Math 129 - Number Fields

Taught by Barry Mazur
Notes by Dongryul Kim

Spring 2016

This course was taught by Barry Mazur. We met twice a week on Tuesdays and Thursdays from 10:00 to 11:30 in Science Center 507. We used the textbook *Number fields* by Daniel M. Marcus. There were 11 students taking the course. There was an in-class final exam, and the course also required one thirty-minutes-long presentation. The course assistant was Kevin Yang.

Contents

1 January 26, 2016

There will be half-hour presentations. I have experimented this in Math 124, and it worked well.

1.1 Algebraic numbers and integers

Definition 1.1. An **algebraic number** is a root of a (monic) polynomial $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ for $a_i \in \mathbb{Q}$. An **algebraic integer** is a root of a monic polynomial with integer coefficients.

These have connection with many branches of mathematics. We can look at the ring A of algebraic integers and talk about $\operatorname{Spec} A$, which we will discuss. This A can be viewed as a lattice in the Euclidean space thus a geometric structure. For instance, the ring

$$\mathbb{Z}[\sqrt{-D}] = \{a + b\sqrt{-D} : a, b \in \mathbb{Z}\}$$

on the complex plane looks like a rectangular lattice. There are also connections with analysis; the zeta function contains information about the nature of prime ideals in A.

Proposition 1.2. *An algebraic integers that is a rational number is an integer.*

Proof. Let $\frac{m}{n}$ be an algebraic integer for $(m, n) = 1$. Then there will be integers $a_{d-1}, a_{d-2}, \ldots, a_0$ such that

$$\left(\frac{m}{n}\right)^d + a_{d-1}\left(\frac{m}{n}\right)^{d-1} + \cdots + a_0 = 0.$$

Then multiplying n^d to both sides, we get

$$m^d + a_{d-1}nm^{d-1} + \cdots + a_0 n^d = 0$$

and thus n divides m. This means that $n = \pm 1$. □

Proposition 1.3. *If α is an algebraic number then there is an integer $N \geq 1$ such that $N\alpha$ is an algebraic number.*

Proof. There is are integers a_i and $N \neq 0$ that makes α a root of the polynomial

$$f(X) = X^d + \frac{a_{d-1}}{N}X^{d-1} + \frac{a_{d-2}}{N}X^{d-2} + \cdots + \frac{a_0}{N} = 0.$$

Then

$$N^d X^d + a_{d-1}N^{d-1}X^{d-1} + a_{d-2}N \cdot N^{d-2}X^{d-2} + \cdots + N^d a_0 = 0$$

and thus $Y = N\alpha$ is the root of

$$F(Y) = Y^d + a_{d-1}Y^{d-1} + a_{d-2}NY^{d-2} + \cdots + N^d a_0 = 0.$$

□

Proposition 1.4. *Let z_1, z_2 be two complex numbers that are linearly independent over $\mathbb{Q}$. Suppose that*

$$\begin{cases} \alpha z_1 = a_{11} z_1 + a_{12} z_2 \\ \alpha z_2 = a_{21} z_1 + a_{22} z_2 \end{cases}$$

for some rational numbers $a_{11}, a_{12}, a_{21}, a_{22}$. Then α is an algebraic number.

Proof. Let

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Q}).$$

Then we see that $\det(\alpha \cdot I_2 - A) = 0$ and hence α is a root of the characteristic polynomial

$$X^2 - \mathrm{tr}(A)X + \det(A).$$

This completes the proof. □

Note that if the a_{ij}s were integers, then α should have been an algebraic integer.

We can generalize it to more variables. In fact, we have the following claim.

Proposition 1.5. *Let $V \subset \mathbb{C}$ be a finite-dimensional $\mathbb{Q}$-vector space, and let $M \subset \mathbb{C}$ be a finitely generated abelian group. Consider an $\alpha \in \mathbb{C}$. If $\alpha \cdot V \subseteq V$, then α is an algebraic number. If $\alpha \cdot M \subseteq M$, then α is an algebraic integer.*

Actually we need to use the fundamental theorem of finitely generated abelian groups. Since M is finitely generated and torsion-free (M is a subset of $\mathbb{C}$), it has to be isomorphic to some $\mathbb{Z}^r$. Then we can run the exactly same argument for the previous proposition.

Also note that the converse is also true. Given an algebraic number/integer $\alpha \in \mathbb{C}$, we can set V/M to be the vector space/abelian group generated by the powers of α.

Corollary 1.6. *Let $K/\mathbb{Q}$ be a field extension of finite degree. Then every element of K is an algebraic number.*

Proof. Just set $V = K$. □

Theorem 1.7. *The sum and product of two algebraic numbers are again algebraic numbers. The sum and product of two algebraic integers are agin algebraic integers.*

Proof. This is because $\mathbb{Q}[\alpha, \beta]$ is a finitely generated vector space over $\mathbb{Q}$, and $\mathbb{Z}[\alpha, \beta]$ is a finitely generated abelian group. □

1.2 Quadratic fields

For a extension field K over $\mathbb{Q}$, we denote by A_K the right of algebraic integers in K. Let us try to describe the structure of A_K for a extension field K over $\mathbb{Q}$ of degree 2. Consider any $\alpha \in K$. By the quadratic formula, we know that $\alpha = r + s \cdot \sqrt{D}$ for some square-free $D \in \mathbb{Z}$. Let $\bar{\alpha} = r - s \cdot \sqrt{D}$ be the Galois conjugate. Then α is the root of the quadratic polynomial

$$X^2 - 2rX + (r^2 - Ds^2) = 0.$$

It follows from this fact that α is an algebraic if and only if both $2r$ and $r^2 - Ds^2$ are integers. In fact, we can more explicitly describe the additive group of algebraic integers.

Exercise 1.8. *Assume that K is a extension field over $\mathbb{Q}$ of degree 2. Then the ring of algebraic integers A_K is either (i) the abelian group generated by 1 and $\sqrt{D}$ or (ii) the abelian group generated by 1 and $(1 + \sqrt{D})/2$.*

2 January 28, 2016

There is a lemma I would like to begin with:

Lemma 2.1. *Let K be a field and let $f(X) \in K[X]$ be a polynomial. If $f(X)$ and $f'(X)$ are relatively prime, then $f(X)$ has no multiple roots.*

Let $\theta \in \mathbb{C}$ be an algebraic number. Then there is a unique irreducible monic polynomial $f_\theta(X) \in \mathbb{Q}[X]$ that has θ as a root with smallest degree d. We can write

$$f_\theta(X) = (X - \theta_1) \cdots (X - \theta_d).$$

By the above lemma and the fact that f and f' has to be relatively prime, we see that $\theta_1, \theta_2, \ldots, \theta_d$ are all distinct. We call the set $\{\theta_1, \ldots, \theta_d\}$ the **full set of Galois conjugates**.

If θ and θ' are Galois conjugates, or in other words, roots of the same irreducible polynomial over $\mathbb{Q}$, then we have a natural isomorphism

$$\begin{array}{ccc} \mathbb{Q}[\theta] & \cong & \mathbb{Q}[\theta'] \\ & \nwarrow \quad \nearrow & \\ & \mathbb{Q} & \end{array}$$

2.1 Gauss's lemma

Factorization in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ might be slightly different. Suppose that we have a polynomial $f(X) \in \mathbb{Z}[X]$ such that the greatest common divisor of the coefficients is 1. Assume that we have a factorization

$$f(X) = g(X) \cdot h(X)$$

where $g(X)$ and $h(X)$ are in $\mathbb{Q}[X]$. Then we can multiply integers on both sides and factor out some greatest common divisors and make the equation into

$$a \cdot f(X) = b \cdot g'(X) \cdot h'(X)$$

where all f, g, h has the property that the greatest common divisor of the coefficients is 1, and a and b are relatively prime. Suppose that there is a prime p that divides a. Then we can reduce everything modulo p and get

$$0 = \bar{b} \cdot \bar{g'}(X) \cdot \bar{h'}(X).$$

This is clearly a contradiction since $\mathbb{F}_p$ is a integral domain. So we have $a = 1$, and likewise, $b = 1$. This means that the factorization in $\mathbb{Q}[X]$ was essentially a factorization in $\mathbb{Z}[X]$.

2.2 Primitive element theorem

Theorem 2.2 (Primitive element theorem)**.** *Suppose we have a field extension K/F of finite degree, that has the property that there are only finitely many intermediate fields. Then there is an element $\gamma \in K$ such that $K = F[\gamma]$.*

Proof. First assume that F is finite. Then K is also finite, and we actually know the structure of any finitely field, and its generated by one element.

Now assume that F is infinite. Let $\alpha, \beta \in K$ be any elements. If we show that $F[\alpha, \beta] = F[\gamma]$ for some $\gamma \in K$, then we can apply this fact multiple times to get

$$F[\alpha_1, \ldots, \alpha_m] = \cdots = F[\gamma]$$

for some γ. Since K is of finite degree over F, it is generated by finitely many elements, and this will finish the proof.

So let us show that $F[\alpha, \beta] = F[\gamma]$ for some γ. Given a $c \in F$, we define $\gamma_c = \alpha + c\beta$. Then we clearly have $F[\gamma_c] \subset F[\alpha, \beta]$ for any c. Since there are finitely many intermediate subfields, there are two $c_1 \neq c_2$ such that

$$F[\gamma_{c_1}] = F[\gamma_{c_2}].$$

This will imply $\alpha + c_1\beta, \alpha + c_2\beta \in F[\gamma_{c_1}]$ and thus $\alpha, \beta \in F[\gamma_{c_1}]$. Then we have

$$F[\alpha, \beta] \subset F[\gamma_{c_1}] \subset F[\alpha, \beta],$$

and the result follows. □

Proposition 2.3. *Let K/F be any field extension of finite degree, and assume that F has characteristic zero. Then there are only finitely many intermediate field extensions.*

To prove this we have to use some Galois theory. We won't assume knowledge, but let me just outline the basic idea.

Proof. Since F has characteristic zero, we see that there is a finite Galois extension L/F where $K \subset L$. Then by the fundamental theorem of Galois theory, the intermediate field extensions corresponds to subgroups of the Galois group, which is finite. So there are only finitely many intermediate field extensions. □

2.3 Roots of unity

Take any $m \geq 1$. We let $\zeta_m = e^{2\pi i/m}$ and

$$\mu_m = \{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}\}.$$

Then we easily see that these are the roots of

$$X^m - 1 = \prod_{j=0}^{m} (X - \zeta_m^j) = \prod_{d|m} \Big(\prod_{(k,d)=1} (X - \zeta_d^k) \Big).$$

It is quite natural to define

$$\Phi_d(X) = \prod_{\substack{(k,d)=1 \\ 1 \le k \le d-1}} (X - \zeta_d^k)$$

and write

$$X^m - 1 = \prod_{d|m} \Phi_d(X).$$

Theorem 2.4. *Any two primitive mth roots of unity are Galois conjugates.*

Proof. We first note that it suffices to show that ζ_m and ζ_m^k are Galois conjugates, because the relation is transitive. And we also note that it suffices to show for prime $k = p \nmid m$.

Let $f(X)$ be the minimal polynomial ζ_m and let

$$X^m - 1 = f(X)g(X).$$

Assume that ζ_m and ζ_m^p are not Galois conjugates. Then ζ_m^p cannot be a root of $f(X)$ and thus must be a root of $g(X)$. This means that ζ_m is a root of $g(X^m)$ and thus $g(X^m) = f(X) \cdot u(X)$ for some $u(X) \in \mathbb{Z}[X]$.

Let us now reduce everything modulo p. We have

$$\bar{g}(X)^p = \bar{g}(X^p) = \bar{f}(X) \cdot \bar{u}(X)$$

and thus $\bar{g}$ and $\bar{f}$ are not relatively prime in $\mathbb{F}_p[X]$. This means that

$$\overline{X^m - 1} = \bar{f}(X) \cdot \bar{g}(X)$$

has to have a multiple root. But this contradicts the fact that $X^m - 1$ and its derivative mX^{m-1} are relatively prime modulo p. Therefore ζ_m and ζ_m^p are Galois conjugates. □

Corollary 2.5. *The polynomial $\Phi_d(X)$ is in $\mathbb{Z}[X]$ and is irreducible.*

3 February 2, 2016

3.1 The fundamental embedding

Because $\mathbb{C}$ is algebraically closed, given a monic polynomial $f(X) \in \mathbb{Q}[X]$, we can always it as

$$f(X) = \prod_{i=1}^{d} (X - \theta_i)$$

where $\{\theta_1, \ldots, \theta_d\}$ are algebraic numbers. Because f has a unique factorization into $f(X) = \prod_{j=1}^{d} f_j(X)$ where $f_j(X)$ are irreducible. Then we can partition the $\theta_1, \ldots, \theta_d$ into sets consisting of Galois conjugates. This means that the set of roots of $f(X)$, whether it is irreducible or not, is a union of full sets of Galois conjugates of algebraic numbers.

We can look at the coefficients of $f(X)$. We have

$$f(X) = X^d - s_1 X^{d-1} + s_2 X^{d-2} - \cdots$$

where

$$\begin{cases} s_1(\theta_1, \ldots, \theta_d) = \theta_1 + \theta_2 + \cdots + \theta_d, \\ s_2(\theta_1, \ldots, \theta_d) = \sum_{i \neq j} \theta_i \theta_j, \\ \qquad\qquad \vdots \\ s_d(\theta_1, \ldots, \theta_d) = \theta_1 \cdots \theta_d. \end{cases}$$

These s_i are the elementary symmetric polynomials.

We have the following proposition.

Proposition 3.1. *The set $\{\theta_1, \ldots, \theta_d\}$ is a finite union of full sets of Galois conjugate of algebraic integers(resp. algebraic integers) if and only if*

$$s_i(\theta_1, \ldots, \theta_d) \in \mathbb{Q}(resp.\mathbb{Z})$$

for each of $i = 1, \ldots, d$.

Because $z \mapsto \bar{z}$ is an automorphism of $\mathbb{C}$ fixing $\mathbb{Q}$, we also have the following.

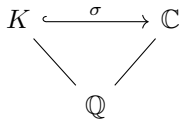
Proposition 3.2. *If θ is an algebraic number, so is $\bar{\theta}$, its complex conjugate. Moreover, $\bar{\theta}$ is a Galois conjugate of θ.*

If we look at a full set of Galois conjugates, then we can always pair up complex conjugates. This means that we can write it as

$$\{\theta_1, \theta_2, \ldots, \theta_r, \theta_{r+1}, \bar{\theta}_{r+1}, \ldots, \theta_{r+s}, \bar{\theta}_{r+s}\}.$$

We have been working on a finite extension field $K/\mathbb{Q}$ of degree d. We can think the set of field homomorphisms $\mathrm{Hom}(K, \mathbb{C})$. We first see that any such

homomorphism is necessarily an embedding, because the kernel, which is an ideal of K, has to be zero. Also, any such homomorphism fixes $\mathbb{Q}$.



There are exactly d such homomorphisms σ; The primitive element theorem tells us that $K = \mathbb{Q}[\theta]$ for some θ, and the image $\sigma(\theta)$ determines σ. On the other hand, the possible values of $\sigma(\theta)$ are the Galois conjugates of σ. So we have a correspondence

$$\{\mathrm{Hom}(K, \mathbb{C})\} \longleftrightarrow \{\theta_1, \ldots, \theta_d\}.$$

Suppose that $d = r + 2s$ and the Galois conjugates of θ consists of r reals and s paris of complex conjugates. Then there are r embeddings $K \hookrightarrow \mathbb{R}$ and s honest complex embeddings $K \hookrightarrow \mathbb{C}$ and their complex conjugates.

Definition 3.3. We define the **fundamental embedding** of K into the Euclidean space as the ring homomorphism $K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$ given by

$$x \mapsto (\sigma_1(x), \ldots, \sigma_r(x), \sigma_{r+1}(x), \sigma_{r+3}(x), \ldots, \sigma_{r+2s-1}(x)),$$

where for each pair of complex conjugate of embeddings, we choose one.

Although we have made a choice, we will later discuss how it can be removed.

3.2 Trace and norm

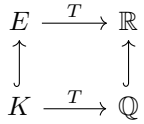
Definition 3.4. Let $K/\mathbb{Q}$ be a finite extension of degree d. For an element $\alpha \in K$, we define its **trace** and **norm** as

$$\mathrm{Trace}(\alpha) = T_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha), \quad \mathrm{Norm}(\alpha) = N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha).$$

We note that

$$T(\alpha + \beta) = T(\alpha) + T(\beta), \quad T(a \cdot \alpha) = a \cdot T(\alpha)$$

for each $a \in \mathbb{Q}$. That is, the map $T : K \to \mathbb{Q}$ is $\mathbb{Q}$-linear. Using the fundamental embedding, we can lift this into an $\mathbb{R}$-linear map $E \to \mathbb{R}$.



This new map $T : E \to \mathbb{R}$ will be given by

$$(v_1, \ldots, v_r, v_{r+1}, v_{r+3}, \ldots, v_{r+2s-1}) \mapsto v_1 + v_2 + \cdots + v_{r+2s}.$$

Likewise, using the fact that N is an homomorphism $K^* \to \mathbb{Q}^*$ as multiplicative groups, we can define $N : E^* \to \mathbb{R}^*$.

$$\begin{array}{ccc} E^* & \xrightarrow{N} & \mathbb{R}^* \\ \uparrow & & \uparrow \\ K^* & \xrightarrow{N} & \mathbb{Q}^* \end{array}$$

3.3 Galois size and S-numbers

Definition 3.5. We define the **Galois size** of an algebraic number α as

$$\text{size}(\alpha) = \max_{i=1}^{d} |\alpha_i|,$$

where $\{\alpha_i\}$ is the set of Galois conjugates.

Theorem 3.6. *There are only a finite number of algebraic integers of degree at most $d < \infty$, and Galois size at most $B < \infty$.*

Proof. We look at its minimal polynomial. Because all its roots are bounded, we see that the coefficients are bounded by abusing the triangle inequality. Then there are finitely many such polynomials, and thus there are finitely many algebraic numbers. □

Corollary 3.7. *Any algebraic integer of Galois size at most 1 is a root of unity.*

Corollary 3.8. *If α is an algebraic integer of Galois size at most 1, then any power of α will also have Galois size at most 1. Then by the previous theorem $\alpha^m = \alpha^n$ for some $m \neq n$, and the result follows.*

Definition 3.9. An **S-number** α is a real algebraic integer greater than 1 such that all its Galois conjugates have absolute value less than 1.

I think this is a beautiful introduction to the approximation of algebraic numbers. For $x \in \mathbb{R}$, we define

$$\|x\| = \text{distance between } x \text{ and its nearest integer.}$$

Then we have the following proposition.

Proposition 3.10 (Salem)**.** *If α is an S-number, then $\|\alpha^n\| \to 0$ as $n \to \infty$. In fact, $\sum_{n=1}^{\infty} \|\alpha^n\|^2$ converges.*

4 February 4, 2016

4.1 Integral closure

Proposition 4.1. *Consider a polynomial equation*

$$f(X) = X^d + a_{d-1}X^{d-1} \cdots + a_0$$

where each a_i is an algebraic number(resp. algebraic integer). Then the root of $f(X)$ is again an algebraic number(resp. algebraic integer).

Proof. Let $f(\theta) = 0$, and look at the field $\mathbb{Q}[a_0, a_1, \ldots, a_{d-1}]$. Because $a_0, \ldots, a_{d-1}$ are algebraic numbers, we see that it is of finite degree over $\mathbb{Q}$. Letting $L = \mathbb{Q}[a_0, \ldots, a_{d-1}, \theta]$, we get a finite extension of a finite extension, which will again be a finite extension field. Multiplication by θ sends L into L, and it follows that θ is algebraic.

The integral version can be done in the same manner. If we let $M = \mathbb{Z}[a_0, \ldots, a_{d-1}, \theta]$, then multiplication by θ sends M to M. This implies that θ is an algebraic integer. □

Definition 4.2. Let $K/\mathbb{Q}$ be an extension of finite degree. Let A_0 be a subring of algebraic integers in K. If a number $\alpha \in K$ is a root of some

$$f(X) = X^d + a_{d-1} + \cdots + a_0$$

for some $a_i \in A_0$, then we say that α is **integral** over A_0. The **integral closure** A is then defined as

$$A = \{\alpha \in K : \alpha \text{ is integral over } A_0\}.$$

If $A = A_0$, we say that A_0 is **integrally closed**.

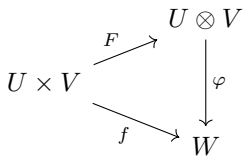
4.2 Fundamental embedding to $K \otimes \mathbb{R}$

Let us recall the fundamental embedding $K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$. We had to make a choice to define the map. We now discuss how to remove this choice.

