Math 80220 Spring 2018 Notre Dame
Introduction to Algebraic Number Theory
Course Notes

Andrei Jorza

Contents

Lecture 1
2018-01-17

(Thanks to Matt Schoenbauer for today's notes.)

1 Euclidean domains

Definition 1.1. R is a Euclidean Domain if there exists a function $d : R \to \mathbb{Z}_{\geq 0}$ such that

- $d(x) = 0 \iff x = 0$
- For all $a, b \in R \setminus \{0\}$, there exist $q, r \in R$ such that $a = bq + r$ and $d(r) < d(b)$. This is called *division with remainder*. q and r are not necessarily unique.

Example 1.2.

- $\mathbb{Z}$, where $d(x) = |x|$.
- If F is a field, $F[x]$ is a Euclidean Domain if

$$d(P) = \begin{cases} 0 & \text{if } P = 0 \\ 1 + \deg(P) & \text{otherwise} \end{cases}$$

- Some classical examples from Algebra 3:

$$\mathbb{Z}[i] \qquad \mathbb{Z}[\zeta_3] \qquad \mathbb{Z}[\sqrt{2}]$$

Here $\zeta_3 = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. In these three cases, the norm function $N(x)$ supplies a Euclidean function. The norm function $N(x)$ is defined for $x \in \mathbb{Q}(\sqrt{r})$, where r is a square-free integer (with $\sqrt{r} \notin \mathbb{Q}$), by

$$N(u + v\sqrt{r}) = u^2 - rv^2.$$

When $r < 0$ it can be seen that $N(u + v\sqrt{r}) = |u + v\sqrt{r}|^2$ is the square of the usual complex modulus function. When $r > 0$, however, the norm function doesn't measure distance in any meaningful way and takes negative values. Nevertheless, the norm function $N(x)$ is multiplicative, i.e., $N(ab) = N(a)N(b)$, and (since $\sqrt{r} \notin \mathbb{Q}$), $N(x) = 0$ iff $x = 0$.

In the three examples above the Euclidean function is defined as

$$d(x) = |N(x)|.$$

We ask the following question: suppose $r \in \mathbb{Z}$ is square-free with $\sqrt{r} \notin \mathbb{Q}$. Under what circumstances does the norm function yield a Euclidean function $d(x) = |N(x)|$ on $\mathbb{Z}[\sqrt{r}]$? What about on $\mathbb{Z}[\frac{1+\sqrt{r}}{2}]$ when $r \equiv 1 \pmod 4$? It's worth pointing out that even if $|N(x)|$ is not a Euclidean function there might be other Euclidean functions.

First, since $N(x) = 0$ iff $x = 0$ it follows that $d(x) = |N(x)|$ always satisfies the first condition for being a Euclidean function. We replace the second condition with a simpler criterion:

Lemma 1.3. *Suppose r is as above, and let $R = \mathbb{Z}[\sqrt{r}]$ (or $\mathbb{Z}[\frac{1+\sqrt{r}}{2}]$ if $r \equiv 1 \mod 4$). Then $d(x)$ is a Euclidean norm function on R if and only if for all $z \in \mathbb{Q}(\sqrt{r})$ there exists $\alpha \in R$ such that $d(z - \alpha) < 1$.*

Proof. We would like to show that for all $a, b \neq 0$, there exists q and r such that $a = bq + r$ and $d(r) < d(b)$. We have $a/b \in \mathbb{Q}(\sqrt{r})$. Choose α so that $d(a/b - \alpha) < 1$. Then we set $q = \alpha$ and $r = a - b\alpha$. Then clearly $a = bq + r$ and

$$d(r) = d(a - b\alpha) = d(b)d(a/b - \alpha) < d(b)$$

as desired. The converse follows from a similar argument. □

Example 1.4. Let $R = \mathbb{Z}[i]$. The fraction field of R is $\mathbb{Q}[i] \subset \mathbb{C}$. We check with a (geometric) lattice argument that for all $z \in \mathbb{C}$, there exists $\alpha \in \mathbb{Z}[i]$ such that $|z - \alpha| < 1$. In this case $d(z - \alpha) = |z - \alpha|^2 < 1$ as desired. This is the standard proof.

Proposition 1.5. *If $r < 0$, $d(x)$ is a Euclidean norm function on $\mathbb{Z}[\sqrt{r}]$ if and only if $r = -1$ or -2.*

Proof. We will apply Lemma 1.3. Essentially we need to show that only when $r = -1, -2$ we can find, for each $z \in \mathbb{Q}(\sqrt{r}) \subset \mathbb{C}$, a lattice point $\alpha \in \mathbb{Z}[\sqrt{r}]$ of *distance* < 1 to z since in this case $d(z - \alpha) = |z - \alpha|^2 < 1$. Every $z \in \mathbb{C}$ is inside a latticial rectangle with sides 1 and $\sqrt{d}$ and therefore any z inside this rectangle is at most as far away from a vertex as half the diagonal. Therefore we require that $\sqrt{1 + |r|}/2 < 1$, i.e., that $|r| < 3$. □

Proposition 1.6. *Suppose $r < 0$ and $r \equiv 1 \mod 4$. Then $\mathbb{Z}[\frac{1+\sqrt{r}}{2}]$ has $d(x)$ as a Euclidean norm function if and only if $r = -3$, -7, or -11.*

Proof. The proof is the same as before but with a different lattice. Indeed, $\mathbb{Z}[\sqrt{r}] \subset \mathbb{Z}[\frac{1+\sqrt{r}}{2}]$ and the RHS lattice also has the centers of the rectangles in the LHS lattice. As in the previous proposition we seek for each $z \in \mathbb{C}$ a lattice point at most distance 1 away from z, again because when $r < 0$ the norm function is the square of the usual distance in $\mathbb{C}$. Each z is in an isosceles triangle with base 1 and height $\frac{\sqrt{d}}{2}$. In a triangle with circumradius R each point in the interior is at most R distance from some vertex, and in this case $R = \frac{r+1}{4\sqrt{r}}$. Requiring $R < 1$ is equivalent to requiring $r < (2 + \sqrt{3})^2$ and the result follows. □

We now turn our attention to the case $r > 0$. In this case $\mathbb{Q}(\sqrt{r}) \subset \mathbb{R}$ and the norm function no longer has a relation to any meaningful notion of distance. We will apply Lemma 1.3 to inquire when $d(x) = |N(x)|$ is a Euclidean function for $\mathbb{Z}[\sqrt{r}]$ for some positive r.

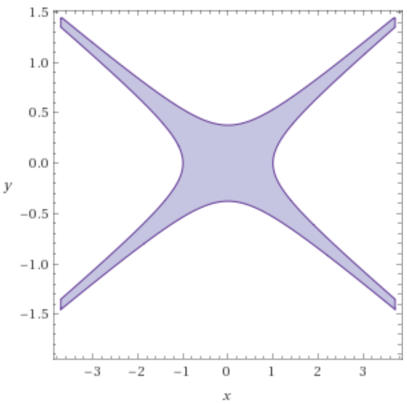
Proposition 1.7. *$\mathbb{Z}[\sqrt{7}]$ is a Euclidean domain with Euclidean norm function $d(x + \sqrt{7}y) = |x^2 - 7y^2|$.*

Proof. We will show that for each $z = x + y\sqrt{r} \in \mathbb{Q}(\sqrt{r})$ there exists a lattice point $\alpha = m + n\sqrt{r} \in \mathbb{Z}[\sqrt{r}]$ such that $d(z - \alpha) < 1$. We will represent z in the xy-plane via the linear map $x + y\sqrt{r} \mapsto (x, y)$, which is an isomorphism $\mathbb{Q}(\sqrt{r}) \cong \mathbb{Q}^2$. Under this isomorphism the lattice $\mathbb{Z}[\sqrt{r}]$ maps to the standard lattice $\mathbb{Z}^2 \subset \mathbb{Q}^2$.

The requirement that for each z there is an α such that $d(z - \alpha) < 1$ is equivalent to the following: if we denote $\mathcal{F}_\alpha = \{z \mid d(z - \alpha) < 1\}$ then

$$\mathbb{Q}(\sqrt{r}) = \bigcup_{\alpha \in \mathbb{Z}[\sqrt{r}]} \mathcal{F}_\alpha.$$

As $\mathbb{Z}[\sqrt{r}] \cong \mathbb{Z}^2$ it suffices to check that the RHS covers the unit square $[0,1] \times [0,1]$. What does $\mathcal{F}_\alpha$ look like? Clearly $\mathcal{F}_\alpha = \alpha + \mathcal{F}_0$ and $\mathcal{F}_0$ looks like:



so it suffices to check that one unit square can be covered by such regions. See the Sage code for today's lecture to see that this can, indeed, be done for $\mathbb{Q}(\sqrt{7})$. $\square$

Lecture 2
2018-01-19

(Thanks to Caitlyn Booms for today's notes.)

Our next example involves a PID which is not a Euclidean domain.

Proposition 1.8. *The ring* $R = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ *is not a Euclidean Domain.*

Proof. We begin with a few facts, whose proofs we'll see later in the course.

(i) R is a PID

(ii) $R^\times = \{\pm 1\}$

(iii) 2 and 3 are irreducible elements in R.

Suppose that R admits a Euclidean Function $d(x)$. Then choose $a \neq 0$, $a \notin R^\times$ such that $d(a)$ is minimal. (For example, if $R = \mathbb{Z}$ and $d(x) = |x|$, then $a = 2$.)

Claim: For every $\alpha \in R$, either $a \mid \alpha$, or $\alpha \equiv \mathit{unit} \mod a$.

Proof of Claim: Use division with remainder to write $\alpha = qa + r$ for some $q, r \in R$ such that $d(r) < d(a)$. Then the minimality of $d(a)$ implies that (r) is not a proper ideal. This gives two cases: if $(r) = 0$, then $a \mid \alpha$, otherwise if $(r) = R$, then $\alpha \equiv \mathit{unit} \mod a$.

Now, consider $\alpha = 2, 3$. By the claim and (ii) above, we have that $\alpha \equiv 0, \pm 1 \mod a$. Then $2 \equiv -1, 0, 1 \mod a$ implies that $a \mid 3, 2, 1$ (but a can't divide 1 since a is not a unit). Similarly, $3 \equiv -1, 0, 1 \mod a$ implies that $a \mid 4, 3, 2$. Since 2 and 3 are irreducible by (iii), we have that $a \mid 2$ or $a \mid 3$. Thus, $a = \pm 2$ or $a = \pm 3$ as R, being a PID, is a UFD. Additionally, if we let $\alpha = \frac{1+\sqrt{-19}}{2} \in R$, we again have $\alpha \equiv -1, 0, 1 \mod a$ which implies that $a \mid \frac{1+\sqrt{-19}}{2} - 1, \frac{1+\sqrt{-19}}{2}, \frac{1+\sqrt{-19}}{2} + 1$. This is a contradiction because 2 and 3 do not divide any of these numbers. Therefore, R is not a Euclidean Domain. $\square$

Example 1.9. $\mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ is a Euclidean Domain, but it is not a norm Euclidean Domain.

Theorem 1.10 (Weinberger, assuming the Generalized Riemann Hypothesis)**.** *Let R be the ring of integers of a finite field extension $K/\mathbb{Q}$. If R is a PID and $|R^\times|$ is infinite, then R is a Euclidean Domain.*

Remark 1. Once we show the Dirichlet unit theorem later in the semester we will be able to show that if R is the ring of integers of a number field then $|R^\times| < \infty$ if and only if $R = \mathbb{Z}$ or $R \subset \mathbb{Q}(\sqrt{r})$ with $r < 0$.

We now recall two important results from algebra, and suggest how we will adapt their proofs to obtain Dedekind's theory of unique factorization in Dedekind domains.

Proposition 1.11. *If R is a Euclidean Domain, then R is a PID.*

Proof. Let I be an ideal of R and let $a \in I$ be such that $d(a) > 0$ is minimal, where d is a Euclidean Function for R. Then $I = (a)$, and thus R is a PID. □

Example 1.12. $\mathbb{Z}[\sqrt{-5}]$ is not a PID as it is not a UFD. For example, $6 \in \mathbb{Z}[\sqrt{-5}]$ can be factored as both $6 = 2 \cdot 3$ and $6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

Proposition 1.13. *If R is a PID, then R is a UFD, i.e. every $a \neq 0$ in R can be written uniquely up to units and permutations as $a = unit \cdot p_1 \cdots p_r$ with each p_i prime.*

Proof. First, we show the existence of such a factorization. To do so, we need to give an algorithm to factorize an element and show that this algorithm always terminates. Pick $a \neq 0$ that is not a unit. Then $(a) \subsetneq R$. Zorn's Lemma implies that (a) is contained in some maximal ideal $\mathfrak{m}$. Since R is a PID, $\mathfrak{m}$ is principal, and in a PID an element is prime if and only if it is irreducible, we must have $\mathfrak{m} = (p_1)$ for some prime p_1. Then $(a) \subset (p_1)$ gives that $a = a_1 \cdot p_1$. Now repeat this process with a_1 to get $a_1 = a_2 \cdot p_2$ with p_2 prime. Continuing this process gives the following ascending chain of ideals in R, $(a) \subset (a_1) \subset (a_2) \subset \cdots$. Then $I = \bigcup_{i=1}^{\infty}(a_i)$ is an ideal of R and so must be principle, i.e. $I = (b)$ for some $b \in R$. Let (a_n) be the first ideal in the ascending chain that contains b. Then we have that $I = (b) = (a_n) = (a_{n+1}) = \cdots$, so the chain stabilizes and our algorithm terminates after n steps.

Remark 2. The key property that we used here is that every ideal of R is generated by a single element, which implies that ascending chains of ideals stabilize. More generally, we will use that every ideal of a Dedekind domain is finitely generated (i.e., that Dedekind domains are Noetherian rings). In fact, rings of integers are generated by only two elements.

Next, we show uniqueness of this factorization. Suppose $a \neq 0$ has two factorizations:

$$a = u \cdot p_1 \cdots p_r = v \cdot q_1 \cdots q_s.$$

We want to show that $\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}$. We prove this by induction on $r + s$. Since p_1 divides the righthand side of the above equation, it must divide some q_i. Say $p_1 \mid q_1$. Then $p_1 = unit \cdot q_1$, and we can now cancel p_1 on both sides of the equation. Then we have $r - 1 + s - 1 < r + s$, so we use the induction hypothesis.

Remark 3. The key properties used here are

1. $p \mid q_1 \cdots q_s$ implies that $p \mid q_i$ for some i, and
2. we can divide by p_1 on both sides.

More generally, we'll show that if R is a ring of integers, then every ideal I of R can be written uniquely up to permutations as $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where each $\mathfrak{p}_i$ is a prime ideal. For example, in $\mathbb{Z}[\sqrt{-5}]$, we have

$$6 = 2 \cdot 3 = (2, 1 + \sqrt{-5}) \cdot (2, 1 - \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$$
$$6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) = (2, 1 + \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) \cdot (2, 1 - \sqrt{-5}) \cdot (3, 1 - \sqrt{-5}).$$

In the general case of Dedekind domains the two properties we used in this theorem will be replaced by

1. If I is an ideal containing a product of prime ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_k$ then I contains some ideal $\mathfrak{p}_i$, and
2. we need to make sense of "inverting a prime ideal". We will do this by developing a theory of **fractional ideals** where inversion is a natural operation.

□

Example 1.14. $\mathbb{Z}[x]$ is a UFD, but it is not a PID.

Lecture 3

2018-01-22

2 Fields and rings of integers

2.1 Number fields

(2.1.1) A field K is a ring such that $K - \{0\} = K^\times$ is the group of invertible elements. If L/K is a finite extension of fields (i.e., $L \supset K$) then $[L : K] = \dim_K L$. If $M/L/K$ are finite extensions then $[M : K] = [M : L][L : K]$.

(2.1.2) An element α is said to be algebraic over K is $P(\alpha) = 0$ for some monic $P \in K[X]$. For α algebraic the field $K(\alpha)$ is the minimal field containing both K and α. Every algebraic α has a minimal polynomial, monic in $K[X]$ obtained as the generator of the (proper) principal ideal in the PID $K[X]$ consisting of all polynomials which vanish at α, in which case $[K(\alpha) : K]$ equals the degree of this minimal polynomial.

Definition 2.1. A number field is defined to be a finite extension of $\mathbb{Q}$.

For any finite extension L/K of fields of characteristic 0 or of finite fields there exists a so-called primitive element $\alpha \in L$ such that $L = K(\alpha)$.

E.g., every quadratic extension L/K, by the quadratic formula, is of the form $L = K(\sqrt{\alpha})$ for some $\alpha \in K$.

(2.1.3) An extension L/K is said to be algebraic if every element of L is algebraic over K.

Fact 1. An element α is algebraic over K if and only if $K(\alpha)/K$ is an algebraic extension if and only if $K(\alpha)/K$ is a finite extension.

As an application we present:

Corollary 2.2. *If α is algebraic of degree d then*

$$K(\alpha) = K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} | a_i \in K\}$$

Proof. The map $K[X] \to K[\alpha]$ given by evaluating a polynomial at α is a ring sujection with kernel $(P(X))$ where P is the minimal polynomial of α over K. Therefore $K[X]/(P(X)) \cong K[\alpha]$. But P has to be irreducible so $(P(X))$ is a maximal ideal and therefore $K[\alpha]$ is a field, thus also equal to $K(\alpha)$. □

Every field K has an algebraic closure $\overline{K}$ which is algebraically closed. If L is any algebraically closed field (such as $\mathbb{C}$) containing K then there is a unique algebraic closure $\overline{K} \subset L$ consisting of all the elements of L which are algebraic over K. This is how we will think of $\overline{\mathbb{Q}}$ as the closure of $\mathbb{Q}$ in $\mathbb{C}$.

(2.1.4) Embeddings. A number field $K/\mathbb{Q}$ can sit inside $\overline{\mathbb{Q}} \subset \mathbb{C}$ in more than one way. For example, $\mathbb{Q}(i) \to \mathbb{C}$ given by $a + bi \mapsto a \pm bi$ provides two distinct embeddings (i.e., injective homomorphisms) of fields which invary $\mathbb{Q}$.

Fact 2. If α is algebraic with minimal polynomial $f(X)$ over K then the embeddings of $K(\alpha)$ into $\overline{K}$ which fix K are parametrized by the roots of $f(X)$. If β is any root the associated embedding fixes K and takes α to β. This produces a unique isomorphism $K(\alpha) \cong K(\beta)$.

Theorem 2.3. *If L/K is finite there are exactly $[L : K]$ embeddings $L \to \overline{K}$ fixing K.*

If $M/L/K$ are finite extensions and α_i are the embeddings of L into $\overline{K}$ fixing K and τ_j are the embeddings of M into $\overline{L} = \overline{K}$ fixing L then the embeddings of M into $\overline{K}$ fixing K are $\sigma_i\tau_j$.

Lecture 4

2018-01-24

2.2 Number Rings

(2.2.1)

Definition 2.4. An algebraic integer is an element α satisfying $P(\alpha) = 0$ for some monic $P \in \mathbb{Z}[X]$. For a number field K we write $\mathcal{O}_K$ for the set of algebraic integers in K.

Recall Gauss' lemma that if $P \in \mathbb{Z}[X]$ is monic and irreducible in $\mathbb{Z}[X]$ then P is irreducible in $\mathbb{Q}[X]$.

(2.2.2)

Proposition 2.5. *An element α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a finite $\mathbb{Z}$-module.*

Proof. Done in class. See textbook Proposition 2.3.4 □

Corollary 2.6. *If α, β are algebraic integers then $\alpha \pm \beta, \alpha \cdot \beta$ are algebraic integers.*

Proof. Done in class. See textbook Proposition 2.3.5 □

The conclusion is that the set $\mathcal{O}_K$ of algebraic integers in the number field K is in fact a ring.

(2.2.3) We have shown that for a number field K the algebraic integers $\mathcal{O}_K$ form a ring.

Definition 2.7. An order is a subring $\mathcal{O} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{O}$ is finite. The ring of integers is said to be the maximal order.

Some examples later.

(2.2.4) Having shown that for a number field K the algebraic integers $\mathcal{O}_K$ form a ring we should answer some natural questions:

1. Is $\mathcal{O}_K$ torsion-free? Of course, since K is.
2. Is $\mathcal{O}_K$ a finite $\mathbb{Z}$-module? We know that every $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ is finite over $\mathbb{Z}$ and the question is whether $\mathcal{O}_K$ is generated by finitely many algebraic integers.
3. A finite $\mathbb{Z}$-module is just a finitely generated abelian group and once we show that $\mathcal{O}_K$ is finite over $\mathbb{Z}$ and torsion-free we deduce that $\mathcal{O}_K \cong \mathbb{Z}^d$ for $d = \operatorname{rank}(\mathcal{O}_K)$. What is this rank?
4. Can we find generators for $\mathcal{O}_K$ as a $\mathbb{Z}$-module?

(2.2.5)

Example 2.8. If m is a square-free integer not equal to 1 then the ring of integers of $\mathbb{Q}(\sqrt{m})$ is $\mathbb{Z}[\sqrt{m}]$ when $m \equiv 2, 3 \pmod 4$ and $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ when $m \equiv 1 \pmod 4$.

Proof. If $a + b\sqrt{m} \in \mathcal{O}_K$ then the minimal polynomial $X^2 - 2aX + a^2 - b^2 m \in \mathbb{Z}[X]$ and so $2a = p \in \mathbb{Z}$. Therefore $p^2 - (2b)^2 m \in 4\mathbb{Z}$ and so $(2b)^2 m$ is an integer. If $2b$ has a denominator, its square would divide the square-free m and so it would have to be 1. Thus $2b = q \in \mathbb{Z}$.

We have $p^2 \equiv q^2 m \pmod 4$. If $m \equiv 2, 3 \pmod 4$ then the only possibility is that p and q are both even as the squares mod 4 are only 0 and 1. This implies that $a, b \in \mathbb{Z}$ and so $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$.

If $m \equiv 1 \pmod 4$ then $p^2 \equiv q^2 \pmod 4$ and so p and q have the same parity is the only relevant condition. Noting that $\frac{1+\sqrt{m}}{2}$ has minimal polynomial $X^2 - X + \frac{1-m}{4} \in \mathbb{Z}[X]$ we deduce that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. □

(2.2.6)

Example 2.9. We have seen above that the ring of integers in $\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ which contains the ring $\mathbb{Z}[\sqrt{5}]$. The quotient has order 2 since any integral element times 2 will be in $\mathbb{Z}[\sqrt{5}]$ and so $\mathbb{Z}[\sqrt{5}]$ is an order in the ring of integers.

(2.2.7) This example leads to a brief exploration of the general setup. If $A \subset B$ are integral domains then $\alpha \in B$ is said to be integral over A if it is the root of a monic polynomial in $A[X]$. The **integral closure** of A in B is the ring (!) of elements of B which are integral over A. (In this language $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.) The ring A is said to be integrally closed in B (or simply integrally closed when B is taken to be $\operatorname{Frac} A$) if it is equal to its integral closure in B.

I gave examples in class in Sage (see the session outputs). For example we saw that $\mathbb{Z}[\sqrt{5}]$ was not integrally closed in $\mathbb{Q}(\sqrt{5})$ which we knew since the ring of integers is larger. Sage also gave us the integral closure of $\mathbb{Z}[\sqrt{5}]$ (implicitly in its fraction field $\mathbb{Q}(\sqrt{5})$ is the whole ring of integers.

That said, there is a geometric perspective on integral elements. Roughly speaking integrally closed rings have few singularities (in codimension 2) and the farther you are from being integrally closed the more singularities you introduce. Here is an explicitly geometric example: The ring $B = \mathbb{C}[t]$ is integrally closed in its fraction field (true of all polynomial rings over fields) and geometrically this ring represents a line. However, the ring $A = \mathbb{C}[t^2, t^3] \subset B = \mathbb{C}[t]$ is not integrally closed because the element $\alpha = t$ is the root of the minimal polynomial $X^2 - t^2 \in A[X]$ but $t \notin A$ as t cannot equal a polynomial of higher degree. What does A represent geometrically? Writing $x = t^2$ and $y = t^3$ produces the equation $y^2 = x^3$ and indeed A represents this cuspidal cubic curve which has a singularity at the origin.

Lecture 5
2018-01-26

2.3 Trace and Norm

(2.3.1)

Definition 2.10. If L/K is a finite extension and σ_i are the embeddings of L into $\overline{K}$ fixing K write

$$\operatorname{Tr}_{L/K}(x) = \sum \sigma_i(x)$$

and

$$N_{L/K}(x) = \prod \sigma_i(x)$$

Fact 3. The maps $\operatorname{Tr}_{L/K}, N_{L/K}$ have image in K. The trace map $\operatorname{Tr}_{L/K} : L \to K$ has the properties that $\operatorname{Tr}_{L/K}(x+y) = \operatorname{Tr}_{L/K}(x) + \operatorname{Tr}_{L/K}(y)$; if $c \in K$ then $\operatorname{Tr}_{L/K}(cx) = c \operatorname{Tr}_{L/K}(x)$; $\operatorname{Tr}_{L/K}(1) = [L : K]$. The norm map $N_{L/K} : L \to K$ has the property that $N_{L/K}(xy) = N_{L/K}(x) N_{L/K}(y)$.

See textbook §2.4.

Example 2.11. If $K = \mathbb{Q}(\sqrt{m})$ then there are exactly two embeddings of K into $\overline{\mathbb{Q}}$ fixing $\mathbb{Q}$, namely $a + b\sqrt{m} \mapsto a \pm b\sqrt{m}$. Thus $\operatorname{Tr}_{K/\mathbb{Q}}(a + b\sqrt{m}) = 2a$ and $N_{K/\mathbb{Q}}(a + b\sqrt{m}) = a^2 - b^2 m$.

(2.3.2)

Proposition 2.12. *If L/K are number fields then* $\operatorname{Tr}_{L/K}, N_{L/K} : \mathcal{O}_L \to \mathcal{O}_K$.

Proof. If α is the root of the monic polynomial $P \in \mathbb{Z}[X]$ and σ is an embedding of L into $\overline{K}$ fixing $K \supset \mathbb{Z}$ it follows that $P(\sigma(\alpha)) = \sigma(P(\alpha)) = \sigma(0) = 0$ and so $\sigma(\alpha)$ is also an algebraic integer. Thus $\operatorname{Tr}_{L/K}(\alpha)$ and $N_{L/K}(\alpha)$ are algebraic integers in K and thus are elements of $\mathcal{O}_K$. □

(2.3.3)

Proposition 2.13. *If $M/L/K$ are number fields then* $\operatorname{Tr}_{M/K} = \operatorname{Tr}_{L/K} \circ \operatorname{Tr}_{M/L}$ *and* $N_{M/K} = N_{L/K} \circ N_{M/L}$.

Proof. Done in class. See textbook Corollary 2.4.4. □

(2.3.4) The trace pairing. Define $(\cdot,\cdot)_{L/K} : L \times L \to K$ by $(x, y)_{L/K} = \operatorname{Tr}_{L/K}(xy)$. It is a K-bilinear form.

Proposition 2.14. *The trace pairing is nondegenerate, i.e., if $(x, y) = 0$ for all y then $x = 0$.*

Proof. Too short to give reference. If $x \neq 0$ then $(x, x^{-1})_{L/K} = \mathrm{Tr}_{L/K}(1) = [L : K] \neq 0$ as number fields have characteristic 0. □

(2.3.5) Discriminants.

Definition 2.15. Suppose L/K is a finite extension of fields. If $\alpha_1, \dots, \alpha_n \in L$ define

$$\mathrm{disc}_{L/K}(\alpha_1, \dots, \alpha_n) = \det((\alpha_i, \alpha_j)_{L/K})_{i,j} \in K$$

Proposition 2.16. *Suppose $[L : K] = n$. Then*

1. $\mathrm{disc}_{L/K}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2_{i,j}$ *where $\sigma_1, \dots, \sigma_n$ are the embeddings $L \to \overline{K}$ fixing K.*
2. $\mathrm{disc}_{L/K}(\alpha_1, \dots, \alpha_n) \neq 0$ *if and only if $\alpha_1, \dots, \alpha_n$ form a basis of L/K.*
3. *If $\alpha_i \in \mathcal{O}_L$ then* $\mathrm{disc}_{L/K}(\alpha_1, \dots, \alpha_n) \in \mathcal{O}_K$.

Proof. Done in class. For part (i) see textbook the first paragraph of §6.2. Part (ii) follows from the fact that the trace pairing is nondegenerate, again at the beginning of §6.2 in the textbook. Finally, if $\alpha_i \in \mathcal{O}_L$ then $(\alpha_i, \alpha_j)_{L/K} \in \mathcal{O}_K$ and so the discriminant is in $\mathcal{O}_K$ since it is the determinant of a matrix with coefficients in $\mathcal{O}_K$. □

(2.3.6) Integral bases. First, recollections on finitely generated abelian groups. If A is a finitely generated abelian group then

$$A \cong \mathbb{Z}^d \oplus \bigoplus \mathbb{Z}/n_i\mathbb{Z}$$

and $d = \mathrm{rank}(A)$ is the rank of A. If B is a finitely generated abelian group and $A \subset B$ is a subgroup then A is also finitely generated and $\mathrm{rank}(A) \leq \mathrm{rank}(B)$.

Theorem 2.17. *Let K be a number field. The following statements are all equivalent and true:*

1. *$\mathcal{O}_K$ is a finite $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.*
2. *$\mathcal{O}_K \subset K$ is a full lattice.*
3. *$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$ where $n = [K : \mathbb{Q}]$. In that case $\alpha_1, \dots, \alpha_n$ is said to be an* **integral basis**.

Proof. Part (ii) is by definition the same as part (i) while part (iii) is part (i) by the theory of finitely generated abelian groups. We will prove part (i).

Pick any basis $\beta_1, \dots, \beta_n$ of $K/\mathbb{Q}$. Since for any $x \in K$ there exists $m \in \mathbb{Z}$ such that $xn \in \mathcal{O}_K$ (if $d_k x^k + d_{k-1}x^{k-1} + \cdots = 0$ then $(d_k x)^k + d_{k-1}(d_k x)^{k-1} + d_{k-2}d_k(d_k x)^{k-2} + \cdots = 0$ and so $d_k x \in \mathcal{O}_K$) we may rescale the β_i such that $\beta_i \in \mathcal{O}_K$.

