x\to\infty}\sum_{n\le x}\frac{1}{n}-\log(x)=\gamma$ (hint: maybe answer is $2\gamma-1$?)

$$\operatorname*{Res}_{s=1} \sum_{p \equiv a \bmod q} \frac{\log(p)}{p^s} = \frac{1}{q-1} - \frac{1}{q-1} \sum_{\substack{\chi \in \widehat{G_q} \\ \chi \neq \chi_0}} \overline{\chi}(a) \operatorname{ord}_{s=1}(L(s,\chi))$$

Lemma. Let $a_i \in \mathbb{C}$ be such that $\sum_{n=1}^{N} a_n$ is bounded independent of N

Then $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $\operatorname{Re}(s) > 1$

Pf. $b_N = \sum_{i=1}^{N} a_i$, so $a_n = b_n - b_{n-1}$

Thus $\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{n=1}^{\infty} \frac{b_n - b_{n-1}}{n^s}$ $\operatorname{Re}(s) > 1$

$$= \sum_{n=1}^{\infty} \frac{b_n}{n^s} - \sum_{n=1}^{\infty} \frac{b_n}{(n+1)^s} = \sum_{n=1}^{\infty} \left| b_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \right|$$

(b_n bounded; $\frac{1}{n^s}\left(1 - \left(1+\frac{1}{n}\right)^{-s}\right)$)

$$< C \sum_{n=1}^{\infty} \left| \frac{1}{n^s} \frac{-s}{n} \right|, \text{ converges for } \operatorname{Re}(s) > 0$$

$$\sum_{n=1}^{N} \chi(n) = \sum_{m=0}^{\lfloor \frac{N}{q} \rfloor} \underbrace{\sum_{r=0}^{q-1} \chi(mq+r)}_{0} + \underbrace{\sum_{r=0}^{N - q\lfloor \frac{N}{q} \rfloor} \chi(r)}_{\text{bounded}}$$

Hence $L(s,\chi)$ analytic for $\operatorname{Re}(s) > 0$, $\chi \neq \chi_0$

Remains to show: $L(1,\chi) \neq 0$,

Prop. $F(s) = \prod_{\chi \in \widehat{G}_q} L(s,\chi)$. Let $s \in \mathbb{R}$, $s > 1$

$F(s) \in \mathbb{R}$ and $F(s) > 1$.

Pf. $\log(F(s)) = \sum_{\chi} \sum_{p} \sum_{u=1}^{\infty} \frac{\chi(p)^u}{u p^{us}} =$

$$\sum_{u=1}^{\infty} \frac{1}{u} \sum_{p} \frac{1}{p^{us}} \sum_{\chi \in \widehat{G}_q} \chi(p^u) = \sum_{u=1}^{\infty} \frac{1}{u} \sum_{\substack{p \\ p^u \equiv 1 \bmod q}} \frac{1}{p^{us}} \cdot (q-1)$$

≥ 0

Since $p^{q-1} \equiv 1 \bmod q$

Prop. $\chi \in \widehat{G}_q$ and assume $\chi((\mathbb{Z}/q\mathbb{Z})^\times) \neq \mathbb{R}$.

Then $L(1,\chi) \neq 0$.

Pf. Suppose $L(1,\chi) = 0$.

$1 \leq F(s) = L(s,\chi_0)\, L(s,\chi)\, L(s,\bar{\chi}) \prod_{\text{other } \chi} L(s,\chi)$

as $s \to 1^+$ — pole at $s=1$ — zero at $s=1$ — zero at $s=1$ — all analytic at $s=1$

$L(s,\bar{\chi}) = \overline{L(s,\chi)}$

Contradiction

Lecture 5 (2011-02-07)

Last time: $\sum_{p \equiv a \bmod q} \frac{\log(p)}{p^s}$ has a pole at $s=1$ 2011-2-7 (5)

provided $L(1,\chi) \neq 0$ for all $\chi \in \widehat{G}$, $\chi \neq \chi_0$

Done if χ is complex.

Lemma. Let $\chi \in \widehat{G}$ be a real character, $\chi \neq \chi_0$. Then $L(1,\chi) \neq 0$
(If you think about it, you see χ must be $(\frac{\cdot}{q})$)

Pf. Assume $L(1,\chi) = 0$. Look at

$$\psi(s) = \frac{L(s,\chi_0)\,L(s,\chi)}{L(2s,\chi_0)}$$

As $s \to 1^+$, $\underbrace{L(s,\chi_0)}_{\text{simple pole}}\,\underbrace{L(s,\chi)}_{0}$ ← analytic at $s=1$

$L(2s,\chi_0)$ analytic for $\mathrm{Re}(s) > \frac{1}{2}$, pole at $s = \frac{1}{2}$

So $\psi(s)$ analytic for $\mathrm{Re}(s) \geq \frac{1}{2}$, $\psi(\frac{1}{2}) = 0$.

$$\psi(s) = \prod_p \frac{(1-\chi_0(p)p^{-s})^{-1}(1-\chi(p)p^{-s})^{-1}}{(1-\chi_0(p)p^{-2s})^{-1}} =$$

$$\prod_{p \neq q} \frac{1-p^{-2s}}{(1-p^{-s})(1-\chi(p)p^{-s})} =$$

$$\prod_{\substack{p \\ \chi(p)=1}} \frac{1+p^{-s}}{1-p^{-s}} = \prod_{\chi(p)=1} (1+p^{-s})(1+p^{-s}+p^{-2s}+\dots)$$

$$\prod_{\chi(p)=1} (1+2p^{-s}+2p^{-2s}+2p^{-3s}+\dots) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad a_n \geq 0 \quad a_1 = 1$$

So $\gamma(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, $a_n \geq 0$ and $a_1 = 1$, $\lim_{s \to \frac{1}{2}} \gamma(s) = 0$.

Look at Taylor series around $s = 2$ (Silverman: don't know what motivates $s=2$)

$$\gamma(s) = \sum_{m=0}^{\infty} b_m (s-2)^m$$

$$b_m = \frac{1}{m!} \frac{d^m}{ds^m} \gamma(s) \Big|_{s=2} = \frac{1}{m!} \sum_{n=1}^{\infty} \frac{(-\log(n))^m a_n}{n^2}$$

Let $b_m = (-1)^m c_m$, with $c_m \geq 0$.

$$c_0 = b_0 = \gamma(2) = \sum_{n=1}^{\infty} \frac{a_n}{n^2} \geq 1 \quad \text{since } a_1 = 1$$

$$\gamma(s) = \sum_{m=0}^{\infty} (-1)^m c_m (s-2)^m = \sum_{m=0}^{\infty} c_m (2-s)^m$$

Let $s \to \frac{1}{2}$

$$\gamma\left(\tfrac{1}{2}\right) = \underbrace{c_0}_{\geq 1} + \underbrace{\sum_{m=1}^{\infty} c_m \left(\tfrac{3}{2}\right)^m}_{\geq 0} \geq 1, \text{ contradiction}$$

Let $\chi_q = \left(\frac{\cdot}{q}\right)$. We showed $L(1, \chi_q) \neq 0$.

What is $\sup\{\varepsilon > 0 \mid L(s, \chi_q) \neq 0 \text{ for all } 1 - \varepsilon < s \leq 1\}$?

Best so far: $\varepsilon = \frac{\text{constant}}{\sqrt{q}}$

Helps in determining $M_{a,q} = \min\{p \mid p \equiv a \bmod q\}$

Back to class field theory!

Motivating Question: Fix $K/\mathbb{Q}$. If L/K is unramified, how big can $[L:K]$ be?

Answer: Arbitrarily large (Golod–Shafarevich). $\exists K$ such that it can be

For example, $K = \mathbb{Q}(\sqrt{-2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13})$.

This is different if L/K is required to be abelian

Thm*. Fix $K/\mathbb{Q}$. There is a finite extension L/K that is the maximal abelian and unramified extension of K, and $[L:K]$ is finite.

L is called the Hilbert class field of K.

Prop. L/K abelian, $\mathfrak{p}$ unramified

a) $(\mathfrak{p}, L/K)$ has order $f(\mathfrak{p})$ in $G_{L/K}$

b) $\mathfrak{p}$ splits completely in $L \iff (\mathfrak{p}, L/K) = 1$

c) Let $J \subset \mathcal{O}_L$ be unramified (i.e. primes dividing J are unramified). Then $(N_{L/K}(J), L/K) = 1$.

(This implies $I_K \xrightarrow{(\cdot, L/K)} G_{L/K}$, $I_K \to I_K / N_{L/K}(I_L)$)

a) $(\mathfrak{P}, L/K)$ generates $D(\mathfrak{P}) \xrightarrow{\sim} \underbrace{Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})}_{\text{cyclic of order } f(\mathfrak{P})}$

b) $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_{r(\mathfrak{p})}$, $r(\mathfrak{p}) f(\mathfrak{p}) = [L:K]$

$\mathfrak{p}$ splits completely $\Leftrightarrow f(\mathfrak{p}) = 1 \Leftrightarrow (\mathfrak{p}, L/K)$ has order 1

c) $J = \prod \mathfrak{P}_i$

$(N_{L/K} J, L/K) = \prod (N_{L/K} \mathfrak{P}_i, L/K) = \prod (\mathfrak{p}_i^{f(\mathfrak{P}_i)}, L/K)$

where $\mathfrak{p}_i = N_{L/K}(\mathfrak{P}_i)$

$= \prod (\mathfrak{p}_i, L/K)^{f(\mathfrak{P}_i)} = 1$

A side on power-residue symbols

$\left(\frac{a}{p}\right)_2 \in \{\pm 1\}$, $\left(\frac{a}{p}\right)_2 \equiv a^{\frac{p-1}{2}} \bmod p$

So we work in $\mathbb{Q}(\zeta_n)$, $\mathbb{Z}[\zeta_n]$

Let $\mathfrak{P} \in \mathrm{Spec}(\mathbb{Z}[\zeta_n])$, $\mathfrak{P} \nmid n$, $\alpha \in \mathbb{Z}[\zeta_n]$, $\mathfrak{P} \nmid \alpha$

Def. $\left(\frac{\alpha}{\mathfrak{P}}\right)_n \in \mu_n$, unique $\left(\frac{\alpha}{\mathfrak{P}}\right) \equiv \alpha^{\frac{N(\mathfrak{P})-1}{n}} \bmod \mathfrak{P}$

$\left(\frac{\alpha}{\mathfrak{P}}\right) = 1 \Leftrightarrow \alpha \equiv \beta^n \bmod \mathfrak{P}$

Example. $K = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, $L = K(\sqrt[3]{2})$

$G_{L/K} \cong \mathbb{Z}/3\mathbb{Z}$

$\sigma \longleftrightarrow i(\sigma)$ $\qquad \sigma(\sqrt[3]{2}) = \zeta_3^{i(\sigma)}\sqrt[3]{2}$

Let π be a prime in $\mathbb{Z}[\zeta_3]$, $\pi \nmid 6$.

$$\left(\frac{\pi, L/K}{}\right)(\sqrt[3]{2}) \equiv (\sqrt[3]{2})^{N(\pi)} \bmod \pi$$

$$\equiv 2^{\frac{N(\pi)-1}{3}} \cdot \sqrt[3]{2} \bmod \pi$$

$$\equiv \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2} \bmod \pi$$

action of Artin symbol is reciprocity symbol

Lecture 6 (2011-02-09)

L/K abelian and unramified (at all places, including infinite places) 2011-2-9 (6)

so $(L/K, \mathfrak{a})$ is defined for all $\mathfrak{a} \in I_K$

Thm*. Let L/K be the largest abelian unramified extension of K. (L is called the Hilbert class field of K).

a) $(L/K, \cdot) : I_K \xrightarrow{\text{onto}} G_{L/K}$

b) kernel is P_K

hence $Cl_K \xrightarrow{\sim} G_{L/K}$

$$\{\text{abelian unramified } M/K\} \longleftrightarrow \{\text{subgroups of } Cl_K\}$$

Corollary. $\mathcal{O}_K$ is a PID $\iff$ K has no abelian unramified extensions

$$\{\text{infinite primes of } K\} \longleftrightarrow \{K \hookrightarrow \mathbb{R}\} \cup \{K \hookrightarrow \mathbb{C}, K \not\subset \mathbb{R}\}/\sim$$

($\sim$: complex conjugation)

Complex primes never ramify

real primes ramify if there is a complex place of L lying over p

ramification index!

$$r_1 + 2r_2 = n$$

$\mathbb{Q}(i)$ p_∞ but there are really two,

$|$ $|$ hence ramification

$\mathbb{Q}$ p_∞ index is 2

1 and 2 are only possible indexes because only extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$

Def. A modulus is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p} \text{ places}} \mathfrak{p}^{n_\mathfrak{p}} \quad \text{with} \quad n_\mathfrak{p} \geq 0, \; n_\mathfrak{p} > 0 \text{ for only finitely many } \mathfrak{p}$$

$n_\mathfrak{p} = 0$ if $\mathfrak{p}$ is complex

$n_\mathfrak{p} = 0$ or 1 if $\mathfrak{p}$ is real

$$\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$$

finite primes, infinite primes

$$I_K(\mathfrak{m}) = \{ \mathfrak{a} \in I_K \mid \gcd(\mathfrak{a}, \mathfrak{m}_0) = 1 \}$$

$$P_{K,1}(\mathfrak{m}) = \{ (\alpha) \mathcal{O}_K \in P_K \mid \alpha \equiv 1 \bmod \mathfrak{m}_0 \text{ and } \sigma_\mathfrak{p}(\alpha) > 0 \text{ for all infinite } \mathfrak{p} \mid \mathfrak{m} \}$$

$\sigma_\mathfrak{p} : K \hookrightarrow \mathbb{R}$

Example. $K = \mathbb{Q}$, $m \in \mathbb{Z}$

$$P_{\mathbb{Q},1}(m) = \{ (a) \mathbb{Z} \mid a \equiv 1 \bmod m \}$$

$$P_{\mathbb{Q},1}(m \cdot \infty) = \{ (a) \mathbb{Z} \mid a \equiv 1 \bmod m, \; a > 0 \}$$

When $\mathfrak{m} = 1$, $I_K(\mathfrak{m}) = I_K$ $P_{K,1}(\mathfrak{m}) = P_K$

Life would be so much easier if there were no real fields, — but it goes on.

Thm: $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ is finite

Pf Sketch, $(I_K(\mathfrak{m}) : P_K \cap I_K(\mathfrak{m}))$ finite using result for classical I_K, P_K

Now show $(P_K \cap I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m}))$ also finite

Def, $H \subset I_K(\mathfrak{m})$ is called a congruence subgroup if $H \supset P_{K,1}(\mathfrak{m})$. Then $I_K(\mathfrak{m})/H$ is called a generalized ideal class group.

ORP: Assume $\mathfrak{m}$ is divisible by all primes (including infinite primes) that ramify in L/K

If ORP, $\left(\frac{L/K}{\cdot}\right) : I_K(\mathfrak{m}) \longrightarrow G_{L/K}$ is well-defined

$\Phi_{\mathfrak{m}}$, or $\Phi_{L/K,\mathfrak{m}}$

Artin Reciprocity Thm

L/K abelian

a) If $\mathfrak{m}$ is a modulus ORP, then $\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to G_{L/K}$ is surjective

b) $\exists\, \mathfrak{m}$, ORP, such that $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$

c) $\exists \mathfrak{m}$ satisfying $\alpha \mathcal{O}_K \in P_{K,1}(\mathfrak{m}) \Rightarrow \Phi_{\mathfrak{m}}(\alpha \mathcal{O}_K) = 1$

$\left(\alpha \equiv 1 \bmod^{*} \mathfrak{m}\right)$ $\qquad$ $\prod \Phi_{\mathfrak{m}}(P_i)$

Ex. $L = \mathbb{Q}(\zeta_n)$, $K = \mathbb{Q}$ $M = n \cdot \infty$

$\Phi_m : I_{\mathbb{Q}}(n \cdot \infty) \to Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$\sigma \leftrightarrow i(\sigma)$

$\sigma(\zeta_n) = \zeta_n^{i(\sigma)}$

$\Phi_m(a\mathbb{Z})(\zeta_n) = \zeta_n^{|a|}$

$a\mathbb{Z} \in P_{\mathbb{Q},1}(n \cdot \infty) \Leftrightarrow a \equiv 1 \bmod n,\ a > 0$

$\ker(\Phi_m) \supseteq P_{\mathbb{Q},1}(n \cdot \infty)$ (actually in this case equal)

Note: $M \mid N \Rightarrow P_{K,1}(N) \subseteq P_{K,1}(M)$

Same theory for $K = \mathbb{Q}(\sqrt{-D})$, $D > 0$ using elliptic curves

Lecture 7 (2011-02-11)

Artin Reciprocity L/K abelian 2011-2-11 (7)

a) $I_K(M) \xrightarrow{\phi_{L/K,M}} G_{L/K}$ is surjective for M a DRP

b) $\exists M$ such that $\ker(\phi_{L/K,M}) \supset P_{K,1}(M)$

Conductor Theorem

$\exists!$ modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ DRP of L/K, such that

a) $\mathfrak{p} \mid \mathfrak{f}(L/K) \iff \mathfrak{p}$ ramifies in L/K

b) If M is DRP for L/K and $\ker(\phi_{L/K,M}) \supset P_{K,1}(M)$

then $\mathfrak{f}(L/K) \mid M$.

$\mathfrak{f}(L/K)$ = conductor of L/K

HW: Show $\mathfrak{f}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \begin{cases} 1 & \text{if } n \le 2 \\ n/2\,\infty & \text{if } n \ge 3,\ 2 \mid n,\ 4 \nmid n \\ n\,\infty & \text{otherwise} \end{cases}$

Existence Theorem

Let M be a modulus for K, let $S \subset I_K(M)$ be a subgroup with $S \supset P_{K,1}(M)$. Then $\exists!$ abelian L/K with ramified primes dividing M satisfying

$\ker(\phi_{L/K,M}) = S$, or equivalently

$\phi_{L/K,M} : I_K(M)/S \xrightarrow{\sim} G_{L/K}$

Cor. L/K, F/K abelian extensions (in some algebraic closure). TFAE:

a) $L \subset F$

b) $\exists$ modulus $\mathfrak{m}$ DRP in L and F such that
$$\ker(\Phi_{L/K,\mathfrak{m}}) \supset \ker(\Phi_{F/K,\mathfrak{m}}) \supset P_{K,1}(\mathfrak{m})$$

Pf. a) $\Rightarrow$ b)

Let $\mathfrak{m}$ be a modulus such that
$$\ker(\Phi_{L/K}) \supset P_{K,1}(\mathfrak{m})$$
$$\ker(\Phi_{F/K}) \supset P_{K,1}(\mathfrak{m})$$

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\phi_{F/K}} & G_{F/K} \\ \| & & \downarrow \sigma \mapsto \sigma|_L \\ I_K(\mathfrak{m}) & \xrightarrow{\Phi_{L/K}} & G_{L/K} \end{array}$$

enough to check on primes, which generate $\cdot$ $(\mathfrak{p}, F/K)|_L = (\mathfrak{p}, L/K)$ because

$$(\mathfrak{p}, F/K)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}_F \Rightarrow (\mathfrak{p}, F/K)(\alpha)^{k'} \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}_L$$

b) $\Rightarrow$ a) $\phi_{F/K} : I_K(\mathfrak{m}) \to G_{F/K}$

$\phi_{F/K}(\ker(\Phi_{L/K})) = H \subset G_{F/K}$, and let $\tilde{L} = F^H$ fixed field of H

So $\tilde{L} \subset \mathfrak{m}$, and using a) $\Rightarrow$ b), we get

$$I_K(\mathfrak{m}) \xrightarrow{\phi_{\tilde{L}/K}} G_{\tilde{L}/K} \qquad \phi^{-1} \text{ — erase}$$

Kronecker-Weber

Thm. Let $L/\mathbb{Q}$ be abelian. Then $\exists\, n \in \mathbb{N}$ such that $L \subset \mathbb{Q}(\zeta_n)$

Pf. By Artin reciprocity, L has a modulus M with $\ker(\Phi_{L/\mathbb{Q}}) \supset P_{\mathbb{Q},1}(M)$

WLOG, write $M = n \cdot \infty$. But $\ker(\Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}) = P_{\mathbb{Q},1}(n \cdot \infty)$

Hence $\ker(\Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}) \subset \ker(\Phi_{L/\mathbb{Q}})$

Hence $\mathbb{Q}(\zeta_n) \supseteq L$.

In particular, $\forall\, p \in \mathbb{Z}$, $\exists\, n$ with $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_n)$.

Suffices to do $\mathbb{Q}(\sqrt{\pm p})$ p prime

$$\mathrm{Disc}(x^p - 1) = \prod_{\substack{\text{roots of} \\ x^p - 1}} p x^{p-1} = p^p \cdot \text{roots of unity}$$

$$= \prod_{\substack{0 \le i,j < p \\ i \neq j}} (\zeta_p^i - \zeta_p^j) = \left(\pm \prod_{0 \le i < j < p} (\zeta_p^i - \zeta_p^j) \right)^2 \in \mathbb{Q}(\zeta_p)$$

So $\exists\, A \in \mathbb{Q}(\zeta_p)$ with $A^2 = \pm p \left(p^{\frac{p-1}{2}}\right)^2$

Hence $\left(\frac{A}{p^{\frac{p-1}{2}}}\right)^2 = \pm p$, since $\sqrt{\pm p} \in \mathbb{Q}(\zeta_p)$,

Hence $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$

HW. $L/\mathbb{Q}$ abelian

let n = smallest integer with $L \subset \mathbb{Q}(\zeta_n)$

then $f(L/\mathbb{Q}) = \begin{cases} n & \text{if } \exists L \hookrightarrow \mathbb{R} \\ n \cdot \infty & \text{if } \nexists L \hookrightarrow \mathbb{R} \end{cases}$

Lecture 8 (2011-02-14)

Hilbert class field is the one with conductor $M=(1)$, i.e. 2011-2-14 (8)

$\exists!$ field K_H with $\ker(\phi_{K_H/H,(1)}) = P_K$

So $Cl_K = I_K/P_K \xrightarrow{\sim} G_{K_H/K}$

Prop. K_H is the maximal abelian unramified extension of K.

Pf. Let L/K be abelian unramified.

$$I_K \xrightarrow{\phi_{L/K,1}} G_{L/K}$$

$f(L/K)=(1)$, so $P_K \subset \ker(\phi_{L/K,1})$

because $\ker(\phi_{K_H/K,1}) \subseteq \ker(\phi_{L/K,1})$, we have $K_H \supseteq L$

Ray Class Field

Let M be a modulus. Then $\exists!$ abelian extension K_M/K such that $\ker(\phi_{K_M/K,M}) = P_{K,1}(M)$

$I_K(M)/P_{K,1}(M) \xrightarrow{\sim} Gal(K_M/K)$

K_M = ray class field of modulus M

HW: $K=\mathbb{Q}$, show $P_{\mathbb{Q},1}(2) = P_{\mathbb{Q},1}(2\cdot\infty)$

ray class field?

Example, $K = \mathbb{Q}$,

$M = (m) \rightsquigarrow \mathbb{Q}(\zeta_m + \zeta_m^{-1})$

$M = (m, \infty) \rightsquigarrow \mathbb{Q}(\zeta_m)$

HW, L/K abelian, show

$$\mathfrak{f}(L/K) = \gcd\{M : \ker(\Phi_{L/K}) \supseteq P_{K,1}(M)\}$$

L/K abelian, M DRP, and a congruence group for L/K, $\ker(\Phi_{L/K,M}) \supseteq P_{K,1}(M)$

$$\Phi_{L/K} : I_K(M) \to G_{L/K}$$

From before, $N_{L/K}(I_L(M)) \subseteq \ker(\Phi_{L/K,M})$

Thm: $\ker(\Phi_{L/K,M}) = N_{L/K}(I_L(M)) \cdot P_{K,1}(M)$

Local Fields

$K/\mathbb{Q}$, $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$, $K_\mathfrak{p}$

$$\mathcal{O}_\mathfrak{p} = \varprojlim \mathcal{O}_K/\mathfrak{p}^i = \{(\alpha_0, \alpha_1, \ldots) \mid \alpha_i \in \mathcal{O}_K/\mathfrak{p}^i, \ \alpha_i \equiv \alpha_{i-1} \bmod \mathfrak{p}^i\}$$

Fact: $\mathcal{O}_\mathfrak{p}$ is an integral domain

(the completed at a prime power, it actually be isomorphic)

#1: K_p = fraction field of $\mathcal{O}_p$

#2: $v_p : K^\times \to \mathbb{Z}$

$\alpha \mathcal{O}_K = \prod \mathfrak{p}^{v_\mathfrak{p}(\alpha)}$ $\quad v_\mathfrak{p}(0) = \infty$

$|\alpha|_\mathfrak{p} = \frac{1}{p^{v_\mathfrak{p}(\alpha)}}$, $p = \mathrm{char}(\mathcal{O}_K/\mathfrak{p})$

$|\ |$ is a non-archimedean absolute value

Thm (Ostrowski) Every absolute value on $\mathbb{Q}$ comes from p-adic or usual one.

