Advanced Algebra I – Algebraic Number Theory, lecture 1

12. 10. 2017

Prof. Yichao Tian tian@math.uni-bonn.de EA60 4.028

Prob. sessions: Dr. Johannes Anschütz, ja@math.uni-bonn.de

Question. What kind of integers $n \geq 1$ can be represented as the sum of two squares? i.e. $n \in \mathbb{Z}_{\geq 1}$ $x^2+y^2 = n$.

From the algebraic point of view:

$R := \mathbb{Z} + \mathbb{Z}i \subseteq \mathbb{C}$ Gauss integers

$N: R \to \mathbb{Z}$ norm,

$\alpha = x+iy \mapsto x^2+y^2 = \alpha\bar{\alpha} = N(\alpha)$

Reformulation: which kind of integers n are in the image of N?

Lemma. (1) $N(\alpha) \geq 0$ $\alpha = 0 \iff N(\alpha) = 0$.

(2) $N(\alpha\beta) = N(\alpha)N(\beta)$

(3) Euclidean division: $\forall \alpha, \beta \in R$, $\alpha \neq 0$ $\exists \gamma, \delta \in R$:
$\beta = \alpha\gamma + \delta$ and $N(\delta) < N(\alpha)$

(4) $N(\alpha) = 1 \iff \alpha \in \{\pm 1, \pm i\}$.

PROOF: (1) is trivial

(2) is trivial

(3) $\mathbb{Q} + \mathbb{Q}i \ni \alpha^{-1}\beta = x + iy$ $y, x \in \mathbb{Q}$

Let $a, b \in \mathbb{Z}$ s.t. $|x-a| \leq \frac{1}{2}$, $|y-b| \leq \frac{1}{2}$

Put $\underbrace{\gamma = a+bi}_{\in R}$, $\eta = \alpha^{-1}\beta - \gamma = (x-a) + (y-b)i$

$\Rightarrow N(\eta) = (x-a)^2 + (y-b)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

$\beta = \alpha\gamma + \underbrace{\alpha\eta}_{\delta \in R}$ $N(\delta) = N(\alpha)N(\eta) < N(\alpha)$ □

Cor. R is a PID.

PROOF: Let $I \subseteq R$ be a nonzero ideal. Choose $\alpha \in I$ s.t. $N(\alpha) > 0$ and $N(\alpha)$ is minimal.

$\forall \beta \in I$ $\exists \gamma, \delta$: $\beta = \gamma\alpha + \delta$, $N(\delta) < N(\alpha)$ $\Rightarrow N(\delta) = 0$ by min. of α.

$\Rightarrow I = \alpha R$ □

Def. An element $\alpha \in R$ is primitive if it cannot be written as $\alpha = \beta\gamma$ with $\beta, \gamma \in R \setminus R^\times$

Easy: α is primitive $\iff (\alpha) \subseteq R$ is prime.

Theorem. (1) Every nonzero element in R can be written as a finite product of primitive elements, and this writing is unique up to units.

(2) Every nonzero ideal $I \subseteq R$ has a unique factorisation as

$$I = \prod_i \mathfrak{p}_i^{m_i} \quad \text{where } \mathfrak{p}_i \text{ is a prime ideal and } \mathfrak{p}_i \neq \mathfrak{p}_j \ (i \neq j).$$

PROOF: Same as always.

(1) $0 \neq \alpha \in R$. If α is primitive, we are done.

If α is not primitive $\Rightarrow \alpha = \beta_1 \cdot \beta_2$ with $N(\beta_1), N(\beta_2) > 1$

$\Leftrightarrow N(\beta_i) < N(\alpha)$. But norms are positive integers, so this process will terminate after finitely many steps:

$\alpha = \beta_1 \beta_2 \cdots \beta_k$ primitive elements.

Uniqueness: Assume $\alpha = \beta_1 \cdots \beta_k = \gamma_1 \cdots \gamma_\ell$ where β_i, γ_j are primitive.

$\beta_i \mid \gamma_1 \cdots \gamma_\ell$ (i.e. $\gamma_1 \cdots \gamma_\ell \in (\beta_i)$)

$\Rightarrow \beta_i \mid \gamma_j$ for some j because of primitiveness

Since γ_j is also primitive $\Rightarrow \beta_i = \gamma_j u$ for some $u \in R^\times$

$\Rightarrow$ induction.

(2) follows from the previous statement. □

Prime ideals in R:

Consider
$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & R \\ \cup & & \cup \\ \mathbb{Z} \cap \mathfrak{p} & \hookrightarrow & \mathfrak{p} \end{array}$$

$\mathbb{Z} \cap \mathfrak{p}$ is prime in $\mathbb{Z}$

- If $\mathbb{Z} \cap \mathfrak{p} = (0) \Rightarrow \mathfrak{p} = 0$
- If $\mathbb{Z} \cap \mathfrak{p} = (2) \Rightarrow 2R \subseteq \mathfrak{p}$

$$R/2R \longrightarrow R/\mathfrak{p}$$

$$R = \mathbb{Z}[x]/(x^2+1) \qquad R/2R \cong \mathbb{Z}[x]/(x^2+1, 2) = \mathbb{F}_2[x]/(x^2+1) = \mathbb{F}_2[x]/(x+1)^2$$

$\Rightarrow \mathfrak{p}$ has to be the preimage of $(1+x) \subseteq R/2R$ in R

$\Rightarrow \mathfrak{p} = (2, 1+i) = (1+i)$

$(1+i)^2 = 2i$

- If $\mathbb{Z} \cap \mathfrak{p} = (p)$ with $p \equiv 1 \ (4)$

$p \in \mathfrak{p}$ but p is not primitive because $R/pR \cong \mathbb{F}_p[x]/(x^2+1)$

but x^2+1 is reducible in $\mathbb{F}_p[x]$ if $p \equiv 1 \ (4)$

(This is because $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$ which is a multiple of 4.)

$\rightarrow$ $p = \alpha\beta$ with $1 < N(\alpha), N(\beta) < N(p) = p^2$

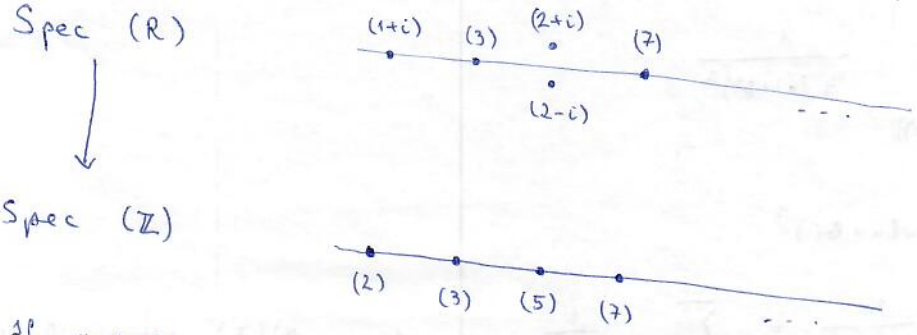
$\Rightarrow$ $\underbrace{N(\alpha)}_{\alpha\bar{\alpha}} = N(\beta) = p$ $\Rightarrow$ $\beta = \bar{\alpha}$ and both α and $\beta = \bar{\alpha}$ are primitive (there are no natural divisors of p)

- If $\mathbb{Z} \cap \mathfrak{p} = (p)$, $p \equiv 3 \ (4)$ $\rightarrow$ $\mathfrak{p} = (\alpha)$ or $(\bar{\alpha})$

p is primitive because $R/pR = \mathbb{F}_p[x]/(x^2+1)$ is a field because x^2+1 is irreducible over $\mathbb{F}_p$

$\Rightarrow$ $\mathfrak{p} = pR$.

So we have a classification of prime ideals of R:



Observation. If m and n are represented by the sum of two squares, so is mn.

This comes immediately from the multiplicativity of the norm.

Let us consider the case $n = p$ prime.

- $p = 2$ $\longrightarrow$ $N(1+i) = 2$
- $p \equiv 1 \ (4)$ $\longrightarrow$ $\exists \alpha \in R$ with $N(\alpha) = p$, as we have seen above.
- $p \equiv 3 \ (4)$ $\longrightarrow$ $\nexists \alpha \in R$ with $N(\alpha) = p$, since p is primitive.

Theorem.
In the general case, an integer n is represented by the sum of two squares iff in the prime factorisation of n any prime $p \equiv 3 \ (4)$ appears with even exponent.

PROOF: If $n = 2^a \prod_{p_i \equiv 1 \ (4)} p_i^{b_i} \prod_{q_j \equiv 3 \ (4)} q_j^{2c_j}$ with $a, b_i, c_j \in \mathbb{Z}_{\geq 1}$

then $N(u) = N(1+i)^a \prod_i N(\alpha_i)^{b_i} \prod_j N(q_j)^{c_j}$. This proves one direction.

In the other direction, assume $n = N(\alpha)$.

Write $\alpha = \prod \beta_i$ with $\beta_i \in R$ primitive elements. $\Rightarrow N(\alpha) = \prod N(\beta_i)$

$$N(\beta_i) = \begin{cases} 2 & \\ p & p \equiv 1 \ (4) \\ p^2 & p \equiv 3 \ (4) \end{cases}$$ (as we have seen before)

□

Analytic method

$$r(n) = \#\{ (x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n \}$$

Question: How do we compute $r(n)$?

Observation: $4 \mid r(n)$ because if (x,y) is a solution, so is (y,x), $(-x,-y)$ and $(-y,-x)$. $|R^\times| = 4$.

$r(2) = 4$, $r(3) = 0$, $r(5) = 8$, $r(6) = 0$, $r(7) = 0$

$$\zeta_R(s) := \sum_{n \geq 1}^{+\infty} \frac{r(n)}{4} \cdot \frac{1}{n^s} \qquad \mathrm{Re}(s) \gg 0$$

$$= \sum_{(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{4 (a^2+b^2)^s}$$

$$(a^2 + b^2)^s = N(a+bi)^s$$

$$\zeta_R(s) = \sum_{\alpha \in R \setminus \{0\}} \frac{1}{4 N(\alpha)^s} = \sum_{0 \neq I \subseteq R} \frac{1}{N(I)^s}$$ where $N(I) = N(\alpha)$ if $(\alpha) = I$.

$$= \prod_{\substack{p \subseteq R \\ \text{prime}}} \underbrace{\left(\sum_{m=0}^{+\infty} \frac{1}{N(p)^{ms}} \right)}_{\frac{1}{1 - (N(p))^{-s}} \text{ geometric series}}$$ using the unique factorisation property of ideals in R

$$= \prod_{\substack{p \subseteq R \\ \text{prime}}} \frac{1}{1 - (N(p))^{-s}} = \underbrace{\frac{1}{1 - 2^{-s}}}_{p = (1+i)} \underbrace{\prod_{p \equiv 1 \ (4)} \frac{1}{(1 - p^{-s})^2}}_{\text{2 primes } \mathfrak{p} \text{ above } p} \prod_{p \equiv 3 \ (4)} \frac{1}{1 - p^{-2s}} =$$

$$= \underbrace{\left(\frac{1}{1-2^{-s}} \prod_{p \equiv 1 \ (4)} \frac{1}{1-p^{-s}} \prod_{p \equiv 3 \ (4)} \frac{1}{1-p^{-s}} \right)}_{\text{on all primes } p} \prod_{p \equiv 1 \ (4)} \frac{1}{1-p^{-s}} \prod_{p \equiv 3 \ (4)} \frac{1}{1+p^{-s}}$$

$$= \underbrace{\prod_{p} \frac{1}{1-p^{-s}}}_{} \underbrace{\prod_{p\equiv 1(4)} \frac{1}{1-p^{-s}} \prod_{p\equiv 3(4)} \frac{1}{1+p^{-s}}}_{} =$$

$$= \zeta(s) \cdot L(\chi, s)$$

$$L(\chi, s) = \prod_{p} \frac{1}{1-\chi(p)p^{-s}} \quad \text{where} \quad \chi(p) = \begin{cases} 0 & p=2 \\ +1 & p\equiv 1\ (4) \\ -1 & p\equiv 3\ (4) \end{cases}$$

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$

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

Here we extend the definition of χ to all integers multiplicatively

$$\Rightarrow \frac{1}{4} \sum_{n=1}^{+\infty} \frac{r(n)}{n^s} = \left(\sum_{n=1}^{+\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}\right)$$

Lemma. $\left(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$ where $b_n = \sum_{\substack{d|n \\ d\geq 1}} a_d$ □

Theorem. $r(n) = 4 \sum_{d|n} \chi(d)$

PROOF: Use the lemma. □

Example. $n = p$ prime $\sum_{d|n} \chi(d) = 1 + \chi(p) = \begin{cases} 1 & p=2 \\ 0 & p\equiv 3\ (4) \\ 2 & p\equiv 1\ (4) \end{cases}$

$n = p^k$

$$\sum_{d|n} \chi(d) = 1 + \chi(p) + \dots + \chi(p^k) =$$

$$= \begin{cases} 1 & p=2 \\ k+1 & p\equiv 1\ (4) \\ \frac{1-(-1)^{k+1}}{2} & p\equiv 3\ (4) \end{cases}$$

(0 or 1 depending on parity of k) □

Def. We say a sequence $(a_n)_{n\geq 1}$ of complex numbers is multiplicative if $a_{mn} = a_m \cdot a_n \quad \forall \gcd(m,n) = 1$.

Lemma. If (a_n) is multiplicative, so is $\left(\sum_{d|n} a_d\right)_{n\geq 1}$.

Using this lemma, we may obtain a general formula for $r(n)$.

PROOF: a_n multipl. $\Leftrightarrow$ if $n = p_1^{m_1} \cdots p_k^{m_k}$ $\forall i\neq j$: $p_i \neq p_j$, $m_i \in \mathbb{Z}_{>0}$ then $a_n = a_{p_1^{m_1}} \cdots a_{p_k^{m_k}}$

$$\Leftrightarrow \sum_{n=1}^{+\infty} \frac{a_n}{n^s} = \prod_p \left(\sum_{m=0}^{+\infty} \frac{a_{p^m}}{p^{ms}} \right)$$

So if we put $\sum_{n=1}^{+\infty} \frac{b_n}{n^s} = \left(\sum_{n=1}^{+\infty} \frac{a_n}{n^s} \right) \left(\sum_{n=1}^{+\infty} \frac{1}{n^s} \right)$ then

$$\sum_{n=1}^{\infty} \frac{b_n}{n^s} = \prod_p \left[\left(\sum_{m=0}^{\infty} \frac{a_{p^m}}{p^{ms}} \right) \left(\sum_{l=0}^{\infty} \frac{1}{p^{ls}} \right) \right] = \prod_p \left[\sum_{m=0}^{\infty} \frac{1}{p^{ms}} \left(\sum_{k=0}^{\infty} a_{p^k} \right) \right]$$

By definition: $b_{p^m} = \sum_{d | p^m} a_d = \sum_{r=0}^{m} a_{p^r}$

$$\sum_{n=1}^{\infty} \frac{b_n}{n^s} = \prod_p \left(\sum_{m=0}^{\infty} \frac{b_{p^m}}{p^{ms}} \right) \Rightarrow b_n = \prod_i b_{p_i^{m_i}} \text{ if } n = p_1^{m_1} \cdots p_r^{m_r}$$

□

Generalisations

n is represented by	conditions on prime factors
$x^2 + 2y^2$	all primes $p \equiv 5, 7 \ (8)$ appear with even exponents
$x^2 + 3y^2$	all primes $p \equiv 2 \ (3)$ appear with even exponents
$x^2 + 5y^2$	(1) any prime $p \equiv 11, 13, 17, 19 \ (20)$ appears with even exponents (2) the total multiplicity of primes $p \equiv 2, 3, 7 \ (20)$ is even

Formulas for the number of solutions may be obtained as well, with some complication arising from condition (2) in the last case.

The case of this problem is that $R = \mathbb{Z}[\sqrt{-5}]$ is not a PID; the class number h_{-5} for R is 2. (The class number is 1 $\Leftrightarrow$ R is a PID.)

There are • 1 binary quadratic forms $f(x,y) = ax^2 + bxy + cy^2$ with discriminant $\Delta = b^2 - 4ac = -4, -8, -12$

• 2 forms with $\Delta = -20$, namely $x^2 + 5y^2$, $2x^2 + 2xy + 3y^2$

Algebraic Number Theory, lecture 1–2

Course contents

1. Basic knowledge on algebraic integers: Dedekind domains, prime decomposition in extension of number field, finiteness thm. of class number. (Prereq.: commutative algebra)
2. Dirichlet series, residue formula for Dedekind zeta function, distribution of ideals
3. Non-archimedean fields, adèles, idèles. Tate's thesis on Fourier analysis on adèles. (Prereq.: Topology)

If we are very fast: some statements in class field theory.

Literature → lecture notes on Tian's homepage for a previous course for parts 1. and 2.

Algebraic integers

16.10.2017

Prop.-Def. Let $A \subset B$ be an extension of rings, $x \in B$. We say that x is integral over A if one of the following conditions holds:

1) x satisfies $x^n + a_1 x^{n-1} + \dots + a_n = 0$, $\forall a_i \in A$
2) $A[x]$ is finitely generated as an A-module
3) $A[x]$ is contained in the subring $B' \subseteq B$ which is a finitely gen. A-mod.

PROOF: 1) ⇒ 2) ⇒ 3) trivial.

3) ⇒ 1): assume $B' = \sum_{i=1}^{n} A\alpha_i$

$x \in B' \Rightarrow x(\alpha_1, \dots, \alpha_n) = (\alpha_1, \dots, \alpha_n) C$ for some $C \in M_{n\times n}(A)$

$(\alpha_1, \dots, \alpha_n)(xI_n - C) = 0$

$\Rightarrow (\alpha_1, \dots, \alpha_n) \det(xI_n - C) = 0$

$\Rightarrow \det(xI_n - C) = 0$

(Convention: all rings are commutative and have 1.) □

Cor. 1) All elements of B integral over A form a subring

2) Let $A \subseteq B \subseteq C$ be extension of rings. Then C int. over A (i.e. $\forall c \in C$ is int. over A) $\Leftrightarrow$ C int. over B and B int. over A.

Def. 1) Let $A \subset B$ be a ring extension.
We define the integral closure of A in B as the subring of B containing all elements integral over A.

2) If A is a domain, we say that A is int. closed if it is the int. closure of itself in its fraction field.

Prop. Every PID is integrally closed.

Proof: Let A be a PID, its fraction field: $K = \mathrm{Frac}(A)$.

$x = \frac{a}{b} \in K$ integral over A.

We may assume that $\gcd(a,b) = 1$ $\Leftrightarrow$ $\nexists$ primitive element dividing a and b.

$$x^n + a_1 x^{n-1} + \dots + a_n = 0 \qquad a_i \in A$$

$$a^n + a_1 a^{n-1} b + \dots + a_n b^n = 0$$

We claim that $b \in A^\times$, so $x \in A$. Otherwise $\exists$ primitive $p \mid b$ $\Rightarrow$

$p \mid a^n \Rightarrow p \mid a \Rightarrow p \mid \gcd(a,b)$ ↯. □

Example. $\mathbb{Z}[\sqrt{-3}]$ is not int. closed since $\frac{1+\sqrt{-3}}{2}$ is integral over $\mathbb{Z}$ (hence over $\mathbb{Z}[\sqrt{-3}]$ as well)

Notation. $K/\mathbb{Q}$ finite ext, $\mathcal{O}_K$ = int. closure of $\mathbb{Z}$ in K. = ring of integers in K.

Prop. Let $K/\mathbb{Q}$ be finite, $x \in K$ with minimal polynomial

$$f(T) = T^n + a_1 T^{n-1} + \dots + a_n \in \mathbb{Q}[T]$$

Then $x \in \mathcal{O}_K$ $\Leftrightarrow$ $\forall a_i \in \mathbb{Z}$.

Proof: $\Leftarrow$ by definition.

$\Rightarrow$ Let $L/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$.

Let $x_1 = x, x_2, \dots, x_n \in L$ be the Galois conjugates of x.

There exist embeddings $\sigma_i : K \hookrightarrow L$, $(\forall i = 1, \dots, n)$.
$x \longmapsto x_i$.

Of course $\forall x_i$ are integral over $\mathbb{Z}$.

$$f(T) = \prod_{i=1}^{n} (T - x_i) = T^n + a_1 T^{n-1} + \dots + a_n$$

$\Rightarrow a_i = (-1)^i \left(i^{\text{th}} \text{ symmetric fuction of } x_i\right) \in \underbrace{\mathcal{O}_K \cap \mathbb{Q}}_{= \mathbb{Z} \text{ because } \mathbb{Z} \text{ is integrally closed.}}$ □

Example. $K = \mathbb{Q}(\sqrt{D})$, $1 \neq D \in \mathbb{Z}$ square-free

Claim. $\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & D \equiv 1 \pmod 4 \end{cases}$

PROOF: Let $\underbrace{a + b\sqrt{D}}_{x} \in K$ be integral over $\mathbb{Z}$

If $b = 0 \Rightarrow x = a \in \mathbb{Z}$

If $b \neq 0 \Rightarrow$ minpoly of x is $f(T) = T^2 - 2aT + (a^2 - b^2 D)$

$\Rightarrow 2a \in \mathbb{Z}$, $a^2 - b^2 D \in \mathbb{Z}$

- If $a \in \mathbb{Z} \Rightarrow b \in \mathbb{Z}$ because D is square-free.
- If $a \equiv \frac{1}{2} \pmod{\mathbb{Z}} \Rightarrow b \equiv \frac{1}{2} \pmod{\mathbb{Z}}$

  Write $a = \frac{2a_1 + 1}{2}$, $b = \frac{2b_1 + 1}{2}$ $\longrightarrow$ $a^2 - b^2 D \in \mathbb{Z} \iff D \equiv 1 \pmod 4$ □

Discriminant & integral basis

Recall. Let K be a field, A a fin. dim. K-algebra.

$\forall x \in A$. $\ell_x : A \longrightarrow A$, $y \longmapsto xy$

$\mathrm{Tr}_{A/K} := \mathrm{Tr}(\ell_x)$, $N_{A/K} := \det(\ell_x)$

Basic properties of trace and norm:

Lemma. Let L/K be a finite ext. of fields.

$\forall x \in L$ with minimal polynomial $f(T) = T^n + a_1 T^{n-1} + \dots + a_n \in K[T]$

Then $\mathrm{Tr}_{L/K}(x) = -[L : K(x)] \cdot a_1$,

$N_{L/K}(x) = \left[(-1)^n a_n\right]^{[L : K(x)]}$

PROOF: exercise. □

Lemma. Let L/K be a separable field extension, Ω/K be an alg. closed ext.

By Galois theory, there are $n = [L : K]$ distinct (K-linear) embeddings $\sigma_i : L \hookrightarrow \Omega$.

Then for every $x \in L$: $\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$, $N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$.

Theorem. Assume L/K is a finite separable extension.

Then the K-linear pairing $\mathrm{Tr}_{L/K}: L \times L \to K$

$$(x,y) \to \mathrm{Tr}_{L/K}(xy) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y)$$

is non-degenerate, i.e. $\forall x \in L$ if $\mathrm{Tr}_{L/K}(xy) = 0$ for all $y \in L \Rightarrow x = 0$.

PROOF: omitted, Serge Lang: Algebra, Chap. VI. § 5. □

Cor. This pairing $\mathrm{Tr}_{L/K}$ induces an isomorphism of K-vector spaces

$$\varphi: \begin{array}{ccc} L & \xrightarrow{\sim} & L^\vee := \mathrm{Hom}_K(L, K) \\ x & \longmapsto & (y \mapsto \mathrm{Tr}_{L/K}(xy)) \end{array}$$

given a basis $\alpha_1, \dots, \alpha_n$ of L/K,

Two bases: $\left.\begin{matrix} \varphi(\alpha_1), \dots, \varphi(\alpha_n) \\ \text{and} \quad \alpha_1^\vee, \dots, \alpha_n^\vee \end{matrix}\right\}$ of $L^\vee$ over K

Where $\alpha_i^\vee$ is defined by: $\alpha_i^\vee(\alpha_j) = \delta_{ij} \quad \forall i,j \in \{1, \dots, n\}$

$\exists a_{ij} \in K$ s.t. $\varphi(\alpha_i) = \sum_{j=1}^{n} a_{ij} \alpha_j^\vee$

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha_k) = \varphi(\alpha_i)(\alpha_k) = \left(\sum_{j=1}^{n} a_{ij} \alpha_j^\vee\right)(\alpha_k) =$$

$$= \sum_{j=1}^{n} a_{ij} \underbrace{\alpha_j^\vee(\alpha_k)}_{\delta_{jk}}$$

$$= a_{ik}$$

In particular, $\det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right) \neq 0$ if $\alpha_1, \dots, \alpha_n$ is a basis of L/K.

Conversely: if $\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)$ is an invertible matrix, then consider the map

$$K^n \xrightarrow{f} L \xrightarrow{g} K^n$$

$$(x_i) \longmapsto \sum_{i=1}^{n} x_i \alpha_i$$

$$x \longmapsto \left(\mathrm{Tr}_{L/K}(x \alpha_i)\right)_{1 \le i \le n}$$

$$\sum_{i=1}^{n} x_i \alpha_i \longmapsto \left(\sum_{i=1}^{n} \mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\, x_j\right)_{1 \le i \le n}$$

Then $g \circ f$ with matrix $\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)$ is an isomorphism.

$\Rightarrow f$ is injective, hence an isomorphism.

$\Rightarrow \alpha_1, \dots, \alpha_n$ is a basis of L/K. This gives an equivalent condition for $\alpha_1, \dots, \alpha_n$ to be a basis.

Remark. In the theorem that L/K is sep. is crucial.

Consider $L = K(\sqrt[p]{a})$, $\mathrm{char}\, K = p$ and $a \in K \setminus K^p$

$\Rightarrow \mathrm{Tr}_{L/K}(x) = 0 \quad \forall x \in L$.

Algebraic Number Theory, lecture 2

L/K finite separable extension

$\alpha_1, \dots, \alpha_n$ basis for L/K

Use $\mathrm{Tr}_{L/K}(\cdot)$ to identify $L \xrightarrow{\sim} L^\vee$

So $\alpha_1^\vee, \dots, \alpha_n^\vee$ are identified with elements in L s.t. $\mathrm{Tr}_{L/K}(\alpha_i \alpha_j^\vee) = \delta_{ij} \ \forall i,j$.

We call $(\alpha_1^\vee, \dots, \alpha_n^\vee)$ the dual basis of $(\alpha_1, \dots, \alpha_n)$.

$\forall x \in L: \quad x = \sum_{i=1}^{n} \mathrm{Tr}_{L/K}(x \alpha_i) \cdot \alpha_i^\vee$.

Application to number fields

Def. $K/\mathbb{Q}$ finite ext., $\alpha_1, \dots, \alpha_n \in K$ where $[K:\mathbb{Q}] = n$.

We put $\mathrm{disc}(\alpha_1, \dots, \alpha_n) := \det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)$ called the discriminant of $\alpha_1, \dots, \alpha_n$.

Lemma. 1) $\mathrm{disc}(\alpha_1, \dots, \alpha_n) \neq 0 \iff (\alpha_1, \dots, \alpha_n)$ is a basis of $K/\mathbb{Q}$

2) If $\beta_1, \dots, \beta_n \in K$ with $(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n) C$ for some $C \in M_{n \times n}(\mathbb{Q})$

$\Rightarrow \mathrm{disc}(\beta_1, \dots, \beta_n) = \mathrm{disc}(\alpha_1, \dots, \alpha_n) \cdot \det(C)^2$.

3) Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings.

$\Rightarrow \mathrm{disc}(\alpha_1, \dots, \alpha_n) = \det\left(\sigma_i(\alpha_j)\right)^2$

PROOF: 1), 2) exercise.

3) $\mathrm{Tr}_{L/K}(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\, \sigma_k(\alpha_j)$

$A := \left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{1 \le i,j \le n}, \quad B := \left(\sigma_i(\alpha_j)\right)_{1 \le i,j \le n}$

$A = {}^tB \cdot B$ (this is easily seen) $\Rightarrow \det A = \det(B)^2$. □

Prop. Let $\alpha \in K$, $f(T) = T^d + a_1 T^{d-1} + \dots + a_d \in \mathbb{Q}[T]$ its minpoly.

Then $\mathrm{disc}(1, \alpha, \dots, \alpha^{n-1}) = \begin{cases} 0 & \text{if } \deg f < [K:\mathbb{Q}] = n \\ (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha)) & \text{if } \deg f = n. \end{cases}$

PROOF: Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the n embeddings.

$\mathrm{disc}(1, \alpha, \dots, \alpha^{n-1}) = \det\left(\sigma_i(\alpha^{j-1})\right)^2$

Recall Vandermonde's formula:

$$\begin{vmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & \ddots & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i<j} (x_i - x_j)$$

In our case, we get $\operatorname{disc}(1, \dots, \alpha^{n-1}) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$

$$N_{K/\mathbb{Q}}(f'(\alpha)) = \prod_{i=1}^{n} \sigma_i(f'(\alpha)) =$$

$$= \prod_{i=1}^{n} \prod_{j \neq i} (\sigma_i(\alpha) - \sigma_j(\alpha))$$

$$= (-1)^{\frac{n(n-1)}{2}} \cdot \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))$$

□

Remark. For any basis $\alpha_1, \dots, \alpha_n$ of $K/\mathbb{Q}$, $\operatorname{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$ all have the same sign, since they only differ by a square factor.

Notation. Label the n distinct embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$ as follows:

$\sigma_1, \dots, \sigma_{r_1}$: $K \hookrightarrow \mathbb{R}$ are the real embeddings

$\sigma_{r_1+2j-1}, \sigma_{r_1+2j} = \overline{\sigma_{r_1+2j-1}} : K \hookrightarrow \mathbb{C}$ are the non-real embeddings for $1 \le j \le r_2$,

where $n = r_1 + 2r_2$. (Ex.: $\mathbb{Q}(\sqrt[3]{2}) = K$ has $r_1 = 1$, $r_2 = 2$).

Prop: For a basis $(\alpha_1, \dots, \alpha_n)$ of $K/\mathbb{Q}$, the sign of $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$ is $(-1)^{r_2}$.

Proof: $\operatorname{disc}(\alpha_1, \dots \alpha_n) = \det(\sigma_i(\alpha_j))^2$

$\det(\sigma_i(\alpha_j)) = \det(\overline{\sigma_i}(\alpha_j)) = (-1)^{r_2} \det(\sigma_i(\alpha_j))$

$$\begin{cases} \overline{\sigma_i} = \sigma_i & \forall\ 1 \le i \le r_1 \\ \overline{\sigma}_{r_1+2j-1} = \sigma_{r_1+2j} & \forall\ 1 \le j \le r_2 \end{cases}$$

$$\Rightarrow \det(\sigma_i(\alpha_j)) \in \begin{cases} \mathbb{R} & \text{if } r_2 \text{ is even} \\ i\mathbb{R} & \text{if } r_2 \text{ is odd} \end{cases}$$

$\Rightarrow \det(\sigma_i(\alpha_j))$ has sign $(-1)^{r_2}$.

□

Prop: $K/\mathbb{Q}$ fin. ext. of deg. n. Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof: Choose $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ which form a basis of $K/\mathbb{Q}$. (We can do this by choosing a basis of K and then multiplying by the product of the denominators.)

Algebraic Number Theory, lecture 2 – 3

$M := \sum_{i=1}^{n} \mathbb{Z}\alpha_i \subseteq \mathcal{O}_K$

$M^\vee := \sum_{i=1}^{n} \mathbb{Z}\alpha_i^\vee \supseteq \mathcal{O}_K$ because $\forall x \in \mathcal{O}_K \quad x = \sum_{i=1}^{n} \underbrace{Tr_{K/\mathbb{Q}}(x\alpha_i)}_{\in \mathbb{Z}} \cdot \alpha_i^\vee$

$\left| M^\vee / M \right| = |\det(Tr_{K/\mathbb{Q}}(\alpha_i\alpha_j))| \neq 0$ because $\alpha_i = \sum_{j=1}^{n} Tr_{K/\mathbb{Q}}(\alpha_i\alpha_j)\,\alpha_j^\vee$

$\Rightarrow \mathcal{O}_K$ is a free abelian group of rank n. □

Def. An integral basis of $K/\mathbb{Q}$ is a basis $\alpha_1, \dots, \alpha_n \in K$ s.t. $\mathcal{O}_K = \sum_{i=1}^{n} \mathbb{Z}\alpha_i$.

$\operatorname{disc}_K := \operatorname{disc}(\alpha_1, \dots, \alpha_n)$ for integral basis $\alpha_1, \dots, \alpha_n$ of $K/\mathbb{Q}$.

Ex. $K = \mathbb{Q}(\sqrt{D})$, $D \neq 1$ square-free.

$\mathcal{O}_K = \mathbb{Z}[\omega_D]$, $\omega_D = \begin{cases} \sqrt{D} & D \equiv 2,3 \ (4) \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \ (4) \end{cases}$

$\operatorname{disc}_K = \operatorname{disc}(1, \omega_D) = \det \begin{pmatrix} 1 & \omega_D \\ 1 & \overline{\omega_D} \end{pmatrix}^2 = (\overline{\omega_D} - \omega_D)^2 = \begin{cases} 4D & D \equiv 2,3 \ (4) \\ D & D \equiv 1 \ (4) \end{cases}$

Ex. $K = \mathbb{Q}(\sqrt[3]{2})$

$\mathbb{Z}[\sqrt[3]{2}] \subseteq \mathcal{O}_K$, we do not know if they are equal.

We can compute the discriminant:

$\operatorname{disc}(1, \sqrt[3]{2}, \sqrt[3]{4}) = (-1) \cdot N_{K/\mathbb{Q}}(f'(\sqrt[3]{2})) = -3^3 \cdot 2^2$

$f(T) = T^3 - 2$, $f'(T) = 3T^2$, $N_{K/\mathbb{Q}}(3\sqrt[3]{4}) = 3^3 \cdot 4$

$[\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}]] \leq 6$

$m = [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}]]$, $\operatorname{disc}_K m^2 = \operatorname{disc}(1, \sqrt[3]{2}, \sqrt[3]{4})$ $\Rightarrow$ $2,3 \nmid m$.

Suppose $K/\mathbb{Q}$ finite, $[K:\mathbb{Q}] = n$. 19.10.2017

Ex. $K = \mathbb{Q}(\alpha)$, $\alpha^3 = 2$

Thm: $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. Equality?

$f(T) = T^3 - 2$

$\operatorname{disc}(1, \alpha, \alpha^2) = -N_{K/\mathbb{Q}}(f'(\alpha)) = -3^3 \cdot 2^2$

Lemma. Let $\beta_1, \dots, \beta_n \in \mathcal{O}_K$ form a basis of $K/\mathbb{Q}$. Then $(\beta_1, \dots, \beta_n)$ is an integral basis iff $\forall$ prime p with $p^2 \mid \operatorname{disc}(\beta_1, \dots, \beta_n)$ and any $x_i \in \{0, \dots, p-1\}$ $(1 \leq i \leq n)$ not all zero we have $\sum_{i=1}^{n} x_i\beta_i \notin p\mathcal{O}_K$

PROOF: Choose an integral basis $(\alpha_1, \dots, \alpha_n)$ of $K/\mathbb{Q}$.

$(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n) \cdot C, \quad C \in M_{n\times n}(\mathbb{Z}), \quad \det(C) \neq 0.$

$(\beta_1, \dots, \beta_n)$ is also integral iff $\det(C) = \pm 1$

Assume $(\beta_1, \dots, \beta_n)$ is not integral. Let $p \mid \det(C)$ be a prime

$\Rightarrow p^2 \mid \operatorname{disc}(\beta_1, \dots, \beta_n) = \operatorname{disc}_K (\det C)^2$

Let $\overline{C} \in M_{n\times n}(\mathbb{F}_p)$, $\det(\overline{C}) = 0$.

Let $(\overline{x_1}, \dots, \overline{x_n}) \in \operatorname{Ker} \overline{C}$, $x_i \in \{0, \dots, p-1\}$ is the lift of $\overline{x_i}$.

Then $\sum_{i=1}^{n} \beta_i x_i = (\alpha_1, \dots, \alpha_n) C \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$

$C \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \equiv 0 \pmod{p} \Rightarrow \sum \beta_i x_i \in p\mathcal{O}_K.$

Conversely: if there exist such p and x_i with $\sum x_i \beta_i \in p\mathcal{O}_K$,

then $(\overline{x_1}, \dots, \overline{x_n}) \in \operatorname{Ker} \overline{C} \Rightarrow \det(\overline{C}) = 0$ in $\mathbb{F}_p \Rightarrow p \mid \det(C)$ □

$\sum \mathbb{Z}\beta_i \subsetneq \mathcal{O}_K \Rightarrow \frac{1}{p} \sum x_i \beta_i \in \mathcal{O}_K$ for some $p^2 \mid \operatorname{disc}(\beta_1, \dots, \beta_n)$.

Prop. Let $\alpha \in \mathcal{O}_K$ s.t. $K = \mathbb{Q}(\alpha)$ and $f(T) \in \mathbb{Z}[T]$ be its min. poly.

Assume that $\forall p$ prime with $p^2 \mid \operatorname{disc}(1, \dots, \alpha^{n-1})$ there exists some $i \in \mathbb{Z}$ (which may depend on p) s.t. $f(T+i)$ is an Eisenstein polynomial for p.

Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Recall: $f(T) = T^n + \dots + a_n \in \mathbb{Z}[T]$ is Eisenstein for p if $p \| a_n$ and $p \mid a_i$ $\forall i$.

Ex. $p=2$: $f(T) = T^3 - 2$ is Eisenstein.

$p=3$: $f(T-1) = (T-1)^3 - 2 = T^3 - 3T^2 + 3T - 3$ } $\Rightarrow \mathbb{Z}[\alpha] = \mathcal{O}_K$.

Ex. $K = \mathbb{Q}(\sqrt[3]{5})$ $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{5}]$ ($\hookrightarrow$ we need to check for 3 and 5)

Remark. 1) It is possible that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ but the condition is not satisfied.

2) $\exists K/\mathbb{Q}$ s.t. $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any $\alpha \in K$.

PROOF: Up to replacing α by $\alpha - i$ it suffices to show that if $f(T)$ is Eisenstein for p then $p \nmid \sum_{i=1}^{n} x_i \alpha^{i-1}$ $\forall x_i \in \{0, \dots, p-1\}$ not all zero.

Put $j := \min\{i \mid x_i \neq 0\}$, put $x := \frac{1}{p}\sum_{i=1}^{n} x_i \alpha^{i-1} = \frac{\alpha^{j-1}}{p}\sum_{i=j}^{n} x_i \alpha^{i-j}$

We want to show that $x \notin O_K$.

$$N_{K/\mathbb{Q}}(x) = \frac{N_{K/\mathbb{Q}}(\alpha)^{j-1}}{p^n} N_{K/\mathbb{Q}}\left(\sum_{i=j}^{n} x_i \alpha^{i-j}\right)$$

$$N_{K/\mathbb{Q}}(\alpha) = (-1)^n a_n$$

$\Rightarrow$ There is some power of p in the denom of $\frac{N_{K/\mathbb{Q}}(\alpha)^{j-1}}{p^n}$.

Claim. $N_{K/\mathbb{Q}}\left(\sum_{i=j}^{n} x_i \alpha^{i-j}\right) \equiv x_j^n \pmod{p}$ $\left[\Rightarrow N_{K/\mathbb{Q}}(x) \notin \mathbb{Z}, \text{ which finishes the proof.}\right]$

Pf: $N_{K/\mathbb{Q}}\left(\sum_{i=j}^{n} x_i \alpha^{i-j}\right) = \prod_{\sigma=1}^{n}\left(\sum_{i=j}^{n} x_i \sigma_\sigma(\alpha^{i-j})\right) =$ $\quad \sigma_\sigma : K \hookrightarrow \mathbb{C}$

$$= \prod_{\sigma=1}^{n}\left(x_j + \sigma_\sigma(\alpha) x_{j+1} + \ldots + \sigma_\sigma(\alpha)^{n-j} x_n\right) =$$

$$= x_j^n + \underbrace{\text{other terms are symm. polynomials in } \sigma_\sigma(\alpha)\text{'s}}$$

each term is a poly in a_i's so divisible by p

Cyclotomic fields

$N \geq 3$ integer, ζ_N N^{th} primitive root of unity in $\mathbb{C}$, e.g. $\zeta_N = e^{\frac{2\pi i}{N}}$

$\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is Galois

$\forall \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$: $\sigma(\zeta_N) = \zeta_N^{a_\sigma}$ for $a_\sigma \in \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$

Get a map $f: \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \longrightarrow \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$

$\sigma \longmapsto a_\sigma$

Prop. The map f is an iso of groups.

Pf: Obviously a homomorphism.

f is injective since every element of the Gal group is determined by its action on the generator element.

Remains to show: surjectivity. Suffices to show: any prime p with $p \nmid N$ lies in the image of f, i.e. $\forall p \nmid N$ ζ_N^p is $\mathbb{Q}$-conjugate to ζ_N.

Consider $g(T) \in \mathbb{Z}[T]$, the min. poly of ζ_N.

$$T^N - 1 = g(T) \cdot h(T) \quad \text{for some } h(T) \in \mathbb{Z}[T].$$

↯ Assume that ζ_N^p is not conjugate to ζ_N.

$\Rightarrow g(\zeta_N^p) \neq 0$ but $h(\zeta_N^p) = 0$. $\Rightarrow g(T) \mid h(T^p)$

Let $\bar{g}, \bar{h}$ be the reduction of g, h resp. in $\mathbb{F}_p[T]$

$\bar{g} \mid \bar{h}(T^p) = \bar{h}(T)^p$ (char p)

If α is a root of $\bar{g}$, then $0 = \bar{h}(\alpha^p) = \bar{h}(\alpha)^p \Rightarrow h(\alpha) = 0$.

$$T^N - 1 = \bar{g}(T) \cdot \bar{h}(T) \quad \text{in } \mathbb{F}_p[T]$$

$\rightarrow \alpha$ is a multiple root of $T^N - 1 \in \mathbb{F}_p[T]$.

But $(T^N - 1)' = N \cdot T^{N-1}$, $N \cdot \alpha^{N-1} \neq 0$ in $\overline{\mathbb{F}_p}$ ↯ □

Cor. 1) $[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \left|\left(\mathbb{Z}/N\mathbb{Z}\right)^\times\right| = \varphi(N)$

2) $\forall N, M \geq 3$ with $\gcd(N, M) = 1$: $\mathbb{Q}(\zeta_{N+M}) = \mathbb{Q}(\zeta_N)(\zeta_M)$ and $\mathbb{Q}(\zeta_N) \cap \mathbb{Q}(\zeta_M) = \mathbb{Q}$.

Pf: 1) trivial.

2) The first equation is trivial.

$$[\mathbb{Q}(\zeta_N\zeta_M) : \mathbb{Q}(\zeta_M)] = [\mathbb{Q}(\zeta_N) : \mathbb{Q}(\zeta_N) \cap \mathbb{Q}(\zeta_M)]$$

So $\mathbb{Q}(\zeta_N) \cap \mathbb{Q}(\zeta_M) = \mathbb{Q} \iff [\mathbb{Q}(\zeta_N\zeta_M) : \mathbb{Q}(\zeta_M)] = \varphi(N)$

But this follows from

$$[\mathbb{Q}(\zeta_N\zeta_M) : \mathbb{Q}(\zeta_M)] = \frac{[\mathbb{Q}(\zeta_{NM}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_M) : \mathbb{Q}]} = \frac{\varphi(NM)}{\varphi(M)} = \varphi(N)$$

□

$\mathcal{O}_{\mathbb{Q}(\zeta_N)} = ?$

$\cup|$

$\mathbb{Z}[\zeta_N]$ We need to compute $\operatorname{disc}(1, \zeta_N, \dots, \zeta_N^{\varphi(N)-1}) = \pm N_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(\Phi_N(\zeta_N))$

where $\Phi_N(T) = \prod_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} (T - \zeta_N^a)$ is the min. poly. of ζ_N.

So first we study Φ_N.

$$T^{N-1} = \prod_{d \mid N} \Phi_d(T) \quad \text{for } N = p^n \text{ with } p \text{ prime.}$$

Then $T^{p^n} - 1 = \Phi_{p^n}(T) \underbrace{\prod_{1 \leq i \leq n-1} \Phi_{p^i}(T)}_{T^{p^{n-1}} - 1}$ $\Rightarrow \Phi_{p^n}(T) = \dfrac{T^{p^n} - 1}{T^{p^{n-1}} - 1} = \sum_{i=0}^{p-1} T^{p^{n-1} \cdot i}$

Lemma. $\operatorname{disc}(1, \zeta_N, \dots, \zeta_N^{\varphi(N)-1}) \mid N^{\varphi(N)}$

Pf: $T^N - 1 = \Phi_N(T) \cdot g(T)$

$$NT^{N-1} = \Phi_N'(T) \cdot g(T) + \Phi_N(T) \cdot g'(T)$$

$T := \zeta_N$ (with $\Phi_N(\zeta_N) = 0$)

$$N\zeta_N^{N-1} = \Phi_N'(\zeta_N) \cdot g(\zeta_N) + 0$$

$$\Rightarrow \left| N_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}\left(\Phi_N'(\zeta_N)\right) \right| \;\Big|\; \left| N_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}\left(N\zeta_N^{N-1}\right) \right| = N^{\varphi(N)}.$$

□

Cor. If $N = p^n$ then $\mathcal{O}_{\mathbb{Q}(\zeta_{p^n})} = \mathbb{Z}[\zeta_{p^n}]$.

Pf: $$\Phi_{p^n}(T+1) = \frac{(T+1)^{p^n} - 1}{(T+1)^{p^{n-1}} - 1} = \sum_{i=0}^{p-1} (T+1)^{p^{n-1} i}$$

$$= T^{p^{n-1}(p-1)} + \dots + p \quad \text{(← const. term)}$$

$$\equiv \sum_{i=0}^{p-1} (T^{p^{n-1}} + 1)^i = \frac{(T^{p^{n-1}} + 1)^p - 1}{(T^{p^{n-1}} + 1) - 1}$$

$$\equiv T^{p^{n-1}(p-1)} \pmod{p}$$

is an Eisenstein polynomial for p.

□

Generalisations to general N.

For this, we need some general facts about the discriminant.

Let K, L be number fields in $\mathbb{C}$. $KL = \left\{ \sum x_i y_i \mid x_i \in K,\ y_i \in L \right\}$

$\cup$

$\mathcal{O}_K \mathcal{O}_L = \left\{ \sum x_i y_i \mid x_i \in \mathcal{O}_K,\ y_i \in \mathcal{O}_L \right\}$

Of course $\mathcal{O}_K \mathcal{O}_L \subseteq \mathcal{O}_{KL}$, but there is no equality in general.

Prop. Assume that $K \cap L = \mathbb{Q}$ and $d = \gcd(\operatorname{disc}_K, \operatorname{disc}_L)$.

Then $\mathcal{O}_{KL} \subseteq \frac{1}{d} \mathcal{O}_K \mathcal{O}_L$.

In particular, if $d = 1$, then $\mathcal{O}_K \mathcal{O}_L = \mathcal{O}_{KL}$.

Pf: Let $(\alpha_1, \dots, \alpha_n)$, $(\beta_1, \dots, \beta_n)$ be integer bases of K, L resp.

$\forall x \in \mathcal{O}_{KL}$ $x = \sum_{ij} \frac{x_{ij}}{r} \alpha_i \beta_j$ where $x_{ij}, r \in \mathbb{Z}$, $r > 0$, $\gcd(r, x_{ij}) = 1$

This writing is unique, and $x \in \mathcal{O}_K \mathcal{O}_L \iff r = 1$.

Need to show: $r \mid d = \gcd(\operatorname{disc}_K, \operatorname{disc}_L)$

By symmetry, it suffices to show that $r \mid \operatorname{disc}_K$.