Definition 4.3. Let U and V be abelian group. Then $f : U \times V \to W$, where W is also an abelian group, is called **bilinear** if

$$f(u_1 + u_2, v) = f(u_1, v) + f(u_2, v), \quad f(u, v_1 + v_2) = f(u, v_1) + f(u, v_2)$$

for any us in U and vs in V. The **tensor product** $U \otimes V$ is defined as the property that for any bilinear $f : U \times V \to W$ there is a unique homomorphism φ such that



commutes. This is given by

$$U \otimes V = \mathbb{Z}[U \times V]/(\text{ideal generated by } R\text{-bilinear relations}).$$

In fact, we can define $U \otimes_R V$ for R-modules U and V.

Let $K/\mathbb{Q}$ be a d-dimensional vector space over $\mathbb{Q}$. Then we see that $K \otimes_{\mathbb{Z}} \mathbb{R}$. This is a d-dimensional vector space over $\mathbb{R}$, and also a ring. In other words, it is an $\mathbb{R}$-algebra.

We come back to the fundamental embedding. Instead of looking at $\mathbb{R}^r \times \mathbb{C}^s$, we embed K into $E = K \otimes \mathbb{R}$. (It doesn't matter whether we tensor over $\mathbb{Z}$ or $\mathbb{Q}$.) Then we get the following:

$$\begin{array}{ccccc} & & K & \hookrightarrow & E = K \otimes \mathbb{R} \\ & \overset{d}{\nearrow} & \uparrow & & \| & \overset{d}{\searrow} \\ \mathbb{Q} & & A & \hookrightarrow & E = K \otimes \mathbb{R} & & \mathbb{R} \end{array}$$

Note that because the ring of integers A in K is an abelian group in E, it forms a lattice. We will later study this beautiful lattice.

Example 4.4. Take $K = \mathbb{Q}[\sqrt{D}]$. Then A is generated by either $\{1, \sqrt{D}\}$ or $\{1, (1+\sqrt{D})/2\}$. In both cases, we see that A form a nice lattice.

Proposition 4.5. *The abelian group A is discrete in $\mathbb{R}^r \times \mathbb{C}^s$.*

Proof. Let C be any compact subset of $\mathbb{R}^r \times \mathbb{C}^s$. Then if α is in C, then all Galois conjugates of α have bounded size. Moreover, the degree is at most d. We have proved last time that this implies that there are only finitely many possible α. This finishes the proof. □

Corollary 4.6. *As an abelian group, A is a free abelian group of rank d.*

4.3 Weil numbers

Definition 4.7. A **Weil number** is an algebraic integer α such that for any Galois conjugate α_i of α, its absolute value is

$$|\alpha_i| = p^{n/2}$$

where p is prime and $n \geq 1$.

Let me make a cultural comment about this. Let $q = p^n$ be a power of a prime, and consider the equation

$$y^2 = g(x)$$

over $\mathbb{F}_q$, where $g(x)$ is a monic polynomial with no multiple roots and of degree $d+2$. How many points are there on this curve over $\mathbb{F}_{q^\nu}$?

Theorem 4.8. *The number of solutions over $\mathbb{F}_{q^\nu}$ is*

$$\#\ \textit{of solutions}/\mathbb{F}_{q^\nu} = q - \sum_{i=1}^{d} \alpha_i^\nu,$$

where $\{\alpha_1, \ldots, \alpha_d\}$ is the set of conjugates of Weil numbers.

4.4 Fermat's last theorem[1]

Theorem 4.9 (Fermat's last theorem)**.** *Let $n \geq 3$ be an integer. There there exist no nonzero integral solutions of*

$$a^n + b^n = c^n.$$

One easy observation is that proving for $n = 4$ and $n = p$ suffices. Because the case $n = 4$ was in the homework, we shall look at the case $n = p$.

Let $\omega = e^{2\pi i/p}$. We see that every element of $\mathbb{Z}[\omega]$ can be uniquely represented as

$$a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}$$

since $X^{p-1} + X^{p-2} + \cdots + X + 1$ is the minimal polynomial of ω.

The theorem is hard, and thus we will do as much as we can. Assume first that $\mathbb{Z}[\omega]$ is a unique factorization domain. Suppose that there is a solution

$$x^p + y^p = z^p$$

where p does not divide any of x, y, z. We can also suppose that x, y, z are relatively prime in $\mathbb{Z}$.

We can factorize the equation into

$$z^p = x^p + y^p = \prod_{i=0}^{p-1}(x + y\omega^i).$$

Suppose that $x + y\omega^i$ and $x + y\omega^j$ have a common prime factor. This means that both numbers are in some ideal $I \subset \mathbb{Z}[\omega]$ that is not the entire ring. Then $y(1 - \omega^{j-i})$ will be in I, and multiplying all the other $(1 - \omega^k)$s, we see that py is in I. On the other hand, because $x + y\omega^i$ divides z^p, we see that $z^p \in I$. But because py and z^p are relatively prime, we get $1 \in I$, which contradicts the fact that I is not the whole ring. This shows that all $x + y, x + y\omega, \ldots, x + y\omega^{p-1}$ are relatively prime, and because they multiply up to a p-th power, we see that all of them must be a p-th power up to a unit. In other words, we have

$$x + y\omega = u\alpha^p$$

for some $u, \alpha \in \mathbb{Z}[\omega]$, where u is a unit.

We now define the class group. Consider the set of all ideals of $\mathbb{Z}[\omega]$, and we define an equivalent relation so that $A \sim B$ for ideals $A, B \subset \mathbb{Z}[\omega]$ if there are principal ideals (α) and (β) such that

$$A \cdot (\alpha) = B \cdot (\beta).$$

Proposition 4.10. *The equivalence classes form a group under multiplication. The equivalence class consisting only of all principal ideals is the identity.*

[1] This was a presentation by Shyam Narayanan.

5 February 9, 2016

We are going to talk about discriminants.

5.1 Discriminant

We have a field K which is of finite degree d over $\mathbb{Q}$. We choose a bunch of numbers $\alpha_1, \dots, \alpha_d \in K$, and embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$.

Definition 5.1. We define the **discriminant** as

$$\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \big(\det\big[\sigma_i(\alpha_j)\big]\big)^2 = \big(\det\big[\sigma_j(\alpha_i)\big]\big)^2.$$

Because we square the determinant, we do not have to specify the order of the numbers and the embeddings. But it depends on the change of basis. Suppose we have $\alpha' = \sum_{j=1}^{d} m_{ij}\alpha_j$ for some $m_{ij} \in \mathbb{Q}$. Then

$$\big[\sigma_j \alpha_i'\big] = M \cdot \big[\sigma_j \alpha_i\big]$$

and thus

$$\operatorname{disc}(\alpha_1', \dots, \alpha_d') = (\det M)^2 \operatorname{disc}(\alpha_1, \dots, \alpha_d).$$

In particular, we can assume that $m_{ij} \in \mathbb{Z}$ and $\det M = \pm 1$, or equivalently, the $\mathbb{Z}$-module generated by $\alpha_1, \dots, \alpha_d$ is same as the $\mathbb{Z}$-module generated by $\alpha_1', \dots, \alpha_d'$. Then it follows that $\operatorname{disc}(\alpha_i)_i = \operatorname{disc}(\alpha_i')_i$.

One thing we notice is that if $\alpha_1, \dots, \alpha_d$ are linearly dependent over $\mathbb{Q}$, then the the rows (or columns) of $[\sigma_j \alpha_i]$ are linearly dependent and hence $\operatorname{disc}(\alpha_1, \dots, \alpha_d) = 0$. So we may as well assume that $\alpha_1, \dots, \alpha_d$ is a $\mathbb{Q}$-basis of K as a $\mathbb{Q}$-vector space.

Definition 5.2. Let A be a $\mathbb{Z}$-module. Then we define its **discriminant** as

$$\operatorname{disc}(A) = \operatorname{disc}(\alpha_1, \dots, \alpha_d),$$

where $\alpha_1, \dots, \alpha_d$ is the basis for A.

Note that we can work over any finite extension field of characteristic zero instead of K and $\mathbb{Q}$.

Theorem 5.3. *Let $T : K \to \mathbb{C}$ be the trace. Then*

$$\operatorname{disc}(\alpha_1, \alpha_2, \dots, \alpha_d) = \big|\det\big[T(\alpha_i\alpha_j)\big]\big|.$$

Proof. It follows from the fact that

$$\big[\sigma_j\alpha_i\big]\big[\sigma_i\alpha_j\big] = \big[\sum \sigma_k(\alpha_i\alpha_j)\big] = \big[T(\alpha_i\alpha_j)\big].$$

□

We are using the fact this $T(x \cdot y)$ is some kind of a bilinear form. Because K is an algebra, multiplication gives a bilinear map, and then T is additive homomorphism.

Theorem 5.4. *Let $\{\alpha_i\}_i$ be linearly independent over $\mathbb{Q}$. Then* $\operatorname{disc}(\alpha_i)_{i=1}^d \neq 0$.

Proof. Suppose that the determinant $\det[T(\alpha_i\alpha_j)] = 0$. Then there will be rational number $a_j \in \mathbb{Q}$ not all zero, such that

$$0 = \sum_{j=1}^{d} a_j T(\alpha_i\alpha_j) = \sum_{j=1}^{d} T(a_j\alpha_i\alpha_j)$$

for any $i = 1, \ldots, d$. If we let $\alpha = \sum_{j=1}^d a_j\alpha_j$, we have

$$T(\alpha \cdot \alpha_i) = 0$$

for any $i = 1, \ldots, d$.

Now we use the fact that $\alpha_1, \ldots, \alpha_d$ form a basis of $\mathbb{Q}$. Then from $T(\alpha\cdot\alpha_i) = 0$, it follows that $T(\alpha \cdot x) = 0$ for any $x \in K$. But this is clearly not true since

$$T(\alpha \cdot 1/\alpha) = T(1) = \sum_{j=1}^{d} \sigma_j(1) = d. \qquad \square$$

Definition 5.5. Let α be an element of K. Then we write

$$\operatorname{disc}(\alpha) = \operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{d-1}).$$

We can calculate $\operatorname{disc}(\alpha)$ it relatively easily. We have

$$\operatorname{disc}(q, \alpha, \alpha^2, \ldots, \alpha^{d-1}) = \det(\sigma_i\alpha^{j-1})^2 = \det((\sigma_i\alpha)^{j-1})^2 = \prod_{j<j'} (\sigma_j\alpha - \sigma_{j'}\alpha)^2$$

by the Vandermonde identity.

Proposition 5.6. *Let α be a primitive element. We have*

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{d-1}) = (-1)^{d(d-1)/2} N(f'(\alpha)),$$

where $f(X)$ is the monic irreducible polynomial over Q.

Proof. Since $f(X) = \prod(X - \sigma_i\alpha)$, we have

$$f'(X) = \sum_{k=1}^{d} \prod_{j\neq k} (X - \sigma_j\alpha)$$

and thus

$$f'(\alpha) = \prod_{j\neq 1} (\alpha - \sigma_j\alpha).$$

Then when we take the norm, it becomes

$$\begin{aligned} N(f'(\alpha)) &= \prod_{i=1}^{d} \sigma_i \prod_{j\neq 1} (\alpha - \sigma_j(\alpha)) \\ &= \prod_{i=1, j\neq 1}^{d} (\sigma_i\alpha - \sigma_i\sigma_j\alpha) = (-1)^{d(d-1)/2} \prod_{k<l} (\sigma_k\alpha - \sigma_l\alpha)^2. \end{aligned}$$

The result follows from what we did just before. □

Example 5.7. Let m be a square free integer, with $m \neq 0, \pm 1$. Let $d \geq 2$ and consider

$$K = \mathbb{Q}[\sqrt[d]{m}] = \mathbb{Q}[X]/(X^d - m).$$

We calculate $\operatorname{disc}(A)$, where

$$A = \sqrt[d]{m}\mathbb{Z} + \zeta_d \sqrt[d]{m}\mathbb{Z} + \cdots + \zeta_d^{d-1} \sqrt[d]{m}\mathbb{Z}.$$

Then

$$\begin{aligned} \operatorname{disc}(A) &= \operatorname{disc}(1, \sqrt[d]{m}, (\sqrt[d]{m})^2, \ldots, (\sqrt[d]{m})^{d-1}) = \pm N(f'(\sqrt[d]{m})) \\ &= \pm N(dm^{(d-1)/d}) = \pm d^d \prod_{k=0}^{d-1} \zeta_d^k m^{(d-1)/d} = \pm d^d m^{d-1}. \end{aligned}$$

In particular, if $A = \mathbb{Z}[\sqrt{m}]$ then $\operatorname{disc} A = \pm 4m$, and if $A = \mathbb{Z}[(1+\sqrt{m})/2]$ then $\operatorname{disc} A = \pm m$.

6 February 11, 2016

Let us start by recalling where we are. Let K be a field of degree d over $\mathbb{Q}$. Let $\alpha \in K$ be a primitive element. Then $1, \alpha, \ldots, \alpha^{d-1}$ form a $\mathbb{Q}$ be a basis of K. Let M be the $\mathbb{Z}$-module generated by $1, \alpha, \ldots, \alpha^{d-1}$. This module will be of rank d.

We can look at the discriminant

$$\operatorname{disc}(M \subset K) = \operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{d-1}) = \pm N(f'(\alpha)).$$

If you wish, you can think of M as a lattice in $K \cong M \otimes_{\mathbb{Z}} \mathbb{Q}$. There are loads of corollaries you can make.

Corollary 6.1. *Let $\alpha = \zeta_p = e^{2\pi i/p}$. Let $K = \mathbb{Q}[\zeta_p]$ and $M = \mathbb{Z}[\zeta_p]$. Then* $\operatorname{disc}(M) = asdfadsf$.

Proof. We know that $\operatorname{disc}(M) = \pm N(f'(\zeta_p))$. Since $f(X)(X-1) = X^p - 1$, we can take the derivative and get $f'(\zeta_p) = p\zeta_p^{p-1}$. Its norm will be

$$N(f'(\zeta_p)) = \frac{Np \cdot (N\zeta_p)^{p-1}}{N(\zeta_p - 1)} = \frac{p^{p-1} \cdot 1}{p} = p^{p-2}.$$

Thus it follows that $\operatorname{disc}(M) = \pm p^{p-2}$. □

Let A be the ring of algebraic integers of K.

Theorem 6.2. *A is lattice in $\mathbb{Z}$, and it is a free abelian subgroup of rank d.*

Proof. We have

$$A \hookrightarrow K \hookrightarrow E = \mathbb{R}^r \times \mathbb{C}^s.$$

As a subgroup of E, the group A is discrete.

Now next week, Johnnie Han will going to prove that every discrete subgroup in $\mathbb{R}^d$ is a free abelian group of rank at most d. Then it has a have rank exactly d because for every element of K multiplied by a large integer is an algebraic integer. □

Definition 6.3. We define the **discriminant** of a number field K as

$$\Delta_K = \text{discriminant of } A.$$

6.1 Reasons for loving the discriminant

Let $K/\mathbb{Q}$ have degree d. We can first find a $\mathbb{Q}$-basis $\alpha_1, \alpha_2, \ldots, \alpha_d$ that are also algebraic integers, and then compute the discriminant $\delta = \operatorname{disc}(\alpha_1, \dot{;}s\alpha_d)$.

Now let $\alpha \in K$ be an arbitrary algebraic integer. There will be unique $x_i \in \mathbb{Q}$ such that $\alpha = \sum x_i \alpha_i$. Apply the various embeddings σ_j, and we get

$$\sigma_j \alpha = \sum x_i \sigma_j \alpha_i.$$

The Cramer's rule tells us that

$$x_i = \frac{\det(\gamma_i)}{\det(\sigma_j(\alpha_i))},$$

where γ_i is the matrix obtained bey replacing the ith column of $(\sigma_j(\alpha_i))$ by $\sigma_j(\alpha)$. When we multiply $\det(\sigma_j(\alpha_i))$ to both sides, we get

$$x_i \cdot \operatorname{disc}(\alpha_1, \ldots, \alpha_d) = \det(\sigma_j(\alpha_i)) \det(\gamma_i).$$

Since the left hand side is in $\mathbb{Q}$ and the right hand side is an algebraic integer, we have

$$x_i = \frac{m_i}{\operatorname{disc}(\alpha_1, \ldots, \alpha_d)}$$

for some integer m_i. This enables us to literally compute the basis for the ring of algebraic integers.

Also, when viewed as a lattice, the abelian group $A \subset \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^d$ has fundamental domain of volume $\sqrt{\Delta_K}$.

6.2 S-numbers[2]

Definition 6.4. Let $\theta > 1$ be a real algebraic integer, and let $\{\alpha_1, \ldots, \alpha_{d-1}\}$ be its Galois conjugates. The number θ is called a **S-number** if $|\alpha_i| < 1$ for all i. We denote the set of S-numbers by S.

Example 6.5. Every rational number greater than 1 is a trivial S-number. The golden ratio $\varphi = (1 + \sqrt{5})/2$ and the solution ρ to $x^3 - x - 1 = 0$ is also a S-number, which turns out to be the smallest S-number.

Theorem 6.6. *Let $\|x\|$ denote the distance from x to its nearest integer. If θ is an S-number, then $\|\theta^n\| \to 0$ as $n \to \infty$.*

Proof. Let θ be of degree d, and let $\alpha_1, \ldots, \alpha_{d-1}$ be its conjugates. Then since

$$\theta^n + \alpha_1^n + \cdots + \alpha_{d-1}^n$$

is a rational number, and an algebraic integer, it is an integer. Then

$$\|\theta^n\| \leq |\alpha_1|^n + \cdots + |\alpha_{d-1}|^n$$

and because the right hand side goes to zero, $\|\theta\| \to 0$. □

Using a very similar argument, we can in fact also show the following.

Theorem 6.7. *Let $\lambda \in \mathbb{Q}[\theta]$. Then $\|\lambda\theta^n\| \to 0$ as $n \to \infty$.*

The converse is open in general, but we can prove the following.

Theorem 6.8. *Let $\theta > 1$ and $\lambda > 0$ be real numbers. If $\sum \|\lambda\theta^n\|^2 < \infty$, then θ is an S-number, and moreover λ is an algebraic number in $\mathbb{Q}[\theta]$.*

[2]This was a presentation by Kat Zhou

7 February 16, 2016

7.1 Dedekind domain

Definition 7.1. A ring A is a **Dedekind domain** if it is an integral domain with the following three propositions.

1) Every ideal of A is finitely generated.

2) Every nonzero prime ideal is a maximal ideal.

3) A is integrally closed in K, the field of fractions of A.

The main use of Dedekind domains will be illustrated in the following theorem.

Theorem 7.2. *The ring of (algebraic) integers in a number field (i.e., a field of degree $d < \infty$ over $\mathbb{Q}$) is a Dedekind domain.*

Proof. We first prove 1). Since A is a free abelian group of rank d, we see that any ideal $I \subset A$ is finitely generated as a $\mathbb{Z}$-module, and thus finitely generated as a ideal.

We next prove 2). Any ideal in A contains some positive integer m, because we can always multiply its inverse times an integer that is in A. Then we have

$$A \longrightarrow\!\!\!\!\!\rightarrow A/mA \longrightarrow\!\!\!\!\!\rightarrow A/I.$$

Since $A/mA \cong (\mathbb{Z}/m\mathbb{Z})^d$ is finite, we see that A/I must also be finite. Now for any prime ideal $P \subset A$, we see that A/P is a finite ring, which must be an integral domain by the definition of a prime ideal. Now exercise 2 on page 82 of our book states that any finite integral domain is a field. Thus A/P is a field and P is a maximal ideal.

We now prove 3). Recall that if α is a root of $f(X)$ with algebraic integer coefficients, then α is also an algebraic integer. Take any element α that satisfies a monic polynomial equation $f(x) = 0$ where the coefficients of f are in A. Then $\alpha \in K$, and α is an algebraic integer. Hence $\alpha \in A$ and so A is integrally closed. □

Theorem 7.3. *Let k be any field. Then the ring of polynomials $k[t]$ is a Dedekind domain, and the ring of power series $k[[t]]$ is also a Dedekind domain.*

Dedekind domains is a incredibly important notion, and it is where most of algebraic number theory resides.