If $K_\mathfrak{p}$ = completion, $\mathcal{O}_\mathfrak{p} = \{\alpha \in K_\mathfrak{p} \mid |\alpha| \leq 1\}$
$\mathfrak{m}_\mathfrak{p} = \{\alpha \in K_\mathfrak{p} \mid |\alpha| < 1\}$

"local field" will refer to a number field completed at a non-archimedean place

Extension fields K local field, $\mathcal{O}_K = \{|x| \leq 1\}$, $\mathfrak{p}_K = \{|x| < 1\}$

$\mathfrak{p}_K \mathcal{O}_L = \mathfrak{p}_L^{e(L/K)}$, $f(L/K) = [\mathcal{O}_L/\mathfrak{p}_L : \mathcal{O}_K/\mathfrak{p}_K)$

L/K unramified, i.e. $e(L/K)=1$, then

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(l_L/l_K) \cong \mathbb{Z}/f(L/K)\mathbb{Z}$$
$$x \mapsto x^{N\mathfrak{p}}$$

Thm. Unramified extensions are Galois,

$$\{L/K \text{ unramified}\} \longleftrightarrow \{\text{finite extensions } l'/l\}$$

K^{ur} = maximal unramified extension of K

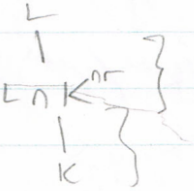
$$G(K^{ur}/K) = \varprojlim_{\rightarrow} G(L/K) \cong \varprojlim_{l'/l \text{ finite}} G(l'/l) = \widehat{\mathbb{Z}}$$

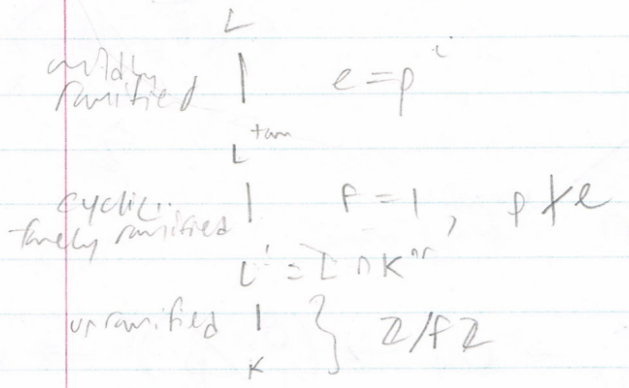
Lecture 9 (2011-02-16)

local field $K/\mathbb{Q}_p$, K^{nr} its maximal unramified extension 2011-2-16 (9)

$\mathrm{Gal}(K^{nr}/K) \cong \hat{\mathbb{Z}}$

Given L/K,





Thm, $K/\mathbb{Q}_p$, L/K abelian, then there is a natural isomorphism

$$(\cdot, L/K): K^*/N_{L/K}(L^*) \xrightarrow{\sim} G_{L/K}$$

↑ Main Thm of Local Class Field Theory

If L/K unramified, $G_{L/K} \cong \mathbb{Z}/f\mathbb{Z}$

Thm, $\{\text{finite abelian } L/K\} \leftrightarrow \{\text{open subgroups of } K^*\}$

$L \longrightarrow N_{L/K}(L^*)$

Thm. K^{ab} = max ab extension

$$1 \to O_K^\times \to K^\times \xrightarrow{v} \mathbb{Z} \to 0$$

$O_K^\times \to$ (local Artin map) $\to Gal(K^{ab}/K^{nr})$; $K^\times \to$ (local Artin map) $\to Gal(K^{ab}/K)$; $\mathbb{Z} \to$ (Frob) $\to Gal(K^{nr}/K)$

$$1 \to Gal(K^{ab}/K^{nr}) \to Gal(K^{ab}/K) \to Gal(K^{nr}/K) \to 0$$

$$Gal(K^{nr}/K) \cong Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}}, \quad x \mapsto x^{Np}$$

Def of $(\cdot, L/K)$ in global:

via global class field theory — group cohomology — Lubin-Tate formal groups

$$1 \to O_{K,1}^\times \to O_K^\times \to (O_K/p)^\times \to 1$$

$O_{K,1}^\times = \{\alpha \in O_K^\times \mid \alpha \equiv 1 \bmod p\}$

$(O_K/p)^\times$: cyclic of order prime to p

$\cong \mathbb{Z}/(Np-1)\mathbb{Z}$

$$\begin{array}{ccccccccc} 1 & \to & O_{K,1}^\times & \to & O_K^\times & \to & (O_K/p)^\times & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & Gal(K^{ab}/K^{tame}) & \to & Gal(K^{ab}/K^{nr}) & \to & Gal(K^{tame}/K^{nr}) & \to & 1 \end{array}$$

So what does $O_{K,1}^\times$ look like? Note $\mathbb{R}^\times \cong \mathbb{R}^+ \times \ldots$ by log

"p-adic Lie group"

$O_{K,1}^\times \cong p^+$ (divisible by p, less small)

$$\alpha \mapsto \log(\alpha) = \log(1 + (\alpha - 1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(\alpha-1)^n}{n!}$$

Lemma $K/\mathbb{Q}_p$, $a_n, b_n \in \mathcal{O}_K$, i.e. $|a_n|, |b_n| \leq 1$

a) $\sum a_n \frac{x^n}{n}$ converges $\forall\, |x| < 1$, i.e. $v(x) > 0$

b) $\sum b_n \frac{x^n}{n!}$ converges $\forall$, $v(x) > \frac{e(K/\mathbb{Q}_p)}{p-1}$

If, Converges $\Leftrightarrow$ n^{th} term $\to 0$ $\Leftrightarrow$ $v(n^{th}\text{ term}) \to \infty$

a) $v\left(a_n \frac{x^n}{n}\right) = n v(x) - v(n) \geq n v(x) -$

b) $v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{n}{p-1}$ $\qquad e(K/\mathbb{Q}_p)$

$v(x) > \frac{v(p)}{p-1}$

Prop Let $r > \frac{e(K/\mathbb{Q}_p)}{p-1}$. Then there are isomorphisms

$$(\mathfrak{p}^r, +) \rightleftarrows (1+\mathfrak{p}^r, \cdot)$$

$$x \longmapsto \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

$$\sum_{n=1}^{\infty} (-1)^{n+1} \frac{(y-1)^n}{n} \longleftarrow y$$

Corollary: $\mathcal{O}_{K,1}^{\times}$ has a subgroup of finite index that is isomorphic to $(\mathfrak{p}^r, +)$

$$(\mathfrak{p}, +) \hookrightarrow (1+\mathfrak{p}\mathbb{Z}_p, \cdot)$$

Lecture 10 (2011-02-18)

Adeles + Ideles

2011-2-18

(10)

$K/\mathbb{Q}$ number field

$M_K = M_K^\circ \cup M_K^\infty$

absolute values on K

M_K° = non archimedian = primes $\mathfrak{p}$

M_K^∞ = $K \hookrightarrow \mathbb{R}$ or pairs of $K \hookrightarrow \mathbb{C}$

$$\mathcal{O}_K \hookrightarrow \prod_{v \in M_K^\infty} K_v \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

$$\mathcal{O}_{K,S} \hookrightarrow \prod_{v \in S} K_v$$ ⇝ suggests $K \hookrightarrow \prod_{v \in M_K} K_v$

Ring of adeles of $K = \mathbb{A}_K$

$$\mathbb{A}_K = \left\{ \alpha = (\alpha_v)_{v \in M_K} \in \prod_{v \in M_K} K_v \;\middle|\; \alpha_v \in \mathcal{O}_v \text{ for all but finitely many } v \right\}$$

(define $\mathcal{O}_v = K_v$ if $v \in M_K^\infty$)

define ideles $\mathbb{I}_K = \mathbb{A}_K^\times$

$$\mathbb{I}_K = \left\{ \alpha \in \prod_{v \in M_K} K_v^\times \;\middle|\; \alpha_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}$$

Note that we get $K \hookrightarrow \mathbb{A}_K$

$K^\times \hookrightarrow \mathbb{I}_K$

If $(X_i)_{i \in I}$ are topological spaces,

$X = \prod X_i$ is a topological space, base of open sets is $\prod_{i \in J} U_i \times \prod_{i \in I \setminus J} X_i$

Typical open set in $\mathbb{A}_K$

$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_v$ (S finite, U_v open in K_v)

topology on $\mathbb{I}_K \neq$ subspace topology from $\mathbb{A}_K$

In general, if R is a topological ring, then $R^\times$ is a topological group, with topology induced by

$$R^\times \hookrightarrow R \times R$$
$$a \longmapsto (a, a^{-1})$$

Distances in $\mathbb{I}_K$: $\alpha = (\alpha_v) \in \mathbb{I}_K$, define

$$\|\alpha\| = \prod_{v \in M_K} |\alpha_v|_v$$

Prop. $K \hookrightarrow \mathbb{A}_K$, $K^\times \hookrightarrow \mathbb{A}_K^\times$ are discrete subgroups

Pf idea, Suppose $\alpha_i \in K$, $\alpha_i \to 0$ as elements of $\mathbb{A}_K$.

$\alpha_i = (\alpha_i, \alpha_i, \dots)$ $\quad 0 = (0, 0, \dots)$

For any finite $S \subset M_K$ and any $\varepsilon > 0$,

$\exists\, i$ such that $|\alpha_i|_v < \varepsilon$ for all $v \in S$

$|\alpha_i|_v \leq 1$ for all v

for example, let $S = M_K^\infty$, $\varepsilon = \frac{1}{2}$

$|\alpha_i|_v < \frac{1}{2}$, $|\alpha_i|_v \leq 1$ for $v \in M_K^0$
for $v \in M_K^\infty$

$1 = \prod_{v \in M_K} |\alpha_i|_v < \frac{1}{2}$

unless $\alpha = 0$

Refine $\mathbb{A}_{K,S} = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$

$\mathbb{A}_{K,S}^\times = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times$

Thm: $\mathbb{A}_K = K + \mathbb{A}_{K, M_K^\infty}$, and $\mathbb{A}_K / K$ is compact,

where $\prod_{v \in M_K^\infty} \{\alpha \in K_v \mid |\alpha|_v \leq B\} \times \prod_{v \in M_K^0} \mathcal{O}_v \longrightarrow \mathbb{A}_K / K$ (continuous surjection)

↑ finitely many open sets

$\| \ \| : \mathbb{A}_K^\times \to \mathbb{R}_{>0}^\times$ is a continuous homomorphism

$\alpha \mapsto \prod_{v \in M_K} |\alpha_v|_v$

Also have $\mathbb{A}_K^\times \twoheadrightarrow I_K$

$\alpha = (\alpha_v)_{v \in M_K} \mapsto \prod_{v \in M_K^\circ} \pi_v^{\mathrm{ord}_v(\alpha_v)}$

Denote this by $\alpha \mathcal{O}_K$. If $\alpha \in K^\times$, this notation is consistent.

The kernel of this map is

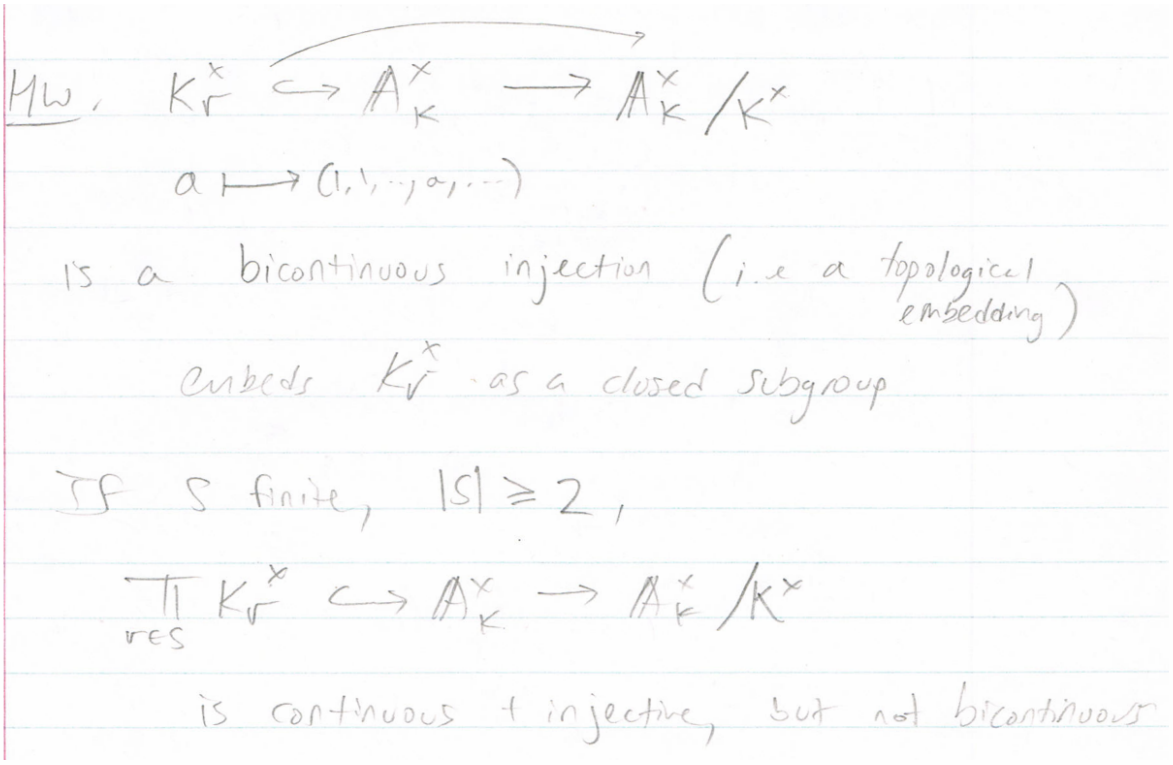
$$\prod_{v \in M_K^\infty} K_v^\times \times \prod_{v \in M_K^\circ} \mathcal{O}_v^\times = \mathbb{A}_{K, M_K^\infty}^\times$$

$\mathbb{A}_K^\times / \mathbb{A}_{K, M_K^\infty}^\times \xrightarrow{\sim} I_K$, hence

$\mathbb{A}_K^\times / K^\times \mathbb{A}_{K, M_K^\infty}^\times \xrightarrow{\sim} I_K / (K^\times) = Cl_K$

$\exists$ finite $S \subset M_K$ so that

$\mathbb{A}_K^\times = K^\times \mathbb{A}_{K,S}^\times$ – choose S so that the primes $\mathfrak{p}$ in S cover Cl_K.


Hw. $K_v^\times \hookrightarrow \mathbb{A}_K^\times \to \mathbb{A}_K^\times / K^\times$
$a \mapsto (1, 1, \ldots, a, \ldots)$
is a bicontinuous injection (i.e a topological embedding)
embeds $K_v^\times$ as a closed subgroup
If S finite, $|S| \geq 2$,
$\prod_{v \in S} K_v^\times \hookrightarrow \mathbb{A}_K^\times \to \mathbb{A}_K^\times / K^\times$
is continuous + injective, but not bicontinuous

Lecture 11 (2011-02-23)

Main Theorem of Class Field Theory 2011-2-23 (11)

$K/\mathbb{Q}$, K^{ab} = maximal abelian extension of K

Then there exists a unique continuous homomorphism

$$[\cdot, K] : \mathbb{A}_K^\times \longrightarrow \mathrm{Gal}(K^{ab}/K) = \varprojlim_{L/K \text{ finite ab}} \mathrm{Gal}(L/K)$$

such that: (K^{ab} built out of finite abelian extensions, so enough to specify on fin)

Let L/K be a finite abelian extension.

(1) If $\alpha \in \mathbb{A}_K^\times$ satisfies $a_v \in \mathcal{O}_v$ for all v, $\alpha_v = 1$ for all v that ramify in L

Then $[\alpha, K]|_L = (\alpha \mathcal{O}_K, L/K)$

(2) If $\alpha \in K^\times$, then $[\alpha, K] = 1$.

(5) $[\cdot, K]$ is surjective

(3) Let L/K abelian extension, $\beta \in \mathbb{A}_L^\times$

$$[\beta, L]|_{K^{ab}} = [N_{L/K}(\beta), K]$$

L^{ab} not necessary K^{ab}

Def. $N_{L/K} : \mathbb{A}_L^\times \to \mathbb{A}_K^\times$, $\beta \mapsto$

(4) $K_v^\times \hookrightarrow \mathbb{A}_K^\times$

$c \mapsto (1, 1, \ldots, c, 1, \ldots)$

Let $v \in M_K$. Then

$$(N_{L/K}(\beta))_v = \prod_{\substack{w \in M_L \\ w|v}} N_{L_w/K_v}(\beta_w)$$

$[\mathcal{O}_v^\times, K]$ = inertia group of v in $\mathrm{Gal}(K^{ab}/K)$

Example: If v is unramified, $c \in K_v^\times \subset \mathbb{A}_K^\times$

$$[c, K]\big|_L = [(1,1,\dots,c,1,\dots), K]\big|_L = \mathrm{Frob}_v^{\mathrm{ord}_v(c)} \in \mathrm{Gal}(L/K)$$

Let $\mathfrak{m}$ be a modulus for K.

Def. $U_{\mathfrak{m}} = \{\alpha \in \mathbb{A}_K^\times \mid \alpha_v \in$

- Computing $[\alpha, K]\big|_L$ for some finite abelian L/K

we want to get it into the form of (1).

Given $\alpha \in \mathbb{A}_K^\times$, find some $c \in K^\times$ such that

$c\alpha_v \in \mathcal{O}_v$ for all v

Pick a modulus $\mathfrak{M}$ for L/K; for ramified primes $v \mid \mathfrak{m}$,

require $c\alpha_v \equiv 1 \bmod \mathfrak{M}\mathcal{O}_v$

(If $\mathrm{ord}_v(\alpha_v) \neq 0$, first divide α by some $a \in K^\times$ to make $\mathrm{ord}_v(a^{-1}\alpha) = 0$)

Because $[\cdot, K)$ doesn't see $K^\times$,

$$[\alpha, K]_L = [c\alpha, K]_L = (c\alpha\mathcal{O}_K, L/K)$$

Example $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_{p^n})$

$\alpha = (1, \ldots 1, \underset{\uparrow}{a}, 1, \ldots 1) \quad a \in \mathbb{Z}_p^*$

$\mathbb{Q}_p$

$(c, \ldots c, ca, c, \ldots c)$

Choose $c \in \mathbb{Z}$ with $ca \equiv 1 \bmod p^n \cdot \infty$

$c \in \mathbb{Z} \quad c > 0 \quad c \equiv a^{-1} \bmod p^n$

$$[\alpha, K]|_L = [c\alpha, K]|_L = (c\alpha\mathcal{O}_K, L/K) = \prod_{\text{prime } q \nmid c} \text{Frob}_q^{\text{ord}_q(c)}$$

$\mathcal{O}_K = \mathbb{Z}$

$$[\alpha, \mathbb{Q}](\zeta_{p^n}) = \zeta_{p^n}^{c} = \zeta_{p^n}^{a^{-1}}$$

HW $\alpha = (1, 1, \ldots \underset{\uparrow}{p^i}, 1, \ldots)$ Show $[\alpha, \mathbb{Q}]|_{\mathbb{Q}(\zeta_{p^n})} = 1$

$\mathbb{Q}_p$ spot

$\beta = (1, 1, \ldots, -p^i, \ldots)$, evaluate $[\beta, \mathbb{Q}]|_{\mathbb{Q}(\zeta_{p^n})}$.

Lecture 12 (2011-02-25)

$\mu_n \subset K$, $\alpha \in \mathcal{O}_K$, $\mathfrak{p} \nmid n\alpha$ 2011-2-25 (12)

n^{th} order residue symbol

$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \in \mu_n$ such that $\alpha^{\frac{N\mathfrak{p}-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \bmod \mathfrak{p}$

If $\mathfrak{a} = \prod \mathfrak{p}_i$, $\left(\frac{\alpha}{\mathfrak{a}}\right)_n = \prod \left(\frac{\alpha}{\mathfrak{p}_i}\right)_n$

$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m}) \to \mu_n$ homomorphism (when $n\alpha \mid \mathfrak{m}$)

For a Kummer extension,

$$\mathrm{Gal}(K(\sqrt[n]{\alpha})/K) \hookrightarrow \mu_n$$
$$\sigma \mapsto \zeta_\sigma = \frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}}$$

Prop. $\mu_n \subset K$, $L = K(\sqrt[n]{\alpha})$, $\alpha \in \mathcal{O}_K \setminus \{0\}$

Choose a modulus $\mathfrak{m}$ such that
1. Every $\mathfrak{p} \mid n\alpha$ has $\mathfrak{p} \mid \mathfrak{m}$
2. $\ker(\Phi_{L/K,\mathfrak{m}}) \supset P_{K,1}(\mathfrak{m})$, i.e. $\mathfrak{m}$ is a modulus for L/K – can always make a modulus bigger, so 1 is ok

exists by Artin reciprocity →

Then $I_K(\mathfrak{m}) \xrightarrow{\Phi_{L/K,\mathfrak{m}}} G_{L/K}$

$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m}) \to \mu_n$, $\sigma \mapsto \zeta_\sigma$

commutes, as .

$\left(\frac{\alpha}{\cdot}\right)_n : \frac{I_K(m)}{P_{K,1}(m)} \xrightarrow{\text{onto}} \text{Image}\left(G_{L/K} \to \mu_n\right)$

$(\mathfrak{P}, L/K)(\sqrt[n]{\alpha}) \equiv (\sqrt[n]{\alpha})^{N\mathfrak{p}} \bmod \mathfrak{P}$ $\quad \mathfrak{P}$ lies above $\mathfrak{p}$

by def of Frobenius

$\equiv \alpha^{\frac{N\mathfrak{p}-1}{n}} \sqrt[n]{\alpha} \bmod \mathfrak{P} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \sqrt[n]{\alpha} \bmod \mathfrak{P}$

so $\frac{(\mathfrak{P}, L/K)(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \bmod \mathfrak{P}$

but n^{th} roots stay distinct, so $(\mathfrak{P}, L/K)(\sqrt[n]{\alpha}) = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \sqrt[n]{\alpha}$

Second statement follows from the fact that $\Phi_{L/K,\mathfrak{m}}$ is surjective.

Prop. $p, q \in \mathbb{Z}$ odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Pf. Let $p^* = (-1)^{\frac{p-1}{2}} p$. We know $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

so equivalently we want to prove $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$

$\frac{I_{\mathbb{Q}}(p \cdot \infty)}{P_{\mathbb{Q},1}(p \cdot \infty)} \xrightarrow{\Phi_{\mathbb{Q}(\zeta_p)/\mathbb{Q}, p\cdot\infty}} \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$

For any subfield $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_p)$, we also get

$$I_{\mathbb{Q}}(p,\infty) / P_{\mathbb{Q},1}(p,\infty) \xrightarrow{\bar{\Phi}_{K,p,\infty}} Gal(K/\mathbb{Q})$$

$Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, cyclic order $p-1$

Hence unique subfield $K \subseteq \mathbb{Q}(\zeta_p)$ with $[K:\mathbb{Q}] = 2$

The only (finite) prime K can be ramified at is p

Hence $K = \mathbb{Q}(\sqrt{p^*})$.

$$(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} I_{\mathbb{Q}}(p,\infty)/P_{\mathbb{Q},1}(p,\infty) \xrightarrow[\text{onto}]{\left(\frac{p^*}{\cdot}\right)} \text{Image}\left(Gal(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) \to \mu_2\right) \subseteq \mu_2$$

$a \bmod p \mapsto a\mathbb{Z}$

So $a \longmapsto \left(\frac{p^*}{a}\right)$ is a surjective homomorphism from

$$(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mu_2$$

but $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, so there is only one such.

But $a \longmapsto \left(\frac{a}{p}\right)$ is also a surjective homomorphism

so they are the same

$\left(\frac{\Pi}{\eta}\right)_n$ depends only on $\prod_{p \mid n} p$ Π and η

Group Cohomology

G a finite group, M a G-module

$\mathbb{Z}[G] = \left\{ \sum_{\sigma \in G} n_\sigma \cdot \sigma \;\middle|\; n_\sigma \in \mathbb{Z},\ n_\sigma = 0 \text{ for all but finitely many } \sigma \right\}$

group ring

$$\left(\sum n_\sigma \sigma\right)\left(\sum n_\tau \tau\right) = \sum_{\sigma,\tau} n_\sigma n_\tau \sigma\tau$$

group ring is non-commutative if G is

M is really a (left) $\mathbb{Z}[G]$-module

$$\left(\sum n_\sigma \sigma\right)(x) = \sum n_\sigma \sigma(x)$$

Examples L/K, $G = \mathrm{Gal}(L/K)$ acts on $L^+, L^\times$

$(\sigma - 1)(x) = \sigma(x) - x \qquad (\sigma - 1)(x) = \frac{\sigma(x)}{x}$

Basic object of study: $M^G = \{ x \in M \mid \sigma(x) = x \text{ for all } \sigma \in G \}$

Example G is cyclic, say $G = \langle \sigma \rangle$

$M^G = \{ x \in M \mid \sigma(x) = x \} = \ker\left((\sigma - 1) : M \to M \right)$

$(\sigma - 1)(x) = 0$

Prop. Let $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$ be an exact sequence of G-modules, where α and β are G-module morphisms (commute with G-action)

Then $0 \to M^G \to N^G \to P^G$ is exact

$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) = M^G$ right adjoint

($\mathbb{Z}$: trivial action)

Lecture 13 (2011-02-28)

Let $L/K/\mathbb{Q}_p$ be a Galois extension of p-adic fields 2011-2-28 (13)

$$1 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{\text{ord}_L} \mathbb{Z} \to 1$$

take fixed elements

$$1 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{\text{ord}_L} \mathbb{Z} \to \mathbb{Z}/e(L/K)\mathbb{Z} \to 1$$

$\| e(L/K)\,\text{ord}_L$

exact $\Leftrightarrow$ unramified

M, N G-modules, then $\text{Hom}_G(M,N) = \text{Hom}_{\mathbb{Z}}(M,N)^G$

where $\text{Hom}_{\mathbb{Z}}(M,N)$ is a G-module by $\sigma \cdot f = \sigma \circ f \circ \sigma^{-1}$

(this is equivalent to requiring $\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ M & \xrightarrow{f} & N \end{array}$ commute)

In particular $\text{Hom}_G(\mathbb{Z}, M) = M^G$, since $\sigma f(\sigma^{-1}(a)) = f(a)$ $\forall a \in M$

implies $f(1) = \sigma(f(1))$

Def A co-induced G-module is one of the form

$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$ where A is an abelian group with trivial G-action

Notation $M^G = \Gamma(G, M) = H^0(G, M)$

possible to use a classifying space for group G, make this sheaf notation rigorous

Thm. There are abelian groups $H^q(G,M)$, $q \geq 0$ and, for each exact sequence $0 \to M \to N \to P \to 0$, connecting homomorphisms $H^q(G,P) \xrightarrow{\delta} H^{q+1}(G,M)$, functorial on exact sequences, such that

(1) $0 \to H^0(G,M) \to H^0(G,N) \to H^0(G,P) \xrightarrow{\delta} H^1(G,M) \to \cdots$ is exact

and (2) if M is coinduced, then $H^q(G,M) = 0$ for $q \geq 1$.