Suppose $\alpha = \sum r_i \beta_i$ with $r_i \in \mathbb{Q}$. Then $(\alpha, \beta_j)_{K/\mathbb{Q}} = \sum r_i (\beta_i, \beta_j)_{K/\mathbb{Q}}$ which can be rewritten as a matrix multiplication $((\beta_i, \beta_j)_{K/\mathbb{Q}})_{i,j}(r_i) = ((\alpha, \beta_i)_{K/\mathbb{Q}})$. Solving using Cramer's rule shows that r_i is a ratio of a determinant of a matrix with coefficients in $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ by $\det((\beta_i, \beta_j)_{K/\mathbb{Q}})_{i,j} = D = \mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \dots, \beta_n)$. Thus $r_i \in \frac{1}{D}\mathbb{Z}$ which implies that

$$\mathcal{O}_K \subset \sum \frac{\beta_i}{D}\mathbb{Z}$$

and so $\mathcal{O}_K$ is a finitely generated abelian group with $\mathrm{rank}(\mathcal{O}_K) \leq [K : \mathbb{Q}]$. But at the same time

$$\sum \mathbb{Z}\beta_i \subset \mathcal{O}_K$$

and so $n \leq \mathrm{rank}(\mathcal{O}_K)$ and the theorem follows. □

(2.3.7) Discriminant of a number field.

Definition 2.18. Suppose K is a number field and $\alpha_1, \ldots, \alpha_n$ is an integral basis of $\mathcal{O}_K/\mathbb{Z}$. Define

$$\operatorname{disc}(K) = \operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$$

Note that if $\beta_1, \ldots, \beta_n$ is another integral basis then there exists a matrix $B \in \mathrm{GL}(n, \mathbb{Z})$ such that $(\beta_i) = B(\alpha_i)$ and so

$$\operatorname{disc}(\beta_i) = \det(B)^2 \operatorname{disc}(\alpha_i)$$

Since $\det B = \pm 1 \in \mathbb{Z}^\times$ it follows that the above definition is independent of the chosen integral basis.

Example 2.19.

1. The discriminant of $\mathbb{Q}(\sqrt{m})$ is $4m$ if $m \equiv 2, 3 \pmod 4$ and m if $m \equiv 1 \pmod 4$.
2. If $m \equiv 1 \pmod 9$ then the discriminant of $\mathbb{Q}(\sqrt[3]{m})$ (see the first problem set for the ring of integers) is $-3m^2$. Also, see the Sage page on the website for Sage code proving this fact.

(2.3.8)

Proposition 2.20. *Let $p > 2$ be prime. Then the ring of integers of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$. In fact for any positive integer n the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.*

Proof. Only did in class the case of p prime. First, note that $\mathbb{Z}[\zeta_p] = \mathbb{Z}[1 - \zeta_p]$ as a basis of the LHS over $\mathbb{Z}$ is $1, \zeta_p, \ldots, \zeta_{p-2}$ while of the RHS is $1, 1 - \zeta_p, (1 - \zeta_p)^2, \ldots, (1 - \zeta_p)^{p-2}$ and it's clear one can go from the LHS basis to the RHS basis using a lower-triangular matrix with 1-s on the diagonal. This matrix is then invertible in $\mathrm{GL}(p - 1, \mathbb{Z})$ and so the two bases are equivalent.

From one of the problems on problem set 1 you computed that ($K = \mathbb{Q}(\zeta_p)$)

$$\operatorname{disc}_{K/\mathbb{Q}}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{(p-1)/2} p^{p-2}$$

But this discriminant (as shown in class) is independent of a $\mathbb{Z}$-basis and so it is also equal to $D = \operatorname{disc}_{K/\mathbb{Q}}(1, 1 - \zeta_p, (1 - \zeta_p)^2, \ldots, (1 - \zeta_p)^{p-2})$.

We have show in class that if $\alpha = a_0 + a_1(1 - \zeta_p) + \cdots + a_{p-2}(1 - \zeta_p)^{p-2} \in \mathcal{O}_K$ then $Da_i \in \mathbb{Z}$ and so we may write

$$\alpha = \frac{m_0 + m_1(1 - \zeta_p) + \cdots + m_{p-2}(1 - \zeta_p)^{p-2}}{p^{p-2}} \in \mathcal{O}_K$$

If $\alpha \notin \mathbb{Z}[\zeta_p] = \mathbb{Z}[1 - \zeta_p]$ then the coefficients m_i are not all divisible by p^{p-2}. In fact we may cancel out any common factor of p among the m_i and write

$$\alpha = \frac{m_0 + m_1(1 - \zeta_p) + \cdots + m_{p-2}(1 - \zeta_p)^{p-2}}{p^k}$$

where not all m_0 are divisible by p and $k \leq p - 2$. Let i be the smallest index such that $p \nmid m_i$. Then

$$\beta = p^{a-1}\alpha - \frac{m_0 + m_1(1 - \zeta_p) + \cdots + m_{i-1}(1 - \zeta_p)^{i-1}}{p} = \frac{m_i(1 - \zeta_p)^i + \cdots + m_{p-2}(1 - \zeta_p)^{p-2}}{p}$$

is also in $\mathcal{O}_K$ since $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_K$.

Note that $N_{K/\mathbb{Q}}(1 - \zeta_p) = (1 - \zeta_p)(1 - \zeta_p^2) \cdots (1 - \zeta_p^{p-1}) = 1^{p-1} + 1^{p-2} + \cdots + 1 + 1 = p$. Since $1 - \zeta_p \mid 1 - \zeta_p^i$ (here $a \mid b$ means $b/a \in \mathcal{O}_K$) it follows that $(1 - \zeta_p)^{p-1} \mid p$. Now

$$p\beta = m_i(1 - \zeta_p)^i + \cdots + m_{p-2}(1 - \zeta_p)^{p-2}$$

in $\mathcal{O}_K$. If $i < p - 2$ then note that $(1 - \zeta_p)^{i+1} \mid (1 - \zeta_p)^{p-2} \mid p$ and so we deduce that $1 - \zeta_p \mid m_i$. But $1 - \zeta_p \mid p$ and since $p \nmid m_i$ it follows that we can find $u, v \in \mathbb{Z}$ such that $m_i a + pb = 1$ which would imply that $1 - \zeta_p \mid 1$. But then $1/(1 - \zeta_p) \in \mathcal{O}_K$ which is impossible because then $N_{K/\mathbb{Q}}(1/(1 - \zeta_p)) = 1/p$ would be an integer. Thus we get a contradiction. If $i = p - 2$ then $p\beta = m_{p-2}(1 - \zeta_p)^{p-2}$ which would imply that $1 - \zeta_p \mid m_{p-2}$ yielding a contradiction as before.

The conclusion is that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ as desired. □

Lecture 6

2018-01-29

---

3 Dedekind domains

3.1 Noetherian rings

(3.1.1)

Definition 3.1. A ring R is said to be noetherian if every increasing chain of ideals $I_1 \subset I_2 \subset \dots$ stabilizes, i.e., $I_n = I_{n+1} = \cdots$ for $n >> 0$. A module M/R is noetherian if every chain of R-submodules $M_1 \subset M_2 \subset \dots$ stabilizes.

Example 3.2. $\mathbb{Z}$, $F[X]$ are noetherian because ideals are principal. The ring $\overline{\mathbb{Z}}$ is not noetherian because $(2) \subset (2^{1/2}) \subset (2^{1/4}) \subset \dots$ doesn't stabilize.

Fact 4 (Some facts from commutative algebra). 1. Quotients of noetherian rings are noetherian.

2. (Hilbert basis theorem) If R is noetherian then $R[X_1, \dots, X_n]$ is noetherian.

3. The noetherian modules over a noetherian ring are precisely the finitely generated ones.

3.2 Unique factorization in Dedekind domains

(3.2.1)

Definition 3.3. An integral domain R is said to be a Dedekind domain if

1. R is noetherian

2. R is integrally closed (i.e., in its fraction field K)

3. Every prime ideal of R is maximal.

Example 3.4. $\mathbb{Z}$ and $\mathbb{F}_p[X]$ are Dedekind domains. The algebraic integers $\overline{\mathbb{Z}}$ is not because it is not noetherian. The ring $\mathbb{Z}[\sqrt{5}]$ is not because it is not integrally closed. The ring $\mathbb{Z}[X]$ is noetherian and integrally closed but the prime ideal (X) is not maximal because $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ is an integral domain which is not a field. Thus $\mathbb{Z}[X]$ is not a Dedekind domain. Finally, (x) is a prime ideal in $\mathbb{C}[x, y]$ which is not a maximal ideal.

(3.2.2)

Theorem 3.5. *If $K/\mathbb{Q}$ is a number field then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. Done in class. See textbook Proposition 3.1.5. The noetherian property follows from $\mathbb{Z}[\alpha_1, \dots, \alpha_n] \to\to \mathcal{O}_K$ for any integral basis (α_i). □

Lecture 7

2018-01-31

Remark 4. The main use of the noetherian condition is the following. Suppose $\mathcal{P}$ is a set of ideals (defined, say, by having a certain property). If R is noetherian then every ideal in $\mathcal{P}$ is contained in an ideal in $\mathcal{P}$ which is maximal in $\mathcal{P}$, i.e., it is not contained in any bigger ideal in $\mathcal{P}$. Indeed, if $I_1 \subset I_2 \subset \dots$ is a chain of ideals in $\mathcal{P}$ then it stabilizes and the "limit" is necessarily in $\mathcal{P}$. Thus Zorn's lemma implies that every ideal is contained in an ideal of $\mathcal{P}$ which is maximal. We will use this many times.

(3.2.3)

Definition 3.6. If R is an integral domain and K is its fraction field, a **fractional ideal** of R is a finitely generated R-submodule of K.

Note that finite generation implies that if I is a fractional ideal then there exists $\alpha \in R$ such that $\alpha I \subset R$, i.e., is an ideal of R.

Example 3.7. $\frac{m}{n}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$. Similarly $\frac{P(X)}{Q(X)}F[X]$ is a fractional ideal of $F[X]$ where F is any field.

Definition 3.8. We define a multiplication law on fractional ideals given by $IJ = \{\sum x_i y_i | x_i \in I, y_i \in J\}$. Note that $IR = I$ for every fractional ideal I of R. With respect to this multiplication and unit a fractional ideal I is invertible if there exists a fractional ideal I^{-1} such that $II^{-1} = R$.

For example $(\frac{m}{n}\mathbb{Z})^{-1} = \frac{n}{m}\mathbb{Z}$.

(3.2.4) Fractional ideals.

Definition 3.9. Let R be a ring and I, J two ideals. Say that $I \mid J$ if $J \subset I$.

Lemma 3.10. *Let R be a noetherian ring. Then every ideal I of R divides a product of prime ideals.*

Proof. Done in class. See textbook Lemma 3.1.10 which really only uses the noetherian property. □

Theorem 3.11. *If R is a Dedekind domain then every fractional ideal is invertible, i.e., the set of fractional ideals is a group.*

Proof. I did this in three steps.

Step 1: We do this for $I = \mathfrak{p}$ a prime ideal of R.

Step 2: Do this for I an ideal of R.

Step 3: Do this for I a fractional ideal of R. This last step is easy, since there exists $\alpha \in R$ nonzero such that αI is an ideal. Then αI is invertible and $I^{-1} = \alpha(\alpha I)^{-1}$.

Steps 1 and 2 are done in the textbook, proof of Theorem 3.1.8 on page 45 where it's phrased only for rings of integers of number fields but the proof is identical in the case of Dedekind domains. □

A feature of the proof of the above theorem: If $\prod \mathfrak{p}_i \subset \mathfrak{p}_p$ where $\mathfrak{p}$ and $\mathfrak{p}_i$ are prime ideals then $\mathfrak{p} = \mathfrak{p}_i$ for some i.

Lecture 8
2018-02-02

(3.2.5) We are ready for unique factorization in Dedekind domains. For clarity, start with a lemma.

Lemma 3.12. *Suppose R is a Dedekind domain and I, J are fractional ideals. If $I = IJ$ then $J \subset R$.*

Proof. We already did this implicitly in the prood of the fact that every ideal is invertible. Here is a sketch:

The fractional ideal I is finitely generated over $\mathbb{Z}$ and so $I = \oplus\mathbb{Z}\alpha_i$ for some α_i. If $x \in J$ then x acting by multiplication on I (since $I = IJ$) has $x\alpha_i = \sum m_{ij}\alpha_j$ and so multiplication by x on I is the same as multiplication on $\oplus\mathbb{Z}\alpha_i$ by the matrix $(m_{ij}) \in M_{n\times n}(\mathbb{Z})$. Multiplication by x thus satisfies, by Cayley-Hamilton, the characteristic polynomial of (m_{ij}) which is monic in $\mathbb{Z}[X]$ and so x will be integral over $\mathbb{Z}$. But R is integrally closed and so $x \in R$. Thus $J \subset R$. □

Theorem 3.13. *Suppose R is a Dedekind domain. Then every fractional ideal I can be written uniquely (up to permutations) as a product $\prod_i \mathfrak{p}_i^{n_i}$ where $n_i \in \mathbb{Z}$ and $\mathfrak{p}_i$ are prime ideals.*

Proof. This is textbook Theorem 3.1.11

First, note that the case of fractional ideals can be reduced to that of ideals by multiplication. Next, if $\prod \mathfrak{p}_i = \prod \mathfrak{q}_j$ then $\prod \mathfrak{p}_i \subset \mathfrak{q}_j$ for each j. Thus by the observation at the end of the previous lecture it follows that $\mathfrak{p}_i = \mathfrak{q}_j$ for some i. Multiplying $\prod \mathfrak{p}_i = \prod \mathfrak{q}_j$ by the inverse of $\mathfrak{p}_i = \mathfrak{q}_j$ yields an equality of products of prime ideals containing fewer factors in each product. Repeating the argument proves the fact that the prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are permutations of each other.

For existence, if not every ideal is a product of primes ideals then there exists a maximal I which is not a product of prime ideals by the noetherian property. The trivial ideal R is a trivial product of primes and so $I \subset \mathfrak{p} \subset R$ where $\mathfrak{p}$ is some prime ideal (every ideal is contained in a maximal ideal!) Therefore $\mathfrak{p} \mid I$ and so $I\mathfrak{p}^{-1} \subset R$ is an ideal. If $I = I\mathfrak{p}^{-1}$ then the above lemma implies that $\mathfrak{p}^{-1} \subset R$ and of course this would imply that $R \subset \mathfrak{p}$ which is false. Thus $I \subsetneq I\mathfrak{p}^{-1}$ and by maximality of I it follows that $I\mathfrak{p}^{-1}$ is invertible and $I^{-1} = \mathfrak{p}^{-1}(I\mathfrak{p}^{-1})^{-1}$. □

Lecture 9
2018-02-05

(3.2.6) The Chinese Remainder Theorem.

Proposition 3.14. *1. Suppose n_i are pairwise coprime integers and $a_i \in \mathbb{Z}$. Then there exists $a \in \mathbb{Z}$ such that $a \equiv q_i \pmod{n_i}$. Equivalently,*

$$\mathbb{Z}/\prod n_i\mathbb{Z} \cong \prod \mathbb{Z}/n_i\mathbb{Z}$$

2. If R is any commutative ring with unit and I_i are pairwise coprime ideals of R (i.e., if $i \neq j$ then $I_i + I_j = R$), then

$$R/\prod I_i \cong \prod R/I_i$$

Proof. Done in class, see textbook §5.1.1 □

(3.2.7) Generators for fractional ideals in Dedekind domains.

Lemma 3.15. *Suppose R is a Dedekind domain and I, J are two ideals. Then there exists $a \in I$ such that $(a)I^{-1}$ and J are coprime.*

Proof. Done in class, see textbook Lemma 5.2.2. □

Theorem 3.16. *If R is a Dedekind domain then every fractional ideal is generated by 2 elements.*

Proof. It suffices to show this for ideals since fractional ideals are scalar multiples of ideals. Suppose $a \in I$ is nonzero. Then the lemma above implies the existence of $b \in I$ such that $(b)I^{-1}$ and (a) are coprime. Now $a, b \in I$ and so $(a, b) \subset I$ where $(a, b) = (a) + (b)$ is the ideal generated by (a) and (b). Thus $I \mid (a, b)$. If $\mathfrak{p}^n \mid (a, b) \mid (a), (b)$ it follows that $\mathfrak{p}^n \mid (a)$ and $\mathfrak{p}^n \mid (b)$. The ideals (a) and $(b)I^{-1}$ are coprime and so $\mathfrak{p} \nmid (b)I^{-1}$. Thus the power of $\mathfrak{p}$ in (b) equals the power of $\mathfrak{p}$ in I and so $\mathfrak{p}^n \mid I$. Thus $(a, b) \mid I$ and we conclude that $I = (a, b)$ is generated by two elements. □

Lecture 10
2018-02-07

4 Ideals in number fields

4.1 Norms of ideals

(4.1.1)

Definition 4.1. If K is a number field and I is a fractional ideal define $||I|| = [\mathcal{O}_K : I]$.

Example 4.2. Say $K = \mathbb{Q}(\sqrt{-23})$ and $I = (2, (-1 + \sqrt{-23})/2)$. Then $\mathcal{O}_K$ is generated as a module over $\mathbb{Z}$ by 1 and $(1 + \sqrt{-23})/2$ and so I as a $\mathbb{Z}$-module is generated by $2, 1 + \sqrt{-23}, (-1 + \sqrt{-23})/2$ and $(\sqrt{-23} + 23)/2$. Playing with generator you see that I is generated over $\mathbb{Z}$ by 2 and $(-1 + \sqrt{-23})/2$ and so the diagonal matrix $(2, 1)$ takes $\mathcal{O}_K$ to I (with respect to the basis $1, (-1 + \sqrt{-23})/2$ of K over $\mathbb{Q}$) and so $||I|| = 2$.

(4.1.2) If $L \subset \mathbb{R}^n$ is a full rank lattice with integral basis $v_1, \ldots, v_n$ then

$$\operatorname{vol}(\mathbb{R}^n/L) = |\det(v_1, \ldots, v_n)|.$$

As a result, if $L \subset L' \subset \mathbb{R}^n$ are rank n lattices then

$$[L' : L] = \frac{\operatorname{vol}(\mathbb{R}^n/L)}{\operatorname{vol}(\mathbb{R}^n/L')}$$

can be computed using linear algebra.

(4.1.3) To apply this perspective to ideals we need a good vector space to work with. Let K be a number field with r real embeddings $\sigma_1, \ldots, \sigma_r$ and s pairs of complex embeddings $\tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s$, with $r + 2s = n = [K : \mathbb{Q}]$. Together they define an embedding $\iota : K \hookrightarrow \mathbb{R}^n$ by:

$$\iota(x) = (\sigma_1(x), \ldots, \sigma_r(x), \operatorname{Re}\tau_1(x), \operatorname{Im}\tau_1(x), \ldots, \operatorname{Re}\tau_s(x), \operatorname{Im}\tau_s(x)).$$

Lemma 4.3. *Let K be a If I is an ideal of $\mathcal{O}_K$ then*

$$||I|| = \frac{\operatorname{vol}(\mathbb{R}^n/\iota(I))}{\operatorname{vol}(\mathbb{R}^n/\iota(\mathcal{O}_K))},$$

where $\operatorname{vol}(\mathbb{R}^n/\iota(\mathcal{O}_K)) = 2^{-s}\sqrt{|d_K|}$.

Proof. I did this in class. See the textbook Lemma 7.1.7. For the second part the idea is that is $e_1, \ldots, e_n$ is an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$ then

$$\begin{aligned}
\operatorname{vol}(\mathbb{R}^n/\iota(\mathcal{O}_K)) &= |\det(\sigma_1(e_j), \ldots, \sigma_r(e_j), \operatorname{Re}\sigma_{r+1}(e_i), \operatorname{Im}\sigma_{r+1}(e_i), \ldots)| \\
&= 2^{-s}\det(\sigma_1(e_j), \ldots, \sigma_r(e_j), \sigma_{r+1}(e_i), \overline{\sigma}_{r+1}(e_i), \ldots) \\
&= 2^{-s}\sqrt{|\operatorname{disc}(K)|}
\end{aligned}$$

since the discriminant is the square of the matrix of embeddings. □

Proposition 4.4. *Suppose K is a number field.*

1. *If $a \in K$ then $||(a)|| = |N_{K/\mathbb{Q}}(a)|$.*

2. *If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ is the residue field then $\dim_{k_\mathfrak{p}} \mathfrak{p}^m/\mathfrak{p}^{m+1} = 1$ and therefore $|\mathcal{O}_K/\mathfrak{p}^m| = |k_\mathfrak{p}|^m$.*

3. *If I and J are fractional ideals of K then $||IJ|| = ||I||||J||$.*

Proof. Done in class. For (1) see textbook Lemma 6.3.3.. In class I used the previous lemma. For the first part of (2) see textbook Proposition 5.2.4. For the second part, note that in the filtration $\mathcal{O}_K/\mathfrak{p}^n \supset \mathfrak{p}/\mathfrak{p}^n \supset \ldots \supset \mathfrak{p}^{n-1}/\mathfrak{p}^n$ each successive quotient is $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong k_\mathfrak{p}$. Thus $|\mathcal{O}_K/\mathfrak{p}^n| = \prod_{i=0}^{n-1} |\mathfrak{p}^i/\mathfrak{p}^{i+1}| = |k_\mathfrak{p}|^n$.

Part (3) is textbook Proposition 6.3.4. □

Lecture 11
2018-02-09

4.2 The class group

Definition 4.5. Let K be a number field. We already know that the fractional ideals of K from a group. The **class group** $\operatorname{Cl}(K)$ of K is the quotient of the group of fractional ideals by the (normal) subgroup of principal fractional ideals. If K is a number field then the class number is $h_K = |\operatorname{Cl}(K)|$.

From the definition $\mathcal{O}_K$ is a PID if and only if $\mathrm{Cl}(K) = 1$ iff $h_K = 1$.

Proposition 4.6. *The set of ideals $\{I \mid ||I|| \leq X\}$ is finite. Moreover, if $\mathfrak{p}$ is a prime ideal with $||\mathfrak{p}|| = p^k$ where $k_{\mathfrak{p}} = \mathbb{F}_{p^k}$ then $\mathfrak{p} \mid (p)\mathcal{O}_K$.*

Proof. Done in class. By unique factorization is suffices to show the second part of the statement. Since $k_{\mathfrak{p}}$ has characteristic p it follows that $p = 0$ in $\mathcal{O}_K/\mathfrak{p}$ and so $p \in \mathfrak{p}$ which implies $\mathfrak{p} \mid (p)\mathcal{O}_K$. The set of ideals I with $||I|| \leq X$ is then a product of the finitely many prime ideals showing up in the factorization of prime numbers $\leq X$, the exponents being at most $\log_2(X)$. □

Theorem 4.7. *Let K be a number field.*

1. *Suppose there exists $\lambda > 0$ such that for every fractional ideal I there exists $\alpha \in I$ with $|N_{K/\mathbb{Q}}(\alpha)| \leq \lambda||I||$. Then $\mathrm{Cl}(K)$ is finite and is generated by prime ideals dividing $(n)\mathcal{O}_K$ for $n \leq \lambda$.*

2. *Such a λ exists. Indeed if $\alpha_1, \ldots, \alpha_n$ is an integral basis of K then one can take*

$$\lambda = \prod_{\sigma : K \hookrightarrow \mathbb{C}} \sum_i |\sigma(\alpha_i)|.$$

Proof. Part one: First note that if the assumption is satisfied by ideals then it is also satisfied by fractional ideals because we proved before that $||(a)I|| = |N_{K/\mathbb{Q}}(a)|||I||$ and some multiple of a fractional ideal is an ideal.

Let I be any fractional ideal and let $\alpha \in I^{-1}$ be such that $|N_{K/\mathbb{Q}}(\alpha)| \leq \lambda||I^{-1}||$. Then $J = (\alpha)I \subset I^{-1}I = \mathcal{O}_K$ has the property that $||J|| = |N_{K/\mathbb{Q}}(\alpha)|||I|| \leq \lambda||I^{-1}||||I|| = \lambda$. Denoting $[I]$ the image of the fractional ideal I in $\mathrm{Cl}(K)$ it follows that some ideal $J \in [I]$ has the property that $||J|| \leq \lambda$.

The finiteness of $\mathrm{Cl}(K)$ is immediate from the previous Proposition.

Part two: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of $\mathcal{O}_K$ and $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \overline{\mathbb{Q}}$ be the embeddings fixing $\mathbb{Q}$. Then $\lambda = \prod_i \sum_j |\sigma_i(\alpha_j)|$ will work. Indeed, let $m = \lfloor \sqrt[n]{||I||} \rfloor$. The set $\{\sum_{j=1}^n m_j\alpha_j | 0 \leq m_i \leq m\} \subset \mathcal{O}_K$ has $(m+1)^n > ||I||$ elements and so at least two elements must be congruent $\mod I$. Let α be the difference of these two elements in which case $\alpha = \sum k_j\alpha_j$ with $-m \leq k_i \leq m$ and $\alpha \in I$. But then

$$\begin{aligned}
|N_{K/\mathbb{Q}}(\alpha)| &= \prod_i |\sigma_i(\sum k_j\alpha_j)| \\
&\leq \prod_i \sum_j |k_j||\sigma_i(\alpha_j)| \\
&\leq m^n\lambda \\
&\leq \lambda||I||
\end{aligned}$$

□

Remark 5. The explicit value of λ obtained above is effective in that for every K it can be computed but it is inefficient in that it's value can be large.

(4.2.1) We'd like a better constant λ in the previous Theorem. To do this, we use a better pigeonhole principle.

Lemma 4.8. *Suppose $\Lambda \subset \mathbb{R}^n$ is a lattice with fundamental volume* $\mathrm{vol}(\Lambda) := \mathrm{vol}(\mathbb{R}^n/\Lambda)$. *Suppose E is a convex region of $\mathbb{R}^n$ which is symmetric around the origin. If* $\mathrm{vol}(E) > 2^n \mathrm{vol}(\Lambda)$ *then E contains a nonzero element of Λ in its interior.*

Proof. Let F be a fundamental parallelotope of Λ, i.e., the locus $\{\sum x_iv_i | x_i \in [0,1]\}$ for $v_1, \ldots, v_n$ a basis of Λ. Then $\mathrm{vol}(F) = \mathrm{vol}(\mathbb{R}^n/\Lambda)$. Since $\frac{1}{2}E = \bigsqcup_{v \in \Lambda} \frac{1}{2}E \cap (v + F)$ (as translates of F cover $\mathbb{R}^n$). Thus (the first inequality is the hypothesis)

$$\begin{aligned}\operatorname{vol}(F) &< 2^{-n}\operatorname{vol}(E)\\ &= \operatorname{vol}(\frac{1}{2}E)\\ &= \sum_{v\in\Lambda}\operatorname{vol}(\frac{1}{2}E\cap(v+F))\\ &= \sum_{v\in\Lambda}\operatorname{vol}(\frac{1}{2}E-v\cap F)\end{aligned}$$

This implies that at least two of the sets $\frac{1}{2}E-v\cap F$ for $v\in\Lambda$ must overlap. Thus we find $x-u=y-v$ in F with $x,y\in\frac{1}{2}E$ and $u,v\in\Lambda$. As E is symmetric around the origin and convex it follows that the difference $x-y\in E$ but $x-y=u-v$ and so $u-v\in E\cap(\Lambda-\{0\})$ as desired. □

Lecture 12
2018-02-12

(4.2.2) Optimizing the constant λ.

Recall that we seek elements α in ideals I with a bound on their norms. The insight of Minkowski's geometry of numbers is that I, being a finite $\mathbb{Z}$-module, is a lattice and so we seek points in a lattice with a certain property. The "idea" of the geometry of numbers is that if Λ is a lattice in $\mathbb{R}^N$ then a convex region of $\mathbb{R}^N$ should have roughly as many lattice points as the volume of the region, normalized so that the "unit cube" of the lattice has volume 1. This makes intuitive sense in the plane (one can approximate, poorly, π by computing the number of lattice points in circles of big radii) and the previous Lemma formalizes this intuition.

We will use the embedding $\iota : K \hookrightarrow \mathbb{R}^n$ from before. Writing $(x_1,\ldots,x_r,y_1,z_1,\ldots,y_s,z_s)\in\mathbb{R}^n$ we define

$$N(x_i,y_j,z_j)=\prod x_i\prod(y_j^2+z_j^2).$$

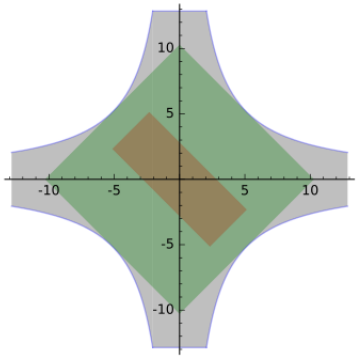
Note that if $x\in K$ then $N(\iota(x))=N_{K/\mathbb{Q}}(x)$.

Since we seek $\alpha\in I-0$ with $|N_{K/\mathbb{Q}}(\alpha)|\le\lambda||I||$ why not simply see $\alpha\in\iota(I)-0$ such that $|N(\alpha)|\le\lambda||I||$, i.e., defining $\mathcal{E}_\lambda=\{v\in\mathbb{R}^n\mid|N(v)|\le\lambda||I||\}$ why not apply the previous lemma to $\mathcal{E}_\lambda$ to show $\mathcal{E}_\lambda\cap(\iota(I)-0)\ne\emptyset$? The reason is that $\mathcal{E}_\lambda$ is not convex.

The previously chosen inefficient value of λ was obtained by, essentially, applying the previous lemma to the parallelepiped

$$\mathcal{B}=\{\sum u_i\alpha_i\mid|u_i|\le\sqrt[n]{||I||}\}.$$

This box, however, is much too small compared to the region $\mathcal{E}_\lambda$ for the same λ. This means that to ensure that $\mathcal{B}\cap\iota(\mathcal{B})-0$ is not empty we need to make λ larger than it should be. For comparison, here are $\mathcal{E}_\lambda$ and $\mathcal{B}$ when $K=\mathbb{Q}(\sqrt{7})$.



