Math 223b : Algebraic Number Theory notes

Alison Miller

Contents

1 January 28 **4**
1.1 Where we are and what's next . . . 4
1.2 Review of global fields and valuations . . . 5
1.3 Adeles as a restricted topological product . . . 5

2 February 1 **7**
2.1 Content and Haar measure . . . 7
2.2 Applications of Adelic Minkowski . . . 9
2.3 Class groups and S-class groups . . . 9

3 February 4 **10**
3.1 $\mathbb{A}_K^\times/K^\times$ vs $\mathbb{A}_K^1/K^\times$ . . . 12
3.2 Change of field and norm map . . . 12

4 February 8 **14**
4.1 Statement of results of global class field theory . . . 14
4.2 Ray class fields and ray class groups . . . 17

5 February 11 **18**
5.1 Ray class fields, continued . . . 18

6 February 15 **21**
6.1 Hilbert Class Field . . . 21
6.2 Side note on idoneal numbers . . . 22
6.3 Ideals become principal in the Hilbert class field . . . 22
6.4 Artin map and change of base . . . 23
6.5 Proof of Principal ideal theorem . . . 23
6.6 Class Field Towers . . . 24

7 February 22 **24**
7.1 Review of the Brauer group . . . 24
7.2 Cohomology of $\mathbb{A}_L^\times$ . . . 25
7.3 Introduction to Brauer Group from the point of view of Central Simple Algebras . . . 26
7.4 Central Simple Algebras and the Brauer Group . . . 28

8 February 25 **28**
8.1 Central Simple Algebras and Tensor Product . . . 28
8.2 Brauer Group in terms of Central Simple Algebras . . . 29
8.3 Classification of Central Simple Algebras . . . 30

9 March 1 **32**
9.1 Extension of base field: . . . 32
9.2 Maximal Subfields of CSAs . . . 33

10 March 4 **35**
10.1 Noether-Skolem . . . 35
10.2 Bijection between Central Simple Algebras and Cocycles . . . 36
10.3 Brauer Groups of Local Fields . . . 37
10.4 Global Fields . . . 38

11 March 8 **39**
11.1 Digression on sums of three cubes . . . 39
11.2 Anabelian philosophy . . . 39
11.3 Class formations . . . 39

12 March 11 **43**
12.1 First inequality and Herbrand quotient for C_L . . . 43
12.2 The Herbrand quotient of $\mathcal{O}_{L,S}^\times$ . . . 44
12.3 Corollaries of First Inequality . . . 45
12.4 The Second Inequality . . . 46

13 March 15 **47**
13.1 Proof of Second Inequality, continued . . . 47

14 March 25 **50**
14.1 What we know now . . . 50
14.2 Towards a global invariant map . . . 50
14.3 Reciprocity Laws . . . 50
14.4 Checking reciprocity laws . . . 52

15 March 29 **53**
15.1 Checking reciprocity laws, continued . . . 53
15.2 The inv map for cyclic extensions. . . . 53

16 April 1 **55**
16.1 Existence . . . 55
16.2 Basic facts about normic extensions . . . 56
16.3 Dirichlet L-functions + generalizations . . . 58

17 April 5 **59**
17.1 Convergence results for general Dirichlet Series . . . 59
17.2 Behavior of partial ζ-functions and Dirichlet L-functions . . . 60

18 April 8 **63**
18.1 Densities for sets of primes . . . 63

19 April 12 **66**
19.1 Cebotarev Density Theorem . . . 66
19.2 Splitting sets of an extension . . . 67
19.3 Intro Complex Multiplication . . . 68

20 April 15 **69**
20.1 Complex Multiplication and Ray Class Fields . . . 69
20.2 Elliptic Functions . . . 70

21 April 19 **73**
21.1 Facts about orders in imaginary quadratic fields and their ideals . . . 73
21.2 Proof that CM j-invariants are algebraic . . . 74
21.3 Ring class fields . . . 74
21.4 Sketch of proof that $j(L)$ generates the ring class field . . . 75
21.5 The j-function as modular function . . . 76

22 April 22 **76**
22.1 Explicit formulas . . . 76
22.2 Modular forms for $\Gamma_0(m)$: . . . 77
22.3 Classification of cyclic index m sublattices . . . 79

23 April 26 **79**
23.1 Proof that the modular polynomial exists and has integer coefficients . . . 79
23.2 The Main Theorem of Complex Multiplication . . . 81

24 April 29 **82**
24.1 Wrapping up the last step in the proof of the main theorem of class field theory . . . 82
24.2 Heegner's Approach to the Class Number 1 Problem . . . 82
24.3 The Cube Root of the j-function . . . 83
24.4 The Weber Functions . . . 84

1 January 28

1.1 Where we are and what's next

Last semester we covered local class field theory. The central theorem we proved was

Theorem 1.1. *If L/K is a finite Galois extension of local fields there exists a canonical map, the local Artin map*

$$\theta_{L/K} : K^\times / NL^\times \to (\mathrm{Gal}(L/K))^{ab}$$

We proved this by methods of Galois cohomology, intepreting both sides as Tate cohomology groups.

To prove this, we needed the following two lemmas:

- $H^1(L/K, L^\times) \cong 0$
- $H^2(L/K, L^\times)$ is cyclic of order $[L : K]$.

This semester: we'll do the analogous thing for L and K global fields. We will need to replace $K^\times$ with $C_K = \mathbb{A}_K^\times / K^\times$.

Then the analogues of the crucial lemmas are true, but harder to prove.

Our agenda this semester:

- start with discussion of global fields and adeles.
- give the adelic statements of global class field theory, with applications (including to the Brauer group)
- algebraic proofs of global class field theory
- then we'll take the analytic approach e.g. L-functions, class number formula, Cebotarev density, analytic proof of second inequality of global class field theory
- finally talk about complex multiplication, elliptic curves, and explicit class field theory for imaginary quadratic fields.

1.2 Review of global fields and valuations

Recall: have a notion of a global field K. Equivalent definitions:

- K is a finite extension of $\mathbb{Q}$ (number field) or of $\mathbb{F}_p(t)$ (function field).
- every completion of K is a local field and K has a product formula $\prod_v |a|_v = 1$.

(The fact that the first implies the second was sketched last semester, the opposite implication is Artin-Whaples and we won't do..)

The set of global fields is closed under taking finite extensions.

We'll primarily focus on the number field case in this class.

Definition. A *place* v of a global field K is an equivalence class of absolute values on K. We say that v is *finite / nonarchimedean* if it comes from a discrete absolute value, otherwise v is *infinite /archimedean* (and $K_v \cong \mathbb{R}$ or $\mathbb{C}$).

We can pick out a distinguished element of this equivalence class, the *normalized* absolute value $|\cdot|_v$ by requiring

$$|\pi_v|_v = |k_v|^{-1}$$

if K_v is nonarchimedean, and $|a|_{\mathbb{R}} = a$, $|a|_{\mathbb{C}} = |a|^2$.

Recall from last semester:

Theorem 1.2 (Product Formula)**.** *If K is a global field then $\prod_v |a|_v = 1$ for any $a \in K^\times$, where v runs through the set of places of K.*

Sketch of how this was done last semester. Check for $K = \mathbb{Q}, \mathbb{F}_p[t]$, then show that if the product formula holds for K, it holds for any finite extension L/K. ($\prod_{v' \text{ extends } v} |a|_{v'} = |a|_v$.) □

Remark. K_v^+ has a Haar measure, unique up to scaling (if v is finite, normalize by $\mu(\mathcal{O}_v) = 1$, if v is infinite use the standard normalization on $\mathbb{R}$ and $\mathbb{C}$.)

For any measurable set $E \subset K_v^+$ and any $a \in K_v^\times$ we have

$$\mu(aE) = |a|_v \mu(E).$$

1.3 Adeles as a restricted topological product

Definition. Suppose that we have topological groups $\{X_i\}_{i \in I}$ are topological groups, and open subgroups $Y_i \subset X_i$ for all but finitely many i. Then the *restricted topological product* of the X_i with respect to the Y_i is given by

$$\prod_i X_i = \{(x_i)_{i \in I} \mid x_i \in Y_i \text{ for all but finitely many } i\}.$$

The group structure here is clear. We take as a basis of open sets those sets of the form

$$\prod_{i \in S} U_i \times \prod_{i \notin S} Y_i$$

where $S \subset I$ is an arbitrary finite set, and $U_i \subset X_i$ are arbitrary open sets. Can check that $\coprod_i X_i$ is a topological group and is Hausdorff if all X_i are.

(Note this is not the same as the subspace topology coming from viewing $\coprod_i X_i$ as a subspace of $\prod_i X_i$.)

Definition. If K is a global field, define $\mathbb{A}_K$ as the restricted topological product $\coprod_v K_v$ of the K_v with respect to the $\mathcal{O}_v$. Can be checked that this is a topological ring, with open cover given by the sets

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

for any finite set S containing the infinite places, and the subspace topology on each $\mathbb{A}_{K,S} \subset \mathbb{A}_K$ agrees with the product topology.

Likewise define $\mathbb{A}_K^\times$ as $\coprod_v K_v^\times$, where now the restricted product is with respect to $\mathcal{O}_v^\times$. Define $\mathbb{A}_{K,S}^\times$ likewise.

Exercise: check the statements implict in the definition above. Show that $\mathbb{A}_K^\times$ is the group of units of $\mathbb{A}_K$.

Caution! The topology on $\mathbb{A}_K^\times$ is not the subspace topology inherited from $\mathbb{A}_K$: indeed, it shouldn't be, because the map $x \to x^{-1}$ is not continuous in the subspace topology. In general, if you have a topological ring R, the correct topology to put on $R^\times$ comes from the embedding of $R^\times \hookrightarrow R \times R$ given by $x \mapsto (x, x^{-1})$.

(Note though that if $R = K_v^\times$ or $\mathcal{O}_v^\times$, this topology on $R^\times$ agrees with the subspace topology coming from R. It's only because of the infinite restricted product that we have issues.)

Proposition 1.3. *$\mathbb{A}_K$ is a locally compact topological ring.*

Proof. all $\mathbb{A}_{K,S}$ are locally compact by Tychonoff. □

Hence the additive group $\mathbb{A}_K^+$ has a Haar measure also, which can be described as the product of the local Haar measures:

$$\mu(\prod_v E_v) = \prod_v \mu(E_v)$$

if $E_v \subset K_v$ is measurable and $E_v = \mathcal{O}_v$ for almost all v.

Note that K^+ embeds into A_K^+ and $K^\times$ embeds into $A_K^\times$, diagonally.

Proposition 1.4. *If L/K is a finite extension, then $\mathbb{A}_L \cong \mathbb{A}_K \otimes_K L$ as topological rings. (Here we topologize $\mathbb{A}_K \otimes_K L$ as follows: by choosing a basis, identify $L \cong K^n$, so $\mathbb{A}_K \otimes_K L \cong \mathbb{A}_K^n$, and use the product topology on $\mathbb{A}_K^n$. One can check that this doesn't depend on choice of basis.)*

Proof. (Sketch): Use fact that $K_v \otimes_K L \cong \prod_{v' \text{ extends } v} L_{v'}$. You'll do the details in the HW. (In fact, you'll also show that this is an isomorphism of $\mathrm{Gal}(L/K)$-modules.) □

Proposition 1.5. *For K a global field, K^+ is discrete (hence closed) in $\mathbb{A}_K^+$ and $\mathbb{A}_K^+/K^+$ is compact.*

Proof. By the previous proposition, it's enough to check this for $K = \mathbb{Q}$ and $K = \mathbb{F}_p(t)$. We'll do $\mathbb{Q}$; the proof for $\mathbb{F}_p(t)$ is similar.

Discrete: the set $U = \prod_{v \neq \mathbb{R}} \mathbb{Z}_v \times (-1, 1)$ is open and $\mathbb{Q} \cap U = \mathbb{Z} \cap (-1, 1) = \{0\}$.

Cocompact: We show this by constructing a compact set D which surjects onto $\mathbb{A}_K^+/K^+$. Let $D = \prod_{v \neq \mathbb{R}} \mathbb{Z}_v \times [-1/2, 1/2]$. We claim $D + \mathbb{Q} = \mathbb{A}_K$, which will give the desired result. Let $a \in \mathbb{A}_K^+$ be arbitrary: we want to show that a is congruent mod $\mathbb{Q}^+$ to some element of D.

Then there are finitely many primes p such that $a_p \notin \mathbb{Z}_p$. For each such p, there exists $r_p \in \mathbb{Q}$ such that $r_p \equiv a_p \pmod{\mathbb{Z}_p}$ and $r_p \in \mathbb{Z}_v$ when $v \neq p$. Then let $r = \sum r_p \in \mathbb{Q}$. Then $a - r \in \prod_{v \neq \mathbb{R}} \mathbb{Z}_v \times \mathbb{R}$. By subtracting off an appropriate $s \in \mathbb{Z}$, get $a - r - s \in \prod_{v \neq \mathbb{R}} \mathbb{Z}_v \times [-1/2, 1/2]$, as desired.

□

2 February 1

As before K is a global field.

Last time, we showed that K is discrete in $\mathbb{A}_K$ and the quotient of additive groups $\mathbb{A}_K^+/K^+$ is compact. Our longer term goal will be to prove a similar statement for $\mathbb{A}_K^\times/K^\times$.

Discreteness of $K^\times$ in $\mathbb{A}_K^\times$ follows from the additive statement: we know that $\mathbb{A}_K^\times$ embeds topologically in $\mathbb{A}_K \times \mathbb{A}_K$ via the map $x \mapsto (x, x^{-1})$, and $K \times K$ is discrete in $\mathbb{A}_K \times \mathbb{A}_K$.

On the other hand we're about to see that, $\mathbb{A}_K^\times/K^\times$ is not compact, so we will have to modify our statement somewhat.

2.1 Content and Haar measure

We now show that $\mathbb{A}_K^\times/K^\times$ is not compact by exhibiting a continuous map from $\mathbb{A}_K^\times/K^\times$ with non-compact image.

Definition. If $a = (a_v) \in \mathbb{A}_K^\times$, the *content* $c(a) = \prod_v |a_v|_v$ (this is defined because $|a_v|_v = 1$ for all but finitely many v.)

HW: The map $c : \mathbb{A}_K^\times \to \mathbb{R}^{>0}$ is a continuous homomorphism. By the product formula, it induces a map $c : \mathbb{A}_K^\times / K^\times \to \mathbb{R}^{>0}$ with infinite image, which means that $\mathbb{A}_K^\times / K^\times$ can't be compact.

The content also has an interpretation in terms of Haar measure.

Proposition 2.1. *For any measurable set $E \subset \mathbb{A}_K^+$, and any $a \in \mathbb{A}_K^\times$, then $\mu(aE) = c(a)\mu(E)$.*

Proof. This follows from the description of μ as a product of local measures, and the local fact that $\mu_v(aE_v) = |a|_v \mu_v(E_v)$. □

Since K^+ is discrete inside $\mathbb{A}_K^+$, we can push forward the measure on $\mathbb{A}_K^+$ to get a Haar measure on $\mathbb{A}_K^+ / K^+$. To be more precise, let D be a measurable fundamental domain for the action of K^+ on $\mathbb{A}_K^+$. (For example with $K = \mathbb{Q}$ we can take $D = \prod_{v \neq \mathbb{R}} \mathbb{Z}_v \times [-1/2, 1/2)$.) Then for $E \subset \mathbb{A}_K^+ / K^+$ Borel define

$$\mu_{\mathbb{A}_K/K}(E) = \mu_{\mathbb{A}_K}(\pi^{-1}(E) \cap D)$$

where $\pi : \mathbb{A}_K \to \mathbb{A}_K / K$ is the projection map.

As a corollary, we get another proof of the product formula: if $a \in K^\times$, then multiplication by a gives an automorphism of $\mathbb{A}_K^+$ which scales the Haar measure by $c(a)$, and also sends K^+ to itself. Hence multiplication by a scales the Haar measure on the quotient $\mathbb{A}_K / K^+$ by $c(a)$. On the other hand, $\mu(\mathbb{A}_K / K^+)$ has finite measure, so $c(a)$ must be 1.

Next question: is $\mathbb{A}_K^\times / K^\times$ compact? No: c is a continuous map from $\mathbb{A}_K^\times / K^\times \to \mathbb{R}^{>0}$, and the latter is not compact. However, that's the only obstruction:

Definition. Let

$$\mathbb{A}_K^1 = \ker(c : \mathbb{A}_K^\times \to \mathbb{R}^{>0})$$

be the subgroup of multiplicative adeles of content 1.

Then $\mathbb{A}_K^1$ is a closed subgroup of $\mathbb{A}_K^\times$, and $K^\times$ is discrete in $\mathbb{A}_K^1$.

We plan to show that $\mathbb{A}_K^1 / K^\times$ is compact, and use this to deduce the finiteness of class group and Dirichlet's units theorem. But first we're going to develop the adelic version of Minkowski's theorem. Recall that the classical Minkowski's theorem says that if L is a lattice in $\mathbb{R}^n$ and S is a convex subset of $\mathbb{R}^n$ symmetric around the origin, then if S has large enough volume (where "large enough" depends on L) there must be a nonzero point of $S \cap L$. We'll prove an analogous theorem replacing $\mathbb{R}^n$ with $\mathbb{A}_K$ and L with K, though we'll work in a bit less generality and only prove the lemma for a certain type of S.

Definition. For $a \in \mathbb{A}_K^\times$, let $S_a \subset \mathbb{A}_K^+$ be the subset defined by

$$S_a = \{x \in \mathbb{A}_K^+ \mid |x_v|_v \leq |a_v|_v \text{ for all } v\}$$

Theorem 2.2 (Adelic Minkowski)**.** *There exists a constant* $C = C_K > 1$*, depending on* K*, such that for every* $a = (a_v) \in \mathbb{A}_K^\times$ *with* $c(a) > C$*, there exists some* $x \in K^\times \cap S_a$ *(in particular,* $x \neq 0$*).*

Proof. Let $B = \prod_{v \text{ finite}} \mathcal{O}_v \times \prod_{v \text{ infinite}} \{x \in K_v \mid |x|_v \leq \frac{1}{2}\} \subset \mathbb{A}_K^+$. Then let $C = \frac{\mu(\mathbb{A}_K^+/K^+)}{\mu(B)}$.

Now, $\mu(aB) = \mu(B)c(a) > \mu(\mathbb{A}_K^+/K^+)$. Hence there exists nonzero $x_1, x_2 \in \cap aB$, $x_1 \neq x_2$ such that $x = x_1 - x_2 \in K^+$. By the nonarchimedean and archimedean triangle inequalities, $x \in S_a$. □

2.2 Applications of Adelic Minkowski

Theorem 2.3. $\mathbb{A}_K^1/K^\times$ *is compact.*

Proof. Let C be as in the Adelic Minkowski, and let $a \in \mathbb{A}_K^\times$ be any idele of content $> C$. Then let

$$D = \mathbb{A}_K^1 \cap S_a = \{x \in \mathbb{A}_K^1 \mid |x_v|_v \leq |a_v|_v \text{ for all } v\}.$$

This set D is compact because it is a closed subset of S_a. We claim that D surjects onto $\mathbb{A}_K^1/K^\times$. For this, let $x \in \mathbb{A}_K^1$ be arbitrary: we need to show that $x^{-1}D$ contains an element of $K^\times$.

For this, note that $x^{-1}S_a = S_{x^{-1}a}$, and $c(x^{-1}a) = c(a) > C$, so by adelic Minkowski, $x^{-1}S_a$ contains some $y \in K^\times$, and this y also lies in $x^{-1}D$.

□

Another application which we won't prove here is

Theorem 2.4 (Strong Approximation)**.** *For any place* v_0*,* K^+ *is dense in* $\mathbb{A}_K^+/K_{v_0}^+ = \prod\!\!\!\prod_{v \neq v_0} K_v^+$

(Proof on HW 2).

2.3 Class groups and S-class groups

Recall that if K is a number field, then the class group $\mathrm{Cl}(K)$ of K is the cokernel of the map $K^\times \to I(K)$ where $I(K)$ denotes the group of fractional ideals of $\mathcal{O}_K$.

We'll now generalize this slightly in a way that also works for function fields.

Definition. K is a global field, S a nonempty finite set of places including all archimedean ones. Let $\mathcal{O}_{K,S} = \{x \in K \mid |x|_v \leq 1 \text{ for all } v \notin S\}$.

If K is a number field, and S is the set of archimedean places of K, then $\mathcal{O}_{K,S} = \mathcal{O}_K$. The ring $\mathcal{O}_{K,S}$ is a Dedekind domain, and the (nonzero) primes of $\mathcal{O}_{K,S}$ are in bijection with places $v \notin S$.

If K is a number field, and $S = \{\text{archimedean places}\} \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, then $\mathcal{O}_{K,S}$ is the localization of K made by inverting those elements $a \in \mathcal{O}_K$ such that all prime factors of the ideal (a) are contained in the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

If K is the function field of a curve C over $\mathbb{F}_q$, then the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ can be viewed as closed points of the scheme C, and $\mathcal{O}_{K,S}$ is the ring of regular functions on the open subset $C - \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Definition. Let $I_{K,S}$ be the group of fractional ideals of $\mathcal{O}_{K,S}$. Then we define the *class group* $\mathrm{Cl}(K, S) = \mathrm{Cl}(\mathcal{O}_{K,S})$ of $\mathcal{O}_{K,S}$ to be the cokernel of the natural map $\phi : K^\times \to I_{K,S}$.

Note that $\ker \phi : K^\times \to I_{K,S}$ is precisely the unit group $\mathcal{O}_{K,S}^\times$.

Next time we'll show that the following two finiteness properties follow from compactness of $\mathbb{A}_K^\times$.

Theorem 2.5. *Let K be a global field and S a nonempty finite set of places of K including all archimedean places.*

Then

- $\mathrm{Cl}(K, S) = \mathrm{Cl}(\mathcal{O}_{K,S})$ *is finite.*
- $\mathcal{O}_{K,S}^\times$ *is finitely generated of rank equal to* $|S| - 1$.

3 February 4

Today we'll deduce the finiteness of the class group and Dirichlet's units theorem from the compactness of $\mathbb{A}_K^1/K^\times$.

Let $\mathbb{A}_{K,S}^\times$ denote the group

$$\mathbb{A}_{K,S}^\times = \{x \in \mathbb{A}_K^\times \mid |x_v|_v = 1 \text{ for all } v \notin S\} = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times$$

of units of $\mathbb{A}_{K,S}$.

and let $\mathbb{A}_{K,S}^1$ denote $\mathbb{A}_{K,S}^\times \cap \mathbb{A}_K^1$: then $\mathbb{A}_{K,S}^1$ is an open subgroup of $\mathbb{A}_K^1$.

The key exact sequence we'll use here is

$$1 \longrightarrow (\mathbb{A}_{K,S}^1 \cdot K^\times)/K^\times \longrightarrow \mathbb{A}_K^1/K^\times \longrightarrow \mathbb{A}_K^1/(\mathbb{A}_{K,S}^1 \cdot K^\times) \longrightarrow 1$$

Here $(\mathbb{A}_{K,S}^1 \cdot K^\times)/K^\times$ is an open subgroup, hence also closed. As a consequence, the last map $\mathbb{A}_K^1/K^\times \to \mathbb{A}_K^1/(\mathbb{A}_{K,S}^1 \cdot K^\times)$ is continuous using the discrete topology on $\mathbb{A}_K^1/(\mathbb{A}_{K,S}^1 \cdot K^\times)$.

Compactness of $\mathbb{A}_K^1/K^\times$ then implies that the quotient $\mathbb{A}_K^1/(\mathbb{A}_{K,S}^1 \cdot K^\times)$ is compact in the discrete topology, hence finite. It also implies that the subgroup $(\mathbb{A}_{K,S}^1 \cdot K^\times)/K^\times$ is

compact. From the first of these facts we'll get the finiteness of class group, and from the second we'll get Dirichlet's units theorem.

To get the finiteness of class group, we now just need

Lemma 3.1.

$$\mathrm{Cl}_S(K) \cong \mathbb{A}_K^1/(\mathbb{A}_{K,S}^1 \cdot K^\times).$$

Proof. Define a map

$$\phi : \mathbb{A}_K^1 \to \mathrm{Cl}_S(K)$$

by $\phi(a) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}$, where $\mathfrak{p}$ ranges over the primes of $\mathcal{O}_{K,S}$ (which we know are in bijection with the places of K not in S).

Then check that ϕ is a surjection and that the kernel is $K^\times \mathbb{A}_{K,S}^1$.

□

Corollary 3.2. $\mathrm{Cl}(\mathcal{O}_{K,S})$ *is finite.*

Now we look at the units group. This is a bit trickier.

Lemma 3.3.

$$(\mathbb{A}_{K,S}^1 \cdot K^\times)/K^\times \cong \mathbb{A}_{K,S}^1/\mathcal{O}_{K,S}^\times$$

Proof. (This is a special case of the second isomorphism theorem: $(A+B)/B \cong A/(A \cap B)$.) □

Combining our lemma with the previous exact sequence, we conclude that that $\mathbb{A}_{K,S}^1/\mathcal{O}_{K,S}^\times$ is compact. This will ultimately allow us to show that $\mathcal{O}_{K,S}^\times$ is large enough, but we need some technical lemmas first:

Lemma 3.4. *The set* $\{x \in \mathcal{O}_{K,S} \mid v(x) \in [1/2, 2] \text{ for all } v \in S\}$ *is finite.*

Proof. This is the intersection inside $\mathbb{A}_K$ of the discrete set K with the compact set $\prod_{v\in S} R_v \times \prod_{v\notin S} \mathcal{O}_v$, where $R_v = \{x \in K_v \mid v(x) \in [1/2, 2]\}$. □

Proposition 3.5. $a \in K^\times$ *is a root of unity iff* $|a|_v = 1$ *for all* v*, and the set of all such* a *is finite.*

Proof. Finiteness of $\{a \mid |a|_v = 1 \text{ for all } v\}$ follows from the previous lemma.

For the equivalence, $\Leftarrow$ is clear. To show $\Rightarrow$ observe that $\{a \mid |a|_v = 1 \text{ for all } v$ is a finite group, hence is torsion. □

Now, consider the homomorphism $\mathcal{L} : \mathbb{A}_{K,S}^\times \to \prod_{v\in S} \mathbb{R} = (\mathbb{R})^S$ given by

$$(\mathcal{L}(a))_v = \log(|a_v|_v)$$

.

It follows from the lemma that $\mathcal{L}(\mathcal{O}_{K,S}^\times)$ is a discrete subset of $\mathbb{R}^n$.

The image $\mathcal{L}(\mathbb{A}_{K,S}^1)$ is contained in the hyperplane $H = \{\sum_v x_v = 0\}$. It may not be all of H, but it does span H as an $\mathbb{R}$-vector space.

Let W be the $\mathbb{R}$-subspace of H spanned by $\mathcal{L}(\mathcal{O}_{K,S}^\times)$. We'll show that in fact $W = H$.

Now, $\mathcal{L}$ induces a map

$$\mathbb{A}_{K,S}^1/\mathcal{O}_{K,S}^\times \to H/W$$

this map has image a compact subgroup of H/W, but H/W is isomorphic to some $\mathbb{R}^i$, so the only such compact subgroup is 0. Hence $\mathcal{L}(\mathbb{A}_{K,S}^1) \subset W$: but we know that $\mathcal{L}(\mathbb{A}_{K,S}^1)$ spans H so we must have $W = H$.

Hence $\mathcal{L}(\mathcal{O}_{K,S})$ is a lattice in H, and so has rank equal to $\dim H = |S| - 1$.

Finally, Proposition 3.5 tells us that the kernel of $\mathcal{L}$ contains only finitely many elements of $\mathcal{O}_{K,S}^\times$, so $\mathcal{O}_{K,S}^\times$ is a finitely generated abelian group of the same rank as $\mathcal{L}(\mathcal{O}_{K,S}^\times)$, and we conclude Dirichlet's units theorem.

3.1 $\mathbb{A}_K^\times/K^\times$ vs $\mathbb{A}_K^1/K^\times$

Recently we've been talking about $\mathbb{A}_K^1/K^\times$. Now we're going to be moving on to class field theory, where $C_K = \mathbb{A}_K^\times/K^\times$ is more important. Brief remarks on the relationship between the two.

If K is a number field, have short exact sequence of topological groups.

$$1 \to \mathbb{A}_K^1/K^\times \to \mathbb{A}_K^\times/K^\times \to \mathbb{R}^{>0} \to 1.$$

If v is any archimedean place of $\mathbb{A}_K^\times/K^\times$, then the map $\mathbb{R}^{>0} \hookrightarrow K_v \hookrightarrow \mathbb{A}_K^\times/K^\times$ gives a splitting of the short exact sequence, so $\mathbb{A}_K^\times/K^\times \cong \mathbb{A}_K^1/K^\times \times \mathbb{R}^{>0}$.

In the case that K is a function field with constant field $\mathbb{F}_q$, have short exact sequence

$$1 \to \mathbb{A}_K^1/K^\times \to \mathbb{A}_K/K^\times \to q^{\mathbb{Z}} \to 1.$$

3.2 Change of field and norm map

Let L/K be a finite separable extension of global fields, not necessarily Galois. We already know that $\mathbb{A}_K$ is a closed subring of $\mathbb{A}_L = L \otimes_K \mathbb{A}_K$. Hence $\mathbb{A}_K^\times$ is a closed subgroup of $\mathbb{A}_L^\times$.

Proposition 3.6. *The inclusion $\mathbb{A}_K^\times/K^\times \hookrightarrow \mathbb{A}_L^\times/L^\times$ is a closed embedding.*

Proof. We'll do the number field case:

Observe that $\mathbb{A}_K^1/K^\times \hookrightarrow \mathbb{A}_L^1/L^\times$ is a closed embedding for purely topological reasons, because $\mathbb{A}_K^1/K^\times$ is compact, and the continuous image of a compact set is compact, hence closed.

Now we use the morphism of split short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{A}_K^1/K^\times & \longrightarrow & \mathbb{A}_K^\times/K^\times & \longrightarrow & \mathbb{R}^{>0} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle [L:K]} & & \\ 1 & \longrightarrow & \mathbb{A}_L^1/L^\times & \longrightarrow & \mathbb{A}_L^\times/L^\times & \longrightarrow & \mathbb{R}^{>0} & \longrightarrow & 1 \end{array}$$

where the last map is $x \mapsto x^{[L:K]}$. Since the maps on the outside are both closed embeddings, and the short exact sequences split as topological groups, the inside map is also a closed embedding.

□

(On next HW, uses a similar technique: for every v $K_v^\times \hookrightarrow A_K^\times/K^\times$ is a closed embedding, but $K_{v_1} \times K_{v_2} \hookrightarrow A_K^\times/K^\times$ is not.).

If L/K is Galois, then $\mathrm{Gal}(L/K)$ acts on $\mathbb{A}_L^\times$ and on $C_L = \mathbb{A}_L^\times/L^\times$. It follows from $\mathbb{A}_L = \mathbb{A}_K \otimes_K L$ that the invariant subgroup of $(\mathbb{A}_L^\times)^{\mathrm{Gal}(L/K)} = \mathbb{A}_K^\times$.

Proposition 3.7. *The subgroup* $C_L^{\mathrm{Gal}(L/K)}$ *of* $\mathrm{Gal}(L/K)$*-invariants is equal to* C_K*.*

Proof. Apply the Galois cohomology long exact sequence to

$$1 \to L^\times \to \mathbb{A}_L^\times \to C_L \to 1$$

to obtain

$$K^\times \to \mathbb{A}_K^\times \to (C_L)^{\mathrm{Gal}(L/K)} \to H^1(L/K, L^\times)$$

and use Hilbert 90. □

(Note by contrast that for normal class groups, in general the subgroup $\mathrm{Cl}(\mathcal{O}_L)^{\mathrm{Gal}(L/K)}$ does not equal $\mathrm{Cl}(\mathcal{O}_K)$.)

