Algebraic number theory

Soham

July 2016

1 Day 1

Definition. A *number field* is a finite extension of $\mathbb{Q}$.

Some examples of number fields are:

1. $\mathbb{Q}$
2. $\mathbb{Q}(i)$
3. $\mathbb{Q}(\sqrt{2})$
4. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Note that the last example is not a primitive extension.

Theorem (Primitive element theorem)**.** If $K/\mathbb{Q}$ is a finite extension, then $\exists \alpha \in K$ with $K = \mathbb{Q}(\alpha)$.

1.1 Invariants of a number field

1. $\mathrm{Gal}(K/\mathbb{Q})$
2. $[K : \mathbb{Q}]$
3. ???

Note that our extensions will not always be Galois. We get separability for free since we are working over $\mathbb{Q}$, which has characteristic zero, but we might not have normality.

1.2 The ring of integers

Definition. If $\alpha \in K$, we say that α is an *algebraic integer* if it satisfies a monic polynomial with integer coefficients.

Definition. The (a priori) set of algebraic integers in K is denoted $\mathcal{O}_K$.

Definition. The *discriminant* of a number field is an invariant associated to $\mathcal{O}_K$ that measures how "complicated" or "big" K is.

1.3 Traces and norms

Let L/K be a field extension, and $\beta \in L$. We have a natural map

$$\begin{aligned} m_\beta : & L \to L \\ & x \mapsto \beta x \end{aligned}$$

which is linear, and hence we have maps

$$\mathrm{Tr}_{L/K} : L \to K, \mathrm{Nm}_{L/K} : L \to K$$

corresponding to the trace and the determinant respectively.
Fact: $\mathrm{Nm}_{L/K}(\alpha\beta) = \mathrm{Nm}_{L/K}(\alpha)\mathrm{Nm}_{L/K}(\beta)$
Choose a basis β_i for $\mathcal{O}_K$ (as a $\mathbb{Z}$-module.) The discriminant $\Delta_K = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\beta_i\beta_j))$ is another invariant.

Theorem. Given n, M positive integers, there are finitely many number fields K with $[K : \mathbb{Q}] = n$ with $\Delta_K = M$.

Theorem. If $B \subseteq \mathcal{O}_K$ is a subring, define Δ_B similarly. $\Delta_B \neq 0 \implies B$ has finite index in $\mathcal{O}_K$. Also,

$$\Delta_B = [\mathcal{O}_K : B]^2 \cdot \Delta_K$$

so we can see whether we've "found" the whole ring of integers by looking at whether Δ_B is squarefree, and, if not, we know what index the subgroup we're looking for has.

Theorem (Dirichlet's unit theorem)**.** If K is a number field of signature (r, s), we have that

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$$

where the signature is defined by letting r be

2 Day 2

2.1 The trace pairing

The map

$$\begin{aligned} \mathrm{Tr} : &L \times L \to K \\ &(x, y) \mapsto \mathrm{Tr}_{L/K}(xy) \end{aligned}$$

is bilinear.
Recall that there is a natural map $V \times V^* \to K$ for V a vector space.
Now, with the trace map in hand, we get a map

$$\begin{aligned} &V \to V^* \\ &v \mapsto \mathrm{Tr}(v, \_) \end{aligned}$$

2.2 A legit non-noetherian ring

$\overline{\mathbb{Z}}$ is not noetherian: consider

$$(\sqrt{2}) \subset (\sqrt[4]{2}) \subset (\sqrt[8]{2}) \subset \cdots$$

2.3 Brief digression

Definition. A *Dedekind domain* is an integral domain R such that

1. R is noetherian
2. R is integrally closed (in its field of fractions)
3. every nonzero prime ideal is maximal

Theorem. A discrete valuation ring (henceforth DVR) is a PID with a unique maximal ideal.

Facts:

1. DVRs are Dedekind domains.
2. Guess: You have a valuation from the power of the generator of the maximal ideal dividing an element.

Theorem. If P is a prime ideal and R is a Dedekind domain, R_P is a DVR.

$\mathcal{O}_K$ is a Dedekind domain. Dedekind domains have unique factorization of ideals.