Consider the dual basis $\alpha_1^\vee, \dots, \alpha_n^\vee \in K$ of $\alpha_1, \dots, \alpha_n$.

i.e. $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j^\vee) = \delta_{ij}$

$\alpha_i^\vee \in \frac{1}{\operatorname{disc}_K} \mathcal{O}_K$ because $\alpha_i = \sum_j \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)\, \alpha_j^\vee$,

Now
$$\begin{pmatrix} \alpha_1^\vee \\ \vdots \\ \alpha_n^\vee \end{pmatrix} = \left(\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)\right)^{-1} \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

$$x\, \alpha_\ell^\vee = \sum_{i,j} \frac{x_{ij}}{r}\, \alpha_i \beta_j\, \alpha_\ell^\vee$$

$$\operatorname{Tr}_{KL/L}(x \alpha_\ell^\vee) = \operatorname{Tr}_{KL/L}\left(\sum_{i,j} \frac{x_{ij}}{r} \alpha_i \beta_j\, \alpha_k^\vee\right) = \sum_{i,j} \frac{x_{ij}}{r} \beta_j \underbrace{\operatorname{Tr}_{KL}(\alpha_i \alpha_\ell^\vee)}_{\delta_{ij}}$$

$\in \operatorname{Tr}_{KL/L}\left(\frac{1}{\operatorname{disc}_K} \mathcal{O}_{KL}\right)$ $\quad = \sum_j \frac{x_{\ell j}}{r} \beta_j$

$\subseteq \frac{1}{\operatorname{disc}_K} \mathcal{O}_L$ *

$\Rightarrow \operatorname{disc}_K \left(\sum_j \frac{x_{\ell j}}{r} \beta_j\right) \in \mathcal{O}_K$. Since $(\beta_1, \dots, \beta_n)$ is a basis of $\mathcal{O}_K / \mathbb{Z}$,

$\operatorname{disc}_K \cdot \frac{x_{\ell j}}{r} \in \mathbb{Z}$ $\forall j, \ell$ $\Rightarrow r \mid \operatorname{disc}_K$ □

* $\operatorname{Tr}_{KL/L}(x) = \operatorname{Tr}_{K/\mathbb{Q}}(x)$ if $x \in K \subseteq KL$. To show this, use $K \cap L = \mathbb{Q}$.

Application

Thm. $\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathbb{Z}[\zeta_N]$ $\forall N \geq 3$.

Pf: Induction on the number of prime factors of N.

- $N = p^N$ done
- $N = N_1 N_2$ with $\gcd(N_1, N_2) = 1$ and $N_1, N_2 \geq 3$.

  $\operatorname{disc}_{\mathbb{Q}(\zeta_{N_i})} \mid N_i^{\phi(N_i)}$ $\quad i = 1, 2$

  $\gcd(\operatorname{disc}_{\mathbb{Q}(\zeta_{N_1})}, \operatorname{disc}_{\mathbb{Q}(\zeta_{N_2})}) = 1$

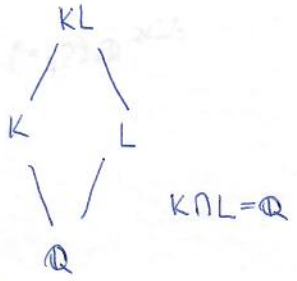
  $\mathbb{Q}(\zeta_{N_1}) \cap \mathbb{Q}(\zeta_{N_2}) = \mathbb{Q}$ $\Rightarrow$ $\mathcal{O}_{\mathbb{Q}(\zeta_{N_1 N_2})} = \mathcal{O}_{\mathbb{Q}(\zeta_{N_1})}\, \mathcal{O}_{\mathbb{Q}(\zeta_{N_2})}$

  $= \mathbb{Z}[\zeta_{N_1}]\, \mathbb{Z}[\zeta_{N_2}]$

  $= \mathbb{Z}[\zeta_{N_1 N_2}]$ □

Algebraic Number Theory, lecture 3–4

Computation of $\operatorname{disc}_{\mathbb{Q}(\zeta_N)}$



$K \cap L = \mathbb{Q}$

just do it for $N = p^n$ here. The general case will use ten following proposition:

$\operatorname{disc}_{KL} = \operatorname{disc}_K^{[L:\mathbb{Q}]} \cdot \operatorname{disc}_L^{[K:\mathbb{Q}]}$ if $\gcd(\operatorname{discs}_K, \operatorname{disc}_L) = 1$

Thm Let p be a prime, $n \geq 1$. Then $\operatorname{disc}_{\mathbb{Q}(\zeta_{p^n})} = \pm p^{p^{n-1}(pn-n-1)}$

where we have "$-$" if $p \equiv 3 \pmod 4$ or $p^n \equiv 4$, "$+$" otherwise.

Pf: $\operatorname{sgn}\left(\operatorname{disc}_{\mathbb{Q}(\zeta_{p^n})}\right) = (-1)^{\frac{\varphi(p^n)}{2}} = (-1)^{\frac{p^{n-1}(p-1)}{2}}$

$$\left|\operatorname{disc}_{\mathbb{Q}(\zeta_{p^n})}\right| = \left| N_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}\left(\Phi'_{p^n}(\zeta_{p^n})\right)\right|$$

$$\Phi_{p^n}(T) = \frac{T^{p^n}-1}{T^{p^{n-1}}-1} = \sum_{i=0}^{p-1} T^{p^{n-1}i}$$

$$\Phi'_{p^n}(\zeta_{p^n}) = \sum i \cdot p^{n-1} \cdot \zeta_{p^n}^{p^{n-1}\cdot i} \qquad \zeta_p = \zeta_{p^n}^{p^{n-1}}$$

- $p=2 \longrightarrow \Phi'_{2^n}(\zeta_{2^n}) = 2^{n-1} \cdot \zeta_{2^n}^{2^{n-1}}$

$$\left|N_{\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}}\left(\Phi'_{2^n}(\zeta_{2^n})\right)\right| = 2^{(n-1)2^{n-1}}$$

- $p \geq 3 \longrightarrow \Phi'_{p^n}(\zeta_{p^n}) = p^{n-1}\left(\sum_{i=1}^{p-1} i\, \zeta_{p^n}^{p^n\cdot(i-1)}\right)\zeta_{p^n}^{p^{n-1}-1}$

$$\left|N_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}\left(\Phi'_{p^n}(\zeta_{p^n})\right)\right| = p^{(n-1)p^{n-1}(p-1)}\left|N_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}\left(\underbrace{\sum_{i=1}^{p-1} i\cdot\zeta_p^{i-1}}_{\Phi'_p(\zeta_p)}\right)\right| =$$

$$= p^{(n-1)p^{n-1}(p-1)}\left|N_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}\left(\Phi'_p(\zeta_p)\right)\right|$$

$$\Phi'_p(\zeta_p) = \prod_{i=2}^{p-1}(\zeta_p - \zeta_p^i) = \zeta_p^{p-2}\prod_{i=1}^{p-2}(1-\zeta_p^i)$$

Note that $\forall i = 1, \dots, p-2$: $\left|N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p^i)\right| = p$ (constant term of $\Phi_p(T+1)$)

So $\left|N_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}\left(\Phi'_p(\zeta_p)\right)\right| = \prod_{i=1}^{p-2}\left|N_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}(1-\zeta_p^i)\right| =$

$$= N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p^i)^{[\mathbb{Q}(\zeta_{p^n}):\mathbb{Q}(\zeta_p)](p-2)}$$

$$= p^{(p-2)p^{n-1}}$$

$$\operatorname{disc}_{\mathbb{Q}(\zeta_{p^n})} = p^{(n-1)p^{n-1}(p-1)} \cdot p^{(p-2)p^{n-1}}$$

$$= p^{p^{n-1}(\underbrace{pn-p-n+1+p-2}_{pn-n-1})}$$

23.10.2017

Dedekind domains

Goal: generalise the notion of the unique factorisation in $\mathbb{Z}$ to $\mathcal{O}_K$.

In $\mathbb{Z}[\sqrt{-1}]$, which is a PID, we have the unique factorisation property.

But in $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ we have $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

but $2 \nmid (1+\sqrt{-5})$, $(1+\sqrt{-5}) \nmid 2$. $\Rightarrow$ we cannot have unique factorisation, even up to units.

Kummer: work with ideals instead of elements.

Def. A ring is noetherian if any of the following equivalent conditions holds:

1) $\forall I \subseteq A$ ideal is fin. generated as an A-module
2) Every nonempty subset of ideals in A contains a maximal element.
3) Every submodule of a fin. generated A-module is fin. generated.

Def. An integral domain A is a Dedekind domain if it is integrally closed, noetherian and every nonzero prime ideal is maximal (that is, $\dim(A) = 1$).

Ex. 1) PID $\Rightarrow$ Dedekind

PF: A PID. We already know that A is int. closed (last week), every ideal is fin. gen. (by one element).

Suffices to show: $\dim A = 1$. Let $\mathfrak{p} \subseteq A$ prime, $\mathfrak{p} \neq (0)$.

$\Rightarrow \mathfrak{p} = (p)$, $\forall a \in A \setminus \mathfrak{p}$: $p \nmid a$.

$(a, p) = (b)$

$\cup$ $\Rightarrow$ $b \mid p$. But p is primitive $\Rightarrow \exists c \in A$: $ac \equiv 1 \pmod{p}$

(p)

$\Rightarrow$ every $a \in A \setminus \mathfrak{p}$ is invertible mod $\mathfrak{p}$ $\Leftrightarrow$ $A/\mathfrak{p}$ is a field $\Leftrightarrow$ $\mathfrak{p}$ maximal. □

2) If A is Dedekind and $S \subseteq A$ is a multiplicative subset, then $S^{-1}A$ is Dedekind.

PF: A noe. $\Rightarrow$ $S^{-1}A$ noe.

A int. cl. $\Rightarrow$ $S^{-1}A$ i.cl. (exercise)

Correspondence between ideals $\Rightarrow \dim S^{-1}A = 1$.

□

Algebraic Number Theory, lecture 4

Prop. A Dedekind, $\mathrm{Frac}(A) = K$, L/K fin. extension & separable.

$B :=$ int. closure of A in L

$\Rightarrow$ B Dedekind.

$$\begin{array}{ccc} L & \supseteq & K \\ \cup & & \cup \\ B & \supseteq & A \end{array}$$

Cor. 1) $\forall K/\mathbb{Q}$ finite $\Rightarrow$ $\mathcal{O}_K$ is Dedekind

2) If C is an affine smooth curve over a field k, then $\Gamma(C, \mathcal{O}_C)$ is Dedekind.

$C \in \mathrm{Spec}$(integral closure of $k[x]$ in $k(C)$)

$\downarrow f$

$\mathbb{A}^1_k$

PROOF OF PROP.: STS: (1) B is a fin. gen. A-module. ($\Rightarrow$ B noetherian as an A-module $\Rightarrow$ noetherian as a B-module $\Rightarrow$ B is noetherian)

(2) $\forall (0) \neq \mathfrak{p} \subsetneq B$ prime is a maximal ideal.

(1): Let $e_1, \dots, e_n \in B$ which form a basis of L/K,

let $e_1^\vee, \dots, e_n^\vee$ be the dual basis wrt. $\mathrm{Tr}_{L/K}$

$\Rightarrow$ $B \subseteq M^\vee = \sum_{i=1}^n A e_i^\vee$ since $\forall x \in B: x = \sum_{i=1}^n x_i e_i^\vee$, $x_i = \mathrm{Tr}_{L/K}(\underbrace{x \cdot e_i}_{\in B}) \in A$

$\Rightarrow$ B is a fin. gen. A-module since A is noetherian.

(2): $(0) \neq \mathfrak{B} \in \mathrm{Spec}\, B$. $\mathfrak{p} := \mathfrak{B} \cap A$

Then $A/\mathfrak{p} \hookrightarrow B/\mathfrak{B}$ injective, and $B/\mathfrak{B}$ is integral over $A/\mathfrak{p}$.

Lemma: $A \subset B$ extension of int. domains, B integral over A.

Then A is a field if B is a field.

Pf: $\Rightarrow$: A is a field

$\exists x \in B \setminus \{0\}$: $x^n + a_1 x^{n-1} + \dots + a_n = 0$, $a_i \in A$, assume $a_n \neq 0$.

$\Rightarrow$ $\underbrace{a_n}_{\text{invertible in } A} = -x(x^{n-1} + \dots + a_1)$

$\Rightarrow$ invertible in B $\Rightarrow \forall x$ is invertible in B ✓

$\Leftarrow$: Assume B is a field.

$y \in A \setminus \{0\}$. $\Rightarrow \exists y^{-1} \in B$, $(y^{-1})^m + b_1 (y^{-1})^{m-1} + \dots + b_m = 0$, $b_i \in A$.

$\cdot y^{m-1}$

$\Rightarrow$ $y^{-1} = -(b_1 + \dots + b_m y^{m-1}) \in A$ □

Def. Let A be Dedekind, $\mathrm{Frac}(A) = K$.

A fractional ideal I is an A-submodule of K s.t. $\exists d \in A \setminus \{0\} : dI \subseteq A$.

(Basically there is a common denominator for the elements of I.)

Ex. $\frac{1}{d}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$,

$\mathbb{Z}\left[\frac{1}{p}\right]$ is not.

If I, J are frac. ideals of A, then $I + J = \{x \in K \mid x = a+b,\ a \in I,\ b \in J\}$,

$JI = I \cdot J = \left\{ x \in K \mid x = \sum_{i=1}^{m} a_i b_i,\ a_i \in I,\ b_i \in J \right\}$ are both frac. ideals. (easy to check)

Thm. Let A be Dedekind, then every nonzero ideal $I \subseteq A$ has a factorisation

$$I = \prod_{i=1}^{m} \mathfrak{p}_i^{a_i} \quad \text{where } \forall \mathfrak{p}_i \in \mathrm{Spec}(A) \setminus \{0\} \text{ and } a_i \in \mathbb{Z}_{>0}$$

This factorisation is unique up to order.

Ex. $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ $\qquad 6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

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

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

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

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

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

PROOF OF THM:

Lemma 1. A noetherian, then every nonzero ideal of A contains a product of nonzero prime ideals.

Pf: Let S be the set of all nonzero ideals of A that do not contain any product of nonzero prime ideals. NTS: $S = \emptyset$.

↯ Assume that S is nonempty.

A is noetherian $\Rightarrow$ S contains a max. element, say $I \subseteq A$

I is not prime and is nonzero

$\Rightarrow \exists\ a, b \in A \setminus I,\ ab \in I$.

$I + (a) \supsetneq I$, $I + (b) \supsetneq I$ and $I + (a) \supseteq \prod \mathfrak{p}_i$, $I + (b) \supseteq \prod \mathfrak{q}_j$

because of the maximality of I.

$$\Rightarrow \underbrace{(I + (a))(I + (b))}_{= I^2 + Ia + Ib + (ab) \subseteq I} \supseteq \prod \mathfrak{p}_i \prod \mathfrak{q}_j$$

↯

□

Algebraic Number Theory, lecture 4

Lemma 2. A Dedekind domain, $(0) \neq \mathfrak{p} \subseteq A$ prime ideal.

$\Rightarrow$ $\mathfrak{p}^{-1} := \{ x \in K = \mathrm{Frac}(A) \mid x\mathfrak{p} \subseteq A \}$ is a fractional ideal and $\mathfrak{p}^{-1}\mathfrak{p} = A$.

(The prime ideals are invertible in the semigroup of frac. ideals. later we will show that this semigroup is in fact a group.)

Pf: Easy: $\mathfrak{p}^{-1}$ fractional i. and $A \subseteq \mathfrak{p}^{-1}$.

$\rightarrow$ $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq A$

$\mathfrak{p}$ is maximal $\Rightarrow$ $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ or $\mathfrak{p}\mathfrak{p}^{-1} = A$.

Sts. $\mathfrak{p} \neq \mathfrak{p}\mathfrak{p}^{-1}$. $\lightning$ Assume $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$.

$\forall x \in \mathfrak{p}^{-1}$: $x\mathfrak{p} \subseteq \mathfrak{p}$ So if $\mathfrak{p} = \sum_{i=1}^{n} Ae_i$,

$x(e_1, \dots, e_n) = (e_1, \dots, e_n) \cdot C$ for some $C \in M_{n\times n}(A)$

$\rightarrow$ $(e_1, \dots, e_n)(x I_n - C) = 0$ $\Rightarrow$ $\det(x I_n - C) = 0$ $\Rightarrow$ x is integral /A.

A is int. closed $\Rightarrow$ $x \in A$. $\Rightarrow$ $\mathfrak{p}^{-1} \subseteq A$.

To get a contradiction, it suffices to produce an element $x \in \mathfrak{p}^{-1} \setminus A$.

Choose $b \in \mathfrak{p} \setminus \{0\}$, let r be the minimal integer s.t.

$\mathfrak{p} \supseteq (b) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where $(0) \neq \mathfrak{p}_i \in \mathrm{Spec}(A)$.

(The existence of a such r uses Lemma 1.)

$\Rightarrow$ $\exists\, i \in \{1, \dots, r\}$ s.t. $\mathfrak{p} \supseteq \mathfrak{p}_i$, because $\mathfrak{p}$ is prime.

We may assume $i = 1$. By the maximality of primes, $\mathfrak{p} = \mathfrak{p}_1$

By the minimality of r, we get $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (b)$

$\Rightarrow$ $\exists\, a \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ s.t. $a \notin (b)$. $\Leftrightarrow$ $\frac{a}{b} \notin A$.

$$\frac{a}{b} \cdot \mathfrak{p} \subseteq \frac{1}{b} \underbrace{\mathfrak{p}_2 \cdots \mathfrak{p}_r}_{a \in} \cdot \mathfrak{p}_1 \subseteq A$$

$\subseteq (b)$

By def. of $\mathfrak{p}^{-1}$, $\frac{a}{b} \in \mathfrak{p}^{-1}$ but $\frac{a}{b} \in A$. $\lightning$ $\Rightarrow$ $\mathfrak{p}\mathfrak{p}^{-1} = A$. $\square$

Now we claim to prove the theorem.

Existence. $\nexists \quad \emptyset \neq S = \{$ nonzero ideals which are not the product of prime ideals$\}$

Noetherian $\Rightarrow \exists\, I \in S$ maximal element

I is not prime, $A \neq I$ because A is the empty product.

By Zorn's lemma choose a prime $\mathfrak{p} \subseteq A$ s.t. $I \subsetneq \mathfrak{p}$.

Then $I \subsetneq \mathfrak{p}^{-1} I \subseteq \mathfrak{p}^{-1} \mathfrak{p} = A$ (Lemma 2)

By the maximality of I, $\mathfrak{p}^{-1} I = \prod_{i=1}^{r} \mathfrak{p}_i$

$$\Rightarrow \underbrace{\mathfrak{p} \cdot \mathfrak{p}^{-1} I}_{I} \subseteq \mathfrak{p} \cdot \prod_{i=1}^{r} \mathfrak{p}_i \quad \lightning$$

Uniqueness. Assume $\prod_{i=1}^{r} \mathfrak{p}_i = \prod_{j=1}^{s} \mathfrak{q}_j$ where $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ are nonzero prime ideals

$$\Rightarrow \prod_{j=1}^{s} \mathfrak{q}_j \subseteq \mathfrak{p}_1 \Rightarrow \exists j : \mathfrak{q}_j \subseteq \mathfrak{p}_1$$

Since $\mathfrak{q}_j$ is maximal, we have $\mathfrak{q}_j = \mathfrak{p}_1$.

$$\Rightarrow \prod_{i=2}^{r} \mathfrak{p}_i = \mathfrak{q}_1 \cdots \mathfrak{q}_{j-1} \mathfrak{q}_{j+1} \cdots \mathfrak{q}_s.$$

By induction on $\min\{r, s\}$ $\Rightarrow r = 1$ and each $\mathfrak{p}_i$ coincides with some $\mathfrak{q}_j$.

□

Corollary. Let A be a Dedekind domain.

Then A is a PID $\Leftrightarrow$ A is a UFD.

Proof: PID $\Rightarrow$ UFD. (true in general)

Suppose A is UFD. Sts: every nonzero prime ideal is principal, because all ideals are products of prime ideals.

Let $\mathfrak{p} \subset A$, $\mathfrak{p} \neq (0)$ be prime, let $x \in \mathfrak{p}$.

A is UFD $\Rightarrow$ $x = p_1 \cdots p_r$ with $\forall p_i \in A$ is primitive, i.e. $(p_i) \subseteq A$ is prime.

$$\left.\begin{array}{l} \underbrace{(p_1 \cdot \dots \cdot p_r)}_{(p_1) \cdots (p_r)} \subseteq \mathfrak{p} \end{array}\right\} \Rightarrow \exists i \text{ s.t. } (p_i) \subseteq \mathfrak{p} \overset{\dim A = 1}{\Longrightarrow} (p_i) = \mathfrak{p}.$$

□

Remark: There are UFDs which are not PIDs.

E.g. $k[X_1, \dots, X_n]$ is such a domain for $n \geq 2$.

Algebraic Number Theory, lecture 4 – 5

Notation. 1) If $I, \mathfrak{J}$ are fractional ideals of a Dedekind domain, we write $I \mid \mathfrak{J}$ if $\mathfrak{J} \subseteq I$.

2) If $(0) \neq (p) \subseteq A$ is a nonzero prime ideal, I fractional ideal

$v_p(I)$ = exponent of p appearing in I. (See the following corollary)

Corollary. Every fractional ideal I of a Dedekind domain A writes uniquely as $I = \prod_{i=1}^{r} p_i^{a_i}$, $a_i \in \mathbb{Z} \setminus \{0\}$. (So $a_i = v_{p_i}(I)$.) □

3) $\forall x \in K$: $v_p(x) := \begin{cases} \infty & \text{if } x = 0 \\ v_p((x)) & \text{if } x \neq 0 \end{cases}$

$(x) = A \cdot x \subseteq K$

Lemma. 1) If $I, \mathfrak{J}$ are fractional ideals, then $I \mid \mathfrak{J} \iff v_p(I) \leq v_p(\mathfrak{J})$ $\forall p$.

2) $I = \{ x \in K \mid v_p(x) \geq v_p(I) \ \ \forall p \}$

3) $v_p(I) + v_p(\mathfrak{J}) = v_p(I\mathfrak{J})$

4) $v_p(I + \mathfrak{J}) \geq \min(v_p(I), v_p(\mathfrak{J}))$ "$=$" holds if $v_p(I) \neq v_p(\mathfrak{J})$

3') $v_p(xy) = v_p(x) + v_p(y)$ $\forall x, y \in K$

4') $v_p(x+y) \geq \min(v_p(x), v_p(y))$ $\forall x, y \in K$ "$=$" holds if $v_p(x) \neq v_p(y)$. □

(In the second part of the course we shall study such functions as v_p.)

Ex. $A = \mathbb{C}[x]$, $p = (x-a)$, $a \in \mathbb{C}$ $\Rightarrow$ $v_p(f)$ is the vanishing order of f at $x = a$ $(f \in \mathbb{C}(x))$.

Recall. Thm. (U.F.L.) A Dedekind, I is a fractional ideal $\Rightarrow$ 26. 10. 2017

$I = \prod p_i^{a_i}$ unique prime decomposition, $a_i \in \mathbb{Z}$, p_i distinct prime ideals.

Moreover, $I \subseteq A \iff \forall a_i \geq 0$.

$I \subseteq \mathfrak{J} \iff v_p(I) \geq v_p(\mathfrak{J})$ $\forall p$ $\iff$ $I\mathfrak{J}^{-1} \subseteq A$.

Corollary. Consider a frac. ideal I, prime ideal $p \subseteq A$.

Then I/Ip is a 1-dim vect. space over $k(p) := A/p$.

Pf: $I \supsetneq Ip$. Take $x \in I \setminus Ip$, $\mathfrak{J} := Ip + xA$

$Ip \subsetneq \mathfrak{J} \subset I$ $\underset{\text{U.F.L.}}{\Longrightarrow}$ $\mathfrak{J} = I$ $\Rightarrow$ I/Ip is generated by 1 element. □

$\mathrm{Div}(A) = \{$ nonzero frac. ideals of $A\}$ is a free abelian group with a basis given by all nonzero prime ideals.

$\mathrm{Div}(A) \supseteq \mathrm{Prin}(A) = \{$ frac. ideals of the form xA, $x \in K^\times\}$

$Cl_A := \mathrm{Div}(A) / \mathrm{Prin}(A)$ ideal class group of A.

Cl_A is trivial $\Leftrightarrow$ A is a PID.

Ex. $A := \mathbb{C}[x,y] / y^2 - f(x)$, $f(x) = (x-a)(x-b)(x-c)$ where $(a-b)(b-c)(c-a) \neq 0$.

Spec (A) is the affine part of an elliptic curve E over $\mathbb{C}$

$Cl_A \cong E(\mathbb{C})$ $\rightarrow$ in this case, Cl_A is quite large.

Thm. (Minkowski) If A is the ring of integers of a number field, then Cl_A is finite.

PROOF LATER.

Lemma. (CRT) Let R be a ring, $I, J \subseteq R$ s.t. $I + J = R$ and $I \cap J = IJ$.

Then $R/IJ \xrightarrow{\varphi} R/I \oplus R/J$ is an isomorphism.

Pf: Injectivity: $\ker(R \to R/I \oplus R/J) = I \cap J = IJ$.

$\Rightarrow R/IJ \to R/I \oplus R/J$ has kernel 0.

Surjectivity: $\mathrm{Im}\,\varphi$ is an R-submodule of $R/I \oplus R/J$

$I + J = R \Rightarrow \exists\, s \in I,\ t \in J$: $s + t = 1 \Rightarrow \varphi(s) = (0,1) \in R/I \oplus R/J$

$\varphi(t) = (1,0) \in R/I \oplus R/J$

But $(1,0)$ and $(0,1)$ generate $R/I \oplus R/J$ as an R-module.

$\Rightarrow \mathrm{Im}\,\varphi = R/I \oplus R/J$. □

Prop. (CRT). Let A be a Dedekind domain, $Q_1, \dots, Q_r$ distinct maximal ideals of A. Then $\forall a_1, \dots, a_r \in \mathbb{Z}_{\geq 1}$:

$$A \Big/ \prod_{i=1}^{r} Q_i^{a_i} \xrightarrow{\sim} \prod_{i=1}^{r} A/Q_i^{a_i}$$

Pf: Induction on $r \geq 1$. $r = 1$ is a trivial case.

Suffices to show:

(1) $Q_1^{a_1} + \prod_{i=2}^{r} Q_i^{a_i} = A$

(2) $Q_1^{a_1} \cap \prod_{i=2}^{r} Q_i^{a_i} = Q_1^{a_1} \prod_{i=2}^{r} Q_i^{a_i}$.

For (1): $\nexists$ if $\mathfrak{p} \subseteq A$ is a nonzero prime ideal with $\mathfrak{p} \supseteq Q_1^{a_1} + \prod_{i=2}^{r} Q_i^{a_i}$

$\Rightarrow \mathfrak{p} \supseteq Q_1^{a_1}$ and $\mathfrak{p} \supseteq \prod_{i=2}^{r} Q_i^{a_i}$

$\Rightarrow \mathfrak{p} \supseteq Q_1$ and $\mathfrak{p} \supseteq Q_i$ $(2 \le i \le r)$. This is impossible since Q_1, Q_i are distinct maximal ideals of A. $\lightning$

$\Rightarrow Q_1^{a_1} + \prod_{i=2}^{r} Q_i^{a_i} = A$.

For (2): $LHS = \left\{ x \in K = \mathrm{Frac}(A) \;\middle|\; v_{Q_1}(x) \ge a_1 \text{ and } v_{Q_i}(x) \ge a_i \;\; \forall\, 2 \le i \le r \right\} =$

$= RHS$ □

Theorem. Let A be Dedekind, with only finitely many maximal ideals. Then A is a PID.

PROOF: Let $Q_1, \dots, Q_r$ be these maximal ideals of A.

A is Dedekind $\Rightarrow$ it suffices to show that all Q_i are principal.

CRT: $A \Big/ \prod_{i=1}^{r} Q_i^2 \xrightarrow{\sim} \prod_{i=1}^{r} A/Q_i^2$

Let $(\pi_1, 1, \dots, 1) \in \prod_{i=1}^{r} A/Q_i^2$ s.t. $\pi_1 \in Q_1 \setminus Q_1^2$.

Let x_1 be the preimage of $(\pi_1, 1, \dots, 1)$

$v_{Q_1}(x_1) = 1, \quad v_{Q_i}(x_1) = 0 \quad \forall\, i \ge 2$

$\Rightarrow (x_1) = Q_1$.

The same works for all Q_i. □

Corollary. For any Dedekind domain A and maximal ideal $\mathfrak{p} \subset A$ the localisation $A_{\mathfrak{p}}$ is a PID.

PF: There is only one maximal ideal, and $1 < \infty$. □

Lemma. Let A be a Dedekind domain, $S \subseteq A$ be a multiplicative subset and $A' := S^{-1}A$. Then:

(1) If $\mathfrak{p} \subseteq A$ is a nonzero prime ideal and $\mathfrak{p}' := \mathfrak{p} \cdot A'$, then $\mathfrak{p}' = A'$ if $S \cap \mathfrak{p} \neq \emptyset$ and $\mathfrak{p}'$ is a prime ideal if $S \cap \mathfrak{p} = \emptyset$. Moreover, we have $A'/\mathfrak{p}' \cong A/\mathfrak{p}$

(2) Let I be a fractional ideal of A with prime decomposition $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$. Put $I' := IA'$. Then I' has prime decomposition

$$I' = \prod_{\substack{i=1 \\ \mathfrak{p}_i' \cap S = \emptyset}}^{r} \mathfrak{p}_i'^{a_i} \quad \text{where } \mathfrak{p}_i' = \mathfrak{p}_i A'.$$

Pf: (1) Standard fact for localisation.

$A'/\mathfrak{p}' = S^{-1}\left(A/\mathfrak{p}\right)$ but if $S \cap \mathfrak{p} \neq \emptyset$, then the image of S in $A/\mathfrak{p}$ is already invertible, and we have $A'/\mathfrak{p}' = S^{-1}\left(A/\mathfrak{p}\right) = A/\mathfrak{p}$.

(2) Use $(I\mathfrak{J})A' = (IA') \cdot (\mathfrak{J}A')$ for frac. ideals $I, \mathfrak{J}$.

Apply this. □

Extensions of Dedekind domains

Motivation. $K/\mathbb{Q}$ finite. How to classify all the prime ideals of $\mathcal{O}_K$?

$$\begin{array}{ccccc} \mathfrak{p} & \subseteq & \mathcal{O}_K & - & K \\ | & & | & & | \\ (p) = \mathfrak{p} \cap \mathbb{Z} & - & \mathbb{Z} & - & \mathbb{Q} \end{array}$$

$\mathfrak{p} \cap \mathbb{Z} = (p) \iff p \cdot \mathcal{O}_K \subseteq \mathfrak{p}$

$\iff \mathfrak{p}$ appears in the prime decomposition of $p \cdot \mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$

General formulation.

Let A be a Dedekind domain with frac. field K, L/K a finite separable extension. Let B be the int. closure of A in L. We know that B is Dedekind as well.

$\mathfrak{p} \subseteq A$ prime ideal $\rightsquigarrow$ how to find the prime decomposition of $\mathfrak{p}B$?

$$\begin{array}{ccccc} & & B & - & L \\ & \diagup\!\diagdown & | & & | \\ \mathfrak{p} & \subseteq & A & - & K \end{array}$$

Assume $pB = \prod_{i=1}^{g} Q_i^{e_i}$ is the prime decomposition of pB, Q_i distinct, $e_i \geq 1$.

Prop. (1) $\forall 1 \leq i \leq g$ $\quad k(Q_i) := B/Q_i$ is a finite extension of $k(p) := A/p$.

(2) If $n := [L:K]$ and $f_i := [k(Q_i) : k(p)]$ then $\sum_{i=1}^{g} e_i f_i = n$

PROOF: Reduction to the case when A is a PID.

Put $A' := A_p$, $B' := BA_p = B_p$.

Then the prime decomposition does not change (previous lemma):

$$pB' = \prod_{i=1}^{g} Q_i'^{e_i} \quad \text{where } Q_i' = Q_i B' \text{ is a prime ideal of } B',$$

and $k(Q_i) \cong k(Q_i')$

Up to replacing A by A' and B by B' we may assume that A is a PID.

We know that B is a torsion-free, finite A-module.

$\Rightarrow$ B is a free A-module of rank n because A is a PID.

B/pB is a vector space over the residue field $k(p) = A/p$ of dim n.

$$B/pB = B/\prod_{i=1}^{g} Q_i^{e_i} \underset{CRT}{\cong} \prod_{i=1}^{g} B/Q_i^{e_i}$$

$$n = \dim_{k(p)}\left(B/pB\right) = \sum_{i=1}^{g} \dim_{k(p)}\left(B/Q_i^{e_i}\right)$$

But $B/Q_i^{e_i}$ admits a filtration $B/Q_i^{e_i} \supseteq Q_i/Q_i^{e_i} \supseteq Q_i^2/Q_i^{e_i} \supseteq \dots \supseteq Q_i^{e_i-1}/Q_i^{e_i} \supseteq 0$.

with subquotient Q_i^j/Q_i^{j+1} $\quad (0 \leq j \leq e-1)$

$$\dim_{k(p)} B/Q_i^{e_i} = \sum_{j=0}^{e-1} \dim_{k(p)} \underbrace{Q_i^j/Q_i^{j+1}}_{\text{1-dimensional over } B/Q_i = k(Q_i)} = e_i \cdot \dim_{k(p)} k(Q_i) = e_i f_i.$$

□

Def. In the situation above,

$e(Q_i|p) := e_i$ is the ramification index of Q_i above p

$f(Q_i|p) := f_i$ is the residue degree of Q_i above p

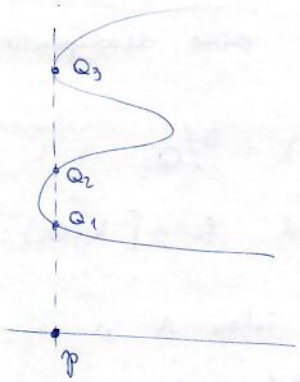
We say that

- Q_i is unramified above p if $e_i = 1$,
- p is unramified in B (or L) if $e_i = 1$ $\forall 1 \leq i \leq g$.
- p splits in B (or L) if $e_i = f_i = 1$ $\forall 1 \leq i \leq g$.
- p is inert in B if $g = 1$ and $e(Q_1|p) = 1$ i.e. pB is prime in B

Spec B

$\mathfrak{p}B = Q_1 Q_2 Q_3^2$

$\mathfrak{p} \in \operatorname{Spec} A$



Theorem. (Kummer) Let $\alpha \in B$ with minimal polynomial $f(x) \in A[x]$.

Suppose that $B/\mathfrak{p}B = k(\mathfrak{p})[\bar{\alpha}]$ where $\bar{\alpha} \in B/\mathfrak{p}B$ is the image of α,

and $f(x) \equiv \prod_{i=1}^{g} h_i^{e_i}(x) \pmod{\mathfrak{p}A[x]}$ where $e_i \geq 1$, $h_i(x) \in A[x]$ are monic polynomials whose images in $k(\mathfrak{p})[x]$ are irreducible and distinct.

Then $Q_i := \mathfrak{p}B + h_i(\alpha)B$ is a max. ideal of B

and $\mathfrak{p}B = Q_1^{e_1} \cdots Q_g^{e_g}$ is the prime decomposition of $\mathfrak{p}B$,

and $f(Q_i \mid \mathfrak{p}) = \deg(h_i)$

Remark. The condition $B/\mathfrak{p}B = k(\mathfrak{p})[\bar{\alpha}]$ is weaker than $B = A[\alpha]$.

For instance, if $\mathfrak{p} \nmid N_{L/K}(f'(\alpha))$, then we have $B/\mathfrak{p}B = k(\mathfrak{p})[\bar{\alpha}]$.

(f irr. and $\deg f = n$)

PF. REM:
Up to replacing A by $A_{\mathfrak{p}}$ we may assume A is PID.

$$\begin{array}{ccc} A[\alpha] & \subseteq & B \quad - \quad L \\ & \searrow & | \qquad | \\ & & A \quad - \quad K \end{array}$$

One can define the discriminant of B/A by using a basis of B (as an A-mod.)

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \cdot N_{L/K}(f'(\alpha))$$

$\operatorname{disc}_{B/A} \mid \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1})$ so if $\mathfrak{p} \nmid N_{L/K}(f'(\alpha))$, then

$$(\operatorname{disc}_{B/A}) \cdot A_{\mathfrak{p}} = \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) A_{\mathfrak{p}} = A_{\mathfrak{p}}$$

$$\Rightarrow (A[\alpha]) A_{\mathfrak{p}} = B_{\mathfrak{p}}. \Rightarrow B/\mathfrak{p}B = B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} = A_{\mathfrak{p}}[\alpha]/\mathfrak{p}A_{\mathfrak{p}}[\alpha] = k(\mathfrak{p})[\bar{\alpha}].$$

Algebraic Number Theory, lecture 5-6

PROOF OF THM:

$$B/Q_i = B/(pB + h_i(\alpha)B) = k(p)[\bar{\alpha}]/(\bar{h}_i(\bar{\alpha})) = k(p)[x]/(\bar{f}(x), \bar{h}_i(x)) =$$

$$= k(p)[x]/(\bar{h}_i) \text{ which is a field since } \bar{h}_i \text{ is irreducible.}$$

$\Rightarrow Q_i \subseteq B$ is indeed maximal.

For the prime decomposition of pB, consider

$$B/pB = k(p)[\bar{\alpha}] = k(p)[x]/(\bar{f}(x)) = k(p)[x]/\left(\prod_{i=1}^{g} \bar{h}_i^{e_i}\right) = \prod_{i=1}^{g} k(p)[x]/\bar{h}_i^{e_i} =$$

$$= \prod_{i=1}^{g} k(p)[\bar{\alpha}]/\bar{h}_i^{e_i}(\bar{\alpha}) \cong \prod_{i=1}^{g} B/(pB + h_i^{e_i}(\alpha)B)$$

To see $pB = \prod_{i=1}^{g} Q_i^{e_i}$ it suffices to show $\underbrace{Q_i^{e_i}}_{(pB + h_i(\alpha)B)^{e_i}} = pB + h_i^{e_i}(\alpha)B$

$\subseteq$ is clear.

To finish the proof, it suffices to see that

$$\dim_{k(p)}\left(B/Q_i^{e_i}\right) = \dim_{k(p)}\left(B/(pB + h_i^{e_i}(\alpha)B)\right)$$

LHS $= e_i[k(Q_i) : k(p)] = e_i f_i$

RHS $= \dim_{k(p)} k(p)[\bar{\alpha}]/(\bar{h}_i^{e_i}(\bar{\alpha})) =$

$= \dim_{k(p)} k(p)[x]/(\bar{f}(x), \bar{h}_i^{e_i}(x)) =$

$= \dim_{k(p)} k(p)[x]/(\bar{h}_i^{e_i}(x)) = e_i \cdot \dim_{k(p)} \underbrace{k(p)[x]/h_i(x)}_{\deg h_i = f_i} \Big\} = e_i f_i$

□

Ex. $K = \mathbb{Q}(\sqrt{D})$, D is a square-free integer 30.10.2017

$p \in \mathbb{Z}$ rational prime

(1) p is ramified in K, i.e. $p\mathcal{O}_K = \mathfrak{p}^2$ iff $p \mid \text{disc}_K = \begin{cases} 4D & D \equiv 2,3 \ (4) \\ D & D \equiv 1 \ (4) \end{cases}$

In particular, 2 is ramified in $K \iff D \equiv 2,3 \ (4)$

(2) If $p \geq 3$ and p is unramified in K (i.e. $p \nmid D$), then p splits in K iff $\left(\frac{D}{p}\right) = 1$.

(3) When $D \equiv 1 \ (4)$: 2 splits in K iff $D \equiv 1 \ (8)$

PROOF: Recall that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $\alpha = \begin{cases} \frac{1+\sqrt{D}}{2} & D \equiv 1 \ (4) \\ \sqrt{D} & D \equiv 2,3 \ (4) \end{cases}$

The min. poly of α is $f(x) = \begin{cases} x^2 - x + \frac{1-D}{4} & D \equiv 1 \ (4) \\ x^2 - D & D \equiv 2,3 \ (4) \end{cases}$

For the proof of (1):

p ramified in $K \overset{\text{Kummer}}{\iff} \bar{f}[x] \in \mathbb{F}_p[x]$ has multiple roots

$\iff p \mid \text{disc}_K = (\alpha - \overline{\alpha})^2 = \begin{cases} D & D \equiv 1 \ (4) \\ 4D & D \equiv 2,3 \ (4) \end{cases}$

(2): Assume p is odd and unram in K.

$\Rightarrow p \nmid \text{disc}_K$. Then p splits in $K \iff \bar{f}(x)$ has two distinct roots in $\mathbb{F}_p$.

So if $\bar{f}(x) = (x-a)(x-b)$ with $a, b \in \mathbb{F}_p$, then $\text{disc}_K = (a-b)^2$

$$\left(\frac{D}{p}\right) = \left(\frac{\text{disc}_K}{p}\right) = 1$$

Conversely, if $\left(\frac{D}{p}\right) = 1$ then $D \equiv c^2 \ (p)$, $p \nmid c$.

Then $\frac{1 \pm c}{2}$ (resp. $\pm c$) are two distinct roots of $\bar{f}(x)$ in $\mathbb{F}_p$

$\overset{\text{Kummer}}{\Longrightarrow}$ p splits in K.

(3): If $D \equiv 1 \ (8)$, $\Rightarrow f(x) \equiv x^2 + x = x(x+1) \pmod 2$ $\overset{\text{Kummer}}{\Rightarrow}$ 2 splits.

If $D \equiv 5 \ (8) \Rightarrow f(x) \equiv x^2 + x + 1 \pmod 2$, which is monic. irred. poly. of deg. 2. in $\mathbb{F}_2[x]$ $\Rightarrow$ 2 is inert in K. □

Example. $K = \mathbb{Q}(\sqrt[3]{2})$ $\mathcal{O}_K = \mathbb{Z}[\alpha]$, $f(x) = x^3 - 2 = 0$.

$\text{disc}_K = -3^3 \cdot 2^2 = -N_{K/\mathbb{Q}}(f'(\alpha))$

$\bar{f}(x) \pmod p$ has multiple roots $\iff p \mid |N_{K/\mathbb{Q}}(f'(\alpha))| = \left| \prod_{i \neq j} (\alpha_i - \alpha_j)^2 \right| \iff$

$\iff p = 2, 3$

If $p = 5 \equiv 2 \pmod 3$: $3 \nmid (p-1)$ so the map $a \mapsto a^3$ induces an isomorphism $\mathbb{F}_p^\times \xrightarrow{\sim} \mathbb{F}_p^\times$

Algebraic Number Theory, lecture 6

$\to \exists a \in \mathbb{F}_p^\times$ s.t. $a^3 = 2$ in $\mathbb{F}_p$

$\Rightarrow f(x) \equiv (x-a)(x^2 + ax + a^2) \pmod 5$

We can take $a = 3$ for $p = 5$ ($3^3 \equiv 27 \equiv 2 \pmod 5$)

$x^2 + ax + a^2 \equiv x^3 - 2x - 1 = (x-1)^2 - 2$ in $\mathbb{F}_5[x]$

$\left(\frac{2}{5}\right) = -1 \Rightarrow (x-1)^2 - 2$ is irreducible.

So: $5\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2$, $f(\mathfrak{p}_1 | 5) = 1$, $f(\mathfrak{p}_2 | 5) = 2$.

This argument can be generalised to arbitrary $p \equiv 2 \pmod 3$.

$p = 7$: $x^3 - 2$ is irreducible in $\mathbb{F}_7[x] \Rightarrow 7\mathcal{O}_K$ is prime in $\mathcal{O}_K$

Theorem. Let $K/\mathbb{Q}$ be a finite extension, $p \in \mathbb{Z}$ be a prime. TFAE:

(1) p is unramified in K

(2) The ring $\mathcal{O}_K/p\mathcal{O}_K$ is reduced (i.e. $\mathcal{O}_K/p\mathcal{O}_K$ has no nilpotent elements)

(3) The $\mathbb{F}_p$-bilinear pairing $\overline{Tr}_{K/\mathbb{Q}}: \mathcal{O}_K/p\mathcal{O}_K \times \mathcal{O}_K/p\mathcal{O}_K \to \mathbb{F}_p$

$(x, y) \longmapsto Tr_{K/\mathbb{Q}}(xy) \bmod p$

is non-degenerate.

(4) $p \nmid \mathrm{disc}_K$.

Pf: (1) $\Leftrightarrow$ (2): If $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p}|p)}$ then $\mathcal{O}_K/p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathcal{O}_K/\mathfrak{p}^{e(\mathfrak{p}|p)}$

$\mathcal{O}_K/p\mathcal{O}_K$ reduced $\Leftrightarrow \forall \mathfrak{p}|p$: $\mathcal{O}_K/\mathfrak{p}^{e(\mathfrak{p}|p)}$ is reduced

$\Leftrightarrow e(\mathfrak{p}|p) = 1 \quad \forall \mathfrak{p}|p$.

(2) $\Leftrightarrow$ (3): If $x \in \mathcal{O}_K/p\mathcal{O}_K$ is nilpotent then xy is nilp. $\forall y \in \mathcal{O}_K/p\mathcal{O}_K$

$\Rightarrow \overline{Tr}_{K/\mathbb{Q}}(xy) = 0 \Rightarrow \overline{Tr}_{K/\mathbb{Q}}$ is degenerate

Converse: if $\mathcal{O}_K/p\mathcal{O}_K$ is reduced then $\mathcal{O}_K/p\mathcal{O}_K = \bigoplus_{\mathfrak{p}|p} k(\mathfrak{p})$

$\mathbb{F}_p$ is perfect. $k(\mathfrak{p})/\mathbb{F}_p$ is fin. separable,

$Tr_{k(\mathfrak{p})/\mathbb{F}_p}$ is non-degenerate $\Rightarrow \overline{Tr}_{K/\mathbb{Q}} = \bigoplus_{\mathfrak{p}|p} Tr_{k(\mathfrak{p})/\mathbb{F}_p}$ non-degen.

(3) $\Leftrightarrow$ (4): $(\alpha_i)_{1 \le i \le n}$ integral basis, $\bar{\alpha}_i \in \mathcal{O}_K/p\mathcal{O}_K$ reductions

$\overline{Tr}_{K/\mathbb{Q}}$ induces a map $\Phi: \mathcal{O}_K/p\mathcal{O}_K \to \left(\mathcal{O}_K/p\mathcal{O}_K\right)^\vee := \mathrm{Hom}_{\mathbb{F}_p}\left(\mathcal{O}_K/p\mathcal{O}_K, \mathbb{F}_p\right)$

Let $(\alpha_i^\vee)_{1 \le i \le n}$ be the basis of $\left(\mathcal{O}_K/p\mathcal{O}_K\right)^\vee$ dual to $(\alpha_i)_{1 \le i \le n}$.

Then the matrix of $\left(\overline{\phi}(\overline{\alpha_i})\right)_{1\le i\le n}$ under $(\overline{\alpha_i}^{\vee})$ is given by

$$\left(\overline{\mathrm{Tr}}_{K/\mathbb{Q}}(\overline{\alpha_i}\overline{\alpha_j})\right)_{1\le i,j\le n}$$

$\overline{\mathrm{Tr}}_{K/\mathbb{Q}}$ nondeg $\Leftrightarrow$ $\overline{\phi}$ is an iso $\Leftrightarrow$ $\det\left(\overline{\mathrm{Tr}}_{K/\mathbb{Q}}(\overline{\alpha_i}\overline{\alpha_j})\right) \neq 0$ in $\mathbb{F}_p$

$\Leftrightarrow$ $\mathrm{disc}_K \not\equiv 0 \pmod p$ □

Different and Discriminant

L/K finite extension of number fields

$$\begin{array}{ccccc} \mathfrak{B} & - & \mathcal{O}_L & - & L \\ | & & | & & | \\ \mathfrak{B}\cap\mathcal{O}_K = \mathfrak{p} & - & \mathcal{O}_K & - & K \end{array}$$

Define $N_{L/K}(\mathfrak{B}) = \mathfrak{p}^{f(\mathfrak{B}|\mathfrak{p})} = \mathfrak{p}^{\dim_{k(\mathfrak{p})} k(\mathfrak{B})}$

Define $N_{L/K}(\mathfrak{J}) = \prod_{\mathfrak{B}} N_{L/K}(\mathfrak{B})^{a_{\mathfrak{B}}}$ where $\mathfrak{J} = \prod_{\mathfrak{B}} \mathfrak{B}^{a_{\mathfrak{B}}}$ is a frac. ideal of $\mathcal{O}_L$.