We'll define a norm map $N : \mathbb{A}_L^\times \to \mathbb{A}_K^\times$ that extends the norm map $L^\times \to K^\times$.

Three equivalent approaches:

$$Na : \det(\times a : \mathbb{A}_L^\times \to \mathbb{A}_L^\times)$$

where we view $\mathbb{A}_L^\times$ as an $\mathbb{A}_K$-module.

$$(Na)_v = \prod_{w \text{ extends } v} N_{L_w/K_v} a_w.$$

When L/K is Galois, then $Na = \prod_{g \in \mathrm{Gal}(L/K)} ga$.

Theorem 3.8. *The norm map* $N : \mathbb{A}_L^\times \to \mathbb{A}_K^\times$ *is continuous and open.*

Proof. Can check that the image/preimage of sets of the form

$$\prod_{v\in S} U_i \times \prod_{v\notin S} \mathcal{O}_v^\times$$

is open, using the definition in terms of local components. For the continuity you just need to use that local norms are continuous.

For openness you need to use the fact that local norm maps are open. We didn't prove this last semester, but it doesn't take much work beyond what we did. Let U be an open subgroup of $L_w^\times$; without loss of generality assume $U \subset \mathcal{O}_w^\times$. We must show that $N_{L_w/K_v}(U)$ is open in $\mathcal{O}_v^\times$: we saw last semester that this is equivalent to being finite index in $\mathcal{O}_v^\times$. First of all, U is a finite index subgroup of $\mathcal{O}_w^\times$ because the latter is compact, so $N_{L_w/K_v}U$ is a finite index subgroup of $N_{L_w/K_v}\mathcal{O}_v^\times$. But $N_{L_w/K_v}\mathcal{O}_v^\times$ is finite index in $\mathcal{O}_v^\times$ by local class field theory, so we're done.

Additionally, because of the restricted product, also need the fact, proved last semester, that if v is a place of K, and w a place of L above v then the local norm map N_{L_w/K_v} maps $\mathcal{O}_w^\times$ onto $\mathcal{O}_v^\times$ whenever L_w/K_v is unramified, which happens for all but finitely many v. □

4 February 8

Side note: related to Vaughan's question about the class number formula last time. If K is a number field, the locally compact group $\mathbb{A}_K^1/K^\times$ has a Haar measure, unique up to scaling, and there turns out to be a particular scaling that is particularly nice for Fourier analysis. Then the class number formula for K has the following adelic interpretation:

$$\operatorname{Res}|_{s=1}\zeta_K(s) = \mu(\mathbb{A}_K^1/K^\times) = \frac{2^{r_1}(2\pi)^{r_2}h(\mathcal{O}_K)\operatorname{reg}(\mathcal{O}_K)}{\sqrt{|\operatorname{disc}(K)|}w_K}$$

where r_1 is the number of real places of K, r_2 the number of complex places, $\operatorname{reg}(\mathcal{O}_K) = \operatorname{vol}(H/\mathcal{L}(\mathcal{O}_K^\times))$ and $w_K = \#(\mu_\infty(\mathcal{O}_K))$. This was proved by Tate in his thesis.

4.1 Statement of results of global class field theory

Let K be a global field. We'll now introduce the statements of the results of global class field theory without proofs.

Theorem 4.1 (Reciprocity map for finite extensions)**.** *For every finite Galois extension* L/K *there is a natural reciprocity map*

$$\theta_{L/K} : C_K \to \operatorname{Gal}(L/K)^{ab}$$

which is surjective, and has kernel equal to NC_L.

If $L'/L/K$ *is a tower, then* $\theta_{L'/K}$ *restricts to* $\theta_{L/K}$.

Definition. A subgroup U of C_K is *normic* if it is equal to NC_L for some finite Galois extension L/K.

(By the same argument as in the local field case, it's enough to assume L/K is abelian.)

Because the norm map is open, any normic subgroup is open, and it is also finite index by the main theorem.

Theorem 4.2 (Existence Theorem)**.** *The normic subgroups of C_K are exactly the open subgroups of finite index.*

Hence we have a bijection between open finite index subgroups of C_K and finite abelian extensions L of K. In one direction, the finite index subgroup $U \subset C_K$ maps to the fixed field $(K^{ab})^{\theta_{/K}(U))}$, while in the other direction, the finite abelian extension L maps to the subgroup $NC_L = \theta_{/K}^{-1}(\mathrm{Gal}(K^{ab}/L))$.

We can assemble the reciprocity maps for finite extensions to get

Theorem 4.3 (Reciprocity map for infinite extensions)**.** *There is a continuous map, the* global reciprocity map

$$\theta_{/K} : C_K = \mathbb{A}_K^\times / K^\times \to \mathrm{Gal}(K^{ab}/K)$$

with dense image and kernel equal to the intersection of all the finite index open subgroups of C_K.

Then $\ker \theta_K$ is the intersection of all the finite index open subgroups of C_K. Can we describe this intersection more explicitly? It's a subgroup of C_K, and must contain the connected component C_K^0. Ultimately we'll show that it is exactly $(C_K)^0$, but this will require looking at C_K and C_K^0 more closely.

Note first that the connected component $(\mathbb{A}_K^\times)^0$ of the identity in $\mathbb{A}_K^\times$ is precisely

$$\prod_{v \text{ complex}} \mathbb{C}^\times \times \prod_{v \text{ real}} \mathbb{R}^{>0}.$$

Let π denote the projection map from $\mathbb{A}_K^\times$ to C_K.

Proposition 4.4. *The connected component $(C_K)^0$ is equal to the closure $D_K = \overline{\pi(\mathbb{A}_K^\times)^0}$ inside C_K.*

Proof. First of all, since connected components are closed, we certainly have $(C_K)^0 \supset D_K$. In class we didn't prove the other inclusion: we'll do so here.

We'll prove that the topological group C_K/D_K is totally disconnected. To this end, we use the following homomorphism of topological groups

$$\phi : \prod_{v \text{ finite}} \mathcal{O}_v^\times \to C_K/D_K$$

given by composing the natural inclusion $\prod_{\nu \text{ finite}} \mathcal{O}_\nu^\times \hookrightarrow \mathbb{A}_K^\times$ with the projection $\mathbb{A}_K^\times \twoheadrightarrow C_K/D_K$. Because the domain of ϕ is totally disconnected, the image $\operatorname{im}\phi$ is also totally disconnected.

We'd be done if we knew that ϕ was surjective; unfortunately this is not the case. However we will show that the image of ϕ is a finite index subgroup of C_K, which is still enough to imply topologically that C_K is totally disconnected.

The cokernel of ϕ is equal to

$$\operatorname{cok}\phi = \mathbb{A}_K^\times / K^\times \cdot \prod_{\nu \text{ finite}} \mathcal{O}_\nu^\times \prod_{\nu \text{ real}} \mathbb{R}^{>0} \prod_{\nu \text{ complex}} \mathbb{C}^\times.$$

We now prove finiteness of $\operatorname{cok}\phi$ by the same method used to prove finiteness of class group (in fact, $\operatorname{cok}\phi$ is actually equal to what's called the *narrow class group* of $\mathcal{O}_K$). The natural map $\mathbb{A}_K^1/K^\times \to \operatorname{cok}\phi$ is surjective because $\mathbb{A}_K^\times$ is generated by $\mathbb{A}_K^1$ and the subgroup $\mathbb{R}^{>0}$ of K_ν for any archimedean place ν. Hence $\operatorname{cok}\phi$ is a compact topological group, but it has the discrete topology, so it must be finite. □

(Another description of D_K is that it is the set of *divisible* elements in C_K: that is, $\cap_{n\geq 0}(C_K)^n$. Proof of this will be on the HW.)

If K is a function field, this means that $C_K^0 = \{1\}$. If K is a number field, then (by current HW) the map $\prod_{\nu \text{ infinite}} K_\nu^\times \hookrightarrow \mathbb{A}_K^\times/K^\times$ is a closed embedding if and only if K has a unique infinite place (K is $\mathbb{Q}$ or an imaginary quadratic field). In that case $C_K^0 \cong K_\infty^\times$: otherwise can be shown (proof is in exercises of Neukirch)

$$C_K/C_K^0 \cong (S^1)^{r_2} \times (\mathbb{A}_K^+/K^+)^{r_1+r_2-1} \times \mathbb{R}^{>0}.$$

Theorem 4.5. *If K is a number field, then $C_K/(C_K)^0$ is a profinite group.*

Proof. We already know that $C_K/(C_K)^0$ is totally disconnected, so it's enough to show compact. But the compact group $\mathbb{A}_K^1/K^\times$ surjects onto $C_K/(C_K)^0$.

□

Corollary 4.6. *For K a number field, C_K^0 is the intersection of all finite index open subgroups of C_K, and $\theta_{/K}$ induces an isomorphism $C_K/C_K^0 \to \operatorname{Gal}(K^{ab}/K)$.*

Proof. Because C_K/C_K^0 is profinite, the intersection of all finite index open subgroups of C_K/C_K^0 is equal to $\{1\}$. Hence the image of all finite index subgroups of C_K is equal to C_K^0.

This plus Theorem 4.3 shows that the map $C_K/C_K^0 \to \operatorname{Gal}(K^{ab}/K)$ is injective. For surjectivity, we already know that the image is dense, but since C_K/C_K^0 is compact, the image must also be closed, so must be all of $\operatorname{Gal}(K^{ab}/K)$. □

For the function field case:

Theorem 4.7. *For K a function field, C_K is totally disconnected, and $\{1\} = C_K^0$ is the intersection of all finite index open subgroups of C_K.*

The map $\theta_{/K}$ is not surjective, but its image can be seen from the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{A}_K^0/K^\times & \longrightarrow & C_K & \longrightarrow & q^{\mathbb{Z}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & I_K & \longrightarrow & \mathrm{Gal}(K^{ab}/K) & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 1. \end{array}$$

where I_K is defined as the kernel of the map $\mathrm{Gal}(K^{ab}/K) \to \hat{\mathbb{Z}}$ and the first downward arrow is an isomorphism.

The global reciprocity map is determined by compatibility properties: specifically, that the square

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\theta_{/K_v}} & \mathrm{Gal}(K_v^{ab}/K_v) \\ \downarrow & & \downarrow \\ \mathbb{A}_K^\times/K^\times & \xrightarrow{\theta_{/K}} & \mathrm{Gal}(K^{ab}/K). \end{array}$$

commutes for all v. Here $\theta_{/K_v}$ is the reciprocity map defined last semester.

More specifically, if L is a finite abelian extension of K and w is any valuation extending L, we have

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\theta_{L_w/K_v}} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{A}_K^\times/K^\times & \xrightarrow{\theta_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

and recall from last semester that, whenever L_w/K_v is unramified, then $\mathcal{O}_v^\times \subset \theta_{L_w/K_v}$

In particular this means we may define

$$\theta_{L/K}(\mathfrak{a}) = \prod_v \theta_{L_w/K_v}(\mathfrak{a}_v)$$

as the right hand side is a finite product, and take the inverse limit over all L/K finite abelian to define $\theta_{/K}(\mathfrak{a})$.

4.2 Ray class fields and ray class groups

Let K be a number field now.

We'll now define a family of open subgroups of C_K containing C_K^0, which by the global class field theory correspondence will give us a family of finite abelian extensions of K.

Definition. A *modulus* $\mathfrak{m}$ of K is a function from (places of K) to $\mathbb{Z}^{\geq 0}$ such that

- $\mathfrak{m}(v) = 0$ for all but finitely many v
- if v is complex then $\mathfrak{m}(v) = 0$
- if v is real then $\mathfrak{m}(v) = 0$ or 1.

As a matter of notation we write $\mathfrak{m} = \prod_v v^{\mathfrak{m}(v)}$, e.g. $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2\infty_1$.

For a modulus $\mathfrak{m} = \prod_v v^{\mathfrak{m}(v)}$, define the *congruence subgroup* $U_{\mathfrak{m}}$ of $\mathbb{A}_K^\times$ by

$$U_{\mathfrak{m}} = \prod_{\mathfrak{p} \text{ finite}} U_{\mathfrak{p},\mathfrak{m}(\mathfrak{p})} \prod_{\substack{v \text{ infinite} \\ \mathfrak{m}(v)=0}} K_v^\times \prod_{\substack{v \text{ finite} \\ \mathfrak{m}(v)=1}} \mathbb{R}^{>0}$$

We'll say that $x \equiv 1 \pmod{\mathfrak{m}}$ if $x \in U_{\mathfrak{m}}$.

Then let $C_K^{\mathfrak{m}}$ be the congruence subgroup of C_K given by $C_K^{\mathfrak{m}} = U_{\mathfrak{m}} \cdot K^\times / K^\times$.

Any open subgroup of $\mathbb{A}_K^\times$ must contain some $U_{\mathfrak{m}}$, hence any open subgroup of C_K must contain some $C_K^{\mathfrak{m}}$.

Definition. The *ray class field* $L_{\mathfrak{m}}$ of modulus $\mathfrak{m}$ is the subfield of K^{ab} fixed by $\theta_{/K}(U_{\mathfrak{m}})$.

Then $L_{\mathfrak{m}}$ is an abelian extension of K with $\mathrm{Gal}(L_{\mathfrak{m}}/K) \cong C_K/C_K^{\mathfrak{m}}$. Next time we'll identify this quotient with the *ray class group*, a generalization of the class group defined classically in terms of ideals.

We'll also work out the example of $K = \mathbb{Q}$.

5 February 11

5.1 Ray class fields, continued

Example. Let $K = \mathbb{Q}$. Then (recall from last semester)

$$\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \cong \prod_p \mathbb{Z}_p^\times \times \mathbb{R}^{>0} \cong \hat{\mathbb{Z}}^\times \times \mathbb{R}^{>0},$$

and the Artin map is given by $\theta_{/\mathbb{Q}}(a, x)$ is the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})$ mapping $\zeta \mapsto \zeta^{a^{-1}}$ for any $\zeta \in \mu_\infty(K)$.

If $\mathfrak{m} = m\infty$ then $U_{\mathfrak{m}} = U_{m\infty}$ is identified with the subgroup $\{(a, x) \in \hat{\mathbb{Z}}^\times \times \mathbb{R}^{>0} \mid a \equiv \pm 1 \pmod{m}\}$, so $L_{m\infty} = \mathbb{Q}(\zeta_m)$.

If $\mathfrak{m} = m$ then $U_{\mathfrak{m}} = U_m$ is identified with the subgroup $\{(a, x) \in \hat{\mathbb{Z}}^\times \mid a \equiv 1 \pmod{m}\}$, and $L_{m\infty} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Definition. The *ray class group* $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$ is the quotient $I_{\mathfrak{m}}/P_{\mathfrak{m}}$, where

- $I_{\mathfrak{m}}$ is the group of fractional ideals of $\mathcal{O}_K$ relatively prime to $\mathfrak{m}$ (that is, $\nu_{\mathfrak{p}}(\mathfrak{a}) = 0$ for any prime $\mathfrak{p} \mid \mathfrak{m}$).
- $P_{\mathfrak{m}} \subset I_{\mathfrak{m}}$ is the subgroup of principal ideals $(\mathfrak{a})$ such that $\mathfrak{a} \in U_{\mathfrak{p},\mathfrak{m}(\mathfrak{p})}$ for all finite places $\mathfrak{p}$ contained in the modulus $\mathfrak{m}$ and $\mathfrak{a}$ is positive at all real places contained in the modulus $\mathfrak{m}$.

(Exercise: if $\mathfrak{m}$ contains no infinite places, there's a natural exact sequence

$$\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times \to \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_K) \to 1.$$

)

Example. $K = \mathbb{Q}$, and $\mathfrak{m} = m$. By the previous exercise, $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^\times / \pm 1$.

Example. $K = \mathbb{Q}$, and $\mathfrak{m} = m\infty$. Then

$$I_{m\infty} \cong \{\mathfrak{a} \in \mathbb{Q}^{>0} \mid \nu_p(\mathfrak{a}) = 1 \text{ for all } p \mid m\}$$

, and $P_{\mathfrak{m}}$ is the kernel of the natural homomorphism $I_{m\infty} \to (\mathbb{Z}/m\mathbb{Z})^\times$.)

Proposition 5.1. $C_K/C_K^{\mathfrak{m}} \cong \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$

Proof. Note $C_K/C_K^{\mathfrak{m}} \cong \mathbb{A}_K^\times / K^\times U_{\mathfrak{m}}$ We want to mimic our earlier proof and make a homomorphism from $\mathbb{A}_K^\times \to \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$ with kernel $K^\times \mathcal{O}_K$. The problem here is what to do with the factors at primes $\mathfrak{p}$ dividing $\mathfrak{m}$. So instead we're going to first map a subgroup of $\mathbb{A}_K^\times$ to $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$.

Let

$$\mathbb{A}_{K,\mathfrak{m}}^\times = \{\mathfrak{a} \in \mathbb{A}_K^\times \mid \mathfrak{a}_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}} \text{ for all finite } \mathfrak{p} \mid \mathfrak{m} \text{ and } \mathfrak{a}_v > 0 \text{ for all real } v\}.$$

Note that $\mathbb{A}_{K,\mathfrak{m}}^\times$ contains $U_{\mathfrak{m}}$: the difference between then is that elements of $\mathbb{A}_{K,\mathfrak{m}}^\times$ can be non-units at finite places not dividing $\mathfrak{p}$, where as elements of $U_{\mathfrak{m}}$ must have all components units. Let $K_{\mathfrak{m}}^\times = K^\times \cap \mathbb{A}_{K,\mathfrak{m}}^\times$.

Now there's a natural homomorphism $\mathbb{A}_{K,\mathfrak{m}}^\times \to \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$ given by $(\mathfrak{a}) \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$. The kernel of this map is $K_{\mathfrak{m}}^\times \cdot U_{\mathfrak{m}}$.

Finally, we can map $\mathbb{A}_{K,\mathfrak{m}}^\times / K_{\mathfrak{m}}^\times U_{\mathfrak{m}} \to \mathbb{A}_K^\times / K^\times U_{\mathfrak{m}}$. Exercise: this map is an isomorphism (this follows e.g. from weak approximation).

□

Example. $\mathfrak{m} = 1$, $\mathrm{Cl}_{\mathfrak{m}}(K) = \mathrm{Cl}(K)$, $L_{\mathfrak{m}} = H$ is the *Hilbert Class Field*, the maximal field extension unramified at any places (including infinite places).

$\mathfrak{m} = \prod_{v\text{real}} v$, $\mathrm{Cl}_{\mathfrak{m}}(K) = \mathrm{Cl}^+(K)$ is called the narrow class group, $L_{\mathfrak{m}} = H^+$ is narrow Hilbert class field.

The isomorphism

$$Cl_{\mathfrak{m}}(\mathcal{O}_K) \to C_K/C_K^{\mathfrak{m}} \to \mathrm{Gal}(L_{\mathfrak{m}}/K)$$

can be described explicitly. Note that $Cl_{\mathfrak{m}}(\mathcal{O}_K)$ is generated by elements of the form $[\mathfrak{p}]$ where $\mathfrak{p}$ is a fractional ideal relatively prime to $\mathfrak{m}$. The isomorphism $Cl_{\mathfrak{m}}(\mathcal{O}_K) \to C_K/C_K^{\mathfrak{m}}$ sends such a $[\mathfrak{p}]$ to class $[\mathfrak{a}]$ of the idele $\mathfrak{a} = (\mathfrak{a}_\nu) \in \mathbb{A}_K^\times$ with $\mathfrak{a}_\mathfrak{p} = \pi$ is a uniformizer of $K_\mathfrak{p}^\times$, and $\mathfrak{a}_\nu = 1$ $\nu \neq \mathfrak{p}$. Then

$$\theta_{L_{\mathfrak{m}}/K}(\mathfrak{a}) = \left(\theta_{(L_{\mathfrak{m}})_{\mathfrak{p}'}/K_\mathfrak{p}}(\pi)\right)|_{L_{\mathfrak{m}}}$$

is the Frobenius element $\mathrm{Frob}_\mathfrak{p}$ in $\mathrm{Gal}(L_{\mathfrak{m}}/K)$ since the local extension is unramified.

It follows that the Frobenius element $\mathrm{Frob}_\mathfrak{p}$ depends only on the class of $\mathfrak{p}$ in $Cl_{\mathfrak{m}}(\mathcal{O}_K)$. Hence these ray class fields are class fields in (a generalization of) the sense we used last semester

Proposition 5.2. *a)* $L_{\mathfrak{m}}$ *is unramified at all primes not dividing* $\mathfrak{m}$.

b) if $\mathfrak{m} \mid \mathfrak{m}'$ *then* $L_{\mathfrak{m}} \subset L_{\mathfrak{m}'}$.

c) $L_{\mathfrak{m}_1} \cap L_{\mathfrak{m}_2} = L_{\gcd \mathfrak{m}_1, \mathfrak{m}_2}$

d) $\cup_{\mathfrak{m}} L_{\mathfrak{m}} = K^{\mathrm{ab}}$,

Proof. For any prime $\mathfrak{p}$ not dividing $\mathfrak{m}$, the image inside C_K of $\mathcal{O}_K^\times$ is contained in $U_{\mathfrak{m}}$. It follows by local-global compatibility that $\theta_{L_{\mathfrak{m}}/K_\mathfrak{p}}\mathcal{O}_\mathfrak{p}^\times$ fixes the completion $(L_{\mathfrak{m}})_{\mathfrak{p}'}$ for any prime $\mathfrak{p}'$ of $L_{\mathfrak{m}}$ extending $\mathfrak{p}$. By local class field theory, this means that $(L_{\mathfrak{m}})_{\mathfrak{p}'}/K_\mathfrak{p}$ is unramified, and hence that $\mathfrak{p}$ is unramified in the extension $L_{\mathfrak{m}}/K$.

(This also works for infinite places with the convention that a real place ν is unramified if and only if every ν' extending ν stays real.)

b) and c) follow from definitions.

for d): any open subgroup of $\mathbb{A}_K^\times$ contains some $U_{\mathfrak{m}}$, so any open subgroup of C_K contains some $C_K^{\mathfrak{m}}$, and d) follows by Galois correspondence. □

Definition. If L is a finite abelian extension of K, then the minimal $\mathfrak{m}$ such that $L \subset L_{\mathfrak{m}}$ is referred to as the *conductor* of L, and written $\mathfrak{f} = \mathfrak{f}_{L/K}$.

This means that $\mathfrak{f}$ is minimal such that the reciprocity map $\theta_{/K} : C_K \to \mathrm{Gal}(L/K)$ factors through $Cl_\mathfrak{f}(K) \cong C_K/C_K^\mathfrak{f}$.

Two interpretations of this: first, this tells us that for any prime $\mathfrak{p}$ of $\mathcal{O}_K$ not dividing $\mathfrak{f}$, L is unramified at $\mathfrak{p}$ and $\mathrm{Frob}_\mathfrak{p} = \left(\frac{L/K}{\mathfrak{p}}\right)$ depends only on the image of $\mathfrak{p}$ in $Cl_\mathfrak{f}(\mathcal{O}_K)$

Secondly, we've stated in the main theorem of class field theory that $\ker \theta_{/K} : C_K \to \mathrm{Gal}(L/K)$ is $N_{L/K}C_L$, so this says that $\mathfrak{f}$ is minimal such that $N_{L/K}C_L \supset C_K^\mathfrak{f}$.

Exercise: the places that ramify in L are exactly those dividing $\mathfrak{f}_{L/K}$.

Example. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{p})$, $p > 0$, $p \equiv 1 \pmod 4$. Here, $\mathfrak{f}_{L/K} = p$ meaning that $L \subset \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, and for any prime q not equal to p, $\left(\frac{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}{q}\right) = \left(\frac{p}{q}\right)$ depends only on the image of q in $(\mathbb{Z}/p\mathbb{Z})^\times/\pm 1$.

6 February 15

6.1 Hilbert Class Field

The case where $\mathfrak{m} = 1$ is particularly nice. We write $L_1 = H = H_K$ and call it the *Hilbert class field* of K. You actually saw this in your homework last semester.

Proposition 6.1. *H_K is the maximal abelian extension of K unramified at any place. (where we use the convention that the extension $\mathbb{C}/\mathbb{R}$ of archimedean places is ramified).*

Proof. We've already shown that $H_K/K = K$ is everywhere unramified. On the other hand, if L is an unramified extension of K, then for any finite place v of K and any place w of L above v, the image $\theta_{/K_v}\mathcal{O}_v^\times$ under the local reciprocity map must be the identity on L_w. Likewise if v is a real place of K, $\theta_{/K_v}\mathbb{R}^\times$ must fix $L_w = K_v$.

Using the local-global compatibility, we conclude that $\theta_{/K}(C_K^1)$ must act as the identity on L, so L must be contained in the fixed field, namely H_K. □

Example. $K = \mathbb{Q}$, $H_K = \mathbb{Q}$.
$K = \mathbb{Q}(i)$, $H_K = \mathbb{Q}(i)$.
$K = \mathbb{Q}(\sqrt{-5})$, $H_K = K(i) = \mathbb{Q}(\sqrt{5}, i)$,
$K = \mathbb{Q}(\sqrt{-23}$, $H_K = K(\alpha)$ where $\alpha^3 - \alpha + 1 = 0$.

Proposition 6.2. *If L/K is Galois then so is H_L/K.*

Proof. Any element of $\mathrm{Aut}(\bar{K})$ sends unramified extensions of L to unramified extensions of L. □

As a consequence have a short exact sequence

$$1 \to \mathrm{Cl}(K) \cong \mathrm{Gal}(H_K/K) \to \mathrm{Gal}(H_K/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 1.$$

Caution: this SES does not have to split for general $K/\mathbb{Q}$: but counterexamples are messy. In the case where K is an imaginary quadratic extension of $\mathbb{Q}$, however, we can make a (non-canonical) splitting by choosing any embedding $H_K \hookrightarrow \mathbb{C}$, and letting the nontrivial element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ lift to complex conjugation on H_K.

However the SES does always induce an action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{Gal}(H_K/K) \cong \mathrm{Cl}(\mathcal{O}_K)$ by conjugation, and this action agrees with the standard action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{Cl}(\mathcal{O}_K)$ (this will follow by facts of class field theory that we haven't yet covered.

Proposition 6.3. *Let $K/\mathbb{Q}$ be an imaginary quadratic extension with Hilbert class field H. For p a prime of $\mathbb{Q}$, there exists $\pi \in \mathcal{O}_K$ with $N_{K/\mathbb{Q}}\pi = p$ if and only if p splits completely in $\mathcal{O}_H$.*

Proof. if p does not split completely in $\mathcal{O}_K$ then neither condition is true. May assume then that p splits completely in $\mathcal{O}_K$, write $(p) = N_{K/\mathbb{Q}}\mathfrak{p}$. If there exists $\pi \in \mathcal{O}_K$ with $N_{K/\mathbb{Q}}\pi = p$ we must have $\mathfrak{p} = (g\pi)$ for some $g \in \mathrm{Gal}(K/\mathbb{Q})$ by unique factorization.

Hence such a π exists iff $\mathfrak{p}$ is principal. But we know $\mathfrak{p}$ is principal iff $\mathfrak{p}$ splits completely in $\mathcal{O}_H$, which is the case iff p splits completely in $\mathcal{O}_H$, as desired. □

Example. p is a norm from $\mathbb{Z}[\sqrt{-5}]$ iff $p = x^2 + 5y^2$ if and only if p splits completely in $\mathbb{Q}(\sqrt{-5}, i)$ iff $p \equiv \pm 1 \pmod 5$ and $p \equiv 1 \pmod 4$.

Example. p is a norm from $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ iff $p = x^2 + xy + 6y^2$ iff p splits completely in $\mathbb{Q}(\sqrt{-23}, \alpha)$ iff $\left(\frac{-23}{p}\right) = 1$ and $x^3 - x + 1$ has a root modulo p.

6.2 Side note on idoneal numbers

Question: for which $D > 0$ is the set of p which are norms from $\mathcal{O}_{\sqrt{-D}}$ be determined by congruence conditions? Answer: suffices (and is also necessary, but we won't be able to show it yet) that H_K must be an abelian extension of $\mathbb{Q}$, which is equivalent to $\mathrm{Gal}(K/\mathbb{Q})$ acting trivially on $\mathrm{Cl}(K)$. But complex conjugation sends an ideal class to its inverse, so this is equivalent to saying that $\mathrm{Cl}(K)$ is 2-torsion.

Theorem 6.4 (Weinberger '73)**.** *There are only finitely many* D *for which this is the case ("Euler's idoneal numbers"): assuming GRH, we know the entire list.*

Very rough heuristic for why we expect this: the size of $\mathrm{Cl}(\mathcal{O}_{\sqrt{-D}})$ grows like $D^{1/2}$: in fact, Brauer-Siegel tells us that $\#(\mathrm{Cl}(\mathcal{O}_{\sqrt{-D}}))$ can be bounded below by a constant times $D^{1/2-\epsilon}$ for any $\epsilon > 0$, but the constant is completely ineffective.

On the other hand, the size of $\#(\mathrm{Cl}(\mathcal{O}_{\sqrt{-D}})[2])$ of the 2-torsion subgroup can be computed explicitly (you did a special case on this on HW last semester), and is (up to a small factor) equal to the number of divisors of D. The number of divisors $d(D)$ is on average approximately $\log D$, though there's some variation in size, there's still an upper bound $d(D) < e^{\log D / \log\log D}$ which is $o(D^\epsilon)$ for every ϵ. As a result we expect that when D gets large enough $\mathrm{Cl}(\mathcal{O}_{\sqrt{-D}})$ is too large to be all 2-torsion.

6.3 Ideals become principal in the Hilbert class field

The Hilbert class field also has another important property, which is that any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ becomes principal in $\mathcal{O}_H$: that is, $\mathfrak{a}\mathcal{O}_H$ is principal. This was the last of Hilbert's conjectures about the Hilbert class field to be settled, in 1929 when Artin reduced it to a group theoretic result (which was in turn proved by Furtwangler).

In order to prove this we'll need a little bit more about the Artin map than we've done so far.

6.4 Artin map and change of base

Suppose L/K is a finite separable extension, and suppose that L'/K is a finite Galois extension containing L. Then we have Artin maps $\theta_{L'/K} : C_K/N_{L'/K}C_{L'} \to \mathrm{Gal}(L'/K)^{ab}$, and $\theta_{L'/L} : C_L/N_{L'/L}C_{L'} \to \mathrm{Gal}(L'/L)^{ab}$.

The inclusion $C_K \hookrightarrow C_L$ induces a map $C_K/N_{L'/K}C_{L'} \to C_L/N_{L'/L}C_{L'}$. What is the corresponding map on the Galois side?

The answer to this is most easily seen using Galois cohomology. Note that the map above can also be described as the restriction map $\mathrm{Res} : \hat{H}^0(L'/K, C_{L'}) \to \hat{H}^0(L'/L, C_{L'})$. Hence we expect to have (and indeed we'll later see that we do have) a diagram

$$\begin{array}{ccccccc} C_K/N_{L'/K}C_{L'} & \xrightarrow{\sim} & \hat{H}^0(L'/K, C_{L'}) & \longrightarrow & \hat{H}^{-2}(L'/K, \mathbb{Z}) & \xrightarrow{\sim} & \mathrm{Gal}(L'/K)^{ab} \\ \downarrow & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow V \\ C_L/N_{L'/L}C_{L'} & \xrightarrow{\sim} & \hat{H}^0(L'/L, C_{L'}) & \longrightarrow & \hat{H}^{-2}(L'/L, \mathbb{Z}) & \xrightarrow{\sim} & \mathrm{Gal}(L'/L)^{ab} \end{array}$$

where V denotes the transfer map defined in HW last semester.