3 Day 3

3.1 Norms of ideals

We want a definition for $\mathrm{Nm}(I)$ for I an ideal of $\mathcal{O}_K$, satisfying the following "common-sense" properties:

1. $\mathrm{Nm}(IJ) = \mathrm{Nm}(I)\mathrm{Nm}(J)$
2. $\mathrm{Nm}(\mathcal{O}_K) = 1$
3. If $\beta \in K$ then $\mathrm{Nm}(\beta) = \mathrm{Nm}((\beta))$

If $p\mathcal{O}_K = P_1^{e_i} \cdots P_g^{e_g}$, we just need to define $\mathrm{Nm}(P_i)$. Note that, with $p \in K$ and $m = [K : \mathbb{Q}]$,

$$\mathrm{Nm}(p) = p^m$$

(the matrix associated to p is just pI_m).
We need $\Pi_{i=1}^g \mathrm{Nm}(P)_i{}^{e_i} = p^m$. Recall Swapnil's postulate

$$\sum_{i=1}^{g} e_i f_i = m$$

which suggests the definition

$$\mathrm{Nm}(P_i) = p^{f_i}$$

or, alternatively,

$$\mathrm{Nm}(I) = [\mathcal{O}_K : I]$$

3.2 Fractional ideals

Definition. A *fractional ideal* in $\mathcal{O}_K$ is a nonzero, finitely generated $\mathcal{O}_K$-submodule of K.

Fact/claim: any fractional ideal has the form $\frac{1}{d}I$ for some $d \in \mathcal{O}_K$ and $I \subseteq \mathcal{O}_K$ an ideal.
For example, $\mathbb{Z} \supset J := \frac{1}{3}(5)$ is fractional, with $J \cdot (3) = (5)$.

Definition (and theorem)**.** The set $\mathrm{Id}(\mathcal{O}_K)$ of fractional ideals of $\mathcal{O}_K$ is a group, freely generated by the prime ideals of $\mathcal{O}_K$.

Definition. A *principal fractional ideal* is one of the form $\alpha\mathcal{O}_K$ for $\alpha \in K^\times$.

Let $\mathrm{Prin}(\mathcal{O}_K)$ denote the subgroup of principal fractional ideals. If I is a fractional ideal, define

$$I^{-1} = \{\alpha \in K : \alpha I \subseteq \mathcal{O}_K\}$$

Definition. The class group of $\mathcal{O}_K$ is

$$\mathrm{Cl}(\mathcal{O}_K) := \mathrm{Id}(\mathcal{O}_K)/\mathrm{Prin}(\mathcal{O}_K).$$

Theorem (Minkowski)**.** There is a set of representatives for the ideal class group consisting of integral ideals I with

$$\mathrm{Nm}(I) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |\Delta_K|^{1/2}$$

Example. $K = \mathbb{Q}(\sqrt{-14})$. The Minkowski bound is

$$\frac{2!}{2^2}\frac{4}{\pi}\sqrt{56} \approx 4.8 < 5$$

4 Day 5

4.1 Hilbert class fields

Let K be a number field with class group $\mathrm{Cl}(K)$, satisfying the following:

- $\mathrm{Gal}(L/K)$ is abelian.
- Every prime $\mathfrak{p}$ in K is unramified in L.

For such an *unramified abelian* extension, we have

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

Moreover, if $H \subseteq \mathrm{Cl}(K)$, then the subfield of L corresponding to H under the Galois correspondence is the one where every ideal in H splits completely.

Example. $K = \mathbb{Q}(\sqrt{-5}), L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$. First note that $\Delta_K = -20$, and (with some more work) that $\Delta_L = -400$. We have that

- $(2) = (2, 1 + \sqrt{-5}) = (\alpha^3 + 2\alpha + 1)^2$
- $(5) = (\sqrt{-5}) = (-\alpha^3 + \alpha^2 - 2\alpha + 2)^2(\alpha^3 + \alpha^2 + 2\alpha + 2)^2$

Notice that we made both ideals principal. This always happens:

Theorem. If $I \subset \mathcal{O}_K$ is an ideal, then $I\mathcal{O}_L$ is principal.

Start with a number field K, and take its Hilbert class field L_0. Then pass to the class field of *that*, L_1. Does this tower ever stabilize?

No: $K = \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13})$ is a counterexample. (Somehow.)

4.2 Moduli

Define

$$\mathfrak{m} = \Pi_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$$

where we think of real and complex embeddings as "infinite primes", and let

$$m(\mathfrak{p}) \geq 0$$
$$m(\text{real embedding}) = 0\text{or}1$$
$$m(\text{complex embedding}) = 0$$

with finitely many exponents nonzero. Now, given $\mathfrak{m}$, let $S(\mathfrak{m}) = \{\mathfrak{p} : m(\mathfrak{p}) > 0\}$.

Let I^S be the product of the ideals not in S.

$$K_{\mathfrak{m},1} = \{\alpha \in K^\times : \alpha \equiv 1 \pmod{\mathfrak{p}^{m(\mathfrak{p})}}, \text{finite } \mathfrak{p}\}$$

where $\alpha_{\mathfrak{p}} > 0$ for infinite $\mathfrak{p} \in \mathfrak{m}$ or something.

Definition. The *ray class group* is defined to be

$$C_m = I^{S(\mathfrak{m})}/K_{\mathfrak{m},1}.$$

We make another definition.

Definition. The *ray class field* is a maximal abelian extension $L_{\mathfrak{m}}/K$ unramified except at places in $S(\mathfrak{m})$.