$H^q(G,M)$ is "unique".

Pf. $M \rightsquigarrow M^G = \mathrm{Hom}_G(\mathbb{Z}, M)$

Take a resolution $\cdots \to F_2 \to F_1 \to F_0 \to \mathbb{Z} \to 0$

where F_i are free $\mathbb{Z}$-modules, and apply $\mathrm{Hom}_G(\cdot, M)$

get a complex (toss out $\mathbb{Z}$)

C^M: $0 \to \mathrm{Hom}_G(F_0, M) \to \mathrm{Hom}_G(F_1, M) \to \cdots$

$H^q(G,M) = q^{th}$ cohomology of C^M =

$$\frac{\ker\left(\mathrm{Hom}_G(F_q, M) \to \mathrm{Hom}_G(F_{q+1}, M)\right)}{\mathrm{im}\left(\mathrm{Hom}_G(F_{q-1}, M) \to \mathrm{Hom}_G(F_q, M)\right)}$$

Abstract nonsense ⇒ long exact sequence

Check $H^0(G,M) = \dfrac{\ker(\mathrm{Hom}_G(F_0,M) \to \mathrm{Hom}_G(F_1,M))}{\mathrm{Im}(0 \to \mathrm{Hom}_G(F_0,M))}$

and $\to F_1 \to F_0 \to \mathbb{Z} \to 0$ exact, so

$0 \to \mathrm{Hom}_G(\mathbb{Z},M) \to \mathrm{Hom}_G(F_0,M) \to \mathrm{Hom}_G(F_1,M)$ exact,

so $\mathrm{Hom}_G(\mathbb{Z},M) = M^G = \ker(\mathrm{Hom}_G(F_0,M) \to \mathrm{Hom}_G(F_1,M))$

so $H^0(G,M) = M^G$

(2) coinduced ⇒ trivial cohomology

Let $M = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$, let N be any G-module.

$\mathrm{Hom}_G(N,M) = \mathrm{Hom}_G(N, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],A))$

ϕ ↘ ↗ $(n \mapsto (\sigma \mapsto \psi(\sigma(n))))$

$\mathrm{Hom}_{\mathbb{Z}}(N,A)$ ψ

$(n \mapsto \phi(n)(e_G))$

so $\mathrm{Hom}_G(N,M) = \mathrm{Hom}_{\mathbb{Z}}(N,A)$, so on $\to F_1 \to F_0 \to \mathbb{Z} \to 0$,

since the F_i are free abelian groups, $F_i \cong_{\mathbb{Z}} \mathbb{Z}^{n_i}$,

$\mathrm{Hom}_G(F_i,M) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{n_i},A) = A^{n_i}$, so the complex is exact,

so cohomology is trivial

For uniqueness: Use $M \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)$

who knows?

$$0 \to M \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M) \to M' \to 0 \qquad m \mapsto (\sigma \mapsto \sigma(m))$$

$$H^q(G, M') \overset{\delta}{\cong} H^{q+1}(G, M) \quad \text{for } q \geq 1$$

because $H^q(G, \text{coinduced}) \to H^q(G, M') \to H^{q+1}(G, M) \to H^{q+1}(G, \text{coinduced})$

$H^q(G, \text{coinduced}) = 0$ and $H^{q+1}(G, \text{coinduced}) = 0$

"dimension shifting"

Def. $Z^1(G, M) = \{f : G \to M \mid f(\sigma\tau) = f(\sigma) + \sigma f(\tau)\}$

the 1-cocycles

the 1-coboundaries

$$B^1(G, M) = \{f : G \to M \mid \exists\, m \in M \text{ such that } f(\sigma) = \sigma(m) - m\}$$

check that $B^1(G, M) \subset Z^1(G, M)$

We have $H^1(G, M) = \dfrac{Z^1(G, M)}{B^1(G, M)}$.

given $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$ we get

$$0 \to M^G \to N^G \to P^G \xrightarrow{\delta} H^1(G, M) \to \cdots$$

Let $p \in P^G$, choose $n \in N$ with $\beta(n) = p$. Construct

$$G \to N$$
$$\sigma \mapsto (\sigma(n) - n)$$

$\sigma(\eta) - \eta$ is actually in M: since

$$\beta(\sigma(\eta) - \eta) = \sigma(\beta(\eta)) - \beta(\eta) = \sigma(\rho) - \rho = 0$$

so get in fact $G \to M$

$$\sigma \mapsto \alpha^{-1}(\sigma(\eta) - \eta)$$

Hilbert 90: $H^1(G_{L/K}, L^\times) = 0$

Lecture 14 (2011-03-02)

Standard complex 2011-3-2 (14)

$F_i = \mathbb{Z}[G^{i+1}]$ $(\sigma\tau_0, \ldots, \sigma\tau_i) = \sigma(\tau_0, \ldots, \tau_i)$

$\cdots \to F_1 \to F_0 \to \mathbb{Z} \to 0$

$\mathbb{Z}[G]$

$\sum n_\sigma \cdot \sigma \to \sum n_\sigma$

$F_i \cong \mathbb{Z}[G]^i$ as $\mathbb{Z}[G]^{i+1}$

$F_i \to F_{i-1}$ by $d(\tau_0, \ldots, \tau_i) = \sum_{j=0}^{i} (-1)^j (\tau_0, \ldots, \widehat{\tau_j}, \ldots \tau_i)$

HW. Prove exactness

Hint. Fix $\sigma \in G$, let $h_\sigma : F_{i-1} \to F_i$ $(\tau_0, \ldots, \tau_{i-1}) \mapsto (\sigma, \tau_0, \ldots, \tau_{i-1})$

Show $d \circ h_\sigma + h_\sigma \circ d = 1$

Can use to compute $H^i(G, M)$. Look at $f \in \mathrm{Hom}_G(F_i, M)$,

a G-module homomorphism $f : \mathbb{Z}[G^{i+1}] \to M$

Notice $f(\tau_0, \ldots, \tau_i) = \tau_0 (1, \tau_0^{-1}\tau_1, \ldots, \tau_0^{-1}\tau_i)$

f corresponds to a map $\phi : G^{i+1} \to M$ by setting

$\phi(\tau_1, \ldots, \tau_i) = f(1, \tau_1, \tau_1\tau_2, \ldots, \tau_1 \ldots \tau_i)$

$d\phi : G^{i+1} \to M$ $\quad$ ϕ is a cocycle $\Leftrightarrow d\phi = 0$

$$d\phi(\tau_1, \dots, \tau_{i+1}) = \tau_1 \phi(\tau_2, \dots, \tau_{i+1}) + \sum_{j=1}^{i} (-1)^j \phi(\tau_1, \dots, \tau_{j-1}, \tau_j \tau_{j+1}, \tau_{j+2}, \dots, \tau_{i+1}) + (-1)^{i+1} \phi(\tau_1, \dots, \tau_i)$$

1-cocycle: $\phi : G \to M$

$$0 = d\phi(\sigma, \tau) = \sigma\phi(\tau) - \phi(\sigma\tau) + \phi(\sigma)$$

i.e. $\phi(\sigma\tau) = \sigma\phi(\tau) + \phi(\sigma)$

$0 \to C \xrightarrow{\alpha} \square \underset{\gamma}{\overset{\beta}{\rightleftarrows}} A$ $\quad$ $H^2(A, C)$ classifies extensions

γ is a homomorphism iff $\gamma(x+y) - \gamma(x) - \gamma(y) = 0$

$H \subset G$ subgroup, get $H^i(G, M) \to H^i(H, M)$

$H \lhd G$, then take $(G/H)^i \to M^H$ to

$G^i \to (G/H)^i \to M^H \hookrightarrow M$

inflation – restriction

Thm. There is an exact sequence

$$0 \to H^1(G/H, M^H) \xrightarrow[i]{\inf} H^1(G, M) \xrightarrow[r]{\text{res}} H^1(H, M)$$

Pf. i injective $\quad G/H \xrightarrow{e} M^H$, call the map

$G \to G/H \xrightarrow{e} M^H \hookrightarrow M$, $\quad$ Suppose $i(c)$ is a coboundary, i.e. $\exists\, m \in M$ such that $i(c)(\sigma) = \sigma(m) - m \;\forall \sigma \in G$

Notice that this only depends on $\sigma \bmod H$

$r \circ i = 0$ because $H \to G \to G/H \xrightarrow{e} M^H \to M$ (the composite $H \to G \to M$ is $i(c)$)

$\ker(r) \subseteq \operatorname{im}(i)$ Let $c \in \ker(r)$,

$H \hookrightarrow G \xrightarrow{c} M \quad r(c) =$ coboundary

$\exists$ an $m \in M$ such that $r(c)(\sigma) = \sigma(m) - m \;\forall \sigma \in H$

Replace c by $c' : G \to M$, $c'(\sigma) = c(\sigma) - (\sigma(m) - m)$

Changed c by a $G \to M$ 1-coboundary. Now $c'(\sigma) = 0 \;\forall \sigma \in H$

Recall $G/H \to M$. Let $\gamma \in H$, $\sigma \in G$.

$\sigma H \mapsto c'(\sigma)$

$c'(\sigma\gamma) = \sigma c'(\gamma) + c'(\sigma)$ ← 1-cocycle condition

This shows $c'(\sigma H)$ is well-defined

Claim: Image $(c') \subset M^H$.

Let $\gamma \in H$, $\sigma \in G$. $\gamma \cdot c'(\sigma) = c'(\gamma\sigma) - c'(\gamma)$

$c'(H\sigma) = c'(\sigma)$

$0 \to H^1(G/H, M^H) \xrightarrow{\inf} H^1(G, M) \xrightarrow{\text{res}} H^1(H, M)^{G/H} \to$

$H^2(G/H, M^H) \to H^2(G, M)$

Spectral sequence

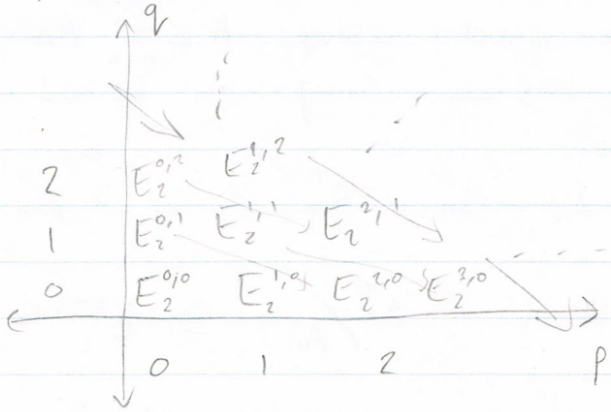
Aim: Show G/H acts on $H^1(H, M)$,

Show image of restriction is inside $H^1(H, M)^{G/H}$

Lecture 15 (2011-03-04)

Spectral Sequences 2011-3-4 (15)

$(E_2^{p,q})$



For the spectral sequences we'll be looking at, all other quadrants are 0.

$$E_2^{p,q} \xrightarrow{\delta_2^{p,q}} E_2^{p+2,q-1} \qquad \delta^{p+2,q-1} \circ \delta^{p,q} = 0$$

for level 2, we have "over 2, down 1"

define $(E_3^{p,q})$ by

$$E_3^{p,q} = \frac{\ker(\delta_2^{p,q})}{\operatorname{im}(\delta_2^{p+2,q-1})} \quad \text{and}$$

$$\delta_3^{p,q} : E_3^{p,q} \to E_3^{p+3,q-2}$$

Continuing, get $(E_r^{p,q})$ and $\delta_r^{p,q}$ for $r = 2,3,4,\dots$

For a given p,q, $E_r^{p,q}$ eventually stabilizies (when the maps into and out of $E_r^{p,q}$ land in the 0 quadrants), call this $E_\infty^{p,q}$

$r > \max(p, q+1)$

Def. The spectral sequence $(E_2^{p,q})$ converges to the graded group $A = \bigoplus_{n=0}^{\infty} A_n$ such that A_n has a composition series (as an abelian group)

$$A_n = A_n^n \supset A_n^{n-1} \supset \cdots \supset A_n^0 \supset 0$$

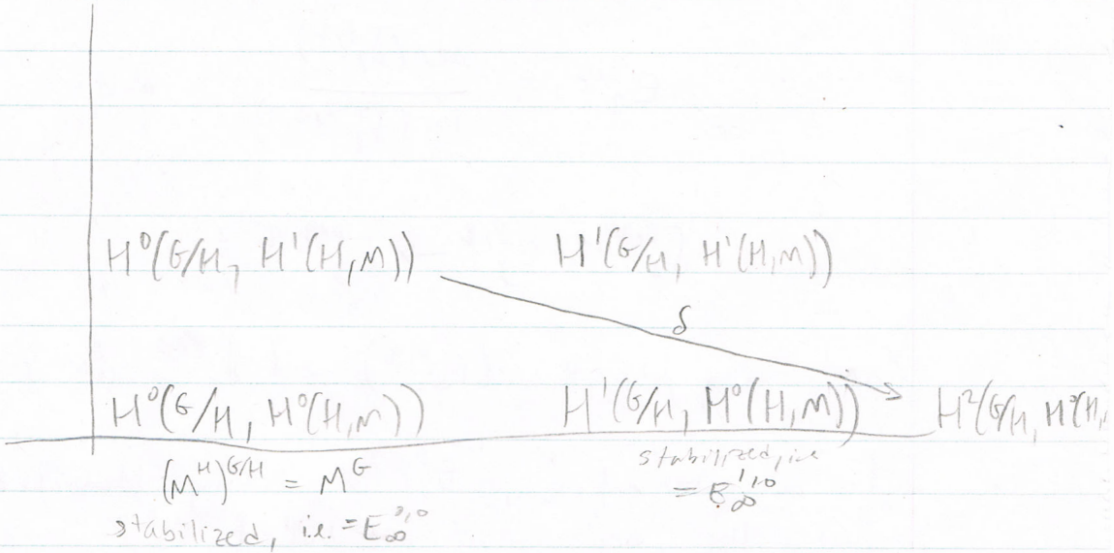
such that $A_n^q / A_n^{q-1} \cong E_2^{n-q,q}$ (?)

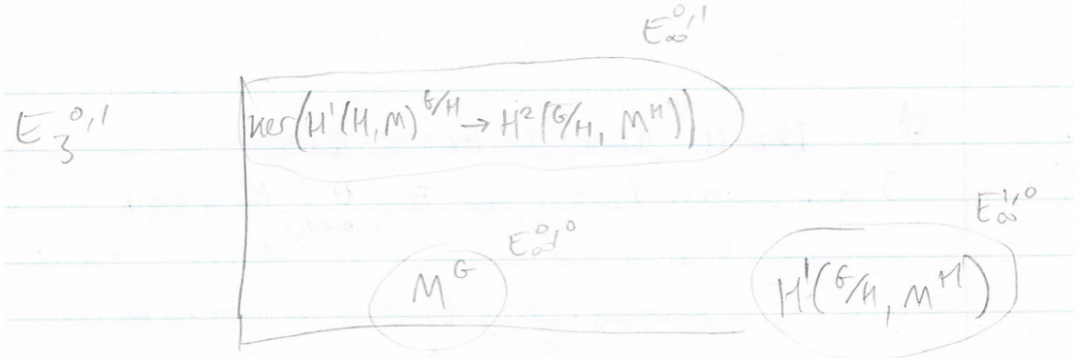
Serre–Hochschild Spectral Sequence

$$E_2^{p,q} = H^p(G/H, H^q(H,M))$$

$E_2^{p,q} \xrightarrow{\delta} E_2^{p+2,q-1}$ messy to write down

$$\boxed{H^p(G/H, H^q(H,M)) \Rightarrow \bigoplus_{n=0}^{\infty} H^n(G,M)}$$





$H^0(G,M) = E_\infty^{0,0} = M^G$ ✓

We need to have a composition series of length 2,

$$H^1(G,M) \supset A \supset 0,$$

with $H^1(G,M)/A = E_\infty^{0,1}$ $A = E_\infty^{1,0}$

$$0 \to A \to H^1(G,M) \to H^1(G,M)/A \to 0$$

$$A = E_\infty^{1,0} = H^1(G/H, M^H), \qquad H^1(G,M)/A = E_\infty^{0,1} = \ker(H^1(H,M)^{G/H} \to H^2(G/H, M^H))$$

(inf, res)

Leray spectral sequence

$X \xrightarrow{f} S$ fiber space, $f^{-1}(s) \cong F$

$$H^p(S, H^q(F,R)) \Rightarrow H^{p+q}(X)$$

Thm L/K Galois extension of fields, then
$H^q(\mathrm{Gal}(L/K), L^\times) = 0$

Pf. Recall normal basis thm.

$\exists \alpha \in L$ such that $L = \bigoplus_{\sigma \in G(L/K)} K \cdot \sigma(\alpha)$

$L^+ = \mathbb{Z}[\mathrm{Gal}(L/K)] \otimes_{\mathbb{Z}} K^+ \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\mathrm{Gal}(L/K)], K^+)$

So L^+ is coinduced

HW: G finite group A abelian group, trivial G-action

$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$

$f \longmapsto \sum_{\sigma \in G} \sigma \otimes f(\sigma)$

Lecture 16 (2011-03-07)

Hilbert Theorem 90 L/K finite Galois, then 2011-3-7 (16)

$$H^1(G_{L/K}, L^\times) = 0$$

Lemma (Independence of characters)
Let $\chi_1, \dots, \chi_n : G \to L^\times$ be distinct characters
Then $\sum_{i=1}^{n} c_i \chi_i = 0 \Rightarrow c_1 = \cdots = c_n = 0$.

Pf. Suppose $\sum_{i=1}^{n} c_i \chi_i = 0$ is a minimal equation of dependency.

$n=1$: $c\chi = 0$, but $\chi(1) = 1$, so $c = 0$.
$n \geq 2$: Fix $\tau \in G$, Then $\forall \sigma \in G$,

$$\sum_{i=1}^{n} c_i \chi_i(\tau\sigma) = 0$$

$$c_1 \chi_1(\tau)\chi_1(\sigma) + \sum_{i=2}^{n} c_i \chi_i(\tau)\chi_i(\sigma) = 0$$

$$c_1 \chi_1(\tau)\chi_1(\sigma) + \sum_{i=2}^{n} c_i \chi_1(\tau)\chi_i(\sigma) = 0$$

$$\sum_{i=2}^{n} c_i (\chi_i(\tau) - \chi_1(\tau))\chi_i(\sigma) = 0 \quad \forall \sigma$$

other

Pf. $\sigma \in G_{L/K}$, $\sigma : L^\times \to L^\times$ let χ_σ be σ considered as a character, $\chi_\sigma(\alpha) = \sigma(\alpha)$.

Let $c : G_{L/K} \to L^\times$ be a 1-cocycle, look at
(distinct characters)

$$\sum_{\sigma \in G_{L/K}} c_\sigma \chi_\sigma$$

(non-zero since in $L^\times$)

By independence of characters, $\sum c_\sigma \chi_\sigma \neq 0$

So $\exists \alpha \in L$ such that $\beta = \sum_{\sigma \in G_{L/K}} c_\sigma \chi_\sigma(\alpha) \neq 0$

Let $\gamma \in G_{L/K}$. Compute

$$\gamma(\beta) = \sum_\sigma \gamma(c_\sigma)\,\gamma(\chi_\sigma(\alpha)) =$$

$$\sum_\sigma \frac{c_{\gamma\sigma}}{c_\gamma}\,\gamma\sigma(\alpha)$$

$$= \frac{1}{c_\gamma} \sum_\sigma c_\sigma \sigma(\alpha)$$

$$= \frac{1}{c_\gamma}\beta \qquad c_\gamma = \frac{\beta}{\gamma(\beta)} = \frac{\gamma(\beta^{-1})}{\beta^{-1}}$$

Cyclic groups

$G = \langle \sigma \mid \sigma^n = 1 \rangle \qquad T = \sigma - 1 \qquad N = \sigma^{n-1} + \cdots + \sigma + 1 \qquad \in \mathbb{Z}[G]$

$$\mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \to \mathbb{Z} \to 0 \qquad TN = NT = 0$$

$\sigma \mapsto 1$ degree map

FTW! This is exact, free resolution.

$$0 \to \mathrm{Hom}_G(\mathbb{Z}[G], M) \xrightarrow{T} \cdots$$

$$H^0(G, M) = M^G \qquad H^{even}(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$$

$$H^{even} = \frac{\ker(\longrightarrow)}{\mathrm{Im}(\longrightarrow)} \qquad H^{odd}(G, \mathbb{Z}) = 0$$

Hilbert Theorem 90

L/K cyclic, $G_{L/K} = \langle \sigma \rangle$

$$0 = H^1(G_{L/K}, L^\times) = \frac{\ker(N)}{\mathrm{im}(T)}$$

Herbrand quotient

G cyclic $= \langle \sigma \rangle$

If $H^{2i}(G,M)$ and $H^{2i+1}(G,M)$ are finite, define

$$h(M) = \frac{\#H^{2i}(G,M)}{\#H^{2i+1}(G,M)}$$

Prop. $0 \to M \to N \to P \to 0$ exact. If two of $h(M), h(N), h(P)$ exist, so does the third, and $h(N) = h(M)h(P)$.

Pf. Long exact sequence

$$H^{2i}(P) \to H^{2i+1}(M) \to H^{2i+1}(N) \to H^{2i+1}(P) \to H^{2i}(M) \to H^{2i}(N) \to H^{2i}(P)$$

$$\frac{|H^{2i}(P)|\,|H^{2i+1}(N)|\,|H^{2i}(M)|}{|H^{2i+1}(M)|\,|H^{2i+1}(P)|\,|H^{2i}(N)|} = 1$$

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

Look at $0 \to M^G \to M \xrightarrow{T} M \to M/TM \to 0$

$0 \to H^{2i+1}(M) \to M^G/TM \xrightarrow{N} M^G \to H^{2i}(M)$

$\|$ $\omega''(N)/\mathrm{Im}(T)$ $\qquad$ $\downarrow$ M^G/NM

$|M^G| = |M/TM|$ so $|H^{2i+1}(M)| = |H^{2i}(M)| \Rightarrow h(M)=1$

Corollary $K=\mathbb{F}_q$, $L=\mathbb{F}_{q^n}$, then $N_{L/K}(L^\times)=K^\times$.

Pf. $H^1(L^\times)=0$, $G_{L/K}$ cyclic

$$h(L^*) = \frac{|H^{\mathrm{odd}}(L^\times)|}{|H^{\mathrm{even}}(L^\times)|} = 1$$

$$H^{\mathrm{even}}(L^\times) = 0 = \frac{\ker(T)}{\mathrm{Im}(N)} = \frac{K^*}{N_{L/K}(L^\times)}$$

Lecture 17 (2011-03-09)

Profinite groups 2011-3-9

(17)

$G = \varprojlim G_i$, each G_i finite

p-adic integers $\mathbb{Z}_p$, $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$, $G = \mathrm{Gal}(\bar{K}/K)$

$\mathrm{Gal}(\bar{K}/K) = \varprojlim_{L/K \text{ finite}} \mathrm{Gal}(L/K)$

basis of open sets around 1 consists of $\{\ker G \to G_i\}_{i \in I}$

Def. A topological group is topologically cyclic if there exists a dense cyclic subgroup

Examples. $\mathbb{Z}_p$, $\hat{\mathbb{Z}}$

Fundamental Theorem of Galois Theory

L/K Galois, then

$\{\text{closed subgroups } H \subset \mathrm{Gal}(L/K)\} \longleftrightarrow \{\text{intermediate fields } K \subset E \subset L\}$

$H \longmapsto L^H$

$\mathrm{Gal}(L/E) \longleftarrow E$

G profinite, M a G-module.

Prop (HW): TFAE

① $M = \bigcup_{\substack{H \lhd G \\ H \text{ open}}} M^H$

② $\forall x \in M$, $\mathrm{Stab}(x) = \{\sigma \in G \mid \sigma(x) = x\}$ is open subgroup of G

③ $G \times M \to M$ is continuous
$(\sigma, x) \mapsto \sigma(x)$

Def. M is called a discrete G-module
(hence forth dropping "discrete")

Example. $G(\bar{K}/K)$ acting on $\bar{K}$ or $\bar{K}^\times$

given $x \in \bar{K}$, $G(\bar{K}/K(x))$ fixes x, finite index

Cohomology of profinite groups

$G = \varprojlim G/H_i$ $\quad H_i = \ker(G \twoheadrightarrow G_i)$, hence $G_i \cong G/H_i$ (surjective)

where H_i finite index

$M = \varinjlim M^{H_i}$

want to make $H^q(G/H_i, M^{H_i})$ into directed system.