Lemma. (1) $\forall\, \mathfrak{J}_1, \mathfrak{J}_2$: $N_{L/K}(\mathfrak{J}_1\mathfrak{J}_2) = N_{L/K}(\mathfrak{J}_1)\, N_{L/K}(\mathfrak{J}_2)$

(2) $\forall$ frac. ideal I of $\mathcal{O}_K$: $N_{L/K}(I\mathcal{O}_L) = I^{[L:K]}$

(3) If M/L is a further finite extension and Q is a frac. ideal of $\mathcal{O}_M$ then $N_{M/K}(Q) = N_{L/K}\left(N_{M/L}(Q)\right)$

Proof. (1) trivial

(2) WMA $I = \mathfrak{p}$ is prime in $\mathcal{O}_K$, $\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{e(\mathfrak{B}|\mathfrak{p})}$

$$N_{L/K}(I\mathcal{O}_L) = \prod N_{L/K}(\mathfrak{B})^{e(\mathfrak{B}|\mathfrak{p})} = \prod \mathfrak{p}^{e(\mathfrak{B}|\mathfrak{p})f(\mathfrak{B}|\mathfrak{p})} = \mathfrak{p}^n.$$

(3) WMA Q is prime in $\mathcal{O}_M$.

$$\begin{array}{ccc} Q & - & M \\ | & & | \\ \mathfrak{B} & - & L \\ | & & | \\ \mathfrak{p} & - & K \end{array}$$

$$N_{M/K}(Q) = \mathfrak{p}^{f(Q|\mathfrak{p})}$$

$$N_{L/K}\, N_{M/L}(Q) = N_{L/K}\left(\mathfrak{B}^{f(Q|\mathfrak{B})}\right) = \mathfrak{p}^{f(Q|\mathfrak{B})f(\mathfrak{B}|\mathfrak{p})}$$

$$f(Q|\mathfrak{p}) = \dim_{k(\mathfrak{p})} k(Q) =$$

$$= \dim_{k(\mathfrak{p})} k(\mathfrak{B}) \cdot \dim_{k(\mathfrak{B})} k(Q)$$

$$= f(\mathfrak{B}|\mathfrak{p})\, f(Q|\mathfrak{B}).$$

□

Special case. $K = \mathbb{Q}$.

For any frac. ideal $\mathfrak{J}$ of $\mathcal{O}_L$ we denote by $N_{L/\mathbb{Q}}(\mathfrak{J})$ the unique element of $\mathbb{Q}_{>0}$ that generates $N_{L/\mathbb{Q}}(\mathfrak{J})$

Algebraic Number Theory, lecture 6

Lemma. For any $I \subseteq \mathcal{O}_L$ and frac. ideal $\mathfrak{F}$ we have

$$N_{L/\mathbb{Q}}(I) = [\mathfrak{F} : I\mathfrak{F}]$$

Pf: Let $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$ prime decomp., $a_i > 0$.

Proceed by induction on $m = \sum_{i=1}^{r} a_i \geq 1$.

If $m = 1$: $I = \mathfrak{p}$ prime $\Rightarrow$ $\mathfrak{F}/\mathfrak{p}\mathfrak{F}$ is a one-dim. vector space over $k(\mathfrak{p})$.

$$\left|\mathfrak{F}/\mathfrak{p}\mathfrak{F}\right| = |k(\mathfrak{p})| = p^{f(\mathfrak{p}|p)} = N_{L/\mathbb{Q}}(\mathfrak{p}).$$

In general, we write $I = \mathfrak{p} \cdot I'$ s.t. $m' = m - 1$.

$$\left|\mathfrak{F}/I\mathfrak{F}\right| = [\mathfrak{F} : I\mathfrak{F}] = \underbrace{[\mathfrak{F} : I'\mathfrak{F}] \cdot [I'\mathfrak{F} : \mathfrak{p}I'\mathfrak{F}]}_{\text{induction}} =$$

$$= N_{L/\mathbb{Q}}(I') \cdot N_{L/\mathbb{Q}}(\mathfrak{p}) = N_{L/\mathbb{Q}}(I)$$

□

Let L/K be as above.

Def. Put $\delta_{L/K}^{-1} := \{x \in L \mid \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_L \ \ \forall y \in \mathcal{O}_L\}$

Clear: $\delta_{L/K}^{-1}$ is a frac. ideal of $\mathcal{O}_L$ s.t. $\delta_{L/K}^{-1} \supseteq \mathcal{O}_L$.

Define the <u>different</u> of L/K as $\delta_{L/K} := \left(\delta_{L/K}^{-1}\right)^{-1} \subseteq \mathcal{O}_L$

Notation. If $K = \mathbb{Q}$: $\delta_L = \delta_{L/\mathbb{Q}}$.

Prop. (1) $N_{K/\mathbb{Q}}(\delta_K) = |\mathrm{disc}_K|$

(2) If M/L is a further finite extension then $\delta_{M/K} = \left(\delta_{M/L}\right)\left(\delta_{L/K} \cdot \mathcal{O}_M\right)$

Pf: (1) $\alpha_1, \ldots, \alpha_n$ integral basis of K

$\alpha_1^\vee, \ldots, \alpha_n^\vee$ dual basis w.r.t. $\mathrm{Tr}_{K/\mathbb{Q}}$

By definition: every $x \in K$ writes as $x = \sum x_i \alpha_i^\vee$,

where $x_i = \mathrm{Tr}_{K/\mathbb{Q}}(x\alpha_i)$

$$\left.\begin{aligned} x \in \delta_K^{-1} &\iff \forall y \in \mathcal{O}_K : \mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z} \\ &\iff \mathrm{Tr}_{K/\mathbb{Q}}(x\alpha_i) \in \mathbb{Z} \qquad \left(\mathcal{O}_K = \textstyle\sum \alpha_i \mathbb{Z}\right) \\ &\iff x \in \textstyle\sum \mathbb{Z}\alpha_i^\vee \end{aligned}\right\} \Rightarrow \delta_K^{-1} = \sum \mathbb{Z}\alpha_i^\vee$$

$$N_{K/\mathbb{Q}}(\delta_K) = [\delta_K^{-1} : \mathcal{O}_K] = \left[\sum \mathbb{Z}\alpha_i^\vee \cdot \sum \mathbb{Z}\alpha_i\right] = \qquad \alpha_i = \sum_j \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\alpha_j^\vee$$

$$= \left|\det\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)\right| = |\mathrm{disc}_K|$$

(2) $x \in \delta_{M/K}^{-1} \iff \forall y \in \mathcal{O}_M \ \ \underbrace{\mathrm{Tr}_{M/K}(xy)}_{\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}} \in \mathcal{O}_K$

$\iff \mathrm{Tr}_{M/L}(xy) \in \delta_{L/K}^{-1} \ \ \forall y \in \mathcal{O}_M$

($\mathrm{Tr}_{M/L}$: L-linear; $\delta_{L/K}^{-1}$: frac. ideal of $\mathcal{O}_L$)

M
|
L
|
K

$\Leftrightarrow \mathrm{Tr}_{M/L}(xy \cdot \delta_{L/K}) \subseteq \mathcal{O}_L \quad \forall y \in \mathcal{O}_M$

$\Leftrightarrow x\,\delta_{L/K} \subseteq \delta_{M/L}^{-1}$

$\Leftrightarrow x \in \delta_{M/L}^{-1} \cdot \delta_{L/K}^{-1}$

$\delta_{M/K}^{-1} = (\delta_{M/L}^{-1})(\delta_{L/K}^{-1}\mathcal{O}_M) \Leftrightarrow \delta_{M/K} = \delta_{M/L}(\delta_{L/K}\mathcal{O}_M)$ □

Def. For any fin. extension of number fields L/K we define the <u>relative discriminant</u> as the ideal $\underline{\mathrm{disc}_{L/K}} := N_{L/K}(\delta_{L/K})$.

Remark. By the same argument as in the case $K=\mathbb{Q}$, we see that a prime $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in L/K iff $\mathfrak{p} \nmid \mathrm{disc}_{L/K}$.

Corollary. We have $|\mathrm{disc}_L| = |\mathrm{disc}_K|^{[L:K]} \cdot N_{K/\mathbb{Q}}(\mathrm{disc}_{L/K})$

Pf: $\delta_L = \delta_{L/K} \cdot (\delta_K \mathcal{O}_L)$

Taking norms, we get:

$|\mathrm{disc}_L| = N_{L/\mathbb{Q}}(\delta_{L/K}) \cdot N_{L/\mathbb{Q}}(\delta_K \cdot \mathcal{O}_L)$

$= N_{K/\mathbb{Q}}(\mathrm{disc}_{L/K}) \cdot N_{K/\mathbb{Q}}(\delta_K)^{[L:K]}$ □

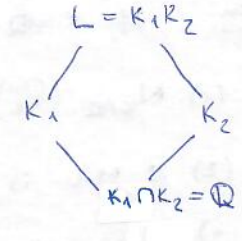
Prop. Let K_1, K_2 be number fields, $K_1 \cap K_2 = \mathbb{Q}$, $L = K_1K_2$, $(K_1, K_2 \subseteq \mathbb{C})$

Then: (1) $\delta_{K_2}\mathcal{O}_L \subseteq \delta_{L/K_1}$

(2) disc_L divides $\mathrm{disc}_{K_1}^{[K_2:\mathbb{Q}]} \cdot \mathrm{disc}_{K_2}^{[K_1:\mathbb{Q}]}$

(3) If $\gcd(\mathrm{disc}_{K_1}, \mathrm{disc}_{K_2}) = 1$ then

$|\mathrm{disc}_L| = |\mathrm{disc}_{K_1}|^{[K_2:\mathbb{Q}]} \cdot |\mathrm{disc}_{K_2}|^{[K_1:\mathbb{Q}]}$



Cor. In the above situation, a rational prime p is unramified in both K_1 and K_2 iff p is unramified in $L = K_1K_2$.

Pf: (2). □

PROOF OF PROP: (1): $(\beta_j)_{1\le j\le n}$ is an integral basis of K_2, $(\beta_j^\vee)_{1\le j\le n}$ dual basis,

Every $x \in K_1K_2 = L$ writes as $x = \sum_{j=1}^{n} x_j \beta_j^\vee$, $x_j = \mathrm{Tr}_{L/K_1}(x\beta_j) \in K_1$

If $x \in \delta_{L/K_1}^{-1}$ then $\forall y \in \mathcal{O}_L \supseteq \mathcal{O}_{K_1}\mathcal{O}_{K_2}$:

$\mathrm{Tr}_{L/K_1}(xy) \in \mathcal{O}_{K_1} \Rightarrow x_j \in \mathcal{O}_{K_1}$

$\Rightarrow \delta_{L/K_1}^{-1} \subseteq \sum_{j=1}^{n} \mathcal{O}_{K_1}\beta_j^\vee \subseteq \mathcal{O}_{K_1}\delta_{K_2}^{-1} \subseteq \delta_{K_2}^{-1}\mathcal{O}_L$. Recall that $\delta_{K_2}^{-1} = \sum_j \mathbb{Z}\beta_j^\vee$

$\Rightarrow \delta_{K_2}\mathcal{O}_L \subseteq \delta_{L/K_1}$.

(2): Follows from taking $N_{L/\mathbb{Q}}$ on both sides.

(3): If $\gcd(\mathrm{disc}_{K_1}, \mathrm{disc}_{K_2}) = 1 \Rightarrow \mathcal{O}_{K_1}\mathcal{O}_{K_2} = \mathcal{O}_L$ (seen last week).

$\Rightarrow \delta_{L/K_1} = \delta_{K_2}\mathcal{O}_L$ by argument of (1) $\Rightarrow \delta_L = (\delta_{K_1}\mathcal{O}_L)(\delta_{K_2}\mathcal{O}_L)$ in (2). □

We have implicitly used the following in the proof:

if $(\beta_1, \dots, \beta_m)$ is a basis of $K_2/\mathbb{Q}$, then it is also a basis of L/K_1.

This is WRONG. This holds only if $[L:K_1] = [K_2:\mathbb{Q}]$, which is not true in general. Counterexample: $K_1 = \mathbb{Q}(\sqrt[3]{2})$, $K_2 = \mathbb{Q}(\sqrt[3]{2}\cdot\zeta_3)$,

$L = K_1K_2 = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, $2 = [L:K_1] \neq [K_2:\mathbb{Q}] = 3$.

In general:

$K_1 \otimes_{\mathbb{Q}} K_2 = \prod_{i=1}^{r} L_i$ product of fields, where L is one of the factors.

Ex.

$K_1 \otimes_{\mathbb{Q}} K_2 \cong K_1[x]/(x^3-2) = K_1[X]/(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}\,x+\sqrt[3]{4}) \cong K_1 \oplus L$.

Let $p: K_1 \otimes_{\mathbb{Q}} K_2 \longrightarrow L$ be the canonical projection.

Then $\mathcal{O}_{K_1\otimes K_2} := \prod_{i=1}^{r} \mathcal{O}_{L_i}$ is the integral closure of $\mathbb{Z}$ in $K_1 \otimes K_2$.

$$\delta^{-1}_{K_1\otimes K_2/K_1} := \prod_{i=1}^{r} \delta^{-1}_{L_i/K_1} = \left\{ x \in K_1 \otimes K_2 \;\middle|\; \mathrm{Tr}_{K_1\otimes K_2/K_1}(xy) \in \mathcal{O}_{K_1} \;\; \forall y \in \mathcal{O}_{K_1\otimes K_2} \right\}$$

$$\mathrm{Tr}_{K_1\otimes K_2/K_1} = \bigoplus_{i=1}^{r} \mathrm{Tr}_{L_i/K_1}$$

$$\begin{array}{ccc} \mathcal{O}_{K_1\otimes_{\mathbb{Q}}K_2} & \xrightarrow{\;p\;} & \mathcal{O}_L \\ \cup & & \cup \\ \mathcal{O}_{K_1}\otimes_{\mathbb{Z}}\mathcal{O}_{K_2} & \longrightarrow & \mathcal{O}_{K_1}\cdot\mathcal{O}_{K_2} \end{array}$$

Let $(\beta_1, \dots, \beta_n)$ be an int. basis of K_2 with dual basis $(\beta_1^\vee, \dots, \beta_n^\vee)$.

Then $K_1 \otimes_{\mathbb{Q}} K_2$ is a vector space with basis $(1\otimes\beta_1^\vee, \dots, 1\otimes\beta_n^\vee)$ over the field K_1.

$\forall x \in K_1 \otimes K_2$ writes uniquely as $x = \sum_{j=1}^{m} x_j \otimes \beta_j^\vee$

where $x_j = \mathrm{Tr}_{K_1\otimes K_2/K_1}\left(x\cdot(1\otimes\beta_j)\right) \in K_1$. (Use the fact that

$\mathrm{Tr}_{K_1\otimes K_2/K_1}\left((1\otimes\beta_j)(1\otimes\beta_i^\vee)\right) = \mathrm{Tr}_{K_1/\mathbb{Q}}(\beta_i^\vee\beta_j) = \delta_{ij}$.)

If $x \in \delta^{-1}_{K_1\otimes K_2/K_1}$, then $x_j \in \mathcal{O}_K$.

$$\delta^{-1}_{K_1\otimes K_2/K_1} \subseteq \sum_j \mathcal{O}_{K_1}(1\otimes\beta_j^\vee) \subseteq \delta^{-1}_{K_2}\,\mathcal{O}_{K_1\otimes K_2}$$

Applying ρ_1 one gets $\delta_{L/K_1}^{-1} \subseteq \delta_{K_2}^{-1} \mathcal{O}_L \iff \delta_{K_2} \mathcal{O}_L \subseteq \delta_{L/K_1}$.

Then (2) follows from (1) by taking norms and the fact that

$$[L : K_1] \leq [K_2 : \mathbb{Q}], \quad [L : K_2] \leq [K_1 : \mathbb{Q}]$$

□

Decomposition of primes in Galois extensions

A Dedekind domain,

$K = \mathrm{Frac}(A)$

L/K Galois extension, finite $\quad G = \mathrm{Gal}(L/K)$

B = int. closure of A in L.

$$\begin{array}{ccc} B & - & L \\ | & & | \\ A & - & K \end{array} \Big) G$$

$\mathfrak{p} \subseteq A$ prime ideal

$$\mathfrak{p} B = \prod_{i=1}^{g} \mathfrak{Q}_i^{e_i} \quad \circlearrowleft G$$

G acts on the set $\{\mathfrak{Q}_1, \dots, \mathfrak{Q}_g\}$

Prop. The action of G on this set $\{\mathfrak{Q}_1, \dots, \mathfrak{Q}_g\}$ is transitive, and we have $e_1 = \dots = e_g =: e$, $f_1 = \dots = f_g =: f$, $e \cdot f \cdot g = n$.

PROOF: Let $\sigma \in G$.

$$\underbrace{\sigma(\mathfrak{p}B)}_{\prod_{i=1}^{r} \sigma(\mathfrak{Q}_i)^{e_i}} = \mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{Q}_i^{e_i}$$

Uniqueness of prime decomposition: if $\sigma(\mathfrak{Q}_i) = \mathfrak{Q}_j$ then $e_i = e_j$.

$$B/\mathfrak{Q}_i \xrightarrow[\sigma]{\sim} B/\sigma(\mathfrak{Q}_i) = B/\mathfrak{Q}_j \quad \text{induced isomorphism} \Rightarrow f_i = f_j$$

$$x \longmapsto \sigma(x)$$

It is enough to show that $\forall \mathfrak{Q}_i \; \exists \sigma \in G : \sigma(\mathfrak{Q}_1) = \mathfrak{Q}_i$.

Lemma: Let R be any ring, $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be prime ideals in R, $I \subseteq R$ an ideal s.t. $I \not\subseteq \mathfrak{p}_i \; \forall i$.

Then $\exists x \in I$ s.t. $x \notin \mathfrak{p}_i \; \forall i$.

PROOF: Wma ~~the $\mathfrak{p}_i$ are distinct and~~ $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j \; \forall i \neq j$ (otherwise just forget about $\mathfrak{p}_i$). Let $x_{i,j} \in \mathfrak{p}_j \setminus \mathfrak{p}_i \; \forall i \neq j$, $a_i \in I \setminus \mathfrak{p}_i \; \forall i$.

$b_i := a_i \prod_{j \neq i} x_{i,j} \in \left(I \cap \bigcap_{j \neq i} \mathfrak{p}_j \right) \setminus \mathfrak{p}_i$

Take $x := \sum b_i \in I$. Then $x_i \equiv b_i \pmod{\mathfrak{p}_i}$ $\forall i$ $\Rightarrow$ $x \notin \mathfrak{p}_i$ $\forall i$. □

We return to proving the proposition.

↯ Assume in contrary that $\exists Q_i$ above $\mathfrak{p}$ s.t. $Q_i \neq \sigma(Q_1)$ $\forall \sigma \in G$.

By the lemma, there is an $x \in Q_i$ s.t. $\underbrace{x \notin \sigma(Q_1) \quad \forall \sigma \in G}_{\sigma(x) \notin Q_1 \quad \forall \sigma \in G}$

$$\left.\begin{array}{l} \underbrace{\prod_{\sigma \in G} \sigma(x)}_{\in Q_i \cap K = \mathfrak{p}} \notin Q_1 \end{array}\right\} \Rightarrow \mathfrak{p} \notin Q_1 \ \lightning$$

□

Def. $\forall$ prime Q of B above $\mathfrak{p}$ define $D(Q|\mathfrak{p}) = \{ \sigma \in G \mid \sigma(Q) = Q \}$ called the decomposition group of Q relative to $\mathfrak{p}$.

$\Rightarrow |G| = g \cdot |D(Q|\mathfrak{p})|$ for any Q above $\mathfrak{p}$.

$D(\sigma(Q)|\mathfrak{p}) = \sigma \cdot D(Q|\mathfrak{p}) \cdot \sigma^{-1}$, that is, the decomposition groups are conjugates of each other.

$\forall \sigma \in D(Q|\mathfrak{p})$ induces an automorphism

$$\begin{array}{ccc} k(Q) = B/Q & \xrightarrow[\sigma]{\sim} & B/\sigma(Q) = B/Q = k(Q) \\ x & \longmapsto & \sigma(x) \end{array}$$

We get a map $\varphi_Q : D(Q|\mathfrak{p}) \longrightarrow \mathrm{Aut}_{k(\mathfrak{p})}(k(Q))$. (The extension $k(Q)/k(\mathfrak{p})$ need not be Galois.)

Def We define $I(Q|\mathfrak{p}) := \ker \varphi_Q = \{ \sigma \in D(Q|\mathfrak{p}) \mid \sigma(x) \equiv x \pmod{Q} \ \forall x \in B \}$, called the inertia subgroup of Q relative to $\mathfrak{p}$.

Prop. Assume $k(\mathfrak{p})$ is perfect. Then $k(Q)$ is Galois over $k(\mathfrak{p})$, and the map φ_Q is surjective, i.e.

$$1 \longrightarrow I(Q|\mathfrak{p}) \longrightarrow D(Q|\mathfrak{p}) \xrightarrow{\varphi_Q} \mathrm{Gal}(k(Q)/k(\mathfrak{p})) \longrightarrow 1$$

is an exact sequence of groups.

Moreover, $|D(Q|\mathfrak{p})| = ef$ and $|I(Q|\mathfrak{p})| = e$.

PROOF: $|D(Q|\mathfrak{p})| = \frac{|G|}{g} = \frac{efg}{g} = ef$

Let $M = L^{D(Q|\mathfrak{p})}$, $N = L^{I(Q|\mathfrak{p})}$

$L - Q$
$|$
$N - Q_N := Q \cap \mathcal{O}_N$
$|$
$M - Q_M = Q \cap \mathcal{O}_M$
$|$
$K - \mathfrak{p}$

$\mathrm{Gal}(L/M) \cong D(Q|\mathfrak{p})$ stabilises Q

By the previous prop.,

Q is the only prime of $\mathcal{O}_L$ above Q_M,
and Q is the only prime of $\mathcal{O}_L$ above Q_N.

$$\left.\begin{aligned} ef &= |D(Q|\mathfrak{p})| = [L:M] = e(Q|Q_M)\cdot f(Q|Q_M) \\ e &= e(Q|\mathfrak{p}) = e(Q|Q_M)\, e(Q_M|\mathfrak{p}) \\ f &= f(Q|Q_M)\, f(Q_M|\mathfrak{p}) \end{aligned}\right\} \Rightarrow e = e(Q|Q_M),\ f = f(Q|Q_M).$$

Similarly, assume $Q_N \mathcal{O}_L = Q^{e'}$. $\Rightarrow e' = e(Q|Q_N) \le e$

Let $\bar{\alpha} \in k(Q)$ be any element, $\alpha \in \mathcal{O}_L$ be a lift of $\bar{\alpha}$.

Consider the minimal polynomial of α over N:

$$f(x) = \prod_{\sigma \in I(Q|\mathfrak{p}) = \mathrm{Gal}(L/N)} (X - \sigma(\alpha))$$

$$f(x) \bmod Q = \prod_{\sigma \in I(Q|\mathfrak{p})} (X - \sigma(\bar{\alpha}))$$

$$\sigma(\alpha) \equiv \alpha \pmod{Q}, \qquad \sigma(\bar{\alpha}) = \bar{\alpha}$$

$$f(x) \bmod Q = (X - \bar{\alpha})^{|I(Q|\mathfrak{p})|}$$

$\to$ any Galois conjugate over $k(Q_N)$ of $\bar{\alpha}$ is $\bar{\alpha}$ itself

Since $k(\mathfrak{p})$ is perfect, we have $\bar{\alpha} \in k(Q_N)$ $\forall \alpha \in k(Q)$

$\to k(Q) = k(Q_N)$, $f(Q|Q_N) = 1$.

$$e' = e(Q|Q_N)\cdot f(Q|Q_N) = [L:N] = |I(Q|Q_N)|.$$

On the other hand, one has

$$1 \longrightarrow I(Q|\mathfrak{p}) \longrightarrow D(Q|\mathfrak{p}) \xrightarrow{\varphi_Q} \mathrm{Aut}_{k(\mathfrak{p})}\, k(Q)$$

Gal. theory $\Rightarrow |\mathrm{Aut}_{k(\mathfrak{p})}\, k(Q)| \le [k(Q) : k(\mathfrak{p})] = f$

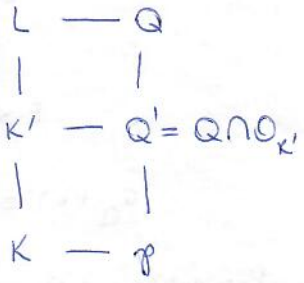
$$|I(Q|\mathfrak{p})| = \frac{|D(Q|\mathfrak{p})|}{|\mathrm{Im}\,\varphi_Q|} \ge \frac{ef}{f} = e$$

$e' = e(Q|Q_N)$ divides $e = e(Q|p) = e(Q|Q_N)\cdot e(Q_N|p)$. $\Rightarrow$

$\Rightarrow$ $e' = e = |I(Q|p)|$, and $|\mathrm{Aut}_{k(p)} k(Q)| = f$, and φ_Q is surjective

$\Rightarrow$ $k(Q)$ is Galois over $k(p)$. □

From now on, we assume K to be a number field.



Prop. Let $K' | K$ be a subextension of L/K, $H := \mathrm{Gal}(L/K')$.

Then:

(1) Q is the only prime above Q' iff $H \subseteq D(Q|p)$

(2) Q' is unramified above p iff $I(Q|p) \subseteq H$.

In general, $e(Q'|p) = \dfrac{|I(Q|p)|}{|H \cap I(Q|p)|}$

(3) If $\{Q_1, \dots, Q_g\}$ are the primes of L above p, then the set of primes of K' above p is in bijection with the set of orbits of H on $\{Q_1, \dots, Q_g\}$ via $\subseteq G \supseteq H$.

PROOF. (3) Easy by the first prop. today.

For (1), (2): $D(Q|p) \cap H = D(Q|Q')$

$I(Q|p) \cap H = I(Q|Q')$

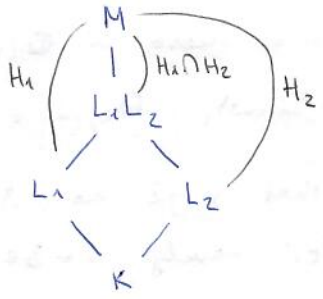
Q is the only prime above Q' $\Leftrightarrow$ $D(Q|Q') = H$

$\Leftrightarrow$ $H \subseteq D(Q|p)$ $\rightarrow$ (1).

$$e(Q'|p) = \frac{e(Q|p)}{e(Q|Q')} = \frac{|I(Q|p)|}{|I(Q|Q')|} = \frac{|I(Q|p)|}{|H \cap I(Q|p)|} \rightarrow (2)$$

□

Cor. Let L_1, L_2 be two finite subextensions of K in K^{alg}, and p be a prime ideal in K. Then p is unramified in L_1 and L_2 if p is unramified in $L_1 L_2$.



PROOF: Choose M/K Galois containing $L_1 L_2$.

$G := \mathrm{Gal}(M/K)$, $H_i := \mathrm{Gal}(M/L_i)$ $(i = 1,2)$

p is unramified in $L_1 \cdot L_2$ $\Leftrightarrow$

$\Leftrightarrow$ $\forall \beta$ of $L_1 L_2$ above p: $e(\beta|p) = 1$

$\Leftrightarrow$ $\forall Q$ of M above p: $H_1 \cap H_2 \supseteq I(Q|p)$.

$\Leftrightarrow$ $\forall Q$ of M above p: $\underbrace{I(Q|p) \subseteq H_1}_{p \text{ unram in } L_1}$ and $\underbrace{I(Q|p) \subseteq H_2}_{p \text{ unram in } L_2}$.

□

Now assume that $\mathfrak{p}$ is unramified in L/K. and $k(\mathfrak{p}) \cong \mathbb{F}_q$.

$$I(\mathcal{Q}|\mathfrak{p}) = 1, \quad D(\mathcal{Q}|\mathfrak{p}) \cong \underbrace{\mathrm{Gal}(k(\mathcal{Q})/k(\mathfrak{p}))}_{\| S}$$

$$\cup \qquad (\mathbb{Z}/f\mathbb{Z})$$

$$\cup$$

$$\sigma_{\mathcal{Q}} := \left(\frac{L/K}{\mathcal{Q}}\right) \longleftrightarrow \sigma_q$$

$\downarrow$

Frobenius element at $\mathcal{Q}$

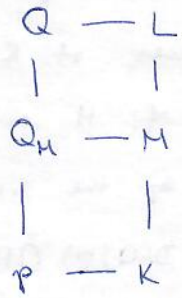
$$\sigma_{\mathcal{Q}}(x) \equiv x^q \pmod{\mathcal{Q}} \quad \forall x \in \mathcal{O}_L$$

Properties. 1) $\left(\frac{L/K}{\sigma(\mathcal{Q})}\right) = \sigma \left(\frac{L/K}{\mathcal{Q}}\right) \sigma^{-1}$

2) If M/K is a Galois subextension of L/K, then

$$\underbrace{\left(\frac{L/K}{\mathcal{Q}}\right)\Big|_M}_{\in \mathrm{Gal}(M/K)} = \left(\frac{M/K}{\mathcal{Q}_M}\right)$$

$$\left(\frac{L/M}{\mathcal{Q}_M}\right) = \left(\frac{L/K}{\mathcal{Q}}\right)^{f(\mathcal{Q}_M|\mathfrak{p})}$$



Ex. $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = \frac{-1+\sqrt{3}}{2}$ (simplest non-Abelian example)

$$G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_3 \cong \langle \sigma, \tau \rangle / (\sigma^3 = 1, \ \tau^2 = 1, \ \tau\sigma\tau = \sigma^2)$$

$$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega, \quad \sigma(\omega) = \omega$$

$$\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\omega) = \bar{\omega} = \omega^2$$

Then p unramified in $L \iff p$ unram. in $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\omega)$

$$\iff p \neq 2, 3$$

$p = 5$ is inert in $\mathbb{Q}(\omega)$ since $X^2 + X + 1$ is irreducible in $\mathbb{F}_5[X]$

$K = \mathbb{Q}(\omega)$, $\mathcal{O}_K/(5) = \mathbb{F}_{25}$

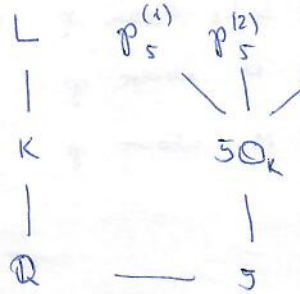
Note that $X^3 - 2$ has 3 distinct roots in $\mathbb{F}_{25}$, and one of them is in $\mathbb{F}_5$, namely $x = 3 \in \mathbb{F}_5$.

There are 3 primes in L above 5:

$$\mathfrak{p}_5^{(1)} = (5, \sqrt[3]{2}, -3)$$

$$\mathfrak{p}_5^{(2)} = (5, \sqrt[3]{2} - 3\omega)$$

$$\mathfrak{p}_5^{(3)} = (5, \sqrt[3]{2} - 3\omega^2)$$



$$D(\mathfrak{P}_5^{(1)} \mid 5) = \{ g \in G \mid g\mathfrak{P}_5^{(1)} = \mathfrak{P}_5^{(1)} \} = \langle \tau \rangle$$

$$D(\mathfrak{P}_5^{(2)} \mid 5) = \langle \sigma\tau \rangle = \sigma^2 D(\mathfrak{P}_5^{(1)} \mid 5)\sigma^{-2} = \mathrm{Gal}\left(L/\mathbb{Q}(\sqrt[3]{2}\,\omega^2)\right)$$

$\mathfrak{P}_5^{(2)} = \sigma^2 \mathfrak{P}_5^{(1)}$

$$D\left(\mathfrak{P}_3^{(5)} \mid 5\right) = \langle \sigma^2\tau \rangle = \mathrm{Gal}\left(L/\mathbb{Q}(\sqrt[3]{2}\,\omega)\right)$$

6.11.2017

Recall. L/K fin. Gal. extension of num. fields,

$G = \mathrm{Gal}(L/K)$

$\mathfrak{p}\mathcal{O}_L = (\mathfrak{Q}_1 \dots \mathfrak{Q}_g)^e$

$$\begin{array}{ccc} \mathcal{O}_L & - & L \\ | & & | \\ \mathfrak{p} & - \mathcal{O}_K - & K \end{array}$$

$f = f(\mathfrak{Q}_1 \mid \mathfrak{p}) = \dots = f(\mathfrak{Q}_g \mid \mathfrak{p}) = |D(\mathfrak{Q}_i \mid \mathfrak{p})|$

$e = |I(\mathfrak{Q}_i \mid \mathfrak{p})|$

We return to cyclotomic fields. Let $N \geq 3$ and be either odd or $4 \mid N$.

Lemma. A rational prime p is ramified in $\mathbb{Q}(\zeta_N)$ iff $p \mid N$.

Moreover, if $p \mid N$, the ramification index of any prime in $\mathbb{Q}(\zeta_N)$ above p is $p^{a-1}(p-1)$ where $a = v_p(N)$.

PROOF: Known: $\mathrm{disc}_{\mathbb{Q}(\zeta_N)} \mid N^{\varphi(N)} \Rightarrow \forall p \nmid N \quad p \nmid \mathrm{disc} \Rightarrow$ unram.

If $p \mid N$, consider the case $N = p^a$.

Known: $\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathbb{Z}[\zeta_{p^a}] = \mathbb{Z}[\zeta_{p^a} - 1]$

Min. poly of $\zeta_{p^a} - 1$ is $\Phi_{p^a}(1+X) = \dfrac{(1+X)^{p^a} - 1}{(1+X)^{p^{a-1}} - 1} = \sum_{i=0}^{p-1} (1+X)^{p^{a-1} i}$

$$\equiv \sum_{i=0}^{p-1} \left(1 + X^{p^{a-1}}\right)^i \pmod{p}$$

$$= \frac{(1+X^{p^{a-1}})^p - 1}{(1+X^{p^{a-1}}) + 1} = \frac{(1+X^{p^{a-1}})^p - 1}{X^{p^{a-1}}} \equiv X^{p^{a-1}(p-1)} \pmod{p}$$

Kummer $\Rightarrow$ $p\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathfrak{p}^{p^{a-1}(p-1)}$ totally ramified.

General: $N = p^a N' \quad (N', p^a) = 1$

$\forall \mathfrak{Q}$ prime above $\mathfrak{p}$:

$e(\mathfrak{Q} \mid \mathfrak{p}) \geq e(\mathfrak{Q} \mid \mathfrak{P})$

$\mathfrak{Q}' = \mathfrak{Q} \cap \mathbb{Q}(\zeta_{N'})$

$e(\mathfrak{Q} \mid \mathfrak{p}) = e(\mathfrak{Q} \mid \mathfrak{Q}') \cdot e(\mathfrak{Q}' \mid \mathfrak{p}) =$

$= e(\mathfrak{Q} \mid \mathfrak{Q}')$

$\leq [\mathbb{Q}(\zeta_N) : \mathbb{Q}(\zeta_{N'})] = [\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}] = p^{a-1}(p-1)$.

$$\begin{array}{ccccc} & & \mathbb{Q} & & \\ & \swarrow & | & \searrow & \\ \mathfrak{Q}' & - & \mathbb{Q}(\zeta_N) & - & \mathbb{Q} \\ & \searrow & | & \swarrow & \\ & & \mathbb{Q}(\zeta_{N'}) & & \mathbb{Q}(\zeta_{p^a}) - \mathfrak{p} \\ & & & \searrow & | \\ & & & & \mathbb{Q} - \mathfrak{p} \end{array}$$

□

Assume $p \nmid N$.

$p\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathfrak{p}_1 \cdots \mathfrak{p}_g \qquad f = |D(\mathfrak{p}_i|p)| \quad i = 1, \dots, g$

$D(\mathfrak{p}_i|p) = \langle \sigma_p \rangle$ where σ_p is the Frobenius element, which is independent of $\mathfrak{p}_i$

σ_p is characterised by: $\sigma_p(\zeta_N) \equiv \zeta_N^p \pmod{\mathfrak{p}_i}$

for any prime $\mathfrak{p}_i$ above p.

Lemma. If $i \not\equiv j \pmod N$ then $\zeta_N^i \not\equiv \zeta_N^j \pmod{\mathfrak{p}}$ for any prime $\mathfrak{p}$ above p. (of $\mathbb{Q}(\zeta_N)$)

Proof: Consider $X^N - 1 =: f(X)$

For any Nth root ζ of unity: $f'(\zeta) = N \cdot \zeta^{N-1} \not\equiv 0 \pmod{\mathfrak{p}}$

because $p \nmid N$ and ζ is a unity in $\mathcal{O}_{\mathbb{Q}(\zeta_N)}$.

$\Rightarrow \overline{f}(X) \in \mathbb{F}_p[X]$ has no multiple roots in $\overline{\mathbb{F}}_p$

$\Rightarrow \zeta_N^i \not\equiv \zeta_N^j \pmod{\mathfrak{p}}$ (otherwise it would be a multiple root) □

Cor. $\sigma_p(\zeta_N) = \zeta_N^p \quad \forall p \nmid N$.

In other words, via the canonical iso

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) & \xrightarrow{\sim} & (\mathbb{Z}/N\mathbb{Z})^\times \\ \psi & & \\ \sigma_p & \longrightarrow & (p \bmod N) \\ \text{(Frobenius)} & & \end{array}$$

□

Proof. $p \nmid N \Rightarrow$ for any prime $\mathfrak{p}$ of $\mathbb{Q}(\zeta_N)$ above p we have

$f(\mathfrak{p}|p) =$ order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$

i.e. the minimal integer f s.t. $p^f \equiv 1 \pmod N$

$g = \dfrac{\varphi(N)}{f}$. In particular, p splits in $\mathbb{Q}(\zeta_N) \Leftrightarrow p \equiv 1 \pmod N$.

For $p \mid N$, write $N = p^a \cdot N'$ where $p \nmid N'$.

Then $p\mathcal{O}_{\mathbb{Q}(\zeta_N)} = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$, $e = p^{a-1}(p-1)$, $g = \dfrac{\varphi(N)}{f}$, $f =$ order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$,

$I(\mathfrak{p}_i|p) \cong \ker\left((\mathbb{Z}/N\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/N'\mathbb{Z})^\times\right) = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_{N'}))$

$D(\mathfrak{p}_i|p) =$ preimage of $\langle p \rangle \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$ in $(\mathbb{Z}/N\mathbb{Z})^\times$

Ex. $L = \mathbb{Q}(\zeta_{31})$, $p = 2$ unram. in L

order of 2 in $(\mathbb{Z}/31\mathbb{Z})^\times$ is 5 $\Rightarrow$ $2\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_6$

$f(\mathfrak{P}_i|2) = 5$ $\quad K = L^{\langle 2 \rangle}$ $\quad 2\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_6$ $\quad f(\mathfrak{p}_i|2) = 1$

30

$$\begin{pmatrix} L \\ | \\ K \\ | \\ \mathbb{Q} \end{pmatrix} \begin{matrix} 5 \\ \\ \\ 6 \end{matrix}$$

Claim. $\nexists\, \alpha \in \mathcal{O}_K$ s.t. $\mathcal{O}_K = \mathbb{Z}[\alpha]$

$\forall\, \exists\, \alpha$: let $f(X) \in \mathbb{Z}[X]$ be its minpoly

Kummer: $\bar{f}(X) = \prod_{i=1}^{6} (X - a_i)$ in $\mathbb{F}_6[X]$

$a_i \neq a_j \ \forall i \neq j, \quad a_i \in \mathbb{F}_2$.

Impossible, $|\mathbb{F}_2| = 2$ $\lightning$

Lemma Let p be an odd prime. We put $p^* = (-1)^{\frac{p-1}{2}} p = \begin{cases} p & p \equiv 1 \ (4) \\ -p & p \equiv 3 \ (4) \end{cases}$

Then $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subextension of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

Pf: The Gal group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ cyclic of order $p-1$

$\Rightarrow$ it has a uq. subgroup H of index 2, $H = (\mathbb{F}_p^\times)^2$

$K := \mathbb{Q}(\zeta_p)^H$ is quadratic over $\mathbb{Q}$

$K = \mathbb{Q}(\sqrt{D})$ for some square-free D

$\Rightarrow \forall\, \ell \neq p$ is unramified in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ hence in $K/\mathbb{Q}$

$\Rightarrow$ the only prime factors of D is p. $\Rightarrow D = p$ or $D = -p$.

The only choice is $D = p^*$. □

Theorem. (Quadratic Reciprocity) p, q odd primes.

Then $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

PROOF: The statement is equivalent to $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$

because $\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$.

$\left(\frac{q}{p}\right) = 1 \iff q \in (\mathbb{F}_p^\times)^2 \iff \sigma_q \in H$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$

$\iff q$ splits in $\mathbb{Q}(\zeta_p)^H = \mathbb{Q}(\sqrt{p^*})$

$\overset{\text{Kummer}}{\iff} X^2 + X + \frac{1-p^*}{2} \pmod q$ has two distinct roots in $\mathbb{F}_q$.

$\iff p^*$ is a quadratic residue mod q

$\iff \left(\frac{p^*}{q}\right) = 1$

□

Exercise. $\forall$ odd prime p we have $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$,

i.e. $\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{otherwise} \end{cases}$

Hint: consider $\mathbb{Q}(\zeta_p) \supseteq \mathbb{Q}(\sqrt{2})$.

Finiteness theorems

Thm 1. (Minkowski) If K is a number field then Cl_K is finite.

Thm 2. (Hermite) Given an integer $d \geq 2$ there exist only finitely many number fields with discriminant d.

Thm 3. (Dirichlet) Let K be a number field.

$r_1 :=$ # of real embeddings of K, $r_2 :=$ # of pairs of non-real embeddings $K \hookrightarrow \mathbb{C}$

$(r_1 + 2r_2 = [K:\mathbb{Q}])$ Then $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r_1 + r_2 - 1$, i.e. $\mathcal{O}_K^\times \cong (\mathcal{O}_K^\times)_{tors} \times \mathbb{Z}^{r_1+r_2-1}$

$$(\mathcal{O}_K^\times)_{tors} \cong \mu(K) = \{ x \in K^\times \mid x^m = 1 \text{ for some } m \}$$

Recall. A subset $\Lambda \subseteq \mathbb{R}^n$ is called a (full) lattice if Λ is a discrete subgroup of $\mathbb{R}^n$ and Λ contains a basis of $\mathbb{R}^n$.

$\Rightarrow$ $rk_{\mathbb{Z}}(\Lambda) = n$ and $\mathrm{vol}(\mathbb{R}^n/\Lambda) < +\infty$

Non-ex. $n=1$, $\Lambda = \mathbb{Z} + \sqrt{2}\,\mathbb{Z} \subseteq \mathbb{R}$ is not discrete

Lemma. (Minkowski) $\Lambda \subseteq \mathbb{R}^n$ a lattice, $X \subseteq \mathbb{R}^n$ a centrally symmetric convex and connected region with $\mu(X) < +\infty$.

Assume $\mu(X) > 2^n \,\mathrm{vol}(\mathbb{R}^n/\Lambda)$. Then $X \cap \Lambda$ contains a non-zero element.

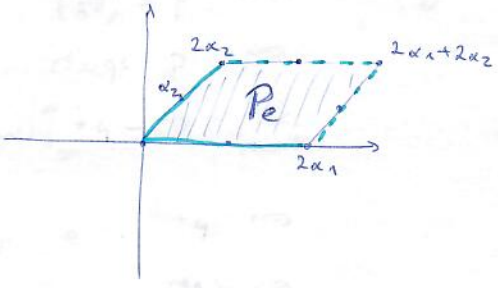
(Cent. symm.: $x \in X \Leftrightarrow (-x) \in X$, convex: if $x, y \in X \Rightarrow \lambda x + (1-\lambda) y \in X \ \forall \lambda \in [0,1]$)

Proof: Let $\mathcal{P}_e$ be the parallelogram spanned by a basis of 2Λ.

$$\mu(\mathcal{P}_e) = \mathrm{vol}(\mathbb{R}^n/2\Lambda) = 2^n \cdot \mathrm{vol}(\mathbb{R}^n/\Lambda)$$

$$\mathbb{R}^n = \coprod_{\lambda \in 2\Lambda} (\lambda + \mathcal{P}_e)$$

$$X = \coprod_{\lambda \in 2\Lambda} (\lambda + \mathcal{P}_e) \cap X$$



$$\infty > \mu(X) = \sum_{\lambda \in 2\Lambda} \mu\left(X \cap (\lambda + P_e)\right)$$

$$\mu\left(X \cap (\lambda + P_e)\right) = \mu\left(P_e \cap (-\lambda + X)\right)$$

By assumption, $\mu(X) = \sum_{\lambda \in 2\Lambda} \mu\left(P_e \cap (-\lambda + X)\right) > \mu(P_e)$

$\Rightarrow \exists\ \lambda_1 \neq \lambda_2 \in 2\Lambda,\ x_1 \neq x_2$ s.t. $-\lambda_1 + x_1 = -\lambda_2 + x_2$

$X \ni \frac{x_1 - x_2}{2} = \frac{\lambda_1 - \lambda_2}{2} \in \Lambda$ and these are $\neq 0$.

↓ convexity ↓ subgroup

□

Application to number fields.

$K/\mathbb{Q}$ number field.

$\forall$ frac. ideal $I \subseteq K$ is a free $\mathbb{Z}$-module of rk n

$\mathrm{Disc}(I) := \mathrm{Disc}(\alpha_1, \dots, \alpha_n)$ for any basis $\alpha_1, \dots, \alpha_n$ of I over $\mathbb{Z}$

Lemma. $\mathrm{Disc}(I) = \mathrm{disc}_K \cdot N_{K/\mathbb{Q}}(I)^2$

Pf: We show first that if $J \subseteq I$ is another frac. ideal then

$\mathrm{Disc}(J) = \mathrm{Disc}(I) \cdot |I/J|^2$

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

$I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} \cdot J \qquad a_i \geq 1$

$I/J \cong \mathcal{O}_K / \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} \qquad |I/J| = \prod_{i=1}^{r} N_{K/\mathbb{Q}}(\mathfrak{p}_i)^{a_i} = \frac{N_{K/\mathbb{Q}}(J)}{N_{K/\mathbb{Q}}(I)}$

Choose a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$ of I,

$\beta_1, \dots, \beta_n$ of J.

$\beta_i = \sum_j c_{ij} \cdot \alpha_j \qquad c_{ij} \in \mathbb{Z}$

$\mathrm{Disc}(J) = \mathrm{Disc}(\beta_1, \dots, \beta_n) = \mathrm{Disc}(\alpha_1, \dots, \alpha_n) \cdot \det(c_{ij})^2$

$|\det(c_{ij})| = |I/J| = [I : J]$

To prove the lemma, choose an ideal J s.t. $I \supseteq J$ and $\mathcal{O}_K \supseteq J$. $\Rightarrow \mathrm{Disc}(I) = \mathrm{Disc}(J) \cdot \frac{N_{K/\mathbb{Q}}(I)^2}{N_{K/\mathbb{Q}}(J)^2}$

$\mathrm{disc}_K = \mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(J) \cdot N_{K/\mathbb{Q}}(J)^2$

$\Rightarrow \mathrm{Disc}(I) = \mathrm{disc}_K \cdot N_{K/\mathbb{Q}}(I)^2.$

□

Denote by $\sigma_1, \dots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$ the real embeddings

$\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2} = \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+2r_2-1}, \sigma_{r_1+2r_2} = \overline{\sigma_{r_1+2r_2-1}} : K \hookrightarrow \mathbb{C}$ the non-real complex embeddings

$\lambda : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2} = \mathbb{R}^n$

$$x \longmapsto \left((\sigma_i(x))_{i=1,\dots,r_1}, (\sigma_{r_1+2j}(x))_{j=1,\dots,r_2} \right)$$

$$\left((y_i)_{i=1,\dots,r_1}, (\zeta_j)_{j=1,\dots,r_2} \right) \mapsto \left((y_i), \operatorname{Re}\zeta_1, \operatorname{Im}\zeta_1, \dots \right)$$

Lemma: For any frac. ideal I of $\mathcal{O}_K$: $\lambda(I) \subseteq \mathbb{R}^n$ is a lattice and

$$\operatorname{Vol}\left(\mathbb{R}^n / \lambda(I)\right) = \frac{1}{2^{r_2}} \sqrt{\operatorname{Disc}(I)} =$$

$$= \frac{1}{2^{r_2}} \sqrt{|\operatorname{disc}_K|} \cdot N_{K/\mathbb{Q}}(I)$$

Pf: $\alpha_1, \dots, \alpha_n$ $\mathbb{Z}$-basis of I

$$\operatorname{Vol}\, \mathbb{R}^n/\lambda(I) = \left| \det\left(\lambda(\alpha_1), \dots, \lambda(\alpha_n) \right) \right|$$

On the other hand,

$$\left(\sigma_i(\alpha_j)\right)_{1 \le i,j \le n} = \begin{pmatrix} I_{r_1 \times r_1} & & & \\ & \begin{pmatrix} 1 & -i \\ 1 & +i \end{pmatrix} & & \\ & & \begin{pmatrix} 1 & -i \\ 1 & +i \end{pmatrix} & \\ & & & \ddots \\ & & & \begin{pmatrix} 1 & -i \\ 1 & +i \end{pmatrix} \end{pmatrix} \times \left(\lambda_{\mathbb{R}}(\alpha_1), \dots, \lambda(\alpha_n) \right)$$

$$\sigma_{r_1+2j-1}(x) = \lambda(x)_{2r_1+2j-1} - i\,\lambda(x)_{r_1+2j}$$

$$\det\left(\left(\sigma_i(\alpha_j)\right)\right) = \det \begin{pmatrix} I & & & \\ & \begin{pmatrix} 1 & -i \\ 1 & +i \end{pmatrix} & & \\ & & \ddots & \\ & & & \begin{pmatrix} 1 & -i \\ 1 & +i \end{pmatrix} \end{pmatrix} \det\left(\lambda(\alpha_1), \dots, \lambda(\alpha_n) \right) = (2i)^{r_2} \det\left(\lambda(\alpha_1), \dots, \lambda(\alpha_n) \right)$$

$$\operatorname{vol}\left(\mathbb{R}^n/\lambda(I)\right) = \frac{1}{2^{r_2}} \left| \det\left(\sigma_i(\alpha_j)\right) \right|$$

$$\operatorname{Disc}(I) = \det\left(\left(\sigma_i(\alpha_j)\right)\right)$$

$$\operatorname{vol}\left(\mathbb{R}^n/\lambda(I)\right) = \frac{1}{2^{r_2}} \sqrt{\operatorname{Disc}(I)}$$

□

Recall.