6.5 Proof of Principal ideal theorem

The group theoretic result is

Theorem 6.5 (Principal Ideal theorem of group theory)**.** *If G is a finite group, $G' = [G, G]$, $G'' = [G', G']$, then the transfer map $G/G' \to G'/G''$ is trivial.*

We won't prove it (most class field theory books skip the proof, though Artin-Tate includes a proof).

We'll deduce from this

Theorem 6.6 (Principal Ideal theorem of class field theory)**.** *The natural map $\mathrm{Cl}(K) \to \mathrm{Cl}(H)$ is trivial.*

Proof. Let H_1 be the class field of H. Observe that H_1/K is unramified, and hence that H is the maximal abelian subextension of H_1.

Let $G = \mathrm{Gal}(H_1/K)$. By the previous observation, the subgroup $\mathrm{Gal}(H_1/H)$ is equal to the commutator subgroup $G' = [G, G]$, and $G'' = \{1\}$.

We get a commutative diagram

$$\begin{array}{ccccccc} \mathrm{Cl}(K) & \xrightarrow{\sim} & C_K/N_{H/K}C_H & \xrightarrow{\theta} & \mathrm{Gal}(H/K)^{ab} & = & G/G' \\ \downarrow & & \downarrow & & \downarrow \sim & & \downarrow \sim \\ & & C_K/N_{H_1/K}C_{H_1} & \xrightarrow{\theta} & \mathrm{Gal}(H_1/K)^{ab} & = & G/G' \\ & & \downarrow & & \downarrow V & & \downarrow V \\ \mathrm{Cl}(H) & \xrightarrow{\sim} & C_H/N_{H_1/H}C_{H_1} & \xrightarrow{\theta} & \mathrm{Gal}(H_1/H)^{ab} & = & G'/G'' \end{array}$$

By the group-theoretic principal ideal theorem, the transfer map V is trivial, hence the map on the left hand side is also trivial. $\square$

6.6 Class Field Towers

(We didn't have time to go into detail about this in class.)

Question: if K is a number field does it embed in L with $|\mathrm{Cl}(L)| = 1$?

one approach: take $H_0 = H$ to be the Hilbert class field of K, H_1 to be the Hilbert class field of H_0, H_3 the Hilbert class field of H_2, etc... If this tower eventually stabilizes at some H_n, then H_n must have class number 1.

On the other hand, if K has any finite extension L with trivial class group, then the compositum HL is an unramified abelian extension of L, so $H \subset L$. Repeating this argument get that every H_n is contained in L, so the class field tower must stabilize.

Hence the answer to this question is yes if and only if the class field tower stabilizes.

It was an open question for a while in the middle of the 20th century whether class field tower must always stabilize. As it turns out, the answer is no. (Golod-Shafarevich)

The proof looks at the maximal pro-p subextension: inductively, define $H_{0,p}$ to be the maximal everywhere unramified abelian extension of K with exponent p, and $H_{i+1,p}$ to be the maximal everywhere unramified abelian extension of $H_{i,p}$ with exponent p. This tower is called the p-*class field tower of* K.

Theorem 6.7 (Golod-Shafarevich)**.** *If the* p*-class field tower stabilizes, then the* p*-rank of* $\mathrm{Cl}(K)$ *is at most* $2 + 2\sqrt{[K:\mathbb{Q}] + 1}$

In particular, if $p = [K:\mathbb{Q}] = 2$ this says that if the 2-rank of $\mathrm{Cl}(K)$ is ≥ 6, then K has an infinite 2-class field tower.

Results of genus theory say that if an imaginary quadratic extension $K/\mathbb{Q}$ has k ramified primes, then the 2-rank of $\mathrm{Cl}(K)$ is equal to $k-1$. (A special case of this was covered on HW last semester). If a real quadratic extension K/Q has k ramified primes then the 2-rank of $\mathrm{Cl}(K)$ is either $k-1$ or $k-2$.

It follows that if $K/\mathbb{Q}$ is imaginary quadratic and has at least 7 ramified primes, or real quadratic and has at least 8 ramified primes, then K has an infinite class field tower.

Actually, using a slightly sharper form of Golod-Shafarevich, in the imaginary quadratic case can show that 6 ramified primes suffice: see Cassels-Frohlich for details.

7 February 22

7.1 Review of the Brauer group

Recall from last semester that if K is any field then $H^2(K, (K^{sep})^\times)$ is called the *Brauer group* of K and will be written $\mathrm{Br}(K)$.

Last semester we looked at the Brauer groups of local fields: if K is a local field then there is a canonical isomorphism $\mathrm{inv} : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$.

Now we'll compute the Brauer group of K when K is a global field, assuming some facts of global class field theory. The basic idea is to use the short exact sequence of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules:

$$1 \to K^{\mathrm{sep}})^\times \to \mathbb{A}_{K^{\mathrm{sep}}}^\times \to C_{K^{\mathrm{sep}}} \to 1$$

where $\mathbb{A}_{K^{\mathrm{sep}}}^\times = \bigcup_{L/K \text{ finite separable}} \mathbb{A}_L^\times$ and likewise $C_{K^{\mathrm{sep}}}^\times = \bigcup_{L/K \text{ finite separable}} C_L^\times$.

7.2 Cohomology of $\mathbb{A}_L^\times$

Let L/K be a finite extension of global fields, with Galois group $G = \mathrm{Gal}(L/K)$. We'll want to compute cohomology of $\mathbb{A}_L^\times$ as a $\mathrm{Gal}(L/K)$-module. Let S be any finite set of places of K including all infinite ones, and let $\bar{S}$ be the set of all primes of L lying above some prime of S.

For simplicity, we'll write $\mathbb{A}_{L,S}^\times = \mathbb{A}_{L,\bar{S}}^\times$.

Then

$$\mathbb{A}_{L,S}^\times = \prod_{v \in S} \prod_{v'|v} L_{v'}^\times \times \prod_{v \notin S} \prod_{v'|v} \mathcal{O}_{v'}^\times.$$

For every v, choose w above v, and let G_w be the decomposition group of w:

$$G_W = g \in G \mid gw = w.$$

Have natural isomorphism $G_w \cong \mathrm{Gal}(L_w/K_v)$.

Also, the G-module

$$\prod_{v'|v} L_{v'}^\times = \prod_{g \in G/G_w} L_{gw}^\times$$

is induced/co-induced from the G_w-module $L_w^\times$.

By Shapiro's lemma, get $H^q(G, \prod_{v'|v} L_{v'}^\times) \cong H^q(G_w, L_w^\times)$, and this isomorphism is induced by

$$H^q(G, \prod_{v'|v} L_{v'}^\times) \xrightarrow{\mathrm{Res}} H^q(G_w, \prod_{v'|v} L_{v'}^\times) \xrightarrow{\pi_*} H^q(G_w, L_w^\times).$$

Hence $H^q(G, \mathbb{A}_{L,S}^\times) \cong \prod_{v \in S} H^q(G_w, L_w^\times) \times \prod_{v \notin S} H^q(G_w, \mathcal{O}_w^\times)$.

Note that if v is unramified in L, then $H^q(G_w, \mathcal{O}_w^\times) \cong H^q(L_w/K_v, \mathcal{O}_w^\times) = 1$: so if S contains all ramified primes, we have

$$H^q(G, \mathbb{A}_{L,S}^\times) \cong \prod_{v \in S} H^q(G_w, L_w^\times)$$

Now, take the direct limit over all sets S containing the ramified primes, and get

$$H^q(G, \mathbb{A}_L^\times) = \lim_S H^q(G, \mathbb{A}_{L,S}^\times) \cong \bigoplus_v H^q(L_w/K_v, L_w^\times)$$

(This also works for Tate cohomology.)

Consequences:

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

$H^2(L/K, \mathbb{A}_L^\times) = \oplus_v \frac{1}{[L_w/K_v]}\mathbb{Z}/\mathbb{Z}$.

We'll later show $H^2(L/K, C_L) \cong \frac{1}{[L/K]}\mathbb{Z}/\mathbb{Z}$, and that the diagram

$$\begin{array}{ccc} H^2(L/K, \mathbb{A}_L^\times) & \longrightarrow & H^2(L/K, C_L) \\ \downarrow \sim & & \downarrow \sim \\ \oplus_v \frac{1}{[L_w/K_v]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \frac{1}{[L/K]}\mathbb{Z}/\mathbb{Z} \end{array}$$

commutes, where the bottom map sends an element of $\frac{1}{[L_w/K_v]}\mathbb{Z}/\mathbb{Z}$ to the sum of its components.

We have a cohomology exact sequence

$$H^1(L/K, C_L) \to H^2(L/K, L^\times) \to H^2(L/K, \mathbb{A}_L^\times) \to H^2(L/K, C_L)$$

By the above observations, plus the fact (which we'll show later) that $H^1(L/K, C_L) = 0$, this exact sequence becomes

$$0 \to H^2(L/K, L^\times) \to \bigoplus_v \frac{1}{[L_w/K_v]}\mathbb{Z}/\mathbb{Z} \to \frac{1}{[L/K]}\mathbb{Z}/\mathbb{Z}$$

After taking direct limits

Theorem 7.1 (Albert-Brauer-Hasse Noether)**.** *There exists a short exact sequence* $0 \to \mathrm{Br}(K) \mapsto \oplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0$.

(and for every v we have an isomorphism $\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$.

7.3 Introduction to Brauer Group from the point of view of Central Simple Algebras

(Reference for all this material is Milne's CFT notes: http://www.jmilne.org/math/CourseNotes/CFT.pdf, chapter 4)

Take a base field K. We'll be interested in non-commutative algebras over K, e.g. the algebra $M_n(K)$ of $n \times n$ matrices

As another example of a non-commutative algebra, take the $\mathbb{R}$-algebra of Hamilton's quaternions $\mathbb{H} = \mathbb{R}\langle i, j\rangle/(i^2 = j^2 = -1, ij = -ji)$, which is spanned over $\mathbb{R}$ by $1, i, j$ and $k = ij = -ji$. This is a division algebra (every nonzero element has an inverse).

Note that if we try to construct the quaternions over $\mathbb{C}$, would get

$$\mathbb{H}_{\mathbb{C}} = \mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}\langle i, j\rangle/(i^2 = j^2 = -1, ij = -ji)$$

which is isomorphic to $M_2(\mathbb{C})$ via the map

$$i \mapsto \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right), \quad j \mapsto \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right).$$

We can say then that $\mathbb{H}$ is a *twist* or *form* of $M_2(\mathbb{R})$, since $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{R}) \otimes_{\mathbb{R}} (\mathbb{C})$.

Generally, for a field K, we will be interested in *twists* of $M_n(K)$, that is, K-algebras A such that $A \otimes_K K^{sep} \cong M_n(K^{sep})$. One thing we'll see is that these twists are classified by elements of a non-abelian Galois cohomology set (no longer a group!) $H^1(K, PGL_n(K^{sep}))$ which we haven't defined yet. We'll get a connecting homomorphism $H^1(K, PGL_n(K^{sep}) \to H^2(K, (K^{sep})^\times) = Br(K)$, which explains how the Brauer group comes into things.

There's another class of noncommutative K-algebras that can be defined in an unrelated way, but turns out to give exactly those K-algebras that are twists of $M_n(K)$ for some n. We'll do that now.

Definition. A K-algebra A is *simple* if A has no nonzero proper two-sided ideals. We say that A is a *central simple algebra* over K if A is a simple algebra and the center $Z(A) = K$.

Example. If A is any division algebra, then the center $Z(A)$ is a field K, and then A is a central simple algebra over K.

Example. For any field K of characteristic not 2, and any $a, b \in K^\times$, define a *generalized quaternion algebra* $H(a, b)$ over K by

$$H(a, b) = K\langle i, j\rangle/(i^2 = a, j^2 = b, ij = -ji).$$

As in the case of ordinary quaternions, $H(a, b)$ has basis $1, i, j, k = ij$.

You'll prove on HW that $H(a, b)$ is central simple.

Example. $M_n(K)$ is central simple over K.

Proof. Let I be a nonzero 2-sided ideal of $M_n(K)$. Choose $x \in I$ nonzero, so $x_{ij} \neq 0$ for some i, j. By rescaling may assume $x_{ij} = 1$. Then I also contains the matrix $e_{ij} = e_{ii}xe_{jj}$. By multiplying by permutation matrices on both sides, get that I contains e_{kl} for all k, l in range, so $I = M_n(K)$. □

7.4 Central Simple Algebras and the Brauer Group

Let $[\phi] \in H^2(L/K, L^\times)$ be arbitrary represented by an inhomogeneous 2-cocycle ϕ.

Definition. $A_\phi = \oplus_{g \in G} L e_g$, where the multiplication structure is determined by $e_g x = g(x) e_g$ for all $g \in G$, $x \in L$ and $e_g e_h = \phi(g,h) e_{gh}$.

The multiplicative identity 1 in A_ϕ is given by $\frac{e_1}{\phi(1,1)}$, and so we have a canonically embedded copy of L inside A given by $Le_1 = L \cdot 1$.

(One can choose the representative cocycle ϕ so that $\phi(1,1) = 1$, and then e_1 is the identity.)

It follows from the cocycle conditions that A_ϕ is an associative K-algebra. Also $[A_\phi : K] = |G|[L : K] = [L : K]^2$.

To check that A_ϕ is well-defined up to isomorphism by the class ϕ, observe that if $\phi'(g,h)/\phi(g,h) = \sigma(g) g \sigma(h)/\sigma(gh)$, then the map $A_\phi \to A_{\phi'}$ sending $e_g \mapsto \sigma(g) e'_g$ is an isomorphism.

Proposition 7.2. *A_ϕ is central simple over K.*

Proof. Central: If $a \in Z(A)$ then a commutes with L so $a \in L = Le_1$, but also a commutes with all e_g so a is in the fixed field of $\mathrm{Gal}(L/K)$ namely K.

Simple: Let I be a nonzero proper ideal of A. Take an element $a = c_1 e_{g_1} + \cdots + c_n e_{g_k} \in I$ with $c_1, \ldots, c_k \in L$, k minimal. WLOG $g_1 = 1$. Since I is not all of A, $k \geq 2$

Take $x \in L$ such that $g_2(x) \neq x$. Then $xa - ax \in I$ but

$$xa - ax = (xc_1 - c_1 x)e_1 + (xc_2 - c_2 g_2(x))e_{g_2} + \cdots = (x - g_2(x))c_2(x)e_{g_2} + \cdots$$

contradicts minimality of k. □

8 February 25

8.1 Central Simple Algebras and Tensor Product

The set of K-algebras has a natural monoid structure on it, given by tensor product: the algebra structure on $A \otimes_K B$ is determined by $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 b_1 \otimes a_2 b_2$. Important special case: $M_n(K) \otimes_K A \cong M_n(A)$.

We now do some results on how simpleness interacts with tensor products.

Proposition 8.1. *If L is a field extension of A, and $A \otimes_K L$ is a simple L-algebra, then A is a simple K-algebra.*

Proof. If I is an ideal of A, then $I \otimes_K L$ is an ideal of $A \otimes_K L$. □

The converse is not true, e.g. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$, is not simple. More generally $L \otimes_K L$ is not simple.

However, if A is central simple then $A \otimes_K L$ is simple over L. More generally:

Proposition 8.2. *A, B are K-algebras, A central simple, B simple implies $A \otimes_K B$ simple.*

Proof. Let I be an ideal of B and let $\sum_{i=1}^{n} a_i \otimes b_i$ be a nonzero element of I with n minimal.

The ideal Aa_1A is equal to all of A, so wlog can assume that $a_1 = 1$. Take commutator with arbitrary element $a \otimes 1$, minimality gives that a commutes with a_i for each i. So $a_i \in K$, and get $\sum_{i=1}^{n} a_i \otimes b_i$ in $K \otimes_K B$ can be written as $1 \otimes b$. Now use that B is simple, to get that I contains $K \otimes_K B$, hence contains $A \otimes_K B$. □

Also, if we let $Z(A)$ denote the center of a K-algebra A,

Proposition 8.3. *Have* $Z(A \otimes B) = Z(A) \otimes_K Z(B)$

Proof. Exercise. □

It follows from the previous two problems that the set of central simple algebras $/K$ forms a monoid under tensor product.

From now on, we are going to require that all central simple algebras over K are finite-dimensional.

8.2 Brauer Group in terms of Central Simple Algebras

The monoid of central simple algebras over K has a submonoid consisting of the matrix algebras $M_n(K)$ for $n \in \mathbb{Z}$. We will define the Brauer group as the quotient of the monoid of central simple algebras over K by the submonoid of matrix algebras. We need to show that this is a group.

Definition. For a K-algebra A, define A^{op} to be the K-algebra which is equal to A as a K-vector space but has the opposite multiplication: $a * b = ba$.

Note that A^{op} is central / simple if and only if A is.

Proposition 8.4. *If A is a central simple algebra of dimension n as a K-vector space, then $A \otimes_K A^{op} \cong \mathrm{End}_K(A) \cong M_n(K)$.*

Proof. We define a homomorphism $\phi : A \otimes_K A^{op} \to \mathrm{End}_K(A)$ as follows.

Let $\phi(a \otimes 1) = \ell_a$, where ℓ_a is the left multiplication map by a: $\ell_a(b) = ab$.

Let $\phi(1 \otimes a) = r_a$, where r_a is the right multiplication map by a: $r_a(b) = ba$.

Because $A \otimes_K A^{op}$ is a central simple algebra, ϕ is injective. However, $\mathrm{End}_K(A) \cong M_n(K)$ and $A \otimes_K A^{op}$ are both K-vector spaces of the same dimension n^2, so ϕ must be an isomorphism. □

Hence we may now give the original definition of the Brauer group:

Definition. The Brauer group $\mathrm{Br}(K)$ is the quotient of the monoid of central simple algebras over K by the monoid of matrix algebras.

From last time, we have a map $H^2(L/K, L^\times) \to \mathrm{Br}(K)$. In this class we'll skip the proof that it's a homomorphism (see Milne for details + references), but I will show that it maps the identity to the identity.

Let A_1 be the central simple algebra corresponding to the trivial cocycle $1 \in H^2(L/K, L^\times)$. That is, $A_1 = \bigoplus_{g \in \mathrm{Gal}(L/K)} Le_g$, and the multiplication is given by $e_g x = g(x)e_g$ for $x \in L$ and $e_{gh} = e_g e_h$.

Then we can define a homomorphism $A_1 \to \mathrm{End}_{K-\mathrm{vec}}(L)$ by sending x to the multiplication by x map, and e_g to the automorphism $g : L \to L$. Because A_1 is central simple, this map is injective, and must be an isomorphism by dimension counting.

8.3 Classification of Central Simple Algebras

In this section we'll show that any central simple algebra is of the form $M_n(D) = M_n(K) \otimes_K D$ where D is a division algebra with center K.

First we need some facts about modules over non-commutative algebras.

Definition. If M is a (finitely generated) module over a K-algebra A, we say that

- M is *simple* if M has no nonzero proper A-submodules.
- M is *semisimple* if M is the direct sum of simple A-modules.
- M is *indecomposable* if M cannot be written as $M_1 \oplus M_2$ with $M_1, M_2 \neq 0$.

Lemma 8.5. *(Schur) If M is a simple A-module, then $\mathrm{End}_A(M)$ is a division algebra.*

Proof. We need to show that any nonzero $\phi \in \mathrm{End}_A(M)$ is a unit. Note that $\ker \phi$ must equal either 0 or M, but can't be M, so must be 0. Likewise, $\mathrm{im}\, \phi$ is either 0 or M, but can't be 0, so must be M. Hence ϕ is an invertible linear transformation, and $\phi^{-1} \in \mathrm{End}_A(M)$, so ϕ is a unit in $\mathrm{End}_A(M)$. □

Proposition 8.6. *If D is a division algebra, then any f.g. D-module M is isomorphic to D^n for a unique n. Any set of n linearly independent vectors of D^n spans.*

Proof. Same as for D a field. □

For V a K-vector space and A a subalgebra of $\mathrm{End}_K(V)$, let $C(A)$ denote the centralizer of A in $\mathrm{End}_K(V)$. Observe that $C(A) = \mathrm{End}_A(V)$.

Theorem 8.7 (Double Centralizer)**.** *If A is simple, then $C(C(A)) = A$ in $\mathrm{End}_K(V)$.*

Proof. Skipped. In Milne's notes (Theorem 1.13 on page 121) he proves this assuming that V semi-simple as an A-module, which is sufficient for the proof of Theorem 8.8 (and we'll later see, using that theorem, that all A-modules are semisimple when A is simple). He also proves a generalization where $\mathrm{End}_K(V)$ is replaced by any central simple algebra B, on page 129, but that requires more theory. □

${}_AA$ denotes A considered as left A-module. Note that $\mathrm{End}_A({}_AA) \cong A^{op}$, and more generally, if V is a free A-module of rank n, $\mathrm{End}_A(V) \cong M_n(A^{op})$.

Theorem 8.8. *Any central simple algebra over K is isomorphic to $M_n(D)$ for D a division algebra.*

Proof. Choose a nonzero simple A-module S (eg a minimal nonzero left ideal of A).

Then A embeds in $\mathrm{End}_K(S)$. Let B be the centralizer of A in $\mathrm{End}_K(S)$: B is a division algebra by Schur. Then $A = \mathrm{End}_B(S)$ by the double centralizer theorem. Since B is a division algebra, $S \cong B^n$ for some n, and then $A = \mathrm{End}_B(S) \cong M_n(B^{op})$ as desired. □

Proposition 8.9. *Let A be a central simple algebra over K.*

Up to isomorphism there's a unique simple module S over A. Every finitely generated A module is semisimple and isomorphic to S^n for some n, so are classified by dimension.

Proof. By classification, $A = M_n(D)$. Then $S = D^n$ is an A-module; easily seen to be simple.

First, we decompose ${}_AA$ (A viewed as a (left) A-module) as a sum of simple A-modules as follows:

$$ {}_AA = \oplus_i S_i,$$

where S_i is the set of all matrices which are 0 outside of the ith column. Each $S_i \cong S$, so is simple.

Now let M be any simple A-module, and $m \in M$ be a nonzero element. Then define a map $\mathrm{phi} : A \to M$ by $\phi(a) = am$. For some i the restriction $\phi|_{S_i}$ must be nonzero, and since both M and S_i are simple, this implies that ϕ is an isomorphism $S \to M$.

We'll only sketch the proof of the second part: if M is a finite-dimensional A-module, we have a surjection $\phi \cong A^m = S^{mn} \to M$ for some m. Hence A is isomorphic to a quotient of S^{mn}: one can show that the only such quotients are isomorphic to S^k for some k. □

Proposition 8.10. *Any CSA A over K is isomorphic to $M_n(D)$ for some division algebra D. The division algebra D and integer n are uniquely determined by A.*

Corollary 8.11. *There is a bijection between the set of division algebras D with center K and $\mathrm{Br}(K)$ given by sending D to the class $[D]$ of D in the Brauer group.*

9 March 1

Proposition 9.1. *Any CSA A over K is isomorphic to $M_n(D)$ for some division algebra D. The division algebra D and integer n are uniquely determined by A.*

Corollary 9.2. *There is a bijection between the set of division algebras D with center K and $\mathrm{Br}(K)$ given by sending D to the class $[D]$ of D in the Brauer group.*

Corollary 9.3. $\mathrm{Br}(K) = 0$ *if K is algebraically closed.*

Proof. Follows from the fact that any finite-dimensional division algebra over K is equal to K (if $x \in D$, $K(x)$ is an algebraic field extension of K, so $x \in K$). □

Wedderburn's theorem says that every finite division algebra is a field: hence $\mathrm{Br}(\mathbb{F}_q) = 0$. (We'll see other ways of proving this later.)

Likewise, the classification of finite-dimensional division algebras over $\mathbb{R}$ gives $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, where the nonzero element is the class $[\mathbb{H}]$ of the quaternions.

9.1 Extension of base field:

If A is a CSA over K, and L/K is any field extension, we've previously seen that $A \otimes_K L$ is a CSA / L. Hence we have a homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(L)$.

Proposition 9.4. *If A is a CSA / K, then $[A : K] = \dim_K A$ is a square.*

Proof. We have $A \otimes_K \overline{K} \cong M_n(K)$ for some n, so $\dim_K A = \dim_{\overline{K}} A \otimes_K \overline{K} = n^2$. □

For L/K any field extension, let $\mathrm{Br}(L/K)$ be the kernel of the natural map $\mathrm{Br}(K) \to \mathrm{Br}(L)$. We'll show that for L/K Galois, $\mathrm{Br}(L/K) \cong H^2(L/K, L^\times)$ (which is what we expect from the other definition of $\mathrm{Br}(K) = H^2(K, (K^{\mathrm{sep}})^\times)$ plus inflation-restriction).

We say that a CSA A/K is split by L if $A \otimes_K L$ is a matrix algebra. Then A is split by L if and only if $[A] \in \mathrm{Br}(L/K)$.

Proposition 9.5. $\mathrm{Br}(K) = \bigcup_{L/K \textit{ finite}} \mathrm{Br}(L/K)$

Proof. Let $A \in \mathrm{Br}(K)$ be arbitrary. We already know that we have an isomorphism $\phi : M_n(\overline{K}) \to A \otimes_K \overline{K}$. Take L large enough that $\phi(e_{ij})$ lies in $A \otimes_K L$: then ϕ restricts to an isomorphism $M_n(L) \to A \otimes_K L$. □

Later we'll be able to sharpen this and show that any element of $\mathrm{Br}(K)$ is split by a finite separable extension L of K (and so also, replacing L by its Galois closure if necessary, by a finite Galois extension of K), but we'll need to develop more tools first.

9.2 Maximal Subfields of CSAs

First we'll ask a more basic question: if A is a CSA over K, how to tell which extensions L of K split A? Let's work out a basic example first.

Example. $K = \mathbb{Q}$, $A = H(-1,-1)$ is the quaternion algebra with generators i, j, k and relations $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$.

Then for any extension L of $\mathbb{Q}$, the algebra $A \otimes_{\mathbb{Q}} L = H_L(-1,-1)$ is a quaternion algebra over L. By your HW, A is split by L if and only if either one of the following two equivalent conditions holds:

- $x^2 + y^2 + z^2 = 0$ has a nonzero solution in L^3.
- $x^2 + y^2 + z^2 + w^2 = 0$ has a nonzero solution in L^4

Consider the case where $L = \mathbb{Q}(\sqrt{D})$ is a quadratic extension of $\mathbb{Q}$, D a squarefree integer. First of all, if $D > 0$, then L embeds in $\mathbb{R}$: since the quadratic forms above are positive definite, we conclude that A is not split by L.

If D is congruent to $1 \pmod 8$, then $\mathbb{Q}(\sqrt{D})$ embeds in $\mathbb{Q}_2$. Again, we can check that the quadratic form $x^2 + y^2 + z^2 = 0$ has only trivial solutions in $\mathbb{Q}_2$ (WLOG $x, y, z \in \mathbb{Z}_2$ are relatively prime, and work mod 4), so it has no solutions in $\mathbb{Q}(\sqrt{D})$.

In any other case, we can use Legendre's three squares theorem to write $-D = a^2 + b^2 + c^2$, for $a, b, c \in \mathbb{Z}$ and then $(a, b, c, \sqrt{D})$ is a solution to $x^2 + y^2 + z^2 + w^2 = 0$, so A is split by L.

In short, $\mathbb{Q}(\sqrt{D})$ splits A iff D is negative and $1 \pmod 8$ iff $-D$ is the sum of three rational squares.

Another equivalent condition is the following: $\mathbb{Q}(\sqrt{D})$ embeds in A. To see this, note that if $\alpha = w + xi + yj + zk$, $w, x, y, z \in \mathbb{Q}$, is an arbitrary element of A, $\alpha^2 = D$ iff $w = 0$ and $x^2 + y^2 + z^2 = -D$. This condition is one we'll be able to generalize.

First we need the following algebraic fact, which we will state without proof:

Theorem 9.6. *Double centralizer theorem for central simple algebras: if A is a CSA, $B \subset A$ simple, and $C = C(B)$, then C is simple, $B = C(C)$ and $[A : K] = [B : K][C : K]$. (As with field extensions, $[A : K]$ denotes the dimension of A as a K-vector space.)*

Proof. (See Milne) □

Corollary 9.7. *If $Z(B) = K$ then $Z(C) = K$ and $A \cong B \otimes_K C$.*

Proof. For the first part, $Z(B) = B \cap C = Z(C)$. For the second part, since both B and C are central simple over K, so is $B \otimes_K C$, and the natural map $B \otimes_K C \to A$ must be injective. By dimension counting it's an isomorphism. □

Corollary 9.8. *For A a CSA/K and $L \subset A$ a field. TFAE:*

a) $L = C(L)$

b) $[L : K]^2 = [A : K]$

c) L *is a maximal commutative* K*-subalgebra.*

Proof. a) implies b) by double centralizer. b)implies c) : if L' is a comm K-subalg of A, then $[L' : K]^2 \leq [L' : K][C(L') : K] = [A : K] = [L : K]^2$, so $[L' : K] \leq [L : K]$, hence L is maximal. c) implies a) : if $x \in C(L) \setminus L$ then $L[x]$ is commutative.

□

Corollary 9.9. *If* D *is a division algebra, the maximal commutative subfields of* D *all have dimension* $[L : K] = \sqrt{[D : K]}$.

Proof. This follows because every commutative subalgebra of D is a field. □

Proposition 9.10. L *splits* A *if and only if there is an algebra* $B \sim A$ *containing a subfield isomorphic to* L *such that* $[B : K] = [L : K]^2$.

Let's correct the proof of the $\Rightarrow$ direction, and give a proof of $\Leftarrow$:

Proof. $\Rightarrow$: L splits A, so also A^{op}, so $A^{op} \otimes_K L \cong \mathrm{End}_L(V)$ for some L-vector space V with $\dim_L(V) = \sqrt{[A : K]}$.

Take B to be the centralizer of A^{op} in $\mathrm{End}_K(V)$. By Corollary 9.7 we have $B \otimes A^{op} \cong \mathrm{End}_K(V)$, so $[B] = [A]$ in $\mathrm{Br}(K)$. Also, $1 \otimes L \subset B$ since $A^{op} \otimes 1$ commutes with $1 \otimes L$. Finally,

$$[B : K] = \frac{[\mathrm{End}_K(V) : K]}{[A^{op} : K]} = \frac{\dim_K(V)^2}{[A : K]} = [L : K]^2 \frac{\dim_L(V)^2}{[A : K]} = [L : K]^2.$$

For other direction, enough to show that L splits B. Say $[L : K] = n$ so $[B : K] = [L : K]^2$. We need a vector space V such that $B \otimes_K L \cong \mathrm{End}_L(V)$: since $B \otimes_K L$ is of dimension n^2 over L, we need V to be an n-dimensional L-vector space.

The obvious choice is $V = B$: however, since B is non-commutative, we'll take the L-vector space structure on B to have L acting by right multiplication. (Alternatively we could take $V = B^{op}$ with L acting by left multiplication, but this will be notationally simpler.)

Then we can map $B \otimes_K L \to \mathrm{End}_L(V)$ by $b \otimes 1 \mapsto \ell_b$ (where ℓ_b is the left multiplication by b map) and $1 \otimes \ell \mapsto r_\ell$ (where r_ℓ is right multiplication by ℓ.) This map is an injection because $B \otimes_K L$ is simple, and is surjective by dimension count.

□

Corollary 9.11. *Suppose* $[L : K] = \sqrt{[D : K]}$. *Then* L *splits* D *iff* L *embeds in* D*; that is, all maximal subfields of* D *split* D.

10 March 4

Last time showed that if D is a division algebra, D is split by any maximal subfield. Can show (see Milne) that any central division algebra contains a separable maximal subfield.