Let $i \leq j$ – there is a map $G/H_j \to G/H_i$, so $H_j \subset H_i$

$$H^q(G/H_i, M^{H_i}) \to H^q(G/H_j, M^{H_j})$$

$$[c_i] \longmapsto [c_j]$$

$$(G/H_j)^q \to (G/H_i)^q \xrightarrow{\text{cocycle } c_i} M^{H_i} \hookrightarrow M^{H_j}$$

$$(G/H_j)^q \xrightarrow{c_j} M^{H_j}$$

need to check works up to coboundary

Def. $H^q(G, M) = \varinjlim H^q(G/H_i, M^{H_i})$

Not necessarily the same as the derived functor cohomology

Alternative: Look at continuous maps $G^q \to M$ (discrete topology)

take $\frac{\text{continuous cocycles}}{\text{continuous coboundaries}}$, also gives $H^q(G, M)$

Example. $H^q(G(\bar{K}/K), \bar{K}^+) = \begin{cases} K & q=0 \\ 0 & q>0 \end{cases}$

$H^q(G(\bar{K}/K), \bar{K}^*) = 0$

follows from results for finite groups – limit of trivial groups is trivial

Def, The Brauergroup of K is $Br(K) = H^2(G(\bar{K}/K), \bar{K}^*)$

Theorem $K/\mathbb{Q}_p$ a finite extension, then

$$Br(K) \cong \mathbb{Q}/\mathbb{Z}$$

Pf Sketch, K_{nr} = Max unramified extension of K

① $H^2(G(\overline{K}/K_{nr}), \overline{K}^\times) = 0$ (won't prove)

② use inflation / restriction

$$\left[\begin{array}{l} H^q(L/K, M) \text{ means } H^q(Gal(L/K), M) \\ H^q(K, M) \text{ means } H^q(\overline{K}/K, M) \\ \quad \shortparallel \\ H^q_{et}(Spec(K), M) \end{array}\right]$$

$$0 \to H^1(K_{nr}/K, K_{nr}^\times) \xrightarrow{inf} H^1(\overline{K}/K, \overline{K}^\times) \xrightarrow{res} H^1(\overline{K}/K_{nr}, \overline{K}^\times) -$$

but Hilbert 90 ⟹ these are all 0. Luckily this implies

$$0 \to H^2(K_{nr}/K, K_{nr}^\times) \xrightarrow{inf} H^2(\overline{K}/K, \overline{K}^\times) \xrightarrow{res} H^2(\overline{K}/K_{nr}, \overline{K}^\times)$$

Step ① ↑ this is 0

thus $Br(K) = H^2(K_{nr}/K, K_{nr}^\times)$

③ $1 \to \mathcal{O}_{nr}^\times \to K_{nr}^\times \xrightarrow{valuation} \mathbb{Z} \to 0$

valuation on $\overline{K}^\times$ has to go to $\mathbb{Q}$

this induces $H^2(\mathcal{O}_{nr}^\times) \to H^2(K_{nr}^\times) \to H^2(\mathbb{Z}) \to H^3(\mathcal{O}_{nr}^\times)$

(4) $H^q(\mathcal{O}_{nr}^\times) = 0 \quad \forall q \geq 1$ (we'll do next time)

(5) Step 4 $\Rightarrow H^2(K_{nr}^\times) \cong H^2(\mathbb{Z})$

Consider $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$

induces $\to H^1(\mathbb{Q}) \to H^1(\mathbb{Q}/\mathbb{Z}) \to H^2(\mathbb{Z}) \to H^2(\mathbb{Q})$

Lemma G profinite, $H^q(G, \mathbb{Q}) = 0 \quad \forall q \geq 1$

(6) $H^2(\mathbb{Z}) \cong H^1(G(K_{nr}/K), \mathbb{Q}/\mathbb{Z}) \cong$
(trivial action $\Rightarrow$ 1-cycles just homomorphisms)

$\mathrm{Hom}_{\mathrm{cont}}(G(K_{nr}/K), \mathbb{Q}/\mathbb{Z})$

$f \longmapsto f(\mathrm{Frob}_u)$

$\| \wr$

$G(\bar{u}/u)$ where u = residue field of K

$\| \wr$

$\hat{\mathbb{Z}}$ topologically cyclic

here $\cong \mathbb{Q}/\mathbb{Z}$

Lecture 18 (2011-03-11)

$K/\mathbb{Q}_p$, want to compute $Br(K) \overset{\text{def}}{=} H^2(\bar{K}/K, \bar{K}^\times)$ 2011-3-11 (18)

we showed it sufficed to look at $H^2(K_{nr}/K, K_{nr}^\times)$

we showed this is isomorphic to $H^2(K_{nr}/K, \mathbb{Z})$ via the map induced by the valuation map on K_{nr}

this is isomorphic to $H^1(K_{nr}/K, \mathbb{Q}/\mathbb{Z})$ by dimension shifting

this is isomorphic to $H^1(\bar{k}/k, \mathbb{Q}/\mathbb{Z}) \cong H^1(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})$

$\xrightarrow{\text{evaluation}} \mathbb{Q}/\mathbb{Z}$

Prop. $H^i(K_{nr}/K, \mathcal{O}_{nr}^\times) = 0$ for $i \geq 1$

If. $1 \to 1 + \mathfrak{p}_{nr} \to \mathcal{O}_{nr}^\times \to \bar{k}^\times \to 1$

Let L/K be a finite unramified extension.

To prove: $H^i(L/K, \mathcal{O}_L^\times) = 0$ (get full result by taking direct limits)

$1 \to 1 + \mathfrak{p}_L \to \mathcal{O}_L^\times \to k_L^\times \to 1$

$G_{L/K} \cong G_{k_L/k_K}$ is cyclic

$H^1(k_L/k_K, k_L^\times) = 0$ by Hilbert 90

$U_L^\times$ is finite, so $H^1($

Herbrand quotient $h(U_L^\times) = 1$

$$1 \to 1 + \mathfrak{p}_K \to O_K^\times \to U_K \to H^1(1+\mathfrak{p}_L) \to H^1(O_L^\times) \to$$

we know this is onto, so this is all 0

This shows $H^i(L/K, 1+\mathfrak{p}_L) \simeq H^i(L/K, O_L^\times)$

Prop. $H^2(K_{nr}/K, O_{nr}^\times) = 0$ Let $\mathfrak{p}_L = \pi_L O_L$

$$1 \to 1 + \mathfrak{p}_L^{n+1} \to 1 + \mathfrak{p}_L^n \to U_L^+ \to 0$$

$$1 + a\pi_L^n \mapsto a \bmod \mathfrak{p}_L$$

$$(1 + a\pi_L^n)(1 + b\pi_L^n) = 1 + (a+b)\pi_L^n + \cdots$$

$H^i(K_t/K_{ur}, U_L^+) = 0$ from before

So $H^i(L/K, 1+\mathfrak{p}_L^n)$ is independent of n.

When n is big enough, we have an isomorphism

$$(1 + \mathfrak{p}_L^n, \cdot) \xrightarrow{\sim} (\mathfrak{p}^n, +)$$ where $p \geq 3$, any $n \geq 1$; $p = 2$, $n \geq 2$

$$\exp(a) = \sum_{k=0}^{\infty} \frac{a^k}{n!} \longleftarrow\!\shortmid\; a$$

$$b \longmapsto \log(b) = -\sum_{k=0}^{\infty} \frac{(b-1)^k}{k}$$

Thus $H^i(L/K, 1+\mathfrak{P}_L^{\wedge}) = H^i(L/K, \mathfrak{P}_L^{\wedge})$

Because $\mathfrak{P}_L^{\wedge} \cong \mathcal{O}_L$, we get

$a \mapsto \frac{a}{\pi_L^{\wedge}}$ (not canonical)

$\cong H^i(L/K, \mathcal{O}_L^+)$

Since these are local fields,

$$\mathcal{O}_L = \mathcal{O}_K[x]/(f(x))$$

where $f(x)$ is monic, irreducible over K

$$f(x) = \prod (x - a_i) = \prod_{\sigma \in G_{L/K}} (x - \sigma(\alpha))$$

$$\mathcal{O}_L^+ = \bigoplus_{\sigma \in G_{L/K}} \mathcal{O}_K \cdot \sigma(\alpha) \cong \mathbb{Z}[G_{L/K}] \otimes_{\mathbb{Z}} \mathcal{O}_K$$

$$\sigma(\alpha) a \longleftrightarrow \sigma \otimes a$$

$\cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G_{L/K}], \mathcal{O}_K)$ since $G_{L/K}$ finite

co-induced by definition, so $H^i(\ ) = 0$ $\forall i \geq 1$

Thus $H^i(L/K, \mathcal{O}_L^{\times}) = 0 \quad \forall i \geq 1$

$H(\mathcal{O}_L^\times) \cong H(1+\mathfrak{p}_L) \cong H(1+\mathfrak{p}_L^n) \cong H(\mathfrak{p}_L^n) \cong H(\mathcal{O}_L) = 0$ (exp, log)

$Br(K) \overset{\text{def}}{=} H^2(\overline{K}/K, \overline{K}^\times) \cong H^2(K_{nr}/K, K_{nr}^\times) \xrightarrow{\sim} H^2(K_{nr}/K, \mathbb{Z}) \xleftarrow[\sim]{\delta} H^1(K_{nr}/K, \mathbb{Q}/\mathbb{Z}) \cong H^1(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$

called "invariant map" — evaluation

$Br(K) \xrightarrow[\sim]{inv_K} \mathbb{Q}/\mathbb{Z}$ functorial

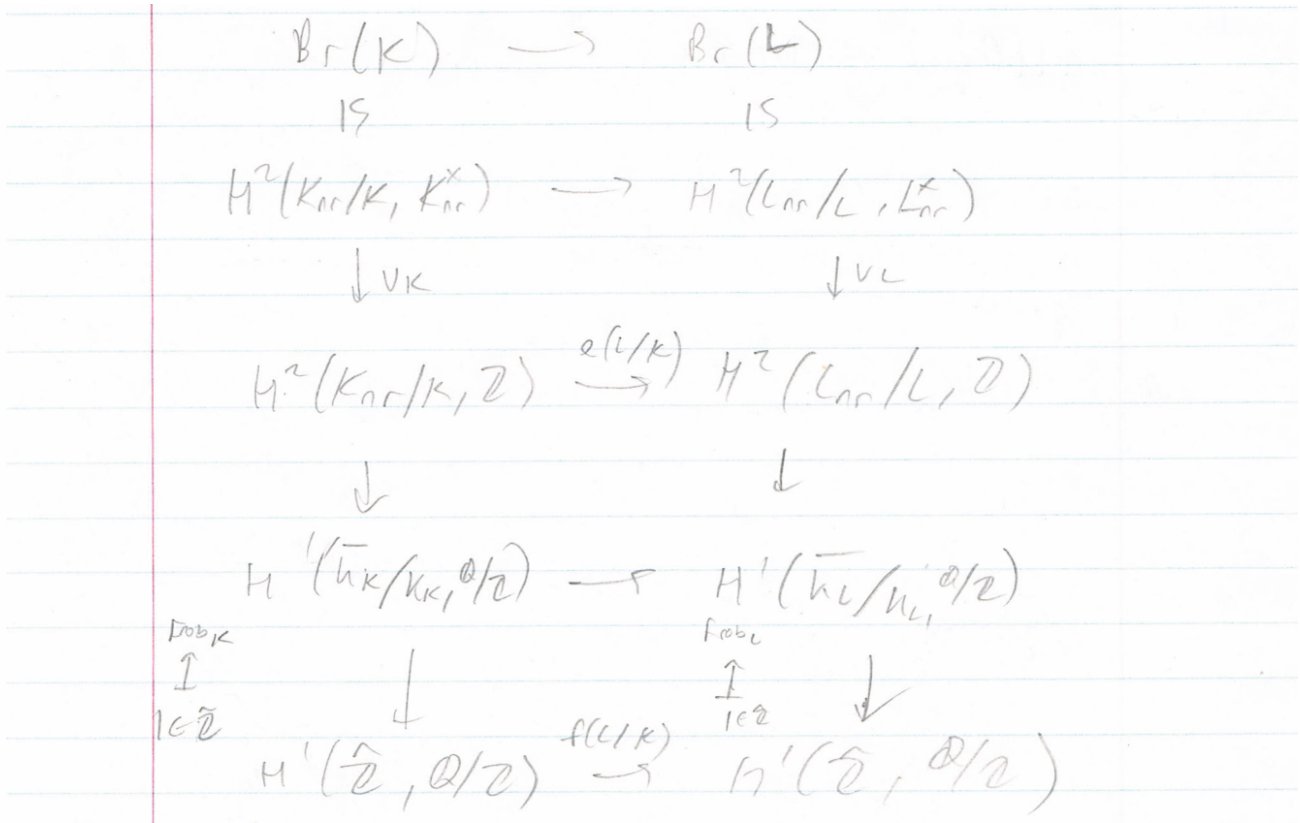
$L/K/\mathbb{Q}_p$ finite, $G(\overline{L}/L) \subset G(\overline{K}/K)$

all H^1's are trivial by Hilbert 90, so

get inflation/restriction on H^2's

$$0 \to H^2(L/K, L^\times) \xrightarrow{inf} H^2(\overline{K}/K, \overline{K}^\times) \xrightarrow{res} H^2(\overline{L}/L, \overline{L}^\times)$$

$$\begin{array}{ccccc} & & inv_{L/K} \downarrow & inv_K \downarrow s & inv_L \downarrow s \\ 0 \to & & ? & \mathbb{Q}/\mathbb{Z} & \longrightarrow \mathbb{Q}/\mathbb{Z} \\ & & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & & \end{array}$$



so this map is multiplication by $e(L/K)f(L/K) = [L:K]$ all thru

Def. The invariant of L/K is

$$u_{L/K} = \mathrm{inv}_{L/K}^{-1}\left(\frac{1}{n}\right) \in H^2(L/K, L^\times)$$

(distinguished generator)

Lecture 19 (2011-03-14)

Group Homology 2011-3-14

(19)

cohomology = derived functor of $M \mapsto M^G$

M^G = largest submodule fixed by G

homology = derived functor of $M \mapsto M_G$

M_G = largest quotient fixed by G

Recall $M^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Let I_G = left ideal generated by all $\sigma - 1$, for $\sigma \in G$

Then $M_G = M/I_G M = M \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G]/I_G$

$H_q(G, \cdot)$ = q^{th} derived functor of $\cdot \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G]/I_G$

Prop. $H_1(G, \mathbb{Z}) \cong I_G/I_G^2$

Pf. $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$

$\sigma \mapsto 1$

$$\to H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}) \to 0$$

$$\| \qquad\qquad \| \qquad\qquad \| \qquad\qquad \| \qquad\qquad \|$$

$$0 \qquad I_G/I_G^2 \xrightarrow{0 \text{ map}} \mathbb{Z}[G]/I_G \qquad \mathbb{Z}/I_G\mathbb{Z}$$

$$\| \qquad\qquad\qquad\qquad \| \qquad\qquad \|$$

$$\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}$$

Prop $H_1(G,\mathbb{Z}) \cong I_G/I_G^2 \cong G^{ab} = G/[G,G]$

$\sigma - 1 \longleftarrow \sigma \bmod [G,G]$ (HW)

Tate cohomology groups G finite

Let $N = \sum_{\sigma \in G} \sigma \in \mathbb{Z}[G]$

Def $\hat{H}^q(G,M) = H^q(G,M)$ for $q \geq 1$

$\hat{H}^0(G,M) = M^G/NM$

$\hat{H}^{-1}(G,M) = \ker(M_G \xrightarrow{N} M_G)$

$\hat{H}^{-q}(G,M) = H_q(G,M)$ for $q \geq 2$

Thm. $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$ gives a long exact sequence

$$\to \hat{H}^q(G,M) \to \hat{H}^q(G,N) \to \hat{H}^q(G,P) \to \hat{H}^{q+1}(G,M) \to \cdots$$

need to check

$$\begin{array}{ccc} \hat{H}^{-1}(G,P) & \to & \hat{H}^0(G,M) \\ \| & & \| \\ \ker(P_G \xrightarrow{N} P_G) & \longrightarrow & M^G/N\cdot M \end{array}$$

$\bar{p} \in P/I_G P$

Choose $n \in N$ with $\beta(n) = p$ (since β surjective)

We know $N \cdot p \in I_G P$

$N \cdot p(n) \in I_G P$ $\quad p(N \cdot n) \in I_G p$ $\quad Np - \sum a_\sigma (\sigma - 1) p_\sigma$ ⋮ n_σ

...

Cup product $\hat{H}^p(G, M) \otimes \hat{H}^q(G, N) \longrightarrow \hat{H}^{p+q}(G, M \otimes N)$

$a \otimes \beta \longmapsto \alpha \cup \beta$

Functorial in M and N, respects connecting homomorphisms $\delta \alpha \cup \beta = \delta(\alpha \cup \beta)$ etc, and for $p = q = 0$ induced by $M^G \otimes N^G \longrightarrow (M \otimes N)^G$

For $p, q \geq 1$, we have

$$\bar{\alpha} \in \hat{H}^p(G, M), \quad \bar{\beta} \in \hat{H}^q(G, N)$$

Choose cocycles $\alpha : \mathbb{Z}[G^{p+1}] \to M$, $\beta : \mathbb{Z}[G^{q+1}] \to N$

Then $\alpha \cup \beta$ is the cohomology class for

$$\mathbb{Z}[G^{p+q+1}] \to M \otimes N$$

$$(\alpha \cup \beta)(\sigma_0, \ldots, \sigma_{p+q}) = \alpha(\sigma_0, \ldots, \sigma_p) \otimes \beta(\sigma_{p+1}, \ldots, \sigma_{p+q})$$

Properties:

- $(\bar{\alpha} \cup \bar{\beta}) \cup \bar{\gamma} = \bar{\alpha} \cup (\bar{\beta} \cup \bar{\gamma})$
- $\bar{\alpha} \cup \bar{\beta} = (-1)^{\dim(\bar{\alpha}) \dim(\bar{\beta})} \bar{\beta} \cup \bar{\alpha}$
- $\mathrm{Res}(\bar{\alpha} \cup \bar{\beta}) = \mathrm{Res}(\bar{\alpha}) \cup \mathrm{Res}(\bar{\beta})$ for Res = restriction (H ⊂ G)

Recall that for $L/K/\mathbb{Q}_p$ we defined

$$u_{L/K} \in H^2(L/K, L^\times) \cong \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}$$

Thm. For all q,

$$\hat{H}^q(G_{L/K}, \mathbb{Z}) \xrightarrow{\cdot \smile u_{L/K}} \hat{H}^{q+2}(G_{L/K}, L^\times)$$

is an isomorphism.

Take $q = -2$

$$\begin{array}{ccc} \hat{H}^{-2}(G_{L/K}, \mathbb{Z}) & \xrightarrow{\smile u_{L/K}} & \hat{H}^0(G_{L/K}, L^\times) \\ \| & & \| \\ H_1(G_{L/K}, \mathbb{Z}) & & K^\times / N_{L/K} L^\times \\ \| & \nearrow \sim & \\ G_{L/K}^{ab} & & \end{array}$$

inverse to the Artin map

Lecture 20 (2011-03-16)

$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$ 2011-3-16 (20)

$N = \sum_{\sigma \in G} \sigma$ $\quad I_G = (\sigma - 1)_{\sigma \in G}$

$\hat{H}^{-1}(P) \to \hat{H}^0(M)$

$\| \text{def}$ $\quad \| \text{def}$

$\ker(H_0(P) \xrightarrow{N} H^0(P))$ $\quad M^G / NM$

$\ker(P/I_G P \xrightarrow{N} P^G)$ Let $\bar{p} \in P/I_G P$ such that $Np = 0$.

Choose $n \in \beta^{-1}(p)$. Then $\beta(Nn) = N\beta(n) = Np = 0$,

so $\exists!\, m \in M$ with $\alpha(m) = Nn$, and set $\delta(\bar{p}) = \bar{m}$

C_K = ideal class group $= I_K / K^\times$

L/K finite Galois $\quad I_K = \prod'_{w \in M_K} K_w^\times$

Thm. $H^2(G_{L/K}, C_L) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ where $n = [L:K]$

$U_{L/K} = \text{inv}_{L/K}^{-1}\left(\frac{1}{n}\right)$ $\quad K_v^\times \cong \left(\prod_{w|v} L_w^\times\right)$

$1 \to L^\times \to I_L \to C_L \to 1$

$1 \to K^\times \to I_K \to C_L^{G_{L/K}} \to H^1(G_{L/K}, L^\times)$

$\|$ Hilbert 90

0

Thm L/K finite Galois number fields

$$\hat{H}^q(G_{L/K}, \mathbb{Z}) \xrightarrow{\cup u_{L/K}} \hat{H}^{q+2}(G_{L/K}, C_L)$$

is an isomorphism

Taking $q = -2$:

$$G_{L/K}^{ab} \xrightarrow{\cup u_{L/K}} C_K / N_{L/K} C_L$$

Take limit over all abelian extensions

$$G_K^{ab/K} \cong \varprojlim C_K / N_{L/K} C_L = C_K / \{\text{universal norms}\}$$

$$\{\alpha \in C_K \mid \forall\, L/K \text{ abelian}, \exists\, \beta_L \in C_L \text{ with } N_{L/K}\beta_L = \alpha_L\}$$

$$\begin{array}{ccccccc} 0 \to & H^2(G_{L/K}, C_K^\times) & \to & H^2(G_{\bar{K}/K}, C_{\bar{K}}) & \to & H^2(G_{\bar{L}/L}, C_{\bar{L}}) \\ & \downarrow \mathrm{inv}_{L/K} & & \downarrow \mathrm{inv}_K & & \downarrow \mathrm{inv}_L \\ 0 \to & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \to & \mathbb{Q}/\mathbb{Z} & \to & \mathbb{Q}/\mathbb{Q} \end{array}$$

HW: $Br(\mathbb{C}) = 0$, $Br(\mathbb{R}) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$

$Br(K) = H^2(G_{\bar{K}/K}, \bar{K}^\times)$

$1 \to \bar{K}^\times \to I_K \to C_K \to 1$

$H^1(I_K) \to H^1(C_K) \to H^2(\bar{K}^\times) \to H^2(I_K) \to H^2(C_K) \to H^3(\bar{K}^\times)$

$0 \quad 0 \quad Br(K) \quad \bigoplus_{v \in M_K} (\mathbb{Q}/\mathbb{Z})_v \quad \mathbb{Q}/\mathbb{Z}$

Hilbert 90

$= 0$ if v real
$= \frac{1}{2}$ if v complex

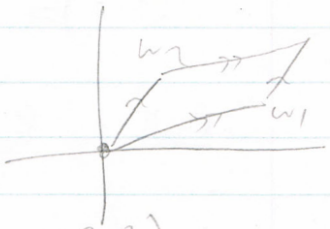
Elliptic curves

Goals: (weak) Mordell-Weil Thm
Complex multiplication

Def: An elliptic curve E is a smooth, projective curve of genus 1, with given point O.

Look at as Riemann surface

$\mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = S^1 \times S^1$



Using Riemann-Roch can be embedded in $\mathbb{P}^2$ as a cubic

$E = \{Y^2Z = X^3 + AXZ^2 + BZ^3\}$

for some A, B (not true if $char = 2, 3$)

Here $O = [0, 1, 0]$ is unique point "at infinity"

We homogenize, get $E: y^2 = x^3 + Ax + B$

Def. This is called a Weierstrass Equation for E

Prop The curve $y^2 = x^3 + Ax + B$ is smooth if and only if $\Delta_E \neq 0$

Def: The discriminant of E is $\Delta_E = -16(4A^3 + 27B^2)$

Def. E is defined over K if $A, B \in K$

We write E/K if E defined over K

$$E(L) = \{(x,y) \in L^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

Example $E: y^2 = x^3 + 1$

$$E(\mathbb{Q}) = \{\mathcal{O}, (0, \pm 1), (-1, 0), (2, \pm 3)\}$$

↑ not so easy to prove

$$\bar{K}(E) = \mathrm{Frac}\left(\bar{K}[x,y] / (y^2 - x^3 - Ax - B)\right)$$

Def. $E \cong E'$ if $\exists$ maps

$\phi: E \to E'$ $\quad \phi \circ \psi = id$, $\psi \circ \phi = id$

$\psi: E' \to E$

ϕ, ψ are rational functions in $\bar{K}(x,y)$

$E \cong E'$ over K if can choose ϕ, ψ with coeffs in K

Lecture 21 (2011-03-18)

$E: y^2 = x^3 + Ax + B$ 2011-3-18

(21)

$E \cong E' \iff E': y^2 = x^3 + Au^4x + Bu^6$

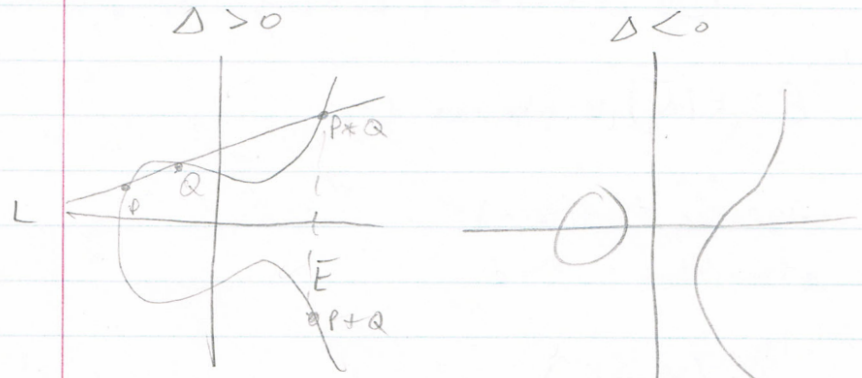
$\frac{A^3}{B^2}$ is an isomorphism invariant

Def. The j-invariant of E is $j(E) = 1728 \frac{4A^3}{-16(4A^3+27B^2)}$

Prop. $E \cong E'$ iff $j(E) = j(E')$, when working over an algebraically closed field.