- Lemma (Minkowski): $\Lambda \subseteq \mathbb{R}^n$ a lattice, X centrally symmetric convex connected. If $\mu(X) > 2^n \cdot \mathrm{Vol}\left(\mathbb{R}^n/\Lambda\right)$, then $X \cap \Lambda$ contains a nonzero element.
- $K/\mathbb{Q}$ number field, $n = [K:\mathbb{Q}] = r_1 + 2r_2$

$$\lambda : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$
$$x \longmapsto \left(\left(\sigma_i(x)\right)_{i=1,\dots,r_1}, \left(\sigma_{r_1+2j}(x)\right)_{j=1,\dots,r_2}\right)$$

- Lemma: $I \subseteq K$ frac. ideal, $\Rightarrow \mathrm{Vol}\left(\mathbb{R}^n/\lambda(I)\right) = \frac{1}{2^{r_2}}\sqrt{|d_K|}\cdot N(I)$ where d_K is the discriminant of K, $N(I) = N_{K/\mathbb{Q}}(I) \in \mathbb{Q}_{>0}$

Theorem. Let K, n, r_1, r_2 be as above, and I be a fractional ideal of $\mathbb{Q}$. Then there exists a nonzero $\alpha \in I$ s.t. $\left|N_{K/\mathbb{Q}}(\alpha)\right| \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}\sqrt{|d_K|}\cdot N(I)$

PROOF: Consider the region

$$B(t) := \left\{ x = (y,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \;\middle|\; \sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq t \right\}$$

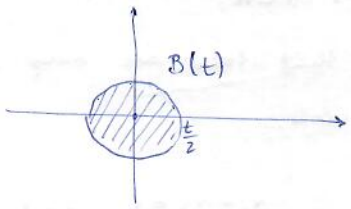
for $t > 0$.

This $B(t)$ is centrally symmetric and convex connected.

Lemma. $\mu(B(t)) = 2^{r_1}\cdot\left(\frac{\pi}{2}\right)^{r_2}\cdot\frac{t^n}{n!}$

Pf: Exercise, just multivariable calculus, induction $r_1 + r_2 \geq 1$

For $r_1 = 0$, $r_2 = 1$:



$r_1 = 1$, $r_2 = 0$

Reduce the case of (r_1, r_2) to $(r_1 - 1, r_2)$ and $(r_1, r_2 - 1)$. □

Choose $t_0 \in \mathbb{R}_{>0}$ s.t. $\underbrace{\mu(B(t_0))}_{2^{r_1}\cdot\left(\frac{\pi}{2}\right)^{r_2}\cdot\frac{t_0^n}{n!}} = 2^n \mathrm{Vol}\left(\mathbb{R}^n/\lambda(I)\right) = 2^n \cdot \frac{1}{2^{r_2}}\sqrt{|d_K|}\cdot N(I)$

$$t_0 = \left(\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}\,N(I)\cdot n!\right)^{1/n}$$

$\forall t > t_0$: $\mu(B(t)) > \mu(B(t_0)) = 2^n \mathrm{Vol}\left(\mathbb{R}^n/\lambda(I)\right)$

Minkowski lemma: $B(t) \cap \lambda(I)$ has a nonzero element.

But $B(t)$ is compact and $\lambda(I)$ is discrete $\Rightarrow B(t) \cap \lambda(I)$ is finite.

Taking $t \to t_0$: $B(t_0) \cap \lambda(I)$ has a nonzero element. ∎

For this α:

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{r_1} |\sigma_i(\alpha)| \prod_{j=1}^{r_2} |\sigma_{r_1+2j}(\alpha)|^2 \leq$$

AM-GM

$$\leq \frac{1}{n^n}\left(\sum_{i=1}^{r_1} |\sigma_i(\alpha)| + 2\sum_{j=1}^{r_2} |\sigma_{r_1+2j}(\alpha)|\right)^n$$

$$\leq \frac{1}{n^n} t_0^n = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} \cdot \sqrt{|d_K|} \cdot N(I), \quad \text{as stated above.}$$

□

Corollary (Minkowski Bound) Every ideal class of K (i.e. elements of Cl_K) contains an integral ideal $\mathfrak{A} \subseteq \mathcal{O}_K$ s.t. $0 < N(\mathfrak{A}) \leq \underbrace{\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}}_{\text{only depends on } K}$.

PROOF: Let $\mathfrak{J}$ be an arbitrary fractional ideal of K.

Apply the previous theorem to $I := \mathfrak{J}^{-1}$.

$\rightarrow$ get $\alpha \in I \setminus \{0\}$: $|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|d_K|}\, N(I)$

$$\underbrace{|N_{K/\mathbb{Q}}(\alpha)\cdot N(I^{-1})|}_{N(\alpha\mathfrak{J})} \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}\sqrt{|d_K|}$$

$\alpha \in I = \mathfrak{J}^{-1} \Rightarrow (\alpha) \subseteq I \Rightarrow (\alpha)\cdot I^{-1} \subseteq \mathcal{O}_K$

$\Rightarrow \underbrace{\alpha\mathfrak{J}}_{\mathfrak{A}}$ is an integral ideal in the same ideal class as $\mathfrak{J}$.

□

Corollary. For any number field K, Cl_K is finite.

PROOF: Minkowski Bound and the fact that there are only finitely many integral ideals of $\mathcal{O}_K$ with a given norm.

□

Examples. 1) $K = \mathbb{Q}(\sqrt[3]{2})$ $\quad \mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ $\quad r_1 = r_2 = 1,\ n = 3$

$$d_K = -2^2 3^3$$

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|} = \frac{3}{3^2}\cdot\frac{4}{\pi}\cdot\sqrt{2^2\cdot 3^3} \approx 2.94 < 3$$

$\Rightarrow$ Every ideal class of K contains an integral ideal $\mathfrak{A} \subseteq \mathcal{O}_K$ with $N(\mathfrak{A}) = 1$ or 2.

- If $N(\mathfrak{A}) = 1 \Rightarrow \mathfrak{A} = \mathcal{O}_K$
- If $N(\mathfrak{A}) = 2 \Rightarrow \mathfrak{A}$ is a prime ideal over the rational prime 2.

So we only need all the primes above 2.

$2\mathcal{O}_K = (\sqrt[3]{2})^3 \Rightarrow$ there is a unique prime ideal over 2, namely $\mathfrak{p} = (\sqrt[3]{2})$. $\Rightarrow \mathfrak{A} = (\sqrt[3]{2})$ is principal.

$\Rightarrow Cl_K = \{0\}$, i.e. there are only principal ideals, i.e. $\mathcal{O}_K$ is a PID.

2) $K = \mathbb{Q}(\sqrt{-14})$ $\quad r_1 = 2,\ r_2 = 1$

$d_K = -56$

$\left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \sqrt{|d_K|} = \frac{4}{\pi} \cdot \frac{2}{2^2} \cdot \sqrt{56} \approx 4.765 < 5$

$N(\mathfrak{a}) = 1, 2, 3$ or 4

- If $N(\mathfrak{a}) = 2 \Rightarrow \mathfrak{a}$ is a prime above 2

  $2\mathcal{O}_K = \mathfrak{m}_2^2 \qquad \mathfrak{m}_2 = (2, \sqrt{-14})$ is non-principal, this is easy to check, b/c we know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$, $x^2 + 14y^2 = 2$ has no integral solution

- If $N(\mathfrak{a}) = 3 \Rightarrow \mathfrak{a}$ is a prime above 3

  $3\mathcal{O}_K = \mathfrak{p}_3 \overline{\mathfrak{p}_3} \qquad \mathfrak{p}_3 = (3, 1+\sqrt{-14}) \qquad \overline{\mathfrak{p}_3} = (3, 1-\sqrt{-14})$

  $\mathfrak{p}_3^2 = (9, 3+3\sqrt{-14}, -13+2\sqrt{-14}) = (9, -2+\sqrt{-14}) = \underbrace{\frac{-2+\sqrt{-14}}{2}}\ \underbrace{(2, \sqrt{-14})}_{\mathfrak{m}_2}$

  $\Rightarrow \mathfrak{a} = \mathfrak{p}_3 \cdot \overline{\mathfrak{p}_3}$

- If $N(\mathfrak{a}) = 4 \Rightarrow \mathfrak{a} = \mathfrak{m}_2^2 = (2)$

$\Rightarrow Cl_K \cong \mathbb{Z}/4\mathbb{Z}$ with generator given by $[\mathfrak{p}_3]$

$[\mathfrak{p}_3]^2 = [\mathfrak{m}_2],\ [\mathfrak{p}_3]^3 = [\overline{\mathfrak{p}_3}],\ [\mathfrak{p}_3]^4 = [\mathcal{O}_K] = 1.$

Hermite's Theorem.

Corollary. For a number field K of deg n: $|d_K|^{1/2} \geq \left(\frac{\pi}{4}\right)^{n/2} \cdot \frac{n^n}{n!}$

PROOF: Applying the theorem to $I = \mathcal{O}_K$, we get $0 \neq \alpha \in \mathcal{O}_K$ s.t.

$$1 \leq \left|N_{K/\mathbb{Q}}(\alpha)\right| \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot \sqrt{|d_K|}$$

$$\Rightarrow \sqrt{|d_K|} \geq \left(\frac{\pi}{4}\right)^{r_2} \cdot \frac{n^n}{n!} \geq \left(\frac{\pi}{4}\right)^{n} \cdot \frac{n^n}{n!} \quad \text{as } r_2 \leq \frac{n}{2} \text{ and } \frac{\pi}{4} < 1$$

□

Put $a_n := \left(\frac{\pi}{4}\right)^{n/2} \cdot \frac{n^n}{n!}$.

$$\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{1/2} \frac{(n+1)^{n+1} \cdot n!}{(n+1)! \cdot n^n} = \left(\frac{\pi}{4}\right)^{1/2} \underbrace{\left(1+\frac{1}{n}\right)^n}_{\text{strictly increasing}}$$

$$> \left(\frac{\pi}{4}\right)^{1/2} \left(1+\frac{1}{2}\right)^2 > 1$$

$\Rightarrow a_n$ is strictly increasing as $n \to \infty$,

and $a_n \geq a_2 = \left(\frac{\pi}{4}\right) \cdot \frac{2^2}{2} = \frac{\pi}{2} > 1$

Corollary. If $K \neq \mathbb{Q}$, then $|d_K| > 1$.

In other words, if K is a number field which is unramified at every rational prime, then $\mathbb{Q} = K$.

Theorem. (Hermite) For a fixed integer d, there are only finitely many number fields with discriminant d.

(The previous Corollary is the special case $d = 1$.)

PROOF: By the pre-previous Corollary, the degree of a number field is bounded above by its discriminant.

So it suffices to show that there are only finitely many number fields K with given $d_K = d$ and given number of real embeddings r_1 and pairs of complex embeddings r_2.

Idea: find $\alpha \in \mathcal{O}_K$ s.t. $K = \mathbb{Q}(\alpha)$ and the coefficients of the minimal polynomial of α over $\mathbb{Q}$ are bounded.

Construction of such an $\alpha \in \mathcal{O}_K$:

Case 1. $r_1 \geq 1$. Consider the region

$$X(c_1, \dots, c_{r_1+r_2}) = \left\{ (y;z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \;\middle|\; \begin{array}{ll} |y_i| \leq c_i & \forall\, i = 1, \dots, r_1, \\ |z_j|^2 \leq c_j & \forall\, j = r_1+1, \dots, r_1+r_2 \end{array} \right\}$$

$X(c_1, \dots, c_{r_1+r_2})$ is centrally symetric and convex.

$$\mu\left(X(c_1, \dots, c_{r_1+r_2})\right) = 2^{r_1} \cdot \pi^{r_2} \cdot \prod_{i=1}^{r_1+r_2} c_i$$

Choose $c_1 > 0$, $0 < c_i < 1$ for $i = 2, \dots, r_1+r_2$, so that (independent of K)

$$\mu\left(X(c_1, \dots, c_{r_1+r_2})\right) > 2^n \cdot \mathrm{Vol}\left(\mathbb{R}^n / \lambda(\mathcal{O}_K)\right) = 2^n \cdot \frac{1}{2^{r_2}} \cdot \sqrt{|d|}$$

Minkowski's lemma: $\exists\, 0 \neq \alpha \in \mathcal{O}_K$ s.t. $\alpha \in \lambda(\mathcal{O}_K) \cap X(c_1, \dots, c_{r_1+r_2})$

$$\Leftrightarrow \quad \begin{array}{ll} |\sigma_i(\alpha)| < c_i & \forall\, i = 1, \dots, r_1 \quad \text{and} \\ |\sigma_{j+r_1}(\alpha)|^2 \leq c_{j+r_1} & \forall\, j = 1, \dots, r_2 \end{array}$$

$$1 \leq |N_{K/\mathbb{Q}}(\alpha)| \leq \sigma_1(\alpha) c_2 \cdots c_{r_1+r_2} \Rightarrow |\sigma_1(\alpha)| > \frac{1}{c_2 \cdots c_{r_1+r_2}} > 1$$

and $|\sigma_i(\alpha)| < 1 \quad \forall\, i \neq 1 \Rightarrow \sigma_i(\alpha) \neq \sigma_1(\alpha) \quad \forall\, i \neq 1$

$\Rightarrow K = \mathbb{Q}(\alpha)$. (Otherwise, there would be $[K : \mathbb{Q}(\alpha)]$ embeddings $\sigma : K \hookrightarrow \mathbb{C}$ extending $\sigma_1|_{\mathbb{Q}(\alpha)}$.)

If $f \in \mathbb{Z}[X]$ is the min. poly. of α, then the coefficient of X in $f(X)$ is bounded in terms of $c_1, \dots, c_{r_1+r_2}$

$\Rightarrow$ $\exists$ only finitely many possibilities for $f(X)$

$\Rightarrow$ $\exists$ only finitely many K.

Case 2. $r_1 = 0$, $r_2 > 0$. Consider the region

$$X(c) = \left\{ z \in \mathbb{C}^{r_2} \mid |\mathrm{Re}\, z_1| < \tfrac{1}{2},\ |\mathrm{Im}\, z_1| < c \text{ and } |z_j|_{\mathbb{C}}^2 < \tfrac{1}{2} \text{ for } 2 \le j \le r_2 \right\}$$

Choose $c > 0$ s.t. $\mu(X(c)) = 2 \cdot c \cdot \left(\frac{\pi}{2}\right)^{r_2 - 1} > 2^{r_2} \cdot 2^{-r_2} \cdot \sqrt{|d|}$

$\longrightarrow$ get $0 \neq \alpha \in \mathcal{O}_K$ s.t. $\lambda(\alpha) \in \lambda(\mathcal{O}_K) \cap X(c)$

$$|\mathrm{Re}\, \sigma_i(\alpha)| < \tfrac{1}{2} \qquad |\mathrm{Im}\, \sigma_i(\alpha)| < c \qquad |\sigma_j(\alpha)|^2 < \tfrac{1}{2} \quad \text{for } 2 \le j \le r_2.$$

Since $|N(\alpha)| = \prod_{j=1}^{r_2} |\sigma_j(\alpha)|^2 \geq 1$,

$$\left(\tfrac{1}{4} + |\mathrm{Im}\, \sigma_1(\alpha)|^2\right) \cdot \left(\tfrac{1}{4}\right)^{r_2 - 1} \geq 1$$

$$|\mathrm{Im}\, \sigma_1(\alpha)| \geq 4^{r_2 - 1} - \tfrac{1}{4} \geqslant \tfrac{3}{4}$$

$$\Rightarrow \sigma_1(\alpha) \neq \sigma_j(\alpha) \quad \forall j \neq 1$$

Similarly we get $K = \mathbb{Q}(\alpha)$ and the minpoly of α has coeff. bounded in terms of c_1 which is indep. of K. □

Dirichlet's Theorem.

$$K^\times \geq \mathcal{O}_K^\times \supseteq \underbrace{(\mathcal{O}_K^\times)_{\mathrm{tors}}}_{=: W_K} = \left\{ x \in \mathcal{O}_K^\times \mid x^n = 1 \text{ for some } n \geq 1 \right\}$$

Lemma. 1) The group W_K is a finite cyclic group.

2) An element $u \in \mathcal{O}_K^\times$ belongs to W_K iff $|\sigma(u)|_{\mathbb{C}} = 1$ $\forall \sigma : K \hookrightarrow \mathbb{C}$.

PROOF: 1) If W_K is not cyclic, then it contains a subgroup of the form $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$ for some prime number p. (W_K is clearly finite since $K/\mathbb{Q}$ is finite.) (W_K consists of roots of unity.)

$\Rightarrow$ $x^p = 1$ has at least p^2 solutions in K, which is impossible.

2) It is clear that $\forall u \in W_K$: $|\sigma(u)|_{\mathbb{C}} = 1$ $\forall \sigma : K \hookrightarrow \mathbb{C}$ since u is a root of unity.

Conversely: if $u \in \mathcal{O}_K$ s.t. $|\sigma_i(u)| = 1$ then all conjugates of u have norm 1 for all complex embeddings.

So the minimal polynomial of u over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$ and its x^i-th term is bounded by $\binom{n}{i}$, where $n = [K:\mathbb{Q}]$.

$\Rightarrow W = \{ x \in \mathcal{O}_K \mid |\sigma(x)|_{\mathbb{C}} = 1 \ \forall \sigma : K \hookrightarrow \mathbb{C} \}$ is a finite set.

If $u \in W$ then $u^k \in W \ \forall k \geq 1 \Rightarrow \exists k' > k$ s.t. $u^{k'} = u^k$

$\Rightarrow u^{k'-k} = 1 \Rightarrow u \in W_K$. □

13.11.2017

Theorem. (Dirichlet) The quotient $\mathcal{O}_K^\times / W_K$ is a free abelian group of rank $r_1 + r_2 - 1$, i.e. $\exists \eta_1, \dots, \eta_{r_1+r_2-1} \in \mathcal{O}_K^\times$ s.t. $\forall x \in \mathcal{O}_K^\times$ writes uniquely as $x = u \cdot \eta_1^{a_1} \cdots \eta_{r_1+r_2-1}^{a_{r_1+r_2-1}}$ where $a_1, \dots, a_{r_1+r_2-1} \in \mathbb{Z}$.

Rmk. The choice of these η_i is not unique in general.

However, if $r_1 + r_2 - 1 = 1$ then there exists a unique $\varepsilon \in \mathcal{O}_K^\times$, $\varepsilon > 1$ s.t. $\mathcal{O}_K^\times = W_K \times \varepsilon^{\mathbb{Z}}$.

(To make sense of $\varepsilon > 1$, note that $r_1 + r_2 = 2 \Leftrightarrow r_1 = r_2 = 1$ or $r_1 = 2, r_2 = 0$ ... nope, this is not the explanation, sorry.)

$\varepsilon > 1$ means that for a fixed real embedding $K \hookrightarrow \mathbb{R}$ the inequality holds.

This ε is called the fundamental unit of $\mathcal{O}_K$.

Example. $K = \mathbb{Q}(\sqrt{2})$, $\varepsilon = \sqrt{2}+1$, $\mathcal{O}_K = \{\pm 1\} \times \{1+\sqrt{2}\}^{\mathbb{Z}}$

Pf: Suppose $\exists\, x + \sqrt{2}\, y \in \mathcal{O}_K^\times$ with $1 < x + y\sqrt{2} < 1 + \sqrt{2}$

$\Rightarrow x - 1 < \sqrt{2}(1 - y)$. One of x and y is positive

- If $x > 0 \Rightarrow x \geq 2 \Rightarrow y < 0$

  $x - y\sqrt{2} > x + y\sqrt{2} > 1$

  $N_{K/\mathbb{Q}}(x - y\sqrt{2}) = (x + y\sqrt{2})(x - y\sqrt{2}) > 1$

  But a unit must have norm ± 1.

- If $y > 0 \Rightarrow y \geq 2 \Rightarrow x \leq -1$.

  $|-x + y\sqrt{2}| > |x + y\sqrt{2}| > 1$

  $N_{K/\mathbb{Q}}(x + \sqrt{2}\, y) = |-x + y\sqrt{2}| \cdot |x + \sqrt{2}\, y| > 1$

$\Rightarrow x + y\sqrt{2}$ is not a unit. □

PROOF OF DIRICHLET'S THM:

Let $\sigma_1, \dots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$ be the real embeddings of K,

σ_{r_1+j}, $\sigma_{r_1+j+r_2} = \overline{\sigma}_{r_1+j} : K \hookrightarrow \mathbb{C}$ the complex emb., $1 \le j \le r_2$.

Recall that $\lambda : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

$$x \longmapsto (\sigma_i(x))_{i=1}^{r_1+2r_2}$$

$$\ell : \mathcal{O}_K^\times \hookrightarrow (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^{r_2})^\times \xrightarrow{\text{Log}} \mathbb{R}^{r_1+r_2}$$

$$(y_i, z_j) \longmapsto (\log y_i, 2\log|z_j|)$$

$1 \le i \le r_1, \quad 1 \le j \le r_2$

Facts. (1) $\ker(\ell) = \{ x \in \mathcal{O}_K^\times \mid \log|\sigma_i(x)| = 0 \quad \forall\, 1 \le i \le r_1 + 2r_2 \}$

$= \{ x \in \mathcal{O}_K^\times \mid |\sigma_i(x)| = 1 \quad \forall\, 1 \le i \le r_1 + 2r_2 \}$

$= W_K$ (Lemma)

(2) $\operatorname{Im}(\ell) \subseteq H = \left\{ x \in \mathbb{R}^{r_1+r_2} \;\middle|\; \sum_{i=1}^{r_1+r_2} x_i = 0 \right\}$

If $x \in \mathcal{O}_K^\times$, then

$$\ell(x) = \left((\log|\sigma_i(x)|)_{1 \le i \le r_1}, \left(2\log|\sigma_{r_1+j}(x)|\right)_{1 \le j \le r_2} \right)$$

$$\sum_{i=1}^{r_1} \log|\sigma_i(x)| + \sum_{j=1}^{r_2} 2\log|\sigma_{r_1+j}(x)| =$$

$$= \log\left(\prod_{i=1}^{r_1} |\sigma_i(x)| \cdot \prod_{j=1}^{r_2} |\sigma_{r_1+j}(x)|^2 \right) = \log\left(N_{K/\mathbb{Q}}(x) \right) = \log 1 = 0$$

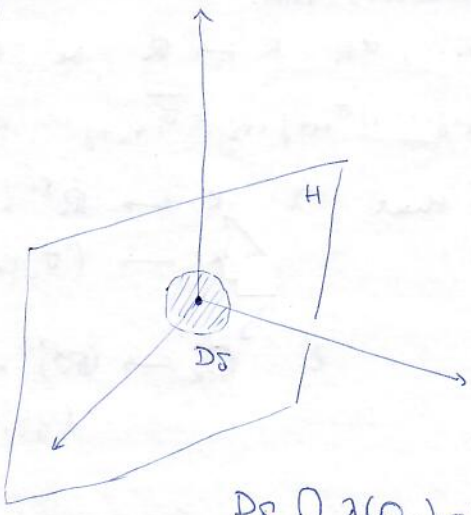
Let $\ell(x) = 0$.

To finish the proof of Dirichlet's theorem, sts. $\operatorname{Im}(\ell)$ is a full lattice in $H \simeq \mathbb{R}^{r_1+r_2-1}$ $\Rightarrow$ $\operatorname{Im}(\ell) \simeq \mathcal{O}_K^\times / \ker(\ell) = \mathcal{O}_K^\times / W_K$ is a free ab. group of rank $r_1 + r_2 - 1$.

We have to check two things:

I) $\mathrm{Im}(\ell)$ is a discrete subgroup of H

II) $\mathrm{rk}_{\mathbb{Z}} \mathrm{Im}(\ell) = r_1 + r_2 - 1$



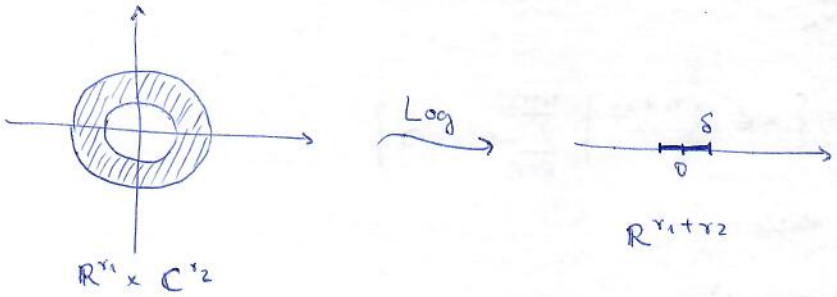
$D_\delta \cap \lambda(\mathcal{O}_K) = \{0\}$

I) $\forall \delta \in \mathbb{R}_{>0}$

$$B_\delta := \{ (y,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid e^{-\delta} \le |y_i| \le e^{\delta}, \; e^{-\delta} \le |z_j|^2 \le e^{\delta} \}$$

$B_\delta \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ compact set

$$\mathrm{Log}\, B_\delta = \{ x \in \mathbb{R}^{r_1+r_2} \mid |x_i| \le \delta \} = D_\delta$$



Known: $\lambda(\mathcal{O}_K) \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as a lattice

$\lambda(\mathcal{O}_K^\times) \cap B_\delta$ is a finite set $\subseteq \lambda(\mathcal{O}_K) \cap B_\delta$

$D_\delta \cap \ell(\mathcal{O}_K^\times) = \mathrm{Log} \circ \lambda(\mathcal{O}_K^\times) \cap D_\delta = \mathrm{Log}\left(\lambda(\mathcal{O}_K^\times) \cap B_\delta\right)$ is also finite

Let $\delta \searrow 0$ $\Rightarrow$ $\lambda(\mathcal{O}_K^\times) \cap B_\delta = \lambda(\mathcal{O}_K^\times) \cap B_0$ if δ is sufficiently small

$\Rightarrow$ for suff. small δ: $D_\delta \cap \ell(\mathcal{O}_K^\times) = D_0 \cap \ell(\mathcal{O}_K^\times) = \{0\}$

$\Rightarrow$ $\ell(\mathcal{O}_K^\times)$ is discrete in $\mathbb{R}^{r_1+r_2}$, hence in H. ✓

II) Claim: $\ell(\mathcal{O}_K^\times)$ has rk at least r_1+r_2-1

Lemma. $\forall\, k \in \mathbb{Z}$ with $1 \le k \le r_1+r_2$ $\exists\, u_k \in \mathcal{O}_K^\times$ s.t. $|\sigma_k(u_k)| > 1$,

and $\forall\, 1 \le i \le r_1+r_2$, $i \neq k$: $|\sigma_i(u_k)| < 1$.

PROOF: Consider the region

$$X(c) = \left\{ (y,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \;\middle|\; |y_i| \le c_i,\ |z_j| \le c_{r_1+j} \quad \begin{matrix} 1 \le i \le r_1 \\ 1 \le j \le r_2 \end{matrix} \right\}$$

$$\mathrm{Vol}\left(X(c)\right) = \prod_{i=1}^{r_1} (2c_i) \prod_{j=1}^{r_2} (\pi c_{r_1+j}) = 2^{r_1} \pi^{r_2} \prod_{i=1}^{r_1+r_2} c_i$$

Choose c_i s.t. $c_i < 1 \quad \forall i \neq \ell$ and $c_\ell := A \Big/ \prod_{i \neq \ell} c_i$

for some $A > \left(\frac{2}{\pi}\right)^{r_2} \cdot (d_K)^{1/2}$

Then $\mathrm{Vol}\left(X(c)\right) = 2^{r_1} \pi^{r_2} A > 2^{r_1} \pi^{r_2} \cdot \left(\frac{2}{\pi}\right)^{r_2} \sqrt{d_K} =$

$$= 2^n \cdot \frac{1}{2^{r_2}} \mathrm{Vol}\left(\mathbb{R}^n / \lambda(\mathcal{O}_K)\right)$$

Minkowski's Lemma $\Rightarrow \exists\, a_1 \in \mathcal{O}_K \setminus \{0\}$ s.t. $\lambda(a_1) \in \lambda(\mathcal{O}_K) \cap X(c)$.

Then: $|\sigma_i(a_1)| \le c_i \quad 1 \le i \le r_1$,

$|\sigma_j(a_1)| \le c_j \quad r_1+1 \le j \le r_1+r_2$

Put $c_i^{(1)} := |\sigma_i(a_1)|, \quad 1 \le i \le r_1, \quad i \neq \ell$,

$c_j^{(1)} := |\sigma_j(a_1)|, \quad r_1+1 \le j \le r_1+r_2, \quad j \neq \ell$

$c_\ell^{(1)} := A \Big/ \prod_{i \neq \ell} c_i^{(1)}$

Applying the same argument to $c_i^{(1)}$, we get $a_2 \in \mathcal{O}_K \setminus \{0\}$:

$$|\sigma_i(a_2)| < c_i^{(1)} = |\sigma_i(a_1)| \quad \forall i \neq \ell$$

For $i = \ell$: $1 \le |N_{K/\mathbb{Q}}(a_2)| = \prod_{i=1}^{r_1} |\sigma_i(a_2)| \prod_{j=r_1+1}^{r_2} |\sigma_j(a_2)| < \prod_{i=1}^{r_1+r_2} c_i^{(1)} = A$

Repeating this process, we get a sequence of nonzero elements

$a_1, a_2, \dots, a_n, a_{n+1}$ s.t. $|\sigma_i(a_{n+1})| < |\sigma_i(a_n)| \quad \forall i \neq \ell$,

$$|N_{K/\mathbb{Q}}(a_n)| < A.$$

Since there are only fin. many integral ideals of $\mathcal{O}_K$ with norm $< A$, $\exists\, m > n$ s.t. $(a_m) = (a_n)$.

$u_\ell := a_m / a_n \in \mathcal{O}_K^\times \Rightarrow |\sigma_i(u_\ell)| = \dfrac{|\sigma_i(a_m)|}{|\sigma_i(a_n)|} < 1 \quad \forall i \neq \ell$,

$$1 = |N_{K/\mathbb{Q}}(u_\ell)| \Rightarrow |\sigma_\ell(u_\ell)| > 1.$$

□

For $1 \le k \le r_1 + r_2$, let $u_k \in \mathcal{O}_K^\times$ be given by the previous Lemma.

$\ell(u_k) \in \mathbb{R}^{r_1+r_2}$ viewed as a column vector.

Then the diagonal entries of the matrix $\left(\ell(u_1), \ell(u_2), \dots, \ell(u_{r_1+r_2})\right) \in M_{r_1+r_2}(\mathbb{R})$ are positive, and all other entries are negative.

We finish the proof by the following:

Lemma. Let $A = (a_{ij})_{1 \le i,j \le r} \in M_r(\mathbb{R})$. Assume the following.

- $a_{ii} > 0 \quad \forall i$
- $a_{ij} < 0 \quad \forall i \ne j$
- $\sum_{i=1}^{r} a_{ij} = 0 \quad \forall j$

Then $\operatorname{rk} A = r - 1$.

Pf: Suffices to show that the first $r-1$ row vectors are $\mathbb{R}$-linearly independent.

$\nexists\, x_i \in \mathbb{R}$, $1 \le i \le r-1$ (not all zero) s.t. $\sum_{i=1}^{r-1} x_i a_{ij} = 0 \quad \forall j$

Put $j = r \Rightarrow a_{i,r} < 0 \quad \forall 1 \le i \le r-1 \Rightarrow$ not all x_i are pos. or neg.

Let $1 \le j_0 \le r-1$ s.t. $x_{j_0} = \max_j x_j > 0$.

Then $0 = \sum_{i=1}^{r-1} x_i a_{ij_0} = x_{j_0} \underbrace{\sum_{i=1}^{r-1} a_{ij_0}}_{>0} + \underbrace{\sum_{\substack{i=1 \\ i \ne j_0}}^{r-1} (x_i - x_{j_0}) a_{ij_0}}_{\ge 0}$

$\sum_{i=1}^{r-1} a_{ij_0} = -a_{rj_0} > 0$

$\Rightarrow x_{j_0} \cdot \sum_{i=1}^{r-1} a_{ij_0} > 0, \quad (x_i - x_{j_0}) a_{ij_0} \ge 0 \quad \forall i \ne j$

$0 > 0$ ↯

This finishes the proof of the thm. □

Algebraic Number Theory, Lecture 10-11

Regulator

Let $\eta_1, \dots, \eta_{r_1+r_2-1}$ be a system of fundamental units s.t.

$$\mathcal{O}_K^\times = W_K \times \eta_1^{\mathbb{Z}} \times \dots \times \eta_{r_1+r_2-1}^{\mathbb{Z}}, \qquad \ell(\eta_1), \dots \ell(\eta_{r_1+r_2-1}) \in H \subseteq \mathbb{R}^{r_1+r_2}$$

Choose $\vec{n} = (x_i) \in \mathbb{R}^{r_1+r_2}$ s.t. $\sum_i x_i = 1$, e.g. $\vec{n} = \frac{1}{r_1+r_2} \cdot (1, \dots, 1)$.

Define the regulator of K to be

$$R_K := \left| \det\left(\vec{n}, \ell(\eta_1), \dots, \ell(\eta_{r_1+r_2-1})\right) \right| \in \mathbb{R}_{>0}.$$

Example. $K = \mathbb{Q}(\sqrt{2})$ $\quad \mathcal{O}_K^\times = \{\pm 1\} \times (1+\sqrt{2})^{\mathbb{Z}}$

$$R_K = \left| \det \begin{pmatrix} 1/2 & \log(1+\sqrt{2}) \\ 1/2 & -\log(1+\sqrt{2}) \end{pmatrix} \right| = \log(1+\sqrt{2})$$

In general, if ε is the fund. unit of a real quadratic field K, then $R_K = \log \varepsilon$.

Next case: cubic field, $r_1 = 1$, $(r_2 = 1, \quad r_1 + r_2 - 1 = 1.)$

$\sigma_1 : K \hookrightarrow \mathbb{R}$.

There is a unique $\varepsilon \in \mathcal{O}_K^\times$, $\varepsilon > 1$ s.t. $\mathcal{O}_K^\times = W_K \times \varepsilon^{\mathbb{Z}}$. (Hard to find.)

Theorem. (Artin) $K/\mathbb{Q}$ cubic field with $r_1 = 1$.

If $\sigma > 1$, $\sigma \in \mathcal{O}_K^\times$ then $|d_K| < 4\sigma^3 + 24$.

PO, see K. Conrad's note on Dirichlet's Thm.

Idea: $|d_K| \le |\mathrm{disc}(1, \sigma, \sigma^2)|$, show that $|\mathrm{disc}(1, \sigma, \sigma^2)| < 4\sigma^3 + 24$. □

Corollary: If $\vartheta \in \mathcal{O}_K^\times$, $\vartheta > 1$ and $4\vartheta^{3/2} + 24 < |d_K|$ then $\vartheta = \varepsilon$ is the fundamental unit of K.

Pf: In general, $\vartheta = \varepsilon^k$, $k \ge 1$.

Apply Artin's Thm to $\sigma = \varepsilon$.

$$|d_K| < 4\varepsilon^3 + 24 = 4\vartheta^{3/2} + 24$$

$$\Rightarrow \quad \vartheta^{3/2} < \vartheta^{3k/2} \quad \Rightarrow \quad 2 > 3k \quad \Rightarrow \quad k = 1. \qquad \square$$

Example. $K = \mathbb{Q}(\sqrt[3]{2})$ $\quad d_K = -2^2 \cdot 3^3 = -108$

$\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ $\quad \mathcal{O}_K \ni u = \sqrt[3]{2} - 1 < 1$

$$\vartheta := \frac{1}{u} = 1 + \sqrt[3]{2} + \sqrt[3]{4} \approx 3.847$$

$$4\vartheta^{3/2} + 24 < |d_K| = 108 \quad \Rightarrow \mathcal{O}_K^\times = \{\pm 1\} \times \vartheta^{\mathbb{Z}}$$

16.11.2017

$K/\mathbb{Q}$ number field

Def. $t \in \mathbb{R}_{>0}$: $N(t) = \#\{ I \subseteq \mathcal{O}_K \text{ ideal} \mid \#(\mathcal{O}_K/I) = N_{K/\mathbb{Q}}(I) = N(I) \leq t \}$

What is the asymptotic behaviour of $N(t)$ as $t \to +\infty$?

Ex. $K = \mathbb{Q}$: $N(t) = [t] \sim t \quad (t \to \infty)$
$= t + O(1)$

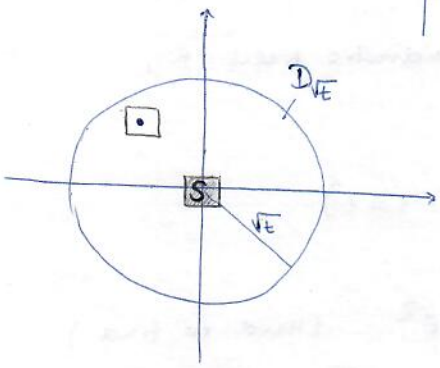
Ex. $K = \mathbb{Q}(i)$ $\mathcal{O}_K = \mathbb{Z}[i]$ PID

$I = (\alpha)$, $\alpha \in \mathcal{O}_K$, $(\alpha) = (\beta) \iff \alpha/\beta \in \mathcal{O}_K^\times$.

$N(t) = \#\{ \alpha \in \mathcal{O}_K \mid |N(\alpha)| \leq t \} \cdot \frac{1}{|\mathcal{O}_K^\times|} = \frac{1}{4} \cdot \#\{ \alpha \in \mathcal{O}_K \mid |N(\alpha)| \leq t \} =$

$\mathcal{O}_K \hookrightarrow \mathbb{C} \cong \mathbb{R}^2$
$a + b\sqrt{-1} \longmapsto (a,b)$

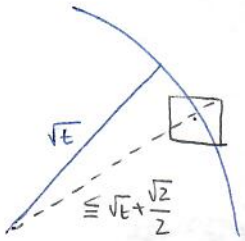
$= \frac{1}{4} \#\{ (a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 \leq t \}$



$S = \{ (x,y) \in \mathbb{R}^2 \mid |x| \leq 1/2, \ |y| \leq 1/2 \}$ square

$$\bigsqcup_{\substack{(a,b) \in \mathbb{Z}^2 \\ a^2+b^2 \leq t}} \left((a,b) + S \right) \subseteq D_{\sqrt{t} + \frac{\sqrt{2}}{2}}$$

$$\bigsqcup_{\substack{(a,b) \in \mathbb{Z}^2 \\ a^2+b^2 \leq t}} \left((a,b) + S \right) \supseteq D_{\sqrt{t} - \frac{\sqrt{2}}{2}}$$



$$\mu\left(D_{\sqrt{t} - \frac{\sqrt{2}}{2}} \right) \leq \sum_{\substack{(a,b) \in \mathbb{Z}^2 \\ a^2+b^2 \leq t}} \overbrace{\mu(S)}^{1} \leq \mu\left(D_{\sqrt{t} + \frac{\sqrt{2}}{2}} \right)$$

$$\pi t - \pi\sqrt{t} + \frac{1}{2} \leq 4 N(t) \leq \pi \left(\sqrt{t} + \frac{\sqrt{2}}{2} \right)^2 = \pi t + \pi\sqrt{t} + \frac{1}{2}$$

$$\Rightarrow \quad N(t) = \frac{\pi}{4} t + O\left(\sqrt{t}\right)$$

Thm. 1. $K/\mathbb{Q}$ number field, $[K:\mathbb{Q}] = n$, r_1 real embeddings, r_2 pairs of complex embeddings. Then $N(t) = \dfrac{2^{r_1} (2\pi)^{r_2} \cdot R_K \, h}{w \cdot \sqrt{|d_K|}} \cdot t + O\left(t^{1 - \frac{1}{n}}\right)$

where R_K is the regulator, $h = \# Cl_K$, $w = \# W_K$ and d_K is the discriminant.

(In the above cases, this formula gives exactly what we have computed.)

Algebraic Number Theory, lecture 11

Variant. Let C be an equivalence class of fractional ideals in Cl_K

$$N_C(t) = \{ I \subseteq \mathcal{O}_K \text{ ideal}, \ I \in C \mid N(I) \le t \}$$

Similarly, we have a formula:

Thm. 2.
$$N_C(t) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot R_K}{w \cdot \sqrt{|d_K|}} \cdot t + O\left(t^{1-\frac{1}{n}}\right)$$

Note that $N_C(t)$ is independent of C and Thm. 2 $\Rightarrow$ Thm. 1.

Lemma 3. Let $\mathfrak{J}$ be a fractional ideal in C^{-1}.

Let $S_t = \{ x \in \mathfrak{J} \mid |N_{K/\mathbb{Q}}(x)| \le t \cdot N(\mathfrak{J}) \} / \mathcal{O}_K^\times$

Then $\alpha \mapsto \alpha \mathfrak{J}^{-1}$ induces a bijection $S_t \xrightarrow{\sim} \{ I \subseteq \mathcal{O}_K, I \in C \mid N(I) \le t \}$

Pf: $S_t \simeq \{$ principal fractional ideals $(\alpha) \subseteq \mathfrak{J}$ with $|N_{K/\mathbb{Q}}(\alpha)| \le t \cdot N(\mathfrak{J}) \} \simeq \{ I \subseteq \mathcal{O}_K, I \in C \mid N(I) \le t \}$

$$\alpha \longmapsto (\alpha) \qquad \underbrace{I}_{(\alpha) \cdot \mathfrak{J} \subseteq \mathcal{O}_K} \qquad I \cdot \mathfrak{J} \subseteq \mathfrak{J}$$

I

□

So we may control the cardinality of S_t, which is much easier than using the original definition for $N_C(t)$.

From now on, fix a fractional ideal $\mathfrak{J}$ in C^{-1}. $\quad N_C(t) = \# S_t$

Pf of Thm 2 in the real quadratic case:

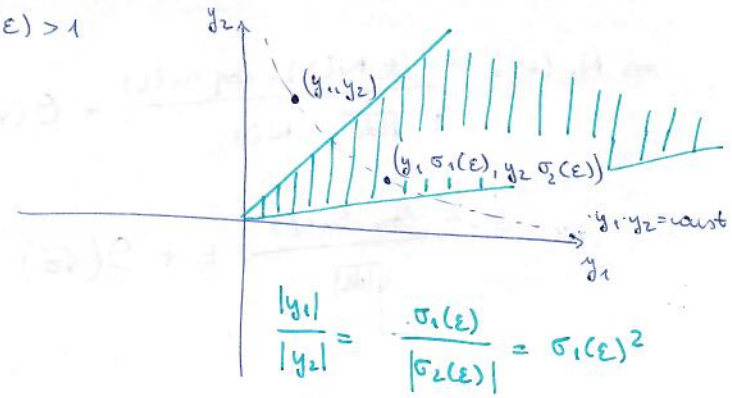
Let $K/\mathbb{Q}$ be a real quadratic extension.

$\mathcal{O}_K^\times = \{ \pm 1 \} \times \varepsilon^{\mathbb{Z}}$ for some fundamental unit ε in $\mathcal{O}_K^\times$

$$\lambda: \quad K \hookrightarrow \mathbb{R}^2$$
$$\alpha \longmapsto (\sigma_1(\alpha), \sigma_2(\alpha))$$
$$\cup$$
$$\mathfrak{J} \longmapsto \lambda(\mathfrak{J})$$

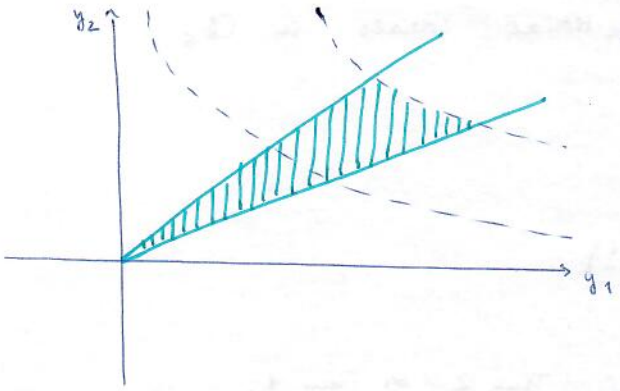
$$\mathrm{Vol}\left(\mathbb{R}^2 / \lambda(\mathfrak{J})\right) = \sqrt{|d_K|} \cdot N(\mathfrak{J})$$

$\sigma_1(\varepsilon) > 1$



$$\frac{|y_1|}{|y_2|} = \frac{\sigma_1(\varepsilon)}{|\sigma_2(\varepsilon)|} = \sigma_1(\varepsilon)^2$$

$\forall\, y_0 = (y_1, y_2) \in \mathbb{R}^2 \setminus \{0,0\}$ $\quad \exists!\ \pi \in \mathbb{Z}$ s.t. $y_0 \cdot \lambda(\varepsilon)^\pi \in \left\{ y=(y_1,y_2)\in\mathbb{R}^2 \;\middle|\; 1 < \frac{|y_1|}{|y_2|} = \frac{\sigma_1(\varepsilon)}{|\sigma_2(\varepsilon)|} = \sigma_1(\varepsilon)^2 \right\}$



Note that $|\sigma_1(\varepsilon)\,\sigma_2(\varepsilon)| = |N_{K/\mathbb{Q}}(\varepsilon)| = 1$.

Every element $\alpha \in \mathcal{I}$ with $N_{K/\mathbb{Q}}(\alpha) \le t \cdot N(\mathcal{I})$ is equivalent, under the action of $\mathcal{E}^{\mathbb{Z}}$, to a unique element in $\mathcal{I} \cap D_{tN(\mathcal{I})}$.

Where $D_{tN(\mathcal{I})} = \left\{ (y_1,y_2)\in\mathbb{R}^2 \;\middle|\; |y_1 y_2| \le tN(\mathcal{I}) \text{ and } 1 \lneq \frac{|y_1|}{|y_2|} < \sigma_1(\varepsilon)^2 \right\}$

$$S_t \xrightarrow{\sim} \lambda(\mathcal{I}) \cap D_{tN(\mathcal{I})} \,/\, \{\pm 1\}$$

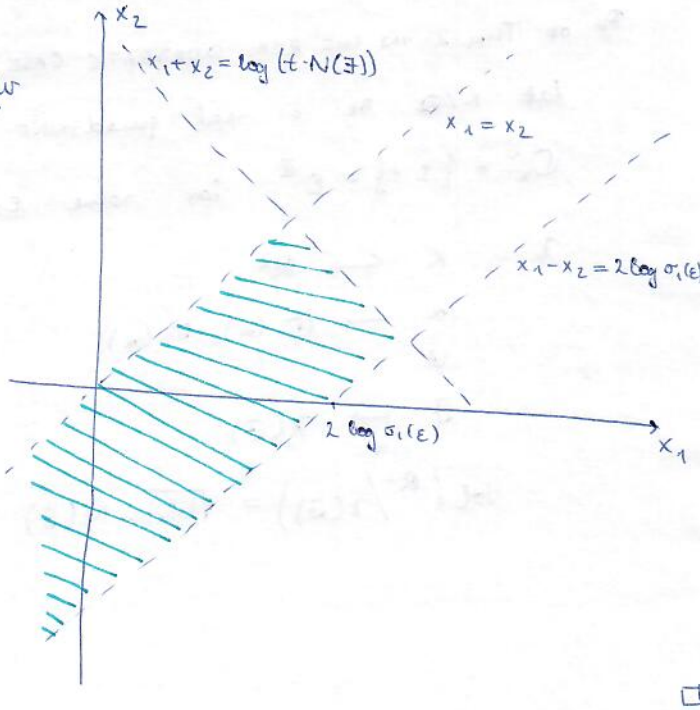
$$N_c(t) = \#S_t = \frac{\#\left(\lambda(\mathcal{I}) \cap D_{tN(\mathcal{I})}\right)}{2}$$

$$= \frac{\mu\left(D_{tN(\mathcal{I})}\right)}{2 \cdot \mathrm{Vol}\left(\mathbb{R}^2/\lambda(\mathcal{I})\right)} + \theta(\sqrt{t})$$

$$\mu\left(D_{tN(\mathcal{I})}\right) = 4 \int_{\substack{y_1,y_2>0 \\ 0<y_1y_2\le N(\mathcal{I})\cdot t \\ 1<\frac{y_1}{y_2}\le \sigma_1(\varepsilon)^2}} dy_1\, dy_2$$

change of variables
$y_i = e^{x_i}$
$dy_i = e^{x_i}\, dx_i$

$$= 4 \int_{\substack{x_1+x_2 \le \log(N(\mathcal{I})\cdot t) \\ 0<x_1-x_2\le 2\log(\sigma_1(\varepsilon))}} e^{x_1+x_2}\, dx_1\, dx_2$$



$$\mu\left(D_{tN(\mathcal{I})}\right) = 4 \int_0^{2\log\sigma_1(\varepsilon)} \int_{u=-\infty}^{\log(tN(\mathcal{I}))} e^u \cdot \frac{du\,dv}{2}$$

Change of var.:
$u = x_1 + x_2$
$v = x_1 - x_2$
$du\,dv = 2\,dx_1\,dx_2$

$$= 4\, tN(\mathcal{I}) \log\sigma_1(\varepsilon)$$

$$\Rightarrow N_c(t) = \frac{4 \cdot tN(\mathcal{I}) \cdot \log\sigma_1(\varepsilon)}{2\sqrt{|d_K|}\cdot N(\mathcal{I})} + \theta(\sqrt{t})$$

$$= \frac{2\log\sigma_1(\varepsilon)}{\sqrt{|d_K|}} \cdot t + \theta(\sqrt{t})$$

□

Algebraic Number Theory, lecture 11

Preliminaries for Theorem 2.