Let $I, J \subset A$ be nonzero ideals. We define their product as

$$I \cdot J = \Big\{ \sum_{k=1}^{r} \alpha_k \beta_k : \alpha_k \in I,\ \beta_k \in J \Big\}.$$

This gives a monoid structure on the set of ideals. Indeed, we have the identity (1), as $(1) \cdot I = I$ for any I. A ideal is called a principal ideal if it is of the form (α) for some α. We can define an equivalence relation

$$I \sim J \quad \Leftrightarrow \quad (\alpha) \cdot I = (\beta) \cdot J.$$

Let K be the field of fractions of A, and let M be a finitely generated additive subgroup of K. If we let $m_1, \ldots, m_r \in K$ be the generates of M, then there must be a $D \in K$ such that $Dm_1, \ldots, Dm_r$ are all in A. We then have abelian subgroups $M \subset K$ and $DM \subset A$. Moreover, if we assume that M is an A-module in K, then DM is also an A-module in A, which is in other words, an ideal. That is, we can write

$$M = \frac{1}{D} \cdot I$$

where I is an ideal.

7.2 Factorization of ideals

Definition 7.4. A finitely generated A-module in K is called a **fractional ideal** of A.

Lemma 7.5. *Let $I \subset A$ be a nonzero ideal and P be a prime ideal. Then $P \mid I$ if and only if $I \subset P$.*

We will prove this later.

Lemma 7.6. *Let $I, J \subset A$ be nonzero ideals, and let P be a prime ideal. Then*

$$P \mid I \cdot J \quad \Longrightarrow P \mid I \text{ or } P \mid J.$$

Proof. Since P is a maximal ideal, we see that A/P is a field. Under the projection map

$$\pi : A \to A/P,$$

the images $\pi(I)$ and $\pi(J)$ are both ideals, and their product must be zero. But an ideal of a field is either the entire field of just zero. Thus one of $\pi(I)$ or $\pi(B)$ must be zero and thus $I \subset P$ or $J \subset P$. □

We can also define the inverses of ideals. Let $I \subset A$ be a ideal, and let $0 \neq \alpha \in I$. Then let

$$J_\alpha = \{\beta \in A : \beta \cdot I \subset (\alpha)\}.$$

Theorem 7.7. *The product of I and J_α is $I \cdot J_\alpha = (\alpha)$.*

To prove this, we need something from the homework.

Lemma 7.8. *Let $H \subsetneq A \subset K$ be a proper ideal, where A is a Dedekind domain and K is the field of fractions. Then for any $\gamma \in K \setminus A$, we have $\gamma \cdot H \subset A$.*

Proof of theorem 7.7. We first see that

$$I \cdot J_\alpha \subset (\alpha)$$

since the definition of J_α makes sure everything lies in (α). In other words, we have

$$H = \frac{1}{\alpha} \cdot I \cdot J_\alpha \subset A.$$

Suppose $H \subsetneq A$. Then using the lemma above, we see that there is an $\gamma \in K \setminus A$ such that $\gamma H \subset A$. Then

$$\gamma \cdot J_\alpha \cdot I \subset (\alpha)$$

and thus by definition of J_α,

$$\gamma \cdot J_\alpha \subset J_\alpha.$$

But then, J_α is a $\mathbb{Z}$-module, that is preserved under multiplication by γ, and it follows that γ is an algebraic integer. This contradicts our definition of γ. □

This gives the cancellation property:

Proposition 7.9 (Cancellation)**.** *If M, N, I are ideals of A and $M \cdot I = N \cdot I$, then $M = N$.*

Proof. Consider any J_α such that $I \cdot J_\alpha = (\alpha)$. Then multiplying J_α to each side we get

$$\alpha M = M \cdot I \cdot J_\alpha = N \cdot I \cdot J_\alpha = \alpha N$$

and hence $M = N$. □

Definition 7.10. The **ideal class group** is the group of equivalence classes of ideals of A (under multiplication). For a number field K, we denote $H(K)$ by the group of ideal classes of A.

There are wildly open questions about the ideal class groups. For example, let $K = \mathbb{Q}[\sqrt{-D}]$ for $D \geq 1$. When does it have trivial ideal class group? It turns out that the answer is

$$-D = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Proposition 7.11. *Let I and N be ideals. Then $I \mid N$ if and only if $N \subset I$.*

Proof. Clearly, if $I \mid N$ then $N = I \cdot J \subset I \cdot A = I$.

Suppose now that $N \subseteq I$ and let us construct a J. Let

$$M = \frac{1}{\alpha} \cdot N \cdot J_\alpha$$

where $\alpha \in I$ and $J_\alpha = \{\beta \in A : \beta \cdot I \subset (\alpha)\}$. Then

$$I \cdot M = \frac{1}{\alpha} \cdot N \cdot I \cdot J_\alpha = N.$$ □

Theorem 7.12 (Unique factorization of ideals)**.** *Every ideal factors uniquely as a product of prime ideals.*

Proof. We first prove the existence of factorization part. Suppose the contrary and consider a maximal counterexample M. There is a maximal ideal $\mathfrak{m}$ with $M \subset \mathfrak{m} \subset A$. We first note that since $\mathfrak{m}$ is itself a prime ideal, M cannot be $\mathfrak{m}$. By the divisibility theorem, there has to exist some ideal I such that $M = \mathfrak{m} \cdot I$. Then I becomes a ideal bigger than M and hence contradicts our assumption that M is maximal.

We now prove the uniqueness, by channeling the old proof of unique factorization property of $\mathbb{Z}$. Suppose that we have

$$P_1 \cdot P_2 \cdot \cdots \cdot P_r = Q_1 \cdot \cdots \cdot Q_s.$$

Then P_1 divides $Q_1 \cdot \cdots \cdot Q_s$ and we can cross of things. Then inductively we see that both sides are equal. □

8 February 18, 2016

Last time we proved the unique factorization of ideals in Dedekind domains. This means that any ideal I can be written as

$$I = \prod_{i=1}^{r} P_i^{e_i}$$

for distinct prime ideals P_i and $e_i > 0$.

8.1 Order of an ideal

Definition 8.1. The **order** ord_P^I of an ideal I over a prime ideal P is the largest exponent e such that $P^e \mid I$. The **order** of an element α is defined as

$$\operatorname{ord}_P(\alpha) = \operatorname{ord}_P((\alpha)).$$

We can write

$$I = \prod_P P^{\operatorname{ord}_P(I)}$$

in a very nice way. There are infinitely many units, which does not count.

The order can be defined even for fractional ideals.

Definition 8.2. Let $M = \frac{1}{\alpha} I$ be a fractional ideal. Then we define

$$\operatorname{ord}_P(M) = \operatorname{ord}_P(I) - \operatorname{ord}_P(\alpha).$$

Then likewise we can write

$$M = \prod_P \operatorname{ord}_P(M).$$

The fractional ideals form a group, because we can always take the inverse. In this sense, the ord is a homomorphism

$$\operatorname{ord}_P : \text{Fract. Ideals} \twoheadrightarrow \mathbb{Z}.$$

It makes perfect sense to define the greatest common divisor and the least common multiple. For any two ideals $I, J \subseteq A$, we define

$$\operatorname{GCD}(I, J) = (I, J), \quad \operatorname{LCD}(I, J) = I \cap J.$$

Then we have

$$\operatorname{ord}_P(\text{GCD}) = \min(\operatorname{ord}_P(I), \operatorname{ord}_P(J)), \quad \operatorname{ord}_P(\text{LCM}) = \max(\operatorname{ord}_P(I), \operatorname{ord}_P(J)).$$

8.2 Finite approximation

Let A be a Dedekind domain. Consider any distinct primes $P_1, \ldots, P_r$ and $e_1, \ldots, e_r \geq 0$.

Lemma 8.3. *There exists an $\alpha \in A$ such that $\operatorname{ord}_{P_i}(\alpha) = e_i$ for $i = 1, \ldots, r$.*

Proof. Let us look at

$$A \supset \prod_{i=1}^{r} P_i^{e_i} \supset \prod_{i=1}^{r} P_i^{e_i+1}.$$

Because the ideals $P_i^{e_i+1}$ are pairwise relatively prime, we can use the Chinese remainder theorem

$$A \longrightarrow\!\!\!\!\!\rightarrow A/\textstyle\prod P_i^{e_i+1} \cong \prod A/P_i^{e_i+1} \supset \prod_{i=1}^{r} P_i^{e_i}/P_i^{e_i+1}$$

Now choose an r-tuple $(u_1, r_2, \ldots, u_r)$ in $\prod P_i^{e_i}/P_i^{e_i+1}$ so that $u_i \neq 0$. We then lift it to some $\alpha \in A$. This α will have the desired property. □

The consequence of this lemma is that every ideal $I \subseteq A$ is generated by two elements. Even better, given any $0 \neq \alpha \in I$, there exists a β such that $I = (\alpha, \beta)$. How do we achieve this? Let us first pick any α and let us look at (α). It will be

$$(\alpha) = \prod_{i=1}^{r} P_i^{E_i} \cdot \prod_{j=1}^{s} Q_j^{F_j}$$

where $E_i \geq e_i$. Now find a β such that $\operatorname{ord}_{P_i} \beta = e_i$ and $\operatorname{ord}_{Q_j} \beta = 0$. Because

$$\operatorname{ord}_P(\alpha, \beta) = \min(\operatorname{ord}_P \alpha, \operatorname{ord}_P \beta),$$

we see that $\operatorname{ord}_{P_i} = e_i$, $\operatorname{ord}_{Q_j} = 0$, and $\operatorname{ord}_R = 0$ for any other R. Thus $(\alpha, \beta) = I$.

8.3 Residue fields

Let $P \subset A$ be a prime ideal. Then A/P must be a field, and because it is finite, it must be isomorphic to $k = \mathbb{F}_q$ for some $q = p^f$. Now let us look at P/P^2. Since P and P^2 are both A-modules, it inherits a natural A-module structure. But because the action of P is trivial, we see that P/P^2 is actually a k-vector space. More generally, for any e the quotient P^e/P^{e+1} is a nontrivial k-vector space.

But what is its dimension? We use the finite approximation property. Consider any $0 \neq \alpha \in P^{e+1}$. Then we know that there has to be a β such that $P^e = (\alpha, \beta)$. But then $P^e/P^{e+1} = (\beta)$. This shows that

$$\dim_k(P^e/P^{e+1}) = 1.$$

8.4 Unique factorization implies principal ideal domain

Theorem 8.4. *Let A be a Dedekind domain. If A is a unique factorization domain, then it is a principal ideal domain.*

This is interesting, because any principal ideal domain is a unique factorization domain, but not all unique factorization domains are principal ideal domains. For instance, the ring $\mathbb{C}[X, Y]$ is not a principal ideal domain, because the ideal (X, Y) is not principal.

Proof. We first note that if A were a UFD, for any $\alpha \in A$, we see that $\alpha \mid \delta \cdot \epsilon$ implies $\alpha \mid \delta$ or $\alpha \mid \epsilon$.

Suppose that A is not a PID. Then there exists an ideal I that is not principal. Then there exists a prime ideal P that is not principal. Since A is a Dedekind domain, there is an ideal M such that

$$P \cdot M = (\alpha)$$

is principal; pick the maximal such M. □

9 February 23, 2016

Let $K/\mathbb{Q}$ be a finite degree extension that splits. Let A be the ring of integers in K, which is a Dedekind domain.

9.1 Quotient of ideals

Proposition 9.1. *Let $0 \neq I \subsetneq A$ be a proper ideal. Then I/I^2 is a cyclic A/I-module.*

Proof. Since A is a Dedekind domain, for any $\alpha \in I$ the ideal I is generated by α and some $\beta \in I$, i.e., $I = (\alpha, \beta)$.

Now fix any $\alpha \in I^2$. Then we have a β such that $I = (\alpha, \beta)$. Then I/I^2 is generated by the image of β. □

Corollary 9.2. *Let $P \subset A$ be prime ideal. Then we have a nice filtration*

$$A = P^0 \supset P^1 \supset P^2 \supset P^3 \supset \cdots \supset P^n \supset P^{n+1} \supset \cdots .$$

*We first note that $\bigcap_{n=0}^{\infty} P^n = \{0\}$. We call $A/P = k_P$ the **residue field** at P. Because P^n/P^{n+1} is a cyclic module, it is a dimension 1 vector space. Thus $|P^n/P^{n+1}| = |k_P| = q_P$.*

We note that q_P can be the same for distinct P. For instance, $(2+i)$ and $(1+2i)$ in $\mathbb{Z}[i]$ have the same q_P.

Definition 9.3. We denote $\|I\| = |A/I|$.

Clearly, we have $\|P^k\| = q_P^k$.

Proposition 9.4. *Let $I, J \subseteq A$ be ideals. Then $\|I \cdot J\| = \|I\| \cdot \|J\|$.*

Proof. Since the Chinese remainder theorem states that

$$A/\prod_P P^{\operatorname{ord}_P I} = \prod_P A/P^{\operatorname{ord}_P I},$$

we have

$$\|I\| = \|\prod_P^{\operatorname{ord}_P I}\| = \prod_P \|P^{\operatorname{ord}_P I}\| = \prod_P q_P^{\operatorname{ord}_P I}.$$

Then

$$\|I\| \cdot \|J\| = \prod_P P^{\operatorname{ord}_P I + \operatorname{ord}_P J} = \|I \cdot J\|. \qquad \square$$

Consider a tower of field extensions

$$\begin{array}{ccc} I \cdot B \subseteq B & \hookrightarrow & L \\ \downarrow & & \downarrow{\scriptstyle n=[L:K]} \\ I \subseteq A & \hookrightarrow & K \\ \downarrow & & \downarrow \\ \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

Proposition 9.5. $\|B/IB| = \|I \cdot B\| = \|I\|^n$.

Proof. We note that it reduces to the case of $I = P$. That is, we need only prove that $\|P \cdot B\| = \|P\|^n$ for prime ideals P. We note that B/PB is a $A/P = k_P$-module. Thus this is equivalent to $\dim_{k_P} B/PB \leq n$.

This is in the homework due this Friday, so let us prove only for $A = \mathbb{Z}$. Let $P = (p)$. Then $B/PB = B/(pB)$, and since B is a free abelian group of rank n, we see that B/pB is a $\mathbb{F}_p$-vector space of rank n. □

Example 9.6. Let $A = \mathbb{Z} \supset (p)$. If $B = \mathbb{Z}[i]$ then

$$PB = \begin{cases} P \cdot \bar{P} & p \equiv 1 \pmod 4 \\ P^2 & p = 2 \\ P & p \equiv 3 \pmod 4. \end{cases}$$

Example 9.7. Consider the example:

$$\begin{array}{ccc} B = \mathbb{C}[\sqrt{t}] & \hookrightarrow & \mathbb{C}(\sqrt{t}) \\ \Big| & & \Big|{\scriptstyle \text{deg.}=2} \\ (t-a) \subseteq A = \mathbb{C}[t] & \hookrightarrow & \mathbb{C}(t) \end{array}$$

We see that

$$(t-a)B = (\sqrt{t} - \sqrt{a})(\sqrt{t} + \sqrt{a})B.$$

This ramifies if and only if $t = 0$.

9.2 Ramification indices and residue field degrees

More generally, we see that for

$$\begin{array}{ccc} p \cdot B \subseteq B & \hookrightarrow & L \\ \Big| & & \Big|{\scriptstyle n} \\ (p) \subset A = \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

we have

$$|B/pB| = \|pB\| = \prod_{i=1}^{r} q_{P_i}^{e_i},$$

where $(p)B = \prod_{i=1}^{r_i} P_i^{e_i}$.

Definition 9.8. We let

$$f(P_i|p) = (\text{relative residue field degree of } P_i \text{ over } p) = [k_{P_i} : \mathbb{F}_p]$$

and $e(P_i|p)$ be the relative ramification index defined by

$$pB = \prod_{P_I} P_i^{e(P_i|p)}.$$

We see that

$$p^n = \|pB\| = \prod_{i=1}^{r} p^{e(P_i|p)\cdot f(P_i|p)}.$$

Therefore we have the following theorem.

Theorem 9.9.

$$[L : Q] = \sum_{P_i|pB} e(P_i|p)f(P_i|p).$$

More generally, for any field extensions $L/K/\mathbb{Q}$ and its corresponding ring of integers $B \hookrightarrow L$ and $A \hookrightarrow K$. We can define $e(Q_j|P)$ and $f(Q_j|P)$ for $Q_j \subset B$ and $P \subset A$ by

$$PB = \prod_j Q_j^{e(Q_j|P)}, \quad f(Q_j|P) = \dim_{k_P} k_{Q_j}.$$

Then likewise we have the following.

Theorem 9.10.

$$[L : K] = \sum_{Q_j|PB} e(Q_j|P) \cdot f(Q_j|P).$$

Example 9.11. Let $K = \mathbb{Q}[\sqrt{D}]$. From the previous theorem, for any prime p in $\mathbb{Z}$, we have

$$p \cdot A = \prod_{i=1}^{r} P_i^{e_i}, \quad \sum_{i=1}^{r} e_i f_i = 2.$$

There are three cases:

$$\begin{cases} r = 2: & e_i = f_i = 1 & (p) = P\bar{P} \\ r = 1: & e_1 = 2, f_1 = 1 & (p) = P^2 \\ r = 1: & e_1 = 1, f_1 = 2 & (p) = P \end{cases}$$

9.3 Spectrum of a ring

Definition 9.12. For a commutative ring A, we define its **spectrum** as

$$\operatorname{Spec} A = \text{set of prime ideals of } A.$$

For any ring homomorphism $\pi : A \to B$, it induces a map $\operatorname{Spec} B \to \operatorname{Spec} A$ just by inverse images, because if $Q \subset B$ is a prime ideal then $\pi^{-1}(Q) \subset A$ is a prime ideal.

Now let A and B be Dedekind domains.

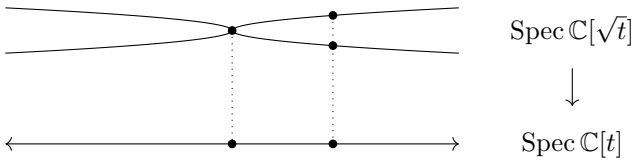
$$\begin{array}{ccc} K & \hookrightarrow & L \\ | & & | \\ A & \hookrightarrow & B \end{array}$$

We first note that $\operatorname{Spec} A$ is simply the set of maximal ideals of A plus the zero ideal $\{0\}$, or in other words, $\operatorname{Spec} A = \max \operatorname{Spec} A \cup \{0\}$. Likewise, $\operatorname{Spec} B = \max \operatorname{Spec} B \cup \{0\}$. Also, clearly $0 \in \operatorname{Spec} B$ maps to $0 \in \operatorname{Spec} Z$, so we can simply look at the map

$$\max \operatorname{Spec} B \to \max \operatorname{Spec} A.$$

This map is surjective, because given any prime ideal P of A, we see that the ideal generated by $\pi(P)$ is a prime ideal, and then $\operatorname{Spec} B \to \operatorname{Spec} A$ maps that ideal to P.

If the map $\operatorname{Spec} B \to \operatorname{Spec} A$ maps $Q \mapsto P$, then we say that Q lies above P and P lies below Q. This is something very pictorial. There are many equivalent



conditions for Q lying above P. The following five conditions are all equivalent to Q lying above P.

(a) $Q \mid PS$
(b) $Q \supset PS$
(c) $Q \supset P$
(d) $Q \cap R = P$
(e) $Q \cap K = P$

Think about this example. Let $f(X) \in \mathbb{Z}[X]$ be an irreducible monic polynomial, and let $A = \mathbb{Z}[X]/(f(X))$. Suppose that this is a Dedekind domain. Let us consider a prime $p \in \mathbb{Z}$. Consider $\bar{f}(X) \in \mathbb{F}_p[X]$ be the reduction of $f(X)$ modulo p. Think about how $\bar{f}(X)$ factorizes in $\mathbb{F}_p[X]$.

10 February 25, 2016

We consider the following setting:

$$\begin{array}{ccc} I \cdot B \subseteq B & \hookrightarrow & L \\ \downarrow & & \downarrow{\scriptstyle n=[L:K]} \\ I \subseteq A & \hookrightarrow & K \\ \downarrow & & \downarrow \\ \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

10.1 Decomposition equation

Theorem 10.1. *Let $I = P$ be a prime ideal of A, and let*

$$PB = \prod_{i=1}^{r} Q_i^{e_i}.$$

Let $f(Q_i|P)$ be the relative field degree. Then

$$[L : K] = \sum_i f(Q_i|P)e(Q_i|P).$$

Note that we have proved this for $A = \mathbb{Z}$. It was done by simply observing that each sides are the exponent of p in

$$\|PB\| = |B/pB| = p^{[L:K]}.$$

But if we prove $\|PB\| = \|P\|^{[L:K]}$, then in general we will get the decomposition equation. That is, the following proposition is simply equivalent to the decomposition equation.

Proposition 10.2.

$$\|PB\| = \|P\|^{[L:K]}.$$

We shall prove the proposition using the following statement:

$$(*) \qquad \|PB\| = \|P\|^n \text{ for some } n \leq [L : K].$$

The verification is left as an homework.