Corollary 10.1. *Any CSA A/K is split by some finite separable extension of K, so also by some Galois extension of K.*

Proof. We have $A \cong M_n(D)$ for some D, so A is split by any separable maximal subfield L of D. Then A is also split by any Galois extension of K containing L (e.g. the Galois closure of L/K). □

Suppose L/K Galois, and $G = \mathrm{Gal}(L/K)$.

Definition. $\mathcal{A}(L/K)$ is the set of CSAs A of degree $[L:K]^2$ split by L

Last time, we proved that the natural map $\mathcal{A}(L/K) \to \mathrm{Br}(L/K)$ is a bijection.
Recall: for $[\phi] \in H^2(L/K, L^\times)$ defined

Definition. $A_\phi = \oplus_{g\in G} L e_g$, where the multiplication structure is determined by $e_g x = g(x)e_g$ for all $g \in G$, $x \in L$ and $e_g e_h = \phi(g,h)e_{gh}$, and the identity element is $e_1/\phi(1,1)$.

This gives us a map $[\phi] \mapsto A_\phi : H^2(L/K, L^\times) \to \mathcal{A}(L/K)$. Today we'll show this map is a bijection, and so induces an isomorphism $H^2(L/K, L^\times) \to \mathrm{Br}(L/K)$.

10.1 Noether-Skolem

Theorem 10.2 (Noether-Skolem)**.** *If A, B are finite-dimensional K-algebras, A simple, B central simple, then any two homs $f, g : A \to B$ are conjugate: related by $g = bfb^{-1}$.*

Example. K arbitrary (char not 2), $f, g : K(\sqrt{(x)}) \to H(x,y)$ given by $f(\sqrt{x}) = i$, $g(\sqrt{x}) = -i$, take $b = j$.

We give the important corollaries first.

Corollary 10.3. *If A is a simple algebra, all automorphisms of A are inner.*

Corollary 10.4. *If A is a central simple algebra over K, and L is a finite extension of K, then any two embeddings $i_1, i_2 : L \hookrightarrow A$ are conjugate to each other by some element of A ($i_2 = a i_1 a^{-1}$ for some $a \in A$).*

We now prove Noether-Skolem

Proof of Noether-Skolem. We handle the case of $B = M_n(K)$ first. We put two different A-module structures on K^n extending the K-vector space structure.

Let $M_1 = K^n$ with A-module structure $a *_1 v = f(a)v$, and let $M_2 = K^n$ with A-module structure $a *_2 v = g(a)v$.

Since A-modules are classified by dimension, there is an A-module isomorphism $\phi : M_1 \to M_2$. Since ϕ is a K-linear map, it can be viewed as a matrix $\phi \in M_n(K)$.

Then $\phi(f(a)v) = g(a)(\phi v)$ for all $v \in K^n$, so $\phi f(a) = g(a)\phi \in M_n(K)$, hence f and g are conjugate as desired.

Now let B be a general central simple algebra over K. We use the fact $B \otimes B^{op}$ is a matrix algebra, and apply the first part to get that the maps $f \otimes 1, g \otimes 1 : A \otimes B^{op} \to B \otimes B^{op}$ are conjugate. That is, there is some $x \in B \otimes B^{op}$ with

$$x(f(a) \otimes b')x^{-1} = (g(a) \otimes b')$$

for all $b' \in B^{op}$. In particular, setting $a = 1$ get that x commutes with $1 \otimes B^{op}$: implies that $x = b \otimes 1$ for some $b \in B$. This b has the desired property. □

10.2 Bijection between Central Simple Algebras and Cocycles

Suppose $A \in \mathcal{A}(L/K)$, and fix an embedding $i : L \hookrightarrow A$ (by Noether-Skolem, i is unique up to inner automorphisms of A.) Identify L with $i(L) \subset A$.

Take any $g \in \mathrm{Gal}(L/K)$. By Noether-Skolem applied to $i, i \circ g : L \to A$ there exists $a_g \in A^\times$ such that $g(x) = a_g x a_g^{-1}$ for all $x \in L$. Here a_g is well defined up to left multiplication by elements of $C(L) = L$, since if

$$g(x) = a_g x a_g^{-1} = b_g x b_g^{-1}$$

for all $x \in L$ we have that $a_g b_g^{-1}$ commutes with $g(x)$ for all $x \in L$.

(Alternatively, a_g is well-defined up to right multiplication by elements of $C(L) = L$, since $a_g^{-1} b_g$ commutes with all $x \in L$. But these come down to the same thing since $a_g \ell = g(\ell) a_g$ for all $ell \in L$.)

Now note that for $g, h \in G$ $(a_g a_h)x(a_g a_h)^{-1} = g(h(x))$, so $a_g a_h$ must equal $\phi(g, h)$ for some $\phi(g, h) \in L$.

This $\phi = \phi_A$ will give our desired cohomology class in $H^2(G, L^\times)$. To check that ϕ is a cocycle, expand$(a_{g_1} a_{g_2})a_{g_3} = a_{g_1}(a_{g_2} a_{g_3})$ and cancel the unit $a_{g_1 g_2 g_3}$ from both sides.

Now, the elements a_g are only defined up to multiplication by elements of L. If we choose a different set of elements $a'_g = \psi(g)a_g$, then the new cocyle ϕ' is given by

$$\phi'(g, h) = \frac{\psi(g, h)}{\psi(g) \cdot g\psi(h)} \phi(g, h)$$

so represents the same class in $H^2(G, L^\times)$.

Easily checked that $A \mapsto A_\phi$ and $\phi \mapsto \phi_A$ are inverses.

Example. $A = H(a, b)$, $L = K(\sqrt{(a)}) \cong K(i)$. Can take $a_1 = 1$, $a_2 = j$. Write $G = \{1, \sigma\}$. Here $\phi(1,1) = \phi(1,\sigma) = \phi(\sigma, 1) = 1$ and $\phi(\sigma,\sigma) = b$.

As well, the following diagrams commute (though again we'll skip proofs)

$$\begin{array}{ccc} \mathrm{Br}(L/K) & \hookrightarrow & \mathrm{Br}(E/K) \\ \downarrow\sim & & \downarrow\sim \\ H^2(L/K, L^\times) & \xrightarrow{\inf} & H^2(E/K, E^\times) \end{array}$$

where $E \supset L$ is a field with E/K finite Galois.

and

$$\begin{array}{ccc} \mathrm{Br}(L/K) & \xrightarrow{A \mapsto A \otimes_K M} & \mathrm{Br}(L/M) \\ \downarrow\sim & & \downarrow\sim \\ H^2(L/K, L^\times) & \xrightarrow{\mathrm{Res}} & H^2(L/M, L^\times) \end{array}$$

where M is any intermediate field.

As a consequence of the first diagram above we get an isomorphism

$$\mathrm{Br}(K) = \bigcup_{L/K} \mathrm{Br}(L/K) = \varinjlim_{L} \mathrm{Br}(L/K) = \varinjlim_{L} H^2(L/K, L^\times) = H^2(K, (K^{\mathrm{sep}})^\times)$$

(where L runs through all finite Galois extensions of K), justifying the terminology $\mathrm{Br}(K)$ used previously in this class.

Corollary 10.5. *If* $[L : K] = n$, $\mathrm{Br}(L/K)$ *is an* n*-torsion group.* $\mathrm{Br}(K)$ *is a torsion group.*

Observe that if K is a local field of characterstic not 2 and H/K is a quaternion algebra, then the class $[H]$ is in the 2-torsion subgroup of $\mathrm{Br}(K)$. Hence there are exactly two isomorphism classes of quaternion algebras over K, one represented by $M_2(K)$ (the "split" quaternion algebra) and one by the unique division algebra D/K of degree 4 ("nonsplit").

10.3 Brauer Groups of Local Fields

First we deal with archimedean local fields. $\mathrm{Br}(\mathbb{C}) = 0$ because $\mathbb{C}$ is algebraically closed. For $\mathbb{R}$ we can compute via cohomology: $\mathrm{Br}(\mathbb{R}) = H^2(\mathbb{R}, \mathbb{C}^\times) \cong \hat{H}^0(\mathbb{R}, \mathbb{C}^\times) = \mathbb{R}^\times / N\mathbb{C}^\times$ is cyclic of order 2.

If K is a nonarchimedean local field: we have already constructed an isomorphism $\mathrm{inv} : \mathrm{Br}(K) \cong H^2(K, (K^{\mathrm{sep}})^\times) \to \mathbb{Q}/\mathbb{Z}$.

We also know that if L/K has degree n, the following diagram commutes

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{\mathrm{Res}} & \mathrm{Br}(L) \\ \downarrow{\scriptstyle \mathrm{inv}} & & \downarrow{\scriptstyle \mathrm{inv}} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\times n} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Hence if $x \in \mathrm{Br}(K)$ has $\mathrm{inv}(x) \in \frac{1}{n}\mathbb{Z}$, then x is split by any extension L with $[L : K] = n$. In particular, x is split by the unramified extension K_n of K of degree n. Now, K_n/K is cyclic, so any element of $\mathrm{Br}(K_n/K)$ is of the form A_a for some $a \in K^\times/NL^\times$ (see problem 2 on current problem set).

10.4 Global Fields

If K is a global field, we can now apply

Theorem 10.6 (Albert-Brauer-Hasse-Noether)**.** *There exists a short exact sequence* $0 \to \mathrm{Br}(K) \mapsto \oplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0$.

Example. $K = \mathbb{Q}$, $A = H(a, b)$ is a quaternion algebra. Then ABHN says that $H(a, b)$ is non-split at an even number of places e.g. $\prod_v (a, b)_v$ is 1. And conversely, given a set S of places with even cardinality, we can produce a quaternion algebra that is split exactly at those places (this is a little stronger than ABHN).

Specialize to case of $a = p, b = q$ positive primes. Then $\prod_v (p, q)_v = 1$. $(p, q)_\infty = 1$, also $(p, q)_p$ is $\left(\frac{q}{p}\right)$, and $(p, q)_q$ is $\left(\frac{p}{q}\right)$, and $(p, q)_2 = (-1)^{(p-1)(q-1)/2}$. Hence in this case we get quadratic reciprocity again!

Let K be a number field now. Just as in the case of local field, there is a special class of fields that splits every element of $\mathrm{Br}(K)$.

Definition. An extension L/K is cyclic cyclotomic if $L \subset K(\zeta_n)$ for some n and $\mathrm{Gal}(L/K)$ is cyclic.

Homework problem: If K is a number field, S a finite set of places of K, m a positive integer there exists L/K cyclic cyclotomic such that $m \mid [L_w : K_v]$ for all places v in S and all w above v.

Corollary 10.7. *If K is a number field and A is any CSA/K there exists a cyclic cyclotomic field that splits A.*

Proof. Choose S to be the set of places for which $\mathrm{inv}_v(A \otimes_K K_v) \neq 0$ and let m be the least common denominator of the values of $\mathrm{inv}_v(A \otimes_K K_v)$.

Then for any v and w as above, $\mathrm{inv}_v(A \otimes_K L_w) = [L_w : K_v]\,\mathrm{inv}_v(A \otimes_K K_v) = 0 \in \mathbb{Q}/\mathbb{Z}$. Hence the class $[A \otimes_K L] \in \mathrm{Br}(L)$ maps to the 0 element in $\prod_w \mathrm{Br}(L_w)$, so L must split A. □

11 March 8

11.1 Digression on sums of three cubes

$$8866128975287528^3 + (-8778405442862239)^3 + (-2736111468807040)^3 = 33$$

(Andrew Booker, https://people.maths.bris.ac.uk/~maarb/papers/cubesv1.pdf, 2019. Originally announced at https://pub.ist.ac.at/ tbrownin/)

General question: which n can be written as $a^3 + b^3 + c^3 \mid a, b, c \in \mathbb{Z}$, and in how many ways? FLT tells us that 0 is not possible, but that's a special case. Local considerations tell us that $n \not\equiv \pm 4 \pmod 9$. Current best guess is that for every other n there is a solution, in fact infinitely many such. Solutions have been found for every $1 \leq n < 114$ not $\pm 4 \pmod 9$ except for $n = 42$, but except for special values of n we only know finitely many solutions.

Case of $n = 3$: known solutions are $(1,1,1)$ and $(4,4,-5)$ (up to permutation). As above, infinitely many solutions are expected. If $a^3 + b^3 + c^3 = 3$ local 3-adic considerations show $a \equiv b \equiv c \equiv 1 \pmod 3$. Using cubic reciprocity can show that also $a \equiv b \equiv c \pmod 9$.

(Hint: 3 is a cube mod $\omega a + \omega^2 b$.)

11.2 Anabelian philosophy

Anabelian philosophy: can understand a field K by studying the absolute Galois group G_K. More generally, given a scheme X, can understand X by studying $\pi_1^{\text{ét}}(X)$.

(Topological analogues: topological 2-manifolds are determined up to homeomorphism by their fundamental groups. Mostow rigidity: in dimension ≥ 3 manifolds of constant negative curvature are determined (as Riemannian manifolds) by their fundamental groups.)

Neukirch-Uchida theorem: if K and L are global fields, $G_K \cong G_L$ if and only if $K \cong L$, and in fact any isomorphism $G_K \to G_L$ is induced by an isomorphism $K \to L$.

11.3 Class formations

Class formations are a way of formalizing the algebraic structure that is common to local and global class field theory: they follow the anabelian philosophy in that they start with the absolute Galois group, viewed as a profinite group.

Let G be a profinite group. We consider the set of open subgroups of G (necessarily of finite index), which we write as $\{G_K \mid K \in X\}$, and refer to these indices K as "fields". The field K_0 with $G_{K_0} = G$ is called the "base field."

Write $K \subset L$ if $G_L \subset G_K$. A pair K, L with $K \subset L$ is called a "layer" L/K. The degree of the layer is $[G_K : G_L]$. We say that L/K is *normal* if G_L is normal in G_K, write $G_{L/K} = G_K/G_L$.

Can formally define intersection and union of subgroups. Define gK by $G_{gK} = gG_Kg^{-1}$.

A formation A is a G-module on which G acts continuously when A is given the discrete topology.

Equivalently: $A = \cup_{U \subset G \text{ open}} A^U$

Write $A^{G_K} = A_K$, so $A = \cup_K A_K$.

E.g. K_0 local, $G = \mathrm{Gal}(K_0^{sep}/K_0)$, $A = (K_0^{sep})^\times$.

Or K_0 global, $G = \mathrm{Gal}(K_0^{sep}/K_0)$, $A = \varinjlim_{K/K_0 \text{ finite}} C_K$.

Write $A_L = A^{G_L}$.

Write $H^q(L/K) = H^q(G_{L/K}, A_L)$. (Also write $H^q(/K) = H^q(G_K, A)$.)

If $E/L/K$ with E/K and L/K normal layers then get inflation map

$H^q(L/K) = H^q(G_{L/K}, A_E^{G_{L/K}/G_{E/K}}) \to H^q(G_{E/K}, A_E) = H^q(E/K)$.

Also: restriction map $\mathrm{Res} : H^q(L/K) \to H^q(L/M)$ and corestriction $\mathrm{Cor} : H^q(L/M) \to H^q(L/K)$.

Suppose that L/K is a normal layer and $g \in G$ is arbitrary. Then there are natural isomorphisms $G_{L/K} \cong G_{gL/gK}$ and $A_L \to A_{gL}$. The isomorphisms induce a natural homomorphism $g^* : H^q(L/K) \to H^q(gL/gK)$. If $g \in G_K$ then $gK = K$ but also $gL = L$ as L/K is normal. Exercise: g^* is the identity.

Definition. A is a *field formation* if for every layer L/K, $H^1(L/K) = 0$.

Example. If K_0 is any field, $G = \mathrm{Gal}((K^0)^{sep}/K_0)$, $A = ((K_0^{sep})^\times)$. (More generally, K any algebraic extension of K^0, $G = \mathrm{Gal}(K/K^0)$, $A = K^\times$.)

Example. If K_0 is a global field, $G = \mathrm{Gal}((K^0)^{sep}/K_0)$, $A = \varinjlim_{K/K_0 \text{ finite}} \mathbb{A}_K$ as K runs through finite extensions of K_0.

If A is a field formation then have inflation restriction exact sequence in deg 2:

$$1 \to H^2(L/K) \to H^2(E/K) \to H^2(E/L).$$

In particular, this means that $H^2(/K) = \bigcup_L H^2(L/K)$.

Definition. A is a *class formation* if for every normal layer L/K there is an isomorphism $\mathrm{inv}_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ such that the diagrams

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \downarrow \mathrm{inf} & & \downarrow \\ H^2(E/K) & \xrightarrow{\mathrm{inv}_{E/K}} & \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} \end{array}$$

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \downarrow \mathrm{Res} & & \downarrow \times[M:K] \\ H^2(L/M) & \xrightarrow{\mathrm{inv}_{L/M}} & \frac{1}{[L:M]}\mathbb{Z}/\mathbb{Z} \end{array}$$

commute.

Example. The simplest example of a class formation:

$G = \hat{\mathbb{Z}}$, $A = \mathbb{Z}$ with trivial action. $G_{K_n} = n\hat{\mathbb{Z}}$, $A_{K_n} = \mathbb{Z}$.

Then, for $m \mid n$, K_n/K_m is a layer and $H^1(K_n/K_m) = H^1(G_{K_m}/G_{K_n}, \mathbb{Z}) = 0$ because G_{K_m}/G_{K_n} is cyclic of order n/m.

Likewise, $H^2(K_n/K_m) \cong \hat{H}^0(K_n/K_m) \cong \mathbb{Z}/(n/m)\mathbb{Z}$, and we can define inv_{K_n/K_m} by composing with $\times\frac{1}{n/m} : \mathbb{Z}/(n/m)\mathbb{Z} \to \frac{1}{n/m}\mathbb{Z}/\mathbb{Z}$.

Example. K_0 local field: $G = \mathrm{Gal}(K_0^{\mathrm{sep}}/K_0)$, $A = (K_0^{\mathrm{sep}})^\times$ is a class formation by last semester.

K_0 global field: $G = \mathrm{Gal}(K_0^{\mathrm{sep}}/K_0)$, $A = \varinjlim_{L/K \text{ finite}} C_L$: we haven't proved this is a class formation, but we will.

Proposition 11.1. *Suppose that A is a class formation. Then*

a)

$$\begin{array}{ccc} H^2(L/M) & \xrightarrow{\mathrm{inv}_{L/M}} & \frac{1}{[L:M]}\mathbb{Z}/\mathbb{Z} \\ \downarrow \mathrm{Cor} & & \downarrow \\ H^2(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \end{array}$$

commutes

b)

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \downarrow g^* & & \downarrow \sim \\ H^2(gL/gK) & \xrightarrow{\mathrm{inv}_{gL/gK}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \end{array}$$

commutes

Proof. For a), we make a big commutative diagram:

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\text{inv}_{L/K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \downarrow \text{Res} & & \downarrow \times[M:K] \\ H^2(L/M) & \xrightarrow{\text{inv}_{L/M}} & \frac{1}{[L:M]}\mathbb{Z}/\mathbb{Z} \\ \downarrow \text{Cor} & & \downarrow \\ H^2(L/K) & \xrightarrow{\text{inv}_{L/K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \end{array}$$

The top square commutes by class formation axiom, and the entire rectangle commutes because $\text{Cor} \circ \text{Res} = [L : K]$. Since the two top vertical arrows are surjective, we can chase the diagram to find that the bottom square commutes.

Part b) will be done on HW, but here's a sketch: first of all, we've observed that if $g \in K$, then $gL = L$, $gK = K$, and $g^* : H^2(L/K) \to H^2(L/K)$ is the identity map, so we already have the commutative diagram.

For the general case, find a field L' extending L such that L'/K_0 is normal. Construct injection $H^2(L/K) \to H^2(L'/K_0)$ and use that to transfer the result from L'/K_0 to L/K. □

Definition. *Fundamental class* $u_{L/K} \in H^2(L/K)$ defined by $\text{inv}(u_{L/K}) = \frac{1}{[L:K]}$.

Proposition 11.2. *Let* $E/L/K$ *be fields with* E/K *normal. Then*

a) $\text{Res}_L u_{E/K} = u_{E/L}$

b) $u_{L/K} = [E : L] \inf u_{E/K}$ *if* $[L : K]$ *normal*

c) $\text{Cor}_K u_{E/L} = [L : K] u_{E/K}$

d) $g^*(u_{E/K}) = u_{gE/gK}$

proof: exercise.

Theorem 11.3. *For any normal layer* L/K*, cup product with* $u_{L/K}$ *gives an isomorphism* $\hat{H}^q(G_{L/K}, \mathbb{Z}) \to \hat{H}^{q+2}(L/K)$

Proof. Exactly the same as in local case. □

In particular, do the case $q = -2$: get isomorphism $G_{L/K}^{ab} \cong \hat{H}^{-2}(G_{L/K}, \mathbb{Z}) \to \hat{H}^0(L/K) = A_K/NA_L$.

As before, we denote the inverse isomorphism $\hat{H}^{-2}(G_{L/K}, \mathbb{Z}) \to G_{L/K}^{ab}$ by $\theta_{L/K}$.

Our goals now: show that G_K, C_K is a class formation. (will focus on number fields case)

Need to show two things: $H^1(L/K)$ is trivial, and construct invariant map $H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

Intermediate steps:

First inequality: show that if L/K is cyclic then $|H^2(L/K)| \geq [L : K]$ (We'll do this by showing that the Herbrand quotient $H^2(L/K)/H^1(L/K) = [L : K]$.)

Second inequality: show that if L/K is cyclic of prime order, then $|H^2(L/K)| \leq [L : K]$.

(Combining Second inequality with Herbrand quotient, get $|H^2(L/K)| = [L : K]$ and $H^1(L/K) = 0$ for cyclic layers. For non-cyclic layers, can deduce that $H^1(L/K)$ vanishes and $H^2(L/K) \leq [L : K]$.) Then: construct $\text{inv}_{L/K}$ from local reciprocity maps.

12 March 11

12.1 First inequality and Herbrand quotient for C_L

Recall: if G is a cylic group and A is a G-module, the Herbrand quotient $h(A)$ is equal to $|\hat{H}^0(G, A)|/|\hat{H}^1(G, A)|$. We'll use the following facts

- the Herbrand quotient is multiplicative in short exact sequences
- $h(A) = 0$ if A finite
- $h(\mathbb{Z}) = |G|$.

We're going to set ourselves up to compute the Herbrand quotient for C_L. First, choose a set of places S of K large enough that:

(a) S contains all infinite places.

(b) S contains all places that ramify in L.

(c) $\mathbb{A}_{L,S}^\times$ surjects onto C_L (can do this by making sure that $\bar{S}$ contains a set of generators for $\text{Cl}(\mathcal{O}_K)$)

(d) $\mathbb{A}_{K,S}^\times$ surjects onto C_K (likewise)

Then we have a short exact sequence

$$1 \to \mathcal{O}_{L,S}^\times \to \mathbb{A}_{L,S}^\times \to C_L \to 1,$$

so the Herbrand quotient $h(C_L) = \frac{h(\mathbb{A}_{L,S}^\times)}{h(\mathcal{O}_{L,S}^\times)}$.

Recall that we've already computed $\hat{H}^i(\mathbb{A}_{L,S}^\times) = \prod_{v \in S} \hat{H}^i(L_w/K_v, L_w^\times)$. Hence the Herbrand quotient $h(\mathbb{A}_{L,S}^\times)$ is equal to the product of the local Herbrand quotients of $L_w^\times$, namely $\prod_{v \in S}[L_w : K_v]$.

12.2 The Herbrand quotient of $\mathcal{O}_{L,S}^\times$

Our strategy here is to show that the Herbrand quotient of $\mathcal{O}_{L,S}^\times$ only depends on the $\mathbb{R}[G]$-module $\mathcal{O}_{L,S}^\times \otimes_{\mathbb{Z}} \mathbb{R}$, which we can describe by Dirichlet's units theorem.

Lemma 12.1. *G is a finite group.*

L/K fields, K infinite.

Two $K[G]$-modules V_1, V_2 are isomorphic iff $V_1 \otimes_K L$ and $V_2 \otimes_K L$ are isomorphic $L[G]$-modules.

Proof. We have an isomorphism: $\mathrm{Hom}_{L[G]}(V_1 \otimes_K L, V_2 \otimes_K L) \cong \mathrm{Hom}_{K[G]}(V_1, V_2) \otimes L$.

We choose K-bases for V_1 and V_2.

We have then have determinant maps $\det : \mathrm{Hom}_{L[G]}(V_1 \otimes_K L, V_2 \otimes_K L) \to L$ which restricts to $\det : \mathrm{Hom}_{K[G]}(V_1, V_2) \to K$. Observe that det is a polynomial map. Because of the assumption that $V_1 \otimes_K L \cong V_2 \otimes_K L$, we know that det not identically 0 on $\mathrm{Hom}_{L[G]}(V_1 \otimes_K L, V_2 \otimes_K L)$. Hence its restriction to $\mathrm{Hom}_{K[G]}(V_1, V_2)$ is not the zero polynomial either, and there must be some $\phi \in \mathrm{Hom}_{K[G]}(V_1, V_2)$ with $\det \phi \neq 0$. □

Remark. Can also prove this via Galois descent when L/K finite Galois, and then deduce the case where L/K is arbitrary. To do this, we observe that $\mathrm{Isom}_{L[G]}(V_1, V_2)$ is a torsor for the group $\mathrm{Aut}_{L[G]}(V_1)$. Can show that $\mathrm{Aut}_{L[G]}(V_1)$ is the group of units in a central simple algebra over L, and that $H^1(G, \mathrm{Aut}_{L[G]}(V_1))$ is trivial. Hence $\mathrm{Isom}_{L[G]}(V_1, V_2)$ is the trivial torsor, which implies that $\mathrm{Isom}_{L[G]}(V_1, V_2)^G = \mathrm{Isom}_{L[G]}(V_1, V_2)$ is nonempty.

Proposition 12.2. *If A, B are G-modules that are f.g. as abelian groups, and $A \otimes_{\mathbb{Z}} \mathbb{R} \cong B \otimes_{\mathbb{Z}} \mathbb{R}$ then $h(A) = h(B)$.*

Proof. By Lemma, $A \otimes_{\mathbb{Z}} \mathbb{Q} \cong B \otimes_{\mathbb{Z}} \mathbb{Q}$.

exercise: this means that there is a finite index subgroup A' of $A/T(A)$ isomorphic (as G-module) to a finite index subgroup B' of $B/T(B)$.

Hence $h(A) = h(A') = h(B') = h(B)$. □

Have isomorphism $(\mathcal{O}_{L,S}^\times) \otimes_{\mathbb{Z}} \mathbb{R} \cong H \subset \prod_{v' \in \bar{S}} \mathbb{R}^+$ given by

$$(a) \otimes 1 \mapsto (\log |a|_{v'})_{v' \in \bar{S}}$$

Extend to isomorphism

$$(\mathcal{O}_{L,S}^\times \oplus \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R} \cong \prod_{v' \in \bar{S}} \mathbb{R}^+$$

So we can apply Proposition 12.2 for the following G-modules:

Let $A = (\mathcal{O}_{L,S}^\times \oplus \mathbb{Z})$. Then $h(A) = [L : K] h(\mathcal{O}_{L,S}^\times)$.

Let $B = \prod_{v \in \bar{S}} \mathbb{Z}$: can decompose as $B = \prod_{v \in S} B_v$, where $B_v = \prod_{v' | v} \mathbb{Z} \cong \mathrm{coInd}_{G_w}^G \mathbb{Z}$.

By Shapiro's lemma, the Herbrand quotient of the G-module $B_v = \mathrm{coInd}_{G_w}^{G} \mathbb{Z}$ is equal to the Herbrand quotient of the G_w-module $\mathbb{Z}$ (with trivial action), but we know that the latter is equal to $|G_w|$.

Hence $h(B) = \prod_v h(B_v) = \prod_{v \in S} |G_w| = \prod_{v \in S} [L_w : K_v]$.

Conclude that $h(A) = \prod_{v \in S} [L_w : K_v]$, and so $h(\mathcal{O}_{L,S}^{\times}) = \frac{\prod_{v \in S} [L_w : K_v]}{[L:K]}$.

Now can compute

$$h(C_L) = \frac{h(\mathbb{A}_{L,S}^{\times})}{h(\mathcal{O}_{K,S}^{\times})} = \frac{\prod_{v \in S} [L_w : K_v]}{\prod_{v \in S} [L_w : K_v] / [L : K]} = [L : K],$$

completing our proof of the first inequality.

We've now proved that $|\hat{H}^0(L/K, C_L)| \geq [L : K]$, that is, $|C_L / NC_K| \geq [L : K]$. Note $C_L / NC_K \cong \mathbb{A}_L^{\times} / L^{\times} N_{L/K} \mathbb{A}_K^{\times}$.

12.3 Corollaries of First Inequality

Corollary 12.3. *L/K finite abelian (or more generally solvable), $D \subset \mathbb{A}_K^{\times}$ with $D \subset N_{L/K} \mathbb{A}_L^{\times}$, $K^{\times} D$ is dense in $\mathbb{A}_K^{\times}$, then $L = K$.*

Proof. Without loss of generality we may assume L/K cyclic: otherwise replace L with $L' \subset L$ such that L'/K is cyclic.

The subgroup $N_{L/K} \mathbb{A}_L^{\times}$ is open in $\mathbb{A}_K^{\times}$, so $K^{\times} N_{L/K} \mathbb{A}_L^{\times}$ is an open subgroup of $\mathbb{A}_K^{\times}$. On the other hand, $K^{\times} N_{L/K} \mathbb{A}_L^{\times}$ contains $K^{\times} D$, so is also dense. Hence $\mathbb{A}_K^{\times} = K^{\times} N_{L/K} \mathbb{A}_L^{\times}$, so

$$|\hat{H}^0(L/K, C_L)| = 1$$

implying $L = K$ by first inequality. □

Corollary 12.4. *Let L/K be a finite abelian extension with $L \neq K$. Then there are infinitely many primes of K that do not split completely in L.*

Proof. We prove the contrapositive: suppose all but finitely many primes split completely in L

Let S contain the infinite primes and all the primes that don't split completely in L.

Let $D = \{x \mid x_v = 1 \text{ for all } v \in S\}$. Then D is contained in $N\mathbb{A}_L^{\times}$ by assumption, and $K^{\times} D$ is dense in $\mathbb{A}_K^{\times}$. (This is weak approximation: $K^{\times}$ is dense in $\prod_{v \in S} K_v^{\times}$.)

Applying the previous corollary, then get $L = K$.

□

Corollary 12.5. *If S is a finite set of places of K and L/K is finite abelian, then $\mathrm{Gal}(L/K)$ is generated by $\left(\frac{L/K}{v}\right) = \mathrm{Frob}_v \in \mathrm{Gal}(L/K)$ for $v \notin S$.*

Proof. (Wlog S contains all ramified and infinite primes.)

Let H be the subgroup of $\mathrm{Gal}(L/K)$ generated by $\{\mathrm{Frob}_v \mid v \notin S\}$.