Prop. $\forall \alpha \in K$, $\exists E/K$ with $j(E) = \alpha$ (K alg closed)

Elliptic curves have a group structure (group object in category of algebraic varieties)



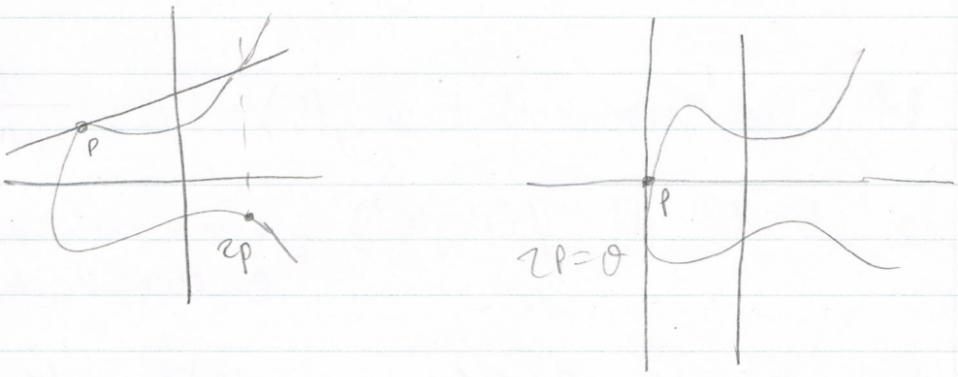
$E \cap L = 3$ pts. (Bezout)

$Q * (P * Q) = P$ for all P, Q

$-P$ = reflection about x-axis

Group law defined by

$$P + Q + P * Q = \mathcal{O}$$



$\frac{dy}{dx} = \frac{3x^2+A}{2y} = \infty \iff y = 0$, x not root of $3x^2+A$

Prop $\{P \in E(\mathbb{C}) \mid 2P = \mathcal{O}\} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Thm. $E = E(\bar{K})$ is abelian group

Pf abelian – trivial
associative – hard

$$-(x_0, y_0) = (x_0, -y_0)$$

If $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, we have

(if $x_1 = x_2$, $y_1 = -y_2$ then $(x_3, y_3) = \mathcal{O}$)

Otherwise, line through (x_1, y_1) and (x_2, y_2)

$L: y = \lambda x + \nu$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ $\qquad \lambda = \frac{3x_1^2 + A}{2y_1}$

$\nu = y_1 - \lambda x_1$ $\qquad \nu = y_1 - \lambda x_1$

$L \cap E: (\lambda x + \nu)^2 = x^3 + Ax + B$

$x^3 - \lambda^2 x^2 + (A - 2\lambda\nu)x + B - \nu^2$

$= (x - x_1)(x - x_2)(x - x_3)$

$-\lambda^2 = -x_1 - x_2 - x_3$ so $x_3 = \lambda^2 - x_1 - x_2$

$y_3 = -(\lambda x_3 + \nu)$

Corollary. Given E/K and field extension L/K,

$E(L) = \{(x, y) \in E \mid x, y \in L\} \cup \{\mathcal{O}\}$ is a subgroup of $E(\bar{K})$

Pf. Closed under $+$ by formula.

Example $E: y^2 = x^3 + 17$

$P = (-2, 3)$, $Q = (-1, 4)$, $R = (2, 5)$ are in $E(\mathbb{Q})$

$Q + R = \left(\frac{-8}{9}, -\frac{109}{27}\right)$ $\qquad 2P = (8, -23)$

HW: Compute $2Q$, $P+Q$

Thm. Let $E: y^2 = x^3 + 17$. Then

a) $E(\mathbb{Q}) = \{mP + nR \mid m, n \in \mathbb{Z}\} \cong \mathbb{Z} \times \mathbb{Z}$

b) $|E(\mathbb{Z})| = 16$

Pf: Hard

These illustrate: Mordell-Weil Thm.

$K/\mathbb{Q}$ number field, E/K is an elliptic curve

$E(K)$ is finitely generated abelian group

$E(K) \cong (\text{finite}) \times \mathbb{Z}^r$ $r = \text{rank } E$

Goal: Weak Mordell-Weil Thm

$E(K)/mE(K)$ is finite.

Siegel's Thm

$E(\mathcal{O}_K)$ finite.

Conjecture: $\forall N \in \mathbb{N}$, $\exists E/\mathbb{Q}$ with $\mathrm{rank}\, E \geq N$

best so far: 28 ish, Noam Elkies

Def $E(K)_{tors} = \{P \in E(K) \mid \exists P = \mathcal{O} \text{ for some } n \geq 1\}$

Thm, Mazur: $|E(\mathbb{Q})_{tors}| \leq 16$ $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$

Merel: $|E(K)_{tors}| \leq C([K:\mathbb{Q}])$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 4$

L-series

$\# E(\mathbb{F}_p) = p + 1 - a_p$

Lecture 22 (2011-03-21)

$E: y^2 = x^3 + Ax + B$ defined over K 2011-3-21

(22)

$[m]: E \to E$

$P \mapsto \underbrace{P + \cdots + P}_{m \text{ times}}$ $\qquad E_{tors} = \bigcup_{m \geq 1} \ker[m]$

$E[m] = \ker[m] = \{P \in E(\bar{K}) \mid [m]P = \mathcal{O}\}$

Note that $[m]P = (f_m(x(P), y(P)), g_m(x(P), y(P)))$

where $f_m, g_m \in K(x, y)$

Ex. Work out f_2 explicitly. In fact, all f_m have only even powers of y, hence can be written in terms of only x.

$E[m]$ = points where denominators of f_m and g_m vanish

Notice that if $P \in E(\bar{K})$ and $\sigma \in G_{\bar{K}/K}$,

$\sigma P \overset{\text{def}}{=} \sigma(x, y) = (\sigma(x), \sigma(y)) \in E(\bar{K})$

$\sigma(P + Q) = \sigma(P) + \sigma(Q)$, so $E(\bar{K})$ is a $G_{\bar{K}/K}$-module

also $E[m]$ is a $G_{\bar{K}/K}$-module

Thm. E/K elliptic curve, $p = \mathrm{char}(K)$

a) If $p \nmid m$, or $p = 0$, then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

b) $E[p^n] \cong$ either $\mathbb{Z}/p^n\mathbb{Z}$ for all n, or 0 for all n (supersingular)

Prop. $\mathrm{Char}(K) = 0$ or $p \geq 3$,
$E: y^2 = x^3 + Ax + B$ (so not all curves in char 3)

then $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Pf $P \in E[2] \iff 2P = 0 \iff$ vertical tangent at $P \iff$

$\left.\frac{dx}{dy}\right|_P = 0 \iff \frac{2y}{3x^2+A} = 0 \iff y = 0$ (provided $3x^2 + A \neq 0$)

What happens if $y = 3x^2 + A = 0$ at $P = (x, y) \in E$?

On any curve $F(x, y) = 0$, a point (x, y) is singular if $F(x, y) = 0$, $\frac{\partial F}{\partial x}(x, y) = 0$, $\frac{\partial F}{\partial y}(x, y) = 0$

$F = y^2 - x^3 - Ax - B$; $\frac{\partial F}{\partial y} = -(3x^2 + A)$, $\frac{\partial F}{\partial y} = 2y$

but we assumed our curve was nonsingular, so

$E[2] = \{O\} \cup \{(x, y) \in E(\bar{K}) \mid y = 0\} =$
$\{O\} \cup \{(\alpha, 0) \mid \alpha^3 + A\alpha + B = 0\}$ has 4 elements
2-torsion $\Rightarrow$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$G_{\bar{K}/K}$ acts on $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

Get $\rho_{E,m} : G_{\bar{K}/K} \longrightarrow \mathrm{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$,

a 2-dimensional representation of $G_{\bar{K}/K}$

Analogous to the 1-dimensional representation

$G_{\bar{K}/K} \longrightarrow \mathrm{Aut}\left(\underbrace{(\ker : \mathbb{C}^\times \to \mathbb{C}^\times)}_{x \mapsto x^m} \right)$

$\mu_m \cong \mathbb{Z}/m\mathbb{Z}$

$\sigma \longmapsto (\zeta \mapsto \sigma(\zeta))$

$K(E[m]) = K(x, y : (x,y) \in E[m])$

$G_{\bar{K}/K}$ maps $K(E[m])$ to itself, so $K(E[m])$ is Galois

$\rho_{E,m} : G(K(E[m])/K) \hookrightarrow GL_2(\mathbb{Z}/m\mathbb{Z})$

Weak Mordell-Weil Theorem

$K/\mathbb{Q}$, E/K, the $E(K)/mE(K)$ finite

to prove full MW theorem, suffices to prove weak for $m = 2$

Elliptic Kummer sequence $[m](x,y) = (f_m(x,y), g_m(x,y))$

$$0 \to E[m] \to E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \to 0$$

is an exact sequence of $G_{\bar{K}/K}$-modules, take cohomology

$$0 \to E[m] \cap E(K) \to E(K) \xrightarrow{[m]} E(K) \to H^1(G_{\bar{K}/K}, E[m]) \to H^1(G_{\bar{K}/K}, E$$

get $0 \to E(K)/mE(K) \to H^1(G_{\bar{K}/K}, E[m]) \to H^1(G_{\bar{K}/K}, E$

life is easier if $E[m] \subset E(K)$ since then $G_{\bar{K}/K}$ action on $E[m]$ is trivial and this turns into Hom

reduce to this case. Let $L = K(E[m])$.

Suppose $E(L)/mE(L)$ finite. To show: $E(K)/mE(K)$ finite.

$$0 \to \frac{E(K) \cap mE(L)}{mE(K)} \to E(K)/mE(K) \to E(L)/mE(L)$$

$$\downarrow \gamma \qquad \downarrow \qquad \downarrow$$

$$0 \to H^1(G_{L/K}, E[m]) \to H^1(G_{E/K}, E[m]) \to H^1(G_{\bar{L}/L}, E[m])$$

claim: bottom is actually part of the inflation-restriction sequence

$$0 \to H^1(G_{L/K}, E[m]) \xrightarrow{\text{inf}} H^1(G_{\bar{K}/K}, E[m]) \xrightarrow{\text{res}} H^1(G_{\bar{L}/L}, E[m]$$

Def of ψ. Let $P \in \bar{E}(K) \cap mE(L)$.

So $P = mQ$ for some $Q \in E(L)$

$$\psi(P)(\sigma) = \sigma(Q) - Q$$

If $E(L)/mE(L)$ finite, then because

$H^1(G_{L/K}, E[m])$ finite (because $G_{L/K}$ and $E(m)$ finite)

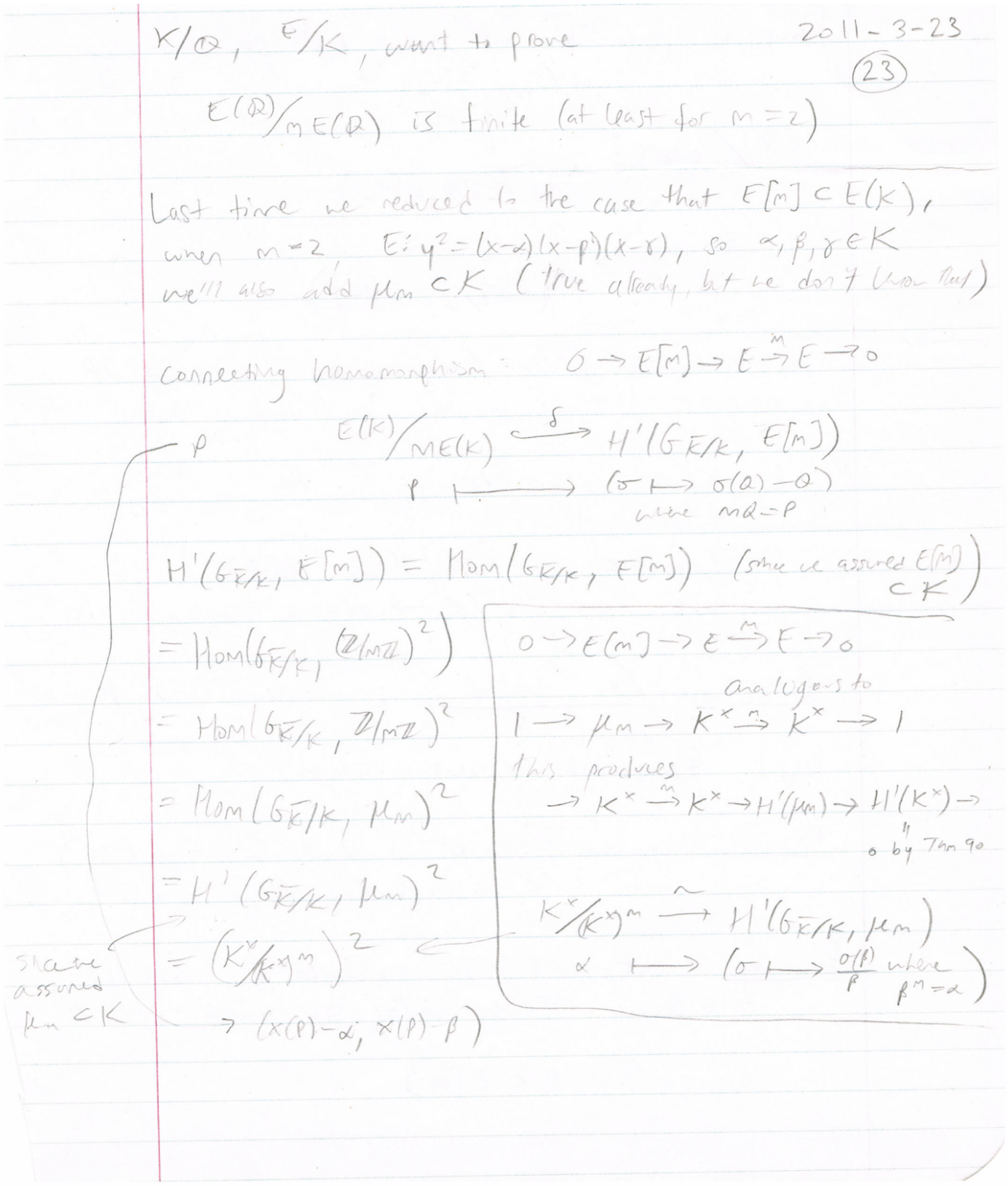
and ψ injective, $\frac{E(K) \cap mE(L)}{mE(K)}$ finite, hence

$E(K)/mE(K)$ finite [in general $H^1(G_{\bar{K}/K}, E[m])$ not finite

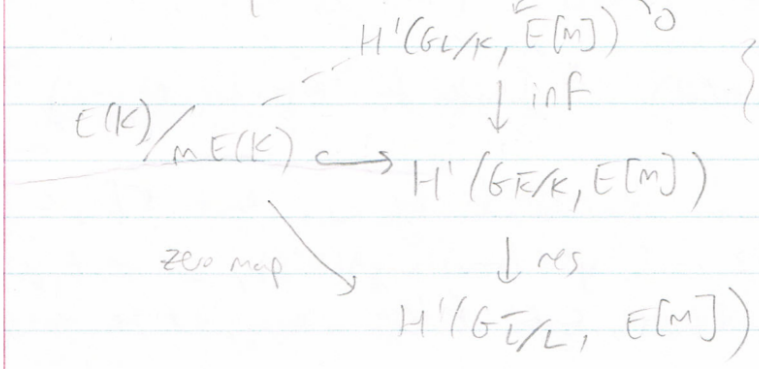
$= H^1(G_{\bar{K}/K}, E)$

$E)[m] \to 0$

Lecture 23 (2011-03-23)



want to replace $\bar{K}$ with smallest field possible, L



the cocycle $(\sigma \mapsto (\sigma(Q)-Q))$ is trivial iff σ acts trivially on Q, so want to define

$L = K(Q : mQ \in E(K))$ the

$E(K)/mE(K) \hookrightarrow H^1(G_{L/K}, E[m])$

$P \longmapsto (\sigma \mapsto \sigma(Q)-Q, \text{ where } mQ = P)$

Claim. L/K finite ; follows from Hurwitz's theorem, and

Prop 1. $G_{L/K}$ has exponent dividing m

Prop 2. There is a finite set of primes $S \subset \mathrm{Spec}(\mathcal{O}_K)$ such that L/K is unramified for all $\mathfrak{p} \notin S$.

Pf of Prop 1: Let $Q \in E(L)$ with $mQ = P$, and let $\sigma \in G_{L/K}$. Then $m(\sigma(Q)) = \sigma(mQ) = \sigma(P) = P$

thus $\sigma(Q) - Q \in E[m]$

Now look at $\sigma^m(Q) - Q$. Can write as

$$(\sigma^{m-1} + \cdots + 1)(\sigma - 1)Q = m(\sigma - 1)(Q) = O$$

$\sigma(Q) \in E[m]$, $E[m] \subset E(K)$

Prop 2. We defined $L = K([m]^{-1}E(K))$.

Fix $Q \in [m]^{-1}E(K)$, and let $F = K(Q)$.

$E: y^2 = x^3 + Ax + B$, $\mathfrak{p}$ prime in F,

reduce mod $\mathfrak{p}$ (assume A, B are $\mathfrak{p}$-integral)

$\tilde{A}, \tilde{B} \in \mathbb{F}_{\mathfrak{p}}$, $\tilde{E}: y^2 = x^3 + \tilde{A}x + \tilde{B}$

$\tilde{E}$ is an elliptic curve $/\mathbb{F}_{\mathfrak{p}} \iff \mathfrak{p} \nmid \Delta = 16(4A^3 + 27B^2)$
$\iff \tilde{\Delta} = 0$

Def. E has good reduction at $\mathfrak{p}$ if $\mathrm{ord}_{\mathfrak{p}}(A), \mathrm{ord}_{\mathfrak{p}}(B) \geq 0$ and $\mathfrak{p} \nmid \Delta$

Assume good reduction; then $\tilde{E}(\mathbb{F}_{\mathfrak{p}})$ is a group, and get a reduction map

$$E(F) \longrightarrow \tilde{E}(\mathbb{F}_{\mathfrak{p}})$$
$$(x, y) \mapsto \begin{cases} (\tilde{x}, \tilde{y}) & \text{if } \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \ (\text{which} \Rightarrow \mathrm{ord}_{\mathfrak{p}}(y) \geq 0) \\ O & \text{else} \end{cases}$$

This is just $\mathbb{P}^n(F) \to \mathbb{P}^n(\mathbb{F}_p)$

$[x_0, \dots, x_n] \mapsto [\widetilde{\lambda x_0}, \dots, \widetilde{\lambda x_n}]$

where we choose $\lambda \in F^\times$ such that $\operatorname{ord}_p(\lambda x_i) \geq 0$ for all i

and $\operatorname{ord}_p(\lambda x_j) = 0$ for some j.

Prop. $E(F) \to \widetilde{E}(\mathbb{F}_p)$ is a group homomorphism

Pf. The group law is defined by $P+Q+R=\mathcal{O} \iff$ P, Q, R collinear, and reduction mod p takes lines to lines

QED (at least if $\widetilde{P}, \widetilde{Q}, \widetilde{R}$ distinct)

Lecture 24 (2011-03-25)

Goal: $K([m]^{-1}E(K))/K$ is finite. 2011-3-25

(24)

If $\mathfrak{p} \nmid \Delta$, get a homomorphism $E(K) \to \tilde{E}(\mathbb{F}_{\mathfrak{p}})$.

Key Lemma. If $\mathfrak{p} \nmid m\Delta$, then $E(K)[m] \hookrightarrow \tilde{E}(\mathbb{F}_{\mathfrak{p}})$

(Analogous to statement that roots of unity remain distinct mod $\mathfrak{p}$)

We only need this for $m = 2$ though. Take Weierstrass equation with coefficients in $\mathcal{O}_K$, then factor as

$E: y^2 = (x-\alpha)(x-\beta)(x-\gamma)$. Then $E[2] = \{\mathcal{O}, (\alpha,0), (\beta,0), (\gamma,0)\}$

maps to $\tilde{E}(\mathbb{F}_{\mathfrak{p}})$ then $\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}$ are distinct mod $\mathfrak{p}$.

But $\Delta = \pm 16(\alpha-\beta)^2(\beta-\gamma)^2(\alpha-\gamma)^2$, so $\mathfrak{p} \nmid \Delta$ gives the result.

Prop. Assume $\mathfrak{p} \nmid m\Delta$. Then

a) $K(E[m])/K$ is unramified at $\mathfrak{p}$.

b) Let $Q \in E(\bar{K})$ with $mQ \in E(K)$, then $K(Q)/K$ is unramified at $\mathfrak{p}$.

Pf. Let $\mathfrak{P}$ be a prime of $K(E[m])$, $\mathfrak{P}/\mathfrak{p}$. Then

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G_{\mathfrak{P}} \mid \sigma(\alpha) = \alpha \bmod \mathfrak{P}\ \forall \alpha\} = \{\sigma \in G_{\mathfrak{p}} \mid \sigma(T) = T \bmod \mathfrak{P}\ \forall T \in E[m]\}$$

$$= \{\sigma \in G_{\mathfrak{p}} \mid \forall T \in E[m],\ \sigma(T) - T \in \ker(E[m] \to \tilde{E} \bmod \mathfrak{p})\} = \{\sigma \in G_{\mathfrak{p}} \mid \sigma(T) = T\ \forall T \in E[m]\} = \{1\}$$

(Lemma says injective)

b) WLOG, using a, we can replace K by $K(E[m])$ (unramified + unramified = unramified).

Let $\mathfrak{P}$ be a prime of $K(\bar{Q})$, $\mathfrak{P} \mid \mathfrak{p}$. Then

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G_{\mathfrak{p}} \mid \sigma(Q) \equiv Q \bmod \mathfrak{p}\} = \{\sigma \in G_{\mathfrak{p}} \mid \sigma(Q) - Q \equiv 0 \bmod \mathfrak{p}\}$$

Note $m(\sigma(Q) - Q) = \sigma(mQ) - mQ = 0$ (because $mQ \in E(K)$, hence fixed by σ)

So $\sigma(Q) - Q \in E[m]$, so $I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G_{\mathfrak{p}} \mid \sigma(Q) - Q = 0\} = \{1\}$.

Corollary. Given E/K, assume $E[m] \subset E(K)$. Let

$S = \{\text{primes } \mathfrak{p} \mid m\Delta\}$. Then.

a) Then $K([m]^{-1}E(K))/K$ is unramified at every $\mathfrak{p} \notin S$ (we showed this for any one point in this, composita of unramified are unramified)

b) $\mathrm{Gal}(K([m]^{-1}E(K))/K)$ is abelian of exponent m.

Pf. a) from prop.

b). Exponent m last time. Pf of abelian?

Let $Q \in E(\bar{K})$, $mQ = P \in E(K)$. Let $\sigma, \tau \in G(K(Q)/K)$

$\sigma(Q) - Q = T_\sigma$ for some $T_\sigma \in E[m]$

$\tau(Q) - Q = T_\tau$ for some $T_\tau \in E[m]$

$\sigma(\gamma(Q)) = \sigma(Q + T_\gamma) = Q + T_\sigma + \underbrace{\sigma(T_\gamma)}_{= T_\gamma \text{ since } E(M) \subset E(K)}$

similarly $\gamma(\sigma(Q)) = Q + T_\gamma + T_\sigma$

Thm. $K/\mathbb{Q}$, S = finite set of primes, $m \geq 2$

Let L = max abelian extension of K of exponent m unramified outside S. Then L/K is finite.

Main Thm of Kummer Theory $K/\mathbb{Q}$, $m \geq 2$, $\mu_m \subset K$

M = max abelian extension of K of exponent m

Then $M = K(\sqrt[m]{\alpha} \mid \alpha \in K^\times)$.

Pf of Thm. WLOG, can expand S, so $S \supset \{p \mid m\}$.

WLOG, can assume $\mu_m \subset K$.

L = largest subfield of M unramified outside S

When is $K(\sqrt[m]{\alpha})$ ramified at p? (assume $p \nmid m$)

$x^m - \alpha = 0$, $\operatorname{disc}(x^m - \alpha) = \pm m^? \cdot \alpha^{m-1}$

Let π be a uniformizer at p (i.e. $\operatorname{ord}_p(\pi) = 1$), so

$\alpha = u \pi^r$, $\sqrt[m]{\alpha} = \sqrt[m]{u}\, \pi^{r/m}$, so $K(\sqrt[m]{\alpha})/K$ unramified at p
(u unit) $\iff m \mid \operatorname{ord}_p(\alpha)$

Let $T_S = \{\alpha \in K^\times/(K^\times)^m \mid \mathrm{ord}_\mathfrak{p}(\alpha) \equiv 0 \bmod m \text{ for all } \mathfrak{p} \in S\}$

Then $L = K(\sqrt[m]{\alpha} : \alpha \in T_S)$.

Goal: show T_S is a finite set.

$$0 \to T_\phi \to T_S \longrightarrow \underbrace{(\mathbb{Z}/m\mathbb{Z} \times \cdots \times \mathbb{Z}/m\mathbb{Z})}_{\#S} \quad \text{finite}$$
$$\alpha \longmapsto (\mathrm{ord}_\mathfrak{p}(\alpha))_{\mathfrak{p} \in S}$$

Goal: T_ϕ is a finite set.