$K = \mathbb{Q}(\sqrt{6})$. We have an exact sequence

$$0 \to U/U_+ \to K^\times/K_+ \to C_{\mathfrak{m}} \to \mathrm{Cl}(K) \to 0.$$

some stuff here that I don't understand about K having two infinite places and a fundamental unit and $\mathbb{Q}(\sqrt{-2}, \sqrt{-3})$ being the "narrow class field" or something

4.3 Completions

If $\mathfrak{p}$ is a prime ideal, define the completion $K_\mathfrak{p}$ to be the set of Cauchy sequences in K under the $\mathfrak{p}$-adic metric

$$|\alpha|_\mathfrak{p} = \mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p})^{-v_\mathfrak{p}(\alpha)}$$

4.3.1 Directed systems, inverse limits

Let I be a poset and A be a directed I-indexed directed set, with maps $f_{ij} : A_j \to A_i$ (we had a vote on which way the arrow should go).

- $\cdots \to \mathbb{Z}/p^4 \to \mathbb{Z}/p^3 \to \mathbb{Z}/p^2 \to \mathbb{Z}/p$.
- $A_n = \mathbb{Z}/n\mathbb{Z}$, $I = \mathbb{N}_{>0}$ with the partial order being induced by divisibility.
- Let K be an algebraically non-closed field that is not $\overline{K}$. If $M \subseteq L \subseteq \mathbb{Q}$, then $\mathrm{Gal}(L/K)$ includes into $\mathrm{Gal}(M/K)$. In fact, there is an exact sequence

$$0 \to \mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \to 0.$$

Define the projective limit to be

$$\{(a_i)_{i\in I} : f_{ij}(a_j) = a_i \text{ for } i \le j\}.$$

We have

- $\varprojlim \mathbb{Z}/p^n = \mathbb{Z}_p$.
- $\varprojlim \mathbb{Z}/n = \hat{\mathbb{Z}}$.
- We know that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n$ (with the Frobenius as the generator). We get

$$\varprojlim \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}}.$$

Also note that $K_\mathfrak{p} = \mathrm{Frac}(\varprojlim \mathcal{O}_K/\mathfrak{p}^n)$.
If L/K is an extension of number fields, we have an inclusion of groups $L^\times \supset (L^{\mathrm{ab}})^\times \supset K^\times$. As subgroups of $K^\times$,

$$\mathrm{Nm}_{L/K}(L^\times) = \mathrm{Nm}_{L^{\mathrm{ab}}/K}((L^{\mathrm{ab}})^\times)$$

so “norms cannot see nonabelian behavior”.

4.4 Local class field theory

Theorem (Some kind of “main theorem”?)**.** Let K be a p-adic field, that is, a finite extension of $\mathbb{Q}_p$. We have

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) = \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \supset W_K^{\mathrm{ab}} \cong K^\times.$$

Now we switch to K for a number field and $K_\mathfrak{p}$ its completion at $\mathfrak{p}$. (Why is this okay? Because we have

Theorem (Krasner's lemma)**.** Every p-adic field arises in this way.

so it's fine.)
There is an exact sequence

$$0 \to I_{\mathbb{Q}_p} \to \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \to 0$$

corresponding to the tower of fields

$$\overline{K}_\mathfrak{p}/K_\mathfrak{p}^{\mathrm{ab}}/K_\mathfrak{p}.$$

Now, $W_{\mathbb{Q}_p}$ is the preimage of $\mathbb{Z} \subset \hat{\mathbb{Z}}$ in $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.
Abelian extensions of $K_\mathfrak{p}$ are in bijection with finite index subgroups of $K_\mathfrak{p}^\times$, where the map is

$$L \mapsto \mathrm{Nm}_{L/K_\mathfrak{p}}(L^\times)$$

and we have $\mathrm{Gal}(L/K_\mathfrak{p}) \cong K_\mathfrak{p}^\times/\mathrm{Nm}_{L/K_\mathfrak{p}}(L^\times)$.

4.4.1 What are the degree 2 extensions of $\mathbb{Q}_p$?

Using the norm map $\mathbb{Q}_p^\times \to \mathbb{Z}$, we have an exact sequence

$$0 \to \mathbb{Z}_p^\times \to \mathbb{Q}_p^\times \to \mathbb{Z} \to 0.$$

There are at least three:

- The image of $(\mathbb{Z}_p^\times)^2$ in $Q_p^\times$ gives us one.
- The preimage of $2\mathbb{Z}$ gives us another.
- ...

4.5 Galois cohomology

Let $G = \mathrm{Gal}(L/K)$, M be a G-module, that is, a $\mathbb{Z}[G]$-module (so an abelian group with a "sensible" G-action).