Def. A function $f: [0,1]^{n-1} \longrightarrow \mathbb{R}^n$ is called **Lipschitz** if

$$\frac{|f(x) - f(y)|}{|x-y|}$$

is uniformly bounded $\forall x, y \in [0,1]^{n-1}$, $x \neq y$.

$C^1 \Rightarrow$ Lipschitz $\Rightarrow$ continuous follows from the definition.

Def. Let $B \subseteq \mathbb{R}^n$ be a bounded region.

$B^{int} = \{ x \in B \mid \exists$ open nbh $x \in U_x \subseteq B \}$, interior,

$\partial B = \overline{B} \setminus B^{int}$ boundary.

We say that ∂B is **$(n-1)$-Lipschitz parametrisable** if it is covered by the images of finitely many Lipschitz functions $f_i: [0,1]^{n-1} \longrightarrow \mathbb{R}^n$.

Lemma. (Marcus: Number fields, Chap. 6, Lemma 2)

Let B be a bounded region in $\mathbb{R}^n$ s.t. ∂B is $(n-1)$-Lipschitz parametrisable, and $\Lambda \subseteq \mathbb{R}^n$ a full lattice

Then $\forall a > 1$ we have $\#(\Lambda \cap aB) = \dfrac{\mu(B)}{\mathrm{Vol}(\mathbb{R}^n/\Lambda)} \cdot a^n + O(a^{n-1})$.

Pf: PO, just pure analysis. Cover the space with small cubes, as we did in $\mathbb{R}^2$. The Lipschitz condition is used to control the error term. □

Pf of THM 2: $K/\mathbb{Q}$ number field, $r_1 + 2r_2 = n$

$$\begin{array}{ccc} K & \xrightarrow{\lambda} & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ \alpha & \longmapsto & \left((\sigma_i(\alpha))_{1 \le i \le r_1}, (\sigma_{r_1+j}(\alpha))_{1 \le j \le r_2} \right) \\ \cup & & \\ \mathfrak{I} & \longmapsto & \lambda(\mathfrak{I}) \end{array}$$

$\mathfrak{I}$: frac. ideal in $\mathcal{C}^{-1}$; $\lambda(\mathfrak{I})$: lattice

$$\forall t > 0: \quad X_t = \left\{ (y, z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \;\middle|\; \left(\prod_{i=1}^{r_1} |y_i| \right) \cdot \left(\prod_{j=1}^{r_2} |z_j|^2 \right) \le t \cdot N(\mathfrak{I}) \right\}$$

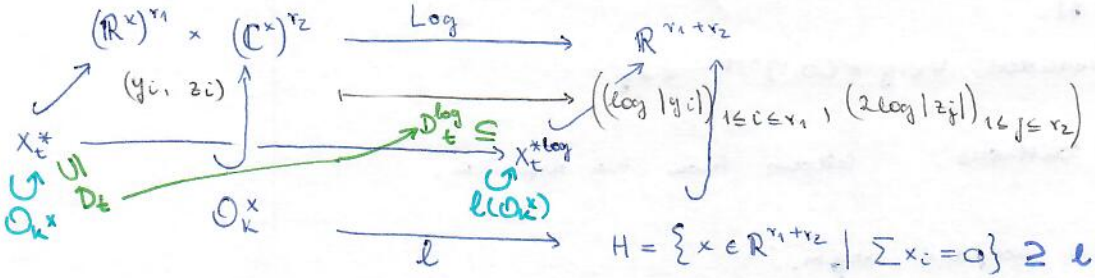
$$\forall \alpha \in K: \quad \lambda(\alpha) \in X_t \iff |N_{K/\mathbb{Q}}(\alpha)| \le t \cdot N(\mathfrak{I})$$

$$N_{\mathcal{C}}(t) = \# \left(\left\{ \alpha \in \mathfrak{I} \mid |N_{K/\mathbb{Q}}(\alpha)| \le t \cdot N(\mathfrak{I}) \right\} \Big/ \mathcal{O}_K^\times \right) = \# \left(\lambda(\mathfrak{I}) \cap X_t \Big/ \mathcal{O}_K^\times \right)$$

Note that $\lambda(\mathcal{I}\setminus\{0\}) \subseteq (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$

$$X_t^* = X_t \cap \left((\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}\right) \circlearrowleft \mathcal{O}_K^\times$$

Choose $\eta_1, \dots, \eta_{r_1+r_2-1} \in \mathcal{O}_K^\times$ s.t. $\mathcal{O}_K^\times = W_K \times \prod_{i=1}^{r_1+r_2-1} \eta_i^{\mathbb{Z}}$



$$X_t^{*\log} = \mathrm{Log}(X_t^*) = \left\{x \in \mathbb{R}^{r_1+r_2} \,\middle|\, \sum_{i=1}^{r_1+r_2} x_i \le \log\left(tN(\mathcal{I})\right)\right\}$$

$$X_t^* = \mathrm{Log}^{-1}(X_t^{*\log})$$

$$\ell(\mathcal{O}_K^\times) = \sum_{i=1}^{r_1+r_2-1} \mathbb{Z}\,\ell(\eta_i) \subseteq H$$

$$\vec{n} = \frac{1}{r_1+r_2}\cdot(1,\dots,1) \in \mathbb{R}^{r_1+r_2}$$

Then $\left(\vec{n}, \ell(\eta_1), \dots, \ell(\eta_{r_1+r_2-1})\right)$ form a basis of $\mathbb{R}^{r_1+r_2}$

A fundamental region of $X_t^{*\log}$ under $\ell(\mathcal{O}_K^\times)$ is given by

$$D_t^{\log} := \left\{ t_0\vec{n} + t_1\ell(\eta_1) + \dots + t_{r_1+r_2-1}\cdot\ell(\eta_{r_1+r_2-1}) \,\middle|\, t_0 \in (-\infty, \log(tN(\mathcal{I}))),\ 0 < t_i \le 1 \quad \forall i = 1,\dots,r_1+r_2-1 \right\}.$$

Now $D_t := \mathrm{Log}^{-1}(D_t^{\log})$ is a fundamental domain of X_t^* under the action of $\prod_{i=1}^{r_1+r_2-1} \eta_i^{\mathbb{Z}} \subseteq \mathcal{O}_K$

$D_t \circlearrowleft W_K$ free action

$$N_c(t) = \#\left(\lambda(\mathcal{I}) \cap X_t^* \,/\, \mathcal{O}_K^\times\right)$$

$$= \#\left(\lambda(\mathcal{I}) \cap D_t \,/\, W_K\right)$$

$$= \frac{\#\left(\lambda(\mathcal{I}) \cap D_t\right)}{w}. \qquad (\text{recall that } w = \#W_K)$$

Note that $D_t = t^{1/n} D_1$, and ∂D_1 is $(n-1)$-Lipschitz parametrisable.

Marcus' Lemma $\Rightarrow$ $$N_c(t) = \frac{\mu(D_1)}{w\cdot \mathrm{Vol}\left(\mathbb{R}^n/\lambda(\mathcal{I})\right)}\cdot\left(t^{1/n}\right)^n + \mathcal{O}\left(t^{\frac{n-1}{n}}\right)$$

Lemma. $\mu(D_1) = 2^{r_1} \cdot \pi^{r_2} \, R_K \cdot N(\mathfrak{J})$.

By assuming this Lemma, we can finish the proof of Thm-2:

$$N_C(t) = \frac{2^{r_1} \cdot \pi^{r_2} \cdot R_K \cdot N(\mathfrak{J})}{w \cdot \frac{1}{2^{r_2}} \cdot \sqrt{|d_K|} \cdot N(\mathfrak{J})} \cdot t + O\left(t^{1-\frac{1}{n}}\right)$$

$$= \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot R_K}{w \cdot \sqrt{|d_K|}} \cdot t + O\left(t^{1-\frac{1}{n}}\right)$$

PF OF LEMMA: $D_1 \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

Lebesgue measure on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is given by $dy_1 \cdots dy_{r_1} \, d\mu_1 \cdots d\mu_{r_2}$

$d\mu_j = \rho_j \, d\rho_j \, d\vartheta_j$ $\qquad z_j = \rho_j \cdot e^{i\vartheta_j}$ polar coordinates

$$\mu(D_1) = \int_{D_1} dy_1 \cdots dy_{r_1} \, d\mu_1 \cdots d\mu_{r_2} =$$

$$= \int_{D_1} dy_1 \cdots dy_{r_1} \, \rho_1 \cdots \rho_{r_2} \, d\rho_1 \cdots d\rho_{r_2} \, d\vartheta_1 \cdots d\vartheta_{r_2}$$

$D_1 = \log^{-1}(D_1^{\log})$, $\quad D_1^{\log} \subseteq \mathbb{R}^{r_1+r_2}$

Change of variables:

$x_i := \log |y_i|, \quad 1 \le i \le r_1$

$x_{j+r_1} := 2\log |z_j| = 2\log \rho_j \quad 1 \le j \le r_2$

$\rho_j = e^{\frac{1}{2} x_{r_1+j}}, \quad d\rho_j = \frac{1}{2} e^{\frac{1}{2} x_{r_1+j}} \, dx_{r_1+j}, \quad dy_i = e^{x_i} dx_i$

$$\mu(D_1) = 2^{r_1} (2\pi)^{2r_2} \int_{D_1^{\log}} e^{x_1 + \cdots + x_{r_1}} dx_1 \cdots dx_{r_1} \, e^{\sum_j x_{r_1+j}} dx_{r_1+1} \cdots dx_{r_1+r_2} =$$

$$= 2^{r_1} \cdot (2\pi)^{2r_2} \int_{D_1^{\log}} e^{\sum_{i=1}^{r_1+r_2} x_i} dx_1 \cdots dx_{r_1+r_2}.$$

Yet another change of variables: define $t_0, \ldots, t_{r_1+r_2-1}$ by

$$\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_{r_1+r_2} \end{pmatrix} = (\vec{n}, \ell(\eta_1), \ldots, \ell(\eta_{r_1+r_2-1})) \begin{pmatrix} t_0 \\ \vdots \\ t_{r_1+r_2-1} \end{pmatrix}$$

Jacobi rule: $dx_1 \cdots dx_{r_1+r_2} = \underbrace{\left| \det(\vec{n}, \ell(\eta_i), \ldots, \ell(\eta_{r_1+r_2-1})) \right|}_{R_K \text{ by definition}} dt_1 \cdots dt_{r_1+r_2-1}$

$\sum_{i=1}^{r_1+r_2} x_i = t_0$

(actually, the def. of the regulator comes from this calculation)

$$\mu(D_1) = 2^{r_1}(2\pi)^{r_2} \int_{D_1^{\log}} e^{t_0} R_K \, dt_0 \cdots dt_{r_1+r_2-1}$$

$$= 2^{r_1}(2\pi)^{r_2} R_K \int_{t_0=-\infty}^{\log N(\mathfrak{J})} e^{t_0} dt_0 \cdot \underbrace{\prod_{i=1}^{r_1+r_2-1} \int_{t_i=0}^{1} dt_i}_{1} = 2^{r_1}(2\pi)^{r_2} R_K \cdot N(\mathfrak{J})$$

□
□

Infinite products

Def. Let $(a_n, n \geq 1)$ be a sequence of complex numbers or complex holomorphic functions in some region of $\mathbb{C}$.

We say $\prod_{n=1}^{\infty}(1+a_n)$ is <u>abs convergent</u> if $\lim_{N\to+\infty}\prod_{n=1}^{N}(1+|a_n|)$ exists.

Note that this implies $\exists \lim_{N\to\infty}\prod_{n=1}^{N}(1+a_n)$

Lemma. $\prod_{n=1}^{\infty}(1+a_n)$ abs. convergent $\iff \sum_{n=1}^{\infty} a_n$ abs convergent

Pf: $\prod_{n=1}^{\infty}(1+a_n)$ abs. convergent $\iff \sum_{n=1}^{\infty}\log(1+|a_n|)$ abs. convergent

Note: $\frac{2}{3}x \leq \log(1+x) \leq x \quad \forall\, 0 \leq x \leq \frac{1}{2}$.

$$\frac{2}{3}\sum_{n=N}^{\infty}|a_n| \leq \sum_{n=N}^{\infty}\log(1+|a_n|) \leq \sum_{n=N}^{\infty}|a_n| \qquad \forall n \geq N,\ |a_n| \leq 1/2,$$

and $|a_n| \to 0$ if either one is convergent, so this holds for $N \gg 1$. □

Lemma. The infinite product $\underbrace{\prod_{p}\frac{1}{1-p^{-s}}}_{\zeta(s)}$ is convergent in $\mathrm{Re}(s)>1$.

We also have $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$, which also converges absolutely for $\mathrm{Re}(s)>1$.

Pf: $$\frac{1}{1-p^{-s}} = 1 + \frac{p^{-s}}{1-p^{-s}}$$

By the prev. Lemma, STS: $\sum_{p}\left|\frac{p^{-s}}{1-p^{-s}}\right|$ is abs. convergent for $\mathrm{Re}(s)>1$.

$$|1-p^{-s}| \geq 1-|p^{-s}| = 1-p^{-\mathrm{Re}(s)} \geq 1-\tfrac{1}{2} \text{ for } \mathrm{Re}(s) \geq 1 = \tfrac{1}{2}$$

$$\Rightarrow \sum_{p}\left|\frac{p^{-s}}{1-p^{-s}}\right| \leq \sum_{p} 2p^{-\mathrm{Re}(s)} < 2\sum_{n=1}^{\infty} n^{-\mathrm{Re}(s)}$$

$$\sum_{n=1}^{\infty} n^{-\mathrm{Re}(s)} \sim \int_{1}^{+\infty} x^{-\mathrm{Re}(s)}\,dx = \frac{1}{1-\mathrm{Re}(s)}\cdot x^{1-\mathrm{Re}(s)}\Big|_{+1}^{+\infty} = \frac{1}{\mathrm{Re}(s)-1}$$

Also see $\sum_{n=1}^{\infty}\frac{1}{n^s}$ is abs convergent in $\mathrm{Re}(s)>1$.

To compare the two expressions, ~~compare~~ consider

$$\prod_{p\leq N}\frac{1}{1-p^{-s}} - \sum_{n=1}^{N}\frac{1}{n^s}$$

$$\left| \prod_{p \le N} \frac{1}{1-p^{-s}} - \sum_{n \le N} \frac{1}{n^s} \right| = \left| \prod_{p \le N} \left(\sum_{m=0}^{\infty} p^{-ms} \right) - \sum_{n \le N} \frac{1}{n^s} \right| =$$

$$= \sum_{\substack{m_1, \dots, m_r > 0 \\ p_i \le N}} \frac{1}{p_1^{m_1} \cdots p_r^{m_r}} - \sum_{n \le N} \frac{1}{n^s}$$

$$= \sum_{\substack{\text{all prime} \\ \text{divisors of } n \\ \text{are } \le N}} \frac{1}{n^s} - \sum_{n \le N} \frac{1}{n^s}$$

$$= \left| \sum_{\substack{n > N \\ \text{prime divisors} \\ \text{of } n \text{ are} \le N}} \frac{1}{n^s} \right| \le \sum_{n > N} \frac{1}{n^{\mathrm{Re}(s)}} \to 0 \qquad \text{as } N \to +\infty, \ \mathrm{Re}(s) > 1$$

$$\Rightarrow \sum_{n=1} \frac{1}{n^s} = \prod_{p} \frac{1}{1-p^{-s}} \quad \forall\, \mathrm{Re}(s) > 1. \qquad \square$$

Lemma: ζ has an analytic continuation to $\mathrm{Re}(s) > 0$ (a meromorphic function on) with a simple pole at $s = 1$ with residue 1.

PROOF: Idea: compare $\zeta(s)$ with $\int_1^{+\infty} x^{-s}\, dx = \frac{1}{1-s} x^{1-s} \Big|_1^{+\infty} = \frac{1}{s-1}$.

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{+\infty} \frac{1}{n^s} - \underbrace{\int_1^{+\infty} x^{-s}\, dx}_{= \sum_{n=1}^{\infty} \int_n^{n+1} x^{-s}\, dx} =$$

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

$$= \sum_{n=1}^{+\infty} \int_n^{n+1} \left(\int_0^x s \cdot t^{-s-1}\, dt \right) dx \qquad n \le t \le x \le n+1$$

$$= s \cdot \sum_{n=1}^{+\infty} \int_{t=n}^{n+1} \left(\int_{x=t}^{n+1} t^{-s-1}\, dx \right) dt$$

$$= s \cdot \sum_{n=1}^{+\infty} \int_n^{n+1} \frac{n+1-t}{t^{s+1}}\, dt$$

We want this to be holomorphic in $\mathrm{Re}(s) > 0$.

↓

abs. convergent in $\mathrm{Re}(s) > 0$

$\Rightarrow$ defines a holomorphic function in $\mathrm{Re}(s) > 0$

$$\left|\int_0^{n+1} \frac{n+1-t}{t^{s+1}}\,dt\right| \le \int_n^{n+1} \frac{|n+1-t|}{t^{1+\mathrm{Re}(s)}}\,dt \le \int_n^{n+1} \frac{dt}{t^{1+\mathrm{Re}(s)}}$$

$$\left|\zeta(s) - \frac{1}{s-1}\right| \le |s| \cdot \sum_{n=1}^{\infty} \int_n^{n+1} \frac{dt}{t^{1+\mathrm{Re}(s)}}$$

$$\le |s| \int_1^{+\infty} \frac{dt}{t^{1+\mathrm{Re}(s)}}$$

$$= |s| \frac{1}{-\mathrm{Re}(s)} \cdot t^{-\mathrm{Re}(s)} \Big|_1^{+\infty} = \frac{|s|}{\mathrm{Re}(s)}$$

$$\zeta(s) = \underbrace{\frac{1}{s-1}}_{\text{mero.}} + \underbrace{s \sum_{n=1}^{+\infty} \int_n^{n+1} \frac{n+1-t}{t^{s+n}}\,dt}_{\text{holo.}} \qquad \text{for } \mathrm{Re}(s) > 0$$

□

Prop. Let $f(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$ be a Dirichlet series abs. convgnt in $\mathrm{Re}(s) \gg 0$.

Let $S_t := \sum_{n \le t} a_n$ for $t \in \mathbb{R}$, and assume that $S_t = \alpha t + O(t^{1-\delta})$

for some $\alpha \in \mathbb{C}$ and $\delta \in \mathbb{R}$.

Then f has an analytic continuation to a meromorphic function on $\mathrm{Re}(s) > 1-\delta$,

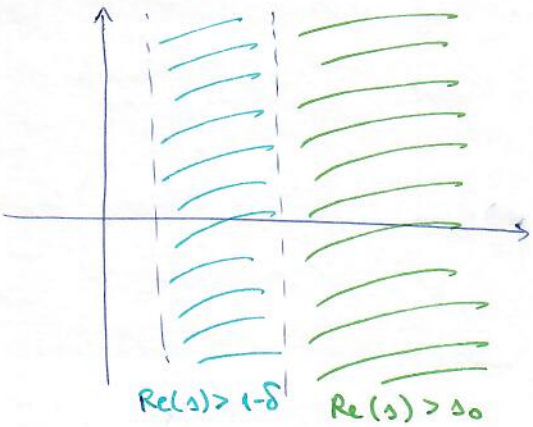
with at most a simple pole at $s = 1$, with residue α.

PF: Put $g(s) := f(s) - \alpha\,\zeta(s) = \sum_{n=1}^{+\infty} \frac{b_n}{n^s}$,

$b_n = a_n - \alpha$.

$$S_t' := \sum_{n \le t} b_n = S_t - \alpha \cdot \lfloor t \rfloor = O(t^{1-\delta}),$$

i.e. $\exists C > 0 : |S_t'| \le C \cdot t^{1-\delta} \quad \forall t \ge 1$



NTS: $g(s)$ admits an analytic continuation

to a holomorphic function in $\mathrm{Re}(s) > 1-\delta$

$$g_N(s) = \sum_{n \le N} \frac{b_n}{n^s} = \sum_{n \le N} \frac{S_n' - S_{n-1}'}{n^s} = \sum_{n \le N} \frac{S_n'}{n^s} - \sum_{n \le N} \frac{S_{n-1}'}{n^s} \qquad (S_0' = 0)$$

$$= \sum_{n=1}^{N} \frac{S_n'}{n^s} - \sum_{n=1}^{N-1} \frac{S_n'}{(n+1)^s} = \sum_{n=1}^{N-1} S_n' \cdot \left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + \frac{S_N'}{N^s} \qquad \text{(Abel's summation)}$$

$$\frac{1}{n^s} - \frac{1}{(n+1)^s} = s \int_n^{n+1} t^{-s-1}\,dt$$

$$\Rightarrow g_N(s) = \sum_{n=1}^{N-1} S_n' \cdot s \cdot \int_n^{n+1} t^{-s-1}\, dt + \frac{S_N'}{N^s}$$

Estimation:

$$\left| \sum_{n=1}^{N-1} S_n' \cdot s \cdot \int_n^{n+1} t^{-s-1}\, dt \right| \le |s| \cdot \sum_{n=1}^{N-1} |S_n'| \cdot \int_n^{n+1} t^{-1-\mathrm{Re}(s)}\, dt \le \qquad \sigma := \mathrm{Re}(s)$$

$$\le C \cdot |s| \cdot \sum_{n=1}^{N-1} \int_n^{n+1} n^{1-\delta}\, t^{-1-\sigma}\, dt \le$$

$$\le C \cdot |s| \cdot \sum_{n=1}^{N-1} \int_n^{n+1} n^{1-\delta}\, t^{-\delta-\sigma}\, dt \qquad n^{1-\delta} \le t^{1-\delta}$$

$$= C \cdot |s| \cdot \int_1^N t^{-\delta-\sigma}\, dt$$

$$= \frac{C \cdot |s|}{1-\delta-\sigma} \cdot t^{1-\delta-\sigma} \Big|_1^N$$

$$= \frac{C \cdot |s|}{\sigma-(1-\delta)} \left(1 - \frac{1}{N^{\sigma-(1-\delta)}}\right) \qquad \text{if } \sigma = \mathrm{Re}(s) > 1-\delta$$

$\to 0$ as $N \to +\infty$

Hence $\sum_{n=1}^{+\infty} S_n' \cdot s \cdot \int_n^{n+1} t^{-s-1}\, dt$ defines a hol. function in $\mathrm{Re}(s) > 1-\delta$.

$$\left| \frac{S_n'}{N^s} \right| \le C \cdot N^{1-\delta-\sigma} \longrightarrow 0 \quad \text{as } N \to +\infty, \text{ if } \sigma > 1-\delta.$$

$$g_N(s) \longrightarrow g(N) = \sum_{n=1}^{+\infty} S_n' \cdot s \cdot \int_n^{n+1} t^{-s-1}\, dt.$$

□

Applications

$K/\mathbb{Q}$ number field

Lemma. The infinite product

$$\prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \text{prime}}} \frac{1}{1-N\mathfrak{p}^{-s}} =: \zeta_K(s)$$

converges absolutely for $\mathrm{Re}(s) > 1$, and

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \text{ideal}}} \frac{1}{(N\mathfrak{a})^s}.$$

Pf: $$|\zeta_K(s)| \le \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{|1-N\mathfrak{p}^{-s}|} \le \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1-N\mathfrak{p}^{-\mathrm{Re}(s)}}.$$

We regroup $\mathfrak{p}$ according to the primes $p \in \mathbb{Z}$, $(p) = \mathfrak{p} \cap \mathbb{Z}$.

$$\prod_{\mathfrak{p}\subseteq\mathcal{O}_K} \frac{1}{1-N\mathfrak{p}^{-\mathrm{Re}(s)}} = \prod_{p} \prod_{\mathfrak{p}\mid p,\ \mathfrak{p}\subseteq\mathcal{O}_K} \frac{1}{1-N\mathfrak{p}^{-\mathrm{Re}(s)}}$$

$$\prod_{\mathfrak{p}\mid p} \frac{1}{1-N\mathfrak{p}^{-\mathrm{Re}(s)}} = \prod_{\mathfrak{p}\mid p} \frac{1}{1-p^{-f(\mathfrak{p}\mid p)\cdot \mathrm{Re}(s)}}$$

Note that $f(\mathfrak{p}\mid p) \geq 1$ and there are at most $[K:\mathbb{Q}]$ primes $\mathfrak{p}$ above p.

$$\prod_{\mathfrak{p}\mid p} \frac{1}{1-N\mathfrak{p}^{-\mathrm{Re}(s)}} \leq \left(\frac{1}{1-p^{-\mathrm{Re}(s)}}\right)^{[K:\mathbb{Q}]}$$

$$|\zeta_K(s)| \leq \left(\underbrace{\prod_{\mathfrak{p}} \frac{1}{1-\mathfrak{p}^{-\mathrm{Re}(s)}}}_{\zeta(\mathrm{Re}(s))}\right)^{[K:\mathbb{Q}]} \quad \text{converges for } \mathrm{Re}(s)>1.$$

$$\zeta_K(s) = \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \frac{1}{(N\mathfrak{a})^s}$$ follows from the same argument* as for $\zeta(s)$. □

Recall. Thm. $K/\mathbb{Q}$ number field, $N(t) = \#\left\{\mathfrak{a}\subseteq\mathcal{O}_K \mid N_{K/\mathbb{Q}}(\mathfrak{a}) \leq t\right\}$

Then $N(t) = \dfrac{2^{r_1}\cdot(2\pi)^{r_2}\cdot R_K \cdot h}{w\cdot\sqrt{|d_K|}}\, t + O\left(t^{1-\frac{1}{n}}\right)$ where $n=[K:\mathbb{Q}]$.

Rmk. (*): $\left|\sum_{\mathfrak{a}\subseteq\mathcal{O}_K,\ N\mathfrak{a}\leq t} \left(\frac{1}{N\mathfrak{a}^s}\right)\right| \leq \sum_{N\mathfrak{a}\leq t} \frac{1}{(N\mathfrak{a})^{\mathrm{Re}\,s}} = \underbrace{\prod_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K \text{ prime} \\ N\mathfrak{p}\leq t}} \frac{1}{1-N\mathfrak{p}^{-\mathrm{Re}\,s}}}_{\text{finitely many terms}}$

~~For the proof of the Thm, we wrote~~

$$\zeta_K(s) = \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \frac{1}{(N\mathfrak{a})^s} = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$$

$$a_n = \#\left\{\mathfrak{a}\subseteq\mathcal{O}_K \mid N\mathfrak{a} = n\right\}$$

$$S_t = \sum_{n\leq t} a_n = N(t) = \kappa t + O\left(t^{1-\frac{1}{n}}\right)$$

Prop. 1. $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ has an analytic cont. to $\mathrm{Re}(s) > 1-\frac{1}{n}$ with a simple pole at $s=1$.

Thm. $\zeta_K(s)$ has an analytic continuation to $\mathrm{Re}(s) > 1 - \frac{1}{n}$ with a simple pole at $s=1$, and

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} \cdot R_K \cdot h}{w \cdot \sqrt{|d_K|}}.$$

Cor. $$\sum_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \text{prime}}} \frac{1}{N\mathfrak{p}^s} = \sum_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \deg \mathfrak{p} = 1}} \frac{1}{N\mathfrak{p}^s} \sim \log \frac{1}{s-1} \quad \text{as } s \to 1^+$$

Here, if $f(s)$ and $g(s)$ are two functions defined in a neighbourhood of 1, we write $f(s) \sim g(s)$ as $s \to 1^+$ (i.e. s approaches 1 from the right on the real axis), if $\lim_{s \to 1^+} \frac{f(s)}{g(s)} = 1$.

In particular, for $K = \mathbb{Q}$ we have $\sum_p \frac{1}{p^s} \sim \log \frac{1}{s-1}$.

Pf of Cor: $$\zeta_K(s) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - N\mathfrak{p}^{-s}} = \frac{\alpha}{s-1} + a_0 + a_1(s-1) + \dots$$

$$= \frac{f(s)}{s-1} \quad \text{where } f(s) \text{ is holo. around } s=1.$$

$$\log \zeta_K(s) = \log \frac{1}{s-1} + \underbrace{\log f(s)}_{\text{holo. around } s=1} \sim \log \frac{1}{s-1}$$

$$\log \zeta_K(s) = \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \log \frac{1}{1 - N\mathfrak{p}^{-s}} = \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \sum_{m=1}^{+\infty} \frac{1}{m N\mathfrak{p}^{ms}} =$$

$$\log \frac{1}{1-x} = \sum_{m=1}^{\infty} \frac{x^m}{m}$$

$$= \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{N\mathfrak{p}^s} + \sum_{m \geq 2} \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{m N\mathfrak{p}^{ms}}$$

$$= \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{N\mathfrak{p}^s} + \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{N\mathfrak{p}^s} + \sum_{m \geq 2} \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{m N\mathfrak{p}^{ms}}$$

$f(\mathfrak{p}|p) =$ $\underbrace{\deg(\mathfrak{p}) = 1}$ $\underbrace{\deg(\mathfrak{p}) \geq 2}_{②}$ $\underbrace{\qquad\qquad}_{③}$

② $$\left| \sum_{\mathfrak{p} \subseteq \mathcal{O}_K,\ \deg(\mathfrak{p}) \geq 2} \frac{1}{N\mathfrak{p}^s} \right| \leq \sum_{p} \sum_{\substack{\mathfrak{p} \mid p \\ \deg(\mathfrak{p}) \geq 2}} \frac{1}{Np^{\mathrm{Re}(s)}} \leq$$

$$\leq \frac{[K:\mathbb{Q}]}{2} \sum_{p} \frac{1}{p^{2\,\mathrm{Re}(s)}} \leq$$

$$\leq \frac{[K:\mathbb{Q}]}{2} \sum_{n} \underbrace{\frac{1}{n^{2\,\mathrm{Re}(s)}}}_{\text{bounded since } \mathrm{Re}(s) > \frac{1}{2}}$$

③ $$\sum_{m \geq 2} \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{m N\mathfrak{p}^{ms}} = \sum_{m \geq 2} \sum_{p} \sum_{\mathfrak{p} \mid p} \frac{1}{m p^{\deg(\mathfrak{p}) \cdot \mathrm{Re}(s) \cdot m}}$$

$$\leq \frac{[K:\mathbb{Q}]}{2} \cdot \sum_{p} \frac{1}{p^{\mathrm{Re}(s)}} < \frac{[K:\mathbb{Q}]}{2} \sum_{n} \underbrace{\frac{1}{n^{\mathrm{Re}(s)}}}_{\text{bounded if } \mathrm{Re}(s) > \frac{1}{2}}$$

$\Rightarrow$ ② and ③ are bounded around $s = 1$.

$$\Rightarrow \sum_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \deg \mathfrak{p} = 1}} \frac{1}{N\mathfrak{p}^s} \sim \log \frac{1}{s-1}$$

□

Def. Let S be a subset of prime ideals of $\mathcal{O}_K$.

We say that S has (Dirichlet) density ρ for $\rho \in [0,1]$ if

$$\sum_{\mathfrak{p} \in S} \frac{1}{N\mathfrak{p}^s} \sim \rho \log \frac{1}{s-1}$$

The previous Corollary says that $S = \{\mathfrak{p} \subseteq \mathcal{O}_K \mid \mathfrak{p} \text{ prime}, \deg(\mathfrak{p}) = 1\}$ has Dirichlet density 1.

Def. $\forall x > 0$: $\pi(x) := \#\{\text{prime ideals } \mathfrak{p} \subseteq \mathcal{O}_K \mid N\mathfrak{p} \leq x\}$ ~~$= \#\{\mathfrak{p} \in S \mid \text{"}\}$~~

$\pi_S(x) := \#\{\mathfrak{p} \in S \mid N\mathfrak{p} \leq x\}$

Natural density: $\lim_{x \to +\infty} \frac{\pi_S(x)}{\pi(x)}$ if it exists.

If S has natural density $\rho \in [0,1]$ $\Rightarrow$ S has Dirichlet density $\rho \in [0,1]$ $\not\Leftarrow$

23.11.2017

Dirichlet L-functions

Def. Character group of finite abelian groups:

G a fin. ab. gp.

$\hat{G} := \mathrm{Hom}(G, \mathbb{C}^\times)$ character gp.

$\chi_1, \chi_2 \in \hat{G}$: $(\chi_1\chi_2)(g) := (\chi_1(g))(\chi_2(g))$. multiplication

Lemma 1. $\exists$ non-canonical isomorphism $G \simeq \hat{G}$.

PF: A general fin. ab. gp. is of the form of product of fin. cyclic gps.

Wlog wma $G \simeq \mathbb{Z}/n\mathbb{Z}$ $\Rightarrow$ $\hat{G} \simeq \mu_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}$

$\chi \mapsto \chi(1 \bmod n)$

$\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$ non-canonical

$\Rightarrow G \simeq \hat{G}$ □

$f: G_1 \to G_2$ $\Rightarrow$ $\hat{f}: \hat{G}_1 \to \hat{G}_2$

$\chi \mapsto \chi \circ f$

Corollary. $0 \to G_1 \to G \to G_2 \to 0$ short exact seq. of fin. ab. gps.

$\Rightarrow 0 \to \hat{G}_2 \to \hat{G} \to \hat{G}_1 \to 0$ is also a short exact sequence.

PF: $\mathrm{Hom}(-, \mathbb{C}^\times)$ is a left exact functor

So $0 \to \hat{G}_2 \to \hat{G} \to \hat{G}_1$ is exact,

In particular: $\hat{G}/\hat{G}_2 \hookrightarrow \hat{G}_1$

$$\left|\hat{G}/\hat{G}_2\right| = \frac{|\hat{G}|}{|\hat{G}_2|} \overset{\text{Lemma}}{=} \frac{|G|}{|G_2|} \overset{\text{exactness}}{=} |G_1| = |\hat{G}_1| \quad \Rightarrow \hat{G} \to \hat{G}_1 \text{ is surjective.}$$

□

One has a canonical map $G \to \hat{\hat{G}} = \mathrm{Hom}(\hat{G}, \mathbb{C}^\times)$

$g \mapsto (\chi \mapsto \chi(g))$

Prop. 3. $G \xrightarrow{\sim} \hat{\hat{G}}$. iso (canonical)

PF: Since $|G| = |\hat{G}| = |\hat{\hat{G}}|$, it sfs that the map is injective,

i.e. $\forall 1 \neq g \in G$ $\exists \chi \in \hat{G}$ s.t. $\chi(g) \neq 1$.

$H := \langle g \rangle \subseteq G$ $\to$ $H \simeq \mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$ $\Rightarrow \hat{H} \neq 0$

$\forall \chi_0 \in \hat{H}$ nontrivial: $\chi_0(g) \neq 1$ since g is the generator.

But $\hat{G} \twoheadrightarrow \hat{H}$ is surjective $\Rightarrow \exists \chi \in \hat{G}$ s.t. $\chi|_H = \chi_0$, $\chi(g) \neq 1$

□

Prop. (1) $\sum_{g\in G} \chi(g) = \begin{cases} 0 & \chi \neq \chi_0 \\ |G| & \chi = \chi_0 \end{cases}$ (χ_0 is the trivial character)

(2) $\forall\, g \in G$: $\sum_{\chi\in \hat{G}} \chi(g) = \begin{cases} 0 & g \neq 1 \\ |G| & g = 1 \end{cases}$

Pf: (2) is a consequence of (1) since we have a canonical identification $G = \hat{\hat{G}}$.

(1): $\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(gh) \qquad \forall\, h \in G$

$= \chi(h) \sum_{g\in G} \chi(g) \quad \Rightarrow (\chi(h)-1)\cdot \sum_{g\in G} \chi(g) = 0$

If $\chi \neq \chi_0 \Rightarrow \exists h: \chi(h) \neq 1 \Rightarrow \sum_{g\in G} \chi(g) = 0.$

If $\chi = \chi_0$, the statement is trivial. □

This was done in full generality, now we specify for Dirichlet characters.

Def. A <u>Dirichlet character</u> is a homomorphism $\chi: \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \longrightarrow \mathbb{C}^\times$ for some $N \geq 1$.

If $M \mid N$, then a Dirichlet char mod M induces a D. char mod N by the map

$$\begin{array}{ccc} \left(\mathbb{Z}/N\mathbb{Z}\right)^\times & \longrightarrow & \mathbb{C}^\times \\ & \searrow \quad \nearrow_{\chi} & \\ & \left(\mathbb{Z}/M\mathbb{Z}\right)^\times & \end{array}$$

For a Dirichlet character $\chi: \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \to \mathbb{C}^\times$ there is a smallest positive integer f_χ s.t. $f_\chi \mid N$ and χ is induced by some character on $\left(\mathbb{Z}/f_\chi\mathbb{Z}\right)^\times$.

Def. f_χ is the <u>conductor</u> of the character χ.

If $f_\chi = N$, then $\chi: \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \to \mathbb{C}^\times$ is called <u>primitive</u>.

Convention. Given a $\chi: \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \to \mathbb{C}^\times$, we view χ as a function on $\mathbb{Z}$.

by $\chi(a) = \begin{cases} \chi(a \bmod f_\chi) & \text{if } \gcd(a, f_\chi) = 1 \\ 0 & \text{if } \gcd(a, f_\chi) > 1 \end{cases}$

There are differences in the literature here: some say

$$\chi(a) = \begin{cases} \chi(a \bmod N) & \gcd(a, N) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Example. $\left(\mathbb{Z}/8\mathbb{Z}\right)^\times \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^{\oplus 2}$

$\| \quad \{1, 3, 5, 7\}$

$\chi(1) = \chi(5) = 1$

$\chi(3) = \chi(7) = -1$ $\Rightarrow f_\chi = 4$

$\chi'(1) = \chi'(7) = 1$

$\chi'(3) = \chi'(5) = -1$ $\Rightarrow f_\chi = 8$

Example. $p \geq 3$ prime, $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times = \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$

$a \longmapsto \left(\frac{a}{p}\right)$ Legendre symbol

The Legendre symbol gives a character with conductor p.

Let χ, ψ be Dirichlet characters with conductors f_χ and f_ψ.

Then we define the product $\chi\psi$ as the primitive character attached to

$$\gamma : \left(\mathbb{Z}/\mathrm{lcm}(f_\chi, f_\psi)\mathbb{Z}\right)^\times \longrightarrow \mathbb{C}^\times$$

In general, $f_{\chi\psi} \neq \mathrm{lcm}(f_\chi, f_\psi)$.

Example. $\chi : \left(\mathbb{Z}/12\mathbb{Z}\right)^\times \longrightarrow \mathbb{C}^\times$

$\chi(1) = \chi(11) = 1$

$\chi(5) = \chi(7) = -1$

$\left(\mathbb{Z}/12\mathbb{Z}\right)^\times \underset{\text{CRT}}{\simeq} \left(\mathbb{Z}/3\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/4\mathbb{Z}\right)^\times \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^{\oplus 2}$

$\psi : \left(\mathbb{Z}/3\mathbb{Z}\right)^\times \longrightarrow \mathbb{C}^\times$

$\psi(1) = 1, \quad \psi(2) = -1$

$\Rightarrow (\chi\psi) : \left(\mathbb{Z}/12\mathbb{Z}\right)^\times \longrightarrow \mathbb{C}^\times$

$1 \longmapsto 1$

$5 \longmapsto \chi(5)\psi(5) = \chi(5)\psi(2) = 1$

$7 \longmapsto \chi(7)\psi(7) = \chi(7)\psi(1) = -1$

$11 \longmapsto \chi(11)\psi(11) = \chi(11)\psi(2) = -1$

$\chi\psi$ has period 4 $\Rightarrow f_{\chi\psi} = 4$.

$\chi\psi : \left(\mathbb{Z}/4\mathbb{Z}\right)^\times \longrightarrow \mathbb{C}^\times$

$1 \longmapsto 1$

$3 \longmapsto -1$

$(\chi\psi)(3) = -1 \qquad \chi(3)\cdot\psi(3) = 0$

In general, $(\chi\psi)(a) \neq \chi(a)\psi(a)$ if $a \mid \operatorname{lcm}(f_\chi, f_\psi)$ but $\gcd(f_{\chi\psi}, a) = 1$.

Def. For a Dirichlet character χ we define

$$L(\chi, s) = \prod_p \frac{1}{1-\chi(p)\cdot p^{-s}},$$

which is clearly abs. convergent if $\operatorname{Re}(s) > 1$.

$$L(\chi, s) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s} \quad \text{by previous discussion.}$$

Prop. If χ is a non-trivial Dirichlet character, then $L(\chi, s)$ has an analytic continuation to a holomorphic function on $\operatorname{Re}(s) > 0$.

PF: $\forall t > 0$: $S_t = \sum_{n \le t} \chi(n) = \mathcal{O}(1)$, i.e. $\exists C > 0$: $|S_t| \le C$, e.g.

$C = f_\chi$ is a good choice:

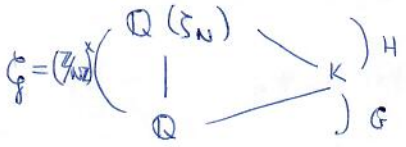
$$\sum_{a=1}^{f_\chi} \chi(k f_\chi + a) = 0 \quad \forall k \in \mathbb{Z}.$$

The statement follows by a Prop. from last time. □

Factorisation of the Dedekind zeta function of abelian number fields

$N \geq 3$.

$G = (\mathbb{Z}/N\mathbb{Z})^\times$



$$0 \to H \to \mathcal{G} \to G \to 0$$

$$0 \to \hat{G} \to \hat{\mathcal{G}} \to \hat{H} \to 0,$$

i.e. $\hat{G}$ is the subgroup of Dirichlet characters mod N that are trivial on H.

Example. $K = \mathbb{Q}(\sqrt{p^*})$ where $p^* = (-1)^{\frac{p-1}{2}} p$, $p \geq 3$ prime.

$K/\mathbb{Q}$ is the unique quadratic subextension of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$

$G = \operatorname{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) \simeq \{\pm 1\} \xrightarrow{\chi} \mathbb{C}^\times$, where χ is the unique nontrivial character

$$H = \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p^*})) \subseteq (\mathbb{Z}/p\mathbb{Z})^\times = \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$$

$$\| \quad (\mathbb{F}_p^\times)^2$$

$$\Rightarrow \chi(a) = \left(\frac{a}{p}\right) \quad \forall a \in (\mathbb{Z}/p\mathbb{Z})^\times$$

Prop. $\zeta_K(s) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1-(N\mathfrak{p})^{-s}} = \prod_{\chi \in \hat{G}} L(\chi, s)$.

Remark. The assumption that K is a subfield of some cyclotomic extension is equivalent to saying that $K/\mathbb{Q}$ is an abelian extension.

(Kronecker — Weber's Theorem, class field theory)

Pf: Sts that for any rational prime p

$$\prod_{\mathfrak{p} \mid p} \frac{1}{1-(N\mathfrak{p})^{-s}} = \prod_{\chi \in \hat{G}} \frac{1}{1-\chi(p)p^{-s}}$$

First consider the case $p \nmid N$. $\Leftrightarrow$ p unramified in $\mathbb{Q}(\zeta_N)$

$$\begin{array}{c} \mathbb{Q}(\zeta_N) \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$$

Let $\sigma_p \in G$ be the Frobenius element at p.

$\sigma_p = \left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)$ $\forall \mathfrak{p} \mid p$, If we view G as a quotient of $(\mathbb{Z}/N\mathbb{Z})^\times$, then σ_p is the image of $p \bmod N$.

$$\begin{array}{ccc} p & \in & (\mathbb{Z}/N\mathbb{Z})^\times \\ \downarrow & & \downarrow \\ \sigma_p & \in & G \end{array}$$

$D_p = \langle \sigma_p \rangle \subseteq G$ decomposition group.

$$\begin{array}{ccc} \mathbb{Q}(\zeta_N) & - & K \\ | & & | \quad \langle \sigma_p \rangle = D_p \\ \mathbb{Q}(\zeta_N)^{\langle p \rangle} & - & E = K^{D_p} \\ & \searrow & | \\ & & \mathbb{Q} \end{array} \qquad \begin{array}{c} \mathfrak{p}_1, \dots, \mathfrak{p}_g \\ | \\ \mathfrak{p}_{E,1}, \dots, \mathfrak{p}_{E,g} \\ \searrow \quad \swarrow \\ p \end{array}$$

$(\mathbb{Z}/N\mathbb{Z})^\times \supseteq \langle p \rangle$

$f(\mathfrak{p}_i \mid p)$ = order of σ_p in $G = |D_p|$

There are $|G| / |D_p|$ prime ideals of $\mathcal{O}_K$ above p and each has residue degree $f = |D_p|$.

$$\text{LHS} = \prod_{\mathfrak{p} \mid p} \frac{1}{(1-N\mathfrak{p})^{-s}} = \left(\frac{1}{1-p^{-fs}}\right)^g \qquad N\mathfrak{p} = p^f, \quad g = \frac{|G|}{f}$$

$D_p \cong \mathbb{Z}/f\mathbb{Z}$, $\quad \hat{D}_p \cong \mu_f$, $\chi \mapsto \chi(\sigma_p)$

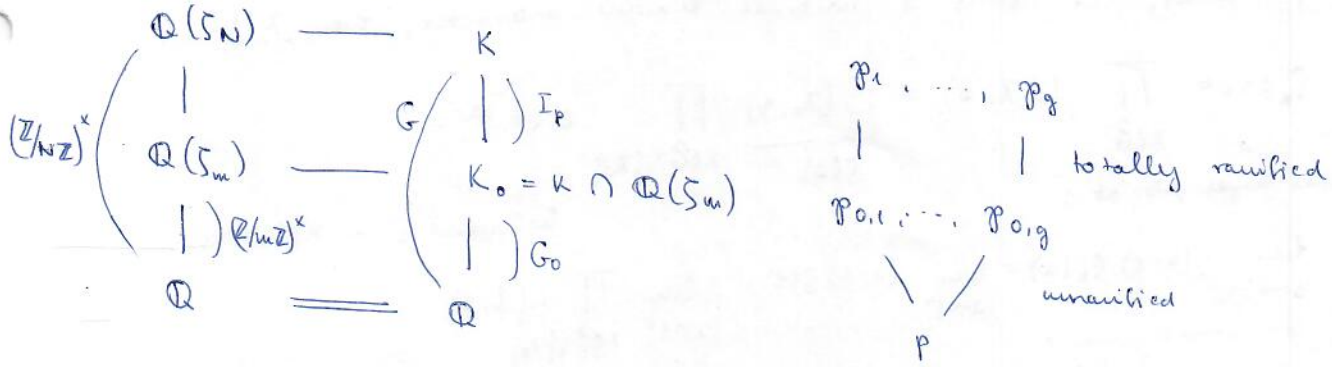
$$0 \to \underbrace{\left(G/D_p\right)^\wedge}_{\text{order } g} \to \hat{G} \to \hat{D}_p \to 0$$

$$\prod_{\chi \in \hat{G}} \frac{1}{1-\chi(\sigma_p)\,p^{-s}} = \prod_{\zeta \in \mu_f} \frac{1}{(1-\zeta p^{-s})^g}$$

$\{\chi(\sigma_p) \mid \chi \in \hat{G}\}$ takes $\zeta \in \mu_f$ with multiplicity g, $\forall \zeta \in \mu_f$

Now we get $\quad \frac{1}{1-p^{-fs}} = \prod_{\zeta \in \mu_f} \frac{1}{1-\zeta p^{-s}} \quad \Rightarrow$ LHS = RHS.