Proof. We look at the extension B over A over $\mathbb{Z}$. Consider any prime (p) in $\mathbb{Z}$ and we look at the decomposition of pA and let it $pA = \prod_{i=1}^{r} P_i^{e_i}$. Then we have $\|pA\| = p^{[K:\mathbb{Q}]}$ and $\|pB\| = p^{[K:Q][L:K]}$.

Now we have

$$\|pB\|_B = \Big\| \prod_{i=1}^{r} P_i^{e_i} B \Big\|_B = \prod \|P_i^{e_i}\|_A^{n_i}$$

for some $n_i \leq [L : K]$. When we look at the exponent of p on both sides, we get

$$[K : \mathbb{Q}][L : K] = \sum_i n_i e(P_i|p) f(P_i|p).$$

But since $[K : \mathbb{Q}] = \sum_i e(P_i|p) f(P_i|p)$ and $n_i \leq [L : K]$, we see that all $n_i = [L : K]$. Thus we get the desired result. □

Let $f(X)$ be a monic irreducible polynomial in $\mathbb{Z}[X]$. Let $A = \mathbb{Z}[X]/(f(X))$ and assume that A is integrally closed. We want to look at how the ideal (p) splits inside A. Let

$$f(X) \equiv \prod_{i=1}^{r} f_i(X)^{e_i} \pmod{p}$$

where each $f_i(X)$ is irreducible modulo p. Let $P_i = (p, f_i(X)) \subset A$. Then we see that

$$A/P_i = \mathbb{Z}/p\mathbb{Z}[X]/(f_i(X))$$

is a field, and hence each P_i is a prime ideal. We also note that

$$\prod P_i^{e_i} = pA.$$

There are theorems such as the Chebotarev density theorem that describes how primes split.

10.2 Ramification and the discriminant

Theorem 10.3. *If $(p) \subset \mathbb{Z}$ ramifies in A, then p divides the discriminant of K.*

Proof. Let $pA = P^e P_2^{e_2} P_3^{e_3} \cdots$ where $e > 1$. Then we can write $pA = PI$ where I is divisible by all prime ideals of A that divide p. Then $I \supsetneq pA$ and therefore we can pick an element $\alpha \in I$ such that $\alpha \notin pA$.

Consider $\alpha_1, \ldots, \alpha_n \in A$ that generated A as an abelian group. There is a representation

$$\alpha = m_1\alpha_1 + m_2\alpha + \cdots + m_n\alpha_n,$$

and since $\alpha \notin pA$, there is a m_i that is not divisible by p. Let it be m_1 be the one, and let A_0 be the free abelian group generated by $\alpha, \alpha_2, \ldots, \alpha_n$. Then we see that the index $|A/A_0|$ is m_1 and thus $\operatorname{disc} A = m_1^2 \operatorname{disc} A_0$. Since p does not divide m_1, it suffices to that p divides $\operatorname{disc} A$.

Now α is in I, and hence α is in any prime ideal of A lying over p. Let L be a field extension of K that is Galois over $\mathbb{Q}$, and let B be the ring of integers in L. Then we see that α is contained in any prime ideal of B, because such an ideal will lie over some prime ideal of A lying over p. Let T be any prime ideal of B lying over p. Then for any $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$, we see that $\alpha \in \sigma^{-1}(T)$ and thus $\sigma(\alpha) \in T$. This shows that the discriminant $\operatorname{disc} K$ is in T and thus is in $T \cap \mathbb{Z} = (p)$. □

10.3 The Kronecker-Weber theorem

Definition 10.4. A cyclotomic field is any extension of the form $\mathbb{Q}[\zeta_n]$ where ζ_n is a primitive nth root of unity.

We note that $\mathrm{Gal}(\mathbb{Q}[\zeta_n], \mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 10.5 (Kronecker-Weber theorem)**.** *Any abelian extension over $\mathbb{Q}$ is a subfield of a cyclotomic extension of $\mathbb{Q}$.*

We first look at the case when $\mathbb{Q}[\sqrt{a}]$ is an abelian extension. Let

$$S = \sum_i \left(\frac{a}{p}\right)\zeta_p^i$$

be the Gauss sum. We have

$$S^2 = \sum_{i,j} \left(\frac{i}{p}\right)\left(\frac{j}{p}\right)\zeta_p^{i+j} = \sum_{i,j} \left(\frac{ij^2}{p}\right)\zeta_p^{j(i+1)} = \sum_{i,j} \left(\frac{i}{p}\right)\zeta_p^{j(i+1)} = \left(\frac{-1}{p}\right)p.$$

This show that $\sqrt{p}$ is in some cyclotomic extension. Therefore any thing that looks like $\sqrt{a/b}$ is contained in some cyclotomic extension.

11 March 1, 2016

11.1 The decomposition group

Let L/K be an Galois extension, and let $G = \mathrm{Gal}(L/K)$. Let A, B be the rings of integers in L and K. Consider a prime ideal $P \subset A$ and let $Q_1, \dots, Q_r$ be all the prime ideals lying over P. Any automorphism $\sigma \in G$ acts and Q_i and gives a prime ideal σQ_i lying over $\sigma P = P$. The marvelous fact is the following.

Theorem 11.1. *G acts transitively on $\{Q_1, \dots, Q_r\}$.*

Clearly G acts on $Q = \{Q_1, \dots, Q_r\}$. We can define the **decomposition group**

$$D = G_{Q_i} = \{\sigma \in G : \sigma Q_i = Q_i\}.$$

Since G/G_{Q_i} has a one-to-one correspondence with the orbit of Q_i, assuming the theorem we will have the following corollary.

Corollary 11.2. *$G/G_{Q_i} = G/D$ has a one-to-one correspondence to $\{Q_1, \dots, Q_r\}$.*

Proof of theorem. Suppose that the orbit of Q_1 and let $Q_1, \dots, Q_s$ under the action of G is smaller than Q, i.e., $s < r$. Then there is a prime ideal Q' outside $\{Q_1, \dots, Q_s\}$ lying over P.

Now apply the finite approximation theorem and find an element $\beta \in b$ with $\beta \equiv 1 \pmod{Q_i}$ for $i = 1, \dots, s$ and $\beta \in Q_i'$. Consider its norm $\alpha = \prod_{\sigma \in G} \sigma\beta$ in A. Since none of the $\sigma\beta$ is in Q_1, we have $\alpha \notin Q_1$. Since $P = Q_1 \cap A$, we have $\alpha \notin P$. On the other hand, since $\beta \in Q'$ we have $\alpha \in Q'$. Then $A \cap Q' = P$ contains α. Thus we arrive at a contradiction. □

Let $PB = Q_1^{e_1} Q_2^{e_2} \cdots Q_r^{e_r}$ and $[L : K] = \sum_{i=1}^{r} e_i f_i$, where $e_i = e(Q_i|P)$ and $f_i = f(Q_i|P)$. Since all prime ideals are Galois conjugates to each other, we have can let $f(Q_i|P) = f$ and $e(Q_i|P)$. Then simply have

$$[L : K] = efr.$$

Now consider $G_Q = D$, and let us look at the tower of extension:

$$\begin{array}{ccccc} L & \longhookleftarrow & B & \longhookleftarrow & Q \\ | & & | & & | \\ L^D & \longhookleftarrow & B_D & \longhookleftarrow & Q_D \\ | & & | & & | \\ K & \longhookleftarrow & A & \longhookleftarrow & P \end{array}$$

Now the transitive theorem says that

$$efr = [L : K] = |G| = |D| \cdot |G/D| = |D| \cdot r$$

and thus $|D| = ef$.

How does Q_D split in P? When we apply the transitivity theorem on L/L^D, which is a Galois extension of its own right, we see that Q is the only prime lying over Q_D by the definition of D. Then we have

$$e(Q|P)f(Q|P) = [L : L^D] = e(Q|Q_D)f(Q|Q_D).$$

Since $e(Q|P) = e(Q|Q_D)e(Q_D|P)$ and $f(Q|P) = f(Q|Q_D)f(Q_D|P)$, we see that

$$e(Q_D|P) = f(Q_D|P) = 1.$$

11.2 The inertia group

Now let us carry out a further analysis on the upper part of the diagram.

Definition 11.3. Any $\sigma \in D = G_Q$ fixes both B and Q to themselves. Thus it gives an isomorphism $B/Q \to B/Q$ over A/P. Now this means that there is a homomorphism

$$0 \longrightarrow I \hookrightarrow D \longrightarrow \mathrm{Gal}(k_Q/k_P).$$

We call this kernel I the **inertia subgroup** associated to Q.

$$\begin{array}{ccccc} L & \hookleftarrow & B & \hookleftarrow & Q \\ | & & | & & | \\ L^I & \hookleftarrow & B_I & \hookleftarrow & Q_I \\ | & & | & & | \\ L^D & \hookleftarrow & B_D & \hookleftarrow & Q_D \end{array}$$

We claim the following.

Proposition 11.4.

$$f(Q|Q_I) = 1.$$

Once we have this, we have

$$\begin{aligned} f &= f(Q|P) = f(Q|Q_I)f(Q_I|Q_D)f(Q_D|P) = f(Q_I|Q_D), \\ e &= e(Q|P) = e(Q|Q_I)e(Q_I|Q_D)e(Q_D|P) = e(Q|Q_I)e(Q_I|Q_D). \end{aligned}$$

Since there is a natural embedding $D/I \hookrightarrow \mathrm{Gal}(k_Q/k_P)$, we see that

$$f \geq |D/I| = e(Q_I|Q_D)f(Q_I|Q_D) = e(Q_I|Q_D)f.$$

Thus $e(Q_I|Q_D) = 1$ and it follows that $e = e(Q|Q_I)$. Thus Q over Q_I has no residue and entire ramification, and Q_I over Q_D has no ramification and entire residue.

Example 11.5. Let $\alpha = \sqrt[3]{14}$ and $\zeta = \zeta_3$. The splitting field of

$$X^3 - 14 = (X - \alpha)(X - \zeta\alpha)(X - \zeta^{-1}\alpha)$$

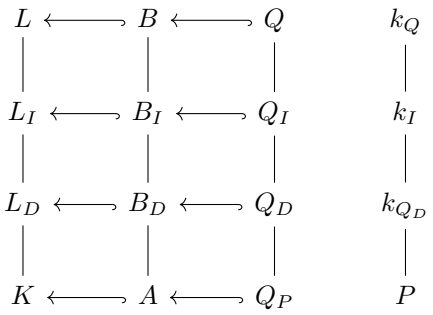
is $L = \mathbb{Q}(\alpha, \zeta)$, with Galois group isomorphic to S_3.

Let us take a random prime 13, and see how it splits in L. Since

$$X^3 - 14 \equiv X^3 - 1 = (X - 1)(X - \zeta)(X - \zeta^2) \pmod{13},$$

we see that (13) splits into three primes Q_1, Q_2, Q_3. Consider $Q = Q_1$ and look at the field L^D. Then we see that $P = (13)$ splits into $PB_D = Q_D R$, and $PB = Q_1 Q_2 Q_3$.

12 March 3, 2016



$$I \lhd D \twoheadrightarrow D/I \hookrightarrow \mathrm{Gal}(k_Q/k_P)$$

This is our setting.

12.1 Ramification in the tower

We know that if we let $Q_1, \ldots, Q_r$ be the set of primes lying over P, then $G = \mathrm{Gal}(L/K)$ acts on the Q_i's transitively. We recall that

$$G \supseteq G_Q = \{\sigma : \sigma Q = Q\}$$

and I_Q is a kernel of the induced map $G_Q \to \mathrm{Gal}(k_Q/k_P)$, or more explicitly,

$$G_Q \rhd I_Q = \{\sigma : \sigma \text{ on } B/Q \text{ is the identity}\}.$$

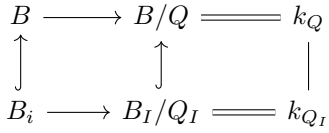
Let us denote $D_i = G_{Q_i}$ and L_{Q_i}. These are also moved in a natural way by any automorphism of L over K. That is, if $\sigma Q_i = Q_{i_\sigma}$, then

$$\sigma L_{D_i} = L_{D_{i_\sigma}}, \quad \sigma L_{I_i} = L_{I_{i_\sigma}}, \quad \sigma G_{Q_i}\sigma^{-1} = G_{Q_{i_\sigma}}, \quad \sigma I_{Q_i}\sigma^{-1} = I_{Q_{i_\sigma}}.$$

Proposition 12.1.

$$f(Q|Q_I) = 1.$$

Proof. We see that it suffices to prove that any automorphism of B/Q that is the identity on B_I/Q_I is the identity on B/Q. This is because any finite field extension of finite fields is Galois.



Let us consider any $\alpha \in B$ and look at the image $\bar{\alpha}$ under the map $B \to B/Q$. Let

$$g(X) = \prod_{\sigma \in I} (X - \sigma\alpha) \in B[X]$$

be the characteristic polynomial of α over L_I. This has coefficients in L_I and thus in B_I. If we reduce it modulo Q_I, then we get

$$\bar{g}(X) = \prod_{\sigma \in I} (X - \bar{\sigma}(\bar{\alpha})) = \prod_{\sigma \in I} (X - \bar{\alpha}).$$

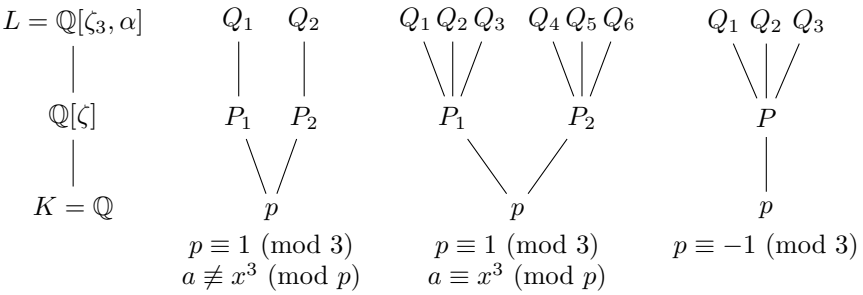
Therefore the only place $\bar{\alpha}$ can be sent is $\bar{\alpha}$. □

Hence we have the exact sequence

$$0 \longrightarrow I_Q \longrightarrow G_Q \longrightarrow \mathrm{Gal}(k_Q/k_P) \longrightarrow 0$$

Example 12.2. Let $a > 1$ be an integer that is cube-free. Take $\alpha = \sqrt[3]{a}$ and $L = \mathbb{Q}[\zeta_3, \alpha]$ be the splitting field of $X^3 - a = (X - \alpha)(X - \zeta\alpha)(X - \zeta^2\alpha)$. This is an S_3-Galois extension. Let $A = \mathbb{Z}$ and B be the ring of integers of $K = \mathbb{Q}$ and L respectively. Consider an prime p not dividing $3a$; this is taking an unramified prime.

Since p is unramified, we see that $pB = \prod_{i=1}^{r} Q_i$ for some primes Q_i in B. Then $6 = f \cdot r$ and we don't have many choices. We can exclude the case $r = 1$ and $f = 6$, because this would say that k_Q/k_P is S_3, but any Galois group of finite extensions of finite fields is cyclic. So we have the following three possibilities.



12.2 Ideal class group of $\mathbb{Q}[\zeta_{23}]$[3]

Definition 12.3. Let R be a Dedekind domain. Let G denote the group of fractional ideals, and let H be the subgroup of principal fractional ideals. We define

$$\mathfrak{h}(R) = G/H$$

as the **ideal class group** of R.

We are going to show that the ideal class group of $\mathbb{Q}[\omega]$, where $\omega = e^{2\pi i/23}$, is nontrivial. Let $\theta = (1 + \sqrt{-23})/2$ and consider the ring of integers of $\mathbb{Q}[\theta]$,

[3] This was a presentation by James Hotchkiss.

which is $\mathbb{Z}[\theta]$. We have the following tower of extensions:

$$\begin{array}{ccc} \mathbb{Q}[\omega] & \hookleftarrow & \mathbb{Z}[\omega] \\ \big| & & \big| \\ \mathbb{Q}[\sqrt{-23}] & \hookleftarrow & \mathbb{Z}[\theta] \\ \big| & & \big| \\ \mathbb{Q} & \hookleftarrow & \mathbb{Z} \end{array}$$

Let us take a prime ideal $\mathfrak{p} = (2, \theta) \subset \mathbb{Z}[\theta]$, and consider any $\mathfrak{q} \subset \mathbb{Z}[\omega]$ lying over $\mathfrak{p}$.

Lemma 12.4. $f(\mathfrak{q}|\mathfrak{p}) = 11$.

Proof. We note that $(2) = (2, \theta) \cdot (2, \bar{\theta})$ in $\mathbb{Z}[\theta]$, and thus $f(\mathfrak{p}|(2)) = 1$. Also, $f(\mathfrak{q}|(2))$ is the multiplicative order of 2 modulo 23, and thus is 11. It follows that $f(\mathfrak{q}|\mathfrak{p}) = 11$. □

Lemma 12.5. *In $\mathbb{Q}[\omega]$, we have $\mathfrak{q} = (2, \theta) = \mathfrak{p}\mathbb{Z}[\omega]$.*

Proof. We have $[\mathbb{Q}[\omega], \mathbb{Q}[\sqrt{-23}]] = 11$, and since $ref = 11$ and $f = 11$, we have $r = e = 1$. Thus we have the desired result. □

Proposition 12.6. *In $\mathbb{Z}[\theta]$, we have $(\theta - 2) = \mathfrak{p}^3$.*

Proof. Recall the **ideal norm** defined as

$$N_{\mathbb{Q}}^{\mathbb{Q}[\sqrt{-23}]}(I) = \mathbb{Z} \cap \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}[\sqrt{-23}]/\mathbb{Q})} I.$$

We proved in the homework that this is multiplicative, and $N(Q) = p^{f(Q|(p))}$, and $N((\alpha)) = N(\alpha)\mathbb{Z}$. Using this, we compute

$$N((\theta - 2)) = (\theta - 2)(\bar{\theta} - 2)\mathbb{Z} = 8\mathbb{Z}.$$

Also, $N(\mathfrak{p}) = 2\mathbb{Z}$. But since the only primes lying over 2 is $\mathfrak{p}$ and $\bar{\mathfrak{p}}$, we see that either $(\theta - 2)$ is either $\mathfrak{p}^3$, $\mathfrak{p}^2\bar{\mathfrak{p}}$, $\mathfrak{p}\bar{\mathfrak{p}}^2$, or $\bar{\mathfrak{p}}^3$. Because $(\theta - 2)$ is in $\mathfrak{p}$ but does not contain $\mathfrak{p}\bar{\mathfrak{p}} = (2)$, we see that $(\theta - 2) = \mathfrak{p}^3$. □

Lemma 12.7. $f(\mathfrak{q}|\mathfrak{p}) = 1$.

Proof. We see that $f(\mathfrak{q}|(2))$ is the order of 2 in $(\mathbb{Z}/23\mathbb{Z})^\times$, which is 11. Thus $f(\mathfrak{p}|(2))$ is 1 or 11, but we can easily check that it cannot be 11. Therefore $f(\mathfrak{p}|(2)$ is 1, and $f(\mathfrak{q}|\mathfrak{p}) = 11$. □

Lemma 12.8. *If $K \subset L$ then there is an homomorphism $\varphi : H(L) \to H(K)$ given by*

$$[I] \mapsto [N_K^L(I)].$$

Proof. We check that if $I \sim J$ then there exists α, β with $\alpha I \beta J$ and then $N(\alpha)N(I) = N(\beta)N(J)$. □

Now let us look at $N_K^L(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}|\mathfrak{p})}$. It follows that $\|\mathfrak{p}\|$ divides $\|\mathfrak{q}\| \cdot f(\mathfrak{q}|\mathfrak{p})$. Thus 3 divides 11 times the order of $\mathfrak{q}$ in the ideal class group, and it follows that $H(L)$ is nontrivial.

13 March 8, 2016

Suppose that L/K is Galois. We look at an intermediate extension L/K'. Then we see that it is also Galois and from the definition we directly get

Lemma 13.1.

$$I_Q(L/K') = I_Q(L/K) \cap \mathrm{Gal}(L/K'),$$
$$G_Q(L/K') = G_Q(L/K) \cap \mathrm{Gal}(L/K) \subset Gal(L/K).$$

Conversely, suppose that L'/K is a Galois sub extension so that $L \supset L' \supset K$. We have a surjective map $G(L/K) \twoheadrightarrow G(L'/K)$.