Instead, we will focus on an intermediary region E_λ, shaded green in the above diagram. It is convex, symmetric with respect to 0, and it's larger than $\mathcal{B}$ which means we can afford to keep λ smaller and still guarantee that E_λ contains a point in $\iota(I) - 0$.

Define

$$E_\lambda = \{(x_i, y_j, z_j) \mid \sum |x_i| + 2\sum \sqrt{y_j^2 + z_j^2} \leq n\sqrt[n]{\lambda ||I||}\}.$$

Then E_λ is convex, symmetrix with respect to the origin, and by the homework exercise due next Friday, its volume is

$$\operatorname{vol}(E_\lambda) = \frac{2^{r-s}\pi^s n^n \lambda ||I||}{n!}.$$

Moreover, by the AM-GM inequality it follows that $E_\lambda \subset \mathcal{E}_\lambda$.

Theorem 4.9. *If K is a number field with r real and $2s$ complex embeddings then we may choose*

$$\lambda = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$$

Proof. It suffices to show that $E_\lambda \cap \iota(I) - 0 \neq \emptyset$, and for this it's enough to check that $\operatorname{vol}(E_\lambda) \geq 2^n \operatorname{vol}(\mathbb{R}^n/\iota(I))$. In the pigeonhole principle lemma it was necessary to show that $\operatorname{vol}(E_\lambda) > 2^n \operatorname{vol}(\mathbb{R}^n/\iota(I))$, but replacing E_λ by $(1+\varepsilon)E_\lambda$ as $\varepsilon \to 0$ implies that $(1+\varepsilon)E_\lambda \cap \iota(I) - 0 \neq \emptyset$. Since $\iota(I)$ is a lattice it will contain finitely many point in $2E_\lambda$ and if none of them are inside or on the boundary of E_λ we could find $\varepsilon > 0$ small enough such that $(1+\varepsilon)E_\lambda$ doesn't contain any of the finitely many such points.

The result now follows from

$$\begin{aligned}\operatorname{vol}(E_\lambda) &= \frac{2^{r-s}\pi^s n^n ||I||}{n!}\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|} \\ &= 2^{r+s}||I||\sqrt{|\operatorname{disc}(K)|}\end{aligned}$$

and

$$\begin{aligned}\operatorname{vol}(I) &= \operatorname{vol}(\mathbb{R}^n/\iota(I)) \\ &= [\mathcal{O}_K : I]\operatorname{vol}(\mathbb{R}^n/\iota(\mathcal{O}_K)) \\ &= ||I||2^{-s}\sqrt{|\operatorname{disc}(K)|}\end{aligned}$$

recalling that $\operatorname{vol}(\mathbb{R}^n/\iota(\mathcal{O}_K)) = 2^{-s}\sqrt{|\operatorname{disc}(K)|}$.

□

Corollary 4.10. *If K is a number field with $2s$ complex embeddings then*

$$|\operatorname{disc}(K)| \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s$$

In particular if $K \neq \mathbb{Q}$ then $K/\mathbb{Q}$ ramifies at some prime.

Proof. The inequality follows from the fact that the Minkowski bound ≥ 1 or else we would get no ideals at all. If $n = [K : \mathbb{Q}] \geq 2$ then the RHS in the inequality is ≥ 2 and we know that $K/\mathbb{Q}$ ramifies at primes dividing the nonunit discriminant. □

(4.2.3) Computing class groups.

Example 4.11. The class group of $K = \mathbb{Q}(\sqrt{-21})$ is $\operatorname{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Computing the Minkowski bound for K gives $\lambda = 5.8\dots$ and so to find the ideals J (representing the classes in $\mathrm{Cl}(K)$) with $||J|| \leq 5$ it suffices to factor $2, 3, 5$ in $\mathcal{O}_K$. Using the problem from the homework 3, we factor $x^2 + 21 \mod 2, 3, 5$ and get (since $\mathrm{disc}(K) = -2^2 \cdot 3 \cdot 7$)

$$\begin{aligned}(2)\mathcal{O}_K &= (2, 1 + \sqrt{-21})^2\\ (3)\mathcal{O}_K &= (3, \sqrt{-21})^2\\ (5)\mathcal{O}_K &= (5, 2 + \sqrt{-21})(5, 2 - \sqrt{-21})\end{aligned}$$

Let $\mathfrak{q}_2 = (2, 1 + \sqrt{-21})$, $\mathfrak{q}_3 = (3, \sqrt{-21})$ and $\mathfrak{q}_5 = (5, 2 + \sqrt{-21})$. We first check that they are not principal, and only do it for the first ideal. Indeed, if $\mathfrak{q}_2 = (\alpha)$ then $|N_{K/\mathbb{Q}}(\alpha)| = ||\mathfrak{q}_2|| = \sqrt{||(2)\mathcal{O}_K||} = ||(2)\mathbb{Z}|| = 2$ but $\alpha = x + y\sqrt{-21}$ can never have norm 2 (or 3 or 5).

Next, it's quick to see (play around with generators) that $\mathfrak{q}_2\mathfrak{q}_3 = (6, 2\sqrt{-21})$ which again is not principal because it has norm 6 whereas $x^2 + 21y^2$ cannot be 6. Moreover, $\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_5 = (6, 2\sqrt{-21})(5, 2 + \sqrt{-21}) = (30, 3 - \sqrt{-21}) = (3 - \sqrt{-21})$ since $N_{K/\mathbb{Q}}(3 - \sqrt{-21}) = 30$.

Let a, b, c be the images of $\mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_5$ in $\mathrm{Cl}(K)$. Then $a^2 = b^2 = 1$ and $abc = 1$ and $\bar{c}c = 1$. We know that every class in $\mathrm{Cl}(K)$ has an ideal which is a product of prime ideals whose image in $\mathrm{Cl}(K)$ is a product of powers of a, b, c. Since $\bar{c} = c^{-1} = ab$ it follows that the only possibilities are $\{1, a, b, ab\}$ and the result follows.

□

Lecture 13
2018-02-14

4.3 Units

(4.3.1) The purpose of this section is to prove the following theorem of Dirichlet:

Theorem 4.12 (Dirichlet unit theorem)**.** *Suppose K is a number field with r real and $2s$ complex embeddings. Then $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r + s - 1$.*

Remark 6. Note that $\alpha \in \mathcal{O}_K^\times$ iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Example 4.13. $K = \mathbb{Q}(\sqrt{m})$ with $m > 0$. Then $r = 2, s = 0$ and the real quadratic field K has rank 1 unit group. E.g., $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}^\times = \pm(2 + \sqrt{3})^{\mathbb{Z}}$.

Example 4.14. $K = \mathbb{Q}(\sqrt{m})$ with $m < 0$. Then $r = 0, s = 1$ and the imaginary quadratic number field K has finite unit group. E.g., $\mathcal{O}_{\mathbb{Q}(\zeta_3)}^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$.

Example 4.15. $K = \mathbb{Q}(\sqrt[3]{2})$ has $r = 1, s = 1$ and so $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}^\times$ has rank 1. It turns out $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}^\times = \pm(\sqrt[3]{2} - 1)^{\mathbb{Z}}$.

Example 4.16. For a more complicated example, take $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Then $\mathcal{O}_K^\times$ has rank 3 and in fact

$$\mathcal{O}_K^\times = \pm\left(\frac{1 + \sqrt{5}}{2}\right)^{\mathbb{Z}}\left(\frac{1 + \sqrt{5}}{2} - \sqrt{3}\right)^{\mathbb{Z}}\left(\frac{1 + \sqrt{5}}{2} - \sqrt{3} - 1\right)^{\mathbb{Z}}$$

Example 4.17. $K = \mathbb{Q}(\zeta_{p^n})$ for p a prime. Then K is a quadratic extension of the real subfield $K^+ = \mathbb{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1}) = \mathbb{Q}(\cos(2\pi/p^n))$. All the embeddings of K^+ are real and $K = K^+(i\sin(2\pi/p^n))$ and so all the $p^{n-1}(p-1)$ embeddings of K are complex. Thus $s = p^{n-1}(p-1)/2$ but we can no longer describe the s generators of $\mathcal{O}_K^\times$ explicitly. However, we can say that $\mathcal{O}_K^\times$ has a finite index subgroup generated (as a group) by ζ_{p^n} and $\zeta_{p^n}^{\frac{1-a}{2}}\dfrac{1 - \zeta_{p^n}^a}{1 - \zeta_{p^n}} = \pm\dfrac{\sin(\pi a/p^n)}{\sin(\pi/p^n)}$ for $1 < a < p^n/2$ coprime to p.

Remark 7. If $K/\mathbb{Q}$ is Galois then either $r = 0$ or $s = 0$ as the Galois group acts transitively (and in fact can be identified with) the set of embeddings into $\mathbb{C}$.

(4.3.2) To understand the class group of K we used the embedding $\iota : K \to \mathbb{R}^n$ taking $\mathcal{O}_K$ to the lattice Λ and we implicitly used that this embedding was additive. To study $\mathcal{O}_K^\times$ we would like to transform the unpleasant multiplicative on $\mathcal{O}_K^\times$ to a much more usable additive structure on a vector space.

Consider the map $\log : \mathbb{R}^n \to \mathbb{R}^{r+s}$ given by

$$\log((x_1, \ldots, x_{r+2s})) = (\log|x_1|, \ldots, \log|x_r|, \log(x_{r+1}^2 + x_{r+2}^2), \ldots)$$

and $\sum : \mathbb{R}^{r+s} \to \mathbb{R}$ given by $\sum(x_1, \ldots, x_{r+s}) = x_1 + \cdots + x_{r+s}$.

Lemma 4.18. *1. The composite map $\log \circ \iota : K^\times \to \mathbb{R}^n$ is additive, i.e., $\log(\iota(xy)) = \log(\iota(x)) + \log(\iota(y))$.*

2. The image of $\mathcal{O}_K^\times$ lies in a hyperplane: $\log(\iota(\mathcal{O}_K^\times)) \subset \Delta$ where $\Delta = \{(x_1, \ldots, x_{r+s}) | x_1 + \cdots + x_{r+s} = 0\}$.

3. The additive subgroup $\log(\iota(\mathcal{O}_K^\times)) \subset \Delta$ is a discrete abelian subgroup and thus a lattice of rank $d \leq \operatorname{rank}(\Delta) = r + s - 1$.

Lemma 4.19. *Part one follows from the definition. Part two uses the fact that $\alpha \in \mathcal{O}_K^\times$ iff $|N_{K/\mathbb{Q}}(\alpha)| = 1$ and $\sum \log(\iota(\alpha)) = \log|N_{K/\mathbb{Q}}(\alpha)|$. For part three: the preimage under $\log$ of any open subset of Δ is an open subset of $\mathbb{R}^n$ which contains finitely many $\iota(\alpha)$ for $\alpha \in \mathcal{O}_K^\times$ as $\iota(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$.*

(4.3.3) $\mathcal{O}_K^\times$ vs $\log \iota(\mathcal{O}_K^\times)$.

Proposition 4.20. *The kernel of $\log \circ \iota|_{\mathcal{O}_K - 0}$ consists of the roots of unity in K and is finite. Thus $\mathcal{O}_K^\times$ is a finitely generated abelian group of the same rank as $\log \iota(\mathcal{O}_K^\times)$.*

Proof. If $\alpha \in \mathcal{O}_K - 0$ has $\log \iota(\alpha) = 0$ then $|\sigma(\alpha)| = 1$ for all embeddings $\sigma : K \hookrightarrow \mathbb{C}$. The minimal polynomial of α is $P_\alpha(X) = \prod(X - \sigma(\alpha)) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ and

$$|a_{n-j}| = |\sum_{i_1 < \ldots < i_j} \sigma_{i_1}(\alpha) \cdots \sigma_{i_j}(\alpha)| \leq \sum_{i_1 < \ldots < i_j} 1 = \binom{n}{j}$$

and so $P_\alpha(X)$ is in the finite set $\mathcal{F} = \{X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X] | |a_{n-j} \leq \binom{n}{j}\}$. But the same is true of P_{α^k} for all k since the Galois conjugates of α^k are α_i^k. Thus P_{α^k} is in the same set. Since there are infinitely many choices for k it follows that $\alpha^k = \alpha^{k'}$ for at least two $k \neq k'$ and thus α is a root of unity.

If $\zeta_n \in K$ then $\mathbb{Q}(\zeta_n) \subset K$ and so $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq [K : \mathbb{Q}]$ which puts a bound on n and so K contains finitely many roots of unity.

Therefore $\log \iota(\mathcal{O}_K^\times) \cong \mathcal{O}_K^\times / \mu(K)$ where $\mu(K)$ is the finite group of roots of unity in K and the conclusion follows. □

Lecture 14

2018-02-16

(4.3.4) Proof of the Dirichlet unit theorem.

Lemma 4.21. *1. There exists a constant λ (in fact $\lambda = \log\left(2^s \pi^{-s} \sqrt{|\operatorname{disc}(K)|}\right)$) such that for any index k between 1 and $r + s$ and any $\alpha = (a_1, \ldots, a_{r+s}) \in \log \iota(\mathcal{O}_K - 0)$ there exists $\beta = (b_1, \ldots, b_{r+s}) \in \log \iota(\mathcal{O}_K^\times - 0)$ with $\sum \beta < \lambda$ and $b_i < a_i$ for all $i \neq k$.*

2. For any index k there exists $\alpha = (u_1, \ldots, u_{r+s}) \in \log \iota \mathcal{O}_K^\times$ such that $u_i < 0$ when $i \neq k$.

Proof. Part one follows from a geometry of numbers type argument. Here's a sketch: choose c_i such that $c_i < \exp(a_i)$ for $i \neq k$ and choose c_k such that $\prod c_i = \exp(\lambda)$. Then finding β as desired is equivalent to finding $x = (x_1, \ldots, x_n) \in \iota(\mathcal{O}_K - 0)$ such that $|x_i| < c_i$ for $i \leq r$ and $x_{r+2i-1}^2 + x_{r+2i}^2 < c_{r+i}$ for $i > 0$. The geometry of numbers requires only that the volume of this region be $> 2^n \operatorname{vol}(\iota(\mathcal{O}_K))$ and the volume can be shown to depend only on λ. For example, if $K = \mathbb{Q}(\sqrt{m})$, $m > 0$ then $\mathbb{R}^n = \mathbb{R}^{r+s} = \mathbb{R}^2$ and the region $|x_i| \leq c_i$ with $c_1 \exp(a_1)$ and $c_1 c_2 = \exp(\lambda)$ has area $4c_1c_2 = 4\exp(\lambda)$.

Part two: part one allows us to construct a sequence $\alpha_m = (a_{m,1}, \ldots, a_{m,r+s}) \ni \log\iota(\mathcal{O}_K - 0)$ with $(a_{m,i})_m$ decreasing for $i \neq k$ and $\sum \alpha_m < \lambda$. Consider the $\sum$ map $\sum : \log\iota(\mathcal{O}_K - 0) \to \mathbb{R}$ taking $\log\iota(\alpha)$ to $\log |N_{K/\mathbb{Q}}(\alpha)|$. If $B > 0$ then $\sum \log\iota(\alpha) \leq B$ implies $|N_{K/\mathbb{Q}}(\alpha)| \leq \exp(B)$ and so $N_{K/\mathbb{Q}}(\alpha)$ takes finitely many integral values (between $-\exp(B)$ and $\exp(B)$). Using the observation with $B = \lambda$ it follows that if $\alpha_m = \log\iota(u_m)$ for $u_m \in \mathcal{O}_K - 0$ then $|N_{K/\mathbb{Q}}(u_m)| \leq \exp(\lambda)$ for all m. By the pigeonhole principle there exist infinitely many indices m such that $|N_{K/\mathbb{Q}}(u_m)| = B$ for some B, which implies that $||(u_m)|| = B$. Since there are finitely many ideals of a particular bound it follows that (u_m) are the same ideal so for two different such indices m and m' we have $u_m = uu_{m'}$ for some $u \in \mathcal{O}_K^\times$. In other words $\alpha_m = \log\iota(u) + \alpha_{m'}$ for $m \neq m'$ for some unit $u \in \mathcal{O}_K^\times$ and the condition on u follows from the fact that the coordinates of α_m are decreasing for $i \neq k$. □

Proof of the Dirichlet Unit Theorem. It suffices to show that $\mathcal{O}_K^\times$ has rank at least $r + s - 1$. The previous lemma guarantees the existence of units u_k such that $\log\iota(u_k)$ have negative coordinates except in index k. Since $\sum \log\iota(u_k) = 0$ it follows that the k-th coordinate of $\log\iota(u_k)$ must be > 0.

Consider the matrix $(u_{i,j})$ where $\log\iota(u_i) = (u_{i,1}, \ldots, u_{i,r+s})$. To show that $\operatorname{rank} \mathcal{O}_K^\times = r+s-1$ it suffices to show that $r + s - 1$ of the $\log\iota(u_k)$ are linearly independent, i.e., the rank of this matrix is $\geq r + s - 1$.

Suppose the rank is $< r + s - 1$ in which case we may assume that there exist $t_1, t_2, \ldots, t_{r+s-s}$ such that $\sum_{j=1}^{r+s-1} t_j u_{i,j} = 0$ for all i. We may assume that the largest coefficient $t_k > 0$. Then

$$\begin{aligned} 0 &= \sum_{j=1}^{r+s-1} t_j u_{k,j} \\ &= t_k u_{k,k} + \sum_{j\neq k, 1\leq j\leq r+s-1} t_j u_{k,j} \\ &\geq t_k u_{k,k} + \sum_{j\neq k, 1\leq j\leq r+s-1} t_k u_{k,j} \\ &= t_k \sum_{j=1}^{r+s-1} u_{k,j} \\ &= -t_k u_{k,r+s} \end{aligned}$$

since $u_{k,j} < 0$ when $j \neq k$ and $\sum_{j=1}^{r+s} u_{k,j} = 0$ for all k. This of course is not possible since $t_k > 0$ and $u_{k,r+s} < 0$ as $k < r + s$. □

Lecture 15
2018-02-19

4.4 S-integers and S-units

No notes for today. If S is a finite set of nonzero prime ideals of K we defined

$$\mathcal{O}_S = \{x \in K \mid v_\mathfrak{p}(x) \geq 0, \forall \mathfrak{p} \notin S\}.$$

I remarked that $\mathcal{O}_S$ is a Dedekind domain as it appears as a localization in commutative algebra. Moreover, $\operatorname{Div}(\mathcal{O}_S)$ is the free abelian group on $\operatorname{Spec}(\mathcal{O}_S) = \operatorname{Spec}(\mathcal{O}_K) - S$, which implies that $\operatorname{Cl}_S(K)$ is a quotient of $\operatorname{Cl}(K)$.

I also showed that $\iota_S : \mathcal{O}_S \hookrightarrow \mathbb{R}^{n+|S|}$ given by $\iota_S(x) = (\sigma_i(x), \operatorname{Re}\tau_j(x), \operatorname{Im}\tau_j(x), ||\mathfrak{p}||^{-v_\mathfrak{p}(x)})$, where $\mathfrak{p} \in S$ gives a discrete embedding of $\mathcal{O}_S$ into $\mathbb{R}^{n+|S|}$.

Furthermore, writing $N_S(x) = N_{K/\mathbb{Q}}(x) \prod_{\mathfrak{p}\in S} ||\mathfrak{p}||^{-v_\mathfrak{p}(x)}$ is an integer for $x \in \mathcal{O}_S$. If $x \in \mathcal{O}_S$ then $x \in \mathcal{O}_S^\times$ iff $|N_S(x)| = 1$ and therefore if we look at $\operatorname{Log}_S : \mathbb{R}^{n+|S|} \to \mathbb{R}^{r+s+|S|}$ given by

$$\operatorname{Log}_S(x_i, y_j, z_j, t_\mathfrak{p}) = (\log|x_i|, \log(y_j^2 + z_j^2), \log|t_\mathfrak{p}|)$$

we see that $\operatorname{Log}_S \mathcal{O}_S^\times$ is a discrete sublattice of $\ker \sum : \mathbb{R}^{r+s+|S|} \to \mathbb{R}$. We concluded that $\mathcal{O}_S^\times$ is a lattice of rank at most $\operatorname{rk} \mathcal{O}_K^\times + |S|$. To show that in fact $\mathcal{O}_S^\times$ has exactly this rank we will introduce the modern language of algebraic number theory.

Lecture 16
2018-02-21

(Notes by Matt Schoenbauer)

5 Adeles and p-adics

5.1 p-adic completions

If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, we define a map

$$v = v_{\mathfrak{p}} : K^\times \to \mathbb{Z}$$

by $v_{\mathfrak{p}}(x) =$ the power of $\mathfrak{p}$ in $(x)\mathcal{O}_K$. We also set $|x|_{v_{\mathfrak{p}}} = ||\mathfrak{p}||^{-v_{\mathfrak{p}}(x)}$. If $\sigma : K \to \mathbb{R}$ is a real embedding, we define

$$|x|_\sigma = |\sigma(x)|$$

where $|\cdot|$ is the absolute value on $\mathbb{R}$. If $\tau : K \to \mathbb{C}$ is a complex embedding, we define

$$|x|_\tau = |\tau(x)|$$

where $|\cdot|$ is the norm on $\mathbb{C}$.

Lemma 5.1.

1. *$|\cdot|_\sigma$ and $|\cdot|_\tau$ are multiplicative.*
2. *$|\cdot|_\sigma$ and $|\cdot|_\tau$ satisfy the triangle inequality.*
3. *If $\mathfrak{p}$ is a prime ideal, and $v = v_{\mathfrak{p}}$, then*

$$|x+y|_v \geq \min\{|x|_v, |y|_b\}$$

where equality holds if $|x|_v \neq |y|_v$.

Proof.

1. Since σ and τ are norms, $|\cdot|_\sigma$ and $|\cdot|_\tau$ are multiplicative.
2. This is clear.
3. By (a), we can reduce to the case $x, y \in \mathcal{O}_K$. If $\mathfrak{p}^n$ divides (x) and (y), then $\mathfrak{p}^n$ divides $(x+y)$. This gives $v(x,y) \geq \min(|x|_v, |y|_v)$, which implies the desired inequality. Now suppose $|x|_v > |y|_v$, which is equivalent to $v(x) < v(g)$. If $v(x+y)$, then

$$v(x) = v(x+y-y) \geq \min\{v(x+y), v(-y)\}.$$

$v(-y) > v(x)$, so that the last term in the above equation is just $v(x+y)$. But we already have

$$v(x+y) \geq \min\{v(x), v(y)\} = v(x)$$

so that equality holds.

□

Terminology:

- A *place* of K is either a real embedding or a pair of complex embeddings on a nonzero prime ideal.

- Places are often denoted by $u, v, w, \dots$ etc.
- $v|\infty$ means v is real or complex.
- $v|\mathbb{R}$ means v is real.
- $v|\mathbb{C}$ means v is complex.
- $v \nmid \infty$ for prime ideals.

We then get a norm function $|\cdot|_v : K \to [0, \infty)$ where $|x|_v = 0$ if and only if $x = 0$.

$$|x|_{v_\mathfrak{p}} = 0 \implies ||\mathfrak{p}||^{-v_\mathfrak{p}(x)} = 0 \implies v_\mathfrak{p}(x) = \infty$$

Definition 5.2. If v is a place of K, then K_v is a metric space completion of $(K, |\cdot|_v)$. The elements of K_v are equivalence classes of Cauchy sequences in K.

Example 5.3. If $v|\mathbb{R}$, we have $\mathbb{Q} \subseteq \sigma(K) \subseteq \mathbb{R}$, which implies $\mathbb{R} = K_v$, since $\overline{\mathbb{Q}} \subseteq \overline{\sigma(K)} \subseteq \mathbb{R}$. If $v|\mathbb{C}$ corresponds to $K \xrightarrow{\tau} \mathbb{C}$, then $\tau(K)$ is dense in $\mathbb{C}$, i.e. $K_v = \mathbb{C}$. This is true since $\mathbb{Q} \subsetneq \tau(K)$ and there is $\alpha \in K \cap (\mathbb{C} \setminus \mathbb{R})$, so that

$$\mathbb{C} = \overline{\mathbb{Q} + \alpha\mathbb{Q}} \subseteq K_v \subseteq \mathbb{C}$$

Terminology: $v|\infty$ is called archimedean or infinite. $v \nmid \infty$ is called nonarchimedean or finite.

Our goal is to understand K_v.

Proposition 5.4. *Suppose $v = v_\mathfrak{p} \nmid \infty$.*

1. *Let $(x_n) \in K$ be a Cauchy sequence. Then*

$$\big|\lim_{n\to\infty} x_n\big|_v = \lim_{n\to\infty} |x_n|_v$$

From this it follows that $|\cdot|_v : K_v^\times \to ||p||^\mathbb{Z}$.

2. *If $x \in K_v$, then $|x|_v = 0$ if and only if $x = 0$.*
3. *K_v is a field. It will be a homework exercise to show that K_v is a topological field.*
4. *Let $\mathcal{O}_v \subseteq K_v$ be given by $\mathcal{O}_v = \{x \in K_v \mid x \in K_v \mid |x|_v \leq 1\}$. Then $\mathcal{O}_v$ is a subring with a unique maximal ideal $m_v = \{x \in K_v \mid |x|_v < 1\}$.*
5. *m_v is a principal ideal.*

Proof. 1.

$$\big|\lim_{n\to\infty} (x_n - 0)\big| = \lim_{n\to\infty} |x_n - 0|$$

by the definition of metric space completions. Now $|x_n| \in ||\mathfrak{p}||^\mathbb{Z}$ if $x_n \neq 0 \in K$:

$$\lim_{n\to\infty} |x_n| \in ||\mathfrak{p}||^\mathbb{Z}$$

which implies

$$|\lim_{n\to\infty} x_n| \in ||\mathfrak{p}||^\mathbb{Z}$$

($\lim_{n\to\infty} x_n \in K$).

2.

$$|x|_v = 0 \iff |x - 0|_v = 0 \iff \mathrm{dist}(x, 0) = 0 \iff x = 0$$

3. Let $x \in K_v \setminus \{0\}$. We need to show that $\frac{1}{x} \in K_v$. Let $x = \lim x_n$, where each $x_n \in K$. Since $x \neq 0$, we have $|x|_v \neq 0$. Now

$$|x_n|_v = \lim_{n\to\infty} |x_n|_v$$

Therefore we can assume that each $|x_n|_v \neq 0$, so that each $x_n \neq 0$. Thus $1/x_n \in K$. We show that

$$\frac{1}{x} = \lim_{n\to\infty} \frac{1}{x_n}$$

We have

$$\left|\frac{1}{x_n} - \frac{1}{x_m}\right|_v = \left|\frac{x_m - x_n}{x_m x_n}\right|_v = \frac{|x_m - x_n|_v}{|x_m x_n|_v}$$

Since $|x_m - x_n| \to 0$, ((x_n) is Cauchy) and the denominator is bounded below, we have that $(\frac{1}{x_n})$ is Cauchy and has limit $\frac{1}{x}$.

To show that K_v is a topological field, one needs to show that the addition, multiplication, and additive and multiplicative inverse functions are continuous.

4. $\mathcal{O}_v$ is closed under multiplication by the multiplicativity of the norm. To show that $\mathcal{O}_v$ is closed under addition, we have

$$x, y \in \mathcal{O}_v \implies |x+y|_v \leq \max\{|x|_v, |y|_v\} \implies x + y \in \mathcal{O}_v$$

We now show that m_v is an ideal. We have

$$\begin{aligned} |x|_v < 1, |y|_v < 1 &\implies |x+y|_v \leq \max\{|x|_v, |y|_v\} \implies x + y \in m_v \\ |x|_v < 1, |y|_v \leq 1 &\implies |xy| < 1 \implies xy \in m_v \end{aligned}$$

Now we show that m_v is a maximal ideal. If $\alpha \in \mathcal{O}_v \setminus m_v$, then $|\alpha|_v = 1$, which implies $|\frac{1}{x}| = 1$, so that $1/\alpha \in \mathcal{O}_v$. If m_v is not maximal, then it is properly contained in some maximal ideal M. But then M has a unit, and is not a proper ideal of $\mathcal{O}_v$.

So, $\mathcal{O}_v$ is a complete *local* ring.

5. Pick any $\alpha \in K$, where $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then $v_p(\alpha) = 1$, so that $|\alpha|_{\mathfrak{p}} = \frac{1}{||\mathfrak{p}||} < 1$, and $\alpha \in m_v$. If $\beta \in m_v$ is any other element, then $||\mathfrak{p}||^{\mathbb{Z}} \ni |\beta|_v < 1$, so that $|\beta|_v = ||\mathfrak{p}||^{-c}$, where $c \geq 1$. Now we have

$$\left|\frac{\beta}{\alpha}\right|_v = \frac{|\beta|_v}{|\alpha|_v} = \frac{1}{||\mathfrak{p}||^{c-1}} \leq 1$$

so that $\beta/\alpha \in \mathcal{O}_v$, so that $m_v \subseteq (\alpha)$.

Any generator for m_v is called a uniformizer of $\mathcal{O}_v$ or K_v. □

Proposition 5.5. *Define $\mathcal{O}_{\mathfrak{p}}$ to be the localization of $\mathcal{O}_K$ at $\mathfrak{p}$. This is the set of fractions a/b where $b \notin \mathfrak{p}$.*

1. *$\mathcal{O}_{\mathfrak{p}} \subseteq K_v$. In fact, $\mathcal{O}_{\mathfrak{p}}$ sits inside $\mathcal{O}_v$ and is dense in $\mathcal{O}_v$.*

2. *$\mathcal{O}_K \subseteq \mathcal{O}_p \subseteq \mathcal{O}_v$, and $\mathcal{O}_K$ is dense in $\mathcal{O}_v$.*

Proof. 1. If $\mathcal{O}_{\mathfrak{p}} \ni x$, then $v_{\mathfrak{p}}(x) \geq 0$, so that $|x|_v \leq 1$. We need all $x \in \mathcal{O}_v - \{0\}$ expressed as a limit of elements in $\mathcal{O}_{\mathfrak{p}}$. By definition, x is the limit of x_n with $x_n \in K^\times$. Also $|x|_v \leq 1$ is the limit of $|x_n|_v$. This implies $|x_n|_v \leq 1$ for n large. We conclude that $K \cap \mathcal{O}_v$ is dense in $\mathcal{O}_v$.