Second case: $p \mid N$. Write $N = p^k \cdot m$, $p^k \parallel N$.



$I_p := \mathrm{Gal}(K/K_0)$ is exactly the inertia group of G at p.

In $\mathcal{O}_{K_0}$: $\quad p\,\mathcal{O}_{K_0} = \mathfrak{p}_{0,1} \cdots \mathfrak{p}_{0,g}$

Above each $\mathfrak{p}_{0,i}$ there is a unique prime ideal $\mathfrak{P}_i$ of $\mathcal{O}_K$ s.t.

$$\mathfrak{p}_{0,i}\,\mathcal{O}_K = \mathfrak{P}_i^e \quad \text{where } e = |I_p|.$$

$f(\mathfrak{P}_i \mid p) = f(\mathfrak{p}_{i,0} \mid p)$ = the order of the image of $p \in (\mathbb{Z}/N\mathbb{Z})^\times$ in $\mathrm{Gal}(k/\mathbb{Q})$.

$$g = \frac{|G/I_p|}{f}$$

$$\hat{G}_0 \subseteq \hat{G} \subseteq \left((\mathbb{Z}/N\mathbb{Z})^\times\right)^\wedge$$

$\| \quad \{\chi \in \hat{G} \mid \chi|_{I_p} \text{ is trivial}\}$

I_p = image of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_m))$ in G

$\hat{G}_0 = \{\chi \in \hat{G} \mid f_\chi \text{ divides } m\}$, i.e. $\hat{G}_0 = \hat{G} \cap \left((\mathbb{Z}/m\mathbb{Z})^\times\right)^\wedge$

$\Rightarrow \forall \chi \in \hat{G} \setminus \hat{G}_0$: $\chi(p) = 0 \quad (p \mid f_\chi)$

$$\text{RHS} = \prod_{\chi \in \hat{G}} \frac{1}{1-\chi(p)\,p^{-s}} = \prod_{\chi \in \hat{G}_0} \frac{1}{1-\chi(p)\,p^{-s}}$$

$$\text{LHS} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \mid p}} \frac{1}{1-(N\mathfrak{p})^{-s}} = \prod_{\substack{\mathfrak{p}_0 \subseteq \mathcal{O}_{K_0} \\ \mathfrak{p}_0 \mid p}} \frac{1}{(1-N\mathfrak{p}_0)^{-s}}$$

$\longrightarrow$ reduce to K_0, the consequence follows from the previous discussion. □

Theorem. Let K, G be as above, $\chi_0 \in \hat{G}_0$ the trivial character.

Then $$\prod_{\substack{\chi \in \hat{G} \\ \chi \neq \chi_0}} L(\chi, 1) = \frac{2^{r_1} (2\pi)^{r_2} R_K \cdot h}{w \cdot \sqrt{|d_K|}}.$$

In particular, if χ is a nontrivial Dirichlet character, then $L(\chi, 1) \neq 0$.

Pf: $\underbrace{\zeta_K(s)}_{\text{has simple pole at } 1} = \prod_{\chi \in \hat{G}} L(\chi, s) = \underbrace{L(\chi_0, s)}_{\zeta(s)} \prod_{\chi \in \hat{G} \setminus \{\chi_0\}} \underbrace{L(\chi, s)}_{\text{holomorphic in } \mathrm{Re}(s) > 0}$

$$\underbrace{\lim_{s \to 1^+} (s-1)\,\zeta_K(s)}_{\text{Res}_{s=1} \zeta_K(s)} = \lim_{s \to 1^+} (s-1)\,\zeta(s) \cdot \lim_{s \to 1^+} \prod_{\chi \in \hat{G} \setminus \{\chi_0\}} L(\chi, s)$$

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \prod_{\chi \in \hat{G} \setminus \{\chi_0\}} L(\chi, 1).$$

□

Corollary. $p \geq 3$ prime, $K = \mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$, $\chi = \left(\frac{\cdot}{p}\right) : \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \longrightarrow \{\pm 1\}$.
(this is the only nontrivial D. char.)

Then $$L(\chi, 1) = \begin{cases} \dfrac{2^2 \cdot \log \varepsilon_K \cdot h}{2\sqrt{p}} & \varepsilon \in \mathcal{O}_K^\times \text{ fundamental unit} \\ & p \equiv 1 \pmod 4 \\ \dfrac{2\pi h}{|\mathcal{O}_K^\times| \cdot \sqrt{p}} & p \equiv 3 \pmod 4 \end{cases}$$

□

Recall. $K \subseteq \mathbb{Q}(\zeta_N)$, $G = \mathrm{Gal}(K/\mathbb{Q})$

$$\underbrace{(\mathbb{Z}/N\mathbb{Z})^\times}_{\simeq \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})} \twoheadrightarrow G \rightsquigarrow \hat{G} \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$$

Theorem. (Dirichlet, 1837) Let $N \geq 1$ and $a \in \mathbb{Z}$, $\gcd(a,N) = 1$.

Then the set of rational prime numbers $p \equiv a \pmod N$ has Dirichlet density $\frac{1}{\varphi(N)}$. In particular, there are infinitely many such primes.

PF: $$L(\chi, s) = \prod_p \frac{1}{1 - \chi(p)\, p^{-s}} \qquad \mathrm{Re}\, s > 1$$

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

$$= \sum_p \sum_{m=1}^{+\infty} \frac{\left(\chi(p)\, p^{-s}\right)^m}{m} \qquad \mathrm{Re}\, s > 1$$

$$= \sum_p \sum_{m=1}^{+\infty} \frac{\chi(p^m)}{m \cdot p^{ms}} \qquad \mathrm{Re}\, s > 1$$

$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ Dirichlet char

$$\Rightarrow \sum_{\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} \chi^{-1}(a)\, \chi(x) = \begin{cases} \varphi(N) & \text{if } x \equiv a \pmod N \\ 0 & \text{if } x \not\equiv a \pmod N \end{cases}$$

This follows from $\displaystyle\sum_{\chi \in G} \chi(g) = \begin{cases} |G| & g = 1 \\ 0 & \text{otherwise} \end{cases}$

$$\sum_\chi \chi^{-1}(a) \log L(\chi, s) = \sum_p \sum_m \sum_\chi \frac{\chi^{-1}(a)\, \chi(p^m)}{m\, p^{ms}}$$

$$= \varphi(N) \sum_p \sum_{\substack{m \geq 1 \\ p^m \equiv a \pmod N}} \frac{1}{m\, p^{ms}}$$

$$= \varphi(N) \sum_{p \equiv a \pmod N} \frac{1}{p^s} + \underbrace{\sum_{m \geq 2} \sum_p \frac{1}{m\, p^{ms}}}_{p^m \equiv a \pmod N}$$

bounded when $s \to 1$

$$\Rightarrow \sum_{p \equiv a \pmod N} \frac{1}{p^s} \sim \frac{1}{\varphi(N)} \sum_\chi \chi^{-1}(a) \log L(\chi, s) \qquad s \to 1$$

$\forall \chi \neq \chi_0$: $L(\chi, 1) \neq 0 \Rightarrow \log L(\chi, 1)$ is bounded as $s \to 1$

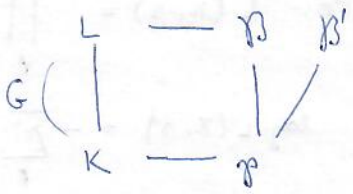
$\chi = \chi_0$: $L(\chi, s) = \zeta(s)$, $\log L(\chi, 1) \sim \log \frac{1}{s-1}$ because ζ has a simple pole at $s = 1$.

$$\Rightarrow \sum_{p \equiv a \pmod N} \frac{1}{p^s} \sim \frac{1}{\varphi(N)} \log \frac{1}{s-1}, \text{ hence the result.}$$

□

Generalisation. L/K Galois extension of number fields,

$G = \mathrm{Gal}(L/K)$.



$\mathfrak{p} \subseteq \mathcal{O}_K$ unramified in L/K

$\mathfrak{P}$ a prime in L above $\mathfrak{p}$

Frobenius substitution: $\sigma_{\mathfrak{P}} = \left(\frac{L/K}{\mathfrak{P}}\right) \in G$

The conjugacy class of $\sigma_{\mathfrak{P}}$ depends only on $\mathfrak{p}$.

Theorem (Chebotarev density thm.)

Let $c \subseteq G$ be a subset of conjugacy classes.

$$S_c := \left\{ \mathfrak{p} \subseteq \mathcal{O}_K \;\middle|\; \text{the conjugacy class of } \sigma_{\mathfrak{P}} \text{ for any } \mathfrak{P} \mid \mathfrak{p} \text{ lies in } c \right\}$$

(e.g. if c = the conj. class of $x \in G$, then $S_c = \left\{ \mathfrak{p} \subseteq \mathcal{O}_K \;\middle|\; \begin{array}{l} \exists \mathfrak{P} \subseteq \mathcal{O}_L,\ \mathfrak{P} \mid \mathfrak{p} \\ \text{and } \sigma_{\mathfrak{P}} = x \end{array} \right\}$

Then the density of S_c is $\frac{|c|}{|G|}$.

↑ both natural and Dirichlet

Example. $L/K = \mathbb{Q}(\zeta_N)/\mathbb{Q}$, $G = \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$

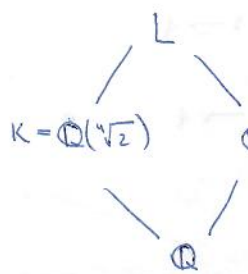
$c = \{\sigma_a\} \subseteq \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$, $a \in \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$

$\sigma_p = \sigma_a \iff p \equiv a \pmod N$ $\Rightarrow$ CDT implies the prev. thm.

Example. $S = \{$ rational primes $p \mid 2$ mod p is a 4^{th} power in $\mathbb{F}_p \}$.

Density of $S = ?$

$K := \mathbb{Q}(\sqrt[4]{2})$, non-Galois ext. of $\mathbb{Q}$, $L := \mathbb{Q}(\sqrt[4]{2}, i)$ Galois closure $(i = \sqrt{-1})$



$$G = \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle \Big/ \sigma^4 = \tau^2 = 1,\ \tau\sigma\tau = \sigma^{-1}$$

$$D_4 = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

$\sigma(\sqrt[4]{2}) = \sqrt[4]{2}\, i$ $\qquad$ $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$

$\sigma(i) = i$ $\qquad$ $\tau(i) = -i$

$p \in S \iff x^4 \equiv 2 \pmod p$ has solutions in $\mathbb{F}_p$.

$\overset{\text{Kummer}}{\iff}$ $\exists \mathfrak{p} \subseteq \mathcal{O}_K$ lying above p s.t. $f(\mathfrak{p}|p) = e(\mathfrak{p}|p) = 1$.

$\iff$ $\exists \mathfrak{P} \subseteq \mathcal{O}_L$ unramified s.t. $\mathfrak{P} \cap \mathcal{O}_L$ has degree 1 mod p

$\iff$ $\exists \mathfrak{P} \subseteq \mathcal{O}_L$ above p s.t. $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(L/K) = \langle \tau \rangle$

$\Updownarrow$

$D_{\mathfrak{P}} \leq \langle \tau \rangle$

$$\begin{array}{ccc} \mathfrak{P} & - & L \\ | & & | \\ \mathfrak{p} & - & K \\ | & & | \\ p & - & \mathbb{Q} \end{array}$$

$f(\mathfrak{p}|p) = 1 = e(\mathfrak{p}|p) \iff D_{\mathfrak{p}} \leq \langle \tau \rangle$

Case 1. $\sigma_{\mathfrak{P}} = 1$ $\Rightarrow$ Chebotarev density set of p has density $\frac{1}{8}$

Case 2. $\sigma_{\mathfrak{P}} = \tau$ The conj. class of τ is $\{\tau, \sigma^2\tau\}$ $\Rightarrow$ we have density $\frac{2}{8}$

$\Rightarrow$ Density of $S = \frac{1}{8} + \frac{2}{8} = \frac{3}{8}$

Formula for $L(\chi, 1)$

χ a Dirichlet character of conductor $f \geq 3$

$\bar{\chi}$ the complex conjugate of χ.

$\zeta = \zeta_f = e^{\frac{2\pi i}{f}}$

Put $\tau(\chi) := \sum_{x \in \mathbb{Z}/f\mathbb{Z}} \chi(x) \cdot \zeta^x$ Gauss sum

and $\tau_a(\chi) := \sum_{x \in \mathbb{Z}/f\mathbb{Z}} \chi(x) \cdot \zeta^{ax}$ Gauss sum for $\forall a \in (\mathbb{Z}/f\mathbb{Z})$

Lemma. (1) $\tau_a(\chi) = \bar{\chi}(a)\, \tau(\chi) \quad \forall a \in \mathbb{Z}/f\mathbb{Z}$

In particular, if $\gcd(a, f) > 1$ then $\tau_a(\chi) = 0$.

(2) $\tau(\chi)\, \tau(\bar{\chi}) = \chi(-1)\, f$

(3) $|\tau(\chi)| = \sqrt{f}$

Pf: (1) Case A: $\gcd(N, a) = 1 \qquad \chi(a)\, \bar{\chi}(a) = 1$

$$\bar{\chi}(a)\, \tau(\chi) = \sum_{x \in \mathbb{Z}/f\mathbb{Z}} \chi(x a^{-1})\, \zeta^{x a^{-1} a}$$

$y = a^{-1} \cdot x$

$$= \sum_{y \in \mathbb{Z}/f\mathbb{Z}} \chi(y) \cdot \zeta^{ya} = \tau_a(\chi).$$

Case B: $d = \gcd(N, a) > 1$

Write $a = da'$, $f = df'$, $\zeta' = \zeta^d$

$$\tau_a(\chi) = \sum_{x \in \mathbb{Z}/f\mathbb{Z}} \zeta^{d a' x}\, \chi(x)$$

$$= \sum_{s=0}^{f'-1} \sum_{t=1}^{d-1} (\zeta')^{a'(s+tf')}\, \chi(s+tf')$$

$$= \sum_{s=0}^{f'-1} (\zeta')^{a's} \cdot \left(\sum_{t=0}^{d-1} \chi(s+tf') \right)$$

Claim. $\sum_{t=0}^{d-1} \chi(s+tf') = 0.$

Pf. $\sum_{t=0}^{d-1} \chi(s+tf') = \sum_{\substack{x \in \mathbb{Z}/f\mathbb{Z} \\ x \equiv s \pmod{f'}}} \chi(x)$

Let H be the kernel of $\left(\mathbb{Z}/f\mathbb{Z}\right)^\times \longrightarrow \left(\mathbb{Z}/f'\mathbb{Z}\right)^\times$.

Then the sum is equal to

$$\sum_{t=0}^{d-1} \chi(s+tf') = \chi(s)\cdot\left(\sum_{x\in H}\chi(x)\right) = 0,$$

because $\chi|_H$ is non-trivial, otherwise the conductor of χ would divide f'.

(2): $$\tau(\chi)\,\tau(\bar\chi) = \sum_{a\in\mathbb{Z}/f\mathbb{Z}} \tau(\chi)\,\bar\chi(a)\,\zeta^a =$$

$$= \sum_{a\in\mathbb{Z}/f\mathbb{Z}} \tau_a(\chi)\,\zeta^a =$$

$$= \sum_{a\in\mathbb{Z}/f\mathbb{Z}} \sum_{x\in\mathbb{Z}/f\mathbb{Z}} \chi(x)\,\zeta^{a(1+x)} = \chi(-1)\,f$$

$$\sum_{a\in\mathbb{Z}/f\mathbb{Z}} \zeta^{a(1+x)} = \begin{cases} 0 & \text{if } x\neq -1 \\ f & \text{if } x=-1 \end{cases}$$

(3): STS: $|\tau(\chi)| = |\tau(\bar\chi)|$, and then use (2).

$$\overline{\tau(\bar\chi)} = \overline{\sum_{x\in\mathbb{Z}/f\mathbb{Z}} \bar\chi(x)} = \sum_{x\in\mathbb{Z}/f\mathbb{Z}} \chi(x)\,\zeta^{-x} =$$

$$= \chi(-1)\sum_{x\in\mathbb{Z}/f\mathbb{Z}} \chi(-x)\,\zeta^{-x} = \chi(-1)\,\tau(\chi).$$

$$\Rightarrow |\tau(\bar\chi)| = |\chi(-1)\,\tau(\chi)| = |\tau(\chi)|$$

Rmk. $\dfrac{\tau(\chi)}{\sqrt{f}} = e^{i\theta}$ by (2), but it is extremely hard to determine θ.

Theorem. Let χ be a Dirichlet character of conductor f.

Then

$$L(\chi, s) = \begin{cases} -\dfrac{\tau(\chi)}{f} \displaystyle\sum_{a=1}^{f-1} \bar{\chi}(a) \log\left(\sin \frac{\pi a}{f}\right) & \text{if } \chi(-1) = +1 \\ \dfrac{\tau(\chi)\, \pi i}{f^2} \displaystyle\sum_{a=1}^{f-1} \bar{\chi}(a) \cdot a & \text{if } \chi(-1) = -1 \end{cases}$$

PF: Consider $\displaystyle\sum_{n=1}^{+\infty} \frac{\zeta^{an}}{n^s}$, converges for $\mathrm{Re}(s) > 1$,

where $\zeta = e^{2\pi i/f}$. When $s = 1$, the series is convergent but not absolute convergent, $\displaystyle\sum_{n=1}^{+\infty} \frac{\zeta^{an}}{n} = \log\left(1 - \zeta^a\right)$.

Here we take the branch of log that takes real values on $\mathbb{R}_{>0}$.

$$\sum_{a=1}^{f-1} \bar{\chi}(a) \sum_{n=1}^{+\infty} \frac{\zeta^{an}}{n^s} = \sum_{n=1}^{+\infty} \frac{1}{n^s} \left(\sum_{a=1}^{f-1} \bar{\chi}(a) \zeta^{an} \right) =$$

$$\left[\sum_{a=1}^{f-1} \bar{\chi}(a) \zeta^{an} = \tau_n(\bar{\chi}) = \chi(n)\, \tau(\bar{\chi}) \right.$$

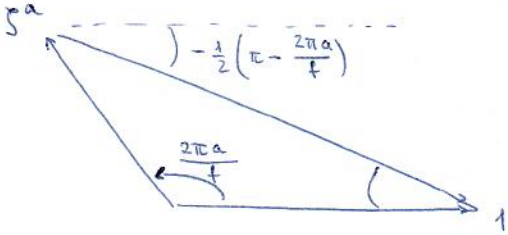
$$\left. \uparrow \text{ Lemma (1)} \right]$$

$$= \left(\sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s} \right) \cdot \tau(\bar{\chi}) = \frac{f}{\chi(-1)\, \tau(\chi)} \cdot L(\chi, s)$$

$$L(\chi, s) = \frac{\chi(-1)\, \tau(\chi)}{f} \sum_{a=1}^{f-1} \bar{\chi}(a) \left(\sum_{n=1}^{+\infty} \frac{\zeta^{an}}{n^s} \right)$$

$$\xrightarrow{s \to 1^+} L(\chi, 1) = \frac{\chi(-1)\, \tau(\chi)}{f} \sum_{a=1}^{f-1} \bar{\chi}(a) \cdot \log\left(1 - \zeta^a\right)$$

$$\log\left(1 - \zeta^a\right) = \log\left|1 - \zeta^a\right| + \left(\frac{a}{f} - \frac{1}{2}\right) \pi i$$



$$(1 - \zeta^a) = \left|1 - \zeta^a\right| \cdot e^{\left(\frac{\pi a}{f} - \frac{\pi}{2}\right) i}$$

$$\left|1 - \zeta^a\right| = 2 \sin \frac{\pi a}{f}$$

Case A. : $\chi(-1) = -1$

$$|1-\zeta^a| = |1-\zeta^{-a}|$$

$$\sum_{a=1}^{f-1} \bar{\chi}(a) \log|1-\zeta^a| = \frac{1}{2} \sum_{a=1}^{f-1} \bar{\chi}(a) \cdot \left(\log|1-\zeta^a| + \log|1-\zeta^{-a}| \right) = $$

$$= \frac{1}{2} \sum_{a=1}^{f-1} \underbrace{\left(\bar{\chi}(a) + \bar{\chi}(-a)\right)}_{0 \text{ since } -\bar{\chi}(a) = \bar{\chi}(-a).} \cdot \log|1-\zeta^a| = 0$$

$$\to L(\chi, 1) = \frac{\tau(\chi)}{f} \sum_{a=1}^{f-1} \bar{\chi}(a) \left(\frac{a}{f} - \frac{1}{2} \right) \pi i = $$

$$= \frac{\tau(\chi)\,\pi i}{f} \sum_{a=1}^{f-1} \bar{\chi}(a) \cdot a$$

Case B. : $\chi(-1) = 1$

$$\sum_{a=1}^{f-1} \bar{\chi}(a) \cdot \left(\frac{a}{f} - \frac{1}{2} \right) = \sum_{a=1}^{f-1} \frac{\bar{\chi}(a)\, a}{f} =$$

$$= \frac{1}{2} \sum_{a=1}^{f-1} \frac{\left(\bar{\chi}(a) + \bar{\chi}(-a)\right) \cdot a}{f}$$

$$= \frac{1}{2} \left(\sum_{a=1}^{f-1} \bar{\chi}(a) + \sum_{b=1}^{f-1} \bar{\chi}(b) \cdot (f-b) \right) \qquad b = f-a$$

$$= \frac{1}{2f} \Bigg(\underbrace{\sum_{a=1}^{f-1} \bar{\chi}(a) \cdot a - \sum_{b=1}^{f-1} \bar{\chi}(b) \cdot b}_{0} + \underbrace{\sum_{b=1}^{f-1} \bar{\chi}(b) \cdot f}_{0} \Bigg) = 0.$$

$$L(\chi, 1) = \frac{-\tau(\chi)}{f} \cdot \sum_{a=1}^{f-1} \bar{\chi}(a) \cdot \log|1-\zeta^a|$$

$$= -\frac{\tau(\chi)}{f} \sum_{a=1}^{f-1} \bar{\chi}(a) \cdot \underbrace{\log\left(2 \sin \frac{\pi a}{f}\right)}_{= \log 2 + \log \sin \frac{\pi a}{f}}$$

$$= -\frac{\tau(\chi)}{f} \cdot \sum_{a=1}^{f-1} \bar{\chi}(a) \cdot \log \sin \frac{\pi a}{f}$$

□

Application

p odd prime, $p \neq 3$

$p^* = p \cdot (-1)^{\frac{p-1}{2}}$, K is the unique quadratic subextension

$$\chi : \mathrm{Gal}(K/\mathbb{Q}) = \{1, -1\} \longrightarrow \mathbb{C}^\times$$

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \longrightarrow \left(\frac{a}{p}\right)$$

$$a$$

$$\begin{array}{c} \mathbb{Q}(\zeta_p) \\ | \\ K = \mathbb{Q}(\sqrt{p^*}) \\ | \\ \mathbb{Q} \end{array}$$

$$L(\chi, 1) = \begin{cases} \dfrac{2^2 \log \varepsilon_K \cdot h}{2\sqrt{p}} & p \equiv 1 \pmod 4 \\ \dfrac{(2\pi) \cdot h}{2} & p \equiv 3 \pmod 4,\ p \geq 5 \end{cases}$$

$$h = \begin{cases} \dfrac{\sqrt{p} \cdot L(\chi, 1)}{\pi} = \dfrac{\sqrt{p}\ \tau(\chi)\ \pi i}{p^2} \displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a = -\frac{p\pi}{p^2} \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a \geqslant 1 \\ \dfrac{\sqrt{p} \cdot L(\chi, 1)}{2 \log \varepsilon_K} = \dfrac{\sqrt{p}\ L(\chi, 1)}{2 \log \varepsilon_K} \displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \log \varepsilon_u^{\frac{au}{p}} = \frac{1}{2 \log \varepsilon_K} \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \log \varepsilon_u^{\frac{au}{p}} \geqslant 1 \end{cases}$$

$$\tau(\chi) = \begin{cases} i\sqrt{p} & p \equiv 3 \pmod 4 \\ \sqrt{p} & p \equiv 1 \pmod 4 \end{cases}$$

There is no elementary way of proving this w/o L-functions.

Class number formula for quadratic fields

30. 11. 2017

$K/\mathbb{Q}$ quadratic

$\chi_K : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathbb{C}^\times$
$= \{1, \tau\}$

$\tau \longmapsto -1$

How to describe χ_K as a Dirichlet character?

d_K = discriminant of $K = \mathbb{Q}(\sqrt{m})$

$d_K = \pm 2^a p_1 \cdots p_r$ $\quad a \in \{0, 2, 3\}$, p_i odd distinct primes

Prop. (1) K is a subfield of $\mathbb{Q}(\zeta_{|d_K|})$.

(2) The non-trivial character χ_K of $\mathrm{Gal}(K/\mathbb{Q})$ is identified with the Dirichlet character χ_{d_K} of conductor $|d_K|$ given by

(a) $\chi_{d_K}(-1) = \dfrac{d_K}{|d_K|}$

(b) $\chi_{d_K}(2) = \begin{cases} (-1)^{\frac{d_K - 1}{8}} & \text{if } d_K \equiv 1 \pmod 4 \\ 0 & \text{if } 2 \mid d_K \end{cases}$

$= \begin{cases} 1 & \text{if } d_K \equiv 1 \pmod 8 \\ -1 & \text{if } d_K \equiv 5 \pmod 8 \\ 0 & \text{if } 2 \mid d_K \end{cases}$

(c) $\chi_{d_K}(p) = \left(\dfrac{d_K}{p}\right)$.

Pf: (1) Induction on the number of prime factors of d_K.

Assume d_K has only one prime factor.

Then either $d_K = (-1)^{\frac{p-1}{2}} p$ for some odd p or $d_K = -4, \pm 8$.

So $K = \mathbb{Q}(\sqrt{d_K}) \subseteq \left(\mathbb{Q}(\zeta_p) \text{ or } \mathbb{Q}(\zeta_4) \text{ or } \mathbb{Q}(\zeta_8)\right)$.

$\zeta_8 = \dfrac{\sqrt{2} + \sqrt{-2}}{2}$

Suppose d_K has $r \geq 2$ prime factors, and for any $d' \mid d_K$, $d' \neq d_K$, $d' \equiv 0, 1, 4 \pmod 8$ we have $\mathbb{Q}(\sqrt{d'}) \subseteq \mathbb{Q}(\zeta_{d'})$.

$d_K = m \cdot p^*$ where $p^* = (-1)^{\frac{p-1}{2}} p$, $\gcd(p, m) = 1$.

$\mathbb{Q}(\sqrt{d_K}) \subseteq \mathbb{Q}(\sqrt{m}, \sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_{|m|}) \cdot \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{|d_K|})$.

This completes the induction.

(2) Prove that the char. $\chi_K = \chi_{d_K}$ $\quad 2 \longmapsto ?$ $\quad p \longmapsto$ Frobenius of p in $K/\mathbb{Q}$

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{|d_K|})/\mathbb{Q}\right) \cong \left(\mathbb{Z}/|d_K|\mathbb{Z}\right)^\times \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$$

$$\chi_{d_K} \searrow \quad \swarrow \chi_K$$

$$\mathbb{C}^\times$$

$$\sigma_{-1}\,\zeta_{d_K} = \zeta_{d_K}^{-1} = \overline{\zeta_{d_K}}$$

$\Rightarrow$ -1 corresponds to the cx. conjugation

$\Rightarrow$ (a)

For (b): $\chi_K(2) = -1 \iff 2$ is inert in $K/\mathbb{Q}$

$\chi_K(2) = 1 \iff 2$ splits in $K/\mathbb{Q}$

2 inert $\iff X^2 - X + \frac{1-d_K}{4} = 0$ has no solutions in $\mathbb{F}_2 \iff d_K \equiv 5\ (8)$

2 splits $\iff X^2 - X + \frac{1-d_K}{4} = 0$ has solutions in $\mathbb{F}_2 \iff d_K \equiv 1\ (8)$

(We are in the case when $d_K \equiv 1\ (4)$, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d_K}}{2}\right]$.)

For (c): if $p \nmid d_K$:

Frobenius at p in $\mathrm{Gal}(K/\mathbb{Q})$ is the img of $p \in \left(\mathbb{Z}/|d_K|\mathbb{Z}\right)^\times$

$$\chi_K(p) = \begin{cases} 1 & \text{if } p \text{ splits in } K/\mathbb{Q} \\ -1 & \text{if } p \text{ inert in } K/\mathbb{Q} \end{cases}$$

$$\iff \begin{cases} X^2 = d_K & \text{has solutions in } \mathbb{F}_p \\ X^2 = d_K & \text{has no solutions in } \mathbb{F}_p \end{cases}$$

$$\iff \begin{cases} \left(\frac{d_K}{p}\right) = 1 \\ \left(\frac{d_K}{p}\right) = -1 \end{cases}$$

Finally we need to prove that χ_K has conductor $|d_K|$. Let f be the conductor.

$$\left(\mathbb{Z}/|d_K|\mathbb{Z}\right)^\times \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$$

$$\searrow \quad \circlearrowleft \quad \nearrow$$

$$\left(\mathbb{Z}/f\mathbb{Z}\right)^\times$$

Then $f \mid d_K$ and is the minimal $\mathbb{Z}^+$ integer s.t. the diagram commutes.

$\iff f$ is the min. pos. integer s.t. $K \subseteq \mathbb{Q}(\zeta_f)$.

But all primes dividing d_K are ramified in $K/\mathbb{Q}$ $\Rightarrow$ all prime factors of d_K must be prime factors of f as well.

Since $d_K = 2^a \cdot p_1 \cdots p_r$, the only question is the exponent of 2 in f.

The only case that is wrong is $d_K = 8 p_1 \cdots p_r$, $f = 4 p_1 \cdots p_r$.

} Suppose this is the case.

$$K = \mathbb{Q}\left(\sqrt{\pm 8 d'}\right) \subseteq \mathbb{Q}\left(\zeta_{4|d'|}\right) \qquad \text{where } d' = p_1^* \cdots p_r^* \equiv 1 \pmod 4$$

↑ the asterisks only encode sign, making sure that $d' \equiv 1 \pmod 4$

But $\sqrt{d'} = \sqrt{p_1^* \cdots p_r^*} \in \mathbb{Q}(\zeta_{p_1}) \cdots \mathbb{Q}(\zeta_{p_r}) = \mathbb{Q}(\zeta_{|d'|})$.

$$\Rightarrow \sqrt{\pm 2} = \sqrt{\pm 2 d'} \Big/ \sqrt{d'} \in \mathbb{Q}\left(\zeta_{4|d'|}\right)$$

$$\sqrt{-1} \in \mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}\left(\zeta_{4|d'|}\right).$$

$$\to \zeta_8 = \frac{\sqrt{2} + \sqrt{-2}}{2} \in \mathbb{Q}\left(\zeta_{4|d'|}\right) \Rightarrow \mathbb{Q}\left(\zeta_{4|d'|}\right) = \mathbb{Q}\left(\zeta_{8d'}\right).$$

This is impossible b/c $\underbrace{\left[\mathbb{Q}\left(\zeta_{4|d'|}\right) : \mathbb{Q}\right]} = \varphi(4d')$

$$< \left[\mathbb{Q}\left(\zeta_{8|d'|}\right) : \mathbb{Q}\right] = \varphi(8d') \quad \lightning.$$

□

Rmk: If $d_K = p^*$: $\chi_{d_K}(q_r) = \left(\frac{p^*}{q_r}\right) = \left(\frac{q_r}{p}\right)$

↑ quad. rec. law

$$\tau(\chi_{d_K}) = \sum_{a \in \left(\mathbb{Z}/d_K\mathbb{Z}\right)} \chi_{d_K}(a) \cdot \zeta_{|d_K|}^a \qquad \overline{\chi}_{d_K} = \chi_{d_K}$$

Recall: $\tau(\chi)\,\tau(\overline{\chi}) = \chi(-1)\, f$ $\Rightarrow$ $\tau(\chi_{d_K})^2 = \chi_{d_K}(-1) \cdot |d_K|$

$$\Rightarrow \tau(\chi_{d_K}) = \pm\sqrt{\chi_{d_K}(-1) \cdot |d_K|}$$

Theorem: $\tau(\chi_{d_K}) = \begin{cases} \sqrt{|d_K|} & \text{if } \chi_{d_K}(-1) = 1 \\ i\sqrt{|d_K|} & \text{if } \chi_{d_K}(-1) = -1 \end{cases}$ where $\sqrt{|d_K|}$ denotes the positive square root of $|d_K|$.

PROOF: Complicated, PO.

References:
- L. Washington: Intro to cyclotomic fields, Chap 4, Cor. 4.6. uses the functional equations of $L(\chi, s)$ and $\zeta_K(s)$
- Davenport: Multiplicative Number Theory. Chap 5? uses Fourier Analysis

Special case: $|d_K| = p$. → Exercise, use eigenvalues.

□

Theorem. (Dirichlet class number formula)

The class number of K is given by $h = -\frac{1}{|d_K|} \cdot \sum_{a=1}^{|d_K|-1} \chi_{d_K}(a) \cdot a$ if $d_K < -4$

$$h = -\frac{1}{\log \varepsilon} \cdot \sum_{a=1}^{\lfloor d_K/2 \rfloor} \chi_{d_K}(a) \cdot \log\left(\sin \frac{\pi a}{d_K}\right) \quad \text{if } d_K > 0,$$

where $\varepsilon \in \mathcal{O}_K^\times$ is the fund. unit of K.

PROOF: $L(\chi, 1) = \begin{cases} \frac{2\pi h}{2\sqrt{|d_K|}} & d_K < -4 \\ \frac{2 \log \varepsilon \, h}{2\sqrt{|d_K|}} & d_K > 0 \end{cases}$ Details are left to the reader. □

Cor. Assume $d_K < -4$, $2 \mid d_K$. Then $h = -\frac{2}{|d_K|} \sum_{0<a<|d_K|/2} \chi_{d_K}(a)\, a + \sum_{0<a<|d_K|/2} \chi_{d_K}(a)$.

PROOF: $h = -\frac{1}{|d_K|} \sum_{0<a<\frac{|d_K|}{2}} \left(\chi_{d_K}(a)\, a + \chi_{d_K}(|d_K| - a)(|d_K| - a) \right) =$

$$\chi_{d_K}(|d_K| - a) = \chi_{d_K}(-a) = -\chi_{d_K}(a)$$

$$= -\frac{1}{|d_K|} \sum_{0<a<\frac{|d_K|}{2}} \left(\chi_{d_K}(a)\, a - \chi_{d_K}(a) \cdot (|d_K| - a) \right) =$$

$$= -\frac{2}{|d_K|} \sum_{0<a<\frac{|d_K|}{2}} \chi_{d_K}(a)\, a + \sum_{0<a<\frac{|d_K|}{2}} \chi_{d_K}(a)$$

□

Example. $K = \mathbb{Q}(\sqrt{-56}) = \mathbb{Q}(\sqrt{-14})$

$\forall$ odd prime p: $\chi_{-56}(p) = \left(\frac{-56}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{7}{p}\right) = \overbrace{\left(\frac{-1}{p}\right)}^{1}\left(\frac{2}{p}\right)\left(\frac{p}{7}\right)(-1)^{\frac{(7-1)(p-1)}{4}}$

$$= (-1)^{\frac{p^2-1}{8}} \cdot \left(\frac{p}{7}\right)$$

$$\chi_{-56}(p) = \begin{cases} +1 & \text{if } p = 3, 5, 9, 13, 19, 23 \\ -1 & \text{if } p = 11, 17 \end{cases}$$

$$\sum_{0<a<28} \chi_{-56}(a) =$$

$$\chi_{-56}(a) = \begin{cases} 0 & \text{if } 2 \mid p \text{ or } 7 \mid p \\ 1 & \text{if } a = 1, 3, 5, 9, 13, 15, 19, 23, 25, 27 \\ -1 & \text{if } a = 11, 17 \end{cases}$$

$$\Rightarrow \sum_{0<a<28} \chi_{-56}(a)\cdot a = 112 \quad \Rightarrow \quad h = -\frac{2}{56}\cdot 112 + 8 = 4$$

This coincides with the computation using Minkowski's bound.

$$Cl_K \cong \mathbb{Z}/4\mathbb{Z}$$

Rmk. Gauss' class number conjecture:

- For each given integer h there exist only finitely many imaginary quadratic extensions $K/\mathbb{Q}$ s.t. $h_K = h$.

  Key: get an explicit lower bound for each K in terms of d_K.

  Solved in the 1980s, using Gauss–Zagier formula, Goldfeld's estimation.

- For each given integer h there exist infinitely many real quadratic fields K with $h_K = h$.

  Still open. Problem: the c.n.f. contains the fundamental unit, which is difficult to compute.

p-adic numbers

Algebraic point of view

Define $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\geq 1} \;\middle|\; x_n \in \mathbb{Z}/p^n\mathbb{Z},\ x_{n+1} \bmod p^n = x_n \right\}$

$\mathbb{Z}_p \subseteq \prod_{n=1}^{+\infty} \left(\mathbb{Z}/p^n\mathbb{Z}\right)$

Prop. $\mathbb{Z}_p$ is an integral domain, and $\mathbb{Z}_p$ has the only max. ideal $p\mathbb{Z}_p$.

Pf: • $\forall x, y \in \mathbb{Z}_p$, $x \neq 0$, $y \neq 0$: want to show that $x \cdot y \neq 0$.

$x = (x_n)_{n\geq 1}$, $y = (y_n)_{n\geq 1}$

Assume $n_0 \geq 1$ is the minimal integer s.t. $x_{n_0} \neq 0$ in $\mathbb{Z}/p^{n_0}\mathbb{Z}$
$n_0 \geq 1$ $y_{n_0} \neq 0$

$xy = (x_n y_n)_{n\geq 1}$, $(xy)_{n_0+n_0} = x_{n_0+n_0} \cdot y_{n_0+n_0} \neq 0$ in $\mathbb{Z}/p^{n_0+n_0}\mathbb{Z}$

$\forall m \geq n_0$: $x_m \neq 0$ in $\mathbb{Z}/p^m\mathbb{Z}$ and $\forall n \geq n_0$: $y_n \neq 0$ in $\mathbb{Z}/p^n\mathbb{Z}$ by $\varprojlim$ def.

$\Rightarrow xy \neq 0$.

• $p\mathbb{Z}_p$ is the unique maximal ideal $\Leftrightarrow \forall x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$: x is invertible.

$x = (x_n)_{n\geq 1}$: $\forall x_n \not\equiv 0 \pmod p$, so $x_n \in \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$

$\Rightarrow \exists y_n \in \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$ s.t. $x_n y_n = 1$ in $\left(\mathbb{Z}/p^n\mathbb{Z}\right)$ $\Rightarrow y = (y_n)_{n\geq 1}$ is the inverse of x_n. □

Define $\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Z}_p\left[\frac{1}{p}\right]$

Topology on $\mathbb{Z}_p$

$\forall a \in \mathbb{Z}_p$ $(a + p^n\mathbb{Z}_p)_{n\geq 1}$ form a fundamental system of neighbourhoods of a

$\longrightarrow$ $\mathbb{Z}_p$ is a Hausdorff topological ring, $\mathbb{Q}_p$ a Hausdorff topological field.

Prop: The top. ring $\mathbb{Z}_p$ is complete in the sense that every Cauchy sequence in $\mathbb{Z}_p$ converges to some unique element in $\mathbb{Z}_p$, and $\mathbb{Z} \subseteq \mathbb{Z}_p$ is dense.

Pf: Assume $(a_n)_{n\geq 1}$ is Cauchy in $\mathbb{Z}_p$, i.e. $\forall m \geq 1$ $\exists N(m) \in \mathbb{Z}_{\geq 1}$ s.t. $\forall n_1, n_2 > N(m)$
$a_{n_1} - a_{n_2} \in p^m\mathbb{Z}_p$. $\Rightarrow$ the img of a_n in $\mathbb{Z}/p^m\mathbb{Z}$ is independent
$b_n \in \mathbb{Z}/p^n\mathbb{Z}$
of n as long as $n > N(m)$.

$\Rightarrow$ $b = (b_m)_{m\geq 1} \in \mathbb{Z}_p$, $b = \lim_{n\to\infty} a_n$.

Algebraic Number Theory, Lecture 15-16

$\mathbb{Z}$ is dense b/c $\mathbb{Z} \longrightarrow \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$ $\forall n \geq 1$. □

Analytic point of view

Define an absolute value $\underline{|\cdot|_p}$: $\mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$, $x \longmapsto p^{-v_p(x)}$

where $\underline{v_p(x)}$ = exponent of p in the prime factorisation of x.

$|x+y|_p \leq \max(|x|_p, |y|_p)$

$|x|_p = 0 \iff x = 0$

$\text{dist}(x,y) = |x-y|_p \quad \forall x,y \in \mathbb{Q}$. $\longrightarrow$ defines a topology on $\mathbb{Q}$.

$\underline{\mathbb{Q}_p}$:= the completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$

Connection between the two approaches:

in the analytic setting, $\mathbb{Q}_p$ has a subring $\underline{\mathbb{Z}_p} = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$, coincides with the previous definition of $\mathbb{Z}_p$.

We will switch between these points of view, and use whichever suits our needs at the time.

Examples. 1) $\frac{1}{1-p} = \sum_{n=0}^{\infty} p^n$ in $\mathbb{Z}_p$ 04.12.2017

2) $\mathbb{Q}_5 \supseteq \mathbb{Z}_5$, $\frac{1}{2} = 3 + 2\cdot 5 + 2\cdot 5^2 + \ldots + 2\cdot 5^n + \ldots$

Verification: $2 \cdot \left(3 + 2 \cdot \sum_{n=1}^{\infty} 5^n\right) \overset{?}{=} 1$

$\iff \forall N: \quad 2 \cdot \left(3 + 2 \cdot \sum_{n=1}^{N} 5^n\right) \equiv 1 \pmod{5^{N+1}}$

$2 \cdot \left(3 + 2 \cdot \sum_{n=1}^{N} 5^n\right) = 6 + 4 \cdot \frac{5^{N+1} - 5}{5-1} = 5^{N+1} + 1 \equiv 1 \pmod{5^{N+1}}$ ✓

3) $\frac{1}{3} = 2 + 3\cdot 5 + 5^2 + \ldots + 3\cdot 5^{2n-1} + 5^{2n} + \ldots$

Verification as above.

Def. A normed field (valuation field) is a field K together with a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ called a norm (or absolute value) s.t.

1) $|x| = 0 \iff x = 0$
2) $|xy| = |x||y| \quad \forall x, y \in K$
3) $|x + y| \leq |x| + |y| \quad \forall x, y \in K$

If $|\cdot|$ satisfies

3') $|x+y| \leq \max(|x|, |y|) \quad \forall x, y \in K$,

then $|\cdot|$ is called non-archimedean (otherwise it is archimedean).

Two norms $|\cdot|_1$ and $|\cdot|_2$ on K are equivalent if $\exists r \in \mathbb{R}_{>0}$ s.t. $|\cdot|_1^r = |\cdot|_2$.

Example. 1) $K = \mathbb{Q}$ $|\cdot|_\infty$ the usual abs. value
$|\cdot|_p$ p-adic norm

2) $K/\mathbb{Q}$ number field

$\forall \sigma : K \hookrightarrow \mathbb{C}$ embedding $|\cdot|_\sigma : K \to \mathbb{R}_{\geq 0}$, $x \mapsto |\sigma(x)|_{\mathbb{C}}$ archimedean

$\forall \mathfrak{p} \subseteq \mathcal{O}_K$ prime: $|\cdot|_{\mathfrak{p}} : K \to \mathbb{R}_{\geq 0}$, $x \mapsto (\underbrace{N\mathfrak{p}}_{p^{f(\mathfrak{p}|p)}})^{-v_{\mathfrak{p}}(x)}$ non-archimedean

$v_{\mathfrak{p}}(x)$ is the exponent of $\mathfrak{p}$ in the prime factorisation of the frac. ideal (x).

3) k field, $K = k(x)$.

If $p(x) \in k[x]$ irreducible, then $\forall f(x) \in k(x)^\times$ writes uniquely as $f(x) = p(x)^e \cdot \frac{g(x)}{h(x)}$ $g, h \in k[x]$, $p(x) \nmid g(x)h(x)$, $e =: v_{p(x)}(f)$

$\forall q \in \mathbb{R}_{>1}$ $|f(x)| = q^e$ is a non-arch norm on K

Def. An additive valuation v on K is a map $v : K \to \mathbb{R} \cup \{+\infty\}$ s.t.

1) $v(x) = +\infty \iff x = 0$
2) $v(xy) = v(x) + v(y)$
3) $v(x+y) \geq \min(v(x), v(y))$.

($v = -\log |\cdot|$ intuitively)

Two additive valuations v_1, v_2 on K are <u>equivalent</u> if $\exists r \in \mathbb{R}: v_2 = r \cdot v_1$.

(eq. classes of add. valuations) $\longleftrightarrow$ (eq. classes of non-arch. norms)

$$v \longmapsto |\cdot| = q^{-v(\cdot)} \qquad q \in \mathbb{R}_{>0}$$

$$v(\cdot) = -\log_q |\cdot| \longleftarrow |\cdot|$$

Prop. Let $(K, |\cdot|)$ be a (non-archimedean) normed field.

1) $|\cdot|$ is non-arch $\iff$ $|\cdot|$ is bounded on the image of $\mathbb{Z} \to K$.
In particular, if $\operatorname{char} K > 0$, then all norms are non-archimedean.

2) If $|\cdot|$ is non-arch. then for $x, y \in K$, $|x| \neq |y|$:
$|x+y| = \max(|x|, |y|)$.

PF: 1) Assume $|\cdot|$ is non-arch.

$\forall n \in \mathbb{Z}_{\geq 1}$: $|n| = |1 + \dots + 1| \leq |1|$ $\Rightarrow$ bounded.

$|-n| = |-1| \cdot |n| = |n| \leq |1|$ $\Rightarrow$ bounded.

Conversely: $|n| \leq C \quad \forall n \in \mathbb{Z}$.

$$\left|(x+y)^n\right| = \left| \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i} \right| \leq \sum_{i=0}^{n} \left|\binom{n}{i}\right| |x|^i |y|^{n-i} \leq$$

$$\leq \sum_{i=0}^{n} |x|^i |y|^{n-i} \cdot C \leq nC \cdot \max(|x|, |y|)^n$$

$\Rightarrow |x+y| \leq (nC)^{1/n} \max(|x|, |y|)$.

$n \longrightarrow \infty \Rightarrow (nC)^{1/n} \longrightarrow 1. \Rightarrow |x+y| \leq \max(|x|, |y|)$

2) Wma $|x| > |y|$.

$|x+y| \leq \max(|x|, |y|) = |x|$.

$|x| = |(x+y) - y| \leq \max(|x+y|, |y|) \leq |x+y|$ $\Big\}$ $|x+y| = |x| = \max(|x|, |y|)$.

□

$(K, |\cdot|)$ normed field $\Rightarrow$ $|\cdot|$ defines a topology on K.

$\forall a \in K$, $\forall \varepsilon \in \mathbb{R}_{>0}$ $U(a, \varepsilon) := \{x \in K \mid |x-a| < \varepsilon\}$ form a fundamental system of open nbhds.

Under this topology, K may not be complete.

Prop. There exists a unique normed field $(\hat{K}, |\cdot|_{\hat{K}})$ s.t.

1) $\hat{K}$ is complete wrt. $|\cdot|_{\hat{K}}$

2) K is canonically a dense subfield of $\hat{K}$, and $|\cdot|_{\hat{K}}\big|_K = |\cdot|$

3) if $f : (K, |\cdot|) \hookrightarrow (L, |\cdot|_L)$ is an embedding of normed fields, with L complete, then f extends uniquely to an embedding $\hat{f} : (\hat{K}, |\cdot|_{\hat{K}}) \hookrightarrow (L, |\cdot|_L)$

Pf: Standard abstract nonsense.

$\hat{K} = \{(a_n)_{n\geq 1}$ Cauchy sequences in $K\}/\sim$

$(a_n)_{n\geq 1} \sim (b_n)_{n\geq 1}$ if $\forall \varepsilon > 0\ \exists N \in \mathbb{Z}:\ \forall n > N\ |a_n - b_n| < \varepsilon$.