Lemma 13.2.

$$\begin{array}{ccc} G(L/K) & \twoheadrightarrow & G(L'/K) \\ \uparrow & & \uparrow \\ G_Q(L/K) & \twoheadrightarrow & G_{Q'}(L'/K) \\ \uparrow & & \uparrow \\ I_Q(L/K) & \twoheadrightarrow & I_{Q'}(L'/K) \end{array}$$

Proof. We see that the map $G(L/K) \to G(L'/K)$ indeed maps things into what we want. Now we need to show that the induced maps are surjective.

For the surjectivity of the map $G_Q(L/K) \twoheadrightarrow G_{Q'}(L'/K)$, we look at the action of $\mathrm{Gal}(L/L')$ on the set of prime ideals $\{Q_1, \dots, Q_r\}$ lying over Q'. Now we find a $\tilde{\sigma}$ such that $\tilde{\sigma}|_{L'} = \sigma$.

The surjectivity of the map $I_Q(L/K) \twoheadrightarrow I_{Q'}(L'/K)$ is left as an exercise. □

13.1 Frobenius structure of a Galois group

Let P be a prime ideal in K and $Q_1, \dots, Q_r$ be the prime ideals in L lying over K. We see that G acts transitively on $Q_1, \dots, Q_r$, and hence G_{Q_j} and G_{Q_i} are conjugates, and likewise I_{Q_j} and I_{Q_i} are conjugates. Thus we can simply introduce a notation G_P and I_P, which are defined up to conjugacy. Then $Q_P/I_P = \mathrm{Gal}(k_Q/k_P)$ for any Q lying over P. Because only finitely many prime ideals P are ramified in L/K, for any unramified P, we get $Q_P \cong \mathrm{Gal}(k_Q/k_P)$.

We know that for any finite field extensions $\mathbb{F}_{q^m}/\mathbb{F}_q$, its Galois group is cyclic of order ω with the generator $\varphi_q : x \mapsto x^q$, which is called the **relative Frobenius map**.

Now we have

$$\mathrm{Gal}(L/K) \supset G_P \cong \mathrm{Gal}(k_Q/k_P) \ni \varphi_P$$

for any unramified P. Now this gives a canonical map

$$P \mapsto \{\varphi_P\}_{\text{conj.}} \in \mathrm{ConjClass}\{\mathrm{Gal}(L/K)\}.$$

This is called the **Frobenius structure** for the Galois group.

The Frobenius structure gives a complete description of how the prime P splits, because $\mathrm{Gal}(L/L_D) = \langle \varphi_p \rangle \subset \mathrm{Gal}(L/K)$. For example, $r = n$ can happen if and only if $\varphi_P = 1$ in $\mathrm{Gal}(L/K)$.

Example 13.3. Let us look at L/K where $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}$. In this case the Galois group is canonically $G \cong (\mathbb{Z}/m\mathbb{Z})^*$. For a prime p, the conjugacy class $\{\varphi_p\}$ is simply p modulo m.

The Chebotarev density theorem states that for any conjugacy class there are infinitely many primes. From the previous example, we see that the Cheboratev density theorem implies the Dirichlet's theorem on arithmetic progressions.

14 March 10, 2016

Let L/K be a Galois extension and $G = \mathrm{Gal}(L/K)$. For any unramified prime P, there is a map

$$P \mapsto \{\phi_P\} \in \mathrm{ConjClass}(\mathrm{Gal}(L/K)),$$

and this $\{\phi_P\}$ completely determines the splitting behavior of P in L/K. For instance, what does $\phi_P = \mathrm{id}$ mean? Since f is the order of ϕ_P in $\mathrm{Gal}(k_Q/k_P)$, we see that $\phi_P = \mathrm{id}$ is equivalent to P splitting completely in K/L.

Let us look at cyclotomic fields. Consider $L = \mathbb{Q}(\zeta_n)$ over $K = \mathbb{Q}$. Then the Frobenius element ϕ for p is the automorphism mapping $\zeta_n \mapsto \zeta_n^p$. Then p splitting completely in K is equivalent to $p = 1 + mn$ for some m. Likewise, p being inert (remaining prime in L) is equivalent to p being a generator of $(\mathbb{Z}/n\mathbb{Z})^\times$.

For fun, let us also look at when p totally ramifies in $\mathbb{Q}(\zeta_n)$. If $n = p^a \cdot m$, the field $\mathbb{Q}(\zeta_n)$ contains $\mathbb{Q}(\zeta_m)$. Since p does not divide m, we see that p unramifies $\mathbb{Q}(\zeta_m)$. (We can simply compute the discriminant to see this.) Then the degree $\varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ must be 1, and we conclude that $m = 1$ or 2. In fact, it is a nice exercise to check that p totally ramifies if and only if $m = 1$ or 2.

14.1 Finiteness of the ideal class group

Let A be the ring of integers of a field K over $\mathbb{Q}$. Recall that $\|I\| = |A/I|$, and that

$$\|(\alpha)\| = |A/\alpha A| = |N_{K/\mathbb{Q}}(\alpha)|.$$

Also, we note that for a fixed $B < +\infty$, there are only finitely many ideals $I \subset A$ with $\|I\| \le B$.

Let us fix $A \subseteq K$.

Lemma 14.1. *There exists a $\lambda < +\infty$ such that for any nonzero ideal I, there exists a $\alpha \in I$ such that $|N_{K/\mathbb{Q}}(\alpha)| \le \lambda \|I\|$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-module basis of A. We are going to make a box

$$\left\{ \sum_{0 \le h_i \le m} h_i \alpha_i \right\}$$

for an integer $m^n \le \|I\| < (m+1)^n$. Then the box maps to A/I, and the number of elements in the box is greater than A/I. Now Dirichlet's box principle says that there are two elements γ, δ that maps to the same element. That is,

$$0 \ne \gamma - \delta = \sum c_i \alpha_i \in I$$

with $|c_i| \le m$. I can now estimate the norm. From

$$N_{K/\mathbb{Q}}\alpha = \prod_{j=1}^{n} \sigma_j \Big(\sum_i c_i \alpha_i \Big) = \prod_{j=1}^{n} \sum_i c_i \sigma_j \alpha_i$$

it follows that

$$|N_{K/\mathbb{Q}}\alpha| = \prod_j \Big| \sum_i c_i \sigma_j \alpha_i = \prod_j \sum_i |c_i||\sigma_j \alpha_i| \leq m^n \prod_j \sum_i |\sigma_j \alpha_i| \leq \|I\|\lambda$$

for $\lambda = \prod_j \sum_i |\sigma_j \alpha_i|$ not dependent on I. □

Corollary 14.2. *The ideal class group $H(K)$ is finite.*

Proof. For any class of ideals in $H(K)$, let us pick an ideal I in it. By the lemma above, we have an ideal $\alpha \in I$ with small $|N_{K/\mathbb{Q}}(\alpha)|/\|I\|$. If we let $(\alpha) = I \cdot J$, then we have

$$|N_{K/\mathbb{Q}}\alpha| = \|I \cdot J\| = \|I\|\|J\| \leq \lambda \|I\|.$$

Then $\|J\| \leq \lambda$. This shows that there are only finitely many possibilities for the inverse element of I in the ideal class group. Thus the ideal class group is finite. □

Example 14.3. Let us compute the ideal class group of $K = \mathbb{Q}(\sqrt{d})$ for $d = 2, 3, -5$. In each case, we have $\lambda = 5.8\ldots, 7.5\ldots, 10.7\ldots$. Thus we can only look at ideals $\|I\|$ with $\|I\| \leq 5, 7, 10$. For such ideals, I, we have that

$$N_{K/\mathbb{Q}} I = \|I\|\mathbb{Z}.$$

Thus we need only look at the prime factorization of (p) in L for $p \leq 5, 7, 10$.

For $d = 2$, we have

$$(2) = (\sqrt{2})^2 \qquad (5) = (5)$$
$$(3) = (3)$$

and because all are principal, we see that $H(K)$ is trivial, i.e., $K = \mathbb{Q}(\sqrt{2})$ is a principal ideal domain.

Likewise

$$(2) = (-1 + \sqrt{3})(1 + \sqrt{3}) \qquad (5) = (5)$$
$$(3) = (\sqrt{3})^2 \qquad (7) = (7)$$

and hence again $H(K)$ is trivial and $\mathbb{Q}(\sqrt{3})$ is a principal ideal domain.

In the $d = -5$ case, we have two ideals

$$I_2 = (2, 1 + \sqrt{5}), \quad I_3 = (3, 1 + \sqrt{5})$$

each with $\|I_2\| = 2$ and $\|I_3\| = 3$. With a little more work, we see that these are inverses in the ideal class group and thus $|H(K)| = 2$.

15 March 22, 2016

15.1 The Minkowski bound

Let $K/\mathbb{Q}$ be a finite extension of degree n. Recall that there are exactly n embeddings of K into $\mathbb{C}$, with r of them real and $2s$ of them literally complex. Let $\sigma_1, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$ be the real embeddings and let $\tau_1, \bar{\tau}_1, \dots, \tau_s, \bar{\tau}_s : K \hookrightarrow \mathbb{C}$ be the purely complex embeddings. Then we have a fundamental embedding

$$K \longhookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$$

than sends

$$\begin{aligned}\alpha &\mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha)) \\ &= (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \Re(\tau_1(\alpha)), \Im(\tau_1(\alpha)), \dots, \Re(\tau_s(\alpha)), \Im(\tau_s(\alpha))).\end{aligned}$$

Now with a suitable change of basis, we can change $\Re(\tau_i(\alpha))$ and $\Im(\tau_i(\alpha))$ into $\tau_i(\alpha)$ and $\bar{\tau}_i(\alpha)$. The determinant of this coordinate change matrix will be $(2i)^s$.

Let $A = \alpha_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. Then we see that the square of the determinant of the matrix

$$\begin{bmatrix} \sigma_1(\alpha) & \cdots & \sigma_r(\alpha) & \tau_1(\alpha) & \bar{\tau}_1(\alpha) & \cdots & \tau_s(\alpha) & \bar{\tau}_s(\alpha) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha) & \cdots & \sigma_r(\alpha) & \tau_1(\alpha) & \bar{\tau}_1(\alpha) & \cdots & \tau_s(\alpha) & \bar{\tau}_s(\alpha) \end{bmatrix}$$

is the discriminant of K.

Consider the image Λ of A under the fundamental embedding. This is a lattice in $\mathbb{R}^n$, and we can look at $\operatorname{vol}(\mathbb{R}^n/\Lambda)$. This is defined as the volume of the fundamental parallelotope for Λ

$$F = \{t_1\alpha_1 + \cdots + t_n\alpha_n : 0 \le t_i < 1\}.$$

Then $\mathbb{R}^n$ is the disjoint union $\mathbb{R}^n = \amalg_{\lambda\in\Lambda}(F + \lambda)$. Because $\operatorname{vol}(\mathbb{R}^n/\Lambda) = |\Lambda_0/\Lambda| \operatorname{vol}(\mathbb{R}^n/\Lambda_0)$, we immediately have the following theorem.

Theorem 15.1.

$$\operatorname{vol}(\mathbb{R}^n/A) = 2^{-s}\sqrt{|\operatorname{disc} A|}.$$

Corollary 15.2.

$$\operatorname{vol}(\mathbb{R}^n/I) = 2^{-s}\sqrt{|\operatorname{disc} A|} \cdot \|I\|.$$

This corollary can help us improve λ. Let us define a funny norm on $\mathbb{R}^n$ as

$$N(x_1, \dots, x_r, y_{r+1}, \dots, y_n) = x_1 \cdots x_r (y_{r+1}^2 + y_{r+2}^2) \cdots (y_{n-1}^2 + y_n^2).$$

This is made so that if x is the image of α under the fundamental embedding, then $N(x) = N_{K/\mathbb{Q}}(\alpha)$.

Let us consider the ball

$$\{x \in \mathbb{R}^n : |N(x)| \le t\}$$

with respect the the norm. We apply Minkowski's theorem.

Theorem 15.3 (Minkowski)**.** *Let $\Omega \subset \mathbb{R}^n$ be a compact, convex, and centrally symmetric set with positive volume. Let Λ be any lattice in $\mathbb{R}^n$. If $\mathrm{vol}(\Omega) \geq 2^n \cdot \mathrm{vol}(\mathbb{R}^n/\Lambda)$ then Ω contains a nonzero lattice point in Λ.*

Because we want to make sure something is in the ball, we want to find a convex, symmetric $\Omega \subset \{x : |N(x)| \leq 1\}$ to have as large volume as possible. This is done by looking at the arithmetic norm

$$AN(x) = \frac{1}{n}\Big(\sum_{i=1}^{s}|x_i| + 2\sqrt{y_{r+1}^2 + y_{r+2}^2} + \cdots + 2\sqrt{y_{n-1}^2 + y_n^2}\Big).$$

Clearly, $\{x : |N(x)| \leq 1\} \supset \{x : |AN(x)| \leq 1\}$, and $\Omega(1) = \{x : |AN(x)| \leq 1\}$ is convex and centrally symmetric. Moreover, we can calculate its volume

$$\mathrm{vol}(\Omega(1)) = \frac{n^n}{n!}2^r\Big(\frac{\pi}{2}\Big)^s.$$

Because $t\Omega(1) = \{x : |AN(x)| \leq t\} \subset \{x : |N(x)| \leq t^n\}$, we can apply the Minkowski theorem to $t\Omega(1)$ and get the following corollaries.

Corollary 15.4. *I contains a point x with*

$$|N(x)| \leq \frac{n!}{n^n}\Big(\frac{8}{\pi}\Big)^s \mathrm{vol}(\mathbb{R}^n/I).$$

Corollary 15.5. *An ideal I contains a nonzero element α with*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s \sqrt{|\mathrm{disc}\, A|} \cdot \|I\|.$$

Corollary 15.6. *Every ideal class contains an ideal J with*

$$\|J\| \leq \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s \sqrt{|\mathrm{disc}\, A|}.$$

Corollary 15.7.

$$|\mathrm{disc}\, A| \geq \frac{n^n}{n!}\Big(\frac{\pi}{4}\Big)^s.$$

Now the right hand side is strictly greater than 1 when $n > 1$.

Corollary 15.8. *Every nontrivial extension $K/\mathbb{Q}$ has discriminant greater than 1, i.e., has some prime that is ramified.*

16 March 24, 2016

Let $K/\mathbb{Q}$ be an extension of degree n. Let r and $2s$ be the number of real and complex embeddings. The fundamental embedding is the map $K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$.

We used the "Existence of an element lemma" to get the Minkowski bound.

Lemma 16.1. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. There exists an $0 \neq x \in \Lambda$ such that $|N(x)| \leq \frac{2^n}{V} \operatorname{vol}(\mathbb{R}/\Lambda)$, where N is the funny norm.*

Theorem 16.2. *Every ideal class is represented by an ideal I with*

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

16.1 Computation of ideal class group

Let us denote $\Delta = \operatorname{disc}(K)$.

Corollary 16.3. *If*

$$|\Delta| < 4\frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2s},$$

then the ring of integers has trivial ideal class group, i.e., its class number is 1. In particular, this is true for $K = \mathbb{Q}(\sqrt{m})$ for $m = 2, 3, 5, 13; -1, -2, -3, -7$.

There is a big difference between the real quadratic case and the imaginary quadratic case.

Theorem 16.4. *The only imaginary quadratic fields of class number 1 is $\mathbb{Q}(\sqrt{m})$ for $m = -1, -2, -3, -7, -11, -19, -43, -67, -163$.*

Conjecture 16.5. *About $3/4$ of the real quadric fields are of class number 1.*

1. $K = \mathbb{Q}(\sqrt{7})$

   The discriminant is $\Delta = 28$ and we only have to check ideals of $\|I\| \leq \frac{1}{2}\sqrt{\Delta} = 2.6\ldots$. Then becuase $(3+\sqrt{7})(3-\sqrt{7}) = (2)$, we see that the class number is 1.

2. $K = \mathbb{Q}(\sqrt{-30})$

   The discrimant is $\Delta = -120$. Then because $\frac{1}{2}\sqrt{120} = 5.47\ldots$, we have to check for primes $2, 3, 5$. Because they all divide 30, they all ramify into

   $$(2) = P_2^2, \quad (3) = P_3^2, \quad (5) = P_5^2.$$

   They are all nontrivial, and also $(\sqrt{-30}) = P_2P_3P_5$. This implies that the ideal class group is isomorphic to $C_2 \times C_2$.

16.2 Higher ramification groups[4]

Let L/K be a Galois extension, and let S, R be the ring of integers in L and R. Consider a prime ideal $\mathfrak{p} \subset R$ and a prime $\mathfrak{q} \subset S$ lying over $\mathfrak{p}$. We define the **higher ramification group** as

$$V_m = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}^{m+1}}\}.$$

We see that any $\sigma \in G = \mathrm{Gal}(L/K)$ induces an automorphism $\overline{\sigma}$ of $S/\mathfrak{q}^{m+1}$ over $R/\mathfrak{q}^{m+1}$ and hence we have a map

$$\iota : G \to \mathrm{Aut}((S/\mathfrak{q}^{m+1})/(R/\mathfrak{q}^{m+1})).$$

Lemma 16.6. *The kernel of ι is $\ker \iota = V_m$.*

We have a tower of normal subgroups of D

$$D \supset V_0 = I \supset V_1 \supset V_2 \supset \cdots.$$

We also have the following lemma, because the intersection of all of them is trivial.

Lemma 16.7. *For all sufficiently large m, $V_m = 1$.*

Theorem 16.8. *Choose an $\pi \in \mathfrak{q} - \mathfrak{q}^2$, and let $\sigma \in I$. Then $\sigma \in V_m$ if and only if $\sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^{m+1}}$.*

Proof. We will first prove a slightly weaker statement.

Proposition 16.9. *Choose an $\pi \in \mathfrak{q} - \mathfrak{q}^2$, and let $\sigma \in V_{m-1}$. Then $\sigma \in V_m$ if and only if $\sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^{m+1}}$.*

Proof. Suppose that $\sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^{m+1}}$. For any $\alpha \in \pi S$, we have $\alpha = \pi\beta$ for some β. Then

$$\sigma(\pi\beta) = \sigma(\pi)\sigma(\beta) \equiv \pi\beta \pmod{\mathfrak{q}^{m+1}}$$

since $\sigma \in V_{m-1}$.

Next we show $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}^{m+1}}$ for any $\alpha \in \mathfrak{q}$. Because $\pi \in \mathfrak{q} - \mathfrak{q}^2$, the principal ideal (π) factorizes as

$$(\pi) = \mathfrak{q} \prod_i \mathfrak{q}_i^{e_i}.$$

If we pick some $\beta \in \prod \mathfrak{q}_i^{e_i}$ then $\alpha\beta \in \pi S$ while $\beta \notin \mathfrak{q}$. Since

$$\beta\sigma(\alpha) \equiv \sigma(\beta)\sigma(\alpha) = \sigma(\beta\alpha) \equiv \beta\alpha \pmod{\mathfrak{q}^{m+1}},$$

we can cancel out β and get the desired result.

Lastly, we look at an arbitrary $\alpha \in S$. This follows from the fact that it is true for $\alpha \in \mathfrak{q}$.[5] □

[4] This was a presentation by Vikram Sundar.

[5] I did not understand the argument.

Now returning to the original problem, assume that $\sigma \in I$ and $\sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^{m+1}}$. Suppose that $\sigma \in V_i - V_{i+1}$. Then because of the previous proposition, we see that $i \geq m$. Hence $\sigma \in V_m$. □

We now look at the structure of the ramification groups.

Theorem 16.10. *For $m \geq 2$, there is a canonical injection $V_{m-1}/V_m \to S/\mathfrak{q}$.*

Proof. We start with a lemma:

Lemma 16.11. *Fix $\pi \in \mathfrak{q} - \mathfrak{q}^2$. For each $\sigma \in V_{m-1}$, there exists an $\alpha_\sigma \in S$ such that*

$$\sigma(\pi) \equiv \pi + \alpha_\sigma \pi^m \pmod{\mathfrak{q}^{m+1}}.$$

Moreover, α_σ is unique modulo $\mathfrak{q}$.