A standard result from commutative algebra (the commutativity of localization and completion at a maximal ideal) implies that $K \cap \mathcal{O}_v$ and the localization $\mathcal{O}_{\mathfrak{p}}$ have the same closures in $\mathcal{O}_v$. This implies that $\mathcal{O}_{\mathfrak{p}}$ is dense in $\mathcal{O}_v$ as well.

2. Pick $x \in \mathcal{O}_\mathfrak{p}$ and $a, b \in \mathcal{O}_K$ so that $x = \frac{a}{b}$ and $v_\mathfrak{p}(b) = 0$. By the definition of localization, $\mathfrak{p}$ does not divide (b), so that $\mathfrak{p}$ and (b) are coprime. This implies that $\mathfrak{p} + (b) = \mathcal{O}_K$, so that there exists $\alpha \in \mathfrak{p}$ and $\beta \in \mathcal{O}_K$ such that $\alpha + \beta b = 1$. Now we have
$$x = \frac{a}{b} = \frac{a\beta}{b\beta} = \frac{\alpha\beta}{1-\alpha} = \alpha\beta(1 + \alpha + \alpha^2 + \cdots)$$
Set
$$x_n = \alpha\beta(1 + \alpha + \alpha^2 + \cdots \alpha^n)$$
Then
$$x - x_n = \alpha\beta(\alpha^{n+1} + \alpha^{n+2} + \alpha^{n+3} + \cdots) = \alpha\beta\alpha^{n+1}(1 + \alpha + \alpha^2 + \cdots)$$
Now we have
$$\begin{aligned} v_\mathfrak{p}(x - x_n) =& v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\beta) + v_\mathfrak{p}(1 + \alpha + \alpha^2 + \cdots) + v_\mathfrak{p}(\alpha^{n+1}) \\ =& v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\beta) + v_\mathfrak{p}(1 + \alpha + \alpha^2 + \cdots) + (n+1)v_\mathfrak{p}(\alpha) \end{aligned}$$
This expression approaches infinity as $n \to \infty$, which implies
$$x = \lim_{n\to\infty} x_n$$

□

Lecture 17
2018-02-23

(Notes by Caitlyn Booms.)

Recall that there are three different places of K, where K is a number field. We have
$$\begin{aligned} v \mid \mathbb{R} \quad &\longleftrightarrow \quad K \hookrightarrow \mathbb{R} \text{ real place} \\ v \mid \mathbb{C} \quad &\longleftrightarrow \quad \{K \hookrightarrow \mathbb{C}\} \text{ complex place, pair of complex embeddings} \\ v \nmid \infty \quad &\longleftrightarrow \quad \text{finite places, prime ideals } \mathfrak{p} \neq 0 \text{ of } \mathcal{O}_K \end{aligned}$$
where the first two places are infinite places, denoted $v \mid \infty$. Any place v produces a norm $|\cdot|_v : K \to [0, \infty)$, and we denote the metric space completion of K with respect to this norm by $(K_v, |\cdot|_v)$. Then $K_v \cong \mathbb{R}$ if $v \mid \mathbb{R}$ and $K_v \cong \mathbb{C}$ if $v \mid \mathbb{C}$. If $v \nmid \infty$, then we say $v = v_\mathfrak{p}$. In the homework, we will show that K_v is a topological field, and we have the following:
$$\begin{aligned} &K_v = \text{ topological field} \\ &\cup \\ &\mathcal{O}_v = \{x \mid |x|_v \leq 1\} \\ &\cup \\ &\mathfrak{m}_v = \{x \mid |x|_v = 1\} = (\alpha)\mathcal{O}_v \quad \forall \alpha \in \mathfrak{p} \setminus \mathfrak{p}^2, \text{ unique maximal ideal.} \end{aligned}$$
Since the completion of K with respect to $|\cdot|_v$ comes with an injection of $K \hookrightarrow K_v$ given by constant Cauchy sequences for every place v, we let each place correspond to this embedding:
$$\begin{aligned} v \mid \mathbb{R} \quad &\text{corresponds to} \quad K \hookrightarrow K_v = \mathbb{R} \\ v \mid \mathbb{C} \quad &\text{corresponds to} \quad K \hookrightarrow K_v = \mathbb{C} \\ v \nmid \infty \quad &\text{corresponds to} \quad K \hookrightarrow K_v. \end{aligned}$$
Notation: $\overline{x}$ denotes the topological closure of x in K_v, which is a complete metric space.
Observe that $\overline{K} = K_v$ and $\overline{\mathcal{O}_K} = \overline{\mathcal{O}_\mathfrak{p}} = \overline{K \cap \mathcal{O}_v} = \mathcal{O}_v$, where $\mathcal{O}_\mathfrak{p}$ is the set of fractions with no $\mathfrak{p}$ in the denominator and the second equality follows from the commutative algebra fact that localization and completion commute for maximal ideals.

Proposition 5.6. *(a)* $\mathcal{O}_v/\mathfrak{m}_v^n \cong \mathcal{O}_K/\mathfrak{p}^n$ *for* $v = v_\mathfrak{p}$

(b) $B_{0,1} = \mathcal{O}_v \subset K_v$ *is compact (Heine-Borel).*

Proof. (a) We have the sequence of maps

$$\mathcal{O}_K \hookrightarrow \mathcal{O}_v \twoheadrightarrow \mathcal{O}_v/\mathfrak{m}_v^n \to 0$$

where $\mathcal{O}_K$ is dense in $\mathcal{O}_v$ and $\mathfrak{m}_v^n = (\alpha^n)\mathcal{O}_v = \{x \in K_v \mid v(x) \geq n = v(\alpha^n)\}$. Then $x \in \mathcal{O}_K$ has $v_\mathfrak{p}(x) \geq n$ if and only if $x \in \mathfrak{p}^n$, so the map

$$\mathcal{O}_K/\mathfrak{p}^n \hookrightarrow \mathcal{O}_v/\mathfrak{m}_v^n$$

is injective. For surjectivity, pick any $a \in \mathcal{O}_v$. Then we seek $x \in \mathcal{O}_K$ such that $x \equiv a \mod \mathfrak{m}_v^n$, which is true if and only if $v(x-a) \geq n$. But $\mathcal{O}_v = \overline{\mathcal{O}_K}$ so this is immediate as $a = \lim x_n$, $x_n \in \mathcal{O}_K$, so we can find $x \in \mathcal{O}_K$ with this property.

(b) Consider the map

$$\phi : \mathcal{O}_v \longrightarrow \prod_{k \geq 1} \mathcal{O}_K/\mathfrak{p}^k.$$

Then ϕ is injective if $\phi(x) = 0$ implies that $x \in \mathfrak{m}_v^k$ for all k, which implies $v(x) \geq k$ for all k so $|x|_v \leq \|\mathfrak{p}\|^k$ for all k. But then $|x|_v = 0$, so $x = 0$ and ϕ is injective. In fact, if the RHS has the product topology where each $\mathcal{O}_K/\mathfrak{p}^k \cong \mathcal{O}_v/\mathfrak{m}_v^k$ has the discrete topology, then ϕ is continuous.
(If X_α are topological spaces and $\prod_{\alpha \in I} X_\alpha$ has the product topology, then the open sets are of the form $\prod_{\alpha \in \text{finite}} U_\alpha \prod_{\alpha \notin \text{finite}} X_\alpha$ where $U_\alpha \subset X_\alpha$ are open sets.)
To see that ϕ is continuous, pick an open set $\prod_{k=1}^{N} U_k \prod_{k>N} \mathcal{O}_K/\mathfrak{p}^k \subset$ RHS. We want to show that the preimage of this set under ϕ is open. Since translation is continuous, it suffices to show this for the open set $W = \{0\} \times \cdots \times \{0\} \times \mathcal{O}_K/\mathfrak{p}^{N+1} \times \cdots$ where the k-th $\{0\}$ is an element of $\mathcal{O}_K/\mathfrak{p}^k$ for $k = 1, \ldots, N$. We have that $\phi^{-1}(W) = \{x \in \mathcal{O}_v \mid v(x) \geq N\} = B_{0,\|\mathfrak{p}\|^{-N}}$ which is a closed ball. However, this is also an open ball because

$$B_{0,\|\mathfrak{p}\|^{-(N-1)}} = \{x \in \mathcal{O}_v \mid v(x) \geq N-1\} = \bigsqcup_{r \in \mathcal{O}_K/\mathfrak{p}} \{x \in \mathcal{O}_v \mid v(x - \alpha^{N-1} r) \geq N\} = \bigsqcup_{r \in \mathcal{O}_K/\mathfrak{p}} B_{\alpha^{N-1}r, \|\mathfrak{p}\|^{-N}}.$$

Therefore, ϕ is a continuous injection. Then $\mathcal{O}_K/\mathfrak{p}^k$ is finite, so is compact, which implies that $\prod \mathcal{O}_K/\mathfrak{p}^k$ is compact. So we have $\mathcal{O}_v \cong \phi(\mathcal{O}_v)$ as topological spaces, and the latter is contained in a compact space, which implies that $\mathcal{O}_v$ is compact.
Conclusion: K_v is a locally compact topological field if $v \nmid \infty$ (obvious if $v \mid \infty$).

□

5.2 Adeles and ideles

Definition 5.7. Let K be a number field. Define the adele of K as

$$\mathbb{A}_K = \prod_{v \text{ places}\{\mathcal{O}_v\}}{}' K_v = \{(x_v) \in \prod K_v \mid x_v \in \mathcal{O}_v \text{ for almost all } v\}.$$

$\mathbb{A}_K$ has the subspace topology inherited from $\prod K_v$ with the product topology.

Proposition 5.8. $\mathbb{A}_K$ *is a locally compact topological ring.*

Proof. Let $(x_v), (y_v) \in \mathbb{A}_K$. Then there exists a finite set S such that $x_v, y_v \in \mathcal{O}_v$ for $v \notin S$. This implies that $x_v + y_v, x_v y_v \in \mathcal{O}_v$ for $v \notin S$, so $x+y, xy \in \mathbb{A}_K$. In the homework, we will show that $\mathbb{A}_K$ is a topological ring. It is locally compact because

$$\prod_{v|\mathbb{R}} [a_v, b_v] \prod_{v|\mathbb{C}} \{\text{closed balls}\} \prod_{v\nmid\infty} \mathcal{O}_v$$

is compact by Tychenoff's Theorem. □

Theorem 5.9. *(a) Define the norm $|\cdot|_{\mathbb{A}_K} : \mathbb{A}_K \to [0,\infty)$ such that $|(x_v)|_{\mathbb{A}_K} = \prod_v |x_v|_v$. Let $\iota : K \hookrightarrow \mathbb{A}_K$ such that $\iota(x) = (x, x, x, \dots)$ which always converges. Then $|\iota(x)|_{\mathbb{A}_K} = 1$ for every $x \in K^\times$ and $\iota(K)$ is a discrete subgroup of $\mathbb{A}_K$.*

(b) $\iota(K)$ is a cocompact lattice in $\mathbb{A}_K$.

Proof. (a): If $x \in K^\times$, then $(x)\mathcal{O}_K = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{v_\mathfrak{p}(x)}$ where S is a finite set, so $v \notin S$ means $v(x) = 0$. This implies that $x \in \mathcal{O}_v$ for $v \notin S$ so $\iota(x) = (x, x, \dots) \in \mathbb{A}_K$. In the homework, we will show that $|K^\times|_{\mathbb{A}_K} = 1$. Then $\iota(K)$ is discrete if and only if $\iota(K)\cap$ open set $=$ finite set. Consider

$$\iota(K) \cap \left(\prod_{v|\mathbb{R}} (-1,1) \prod_{v|\mathbb{C}} \{|z| < 1\} \prod_{v\nmid\infty} \mathcal{O}_v \right) = \{x \in K \mid x \in (-1,1) \text{ for } v|\mathbb{R}, |x| < 1 \text{ for } v|\mathbb{C}, v \nmid \infty\}$$

where the set $\iota(K)$ is intersected with is an open set. Then we have

$$|x|_{\mathbb{A}_K} = \prod_{v|\mathbb{R}} |x|_v \prod_{v|\mathbb{C}} |x|_v \prod_{v\nmid\infty} |x|_v$$

is in the open ball with $|\cdot|_{\mathbb{A}_K} < 1$, but $|K^\times|_{\mathbb{A}_K} = 1$. Thus, we must have

$$\iota(K) \cap \left(\prod_{v|\mathbb{R}} (-1,1) \prod_{v|\mathbb{C}} \{|z| < 1\} \prod_{v\nmid\infty} \mathcal{O}_v \right) = \{0\}$$

which gives that $\iota(K)$ is discrete.

Lecture 18

2018-02-26

(Notes by Matt Schoenbauer.)

(b): We have

$$\mathbb{A}_K / K = \bigcup_S K_\infty \times K_S \times \prod_{v\notin S} \mathcal{O}_v / K.$$

Pick

$$(a_v) \in K_\infty \times K_S \times \prod_{v\notin S} \mathcal{O}_v$$

Claim 1. $(a_v) \in K + K_\infty \times K_{S\setminus\{u\}} \times \prod_{v\in S\setminus\{u\}} \mathcal{O}_v$ for any $u \in S$.

Pick $u \in S$. If $a_u \in \mathcal{O}_u$ there is nothing to do. Otherwise $a_u \in K_u = \mathrm{Frac}\mathcal{O}_u$ but not in $\mathcal{O}_u$ so $n_u = -u(a_u) > 0$. Now pick any $\varpi_u \in \mathfrak{p}_u \setminus \mathfrak{p}_u^2$, where $\varpi_u \in \mathcal{O}_K$. Then

$$a_u = \frac{b_u}{\varpi_u^{n_u}}$$

for some $b_u \in \mathcal{O}_u$. The Chinese Remainder Theorem gives $x_u \in \mathcal{O}_K$ such that $x_u \equiv b_n \mod \mathfrak{p}_u^{n_u}$ and $x_u \equiv 0 \mod \frac{\varpi_u^{n_u}}{\mathfrak{p}_u^{n_u}}$ (since $\varpi_u^{n_u}/\mathfrak{p}_u^{n_u}$ and $\mathfrak{p}_u^{n_u}$ are coprime). Note that we have

$$(a_v)_v - \left(\frac{x_u}{\varpi_u^{n_u}}\right)_v \in \mathbb{A}_K$$

where $\frac{x_u}{\varpi_u^{n_u}}$ is identified with an element of $\mathbb{A}_K$ via the embedding ι.

When $v = u$ note that

$$x_u \equiv b_u \mod \mathfrak{p}_u^{n_u} \implies \mathfrak{p}_u^{n_u} \mid x_u - b_u$$

so

$$u(x_u - b_u) \geq n_u = u(\varpi_u^{n_u}).$$

This implies that

$$a_u - \frac{x_u}{\varpi_n^{n_u}} = \frac{b_u - x_u}{\varpi_u^{n_u}} \in \mathcal{O}_u.$$

When $v \notin S$, the assumption that $\frac{\varpi_u^{n_u}}{\mathfrak{p}_u^{n_u}} \mid x_u$ in $\mathcal{O}_K$ implies that $v(x_u) \geq v\left(\frac{\varpi_n^{n_u}}{\mathfrak{p}_u^{n_u}}\right) = v(\varpi_u^{n_u})$ and so $a_v - x_u/\varpi_u^{n_u} \in \mathcal{O}_v$.

We conclude that $(a_v) - \iota(x_u/\varpi_u^{n_u}) \in K_\infty K_{S-\{u\}} \prod_{v \notin S-\{u\}} \mathcal{O}_u$. Inductively we deduce that $(a_v) \in K + K_\infty \prod_{v\nmid\infty} \mathcal{O}_v$ and so

$$\mathbb{A}_K/K = (K + K_\infty \prod \mathcal{O}_v)/K = K_\infty \prod \mathcal{O}_v/(K \cap K_\infty \prod \mathcal{O}_v) = K_\infty \prod \mathcal{O}_v/\mathcal{O}_K = (K_\infty/\mathcal{O}_K) \prod \mathcal{O}_v.$$

This is compact by Tychonoff and the fact that $\mathcal{O}_K$ is a full rank lattice in K_∞. □

Recall that $|\cdot|_K : \mathbb{A}_K \to [0, \infty)$ is defined by $|(a_v)|_K = \prod |a_v|_v$.

Proposition 5.10. *If $(a_v) \in \mathbb{A}_K$ then $|(a_v)|_K \neq 0$ if and only if $(a_v) \in \mathbb{A}_K^\times$ where*

$$\mathbb{A}_K^\times = \prod_{\{\mathcal{O}_v^\times\}}{}' K_v^\times = \{(a_v) \in \prod K_v^\times \mid a_v \in \mathcal{O}_v^\times \text{ for almost all } v\}.$$

Proof. Clearly $a_v \neq 0$ and if $a_v \notin \mathcal{O}_v^\times$ then $a_v \in \mathfrak{m}_v$ so $|a_v|_v \leq ||\mathfrak{p}_v||^{-1} \leq 2^{-1}$. But if $a_v \notin \mathcal{O}_v^\times$ for infinitely many v then $(a_v)|_K \leq \prod 1/2 = 0$. □

Definition 5.11. Let $\mathbb{A}_K^1 \subset \mathbb{A}_K^\times$ be the kernel of the group homomorphism $|\cdot|_K : \mathbb{A}_K^\times \to (0, \infty)$.

Remark 8. The most natural topology to put on $\mathbb{A}_K^\times$ is the smallest topology that makes the map $\mathbb{A}_K^\times \to \mathbb{A}_K \times \mathbb{A}_K$ given by $x \mapsto (x, x^{-1})$ continuous. This topology is NOT the subset topology from $\mathbb{A}_K$. However, the two subset topologies on $\mathbb{A}_K^1 \subset \mathbb{A}_K$ and $\mathbb{A}_K^1 \subset \mathbb{A}_K^\times$ are the same.

Theorem 5.12. *The map $\iota : K \to \mathbb{A}_K$ takes $K^\times$ to $\mathbb{A}_K^1$ and under this map $K^\times$ is a cocompact lattice in $\mathbb{A}_K^1$, i.e., $\mathbb{A}_K^1/K^\times$ is compact.*

We give two applications.

Application 5.13. The finiteness of the class group. The map $\mathbb{A}_K^1 \to \mathrm{Div}(K)$ sending (a_v) to $\sum_{v\nmid\infty} v(a_v)[v]$ is continuous and surjective. The projection to $\mathrm{Cl}(K)$ factors through $\mathbb{A}_K^1/K^\times$ and therefore $\mathrm{Cl}(K)$ is a discrete group (a quotient of $\mathrm{Div}(K)$) which is the image of the compact group $\mathbb{A}_K^1/K^\times$. It is therefore discrete and compact and so finite.

Application 5.14. The Dirichlet unit theorem. The map from the previous application fits in the following exact sequences

$$1 \to K_\infty^1 \prod \mathcal{O}_v^\times / \mathcal{O}_K^\times \to \mathbb{A}_K^1 / K^\times \to \mathrm{Cl}(K) \to 1$$

where $K_\infty^1 \subset K_\infty$ are the tuples of product 1. The kernel is closed (K_∞^1 is closed in K_∞, and so are $\mathcal{O}_v^\times$ in K_v) inside the compact set $\mathbb{A}_K^1/K^\times$ and therefore it is compact. Consider the map

$$\log : K_\infty^1 \prod \mathcal{O}_v^\times \to \mathbb{R}^{r+s}$$

sending (x_v) to $(\log |x_v|_v)_{v|\infty}$. This map lands in the kernel $\cong \mathbb{R}^{r+s-1}$ of Σ and factors through $\mathcal{O}_K^\times$ so

$$\log : K_\infty^1 \prod \mathcal{O}_v^\times / \mathcal{O}_K^\infty \to \mathbb{R}^{r+s-1} / \log \mathcal{O}_K^\times.$$

But the LHS is compact and log is continuous so the RHS is compact which implies that $\log \mathcal{O}_K^\times$ is cocompact in $\mathbb{R}^{r+s-1}$.

Lecture 19
2018-02-28

First, if G is a locally compact topological group there exists a unique up to scalars (left) Haar measure vol_G which is finite on compact measurable sets and satisfies

$$\mathrm{vol}_G(gX) = \mathrm{vol}_G(X)$$

for all $g \in G$ and X measurable.

On the homework you had to show that if vol_v is the Haar measure on the abelian group $(K_v, +)$ and vol_K is the Haar measure on the abelian group $(\mathbb{A}_K, +)$ then

$$\mathrm{vol}_v(aX) = |a|_v \,\mathrm{vol}_v(X)$$
$$\mathrm{vol}_K(aX) = |a|_K \,\mathrm{vol}_K(X)$$

The idea in both cases is that if R is a locally compact topological ring with Haar measure vol_R on the abelian group $(R, +)$ then for $a \in R$ the map $\mathrm{vol}_a(X) = \mathrm{vol}_R(aX)$ is another Haar measure which is then off from $\mathrm{vol}_R(X)$ by a scalar which can be computed using any suitable compact X.

Theorem 5.15. *(Adelic Minkowski) Suppose $X \subset \mathbb{A}_K$ is a compact set with $\mathrm{vol}_K(X) > \mathrm{vol}_K(\mathbb{A}_K/K)$. Then there exist $a \neq b \in X$ such that $a - b \in K$.*

Proof. Let $F \subset \mathbb{A}_K$ be a fundamental region for $\mathbb{A}_K/K$. Its closure is compact and has the same volume as $\mathbb{A}_K/K$. Then

$$\mathrm{vol}_K(X) = \sum_{u \in K} \mathrm{vol}_K(X \cap (F + u)) = \sum_{u \in K} ((X - u) \cap F) > \mathrm{vol}_K(F).$$

We used the Haar property in the second equality. By the pigeonhole principle this implies that there exist $u \neq v \in K$ such that $X - u \cap X - v \neq \emptyset$. This implies that there exist $a, b \in X$ such that $a - u = b - v$ and so $a - b = u - v \in K^\times$. □

Theorem 5.16. *The subgroup $K^\times$ of $\mathbb{A}_K^\times$ is a cocompact lattice in $\mathbb{A}_K^1$.*

Proof. That it lands in $\mathbb{A}_K^1$ you had to show on the homework. It is discrete since K is discrete in $\mathbb{A}_K$ and $\mathbb{A}_K^1 \subset \mathbb{A}_K$ is a closed subset. It remains to show that $\mathbb{A}_K^1/K^\times$ is compact.

Fix $c_v > 0$ such that $c_v = 1$ for almost all v and consider $X = X_{\{c_v\}} = \{(x_v) \in \mathbb{A}_K \mid |x_v| \leq c_v, \forall v\}$. Increasing finitely many c_v we can ensure that $\mathrm{vol}_K(X) > \mathrm{vol}_K(\mathbb{A}_K/K)$.

Let $a = (a_v) \in \mathbb{A}_K^1$ be any idele of unit norm. Then

$$\mathrm{vol}_K(a^{-1}X) = |a|_K^{-1} \,\mathrm{vol}_K(X) = \mathrm{vol}_K(X) > \mathrm{vol}_K(\mathbb{A}_K/K)$$

and so adelic Minkowski implies that there exist $u \neq v \in X$ such that $u/a - v/a = \gamma \in K^\times$. But then we deduce that

$$a = \gamma^{-1}(u - v) \in K^\times(X - X).$$

As a result

$$\mathbb{A}_K^1/K^\times = K^\times(X - X)/K^\times$$

and so $\mathbb{A}_K^1/K^\times$ is the image under the projection of $X - X$. But X is compact (Tychonoff) and $-$ is continuous so $X - X$ is compact and therefore $\mathbb{A}_K^1/K^\times$ is compact. □

6 Ramification and Galois theory

6.1 Prime ideals under extensions

A basic question is the following. Suppose L/K are number fields and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ and will decompose into a product of prime ideals of $\mathcal{O}_L$. What are these prime factors? And what arithmetic significance do they have? Can they be predicted?

Example 6.1. (From algebra) If $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. The ideal $(2)\mathbb{Z}[i]$ factors as $(1 + i)^2$. If p is a prime $\equiv 3 \pmod 4$ then $(p)\mathbb{Z}[i]$ stays a prime ideal in $\mathbb{Z}[i]$. If $p \equiv 1 \pmod 4$ then $(p)\mathbb{Z}[i]$ splits as a product $(p)\mathbb{Z}[i] = \mathfrak{q}\bar{\mathfrak{q}}$. For example $(5)\mathbb{Z}[i] = (2 + i)(2 - i)$.

Proposition 6.2. *Suppose L/K are number fields (also works for a finite extension of fraction fields of integral rings). If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_L$ then the following are equivalent:*

1. $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$
2. $\mathfrak{q} \supset \mathfrak{p}$
3. $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$
4. $\mathfrak{q} \cap K = \mathfrak{p}$.

If any of these condition are satisfied we say $\mathfrak{q} \mid \mathfrak{p}$ or $\mathfrak{q}$ lies above $\mathfrak{p}$ or $\mathfrak{p}$ lies below $\mathfrak{q}$.

Proof. 1 implies 2 becauase $\mathfrak{p} \subset \mathfrak{p}\mathcal{O}_L$. 2 implies 3 because $\mathfrak{q} \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$, it is proper (otherwise 1 would be in $\mathfrak{q}$) and contains $\mathfrak{p}$ and so must equal $\mathfrak{p}$ by maximality of $\mathfrak{p}$. 3 implies 4 because $\mathcal{O}_L \cap K = \mathcal{O}_K$. Finally 4 implies 1 because then $\mathfrak{p} \subset \mathfrak{q}$ and so $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}$. □

Proposition 6.3. *Suppose L/K are number fields.*

1. *Every prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ lies above a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.*
2. *Every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lies below a prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$.*

Proof. For the first part note that $\mathfrak{q} \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$. It cannot be everything because then $1 \in \mathfrak{q}$ and if $\alpha \in \mathfrak{q}$ then $\alpha \mid N_{L/K}(\alpha) \in \mathcal{O}_K$ and so $\mathfrak{q} \cap \mathcal{O}_K \neq 0$. Moreover,

$$\mathcal{O}_K/(\mathcal{O}_K \cap \mathfrak{q}) \cong (\mathcal{O}_K + \mathfrak{q})/\mathfrak{q} \subset \mathcal{O}_L/\mathfrak{q}$$

The RHS being a field implies that the LHS is an integral domain and so $\mathfrak{q} \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.

For the second part, we seek $\mathfrak{q}$ of the form $\mathfrak{p}\mathcal{O}_L$. Since $\mathfrak{p}$ is proper it follows that $\mathfrak{p}^{-1} \supsetneq \mathcal{O}_K$ and so $\mathfrak{p}^{-1} = \sum \mathbb{Z}\alpha_i$ where at least one of the α_i is not in $\mathcal{O}_K$. With $\alpha = \alpha_i \notin \mathcal{O}_K$ we have $\alpha\mathfrak{p}\mathcal{O}_L \subset \mathfrak{p}^{-1}\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$. If $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$ it would follows that $\alpha\mathcal{O}_L \subset \mathcal{O}_L$ but then we'd deduce that $\alpha \cdot 1 \in \mathcal{O}_L$ contradicting our choice. Thus $\mathfrak{p}\mathcal{O}_L \subsetneq \mathcal{O}_L$. Finally, any prime factor $\mathfrak{q}$ of $\mathfrak{p}\mathcal{O}_L$ will lie above $\mathfrak{p}$. □

Example 6.4. Suppose m is square-free, different from 1 and $\equiv 2, 3 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{m})$ in which case $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$.

1. If $X^2 - m = 0$ has no solutions in $\mathbb{F}_p$ then
$$\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - m) \to \mathbb{F}_p[X]/(X^2 - m)$$
is surjective onto the field $\mathbb{F}_p[X]/(X^2 - m)$ and has kernel $(p)\mathcal{O}_K$. Thus $(p)\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.

2. If $X^2 - m = 0$ has two solutions in $\mathbb{F}_p$, with representatives a and $-a$ in $\mathbb{Z}$ then
$$\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - m) \to \mathbb{F}_p[X]/(X^2 - m) \cong \mathbb{F}_p[X]/(X - a) \oplus \mathbb{F}_p[X]/(X + a) \cong \mathbb{F}_p \oplus \mathbb{F}_p$$
is again surjective. The preimage of $\mathbb{F}_p \oplus 0$ is the ideal $(p, \sqrt{m} - a)$ which is then prime since the image is a field. Similarly the preimage of $0 \oplus \mathbb{F}_p$ is the prime ideal $(p, \sqrt{m} + a)$ and
$$(p)\mathcal{O}_K = (p, \sqrt{m} - a)(p, \sqrt{m} + a)$$
is the decomposition into primes.

3. Finally, if $p \mid m$ then
$$\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - m) \to \mathbb{F}_p[X]/(X^2)$$
is surjective and the preimage $(p, \sqrt{m})$ of $X\mathbb{F}_p[X]/(X^2)$ is a prime ideal with $(p)\mathcal{O}_K = (p, \sqrt{m})^2$.

Lecture 20
2018-03-02

6.2 Ramification and inertia indices

Definition 6.5. If R is a Dedekind domain and $\mathfrak{p}$ is a prime (and therefore maximal) ideal then the **residue field** at $\mathfrak{p}$ is $k_{\mathfrak{p}} = R/\mathfrak{p}$.

Suppose now that L/K are number fields, $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_L$ such that $\mathfrak{q} \mid \mathfrak{p}$. Then $k_{\mathfrak{q}} = \mathcal{O}_L/\mathfrak{q} \supset (\mathfrak{q} + \mathcal{O}_K)/\mathfrak{q} \cong \mathcal{O}_K/\mathfrak{p} = k_{\mathfrak{p}}$ and so $k_{\mathfrak{q}}$ is a finite extension of $k_{\mathfrak{p}}$.