We define a sequence of functors (?) H^r, r is a nonnegative integer.

$$H^0(G, M) = M^G = \{m \in M : gm = m \forall g \in G\}.$$
$$H^0(G, L) = K$$
$$H^0(G, L^\times) = K^\times$$

Now suppose that M = "automorphisms of an L-structure".

Morally, $H^1(G, M)$ measures how many "K-structures" there are that become isomorphic to M after base change from K to L. (Tensor with L?)

$$H^1(G, L) = 0$$
$$H^1(G, L^\times) = 0$$

(The second generalizes to $GL_n(L)$.) What does $H^2(G, M)$ measure?

$$H^2(G, L) = 0$$
$$H^2(G, L^\times) = \mathbb{Z}/[L : K]$$

4.6 The Brauer group

In general, we call

$$H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$$

the Brauer group of K, and there is a bijection between the Brauer group and the set of central simple K-algebras up to equivalence.

K p-adic,

$$H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \cong \mathbb{Q}/\mathbb{Z}$$

For K a number field,

$$0 \to H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) \to \bigoplus_{\mathfrak{p} \text{ prime}} H^2(\mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p}), \overline{K_\mathfrak{p}}^\times) \to \mathbb{Q}/\mathbb{Z} \to 0$$

A *quaternion algebra* over a number field K looks like $\mathbb{H}_{a,b}$.

4.7 Cohomology!

Define

$$C^r(G,M) = \{\text{maps } G^r \to M\}$$

and boundary maps

$$d : C^r(G,M) \to C^{r+1}(G,M)$$

defined in such a way that $d^2 = 0$.

Example. a

We get a chain complex

$$\cdots \to C^{r-1}(G,M) \to C^r(G,M) \to C^{r+1}(G,M) \to \cdots$$

and the *group homology* is defined to be

$$H^r(G,M) = \ker d / \operatorname{im} d$$

where we choose d "sensibly", to quote Alfonso.

4.7.1 Another perspective

Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence of G-modules. Applying the "fixed-points" functor, we get

$$0 \to A^G \to B^G \to C^G$$

and this sequence continues to the left using the right derived functors of $\_^G$, which are precisely group cohomology!

$$0 \to A^G \to B^G \to C^G \to H^1(G,A) \to H^1(G,B) \to H^1(G,C) \to H^2(G,A) \to \cdots$$

We also have

$$H^2(G,M) \cong \operatorname{Ext}^1(G,M)$$

so H^2 classifies all Es that fit into exact sequences $0 \to M \to E \to G \to 0$.
There is a cup product map

$$H^r_T(G,M) \times H^s_T(G,N) \to H^{r+s}_T(G, M \otimes N)$$

such that

5 The "difficult" integral

Define

$$\zeta_K(s) = \sum_{I \neq 0} \frac{1}{N(I)^s} = \prod_{\text{prime } P} \frac{1}{1 - N(P)^{-s}}$$

$$L(\chi, s) = \sum_{I \neq 0} \frac{\chi(s)}{N(I)^s} = \prod_{\text{prime } P} \frac{1}{1 - \chi(P)N(P)^{-s}}$$

$$\chi_\infty(\alpha) = \begin{cases} 1 & \text{if } N(\alpha) > 0 \\ -1 & \text{if } N(\alpha) < 0 \end{cases}$$

6 Attempt #1

Let

$$F(a) = \int_0^1 \frac{\log(1+x^a)}{1+x}\,\mathrm{d}x$$

Let's try parts:

$$\begin{aligned} F(a) &= \log(1+x^a)\log(1+x)\big|_0^1 - \int_0^1 \frac{\log(1+x)}{1+x^a} a x^{a-1}\,\mathrm{d}x \\ &= (\log 2)^2 - F(1/a) \end{aligned}$$

so

$$F(a) + F(1/a) = (\log 2)^2$$

Now we expand the integrand of F as a series:

$$\begin{aligned} F(a) &= \int_0^1 \left(\sum_{k=1}^{\infty}(-1)^{k-1}x^{k-1}\right)\left(\sum_{n=1}^{\infty}\frac{(-1)^n x^{na}}{n}\right)\mathrm{d}x \\ &= \int_0^1 \sum_{n,k=1}^{\infty}(-1)^{n+k}\frac{x^{an+k-1}}{n}\,\mathrm{d}x \\ &= \sum_{n,k=1}^{\infty}(-1)^{n+k}\frac{x^{an+k}}{n(an+k)}\,\mathrm{d}x \\ &= \sum_{n,k=1}^{\infty}\frac{(-1)^{n+k}}{n(an+k)}\,\mathrm{d}x \end{aligned}$$

Our integral is $F(w) = F(2+\sqrt{3})$. Note that $\bar{w} = 1/w$, so that

$$F(w) - f(\bar{w}) = \sum_{n,k=1}^{\infty}(-1)^{n+k}\frac{-2\sqrt{3}}{n^2+4nk+k^2}$$