Proof. Note that $\pi^m = \mathfrak{q}^m - \mathfrak{q}^{m+1}$. Then $\sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^m}$ by definition. Let $(\pi^m) = \mathfrak{q}^m \prod \mathfrak{q}_i^{e_i}$. By the Chinese remainder theorem, there exists a unique x up to modulo $\mathfrak{q}(\pi^m)$ such that

$$x \equiv \sigma(\pi) - \pi \pmod{\mathfrak{q}^{m+1}}, \quad x \equiv 0 \pmod{\prod \mathfrak{p}_i^{e_i}}.$$

Letting $x = \alpha\pi^m$, we get an α up to modulo $\mathfrak{q}$. It is clear that the congruence above is equivalent to $\sigma(\pi) \equiv \pi + \alpha\pi^m \pmod{\mathfrak{q}^{m+1}}$. □

This lemma gives a map $V_{m-1} \to S/\mathfrak{q}$. If fact, this is a homomorphism because

$$\sigma(\tau(\pi)) \equiv \sigma(\pi + \alpha_\tau \pi^m) \equiv \sigma(\pi) + \sigma(\alpha_\tau)\pi^m \equiv \pi + (\alpha_\sigma + \alpha_\tau)\pi^m \pmod{\mathfrak{q}^{m+1}}.$$

Also, the kernel is V_m by definition. This induces an injective map $V_{m-1}/V_m \to S/\mathfrak{q}$. □

Corollary 16.12. *Let $p = \operatorname{char}(S/\mathfrak{q})$. The quotient V_{m-1}/V_m is an abelian group of order a power of p.*

Similarly, we have the following.

Theorem 16.13. *There is a canonical injection $I/V_1 \to (S/\mathfrak{q})^\times$.*

Corollary 16.14. *The quotient I/V_1 is a cyclic group of order dividing $|S/\mathfrak{q}|-1$.*

17 March 29, 2016

We have the fundamental embedding $K \to E \cong \mathbb{R}^r \times \mathbb{C}^s$ as usual.

Lemma 17.1 (Pliability lemma)**.** *Let $C_1, \dots, C_{r+s} > 0$ be real numbers and assume that $\prod C_i \geq (2/\pi)^s \sqrt{|\mathrm{disc}(A)|}$. Then there exists an element α with $|N_{K/\mathbb{Q}}(\alpha)| < (2/\pi)^s \sqrt{|\mathrm{disc}(A)|}$, and*

$$|x_i| \leq C_i \quad (i = 1, \dots, r), \quad y_{r+1}^2 + y_{r+2}^2 \leq C_{r+1}, \ \dots \ , y_{2n-1}^2 + y_{2n}^2 \leq C_{r+s}.$$

Proof. The set $|x_i| \leq C_i, y_{r+2i-1}^2 + y_{r+2i}^2 \leq C_{r+i}$ is convex and centrally symmetric. We can apply Minkowski's theorem. □

17.1 Logarithm of the fundamental embedding

The fundamental embedding maps $A \subset K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$. This map is homomorphism between rings, and this induces a homomorphism of groups $A^* \subset K^* \hookrightarrow (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$. I am going to write the group of units $A^* = U$ and $(\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$. Now we can map this to

$$A^* \subset K^* \hookrightarrow (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \xrightarrow{\text{“log”}} \mathbb{R}^{r+s}$$

by sending

$$\begin{aligned}(x_1, \dots, x_r, &y_{r+1}, y_{r+2}, \dots, y_{n-1}, y_n) \\ &\mapsto (\log|x_1|, \dots, \log|x_r|, \log(y_{r+1}^2 + y_{r+2}^2), \dots, \log(y_{2n-1}^2 + y_{2n}^2))\end{aligned}$$

in the logarithm map. I am happy to call the composition also as log.

Proposition 17.2. *If for $\alpha \in K^*$ and $\log(\alpha) = (a_1, \dots, a_{r+s})$, then*

$$\sum_{i=1}^{r+s} a_i = \log|N(\alpha)|.$$

Proof. This is straightforward given the definition of the logarithm map. □

Corollary 17.3. *The map* log *maps U to $H \subset \mathbb{R}^{r+s}$, where $H = \{(a_1, \dots, a_{r+s}) : \sum a_i = 0\}$.*

The first question is, what is the kernel of $U \to H$? It consists of roots of unity, and hence is a finite cyclic group of roots of unity.

$$0 \longrightarrow \left\{ \begin{matrix} \text{finite} \\ \text{cyclic} \\ \text{group} \end{matrix} \right\} \longrightarrow U \longrightarrow H$$

Moreover, it has discrete image. (Think about this.)

Theorem 17.4 (Dirichlet unit theorem)**.** *The image of U is a full lattice in $H \cong \mathbb{R}^{r+s-1}$.*

Corollary 17.5. *U is an abelian group isomorphic to the product of a finite cyclic group and $\mathbb{Z}^{r+s-1}$.*

I will give the proof next time, and in the remaining minute, let us work out an example.

Example 17.6. Consider the case $r + s - 1 = 1$. If $(r, s) = (2, 0)$, it is a real quadratic field. If $(r, s) = (1, 1)$, it is a cubic filed with unique real embedding. In these cases, U is $\mathbb{Z}$ times a finite cyclic group.

18 March 31, 2016

Recall the pliability lemma:

Lemma 18.1 (Pliability lemma)**.** *For any positive number $C_1, \dots, C_{r+s}$ with $\prod C_i \geq (2/\pi)^s \sqrt{|\Delta|} = B$, there is an $\alpha \in A$ such that $|N_{K/\mathbb{Q}}(\alpha)| \leq B$ and $|\sigma_i(\alpha)| \leq C_i$ and $|\tau_j(\alpha)|^2 \leq C_{r+j}$.*

The logarithm map is the group homomorphism defined as

$$U = A^* \hookrightarrow K^* \hookrightarrow (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \xrightarrow{\log} \mathbb{R}^{r+s}.$$

We noted that the image lies in the hyperplane $H = \{\sum a_i = 0\}$, and the kernel is the roots of unity.

18.1 Dirichlet unit theorem

Theorem 18.2 (Dirichlet unit theorem)**.** *The image of U under* log*, which is isomorphic to $U/\ker \log$, is a lattice of rank $r + s - 1$.*

Lemma 18.3. *Let k be an integer with $1 \leq k \leq r + s$ and $\alpha \in A$ be a nonzero integer. Let $\log \alpha = (a_1, \dots, a_{r+s})$. Then there exists a nonzero $\beta \in A$ with $\log \beta = (b_1, \dots, b_{r+s})$ such that $|N_{K/\mathbb{Q}}(\beta)| \leq (2/\pi)^s \sqrt{|\Delta|}$ and $b_i < a_i$ for $i \neq k$.*

The point is that we know nothing about b_k at all!

Proof. Take C_i smaller than e^{a_i} for $i \leq k$ and take any C_k so that $\prod C_i = (2/\pi)^s \sqrt{|\Delta|}$. Then we get what we want from the pliability lemma. □

Proof of the Dirichlet unit theorem. Take any nonzero $\alpha^{\{1\}} \in A$. Using the lemma, we can inductively define a sequence of nonzero integers $\alpha^{\{1\}}, \alpha^{\{2\}}, \dots$ with $\log \alpha^{\{i\}} = (a_1^{\{i\}}, \dots, a_{r+s}^{\{i\}})$ such that $|N_{K/\mathbb{Q}}(\alpha^{\{m\}})| \leq B$ and

$$a_i^{\{1\}} > a_i^{\{2\}} > a_i^{\{3\}} > \cdots$$

for all $i \neq k$.

Note that $\|(\alpha^{\{m\}})\| = |N_{K/\mathbb{Q}} \alpha^{\{m\}}| \leq B$. The sequence of ideals generated by $\alpha^{\{m\}}$ has bounded norm, and therefore there must be $m < n$ such that $(\alpha^{\{m\}}) = (\alpha^{\{n\}})$. Then $\alpha^{\{m\}} = u_k \alpha^{\{n\}}$ for some u_k, and this u_k must be a unit. If we let $\log u_k = (v_1, \dots, v_{r+s})$, then by definition $v_i < 0$ for $i \neq k$. It automatically follows that $v_k > 0$ since they must add up to zero.

We claim that u_k is linearly independent in the logarithm space (or equivalently, under multiplication). Consider the matrix

$$\begin{matrix} u_1 \\ \vdots \\ u_{r+s} \end{matrix} \quad \begin{pmatrix} v_{1,1} & \cdots & v_{1,r+s} \\ \vdots & \ddots & \vdots \\ v_{r+s,1} & \cdots & v_{r+s,r+s} \end{pmatrix}$$

We want to prove that this matrix has rank $r+s-1$. It has a special property: all diagonal entires are positive and the off-diagonal entries are negative. Also the sum of each row is zero. This gives a linear relation above columns $\sum c_i = 0$. Suppose that there exists another linear relation $\sum t_i c_i = 0$. We can suppose that $t_k = 1$ is the maximum and then $1 = t_k \geq t_i$ for all other i. Let us look at the kth entry. Then

$$0 = \sum t_i v_{k,i} = v_{k,k} + \sum_{i \neq k} t_i v_{k,i} \leq v_{k,k} + \sum_{i \neq k} v_{k,i} = 0$$

where equality can hold only if all $t_1 = t_2 = \cdots = t_{r+s} = 1$. Therefore the rank is $r+s-1$. □

Example 18.4. Let $K = \mathbb{Q}[\sqrt{D}]$ with $0 < D \not\equiv 1 \pmod 4$ squarefree. Then because $s = 0$ and $r = 2$, we see that the set of units is $\{\pm 1\} \times u^{\mathbb{Z}}$ for some $u > 1$.

18.2 The different ideal[6]

For a number field K, we denote by $\mathcal{O}_K$ its ring of integers.

Example 18.5. Let $\alpha^3 - \alpha - 1 = 0$ and consider the field $K = \mathbb{Q}(\alpha)$. Then $\operatorname{disc}(\mathbb{Z}[\alpha]) = 23.$ and so $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\operatorname{disc} K = 23$. We know that 23 ramifies and because $x^3 - x - 1 = (x-3)(x-10)^2 \pmod{23}$, it splits into $\mathfrak{pq}^2$. But we don't know which one ramifies.

Definition 18.6. Let L be a lattice in K. We define the **dual lattice** as

$$L^\vee = \{\alpha \in K : T_{K/\mathbb{Q}}(\alpha L) \subset \mathbb{Z}\}.$$

For a lattice $L = \bigoplus \mathbb{Z} e_i$, we have $L^\vee = \bigoplus \mathbb{Z} e_i^\vee$, where $\{e_i^\vee\}$ is the dual basis of $\{e_i\}$ with respect to the trace.

Proposition 18.7. *For any lattice L, we have the following.*

(1) $L^{\vee\vee} = L$

(2) $L_1 \subset L_2$ *if and only if* $L_1^\vee \supset L_2^\vee$

(3) $(L_1 + L_2)^\vee = L_1^\vee \cap L_2^\vee$

(4) $(L_1 \cap L_2)^\vee = L_1^\vee + L_2^\vee$

(5) $(\alpha L)^\vee = \alpha^{-1} L^\vee$

Proposition 18.8. *For a fractional ideal $\mathfrak{a}$ in K, its dual $\mathfrak{a}^\vee$ is also a fractional ideal. Moreover, $\mathfrak{a}^\vee = \mathfrak{a}^{-1}\mathcal{O}_K^\vee$.*

Proposition 18.9. *$\mathcal{O}_K$ is the largest fractional ideal in K whose elements all have trace in $\mathbb{Z}$.*

[6] This was a presentation by Amanda Glazer

Definition 18.10. We define the **different ideal** of K as

$$D_K = (\mathcal{O}_K^\vee)^{-1} = \{x \in K : x\mathcal{O}_K^\vee \subset \mathcal{O}_K\}.$$

Example 18.11. Let $K = \mathbb{Q}(i)$. Then $\mathcal{O}_K = \mathbb{Z}[i]$ and we see that $\mathbb{Z}[i]^\vee = \frac{1}{2}\mathbb{Z}[i]$. Then $D = 2\mathbb{Z}[i]$.

Theorem 18.12. *The norm of the different ideal is* $\|D_K\| = |\mathrm{disc}(K)|$.

Lemma 18.13. *For any nonzero ideal* $\mathfrak{a}$ *in* $\mathcal{O}_K$, $\mathfrak{a} \mid D_K$ *if and only if* $T(\mathfrak{a}^{-1}) \subseteq \mathbb{Z}$.

Theorem 18.14 (Dedekind)**.** *The prime ideal factors of* D_K *are the primes in* K *that ramify over* $\mathbb{Q}$. *More precisely, for any prime ideal* $\mathfrak{p}$ *in* $\mathcal{O}_K$ *lying over a prime number* p *with ramification index* $e = e(\mathfrak{p} \mid p)$, *the exact power of* $\mathfrak{p}$ *in* D_K *is* $\mathfrak{p}^{e-1}$ *if* $p \nmid e$ *and* $\mathfrak{p}^e$ *if* $p \mid e$.

Example 18.15. Let us go back to the example $\alpha^3 - \alpha - 1 = 0$. Because we have $23 = (\mathfrak{p}\mathfrak{q}^2)$ and $N(D_K) = |\mathrm{disc}(K)| = 23$, we have $D_K = \mathfrak{q}$. Hence we can simply compute D_K to get $\mathfrak{q}$.

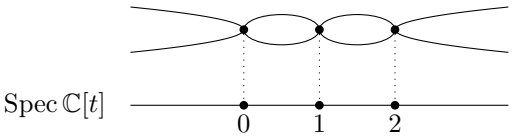
19 April 5, 2016

Recall Minkowski's bound: every ideal class has a representative ideal I with

$$\|I\| \le \left(\frac{4}{\pi}\right)^r \frac{n!}{n^n}\sqrt{|\Delta|}.$$

A corollary is that every nontrivial field extension has a prime that ramifies.

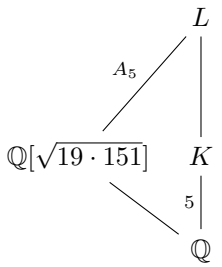
There is a function field analogue of the theory. Consider $\mathbb{C}[t] \subset \mathbb{C}(t)$ be the ring of integers and let K be a finite field extension of $\mathbb{C}(t)$ with A its ring of integers. The splitting of primes can be described geometry. Suppose that $A = \mathbb{C}[t,y]/(y^2 - g(t))$ where $g(t) = t(t-1)(t-2)$. Each prime in $\operatorname{Spec}\mathbb{C}[t] = \mathbb{C}$ (we ignore the zero ideal) either splits into two discint primes, ramifies, or has residue degree 2. But there is no such thing as residue degree 2, because $\mathbb{C}$ is algebaically closed.



Now there is a geometric reason why there always has to be a ramification. Becasue $\mathbb{C}$ has trivial fundamental group, there cannot be a covering space with no ramification. Likewise in the $\mathbb{Q}$ case, what we are saying when we state that every extension has a ramification is that $\operatorname{Spec}\mathbb{Z}$ has trivial "fundamental group." But in this case, things are more subtle.

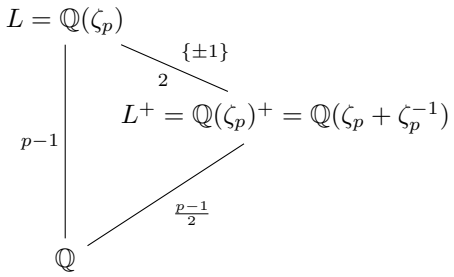
Example 19.1. Consider α be the root of $X^5 - X + 1$ and let $K = \mathbb{Q}[\alpha]$. Because $\operatorname{disc}\mathbb{Z}[\alpha] = 5356$ is squarefree, it is the ring of integers. The Minkowski bound tells us that to find $H(K)$ we need only look at primes P with $\|P\| < 4$. But there are no prime ideals with norm 2 or 3, because the polynomial $X^5 - X + 1$ has no root in $\mathbb{F}_2$ and $\mathbb{F}_3$. Therefore we conclude that A is an principal ideal domain.

Now let us look at the Galois closure L of K.



It can be checked that L over $\mathbb{Q}[\sqrt{19 \cdot 151}]$ is unramified.

Example 19.2. Let ζ_p be the pth root of unity. We have



This L^+ is totally real, i.e., has only real embeddings. By the Dirichlet unit theorem, the unit group $U(L^+)$ has rank $(p-1)/2 + 0 - 1 = (p-3)/2 = \rho$ and L also has rank $0 + (p-1)/2 - 1 = \rho$. Furthermore, because the roots of unity contained in both fields are $\{\pm 1\}$ and μ_p, we have

$$U(L^+) \cong \{\pm 1\} \times \mathbb{Z}^\rho \subsetneq \mu_p \times \mathbb{Z}^\rho \cong U(L).$$

For instance, the units of $\mathbb{Z}[\zeta_5]$ are just a root of unity times a unit of $\mathbb{Z}[(1+\sqrt{5})/2]$.

19.1 Counting ideals in ideal classes

Define

$$i(t) = \big|\{\text{ideals } I \text{ in } A \text{ with } \|I\| \le t\}\big|$$

and for an ideal class $C \in H(K)$, define

$$i_C(t) = \big|\{\text{ideals } I \text{ in } A \text{ with } \|I\| \le t \text{ representing } C\}\big|.$$

Clearly we have

$$i(t) = \sum_{C \in H(K)} i_C(t).$$

Theorem 19.3 (Equidistribution theorem)**.**

$$\frac{i_C(t)}{t} = \kappa_K + O(t^{-n^{-1}}),$$

where κ_K only depends on K and not on C.

If K is real and quadratic, then

$$\kappa = \frac{2 \log u}{\sqrt{|\Delta|}}.$$

Also, we have a corollary $i(t) = h\kappa t + O(t^{1-n^{-1}})$.

First fix $C \in H(K)$ and an ideal J representing the inverse class $C^{-1} \in H(K)$. Then for any $I \in C$, the product IJ is principal and hence there is a number α_I for which

$$I \cdot J = (\alpha_I).$$

This α_I is well-defined only up to multiplication by $U = A^*$. The coset $U \cdot \alpha_I$ is really well-defined. Since

$$\|I \cdot J\| = \|I\| \cdot \|J\| = \|(\alpha_I)\| = |N_{K/\mathbb{Q}}\alpha_I|,$$

there is a correspondence

$$\left\{\begin{matrix}\text{ideals } I \in C \\ \text{with } \|I\| \leq t\end{matrix}\right\} \quad \longleftrightarrow \quad \left\{\begin{matrix}U\alpha_I \subseteq J \text{ with} \\ |N_{K/\mathbb{Q}}(\alpha_I)| \leq t \cdot \|J\|\end{matrix}\right\}.$$

Let us look at the easy case $K = \mathbb{Q}(\sqrt{-D})$. Then $\Delta = -D, -4D$ and $w = |U| = 2, 4, 6$. Also, $\|(\alpha)\| = |\alpha|^2$. Because U is finite, we have a formula

$$i_C(t) = \frac{|\{\alpha \in J : |\alpha|^2 \leq t\|J\|\}}{w}.$$

This is couting the elements of the lattice $J \subset \mathbb{C}$ that is contained in the circle of radius $\sqrt{t\|J\|}$.

20 April 7, 2016

Let K be a extension of $\mathbb{Q}$ and let $H(K)$ be its ideal class group. Fix a class $C \in H(K)$, and define

$$i_C(t) = |\{I \text{ representing } C : \|I\| \le t\}|.$$

20.1 Equidistribution of ideals in ideal classes

Theorem 20.1.

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

Fix an ideal J representing C^{-1}. Then for any I, there exists an α_I such that $IJ = (\alpha_I)$. Then

$$|N_{K/\mathbb{Q}}| = \|(\alpha_I)\| = \|I\|\|J\|.$$

That is, there is a bijection

$$\{I : I \in C, \|I\| \le t\} \quad \longleftrightarrow \quad \{U\alpha_I \subset J : |N_{K/\mathbb{Q}}\alpha_I| \le t\|J\|\}$$

where U is the unit group. If we decompose U as $U = W \times V$ where W is a finite cyclic group and V is a free abelian group of rank $r + s - 1$, then we can even write

$$\begin{aligned} |\{I : I \in C, \|I\| \le t\}| &= |\{U\alpha_I \subset J : |N_{K/\mathbb{Q}}\alpha_I| \le t\|J\|\}| \\ &= \frac{|\{V\alpha_I \subset J : |N_{K/\mathbb{Q}}\alpha_I| \le t\|J\|\}|}{|W|}. \end{aligned}$$

Let us look at the special case $K = \mathbb{Q}(-\sqrt{D})$ where D is squarefree and is positive. Our problem is to count $\alpha \in J$ such that $|\alpha|^2 | t\|J\|$. That is, we need to compute

$$i_C(t) = |\{\alpha \in J : |\alpha|^2 \le t\|J\|\}|.$$

In a more general context, for any lattice $\Lambda \subset \mathbb{C}$ let us count the lattice point in the circle of radius ρ. If we denote the fundamental parallelogram by

$$F = \{t_1\lambda_1 + t_2\lambda_2 : 0 \le t_i < 1\},$$

where λ_1, λ_2 is the basis, we can tile the whole plane by translates of F as $\coprod_{\lambda\in\Lambda}(F + \lambda)$. Let

$$\begin{aligned} n(\rho) &= \#\text{lattice-points in this circle,} \\ n^-(\rho) &= \#\text{translates } F + \lambda \text{ contained in this circle.} \\ n^+(\rho) &= \#\text{translates } F + \lambda \text{ that meet the circle.} \end{aligned}$$

Clearly $n^-(\rho) \le n(\rho) \le n^+(\rho)$ and $n^-(\rho)\operatorname{vol}(F) \le \pi\rho^2 \le n^+(\rho)\operatorname{vol}(F)$. Moreover, $n^+(\rho) - n^-(\rho)$ is the number of $F + \lambda$ that intersect the boundary of the

circle, and thus is contained in some "shell" around the boundary. If we denote by δ the longest diagonal of F, we see that

$$(n^+(\rho) - n^-(\rho)) \operatorname{vol}(F) \leq \pi(\rho+\delta)^2 - \pi(\rho-\delta)^2.$$

It follows that

$$|n(\rho)\operatorname{vol}(F) - \pi\rho^2| \leq C\rho = O(\rho), \quad n(\rho) = \frac{\pi\rho^2}{\operatorname{vol}(F)} + O(\rho).$$

In out case, $\rho = \sqrt{t\|J\|}$ and $\operatorname{vol}(F) = \frac{1}{2}\sqrt{\Delta}\|J\|$. When we plug this in, we get

$$i_C(t) = \frac{2\pi}{|W|\sqrt{|\Delta|}}t + O(t^{1/2}).$$

That is, $\kappa = 2\pi/|W|\sqrt{|\Delta|}$ is independent of C. We have not used anything about the ideal class group but somehow still have derived this result!