Definition 6.6. The **inertia index** $f_{\mathfrak{q}/\mathfrak{p}} = [k_{\mathfrak{q}} : k_{\mathfrak{p}}]$. The **ramification index** is the exponent $v_{\mathfrak{q}}(\mathfrak{p}\mathcal{O}_L)$ of the prime ideal $\mathfrak{q}$ in the prime ideal decomposition of $\mathfrak{p}\mathcal{O}_L$.

Example 6.7. Let $K = \mathbb{Q}(i)$. We already know that $(2)\mathcal{O}_K = (1+i)^2$, $(p)\mathcal{O}_K$ is prime when $p \equiv 3 \pmod 4$ and if $p \equiv 1 \pmod 4$ then $(p)\mathcal{O}_K = (a + bi)(a - bi)$ where $p = a^2 + b^2$. Let's compute the ramification and inertia indices.

1. $p = 2$ and $\mathfrak{q} = (2 + i)$. Then $e_{\mathfrak{q}/p} = 2$ and $k_{\mathfrak{q}} = \mathbb{Z}[i]/(1 + i) \cong \mathbb{Z}[X]/(X^2 + 1, X + 1) \cong \mathbb{Z}/2 \cong \mathbb{F}_2$ and so $f_{\mathfrak{q}/p} = 1$.

2. $p \equiv 1 \pmod 4$ with $a^2 + 1 \equiv 0 \pmod p$. Let $\mathfrak{q}_1 = (p, a + i)$ and $\mathfrak{q}_2 = (p, a - i)$ (If $p = u^2 + v^2$ then $(p, a+i) = (u+vi)$ and $(p, a-i) = (u-vi)$). Since the setup is symmetric we only compute for $\mathfrak{q} = \mathfrak{q}_1$. Clearly $e_{\mathfrak{q}/p} = 1$ from the prime decomposition. Next, $\mathbb{Z}[i]/(p, a + i) \cong \mathbb{Z}[X]/(X^2 + 1, p, a + X) \cong \mathbb{F}_p/(a^2 + 1) = \mathbb{F}_p$ and so $f_{\mathfrak{q}/p} = 1$.

3. If $p \equiv 3 \pmod 4$ then $\mathfrak{q} = (p)\mathbb{Z}[i]$ is a prime ideal and so $e_{\mathfrak{q}/p} = 1$. Now $\mathbb{Z}[i]/p\mathbb{Z}[i] \cong \mathbb{F}_p[X]/(X^2+1) \cong \mathbb{F}_{p^2}$ since $X^2 + 1$ doesn't have a root mod p. Thus $f_{\mathfrak{q}/p} = 2$.

Our goal theorem is the following:

Theorem 6.8. *If L/K are number fields, $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are the distinct prime ideals of $\mathcal{O}_L$ appearing in the prime factorization of $\mathfrak{p}\mathcal{O}_L$. Then*
$$\sum_{i=1}^{r} e_{\mathfrak{q}_i/\mathfrak{p}} f_{\mathfrak{q}_i/\mathfrak{p}} = [L : K]$$

Proposition 6.9. *Suppose $M/L/K$ is a tower of number fields and $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ ideals of $\mathcal{O}_K$, $\mathcal{O}_L$ and $\mathcal{O}_M$ respectively such that $\mathfrak{p} \mid \mathfrak{q} \mid \mathfrak{r}$. Then*

$$\begin{aligned} e_{\mathfrak{r}/\mathfrak{p}} &= e_{\mathfrak{r}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}} \\ f_{\mathfrak{r}/\mathfrak{p}} &= f_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}} \end{aligned}$$

Proof. This follows from definitions. □

Lemma 6.10. *Let L/K be number fields and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Then $\dim_{k_\mathfrak{p}}(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) \leq [L : K]$.*

Proof. Let $n = [L : K]$. We need to show that any $n + 1$ elements $\alpha_1, \ldots, \alpha_{n+1}$ of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ have a nontrivial $k_\mathfrak{p}$ dependence. Since $\dim_K L = n$, there exist $\beta_1, \ldots, \beta_{n+1} \in K$, not all 0, such that $\sum \alpha_i\beta_i = 0$. Multiplying by suitable integers we may assume that $\beta_i \in \mathcal{O}_K$ and we'd like to find such a dependence such that the images of $\beta_i \in \mathcal{O}_K$ in $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ are not all 0. Suppose $\beta_i \in \mathfrak{p}$ for all i. Then the ideal $J = (\beta_1, \ldots, \beta_{n+1}) = \sum \mathcal{O}_K\beta_i \subset \mathfrak{p}$. Let $J^{-1} = \sum \mathcal{O}_K\gamma_i$. Then $JJ^{-1} = \sum \mathcal{O}_K\beta_i\gamma_j = \mathcal{O}_K$ and thus $\beta_i\gamma_j \in \mathcal{O}_K$ for all i, j and $\beta_{i_0}\gamma_{j_0} \notin \mathfrak{p}$ for some i_0, j_0. Then $\sum \alpha_i\beta_i = 0$ implies $\sum \alpha_i\beta_i\gamma_{j_0} = 0$ is a linear dependence among the α_i, with coefficients in $\mathcal{O}_K$ and such that at least one of the coefficients $(\beta_{i_0}\gamma_{j_0})$ does not vanish in $k_\mathfrak{p}$. Thus α_i are dependent over $k_\mathfrak{p}$ and the conclusion follows. □

Theorem 6.11. *Suppose L/K are number fields.*

1. *If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}_i$ are the distinct prime factors of $\mathfrak{p}\mathcal{O}_L$ then*

$$\sum e_{\mathfrak{q}_i/\mathfrak{p}} f_{\mathfrak{q}_i/\mathfrak{p}} = [L : K]$$

where recall that $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_{\mathfrak{q}_i/\mathfrak{p}}}$ and $f_{\mathfrak{q}_i/\mathfrak{p}} = [k_{\mathfrak{q}_i} : k_\mathfrak{p}]$.

2. *If I is a fractional ideal of K then $||I\mathcal{O}_L|| = ||I||^{[L:K]}$.*

Proof. By the multiplicativity of norm we have:

$$||\mathfrak{p}\mathcal{O}_L|| = \prod ||\mathfrak{q}_i||^{e_i} = \prod |k_{\mathfrak{q}_i}|^{e_i} = \prod |k_\mathfrak{p}|^{e_i f_{\mathfrak{q}_i/\mathfrak{p}}} = ||\mathfrak{p}||^{\sum e_i f_i}$$

We first prove (1) for $K = \mathbb{Q}$. Indeed, then $\mathfrak{p} = (p)$ and so $\mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{F}_p^{[L:K]}$ since $\mathcal{O}_L$ is a rank n free $\mathbb{Z}$-module which implies that $p^n = p^{\sum e_i f_i}$ and the conclusion follows.

Next we prove (2). By multiplicativity of the norm of an ideal and the fact that $||aI|| = |N_{K/\mathbb{Q}}(a)|||I||$ it suffices to treat the case of prime ideals $I = \mathfrak{p}$ in which case we need to show that $||\mathfrak{p}\mathcal{O}_L|| = ||\mathfrak{p}||^n$ where $n = [L : K]$. Let p be the prime of $\mathbb{Z}$ below $\mathfrak{p}$ of $\mathcal{O}_K$ and let $(p)\mathcal{O}_K = \prod \mathfrak{p}_i^{e_{\mathfrak{p}_i/p}}$. From the lemma we know that $\dim_{k_{\mathfrak{p}_i}} \mathcal{O}_L/\mathfrak{p}_i\mathcal{O}_L \leq [L : K]$ while from part (1) we know that $\sum e_{\mathfrak{p}_i/p} f_{\mathfrak{p}_i/p} = [K : \mathbb{Q}]$ and, equivalently for $L/\mathbb{Q}$, $||(p)\mathcal{O}_L|| = p^{[L:\mathbb{Q}]}$. So

$$\begin{aligned} p^{[L:\mathbb{Q}]} &= ||(p)\mathcal{O}_L|| \\ &= \prod ||\mathfrak{p}_i\mathcal{O}_L||^{e_{\mathfrak{p}_i/p}} \\ &= \prod |\mathcal{O}_L/\mathfrak{p}_i\mathcal{O}_L|^{e_{\mathfrak{p}_i/p}} \\ &\leq \prod |k_{\mathfrak{p}_i}|^{[L:K]e_{\mathfrak{p}_i/p}} \\ &= \prod |\mathbb{F}_p|^{[L:K]f_{\mathfrak{p}_i/p}e_{\mathfrak{p}_i/p}} \\ &= p^{[L:K][K:\mathbb{Q}]} = p^{[L:\mathbb{Q}]} \end{aligned}$$

Therefore all inequalities are equality and so $||\mathfrak{p}_i\mathcal{O}_L|| = ||\mathfrak{p}_i||^{[L:K]}$ for all i and in particular for $\mathfrak{p} = \mathfrak{p}_i$ for some i.

Finally, from (2) we deduce (1). We already know that

$$||\mathfrak{p}\mathcal{O}_L|| = ||\mathfrak{p}||^{\sum e_{\mathfrak{q}_i/\mathfrak{p}} f_{\mathfrak{q}_i/\mathfrak{p}}}$$

and $||\mathfrak{p}\mathcal{O}_L|| = ||\mathfrak{p}||^{[L:K]}$ from part (2) and the conclusion follows.

□

Lecture 21
2018-03-05

6.3 Factoring prime ideals in extensions

Theorem 6.12. *Suppose L/K are number fields and $L = K(\alpha)$ for an integral element α with minimal polynomial $f(X) \in \mathcal{O}_K[X]$. Suppose $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ lying above a prime p of $\mathbb{Q}$ such that $p \nmid [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$. Let $\overline{f}(X) = \prod \overline{g_i}(X)^{e_i}$ be the prime factorization of $f(X) \mod \mathfrak{p}$ in $k_{\mathfrak{p}}[X]$. Then $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$ are prime ideals lying above $\mathfrak{p}$, $f_{\mathfrak{q}_i/\mathfrak{p}} = \deg g_i(X)$ and*

$$\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_i}.$$

I proved this in class. I'll write it up but in the meantime check ou
`http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/dedekindf.pdf`

Theorem 6.13. *Let $K/\mathbb{Q}$ be a number field. If a prime p ramifies in K then $p \mid \operatorname{disc}(K)$.*

Proof. For now the "only if" direction, the other part begin deferred until after Galois theory.

Suppose $\mathfrak{q}^2 \mid (p)\mathcal{O}_K$. Then $(p)\mathcal{O}_K = \mathfrak{q}I$ where I is divisible by all the prime ideals dividing (p). Let $\alpha \in I - (p)$. Then $\alpha \in \mathfrak{q}$ for every $\mathfrak{q} \mid (p)$.

Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the embeddings fixing $\mathbb{Q}$ and let $L = \prod \sigma_i(K)$ be the composite. For every prime ideal $\mathfrak{q} \mid (p)$ of $\mathcal{O}_K$ write $\mathfrak{q}\mathcal{O}_L = \prod \mathfrak{r}_i$ as a product of (not necessarily distinct) prime ideals of $\mathcal{O}_L$. Since $\alpha \in \mathfrak{q}$ it follows that $\alpha \in \mathfrak{r}_i$ and as $\mathfrak{q}$ varies across the prime ideals dividing $(p)\mathcal{O}_K$, $\mathfrak{r}_i$ varies across the prime ideals dividing $(p)\mathcal{O}_L$. Thus $\alpha \in \mathfrak{r}$ for every prime ideal $\mathfrak{r} \mid (p)$ of $\mathcal{O}_L$.

For every $\sigma = \sigma_i$, $\sigma(\mathfrak{r})$ is also a prime ideal of $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. Thus $\alpha \in \sigma(\mathfrak{r})$ and so $\sigma(\alpha) \in \mathfrak{r}$ for every σ.

Suppose $\alpha_1, \dots \alpha_n$ is an integral basis of $\mathcal{O}_K$ and $\alpha = \sum m_i\alpha_i$. Since $\alpha \notin (p)$ it follows that at least one m_i, say m_1 is not divisible by p. Now the determinant $\det(\sigma_i(\alpha), \sigma_i(\alpha_2), \dots \sigma_i(\alpha_n))_{i=1,\dots,n}$ is a linear combination of products of elements of $\mathcal{O}_L$ with at least one fact in $\mathfrak{r}$ which implies that $D = \operatorname{disc}_{K/\mathbb{Q}}(\alpha, \alpha_2, \dots, \alpha_n)$, which is the square of this determinant, must be in $\mathfrak{r}$ for all $\mathfrak{r} \mid (p)$ of $\mathcal{O}_L$. Thus $D \in \mathfrak{r} \cap \mathbb{Q} = (p)$.

But we've seen before that $\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) = \det(B)^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(B)^2 \operatorname{disc}(K)$ where B is the matrix taking $\alpha_1, \dots, \alpha_n$ to $\alpha, \alpha_2, \dots, \alpha_n$. Since $\det(B) = m_1$ is coprime to p is follows that $p \mid \operatorname{disc}(K)$ as desired.

□

Remark 9.

1. If $M/L/K$ are number fields and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ which ramifies in L then $\mathfrak{p}$ ramifies in M.
2. If L/K are number fields, $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ above p then $\mathfrak{p}$ ramifies in L implies $p \mid \operatorname{disc}(L)$.
3. As a corollary only finitely many prime ideals of $\mathcal{O}_K$ can ramify in L because the previous remark implies that if $\mathfrak{p}$ ramifies in L then $\mathfrak{p} \mid \operatorname{disc}(L)\mathcal{O}_K$.

Example 6.14. Suppose L/K is the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. The discriminant if $\pm p^{p-2}$ so only p ramifies.

1. Clearly $(p) = (\zeta_p - 1)^{p-1}$ so if we write $\mathfrak{p} = (\zeta_p - 1)$ then $f_{\mathfrak{p}/p} = 1$ and $e_{\mathfrak{p}/p} = p - 1$.

2. If $q \neq p$ then q doesn't ramify in $\mathbb{Q}(\zeta_p)$. Let r be the smallest integer such that $q^r \equiv 1 \pmod p$ which implies that $\Phi_p(X)$, the minimal polynomial of ζ_p, will split into linear factors over $\mathbb{F}_{q^r}$ but will stay irreducible over any smaller finite field. This implies that $\Phi_p(X) \mod q$ is a product $g_1(X) \cdots g_k(X)$ where $g_i(X)$ are minimal polynomials of generators of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$. As a result $\deg g_i(X) = r$ and so $kr = p - 1$. We conclude that (q) factors over $\mathbb{Q}(\zeta_p)$ into $(p-1)/r$ factors with $e_{\mathfrak{q}/q} = 1$ and $f_{\mathfrak{q}/q} = r$.

Lecture 22
2018-03-07

6.4 Ramification in Galois extensions

Proposition 6.15. *Let L/K be a Galois extension of number fields.*

1. *$\sigma \in \mathrm{Gal}(L/K)$ acts on $\mathcal{O}_L$.*
2. *if $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_L$ above a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ then $\sigma(\mathfrak{q})$ is also a prime ideal of $\mathcal{O}_L$ above $\mathfrak{p}$.*
3. *$\mathrm{Gal}(L/K)$ acts transitively on the set of prime factors of $\mathfrak{p}\mathcal{O}_L$.*
4. *if $\mathfrak{q}, \mathfrak{q}' \mid \mathfrak{p}$ then*

$$e_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{q}'/\mathfrak{p}}$$
$$f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}'/\mathfrak{p}}$$

5. *If $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{q}_i^e$ with e the common ramification index and f the common inertia index then $ref = [L : K]$.*

Proof. First part: same polynomial.

Second part: if $xy \in \sigma(\mathfrak{q})$ then $\sigma^{-1}(x)\sigma^{-1}(y) \in \mathfrak{q}$ and so $x \in \sigma(\mathfrak{q})$ or $y \in \sigma(\mathfrak{q})$. Thus $\sigma(\mathfrak{q})$ is a prime ideal. Also $\sigma(\mathfrak{q}) \cap K = \sigma(\mathfrak{q} \cap K) = \sigma(\mathfrak{p}) = \mathfrak{p}$.

Third part: Suppose $\mathfrak{q}$ and $\mathfrak{q}'$ are distinct prime factors of $\mathfrak{p}\mathcal{O}_L$ and $\mathfrak{q}' \neq \sigma(\mathfrak{q})$ for all $\sigma \in \mathrm{Gal}(L/K)$. By the Chinese Remainder Theorem we can find $\alpha \in \mathcal{O}_L$ such that

$$\alpha \equiv 0 \pmod{\mathfrak{q}'}$$
$$\alpha \equiv 1 \pmod{\alpha(\mathfrak{q})}$$

for all $\alpha \in \mathrm{Gal}(L/K)$. Then $N_{L/K}(\alpha) = \prod \sigma_i(\alpha) \in \mathfrak{q}' \cap K = \mathfrak{p}$. But $\sigma_i(\alpha) \notin \mathfrak{p} \subset \mathfrak{q}$ for all σ giving a contradiction.

Fourth part: If $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_i}$ then $\mathfrak{p}\mathcal{O}_L = \prod \sigma(\mathfrak{q}_i)^{e_i}$. Since $\mathrm{Gal}(L/K)$ acts transitively it follows that $e_i = e_j$ for all i, j. Moreover, $k_{\mathfrak{q}_i} = k_{\mathfrak{q}_j}$ by the same argument and so the equality of inertial indices follows.

Fifth part: immediate from $\sum e_i f_i = [L : K]$. □

Definition 6.16. Suppose L/K are number fields and $\mathfrak{q} \mid \mathfrak{p}$ ideals of $\mathcal{O}_L$ and $\mathcal{O}_K$. The **decomposition group** $D_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\mathfrak{q}) = \mathfrak{q}\}$. Then $D_{\mathfrak{q}/\mathfrak{p}} = \mathrm{Stab}_{\mathrm{Gal}(L/K)}(\mathfrak{q})$.

Lemma 6.17. 1. *If $\sigma \in \mathrm{Gal}(L/K)$ then $\sigma D_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1} = D_{\sigma(\mathfrak{q})/\mathfrak{p}}$.*

2. *If $\mathfrak{p} = \prod_{i=1}^r \mathfrak{q}_i^e$ then $|D_{\mathfrak{q}/\mathfrak{p}}| = ef$.*
3. *If $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$ then σ induces an automorphism σ on $k_{\mathfrak{q}}$ which fixes $k_{\mathfrak{p}}$. This yields a homomorphism $D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$.*

Proof. Part 1: This is true of all group actions. This implies that all decomposition groups have the same cardinality.

Part 2: Since $\mathrm{Gal}(L/K)$ acts transitively on the set of primes $\mathfrak{q}_i$ in $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{q}_i^e$ it follows that $[L:K] = |\,\mathrm{Gal}(L/K)| = r|D_{\mathfrak{q}/\mathfrak{p}}|$ and so $|D_{\mathfrak{q}/\mathfrak{p}}| = ef$. Here I use that if G acts on a finite set X and $x \in X$ has stabilizer H then $Gx = (G/H)x$ has as many elements as the set G/H; if the action is transitive then $|X| = |G/H|$ and so $|H| = |G|/|X|$.

Part 3: Follows from definitions. □

Definition 6.18. For $\mathfrak{q} \mid \mathfrak{p}$ the **inertia subgroup** $I_{\mathfrak{q}/\mathfrak{p}}$ is the kernel $0 \to I_{\mathfrak{q}/\mathfrak{p}} \to D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p})$. It consists of $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$ such that $\sigma(x) \equiv x \pmod{\mathfrak{q}}$ for all $x \in \mathcal{O}_L$.

Example 6.19. In the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ the decomposition group of $\mathfrak{p}/p$ is the entire Galois group since $(p) = \mathfrak{p}^{p-1}$, here $\mathfrak{p} = (\zeta_p - 1)$. The inertia subgroup consists of σ such that $\sigma = \mathrm{id}$ on $\mathbb{F}_p$, i.e., $\sigma(x) \equiv x \pmod{\mathfrak{p}}$ for all x. It's enough to check this for $x = \zeta_p$ and if $\sigma \in G_{K/\mathbb{Q}}$ sends ζ_p to ζ_p^a for some a coprime to p then clearly $\zeta_p - 1 \mid \zeta_p^a - \zeta_p$ and so $I_{\mathfrak{p}/p} = D_{\mathfrak{p}/p} = G_{K/\mathbb{Q}}$.

Lecture 23

2018-03-09

Suppose L/K is a Galois extension of number fields. Let $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ and $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{q}_i^e$ with $f = f_{\mathfrak{q}/\mathfrak{p}}$. Let $L^D = L^{D_{\mathfrak{q}/\mathfrak{p}}}$ and $L^I = L^{I_{\mathfrak{q}/\mathfrak{p}}}$ in which case we get extensions $L/L^I/L^D/K$. Let $\mathfrak{q}_I = \mathfrak{q} \cap L^I$ and $\mathfrak{q}_D = \mathfrak{q} \cap L^D$ in which case $\mathfrak{q} \mid \mathfrak{q}_I \mid \mathfrak{q}_D \mid \mathfrak{p}$.

Theorem 6.20.

1. *The sequence $0 \to I_{\mathfrak{q}/\mathfrak{p}} \to D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p}) \to 0$ is exact and $|I_{\mathfrak{q}/\mathfrak{p}}| = e_{\mathfrak{q}/\mathfrak{p}}$.*
2. *We have*

$$\begin{array}{ll} e_{\mathfrak{q}/\mathfrak{q}_I} = e_{\mathfrak{q}/\mathfrak{p}} & f_{\mathfrak{q}/\mathfrak{q}_I} = 1 \\ e_{\mathfrak{q}_I/\mathfrak{q}_D} = 1 & f_{\mathfrak{q}_I/\mathfrak{q}_D} = f_{\mathfrak{q}/\mathfrak{p}} \\ e_{\mathfrak{q}_D/\mathfrak{p}} = 1 & f_{\mathfrak{q}_D/\mathfrak{p}} = 1 \end{array}$$

In particular $\mathfrak{q}_D$ is inert in L, $\mathfrak{q}_I/\mathfrak{p}$ is unramified, and $\mathfrak{q}/\mathfrak{q}_I$ is totally ramified.

Proof. First, $[L : L^D] = ef$ from the previous proposition and so $[L^D : K] = r$. Since $\mathrm{Gal}(L/L^D) = D_{\mathfrak{q}/\mathfrak{p}}$ acts transitively on the primes above $\mathfrak{q}_D$ but acts trivially on $\mathfrak{q}$ it follows that $f_{\mathfrak{q}/\mathfrak{q}_D} e_{\mathfrak{q}/\mathfrak{q}_D} = [L : L^D] = ef$. But $e = e_{\mathfrak{q}/\mathfrak{q}_D} e_{\mathfrak{q}_D/\mathfrak{p}}$ and $f = f_{\mathfrak{q}/\mathfrak{q}_D} f_{\mathfrak{q}_D/\mathfrak{p}}$ and so $e_{\mathfrak{q}_D/\mathfrak{p}} = f_{\mathfrak{q}_D/\mathfrak{p}} = 1$.

(1): Let $G_{k_\mathfrak{q}/k_\mathfrak{p}} = \langle \phi \rangle$ where $\phi(x) = x^{|k_\mathfrak{p}|}$ is the Frobenius generator. Let $\alpha \in \mathcal{O}_L$ such that $k_\mathfrak{q} = k_\mathfrak{p}(\alpha)$ andwrite

$$P(X) = \prod_{\sigma \in D_{\mathfrak{q}/\mathfrak{p}}} (X - \sigma(\alpha)) \in \mathcal{O}_{L^D}[X].$$

Then $P(X) \mod \mathfrak{q}_D \in k_{\mathfrak{q}_D}[X] = k_\mathfrak{p}[X]$ from the above. Since $P(X) \mod \mathfrak{q}_D$ vanishes at α it follows that

$$\phi(P(\alpha) \mod \mathfrak{q}_D) = P(\phi(\alpha)) \mod \mathfrak{q}_D = 0$$

and so $\phi(\alpha)$ is also a root of $P(X) \mod \mathfrak{q}_D$ and therefore $\phi(\alpha) \equiv \sigma(\alpha) \pmod{\mathfrak{q}_D}$ for some $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$. But then ϕ is the image of σ under $D_{\mathfrak{q}/\mathfrak{p}} \to G_{k_\mathfrak{q}/k_\mathfrak{p}}$ as α generates $k_\mathfrak{q}$ over $k_\mathfrak{p}$.

(2): Next, if $\alpha \in \mathcal{O}_L$ is such that $k_\mathfrak{q} = k_{\mathfrak{q}_I}(\alpha)$ then $g(X) = \prod_{\sigma \in I_{\mathfrak{q}/\mathfrak{p}}} (X - \sigma(\alpha)) \in \mathcal{O}_{L^I}[X]$. Since $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$ for $\sigma \in I_{\mathfrak{q}/\mathfrak{p}}$ it follows that $g(X) \equiv (X - \alpha)^{|I_{\mathfrak{q}/\mathfrak{p}}|} \pmod{\mathfrak{q}}$. The minimal polynomial of α over $k_{\mathfrak{q}_I}$ is irreducible over a perfect field so is separable. It also divides $g(X) \mod \mathfrak{q}_I$. However, $g(X)$ has a single root over $k_\mathfrak{q}$ and therefore the only separable polynomial dividing it is $X - \alpha$ which is then in $k_{\mathfrak{q}_I}[X]$. We conclude that $\alpha \in k_{\mathfrak{q}_I}$ and so $k_\mathfrak{q} = k_{\mathfrak{q}_I}(\alpha) = k_{\mathfrak{q}_I}$ so $f_{\mathfrak{q}/\mathfrak{q}_I} = 1$ as desired. From the multiplicativity of inertial indices we conclude that $f_{\mathfrak{q}_I/\mathfrak{q}_D} = f$.

If k is the number of primes of L^I above $\mathfrak{q}_D$ then $k e_{\mathfrak{q}_I/\mathfrak{q}_D} f_{\mathfrak{q}_I/\mathfrak{q}_D} = [L^I : L^D] = [D_{\mathfrak{q}/\mathfrak{p}} : I_{\mathfrak{q}/\mathfrak{p}}] \leq [k_\mathfrak{q} : k_\mathfrak{p}] = f_{\mathfrak{q}/\mathfrak{p}}$. We conclude that $k = e_{\mathfrak{q}_I/\mathfrak{q}_D} = 1$ and so $e_{\mathfrak{q}/\mathfrak{q}_I} = e_{\mathfrak{q}/\mathfrak{p}}$. □

Proposition 6.21. *Suppose L/K, $\mathfrak{q} \mid \mathfrak{p}$, L^I and L^D as before.*

1. *L^D is the largest subextension such that $\mathfrak{q} \cap L^D/\mathfrak{p}$ has $e = f = 1$.*
2. *If $G_{L/K}$ is abelian then L^D is the largest subextension in which $\mathfrak{p}$ splits completely.*
3. *L^I is the smallest subextension such that $\mathfrak{q}/\mathfrak{a}_I$ is totally ramified. Equivalently L^I is the largest extension such that $\mathfrak{q}_I/\mathfrak{p}$ is unramified.*

Proof. (1): Suppose $L/K'/K$ such that $\mathfrak{q} \cap K'/\mathfrak{p}$ has $e = f = 1$ and let $H = G_{L/K'}$. Let $\mathfrak{p}' = \mathfrak{q} \cap K'$ in which case immediately from the definition it follows that $D' = D_{\mathfrak{q}/\mathfrak{p}'} = D_{\mathfrak{q}/\mathfrak{p}} \cap H$ and similarly $I' = I_{\mathfrak{q}/\mathfrak{p}'} = I_{\mathfrak{q}/\mathfrak{p}} \cap H$. Thus the tower $L/L^I/L^D/K$ in the case of L/K' and $\mathfrak{q} \mid \mathfrak{p}'$ becomes $L/L^{I'}/L^{D'}/K'$ with $L^{I'}/L^I$ and $L^{D'}/L^D$.

Since $e_{\mathfrak{p}'/\mathfrak{p}} = f_{\mathfrak{p}'/\mathfrak{p}} = 1$ and so $e_{\mathfrak{q}/\mathfrak{p}'} = e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{q}/\mathfrak{p}'} = f_{\mathfrak{q}/\mathfrak{p}}$. This implies that $[L : L^{I'}] = [L : L^I]$ and $[L^{I'} : L^{D'}] = [L^I : L^D]$. But since $L^D \subset L^{D'}$ it follows that $L^D = L^{D'}$ and so $D_{\mathfrak{q}/\mathfrak{p}} \subset H$. This gives $K' \subset L^D$ as desired.

(2): In this case $D_{\mathfrak{q}/\mathfrak{p}}$ is independent of $\mathfrak{q}$ as decomposition groups are all conjugate. We conclude that $e = f = 1$ for all $\mathfrak{q}/\mathfrak{p}$ and therefore $\mathfrak{p}$ splits completely in L^D.

(3): Suppose K'/K is the largest subextension in which $\mathfrak{p}'/\mathfrak{p}$ is unramified. Then $e_{\mathfrak{q}/\mathfrak{p}'} = e_{\mathfrak{q}/\mathfrak{p}}$ and the same argument as in the first part shows that $L^I \subset L^{I'} \subset L$ are such that $[L : L^{I'}] = [L : L^I]$ which implies that $L^I = L^{I'}$. But then $K' \subset L^{I'} = L^I$ as desired.