Extension of $|\cdot|$ to $\hat{K}$: $|(a_n)_n|_{\hat{K}} := \lim_{n\to\infty} |a_n|$

(Check well-definedness.)

$K \hookrightarrow \hat{K}$: $a \mapsto (a, a, a, \ldots)$

$\hat{K}$ is a field: $(a_n)_n \neq 0 \Rightarrow$ wma $a_n \neq 0$: remove zeros, only finitely many, this is still a Cauchy sequence. $b_n := a_n^{-1} \Rightarrow (b_n)_n$ a Cauchy sequence, $(a_n)_n \cdot (b_n)_n = 1$.

Def. Let $(K, |\cdot|)$ be a non-archimedean number field, $v : K \to \mathbb{R} \cup \{+\infty\}$ an additive valuation corresponding to $|\cdot|$.

Put $\mathcal{O}_K := \{x \in K \mid |x| \leq 1\} = \{x \in K \mid v(x) \geq 0\}$.

$\mathcal{O}_K$ is a subring of K, called the valuation ring of $|\cdot|$ or v.

If $v(K^\times) \subseteq \mathbb{R}$ is a discrete subgp., then we say that $|\cdot|$ or v is a discrete valuation and $\mathcal{O}_K$ is a discrete valuation ring.

Rmk. All discrete subgps of $\mathbb{R}$ are of the form $\mathbb{Z} \cdot c \subseteq \mathbb{R}$.

Then $\frac{1}{c} \cdot v : K^\times \to \mathbb{R}$ has image $\mathbb{Z}$, called the normalised additive valuation on K.

Examples. 1) $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$

2) $K = k(x)$, $v = v_{p(x)}$ associated to $p(x) \in k[x]$ irreducible polynomial

$\Rightarrow \mathcal{O}_K = k[x]_{(p(x))}$

3) $K = \mathbb{C}\{\{z\}\} = \{ f \in \mathbb{C}((z)) \mid f(z)$ converges in some nbh. of $z=0$ to a meromorphic function $\}$

$v : K \longrightarrow \mathbb{R}$

$\sum_{n \gg -\infty} a_n z^n = f \longmapsto$ order of f at $z=0 = \min\{n \in \mathbb{Z} \mid a_n \neq 0\}$

Laurent series

$\mathcal{O}_K = \{ f \in K \mid f(z)$ defines a holomorphic function in a nbh. of $z=0 \}$

$\hat{K} = \mathbb{C}((z))$, $\mathcal{O}_{\hat{K}} = \mathbb{C}[\![z]\!]$

Prop: Two non-archimedean norms $|\cdot|_1$ and $|\cdot|_2$ on K are equivalent iff their associated valuation rings are the same.

Pf: "$\Rightarrow$" $|\cdot|_2 = |\cdot|_1^r$ for some $r \in \mathbb{R}_{>0}$

$\Rightarrow |x|_2 \leq 1$ iff $|x|_1 \leq 1$ $\Rightarrow$ they define the same valuation ring.

"$\Leftarrow$" $|\cdot|_1$ and $|\cdot|_2$ define $\mathcal{O}_K$ as val. ring.

- If $\mathcal{O}_K = K \Rightarrow \forall x \neq 0$: $|x|_i \leq 1$ and $|x^{-1}|_i \leq 1 \Rightarrow |x|_i = 1$, $i = 1,2$.

- If $\mathcal{O}_K \subsetneq K$: let $b \in K$, $|b|_1 > 1 \iff b \notin \mathcal{O}_K$

$\Rightarrow |b|_2 > 1$. Let $c > 0$ s.t. $|b|_2^c = |b|_1$

Up to replacing $|\cdot|_2$ by $|\cdot|_2^c$, wma $|b|_2 = |b|_1$.

We prove that $\forall x \in K$ $|x|_1 = |x|_2$.

$x = 0$: trivial

$x \neq 0$: $\exists \rho \in \mathbb{R}$ s.t. $|x|_1 = |b|_1^\rho$

$\forall \frac{r}{s} \in \mathbb{Q}$ we have $|x|_1 = |b|_1^\rho \leq |b|_1^{r/s}$

$\iff |b^{-r} \cdot x^s|_1 \leq 1 \iff b^{-r} x^s \in \mathcal{O}_K \iff |b^{-r} x^s|_2 \leq 1 \iff |x|_2 \leq |b|_2^{r/s}$

$\forall \frac{m}{n} \in \mathbb{Q}$: $\rho \geq \frac{m}{n}$ $|x|_1 = |b|_1^\rho \geq |b|_1^{m/n} \iff b^m x^{-n} \in \mathcal{O}_K \iff |x|_2 \geq |b|_2^{m/n}$

$|b|_2^{m/n} \leq |x|_2 \leq |b|_1^{r/s}$ $\quad \frac{r}{s} \to \rho^+$, $\frac{m}{n} \to \rho^-$ $\Rightarrow |x|_2 = |b|_2^\rho = |b|_1^\rho = |x|_1$ $\square$

Prop. $(K, |\cdot|)$ a non-arch. val. field, $\mathcal{O}_K \subseteq K$ val. ring. Then:

(1) $\mathcal{O}_K$ is an integrally closed local domain with maximal ideal

$$\mathfrak{m}_K = \{x \in K \mid |x| < 1\}$$

(2) $\hat{K}$ = completion of K wrt. $|\cdot|$, then $\mathcal{O}_{\hat{K}} \cong \varprojlim_n \mathcal{O}_K/(\pi^n) \quad \forall \pi \in \mathfrak{m}_K \setminus \{0\}$

(3) $\mathcal{O}_K$ is a DVR if $\mathcal{O}_K$ is a local Dedekind domain

In particular, if $|\cdot|$ is discrete, then $\mathfrak{m}_K$ is principal and all the (nonzero) ideals of $\mathcal{O}_K$ are of the form $\mathfrak{m}_K^n$, $n \in \mathbb{Z}_{\geq 0}$, and $\mathfrak{m}_K^n/\mathfrak{m}_K^{n+1}$ is one-dim over $\mathcal{O}_K/\mathfrak{m}_K\mathcal{O}_K$.

Pf: (1) $\mathcal{O}_K$ is integrally closed: $\forall x \in K$ integral over $\mathcal{O}_K$ $\exists$ monic polynomial

$$x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = 0, \quad \text{with } a_i \in \mathcal{O}_K.$$

Assume $x \notin \mathcal{O}_K$, $|x| > 1$

$$\forall i > 1: \quad |a_i x^{n-i}| = \underbrace{|a_i|}_{\leq 1} \cdot |x|^{n-i} \leq |x|^{n-i} < |x|^n$$

$$0 = |x^n + a_1 x^{n-1} + \dots + a_n| = \max\left(|a_i x^{n-i}|\right) = |x|^n > 1 \quad \lightning$$

$\mathfrak{m}_K$ is the unique max. ideal of $\mathcal{O}_K$: let $x \in \mathcal{O}_K \setminus \mathfrak{m}_K$.

$$|x| = 1 \Rightarrow |x^{-1}| = |x|^{-1} = 1 \Rightarrow x^{-1} \in \mathcal{O}_K, \text{ i.e. } x \in \mathcal{O}_K^\times.$$

(2) Denote $R = \varprojlim_n \mathcal{O}_K/(\pi^n)$.

Define $\varphi: R \longrightarrow \mathcal{O}_{\hat{K}}$ as follows:

$(\bar{a}_n)_{n \geq 1} \in R$, let $a_n \in \mathcal{O}_K$ be a lift of $\bar{a}_n \in \mathcal{O}_K/(\pi^n)$

Claim. $(a_n)_{n \geq 1}$ is a Cauchy sequence in $\mathcal{O}_K \subseteq K$.

B/c: $a_{n+1} \equiv a_n \pmod{\pi^n}$

$\bar{a}_{n+1} \mapsto \bar{a}_n \in \mathcal{O}_K/(\pi^n)$

$$\varphi\left((\bar{a}_n)_{n \geq 1}\right) := (a_n)_{n \geq 1}$$

$[(a_n)_{n \geq 1}] \in \mathcal{O}_{\hat{K}}$ b/c $|(a_n)_{n \geq 1}|_{\hat{K}} = \lim_{n \to \infty} |a_n| \leq 1$

Define $\psi: \mathcal{O}_{\hat{K}} \longrightarrow R$: let $(a_n)_{n \geq 1}$ be a Cauchy sequence with $|(a_n)_n|_{\hat{K}} \leq 1$.

Up to replacing $(a_n)_n$ by an equivalent Cauchy sequence, wma:

$a_n \in \mathcal{O}_K$ and $|a_{n+1} - a_n| \leq \pi^n$, $0 \neq \pi \in \mathfrak{m}_K$

$\Downarrow$

$0 < |\pi| < 1$.

Let $\bar{a}_n$ be the img of a_n in $\mathcal{O}_K/(\pi^n)$.

We want to def. $\psi((a_n)_{n\geq 1}) = (\bar{a}_n)_{n\geq 1}$

Need to check: $a_{n+1} \equiv a_n \pmod{\pi^n \mathcal{O}_K}$

$$b := \frac{a_{n+1}-a_n}{\pi^n} \in K$$

$$|b| = \frac{|a_{n+1}-a_n|}{|\pi|^n} \leq 1 \quad \Rightarrow \quad b \in \mathcal{O}_K$$

$$a_{n+1} = a_n + \pi^n b \in a_n + \pi^n \mathcal{O}_K \quad \checkmark$$

Easy to see: $\psi\circ\varphi = id$, $\varphi\circ\psi = id$ (follows from their def.)

$$\Rightarrow \hat{\mathcal{O}_K} \cong \varprojlim_n \mathcal{O}_K/(\pi^n) \quad \checkmark$$

(3) "$\Rightarrow$": Assume $|\cdot|$ is discrete. Let v be an additive valuation corresp. to $|\cdot|$.

Then $v(K^\times) \subseteq \mathbb{R}$ discrete subgp. $\Rightarrow v(K^\times) = e\mathbb{Z}$ for some $e>0$.

Choose $\pi \in \mathcal{O}_K$ with $v(\pi) = e$.

Claim: $\mathfrak{m}_K = (\pi)$. and every element $x \in K^\times$ writes uniquely as

$$x = \pi^n \cdot u \qquad n\in\mathbb{Z},\ u \in \mathcal{O}_K^\times.$$

$\forall x \in \mathfrak{m}_K$: $v(x) > 0$, $v(\mathfrak{m}_K) = e\mathbb{Z}_{\geq 1}$

$\Rightarrow v(x) \geq e = v(\pi) \Rightarrow v\left(\frac{x}{\pi}\right) \geq 0 \Rightarrow \frac{x}{\pi} \in \mathcal{O}_K \Rightarrow x \in \pi\mathcal{O}_K$

$\Rightarrow \mathfrak{m}_K = \pi\mathcal{O}_K$.

$\forall x \in K^\times$: $v(x) = e\cdot n \qquad v\left(\frac{x}{\pi^n}\right) = v(x) - v(\pi^n) = 0$

$\frac{x}{\pi^n} \in \mathcal{O}_K^\times \Rightarrow x = \pi^n \cdot u, \quad u \in \mathcal{O}_K^\times$.

Claim: All nonzero ideals of $\mathcal{O}_K$ are $\mathfrak{m}_K = (\pi^n)$.

Hence $\mathcal{O}_K$ is noetherian, and int. closed by (1), and $\mathfrak{m}_K = (\pi)$ is the only nonzero prime ideal. $\Rightarrow \mathcal{O}_K$ local Dedekind.

"$\Leftarrow$": $\mathcal{O}_K$ local Dedekind $\Rightarrow$ all nonzero ideals are of the form $\mathfrak{m}_K^n = (\pi)^n$. Reverse the argument above: define $v(x)$ to be the max exponent n s.t. $x \in \mathfrak{m}_K^n$.

$\rightarrow$ v extends to a discrete val. on $K \rightarrow \mathcal{O}_K$ is a DVR. $\square$

7.12.2017

$(K, |\cdot|)$ is a non-archimedean normed field

$\mathcal{O}_K = \{ x \in K \mid |x| \leq 1 \}$ closed unit ball in K

The boundary of $\mathcal{O}_K$ is "thick": $\forall a \in \mathcal{O}_K$, $|a| = 1$:

$$B(a,1) = \{ x \in K \mid |x-a| < 1 \} \subseteq \mathcal{O}_K$$

Structure of complete discrete valuation fields

K complete wrt $|\cdot|$

Assume $|\cdot|$ is discrete, let $v : K \to \mathbb{Z} \cup \{+\infty\}$ be the normalised additive valuation.

Let $\pi \in K$ with $v(\pi) = 1$. $\Rightarrow$ $\mathfrak{m}_K = (\pi)$.

Fix a set of representatives $S \subseteq \mathcal{O}_K$ for $k := \mathcal{O}_K / (\pi)$ $(0 \in S)$.

e.g. $K = \mathbb{Q}_p$, $S = \{0, 1, \dots, p-1\}$. or $K = \mathbb{C}((t))$, $k = \mathbb{C}$, $S = \mathbb{C}$

Prop. Every element of K writes uniquely as a Laurent series

$$x = \sum_{n \gg -\infty} a_n \pi^n$$

Pf: $\forall x \in K^\times$ writes uniquely as $x = \pi^n \cdot u$ $n = v(x)$, $u \in \mathcal{O}_K^\times$

Wma $x \in \mathcal{O}_K$ (multiply by a power of π)

Let $\overline{x} \in k$ be the img of x.

$a_0 \in S$:= the lift of $\overline{x}$ in S

$\Rightarrow$ $x - a_0 \in \mathfrak{m}_K = (\pi)$, $x = a_0 + \pi x_1$ for $x_1 \in \mathcal{O}_K$

Repeat this process. $x = a_0 + a_1 \pi + \dots + a_N \pi^N + a_{N+1} \pi^{N+1}$,

$a_i \in S$, $x_i \in \mathcal{O}_K$.

$N \to +\infty$, use completeness $\Rightarrow$ $x = \sum_{n=0}^{+\infty} a_n \pi^n \in \mathcal{O}_K$. □

Case when $k = \mathbb{F}_q$, $q = p^a$ $\to$ there is a canonical choice for S.
$\operatorname{char} k = p$

Lemma. Let $n \geq 1$, $x \in \mathcal{O}_K$. Then $(1 + \pi^n x)^p \in 1 + \pi^{\gamma(n)} \mathcal{O}_K$.

where $\gamma(n) := \min \{ v(p) + 1, np \} \geq n + 1$.

By convention, if $\operatorname{char} K = 0$, then $v(p) = +\infty$.

Pf: $(1+\pi^u x)^p = 1 + p\pi^u x + \binom{p}{2}(\pi^u x)^2 + \dots + \binom{p}{p-1}(\pi^u x)^{p-1} + (\pi^u x)^p$

$v\left(\binom{p}{i}(\pi^u x)^i\right) \geq \gamma(u) \quad 1 \leq i \leq p$

$\Rightarrow v\left((1+\pi^u x)^p - 1\right) \geq \gamma(u)$ □

Cor. $\forall n \geq 1 \quad x \in \mathcal{O}_K$: $(1+\pi^u x)^{q^n} \in 1+\pi^{u+1}\mathcal{O}_K$

Pf: Apply the lemma n times. □

Prop. $\forall a \in \xi \cong \mathbb{F}_q \quad \exists!$ a lift $[a] \in \mathcal{O}_K$ s.t. $[a]^q = [a]$.

In particular: if $\operatorname{char} K = 0$, then $a \mapsto [a]$ gives an embedding of $\mathbb{F}_q \cong k$ to K.

Pf: If $a = 0 \Rightarrow [a] = 0$.

If $a \neq 0 \Rightarrow$ let $\tilde{a} \in \mathcal{O}_K$ be an arbitrary lift of a.

Consider the sequence $\left(\tilde{a}^{q^n}\right)_{n \geq 1}$.

Claim: This is a Cauchy sequence.

$$\left|\tilde{a}^{q^n} - \tilde{a}^{q^m}\right| = \left|\tilde{a}^{q^m}\left(\tilde{a}^{q^m(q^{n-m}-1)} - 1\right)\right| \qquad \forall n \geq m$$

Note $a^{q^{n-m}-1} = 1$ (since $a^{q-1} = 1$)

$\Rightarrow \tilde{a}^{q^{n-m}-1} = 1 + \pi b, \quad b \in \mathcal{O}_K$.

$\tilde{a}^{q^m \cdot (q^{n-m}-1)} - 1 = (1+\pi b)^{q^m} - 1 \in \pi^{m+1}\mathcal{O}_K$

So $\left|\tilde{a}^{q^n} - \tilde{a}^{q^m}\right| \leq |\pi|^{m+1} \qquad 0 < |\pi| < 1$

$\downarrow$

0 as $n \geq m \to +\infty$. ✓

K is complete $\Rightarrow \left(\tilde{a}^{q^n}\right)_{n \geq 1}$ converges to some $[a] \in K$.

$\left|\tilde{a}^{q^n}\right| = 1 \Rightarrow |[a]| = 1$.

Then $[a]^q = [a]$. □

Rmk. If $a \neq 0$, $[a] \in \mu_{q-1}(K)$ and if $\operatorname{char} K = 0$ then $a \mapsto [a]$ is multiplicative but not additive: $[a+b] \neq [a] + [b]$.

Def. $[a]$ is the Teichmüller lift of $a \in k$.

Example. $\mathbb{Z}_p \supseteq \mu_{p-1}(\overline{\mathbb{Q}})$

Cor. Every $x \in K$ writes uniquely as $x = \sum_{n \gg -\infty} [a_n]\, \pi^n$ $\quad [a_n] \in k$

If $\operatorname{char} K = p$, then $K \cong k((\pi))$. □

Structure of $K^\times$

$U_K = \mathcal{O}_K^\times$ $\qquad 0 \longrightarrow U_K \longrightarrow K^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0$

Def. $U_K^n := \{ x \in U_K \mid x \equiv 1 \pmod{\pi^n} \}$ $\quad \forall n \geq 1$.

We get a filtration: $U_K^0 \supsetneq U_K^1 \supsetneq U_K^2 \supsetneq \dots$

The filtration $\{U_K^n \mid n \geq 1\}$ is separated and exhausted.

$\bigcap_{n>0} U_K^n = 1$ $\qquad$ $\bigcup_{n \geq 0} U_K^n = U_K$

Since K is complete, $U_K = \varprojlim_n U_K / U_K^n$

We have an isomorphism of ab. groups

$$U_K / U_K^1 \cong k^\times \qquad U_K^n / U_K^{n+1} \cong k \qquad \forall n \geq 1$$

$$\forall n \geq 1: \quad (1+\pi^n x)\cdot(1+\pi^n y) = 1 + \pi^n(x+y) + \pi^{2n} x\cdot y \equiv 1 + \pi^n(x+y) \pmod{U_K^{n+1}}$$

Hensel's Lemma.

Let $(K, |\cdot|)$ be a complete non-archimedean field, not necessary a discrete valuation field.

For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x]$, define its Gauss norm to be

$$\|f\| := \max_{0 \leq i \leq n} \{ |a_i| \}$$

Def. $f(x)$ is primitive if $\|f\| = 1$, i.e. $f(x) \in \mathcal{O}_K[x]$ and $0 \neq \bar{f}(x) \in k[x]$ $(k = \mathcal{O}_K / \mathfrak{m}_K)$.

Prop. (HL) Assume $f(x) \in \mathcal{O}_K[x]$ is primitive, and $\bar{f}(x) = \bar{g}(x)\,\bar{h}(x)$ in $k[x]$ where $\bar{g}, \bar{h} \in k[x]$ are rel. prime.

Then $f(x)$ admits a factorisation $f(x) = g(x)\,h(x)$ where $g, h \in \mathcal{O}_K[x]$ and $\deg g = \deg \bar{g}$, $g(x) \bmod \mathfrak{m}_K = \bar{g}(x)$, $h(x) \bmod \mathfrak{m}_K = \bar{h}(x)$.

Moreover, $g(x)$ and $h(x)$ are unique up to $\mathcal{O}_K^\times$.

Rmk. The roles of g and h are not symmetric. By switching roles, we get a different factorisation.

PF: Idea: Construct $g_n, h_n \in \mathcal{O}_K[x]$ that approximate g, h up to modulo π^{n+1}. (Fix $\pi \in \mathfrak{m}_K \setminus \{0\}$; π need not be the uniformiser of K, which may not even exist.)

$r := \deg \bar{g}$, $s := \deg f - \deg \bar{g} \geq \deg \bar{h}$.

Take $g_0, h_0 \in \mathcal{O}_K[x]$ s.t. $\deg g_0 = r$, $g_0 \bmod \mathfrak{m}_K = \bar{g}$

and $\deg h_0 \leq s$, $h_0 \bmod \mathfrak{m}_K = \bar{h}$.

and $g_0 h_0 \equiv f \pmod{\mathfrak{m}_K}$.

Since $\gcd(\bar{g}, \bar{h}) = 1$, $\exists a, b \in \mathcal{O}_K[x]$ s.t. $a g_0 + b h_0 \equiv 1 \pmod{\mathfrak{m}_K}$.

If $g_0 h_0 = f \Rightarrow$ ✓

Else take $\pi \in \mathfrak{m}_K \setminus \{0\}$ s.t. π divides all the coeffs of $f - g_0 h_0$ and $a g_0 + b h_0 - 1$.

Assume that we have constructed $g_{n-1}, h_{n-1} \in \mathcal{O}_K[x]$. s.t.

$$\deg g_{n-1} = r, \quad g_{n-1} \equiv g_0 \pmod{\pi}$$

$$\deg h_{n-1} \leq s \quad h_{n-1} \equiv h_0 \pmod{\pi}$$

$$g_{n-1} \cdot h_{n-1} \equiv f \pmod{\pi^n}$$

(and $g_0, h_0, g_1, h_1, \dots, g_{n-2}, h_{n-2}$ are also constructed).

Write $f = g_{n-1} h_{n-1} + \pi^n f_n$.

$$\deg f_n = \deg\left(f - g_{n-1} h_{n-1}\right) \leq \deg f$$

Assume $g_n = g_{n-1} + \pi^n p_n$

$h_n = h_{n-1} + \pi^n q_n$ $\quad p_n, q_n \in \mathcal{O}_K[x]$, $\deg p_n \leq r-1$, $\deg q_n \leq s$.

Want to determine p_n, q_n by setting equations

$$g_n h_n \equiv f \pmod{\pi^{n+1}}$$

$$\left(g_{n-1} + \pi^n p_n\right)\left(h_{n-1} + \pi^n q_n\right) \equiv g_{n-1} h_{n-1} + \pi^n f_n \pmod{\pi^{n+1}}$$

$$\pi^{\nu}\left(p_n h_{n-1} + q_n g_{n-1}\right) \equiv \pi_v^{\kappa} f_n \pmod{\pi}$$

$$\iff \quad p_n h_0 + q_n g_0 \equiv f_n \pmod{\pi}$$

$$f_n b h_0 + f_n a g_0 \equiv f_n \pmod{\pi}$$

$\deg g_0 = r$. By Euclidean division in $k[x]$:

$\exists u, v \in \mathcal{O}_k[x]$ s.t. $f_n b \equiv u g_0 + v \pmod{\pi}$

$\deg v \le \deg g_0 - 1$

$$u g_0 + v h_0 + f_n a g_0 \equiv f_0 \pmod{\pi}$$

$$v h_0 + (f_n a + u h_0) g_0 \equiv f_0 \pmod{\pi}$$

Take $p_n := v$. $q_n :=$ (deg ≤ 1 part of $f_1 a + u g_0$) (use $\deg f_n \le \deg f$)

$\Rightarrow p_n h_0 + q_n g_0 \equiv f_n \mod \pi$, and we are done. □

Cor. Let $f(x) \in \mathcal{O}_k[x]$ and $\alpha_0 \in \mathcal{O}_k$ be such that $f(\alpha_0) \equiv 0 \pmod{m_k}$, and $f'(\alpha_0) \not\equiv 0 \pmod{m_k}$.

Then $\exists!\ \alpha \in \mathcal{O}_k$ s.t. $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{m_k}$.

Pf: Apply HL to $\bar{f} = \underbrace{(x - \overline{\alpha_0})}_{\bar{g}(x)} \cdot \bar{h}(x)$

$f'(\alpha_0) \not\equiv 0 \pmod{m_k} \iff \gcd(\bar{g}, \bar{h}) = 1$. The lift of $\bar{g}$ is linear $\Rightarrow$ it has a root α. □

Example: $f(x) = x^2 - a$ $\quad a \in \mathbb{Z}$ square-free

$p \nmid 2a \Rightarrow$ if $\left(\frac{a}{p}\right) = 1$ then $f(x)$ admits a root in $\mathbb{Z}_p$.

$x^2 - a \equiv (x+\alpha)(x-\alpha) \pmod{p}$

$f'(\alpha) = 2\alpha \not\equiv 0$ because $p \nmid 2a$

Cor. $\Rightarrow \exists \tilde{\alpha} \in \mathbb{Z}_p$, $\tilde{\alpha} \equiv \alpha \pmod{p}$ root of f

Cor. If $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ is an irreducible polynomial,

then $\underbrace{\|f\|}_{= \max_{0 \le i \le n} \{|a_i|\}} = \max\{|a_0|, |a_n|\}$.

PF: Up to multiplying by a scalar in $K^\times$, wma $\|f\| = 1$, i.e.

$f(x) \in \mathcal{O}_K[x]$ primitive. (So we will be able to apply HL.)

Assume $\exists\ 1 \le i \le n-1$ s.t. $|a_i| > \max\{|a_0|, |a_n|\}$

Then $\bar f(x) = \bar a_j x^j + \dots + \bar a_{n-1} x^{n-1}$ for some $1 \le j \le n-1$, $\bar a_j \neq 0$.

Apply HL to $\bar g = x^j$, $\bar h = \bar a_j + \dots + \bar a_n x^{n-j}$ $\bar a_j \neq 0$

$\Rightarrow f(x) = g(x)\,h(x)$, $\deg g = \deg \bar g \le n-1$ contradicts the irreducibility of f. □

Now we turn to <u>functional analysis</u>.

<u>Def</u> V vector space over a complete non-archimedean field $(K, |\cdot|)$.

A <u>norm on V</u> is a map $\|\cdot\| : V \longrightarrow \mathbb{R}_{\ge 0}$ s.t.

(1) $\|x\| = 0 \iff x = 0$

(2) $\|\lambda \cdot x\| = |\lambda| \cdot \|x\|$ $\forall \lambda \in K$ $\forall x \in V$.

(3) $\|x+y\| \le \max\{\|x\|, \|y\|\}$ $\forall x, y \in V$.

<u>Def</u>. Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ are <u>equivalent</u> on V if $\exists\ C_1, C_2 \in \mathbb{R}_{>0}$ s.t.

$$C_1 \|x\|_1 \le \|x\|_2 \le C_2 \|x\|_1 \qquad \forall x \in V.$$

Equivalent norms define the same topology on V.

<u>Prop.</u> Let V be a finite dimensional vector space over K.

Then any two norms on V are equivalent, and V is complete (wrt. any of these norms).

PF: Choose a basis of V/K: $(v_1, \dots, v_n)$.

$$\forall x = \sum_{i=1}^n x_i v_i \in V$$

Def. $\|x\| := \max_{1 \le i \le n} \{|x_i|\}$. This is a norm wrt. which V is complete.

It remains to show that any norm $\|\cdot\|'$ on V is equivalent to this one.

$$\Big\| \sum_{i=1}^n x_i v_i \Big\|' \le \max_{1 \le i \le n} \|x_i v_i\| = \max_{1 \le i \le n} |x_i| \cdot \|v_i\| \le C_2 \max_{1 \le i \le n} |x_i|$$

$$C_2 := \max_{1 \le i \le n} \|v_i\|$$

To get $\|\cdot\|' \geq C_i \|\cdot\|$, use induction on $n = \dim V$.

$n = 1$ is trivial.

$n \geq 2$: suppose it is true for $n-1$.

For $1 \leq i \leq n$, let $V_i := K v_1 + \ldots + K v_{i-1} + K v_{i+1} + \ldots + K v_n$,

V_i is complete wrt $\|\cdot\|'$

$\Rightarrow$ $v_i + V_i \subseteq V$ closed (Hausdorffness) $\longleftarrow$ This is the key step.

$0 \notin v_i + V_i \Rightarrow \exists\, \varepsilon > 0$ s.t. $U(0,\varepsilon) = \{x \in V \mid \|x\|' < \varepsilon\}$ is disjoint with $v_i + V_i$.

$\Rightarrow \forall x \in V_i : \|x + v_i\|' \geq \varepsilon$.

Now $x = \sum a_i x_i \in V$.

Suppose $\|x\| = \max\limits_{1 \leq i \leq n} \{|a_i|\} = |a_r| > 0$

Then

$$\|x\|' = |a_r| \left\| \frac{a_0}{a_r} v_1 + \ldots + \frac{a_{r-1}}{a_r} v_{r-1} + v_r + \ldots + \frac{a_n}{a_r} v_n \right\| \geq$$

$$\geq \varepsilon \cdot |a_r| = \varepsilon \cdot \|x\|.$$

□

11.12.2017

Theorem. Let L/K be a finite extension of fields of deg n.

Assume that K is complete wrt a non-arch. norm $|\cdot|$.

Then there is a unique norm $|\cdot|_L$ extending $|\cdot|$ on K and $\forall x \in L$:

$|x|_L = |N_{L/K}(x)|^{1/n}$. Moreover, L is complete wrt $|\cdot|_L$.

Pf: Two things to check.

1) $|\cdot|_L$ defines a norm on L, extending $|\cdot|$ on K

2) If $|\cdot|_L'$ is another norm with this prop., then $|\cdot|_L = |\cdot|_L'$.

(completeness follows from finite dimensionality of L.)

It is clear that $|x|_L = |x|$ if $x \in K$.

First we prove that the int. closure of $\mathcal{O}_K$ in L, denoted by $\mathcal{O}_L$, coincides with $\{x \in L \mid |x|_L \leq 1\}$.

If $x \in \mathcal{O}_L$: $N_{L/K}(x) \in \mathcal{O}_K \Rightarrow |x|_L \leq 1$

If $|x|_L \leq 1$: let $f(T) \in K[T]$ be the monic min. polynomial of x over K

$$f(T) = T^d + a_{d-1}T^{d-1} + \dots + a_1 T + a_0$$

$$a_0 = (-1)^d N_{K(x)/K}(x) \qquad |x|_L = \underbrace{|N_{L/K}(x)|^{1/n}}_{\left|\left(N_{K(x)/K}(x)\right)^{n/d}\right|^{1/n} = |N_{K(x)/K}(x)|^{1/d}} \leq 1$$

$\Rightarrow |a_0| = |x|_L^d \leq 1$

f irreducible $\Rightarrow \|f\| = \max\{1, |a_0|\} \leq 1$

$\Rightarrow \forall a_i \in \mathcal{O}_K \Rightarrow x \in \mathcal{O}_L$. ✓

To finish the proof of 1):

- $|x \cdot y|_L = |N_{L/K}(xy)|^{1/n} = |N_{L/K}(x)|^{1/n} |N_{L/K}(y)|^{1/n} = |x|_L \cdot |y|_L$. ✓
- $|x+y|_L \leq \max\{|x|_L, |y|_L\}$:

  Wma $y \neq 0$. Divide by y: it sts $|x+1|_L \leq \max\{|x|, 1\}$ and $|x|_L \leq |y|_L$

  $\forall x \in L$ with $|x|_L \leq 1$.

  This follows from the fact that $\mathcal{O}_L = \{x \in L \mid |x|_L \leq 1\}$ and the fact that $\mathcal{O}_L$ is a subring (b/c it is an int. closure),

  $x \in \mathcal{O}_L \Rightarrow 1+x \in \mathcal{O}_L$. ✓

2) First we prove $|\alpha|_L \leq 1 \iff |\alpha|_L' \leq 1$. $\forall \alpha \in L$.

Consider the minimal monic polynomial $f(T) = T^d + a_{d-1}T^{d-1} + \dots + a_0 \in K[T]$ of α. If $|\alpha|_L \leq 1$, then $|a_0| = |(-1)^d N_{K(\alpha)/K}(\alpha)| = |\alpha|_L^d \leq 1$

$\|f\| = \max\{1, |a_0|\} \Rightarrow \forall a_i \in \mathcal{O}_K$.

If $|\alpha|_L' > 1$ then

$$|\alpha|_L' > \underbrace{|a_i \alpha^i|_L'}_{|a_i| \cdot (|\alpha|_L')^i} \qquad \forall\, 0 \leq i \leq d-1$$

$$0 = |f(\alpha)|_L' = |\alpha^d|_L' > 1 \quad \lightning$$

If $|\alpha|_L < 1$: we claim that $\forall a_i \in \mathfrak{m}_K$, i.e. $\forall |a_i| < 1$.

$|a_0| = |\alpha|_L^d < 1$ if there exists any j with $|a_j| = 1$.

Let i be the minimal of such j's. $(1 \le i \le d-1)$

Then the reduction of $f(T)$ in $k[T]$ $\quad (k = \mathcal{O}_K/\mathfrak{m}_K)$

is $\overline{f}(T) = \overline{a_i}\, T^i + \dots + T^d$

$= T^i \left(\overline{a_i} + \dots + T^{d-i} \right)$

HL $\Rightarrow$ $f(T) = g(T)\, h(T)$ with $\deg g = i$, $\overline{g} = T^i$.

This contradicts with the irreducibility of f. $\lightning$

Since $\alpha^d + a_{d-1}\alpha^{d-1} + \dots + a_0 = 0$,

$\exists\, 0 \le i \le d-1$ s.t. $|\alpha^d|_L' \le |a_i \alpha^i|_L'$

$(|\alpha|_L')^{d-i} \le |a_i|$

$|\alpha|_L' \le |a_i|^{\frac{1}{d-i}} < 1$

In summary: we proved that $\forall \alpha \in L \setminus \{0\}$.

$|\alpha|_L \le 1 \Rightarrow |\alpha|_L' \le 1$

$|\alpha|_L < 1 \Rightarrow |\alpha|_L' < 1$

Applying to α^{-1}:

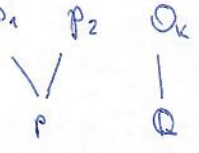
$|\alpha|_L > 1 \Rightarrow |\alpha|_L' > 1$.

i.e. $|\alpha|_L \le 1 \Leftrightarrow |\alpha|_L' \le 1$. So $|\cdot|_L$ and $|\cdot|_L'$ define the same valuation ring $\Rightarrow$ they are equivalent.

But they are both extensions of $|\cdot|$ on K $\Rightarrow$ $|\cdot|_L = |\cdot|_L'$. $\square$

Rmk. The assumption that K is complete is crucial.

E.g. let $K/\mathbb{Q}$ be a finite extension. If p splits in K then $|\cdot|_p$ on $\mathbb{Q}$ has exactly two extensions to K, corresponding to the 2 prime ideals of $\mathcal{O}_K$ above p.



Rmk. In terms of additive valuations, the extension of an additive valuation v on K to L is given by

$$v_L(x) = \frac{1}{n} v\left(N_{L/K}(x)\right) \qquad \forall x \in L.$$

Hence we have a unique extension of $|\cdot|$ or v from K to $\overline{K}$.

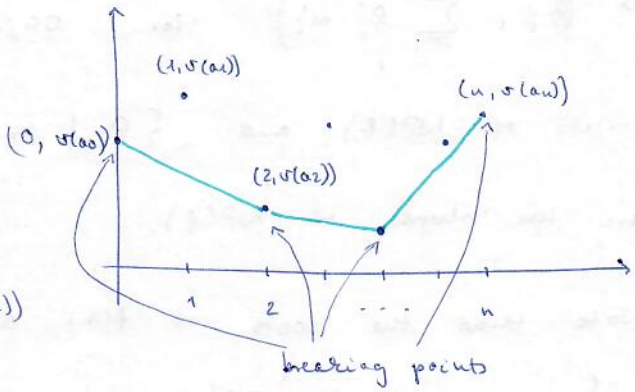
Newton polygon

Assume that K is a discrete valuation field with (normalised) additive valuation v.

$$v : K \longrightarrow \mathbb{Q} \cup \{+\infty\}$$

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x]$.

Def. The Newton polygon of $f(x)$ is the lower convex envelope in $\mathbb{R}^2$ of $\{ (i, v(a_i)) \mid 0 \le i \le n \}$



Assume that a breaking points of NP(f) are

$$(q_0, t_0) = (0, v(a_0)), \dots, (q_r, t_r) = (n, v(a_n))$$

$(r \le n)$.

Put $s_j := \dfrac{t_{j-1} - t_j}{q_j - q_{j-1}}$. Then $s_1 > s_2 > \dots > s_r$, these are the negative of the slope of the line segments.

Prop. For each j with $1 \le j \le r$ there are exactly $m_j := q_j - q_{j-1}$ roots of $f(x)$ in $\overline{K}$ with valuation s_j. (Note that $\sum_j m_j = n$).

Pf: $f(x) = a_0 + a_1 x + \dots + a_n x^n$ Wma $a_0 = 1$.

Let $\alpha_1, \dots, \alpha_n \in \overline{K}$ be s.t. $f(x) = \prod_{i=1}^{n} (1 - \alpha_i x)$

Denote by $\rho_1 < \dots < \rho_{r'}$ the distinct valuations of α_i.

Let m'_j be the multiplicity of ρ_j. $\sum m'_j = n$.

Put $q'_0 := 0$ and $m'_0 = 0$. and

$$q'_j = \sum_{i=1}^{j} m'_i \quad \Rightarrow \quad q'_j - q'_{j-1} = m'_j$$

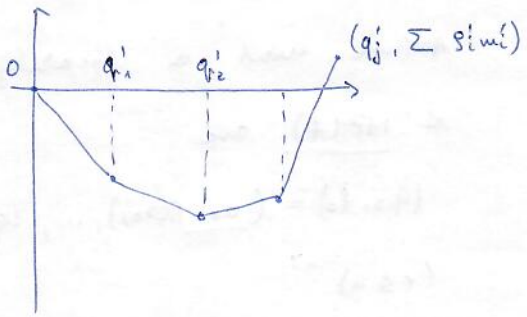
We label the α_i so that $v(\alpha_i) = \rho'_j$ if $q'_{j-1} + 1 \le i \le q'_j$

Then we have $a_i = (-1)^i \sum_{1 \le j_1 < \cdots < j_i \le n} \alpha_{j_1} \alpha_{j_2} \cdots \alpha_{j_i}$

$$\Rightarrow v(a_{q'_j}) = v(\alpha_1 \alpha_2 \cdots \alpha_{q'_j}) = \sum_{i=1}^{j} \rho'_i m'_i$$

and $q'_{j-1} \le i \le q'_j$, one has $v(a_i) \ge \sum_{\ell=1}^{j-1} \rho'_\ell m'_\ell + (i - q'_{j-1}) \rho'_j$.

$\Rightarrow \left(q'_j, \sum_{i=1}^{j} \rho'_i m'_i\right)$ for $0 \le j \le r-1$ are exactly the breaking points of $NP(f)$ and $\{\rho'_i \mid 1 \le i \le r\}$ are the slopes of $NP(f)$.



Note that the roots of $f(x)$ are exactly α_i^{-1} with valuation $-\rho'_i$

$\lambda_i = -\rho'_i$

□

Cor. In the above situation, if $f(x)$ is irreducible in $K[x]$ then $NP(f)$ has only one slope.

Conversely, if $NP(f)$ has only one slope of the form $\lambda = \frac{t}{n}$ with $\gcd(t,n) = 1$ where $n = \deg f$, then f is irreducible.

In particular, an Eisenstein polynomial is irreducible in $O_K[x]$.

Pf: If $f(x)$ is irreducible, then all the roots of $f(x)$ have the same valuation, namely $v(\alpha) = \frac{1}{\deg f} v\left(\frac{a_n}{a_0}\right)$. $\left(f(x) = a_n x^n + \cdots + a_0\right)$

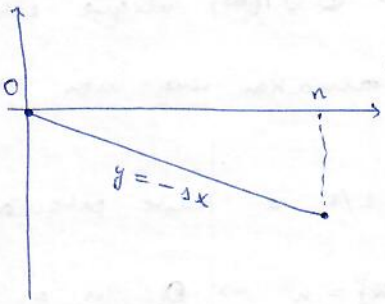
for all roots α of f.

$\Rightarrow$ $NP(f)$ has only one slope by the Prop. above.

Conversely, assume that $NP(f)$ is given by the line segment

$y = -\frac{t}{n}x$ on $0 \le x \le n$.

This line segment does not pass through any integral points except for $(0,0)$ and $(n, -t)$ s/c $\gcd(n,t) = 1$.



$\lightning$ If $f(x)$ was not irreducible, then $f(x) = g(x)\,h(x)$ $\quad g, h \in K[x]$

where $g(x)$ is irreducible of degree $m < n$.

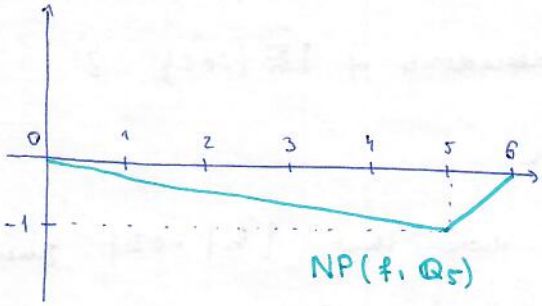
$\Rightarrow$ $NP(g)$ has end point $(m, -tm)$.

But $-tm \notin \mathbb{Z}$, contradiction. $\lightning$

□

Example. $f(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \frac{x^5}{5} + \frac{x^6}{6} \in \mathbb{Q}[x]$ Is f irreducible?

$\mathbb{Q} \hookrightarrow \mathbb{Q}_5$, inherited valuation.



$f(x)$ has 5 roots in $\overline{\mathbb{Q}_5}$ with val. $1/5$

and 1 root in $\overline{\mathbb{Q}_5}$ with val. -1

$\rightarrow$ $f(x) = g(x)\,h(x)$ $\quad \deg g = 5, \ \deg h = 1$.

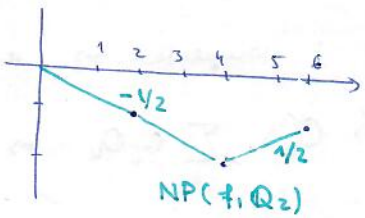
in $\mathbb{Q}_5[x]$

Both g and h are irreducible by the above discussion.

$\mathbb{Q} \hookrightarrow \mathbb{Q}_2$, $NP(f, \mathbb{Q}_2)$

$\Rightarrow$ f has no root in $\mathbb{Q}_2$

$\Rightarrow$ f is irreducible in $\mathbb{Q}[x]$



We could have looked at $\mathbb{Q} \hookrightarrow \mathbb{Q}_3$ and obtained a different factorisation.

14.12.2017

Finite extensions of complete discrete valuation fields

K complete discrete val. field

$v_K : K \to \mathbb{Z} \cup \{\infty\}$ normed valuation

$v_{\bar{K}} : \bar{K} \to \mathbb{Q} \cup \{\infty\}$ unique extension to $\bar{K}$.

$\mathcal{O}_K \subseteq K$ valuation ring with max. ideal $\mathfrak{m}_K$. $\pi_K \in \mathcal{O}_K$ uniformiser i.e. $(\pi_K) = \mathfrak{m}_K$.

$L \subseteq \bar{K}$, L/K a finite extension

Lemma. $[L:K] = n \Rightarrow \mathcal{O}_L$ is a finite free $\mathcal{O}_K$-module of rk n.

Pf: For $x \in \mathcal{O}_L$ let $\bar{x} \in \mathcal{O}_L/\pi_K\mathcal{O}_L$ be its reduction.

Let $\{b_i \mid i \in I\} \subseteq \mathcal{O}_L$ s.t. $\{\bar{b}_i \mid i \in I\} \subseteq \mathcal{O}_L/\pi_K\mathcal{O}_L$ form a base over $k = \mathcal{O}_K/\pi_K\mathcal{O}_K$.

$\{$ Assume $\sum_i a_i b_i = 0$ where $\forall a_i \in K$, some $a_i \neq 0$.

Multiply by $\pi_K \longrightarrow$ wma $a_i \in \mathcal{O}_K$ and there is some $a_i \in \mathcal{O}_K^\times$.

$\Rightarrow \sum_i \bar{a}_i \bar{b}_i = 0$. Some $\bar{a}_i \neq 0$ since $a_i \in \mathcal{O}_K^\times$. Thus contradicting the lin. independence of $\{\bar{b}_i \mid i \in I\}$. $\}$ $\Rightarrow \{b_i \mid i \in I\}$ lin. indep. and $\#I \leq n$.

We will show that $\{b_i \mid i \in I\}$ generate $\mathcal{O}_L$ over $\mathcal{O}_K$.

$\{\bar{b}_i \mid i \in I\}$ generate $\mathcal{O}_L/\pi_K\mathcal{O}_L$ over k.

$\Rightarrow$ for $x \in \mathcal{O}_L$ there are $a_i^{(0)} \in \mathcal{O}_K$ s.t. $x \in \sum_i a_i^{(0)} \cdot b_i + \pi_K \mathcal{O}_L$.

Inductively, there are $a_i^{(\ell)} \in \mathcal{O}_L$ s.t.

$$x \in \sum_i \underbrace{\left(a_i^{(0)} + \ldots + a_i^{(\ell)} \cdot \pi_K^{\ell}\right)}_{\in \mathcal{O}_K,\ \text{these form a Cauchy sequence } (\ell \in \mathbb{N})} b_i + \pi_K^{\ell-1} \mathcal{O}_K.$$

K is complete $\Rightarrow$ the sequence converges in $\mathcal{O}_K$, $x \in \sum_i b_i \mathcal{O}_K$

$\Rightarrow \mathcal{O}_L = \sum_i b_i \mathcal{O}_K \Rightarrow L = \sum_i b_i K \Rightarrow \#I = n.$ □

Rmk. $b_1, \dots, b_n \in \mathcal{O}_L$ basis $/\mathcal{O}_K \iff \overline{b_1}, \dots, \overline{b_n} \in \mathcal{Q}/\pi_K \mathcal{Q}$ basis $/k$

by the proof. This is like Nakayama's Lemma.

Recall: for $x \in L$ $\quad v_K(x) = \frac{1}{n} \cdot v_K\left(N_{L/K}(x)\right)$

$\Rightarrow v_K(L^\times) = \frac{1}{e}\mathbb{Z} \subseteq \frac{1}{n}\mathbb{Z}$ for some $e \geq 0$, $e \mid n$

Def. $e(L|K) = e$ is the ramification index.

Equivalently: $\pi_K = u \cdot \pi_L^e$ where π_L is an uniformiser of L, $u \in \mathcal{O}_L^\times$.

$k_L := \mathcal{O}_L/\pi_L$. This is an extension of k. The extension is finite.

$$\mathcal{O}_L/\pi_K \mathcal{O}_L \longrightarrow \mathcal{O}_L/\pi_L \mathcal{O}_L = k_L.$$

Def. $f(L|K) = [k_L : k]$ residue degree.

Def. L/K is unramified if $e(L|K) = 1$ and k_L/k is separable*. Equivalently, an uniformiser in K remains an uniformiser in L.

* This condition is there so that this coincides with a notion of alg. geo. Always satisfied if k is perfect, e.g. $K = \mathbb{Q}_p$, $k = \mathbb{F}_p$.

Def. L/K is totally ramified if $f(L|K) = 1$.

Prop. 1) $e(L|K)\, f(L|K) = n = [L:K]$

2) $\alpha_1, \dots, \alpha_f \in \mathcal{O}_L$ s.t. $\overline{\alpha_1}, \dots, \overline{\alpha_f} \in k_L$ are a basis $/k$.

Then $\{\alpha_i \pi_L^{j-1} \mid 1 \leq i \leq f,\ 1 \leq j \leq e\}$ form a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$.

Pf: 1) $\dim_k \mathcal{O}_L/\pi_K \mathcal{O}_L = n$.

$\pi_K \mathcal{O}_L = (\pi_L^e)$.

$\Rightarrow$ Filtration $\mathcal{O}_L/\pi_L^e \supsetneq (\pi_L)/(\pi_L^e) \supsetneq \dots \supsetneq (\pi_L^{e-1})/(\pi_L^e) \supsetneq 0$

with resp. quotients $(\pi_L^i)/(\pi_L^{i+1}) \cong k_L$. $\Rightarrow n = e \cdot f$. ✓

2) $\{\bar{\alpha}_i\ \bar{\pi}_L^{j+1}\}$ generate $\mathcal{O}_L/\pi_K\mathcal{O}_L$ / k and form a basis

$\Rightarrow \{a_i\ \pi_L^{j+1}\}$ form a basis of $\mathcal{O}_L$ / $\mathcal{O}_K$ by the Rmk. □

Assume that L is a totally ramified extension, i.e. $e(L|K) = n$.