Let us do some proof analysis. How much information about the geometry of the circle do we need? If we have any region (closure of an open set) B and a lattice Λ, then

$$|\Lambda \cap tB| \leq \frac{\operatorname{vol}(tB)}{\operatorname{vol}(\mathbb{R}^n/\Lambda)} + \epsilon(t)$$

by the same shell technique.

20.2 The Chebotarev density theorem

This was my presentation. See appendix.

21 April 12, 2016

Let $A \subset K$ be the ring of integers, and let C be an ideal class in the ideal class group $H(K)$. Pick J be an ideal in the ideal class C^{-1}. Then for all I there is an α_I such that $IJ = \alpha_I U$, where U is the unit group. The Dirichlet unit theorem states that $U = W \times V$ where V is the free abelian group generated by $\{u_1, \dots, u_{r+s-1}\}$ and W is a finite cyclic group with $w = |W|$. We then know that

$$\begin{aligned} i_C(t) &= |\{I \in C : \|I\| \le t\}| \\ &= |\{(\alpha_I) : \alpha_I \in J \text{ and } \|(\alpha_I)\| \le t\|J\|\}| \\ &= |\{\alpha U : \alpha \in J \text{ and } |N(\alpha)| \le t\|J\|\}| \\ &= \frac{1}{w}|\{\alpha V : \alpha \in J \text{ and } |N(\alpha)| \le t\|J\|\}|. \end{aligned}$$

21.1 Distribution of ideals in the class group

We also have the following diagram.

$$\begin{array}{ccccccccc} & & V & \hookrightarrow & (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s & & & & \\ & & \downarrow{\scriptstyle \log} & & \downarrow{\scriptstyle \log} & & & & \\ 0 & \longrightarrow & H & \longrightarrow & \mathbb{R}^{r+s} & \longrightarrow & \mathbb{R} & \longrightarrow & 0 \end{array}$$

So far, everything is pretty much canonical, but we will now make a choice and construct a splitting of the exact sequence on the bottom row. Let

$$\mathbb{R}^{r+s} = H \times \mathbb{R}.$$

Since translates of the fundamental parallelotope tile H, we see that

$$\mathbb{R}^{r+s} = \coprod_{\lambda \in \Lambda_V} (F_V \times \mathbb{R} + \lambda).$$

Define $B = \log^{-1}(F_V \times \mathbb{R})$. Then it follows that

$$(\mathbb{R}^*)^r \times (\mathbb{C}^*)^s = \amalg_{u \in V} uB.$$

Now this relevant to our discussion on $i_C(t)$. If we denote $B(t) = \{x \in B : |N(x)| \le T\}$, we have

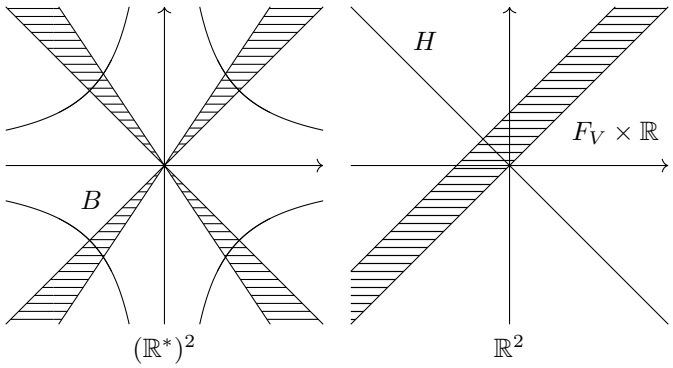
$$\begin{aligned} i_C(t) &= \frac{1}{w}|\{\alpha V : \alpha \in J, |N(\alpha)| \le T = t\|J\|\}| \\ &= \frac{1}{w}|\{\alpha \in B : \alpha \in J, |N(\alpha)| \le T\}| \\ &= \frac{1}{w}|B(T) \cap J|. \end{aligned}$$

Here, $B(T) = t^{1/n}B(1)$.

Let us look at the case of the real quadratic field K. In this case, $r = 2$ and $s = 0$, so the logarithm map is like $\log : (\mathbb{R}^*)^2 \to \mathbb{R}^2$ given by

$$(u, u') \mapsto (\log|u|, \log|u'|).$$

Then we have the following pictures.



We have the general lemma:

Lemma 21.1. *If $\Lambda \subset \mathbb{R}^n$ is a lattice and D is a "nice" region, then*

$$|\Lambda \cap tD| = \frac{\mathrm{vol}(D)}{\mathrm{vol}(\mathbb{R}^n/\Lambda)}t^n + O(t^{n-1}).$$

Applying to our case, we get

$$|J \cap B(T)| = \frac{\mathrm{vol}(B(\|J\|))}{\mathrm{vol}(\mathbb{R}^n/J)}t + O(t^{1-n^{-1}}) = \frac{\mathrm{vol}(B(1))}{\mathrm{vol}(\mathbb{R}^n/A)}t + O(t^{1-n^{-1}}).$$

Because we know that $\mathrm{vol}(\mathbb{R}/A) = 2^{-s}\sqrt{|\Delta|}$, we finally get

$$i_C(t) = 2^s\frac{\mathrm{vol}(B(1))}{\sqrt{|\Delta|}w}t + O(t^{1-n^{-1}}).$$

In the real quadratic case, the volume of the curved triangle can be computed easily.

21.2 The regulator

We define the regulator as a generalization of $\log u$. Let $u_1, \ldots, u_{r+s-1}$ be the basis for V. We are going to look at the matrix with rows

$$\begin{pmatrix}\log|\sigma_1(u_k)| & \cdots & \log|\sigma_r(u_k)| & 2\log|\tau_1(u_k)| & \cdots & 2\log|\tau_s(u_k)|\end{pmatrix}.$$

This is an $m \times (m-1)$ matrix, but all the row-sums are 0.

We are now going to build a determinant out of this. Let that matrix be M, and let us augment this by adding a last row $a = (a_1, \ldots, a_m)$ and make it into $\tilde{M} = M(a)$. Because all the row-sums are 0, if $\sum a_i = 0$ then $\det M(a) = 0$. That is, M as a linear functional is a constant times $\sum a_i$.

Definition 21.2. We define the **regulator** of K as

$$\mathrm{Reg}(K) = R(K) = \det M(a)$$

for any a with $\sum a_i = 1$.

22 April 14, 2016

Let K be a number field with degree $[K:\mathbb{Q}] = d$. For any class C, we have

$$\begin{aligned} i_C(t) = |\{I \in C : \|I\| \le t\}| &= \frac{\operatorname{vol}(B(\|J\|))}{\operatorname{vol}(\mathbb{R}^d/J)w} t + O(t^{1-1/d}) \\ &= \frac{2^s \operatorname{vol}(B(1))}{\sqrt{|\Delta|}w} t + O(t^{1-1/d}), \end{aligned}$$

where $B(T) = \{x \in B : |Nx| \le T\}$. We have defined something called a regulator, and in fact, there is the following proposition.

Proposition 22.1. $\operatorname{vol}(B(1)) = 2^r \cdot \pi^s \cdot \operatorname{Reg}(K)$.

We shall not prove this, but you should read the proof in Marcus.

There is a relation between the regulator and the class number.

Theorem 22.2 (Brouer-Siegel theorem)**.** *Let $K_1, K_2, \dots$ be a sequence of Galois extensions of $\mathbb{Q}$. Let $n_i = [K_i : \mathbb{Q}]$, $h_i = |H(K_i)|$, $R_i = \operatorname{Reg}(K_i)$, $\Delta_i = |\operatorname{disc}(K_i)|$. If $n_i/\log|\Delta_i| \to 0$ as $i \to \infty$, then*

$$\lim_{i\to\infty} \frac{\log(h_i R_i)}{\log\sqrt{|\Delta_i|}} = 1.$$

That is, the product hR is "going to be" more regular than h or R separately.

As a related topic, there is the Gauss class number problem. There is a beautiful expository paper written by D. Goldfeld, *Gauss' Class Number Problem and Imaginary Quadratic Fields*, BAMS (1985). It will be totally accessible to you, and it gives the effective estimate $h(D) > c(\log|\Delta|)^{1-\epsilon}$ for every $\epsilon > 0$ and some $c = c_\epsilon$.

22.1 Dirichlet Series

Let us now move on to the next topic. Consider the series

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

for a complex $s = x+iy$. We have to check whether the series converge absolutely and uniformly on some compact set.

Lemma 22.3. *Let $A_n = a_1 + \cdots + a_n$. If $A_n = O(n^r)$ for some $r \ge 0$, then $D(s)$ converges for $\Re(s) = x > r$.*

Proof. We have

$$\begin{aligned} \sum_{n=m}^{M} \frac{a_n}{n^s} &= \sum_{n=m}^{M} \frac{A_n}{n^s} - \sum_{n=m}^{M} \frac{A_{n-1}}{n^s} \\ &= \frac{A_M}{M^s} - \frac{A_{m-1}}{m^s} + \sum_{n=m}^{M-1} A_n\Big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big). \end{aligned}$$

Because

$$\Big|\Big(\frac{1}{n^s}-\frac{1}{(n+1)^s}\Big)\Big| = \Big|\int_{t=n}^{n+1}\frac{sdt}{t^{s+1}}\Big| \le |s|\Big|\int_{n}^{n+1}\frac{At}{t^{x+1}}\Big| \le |s|n^{-(x+1)},$$

we have the estimate

$$\begin{aligned}\sum_{n=m}^{M}\frac{a_n}{n^3} &= \frac{A_M}{M^s}-\frac{A_{M-1}}{m^s}+\sum_{n=m}^{M-1}A_n\Big(\frac{1}{n^s}-\frac{1}{(n+1)^s}\Big)\\ &\le B\bigg(\frac{M^r}{M^x}+\frac{m^r}{m^x}+|s|\sum_{n=m}^{M}n^{r-x-1}\bigg).\end{aligned}$$

It follows that the sum converges absolutely. □

We can now define the functinos we are really intereseted in.

Definition 22.4. Let $K/\mathbb{Q}$ be a finite extension. We define the **Dedekind zeta function** as

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

where $j_n = \{I \subset A : \|I\| = n\}$.

22.2 Minkowski's theorem[7]

Minkowski's theorem was proved by 1889 and was used to prove Lagrange's Square theorem. The statement is as follows:

Theorem 22.5. *Let $\Omega \subset \mathbb{R}^N$ be a convex, centrally symmetric body with volume $\mathrm{vol}(\Omega) > 2^N$. Then Ω contains a non-zero lattice point.*

Proof. We can write the volume condition as $\mathrm{vol}(\frac{1}{2}\Omega) > 1$. Then there exist two points $P, Q \in \frac{1}{2}\Omega$ whose difference has integer coordinates. It follows that $P - Q = \frac{1}{2}(2P + (-2Q))$ is in Ω. □

[7]This was a presentation by Salash Nabaala.

23 April 19, 2016

Recall that we defined the **Dirichlet series** as a series of the form

$$D(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

for $s \in \mathbb{C}$, and we have shown the following lemma.

Lemma 23.1. *If $a_1 + \cdots + a_n = O(n^r)$, then $D(s)$ converges uniformly in a compact subset of the half-plane $\Re(s) > r$.*

We have also defined the Dedekind zeta function for a given number field K as

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

where $j_n = |\{I \subset A : \|I\| = n\}|$ is the number of ideals with norm exactly n. We already have an estimate of the number of ideals with norm at most t:

$$i(t) = \sum_{k \le t} j_k = h_K \cdot \kappa \cdot t + O(t^{1-1/n}).$$

Then $A_n = O(n)$ and hence we have the following.

Proposition 23.2. *The Dedekind zeta function $\zeta_K(s)$ converges (absolutely, uniformly in a compact subset of) in the half-plane $\Re(s) > 1$.*

23.1 The L-function

We can also define the partial Dedekind zeta function. Fix a $C \in H(K)$ and define $j_{n,C} = |\{I \in C : \|I\| = n\}|$. Let

$$\zeta_{K,C}(s) = \sum_{n=1}^{\infty} \frac{j_{n,C}}{n^s}.$$

Then by the equidistribution theorem, we again have the same result for $\zeta_{K,C}(s)$.

Now consider a **character**, i.e., a group homomorphism

$$\chi : H(K) \to \mathbb{C}^*.$$

We are going to "weight" the partial Dedekind zeta functions by this character and define the **L-function**

$$L(K, \chi; s) = \sum_{C \in H(K)} \chi(c)\zeta_{K,C}(s) = \sum_{n=1}^{\infty} \frac{\sum_{C \in H(K)} \chi(C) j_{n,C}}{n^s}.$$

Let us check where this converges. By the equidistribution theorem,

$$a_1 + \cdots + a_n = \sum_{k \le n} j_{k,\chi} = \sum_{C \in H(K)} \chi(C) i_C(n) = \left(\sum_{C \in H(K)} \chi(C) \right) \kappa t + O(t^{1-1/n}).$$

But the sum of the character is 0 unless χ is the trivial character $\mathbf{1}$.[8] So if χ is trivial, we retrieve

$$L(K, \mathbf{1}; s) = \zeta_K(s)$$

and if χ is nontrivial, then $L(K, \chi; s)$ converge for $\Re(s) > 1 - 1/n$. In particular, it converges in a neighborhood of $s = 1$.

As a general remark, the **Riemann zeta function** is the case $K = \mathbb{Q}$ and is simply $\zeta(s) = \zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} 1/n^s$. This actually extends to be a holomorphic function on $\mathbb{C} \setminus \{1\}$ and is meromorphic at $s = 1$ with a simple pole. That is, $(s-1)\zeta(s)$ is holomorphic everywhere.

23.2 Extending the zeta function

Going back to our discussion on the Dirichlet zeta function, we want to extend the range of convergence of the Dirichlet zeta function. We first look at the Riemann zeta function $\zeta(s)$. Let us consider the analytic function

$$\epsilon_a(s) = 1 - a^{1-s} = 1 - e^{(\log a)(1-s)}.$$

The zeros are the number of the form $s_k = 1 + 2\pi i k / \log a$, where $k \in \mathbb{Z}$. Note that if p and q are distinct primes, then $\epsilon_p(s)$ and $\epsilon_q(s)$ have exactly one common zero, namely $s = 1$. We are going to look at the "p-deprived" Riemann zeta function

$$\zeta^{(p)}(s) = (1 - p^{1-s})\zeta(s) = (1 - p^{1-s}) \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{c_{p,n}}{n^s},$$

where $c_{p,n} = 1$ if $p \nmid n$ and $c_{p,n} = 1 - p$. The interesting fact is that in this case, $a_1 + \cdots + a_n = O(n^0)$! It follows that $(1 - p^{1-s})\zeta(s)$ is convergent on (uniformly on a compact subset of) the domain $\Re(s) > 0$. That is, $\zeta(s)$ is at least meromorphic for $\Re(s) > 0$ and has poles possibly at the zeros of $\epsilon_p(s) = 1 - p^{1-s}$. The only common pole is placed at $s = 1$, and hence we have the following proposition.

Proposition 23.3. *The Riemann zeta function $\zeta(s)$ extends to a meromorphic function on the half-plane $\Re(s) > 0$ and as a simple pole at $s = 1$.*

Using this fact, we can extend the Dedekind zeta function to a larger domain.

Theorem 23.4. *The Dedekind zeta function $\zeta_K(s)$ extends to the half-plane $\Re(s) > 1 - 1/n$ and has a simple pole at $s = 1$.*

[8] Let G be any finite group and let $\chi : G \to \mathbb{C}^*$ be a character. If χ is nontrivial, i.e., there exists a g_0 with $\chi(g_0) \neq 1$, then $\sum \chi(g) = \sum \chi(g_0 g) = \chi(g_0) \sum \chi(g)$ and hence the sum must be zero.

Proof. Let us consider a single ideal class C. We have

$$\zeta_{K,C}(s) = \sum_{n=1}^{\infty} \frac{j_{n,C}}{n^s} = \sum_{n=1}^{\partial} \frac{j_{n,C}}{\kappa} + \kappa \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The first sum converges on $\Re(s) > 1 - 1/[K : \mathbb{Q}]$, because $j_{1,C} + \cdots + j_{n,C} = O(n^{1-1/[K:\mathbb{Q}]})$. The second some, as we have shown above, can be extended to $\Re(s) > 0$ with a pole at $s = 1$. Therefore, $\zeta_{K,C}(s)$ can be extended to a meromorphic function on $\Re(s) > 1 - 1/[K : \mathbb{Q}]$ with a simple pole at $s = 1$. Then we can add all these up to see that $\zeta_K(s)$ can be extended to $\Re(s) > 1 - 1/[K : \mathbb{Q}]$. □

24 April 21, 2016

If you remember, we used $1 - a^{1-s} = f_a(s)$ as a tool to extend analyticity. We estimate

$$\begin{aligned} f_a(s) &= 1 - \exp((\log a)(1-s)) = 1 - 1 - (\log a)(1-s)(1 + O(1-s)) \\ &= (1-s) \cdot (c + O(1-s)). \end{aligned}$$

Then $f_p(s)\zeta(s)$ is defined analytically near $s = 1$. It follows that $\zeta(s) \cdot (s-1)$ is analytic near $s = 1$ and is nonzero at $s = 1$. Using this we showed that $\zeta_{K,C}$ extends to a meromorphic function at $\Re(s) > 1 - 1/[K : \mathbb{Q}]$ with a simple pole at $s = 1$. We simply collected a κ from all the terms and made

$$\sum_{n=1}^{\infty} \frac{j_{n,C}}{n^s} = \sum_{n=1}^{\infty} \frac{j_{n,C} - \kappa}{n^s} + \kappa\zeta(s).$$

Then the partial sums are $O(n^{1-1/[K:\mathbb{Q}]})$.

24.1 Infinite products

We want to change the zeta functions into infinite products like

$$\prod_{i=1}^{m} (1 - a_i)^{-1} = \sum_{(r_1,\dots,r_j)} \prod_{i=1}^{m} a_i^{r_i}.$$

But we need to make sure the infinite product as m goes to ∞ makes sense.

To achieve this, assume that $|a_i| < 1$ and $\sum_{i=1}^{\infty} |a_i| < \infty$. We want to first make sure that $\prod_{i=1}^{\infty}(1 - a_i)^{-1}$ makes sense. In the case in which all a_i are positive reals, we can use the fact that

$$\frac{\log(1-x)}{x} \to 1$$

as $x \to 0$. Then the fact that $\sum |a_i|$ converges implies that the product converges. In the complex case, there is an issue of $\log z$ being defined only up to a integer multiple of $2\pi i$, but we can simply choose the one closest to 0 and do the same thing. Once we have that the sum of the logs converges, then we can exponentiate to get what we want.

So taking m to ∞, and using unique factorization, we can say the following.

Theorem 24.1. *If $\Re(s) > 1$, then*

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{\|P\|^s}\right)^{-1}.$$

If we can express $\zeta_K(s)$ as the infinite product like the above, then how can $\zeta_{K,C}(s)$ be expressed? If we simply take the product over primes in C, then

$$\prod_{P \in C} \left(1 - \frac{1}{\|P\|^s}\right)^{-1} = \sum_{I \text{ divisible only by } P \in C} \frac{1}{\|I\|^s},$$

which is not really satisfactory. Instead, if we look at the L-function,

$$L(K, \chi, s) = \prod_P \Big(1 - \frac{\chi(P)}{\|P\|^s}\Big)^{-1}$$

because $\chi(\prod P_i) = \prod \chi(P_i)$.