□

Lecture 24

2018-03-19

Corollary 6.22. *Suppose $L, L'/K$ are number fields such that a prime ideal $\mathfrak{p}$ of K is unramified in L and L'. Then $\mathfrak{p}$ is unramified in LL'.*

Proof. Let M be the Galois closure of LL' and let $\mathfrak{r}$ be a prime of M above $\mathfrak{p}$. Let $\mathfrak{q} = \mathfrak{r} \cap L$ and $\mathfrak{q}' = \mathfrak{r} \cap L'$. Then $\mathfrak{q}/\mathfrak{p}$ unramified implies that $L \subset M^{I_{\mathfrak{r}/\mathfrak{p}}}$ and similarly for L'. Thus $LL' \subset M^{I_{\mathfrak{r}/\mathfrak{p}}}$. Varying $\mathfrak{r}$ we conclude that $\mathfrak{p}$ is unramified in LL'. □

Corollary 6.23. *Suppose L/K are number fields and $\mathfrak{p}$ is a prime of $\mathcal{O}_K$. If $\mathfrak{p}$ is unramified in L then it is unramified in the Galois closure of L/K.*

Proof. Let M/K be the normal closure of L/K. Since $\mathfrak{p}$ is unramified in L it is also unramified in $\sigma(L)$ for every $\sigma \in \mathrm{Gal}(M/K)$. Therefore, if $\mathfrak{q} \mid \mathfrak{p}$ is a prime of $\mathcal{O}_M$ and $M^I = M^{I_{\mathfrak{q}/\mathfrak{p}}}$ it follows that $\sigma(L) \subset M^I$ as M^I is the maximal extension in which p is unramified. This implies that $M = \prod \sigma(L) \subset M^I$ which means that $\mathfrak{p}$ is unramified in M. □

6.5 Applications of ramification

6.5.1 Frobenius

If L/K with ideals $\mathfrak{q} \mid \mathfrak{p}$ such that $\mathfrak{q}/\mathfrak{p}$ is unramified then $D_{\mathfrak{q}/\mathfrak{p}} \cong G_{k_{\mathfrak{q}}/k_{\mathfrak{p}}}$.

Since $G_{k_{\mathfrak{q}}/k_{\mathfrak{p}}}$ is cyclic generated by a lift of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ it follows that we may lift $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ to $D_{\mathfrak{q}/\mathfrak{p}}$, well defined up to inertia.

Lemma 6.24. *If $\sigma \in G_{L/K}$ then $\mathrm{Frob}_{\sigma(\mathfrak{q})/\mathfrak{p}} := \sigma \, \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \, \sigma^{-1}$ lifts a generator of $G_{k_{\sigma(\mathfrak{q})}/k_{\mathfrak{p}}} \cong G_{k_{\mathfrak{q}}/k_{\mathfrak{p}}}$ and thus the conjugacy class of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is independent of the choice of $\mathfrak{q}$. In particular if $G_{L/K}$ is abelian then $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ as a Galois element does not depend on $\mathfrak{q}$.*

Proof. Follows from the fact that $D_{\sigma(\mathfrak{q})/\mathfrak{p}} = \sigma D_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1}$. □

Definition 6.25. We denote $\mathrm{Frob}_{\mathfrak{p}}$ the conjugacy class of any $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$.

Example 6.26. If $p \neq q$ are odd primes then $\mathbb{Q}(\zeta_p)$ is unramified at q. Say $\mathfrak{r} \mid q$. What is $\mathrm{Frob}_{\mathfrak{r}/q} \in \mathrm{Gal}(K/\mathbb{Q})$? We know $G_{K/\mathbb{Q}} \cong \mathbb{F}_p^\times$ and if q has exact order r in $\mathbb{F}_p^\times$ then $f_{\mathfrak{r}/q} = r$ and so $\mathrm{Frob}_{\mathfrak{r}/q}(x) = x^q$ in $\mathbb{F}_{q^r}^\times$. Since $\zeta_p \in \mathbb{F}_{q^r}^\times$ it follows that $\mathrm{Frob}_{\mathfrak{r}/q}(\zeta_p) = \zeta_p^q$ and so $\mathrm{Frob}_{\mathfrak{r}/q}$ has image $q \in \mathbb{F}_p^\times$.

Remark 10. In particular, if

$$\rho : G_{L/K} \to \mathrm{GL}(n, F)$$

is a homomorphism such that $\rho(I_{\mathfrak{q}/\mathfrak{p}}) = I_n$ for all $\mathfrak{q}$ lying above a fixed prime $\mathfrak{p}$ then $\rho(\mathrm{Frob}_{\mathfrak{p}})$ has a well-defined trace. Indeed, follows from the fact that the trace of a matrix is a class function.

Lecture 25

2018-03-21

6.5.2 Dedekind's theorem on cycle types

Let $K/\mathbb{Q}$ be a finite Galois extension, $\alpha \in \mathcal{O}_K$ with minimal polynomial $f(X) \in \mathbb{Z}[X]$. Writing $\alpha_1, \ldots, \alpha_n$ for the roots of $f(X)$ it follows that $G_{K/\mathbb{Q}} \subset S_n$ as permutations of the set $\{\alpha_1, \ldots, \alpha_n\}$.

Theorem 6.27 (Dedekind)**.** *Let $K/\mathbb{Q}$ as above and p a prime number not dividing the discriminant of $f(X)$. Let*

$$f(X) \mod p = \prod_{i=1}^{r} \overline{g_i(X)} \pmod p$$

be the prime factorization in $\mathbb{F}_p[X]$ into distinct irreducible polynomials. Then there exists $\sigma \in G_{K/\mathbb{Q}}$ with cycle type (in S_n) $(\deg \overline{g_1(X)}, \ldots, \deg \overline{g_r(X)})$.

Tate. Let $R = \mathbb{Z}[\alpha_1, \ldots, \alpha_n] \subset \mathcal{O}_K$ and let $\mathfrak{m}$ be a maximal ideal of R containing p. Then $\mathfrak{m} \cap \mathbb{Z} = p\mathbb{Z}$ and therefore

$$R/\mathfrak{m} \cong \mathbb{Z}[\alpha_1, \ldots, \alpha_n]/\mathfrak{m} \cong \mathbb{F}_p(\alpha_1, \ldots, \alpha_n) = E$$

is the splitting field of $f(X) \mod p$.

The Galois group $G_{K/\mathbb{Q}}$ acts on R and we denote $D_{\mathfrak{m}} = \{\sigma \in G_{K/\mathbb{Q}} \mid \sigma(\mathfrak{m}) = \mathfrak{m}\}$. Then $D_{\mathfrak{m}}$ acts on $R/\mathfrak{m} \cong E$ and therefore we obtain a homomorphism $\Theta : D_{\mathfrak{m}} \to G_{E/\mathbb{F}_p}$.

If $\Theta(\sigma) = 1$ it follows that $\sigma(x) \equiv x \pmod{\mathfrak{m}}$ for all $x \in R$. If $\sigma \neq 1$ then $\sigma(\alpha_i) = \alpha_j$ for some $j \neq i$ (recall that $G_{K/\mathbb{Q}}$ permutes the roots of $f(X)$) and so $\alpha_i \equiv \alpha_j \pmod p$. But this would imply that p divides the discriminant of $f(X)$ contradicting the hypothesis. Therefore Θ is injective.

Note suppose that $a \in E^{\mathrm{Im}\,\Theta}$. By the Chinese remainder theorem there exists $\alpha \in R$ such that $\alpha \equiv a \pmod{\mathfrak{m}}$ and $\alpha \equiv 0 \pmod{\sigma^{-1}(\mathfrak{m})}$ for all $\sigma \in G_{K/\mathbb{Q}} - D_{\mathfrak{m}}$. Let

$$g(X) = \prod_{\sigma \in G_{K/\mathbb{Q}}} (X - \sigma(\alpha)) \in R[X]^{G_{K/\mathbb{Q}}} = \mathbb{Z}[X].$$

Modulo $\mathfrak{m}$ we see that

$$g(X) \mod \mathfrak{m} = \prod_{\sigma \in D_{\mathfrak{m}}} (X - a) \prod_{\sigma \in G_{K/\mathbb{Q}} - D_{\mathfrak{m}}} X = (X - a)^u X^v$$

by choice of α. The minimal polynomial of a over $\mathbb{F}_p$ is separable and irreducible and must divide $g(X)$ and the only such polynomial can be $X - a$. We conclude that $a \in \mathbb{F}_p$ and so $E^{\mathrm{Im}\,\Theta} = \mathbb{F}_p$ so $\mathrm{Im}\,\Theta = G_{E/\mathbb{F}_p}$ which implies that Θ is surjective as well.

Finally, consider the Frobenius map $x \mapsto x^p$ generating $G_{E/\mathbb{F}_p}$. There exists $\sigma \in D_{\mathfrak{m}}$ such that $\Theta(\sigma) = \phi$. But σ must permute the roots of each $\overline{g_i(X)}$ and since the order of $\phi(x)$ as an automorphism of the splitting field of $\overline{g_i(X)}$ is exactly $\deg \overline{g_i(X)}$ it follows that as a permutation of the roots of $\overline{g_i(X)}$ the automorphism σ is a cycle of length exactly $\deg \overline{g_i(X)}$.

Partitioning the roots $\{\alpha_1, \ldots, \alpha_n\} \mod p$ into roots of the various $\overline{g_i(X)}$ we obtain the desired result. □

Example 6.28. The polynomial $X^7 - X - 1$ is irreducible mod 2 so its Galois group has a 7-cycle. It factors into a quadratic times a quintic mod 3 so the Galois group has a σ with cycle tpe $(2,5)$. Then σ^5 is a transposition and so the Galois group has a transposition and a 7-cycle. But S_7 is generated by such elements so the Galois group is S_7.

Lecture 26
2018-03-23

7 Higher ramification

Definition 7.1. Suppose L/K is a Galois extension of number fields and $\mathfrak{q} \mid \mathfrak{p}$ are prime ideals of $\mathcal{O}_L$ and $\mathcal{O}_K$. Let

$$D_{\mathfrak{q}/\mathfrak{p},m} = \{\sigma \in D_{\mathfrak{q}/\mathfrak{p}} | \sigma(x) \equiv x \pmod{\mathfrak{q}^m}\}.$$

Example 7.2.

$$\begin{aligned} D_{\mathfrak{q}/\mathfrak{p},0} &= D_{\mathfrak{q}/\mathfrak{p}} \\ D_{\mathfrak{q}/\mathfrak{p},1} &= I_{\mathfrak{q}/\mathfrak{p}} \\ D_{\mathfrak{q}/\mathfrak{p},2} &= P_{\mathfrak{q}/\mathfrak{p}} \end{aligned}$$

where $P_{\mathfrak{q}/\mathfrak{p}}$ is "wild inertia".

Theorem 7.3. *Suppose L/K, $\mathfrak{q} \mid \mathfrak{p}$ and $D_{\mathfrak{q}/\mathfrak{p},m}$ as above.*

1. *For $m \geq 0$ the group $D_{\mathfrak{q}/\mathfrak{p},m}$ is normal in $D_{\mathfrak{q}/\mathfrak{p}}$.*
2. *The filtration $D = D_0 \supset D_1 \supset \dots$ is separated, i.e., $\cap D_m = \{1\}$.*
3. *There exist injections $I_{\mathfrak{q}/\mathfrak{p}}/P_{\mathfrak{q}/\mathfrak{p}} \hookrightarrow k_{\mathfrak{q}}^\times$ and for $m \geq 2$, $D_m/D_{m+1} \hookrightarrow k_{\mathfrak{q}}$.*
4. *$P_{\mathfrak{q}/\mathfrak{p}}$ is the p-Sylow subgroup of $I_{\mathfrak{q}/\mathfrak{p}}$.*
5. *$D_{\mathfrak{q}/\mathfrak{p}}$ is a solvable group.*

Proof. Normality is straightforward. If $\alpha \neq 1$ in $D_{\mathfrak{q}/\mathfrak{p}} \subset G_{L/K}$ then $\sigma(\alpha) \neq \alpha$ for some $\alpha \in \mathcal{O}_L$. But then $\alpha \in D_{\mathfrak{q}/\mathfrak{p},m}$ implies $\sigma(\alpha) - \alpha \in \mathfrak{q}^m$ and so $m \leq v_{\mathfrak{q}}(\sigma(\alpha) - \alpha) < \infty$. This implies the second part.

Remark that $D_0/D_1 = D_{\mathfrak{q}/\mathfrak{p}}/I_{\mathfrak{q}/\mathfrak{p}} \cong G_{k_{\mathfrak{q}}/k_{\mathfrak{p}}} \cong \mathbb{Z}/f_{\mathfrak{q}/\mathfrak{p}}\mathbb{Z}$ is cyclic.

For (3) I only have the idea: $D_{\mathfrak{q}/\mathfrak{p}} \cong G_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}$ and the maps are $D_{\mathfrak{q}/\mathfrak{p},m} \to k_{\mathfrak{q}}$ are given by

$$\sigma \mapsto \frac{\sigma(\varpi) - \varpi}{\varpi^m} \mod \varpi$$

where $\varpi \in \mathfrak{q} - \mathfrak{q}^2$ is a uniformizer for $L_{\mathfrak{q}}$. Here I used that if $\sigma \in D_{\mathfrak{q}/\mathfrak{p},m}$ then $\frac{\sigma(\varpi)-\varpi}{\varpi^m} \in \mathcal{O}_{L_{\mathfrak{q}}}$ and so its reduction mod ϖ is in $k_{L_{\mathfrak{q}}} \cong k_{\mathfrak{q}}$. Showing that the map is a well-defined injective homomorphism as in part (3) follows from standard results over the p-adics.

From (3) we conclude that $P_{\mathfrak{q}/\mathfrak{p}}$ is a p-power group and $I_{\mathfrak{q}/\mathfrak{p}}/P_{\mathfrak{q}/\mathfrak{p}}$ has order dividing $|k_{\mathfrak{q}}| - 1$ so is coprime to p. We conclude that P is the p-Sylow subgroup of I.

Finally, the filtration from (2) has abelian graded pieces so $D_{\mathfrak{q}/\mathfrak{p}}$ is solvable. □

Lecture 27
2018-03-26

7.1 The different ideal

Let L/K be number fields. Recall that $\mathrm{Tr}_{L/K} = (\cdot,\cdot)_{L/K} : L \times L \to K$ is a perfect pairing.

Definition 7.4. If I is a fractional ideal of L the dual $I^\vee$ under the trace pairing is defined as

$$I^\vee = \{x \in L | (x, I)_{L/K} \subset \mathcal{O}_K\}$$

Proposition 7.5. *1. The dual $\mathcal{O}_L^\vee$ is a fractional ideal of L.*

2. For any fractional ideal I, the dual $I^\vee$ is a fractional ideal and $I^\vee = I^{-1}\mathcal{O}_L^\vee$.

3. Have $I^{\vee\vee} = I$.

Proof. (1): Let $\alpha_1, \ldots, \alpha_n$ be in $\mathcal{O}_L$ such that they are a basis of L over K and such that $\mathcal{O}_L \supset \oplus\alpha_i\mathcal{O}_K$. Then

$$\mathcal{O}_L^\vee \subset (\oplus\alpha_i\mathcal{O}_K)^\vee$$

and if $\sum u_i\alpha_i \in \oplus K\alpha_i = L$ is in $\mathcal{O}_L^\vee$ then we see that

$$((\alpha_i, \alpha_j)_{L/K})_{1\le i,j\le n}(u_i)_{1\le i\le n} \in M_{n\times 1}(\mathcal{O}_K)$$

so $\sum u_i\alpha_i \in \det((\alpha_i, \alpha_j)_{L/K})^{-1}\mathcal{O}_K$. We conclude that $\mathcal{O}_L^\vee$ is noetherian.

Moreover, since $(\mathcal{O}_L, \mathcal{O}_L)_{L/K} \subset \mathcal{O}_K$ it follows that $\mathcal{O}_L \subset \mathcal{O}_L^\vee$ so $\mathcal{O}_L^\vee$ is a fractional ideal of L as desired: indeed, it is a noetherian submodule of L of $\mathbb{Z}$-rank at least $[L : \mathbb{Q}]$ and so it has exactly this $\mathbb{Z}$-rank.

(2): Note that $x \in I^\vee$ iff $(xI, \mathcal{O}_L) \subset \mathcal{O}_K$ iff $(xI\mathcal{O}_L, \mathcal{O}_L) \subset \mathcal{O}_K$ iff $xI \subset \mathcal{O}_L^\vee$ iff $x \in I^{-1}\mathcal{O}_L^\vee$.

(3): Straightforward. □

Definition 7.6. Let L/K be number fields. The **different** is the (fractional) ideal $\mathcal{D}_{L/K} = (\mathcal{O}_L^\vee)^{-1}$.

Remark 11. Since $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathcal{O}_K$ it follows that $\mathcal{O}_L \subset \mathcal{O}_L^\vee$ and so $\mathcal{D}_{L/K} \subset \mathcal{O}_L$ is an ideal.

Example 7.7. In class I worked out the example of quadratic extensions to see that $\mathcal{D}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}} = (2\sqrt{m})$ if $m \equiv 2, 3 \pmod 4$.

Lemma 7.8. *Suppose $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ where α has minimal polynomial $f(X) \in \mathcal{O}_K[X]$. Then*

$$\mathcal{D}_{L/K} = (f'(\alpha)).$$

(More generally $\mathcal{D}_{L/K} = (f'_\alpha(\alpha) \mid \alpha \in \mathcal{O}_L$ st $L = K(\alpha))$.)

Proof. This is a standard result. See, e.g., Theorem 3.7 in `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf` where it's only for $\mathbb{Z}$ but works for $\mathcal{O}_K$. □

Example 7.9. For $m \equiv 1 \pmod 4$ we saw that $\mathcal{O} = \mathbb{Z}[(1+\sqrt{m})/2]$ with $\alpha = (1+\sqrt{m})/2$ having minimal polynomial $X^2 - X - (m-1)/4$. Then

$$\mathcal{D}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}} = (2\alpha - 1) = (\sqrt{m}).$$

Lecture 28
2018-03-28

Theorem 7.10. *Let L/K be a finite extension of number fields and $\mathfrak{q}/\mathfrak{p}$ prime ideals.*

1. $v_\mathfrak{q}(\mathcal{D}_{L/K}) \ge e_{\mathfrak{q}/\mathfrak{p}} - 1$ and

2. $\mathfrak{q}/\mathfrak{p}$ is ramified if and only if $\mathfrak{q} \mid \mathcal{D}_{L/K}$.

Proof. (1): This is vacuous if $\mathfrak{q}/\mathfrak{p}$ is unramified so suppose otherwise. Write $e = e_{\mathfrak{q}/\mathfrak{p}}$ in which case $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^{e-1}\mathfrak{a}$ where $\mathfrak{a}$ and $\mathfrak{p}$ have the same prime factors in $\mathcal{O}_L$. Note that $v_{\mathfrak{q}}(\mathcal{D}_{L/K}) \geq e-1$ iff $\mathcal{D}_{L/K} \subset \mathfrak{q}^{e-1}$ iff $\mathfrak{q}^{-(e-1)} \subset \mathcal{O}_L^\vee$ iff $\operatorname{Tr}_{L/K}(\mathfrak{q}^{-(e-1)}) \subset \mathcal{O}_K$ iff $\mathfrak{p}\operatorname{Tr}_{L/K}(\mathfrak{q}^{-(e-1)}) \subset \mathfrak{p}$. Since $\operatorname{Tr}_{L/K}$ is trivial on K this is equivalent to $\operatorname{Tr}_{L/K}(\mathfrak{p}\mathfrak{q}^{-(e-1)}) \subset \mathfrak{p}$ iff $\operatorname{Tr}_{L/K}(\mathfrak{a}) \subset \mathfrak{p}$.

We'll show that if $\alpha \in \mathfrak{a}$ then $\operatorname{Tr}_{L/K}(\alpha) = 0$ in $k_{\mathfrak{p}}$. Let M be the matrix of multiplication by α with respect to any K-basis of L. Then M^e is the matrix of multiplication by α^e. But $\alpha^e \in \mathfrak{a}^e \subset \mathfrak{p}$ and so $\alpha^e \equiv 0 \pmod{\mathfrak{p}}$. But then $M^e = 0$ as a matrix over $k_{\mathfrak{p}}$ and so $M \mod \mathfrak{p}$ has all eigenvalues equal to 0 which implies that

$$\operatorname{Tr}_{L/K}(\alpha) = \operatorname{Tr} M = 0 \mod \mathfrak{p}$$

as desired.

(2): Suppose now that $\mathfrak{q} \mid \mathcal{D}_{L/K}$. We need to show that $\mathfrak{q}/\mathfrak{p}$ is ramified. We will only show this in the case when $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$. For the general case, remark that

$$\mathcal{D}_{L/K}\mathcal{O}_{L_{\mathfrak{q}}} = \mathcal{D}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}$$

and therefore $\mathfrak{q} \mid \mathcal{D}_{L/K}$ iff $\mathfrak{q} \mid \mathcal{D}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}$. In the local setting it is a consequence of Hensel's lemma that $\mathcal{O}_{L_{\mathfrak{q}}}$ can always be written as $\mathcal{O}_{K_{\mathfrak{p}}}[\alpha]$ for some α.

Suppose, therefore, that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and α has minimal polynomial $f(X) \in \mathcal{O}_K[X]$. Then we proved last time that $\mathcal{D}_{L/K} = (f'(\alpha))$. If $\mathfrak{q} \mid \mathcal{D}_{L/K}$ then $f'(\alpha) \equiv 0 \pmod{\mathfrak{q}}$.

Let $f(X) = \prod_{i=1}^r \overline{g_i(X)}^{e_i}$ in $k_{\mathfrak{p}}[X]$ where $\overline{g_i(X)}$ are distinct irreducible polynomials. Then

$$\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_i}$$

where $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + (g_i(\alpha))\mathcal{O}_L$.

Since $f(\alpha) = 0 \equiv 0 \pmod{\mathfrak{q}}$ it follows that $g_i(\alpha) \equiv 0 \pmod{\mathfrak{q}}$ and we may arrange so that $g_1(\alpha) \in \mathfrak{q}$ which implies that $\mathfrak{q} = \mathfrak{q}_1$. If $\mathfrak{q}/\mathfrak{p}$ were unramified then $e_1 = 1$. In this case the fact that $\overline{f'(\alpha)} \equiv 0 \pmod{\mathfrak{q}}$ implies that $g_i'(\alpha) = f'(\alpha) \equiv 0 \pmod{\mathfrak{q}}$. But this would contradict the fact that $\overline{g_1(X)}$ is a separable polynomial. □

In fact one can pin down the actual power of $\mathfrak{q}$ in $\mathcal{D}_{L/K}$.

Theorem 7.11. *With the notation of the previous theorem:*

$$v_{\mathfrak{q}}(\mathcal{D}_{L/K}) = \sum_{\ell \geq 1}(|D_{\mathfrak{q}/\mathfrak{p},\ell}| - 1).$$

We didn't prove this as most naturally it's proven in the local setting, again using Hensel's lemma. However, I gave the following consequence.

Corollary 7.12. *If $\mathfrak{q}/\mathfrak{p}$ is "tamely ramified", i.e., $p \nmid e_{\mathfrak{q}/\mathfrak{p}}$ (where $\mathfrak{q}/\mathfrak{p}/p$) then $v_{\mathfrak{q}}(\mathcal{D}_{L/K}) = e_{\mathfrak{q}/\mathfrak{p}} - 1$.*

Proof. In this case $I_{\mathfrak{q}/\mathfrak{p}}$ has size $e_{\mathfrak{q}/\mathfrak{p}}$ coprime to p and so $P_{\mathfrak{q}/\mathfrak{p}} = \operatorname{Syl}_p(I_{\mathfrak{q}/\mathfrak{p}}) = \{1\}$ and the higher ramification filtration trivializes for $\ell \geq 2$. Therefore

$$v_{\mathfrak{q}}(\mathcal{D}_{L/K} = \sum_{\ell \geq 1}(|D_{\mathfrak{q}/\mathfrak{p},\ell}| - 1) = |I_{\mathfrak{q}/\mathfrak{p}}| - 1 = e_{\mathfrak{q}/\mathfrak{p}} - 1.$$

□

8 Dirichlet series, ζ-functions and L-functions

8.1 Formal Dirichlet series

Definition 8.1. A Dirichlet series is, a priori, a formal series

$$D_{\{a_n\}}(s) = \sum_{n=1} \frac{a_n}{n^s}.$$

Lemma 8.2.

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$

Proof. Use the geometric series, open parentheses and unique factorization over $\mathbb{Z}$. □

Theorem 8.3 (Möbius inversion)**.** *Suppose (a_n) and (b_n) are sequences of complex numbers such that for all $n \geq 1$ we have $a_n = \sum_{d|n} b_d$. Then*

$$b_n = \sum_{d|n} a_d \mu(n/d)$$

where $\mu(n)$ is 0 for n not square free and $(-1)^k$ if n is square free with k prime factors.

Proof. Note that if $D_{(a_n)}(s)D_{(b_n)}(s) = D_{(c_n)}(s)$ then $c_n = \sum_{d|n} a_d b_{n/d}$. The relation in the problem can be written as $D_{(a_n)}(s) = \zeta(s)D_{(b_n)}(s)$ and so $D_{(b_n)}(s) = D_{(a_n)}(s)/\zeta(s)$ so it suffices to show that $1/\zeta(s) = D_\mu(s)$. But this is immediate as

$$1/\zeta(s) = \prod \left(1 - \frac{1}{p^s}\right) = \sum_n \frac{\mu(n)}{n^s}.$$

□

Lecture 29

2018-04-04

8.2 Analytic properties of Dirichlet series

Lemma 8.4. *If $A_t = \sum_{n=1}^t a_n = O(t^r)$ for some real number r then the Dirichlet series $\sum \frac{a_n}{n^s}$ converges on* $\mathrm{Re}(s) > r$ *and is holomorphic in that region.*

Proof. If $|A_t| \leq Bt^r$ for some B then

$$\begin{aligned}
|\sum_{n=1}^t \frac{a_n}{n^s}| &= |\sum_{n=1}^t \frac{A_n - A_{n-1}}{n^s}| \\
&= |\frac{A_t}{t^s} - A_1 + \sum_{n=1}^{t-1} A_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)| \\
&\leq Bt^{r - \mathrm{Re}\, s} + |A_1| + B\sum_{n=1}^{t-1} n^r \left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| \\
&\leq Bt^{r - \mathrm{Re}\, s} + |A_1| + B|s| \sum_{n=1}^{t-1} n^{r - \mathrm{Re}\, s - 1} \\
&\leq Bt^{r - \mathrm{Re}\, s} + |A_1| + B|s| + B|s| \left(\frac{(t-1)^{r - \mathrm{Re}\, s} - 1}{r - \mathrm{Re}\, s}\right) dx
\end{aligned}$$

and this converges when $\mathrm{Re}\, s > r$ as desired. Holomorphicity follows from the fact that this convergence is uniform on compact sets. □

Example 8.5. The Riemann zeta function $\zeta(s)$ is holomorphic in the region $\mathrm{Re}\, s > 1$ while $\sum_{n \geq 1} \frac{(-1)^n}{n^s}$ is holomorphic when $\mathrm{Re}\, s > 0$.

8.3 Counting ideals and the Dedekind zeta function

Let K be a number field.

Definition 8.6. The Dedekind ζ-function is

$$\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \frac{1}{||I||^s}.$$

Writing $c(n)$ for the number of ideals of norm exactly n this becomes

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}.$$

To establish the analytic properties of $\zeta_K(s)$ we want to study the partial sums

$$n_K(x) = \sum_{n \leq x} c(n),$$

where $n_K(x)$ is the number of ideals I with $||I|| \leq x$. Over $\mathbb{Q}$, this is easy: all ideals are of the form $n\mathbb{Z}$ and so the number $n_{\mathbb{Q}}(t) = \lfloor t \rfloor = t -$ small error.

Theorem 8.7. *Let K be a number field and $C \in \mathrm{Cl}(K)$. Let $n_C(t)$ be the number of ideals of K in the class C of norm at most t. Then*

$$n_C(t) = \kappa t + O(t^{1-\frac{1}{n}})$$

where $n = [K : \mathbb{Q}]$ and

$$\kappa = \frac{2^r (2\pi)^s R_K}{w\sqrt{|\operatorname{disc}(K)|}}$$

Here r is the number of real embeddings, $2s$ is the number of torsion embeddings, w is the number of roots of unity in K and R_K, the **regulator**, *is the volume of $\log \iota(\mathcal{O}_K^\times)$ in $\Delta = \ker(\mathbb{R}^{r+s} \xrightarrow{\Sigma} \mathbb{R})$.*

Summing over $C \in \mathrm{Cl}(K)$ we get the estimate

$$n_K(t) = h_K \kappa t + O(t^{1-1/n})$$

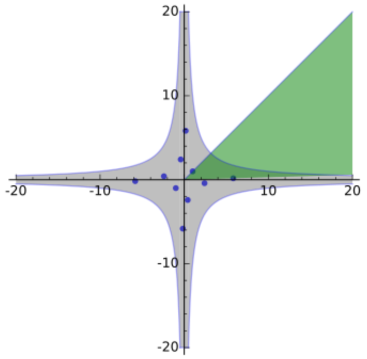
Example 8.8. When $K = \mathbb{Q}(i)$ then $n_K(x)$ is the number of $a = m + ni$ with norm $|a|^2 = m^2 + n^2 \leq x$, up to the units $\pm 1, \pm i$. This is approximately the area of the quarter circle of radius $\sqrt{x}$, i.e., $\pi x/4$. This equals $2\pi/(w\sqrt{|d_K|})$ as $w = 4$ and $d_K = -4$.

Example 8.9. When $K = \mathbb{Q}(\sqrt{2})$ we expect

$$n_K(x) \approx \frac{2^2 \cdot \log(\sqrt{2}+1)}{2\sqrt{8}} = \frac{\log(\sqrt{2}+1)}{\sqrt{2}}.$$

Embed $K \hookrightarrow K_\infty \cong \mathbb{R}^2$ via $\iota(a + b\sqrt{2}) = (a + b\sqrt{2}, a - b\sqrt{2})$. Then $N_{K/\mathbb{Q}}(z) = \prod \iota(z)$ and therefore $|N_{K/\mathbb{Q}}(z)| \leq x$ iff $\iota(z) = (a, b)$ with $|ab| \leq x$.

Recall that $\mathcal{O}_K^\times = \pm(\sqrt{2}+1)^{\mathbb{Z}} = \pm\alpha^{\mathbb{Z}}$. Note that every $z \in K_\infty$ is equivalent up to $\iota(\mathcal{O}_K^\times)$ to an element of the first quadrant. We conclude that $K_\infty/\iota(\mathcal{O}_K^\times)$ has as fundamental domain the cone in the first quadrant between the ray containing the unit $\iota(1)$ and the ray containing the unit $\iota(\alpha^2)$.



It suffices to estimate the number of lattice points in $\mathcal{O}_K$ inside the intersection of the two regions.