Let M be the subfield of L fixed by H. Then all primes of K that do not lie above primes in S must split completely in M. By the contrapositive of previous corollary, must have $M = K$. By Galois correspondence, $H = \mathrm{Gal}(L/K)$. □

12.4 The Second Inequality

We'll next work towards proving

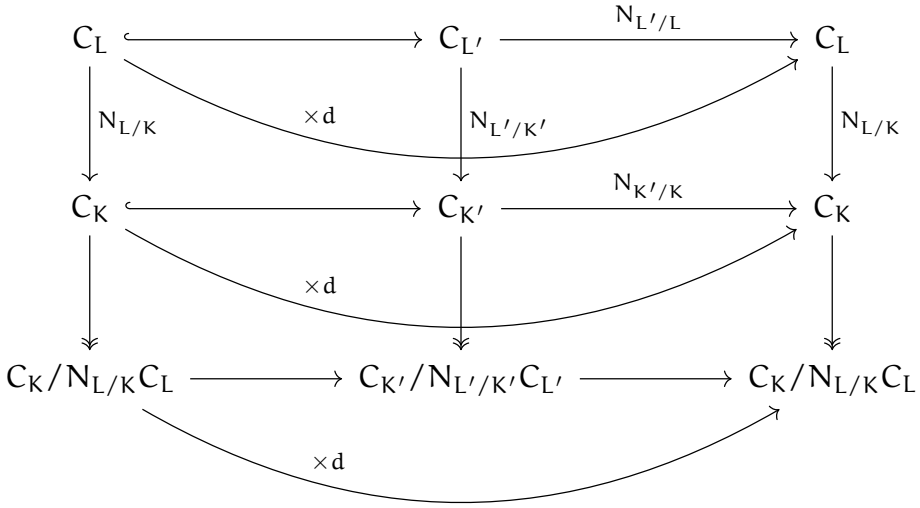
Theorem 12.6 (Second Inequality)**.** K *a number field,* L/K *cyclic of degree* p, $|\hat{H}^0(L/K, C_L)| = |C_L/N_{L/K}C_K| \leq p$

Claim: it's enough to show this when K contains the pth roots of unity.

Proof of Claim: Suppose L/K is any cyclic extension of global fields of degree p. let $K' = K(\zeta_p)$, $L' = L(\zeta_p) = LK'$.

Observe that the degree d of K'/K divides $p-1$, so K' and L are linearly disjoint, and $[L' : L] = d$ also.

We get a commutative diagram



Observe that C_K/NC_L is a group of exponent p relatively prime to d, so multiplication by d is an automorphism of C_K/NC_L. Looking at the bottom row, we see that the induced map $C_K/N_{L/K}C_L \to C_{K'}/N_{L'/K'}C_{L'}$ must be injective, and $C_{K'}/N_{L'/K'}C_{L'} \to C_K/N_{L/K}C_L$ must be surjective.

Hence $|C_K/N_{L/K}C_L| \leq |C'_K/N_{L'/K'}C'_L|$, and so it's enough to bound the size of the latter. □

13 March 15

13.1 Proof of Second Inequality, continued

Last time we showed we could assume K contains μ_p. By Kummer $L = K(\sqrt[n]{a})$ for some $a \in K^\times$.

Need to show that $[\mathbb{A}_K^\times : K^\times N\mathbb{A}_L^\times] \leq p$.

We'll actually show that $[\mathbb{A}_K^\times : K^\times F] \leq p$, where $F \subset N\mathbb{A}_L^\times$ is an appropriately chosen subgroup.

Let S be any finite set of places of K satisfying the following

(a) S contains all infinite places and all primes dividing p,

(b) S contains all v with $|a|_v \neq 1$. (so a is an S-unit)

(c) $\mathbb{A}_{K,S}^\times \to C_K$ is a surjection (we saw that we could do this last time)

Let $v_1, \ldots, v_k$ be additional places of K, to be chosen later, subject to the condition that each v_i splits completely in L. Choosing the v_i is the hardest part of the proof.

Let $S^* = S \cup \{v_1, \ldots, v_k\}$.

Now take

$$F = \prod_{v \in S} (K_v^\times)^p \prod_{i=1}^{k} K_{v_i} \prod_{v \notin S^*} \mathcal{O}_v^\times.$$

We check that $F \subset N\mathbb{A}_L^\times$: we know that we can do this locally.

For $v \in S$, $(K_v^\times)^p \subset N_{L_w/K_v} L_w^\times$ as $[L_w : K_v]$ divides p.

For each v_i, $L_{w_i} = K_{v_i}$ as v_i splits completely. So $N_{L_{w_i}/K_{v_i}} L_{w_i}^\times = K_{v_i}^\times$ as needed.

For $v \notin S^*$, we know that L_w/K_v is unramified, so $N_{L_w/K_v} L_w^\times$ includes $\mathcal{O}_v^\times$ as needed.

Lemma 13.1. *Let K be a global field, v a finite place of K such that K_v does not have residue characteristic p, and $b \in K^\times$. Then v is unramified in $K(\sqrt[p]{b})/K$ iff $b \in \mathcal{O}_v^\times \cdot (K_v)^p$, and v splits completely iff $b \in K_v^p$.*

Proof. exercise. □

Corollary: L/K is unramified outside S, as needed in the proof above that $F \subset N_{L/K}\mathbb{A}_L^\times$.

Now we break up $[\mathbb{A}_K^\times : K^\times F]$ into a local and global component.

Observe that $F \subset \mathbb{A}_{K,S^*}^\times$: since $\mathbb{A}_{K,S*}^\times$ surjects onto $\mathbb{A}_K^\times / K^\times$, we have that

$$\mathbb{A}_{K,S^*}^\times \twoheadrightarrow \mathbb{A}_K^\times / K^\times F$$

with kernel $\mathcal{O}_{K,S}^\times \cdot F$, so

$$\mathbb{A}_K^\times / K^\times F \cong \mathbb{A}_{K,S^*}^\times / \mathcal{O}_{K,S^*}^\times \cdot F$$

Now, have SES:

$$0 \to \mathcal{O}_{K,S^*}^\times \cdot F/F \to \mathbb{A}_{K,S^*}/F \to \mathbb{A}_{K,S^*}/\mathcal{O}_{K,S^*}^\times \cdot F \to 1$$

where the first term $\mathcal{O}_{K,S^*}^\times \cdot F/F \cong \mathcal{O}_{K,S^*}^\times/F \cap \mathcal{O}_{K,S^*}^\times$ by the second isomorphism theorem.

So

$$[\mathbb{A}_K^\times : K^\times F] = [\mathbb{A}_{K,S^*} : F]/[\mathcal{O}_{K,S^*} : F \cap \mathcal{O}_{K,S^*}^\times]. \tag{1}$$

and we just need to find $[\mathbb{A}_{K,S^*} : F]$ and $[\mathcal{O}_{K,S^*} : F \cap \mathcal{O}_{K,S^*}^\times]$.

The first one is a product of local factors:

$$[\mathbb{A}_{K,S^*} : F] = \prod_{v \in S} K_v^\times/(K_v^\times)^p$$

By HW: if K_v is a local field containing μ_p, then $K_v^\times/(K_v^\times)^p = p^2 \cdot |p|_v^{-1}$.

Hence $[\mathbb{A}_{K,S^*} : F] = \prod_{v\in S} p^2 \cdot \prod_{v\in S} |p|_v^{-1}$.

The second term vanishes by the product formula (using $|p|_v = 1$ for $v \notin S$), so.

$$[\mathbb{A}_{K,S^*} : F] = p^{2|S|}$$

For the global part, observe that $F \cap \mathcal{O}_{K,S^*}^\times$ contains $(\mathcal{O}_{K,S^*}^\times)^p$. So

$$[\mathcal{O}_{K,S^*} : F \cap \mathcal{O}_{K,S^*}^\times] = [\mathcal{O}_{K,S^*} : (\mathcal{O}_{K,S^*}^\times)^p]/[F \cap \mathcal{O}_{K,S^*}^\times : (\mathcal{O}_{K,S^*}^\times)^p]$$

$$[\mathcal{O}_{K,S^*} : (\mathcal{O}_{K,S^*}^\times)^p] = p^{|S^*|} = p^{|S|+k}$$

by Dirichlet's units theorem plus the fact that K contains μ_p.

So, plugging into equation 1, get

$$[A_K : K^\times F] = p^{|S|-k}[F \cap \mathcal{O}_{K,S^*}^\times : (\mathcal{O}_{K,S^*}^\times)^p]$$

We'll show we can choose places $v_1, \ldots, v_k$, split in L/K with $k = |S| - 1$ and $F \cap \mathcal{O}_{K,S^*}^\times = (\mathcal{O}_{K,S^*}^\times)^p$.

Proposition 13.2. *Suppose that $v_1, \ldots, v_k$ are places of K such that if $K(\sqrt[p]{b})$ is unramified outside S^* and completely split at all primes of S, then $b \in (K^\times)^p$. Then $F \cap \mathcal{O}_{K,S^*} = \mathcal{O}_{K,S^*}^p$.*

Proof. Proof: suppose $b \in F \cap \mathcal{O}_{K,S^*}$. Then by lemma 13.1, $K(\sqrt[p]{b})$ has the appropriate behavior, hence $b \in (K^\times)^p$, but since b is an S^*-unit, in fact $b \in \mathcal{O}_{K,S^*}^p$. □

Now it's enough to show we can choose $v_1, \ldots, v_k$ with $k = |S| - 1$ satisfying the conditions of Proposition and such that each v_i splits completely in L.

Let $T = K(\sqrt[p]{\mathcal{O}_{K,S}^\times})$. Then T/K is an extension of exponent p with

$$\mathrm{Gal}(T/K) \cong \mathrm{Hom}(\mathcal{O}_{K,S}/(\mathcal{O}_{K,S})^p, \mu_p) \cong (\mathbb{Z}/p)^{|S|}.$$

Note that $L = K(\sqrt[p]{a}) \subset T$, and $\mathrm{Gal}(T/L)$ is an extension of exponent p with $\mathrm{Gal}(T/L) \cong (\mathbb{Z}/p)^k$ where $k = |S| - 1$. Choose places $w_1, \ldots, w_k$ of L, not lying above any places of S, such that $\mathrm{Frob}_{w_1}, \ldots, \mathrm{Frob}_{w_k} \in \mathrm{Gal}(T/L)$ form a basis for $\mathrm{Gal}(T/L)$ as a $\mathbb{F}_p$-vector space: this here is where we are using the first inequality.

Let $v_1, \ldots, v_k$ be the places of K below $w_1, \ldots, w_k$.

We now look at their splitting behavior in L. Observe that the elements $\mathrm{Frob}_{w_i} \in \mathrm{Gal}(T/L)$ and $\mathrm{Frob}_{v_i} \in \mathrm{Gal}(T/K)$ are related by $\mathrm{Frob}_{w_i} = \mathrm{Frob}_{v_i}^{e_{w_i/v_i}}$ where $e = e_{w_i/v_i}$ is the inertia degree, which can be either 1 or p. But if $e = p$, then have $\mathrm{Frob}_{w_i} = 0$, contradicting that Frob_{w_i} generates, so $e = 1$ and v_i splits completely in L.

Choose one more place v_{k+1} so that $\mathrm{Frob}_{v_1}, \ldots, \mathrm{Frob}_{v_{k+1}}$ generate $\mathrm{Gal}(T/K)$.

Next, we show that

Lemma 13.3. *The natural map*

$$\phi : \mathcal{O}_{K,S}^\times / (\mathcal{O}_{K,S}^\times)^p \to \prod_{i=1}^{k+1} \mathcal{O}_{v_i}^\times / (\mathcal{O}_{v_i}^\times)^p$$

is bijective.

Proof. Injectivity is Kummer theory: Suppose $c \in \mathcal{O}_{K,S}^\times$, is such that $[c] \in \ker \phi$. Then consider the extension $K(\sqrt[p]{c}) \subset T$.

For each i, c is a pth power in $\mathcal{O}_{v_i}^\times$, so v splits completely in $K(\sqrt[p]{c})$, hence Frob_{v_i} fixes $K(\sqrt[p]{c})$ for $1 \leq i \leq k+1$. Since the Frob_{v_i} generate, we have $K(\sqrt[p]{c}) = K$, so c is a pth power and $[c] = 1$.

Surjectivity then follows by counting orders: RHS has order p^{k+1}, LHS has order $p^{|S|} = p^{k+1}$

□

Corollary 13.4. *The map*

$$\mathcal{O}_{K,S}^\times / (\mathcal{O}_{K,S}^\times)^p \to \prod_{i=1}^{k} \mathcal{O}_{v_i}^\times / (\mathcal{O}_{v_i}^\times)^p$$

is surjective.

Now we can show that the places v_i satisfy Proposition 13.1.

For this: Let $M = K(\sqrt[p]{b})$. Then let $D = \prod_{v \in S} K_v^\times \times \prod_{v_i} (K_{v_i})^p \times \prod_{v \notin S^*} \mathcal{O}_v^\times$. Then for the same reasons as previously, $D \subset N\mathbb{A}_M^\times$.

On the other hand, $DK^\times$ contains $D\mathcal{O}_{K,S}^\times$, which contains $\mathbb{A}_{K,S}^\times$ by the previous corollary. By assumption on S, $\mathbb{A}_K^\times = \mathbb{A}_{K,S}^\times K^\times$, so $DK^\times$ contains all of $\mathbb{A}_K$. By our corollary to the first inequality, $M = K$ as required.

(Vague discussion at the end of class about what is really going on with this proof, and the relationship between F and D. I think this is probably related to Tate duality: see the exercises on page 404 of Neukirch's Algebraic Number Theory for statements.)

14 March 25

14.1 What we know now

We proved last week that if L/K is a degree p cyclic extension of number fields, then $|\hat{H}^0(L/K, C_L)| = |H^2(L/K), C_L| = p$, and $|H^1(L/K, C_L)| = 1$.

By HW, this implies that $H^1(L/K, C_L) = 1$ for any Galois extension L/K, and also $|H^2(L/K), C_L| \leq [L : K]$.

Some consequences:

Corollary 14.1. *For any finite Galois extension L/K of number fields, the map $H^2(L/K, L^\times) \to \bigoplus_v H^2(L_w/K_v, L_w^\times)$ is injective.*

Proof. Use short exact sequence $0 \to L^\times \to \mathbb{A}_L^\times \to C_L \to 0$. □

Corollary 14.2 (Hasse Norm Theorem)**.** *If L/K is a cyclic extension and $a \in K^\times$, then $a \in NL_w^\times$ for all primes w of $L^\times$ implies $a \in NL^\times$.*

Proof. This is just the statement that $\hat{H}^0(L/K, L^\times) \to \prod_w \hat{H}^0(L_w/K_v, L_w^\times)$ is injective, but $\hat{H}^0 \cong H^2$ by periodicity. □

Note that the statement that L/K is cyclic is critical here: there are counterexamples without, e.g. $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, e.g. $a = 5^2$. (However can show that the subgroup of global norms is still finite index in the local norms, that is, $|K^\times \cap N\mathbb{A}_L^\times / NL^\times| < \infty$.)

14.2 Towards a global invariant map

We want to show that $C_{\bar{K}}$ is a class formation. What we have so far shows that it is a field formation, but we still need the invariant map $H^2(L/K, C_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

We can easily define a closely related map $\mathrm{inv}_{L/K} : H^2(L/K, \mathbb{A}_L^\times) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ by $\mathrm{inv}_{L/K}(c) = \sum_v \mathrm{inv}_{L_w/K_v} c$. We want to make a map $\mathrm{inv} : H^2(L/K, C_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ that completes the commutative triangle. However we have the issue that the induced map $H^2(L/K, \mathbb{A}_L^\times) \to H^2(L/K, C_L)$ is neither injective or surjective. To deal with the failure of injectivity we need to prove a reciprocity law.

14.3 Reciprocity Laws

Let L/K be a finite extension of number fields. We're going to work towards proving the following reciprocity laws:

(a) inv-reciprocity: for L/K if $\alpha \in H^2(L/K, L^\times)$ then $\sum_v \mathrm{inv}_v \alpha = 0$ in $\mathbb{Q}/\mathbb{Z}$.

(b) θ-reciprocity: for L/K if $\alpha \in K^\times$ then $\prod_v \theta_{L_w/K_v} \alpha = 1$ in $\mathrm{Gal}(L/K)^{ab}$.

We want these to hold for all L/K. This week we'll prove inv-reciprocity and θ-reciprocity for all L/K.

Before this, we need some technical lemmas which will let us reduce to the case of cyclotomic extensions.

Remember from our discussion of Brauer Groups + HW:

Proposition 14.3. *If K is a number field, and $\alpha \in \mathrm{Br}(K) = H^2(K, \bar{K}^\times)$, there exists some cyclic cyclotomic extension L/K such that $\mathrm{Res}\,\alpha = 0 \in \mathrm{Br}(L)$, or equivalently, such that α lies in the image of the inflation map $H^2(L/K, L^\times) \to \mathrm{Br}(K)$.*

(In terms of central simple algebras: α is split by L)

Compatibilities between the maps $\mathrm{inv}_{L/K} : H^2(L/K, \mathbb{A}_L^\times) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$:

$$\mathrm{inv}_{N/K}(\inf c) = \mathrm{inv}_{L/K}(c)$$

when $N/L/K$ is a tower with N/K and L/K Galois, and

$$\mathrm{inv}_{N/L}(\mathrm{Res}_{L/K} c) = [L : K]\,\mathrm{inv}_{N/K}(c)$$

$$\mathrm{inv}_{N/L}(\mathrm{Cor}\, c) = \mathrm{inv}_{N/K}(c)$$

when $N/L/K$ is a tower with N/K Galois (so also N/L)

In other words, we almost have a class formation, except that $\mathrm{inv}_{L/K}$ is not an isomorphism: in general it's neither injective nor surjective.

We check

$$\mathrm{inv}_{N/L}(\mathrm{Res}_{L/K} c) = [L : K]\,\mathrm{inv}_{N/K}(c)$$

which is the hardest of these. Indeed:

$$\begin{aligned}
\mathrm{inv}_{N/L}(\mathrm{Res}_{L/K} c) &= \sum_w \mathrm{inv}_{N_{w'}/L_w}(\mathrm{Res}_{L_w/K_v} c) \\
&= \sum_w [L_w : K_v]\,\mathrm{inv}_{N_{w'}/K_v} c \\
&= \sum_v \sum_{w|v} [L_w : K_v]\,\mathrm{inv}_{N_{w'}/K_v} c \\
&= [L : K]\,\mathrm{inv}_{N/K}(c).
\end{aligned}$$

Let's also define $\theta_{L/K} : \mathbb{A}_K^\times \to \mathrm{Gal}(L/K)^{ab}$ by $\theta_{L/K}(a) = \prod_v \theta_{L_w/K_v} a_v$. That is, θ-reciprocity is the statement that $K^\times \subset \ker\theta$.

These maps are related by

Proposition 14.4. $\chi(\theta_{L/K}(a)) = \mathrm{inv}_{L/K}([a] \cup \delta\chi)$.

for any $\chi \in \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \cong H^1(L/K, \mathbb{Q}/\mathbb{Z})$, and $a \in \mathbb{A}_K^\times$.

Proof. Follows from the same statement for local θ and inv, which we proved last semester. $\square$

For any L/K, inv-reciprocity implies θ-reciprocity.

Observe that θ-reciprocity implies inv-reciprocity if L/K cyclic. Indeed choose χ to generate $H^1(L/K, \mathbb{Q}/\mathbb{Z})$, so $\delta\chi$ generates $H^2(L/K, \mathbb{Z})$. For any $[a] \in \hat{H}^0(L/K, L^\times)$ we have, $0 = \chi(\theta_{L/K}(a)) = \mathrm{inv}_{L/K}([a] \cup \delta\chi)$. But $- \cup \delta\chi$ is an isomorphism $\hat{H}^0(L/K, L^\times) \to H^2(L/K, L^\times)$, so $\mathrm{inv}_{L/K}$ is 0 on all of $H^2(L/K, L^\times)$.

14.4 Checking reciprocity laws

We start out by checking θ-reciprocity for $K = \mathbb{Q}$ and L a cyclotomic extension: note that for us this will mean that L is any subfield of $\mathbb{Q}(\zeta_n)$: but it's enough to check when $L = \mathbb{Q}(\zeta_n)$.

In fact, it's enough to check when $L = \mathbb{Q}(\zeta_{\ell^r})$, since any cyclotomic extension is a compositum of such.

We just need to check θ-reciprocity for a generating set of $\mathbb{Q}^\times$: we check it for $a = \ell$, $a = p \neq \ell$, and $a = -1$.

$a = p \neq \ell$

- $\theta_\ell(p)$ sends $\zeta \mapsto \zeta^{p^{-1}}$ (Lubin-tate)
- $\theta_p(p) = \mathrm{Frob}_p$ (unramified theory) which sends $\zeta \mapsto \zeta^p$
- $\theta_{p'}(p) = 1$ (unramified)
- $\theta_\infty(p) = 1$

$a = \ell$

- $\theta_\ell(\ell) = 1$ (Lubin-Tate)
- $\theta_{p'}(\ell) = 1$ (unramified theory) when $p' \neq \ell$
- $\theta_\infty(\ell) = 1$

$a = -1$

- $\theta_{p'}(-1) = 1$ all $p' \neq \ell$
- $\theta_\ell(-1)$ sends $\zeta \mapsto \zeta^{-1}$ (Lubin-Tate)
- $\theta_\infty(-1)$ is complex conjugation.

So everything checks out and θ-reciprocity holds for $L/\mathbb{Q}$ cyclotomic. It follows that inv-reciprocity holds for $L/\mathbb{Q}$ cyclic cyclotomic.

15 March 29

15.1 Checking reciprocity laws, continued

Recall we have two statements of reciprocity:

(a) inv-reciprocity for L/K : if $\alpha \in H^2(L/K, L^\times)$ then $\operatorname{inv} \alpha = \sum_v \operatorname{inv}_v \alpha = 0$ in $\mathbb{Q}/\mathbb{Z}$.

(b) θ-reciprocity for L/K : if $\alpha \in K^\times$ then $\theta(\alpha) = \prod_v \theta_{L_w/K_v} \alpha = 1$ in $\operatorname{Gal}(L/K)^{ab}$.

We know that inv-reciprocity implies θ-reciprocity, but only get the converse when L/K cyclic.

We explicitly checked θ-reciprocity for $L/\mathbb{Q}$ cyclotomic. Hence inv-reciprocity also holds for $L/\mathbb{Q}$ cyclic cyclotomic.

However, last time we showed that any element of $\operatorname{Br}(\mathbb{Q})$ is represented by some $H^2(L/\mathbb{Q}, L^\times)$ where L is cyclic cyclotomic. It follows from compatibility with inflation that inv-reciprocity holds for $K = \mathbb{Q}$, L arbitrary.

Now, suppose that K and L are arbitrary. Let $E/\mathbb{Q}$ be a Galois extension with $L \subset E$. Then have $H^2(L/K, L^\times) \xrightarrow{\inf} H^2(E/K, E^\times) \xrightarrow{\text{Cor}} H^2(E/Q, \mathbb{Q}^\times)$, and both maps are compatible with inv, so inv-reciprocity holds for arbitrary L/K. Hence also θ-reciprocity holds.

Observe: now we have a map $\theta : \mathbb{A}_K^\times / K^\times N\mathbb{A}_L^\times \to \operatorname{Gal}(L/K)^{ab}$. One route would be to stop here and show that this map is an isomorphism, but instead we'll push on and work on showing that the ideles form a class formation, which will automatically give us everything.

15.2 The inv map for cyclic extensions.

We now look at the case when L/K is cyclic. In this case we'll see that the map inv : $H^2(L/K, \mathbb{A}_L^\times) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ induces a unique isomorphism inv : $H^2(L/K, C_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

Proposition 15.1.

$$1 \to H^2(L/K, L^\times) \xrightarrow{i_*} H^2(L/K, \mathbb{A}_L^\times) \xrightarrow{\text{inv}} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \to 0$$

is exact when L/K *is cyclic.*

Proof. Surjectivity: need to show that $[L : K]$ is the least common multiple of the local degrees $[L_w : K_v]$. This follows from the fact that elements Frob_v, of order $[L_w : K_v]$ generate the cyclic group $\operatorname{Gal}(L/K)$ of order $[L : K]$.

$\ker \text{inv} = \operatorname{im} i_*$: We already have $\ker \text{inv} \supset \operatorname{im} i_*$. To get equality, we count orders, and compare with the following exact sequence:

$$1 \to H^2(L/K, L^\times) \to H^2(L/K, \mathbb{A}_L^\times) \xrightarrow{j_*} H^2(L/K, C_L) \xrightarrow{\delta} H^3(L/K, K^\times) = 1$$

where the final term is 1 by Hilbert 90 and periodicity of cohomology for cyclic groups.

Surjectivity of inv tells us that the index of $\ker \mathrm{inv}$ in $H^2(L/K, \mathbb{A}_L^\times)$ is precisely $[L : K]$.

On the other hand, the cohomology exact sequence tells us that index of $\mathrm{im}\, i_*$ in $H^2(L/K, \mathbb{A}_L^\times)$ is equal to $|H^2(L/K, C_L)|$, which is at most $[L : K]$ by the second inequality.

Since we know already $\ker \mathrm{inv} \supset \mathrm{im}\, i_*$, the index of the former in $H^2(L/K, \mathbb{A}_L^\times)$ is at most that of the latter: comparing with the previous two observations, equality must hold and $\ker \mathrm{inv} = \mathrm{im}\, i_*$ (and both have index $[L : K]$ in $H^2(L/K, \mathbb{A}_L^\times)$. □

It follows from the previous proof that if L/K is cyclic, the invariant map $\mathrm{inv} : H^2(L/K, \mathbb{A}_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ factors through $H^2(L/K, C_L)$. Then the induced map, which we denote by

$$\mathrm{inv} : H^2(L/K, C_L) \to \frac{1}{[L : K]}\mathbb{Z}/\mathbb{Z},$$

is an isomorphism.

Unfortunately this approach doesn't work to define $\mathrm{inv} : H^2(L/K, C_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ when L is not cyclic. We'll have to do the same thing we did last semester, which is to diagram-chase to move inv from the extensions we understand to the ones we don't.

We'll need to show the following lemma:

Lemma 15.2. *L/K any Galois extension, L'/K cyclic with $[L' : K] = [L : K]$, then $H^2(L/K, C_L)$ and $H^2(L'/K, C_L)$ have same image inside $H^2(\bar{K}/K, C_{\bar{K}}) = \bigcup_M H^2(M/K, C_M)$.*

Proof. For brevity let $H^2(L/K)$ denote $H^2(L/K, C_L)$.

To show $\inf H^2(L'/K) \subset \inf H^2(L/K)$: let $N = LL'$, so N/L is cyclic with $[N : L] \mid [L' : K]$.

There's a left exact sequence: $1 \to H^2(L/K) \to H^2(N/K) \to H^2(N/L)$.

Suppose $c \in H^2(L'/K)$. Then lift c to $\tilde{c} \in H^2(L'/K, \mathbb{A}_L^\times)$.

We need to show that $\mathrm{Res}_{L/K} \inf_{N/L'} c = 0$ inside $H^2(N/L)$: for this enough to check that it has invariant 0.

$$\begin{aligned}
\mathrm{inv}_{N/L}(\mathrm{Res}_{L/K} \inf_{N/L'} c) &= \mathrm{inv}_{N/L}(\mathrm{Res}_{L/K} \inf_{N/L'} j_*(\tilde{c})) \\
&= \mathrm{inv}_{N/L}\, j_*(\mathrm{Res}_{L/K} \inf_{N/L'}(\tilde{c})) \\
&= \mathrm{inv}_{N/L}(\mathrm{Res}_{L/K} \inf_{N/L'}(\tilde{c})) \\
&= [L : K]\, \mathrm{inv}_{L'/K}(\tilde{c}) \\
&= 0.
\end{aligned}$$

for equality, compare orders and use second inequality.

□

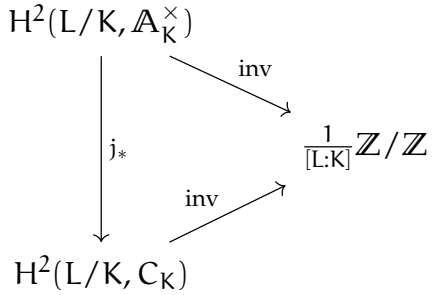
The maps $\mathrm{inv} : H^2(L'/K) \to \frac{1}{[L':K]}\mathbb{Z}/\mathbb{Z}$ for L'/K cyclic glue to give an isomorphism

$$\mathrm{inv}_{/K} : H^2(\bar{K}/K) = \lim_{L/K \text{ Galois}} H^2(L/K) = \lim_{L/K \text{ cyclic}} H^2(L/K) \to \mathbb{Q}/\mathbb{Z}.$$

By the previous lemma, this restricts to an isomorphism $\mathrm{inv}_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

We define the fundamental class $u_{L/K} \in H^2(L/K)$ by $\mathrm{inv}(u_{L/K}) = \frac{1}{[L:K]}$

Observe that the following diagram commutes



Now we know that C_K is a class formation. (Really we need to check that inv is compatible with inflation and restriction, but that's straightforward.) By Tate's theorem $\cup u_{L/K} : \hat{H}^i(L/K, \mathbb{Z}) \to \hat{H}^{i+2}(L/K, C_K)$ is an isomorphism.

In particular, for $i = -2$, we get an isomorphism $\mathrm{Gal}(L/K)^{ab} \to C_K/NC_L$.

Let $\theta_{L/K}$ be the inverse of this isomorphism. The cup product is compatible with inflation, restriction, corestriction, conjugation, so $\theta_{L/K}$ is also.

The argument we did last semester for $\chi(\theta_{L/K}(a)) = \mathrm{inv}(a \cup \delta\chi)$ works equally well in any class formation, and this property determines θ.

To check that $\theta_{L/K} : C_K/NC_L \to \mathrm{Gal}(L/K)^{ab}$ is given by $\theta([a]) = \prod_v \theta_v a_v$, let $\theta'([a]) = \prod_v \theta_v a_v$, and we check $\chi(\theta'(a)) = \mathrm{inv}(a \cup \delta\chi)$: but we've previously observed this (using the inv map from $H^2(L/K, \mathbb{A}_K^\times)$, but we've seen that the two different inv maps are compatible).

Proposition 15.3. *$\theta_{L/K}$ is continuous using the adelic topology on C_K and the discrete topology on $\mathrm{Gal}(L/K)^{ab}$*

Proof. This is equivalent to showing that $\ker \theta_{L/K} = N_{L/K}C_L$ is open in C_K, which we've already seen.

Alternatively, use formula for $\theta_{L/K}$ as a product of local factors and show continuity directly. □

16 April 1

16.1 Existence

We observed at the end of last time that $\theta_{L/K} : C_K \to \mathrm{Gal}(L/K)$ is continuous.

Taking the direct limit over all finite Galois L/K, we observe that $\theta_{/K} : C_K \to \mathrm{Gal}(\bar{K}/K)$ is also continuous.

The kernel of $\theta_{/K}$ is the intersection of all normic subgroups of C_K. Where, analogously to last semester, $A \subset C_K$ is normic if $A = NC_L$ for some L/K finite Galois. We now need to prove

Theorem 16.1 (Existence Theorem)**.** *The normic subgroups of C_K are exactly the finite index open subgroups.*

We've already shown that normic subgroups are open and finite index: the hard part is the other direction.

16.2 Basic facts about normic extensions

In the local field context, we proved a bunch of theorems about basic properties of normic subgroups, and these results carry over automatically.

Basic facts of normic subgroups move over: normic subgroups correspond 1-1 to finite abelian extensions of K, and if A corresponds to L then $[C_K : A] = [L : K]$.

A and B normic implies $A \cap B$ normic,

A normic implies $A' \supset A$ normic.

We'll show that any finite index open subgroup of C_K is normic.

For any finite set S of primes of K, let U_S be the image of $\prod_{v\in S} 1 \times \prod_{v\notin S} \mathcal{O}_v^\times$ in C_K.

Any open subgroup of finite index in C_K must contain $(C_K)^n U_S$ for some n and S.

Theorem 16.2. *Let K be a number field, and S is a finite set of primes of K such that*

- *S contains the infinite primes and primes dividing n*
- *$\mathbb{A}_{K,S}^\times$ surjects onto C_K.*

If K contains μ_n then $(C_K)^n U_S$ is the norm group of $T = K(\sqrt[n]{(\mathcal{O}_{K,S}^\times)})/K$.

If K does not contain μ_n then $(C_K)^n U_S$ is still normic.