24.2 Density of primes

Generally, let Π be the set of all primes, and let $\mathcal{P}$ be any subset of Π. Our goal is to measure how "large" is $\mathcal{P}$ compared to Π.

1. Natural density:
   We define
   $$\delta_{\text{natural}} = \lim_{X \to \infty} \frac{|\{P \in \mathcal{P} : \|P\| \le X\}|}{|\{P \in \Pi : \|P\| \le X\}|}.$$
   This is the only density that really speaks to you. But this is very hard to show that the natural density exists. So we sometimes use other "smoother" densities.

2. Polar density:
   We first define a zeta function
   $$\zeta_{K,\mathcal{P}}(s) = \prod_{P \in \mathcal{P}} \Big(1 - \frac{1}{\|P\|^s}\Big)^{-1}.$$
   We say that $\mathcal{P}$ has polar density m/n if $\zeta^{K,\mathcal{P}}(s)^n$ extends to a meromorphic function about $s = 1$ and has a pole of order m at $s = 1$.

24.3 Odlyzko's bound

Let r_1 and r_2 be r and s in the usual class notation. (We need to reserve s for the complex variable.) The Minkowski bound says that

$$\log|D_k| \ge (2 - o(1))n - 2(\log(4/\pi))r_2.$$

We've only extended the zeta function to $\Re(s) > 1-\epsilon$, but we have the functional equation

$$\begin{aligned}\Lambda_K(s) &= \left(\frac{\sqrt{|D_K|}}{2^{r_2}\pi^{n/2}}\right)^s \Gamma\Big(\frac{s}{2}\Big)^{r_1} \Gamma(s)^{r_2} \zeta_K(s) \\ &= \left(\frac{\sqrt{|D_K|}}{2^{r_2}\pi^{n/2}}\right)^{1-s} \Gamma\Big(\frac{1-s}{2}\Big) \Gamma(1-s)^{r_2} \zeta_K(1-s).\end{aligned}$$

If we define $\Lambda_K^*(s) = s(s-1)\Lambda_K(s)$, there is a Hadamard product formula

$$\Lambda_K^*(s) = e^{a+bs} \prod_\rho \Big(1 - \frac{s}{\rho}\Big) e^{s/\rho},$$

where we take the product over the nontrivial zeros ρ.

Now when you take the log of the Hadamard product formula and take the derivative and do some stuff, you get

$$\log|D_K| = r_1\Big(\log\pi - \frac{\Gamma'}{\Gamma}\Big(\frac{s}{2}\Big)\Big) + 2r_2(\log 2\pi - \frac{\Gamma'}{\Gamma}(s)\Big) - \frac{2}{s-1} - \frac{2}{s} - 2\frac{\zeta_K'}{\zeta_K}(s) + 2\sum_\rho \Re\frac{1}{(s-\rho)}.$$

for $s \in \mathbb{R}$ and is greater than 1. (This formula is due to Artin.)

We need a lemma:

Lemma 24.2. *The inequality*

$$\frac{\partial^m}{\partial s^m}\Big(-\frac{\zeta_K'}{\zeta_K}\Big)(s) > 0$$

holds if and only if m is even.

If we take the mth derivative with respect to s, then we get

$$\delta_m \log|D_K| > (-1)^m\Big[r_1\frac{\partial^m}{\partial s^m}\Big(\log\pi - \frac{\Gamma'}{\Gamma}(x/2) + r_2\frac{\partial^m}{\partial m^s}\Big(\log 2\pi - \frac{\Gamma'}{\Gamma}(s)\Big] + m!,$$

where δ_m is 1 if $m = 0$ and 0 otherwise. Plugging some appropriate values in, we get

$$|D_k|^{1/n} > (22.38)^{r_1/n}(11.9)^{2r_2/n}.$$

If you do some more work, you get

$$|D_k|^{1/n} > (215)^{r_1/n}(44.7)^{2r_2/n},$$

and this is Odlyzko's bound.

25 April 26, 2016

We have the curious lemma that says if $\sum |a_i| < \infty$ and $|a_i| < 1$ then $\prod (1-a_i)^{-1}$ converges. Using this, we established the infinite product structure

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{\|P\|^s}\right)^{-1} = \sum_I \frac{1}{\|I\|^s}$$

of the zeta function.

Let S be a finite set of primes of K. Let us define

$$\zeta_K^{\{S\}} = \prod_{P \notin S} \left(1 - \frac{1}{\|P\|^s}\right)^{-1}.$$

Then this can be written as a product of a harmless function and $\zeta_K^{\{S\}}$ as

$$\zeta_K^{\{S\}}(s) = \prod_{P \in S} \left(1 - \frac{1}{\|P\|^s}\right) \zeta_K^{\{S\}}(s).$$

Then because ζ_K is meromorphic on $\Re(s) > 1 - 1/n$ with a simple pole at $s = 1$, the new $\zeta_K^{\{S\}}$ also has the same behavior.

25.1 Polar density

Let $\mathcal{P}$ be a set of primes of K. We are going the define a notion of some density of $\mathcal{P}$ in the set of all primes of K. Let us define

$$\zeta_{K,\mathcal{P}}(s) = \prod_{P \in \mathcal{P}} \left(1 - \frac{1}{\|P\|^s}\right)^{-1}.$$

We would like the have an "analytic" extension to a neighborhood of $s = 1$.

Definition 25.1. If $(\zeta_{K,\mathcal{P}}(s))^n$ can be extended to a neighborhood of $s = 1$ and has a pole of order m at $s = 1$, then we say

$$\delta_{\text{polar}}(\mathcal{P}) = \frac{m}{n}.$$

This is the same as saying that $(s-1)^m f(s)^n$ can be extended to an analytic function around 1 with nonzero at $s = 1$. The density is well-defined, because $(s-1)^{m\lambda} f(s)^{n\lambda} = ((s-1)^m f(s)^n)^\lambda$. Also, with the same type of argument, you can check that if $\mathcal{P}_1$ and $\mathcal{P}_2$ are disjoint, then

$$\delta_{\text{polar}}(\mathcal{P}_1 \cup \mathcal{P}_2) = \delta_{\text{polar}}(\mathcal{P}_1) + \delta_{\text{polar}}(\mathcal{P}_2),$$

assuming that two of them exist.

We also note that (this is in one of the problem set) if $\mathcal{P}$ has a polar density, then the Dirichlet density

$$\delta_{\text{Dir}}(\mathcal{P}) = \lim_{s \to 1+} \frac{\sum_{P \in \mathcal{P}} \|P\|^{-s}}{\sum_P \|P\|^{-s}}$$

exists and is equal to the polar density.

25.2 A density theorem

Theorem 25.2. *Let L/K be a Galois extension, and let $\mathcal{P}$ the set of primes of K that split completely in L. Then $\mathcal{P}$ has a polar density, and it is equal to $1/[L:K]$.*

Corollary 25.3. *Any L/K has the property that infinitely many primes of K split completely in L.*

Proof. Let M be the Galois closure of L/K. Then a prime P of K splits completely in F if and only if it splits completely in L. The corollary follows. □

Example 25.4. Any cubic (non Galois) extension of $\mathbb{Q}$ has one sixth of the set of rational primes completely splitting in it.

Because there are only finitely many primes that ramify and we don't want to see them, we let

$$\zeta'_{K,\mathcal{P}}(s) = \prod_{\substack{P\in\mathcal{P},\\ P \text{ unramified}}} \left(1 - \frac{1}{\|P\|^s}\right)^{-1}.$$

Let $\mathcal{R}$ be any set of primes of L that contain all primes that split completely over $\mathbb{Q}$. Then

$$\zeta'_{L,\mathcal{R}}(s) \cdot D(s) = \zeta'_L(s)$$

where

$$D(s) = \prod_{P\notin\mathcal{R},\text{unramified}} \left(1 - \frac{1}{\|P\|^s}\right)^{-1}.$$

Because all such P will have norm $\|P\| = p^e$ for $e > 1$, we see that $D(s)$ can be extended to an analytic function around $s = 1$.

Now let $\mathcal{Q}$ be the set of primes of L that have split completely in L/K and let $\mathcal{P}$ be the set of primes of K that split completely in L. Then there is a $[L:K]$-to-1 surjection

$$\mathcal{Q} \to \mathcal{P},$$

and if Q lies over P then $\|Q\| = \|P\|$. It follows that

$$\zeta_{L,\mathcal{Q}}(s) = \zeta_{K,\mathcal{P}}(s)^{[L:K]}.$$

This is true for $\Re s > 1$, so if we extend it to a neighborhood of $s = 1$ they will also agree. Hence we get the theorem.

25.3 Cyclotomic units[9]

Let ζ_n be a nth root of unity, and let K^* denote the units of $\mathbb{A} \cap K$ and K^+ denote the maximal real subfield.

[9]This was a presentation by David Mende.

Definition 25.5. Let V_n be the multiplicative group generated by

$$\{\pm\zeta_n\} \cup \{1-\zeta_n^a : 1 \le a < n\}.$$

Then define $C_n = V_n \cap \mathbb{Q}[\zeta_n]^*$ and in general, for any $K \subset \mathbb{Q}[\zeta_n]$, define $C_K = C_n \cap K^*$.

Our goal is to show that $[\mathbb{Q}(\zeta_n)^* : C_n]$ is finite. We first do it for $n = p^m$.

Proposition 25.6. *The set* $\{-1, \xi_a\}$ *generate* $C^+_{\mathbb{Q}(\zeta_n)}$*, where*

$$\xi_a = \zeta^{(1-a)/2}\frac{1-\zeta^a}{1-\zeta} = \pm\frac{\sin(\pi a/p^m)}{\sin(\pi/p^m)}$$

for $\gcd(a,p) = 1$ *and* $1 < a < p^m/2$.

Sketch of proof. A general element of V_{p^m} will have the form

$$\xi = \pm\zeta^d \prod_{\substack{1\le a<p^m/2\\ \gcd(a,p)=1}} (1-\zeta^a)^{c_a}.$$

Using some facts, we see that $\sum c_a = 0$. Then

$$\xi = \pm\zeta^e \prod \left(\frac{1-\zeta^a}{1-\zeta}\right)^{c_a} = \pm\zeta^e \prod \xi_a^{c_a}.$$

Because $\xi \in C^+_{\mathbb{Q}(\zeta_n)}$ must be real, we see that ξ is generated by ξ_as and -1. □

To show that the set $\{\xi_a\}$ actually generate $C_{\mathbb{Q}(\zeta)^+}$, we compute the regulator of $\{\xi_a\}$. It is

$$\begin{aligned}\operatorname{Reg}(\{\xi_a\}) &= \pm\det(\log|\xi_a^+|) = \prod \sum_{1\le a<p^m/2} \chi(a)\log|1-\zeta^a| \\ &= \prod -\tau(\chi)L(1,\chi)/2 \neq 0.\end{aligned}$$

A The Chebotarev density theorem

A.1 The Frobenius element

Let L/K be a Galois extension, and let $\mathfrak{P}$ be a prime lying over $\mathfrak{p}$. Recall that the decomposition and interia groups associated to $\mathfrak{P}$ are defined as thus:

$$D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma\mathfrak{P} = \mathfrak{P}\},$$
$$I(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma\alpha \equiv \alpha \pmod{\mathfrak{P}} \text{ for all } \alpha \in \mathcal{O}_L\}.$$

We have a tower of extensions.

$$\begin{array}{ccccc}
L & \longleftarrow & \mathcal{O}_L & \longleftarrow & \mathfrak{P} \\
{\scriptstyle e}\big| & & \big| & & \big|{\scriptstyle \text{total ram., no res.}} \\
L^I & \longleftarrow & \mathcal{O}_{L^I} & \longleftarrow & \mathfrak{P}_I \\
{\scriptstyle f}\big| & & \big| & & \big|{\scriptstyle \text{no ram., total res.}} \\
L^D & \longleftarrow & \mathcal{O}_{L^D} & \longleftarrow & \mathfrak{P}_D \\
{\scriptstyle r}\big| & & \big| & & \big|{\scriptstyle \text{no ram., no res.}} \\
K & \longleftarrow & \mathcal{O}_K & \longleftarrow & \mathfrak{p}
\end{array}$$

If we assume that $\mathfrak{p}$ does not ramify, then in that case I is trivial and the map

$$D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$$

is an isomophism. The Galois group $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is generated by the Frobenius map $\alpha \mapsto \alpha^{\|\mathfrak{p}\|}$. Using the isomorphism, we can canonically define the Frobenius element $\phi(\mathfrak{P}|\mathfrak{p}) \in D(\mathfrak{P}|\mathfrak{p}) \subseteq \mathrm{Gal}(L/K)$ that corresponds to the Frobenius map on the residue fields. Since $\phi(\sigma\mathfrak{P}|\mathfrak{p}) = \sigma\phi(\mathfrak{P}|\mathfrak{p})\sigma^{-1}$ for any $\sigma \in \mathrm{Gal}(L/K)$, an unramified prime $\mathfrak{p}$ canonically gives a conjugacy class

$$\{\phi(\mathfrak{P}|\mathfrak{p})\}_{\text{conj.}} \in \mathrm{ConjClass}(\mathrm{Gal}(L/K))$$

of the Galois group. We shall denote this conjugacy class by $\mathrm{Frob}_{\mathfrak{p}}$.

A.2 The Chebotarev density theorem

The Chebotarive density theorem describes the distribution of primes with a given Frobineous element. Chebotarev proved the theroem in 1922, and the ideas used in the proof inspired Artin to prove his reciprocity theorem.

Before giving the statement of the theorem, we need a notion for measuring how many primes there are.

Definition A.1. Let M be a set of prime ideals of K. We define the **Dirichlet density** of M as

$$d(M) = \lim_{s \to 1+} \frac{\sum_{\mathfrak{p} \in M} \|\mathfrak{p}\|^{-s}}{\sum_{\mathfrak{p}} \|\mathfrak{p}\|^{-s}}$$

if the limit exists. Likewise, we define the **natural density** of M as

$$\delta(M) = \lim_{x \to \infty} \frac{\#\{\mathfrak{p} \in M : \|\mathfrak{p}\| \leq x\}}{\#\{\mathfrak{p} : \|\mathfrak{p}\| \leq x\}}.$$

If the natural density exists, then the Dirichlet density also exists and they are the same. However, the existence of the Dirichlet density does not imply the existence of the natural density.

Theorem A.2 (Chebotarev density theorem)**.** *Let L/K be a finite Galois extension between number fields and let C be a conjugacy class of* $\mathrm{Gal}(L/K)$*. Then*

$$d(\{\mathfrak{p} : \mathrm{Frob}_{\mathfrak{p}} = C\}) = \frac{|C|}{[L:K]}.$$

In fact, the natural density of the set also exists and is equal to $|C|/[L:K]$.

A.3 Consequences

There are direct corollaries to the theorem concerning the densities of certain classes of primes. Historically, the Dirichlet density theorem and the Frobenius density theorem was generalized by Chebotarev, but it is still worthwhile to see how Chebotarev's theorem implies the other ones.

Theorem A.3 (Dirichlet density theorem)**.** *Let $m \geq 2$ be an integer and a be relatively prime to m. Then the primes of the form $mk + a$ have Dirichlet density $1/\varphi(m)$.*

Proof. Consider the field $L = \mathbb{Q}[\zeta_m]$. Because this is the splitting field of $X^m - 1$, it is Galois, and its Galois group can be identified with $(\mathbb{Z}/m\mathbb{Z})^\times$ through the map $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q})$ given by

$$a \mapsto (\zeta_m \mapsto \zeta_m^a).$$

Consider a rational prime $p \in \mathbb{Z}$ that is unramified. Because $\mathrm{Gal}(L/\mathbb{Q})$ is abelian, all conjugacy classes have size 1. It follows that if $\mathrm{Frob}_p = \phi$ then

$$\phi(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}$$

for any $\alpha \in \mathcal{O}_L$ and all primes $\mathfrak{P}$ lying over p. Because $p\mathcal{O}_L$ is the product of all such $\mathfrak{P}$, we further have

$$\phi(\alpha) \equiv \alpha^p \pmod{p\mathcal{O}_L}.$$

We note the only automorphism given by $\zeta_m \mapsto \zeta_m^p$ onlysatisfies that criterion. Therefore $\mathrm{Frob}_p = \{p\} \subset (\mathbb{Z}/m\mathbb{Z})^\times$.

Applying the Chebotarev density theorem, we immediately get that the set of primes that are a modulo m has density $1/\varphi(m)$, because $[L:\mathbb{Q}] = \varphi(m)$. □

Consider a monic polynomial f with integer coefficients that does not have a double root. For each p, the reduced polynomial $\tilde{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ might or might not be reducible. If the factorization has polynomials of degree $n_1, \ldots, n_t$(where $n_1 + \cdots + n_t = n$), then say that p has **decompoisition type** $(n_1, \ldots, n_t)$.

Let L be the splitting field of f over $\mathbb{Q}$. Then L is Galois over $\mathbb{Q}$ and contains all the roots $\alpha_1, \ldots, \alpha_n$, where $\deg f = n$. Each element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$

permutes these roots and thus divides them into disjoint cycles. We say that $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ has **cyclic pattern** $(n_1, \ldots, n_t)$ if the action of σ on $\alpha_1, \ldots, \alpha_n$ is composed of cyclics of size $n_1, \ldots, n_t$.

Theorem A.4 (Frobenius density theorem)**.** *The density of the set of primes p for which f has a given decomposition type $(n_1, \ldots, n_t)$ exists, and is equal to $1/[L : \mathbb{Q}]$ times the number of $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ with cyclic pattern $(n_1, \ldots, n_t)$.*

Proof. Clearly the set

$$S_{(n_1,\ldots,n_t)} = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) : \sigma \text{ has cyclic pattern } (n_1, \ldots, n_t)\}$$

is stable under conjugation and hence is a disjoint union of conjugacy classes.

Consider a prime p with decomposition type $(n_1, \ldots, n_t)$. Because we are concerned with the density of primes, we may further assume that p does not divide the discriminant of f. It suffices to prove that the Frobenius element Frob_p consists of automorphisms of cyclic pattern $(n_1, \ldots, n_t)$. Then we would be able use the Chebotarev density theorem to conclude that the density of primes with decomposition type $(n_1, \ldots, n_t)$ is $|S_{(n_1,\ldots,n_t)}|/[L : \mathbb{Q}]$.

Let us look at one prime $\mathfrak{P}$ lying over p. Let $r_1, \ldots, r_d$ be the roots of f so that

$$f(X) = (X - r_1)(X - r_2) \cdots (X - r_d).$$

When we reduce it modulo $\mathfrak{P}$, we get

$$f(X) = (X - \tilde{r}_1)(X - \tilde{r}_2) \cdots (X - \tilde{r}_d) \in (\mathcal{O}_L/\mathfrak{P})[X]$$

where $\tilde{r}_i$ is the image of r_i under the projection map $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}$. It follows from the assumption that p does not divide $\operatorname{disc} f$ that all $\tilde{r}_i$ are distinct. (If $\tilde{r}_i = \tilde{r}_j$ then $r_i - r_j \in \mathfrak{P}$ and hence $\operatorname{disc} f \in \mathfrak{P}$.) Because the Galois group $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z}))$ is generated by σ, a polynomial in $(\mathcal{O}_L/\mathfrak{P})[X]$ is in $(\mathbb{Z}/p\mathbb{Z})[X]$ if and only if it is invariant under σ. If σ has a cyclic structure

$$\sigma : \tilde{r}_1 \mapsto \tilde{r}_2 \mapsto \cdots \mapsto \tilde{r}_n \mapsto \tilde{r}_1,$$

then

$$\sigma\left(\prod_{i=1}^{n}(X - \tilde{r}_i)\right) = \prod_{i=1}^{n}(X - \tilde{r}_{i+1}) = \prod_{i=1}^{n}(X - \tilde{r}_i)$$

and hence $(X - \tilde{r}_1) \cdots (X - \tilde{r}_n)$ is fixed under σ. However, every proper divisor of $(X - \tilde{r}_1) \cdots (X - \tilde{r}_n)$ that is not 1 is not fixed by σ. Therefore

$$(X - \tilde{r}_1) \cdots (X - \tilde{r}_n) \in (\mathbb{Z}/p\mathbb{Z})[X]$$

is irreducible. It follows that $f(X)$ factors modulo p exactly accoriding to the cyclic structure of σ. □

Index