$\alpha \in T_\phi \iff \mathrm{ord}_\mathfrak{p}(\alpha) \equiv 0 \bmod m \ \forall \mathfrak{p} \iff$

$\alpha \mathcal{O}_K = \mathfrak{b}_\alpha^m$ for some ideal $\mathfrak{b}_\alpha$

$$1 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m \to T_\phi \to \underbrace{I_K/K^\times}_{Cl_K} \quad \text{finite}$$

finite by Dirichlet

$$\alpha \longmapsto [\mathfrak{b}_\alpha]$$

$[\mathfrak{b}_\alpha] = 1 \iff \mathfrak{b}_\alpha = \beta\mathcal{O}_K \iff \alpha\mathcal{O}_K = \mathfrak{b}_\alpha^m = \beta^m\mathcal{O}_K \iff$

$\alpha = u\beta$ for some $u \in \mathcal{O}_K^\times$

hence T_ϕ finite.

$$0 \to E(K)/mE(K) \to H^1(G_{L/K}, E[m]) \to H^1(G_{\bar{K}/K}, E(\bar{K}))$$

L/K finite

$$0 \to E(K)/mE(K) \to \underbrace{S^{(m)}(E/K)}_{\text{selmer group}} \to \underbrace{Ш(E/K)[m]}_{\text{Shafarevich–Tate group}} \to 0$$

CM: describe abelian extensions of imaginary quadratic fields using torsion points on elliptic curves.

$K = \mathbb{Q}(\sqrt{-D})$, construct E/K with $\mathrm{End}(E) = \mathcal{O}_K$

Then $K(j(E)) =$ Hilbert class field of K.

Lecture 25 (2011-04-04)

We've proven weak Mordell-Weil / 2011-4-4
$E(\mathbb{Q})/mE(\mathbb{Q})$ is finite (25)

How does this get us that $E(\mathbb{Q})$ is finitely generated?
Define a "size" function and show $size(mP) > size(P)$

Height function — arithmetic complexity

Def. The height of $\alpha = \frac{a}{b} \in \mathbb{Q}$ is $H(\alpha) = \max\{|a|, |b|\}$

$P \in \mathbb{P}^n(\mathbb{Q})$, $P = [a_0, \ldots, a_n]$ where $a_i \in \mathbb{Z}$, $\gcd(a_i) = 1$

Then $H(P) = \max |a_i|$.

Thm. a) $\{P \in \mathbb{P}^n(\mathbb{Q}) \mid H(P) \le B\}$ is finite
b) Let $\phi : \mathbb{P}^n \to \mathbb{P}^n$ be a degree d homogeneous map. Then $c_1 H(P)^d \le H(\phi(P)) \le c_2 H(P)^d$ where the c_i depend only on ϕ

H/W 1) What is $|\{P \in \mathbb{P}^n(\mathbb{Q}) \mid H(P) \le B\}|$?
2) Prove b.

$K/\mathbb{Q}$, $P = [a_0, \ldots, a_n] \in \mathbb{P}^n(K)$

$$H(P) = \prod_{v \in M_K} \max\{|a_0|_v, \ldots, |a_n|_v\}^{\frac{[K_v : \mathbb{Q}_v]}{[K:\mathbb{Q}]}}$$

this term does two things - ensures that the same point looked at in $\mathbb{P}^n(L)$ L/K, gives same height, and makes it well-defined - scaling P by λ introduces $\left(\prod_{v \in M_K} |\lambda|_v^{[K_v:\mathbb{Q}_v]}\right)^{1/[K:\mathbb{Q}]}$ $= 1$ by

HW: Check that definitions are the same when $K = \mathbb{Q}$.

Kronecker's Lemma: $\prod_{\alpha \in \mathbb{Q}} H(\alpha) = 1 \iff \alpha$ is a root of unity

(Analog for torsion points?)

$E: y^2 = x^3 + Ax + B$, $P = (x, y) \in E(K)$

Def: $H(P) = \begin{cases} H(x) & \text{if } P \neq \mathcal{O} \\ 1 & \text{if } P = \mathcal{O} \end{cases}$

$h(P) = \log(H(P))$

Prop: a) $\{P \in E(K) \mid h(P) \leq C\}$ is finite

b) $h(mP) = m^2 h(P) + \mathcal{O}_{E,m}(1)$

c) $h(P+Q) \leq 2h(P) + 2h(Q) + \mathcal{O}_E(1)$

Pf of Mordell-Weil Theorem: Choose $Q_1, \ldots, Q_r \in E(K)$ which represent the finitely many cosets of $E(K)/mE(K)$

Goal: Find some C such that

$\{Q_1, \ldots, Q_r\} \cup \{P \in E(K) \mid h(P) \leq C\}$

generates $E(K)$. Take any $P \in E(K)$, then we can write

$P = P_0 = mP_1 + Q_{i_1}$

$P_1 = mP_2 + Q_{i_2}$

$\vdots$

$P_{t-1} = mP_t + Q_{i_t}$

Some middle step: $P_{j-1} = mP_j + Q_{ij}$

$$h(mP_j) = h(P_{j-1} - Q_{ij}) \le 2h(P_{j-1}) + 2h(Q_{ij}) + C_1$$

$$\le 2h(P_{j-1}) + C_2 \quad \text{where } C_2 = 2\max\{h(Q_i)\} + C_1$$

but $h(mP_j) \ge m^2 h(P_j) - C_3$, so

$$h(P_j) \le \frac{2}{m^2} h(P_{j-1}) + C_4, \quad C_4 \text{ depends on } E, m, Q_1, \dots, Q_r$$

(Statement that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite for $m=1$ doesn't convey any info since $m \ge 2$)

Hence

$$h(P_t) \le \frac{2}{m^2} h(P_{t-1}) + C_4$$

$$\le \left(\frac{2}{m^2}\right)^2 h(P_{t-2}) + \left(\frac{2}{m^2} + 1\right) C_4$$

$$\le \left(\frac{2}{m^2}\right)^t h(P_0) + \left(\left(\frac{2}{m^2}\right)^{t-1} + \cdots + \left(\frac{2}{m^2}\right) + 1\right) C_4$$

$$\le \left(\frac{2}{m^2}\right)^t h(P_0) + \frac{1}{1 - \frac{2}{m^2}} C_4$$

$$\le \frac{1}{2^t} h(P_0) + 2C_4$$

We had $P = m^t P_t + \sum_{j=1}^{t} m^{j-1} Q_{ij}$, done.

How to make effective? need to find the $Q_1, \dots, Q_r$ (easy to find $\{P \in E(K) \mid h(P) \le C\}$, in principle). But $E(K)/mE(K) \hookrightarrow$ finite group (we know we showed $E(K)/mE(K)$ finite, and we don't know how to determine if an element of (finite group) came from $E(K)/mE(K)$)

$\alpha \in \overline{\mathbb{Q}}^\times$, then $h(\alpha^d) = d\, h(\alpha)$

$P \in E(K)$, then $h(mP) = m^2 h(P) + O_{E,m}(1)$

Thm (Neron–Tate) canonical height

$$\hat{h}(P) = \lim_{m\to\infty} \frac{1}{m^2} h(mP) \quad \text{exists}$$

$\lim_{m\to\infty} \frac{1}{m^3} h(mP)$ exists just always 0

and a) $\hat{h}(P) = h(P) + O_E(1)$

b) $\hat{h}(mP) = m^2 \hat{h}(P)$

The map $E(K) \times E(K) \to \mathbb{R}$

$$(P, Q) \longmapsto \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

is a bilinear form, non degenerate on $E(K)/$torsion

d) $\hat{h}(P) = 0 \iff P$ torsion pt. (analog of Kronecker's theorem)

Lehmer's conjecture

$\alpha \in \overline{\mathbb{Q}}^\times$, α not a root of unity

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]}$$

(c absolute constant (avoids silly $h(\sqrt{2}) = \frac{1}{2} h(2)$))

Elliptic version

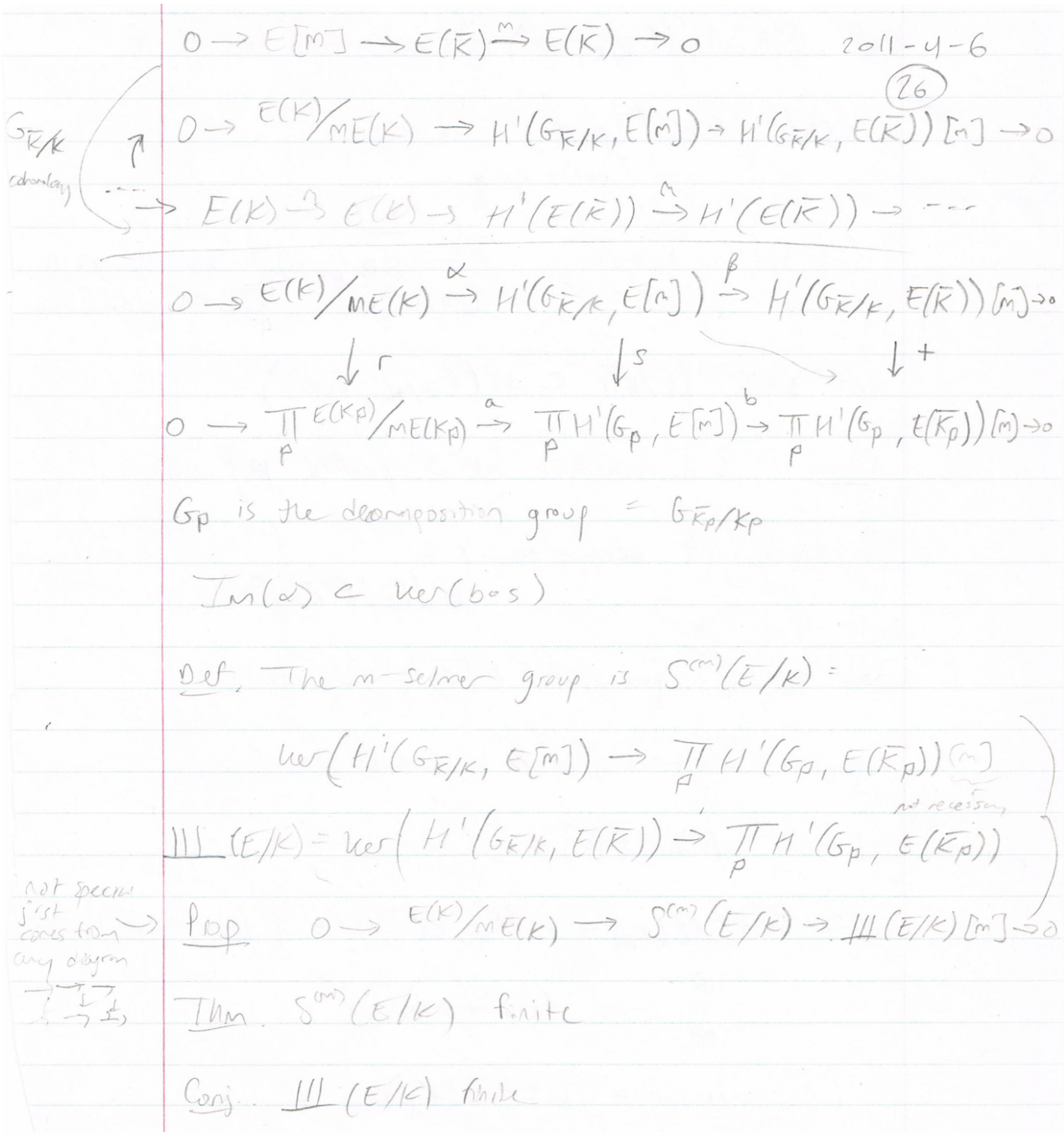
$$\hat{h}(P) \geq \frac{c_{E/K}}{[K(P):K]}$$

Lang's Conjecture

$E/\mathbb{Q}$, $P \in E(\mathbb{Q})$ non torsion

$\hat{h}(P) \geq c_1 \log|\mathrm{Disc}_E| - c_2$

Lecture 26 (2011-04-06)



Def $\xi \in H^1(G_{\bar{K}/K}, M)$ is unramified at p if

$\mathrm{Res}(\xi) \in H^1(I_p, M)$ is 0

I inertia group

Once fix an embedding $\bar{K} \hookrightarrow \bar{K_p}$, get specific group $I_p \subset G_p \subset G_{\bar{K}/K}$

Let $\xi \in S^{(m)}(E/K) \subset H^1(G_{\bar{K}/K}, E[m])$

Claim: ξ is unramified at p provided $p \nmid m\Delta_E$

↑ i.e., E stays an elliptic curve mod p

Pf We know ξ becomes trivial in $H^1(G_p, E(\bar{K_p}))[m]$

so there is a point $P \in E(\bar{K_p})$ such that

$\xi(\sigma) = \sigma(P) - P$ for all $\sigma \in G_p$

Notice $\xi(\sigma) \in E[m]$

$$0 \to E(K_p)/mE(K_p) \to H^1(G_p, E[m]) \to H^1(G_p, E(\bar{K_p}))[m] \to 0$$

$$R \quad \longrightarrow \quad (\sigma \mapsto \sigma(P) - P)$$

$\| \; mP$

since with $mP \in E(K_p)$

Now take $\tau \in I_p$, so τ fixes everything mod $\mathfrak{p}$

$\widetilde{\zeta(\tau)} = \widetilde{\tau(P) - P} \bmod \mathfrak{p} = \bar{\sigma} \bmod \mathfrak{p}$

$E[m] \hookrightarrow \widetilde{E[m]} \bmod \mathfrak{p}$

provided $p \nmid m$ and E has good reduction at p

$\therefore \zeta(\tau) = 0 \quad \forall \tau \in I_p$, hence ζ is unramified at p

Def M a finite $G_{\bar{K}/K}$-module
S finite set of primes

(e.g. $M = E[m]$, $S = \{p \mid m\Delta_E\}$)

$H^1(G_{\bar{K}/K}, M; S) = \{\zeta \in H^1(G_{\bar{K}/K}, M) \mid \zeta$ is unramified for all $p \notin S\}$

Prop. E/K, $S = \{p \mid m\Delta_E\}$. Then

$$S^{(m)}(E/K) \subset H^1(G_{\bar{K}/K}, E[m]; S)$$

Thm. $H^1(G_{\bar{K}/K}, M; S)$ is finite.

Pf ① Using inflation-restriction, can assume $G_{\bar{K}/K}$ acts trivially on M

② Let $m = \#M$, and adjoin $\mu_m \subset K$.

Let L = max abelian extension of K of exponent m that is unramified at every $p \notin S$

we have proved L/K finite

$$H^1(G_{\bar{K}/K}, M; S) \to \text{Hom}(G_{\bar{K}/K}, M; S) \hookrightarrow \text{Hom}(G_{L/K}, M)$$

finite

Example. $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$, $\alpha, \beta, \gamma \in \mathbb{Z}$

$$S = \{2\} \cup \{p \mid (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)\}$$

Then $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow S^{(2)}(E/\mathbb{Q}) \hookrightarrow (\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2})^S$

$\left(\langle -1, 17 \rangle / \text{squares}\right)^2$

$\text{rank}_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q}) \leq 2(\#S+1)$

$\text{rank}\, E(\mathbb{Q}) \leq 2\#S$

$y^2 = x^3 - 12x^2 + 20x = x(x-2)(x-10)$

$S = \{-1, 2, 5\}$ rank $\in 6$

(actually rank $= 1$)

BSD conjecture

a) $\text{ord}_{s=1} L(E,s) = \text{rank}\, E(\mathbb{Q})$

$$L(E,s) = \prod_{p \nmid \Delta_E} \frac{1}{1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}} \cdot \prod_{p \mid \Delta_E} \frac{1}{1 - \frac{a_p}{p^s}}$$

b) $L(E,s) = c_E (s-1)^{\operatorname{rank} E(\mathbb{Q})} + \cdots$

$\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y}$ $\qquad c_p = \#\left(E(\mathbb{Q}_p)/E_{ns}(\mathbb{Q}_p)\right)$

Γ_{pts} s.t. $\tilde{P}$ (mod p) is nonsingular

$\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$

Choose basis $P_1, \ldots, P_r$ for $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$

$R_E = \det(\langle P_i, P_j \rangle)$

Conjecture

$$c_E = \Omega_E \left(\prod_{p \mid \Delta_E} c_p \right) \frac{R_E \, \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2}$$

Lecture 27 (2011-04-08)

Elliptic Curves over $\mathbb{C}$ — 2011-4-8 (27)

Trig functions, $f(z+\omega) = f(z) \quad \forall z \in \mathbb{C}$

Def. A lattice in $\mathbb{C}$ is a subgroup of the form

$L = \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}\}$ for ω_1, ω_2 $\mathbb{R}$-linearly independent

Def. An elliptic function for L is a meromorphic function $f: \mathbb{C} \to \mathbb{C}$ such that $f(z+\omega) = f(z) \quad \forall z \in \mathbb{C}, \omega \in L$

Def. A fundamental domain for $\mathbb{C}/L$ is

$D = \{a + t_1\omega_1 + t_2\omega_2 \mid 0 \le t_1, t_2 < 1\} \xleftrightarrow{\text{bijection}} \mathbb{C}/L$

not a homeomorphism

Let $\overline{D}$ = closure of D

Thm. Let $f \in \mathbb{C}(\Lambda)$. If f has no poles, then f is constant. If f has no zeros, then f is constant

Pf f continuous on $\overline{D}$, hence bounded on $\overline{D}$, hence bounded on $\mathbb{C}$, hence by Liouville $\Rightarrow$ f constant (use $1/f$ for second part).

Given $f \in \mathbb{C}(L)$ and $\omega \in \mathbb{C}$,

$\operatorname{ord}_\omega f$ = order of zero (pole) at ω

$\operatorname{res}_\omega f$ = residue at ω

$$f(z) = (z-w)^{\operatorname{ord}_w(f)} g(z)$$

$$f(z) = \cdots + \frac{\operatorname{res}_w(f)}{z-w} + \cdots$$

$$\operatorname{res}_w(f) = \frac{1}{2\pi i} \int_{|z-w|=\varepsilon} \frac{f(z)}{z-w}\, dz$$

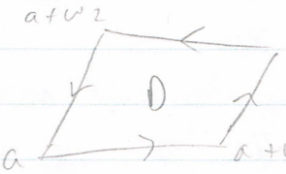
Prop. $f \in \mathbb{C}(L)$, then

a) $\sum_{w \in \mathbb{C}/L} \operatorname{ord}_w(f) = 0$

b) $\sum_{w \in \mathbb{C}/L} \operatorname{res}_w(f) = 0$

c) $\sum_{w \in \mathbb{C}/L} \operatorname{ord}_w(f) \cdot w =$

Pf. b) Cauchy Residue Thm, $\sum_{w \in R} \operatorname{res}_w(f) = \frac{1}{2\pi i} \int_{\partial R} f(z)\, dz$



(might have to move boundary)

$$2\pi i \sum_{w \in \mathbb{C}/L} \operatorname{res}_w(f) = \int_a^{a+w_1} + \int_{a+w_1}^{a+w_1+w_2} + \int_{a+w_1+w_2}^{a+w_2} + \int_{a+w_2}^{a}$$

$$= 0$$

a) $\operatorname{ord}_w f = \operatorname{res}_w \frac{f'}{f} = \operatorname{res}_w \frac{d}{dz} \log(f(z))$

$f'/f \in \mathbb{C}(L)$, use b) $\Rightarrow$ equals 0

c) HW. $\int_{\partial D} z \frac{f'(z)}{f(z)} dz$ look in book

What are some elliptic functions?

$\sum_{w \in L} \frac{1}{(z+w)^2}$? Doesn't quite converge

$f \in \mathbb{C}(L)$ f not constant $\Rightarrow$ # of poles ≥ 1

If # poles $= 1$, say $\operatorname{ord}_0 f = -1$

$\Rightarrow$ # zeros $= 1$ by a) but then by c) $z - t \in L$ Leave fingers in same contradiction

$\operatorname{ord}_t(f) = 1$

thus at least two poles

Weierstrass: double poles

Jacobi: poles at a and $-a$

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{w \in L \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

Thm. a) $\wp$ is absolutely convergent on all compact subsets of $\mathbb{C} - L$

b) $\wp(z) = \wp(-z)$ c) $\wp(z) \in \mathbb{C}(L)$

Pf b) $\frac{1}{(-z-w)^2} = \frac{1}{(z+w)^2}$

c) $\wp'(z) = -\frac{2}{z^3} + \sum_{w \neq 0} \frac{2}{(z-w)^3} = -2\sum_{w \in L} \frac{1}{(z-w)^3}$

clearly $\wp'(z) \in \mathbb{C}(L)$

so $\wp(z+w) = \wp(z) + c_w$ set $z = -\frac{w}{2}$

$\wp(\frac{w}{2}) = \wp(-\frac{w}{2}) + c_w$

equal

hence $c_w = 0$

Lecture 28 (2011-04-11)

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

2011-4-11

(28)

want to prove it is absolutely convergent on $\mathbb{C} - L$

Fix a $z \in \mathbb{C} - L$, suffices to show

$$\sum_{\substack{\omega \in L \\ |\omega| > B}} \left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| \quad \text{finite for some } B$$

($B = 2|z|+1$ will work)

$$= \sum_{|\omega|>B} \frac{1}{|\omega|^2} \left| \frac{1}{(1-\frac{z}{\omega})^2} - 1 \right|$$

$$= \sum_{|\omega|>B} \frac{1}{|\omega|^2} \left| \sum_{n=1}^{\infty} n \left(\frac{z}{\omega}\right)^{n-1} - 1 \right|$$

$$= \sum_{|\omega|>B} \frac{1}{|\omega|^2} \left| \sum_{n=2}^{\infty} n \left(\frac{z}{\omega}\right)^{n-1} \right|$$

$$= \sum_{n=2}^{\infty} n |z|^{n-1} \sum_{|\omega|>B} \frac{1}{|\omega|^{n+1}}$$

$$\leq \sum_{n=2}^{\infty} n |z|^{n-1} \sum_{k=B}^{\infty} \frac{\#\{\omega \in L \mid k \leq |\omega| < k+1\}}{k^{n+1}}$$

$$\leq \sum_{n=2}^{\infty} n |z|^{n-1} \sum_{k=B}^{\infty} \frac{c_L \cdot \text{Area}\{s \in \mathbb{C} \mid k \leq |s| < k+1\}}{k^{n+1}}$$

$$\leq \sum_{n=2}^{\infty} n |z|^{n-1} \sum_{k=B}^{\infty} \frac{c_L \pi (2k+1)}{k^{n+1}} \leq 3 c_L \pi \underbrace{\sum_{n=2}^{\infty} n |z|^{n+1} \sum_{k=B}^{\infty} \frac{1}{k^n}}_{\text{converges}}$$

HW: $\#\{\omega \in L \mid |\omega| \le B\} = \frac{\pi B^2}{\text{Area}(\mathcal{O}_L)} + O(B)$

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

$$= \frac{1}{z^2} + \sum_{\omega \in L}{}' \frac{1}{\omega^2} \left(\frac{1}{(1-\frac{z}{\omega})^2} - 1 \right)$$

$$= \frac{1}{z^2} + \sum_{\omega \in L}{}' \frac{1}{\omega^2} \sum_{n=2}^{\infty} n \left(\frac{z}{\omega}\right)^{n-1}$$

$$= \frac{1}{z^2} + \sum_{n=2}^{\infty} n z^{n-1} \left(\sum_{\omega \in L}{}' \frac{1}{\omega^{n+1}} \right)$$

Def. $G_n(L) = \sum_{\omega \in L}{}' \frac{1}{\omega^n}$. (Eisenstein series)

Prop. a) $G_n(L)$ absolutely convergent for $n \ge 3$ (add annuli)

b) n odd $\Rightarrow G_n(L) = 0$ (since $\omega \in L \iff -\omega \in L$)

Thm. In a neighborhood of 0,

$$\wp(z) = \frac{1}{z^2} + \sum_{n=2}^{\infty} n G_{n+1}(L) \cdot z^{n-1}$$

$$= \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(L) \, z^{2k}$$

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \cdots$$ — hint to cancel their poles

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20 G_6 z^3 + \cdots$$

$$\wp'(z)^2 - 4\wp(z)^3 = (-24G_4\tfrac{1}{z^2} - 80G_6 + \cdots) - 4(9G_4\tfrac{1}{z^2} + 15G_6 + \cdots)$$

$$= -60G_4\tfrac{1}{z^2} - 140G_6 + \cdots$$

$$\underbrace{\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6}_{\text{meromorphic, elliptic (i.e. in } \mathbb{C}(L))} = \underbrace{0z^2 + 0z^4 + \cdots}_{\text{holomorphic, vanishes at } z=0}$$

$\downarrow$ LHS is constant 0

Thus

$$\wp'(z)^2 = 4\wp(z)^3 - \underbrace{60G_4(L)}_{g_2(L)}\wp(z) - \underbrace{140G_6(L)}_{g_3(L)}$$

Theorem: a) $4x^3 - g_2(L)x - g_3(L)$ has distinct roots

b) The map $\phi: \mathbb{C}/L \longrightarrow \mathbb{P}^2(\mathbb{C})$

$z \longmapsto [\wp(z), \wp'(z), 1]$

is a holomorphic isomorphism (as Riemann surfaces) from $\mathbb{C}/L$ to $E(\mathbb{C}): y^2 = 4x^3 - g_2x - g_3$

c) ϕ is a group homomorphism

Pf. a) $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ because $\wp$ even $\Rightarrow \wp'$ odd

$\swarrow$

$$\wp'(\tfrac{\omega_1}{2}) = -\wp'(-\tfrac{\omega_1}{2}) = -\wp'(\tfrac{\omega_1}{2} - \omega_1) = -\wp'(\tfrac{\omega_1}{2})$$

hence $\wp'(\frac{\omega_1}{2}) = 0$, similarly $\wp'(\frac{\omega_2}{2}) = 0$, also $\wp'(\frac{\omega_1+\omega_2}{2}) = 0$

Let $\omega_3 = \omega_1 + \omega_2$

$\wp(\frac{\omega_i}{2})$ is a root of $4x^3 - g_2 x - g_3$ $1 \le i \le 3$

$\wp(z) - \wp(\frac{\omega_1}{2})$ — zero at $\frac{\omega_1}{2}$
— derivative also zero at $\frac{\omega_1}{2}$
exactly 2 poles (since $\wp$ has 2 poles)
hence exactly 2 zeros on $\mathbb{C}/L$

thus there are no other solutions to $\wp(z) = \wp(\frac{\omega_1}{2})$ other than $z = \frac{\omega_1}{2}$

thus $4x^3 - g_2 x - g_2 = 4\prod_{i=1}^{3}(x - \wp(\frac{\omega_i}{2}))$
distinct

b) Φ is injective

Suppose $\wp(z_1) = \wp(z_2)$ and $\wp'(z_1) = \wp'(z_2)$

Can assume $2z_1 \notin L$ first.