(The motivation for this choice of field is that the fixed field of $\theta_{/K}((C_K)^n U_S)$ is the maximal exponent n extension of K unramified outside K. We know how to find this by Kummer theory.)

Proof. This is going to be a lot like our proof of the second inequality. First we observe that

$$\mathrm{Gal}(T/K) \cong \mathrm{Hom}(\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n, \mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^{|S|}$$

One consequence is that $(C_K)^n$ is in the kernel of $\theta_{T/K}$, and so $(C_K)^n \subset N_{T/K}C_T$.

Also T is unramified outside S, so $\prod_{v\in S} 1 \times \prod_{v\notin S} \mathcal{O}_v^\times \subset N_{T/K}\mathbb{A}_T^\times$.

This gives one inclusion $(C_K)^n U_S \subset NC_T$.

To get the other inclusion, we show that $|C_K/(C_K)^n U_S| = |C_K/NC_T|$. First $|C_K/NC_T| = |\mathrm{Gal}(T/K)|$ which is $n^{|S|}$ by our previous computation of $\mathrm{Gal}(T/K)$.

It will take more work to compute $|C_K/(C_K)^n U_S|$.

We use our assumption that $\mathbb{A}_{K,S}$ surjects onto C_K. Since

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

we also have that $\prod_{v\in S} K_v^\times$ surjects onto C_K/U_S, and there is a short exact sequence

$$1 \to \mathcal{O}_{K,S}^\times \to \prod_{v\in S} K_v^\times \to C_K/U_S \to 1.$$

Quotienting out by nth powers (or equivalently tensoring with $\mathbb{Z}/n\mathbb{Z}$) , we get a right exact sequence

$$\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n \to \prod_{v\in S}(K_v^\times)/(K_v^\times)^n \to C_K/(C_K)^n U_S \to 1 \tag{2}$$

We can calculate the orders of everything here:

We already know that $|\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n| = n^{|S|}$.

For each n, $(K_v^\times)/(K_v^\times)^n$ has order $n^2|n|_v^{-1}$ (We've seen this for n prime: exercise to extend this to all n).

Multiplying together and using the product formula, we see that $\prod_{v\in S}(K_v^\times)/(K_v^\times)^n$ has order $n^{2|S|}\prod_{v\in S}|n|_v^{-1} = n^{2|S|}$.

If we show that $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n$ injects into $\prod_v K_v^\times/(K_v^\times)^n$, it will follow from (2) that

$$|C_K/(C_K)^n U_S| = p^{|N|} = |\mathrm{Gal}(T/K)| = |C_K/NC_T|$$

and thus we must have $(C_K)^N U_S = C_T$.

Again, we use Kummer theory: if $[a]$ is in the kernel of the map

$$\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n \to \prod_v K_v^\times/(K_v^\times)^n,$$

then $L = K(\sqrt[n]{a})$ is unramified outside S and totally split everywhere in S, meaning that $\mathbb{A}_{K,S} \subset N\mathbb{A}_L^\times$, and so $C_K = NC_L$ and $K = L = K(\sqrt[n]{a})$. It follows that $a \in (\mathcal{O}_{K,S}^\times)^n$.

That proves the theorem when K contains the nth roots of unity.

For the part when K does not contain nth roots of unity, we do the same thing we did for local fields.

let $K' = K(\mu_n)$, S' the set of primes above S, then exists L'/K' such that $(C_{K'})^n U_{S'} = N_{L'/K'}C_{L'}$. Extend L' to L/K Galois.

Then $N_{L/K}C_L \subset N_{K'/K}N_{L'/K'}(C_L') = N_{K'/K}(C_{K'})^n U_{S'} \subset (C_K)^n U_S$, so $(C_K)^n U_S$ contains a normic subgroup, and is itself normic. □

16.3 Dirichlet L-functions + generalizations

Dirichlet L-functions: Let K be a number field and let $\mathfrak{m}$ be a modulus of $\mathcal{O}_K$. Then a Dirichlet character χ of modulus $\mathfrak{m}$ is a homomorphism $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K) \to S^1$, and the associated Dirichlet L-function is

$$L(s,\chi) = \sum_{(\mathfrak{a},\mathfrak{m})=1} \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s} = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}}$$

where here $N\mathfrak{p}$ is the absolute norm $N\mathfrak{p} = \#(\mathcal{O}_K/\mathfrak{p})$.

Example: $K = \mathbb{Q}$, $\mathfrak{m} = m\infty$, χ is a character $\mathbb{Z}/m\mathbb{Z}^\times \to S^1$.

We'll be spending this section of the class studying Dirichlet L-functions, but before doing that I want to briefly mention a couple generalizations.

Hecke L-functions : instead of taking a character $\mathrm{Cl}_{\mathfrak{m}} \cong C_K/C_K^{\mathfrak{m}} \to S^1$, use an arbitrary continuous homomorphism $\psi : C_K \to S^1$, which can now be surjective rather than having finite image. The Hecke L-function of ψ is

$$\prod_{\mathfrak{p}\notin S} \frac{1}{1-\psi(\pi_{\mathfrak{p}})N\mathfrak{p}^{-s}}.$$

Here $\pi_{\mathfrak{p}} \in C_K$ is the element represented by the idele which is a uniformizer $\pi_{\mathfrak{p}}$ in the $\mathfrak{p}$-component, and 1 everywhere else. This factor is well-defined independent of $\pi_{\mathfrak{p}}$ provided that ψ is constant on the image of $\mathcal{O}_{\mathfrak{p}}^\times$. By continuity, this is the case for all but a finite set S of primes, which are referred to as the "ramified" primes and are excluded from the Euler product.

While Dirichlet L-functions are can be used to show e.g. Dirichlet's theorem that the residues of primes of $\mathbb{Z}$, are equidistributed in $\mathbb{Z}/m\mathbb{Z}^\times$, Hecke L-functions can be used to show that the arguments of prime ideals of $\mathbb{Z}[i]$ are equidistributed. More precisely, any prime ideal of $\mathbb{Z}[i]$ can be written as (π) for a unique π in the upper right-hand quadrant, and the arguments of those generators π are equidistributed in the interval $[0, \pi/2]$.

Artin L-functions: Recall that $C_{\mathfrak{m}} \cong \mathrm{Gal}(L_{\mathfrak{m}}/K)$ is the Galois group of the ray class field of modulus $\mathfrak{m}$. Hence we can view Dirichlet L-functions as being of the form

$$\prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathrm{Frob}_{\mathfrak{p}})N\mathfrak{p}^{-s}} \tag{3}$$

where now χ is a character $\mathrm{Gal}(L_{\mathfrak{m}}/K) \to S^1$, and $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L_{\mathfrak{m}}/K)$.

If now we replace $L_{\mathfrak{m}}$ by an arbitrary, possibly non-abelian, Galois extension L/K, then (3) still describes an L-function. Of course, if χ is just a homomorphism $\mathrm{Gal}(L/K) \to S^1$ then χ factors through the Galois group of the maximal abelian subextension and we get nothing new. However if we expand our notion of character to include characters of

irreducible representations of $\mathrm{Gal}(L/K)$, of any dimension, then we get a larger class of L-functions knows an *Artin* L*-functions* which play an important role in modern number theory.

17 April 5

17.1 Convergence results for general Dirichlet Series

(The reference for this part of the class is Milne's notes. In general we'll just sketch the proofs of the analytic results, but Milne proves things in more detail.)

Given a Dirichlet series $\sum \frac{a_n}{n^s}$, we now consider its domain of convergence.

As long as a_n is $O(n^b)$ for some b, the Dirichlet series will converge locally uniformly and absolutely to an analytic function in the half-plane $\mathrm{Re}\, s > b+1$. For the Riemann zeta function, this is the best we can do as $\zeta(s) \to \infty$ as $s \to 1$. However, can sometimes extend further: e.g. the Dirichlet L-function of a non-trivial Dirichlet character converges locally uniformly (but not absolutely) for $\mathrm{Re}\, s > 1$.

Proposition 17.1. *Let* $S(x) = \sum_{n \le x} a_s$ *be the sequence of partial sums. If* $S(x) = O(x^b)$*, then* $\sum \frac{a_n}{n^s}$ *converges locally uniformly to an holomorphic function in the half plane* $\mathrm{Re}\, s > b$*.*

Proof. (Non-rigorous Sketch, see pg 181 of Milne's Class Field Theory for a full proof).

Partial summation: rewrite the sum as

$$\sum_n S(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)$$

Then we can approximate the finite difference

$$\frac{1}{n^s} - \frac{1}{(n+1)^s}$$

by the derivative

$$\left(\frac{d}{dx} - x^{-s}\right)|_{x=n} = s n^{-s-1}$$

. Hence $S(n)(\frac{1}{n^s} - \frac{1}{(n+1)^s})$ is $O(n^{b-s-1}) = O(n^{b-\mathrm{Re}\, s-1})$, so the series converges locally uniformly for $\mathrm{Re}\, s > b$. □

Proposition 17.2. *Can meromorphically continue* $\zeta(s)$ *to the strip* $\mathrm{Re}\, s > 0$*, with at most a pole at* $s = 1$*.*

Proof. We can't apply the previous proposition to $\zeta(s)$ because it's not holomorphic at $s = 1$, so we multiply it by a factor to kill the pole, and consider

$$\zeta_2(s) = \zeta(s)(1 - 2^{1-s}) = \frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} \cdots$$

The Dirichlet series for $\zeta_2(s)$ is holomorphic for $\operatorname{Re} s > 0$ by the previous proposition. Hence we can meromorphically extend $\zeta(s)$ to $\operatorname{Re} s > 0$ by $\zeta(s) = \frac{\zeta_2(s)}{1-2^{1-s}}$. This tells us that $\zeta(s)$ is holomorphic everywhere in the region except possibly at $s = 1 + k\frac{2\pi i}{\log 2}$ for $k \in \mathbb{Z}$: this is not quite good enough, since we want $\zeta(s)$ holomorphic everywhere but $s = 1$.

So we do the same thing again with 3 in place of 2: let

$$\zeta_3(s) = \zeta_s(1 - 3^{1-s}) = \frac{1}{1^s} + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \cdots$$

The same argument as before tells us that $\zeta(s)$ is holomorphic at all points of $\operatorname{Re} s > 0$ except possibly $1 + k\frac{2\pi i}{\log 3}$ for $k \in \mathbb{Z}$. Since $\frac{\log 2}{\log 3} \notin \mathbb{Q}$, combining this our previous result tells us that $\zeta(s)$ is holomorphic everywhere in $\operatorname{Re} s > 0$ excepting $s = 1$, where it may have a pole.

□

Lemma 17.3. *For s real and $s > 1$, $\zeta(s) \in [\frac{1}{s-1}, 1 + \frac{1}{s-1}]$, so the Riemann zeta function has a simple pole at $s = 1$ with residue 1.*

Proof. Consider upper and lower Riemann sums for $\int_1^\infty x^{-s} = \frac{1}{s-1}$. □

Proposition 17.4. *if $S(n) - a_0 n \leq Cn^b$, $\sum \frac{a_n}{n^s}$ can be analytically continued to a meromorphic function on $\Re(s) > b$ with a simple pole at $s = 1$ with residue a_0.*

Proof. Use

$$\sum \frac{a_n}{n^s} = a_0\zeta_n(s) + \sum \frac{a_n - a_0}{n^s}.$$

□

17.2 Behavior of partial ζ-functions and Dirichlet L-functions

Now want to understand the behavior of Dirichlet L-functions.

Let $\mathfrak{m}$ be a modulus of K, and let $\mathfrak{K}$ be a class in $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$. Then we can define the partial zeta function:

$$\zeta(s, \mathfrak{K}) = \sum_{\mathfrak{a} \in \mathfrak{K}} \frac{1}{N\mathfrak{a}^s}.$$

This not an L function (no Euler product), but the partial zeta functions of modulus $\mathfrak{m}$ have the same linear span as the Dirichlet L-functions of modulus $\mathfrak{m}$.

To apply Prop 17.4 we'll need to get bounds on

$$S(x, \mathfrak{K}) = \#\{\text{ ideals } \mathfrak{a} \in \mathfrak{K} \mid N\mathfrak{a} \leq x\}$$

The relevant bounds are the following, whose proof we'll only sketch

Proposition 17.5.

$$S(x, \mathfrak{K}) = g_{\mathfrak{m}} x + O(x^{1-1/d})$$

where

$$g_{\mathfrak{m}} = \frac{2^r (2\pi)^s \operatorname{reg}(\mathfrak{m})}{w_{\mathfrak{m}} N\mathfrak{m} |\operatorname{Disc}(K)|^{1/2}}$$

In particular, it doesn't depend on $\mathfrak{K}$.

We haven't defined all the notation in the definition of $g_{\mathfrak{m}}$, so let's do that now. As usual, r is the number of real places of K and s the number of complex places.

The norm $N\mathfrak{m}$ is equal to $N(\mathfrak{m}_{\text{fin}})2^{r_{\mathfrak{m}}}$ where $\mathfrak{m}_{\text{fin}}$ is the finite part of $\mathfrak{m}$ and $r_{\mathfrak{m}}$ is the number of real places of $\mathfrak{m}$. *(I forgot the $2^{r_{\mathfrak{m}}}$ in class!)*

The last two factors $\operatorname{reg}(\mathfrak{m})$ and $w_{\mathfrak{m}}$ both involve the unit group

$$\mathcal{O}_{K,\mathfrak{m}}^{\times} = \{a \in \mathcal{O}_K^{\times} \mid a \equiv 1 \pmod{\mathfrak{m}} \text{ and } |a|_v > 0 \text{for all real } v \mid \mathfrak{m}\}.$$

First of all, $w_{\mathfrak{m}}$ is the number of roots of unity in $\mathcal{O}_{K,\mathfrak{m}}^{\times}$.

Then $\operatorname{reg}(\mathfrak{m})$ = regulator of $\mathfrak{m}$: recall we have a map $\mathcal{L} = \mathcal{O}_K^{\times} \hookrightarrow \prod_{v|\infty} \mathbb{R}^+$ given by $a \mapsto |\log a_{v_1}, \cdots \log a_{v_{r+s}}|$: in fact the image is a lattice inside a hyperplane H. The regulator $\operatorname{reg}(\mathfrak{m})$ is the covolume of $\mathcal{L}(\mathcal{O}_{K,\mathfrak{m}}^{\times})$ inside H.

If $\mathfrak{m} = 1$, we write $\operatorname{reg}(\mathfrak{m}) = \operatorname{reg}(\mathcal{O}_K)$, and this is called the *regulator* of $\mathcal{O}_K$.

In the case where K is a real quadratic field then $\operatorname{reg}(\mathfrak{m}) = \log |u|$ where $u \in K \subset \mathbb{R}^{\times}$, $u > 0$ is a generator for $\mathcal{O}_{K,\mathfrak{m}}^{\times}$ with $|u| > 1$.

We won't give a full proof of Proposition 17.5, but some comments:

To count

$$S(x, \mathfrak{K}) = \#\{\text{ ideals } \mathfrak{a} \in \mathfrak{K} \mid N\mathfrak{a} \leq x\},$$

choose any representative $\mathfrak{c} \in \mathfrak{K}$. Then any $\mathfrak{a} \in \mathfrak{K}$ is of the form $\mathfrak{a} = a\mathfrak{c}$ where $a \in \mathfrak{c}^{-1}$ and $a \equiv 1 \pmod{\mathfrak{m}}$, and a is uniquely defined up to multiplication by elements of $\mathcal{O}_{K,\mathfrak{m}}^{\times}$.

In class we sketched out how this count works when K is imaginary quadratic or real quadratic.

If K is imaginary quadratic: for simplicity assume that $w_{\mathfrak{m}} = 1$, so $\mathcal{O}_{K,\mathfrak{m}}^{\times}$ is trivial. Then the region of allowable a is the intersection of the disc $|Na| < \frac{x}{|N\mathfrak{c}|}$ with the lattice $\{a \in \mathfrak{c}^{-1} \mid a \equiv 1 \pmod{\mathfrak{m}}\}$, so can use geometry of numbers to count the number of lattice points in a region.

Now let K be real quadratic (and again we'll assume $w_{\mathfrak{m}} = 1$ for simplicity). Then $\mathcal{O}_K$ embeds as a lattice inside $\mathbb{R} \times \mathbb{R}$, of which $\{a \in \mathfrak{c}^{-1} \mid a \equiv 1 \pmod{\mathfrak{m}}\}$ is a sublattice. In this case the set

$$\{a \in \mathbb{R} \times \mathbb{R} \mid |Na| < \frac{x}{|N\mathfrak{c}|}\}$$

is a region bounded by hyperbolas, having infinite volume, and containing infinitely many lattice points. However, in this case a is only unique up to multiplication by

elements of $\mathcal{O}_{K,\mathfrak{m}}^\times$, and one can show that the volume of a fundamental domain is proportional to $\frac{x \operatorname{reg} \mathfrak{m}}{|N\mathfrak{c}|} = \frac{x \log |u|}{|N\mathfrak{c}|}$.

Now, we give a sketch proof of Proposition 17.5:

Sketch: Let $\mathfrak{c}$ be any representative of the ray class $\mathfrak{K}$. By the argument given above, $S(x, \mathfrak{K})$ counts the number of $a \in \mathfrak{c}^{-1}$ with $a \equiv 1 \pmod{\mathfrak{m}}$ (and a positive at all real places of $\mathfrak{m}$), such that $Na < \frac{x}{N\mathfrak{c}}$, modulo the action of $\mathcal{O}_K^\times$.

Let $\mathcal{F}$ be a fundamental domain for $\prod_{v|\infty} K_v / \mathcal{O}_K^\times$. Then we are counting the number of points of a certain lattice that lie in $\mathcal{F}$ and have $Nf < y$. We can estimate this with geometry of numbers:

The volume of $\{f \in \mathcal{F} \mid Nf < \frac{x}{N\mathfrak{c}}\}$ is equal to $\frac{2^r (2\pi)^s \operatorname{reg}(\mathfrak{m})}{w_{\mathfrak{m}} N\mathfrak{c}} x$. The lattice $\{a \in \mathfrak{c}^{-1} \mid a \equiv 1 \pmod{\mathfrak{m}}\}$ has covolume $\sqrt{|\operatorname{Disc}(K)|} \frac{N\mathfrak{m}}{N\mathfrak{c}}$.

Hence

$$S(x, \mathfrak{K}) = \frac{2^r (2\pi)^s \operatorname{reg}(\mathfrak{m})}{w_{\mathfrak{m}} N\mathfrak{m} |\operatorname{Disc}(K)|^{1/2}} x + O(x^{1-1/d})$$

(the error term is proportional to the surface area of $\mathcal{F}$), as desired.

□

Combining with Proposition 17.4, we get.

Proposition 17.6. *The partial zeta function $\zeta(s, \mathfrak{K})$ has analytic continuation to $\operatorname{Re} s > 1 - \frac{1}{d}$ with a simple pole at $s = 1$ of residue $g_{\mathfrak{m}}$, and no other poles.*

Theorem 17.7. *The function $L(s, \chi)$ analytically continues to $\operatorname{Re} s > 1 - \frac{1}{d}$ (where $d = [K : \mathbb{Q}]$)*

If χ is not the trivial character then $L(s, \chi)$ is holomorphic at $s = 1$. If χ is trivial then $L(s, \chi)$ has a pole of residue $|\operatorname{Cl}_{\mathfrak{m}}(\mathcal{O}_K)| g_{\mathfrak{m}}$.

Proof. We have $L(s, \chi) = \sum_{\mathfrak{K}} \chi(\mathfrak{K}) \zeta(s, \mathfrak{K})$, so it analytically continues to $\operatorname{Re} s > 1 - \frac{1}{d}$, with only pole at $s = 1$ with residue $\sum_{\mathfrak{K}} \chi(\mathfrak{K}) g_{\mathfrak{m}}$. □

Specializing to $\mathfrak{m} = (1)$ and $\chi = 1$:

Theorem 17.8 (Class Number Formula)**.** *$\zeta_K(s)$ has a simple pole at $s = 1$ with residue $\frac{2^r (2\pi)^s \operatorname{reg}(K) h_K}{w_K |\operatorname{Disc}(K)|^{1/2}}$.*

Special cases: when K is imaginary quadratic this is $\frac{2\pi h_K}{|\operatorname{Disc}(K)|^{1/2}}$: so we actually get a formula for h_K.

When K is real quadratic this is $\frac{\operatorname{reg}(K) h_K}{w_K |\operatorname{Disc}(K)|^{1/2}}$.

The Class Number Formula is important for a number of reasons: one is that it's analogous to the Birch and Swinnerton-Dyer conjecture (see Zagier "The Birch-Swinnerton-Dyer Conjecture from a Naive Point of View", and Lemmermeyer "Conics: A poor man's elliptic curve")

18 April 8

18.1 Densities for sets of primes

Let T be a set of primes of $\mathcal{O}_K$. There are multiple reasonable notions of density for T.

Definition. The natural density is $\lim_{x\to\infty} \frac{\#\{\mathfrak{p}\in T | N\mathfrak{p}\leq x\}}{\#\{\mathfrak{p}|N\mathfrak{p}\leq x\}}$.

Definition. Dirichlet density: if $\sum_{\mathfrak{p}\in T} \frac{1}{N\mathfrak{p}^s} = \delta \log \frac{1}{1-s} + O(1)$ as $s \to 1^+$, then T has Dirichlet density δ.

Definition. Polar density: if $(\prod_{\mathfrak{p}\in T}(1-\frac{1}{N\mathfrak{p}^s})^{-1})^n$ can be meromorphically continued to a neighborhood of $s = 1$ with a pole of order m at $s = 1$, then the polar density of T is m/n.

All three densities have the following properties

- They are monotonic where defined.
- finite additivity
- if T has density 0, so does any subset of T.
- finite sets have density 0

Verifications of these are straightforward.

Proposition 18.1. *If T has a natural density, then T also has a Dirichlet density and the two are equal.*

If T has a polar density, then T also has a Dirichlet density and the two are equal.

Sketches. For natural density, use partial summation.

For polar density, use

$$\log(\prod_{\mathfrak{p}\in T}(1-\frac{1}{N\mathfrak{p}^s})^{-1}) = \sum_{\mathfrak{p}\in T}\frac{1}{N\mathfrak{p}^s} + O(1)$$

as $s \to 1^+$ □

Remark. The set of primes of $\mathbb{Z}$ with leading digit 1 (in decimal) has a Dirichlet density $(\frac{\log 2}{\log 10})$ but no natural density.

Remark. Polar density must be a rational number, whereas natural and Dirichlet densities can be irrational.

Proposition 18.2. *The set of all primes of $\mathcal{O}_K$ has density 1 in all three definitions.*

Proof. This is clear for natural density, so must also hold for Dirichlet density.

For polar density, note that we've proved that $\zeta_K(s) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} (1 - \frac{1}{N\mathfrak{p}^s})^{-1}$ has a simple pole at $s = 1$. □

We'll be working with Dirichlet densities here: the sets we'll be considering will also have natural density, but that would require more careful error-bounding.

Proposition 18.3. *The set* T *of primes* $\mathfrak{p}$ *of* $\mathcal{O}_K$ *such that* $N\mathfrak{p}$ *is not a prime of* $\mathbb{Z}$ *has polar density* 0.

Proof. Let $d = [K : \mathbb{Q}]$. Write

$$\prod_{\mathfrak{p} \in T} (1 - \frac{1}{N\mathfrak{p}^s})^{-1} = \prod_{j=2}^{d} \prod_{p} (1 - p^{-js})^{-\#\{\mathfrak{p} | N\mathfrak{p} = p^j\}}$$

Because $\#\{\mathfrak{p} \mid N\mathfrak{p} = p^j\} \leq d$ always, this is a sub-product of $\zeta(2s)^d \zeta(3s)^d \cdots \zeta(ds)^d$, which converges for $\Re s > 1/2$.

Hence

$$\prod_{\mathfrak{p} \in T} (1 - \frac{1}{N\mathfrak{p}^s})^{-1}$$

also converges to a holomorphic function on $\Re s > 1/2$. □

Proposition 18.4. *Let* L *be a finite Galois extension of* K. *Then the set of primes of* K *that split completely in* L, *denoted* $\mathrm{Spl}(L/K)$, *has polar density* $\frac{1}{[L:K]}$.

Proof. Let S be this set, and let T be the set of primes above S.

We observe if $\mathfrak{p}_L$ is a prime of L with $N\mathfrak{p}_L$ prime, and which does not lie above a ramified prime of K, then $\mathfrak{p}_L \in T$. For this note that if we let $\mathfrak{p}_K$ be the prime of K under L, we have $N\mathfrak{p}_L = N\mathfrak{p}_K^{[L:K]/g}$, where g is the number of primes of L above K. Hence $N\mathfrak{p}_L$ is only prime in the case $g = [L : K]$, which means that $\mathfrak{p}_K \in \mathrm{Spl}(L/K)$.

Then T has polar density 1 by the previous proposition and the fact that there are only finitely many ramified primes. We also observe

$$\prod_{\mathfrak{p}_L \in T} (1 - \frac{1}{N\mathfrak{p}_L^s})^{-1}) = \prod_{\mathfrak{p}_K \in S} (1 - \frac{1}{N\mathfrak{p}^s})^{-1})^{[L:K]}$$

so S must have polar density $\frac{1}{[L:K]}$. □

Now we work towards the proof of the second inequality. Note that we haven't used any class field theory so far.

Theorem 18.5. *Let* H *be any subgroup of* $\mathrm{Cl}_m = \mathrm{Cl}_m(\mathcal{O}_K)$, *and let* $G = \mathrm{Cl}_m(\mathcal{O}_K)/H$.

Then at most one character χ *of* H *can have* $L(1, \chi) = 0$, *and it must be a simple zero.*

The Dirichlet density $\delta(\mathfrak{p} \mid [\mathfrak{p}] \in H)$ *is* $\frac{1}{|G|}$ *if* $L(1, \chi) \neq 0$ *for all characters of* Cl_m / H, *and* 0 *if* $L(1, \chi) = 0$ *for some* χ.

Proof. Consider the behavior of $f(s) = \frac{1}{|G|}\sum_\chi \log(L(s,\chi))$ as $s \to 1^+$ where χ ranges over all characters of G.

This is

$$\sum_{\mathfrak{p}} \frac{1}{|G|}\sum_{\chi} -\log(1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}) = \left(\sum_{\mathfrak{p}} \frac{1}{|G|}\sum_{\chi} \chi(\mathfrak{p})N\mathfrak{p}^{-s}\right) + O(1)$$
$$= \sum_{[\mathfrak{p}]\in H} Np^{-s} + O(1)$$

(we skip the details of checking convergence).

On the other hand, we also have

$$f(s) = \frac{1}{|G|}\log\frac{1}{1-s}\left(-\sum_\chi \operatorname{ord}_{s=1} L(s,\chi)\right) + O(1).$$

Hence

$$\sum_{[\mathfrak{p}]\in H} Np^{-s} = \frac{1}{|G|}\log\frac{1}{1-s}\left(-\sum_\chi \operatorname{ord}_{s=1} L(s,\chi)\right) + O(1)$$

so the set $\{\mathfrak{p} \mid [\mathfrak{p}] \in H\}$ has Dirichlet density $\frac{1-\sum_{\chi\neq 1}\operatorname{ord}_{s=1} L(s,\chi)}{|G|}$.

Since Dirichlet density is non-negative, we can only have $\operatorname{ord}_{s=1} L(s,\chi) > 0$ for one nontrivial χ, and that χ must have a simple zero. The result follows.

□

To get rid of the annoying possibility that some $L(1,\chi)$ might have a zero at $s = 1$, we'll have to use class field theory. But first we'll give the analytic proof of the second inequality.

Theorem 18.6. *L/K Galois, $\mathfrak{m}$ a modulus:*

Then $|C_K^\times / N_{L/K}C_L^\times U_\mathfrak{m}| \le [L:K]$.

Since we can take $\mathfrak{m}$ such that $U_\mathfrak{m} \subset C_L^\times$, we get also that $|C_K^\times / N_{L/K}C_L^\times| \le [L:K]$.

Proof. $G = C_K^\times / N_{L/K}C_L^\times U_\mathfrak{m} \cong Cl_\mathfrak{m}(\mathcal{O}_K)/H$, where H is the subgroup of $Cl_\mathfrak{m}(\mathcal{O}_K)$ generated by ideals which are norms from L.

We know that Dirichlet density $\delta\{\mathfrak{p} \mid [\mathfrak{p}] \in H\}$ is either $\frac{1}{|G|}$ or 0.

On the other hand, if $\mathfrak{p}$ splits completely in L, then $[\mathfrak{p}] \in H$, so the density must be $\ge \frac{1}{[L:K]}$, and we must have $|G| \le [L:K]$.

As a corollary, we see that for any nontrivial character χ of G, $L(1,\chi) \neq 0$. □

Corollary 18.7. *If χ is a nontrivial character of $Cl_\mathfrak{m}(\mathcal{O}_K)$ then $L(1,\chi) \neq 0$.*

Proof. In the setup of the previous theorem, take L such that $N_{L/K}C_L^\times \subset U_\mathfrak{m}$ (here we are using the existence theorem of class field theory). Then $G = Cl_\mathfrak{m}(\mathcal{O}_K)$ and we see, as in the proof above, that for any nontrivial character χ of G, $L(1,\chi) \neq 0$. □

Proposition 18.8. *Let* C *be any subset of* $\mathrm{Cl}_{\mathfrak{m}} = \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$. *Then the Dirichlet density of* $\{\mathfrak{p} \mid [\mathfrak{p}] \in C\}$*is* $\frac{|C|}{|\mathrm{Cl}_{\mathfrak{m}}|}$

Proof. Enough to do when $C = \{\mathfrak{K}\}$ is a singleton.

Then, by the same argument used in the proof of Theorem 18.5

$$\sum_{\mathfrak{p} \in \mathfrak{K}} \frac{1}{N\mathfrak{p}^s} = \frac{1}{|\mathrm{Cl}_{\mathfrak{m}}|} \sum_{\chi} \overline{\chi(K)} \log L(s, \chi) + O(1) = \frac{1}{|\mathrm{Cl}_{\mathfrak{m}}|} \log(1/(1-s)) + O(1) \text{ as } s \to 1^+$$

where χ runs over all characters of modulus $\mathfrak{m}$. Here the $\frac{1}{|\mathrm{Cl}(\mathfrak{m})|} \log(1/(1-s))$ comes from $L(s, 1)$, and all other L-functions are $O(1)$ as $s \to 1^+$. □

This is the natural generalization of Dirichlet's theorem to arbitrary number fields, and is enough to give Cebotarev density for abelian extensions. Next time we'll prove full Cebotarev density.

19 April 12

19.1 Cebotarev Density Theorem

Setup: let L/K be a Galois extension of number fields. Then we have a map

(unramified primes of K) $\to$ (conjugacy classes of $\mathrm{Gal}(L/K)$)

given by $\mathfrak{p} \mapsto [\mathrm{Frob}_{\mathfrak{p}}]$.

Theorem 19.1 (Cebotarev Density Theorem)**.** *For any conjugacy class* $[g]$ *of* $G = \mathrm{Gal}(L/K)$*, the set of primes*

$$T_g = \{\mathfrak{p} \mid [\mathrm{Frob}_{\mathfrak{p}}] = [g]\}$$

has Dirichlet density $\frac{|[g]|}{|G|}$.

Remark. Lagarias and Odlyzko have developed effective versions of Cebotarev which give an upper bound on the size of the smallest element of T_g.

We've already proved this for the special case where $g = 1$: in that case $T_1 = \mathrm{Spl}(L/K)$.

We first apply the results from last time to get the case when L/K is abelian, and then we'll bootstrap from there using the same argument that worked when $g = 1$.