$\Rightarrow v_K(\pi_L) = \frac{1}{n}$.

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{O}_K[x]$ be the monic minimal polynomial of π_L over $\mathcal{O}_K$.

$\Rightarrow a_i$ are polynomials in the Gal conjugates of π_L.

$\Rightarrow v_K(a_i) > 0$ and $v_K(a_0) = v_K(N_{L/K}(\pi_L)) = n\, v_K(\pi_L) = 1$.

$\Rightarrow f$ is an Eisenstein polynomial.

(Conversely, if π_L has an Eisenstein min. polynomial, then the extension is totally ramified.)

By previous prop. $\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

Thm. Let k'/k be a finite separable extension. Then

1) there is an unramified K'/K s.t. $k_{K'} = k'$.

The field K' is unique up to iso and K'/K is Galois iff k'/k is Galois.

2) L/K finite extension.

$$\mathrm{Hom}_{K\text{-alg}}(K', L) \simeq \mathrm{Hom}_{k\text{-alg}}(k', k_L). \qquad \text{("adjunction")}$$

In particular, if k'/k is Galois then we have a canonical iso

$$\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(k'/k).$$

In other words:

$$\begin{array}{ccc} \{L/K \text{ finite extensions}\} & \xrightarrow{\text{reduce}} & \{k_L/k \text{ finite}\} \\ \cup\!| & & \cup\!| \\ \{K'/K \text{ unramified ext.}\} & \xleftarrow[\text{equivalence of categories}]{\sim} & \{k'/k \text{ finite sep.}\} \end{array}$$

Pf: 1) $k' \simeq k[x]/\bar{f}(x)$ by finite separability where $\bar{f}(x) \in k[x]$ is irreducible monic.

Let $f(x) \in \mathcal{O}_K[x]$ be monic with reduction $\bar{f}(x)$.

Then $f(x)$ is irreducible (since its reduction is).

Set $K' := K[x]/f(x)$, $\alpha := \bar{x} \in K'$.

$\Rightarrow v(\alpha) = 0$ and $k' = k[x]/\bar{f}(x) \longrightarrow k_{K'}$

$x \longmapsto \alpha$

$\Rightarrow k' = k_{K'}$ as $n := \deg f = [k' : k] = [K' : K]$.

Moreover, $f(K' \mid K) = n = [K' : K] \Rightarrow K'/K$ is unramified.

Note that up to this point, we have barely used separability.

If we show 2), then the uniqueness claim and the claim about Galois extensions of 1) will also follow. ✓

2) L/K finite.

$$\mathrm{Hom}_{K\text{-alg}}(K', L) \xleftrightarrow{1\text{-}1} S(L) = \{\beta \in L \mid f(\beta) = 0\}$$

$$\mathrm{Hom}_{k\text{-alg}}(k', k_L) \xleftrightarrow{1\text{-}1} S(k_L) = \{\gamma \in k_L \mid \bar{f}(\gamma) = 0\}$$

$\updownarrow$ 1-1 by HL using the separability of $\bar{f}$.

□

Cor. L/K finite, k_L/k sep. Then there is a unique $L_0 \subseteq L$ subextension field of K s.t. L_0/K is unram and $k_{L_0} = k_L$.

Moreover, L_0 contains all $K' \subseteq L$ for which K'/K is unram. □

Example $\overline{\mathbb{F}_p} = \bigcup_{(n,p)=1} \mathbb{F}_p[\zeta_n]$ where ζ_n is a primitive n^{th} root of unity.

$\Rightarrow \mathbb{Q}_p(\zeta_n)$ for $(n,p) = 1$ is unramified, $\bigcup_{(n,p)=1} \mathbb{Q}_p(\zeta_n)$ is the maximal unramified extension of $\mathbb{Q}_p$.

From now on, let L/K and k_L/k be separable.

$$\mathbb{Z} \xleftrightarrow{1:1} \{\mathfrak{a} \subseteq L \text{ fractional}\}$$
$$i \longmapsto (\pi_L)^i$$

$$\underline{v_L(\mathfrak{A})} \longleftrightarrow \mathfrak{A}$$
$$\| $$
$$\min_{x \in \mathfrak{A}} \{v_L(x)\}, \quad v_L : L \to \mathbb{Z} \cup \{\infty\} \text{ normed valuation}$$

Def. $\underline{N_{L/K}(\mathfrak{A})} := \left(N_{L/K}(\pi_L)\right)^{v_L(\mathfrak{A})} \subseteq K$ fractional ideal.

Lemma. $v_K(N_{L/K}(\mathfrak{A})) = f(L|K) \cdot v_L(\mathfrak{A})$

Pf: It suffices to show that $v_K(N_{L/K}(\pi_L)) = f(L|K)$ since both sides are grp. homomorphisms. on $\mathfrak{A}$.

$L_0 \subseteq L$ max. unram subextension, $f(L_0|K) = f(L|K)$

$$\Rightarrow N_{L/K}(\pi_L) = N_{L_0/K}\big(\underbrace{N_{L/L_0}(\pi_L)}_{\text{uniformiser of } L_0 \text{ since } L/L_0 \text{ is totally ramified}}\big)$$

$\Rightarrow$ wlog: $L_0 = L$.

$\pi_L = \pi_K \cdot u \quad (u \in \mathcal{O}_L^\times)$ and $v_K(N_{L/K}(\pi_L)) = v_K(N_{L/K}(\pi_K)) =$

$= [L:K] = f(L|K)$. □

Recall: $Tr_{L/K} : L \times L \to K$ is a non-degenerate bilinear form.
$(x,y) \mapsto Tr_{L/K}(xy)$

Set $\underline{\vartheta} := \{x \in L \mid Tr_{L/K}(x \cdot y) \in \mathcal{O}_K \ \forall y \in \mathcal{O}_L\}$ "dual lattice of $\mathcal{O}_L$"

$\to \vartheta$ is a fractional ideal of L, $\mathcal{O}_L \subseteq \vartheta$.

Def. $\underline{\delta_{L/K}} := \vartheta^{-1}$ different of L/K

$\underline{\mathfrak{d}_{L/K}} := N_{L/K}(\delta_{L/K})$ discriminant of L/K.

Prop. $K \subseteq K' \subseteq L$ subextension $\Rightarrow \delta_{L/K} = \left(\delta_{K'/K}\mathcal{O}_L\right) \cdot \delta_{L/K}$

and $\mathfrak{d}_{L/K} = N_{K'/K}(\mathfrak{d}_{L/K}) \cdot \mathfrak{d}_{K'/K}^{[L:K']}$.

Pf: The same as for number fields. □

Prop. Assume $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, $f(x) \in \mathcal{O}_K[x]$ monic min. poly of α.

$\Rightarrow \delta_{L/K} = (f'(\alpha))$.

Pf: The same as Exercise 4.1. □

Prop. 1) Assume L/K is totally ramified, $e := e(L|K)$.

$\Rightarrow v_L(\delta_{L/K}) \geq e-1$

and we have "=" iff e is prime to $\mathrm{char}\, k$, in which case we say that L/K is tamely ramified.

2) L/K is unramified iff $v_L(\delta_{L/K}) = 0$.

Pf: 1) $\pi_L \in L$ uniformiser, $f(x)$ monic min. poly. of π_L.

L tot. ram., $\mathcal{O}_L = \mathcal{O}_K[\pi_L] \Rightarrow f(x) = \sum_{i=1}^{n} a_i x^i$ Eisenstein

$$v_L(\delta_{L/K}) = v_L(f'(\pi_L)) = v_L\left(e\pi_L^{e-1} + a_{e-1}(e-1)\pi_L^{e-1} + \dots + a_1\right)$$

$$v_L(i a_i \pi_L^{i-1}) = i-1 + v_L(i a_i) \geq \underbrace{i-1+e}_{\geq e} \quad \text{for } 1 \leq i \leq e-1.$$

$\pi_K \mid a_i$

On the other hand:

$$v_L(e\pi_L^{e-1}) = v_L(e) + e - 1 \geq e-1 \Rightarrow v_L(f'(\pi_L)) \geq e-1$$

Δ ineq.

If $v_L(e) > 0 \Rightarrow v_L(f'(\pi_L)) > e-1$.

If $v_L(e) = 0 \Rightarrow v_L(f'(\pi_L)) = v_L(e \cdot \pi_L^{e-1}) = e-1$. ✓

2) • L/K unram $\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\alpha]$, $f(x)$ the monic min poly of α.

s.t. $\overline{f}(x) \in k[x]$ is irreducible and separable.

$\Rightarrow \overline{f}'(\alpha) \neq 0$ by sep.

$$0 = v_L(f'(\alpha)) = v_L(\delta_{L/K}). \quad ✓$$

• Conversely: if $v_L(\delta_{L/K}) = 0$, let L_0 be the max. unram subext.

$$\delta_{L/K} = \underbrace{(\delta_{L_0/K}\,\mathcal{O}_L)}_{\mathcal{O}_L} \cdot \delta_{L/L_0} \qquad v_L(\delta_{L/L_0}) \geq e-1 \text{ where } e = [L:L_0] \geq 1$$

$$\Rightarrow 0 = v_L(\delta_{L/K}) \geq e-1 \Rightarrow e = 0,$$

$$\Rightarrow L = L_0$$

□

Let $K^{sep} \supseteq K$ be a separable closure of K.

Def. $K^{un} := \bigcup_{K^{sep}/L/K \text{ unramified}} L \subseteq K^{sep}$ maximal unramified extension

$K^{tr} := \bigcup_{K^{sep}/L/K} L \subseteq K^{sep}$ maximal tamely ramified extension

L/K at most tamely ram. & k_L/k is sep.

$\Rightarrow$ K^{un}, K^{tr} are (infinite) Galois extensions over K.

$$Gal(K^{un}/K) \simeq Gal(k^{sep}/k)$$

Lemma. $\pi_K \in K$ uniformizer $\Rightarrow$ $K^{tr} = K^{un} \cdot \bigcup_{(n,p)=1} K(\sqrt[n]{\pi_K})$ where $p = \text{char } k$, and ℓ if char $k = 0$

This implies $Gal(K^{tr}/K) \simeq Gal(k^{sep}/k) \ltimes \underbrace{\varprojlim_{(n,p)=1} \mu_n(k^{sep})}_{\simeq \prod_{\ell \neq p} \mathbb{Z}_\ell}$,

e.g. for $K = \mathbb{Q}_p$: $Gal(K^{tr}/K) \simeq \hat{\mathbb{Z}} \ltimes \prod_{\ell \neq p} \mathbb{Z}_\ell$

Pf: RHS $\subseteq K^{tr}$. ✓

Let L/K be at most tamely ram. subextension, $L_0 \subseteq L$ max. unramified.

$\Rightarrow e := [L : L_0]$ prime to char k. Wlog $\mu_e(K^{sep}) \subseteq L$.

$\pi_L^e = u \cdot \pi_K$ where $u \in \mathcal{O}_L^\times$

e prime to char k $\Rightarrow$ $L' = L(\sqrt[e]{u})$ unram over L, $\left(\sqrt[e]{u}^{-1} \pi_L\right)^e = \pi_K$.

Let $L_0' \subseteq L'$ max. unram in L'.

$L_0'(\sqrt[e]{\pi_K}) \subseteq L'(\pi) = L_0' \cdot L \subseteq L' \Longrightarrow L_0'(\sqrt[e]{\pi_K}) = L'$

$\uparrow$

$f(L_0'(\sqrt[e]{\pi_K})|K) = f(L'|K)$

$e(L_0'(\sqrt[e]{\pi_K})|K) = e(L'|K)$.

□

Galois extensions of complete discrete valuation fields

K discrete valuation field, $k = \mathcal{O}_K/\mathfrak{m}_K$

L/K Galois extension s.t. the residue extension k_L/k is separable.

$G := \mathrm{Gal}(L/K)$.

We know that there is a maximal unramified subextension $L_0/K \subseteq L/K$, L_0/K is Galois.

$$G \longrightarrow \mathrm{Gal}(L_0/K) \cong \mathrm{Gal}(k_L/k)$$

Def. Inertia subgroup $I := I_{L/K} = \ker(G \twoheadrightarrow \mathrm{Gal}(L_0/K))$.

$$\begin{array}{ccc} v_L : & L^\times & \longrightarrow \mathbb{Z} \\ & \cup & \\ & \pi_L & \longmapsto 1 \end{array}$$

a normalised additive valuation

From now on, $L_0 = K$, i.e. L/K is totally ramified.

$\forall n \in \mathbb{Z}_{\geq 1}$ define $G_n = \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq n+1\}$

Thus we get $G = G_0 \supseteq G_1 \supseteq \dots$

Rmk $G_n = \{\sigma \in G \mid \forall x \in \mathcal{O}_L \quad v_L(\sigma(x) - x) \geq n+1\}$. This condition is seemingly stronger, but in fact is equivalent: (and hence the def. of G_n is independent of the choice of π_L)

write $x = \sum_{i=0}^{+\infty} a_i \pi_L^i$, $a_i \in \mathcal{O}_K$

$$\Rightarrow \quad \sigma(x) - x = \sum_{i=0}^{+\infty} a_i \sigma(\pi_L)^i - \sum_{i=0}^{+\infty} a_i \pi_L^i$$

$$= \sum_{i=0}^{+\infty} a_i (\sigma(\pi_L)^i - \pi_L^i) \quad \Rightarrow \quad \sigma(\pi_L) - \pi_L \mid \sigma(x) - x \quad \forall x \in \mathcal{O}_L$$

$$v_L(\sigma(x) - x) \geq v_L(\sigma(\pi_L) - \pi_L) \geq n+1 \quad \text{if } \sigma \in G_n.$$

Recall. $U_K = \mathcal{O}_K^\times$.

Def. $U_L^n := \{x \in U_L \mid x \equiv 1 \pmod{\pi_L^n}\} = 1 + \pi_L^n \mathcal{O}_L \qquad \forall n \geq 1$

Then $U_L \supseteq U_L^1 \supseteq \dots \supseteq U_L^n \supseteq \dots$,

and we have $G_n = \left\{\sigma \in G \mid \frac{\sigma(\pi_L)}{\pi_L} \in U_L^n\right\} \quad \forall n \geq 1$

Easy to check: $G_n \trianglelefteq G$.

We get a map

$$\vartheta_n : G_n/G_{n+1} \longrightarrow U_L^n/U_L^{n+1}$$

$$\sigma \bmod G_{n+1} \longmapsto \frac{\sigma(\pi_L)}{\pi_L} \bmod U_L^{n+1}$$

In fact, this map is injective.

In particular, G_n/G_{n+1} is abelian.

Prop. (1) If $\mathrm{char}(k) = 0$ then $G_1 = \{1\}$, and G_0/G_1 is a cyclic finite group.

(2) If $\mathrm{char}(k) = p > 0$ then G_1 is a finite group of p power order, and G_0/G_1 is a finite cyclic group of order prime to p.

In particular, $G = G_0$ is solvable.

Pf: $$U_L^n/U_L^{n+1} \cong \begin{cases} k_L^\times & n = 0 \\ k_L & n \geq 1 \end{cases}$$

If $\mathrm{char}(k) = 0$ $\rightarrow$ k_L contains no finite subgroups $\Rightarrow$ $G_n/G_{n+1} = 1 \quad \forall n \geq 1$.

$\bigcap_{n \geq 1} G_n = \{1\}$ since this intersection has elements with the property

$v_L(\sigma(x) - x) \geq n \quad \forall n$, i.e. σ fixes every element of $\mathcal{O}_L$, hence $\sigma = 1$.

$\Rightarrow G_1 = \{1\}$.

$G_0 = G_0/G_1 \hookrightarrow k_L^\times$ Any finite subgroup of k_L consists of some roots of unity and is hence cyclic. ✓

finite gp.

If $\mathrm{char}(k) = p > 0$: $\vartheta_n(G_n/G_{n+1}) \subseteq k_L \quad \forall n \geq 1 \rightarrow G_n/G_{n+1} \cong \mathbb{F}_p^{d_n}$

$\rightarrow$ G has power p order.

$G_0/G_1 \hookrightarrow k^\times \qquad (k_L^\times)_{\mathrm{tors}} \cong \{\zeta \in k_L^\times \mid \zeta^m = 1 \text{ for some } m,\ p \nmid m\}$. □

Example $K = \mathbb{Q}_p$, $L = \mathbb{Q}_p(\zeta_{p^n})$, $n \geq 1$.

Then the minimal polynomial of $\zeta_{p^n} - 1$ over $\mathbb{Q}$ is

$$f(x) = \Phi_{p^n}(1+x) = \frac{(1+x)^{p^n} - 1}{(1+x)^{p^{n-1}} - 1} = \sum_{i=0}^{p-1} (1+x)^{p^{n-1} i} = x^{p^{n-1}(p-1)} + \underbrace{\ldots + p}_{p \mid}$$

$\rightarrow$ $f(x)$ is Eisenstein $/\mathbb{Q}_p$ $\overset{\text{NP}}{\Rightarrow}$ $f(x)$ is irreducible $/\mathbb{Q}_p$

$$e\left(\mathbb{Q}_p(\zeta_{p^n}) \mid \mathbb{Q}_p\right) = p^{n-1}(p-1)$$

$\eta_n = \zeta_{p^n} - 1$ is a uniformizer of $\mathbb{Q}_p(\zeta_{p^n}) = L$

$$v_L = e\, v_p = p^{n-1}(p-1)\, v_p.$$

$$G = \mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{p^n}) / \mathbb{Q}_p\right) \cong \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \xleftarrow{\sim} \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$$

$$\sigma_a \longleftarrow a$$

$$\sigma_a(\zeta_{p^n}) = \zeta_{p^n}^a$$

There is an obvious filtration on $G \cong \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$:

$$G^{(r)} = \left\{ \sigma_a \;\middle|\; a \in (1+p^r\mathbb{Z}) \mod p^n\mathbb{Z} \right\}$$

$$\cong \left(1+p^r\mathbb{Z}\right) \Big/ \left(1+p^n\mathbb{Z}\right) \qquad \forall\, 1 \le r \le n-1$$

$\forall \sigma_a \in G^{(r)} \setminus G^{(r+1)}$: $v_L\left(\sigma_a(\eta_n) - \eta_n\right) = v_L\left(\sigma_a(\zeta_{p^n}-1) - (\zeta_{p^n}-1)\right) =$

$a = 1+p^r b$, $b \in \mathbb{Z}\setminus p\mathbb{Z}$

$$= v_L\left(\zeta_{p^n}^a - \zeta_{p^n}\right) = v_L\left(\zeta_{p^n}\cdot\left(\zeta_{p^n}^{a-1}-1\right)\right) =$$

$$= v_L\left(\zeta_{p^n}^{p^r b} - 1\right) = v_L\left(\zeta_{p^{n-r}}^{b} - 1\right)$$

$\zeta_{p^{n-r}}^b = \left(\zeta_{p^n}\right)^{p^r b}$ is a primitive p^{n-r}-th root of unity.

$$v_p\left(\zeta_{p^{n-r}}^b - 1\right) = \frac{1}{e\left(\mathbb{Q}_p(\zeta_{p^{n-r}}) \mid \mathbb{Q}_p\right)} = \frac{1}{p^{n-r-1}\cdot(p-1)}$$

$$v_L\left(\zeta_{p^{n-r}}^b - 1\right) = p^{n-1}(p-1)\, v_p\left(\zeta_{p^{n-r}}^b - 1\right) = p^r \qquad \forall\, \sigma_{1+p^r b} \in G^{(r)} \setminus G^{(r+1)}$$

The ramification filtration on G is

$$G_u = \begin{cases} G & \text{if } u = 0 \\ G^{(r)} & \text{if } p^{r-1} \le u \le p^r - 1 \text{ for some } 1 \le r \le n-1 \\ \{1\} & \text{if } u \ge p^{n-1} \end{cases}$$

Global applications

Global: for number fields.

Local: arch. or non-arch complete valuation fields.

Classify the equivalence classes of norms on a number field.

$\mathbb{Q}$: $|\cdot|_\infty$, $|\cdot|_p$ $\forall$ rat. prime p. ⟶ we have already seen this.

Thm. (Ostrowski) (1) The norm $|\cdot|_p$ is not equivalent to $|\cdot|_q$ if $p,q \leq \infty$, $p \neq q$.

(2) Every nontrivial norm on $\mathbb{Q}$ is equivalent to one of the $|\cdot|_p$.

PF: (1) If one of the p,q is ∞, clearly $|\cdot|_p \not\sim |\cdot|_q$ since one is archimedean and the other is not.

If both p,q are finite, then the valuation ring for $|\cdot|_p$ is $\mathbb{Z}_{(p)}$, which differs from $\mathbb{Z}_{(q)}$ $\Rightarrow$ $|\cdot|_p \not\sim |\cdot|_q$.

(2) Let $|\cdot|$ be a non-trivial norm on $\mathbb{Q}$.

If $|\cdot|$ is non-archimedean: the valuation ring is

$$\mathcal{O}_{|\cdot|} = \{ a \in \mathbb{Q} \mid |a| \leq 1 \} \quad \text{with max. ideal} \quad \mathfrak{m}_{|\cdot|} = \{ a \in \mathbb{Q} \mid |a| < 1 \} \subseteq \mathcal{O}_{|\cdot|}$$

$$\mathbb{Z} \subseteq \mathcal{O}_{|\cdot|} \Rightarrow \mathbb{Z} \cap \mathfrak{m}_{|\cdot|} = (p) \Rightarrow \mathbb{Z}_{(p)} \subseteq \mathcal{O}_{|\cdot|}$$

But $\mathbb{Z}_{(p)}$ is integrally closed and $\mathcal{O}_{|\cdot|}$ has fraction field $\mathbb{Q}$.

$\Rightarrow \mathbb{Z}_{(p)} = \mathcal{O}_{|\cdot|} \Rightarrow |\cdot|$ has the same val. ring as $|\cdot|_p \Rightarrow |\cdot| \sim |\cdot|_p$.

If $|\cdot|$ is archimedean: NTS $\forall n \in \mathbb{Z}_{n>0}$: $|n| = n^c$.

$|\cdot|$ is unbounded on $\mathbb{Z}$ $\Rightarrow$ let $n_0 > 0$ be the smallest integer with $|n| > 1$, and let $c \in \mathbb{R}_{>0}$ be s.t. $|n_0| = n_0^c$.

$\forall n \in \mathbb{Z}$: write $n = a_0 + a_1 n_0 + \dots + a_s n_0^s$, $a_i \in \{0, 1, \dots, n_0 - 1\}$,

$$|n| \leq |a_0| + |a_1| \cdot n_0^c + \dots + |a_s| \cdot n_0^{cs}$$

$\forall |a_i| \leq 1$ by $n_0 \geq a_i$.

$$\Rightarrow |n| \leq 1 + n_0^c + \dots + n_0^{cs} = n_0^{cs} \cdot \left(1 + \frac{1}{n_0^c} + \dots + \frac{1}{n_0^{cs}}\right) <$$

$$< \underbrace{\left(\sum_{i=0}^{\infty} \frac{1}{n_0^{ci}}\right)}_{=: A} \cdot n_0^{cs}$$

Hence $\forall n \in \mathbb{Z}_{\geq 0}$: $|n| \leq A \cdot n^c$

$\Rightarrow$ $|n|^2 \leq A \cdot n^{2c}$

$\Rightarrow$ $|n| \leq \sqrt[2]{A} \cdot n^c$ $\Rightarrow$ $|n| \leq n^c$ $\lim_{s \to \infty}$

For $n_0^{s+1} > n \geq n_0^s$ we have:

$$|n| \geq |n_0|^{s+1} - |n_0^{s+1} - n|$$
$$\geq n_0^{c\cdot(s+1)} - (n_0^{s+1} - n)^c$$
$$(n_0^{s+1} - n)^c \leq (n_0^{s+1} - n_0^s)^c$$
$$= n_0^{c\cdot(s+1)} \cdot \left(1 - \frac{1}{n_0}\right)^c$$

$$\Rightarrow \quad |n| \geq n_0^{c(s+1)} - n_0^{c\cdot(s+1)} \left(1 - \frac{1}{n_0}\right)^s$$
$$= n_0^{c(s+1)} \underbrace{\left(1 - \left(1 - \frac{1}{n_0}\right)^s\right)}_{A' \text{ indep. of } n} \geq A' n^s$$

$\Rightarrow$ $|n^s| \geq A' \cdot n^{cs}$ $\Rightarrow$ $|n| \geq \sqrt[s]{A'} \cdot n^c$ $\Rightarrow$ $|n| \geq n^c$. $\Rightarrow |n| = n^c$. $\forall n \in \mathbb{Z}_{\geq 1}$ $\square$

Def. Let K be a number field. A place of K is an equivalence class of non-trivial norms on K.

Ostrowski's thm says that $\left\{\text{places of } \mathbb{Q}\right\} \longleftrightarrow \{p \in \mathbb{Z} \mid p \text{ prime}\} \cup \{\infty\}$

Let $K/\mathbb{Q}$ be an arbitrary number field, $n := [K:\mathbb{Q}] = r_1 + 2r_2$,

so we have $\sigma_i : K \hookrightarrow \mathbb{R}$ $\quad 1 \leq i \leq r_1$

$\sigma_{r_1+j}, \overline{\sigma}_{r_1+j} : K \hookrightarrow \mathbb{C}$ $\quad 1 \leq j \leq r_2$

embeddings into $\mathbb{R}$ resp. $\mathbb{C}$.

Def.
$\forall\ 1 \leq i \leq r_1 + r_2$ $\quad |\cdot|_{\sigma_i} : K \longrightarrow \mathbb{R}_{\geq 0}$
$x \longmapsto |\sigma_i(x)|_{\mathbb{C}}$

This defines $r_1 + r_2$ archimedean norms on K.

Def. $\forall \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ let $v_{\mathfrak{p}}(x) := (\text{exponent of } \mathfrak{p} \text{ in the prime decomposition of } x\mathcal{O}_K)$,

and $\forall x \in K^\times$ let $|x|_{\mathfrak{p}} := N_{K/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$.

Note that $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^{f(\mathfrak{p}|p)} = \#\left(\mathcal{O}_K/\mathfrak{p}\right)$; and $|\cdot|_{\mathfrak{p}}$ is non-archimedean.

Thm. (1) any two norms $|\cdot|_v$ for $v \in \{\sigma_i \mid 1 \le i \le r_1+r_2\} \cup \operatorname{Spec} \mathcal{O}_K$ are not equivalent.

(2) any non-trivial norm on K is equivalent to one of these $|\cdot|_\sigma$.

PF: (1) Obviously $|\cdot|_{\sigma_i} \not\sim |\cdot|_{\mathfrak{p}}$.

If $\mathfrak{p} \neq \mathfrak{q}$, then $|\cdot|_{\mathfrak{p}} \not\sim |\cdot|_{\mathfrak{q}}$.

It remains to show that $|\cdot|_{\sigma_i} \not\sim |\cdot|_{\sigma_j}$, $i \neq j$, $1 \le i,j \le r_1+r_2$.

Recall that we have an embedding

$$\lambda : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$
$$x \mapsto (\sigma_i(x), \sigma_{r_1+j}(x))$$

and $\lambda(\mathcal{O}_K)$ is a full lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

$\lambda(K)$ is dense in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Hence $\forall\, 1 \le i \le r_1+r_2$ $\exists x_i \in K$: $|\sigma_i(x_i)|_{\mathbb{C}} = |x_i|_{\sigma_i} < 1$,

$|x_i|_{\sigma_j} > 1$ $\quad \forall j \neq i$

So $(x_i^n)_{n \ge 1} \longrightarrow 0$ for $|\cdot|_{\sigma_i}$,

but $(x_i^n)_{n \ge 1}$ diverges for $|\cdot|_{\sigma_j}$ $\Rightarrow |\cdot|_{\sigma_i} \not\sim |\cdot|_{\sigma_j}$ since the induced topologies are different. ✓

(2) Suppose $|\cdot|$ is a non-trivial norm on K.

If $|\cdot|$ is non-archimedean: $\{x \in \mathcal{O}_K \mid |x| < 1\} =: \mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_K$.

$\to \mathcal{O}_{|\cdot|} := \{x \in K \mid |x| \le 1\} = \mathcal{O}_{K\mathfrak{p}}$

$\Rightarrow |\cdot| \sim |\cdot|_{\mathfrak{p}}$.

If $|\cdot|$ is archimedean: let $\hat{K}$ be the completion of K wrt $|\cdot|$.

$$\begin{array}{ccc} K & \hookrightarrow & \hat{K} \\ | & & | \\ \mathbb{Q} & \hookrightarrow & \mathbb{R} \end{array}$$

The restriction of $|\cdot|$ to $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ by Ostrowski's theorem (as this is the only eq. class of arch. norms on $\mathbb{Q}$.)

$\Rightarrow$ the closure of $\mathbb{Q}$ in $\hat{K}$ is exactly $\mathbb{R}$ (the completion of $\mathbb{Q}$ wrt. $|\cdot|$).

$\hat{K}/\mathbb{R}$ is a finite extension. This is because there is a surjection $K \otimes_{\mathbb{Q}} \mathbb{R} \twoheadrightarrow \hat{K}$ (this is a surjection since K is dense in $\hat{K}$ and $\mathbb{R}$ is complete), and $K/\mathbb{Q}$ is finite.

Hence $\hat{K} \cong \mathbb{C}$ or $\mathbb{R}$, i.e. $K \hookrightarrow \hat{K}$ must be one of the embeddings σ_i $(1 \le i \le r_1)$ or σ_{r_1+j} $(1 \le j \le r_2)$.

$\Rightarrow |\cdot| \sim |\cdot|_{\sigma_i}$ or $|\cdot|_{\sigma_{r_1+j}}$. □

Here the key was to apply the classification of norms on $\mathbb{Q}$ (i.e. Ostrowski's theorem).

21.12.2017

Recall: $\{\text{arch places of } K\} \longleftrightarrow \{\sigma : K \hookrightarrow \mathbb{C}\} / \text{complex conjugation}$

$\{\text{non-arch places of } K\} \longleftrightarrow \{\text{prime ideals of } \mathcal{O}_K\}$

Thm: Let $v_1, \dots, v_r$ be distinct places of K. Then the diagonal embedding $K \hookrightarrow \prod_{i=1}^{r} K_{v_i}$, where K_{v_i} is the completion wrt v_i, has dense image.

Rmk: The difficult thing here is that we can simultaneously approximate.

Rmk: If all v_i are archimedean, then this follows from the fact that $\lambda : \mathcal{O}_K \hookrightarrow K^{r_1} \times \mathbb{C}^{r_2}$ is a full lattice.

If all the v_i are non-archimedean, then the statement follows from the CRT: $\mathcal{O}_K \longrightarrow \prod_{i=1}^{r} \mathcal{O}_K/\mathfrak{p}_i^n$ $\quad \mathfrak{p}_i \neq \mathfrak{p}_j \ \forall n$

$$\mathcal{O}_K \longrightarrow \varprojlim_n \prod_i \mathcal{O}_K/\mathfrak{p}_i^n = \prod_i \varprojlim_n \mathcal{O}_K/\mathfrak{p}_i^n = \prod_i \underbrace{\mathcal{O}_{K_{v_i}}}_{\text{valuation ring}},$$ has dense img.

This is the same argument as the equivalence of the algebraic and topological completion of $\mathbb{Z}_p$.

PF OF THM: Several reduction steps.

STEP I. $K \subset K_{v_i}$ dense $\Rightarrow$ it suffices to show that

$\forall x_1, \dots, x_r \in K \quad \forall \varepsilon > 0 \quad \exists \xi \in K : \quad |\xi - x_i|_{v_i} < \varepsilon$.

Claim 1. $\forall i$ with $1 \le i \le r \quad \forall \delta > 0 \quad \exists \xi_i \in K$ s.t. $|\xi_i - 1|_{v_i} < \delta$, $|\xi_i|_{v_j} < \delta$ $\forall i \neq j$.

The Claim implies the Thm: take $\xi = \sum_{i=1}^{r} x_i \xi_i$.

$$|\xi - x_i|_{v_i} = \left| x_i(\xi_i - 1) + \sum_{j \neq i} x_j \xi_j \right|_{v_i} \le |x_i|_{v_i} |\xi_i - 1|_{v_i} + \sum_{i \neq j} |x_j|_{v_i} |\xi_j|_{v_i} <$$

$$< \delta \sum_{i=1}^{r} |x_j|_{v_i}$$

STEP II Reduce to the pf of

Claim 2. $\forall 1 \le i \le r \quad \exists \xi \in K$ s.t. $|\xi|_{v_i} > 1$ and $|\xi|_{v_j} < 1 \quad \forall i \neq j$

Claim 2 $\Rightarrow$ Claim 1:

$$\left| \underbrace{\frac{\xi^n}{1+\xi^n}}_{\frac{1}{1+\xi^n}} - 1 \right|_{v_i} \longrightarrow 0 \quad \text{as} \quad n \to \infty$$

$$\forall j \neq i : \quad \left| \frac{\xi^n}{1+\xi^n} \right|_{v_j} \longrightarrow 0 \quad \text{as} \quad n \to \infty$$

STEP III Pf of Claim 2

We proceed by induction on $r \ge 2$.

$r = 2$: this follows from $v_1 \not\sim v_2$.

Assume we have already found a $\xi \in K$ s.t. $|\xi|_{v_1} > 1$, $|\xi|_{v_i} < 1 \quad \forall 2 \le i \le r-1$.

Consider $|\xi|_{v_r}$. There are three cases:

- if $|\xi|_{v_r} < 1$, we are done.

- if $|\xi|_{v_r} = 1 \Rightarrow \exists\, \alpha \in K : |\alpha|_{v_1} > 1$ and $|\alpha|_{v_r} < 1$ by $v_1 \neq v_r$.

  Then $\xi^N \alpha$ satisfies the requirement if N is sufficiently large.

- if $|\xi|_{v_r} > 1$, let α be as above.

  Then $\frac{\xi^N}{1+\xi^N} \cdot \alpha$ satisfies the requirement for $N \gg 0$. □

Let L/K be a finite extension of number fields, w a place of L.

$K_v :=$ closure of K in L_w,

and K_v is hence the completion of K at some place v.

$$\begin{array}{ccc} L & \text{---} & L_w \\ | & & | \\ K & \text{---} & K_v \end{array}$$

Assume that w is a non-archimedean place, or equivalently, $\mathfrak{p}_w \subseteq \mathcal{O}_L$.

$\mathfrak{p}_v := \mathfrak{p}_w \cap \mathcal{O}_K$

$$\begin{array}{ccccccc} \mathfrak{p}_w & \subseteq & \mathcal{O}_L & \text{---} & L & \text{---} & L_w \supseteq \mathcal{O}_{L_w} \\ | & & | & & | & & | \\ \mathfrak{p}_v & \subseteq & \mathcal{O}_K & \text{---} & K & \text{---} & K_v \supseteq \mathcal{O}_{K_v} \\ & & e(\mathfrak{p}_w|\mathfrak{p}_v) & & \overset{?}{=} & & e(L_w|K_v) \\ & & f(\mathfrak{p}_w|\mathfrak{p}_v) & & & & f(L_w|K_v) \end{array}$$

$$\mathcal{O}_{K_v} = \varprojlim_n \mathcal{O}_K/\mathfrak{p}_v^n = \hat{\mathcal{O}}_{K,\mathfrak{p}_v}$$

$$\mathcal{O}_{L_w} = \varprojlim_n \mathcal{O}_L/\mathfrak{p}_w^n = \hat{\mathcal{O}}_{L,\mathfrak{p}_w}$$

For the ramification indices and inertia degrees above, we have equalities.

This is because:

$$k_w = \mathcal{O}_L/\mathfrak{p}_w = \hat{\mathcal{O}}_{L,\mathfrak{p}_w}/\mathfrak{p}_w\hat{\mathcal{O}}_{L,\mathfrak{p}_w} = \mathcal{O}_{L_w}/\mathfrak{m}_{L_w}$$

$$k_v = \mathcal{O}_K/\mathfrak{p}_v \cong \mathcal{O}_{K_v}/\mathfrak{m}_{K_v}$$

$$f(\mathfrak{p}_w|\mathfrak{p}_v) = [k_w : k_v] = f(L_w|K_v) \quad \checkmark$$

$$\mathfrak{p}_v\mathcal{O}_L = \prod_{w|v} \mathfrak{p}_w^{e(\mathfrak{p}_w|\mathfrak{p}_v)}$$

localisation: $\mathfrak{p}_v\mathcal{O}_{L,\mathfrak{p}_w} = (\mathfrak{p}_w\mathcal{O}_{L,\mathfrak{p}_w})^{e(\mathfrak{p}_w|\mathfrak{p}_v)}$

completion: $\mathfrak{p}_v\hat{\mathcal{O}}_{L,\mathfrak{p}_v} = (\mathfrak{p}_w\hat{\mathcal{O}}_{L,\mathfrak{p}_w})^{e(\mathfrak{p}_w|\mathfrak{p}_v)}$

$$\| \qquad\qquad \Rightarrow e(\mathfrak{p}_w|\mathfrak{p}_v) = e(L_w|K_v).$$

$$\mathfrak{m}_{K_v}\mathcal{O}_{L_w} = \mathfrak{m}_{L_w}^{e(\mathfrak{p}_w|\mathfrak{p}_v)}$$

Write $f(w|v)$ and $e(w|v)$ for these.

Thm. Given a place v of K we have a canonical isomorphism

$$L \underset{K}{\otimes} K_v \cong \prod_{w|v} L_w$$

Pf: Write $L = K[x]/(f(x))$ for some irreducible $f(x) \in K[x]$.

Suppose that $f(x) = \prod_{i=1}^{r} g_i(x)$ is the decomposition into prime factors in $K_v[x]$.

Since f has no multiple roots (separability in char 0), $\forall i \neq j$ $g_i(x)$ and $g_j(x)$ are copime.

$$L \underset{K}{\otimes} K_v = K[x]/(f(x)) \underset{K}{\otimes} K_v = K_v[x]/(f(x))$$

$$= K_v[x]/\left(\prod_i g_i(x)\right) = \prod_{i=1}^{r} K_v[x]/(g_i(x))$$

Put $L_i := K_v[x]/(g_i(x))$, this is a finite extension of K_v.

But $|\cdot|_v$ on K extends uniquely to L_i so L_i is a complete normed field.

$$L \hookrightarrow L \underset{K}{\otimes} K_v \xrightarrow{pr_i} L_i$$

$$x \longmapsto x \otimes 1$$

K is dense in K_v $\Rightarrow$ L is dense in $L \underset{K}{\otimes} K_v$

$\Rightarrow$ L is dense in L_i

$\Rightarrow$ L_i is the completion of L wrt some place w

$\Rightarrow$ $w | n$

$$L \underset{K}{\otimes} K_v \cong \prod_i L_i \hookrightarrow \prod_{w|v} L_w$$

To see that it is an iso, it suffices to show that $L \underset{K}{\otimes} K_v \longrightarrow L_w$ is a surjective map.

By the univ prop of the tensor product, $\exists\, L \underset{K}{\otimes} K_v \longrightarrow L_w$

L is dense in $L \underset{K}{\otimes} K_v$ (and also in L_w) and both $L \underset{K}{\otimes} K_v$ and L_w are complete wrt its canonical topology as a finite dimensional K_v-vector space,

so $L \underset{K}{\otimes} K_v \longrightarrow\!\!\!\!\rightarrow L_w$ is surjective, i.e. L_w is a quotient of $L \underset{K}{\otimes} K_v$ as a K_v-algebra. $\Rightarrow L_w \cong L_i$, hence the theorem. $\square$

Rmk. $[L:K] = \left[\underbrace{L \underset{K}{\otimes} K_v}_{\prod_{w|v} L_w} : K_v\right] = \sum_{w|v} [L_w : K_v] = \sum_{w|v} f(w|v) \cdot e(w|v)$,

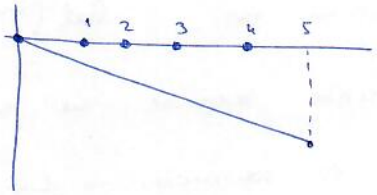
so we get a new proof of the fundamental equality $[L:K] = \sum_{w|v} f(w|v) \cdot e(w|v)$.

Cor. $\forall x \in L \quad Tr_{L/K}(x) = \sum_{w|v} Tr_{L_w/K_v}(x)$

$$N_{L/K}(x) = \prod_{w|v} N_{L_w/K_v}(x)$$

Pf: $Tr_{L/K}(x) = Tr_{L \underset{K}{\otimes} K_v / K_v}(x) = \sum_{w|v} Tr_{L_w/K_v}(x)$, same for the norm. □

Ex. $f(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \frac{x^5}{5}$



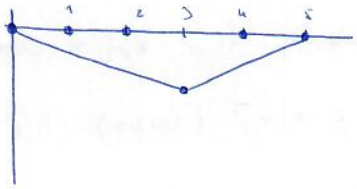
5-adic NP $(f(x))$

$\Rightarrow$ f is irreducible in $\mathbb{Q}_5[x]$

$\Rightarrow$ f is irreducible in $\mathbb{Q}[x]$

$L := \mathbb{Q}[x]/(f(x))$. Consider the prime decomposition of 3 in $\mathcal{O}_L$.

$$\left\{\begin{matrix}\text{primes of } L \\ w|3\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{direct factors} \\ \text{of } L \underset{K}{\otimes} K_v\end{matrix}\right\}$$



3-adic NP $(f(x))$

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

deg 3 with roots of 3-adic val $1/3$

deg 2 with roots of 3-adic valuation $-1/2$

$$L \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_3 = \mathbb{Q}_3[x]/(g(x)) \oplus \mathbb{Q}_3[x]/(h(x)) = L_{\mathfrak{p}_1} \oplus L_{\mathfrak{p}_2}$$

$\rightarrow$ $3\mathcal{O}_L = \mathfrak{p}_1^3 \mathfrak{p}_2^2$ since $L_{\mathfrak{p}_1}/\mathbb{Q}_3$ is totally ramified of deg 3,

$L_{\mathfrak{p}_2}/\mathbb{Q}_3$ is totally ramified of deg 2.

Comparison of local and global Galois groups

L/K finite Galois number field extension

$G := \mathrm{Gal}(L/K)$

w : place of L

v : place of K induced by w

$$\begin{array}{ccc} L & \hookrightarrow & L_w \\ | & & | \\ K & \hookrightarrow & K_v \end{array}$$

L_w/K_v is Galois

$L_w = K_v(x)$ with $x \in L$ because L_w is a quotient of $L \underset{K}{\otimes} K_v$

The embedding $L \hookrightarrow L_w$ induces a map

$i_w : \mathrm{Gal}(L_w/K_v) \longrightarrow G = \mathrm{Gal}(L/K)$

Prop. i_w induces an iso $\mathrm{Gal}\left(L_w/K_v\right) \xrightarrow{\sim} D_{w|v} = \left\{\sigma \in G \;\middle|\; \sigma(\mathfrak{p}_w) = \mathfrak{p}_w\right\}$

Pf: i_w is injective because the embedding $L \hookrightarrow L_w$ has dense img. and the Galois action is continuous in L_w.

Let $\mathfrak{m}_{L_w} \subseteq \mathcal{O}_{L_w}$ be the maximal ideal of the val ring of L_w.

$\mathrm{Gal}(L_w/K_v)$ stabilises $\mathfrak{m}_{L_w}$.

$\Rightarrow i_w(\mathrm{Gal}(L_w/K_v))$ stabilises $L \cap \mathfrak{m}_{L_w} = \{x \in L \mid |x|_w < 1\} = \mathfrak{p}_w \subset \mathcal{O}_L$

$\Rightarrow \mathrm{im}(i_w) \subseteq D_{w|v}$

Now $|\mathrm{Gal}(L_w/K_v)| = [L_w : K_v] = e(w|v) \cdot f(w|v)$

$|D_{w|v}| = e(w|v) \cdot f(w|v)$

$\Rightarrow i_w : \mathrm{Gal}(L_w/K_v) \xrightarrow{\sim} D_{w|v}$. □

Rmk. Actually, i_w induces an isomorphism $I(L_w|K_v) \xrightarrow{\sim} I = \left\{\sigma \in D_{w|v} \;\middle|\; \sigma(x) \equiv x \bmod \mathfrak{p}_w \quad \forall x \in \mathcal{O}_L\right\}$

Ex. $f(x) = x^5 - x - 1 \in \mathbb{Q}[x]$

$\bar{f}(x) \in \mathbb{F}_5[x]$ Artin–Schreier polynomial $\Rightarrow$ irreducible $\Rightarrow f(x) \in \mathbb{Q}[x]$ irreducible

$K := \mathbb{Q}[x]/(f(x))$ $\quad L :=$ Galois closure of $K/\mathbb{Q}$.

$G = \mathrm{Gal}(L/\mathbb{Q}) = ?$

$G \hookrightarrow S_5$ obviously

$5 \mid [L:\mathbb{Q}] = |G| \Rightarrow$ G contains an element of order 5 in S_5,

i.e. a 5-cycle $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$

$f(x) \bmod 2 \equiv (x^2+x+1)(x^3+x^2+1)$ in $\mathbb{F}_2[x]$

irreducible in $\mathbb{F}_2[x]$ since they have no roots and are of degree ≤ 3

Hensel's Lemma $\Rightarrow$ $f(x) = g(x) \cdot h(x)$ where $\deg g = 2$, $\deg h = 3$.

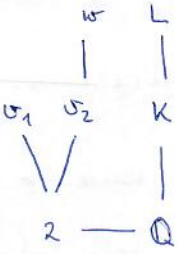
in $\mathbb{Q}_2[x] \supseteq \mathbb{Z}_2[x]$

g, h are irreducible in $\mathbb{Q}_2[x]$

$\Rightarrow$ There are 2 places above 2:

$f(v_1 \mid 2) = 2 \quad e(v_1 \mid 2) = 1$

$f(v_2 \mid 2) = 3 \quad e(v_2 \mid 2) = 1$



L_w = composition of K_{v_1} and K_{v_2} in $\overline{\mathbb{Q}_2}$

unramified of deg 6

K_{v_2}

unramified of degree 3

$\mathbb{Q}$

$\Rightarrow \mathrm{Gal}(L_w / K_v) \cong \mathbb{Z}/2\mathbb{Z} = \langle 1, \tau \rangle \hookrightarrow G \hookrightarrow S_5$

τ exchanges the two roots of $g(x)$ and stabilises all three roots of $h(x)$.

$\Rightarrow$ τ is a transposition

$\Rightarrow$ $G \subseteq S_5$ contains a 5-cycle and a transpose.

Lemma. $G \subseteq S_5$ is a subgroup containing a 5-cycle and a transpose $\Rightarrow G = S_5$. ∎

$\Rightarrow$ $G \tilde{=} S_5$.

So we have determined the global Galois group using local methods.

Product formula

K: number field

v: a place of K

$$|x|_v := \begin{cases} N(\mathfrak{p}_v)^{-v_{\mathfrak{p}_v}(x)} & \text{if } v \text{ is non-archimedean corresponding to } \mathfrak{p}_v \subseteq \mathcal{O}_K \\ |\sigma(x)|_{\mathbb{R}} & \text{if } v \text{ is induced by } \sigma : K \hookrightarrow \mathbb{R} \\ |\sigma(x)|_{\mathbb{C}}^2 & \text{if } v \text{ is induced by } \sigma : K \hookrightarrow \mathbb{C} \end{cases}$$

Warning: $|\sigma(x+y)|_{\mathbb{C}}^2 \leq |\sigma(x)|_{\mathbb{C}}^2 + |\sigma(y)|_{\mathbb{C}}^2$ does not hold!

Prop. $\forall x \in K^\times$: $\prod_v |x|_v = 1$.

Pf: Consider $K = \mathbb{Q}$. Need to check the formula for $x = \pm 1$ or p.

Both trivial $|p|_p \, |p|_\infty = 1$. ✓

General case. $\prod_v |x|_v = \prod_{p \leq \infty} \left(\prod_{v|p} |x|_v \right)$

Lemma. $\forall p \leq \infty \ \forall x \in K^\times$: $\left| N_{K/\mathbb{Q}}(x) \right|_p = \prod_{v|p} |x|_v$

Pf: $\left| N_{K/\mathbb{Q}}(x) \right|_p = \left| \prod_{v|p} N_{K_v/\mathbb{Q}_p}(x) \right|_p = \prod_{v|p} \left| N_{K_v/\mathbb{Q}_p}(x) \right|_p$

Need: $\left| N_{K_v/\mathbb{Q}_p}(x) \right|_p = |x|_v \quad \forall x \in K^\times$

Distinguish $p = \infty$ and $p < \infty$, verify the definition.