Remark 12. I also explained that if we choose vol_v Haar measures on $K_v^\times$ which are self-dual, i.e., they satisfy the Plancherel formula in Fourier analysis, then

$$\mathrm{vol}(\mathbb{A}_K^1/K^\times) = \frac{2^r(2\pi)^s R_K h_K}{w\sqrt{|d_K|}}.$$

Indeed, one has exact sequences

$$1 \to K_\infty^1 \prod \mathcal{O}_v^\times/\mathcal{O}_K^\times \to \mathbb{A}_K^1/K^\times \to \mathrm{Cl}(K) \to 1$$

and

$$1 \to \{\pm 1\}^r(S^1)^s \prod \mathcal{O}_v^\times/\mu_\infty(K) \to K_\infty^1 \prod \mathcal{O}_v^\times \to \mathbb{R}^{r+s-1}/\log(\mathcal{O}_K^\times) \to 0$$

and so

$$\mathrm{vol}(\mathbb{A}_K^1/K^\times) = \mathrm{vol}(\{\pm 1\}^r(S^1)^s \prod \mathcal{O}_v^\times)\,\mathrm{vol}(\mathbb{R}^{r+s-1}/\log(\mathcal{O}_K^\times))\,\mathrm{vol}(\mathrm{Cl}(K))/\mathrm{vol}(\mu_\infty(K)).$$

Finally, $\mathrm{vol}(\{\pm 1\}) = 2$, $\mathrm{vol}(S^1) = 2\pi$, $\mathrm{vol}(\mathrm{Cl}(K)) = h_K$, $\mathrm{vol}(\mu_\infty(K)) = w$, $\mathrm{vol}(\mathbb{R}^{r+s-1}/\log(\mathcal{O}_K^\times)) = R_K$, and for the self-dual Haar measures

$$\mathrm{vol}(\prod \mathcal{O}_v^\times) = \prod \mathrm{vol}_v(\mathcal{O}_v^\times) = \prod ||\mathcal{D}_{K_v/\mathbb{Q}_p}||^{-1/2} = ||\mathcal{D}_{K/\mathbb{Q}}||^{-1/2} = |d_K|^{-1/2}.$$

Lecture 30
2018-04-06

Lemma 8.10. *Fix $J \in C^{-1}$. There is a bijection between the sets $\{I \in C | ||I|| \leq t\}$ and $\{(\alpha) \subset J | |N_{K/\mathbb{Q}}(\alpha) \leq t||J||\}$.*

Proof. The maps are $I \mapsto IJ$ which has to be principal (1 in $\mathrm{Cl}(K)$) and $(\alpha) \mapsto (\alpha)J^{-1}$ which lies in C. Indeed, $||IJ|| = ||I||||J|| \leq t||J||$ and $||(\alpha)J^{-1}|| = ||(\alpha)||||J||^{-1} = |N_{K/\mathbb{Q}}(\alpha)|||J||^{-1} \leq t$. □

Proof of the theorem. By the previous lemma we only need to count principal ideals $(\alpha) \subset J$ with $||(\alpha)|| \leq t||J||$ and the difficulty consists in the fact that (α) determines the element α up to a unit.

Recall the map $K \to K_\infty = \mathbb{R}^n$ given by $\iota : x \mapsto (\sigma_i(x), \mathrm{Re}\,\tau_i(x), \mathrm{Im}\,\tau_i(x))$ where σ_i are the real embeddings and $\tau_i, \overline{\tau}_i$ are the complex embeddings. Then $\iota(J) \subset \mathbb{R}^n$ is a lattice. Further recall the maps $\log : \mathbb{R}^n - 0 \to \mathbb{R}^{r+s}$ given by $(x_i) \mapsto (\log(|x_1|), \ldots, \log(|x_r|), \log(x_{r+1}^2 + x_{r+2}^2), \ldots)$ and $\sum : \mathbb{R}^{r+s} \to \mathbb{R}$ given by adding the coordinates. Then for every $x \in K^\times$ one has $\sum \log \iota(x) = \log |N_{K/\mathbb{Q}}(x)|$. Remark that $\ker \log = \{\pm 1\}^r(S^1)^s$ and that the kernel of $\log \circ \iota$ is the group of roots of unity in K.

Consider $\mathcal{F}$ a fundamental parallelotope of $\log \iota(\mathcal{O}_K^\times) \subset \Delta \subset \mathbb{R}^{r+s}$, i.e., the span of a basis of $\log \iota(\mathcal{O}_K^\times)$ with coefficients in $[0, 1)$. Also let $\mathcal{D} \subset \mathbb{R}^{r+s}$ the region spanned by $\mathcal{F}$ and the ray pointing in the direction of $(1, \ldots, 1, 2, \ldots, 2)$ (where 1 appears r times and 2 appears s times).

Note that $n_C(t)$ is the number of $\{(\alpha) \subset J || N_{K/\mathbb{Q}}(\alpha)| \leq t||J||\} \cong \{\alpha \in J||N_{K/\mathbb{Q}}(\alpha) \leq t||J||\}/\mathcal{O}_K^\times$ and via ι this becomes

$$n_C(t) = w^{-1}|\{\iota(\alpha) \in \iota(J)|N(\iota(\alpha)) \leq t||J||\}/\iota(\mathcal{O}_K^\times)|$$

because $|\ker \log \circ \iota| = w$.

Further composing with $\log : \mathbb{R}^n \to \mathbb{R}^{r+s}$ we see that $\mathbb{R}^{r+s}/\log \iota(\mathcal{O}_K^\times) \cong \mathcal{D}$ and, since $\ker \log \iota$ consists of roots of unity it follows that

$$\{\iota(\alpha) \in \iota(J)|N(\iota(\alpha)) \leq t||J||\}/\iota(\mathcal{O}_K^\times) \cong \{\iota(\alpha) \in \iota(J)|N(\iota(\alpha)) \leq t||J||, \log \iota(\alpha) \in \mathcal{D}\}$$

Let $\mathcal{D}_\lambda \subset \mathcal{D}$ consist of tuples $(x_1, \ldots, x_{r+s}) \in \mathcal{D}$ with $\sum(x_i) \leq \lambda$. Then $N(\iota(\alpha)) \leq t||J||$ is equivalent to $\sum \log \iota(\alpha) \leq \log(t||J||)$ and so, putting everything together,

$$n_C(t) = w^{-1}|\{\iota(\alpha) \in \iota(J)|N(\iota(\alpha)) \leq t||J||, \log \iota(\alpha) \in \mathcal{D}\}| = w^{-1}|\{\iota(\alpha) \in \iota(J)| \log \iota(\alpha) \in \mathcal{D}_{\log(t||J||)}\}$$

Then

$$n_C(t) = w^{-1}|\{\iota(\alpha) \in \iota(J) \cap \mathcal{D}'_{\log(t||J||)}\}| = w^{-1}|\iota(J) \cap \log^{-1} \mathcal{D}_{\log(t||J||)}|$$

We need to estimate $n_C(t) = w^{-1}|\iota(J) \cap \log^{-1} \mathcal{D}_{\log(t||J||)}|$.

It is a general analytical statement from the geometry of number that if $\mathcal{C}$ is a region in $\mathbb{R}^n$ with a "nice" boundary $\partial\mathcal{C}$ and $\Lambda \subset \mathbb{R}^n$ is a lattice then

$$\begin{aligned}|\Lambda \cap x\mathcal{C}| &= \frac{\mathrm{vol}(x\mathcal{C})}{\mathrm{vol}(\Lambda)} + O\left(\frac{\mathrm{vol}(\partial x\mathcal{C})}{\mathrm{vol}(\partial\Lambda)}\right) \\ &= x^n \frac{\mathrm{vol}(\mathcal{C})}{\mathrm{vol}(\Lambda)} + O(x^{n-1})\end{aligned}$$

(where $\mathrm{vol}(\partial\Lambda)$ represents the surface area of the fundamental parallelotope).

We will apply this to $\Lambda = \iota(J)$ and $\mathcal{C} = \log^{-1} \mathcal{D}_{\log(||J||)}$. First, note that

$$\log^{-1} \mathcal{D}_{\log(t||J||)} = \sqrt[n]{t} \log^{-1} \mathcal{D}_{\log(||J||)}$$

Indeed, under the log map the region $x \log^{-1} \mathcal{D}_{\log(||J||)}$ becomes $(\log(x), \ldots, \log(x), 2\log(x), \ldots, 2\log(x)) + \mathcal{D}_{\log(||J||)}$ which by definition is just $\mathcal{D}_{n\log(x)+\log(||J||)} = \mathcal{D}_{\log(x^n||J||)}$.

Thus

$$\begin{aligned}n_C(t) &= w^{-1}|\iota(J) \cap \log^{-1} \mathcal{D}_{\log(t||J||)}| \\ &= w^{-1}|\iota(J) \cap \sqrt[n]{t} \log^{-1} \mathcal{D}_{\log(||J||)}| \\ &= w^{-1} \frac{\mathrm{vol}(\log^{-1} \mathcal{D}_{\log(||J||)})}{\mathrm{vol}(\iota(J))} t + O(t^{1-1/n})\end{aligned}$$

Claim: For all λ we have

$$\mathrm{vol}(\log^{-1} \mathcal{D}_\lambda) = 2^r \pi^s e^\lambda.$$

Assuming this claim we compute

$$\frac{\mathrm{vol}(\log^{-1} \mathcal{D}_{\log(||J||)})}{\mathrm{vol}(\iota(J))} = \frac{2^r \pi^s ||J||}{2^{-s}||J||\sqrt{|d_K|}}$$

and the desired result follows.

Proof of claim. It remains to compute $\mathrm{vol} \log^{-1} \mathcal{D}_\lambda$. Consider the map $\log : K_\infty - 0 \to \mathbb{R}^{r+s}$ from before. Writing $(u_1, \ldots, u_r, v_1, \ldots, v_s)$ for the variables on $\mathbb{R}^{r+s}$ and changing variables $x_i = \varepsilon_i e^{u_i}$ with

$\varepsilon_i \in \{\pm 1\}$ and $y_j = e^{v_j/2}\cos\theta_j$, $z_j = e^{v_j/2}\sin\theta_j$ with $\theta_j \in [0, 2\pi]$ we see that

$$\begin{aligned}\operatorname{vol}\log^{-1}\mathcal{D}_\lambda &= \int_{\log^{-1}\mathcal{D}_\lambda} \prod dx_i \prod dy_j dz_j \\ &= \int_{\mathcal{D}_\lambda}\int_{\{\pm1\}^r}\int_{(S^1)^s} 2^{-s} e^{\sum u_i + \sum v_j} \prod d\theta_j \prod d\varepsilon_i \prod du_i \prod dv_j \\ &= 2^r \pi^s \int_{\mathcal{D}_\lambda}\int_{(S^1)^s} e^{\sum u_i + \sum v_j} \prod du_i \prod dv_j\end{aligned}$$

Writing $t = \sum u_i + \sum v_j \leq \lambda$ and using Fubini we see that

$$\begin{aligned}\operatorname{vol}\log^{-1}\mathcal{D}_\lambda &= 2^r\pi^s \int_{\mathcal{F}}\int_{-\infty}^{\lambda} e^t dt d\operatorname{vol}_{\mathcal{F}} \\ &= 2^r\pi^s \operatorname{vol}(\mathcal{F}) e^\lambda\end{aligned}$$

as desired since $R_K = \operatorname{vol}(\mathcal{F})$. □

Lecture 31

2018-04-09

8.4 The analytic class number formula

Let K be a number field.

Proposition 8.11. *$\zeta_K(s)$ converges and is holomorphic for* $\operatorname{Re}(s) > 1$.

Proof.

$$\begin{aligned}\zeta_K(s) &= \sum_I \frac{1}{||I||^s} \\ &= \sum_{t=1}^{\infty} \sum_{||I||=t} \frac{1}{t^s}\end{aligned}$$

Writing a_n for the number of ideals of norm n it follows that $n_K(t) = \sum_{n=1}^t a_n = O(t)$ and convergence follows from the lemma. □

Theorem 8.12 (Analytic Class Number Formula)**.** *Let K be a number field.*

The Riemann ζ-function $\zeta(s)$ can be extended to a meromorphic function on $\operatorname{Re} s > 0$ *with a simple pole at $s = 1$ and*

$$\lim_{s\to 1}(s-1)\zeta(s) = 1$$

The Dedekind ζ-function $\zeta_K(s)$ can be extended to a meromorphic function on $\operatorname{Re} s > 1 - 1/[K:\mathbb{Q}]$ *with a simple pole at $s = 1$ with*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^r(2\pi)^s h_K R_K}{w\sqrt{|d_K|}}.$$

In fact $\zeta_K(s)$ can be extended meromorphically to $\operatorname{Re} s > 0$ *with a simple pole only at $s = 1$.*

Proof. Part one. The function $f(s) = (1 - 2^{1-s})\zeta(s)$ can be written as

$$f(s) = \sum_{n=1}^{\infty} (-1)^{n-1} n^{-s}$$

for $\operatorname{Re} s > 1$ but the latter is is holomorphic for $\operatorname{Re} s > 0$ by the lemma as $\sum_{n=1}^{t}(-1)^{n-1} = O(1)$. This implies that $\zeta(s)$ is meromorphic with poles possibly when $2^{1-s} = 1$, i.e., when $(1-s)\log(2) = 2\pi i k$ for some $k \in \mathbb{Z}$.

Similarly the function $g(s) = (1-3^{1-s})\zeta(s)$ can be written as

$$g(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

for $\operatorname{Re} s > 1$ where $a_n = 1$ unless $3 \mid n$ in which case $n = -2$. Again $g(s)$ makes sense as a holomorphic function when $\operatorname{Re} s > 0$ and so $\zeta(s)$ is meromorphic with poles possibly when $3^{1-s} = 1$, i.e., when $(1-s)\log(3) = 2\pi i \ell$ for some $\ell \in \mathbb{Z}$.

Suppose $\zeta(s)$ has a pole at some s such that $(1-s)\log(2) = 2\pi i k$ and $(1-s)\log(3) = 2\pi i \ell$. Then $2^\ell = 3^k$ and so $\ell = k = 0$ and $s = 1$. Thus $\zeta(s)$ is meromorphic with only possible pole at $s = 1$. Let's compute the residue:

$$\begin{aligned}\lim_{s\to 1}(s-1)\zeta(s) &= \lim_{s\to 1}\frac{f(s)(s-1)}{1-2^{1-s}}\\ &= \frac{f(1)}{\log(2)}\\ &= 1\end{aligned}$$

as

$$f(1) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots = \log(1+1) = \log(2)$$

Part two. Recall that for $\operatorname{Re} s > 1$ one has

$$\begin{aligned}\zeta_K(s) &= \sum_{n=1}^{\infty}\frac{n_K(n) - n_K(n-1)}{n^s}\\ &= h_K\kappa\zeta(s) + \sum_{n=1}^{\infty}\frac{n_K(n) - n_K(n-1) - \kappa h_K}{n^s}\end{aligned}$$

Again by our lemma it follows that $\zeta_K(s) - h_K\kappa\zeta(s)$ is holomorphic for $\operatorname{Re}(s) > 1 - 1/[K:\mathbb{Q}]$ since

$$\sum_{n=1}^{t}(n_K(n) - n_K(n-1) - \kappa h_K) = n_K(t) - \kappa h_K t = O(t^{1-1/[K:\mathbb{Q}]})$$

This implies that $\zeta_K(s) - h_K\kappa\zeta(s)$ is holomorphic for $\operatorname{Re} s > 1 - 1/[K:\mathbb{Q}]$ and so the same must be true of $\zeta_K(s)$. For the residue computation note that

$$\begin{aligned}\lim_{s\to 1}(s-1)\zeta_K(s) &= \lim_{s\to 1}(s-1)(\zeta_K(s) - h_K\kappa\zeta(s)) + h_K\kappa\lim_{s\to 1}(s-1)\zeta(s)\\ &= h_K\kappa\end{aligned}$$

as in the first limit one has the product of two functions which are continuous at $s = 1$.

□

8.5 Functional equations

Recall the Euler Γ function:

$$\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx$$

We will use two variants:

$$\begin{aligned}\Gamma_{\mathbb{R}}(s) &= \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\\ \Gamma_{\mathbb{C}}(s) &= 2(2\pi)^{-s}\Gamma(s)\end{aligned}$$

Lemma 8.13. *1. $\Gamma(x+1) = x\Gamma(x)$ and thus*

$$\Gamma(x-n) = \frac{\Gamma(x)}{(x-1)\cdots(x-n)}.$$

2. $\Gamma(x)$ is holomorphic in the region $\operatorname{Re} x > 0$.

3. Γ has no zeros and has simple poles only at negative integers.

4. $\Gamma(n) = (n-1)!$ for $n \geq 1$.

5. $\Gamma(1/2) = \sqrt{\pi}$ and $\Gamma(1/2-n) = \dfrac{(-4)^n n! \sqrt{\pi}}{(2n)!}$.

Proof. (1): Integration by parts and induction.

(2): The integral converges absolutely and uniformly in compact sets when $\operatorname{Re} x > 1$ so it is holomorphic in this region.

(3): Uses more complex analysis than what I'm willing to do. The part about poles follows from part (1).

(4): Induction.

(5): Using $x = y^2$ we get

$$\Gamma(1/2) = \int_0^\infty x^{-1/2} e^{-x} dx = 2\int_0^\infty e^{-y^2} dy = \int_{-\infty}^\infty e^{-y^2} dy = \sqrt{\pi}.$$

The formula at $1/2 - n$ follows from part (1). □

Theorem 8.14. *Let K be a number field with r_1 real and $2r_2$ complex places. Write*

$$\Lambda(s) = |d_K|^{s/2} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} \zeta_K(s)$$

Then $\Lambda(s) = \Lambda(1-s)$ when $\operatorname{Re} s \in (0,1)$ in which case $\zeta_K(s)$ and $\zeta_K(1-s)$ make sense. Defining $\Lambda(s)$ by $\Lambda(s)$ for $\operatorname{Re} s > 0$ and $\Lambda(1-s)$ for $\operatorname{Re} s < 1$ we obtain the meromorphic continuation of $\zeta_K(s)$ to all of $\mathbb{C}$ with a simple pole at $s = 1$.

Proof. Not given. Follows from the Poisson summation formula for Fourier transforms. Perhaps later I'll give the proof for the Riemann zeta function. □

Corollary 8.15 (A basic version of Birch and Swinnerton-Dyer)**.** *The function ζ_K has a zero of order $r_1 + r_2 - 1$ at $s = 0$ and $\zeta_K(s)$ has the following Taylor expansion around $s = 0$:*

$$\zeta_K(s) = -\frac{h_K R_K}{w_K} s^{r_1+r_2-1} + O(s^{r_1+r_2}).$$

Proof. Using the previous lemma on the Γ-function we get $\Gamma_{\mathbb{R}}(s) = \frac{2\pi}{s}\Gamma_{\mathbb{R}}(s+2)$ and $\Gamma_{\mathbb{C}}(s) = \frac{2\pi}{s}\Gamma_{\mathbb{C}}(s+1)$ have simple poles at $s = 0$. These formulae transform the functional equation into

$$|d_K|^{s/2} \frac{(2\pi)^{r_1}}{s^{r_1}} \Gamma_{\mathbb{R}}(s+2)^{r_1} \frac{(2\pi)^{r_2}}{s^{r_2}} \Gamma_{\mathbb{C}}(s+1)^{r_2} \zeta_K(s) = |d_K|^{(1-s)/2} \Gamma_{\mathbb{R}}(1-s)^{r_1} \Gamma_{\mathbb{C}}(1-s)^{r_2} \zeta_K(1-s)$$

Recall that ζ_K has a simple pole at $s = 1$ and so $\zeta_K(1-s) = \dfrac{f(s)}{s}$ where $f(0) = -\dfrac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w\sqrt{|\operatorname{disc}(K)|}}$. Therefore

$$\zeta_K(s) = \frac{s^{r_1+r_2-1} f(s) |d_K|^{(1-2s)/2} \Gamma_{\mathbb{R}}(1-s)^{r_1} \Gamma_{\mathbb{C}}(1-s)^{r_2}}{2^{r_1+r_2} \pi^{r_1+r_2} \Gamma_{\mathbb{R}}(s+2)^{r_1} \Gamma_{\mathbb{C}}(s+1)^{r_2}}$$

In this expression the only factor vanishing at $s = 0$ is $s^{r_1+r_2-1}$ and so the order of vanishing is as desired. Taking derivatives at 0 we get

$$\begin{aligned}\frac{\zeta_K^{(r_1+r_2-1)}(0)}{(r_1+r_2-1)!} &= \frac{f(0)\sqrt{|d_K|}\Gamma_{\mathbb{R}}(1)^{r_1}\Gamma_{\mathbb{C}}(1)^{r_2}}{2^{r_1+r_2}\pi^{r_1+r_2}\Gamma_{\mathbb{R}}(2)^{r_1}\Gamma_{\mathbb{C}}(1)^{r_2}} \\ &= \frac{f(0)\sqrt{|d_K|}\pi^{-r_2}}{2^{r_1+r_2}\pi^{r_1+r_2}\pi^{-r_1}\pi^{-r_2}} \\ &= -\frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{2^{r_1+r_2}\pi^{r_2}w} \\ &= -\frac{h_K R_K}{w}\end{aligned}$$

using $\Gamma_{\mathbb{R}}(1) = \pi^{-1/2}\Gamma(1/2) = 1$, $\Gamma_{\mathbb{C}}(1) = 2(2\pi)^{-1} = \pi^{-1}$ and $\Gamma_{\mathbb{R}}(2) = \pi^{-1}$.

□

Lecture 32
2018-04-11

8.6 *L*-functions of characters

Definition 8.16. Let G be a finite abelian group. A **character** of G is a group homomorphism $\chi : G \to \mathbb{C}^\times$.

Proposition 8.17. *The set $\widehat{G}$ of all characters of G is a finite abelian group.*

1. *If G and H are finite abelian groups then $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$.*
2. *There is a non-canonical isomorphism $G \approx \widehat{G}$.*
3. *There is a canonical isomorphism $\widehat{\widehat{G}} \cong G$ given by $g \mapsto (\chi \mapsto \chi(g))$.*

Proof. Part one: If $\chi \in \widehat{G \times H}$ let $\chi_1(g) = \chi(g, 1)$ and $\chi_2(h) = \chi(1, h)$. Then $\chi(g, h) = \chi_1(g)\chi_2(h)$ and we get a map $\widehat{G \times H} \to \widehat{G} \times \widehat{H}$ given by $\chi \mapsto \chi_1 \times \chi_2$. This is clearly an isomorphism.

Part two: If $G = \mathbb{Z}/n\mathbb{Z}$ then every $\chi \in \widehat{G}$ is uniquely defined by $\chi(1) \in \mu_n$ and so $\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mu_n$. But $\mu_n \approx \mathbb{Z}/n\mathbb{Z}$ identifying ζ_n^k with k for a choice of primitive n-th root ζ_n. The result now follows from this and part one.

Part three: The given map is a canonical homomorphism. Suppose it is not injective. Then there exists $g \in G$ such that $\chi(g) = 1$ for every $\chi \in \widehat{G}$. But there is a nontrivial character of $\langle g \rangle$ sending g to a primitive root of 1 of order equal to the order of g. This defines a character $G \twoheadrightarrow \langle g \rangle \to \mathbb{C}^\times$ which is not trivial on g. Finally, we have an injective homomorphism between finite sets of the same size (from part two) and so it is an isomorphism. □

Definition 8.18. A character mod N is a character of the group $(\mathbb{Z}/N\mathbb{Z})^\times$, i.e., a homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. The L-function of χ is the Dirichlet series

$$L(\chi, s) = \sum_{(n,N)=1} \frac{\chi(n)}{n^s}$$

which converges to a holomorphic function on $\operatorname{Re} s > 1$.

Proposition 8.19. *If χ is a character mod N which is not the trivial character then*

1. $\sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(k) = 0$
2. *$L(\chi, s)$ is analytic when $\operatorname{Re} s > 0$.*

Proof. If G is any finite abelian group and $\chi : G \to \mathbb{C}^\times$ is any nontrivial homomorphism then $\sum_{g\in G} \chi(g) = 0$. Indeed, $\chi \neq 1$ implies that $\chi(h) \neq 1$ for some $h \in G$. Then

$$\begin{aligned}\sum_{g\in G} \chi(g) &= \sum_{gh\in G} \chi(gh) \\ &= \chi(h) \sum_{g\in G} \chi(g)\end{aligned}$$

and so the sum must vanish.

Look at the partial sums $A_t = \sum_{n=1}^{t} \chi(t)$. The sum over representatives of $\mathbb{Z}/N\mathbb{Z}$ is 0 and so $|A_t| \leq \sum |\chi(k)| = \varphi(N)$ is bounded. Thus $L(\chi, s)$ is holomorphic for $\operatorname{Re} s > 0$ by the lemma from lecture 29. □

Lecture 33
2018-04-13

8.7 Euler products and factorizations of Dedekind zeta functions

Proposition 8.20. *Have*

$$\begin{aligned}\zeta(s) &= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \\ \zeta_K(s) &= \prod_{\mathfrak{p}} \left(1 - \frac{1}{||\mathfrak{p}||^s}\right)^{-1} \\ L(\chi, s) &= \prod_{p\nmid N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}\end{aligned}$$

where p is a prime and $\mathfrak{p}$ is a prime ideal.

Proof. Follows from unique factorization in Dedekind domains and the fact that χ is a homomorphism. □

Proposition 8.21. *Suppose G is a finite abelian group and $N > 1$ an integer.*

1. *If $\chi \in \widehat{G}$ then*

$$\prod_{g\in G} (X - \chi(g)) = (X^a - 1)^b$$

where $a = |\operatorname{Im} \chi|$ is the order of χ in $\widehat{G}$ and $b = |\ker \chi| = |G|/a$.

2. *If $p \in (\mathbb{Z}/N\mathbb{Z})^\times$ has order exactly r then*

$$\prod_{\chi\in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} (X - \chi(p)) = (X^r - 1)^{\varphi(N)/r}$$

Proof. Part one: Since χ is a homomorphism, $\operatorname{Im} \chi \subset \mathbb{C}^\times$ is a subgroup and thus isomorphic to μ_a for $a = |\operatorname{Im} \chi|$. Now

$$\begin{aligned}\prod_{g\in G} (X - \chi(g)) &= \prod_{g\in \ker \chi} \prod_{h\in G/\ker \chi} (X - \chi(gh)) \\ &= \prod_{h\in G/\ker \chi} (X - \chi(h))^b \\ &= \prod_{\zeta\in \operatorname{Im} \chi \cong \mu_a} (X - \zeta)^b \\ &= (X^a - 1)^b\end{aligned}$$

Finally, the statements about a being the order of χ in $\widehat{G}$ and $ab = |G|$ are immediate from the fact that $\operatorname{Im}\chi = \mu_a$ and the first isomorphism theorem.

Part two: Let $G = (\mathbb{Z}/N\mathbb{Z})^\times$ and $\psi_p \in \widehat{\widehat{G}}$ given by $\psi_p(\chi) = \chi(p)$ for any $\psi \in \widehat{G}$. Then $\prod\limits_{\chi\in\widehat{G}}(X - \chi(p)) = \prod\limits_{\chi\in\widehat{G}}(X - \psi_p(\chi))$. We will apply part one to the group $\widehat{G}$ and the element ψ_p and deduce that this product is $(X^a - 1)^b$ where $a = |\operatorname{Im}\psi_p|$ is the order of ψ_p and $b = |\ker\psi_p| = \varphi(N)/a$. But the order of ψ_p in $\widehat{\widehat{G}}$ is the same as the order r of p in G. □

Theorem 8.22. *Suppose $K = \mathbb{Q}(\zeta_N)$ for $N > 1$. Then*

$$\zeta_K(s) = \prod_{\mathfrak{p}|N}\left(1 - \frac{1}{||\mathfrak{p}||^s}\right)^{-1}\prod_{\chi\in\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} L(\chi, s)$$

where

$$\zeta(s) = \prod_{p|N}\left(1 - \frac{1}{p^s}\right)^{-1} L(1, s)$$

for the trivial $\bmod N$ *character.*

Proof. We only need to show that

$$\prod_{\mathfrak{p}\nmid N}\left(1 - \frac{1}{||\mathfrak{p}||^s}\right)^{-1} = \prod_{\chi\in\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} L(\chi, s)$$

which is equivalent to

$$\prod_{\mathfrak{p}\nmid N}\left(1 - \frac{1}{||\mathfrak{p}||^s}\right)^{-1} = \prod_{\chi\in\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}}\prod_{p\nmid N}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

For this it suffices to show that

$$\prod_{\chi\in\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}}\left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{\mathfrak{p}|p}\left(1 - \frac{1}{||\mathfrak{p}||^s}\right)$$

Let r be the number of prime ideals of K above p and f the inertia index of $\mathfrak{p}$ (independent of $\mathfrak{p} \mid p$ since $K/\mathbb{Q}$ is Galois). Then the RHS is $\left(1 - \frac{1}{p^{fs}}\right)^r$ and so it suffices to show that

$$\prod_{\chi\in\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}}(p^s - \chi(p)) = (p^{fs} - 1)^r$$

By a previous proposition the LHS is $(p^{as} - 1)^b$ where a is the order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$ and $b = \varphi(N)/a$. Thus is suffices to show that $a = f$.