$\wp(z) - \wp(z_1)$ — zero at $z = z_1, z = -z_1$
— zero at $z = z_2$
2 poles $\Rightarrow$ 2 zeros

thus $z_2 \equiv \pm z_1 \bmod L$

If $z_2 \equiv -z_1 \bmod L$, then $\wp'(z_2) = \wp'(-z_1) = -\wp'(z_1)$
contradiction

If $2z_1 \in L$, then —

ϕ surjective: Let $(a,b) \in E(\mathbb{C})$

$\wp(z) - a$ elliptic, 2 poles $\Rightarrow$ it has a zero

So $\exists\, z_0$ with $\wp(z_0) = a$. Then $\wp'(z_0)^2 = b^2$,

so $\pm z_0$ works to get $\phi(z_0) = (a,b)$

Lecture 29 (2011-04-13)

$\phi : \mathbb{C}/L \to E(\mathbb{C})$
$z \longmapsto (\wp(z), \wp'(z))$

2011-4-13
29

Prop. ϕ is a homomorphism.

We need two facts: $\mathbb{C}(L) = \mathbb{C}(\wp(z), \wp'(z))$ (I)

(II) Let $D = \sum_w n_w w \in Div(\mathbb{C}/L)$, note
$div(f) = \sum ord_w(f)\, w$. We showed $div(f) \in L$.
In fact, $D = div(f) \Leftrightarrow D \in L$.

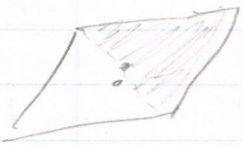
Pf. (I) Let $f \in \mathbb{C}(L)$

$f(z) + f(-z)$
$(f(z) - f(-z))\wp'(z)$
$\Big\}$ even elliptic functions

To show: $f \in \mathbb{C}(L)$, f even $\Rightarrow f \in \mathbb{C}(\wp(z))$

$$div(f) = \sum \underbrace{ord_w(f)}_{n_w} w = n_0(0) + \sum_{(\mathbb{C}/L)/(\pm 1)} n_w(w) + n_w(-w)$$

$$= n_0(0) + \sum_{(\mathbb{C}/L)/(\pm 1)} n_w((w) + (-w))$$



$div(\wp(z) - \wp(w)) = (w) + (-w) - 2(0)$

$g(z) = \prod_{w \in (\mathbb{C}/L)/(\pm 1)} (\wp(z) - \wp(w))^{n_w}$

$div(f(z)/g(z)) = N(0)$

$\Downarrow$

$div(f(z)/g(z)) = 0$

$div(g(z)) = n(0) + \sum n_w((w) + (-w))$

$f(z) = c \cdot g(z)$

$1 \to \mathbb{C}^\times \to \mathbb{C}(L)^\times \to Div^\circ(\mathbb{C}/L) \xrightarrow{\text{sum}} \mathbb{C}/L \to 0$

divisors of degree 0 ; $\mathbb{C}/L \cong E(\mathbb{C})$

$f \mapsto div(f)$

$Pic^\circ(\mathbb{C}/L) \overset{\text{def}}{=} Div^\circ(\mathbb{C}/L) / div(\mathbb{C}(L)^\times)$

$Pic^\circ : Var \to Grp$ (smooth projective $\to$ Grp.Var)

$V_1 \to V_2$ gives $Pic^\circ(V_1) \to Pic^\circ(V_2)$

$\mathbb{C}/L \longleftrightarrow E_L$

Maps between elliptic curves

Def. An *isogeny* $\phi : E_1 \to E_2$ is a morphism with $\phi(\mathcal{O}_1) = \mathcal{O}_2$

Thm. Every isogeny is a homomorphism

Prop. Let $\phi : \mathbb{C}/L_1 \to \mathbb{C}/L_2$ be holomorphic and $\phi(0) = 0$. Then $\exists \alpha \in \mathbb{C}^\times$ with $\alpha L_1 \subset L_2$, and $\phi(z) = \alpha z$ (i.e. $\phi(z \bmod L_1) = \alpha z \bmod L_2$)

Pf.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\psi} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/L_1 & \xrightarrow{\phi} & \mathbb{C}/L_2 \end{array}$$

$\psi(0) = 0$, ψ holomorphic (universal cover property)

Let $w \in L_1$, then

$\psi(z+w) - \psi(z) \in L_2$ So we get a map

$\mathbb{C} \to L_2$ (discrete) $\Rightarrow$

$z \mapsto \psi(z+w) - \psi(z)$

$\psi(z+\omega) = \psi(z) + c_\omega$ for all z

$\psi'(z+\omega) = \psi'(z)$ for all z and $\omega \in L_1$

$\psi' \in \mathbb{C}(L_1)$

but ψ holomorphic $\Rightarrow$ ψ' holomorphic

$\psi'(z) = \alpha$ for some $\alpha \in \mathbb{C}$

so $\psi(z) = \alpha z + \beta$, $\psi(0) = 0$

$\psi(z) = \alpha z$

$\phi(z) = \alpha z$

Thm 1 $\{\alpha \in \mathbb{C} \mid \alpha L_1 \subset L_2\} \longrightarrow \{$ holomorphic $\phi : \mathbb{C}/L_1 \to \mathbb{C}/L_2$, $\phi(0) = 0\}$

$\alpha \longmapsto (\phi_\alpha : z \mapsto \alpha z)$

is bijective

Pf. we just did onto. injective: $\phi_\alpha = \phi_\beta \Rightarrow$

$(\alpha - \beta) z \in L_1 \quad \forall z \in \mathbb{C}$

$\Rightarrow \alpha = \beta$

Thm 2. $\{$isogenies $E_1 \to E_2\} \to \{$ holomorphic $\phi : \mathbb{C}/L_1 \to \mathbb{C}/L_2$, $\phi(0) = 0\}$

Group $\mathrm{Hom}(E_1, E_2) \subset \mathbb{C}$

Ring $\mathrm{End}(E_1) \subset \mathbb{C}$

Lecture 30 (2011-04-15)

2011-4-15 (30)

(a) Thm. $\{\alpha \in \mathbb{C} : \alpha L_1 \subset L_2\} \xrightarrow{\text{bijective}} \{\text{holomorphic } \phi : \mathbb{C}/L_1 \to \mathbb{C}/L_2 \mid \phi(0)=0\}$

$\alpha \longmapsto \phi_\alpha(z) = \alpha z$

(b) $\{\text{isogenies } E_{L_1} \to E_{L_2}\} \xrightarrow{\text{bijective}} \{\text{holomorphic } \mathbb{C}/L_1 \to \mathbb{C}/L_2 \mid 0 \mapsto 0\}$

Pf. (a) last time,

(b) well-defined, injective

$$\begin{array}{ccc} E_{L_1}(\mathbb{C}) & \longrightarrow & E_{L_2}(\mathbb{C}) \\ \| & & \| \\ \mathbb{C}/L_1 & \longrightarrow & \mathbb{C}/L_2 \end{array}$$

Let $\phi_\alpha : \mathbb{C}/L_1 \to \mathbb{C}/L_2$ $\alpha L_1 \subset L_2$

Get a map $E_{L_1}(\mathbb{C}) \to E_{L_2}(\mathbb{C})$

$$(\wp(z, L_1), \wp'(z, L_1)) \longmapsto (\wp(\alpha z, L_2), \wp'(\alpha z, L_2))$$

Need to show $\wp(\alpha z, L_2), \wp'(\alpha z, L_2) \in \mathbb{C}(\wp(z, L_1), \wp'(z, L_1))$

Let $w \in L_1$ then (last time: $= \mathbb{C}(L_1)$)

$$\wp(\alpha(z+w), L_2) = \wp(\alpha z + \alpha w, L_2) = \wp(\alpha z, L_2) \quad \checkmark$$

$\alpha w \in L_2$

Thm. $V, W \subset \mathbb{P}^n(\mathbb{C})$ be smooth projective varieties. If $\phi : V(\mathbb{C}) \to W(\mathbb{C})$ is holomorphic, then it is algebraic.

Corollary. $E_{L_1} \cong E_{L_2} \iff \exists c \in \mathbb{C}^\times$ with $cL_1 = L_2$

Def. $\mathrm{End}(E) = \{\text{isogenies } E \to E\}$

$(\phi + \psi)(P) = \phi(P) + \psi(P)$

$(\phi\psi)(P) = \phi(\psi(P))$

$\mathbb{Z} \hookrightarrow \mathrm{End}(E)$

$n \mapsto (P \mapsto nP)$

Corollary. $\mathrm{End}(E_L) \cong \{\alpha \in \mathbb{C} \mid \alpha L \subset L\}$

Corollary. $E_L[n] = \ker\left(\mathbb{C}/L \xrightarrow{z \mapsto nz} \mathbb{C}/L\right) = \frac{1}{n}L/L$

If $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, this is $\cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cdot \omega_1 + \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cdot \omega_2$

Uniformization Thm. Let $E/\mathbb{C}$ be an elliptic curve

then $\exists! L$ such that $\mathbb{C}/L \to E(\mathbb{C})$

$(\wp, \wp')$

$g_2(L) = -a$

$g_3(L) = -b$

Thm. Let $E/\mathbb{C}$. Then

$\mathrm{End}(E) = \begin{cases} \mathbb{Z} \\ \text{order in a quadratic imaginary field} \end{cases}$ (CM)

Def. $K/\mathbb{Q}$ number field, an order is a subring $R \subset \mathcal{O}_K$ with $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$.

Lecture 31 (2011-04-18)

$z \longmapsto (\wp(z), \wp'(z))$

$\mathbb{C}/L \longrightarrow E_L(\mathbb{C})$ 2011-4-18

(31)

$\mathrm{End}(E_L) \cong \mathrm{End}(L) = \{\alpha \in \mathbb{C} \mid \alpha L \subset L\}$

Invariant differential

$$\omega_L = \frac{dx}{y} = \frac{d\wp(z)}{\wp'(z)} = dz$$

Given $\alpha \in \mathrm{End}(L)$, get $[\alpha]_{E_L} \in \mathrm{End}(E_L)$, make precise by requiring $[\alpha]_{E_L}^* \omega_{E_L} = \alpha \omega_{E_L}$ (alternative would be $\bar{\alpha} \omega_{E_L}$)

$\phi : E_1 \to E_2 \qquad \phi \circ [\alpha]_{E_1} = [\alpha]_{E_2} \circ \phi$

K quadratic imaginary field, R ring of integers of K

$\mathcal{E}\ell\ell(R) = \{E/\mathbb{C} \mid \mathrm{End}(E) = R\} / \mathbb{C}\text{-isomorphism}$

$\cong \{\text{lattices } L \subset \mathbb{C} \mid \mathrm{End}(L) = R\} /$ homothety

Is there an $E/\mathbb{C}$ with $\mathrm{End}(E) = R$? Yes.

E_R (R is a lattice) $\quad E_R(\mathbb{C}) = \mathbb{C}/R$

If $\mathfrak{a}$ is any fractional ideal, $E_{\mathfrak{a}} \in \mathcal{E}\ell\ell(R)$

Get $Cl(K) \longrightarrow \mathcal{E}\ell\ell(R)$ (action, simply transitive)

$\mathfrak{a} \longmapsto E_{\mathfrak{a}}$

$y^2 = x^3 + x$, $R = \mathbb{Z}[i]$

$[i](x,y) = (-x, iy)$

$y^2 = x^3 + 1$ $R = \mathbb{Z}[\zeta_3]$

$[\zeta_3](x,y) = (\zeta_3 x, y)$

$y^2 = x^3 + 4x^2 + 2x$ $R = \mathbb{Z}[\sqrt{-2}]$

$[\sqrt{-2}](x,y) = \left(-\frac{1}{2}\left(x + 4 + \frac{2}{x}\right), -\frac{1}{2\sqrt{-2}}\, y\left(1 - \frac{2}{x^2}\right)\right)$

$\ker[\sqrt{-2}] = \{\mathcal{O}, (0,0)\}$

HW. Let $R \subset \mathbb{Q}(\sqrt{-D})$ be an order, prove $\exists! c \in \mathbb{N}$ with $R = \mathbb{Z} + c\mathcal{O}_K$ (c is the conductor)

Pf of Thm. $E = E_L$, $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$

$\mathrm{End}(E) = \{\alpha \in \mathbb{C} \mid \alpha L \subset L\}$

$$\alpha\omega_1 = a\omega_1 + b\omega_2$$
$$\alpha\omega_2 = c\omega_1 + d\omega_2$$

$$\begin{pmatrix} \alpha - a & -b \\ -c & \alpha - d \end{pmatrix} \underbrace{\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}}_{\text{not } 0} = 0$$

$$\det = \alpha^2 - (a+d)\alpha + (ad - bc) = 0$$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, because $\alpha = a + b\frac{\omega_2}{\omega_1}$, $\frac{\omega_2}{\omega_1} \in \mathbb{C} - \mathbb{R}$, $\alpha \notin \mathbb{Z}$

so $\mathbb{Q}(\alpha) = \mathbb{Q}(\frac{\omega_2}{\omega_1})$, quadratic imaginary

$R = \mathrm{End}(E) \subset K$, $R \otimes \mathbb{Q} = K$ ⌐

If $\mathfrak{a} \subset K$ a fractional ideal; L a lattice

$$\mathfrak{a}L = \{a_1\lambda_1 + \cdots + a_n\lambda_n \mid a_i \in \mathfrak{a},\ \lambda_i \in L\}$$

Thm. a) $L \subset \mathbb{C}$ a lattice, with $\mathrm{End}(\mathbb{C}_L) = R$, $\mathfrak{a}$, $\mathfrak{b}$ fractional ideals

1) $\mathfrak{a}L$ is a lattice
2) $E_{\mathfrak{a}L} \in \mathcal{E}\ell\ell(R)$
3) $E_{\mathfrak{a}L} \cong E_{\mathfrak{b}L} \iff \bar{\mathfrak{a}} = \mathfrak{b}$ in $Cl(K)$

b) We get a well-defined action of $Cl(K)$ on $\mathcal{E}\ell\ell(R)$

$$\bar{\mathfrak{a}} * E_L = E_{\bar{\mathfrak{a}}^{-1}L}$$

and this action is simply transitive:

$$\bar{\mathfrak{a}} * E_L = \bar{\mathfrak{b}} E_L \iff \bar{\mathfrak{a}} = \bar{\mathfrak{b}}$$

So $\#Cl(K) = \#\mathcal{E}\ell\ell(R)$

Pf 1) We can find $d \in \mathbb{Z}$, $d \geq 1$ with $d\mathfrak{a} \subset R$ and $dR \subset \mathfrak{a}$, i.e. $dR \subset \mathfrak{a} \subset \frac{1}{d}R$. Since $\mathrm{End}(L) = R$, we have $RL = L$. Thus

$$\underbrace{dRL}_{=dL} \subset \mathfrak{a}L \subset \underbrace{\tfrac{1}{d}RL}_{=\frac{1}{d}L}$$

dL: spans; $\frac{1}{d}L$: discrete

2) $\mathrm{End}(E_{aL}) = \mathrm{End}(aL) = \{\alpha \in \mathbb{C} \mid \alpha aL \subset aL\}$ (mult by a^{-1})

$= \{\alpha \in \mathbb{C} \mid \alpha RL \subset RL\} = \{\alpha \in \mathbb{C} \mid \alpha L \subset L\} =$

$\mathrm{End}(L) = \mathrm{End}(E_L) = R$

3) ($\Leftarrow$) $\bar{a} = \bar{b} \Rightarrow a = cb \Rightarrow a, b$ homothetic

$\Rightarrow E_{aL} \cong E_{bL}$

($\Rightarrow$) $E_{aL} \cong E_{bL} \Rightarrow aL = cbL$ for some

$c \in \mathbb{C} \Rightarrow \begin{cases} ac^{-1}b^{-1}L = L \\ a^{-1}cbL = L \end{cases}$

$\mathrm{End}(L) = R$, so $\begin{matrix} ac^{-1}b^{-1} \subset R \\ a^{-1}cb \subset R \end{matrix} \Rightarrow c \in K \Rightarrow a = cb$

hence $\bar{a} = \bar{b}$

b) let $E_1, E_2 \in \mathcal{E}\ell\ell(R)$

$L_1 = \mathbb{Z} + \mathbb{Z}\tau_1$ for E_1

$L_1 = \mathbb{Z} + \mathbb{Z}\tau_2$ for E_2

From before, $\tau_1, \tau_2 \in K$ $(\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2) = K)$

$L_1 = L_2$ are fractional ideals of K

$\| \quad \|$

$a_1 \quad a_2$ $\qquad E_1 = E_{L_1} = E_{a_1}$

$\overline{a_1 a_1^{-1}} * E_1 = \overline{a_1 a_2^{-1}} * E_{a_1} = E_{a_2} = E_2$

hence transitive

Simply transitive by 3.

Example. $L = \mathbb{Z}[i]$, $\mathrm{End}(E_L) = \mathbb{Z}[i]$

$E_L : y^2 = 4x^3 - g_2(L)x - g_3(L)$

$g_3(L) = g_3(iL) = i^{-6} g_3(L) = -g_3(L) \Rightarrow$

$g_3(L) = 0$

so $[i](x, y) = (-x, iy)$

(Check this is the right one – i.e., $\int \frac{dx}{y} = i \frac{dx}{y}$)

Thm Hurwitz. $g_2(\mathbb{Z}[i]) = 64 \left(\int_0^1 \frac{dt}{\sqrt{1-t^4}} \right)^4$

period

$E/\mathbb{C}$, $K/\mathbb{Q}$, $\mathrm{End}(E) = \mathcal{R}$

Goal #1 $K(j(E)) =$ Hilbert class field of K

Let $\sigma_{\mathfrak{p}} = (\mathfrak{p}, K(j(E))/K)$, write $E = E_{\mathfrak{L}}$

$\sigma_{\mathfrak{p}}(j(E_{\mathfrak{L}})) = j(\bar{\mathfrak{p}} * E_{\mathfrak{L}}) = j(E_{\mathfrak{p}^{-1}\mathfrak{L}})$

In general, $\sigma_{\mathfrak{p}}($analytic function of $\gamma) =$ analytic function of $\mathfrak{p}^{-1}\gamma$

Note that $\sigma \in \mathrm{Aut}(\mathbb{C})$, in general

$$\sigma\left(\sum_{n=0}^{\infty} a_n\right), \quad a_n \in \overline{\mathbb{Q}}$$
$$\neq \sum_{n=0}^{\infty} \sigma(a_n)$$

Lecture 32 (2011-04-20)

2011-4-20 (32)

Prop. a) $E/\mathbb{C}$, $\sigma \in \mathrm{Aut}(\mathbb{C})$
Then $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$

b) If E has CM, then $j(E) \in \overline{\mathbb{Q}}$.

c) $\mathcal{E}\ell\ell(R) = \dfrac{\{E/\overline{\mathbb{Q}} : \mathrm{End}(E) = R\}}{\overline{\mathbb{Q}}\text{-isomorphism}}$

Pf. a) $\mathrm{End}(E) \xrightarrow{\sim} \mathrm{End}(E^\sigma)$ $\qquad E^\sigma = \sigma(E)$, $\phi^\sigma = \sigma(\phi)$
$\phi \longmapsto \phi^\sigma$
$\gamma^{\sigma^{-1}} \longmapsto \gamma$

b). Let $E \in \mathcal{E}\ell\ell(R)$ (really an equivalence class)

Then $\forall \sigma \in \mathrm{Aut}(\mathbb{C})$, $E^\sigma \in \mathcal{E}\ell\ell(R)$

$\dfrac{\{E^\sigma : \sigma \in \mathrm{Aut}(\mathbb{C})\}}{\text{isomorphism}} \subseteq \underbrace{\mathcal{E}\ell\ell(R)}_{\text{finite}}$ $\qquad \#\mathcal{E}\ell\ell(R) = \#Cl(R)$

$\{j(E^\sigma) : \sigma \in \mathrm{Aut}(\mathbb{C})\}$

$\{j(E)^\sigma : \sigma \in \mathrm{Aut}(\mathbb{C})\}$ $\qquad E^\sigma : y^2 = x^3 + A^\sigma x + B^\sigma$

finite

Hence $j(E)$ algebraic and $[\mathbb{Q}(j(E)) : \mathbb{Q}] \le h_K$

c) follows from a) + b)

$R \longrightarrow \mathrm{End}(E)$
$\alpha \longmapsto [\alpha]_E$

Thm. a) $E \in \mathcal{E}\ell\ell(R)$ $\alpha \in R$, $\sigma \in \mathrm{Aut}(\mathbb{C})$

$([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma}$

b) $E \in \mathcal{E}\ell\ell(R)$, say E defined over some field L
$K = R \otimes_{\mathbb{Z}} \mathbb{Q}$

Then $\mathrm{End}(E) = \mathrm{End}_{LK}(E)$

Pf. a) $\omega_E = \frac{dx}{y}$ $\quad [\alpha]_E^* \omega_E = \alpha \omega_E$

$\omega_{E^\sigma} = \frac{dX}{Y}$

so $(\omega_E)^\sigma = \omega_{E^\sigma}$

$E: y^2 = x^3 + Ax + B$
$E^\sigma: Y^2 = X^3 + A^\sigma X + B^\sigma$

$(([\alpha]_E)^\sigma)^* \omega_{E^\sigma}^\sigma = \alpha^\sigma \omega_{E^\sigma}^\sigma$

but $(([\alpha]_E)^\sigma)^* \omega_{E^\sigma} = \alpha^\sigma \omega_{E^\sigma} = ([\alpha^\sigma]_{E^\sigma})^* \omega_{E^\sigma}$

$\mathrm{End}(E) \hookrightarrow \mathrm{End}(\text{differential forms})$
$\phi \longmapsto \phi^*$

because $\phi = [\alpha]_E$ for some α and $[\alpha]_E^* \omega_E = \alpha \omega_E$
so kernel $= \{\alpha = 0\}$

this because they have the same action,
$([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma}$

b) $[\alpha] \in \mathrm{End}(E)$, where E/L

If σ fixes LK, then $E^\sigma = E$ and $\alpha^\sigma = \alpha$

So $([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma} = [\alpha]_E$

so $[\alpha]_E$ fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/LK)$

Thm.

Corollary. $E \in \mathcal{E}\ell\ell(R)$, then $K(j(E), E_{tors})/K(j(E))$ is an abelian extension

Pf. Let $H = K(j(E))$, $L = H(E[m])$

Enough to show L/H is abelian. We have

$$\rho : G_{L/H} \hookrightarrow \mathrm{Aut}(E[m]) = GL_2(\mathbb{Z}/m\mathbb{Z})$$
$$\sigma \longmapsto (P \mapsto P^\sigma)$$

Notice that if $\phi \in R \cong \mathrm{End}(E)$, $\phi^\sigma = \phi$ $\forall \sigma \in G_{L/H}$

$$\rho(G_{L/H}) \subset \mathrm{Aut}_{R/mR}(E[m]) \cong (R/mR)^\times$$

($\mathrm{Aut}_{R/mR}$: anything R/mR-acts trivially)

$E[m] = \frac{1}{m}L/L$ and $RL = L$ because $E[m] \cong$ free R/mR-module of rank 1

$\rho : G_{L/H} \hookrightarrow (R/mR)^\times$

Thm. $\exists\ C_E$ with $[(R/mR)^\times : \rho(G_{L/H})] \leq C_E$

Thm (Serre). If $\exists$ doesn't have C_E, $\exists\ C_E$ with

$$[GL_2(\mathbb{Z}/m\mathbb{Z}) : \rho(G_{L/H})] \leq C_E$$

- $G_{\bar{K}/K}$ acts on $Cl(R)$
- $Cl(R)$ acts simply transitively on $Ell(R)$

So fix some $E \in Ell(R)$, get a map

$$F_E : G_{\bar{K}/K} \to Cl(R) \qquad \bar{\alpha}^* E_L \overset{\text{as}}{=} E_{\alpha^{-1}L}$$

$$\sigma \longmapsto F(\sigma) \quad \left(\begin{array}{c}\text{Unique} \\ \text{such that} \\ F(\sigma) * E = E^\sigma\end{array}\right)$$

Thm. F is a homomorphism, F is independent of E

Lecture 33 (2011-04-22)

$K/\mathbb{Q}$, $R = \mathcal{O}_K$, $E \in \mathcal{E}\ell\ell(R)$ 2011-4-22 (33)

$F: Gal(\bar{K}/K) \longrightarrow Cl(R)$ defined by

$\sigma \longmapsto F(\sigma)$ such that $F(\sigma) \cdot E = E^{\sigma}$

Thm. a) F is a homomorphism

b) F is independent of the choice of $\bar{E}$

Pf a) easy from the def

b) see book (key: show $(\bar{\alpha} * E)^{\sigma} = \bar{\alpha} * E^{\sigma}$

Thm. $E \in \mathcal{E}\ell\ell(R)$

a) $K(j(E)) = H$ Hilbert class field of K

b) $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}] = h$

c) $\{ j(E)^{\sigma} \mid \sigma \in G_{\bar{K}/K} \} = \{ j(E') \mid E' \in \mathcal{E}\ell\ell(R) \}$

d) $j(E)^{(\alpha, H/K)} = j(\bar{\alpha} * E)$

Lemma There is a finite set of primes $S \subset \mathbb{Z}$ such that for all $p \notin S$ that split as $p = \mathfrak{P}_1\mathfrak{P}_2$ in K,

$$F(\sigma_{\mathfrak{P}}) = \bar{p} \in Cl(R)$$

Frobenius, $(\mathfrak{P}, K^{ab}/K)$

Pf (Lemma ⇒ Thm) $F: G_{\bar{K}/K} \to Cl(R)$

Let L = fixed field of $\ker(F)$, so

$F: G_{L/K} \hookrightarrow Cl(R)$

$G_{\bar{K}/L} = \ker(F) = \{\sigma \in G_{\bar{K}/K} \mid F(\sigma) = 1\}$

$= \{\sigma \in G_{\bar{K}/K} \mid F(\sigma) * E \cong E\}$

$= \{\sigma \in G_{\bar{K}/K} \mid E^\sigma = E\} = \{\sigma \in G_{\bar{K}/K} \mid j(E^\sigma) = j(E)\}$

$= \{\sigma \in G_{\bar{K}/K} \mid j(E)^\sigma = j(E)\} = G_{\bar{K}/K(j(E))}$

so $L = K(j(E))$.