Proposition 19.2 (Abelian Cebotarev Density)**.** *Let* L/K *be an abelian extension. Then* L/K *satisfies the Cebotarev density theorem.*

Proof. Pick $\mathfrak{m}$ with $L \subset L_{\mathfrak{m}}$, and let $H \subset \mathrm{Cl}_{\mathfrak{m}}$ be the subgroup corresponding to $\mathrm{Gal}(L/K) \subset \mathrm{Gal}(L_{\mathfrak{m}}/K)$. Then $\mathrm{Frob}_{\mathfrak{p}} = g \in \mathrm{Gal}(L/K)$ if and only if $[\mathfrak{p}] \in gH$, and the result follows from Proposition 18.8. □

Proof of Full Cebotarev Density. We'll ignore all primes of K that ramify in L, since there are only finitely many such. Let $[L : K] = n$, and let the order of the element $g \in G$ be m.

Let M be the intermediate field $L^{\langle g \rangle}$ fixed by the cyclic subgroup generated by g, so L/M is cyclic of degree m. Importantly, L/M is abelian, so we'll be able to use Abelian Cebotarev. On the other hand M/K might not even be Galois, but that will be fine.

First we look at what it means for $\mathfrak{p}$ to belong to the set T_g. If that is the case then $[\mathrm{Frob}_\mathfrak{p}] = [g]$, and for some prime $\mathfrak{p}_L$ above $\mathfrak{p}$, the Frobenius element of $\mathrm{Gal}(L/K)$ at $\mathfrak{p}_L$ is equal to g. In particular, this means that g generates the decomposition group $D_{\mathfrak{p}_L}$, and M is the decomposition field of $\mathfrak{p}_L$.

Let $\mathfrak{p}_M$ be the unique prime of M under $\mathfrak{p}_L$. Then the inertia degree $f_{M/K} = 1$, and $\mathrm{Frob}_{\mathfrak{p}_M} = g \in \mathrm{Gal}(L/M)$. Let $T_{M,g}$ be the set of $\mathfrak{p}_M$ satisfying these properties. If we have any $\mathfrak{p}_M \in T_{M,g}$, then $\mathfrak{p} = \mathfrak{p}_M \cap \mathcal{O}_K$ belongs to T_g (but the map $\mathfrak{p}_M \mapsto \mathfrak{p}$ is not one-to-one).

Observe that

$$\sum_{\mathfrak{p}_M \in T_{M,g}} \frac{1}{N\mathfrak{p}_M^s} = \sum_{\mathrm{Frob}(\mathfrak{p}_M)=g} \frac{1}{N\mathfrak{p}_M^s} + O(1) = \frac{1}{m} \log(1/(1-s)) + O(1) \tag{4}$$

by abelian Cebotarev.

Now we need to move down to K. To do this we need to know how many $\mathfrak{p}_M \in T_{M,g}$ lie above some $\mathfrak{p}$ in T_g. Since $\mathfrak{p}_L$ is uniquely determined by $\mathfrak{p}_M$, it's enough to count the number of $\mathfrak{p}_L$ lying above $\mathfrak{p}$ with $\mathrm{Frob}_{\mathfrak{p}_L} = g$.

For this, first choose some $\mathfrak{p}_{L,0}$ with $\mathrm{Frob}_{\mathfrak{p}_{L,0}} = g$. Any other prime of L lying above $\mathfrak{p}$ takes the form $\mathfrak{p}_L = h\mathfrak{p}_{L_0}$, where h is unique up to right multiplication by powers of g. Then $\mathrm{Frob}_{h\mathfrak{p}_{L_0}} = hgh^{-1}$, which equals g iff h is in the centralizer of g. So the number of possible $\mathfrak{p}_L$ is equal to $\frac{|C(g)|}{m} = \frac{n}{|[g]|m}$.

Combining with (4), we get that

$$\sum_{\mathfrak{p} \in T_g} \frac{1}{N\mathfrak{p}^s} = \frac{|[g]|m}{n} \sum_{\mathfrak{p}_M \in T_{M,g}} \frac{1}{N\mathfrak{p}_M^s} = \frac{|[g]|}{n} \log(1/(1-s)) + O(1)$$

□

19.2 Splitting sets of an extension

Recall that for L/K a finite extension, $\mathrm{Spl}(L/K)$ denotes the set of primes of K that split completely in L. The notation $\mathrm{Spl}(L/K)$ makes sense regardless of whether L/K is Galois.

Exercise: $\mathrm{Spl}(L/K) = \mathrm{Spl}(L'/K)$ where L'/K is the Galois closure of L/K.

Hence if L/K is not Galois the Dirichlet density of $\mathrm{Spl}(L/K) = \mathrm{Spl}(L'/K)$ is $\frac{1}{[L':K]}$.

Galois extensions are entirely characterized by their splitting sets.

Theorem 19.3. *If L, L' are Galois extensions of K, then $\mathrm{Spl}(L/K) = \mathrm{Spl}(L'/K)$ implies $L = L'$.*

Proof. If $\mathrm{Spl}(L/K) = \mathrm{Spl}(L'/K)$ then $\mathrm{Spl}(LL'/K) = \mathrm{Spl}(L/K)$. But $\mathrm{Spl}(LL'/K)$ has density $\frac{1}{[LL':K]}$ and $\mathrm{Spl}(L/K)$ has density $\frac{1}{[L:K]}$, so $[LL' : K] = [L : K]$ and $L' \subset L$. Likewise $L \subset L$ and $L = L'$. □

In fact this proves a little bit more. Write $S \doteq T$ if the sets $S \setminus T$ and $T \setminus S$ are both finite. Then the proof above shows that $\mathrm{Spl}(L/K) \doteq \mathrm{Spl}(L'/K)$ implies $L = L'$.

Note that this fails if L and L' are not Galois: in fact, there exist non-isomorphic non-Galois extensions L, L' of a number field K such that every prime of K has the same splitting behavior in L as in L'. (See pages 362-363 of Cassels-Frohlich for an outline.)

Corollary 19.4. *If $f(x) \in \mathbb{Z}[x]$ is a polynomial such that f splits into linear factors in $\mathbb{F}_p$ for all but finitely many p, then f splits into linear factors in $\mathbb{Z}[x]$.*

In fact (HW) a stronger fact is true: if f is irreducible and has a root in $\mathbb{F}_p$ for all but finitely many p, then f has a root in $\mathbb{Q}$. (Irreducibility is necessary: for a counterexample see $(x^2-2)(x^2-3)(x^2-6)$.)

I mentioned also that there are irreducible polynomials over $\mathbb{Z}$ such that their reduction mod all but finitely many primes is irreducible, but didn't give an example. One simple example is $f(x) = x^4 + 1$: here 2 is the only ramified prime in the splitting field $K = \mathbb{Q}[x]/(x^4+1)$. If p is odd, the element Frob_p will be an element of order either 1 or 2

19.3 Intro Complex Multiplication

Recall that for $\mathbb{Q}$ Kronecker-Weber gives us an explicit description of $\mathbb{Q}^{ab} = \bigcup_n \mathbb{Q}(\zeta_n)$. More specifically, the field $\mathbb{Q}(\zeta_n)$ is the ray class field of modulus $n\infty$.

The reason this works is that we're adjoining torsion points of an algebraic group. In this case, the algebraic group is the multiplicative group $\mathbb{G}_m$, which has endomorphism ring $\mathrm{End}(\mathbb{G}_m) \cong \mathbb{Z}$. For every n we have the torsion subgroup$\mathbb{G}_m[n] = \mu_n$ of points killed by the nth power map. Then we have an inclusion $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(\mathbb{G}_m[n]) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, which we've seen is an isomorphism.

Ideally we'd like to generalize this setup with $\mathbb{Q}$ replaced by some other number field K. (Ultimately this will only work for K imaginary quadratic.) However, if $K \neq \mathbb{Q}$, K^{ab} is larger than $K(\zeta_\infty) = \mathbb{Q}^{ab}$.

So we'll want to replace $\mathbb{G}_m$ by some other one-dimensional algebraic group. We don't have many choices: in fact, the only other thing we can really do is take E to be an elliptic curve defined over K.

If we just take E to be a general elliptic curve defined over K, then the n-torsion subgroup $E[n] = E[n](\bar{K})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$. The extension $K(E[n])$ then has Galois group embedding into $\mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, so this is not a reliable way of producing abelian extensions.

Instead, as in the Lubin-Tate theory, we will want to consider elliptic curves with extra endomorphisms. We'll later see the important theorem:

Proposition 19.5. *If E is an elliptic curve over $\mathbb{C}$, then the endomorphism algebra $\mathrm{End}(E)$ is isomorphic either to $\mathbb{Z}$ or to an order $\mathcal{O}$ in an imaginary quadratic field.*

In the latter case we say E has CM by $\mathcal{O}$.

So we might try the following: let K be an imaginary quadratic field. Suppose we can find an elliptic curve E defined over K with CM by $\mathcal{O}_K$, and such that all endomorphisms of E are defined over K. Then for any ideal $\mathfrak{a}$ of $\mathcal{O}_K$ let $E[\mathfrak{a}]$ be the $\mathfrak{a}$-torsion subgroup of E, namely

$$E[\mathfrak{a}] = \{x \in E(\mathbb{C}) \mid \alpha x = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

Then one can show $E[\mathfrak{a}] \cong \mathcal{O}_K/\mathfrak{a}$ as $\mathcal{O}_K/\mathfrak{a}$-modules, and $\mathrm{Aut}_{\mathcal{O}_K}(E[\mathfrak{a}]) \cong (\mathcal{O}_K/\mathfrak{a})^\times$. Hence we'd get an injection

$$\mathrm{Gal}(K(E[\mathfrak{a}])/K) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K}(E[\mathfrak{a}]) \cong (\mathcal{O}_K/\mathfrak{a})^\times,$$

meaning that here $K(E[\mathfrak{a}])$ is legitimately an abelian extension of K.

The bad news here is this setup works out for only finitely many imaginary quadratic fields K: in fact, exactly those with class number 1, because E is not generally defined over K.

However, leads us to ask what is the minimal field of definition of an elliptic curve E with CM over K, which turns out to be a great question. The answer here is that any elliptic curve E with complex multiplication by K is defined, not over K, but over the Hilbert class field H of K.

20 April 15

20.1 Complex Multiplication and Ray Class Fields

If K is an imaginary quadratic field, then any elliptic curve E with complex multiplication by E is defined, not over K, but over the Hilbert class field H of K. In fact, $H = K(j(E))$ is generated by the j-invariant, and the minimal polynomial for $j(E)$ over K is $\prod_{E' \text{ CM by } \mathcal{O}_K}(x - j(E'))$. So this already gives us a way to get explicit generators for H.

Note that this means that the number of elliptic curves with CM by $\mathcal{O}_K$ is finite and equal to h_K.

If we want to go beyond H and construct the ray class field $L_{\mathfrak{m}}$, then we follow the plan sketched last time. Let E be any elliptic curve with CM by $\mathcal{O}$. We know that E is defined over H, so the field $H(E[\mathfrak{m}])$ generated by adjoining coordinates of the $\mathfrak{m}$-torsion points of E is an abelian extension of H, which one can show is unramified only over primes dividing $\mathfrak{m}$. By the argument above $H(E[\mathfrak{m}])$ is an abelian extension of H, and we have an injection $\mathrm{Gal}(H(E[\mathfrak{m}])/H) \hookrightarrow (\mathcal{O}_K/\mathfrak{m})^\times$: this should in fact be an isomorphism.

Then $H(E[\mathfrak{m}])$ may not be an abelian extension of K, but one can show $[H(E[\mathfrak{m}]) : L_{\mathfrak{m}}] \leq 6$, so we're not very far off.

In support of this, note that $\mathrm{Gal}(L_{\mathfrak{m}}/H)$ is the kernel of the natural map $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_K)$, which is in turn the quotient of $(\mathcal{O}_K/\mathfrak{m})^\times$ by the image of $\mathcal{O}_K^\times$. On the other hand, $\mathrm{Gal}(H(E[\mathfrak{m}])/H) \cong (\mathcal{O}_K/\mathfrak{m})^\times$, so this is consistent with $H(E[\mathfrak{m}])/H$ being a subextension of $\mathrm{Gal}(L_{\mathfrak{m}}/H)$ (and note this means that the degree $[H(E[\mathfrak{m}])/H : L_{\mathfrak{m}}]$ is at most 6).

We'll now develop enough of the theory of elliptic curves to be able to prove all this. We'll start from the analytic point of view, via elliptic functions. References for this section are Cox *Primes of the Form* $x^2 + ny^2$ and Silverman *Advanced Topics in the Arithmetic of Elliptic Curves*. I'll start out following Cox, but eventually we'll go beyond what Cox does

20.2 Elliptic Functions

Let L be a lattice in $\mathbb{C}$. Then an *elliptic function* for L is a meromorphic function on $\mathbb{C}/L$. Equivalently, if ω_1, ω_2 are generators for L, an elliptic function is a meromorphic function f on $\mathbb{C}$ with $f(z) = f(z + \omega_1) = f(z + \omega_2)$.

Weierstrass $\wp$-function.

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\omega \in L \smallsetminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Fix L and write $\wp(z) = \wp(z, L)$.

Proposition 20.1. *$\wp(z)$ is an elliptic function for L whose only poles are double poles at the points of L.*

Proof. To show convergence we'll need

Exercise: if L is a lattice in $\mathbb{C}$ and $r > 2$ is a positive integer then $G_r(L) = \sum_{\omega \in L \smallsetminus \{0\}} \frac{1}{\omega^r}$ converges absolutely. (This is an Eisenstein series for L.)

Then, assuming z, $\frac{1}{z-\omega}$ bounded,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{\omega^2 - (z-\omega)^2}{\omega^2 (z-\omega)^2} = O(\omega^{-3})$$

so the series for $\wp(z)$ converges locally uniformly and absolutely on $\mathbb{C}^2 - L$.

Likewise, for any $\omega \in L$, in the neighborhood of $z = \omega$, we have $\wp(z) = \frac{1}{(z-\omega)^2} +$ holomorphic.

First, we have $\wp(-z) = \wp(z)$: clear since $\omega \in L$ iff $-\omega \in L$.

Now, to check periodicity, observe that for any $\omega \in L$, the function $\wp(z, L) - \wp(z + \omega, L)$ is entire, so must be constant. But picking $z = -\omega/2$ we have that the constant must be 0. Hence $\wp(z, L)$ is an elliptic function. $\square$

The Weierstrass $\wp$-function does not generate the field of meromorphic functions on $\mathbb{C}/L$: to do that we must also add in the derivative

$$\wp'(z) = -2\sum_{\omega\in L}\frac{1}{(z-\omega)^3}.$$

This is a function on $\mathbb{C}/L$ with a pole of order 3 at 0: hence it must have three zeroes. Can check that these occur at the three nonzero points of $\frac{1}{2}L/L$.

We'll be able to get an algebraic relation between these two. For this it will be useful to get a power series for $\wp(z)$ at the origin.

Lemma 20.2.

$$\wp(z) = \frac{1}{z^2} + \sum_{n\geq 1}(2n+1)G_{2n+2}z^{2n}.$$

Recall $G_n = \sum_{\omega\in L-0}\omega^{-n}$.

Proof. Sum

$$\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \sum_{m\geq 1}(m+1)\omega^{-m-2}z^m$$

over all $\omega \in L \smallsetminus 0$, and observe that the terms with even exponent vanish. □

Can check that

$$(\wp'(z))^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$$

where $g_2(L) = 60G_4(L)$ and $g_3(L) = 140G_6(L)$: check this by checking that the difference between both sides is entire and vanishes at the origin.

As a corollary, get (exercise: by induction) that all $G_{2n}(L)$ are polynomials in $g_2(L)$ and $g_3(L)$. If we put a grading on the ring generated by g_2 and g_3 by saying that g_2 has weight 2 and g_3 has weight 3 then G_{2n} has weight n.

If we let E be the elliptic curve with equation $y^2 = 4x^3 - g_2x - g_3$, the map $z \mapsto (\wp(z), \wp'(z))$ is a map of Riemann surfaces $\mathbb{C}/L \to E$. We'll next show that it's an isomorphism.

Proposition 20.3. $\wp(z) = \wp(w)$ *iff* $z \equiv \pm w \pmod{L}$.

Proof. View $\wp(z) - \wp(w)$ as a function of $z \in \mathbb{C}/L$. It has its only pole of order 2 at $z = 0$, so must have exactly two zeroes (with multiplicity). If $w \notin L/2$ then these are two single zeroes at $\pm w$, if $w \in L/2$ then this is one double zero at w. □

Corollary 20.4. *The map* $\mathbb{C}/L \to E$ *given by* $z \mapsto (\wp(z), \wp'(z))$ *is an isomorphism.*

Proof. First we show injectivity: suppose $(\wp(z), \wp'(z)) = (\wp(w), \wp'(w))$. By the previous proposition we have $w \equiv \pm z \pmod{L}$. If $z \in 1/2L$ then we're done. Otherwise, we only know that $w \equiv \pm z \pmod{L}$. But $\wp'(z) \neq 0$, so $\wp'(-z) = -\wp'(z) \neq \wp'(z)$, ruling out $w \equiv -z$.

Surjectivity follows from complex analysis: the image of the map must be open and compact, so the map is surjective. □

It then follows that $z \mapsto (\wp(z), \wp'(z))$ is injective, so gives an isomorphism $\mathbb{C}_L \cong E$.) Consequence: any elliptic function is a rational function in $\mathfrak{p}, \mathfrak{p}'$.

Proposition 20.5. *Addition Theorem:*

$$\wp(z+w) = -\wp(z) - \wp(w) + \left(\frac{1}{4}\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2$$

Sketch. Viewed as a function of z the difference of both sides is holomorphic everywhere and vanishes at the origin. □

Define discriminant

$$\Delta(L) = g_2^3 - 27g_3^2$$

this is (up to a factor of 16) the discriminant of the polynomial $4x^3 - g_2x - g_3$ and is never 0.

and define $j(L) = 1728\frac{g_2^3}{\Delta}$.

Theorem 20.6. *If* L *and* L' *are lattices in* $\mathbb{C}$ *then* $j(L) = j(L')$ *iff* L' *is homothetic to* L.

Proof. Only if direction is clear. If $j(L) = j(L')$ then there exists λ with $g_2(L) = \lambda^2 g_2(L')$, $g_3(L) = \lambda^3 g_3(L')$. As consequence $G_{2n}(L) = \lambda^n G_{2n}(L')$.

Hence $\wp_L(\lambda z) = \wp_{L'}(z)$. Comparing poles we have $\lambda^{-1}L = L'$. □

Now we study which $\mathbb{C}/L$ have extra endomorphisms. Terminology: an isogeny from $E \to E'$ is a nonzero homomorphism of complex Lie groups.

Note that if $\phi : \mathbb{C}/L \to \mathbb{C}/L'$ is an isogeny, then ϕ lifts to a homomorphism $\tilde{\phi} : \mathbb{C} \to \mathbb{C}$, and $\tilde{\phi}$ must be multiplication by some α.

Theorem 20.7. L *a lattice,* $\wp(z) = \wp_L(z)$, $\alpha \in \mathbb{C}$ *not an integer.*

Then TFAE:

a) The multiplication by α *map* $\mathbb{C} \to \mathbb{C}$ *induces an isogeny* $\mathbb{C}/L \to \mathbb{C}/L$.

b) $\alpha L \subset L$

c) $\wp(\alpha z)$ *is a rational function in* $\wp(z)$

d) There is an order $\mathcal{O}$ in an imaginary quadratic field K such that $\alpha \in \mathcal{O}$ and L is homothetic to a proper fractional $\mathcal{O}$-ideal.

(Here an order $\mathcal{O}$ of K is a subring of K which is a $\mathbb{Z}$-module of rank 2, or equivalently, is a finite index subring of $\mathcal{O}_K$.)

Proof. a) $\Leftrightarrow$ b) is clear.

For c) implies b), if $\wp(\alpha z)$ is a rational function in $\wp(z)$, then the set of poles of $\wp(\alpha z)$ must be invariant under translation by L. But that set is $\alpha^{-1}L$, so must have $\alpha^{-1}L \supset L$, equivalent to b)

a) implies c): pull back the function $\wp(z)$ by the map $\alpha : \mathbb{C}/L \to \mathbb{C}/L$ to get that $\wp(\alpha z)$ is a meromorphic function on $\mathbb{C}/L$, that is, an elliptic function for L. We also have $\wp(\alpha z) = \wp(-\alpha z)$, so $\wp(\alpha z)$ is an even elliptic function for L. Exercise: $\wp(z)$ generates the field of even elliptic functions on $\mathbb{C}/L$, and the implication follows.

d) implies b) is clear.

for b) implies d): wlog $1 \in L$. Then, since $\alpha L \subset L$, we have $\mathbb{Z}[\alpha] \subset L$. Hence $\mathbb{Z}[\alpha]$ is a $\mathbb{Z}$-module of rank 2, so α must be an algebraic integer of degree 2. Also, since $\mathbb{Z}[\alpha]$ is discrete in $\mathbb{C}$, the ring $K(\alpha)$ must be an imaginary quadratic field. Let $\mathcal{O} = \mathbb{Z}[\alpha]$: we have $L \supset \mathcal{O}$, and both are lattices in $\mathbb{C}$, so we must also have $\frac{1}{n}\mathcal{O} \supset L$ for some n. As well, $\mathcal{O}L \subset L$, so L is a fractional ideal of $\mathcal{O}$, as desired. □

21 April 19

21.1 Facts about orders in imaginary quadratic fields and their ideals

Recall:

Definition. An order $\mathcal{O}$ in an imaginary quadratic field K is a subring of K which is a $\mathbb{Z}$-module of rank 2, or equivalently, is a finite index subring of $\mathcal{O}_K$.

Proposition 21.1. *If $\mathcal{O}$ is an order in an imaginary quadratic field K, the order $\mathcal{O}$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for some $f \in \mathbb{Z}$, called the* conductor *of $\mathcal{O}$.*

Proof. Take $f = [\mathcal{O}_K : \mathcal{O}]$. Then certainly $\mathcal{O} \supset \mathbb{Z} + f\mathcal{O}_K$, but both rings have index f in $\mathcal{O}$. □

(More generally, the conductor of an order $\mathcal{O}$ in an arbitrary number field K is the largest ideal $\mathfrak{f}$ of $\mathcal{O}_K$ such that $\mathcal{O} \supset \mathfrak{f}$.)

If $\mathcal{O}$ is an order in an imaginary quadratic field, then the class group $\mathrm{Cl}(\mathcal{O})$ is the quotient of the group of all invertible fractional ideals of $\mathcal{O}$, modded out by all principal fractional ideals. Let $h(\mathcal{O}) = |\mathrm{Cl}(\mathcal{O})|$.

Definition. A fractional ideal $\mathfrak{a}$ of a quadratic order $\mathcal{O}$ is proper if and only if $\mathfrak{a}$ is not a fractional ideal of $\mathcal{O}'$ for $\mathcal{O}' \supset \mathcal{O}$. Equivalently, the set $\mathrm{End}_{\mathcal{O}}(\mathfrak{a}) = \{x \mid x\mathfrak{a} \subset \mathfrak{a}\}$ is equal to $\mathcal{O}$.

Example. If τ is a root of $ax^2 + bx + c = 0$, with $\gcd(a, b, c) = 1$, then the lattice $\langle 1, \tau \rangle$ is a proper ideal of $\mathbb{Z}[a\tau]$.

Theorem 21.2. *A fractional ideal $\mathfrak{a}$ of an order $\mathcal{O}$ is proper of if and only if $\mathfrak{a}$ is invertible.*

Proof. $\Leftarrow$: if $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ then $x\mathfrak{a} \subset \mathfrak{a}$ implies $x\mathcal{O} \subset \mathcal{O}$, so $x \in \mathcal{O}$.

$\Rightarrow$: WLOG $\mathfrak{a} = \langle 1, \tau \rangle$ with $a\tau^2 + b\tau + c = 0$. Let $\mathfrak{b} = \langle 1, \bar{\tau} \rangle$. Then $\mathfrak{a}\mathfrak{b} = \langle 1, \tau, \bar{\tau}, \tau\bar{\tau} \rangle = \frac{1}{a}\mathbb{Z}[a\tau]$.

□

(Remark: the generalization to orders in higher degree number fields is not true: counterexample $K = \mathbb{Z}(\sqrt[3]{2})$, $\mathcal{O} = \mathbb{Z} + 2\mathcal{O}_K$, $\mathfrak{a} = \langle 8, 2\sqrt[3]{2}, 2\sqrt[3]{4} \rangle$.)

This means that if $L \subset \mathbb{C}$ is a lattice such that $\mathbb{C}/L$ has complex multiplication, there is a unique imaginary quadratic order $\mathcal{O}$ such that L is homothetic to an invertible ideal of $\mathcal{O}$. This order $\mathcal{O}$ is given by $\{\alpha \in \mathbb{C} \mid \alpha L \subset L\} = \mathrm{End}(\mathbb{C}/L)$.

21.2 Proof that CM j-invariants are algebraic

Theorem 21.3. *Let $\mathcal{O}$ be an order in an imaginary quadratic field, and let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. Then $j(\mathfrak{a})$ is an algebraic number of degree at most $h(\mathcal{O})$.*

Proof. Consider the set $S = \{j(E) \mid \mathrm{End}(E) \cong \mathcal{O}\} \subset \mathbb{C}$: this set is invariant under $\mathrm{Aut}(\mathbb{C})$. However the set $\mathbb{C} \smallsetminus \bar{\mathbb{Q}}$ of all transcendentals forms a single infinite orbit for $\mathrm{Aut}(\mathbb{C})$ (proof uses the theory of transcendence bases), so the finite set S can't contain any transcendentals.

Now we know $S \subset \bar{\mathbb{Q}}$ is invariant under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and has size equal to $h(\mathcal{O})$. It follows that any element of S is an algebraic number of degree $\leq h(\mathcal{O})$. In particular, $j(\mathfrak{a}) \in S$ so we're done.

□

21.3 Ring class fields

Later we'll show this is sharp, and that $j(E)$ generates the ring class field of $\mathcal{O}$, which we now define. In the case where $\mathcal{O} = \mathcal{O}_K$ the ring class field of $\mathcal{O}$ is the Hilbert class field of K.

Definition. If $\mathcal{O}$ is an order in an imaginary quadratic field K, the ring class field $L_{\mathcal{O}}$ is the abelian extension of K defined by the condition that

$$\mathrm{Gal}(L_{\mathcal{O}}/K) = \mathbb{A}_K^\times / K^\times \cdot \prod_{v \text{finite}} U_v^\times \times \mathbb{C}^\times$$

where U_v is the closure of $\mathcal{O}$ in the ring of integers $\mathcal{O}_v^\times$ of the localization $K_v^\times$. Exercise: $\mathrm{Gal}(L_\mathcal{O}/K) \cong \mathrm{Cl}(\mathcal{O})$.

In particular $\mathcal{O}$ can be written as $\mathbb{Z} + f\mathcal{O}_K$, and then $U_v = (\mathbb{Z}_p + f\mathcal{O}_v)^\times$. Observe that $L_\mathcal{O} \subset L_f$ where L_f is the ray class field of K with modulus f.

Exercise: if p is a prime of $\mathbb{Z}$ relatively prime to $\operatorname{disc}\mathcal{O} = f^2 \operatorname{disc}\mathcal{O}_K$, p splits completely in $L_\mathcal{O}$ if and only if $p = \pi\bar{\pi}$ for $\pi \in \mathcal{O}$. (We previously did this when $\mathcal{O} = \mathcal{O}_K$.)

So far we've seen that if L is a lattice with $\mathrm{End}(L) = \mathcal{O}$ is larger than $\mathbb{Z}$ ("L has complex multiplication by $\mathcal{O}$"), then $\mathcal{O}$ is an order in an imaginary quadratic field, L is homothetic to some proper fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ (write $L \sim \mathfrak{a}$), and $j(L) = \jmath(\mathfrak{a})$ is an algebraic number of degree at most equal to $h(\mathcal{O})$.

We want to improve this by showing that $j(L)$ is an algebraic integer of degree precisely equal to $h(\mathcal{O})$, and that $K(j(L))$ is the ring class field $L_\mathcal{O}$.

21.4 Sketch of proof that $j(L)$ generates the ring class field

We're going to be giving Deuring's original proof of this fact, roughly following the exposition in Cox's book.

Three key ingredients:

First: Characterization of lattices with complex multiplication using cyclic sublattices.

Definition. A sublattice L' of L with $L/L' \cong \mathbb{Z}/m\mathbb{Z}$ is called a *cyclic sublattice of index m*.

Proposition 21.4. *A lattice L has complex multiplication if and only if there is a prime p (in fact, infinitely many such!) and a cyclic index p sublattice L' of L such that L' is homothetic to L.*

Proof. The $\Leftarrow$ implication is clear.

For $\Rightarrow$: WLOG $L = \mathfrak{a}$, where $\mathfrak{a}$ is an ideal of $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. Let p be a prime relatively prime to $\mathfrak{a}$ and $\operatorname{Disc}\mathcal{O}$ such that p splits in the ring class field $L_\mathcal{O}$, so $p = \pi\bar{\pi}$ for $\pi \in \mathcal{O}$. Then let $L' = \pi L$: certainly L' is homothetic to L, and also $L'/L \cong \mathcal{O}_K/\pi\mathcal{O}_K \cong \mathbb{Z}/\mathfrak{p}\mathbb{Z}$. □

Second: Modular forms and q-expansions:

We'll use these to show that there exists an equation $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$ *the modular equation of level* m such that if L is a lattice in $\mathbb{C}$ and L' a cyclic sublattice of index m, then $\Phi_m(j(L), j(L')) = 0$. Combining this with the first part, we get if L has complex multiplication, then $\Phi_m(j(L), j(L)) = 0$ for some m. We'll be able to show that the leading coefficient of $\Phi_m(X, X)$ is 1 when m is prime, giving integrality.

Third: It still remains to show that $K(j(L)) = L_\mathcal{O}$. We'll do this by checking that the same primes of K split completely in both fields. (Actually we'll have to be a little more careful than that, because we won't yet know that $K(j(L))$ is Galois.)

21.5 The j-function as modular function

Theorem 21.5. *For any τ in the upper half-plane $\mathbb{H} = \{\mathrm{Im}\,\tau > 0\}$, Define $g_2(\tau) = g_2([1,\tau])$, $g_3(\tau) = g_3([1,\tau])$ and $j(\tau) = j([1,\tau])$ as the corresponding functions of the lattice in $\mathbb{C}$ generated by 1 and τ.*

Let $SL_2(\mathbb{Z})$ act on $\mathbb{H}$ by $\gamma(\tau) = \frac{a\tau+b}{c\tau+d}$ where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Note that if $[1,\tau] = L$ then $[1,\gamma\tau] = (c\tau+d)^{-1}L$ is homothetic to L.

We then observe that for any matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, we have $g_2(\gamma(\tau)) = (c\tau+d)^4 g_2(\tau)$, $g_3(\gamma(\tau)) = (c\tau+d)^6 g_3(\tau)$.

Finally, $j(\gamma(\tau)) = j(\tau)$, so j descends to a function on the modular curve $Y(1) = SL_2(\mathbb{Z})\backslash\mathbb{H}$. Draw standard fundamental domain for $SL_2(\mathbb{Z})\backslash\mathbb{H}$, and observe that $Y(1)$ is a punctured sphere.

We can compactify $Y(1)$ to a compact Riemann surface $X(1)$ by adding a point at infinity. The function field of $X(1)$ is then the field of *modular functions* defined by

Definition. A meromorphic function $f(\tau)$ on the upper half-plane is a modular function for $SL_2(\mathbb{Z})$ if $f(\gamma\tau) = f(\tau)$ for all $\gamma \in SL_2(\mathbb{Z})$, and if $f(\tau)$ can be written as a Laurent series $\sum_{n\geq -k} c_n q^n$ in $q = e^{2\pi i\tau}$ that converges for $\mathrm{Im}\,\tau$ sufficiently large.