But f is the degree of any irreducible factor of the cyclotomic polynomial Φ_N in $\mathbb{F}_p[X]$ (since $\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathbb{Z}[\zeta_N]$ so there is no restriction on p). Such an irreducible factor has as roots primitive N-th roots of 1 which would then be defined over $\mathbb{F}_{p^f}$ (and no smaller subfield) and the result follows as on the homework from the fact that $\mathbb{F}_{p^f}^\times \cong \mathbb{Z}/(p^f - 1)\mathbb{Z}$ and so $N \mid p^f - 1$ (but not so for smaller exponents) which is equivalent to f being the order a of p. □

Corollary 8.23. *If χ is a nontrivial character* $\bmod N$ *then $L(\chi, 1) \neq 1$.*

Proof. From the previous theorem we get

$$(s-1)\zeta_K(s) = (s-1)\zeta(s)\prod_{p\nmid N}\left(1-\frac{1}{p^s}\right)\prod_{\mathfrak{p}|N}\left(1-\frac{1}{||\mathfrak{p}||^s}\right)^{-1}\prod_{\chi\neq 1}L(\chi,s)$$

Taking $\lim\limits_{s\to 1}$ we get that $\prod_{\chi\neq 1}L(\chi,1)$ is nonzero. □

8.8 Analytic density of primes

Lemma 8.24. *Let $K/\mathbb{Q}$ be a number field. As $s\to 1^+$ we have the estimate*

$$\sum_{\mathfrak{p}}\frac{1}{||\mathfrak{p}||^s} = \log\zeta_K(s) + O(1) = -\log(s-1) + O(1)$$

Proof. We have

$$\begin{aligned}
\log\zeta_K(s) &= \log\prod_{\mathfrak{p}}\left(1-\frac{1}{||\mathfrak{p}||^s}\right)^{-1}\\
&= -\sum_{\mathfrak{p}}\log\left(1-\frac{1}{||\mathfrak{p}||^s}\right)\\
&= \sum_{\mathfrak{p}}\sum_{n\geq 1}\frac{1}{n||\mathfrak{p}||^{ns}}\\
&= \sum_{\mathfrak{p}}\frac{1}{||\mathfrak{p}||^s} + \sum_{\mathfrak{p}}\sum_{n\geq 2}\frac{1}{n||\mathfrak{p}||^{ns}}
\end{aligned}$$

and so

$$\begin{aligned}
\left|\log\zeta_K(s) - \sum_{\mathfrak{p}}\frac{1}{||\mathfrak{p}||^s}\right| &\leq \sum_{\mathfrak{p}}\sum_{n\geq 2}\frac{1}{n||\mathfrak{p}||^{ns}}\\
&< \sum_{\mathfrak{p}}\frac{1}{||\mathfrak{p}||^s(||\mathfrak{p}||^s-1)}\\
&< \sum_{\mathfrak{p}}\frac{2}{||\mathfrak{p}||^{2s}}\\
&< 2\zeta_K(2s)
\end{aligned}$$

since $||\mathfrak{p}||^s > 2$ and so $||\mathfrak{p}||^s - 1 > ||\mathfrak{p}||^s/2$.

The first estimate then follows from the fact that $\zeta_K(s)$ is holomorphic around $s=2$. The second estimate follows from the fact that $\zeta_K(s)$ has a simple pole at $s=1$. □

Lecture 34
2018-04-16

Definition 8.25. Suppose $\mathcal{P}$ is a set of prime ideals of $K/\mathbb{Q}$. The set $\mathcal{P}$ is said to have **natural density** $d(\mathcal{P})$ if

$$d(\mathcal{P}) = \lim_{x\to\infty}\frac{|\{\mathfrak{p}\in\mathcal{P}|||\mathfrak{p}||<x\}|}{|\{\mathfrak{p}|||\mathfrak{p}||<x\}|}$$

exists.

The set $\mathcal{P}$ is said to have **Dirichlet density** $\delta(\mathcal{P})$ if

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

exists.

Note that, if they exist, then $\delta(\mathcal{P}) \leq 1$ and $d(\mathcal{P}) \leq 1$.

Proposition 8.26. *1. If $\mathcal{P}$ is finite then $d(\mathcal{P}) = \delta(\mathcal{P}) = 0$.*

2. If $\mathcal{P} \subset \mathcal{Q}$ then $\delta(\mathcal{P}) \leq \delta(\mathcal{Q})$.

3. Have $\delta(\mathcal{P} \cup \mathcal{Q}) \leq \delta(\mathcal{P}) + \delta(\mathcal{Q})$ with equality when $\delta(\mathcal{P} \cap \mathcal{Q}) = 0$ (e.g., when the intersection is finite or empty).

4. If $d(\mathcal{P})$ exists and equals $\alpha \in [0,1]$ then $\delta(\mathcal{P}) = d(\mathcal{P}) = \alpha$.

Proof. The only part requiring work is the last one, but we'll skip that since it reduces to basic, but unenlightening calculus. □

8.9 Primes in arithmetic progression

The goal of this section is the following theorem.

Theorem 8.27 (Dirichlet's theorem on primes in arithmetic progressions)**.** *Let $n \geq 2$ and a coprime to n. The set $\mathcal{P}_{a,n}$ of primes $p \equiv a \pmod n$ has density (either natural or Dirichlet) equal to $1/\varphi(n)$. In particular the set $\mathcal{P}_{a,n}$ is infinite.*

Proof. We will only show that the Dirichlet density is $1/\varphi(n)$, which already implies that $\mathcal{P}_{a,n}$ is infinite.

First, writing $G = (\mathbb{Z}/n\mathbb{Z})^\times$ note that

$$\sum_{\chi\in\widehat{G}} \chi(a^{-1}p) = \begin{cases} \varphi(n) & p \equiv a \pmod n \\ 0 & p \not\equiv a \pmod n \end{cases}$$

for any prime p. Thus

$$\varphi(n) \sum_{p\in\mathcal{P}_{a,n}} \frac{1}{p^s} = \sum_{p} \sum_{\chi\in\widehat{G}} \frac{\chi(a^{-1}p)}{p^s}$$

For $s \to 1^+$ we have

$$\begin{aligned} \sum_{\chi\in\widehat{G}} \chi(a^{-1}) \log(L(\chi,s)) &= -\sum_{\chi\in\widehat{G}} \sum_{p} \chi(a^{-1}) \log\left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_{\chi,p} \sum_{n\geq 1} \frac{\chi(a^{-1})\chi(p)^n}{np^{ns}} \\ &= \varphi(n) \sum_{p\in\mathcal{P}_{a,n}} \frac{1}{p^s} + \sum_{\chi,p} \sum_{n\geq 2} \frac{\chi(a^{-1})\chi(p)^n}{np^{ns}} \end{aligned}$$

using the previous identity. The term $\displaystyle\sum_{\chi,p}\sum_{n\geq 2} \frac{\chi(a^{-1})\chi(p)^n}{np^{ns}}$ is holomorphic around $s = 1$ by an argument similar to the estimate from the previous section.

We conclude that for $s \to 1^+$ we have

$$\begin{aligned}\varphi(n) \sum_{p \in \mathcal{P}_{a,n}} \frac{1}{p^s} &= \sum_{\chi \in \widehat{G}} \chi(a^{-1}) \log(L(\chi, s)) + O(1) \\ &= \log(L(1,s)) + \sum_{\chi \neq 1} \chi(a^{-1}) \log(L(\chi, s))\end{aligned}$$

Now

$$\log(\zeta(s)) = \log(L(1,s)) - \sum_{p \mid n} \log\left(1 - \frac{1}{p^s}\right) = \log(L(1,s)) + O(1)$$

around $s = 1$ and so

$$\begin{aligned}\delta(\mathcal{P}_{a,n}) &= \lim_{s \to 1^+} \frac{\sum_{p \in \mathcal{P}_{a,n}} p^{-s}}{-\log(s-1)} \\ &= \lim_{s \to 1^+} \frac{\varphi(n)^{-1} \log(\zeta(s)) + \varphi(n)^{-1} \sum_{\chi \neq 1} \log(L(\chi, s)) + O(1)}{-\log(s-1)} \\ &= \lim_{s \to 1^+} \frac{\varphi(n)^{-1} \log(\zeta(s)) + O(1)}{-\log(s-1)} \\ &= \frac{1}{\varphi(n)}\end{aligned}$$

Here we used that for $\chi \neq 1$, $L(\chi, 1) \neq 0$ and so $\log(L(\chi, 1)) = O(1)$.

□

Lecture 35
2018-04-18

8.10 The Chebotarëv density theorem

First, it's read Chebotaryóv.

Let L/K be a finite Galois extension of number fields. Recall that for $\mathfrak{q} \mid \mathfrak{p}$ prime ideals of L and K one has $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in G_{L/K}$ well-defined up to an element of inertia $I_{\mathfrak{q}/\mathfrak{p}}$. If $\mathfrak{q}/\mathfrak{p}$ is unramified then $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is uniquely defined. Moreover, if $\mathfrak{q}' = \sigma(\mathfrak{q})$ is some other prime ideals above $\mathfrak{p}$ where $\sigma \in G_{L/K}$ then $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}} = \sigma \, \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \, \sigma^{-1}$ and so one gets a well-defined conjugacy class

$$\mathrm{Frob}_{\mathfrak{p}} = \{\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in G_{L/K} | \mathfrak{q} \mid \mathfrak{p}\}$$

Theorem 8.28 (The Chebotarëv density theorem)**.** *Suppose $C \subset G_{L/K}$ is a conjugacy class. Then the set $\mathcal{P}_C$ of prime ideals $\mathfrak{p}$ of K such that the conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$ is C has both natural and Dirichlet density*

$$\delta(\mathcal{P}_C) = \frac{|C|}{|G_{L/K}|}$$

Proposition 8.29. *The Dirichlet theorem on primes in arithmetic progressions is equivalent to Chebotarev for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.*

Proof. Indeed, taking $L = \mathbb{Q}(\zeta_n)$ and $K = \mathbb{Q}$ then $G_{L/K}$ is abelian $\cong (\mathbb{Z}/n\mathbb{Z})^\times$ and so every conjugacy class consists of one element. Taking $C = a \in (\mathbb{Z}/n\mathbb{Z})^\times$ we deduce that the density of primes p such that $\mathrm{Frob}_p = a$ is $1/\varphi(n)$. But Frob_p is $p \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

Proposition 8.30. *If Chebotarev is true for the abelian Galois extension M/K then it is true for L/K for any $M/L/K$.*

Proof. Let $c \in G_{L/K}$ with preimage $\{c_1, \ldots, c_d\} \subset G_{M/K}$ where $d = [M : L]$. Then

$$\begin{aligned}\delta(\{\mathfrak{p} | \operatorname{Frob}_{\mathfrak{p}} = c\}) &= \delta(\{\mathfrak{p} | \operatorname{Frob}_{\mathfrak{p}} \in \{c_1, \ldots, c_d\}\}) \\ &= \sum \delta(\{\mathfrak{p} | \operatorname{Frob}_{\mathfrak{p}} = c_i\}) \\ &= \frac{d}{|G_{M/K}|} \\ &= \frac{1}{|G_{L/K}|}\end{aligned}$$

as desired. □

Example 8.31.

1. If $P(X) \in \mathbb{Z}[X]$ is monic irreducible then Chebotarev implies that the density of p such that $P(X) \mod p$ splits as a product of distinct irreducible polynomials of degrees $(d_1, \ldots, d_k)$ is equal to the probability that an element of $G_{K/\mathbb{Q}} \subset S_n$ has cycle type $(d_1, \ldots, d_k)$. I gave as an example `2017s-m30820/handouts/galQ.pdf`.
2. The density of primes p such that $\Phi_N(X) \mod p$ factors as a product of irreducible polynomials of degree $d \mid \varphi(N)$ is $\frac{n_d}{\varphi(N)}$ where n_d is the number of elements of degree d in $(\mathbb{Z}/N\mathbb{Z})^\times$.
3. $X^3 - 2$ stays irreducible modulo 1/3 of primes, splits into linear factors modulo 1/6 of the primes, and factors as a linear times an irreducible quadratic modulo 1/2 of the primes.

Lecture 36
2018-04-20

I proved in class Chebotarev using a step-by-step reduction that can be found, e.g., in Fried-Jarden's Field arithmetic. I'll attach some handwritten notes, but here are the ideas:

1. Extensions of the form $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ follow from Dirichlet.
2. Analogously one gets general cyclotomic extensions of the form $K(\zeta_n)/K$.
3. From the previous proposition one deduces Chebotarev for subextensions of cyclotomic extensions.
4. I proved that given any L/K and any $m \geq 1$ there exists M/K cyclic of degree m and cyclotomic (i.e., inside some $K(\zeta_M)$) such that $M \cap L = K$.
5. I used this to show Chebotarev for cyclic extensions L/K.
6. I then used the fact that the density of primes $\mathfrak{p}$ such that $||\mathfrak{p}|| > ||\mathfrak{p} \cap \mathbb{Q}||$ is 0 and deduced Chebotarev for all L/K.

Lecture 37
2018-04-23

8.11 Fourier transforms

If G is an abelian topological group we denote by $\widehat{G}$ the group of homomorphisms $\chi : G \to S^1 \subset \mathbb{C}^\times$. Then $\widehat{G}$ is a topological abelian group, called the Pontryagin dual of G. A basis for the topology on $\widehat{G}$ is given by sets of the form $\{\chi : G \to S^1 \mid \chi(K) \subset U\}$ where $K \subset G$ is compact and $U \subset S^1$ is open.

I mentioned that if G is compact then $\widehat{G}$ is discrete, and if G is discrete then $\widehat{G}$ is compact.

Example 8.32.

1. If $G = \mathbb{Z}/n\mathbb{Z}$ then $\widehat{G} \cong \mu_n$ canonically, and noncanonically it is $\widehat{G} \approx \mathbb{Z}/n\mathbb{Z}$ associating to $a \in \mathbb{Z}/n\mathbb{Z}$ the character $\chi_a(x) = \zeta^{ax}$ for a choice of $\zeta \in \mu_n$.

2. If $G = \mathbb{Z}$ then $\widehat{G} \cong S^1$ is compact.

3. If $G = \mathbb{R}$ then $\widehat{G} \approx \mathbb{R}$ associating to $a \in \mathbb{R}$ the character $\chi_a(x) = e^{2\pi i a x}$.

4. If $G = S^1$ compact then $\widehat{G} \cong \mathbb{Z}$ is discrete, associating to $a \in \mathbb{Z}$ the character $\chi_a(x) = x^a$.

5. If $G = \mathbb{C}$ then $\widehat{G} \approx \mathbb{C}$ associating to $a \in \mathbb{C}$ the character $\chi_a(z) = e^{4\pi i \operatorname{Re}(az)}$.

If G is locally compact we choose a Haar measure μ_G. For a Schwarz function $f : G \to \mathbb{C}$ we define the Fourier transform $\widehat{f} : \widehat{G} \to \mathbb{C}$ by

$$\widehat{f}(\chi) = \int_G f(g)\chi(g) d\mu_G,$$

a Schwarz function on $\widehat{G}$. Note that $\widehat{f}$ depends on μ_G.

Some special cases:

1. Let $G = \mathbb{Z}/n\mathbb{Z}$ with μ_G the discrete measure. With $\widehat{G} \approx G$ from above get $\widehat{f} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ given by

$$\widehat{f}(x) = \sum_y f(y) e^{2\pi i x y / n}.$$

2. Let $G = \mathbb{R}$ with μ_G the measure dx. With $\widehat{G} \approx G$ from above get $\widehat{f} : \mathbb{R} \to \mathbb{C}$ given by

$$\widehat{f}(x) = \int_{-\infty}^{\infty} f(y) e^{2\pi i x y} dy.$$

Lecture 38

2018-04-25

The L^2-norm of an L^2-integrable function $f : G \to \mathbb{C}$ is

$$||f||_2 = \int_G |f(g)|^2 d\mu_G.$$

When $G = \mathbb{Z}/n\mathbb{Z}$ and μ_G is the discrete measure then

$$||f||_2 = \sum_x |f(x)|^2.$$

Proposition 8.33. *Let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ be a function.*

1. *(Double Fourier) $\widehat{\widehat{f}}(x) = nf(-x)$.*

2. *(Plancherel identity) $||\widehat{f}||_2 = n||f||_2$.*

3. *$\widehat{\overline{f}}(x) = \overline{\widehat{f}(-x)}$.*

Proof. We begin by remarking that if $\zeta \in \mu_n$ then

$$\sum_{a \in \mathbb{Z}/n\mathbb{Z}} \zeta^a = \begin{cases} 0 & \zeta \neq 1 \\ n & \zeta = 1 \end{cases},$$

which can be proven using the geometric series.

(1): Write $\zeta = e^{2\pi i/n}$. Then

$$\begin{aligned}\widehat{\widehat{f}}(x) &= \sum_y \widehat{f}(y)\zeta^{xy} \\ &= \sum_y \sum_z f(z)\zeta^{xy+yz} \\ &= \sum_z f(z) \sum_y (\zeta^{x+z})^y\end{aligned}$$

The sum over y is then 0 unless $x + z = 0 \mod n$ in which case it is n and so

$$\widehat{\widehat{f}}(x) = nf(-x)$$

as desired.

(2): We compute

$$\begin{aligned}||\widehat{f}||_2 &= \sum_y |\widehat{f}(x)|^2 \\ &= \sum_y \widehat{f}(y)\overline{\widehat{f}(y)} \\ &= \sum_y \sum_{a,b} f(a)\overline{f(b)}\zeta^{ay-bz} \\ &= \sum_{a,b} f(a)\overline{f(b)} \sum_y (\zeta^{a-b})^y\end{aligned}$$

Again the sum over y is 0 unless $a = b$ in which case it is n, and so

$$||\widehat{f}||_2 = n\sum_a f(a)\overline{f(a)} = n||f||_2.$$

(3): This is straightforward. □

8.12 Gauss sums of characters

A character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ also gives a composite character $\chi : (\mathbb{Z}/Nd\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ for any d. Thus a character $\chi \mod N$ is also a character $\mod Nd$ and so given χ there is an ambiguity on what group it is a character of. In particular, given $\chi \mod N$ there might exists $d \mid N$ such that χ comes from a character $\mod d$. For example the trivial character always comes from a character $\mod 1$.

Definition 8.34. The conductor f_χ of a character χ is the smallest integer such that χ is a character mod f_χ. A character $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ is said to be **primitive** if n is the conductor of χ.

For example the character mod 8 taking 1 and 5 to 1 and 3 and 7 to -1 in fact comes from the character mod 4 taking k to $(-1)^{(k-1)/2}$ and so has conductor 4.

Proposition 8.35. *Suppose $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ is a primitive character. We extend by 0 to a function $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$. Then*

$$\widehat{\chi}(x) = \overline{\chi(x)}\widehat{\chi}(1).$$

Proof. If $(x, n) = 1$ then $\{xy | y \in \mathbb{Z}/n\mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$ and so

$$\begin{aligned}\widehat{\chi}(x) &= \sum_y \chi(y)\zeta^{xy} \\ &= \sum_z \chi(zx^{-1})\zeta^z \\ &= \chi(x)^{-1}\widehat{\chi}(1).\end{aligned}$$

The result follows from: $\chi(x)\overline{\chi}(x) = |\chi(x)|^2 = 1$ because $\operatorname{Im}\chi$ consists of roots of unity.

If $(x, n) = d > 1$ then the RHS vanishes as $\chi(x) = 0$. Write $x = dk$ and $n = gm$. The character χ has conductor n and so it does not come from a character modulo m. In other words χ is not trivial on the kernel $1 + m\mathbb{Z}/n\mathbb{Z}$ of the quotient $(\mathbb{Z}/n\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$. Thus for some $u \equiv 1 \pmod{m}$ and coprime to n the character $\chi(u) \neq 1$. But then multiplying by u coprime to n permutes terms so

$$\begin{aligned}
\widehat{\chi}(x) &= \sum_y \chi(y)\zeta^{xy} \\
&= \sum_y \chi(yu)\zeta^{xyu} \\
&= \chi(u)\sum_y \chi(y)\zeta^{xyu}
\end{aligned}$$

Since $u \equiv 1 \pmod{m}$ it follows that $\zeta^{xyu} = e^{2\pi i dkyu/dm} = e^{2\pi i kyu/m} = e^{2\pi i ky/m} = \zeta^{xy}$ which implies that

$$\begin{aligned}
\widehat{\chi}(x) &= \chi(u)\sum_y \chi(y)\zeta^{xy} \\
&= \chi(u)\widehat{\chi}(x)
\end{aligned}$$

Therefore $\widehat{\chi}(x) = 0$ as $\chi(u) \neq 1$. □

Definition 8.36. Suppose $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ is a primitive character extended by 0 to $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$. The Gauss sum of χ is

$$\tau(\chi) = \widehat{\chi}(1).$$

Proposition 8.37. *1.* $\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi})$.

2. $|\tau(\chi)| = \sqrt{n}$.

Proof. (1):

$$\begin{aligned}
\overline{\tau(\chi)} &= \overline{\widehat{\chi}(1)} \\
&= \widehat{\overline{\chi}}(-1) \\
&= \overline{\overline{\chi(-1)}}\widehat{\overline{\chi}}(1) \\
&= \chi(-1)\tau(\overline{\chi}).
\end{aligned}$$

(2): From Plancherel we know that $||\overline{\chi}||_2 = n||\chi||_2$. But the LHS is

$$||\widehat{\chi}||_2 = \sum |\widehat{\chi}(x)|^2 = \sum |\overline{\chi}(x)\widehat{\chi}(1)|^2 = |\tau(\chi)|^2 \sum |\chi(x)|^2 = \varphi(n)|\tau(\chi)|^2$$

and the RHS is

$$n||\chi||_2 = n\sum |\chi(x)|^2 = n\varphi(n).$$

□

Example 8.38. 1. If $\chi_3 = \left(\frac{\cdot}{3}\right)$ then $\tau(\chi_3) = \zeta_3 - \zeta_3^2 = i\sqrt{3}$.

2. More generally, if $\operatorname{Im}\chi = \{-1, 1\}$ then $\chi = \overline{\chi}$ and we conclude that

$$\overline{\tau(\chi)} = \chi(-1)\tau(\chi)$$

If $\chi(-1) = 1$ then $\tau(\chi) \in \mathbb{R}$ and if $\chi(-1) = -1$ then $\tau(\chi) \in i\mathbb{R}$.

3. If $\chi = \left(\frac{\cdot}{p}\right)$ for an odd prime p then χ is primitive $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ with image $\{-1, 1\}$. If $p \equiv 1 \pmod{4}$ then $\chi(-1) = 1$ so $\tau(\chi) \in \mathbb{R}$. If $p \equiv 3 \pmod{4}$ then $\chi(-1) = -1$ so $\tau(\chi) \in i\mathbb{R}$.

Lecture 39
2018-04-27

8.13 Special values of L-functions at non-positive integers

The Bernoulli numbers B_n are the coefficients

$$\frac{t}{e^t-1} = \sum B_n \frac{t^n}{n!}$$

If χ is a character then $B_{n,\chi}$ is defined by

$$\sum_{a=1}^{f_\chi} \frac{te^{at}}{e^{f_\chi t}-1} = \sum_{n\geq 0} B_{n,\chi}\frac{t^n}{n!}$$

with

$$B_{1,\chi} = \frac{1}{f_\chi}\sum_{a=1}^{f_\chi}\chi(a)a$$

In fact one can show that the definition of $B_{n,\chi}$ doesn't change if one replaces f_χ in the definition by any multiple of it.

From homework we know:

$$\zeta(2n) = \frac{(-1)^{n+1}B_{2n}(2\pi)^{2n}}{2(2n)!}$$
$$\zeta(1-2n) = -\frac{B_{2n}}{2n}$$

Suppose now that χ is a primitive character, i.e., a character modulo its conductor f_χ. If χ were treated as a character modulo $f_\chi d$ then:

$$L(\chi,s) = \prod_{p\mid d, p\nmid f_\chi}\left(1-\frac{\chi(p)}{p^s}\right)^{-1} L(\chi \mod f_\chi d, s)$$

Theorem 8.39. *If χ is a primitive character then*

$$L(\chi, 1-n) = -\frac{B_{n,\chi}}{n}$$

Proof. This is a long but not difficult computation in complex analysis. □

8.14 The functional equation

A section containing two theorems without proofs because either they are too hard or unilluminating.

Definition 8.40. A character χ is said to be odd if $\chi(-1) = -1$. It is even if $\chi(-1) = 1$.

Theorem 8.41. *Suppose χ is a character of conductor f_χ. If $\chi(-1) = -1$ let $\delta_\chi = 1$ and if $\chi(-1) = 1$ let $\delta_\chi = 0$. Then*

$$f_\chi^{s/2}\Gamma_{\mathbb{R}}(s+\delta_\chi)L(\chi,s) = W_\chi f_\chi^{(1-s)/2}\Gamma_{\mathbb{R}}(1-s+\delta_\chi)L(\overline{\chi},1-s)$$

where $W_\chi = \dfrac{\tau(\chi)}{i^{\delta_\chi}\sqrt{f_\chi}}$.

Recall that we showed in class that if $K = \mathbb{Q}(\zeta_N)$ then

$$\zeta_K(s) = \prod_{\mathfrak{p}\mid N}\left(1-\frac{1}{||\mathfrak{p}||^s}\right)\prod_{\chi \mod N} L(\chi \mod N, s)$$

Theorem 8.42. *If $K/\mathbb{Q}$ is abelian then*

$$\zeta_K(s) = \prod_{\chi} L(\chi, s)$$

where χ ranges through the character of the abelian Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. This is analogous to the factorization from the section on primes in arithmetic progressions. □

8.15 Special value of L-functions at 1

Theorem 8.43. *Suppose χ is a nontrivial character.*

1. *If $\chi(-1) = -1$ (χ is said to be odd) then*

$$L(\chi, 1) = \frac{\pi i \tau(\chi)}{f_\chi} B_{1,\overline{\chi}}$$

2. *If $\chi(-1) = 1$ (χ is said to be even) then*

$$L(\chi, 1) = -\frac{\tau(\chi)}{f_\chi} \sum_{a=1}^{f_\chi} \overline{\chi}(a) \log|1 - \zeta_{f_\chi}^a|$$

Proof. Part one: Using the functional equation for χ odd with $\delta_\chi = 1$ we get

$$\begin{aligned} L(\chi, 1) &= \frac{W_\chi f_\chi^{-1/2} \Gamma_{\mathbb{R}}(1) L(\overline{\chi}, 0)}{\Gamma_{\mathbb{R}}(2)} \\ &= -\frac{\pi \tau(\chi) B_{1,\overline{\chi}}}{i f_\chi} \\ &= \frac{\pi i \tau(\chi)}{f_\chi} B_{1,\overline{\chi}} \end{aligned}$$

where $\Gamma_{\mathbb{R}}(2) = \pi^{-1}\Gamma(2) = \pi^{-1}$ and $\Gamma_{\mathbb{R}}(1) = \pi^{-1/2}\Gamma(1/2) = 1$.

Lecture 40

2018-04-30

Part two: For $\chi(-1) = 1$ and $\chi \neq 1$ everything converges in the following computation. We are using the results from Gauss sums for replacing $\chi(n)$ with Gauss sums.

$$\begin{aligned} L(\chi, 1) &= \sum_{n \geq 1} \frac{\chi(n)}{n} \\ &= \sum_{n \geq 1} \frac{\widehat{\chi}(n)}{n \widehat{\chi}(1)} \\ &= \sum_{n \geq 1} \frac{1}{n \tau(\overline{\chi})} \sum_{a=1}^{f} \overline{\chi}(a) e^{2\pi i a n / f} \\ &= \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{f} \overline{\chi}(a) \sum_{n \geq 1} \frac{1}{n} e^{2\pi i a n / f} \\ &= -\frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{f} \overline{\chi}(a) \log(1 - \zeta_f^a) \end{aligned}$$

But $\tau(\overline{\chi}) = \chi(-1)\overline{\tau(\chi)} = \overline{\tau(\chi)} = f/\tau(\chi)$ and $\log(1-\zeta_f^a) + \log(1-\zeta_f^{-a}) = 2\log|1-\zeta_f^a|$ and so

$$\begin{aligned} L(\chi,1) &= -\frac{\tau(\chi)}{f}\frac{1}{2}\sum_{a=1}^{f}(\overline{\chi}(a)\log(1-\zeta_f^a) + \overline{\chi}(-a)\log(1-\zeta_f^{-a})) \\ &= -\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\overline{\chi}(a)\log|1-\zeta_{f_\chi}^a| \end{aligned}$$

since $\chi(-1) = 1$.

□

Corollary 8.44. *If χ is odd then $B_{1,\chi} \neq 0$.*

Proof. Follows from the previous theorem and the fact that $L(\chi,1) \neq 0$. There is no elementary proof of this. □

Example 8.45. If $\chi_3 = \left(\frac{\cdot}{3}\right)$ then we compute $B_{1,\overline{\chi_3}} = -1/3$ and we already computed $\tau(\chi_3) = i\sqrt{3}$ and $f_\chi = 3$ and so we deduce that

$$L(\chi_3, 1) = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \cdots = \frac{\pi}{3\sqrt{3}}$$

9 Kummer's proof of Fermat's Last Theorem for regular primes

Definition 9.1. A prime p is **regular** if $p \nmid h_{\mathbb{Q}(\zeta_p)}$.

Remark 13. Most primes < 100 are regular but it's still open whether there exist infinitely many regular primes. On the other hand, it's not hard to show that there exist infinitely many irregular primes.

Remark 14. One can show that p is regular if and only if p does not divide the numerator of the Bernoulli number B_k for odd $k \leq p-3$. This is computationally fast.

Theorem 9.2 (Kummer)**.** *Suppose $p > 3$ is a regular prime. Then $x^p + y^p = z^p$ in $\mathbb{Z}$ implies $xyz = 0$.*

As a preparatory point I stated, with examples, but no proof:

Proposition 9.3. *Let $p > 2$ be a prime. Then $\mathbb{Z}[\zeta_p]^\times = \langle\zeta_p\rangle\mathbb{Z}[\zeta_p + \zeta_p^{-1}]^\times$.*

Remark 15. I added that if $a, b \not\equiv 0 \pmod{p}$ then $\dfrac{1-\zeta_p^a}{1-\zeta_p^b} \in \mathbb{Z}[\zeta_p]^\times$ and showed explicitly how to write it as a root of unity times a unit in the maximal totally real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

For more information check out `https://www3.nd.edu/~ajorza/courses/2014s-m80220/notes/lecture29.pdf` and `https://www3.nd.edu/~ajorza/courses/2014s-m80220/notes/lecture30.pdf` on cyclotomic units.

Lecture 41
2018-05-02

Today's lecture (and the end of the previous) was devoted to showing:

Theorem 9.4. *Let $x, y, z \in \mathbb{Z}$ not divisible by p, a regular prime > 3. Then $x^p + y^p \neq z^p$.*

Proof. I followed Emily Riehl's senior thesis. □

At the end I monologued a little about class field theory and the Langlands program.