Claim $I(\mathfrak{C}_{L/K}) \xrightarrow{(\cdot, L/K)} G_{L/K} \xrightarrow{F} Cl(R)$ ($\mathfrak{C}_{L/K}$: conductor of L/K)

$F((\mathfrak{a}, L/K)) = \bar{\mathfrak{a}}$

Pf of Claim, use the fact that $I(\mathfrak{C}_{L/K})/P(\mathfrak{C}_{L/K})$ is finite and Dirichlet's thm (generally, Tchebotarev thm) guarantees each ideal class in contains infinitely many degree 1 prime ideals. So we can find $\mathfrak{p}$ a prime ideal (i.e. norm down to $\mathbb{Q}$ = prime)

with $\bar{a} = \bar{p}$ in $I(C_{L/K})/P(C_{L/K})$.

and $N_{K/\mathbb{Q}} \mathfrak{P} = p \notin S$ (by Lemma, infinitely many primes – finitely many = infinitely many)

$a = \beta p$ for some $\beta \equiv 1 \bmod C_{L/K}$

Lemma says $F((p, L/K)) = \bar{p} \in Cl(R)$

$(a, L/K) = (\beta p, L/K) = (p, L/K)$ because $\beta \equiv 1 \bmod C_{L/K}$

$F((a, L/K)) = \bar{\mathfrak{P}} = \bar{a}$ ✓

In particular, $F((\alpha R, L/K)) = \overline{\alpha R} = 1$ in $Cl(R)$

F is injective on $G_{L/K}$, so $(\alpha R, L/K) = 1$

for all (Calmostly) principal ideals αR with $(\alpha R, L/K) = 1$

this forces $G_{L/K} = (1)$ ("too many" things going to 1)

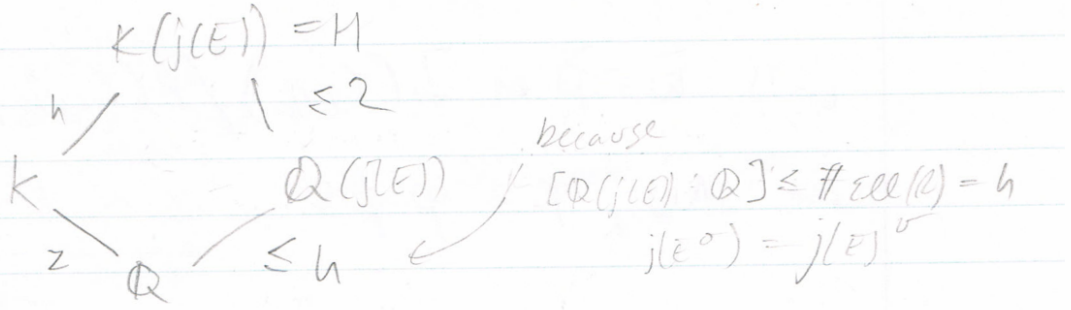
so L/K unramified, so $L \subset H$

but $I_K \twoheadrightarrow Cl(R)$ so $[L:K] \geq h$

$F((a, L/K)) = \bar{a}$

$F: G_{L/K} \twoheadrightarrow Cl(R)$ So $L = H$

this is a), and half of b)



So we must actually have $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h$

c) follows because we know $Cl(R)$ acts transitively on $Ell(R)$ and $F : G_{L/K} \twoheadrightarrow Cl(R)$

$\Rightarrow G_{L/K}$ acts transitively on $Ell(R)$

d) claim says $F((a, L/K)) = a$

$\Rightarrow E^{(a, L/K)} = F((a, L/K)) * E = \bar{a} * E$

from claim, now take j's

$K = \mathbb{Q}(\sqrt{-D})$, $R = \mathbb{Z}[\tau]$, $\tau = \frac{D + \sqrt{-D}}{2}$

$g_2(D + \tau\mathbb{Z})$
$g_3(D + \tau\mathbb{Z})$

$j = 1728 \frac{g_2^3}{g_2^3 - 27 g_3^2}$

$G_k(D + \tau\mathbb{Z}) = \sum_{m,n \in \mathbb{C}}$

$q = e^{2\pi i \tau}$

$j(\tau) = \frac{1}{q} + \sum_{n \geq 0} c_n q^n \quad c_n \in \mathbb{Z}$

Lecture 34 (2011-04-25)

$I(\mathfrak{b})$ = fractional ideals prime to $\mathfrak{b}$ 2011-4-25

$P(\mathfrak{b}) = \{(\alpha) \mid \gcd((\alpha), \mathfrak{b}) = 1\}$ (34)

$P_1(\mathfrak{b}) = \{(\alpha) \mid \alpha \equiv 1 \bmod \mathfrak{b}\}$

lemma. $I(\mathfrak{b})/P(\mathfrak{b}) \xrightarrow{\sim} I(1)/P(1) = Cl(R)$

Pf. $I(\mathfrak{b}) \to I(1)/P(1)$

$\ker = I(\mathfrak{b}) \cap P(1) = P(\mathfrak{b})$, so injective

Let $\mathfrak{a} \in I(1)$, look at $\bar{\mathfrak{a}} \in Cl(R)$. By

Dirichlet, $\exists$ prime $\mathfrak{p} \in \bar{\mathfrak{a}}$ with $\mathfrak{p} \nmid \mathfrak{b}$ (only finitely many primes dividing $\mathfrak{b}$)

Then $\mathfrak{p} \in I(\mathfrak{b}) \leftrightarrow \bar{\mathfrak{p}} = \bar{\mathfrak{a}}$

Prop. L/K abelian, Suppose $P(C_{L/K}) \subseteq \ker(\cdot, L/K)$

Then $L \subset H$ = Hilbert class field.

Pf. Replace L by LH, note $C_{LH/K} = C_{L/K}$

Know $H \subset L$, so now want to show $H = L$.

$$\begin{array}{ccc} \frac{I(C_{L/K})}{P(C_{L/K})} & \xrightarrow{(\cdot, L/K)} & G_{L/K} \\ \text{lemma} \downarrow & & \downarrow \text{restriction} \\ Cl(R) = \frac{I(1)}{P(1)} & \xrightarrow[\sim]{(\cdot, H/K)} & G_{H/K} \end{array}$$

Thus

$$\#G_{H/K} = \#\,Cl(R) = \#\frac{I(C_{L/K})}{P(C_{L/K})} \geq \#G_{L/K} \geq \#G_{H/K}$$

Thus $G_{H/K} = G_{L/K}$; so $L = H$.

Topics to prove Lemma

Frobenius map and inseparability

$E: y^2 = x^3 + Ax + B \qquad E^{(p)}: y^2 = x^3 + A^p x + B^p$

The Frobenius map $\phi_p : E \to E^{(p)}$ is $(x, y) \mapsto (x^p, y^p)$

ϕ_p is purely inseparable:

Def. Let $\phi : C_1 \to C_2$ be a non-constant morphism between nonsingular projective curves

$$\phi^* : k(C_2) \to k(C_1)$$
$$f \longmapsto f \circ \phi$$

$$\deg(\phi) = [k(C_1) : \phi^* k(C_2)]$$

$\deg(\phi_p) = p \qquad \deg_i(\phi) =$ inseparability degree of $k(C_1)/\phi^* k(C_2)$

Prop. If $\phi : C_1 \to C_2$ is inseparable, then ϕ factors as $C_1 \xrightarrow{\varphi_p} C_1^{(q)} \xrightarrow{\psi} C_2$ with $\phi = \psi \circ \varphi_p$.

Pf. Given L/K, char $= p$, can write

L
| purely inseparable
M
| separable
K

How can we tell whether ϕ is inseparable?

$f(x)$ irreducible $\in K[x]$, $K(\alpha)/K$ inseparable $\iff$ $f(\alpha) = 0$, $f'(\alpha) = 0 \iff f'(x) = 0$

Let ω = differential 1-form on C_2

$\omega = f\,dg$ where $f, g \in k(C)$

$\phi : C_1 \to C_2$, ω on C_2

$\phi^* \omega = (\phi^* f)\, d(\phi^* g)$

Prop $\phi: C_1 \to C_2$ is inseparable iff

$\phi^* \omega = 0$, where $\omega \neq 0$ is a 1-form on C_2

Pf. ϕ insep $\iff \phi = \gamma \circ \phi_p$ some

$\gamma: C_1^{(p)} \to C_2$

Corollary. If $p \nmid n$ then $n + m\phi_p$ is separable

If. $(n + m\phi_p)^* \omega = n^* \omega + m\phi_p^* \omega$

$\neq 0$

Used to prove $\#E(\mathbb{F}_p) = p + 1 - a$, $|a| < 2\sqrt{p}$

$(p, 4/k)\ E = (\overline{p} + E)$ Frobenius

$E \longrightarrow \overline{p}^* E$ inseparable when reduce mod p

Reduction of isogenies mod $\mathfrak{p}$

good reduction: E/L, L number field

$\tilde{E}$ mod $\mathfrak{p}$: $y^2 = x^3 + \tilde{A}x + \tilde{B}x$

If $\phi: E \to E$, can reduce $\tilde{\phi}: \tilde{E} \to \tilde{E}$

Thm $\deg(\widehat{\phi}) = \deg(\phi)$

Pf idea. Look at action on torsion points

because $E[\ell] \to \widetilde{E}[\ell]$ is an isomorphism if $\beta \nmid \ell$.

$$\begin{array}{ccc} E[\ell] & \xrightarrow{\phi} & E[\ell] \\ \downarrow & & \downarrow \\ \widetilde{E}[\ell] & \xrightarrow[\widehat{\phi}]{} & \widetilde{E}[\ell] \end{array}$$

Lecture 35 (2011-05-04)

Main Thm. $j(E)^{(\mathfrak{a}, K^{ab}/K)} = j(\overline{\mathfrak{a}}^{*}E)$ 2011-5-4 (35)

Lemma. $\exists$ finite set of primes S such that if $p \notin S$, p splits as $pR = \mathfrak{P}\mathfrak{P}'$ in R

Then $j(E)^{(\mathfrak{P}, K^{ab}/K)} = j(\overline{\mathfrak{P}}^{*}E)$

($(\mathfrak{P}, K^{ab}/K)$: p-power Frobenius)

Pf. $Ell(R) = \{E_1, \dots, E_n\}$ with $E_i/\mathbb{Q}$
Take some finite Galois L/K

Let $\mathfrak{b}$ be an ideal with $\overline{\mathfrak{b}} = \overline{\mathfrak{p}}^{-1}$ in $Cl(R)$, $\mathfrak{P} \nmid \mathfrak{b}$
$p = \beta R$

$$\begin{array}{ccccccc}
\mathbb{C}/\Lambda & \xrightarrow[z \mapsto z]{} & \mathbb{C}/\mathfrak{p}^{-1}\Lambda & \xrightarrow[z \mapsto z]{} & \mathbb{C}/\mathfrak{b}^{-1}\mathfrak{p}^{-1}\Lambda = \mathbb{C}/\beta\Lambda & \xrightarrow[z \mapsto \beta^{-1}z]{} & \mathbb{C}/\Lambda \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
E & \xrightarrow{\phi} & \overline{\mathfrak{p}}^{*}E & \xrightarrow{\psi} & \overline{\mathfrak{p}\mathfrak{b}}^{*}\Lambda & \xrightarrow{\qquad\lambda\qquad} & E
\end{array}$$

$\lambda \circ \psi \circ \phi$ is inseparable

$(\lambda \circ \psi \circ \phi)^{*}\omega_E = (\lambda \circ \psi \circ \phi)^{*}dz = d((\lambda \circ \psi \circ \phi)(z)) = d(\beta z) =$

$\beta\, dz = \beta\, \omega_E$

Reduce mod $\mathfrak{P}$.

$$(\tilde{\lambda}\circ\tilde{\tau}\circ\tilde{\phi})^*\tilde{\omega}_E = \tilde{\beta}\,\tilde{\omega}_{\tilde{E}} \bmod \mathfrak{P}$$

$$= \tilde{0} \bmod \mathfrak{P}$$

So $\tilde{\lambda}\circ\tilde{\tau}\circ\tilde{\phi}$ is inseparable

$\mathfrak{p}\mathfrak{b} = \beta R$, so $\mathfrak{P} \mid \mathfrak{p} \mid \beta$

$\deg(\tilde{\lambda}) = \deg(\lambda) = 1$ because isomorphism

$\deg(\tilde{\tau}) = \deg(\tau) = N_{K/\mathbb{Q}}(\mathfrak{b})$ ← prime to $\mathfrak{p}$

$\deg(\tilde{\phi}) = \deg(\phi) = N_{K/\mathbb{Q}}(\mathfrak{p}) = p$

$\tilde{\phi}$ is inseparable and has deg p

$$\tilde{E} \xrightarrow{\tilde{\phi}} \widetilde{\bar{\mathfrak{p}}^* E} \bmod \mathfrak{P}$$

Frob_p ↘ $\tilde{E}^{(p)}$ ↗ $\deg(l)$ (hence isomorphism)

$$j(\widetilde{\bar{\mathfrak{p}}^* E}) = j(\tilde{E}^{(p)}) = j(\tilde{E})^p \bmod \mathfrak{P}$$

$$j(E)^p \equiv j(E)^{(\mathfrak{p},L/K)} \bmod \mathfrak{P} \text{ by def of Artin map}$$

$\uparrow \sigma_{\mathfrak{p}}$ for convenience

$j(E)^p \equiv j(E)^{(p,\, 4/(c))} \equiv j(E^{\sigma_p}) \pmod{\mathfrak{P}}$

$j(\bar{\mathfrak{p}} * E) \equiv j(E^{\sigma_p}) \pmod{\mathfrak{p}}$

this is one of $j(E_1), \ldots, j(E_n)$

$j(\bar{\mathfrak{p}} * E) = j(E^{\sigma_p})$ since $\mathfrak{p}$ was assumed to be prime of good reduction

Lecture 36 (2011-05-06)

$E \in Ell(R)$ $R = \mathcal{O}_K$ Last time 2011-5-6 (36)

Thm. a) $H = K(j(E))$

b) $j(E)^{(a, H/K)} = j(\bar{a} * E)$

Goal: Generate K^{ab}

Analogy: $\mathbb{Q}^{ab} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)$ $\zeta_n^{((a), \mathbb{Q}^{ab}/\mathbb{Q})} = \zeta_n^{|a|}$ for $(a, n) = 1$

Complication: adding in torsion points is not guaranteed to create abelian extensions

$P \in E_{tors}$ $H(P)$ / H / K not abelian

fix this by only adding x coordinate

cause: automorphisms of $\bar{E}$

Fix $E: y^2 = x^3 + Ax + B$ $A, B \in H = K(j(E))$

Def. $P \in E(\bar{K})$, $h(P)$ (not height) $= \begin{cases} x(P) & \text{if } AB \neq 0 \\ x(P)^3 & \text{if } A = 0 \\ x(P)^2 & \text{if } B = 0 \end{cases}$

Thm. Let $\mathfrak{d} \subset R$ be an ideal. Then $K(j(\bar{E}), h(\bar{E}[\mathfrak{d}]))$

is the ray class field of K of conductor $\mathfrak{d}$ (or maybe dividing $\mathfrak{d}$)

abelian
- $H(E[\vec{a}])$ — if $AB \neq 0$, deg $= 2^r$
- $H(h(E[\vec{a}]))$
- $K(j(E)) = H$ — abelian

looks like a generalized dihedral group

Lemma For all but finitely many degree 1 primes $\mathfrak{p}$ (i.e. principal, since $Cl(K) \xrightarrow{\sim} Gal(H/K)$, $(\cdot, H/K)$) in K satisfying $(\mathfrak{p}, H/K) = 1$, there is a unique $\pi_\mathfrak{p} \in R$ such that $\mathfrak{p} = \pi_\mathfrak{p} R$

$$\begin{array}{ccc} E & \xrightarrow{[\pi_\mathfrak{p}]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\text{Frob}_\mathfrak{p}} & \tilde{E} \end{array}$$ commutes.

Pf. See book

Pf of Thm Let $L = K(j(E), h(E[\vec{a}]))$

$H = K(j(E))$

K

To show: For all but finitely many degree 1 primes $\mathfrak{p}$,

$$(\mathfrak{p}, L/K) = 1 \iff \underbrace{\mathfrak{p} = \mu R,\ \mu \equiv 1 \bmod \mathfrak{c}}_{\mathfrak{p} \in P_1(\mathfrak{c})}$$

First: $\mathfrak{p} \in P_1(\mathfrak{c}) \Rightarrow (\mathfrak{p}, L/K) = 1$

We're given $\mathfrak{p} = \mu R$, $\mu \equiv 1 \bmod \mathfrak{c}$

Lemma gives $\pi \in R$, $\mathfrak{p} = \pi R$ such that

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\mathrm{Frob}_{\mathfrak{p}}} & \tilde{E} \end{array}$$

So $\pi = \{\mu$ for $\{ \in R^\times$. To Show: $(\mathfrak{p}, L/K)$ acts trivially on $\psi(E[\mathfrak{c}])$

Let $T \in E[\mathfrak{c}]$

$$\widetilde{T^{(\mathfrak{p}, L/K)}} = \tilde{T}^{\mathrm{Frob}_{\mathfrak{p}}} = \widetilde{[\pi](T)}$$

$\in E_{\text{ns}}$

$\in E_{\text{ns}}$

Erased

Now for other direction:

$1 = (\mathfrak{p}, L/K) \Rightarrow 1 = (\mathfrak{p}, L/K)|_H = (\mathfrak{p}, H/K)$

so $\mathfrak{p}$ is principal. The lemma says

$\mathfrak{p} = \pi R$, $\pi : E \to E$

$\downarrow \qquad \downarrow$

$\widehat{E} \xrightarrow{\text{Frob}_{\mathfrak{p}}} \widetilde{E}$

Choose some $\sigma \in \mathrm{Gal}(\overline{K}/K)$ with

$\sigma|_{K^{ab}} = (\mathfrak{p}, K^{ab}/K)$

$\sigma|_L = (\mathfrak{p}, L/K) = 1$

$\sigma|_H = 1$

Let $T \in E[\mathfrak{a}]$. Then $\widetilde{h([\pi]T)} =$

$h(\widetilde{[\pi]}\,\widetilde{T}) = h(\widetilde{T}^{\text{Frob}_{\mathfrak{p}}}) = h(\widetilde{T}^{(\mathfrak{p}, L/K)})$

by assumption $(\mathfrak{p}, L/K) = 1$, so this is $h(\widetilde{T})$

so $\widetilde{[\pi]}T = \widetilde{[\xi_T]}T$ for some $\xi_T \in R^\times$

$\widetilde{[\pi - \zeta_T]T} = \widehat{0} \Rightarrow [\pi - \zeta_T]T = 0$

$E[d]$ is a cyclic R/d-module, so because $[\pi - \zeta_T]$ kills $E[d]$, we have $\pi - \zeta \in d$, so $\pi \equiv \zeta \bmod d$, so

$$p = \pi R = \zeta R$$

Lecture 37 (2011-05-09)

$x \in \mathbb{A}_K^*$, $\alpha \in K^*$ 2011-5-9 (37)

want to define $x\alpha \in K^*$ (can't actually do this)

Lemma. $\mathfrak{a}$ a fractional ideal, can look at quotient group $K/\mathfrak{a}$

$$K/\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}$$

(simplest case: $\mathbb{Q}/\mathbb{Z} \cong \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p$)

Recall that we defined $(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}})}$,

ideal corresponding to the adele x

Define
$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\cdot x} & K/(x)\mathfrak{a} \\ \| & & \| \\ \bigoplus K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} & \longrightarrow & \bigoplus K_{\mathfrak{p}}/((x)\mathfrak{a})_{\mathfrak{p}} \end{array}$$

$$(\alpha_{\mathfrak{p}} + \mathfrak{a}_{\mathfrak{p}}) \longmapsto (x_{\mathfrak{p}}\alpha_{\mathfrak{p}} + x\mathfrak{a}_{\mathfrak{p}})$$

Recall $[\,,K] : \mathbb{A}_K^* \to \mathrm{Gal}(K^{ab}/K)$

surjective; continuous; K^* is in the kernel

Main Theorem of Complex Multiplication (MTCM)

$K/\mathbb{Q}$ imaginary quadratic field, $R = \mathcal{O}_K$

$E \in \mathrm{Ell}(R)$. For an arbitrary $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$

choose $s \in \mathbb{A}_K^*$ such that $\sigma|_{K^{ab}} = [s, K]$.

Fix $f: \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$ with $\mathfrak{a} \subset K$.

Then $\exists f': \mathbb{C}/(s)^{-1}\mathfrak{a} \xrightarrow{\sim} E^{\sigma}(\mathbb{C})$ such

that this commutes

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\cdot s^{-1}} & K/s^{-1}\mathfrak{a} \\ f \downarrow & & \downarrow f' \\ E(\mathbb{C}) & \xrightarrow[\sigma]{} & E^{\sigma}(\mathbb{C}) \end{array}$$

Note: 1) $f(K/\mathfrak{a}) = E(\mathbb{C})_{tors}$

2) σ is not a $\mathbb{C}$-continuous map

3) $\underbrace{f(t)^{\sigma}}_{\text{Galois action}} = \underbrace{f'(s^{-1} \cdot t)}_{\text{analytic action}}$

Want to study how much $\bar{\mathbb{Q}}$ moves torsion points around

E/L, not necessarily with CM, consider $E[m]$

$\rho_m : G_{\bar{L}/L} \longrightarrow Aut(E[m])$

$\cong$ choose a basis

$GL_2(\mathbb{Z}/m\mathbb{Z})$

Thm (Serre) There is a constant $C_{E/L}$ such that $Aut(E[m]) / \rho(G_{\bar{L}/L}) \leq C_{E/L}$

(just cosets, since not necessarily normal)

actually only true if E does not have CM

(Serre curve: one with $C_{E/L} = 1$)

Conjecture: fix L. Then $\sup_{E/L} (C_{E/L}) < \infty$.

If E has CM, then (assuming $K \subset L$)

$G_{\bar{L}/L}$ commutes with $End(E)$

So $\rho_M(G_{L/L}) \subset Aut_R(E[M]) \cong (R/MR)^\times$

($E[M]$ is a free rank 1 R/MR-module)

Thm With E has CM, $\exists\, C_{E/L}$ such that

$$\#\frac{(R/MR)^\times}{\rho_M(G_{L/L})} \leq C_{E/L} \quad \text{for all } M \geq 1$$

Pf. **Case 1** Assume $L = K(j(E)) = H$

Choose some $a \in Aut_R(E[M]) = (R/MR)^\times$

Choose an $\alpha \in R$ with $\alpha \equiv a \bmod MR$

Choose $s \in \mathbb{A}_K^*$ with $(s) = \alpha^{-1}R$

s acts on $E[M]$ via $[\alpha]$

$s = [s, K]$ but only defined up to unit, i.e. up to some automorphism of E

$$G_{L/L} \xrightarrow{\rho_M} (R/MR)^\times \longrightarrow (R/MR)^\times/R^\times$$

(surjective)

needed $L = H$ so that

$E(\mathbb{C}) \longrightarrow E^\sigma(\mathbb{C})$ $= E$ in good form

For arbitrary L/K

$$[(K/\mathfrak{m}_K)^\times : \rho_{\mathfrak{m}}(G_{L/L})]$$

$$= [(K/\mathfrak{m}_K)^\times : \rho_{\mathfrak{m}}(G_{\bar{H}/H})][\rho_{\mathfrak{m}}(G_{\bar{H}/H}) : \rho_{\mathfrak{m}}(G_{L/L})]$$

$$\leq \#R^\times \cdot [G_{\bar{H}/H} : G_{L/L}]$$

$$= \#R^\times \cdot [L:H]$$