22 April 22

22.1 Explicit formulas

Let $q = e^{2\pi i\tau}$. Then

$$G_{2k}(\tau) = G_{2k}([1,\tau]) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n\geq 1}\sigma_{2k-1}(n)q^n$$

where $\sigma_{2k-1}(n)$ is the sum of the $(2k-1)$st powers of the divisors of n. (Proof will be on HW.)

Specifically,

$$g_2(\tau) = 60G_4(\tau) = \frac{4}{3}\pi^4(1 + 240\sum\sigma_3(n)q^n)$$

and

$$g_3(\tau) = 140G_6(\tau) = \frac{8}{27}\pi^6(1 - 504\sum\sigma_5(n)q^n).$$

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2 = (2\pi)^{12}\sum_{n\geq 1}\tau(n)q^n$$

where all $\tau(n) \in \mathbb{Z}$ and $\tau(1) = 1$. .

$$j(z) = \frac{1728g_2^3}{\Delta} = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n = \frac{1}{q} + 744 + 196884q + \cdots$$

where all coefficients are integers.

Hence $j(z)$ in in fact a modular function – indeed, j is a meromorphic function on $X(1)$ with a simple pole at the cusp. Hence j induces an isomorphism $X(1) \to \mathbb{CP}^1$.

In particular, this means that

Theorem 22.1. *The field of modular functions for* $SL_2(\mathbb{Z})$ *is equal to* $\mathbb{C}(j(z))$.

22.2 Modular forms for $\Gamma_0(m)$:

$$\Gamma_0(m) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \pmod{m}\}$$

$Y_0(m) = \Gamma_0(m)\backslash\mathbb{H}$.

Last time we constructed a fundamental domain $\mathcal{F}$ for the upper half-plane under the action of $SL_2(\mathbb{Z})$: this means that the translates $\{\gamma\mathcal{F} \mid \gamma \in SL_2(\mathbb{Z})\}$ form a tiling of the hyperbolic plane $\mathbb{H}$. Then, if $SL_2(\mathbb{Z}) = \Gamma_0(m)\gamma_1 \cup \cdots \cup \Gamma_0(m)\gamma_{d_m}$ is a right coset decomposition, $\mathcal{F}_m = \cup_i \gamma_i \mathcal{F}$ is a fundamental domain for $\Gamma_0(m)$.

(e.g. $Y_0(p)$ has index $p+1$ in $SL_2(\mathbb{Z})$, sketch fundamental domain).

Proposition 22.2. $Y_0(m) = \Gamma_0(m)\backslash\mathbb{H}$ *parametrizes pairs of lattices* $L, L' \subset \mathbb{C}$ *where* $L' \subset L$ *is cyclic of index* m*, up to homothety*

Proof. The parametrization is given by $\tau \mapsto [1, \tau], [1, m\tau]$. Easily seen to be well-defined and surjective.

We already know that $SL_2(\mathbb{Z})\backslash\mathbb{H}$ parametrizes lattices L, so it's enough to show that for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$

$$[1, m\tau] \sim [1, m\gamma\tau]$$

($\sim$ denotes homothety) iff $\gamma \in \Gamma_0(m)$.

But

$$[1, m\gamma\tau] = [1, \frac{m(a\tau + b)}{c\tau + d}] \sim [c\tau + d, m(a\tau + b)]$$

and the latter is an index m sublattice of L, so it equals $[1, m\tau]$ if and only if it is contained in $[1, m\tau]$, which happens exactly when $c \equiv 0 \pmod{m}$. □

Compactify $Y_0(m)$ to $X_0(m)$ by adding in points at cusps (there will be multiple cusps now). A modular function for $\Gamma_0(m)$ is a meromorphic function on $X_0(m)$.

Equivalent condition: f is a function on $\mathbb{H}$ with $f(\gamma\tau) = f(\tau)$ for any γ in $\Gamma_0(\tau)$, and also for any $\gamma \in SL_2(\mathbb{Z})$, $f(\gamma(\tau))$ is a Laurent series in $q^{1/m}$.

Of course any modular function for $SL_2(\mathbb{Z})$, e.g. $j(\tau)$ is also a modular function for the subgroup $\Gamma_0(m)$. On the other hand, $j(m\tau)$ is a modular function for $\Gamma_0(m)$, since we've seen that the homothety type of the lattice $[1, m\tau]$ is $\Gamma_0(m)$ invariant.

Observe that $X_0(m)$ is a ramified cover of $X(1)$ with degree equal to (HW!)

$$[SL_2(\mathbb{Z}) : \Gamma_0(m)] = m \prod_{p|m} (1 + \frac{1}{p}).$$

Denote this degree by d_m.

Hence the field of modular functions for $\Gamma_0(m)$ is a degree d_m extension of $\mathbb{C}(j(z))$. In particular, this tell us already that there's some algebraic relation between $j(z)$ and $j(mz)$, of degree at most d_m.

Caution: the covering of curves $X_0(m) \to X(1)$ is not normal, and likewise, the extension of function fields is not Galois.

Proposition 22.3. *$j(\tau)$ and $j(m\tau)$ generate the field of modular functions for $\Gamma_0(m)$.*

Proof. It'll be enough to show that $[\mathbb{C}(j(\tau), j(m\tau)) : \mathbb{C}(j(\tau))] \geq d_m$.

For this, we use the following strategy: if L/K is a field extension (not necessarily Galois), to show $[L : K] \geq d$ it's enough to exhibit a (possibly infinite) extension field E/K and d distinct embeddings $L \hookrightarrow E$ extending the fixed embedding $K \hookrightarrow E$.

In our case, $K = \mathbb{C}(j(\tau))$, $L = \mathbb{C}(j(\tau), j(m\tau))$, and E is the field of meromorphic functions on the upper half plane. We aready have a natural embedding of K into E. Then for any $[\gamma] \in \Gamma_0(m)\backslash SL_2(\mathbb{Z})$, define an embedding $\phi_\gamma : L \hookrightarrow E$ by

$$j(\tau) \mapsto j(\gamma(\tau)) = j(\tau), \quad j(m\tau) \mapsto j(m\gamma\tau).$$

These embeddings are all distinct, (the lattices $[1, m\gamma\tau]$ are generically distinct, so have distinct j-invariants), and the result follows. □

Our agenda here is to construct a minimal polynomial $\Phi_m(X, Y)$ such that $\Phi_m(j(m\tau), j(\tau)) = 0$. This polynomial is known as the *modular polynomial* or *modular equation*.

Note that we must have $\Phi_m(j(m\gamma\tau), j(\tau)) = 0$ for every $\gamma \in SL_2(\mathbb{Z})$.

Let

$$f_m(X, \tau) = \prod_{\gamma \in \Gamma_0(m)\backslash SL_2(\mathbb{Z})} (X - j(m\gamma\tau)) = \prod_{L' \subset [1,\tau] \text{ cyclic index } m} (X - j(L')) \tag{5}$$

This is a polynomial in X whose coeffs are functions of τ. We'll show that actually this can be written as $f_m(X, \tau) = \Phi_m(X, j(\tau))$ with $\Phi_m \in \mathbb{Z}[X, Y]$.

First, observe that $f_m(X, \tau) = f_m(X, \gamma\tau)$ so each coeff of X^i of $f_m(X, \tau)$ is a holomorphic function on $SL_2(\mathbb{Z})\backslash\mathbb{H}$. To show that these coefficients are actually modular functions, we need to show that they can be expressed as power series in $q = e^{2\pi i\tau}$.

We'll work on making our formula for $f_m(X, \tau)$ more explicit, so that we can show that the coefficients of $f_m(X, \tau)$ are not just modular function, but elements of $\mathbb{Z}[j]$.

22.3 Classification of cyclic index m sublattices

Let $L = [1, \tau]$: then any cyclic index m sublattice $L' \subset L$ must have generators of the form $[d, a\tau + b]$ where $ad = m$, $0 \leq b < d$ and $(a, d) = 1$.

In other words: Let $C(m) = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mid ad = m, 0 \leq b < d, (a, b, d) = 1\}$. Then any cyclic index m sublattice of $[1, \tau]$ is homothetic to $[1, \gamma\tau]$ for some $\gamma \in C_m$.

Equivalently, get a classification of cosets $\Gamma_0(m)\backslash \mathrm{SL}_2(\mathbb{Z})$: these are all of the form $\mathrm{SL}_2(\mathbb{Z}) \cap \gamma\sigma_0^{-1}\mathrm{SL}_2(\mathbb{Z})\sigma$, where $\sigma_0 = \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and $\sigma \in C(m)$ is arbitrary.

23 April 26

23.1 Proof that the modular polynomial exists and has integer coefficients

Theorem 23.1. *The function $f_m(X, \tau)$ defined in (5) can be written as $\Phi_m(X, j(\tau))$ where $\Phi_m \in \mathbb{Z}[X, Y]$. Furthermore, Φ_m is irreducible as an element of $\mathbb{C}(Y)[X]$.*

Proof. We've previously observed that the coefficients of $f_m(X, \tau)$ are invariant under the $\mathrm{SL}_2(\mathbb{Z})$ action on $\tau \in \mathbb{H}$. If we also show that they belong to $\mathbb{Z}((q))$, this will say that they are modular functions with integer q-expansions that are holomorphic away from the cusp. Exercise: the ring of such modular functions is precisely $\mathbb{Z}[j(\tau)]$. The theorem will then follow.

Recall

$$f_m(X, \tau) = \prod_{L' \subset [1,\tau] \text{ cyclic index } m} (X - j(L')) = \prod_{\sigma \in C(m)} (X - j(\sigma\tau))$$

so its coefficients are, up to sign, elementary symmetric polynomials in the set $j(\sigma\tau)$.

Let $Q = q^{1/m} = e^{2\pi i\tau/m}$ and $\zeta_m = e^{2\pi i/m}$. For any $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, $e^{2\pi i\sigma\tau} = \zeta_m^{ab} Q^{a^2}$, and so

$$j(\sigma\tau) = \zeta_m^{-ab} Q^{-a^2} + \sum_{k \geq 0} c_k \zeta_m^{abk} Q^{a^2 k}.$$

is a Laurent series in $Q = q^{1/m}$ with integer coefficients. Hence the coefficient of X^i in $f_m(X, \tau)$ is an element of $\mathbb{Z}[\zeta_m]((q^{1/m}))$. However, we also have $f_m(X, \tau) = f_m(X, \tau + 1)$, so this Laurent series must actually belong to $\mathbb{Z}[\zeta_m]((q))$. Additionally, we observe that the set of q-series for $\{j(\sigma\tau) \mid \sigma \in C(m)\}$ is invariant under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, so all coefficients of $f_m(X, \tau)$ actually belong to $\mathbb{Z}((q))$.

Finally, we check irreducibility: We already know that the minimal polynomial of $j(m\tau)$ over the field $\mathbb{C}(j(\tau))$ has degree d_m, so it must be equal to $\Phi_m(X, j(\tau))$ (up to scaling by elements of the field $\mathbb{C}(j(\tau))$. It follows that Φ_m must be irreducible as a polynomial in $\mathbb{C}(Y)[X]$. □

Properties of the modular equation:

Proposition 23.2. *(a)* $\Phi_m(X,Y) = \Phi_m(Y,X)$ *if* $m > 1$

(b) If m *is not a square, then* $\Phi_m(X,X)$ *is a polynomial of degree* > 1 *with leading coefficient* ± 1

(c) If m *is a prime then* $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \pmod{p}$. *(Kronecker congruence).*

Proof. a): the roots of $\Phi_m(j(L),X)$ are the j-invariants of the lattices L' such that L' has a cyclic index m sublattice homothetic to L. However (argue) this is the case iff L has a cyclic index m sublattice homothetic to L'. This shows that $\Phi_m(j(L),X)$ is equal to $\Phi_m(X,j(L)))$ up to a constant factor. Since $j(L)$ can be any complex number, we have that $\Phi_m(Y,X) = c\Phi_m(X,Y)$, and the constant c must be ± 1. But if c were equal to -1, we'd have $\Phi_m(X,X) = 0$ for all X, which is impossible since we know $\Phi_m(j(L),j(L)) \neq 0$ when L doesn't have CM.

b) : Enough to show that if $\Phi_m(j(\tau),j(\tau)) = \sum_{k \geq -N} c_k q^k$ then $c_{-N} = 1$.

Each factor here is

$$j(\tau) - j(\sigma(\tau)) = (Q^{-n} - \zeta^{ab} Q^{-a^2}) + \mathrm{holomorphic}$$

by assumption the leading terms don't cancel, so leading coefficient c_{-N} is a root of unity.

But we also have $c_{-N} \in \mathbb{Z}$ so $c_{-N} = \pm 1$.

c) The set $C(p)$ has the following $p-1$ elements: $\sigma_i = \left(\begin{smallmatrix} 1 & i \\ 0 & p \end{smallmatrix}\right)$ for $i = 0, \ldots, p-1$, and $\sigma_\infty = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

We'll work in $\mathbb{Z}[\zeta_p][X]((Q))$, and show that

$$\overline{\Phi_m(X, j(\tau))} \equiv (j(\tau)^p - X)(X^p - j(\tau)) \pmod{1 - \zeta_p}$$

First, since $e^{2\pi i \sigma_\infty \tau} = Q^{p^2} = q^p$, $j(\sigma_\infty \tau) \equiv j(\tau)^p \bmod 1 - \zeta_p$ by Frobenius.

On the other hand, observe that

$$j(\sigma_i \tau) = \zeta_p^{-i} Q^{-1} + \sum_{k \geq 0} c_k \zeta_m^{ik} Q^k \equiv Q^{-1} + \sum_{k \geq 0} c_k Q^k \pmod{1 - \zeta_p}$$

for $i = 0, \ldots, p-1$.

We now multiply the factors together, and get

$$\Phi_m(X, j(\tau)) \equiv (X - j(\tau)^p)(X - Q^{-1} - \sum_{k \geq 0} c_k Q^k)^p \equiv (X - j(\tau)^p)(X^p - j(\tau)) \pmod{1 - \zeta_p}.$$

Since both sides of this equality have integer coefficients, the equality also holds mod p. Hence the difference of both sides is an element of $p\mathbb{Z}[X]((q)) \cap \mathbb{C}[X, j(\tau)] = \mathbb{Z}[X, j(\tau)]$ and the result follows.

□

Corollary 23.3. *If L has complex multiplication by $\mathcal{O}$, then $j(L)$ is an algebraic integer.*

Proof. We've previously seen that there exists a prime p (in fact, infinitely many such) and a cyclic sublattice L' of L of index p such that L' is homothetic to L.

Hence $\Phi_p(j(L), j(L)) = \Phi_p(j(L'), j(L)) = 0$, but we've just seen that Φ_p has leading coefficient ± 1. □

23.2 The Main Theorem of Complex Multiplication

We now prove

Theorem 23.4 (Main Theorem of Complex multiplication)**.** *If $\mathfrak{a}$ is an invertible ideal of an order $\mathcal{O}$ in a quadratic field K, then $K(j(\mathfrak{a})) = L_{\mathcal{O}}$.*

Proof. Exercise: $L_{\mathcal{O}}$ is Galois over $\mathbb{Q}$. In fact $\mathrm{Gal}(L_{\mathcal{O}}/\mathbb{Q}) \cong \mathrm{Cl}(\mathcal{O}) \rtimes \mathbb{Z}/2\mathbb{Z}$. (Here the nontrivial element $\sigma \in \mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Cl}(\mathcal{O})$ by $\sigma([\mathfrak{a}]) = [\mathfrak{a}^{-1}]$).

Let $M = K(j(\mathfrak{a}))$, and $L = L_{\mathcal{O}}$. First we show that $M \subset L$ by showing that, with finitely many exceptions, any prime of $\mathbb{Q}$ that splits completely in L also splits completely in M.

Exclude the primes p that divide $\mathrm{Disc}\,\mathcal{O}$. Also exclude any primes p such that p divides the index $[\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$.

If p splits completely in $L_{\mathcal{O}}$ then (by HW) $p = N\pi$ where $\pi \in \mathcal{O}$. Then $\pi\mathfrak{a}$ is homothetic to $\mathfrak{a}$, so $j(\mathfrak{a})$ is a root of the polynomial $\Phi_p(X, X)$.

Note that the mod p reduction of $\Phi_p(X, X)$ is $-(X^p - X)^2$. So if $\mathfrak{p}_M$ is any prime of M above p, then $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{p}_M}$. Hence the reduction $\overline{j(\mathfrak{a})} \in \mathcal{O}_M/\mathfrak{p}_M$ actually belongs to $\mathbb{F}_p$.

Because of our assumption that $p \nmid [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$, we know $\mathcal{O}_M/\mathfrak{p}_M$ is generated by $\overline{j(\mathfrak{a})}$, and so $\mathcal{O}_M/\mathfrak{p}_M \cong \mathbb{F}_p$. Since we chose $\mathfrak{p}_M$ over $\mathfrak{p}$ arbitrary, it follows that p splits completely in $K_{\mathfrak{m}}$.

For the other direction: we'll show that, with finitely many exceptions, any prime in $\mathrm{Spl}'(M/\mathbb{Q})$ (that is, any p in $\mathbb{Q}$ with at least one completely split factor in M) is also in $\mathrm{Spl}(L/\mathbb{Q})$. By Problem 1 on Problem Set 10, this implies $L = M$.

Exclude the finite set of primes p dividing $\mathrm{Disc}\,\mathcal{O}$ or sharing a factor with $\prod_{i<j}(j(\mathfrak{a}_i) - j(\mathfrak{a}_j)) \in \mathcal{O}_L$.

If $p \in \mathrm{Spl}'(M/\mathbb{Q})$ then p must split completely in K, write $p = N\mathfrak{p}$. We'll show $\mathfrak{p} \cap \mathcal{O} = \pi\mathcal{O}$ for some π: (assuming p relatively prime to the conductor) this will then imply

$$p = [\mathcal{O}_K : \mathfrak{p}] = [\mathcal{O} : \mathfrak{p} \cap \mathcal{O}] = [\mathcal{O} : \pi\mathcal{O}] = N\pi$$

so $p \in \mathrm{Spl}(L/\mathbb{Q})$.

We'll do the last part next time. □

‘

24 April 29

24.1 Wrapping up the last step in the proof of the main theorem of class field theory

The last thing we need for our proof is: if $p \in \mathrm{Spl}'(M/\mathbb{Q})$ and $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ above p then $\mathfrak{p} \cap \mathcal{O} = \pi\mathcal{O}$, with finitely many exceptions.

For our exceptions: we may assume p does not divide $\mathrm{Disc}\,\mathcal{O}$ and that it is relatively prime to $\prod_{i<j}(j(\mathfrak{a}_i) - j(\mathfrak{a}_j)) \in \mathcal{O}_L$.

By assumption there is a prime $\mathfrak{p}_M$ above $\mathfrak{p}$ such that $\mathcal{O}_M/\mathfrak{p}_M \cong \mathbb{F}_p$.

Now, let $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$. We have that $\mathfrak{a}'$ is a cyclic sublattice of $\mathfrak{a}$ of index p.

Then $\Phi_m(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$. Let $\mathfrak{p}_L$ be any prime of L above $\mathfrak{p}_M$.

Working in $\mathcal{O}_L/\mathfrak{p}_L$ we have

$$(\overline{j(\mathfrak{a}')}^p - \overline{j(\mathfrak{a})})(\overline{j(\mathfrak{a})}^p - \overline{j(\mathfrak{a}')}) = 0$$

so one of the factors equals 0. Since we know that $\overline{j(\mathfrak{a})} \in \mathcal{O}_M/\mathfrak{p}_M \cong \mathbb{F}_p$ is a fixed point of Frobenius, either way we must have $\overline{j(\mathfrak{a})} = \overline{j(\mathfrak{a}')}$.

Hence we conclude that $j(\mathfrak{a})$ and $j(\mathfrak{a}')$ are congruent modulo $\mathfrak{p}_L$. However, by our assumption that $\mathfrak{p}_L \nmid \prod_{i<j}(j(\mathfrak{a}_i) - j(\mathfrak{a}_j))$, this can only happen if $j(\mathfrak{a}) = j(\mathfrak{a}')$.

So $\mathfrak{a}' = \pi\mathfrak{a}$ for some $\pi \in \mathcal{O}$. Since $\mathfrak{a}'$ is an invertible ideal, it follows that $\pi\mathcal{O} = \mathfrak{p} \cap \mathcal{O}$, and we're done.

(Question asked in class: what can we say about the primes that divide $\prod_{i<j}(j(\mathfrak{a}_i) - j(\mathfrak{a}_j))$? I don't know, although there very nice result of Gross and Zagier on the prime factorization of

$$\prod_{\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})} \prod_{\mathfrak{a}' \in \mathrm{Cl}(\mathcal{O}')} (j(\mathfrak{a}) - j(\mathfrak{a}'))$$

when $\mathcal{O}$ and $\mathcal{O}'$ are orders in distinct quadratic fields. In particular, all of the prime factors are small. However this doesn't apply here.)

In fact, one can explicitly describe how $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(\mathcal{O})$ acts on the set $\{j(\mathfrak{a}) \mid \mathfrak{a} \in \mathrm{Cl}(\mathcal{O})\}$:

Theorem 24.1. *For any unramified prime $\mathfrak{p}$ of $\mathcal{O}_K$ relatively prime to the conductor of $\mathcal{O}$,*

$$\mathrm{Frob}_{\mathfrak{p}}((j(\mathfrak{a}))) = j((\overline{\mathfrak{p}} \cap \mathcal{O})\mathfrak{a}).$$

24.2 Heegner's Approach to the Class Number 1 Problem

Now we're going to sketch Heegner's proof of the Class Number 1 Problem (see Cox for details).

Philosophy: A Heegner point on a modular curve $X = \Gamma\backslash\mathbb{H}$ is a point x coming from a lattice with complex multiplication by some order $\mathcal{O}$. In general these points will not be defined over $\mathbb{Q}$, but will be defined over $\bar{\mathbb{Q}}$.

In the case when $X = X(1) = SL_2(\mathbb{Z})\backslash\mathbb{H}$, and $\mathcal{O}$ has class number 1, the unique Heegner point $x_{\mathcal{O}}$ with CM by $\mathcal{O}$ is necessarily a rational point (this is equivalent to our previous statement about $j(\mathcal{O})$ having degree 1 over $\mathbb{Q}$.)

For general X, Heegner points need not be $\mathbb{Q}$-points, but we still get a lot of control over the field of definition of a Heegner point, and in some special cases we can still prove that they are defined over a smaller field than one might naively expect. We'll be able to exploit this to show that Heegner points with class number 1 yield integer solutions to a Diophantine equation of the form $Y^2 =$quartic, which we can then classify.

24.3 The Cube Root of the j-function

Recall $j = \frac{1728g_2^3}{\Delta}$. We can take the cube root to define a new function $\gamma_2 = \frac{12g_2}{\Delta^{1/3}}$: note that Δ is never zero on the upper-half plane, so it has a unique cube root $\Delta^{1/3}$ with q-expansion $\Delta^{1/3} = q^{1/3} + \cdots$.

For general $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, $\gamma_2(\tau)$ and $\gamma_2(\gamma\tau)$ differ by a cube root of unity. Can show that $\gamma_2(\gamma\tau) = \gamma_2(\tau)$ iff $3 \mid b, c$ or $3 \mid a, d$.

It follows from this that $\gamma_2(3\tau)$ is a modular function for $\Gamma_0(9)$, so $\gamma_2(3\tau)$ is a rational function in $j(\tau)$ and $j(9\tau)$.

Theorem 24.2. *Let $\mathcal{O}$ be an order in an imaginary quadratic field, and $3 \nmid D = \mathrm{Disc}(\mathcal{O})$.*

Let $\tau_0 = \sqrt{-m}$ if $D = -4m$ and $\tau_0 = \frac{3+\sqrt{-m}}{2}$ otherwise (importantly, $\gcd(\tau_0, 3) = 1$).

Then $\mathbb{Q}(\gamma_2(\tau_0)) = \mathbb{Q}(j(\tau_0))$.

Proof. Applying the HW (and checking that the appropriate conditions apply) we have that $\gamma_2(\tau_0) \in \mathbb{Q}(j(\tau_0/3), j(3\tau_0))$. Can check that that both $[1, 3\tau_0]$ and $[1, \frac{\tau_0}{3}]$ are invertible ideals of $\mathcal{O}' = \mathbb{Z}[3\tau]$, so $j(\tau_0/3), j(3\tau_0) \in L_{\mathcal{O}'}$. It follows that $\gamma_2(\tau_0) \in L_{\mathcal{O}'}$.

The next step is to show $\gamma_2(\tau_0) \in L_{\mathcal{O}}$. First we compute the degree $[L_{\mathcal{O}'} : L_O]$.

Assuming $\mathcal{O}^\times = \pm 1$ for simplicity, one can show (we skip details),

$$\mathrm{Gal}(L_{\mathcal{O}'}/L_{\mathcal{O}}) = |\ker(\mathrm{Cl}(O') \to \mathrm{Cl}(O))| \cong ((\mathcal{O}/3\mathcal{O})^\times/\mathbb{Z}/3\mathbb{Z}^\times).$$

In particular, the degree is either 2 or 4.

Now, we observe that $[L_{\mathcal{O}}(\gamma_2(\tau_0)) : L_{\mathcal{O}}] \mid 3$ as $\gamma_2(\tau_0)^3 = j(\tau_0) \in L_{\mathcal{O}}$. But also $[L_{\mathcal{O}}(\gamma_2(\tau_0)) : L_{\mathcal{O}}] \mid [L_{\mathcal{O}'} : L_{\mathcal{O}}] \mid 4$. As 3 and 4 are relatively prime, conclude that $\gamma_2(\tau) \in L_{\mathcal{O}}$.

Now, one can check that $\gamma_2(\tau)$ is real, and that $\mathbb{Q}(j_2(\tau)) = L_{\mathcal{O}} \cap \mathbb{R}$. Hence $\mathbb{Q}(\gamma_2(\tau) \subset \mathbb{Q}(j(\tau))$, and the other inclusion is clear. □

24.4 The Weber Functions

We now introduce three more modular functions: $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$ can be defined as power series lying in $\mathbb{Q}((q^{1/48}))$. They are modular functions for $\Gamma(48)$, but we won't use that directly. One can show that $\mathrm{SL}_2(\mathbb{Z})$ fixes the set $\{\mathfrak{f}^{48}, \mathfrak{f}_1^{48}, \mathfrak{f}_2^{48}\}$, and can describe the $\mathrm{SL}_2(\mathbb{Z})$ action on the three functions explicitly.

Important property: $\mathfrak{f}^8, -\mathfrak{f}_1^8, -\mathfrak{f}_2^8$ are roots of $X^3 - \gamma_2 x - 16$.

Useful identities: $\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$ and $\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$.

Important property:

Proposition 24.3. *If $m \equiv 3 \pmod 8$ and $K = \mathbb{Q}(\sqrt{-m})$ then $K(\mathfrak{f}(\sqrt{-m})^2)$ is the ring class field of $\mathcal{O} = \mathbb{Z}[\sqrt{-m}]$ (note that $\mathcal{O}$ is not the full ring of integers).*

Proof. Proof is similar to the previous proposition, but messier: for $\tau_0 = \sqrt{-m}$, use that $\mathfrak{f}(8\tau_0)^6$ is a modular form for $\Gamma_0(64)$.

Ultimately have to do a bit of Galois theory as well as degree counting. □

Theorem 24.4. *Let K be an imaginary quadratic field of discriminant d_K. Then $h(\mathcal{O}_K) = 1$ iff*

$$d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163$$

Proof. Easy cases: if $4 \mid d_K$ then 2 ramifies in $\mathcal{O}_K$, and so $\mathcal{O}_K$ must contain an ideal of norm 2. This ideal can be principal only if $d_K = -4, -8$.

So d_K is odd. By genus theory, $|\mathrm{Cl}(K)[2]| = 2^{n-1}$ where n is the number of prime factors of d_K. Hence we must have $d_K = -p$. May assume $p \neq 3$. If $p \equiv 7 \bmod 8$, then 2 splits in $\mathcal{O}_K$, and so again $\mathcal{O}_K$ must contain a principal ideal of norm 2: only possible if $d_K = -7$.

Left with $d_K = -p = -3 \pmod 8$. We already know that $d_K = -3$ has class number 1, so will assume that $3 \nmid p$.

Let $\mathcal{O} = \mathcal{O}_K$ and $\mathcal{O}' = \mathbb{Z}[\sqrt{-p}]$. By a similar argument to the one sketched above, $\mathrm{Gal}(L_{\mathcal{O}'}/L_{\mathcal{O}}) \cong (\mathcal{O}/2\mathcal{O})^\times/\mathbb{F}_2^\times$ has order 3 (as 2 is inert in $\mathcal{O}_K$). Hence $[L_{\mathcal{O}'} : L_{\mathcal{O}}] = 3$. If K has class number 1, then $L_{\mathcal{O}} = K$, and $[K(j(\sqrt{-p})) : K] = 3$. Taking real subfields, we get that $\mathbb{Q}(j(\sqrt{-p}))$ is a degree 3 extension of $\mathbb{Q}$. Hence $\mathbb{Q}(\mathfrak{f}(\sqrt{-p})^2)$ is a cubic extension of $\mathbb{Q}$.

Let $\tau_0 = \frac{3+\sqrt{-p}}{2}$ and $\alpha = \zeta_8^{-1}\mathfrak{f}_2(\tau_0)^2$.

Using the Weber function identities

$$\frac{\sqrt{2}}{\mathfrak{f}_2(\tau_0)} = \mathfrak{f}_1(2\tau_0) = \mathfrak{f}_1(3 + \sqrt{-p}) = \zeta_{16}^{-1}\mathfrak{f}(\sqrt{-p})$$

One deduces $\alpha = \frac{2}{\mathfrak{f}(\sqrt{-p})^2}$, so α, and also α^4, generate the cubic field $\mathbb{Q}(\mathfrak{f}(\sqrt{-p})^2)$.

What is the minimal polynomial of α^4 over $\mathbb{Q}$?

On the one hand $\alpha^4 = -f_2(\tau_0)^8$, which satisfies

$$x^3 - \gamma_2(\tau)x - 16 = 0.$$

This means that $\gamma_2(\tau)$ is an integer such that a solution to $x^3 - \gamma_2(\tau)x - 16 = 0$. is the fourth power of another element of the same cubic field $\mathbb{Q}(f(\sqrt{-p})^2)$! This is not something that normally happens.

To see what the specific constraint is on γ_2, let $x^3 + ax^2 + bx + c = 0$ be the minimal polynomial of α (which is an algebraic integer because α^4 is).

Then α^2 has minimal polynomial $x^3 + ex^2 + fx + g = 0$ with $e = 2b - a^2$, $f = x^2 - 2ac$, $g = -c^2$ and α^4 has minimal polynomial

$$x^3 + (2f - e^2)x^2 + (f^2 - 2eg)x - g^2.$$

Setting the minimal polyomials equal, get $2f = e^2$, $g^2 = 16$, $f^2 - 2eg = -\gamma_2(\tau_0)$. Deduce $g = -4$, $c = \pm 2$, wlog $c = 2$. Plugging in to $2f = e^2$, we obtain $2(b^2 - 4a) = (2b - a^2)^2$.

Oberving that a and b must be even, and setting $X = -a/2$ and $Y = (b - a^2)/2$, we get the equation $2X(X^3 + 1) = Y^2$.

Standard methods show that this equation only has the roots

$$(X, Y) = (0, 0), (-1, 0), (1, \pm 2), (2, \pm 6).$$

If we then solve for $j(\tau_0)$, we get exactly the j-invariants for

$$d_K = -3, -19, -67, -11, -163, -43$$

respectively. □