Part II — Number Fields

Theorems

Based on lectures by I. Grojnowski

Notes taken by Dexter Chua

Lent 2016

Part IB Groups, Rings and Modules is essential and Part II Galois Theory is desirable

Definition of algebraic number fields, their integers and units. Norms, bases and discriminants. [3]

Ideals, principal and prime ideals, unique factorisation. Norms of ideals. [3]

Minkowski's theorem on convex bodies. Statement of Dirichlet's unit theorem. Determination of units in quadratic fields. [2]

Ideal classes, finiteness of the class group. Calculation of class numbers using statement of the Minkowski bound. [3]

Dedekind's theorem on the factorisation of primes. Application to quadratic fields. [2]

Discussion of the cyclotomic field and the Fermat equation or some other topic chosen by the lecturer. [3]

Contents

0 Introduction

1 Number fields

Lemma. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, i.e. $\alpha \in \mathbb{Q}$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}$.

Theorem. $\mathcal{O}_L$ is a ring, i.e. if $\alpha, \beta \in \mathcal{O}_L$, then so is $\alpha \pm \beta$ and $\alpha\beta$.

Proposition.

(i) Let $R \subseteq S$ be rings. If $S = R[s]$ and s is integral over R, then S is finitely-generated over R.

(ii) If $S = R[s_1, \cdots, s_n]$ with s_i integral over R, then S is finitely-generated over R.

Theorem. If S is finitely-generated over R, then S is integral over R.

Corollary. Let $L \supseteq \mathbb{Q}$ be a number field. Then $\mathcal{O}_L$ is a ring.

Corollary. If $A \subseteq B \subseteq C$ be ring extensions such that B over A and C over B are integral extensions. Then C is integral over A.

Lemma. If $f \in K[x]$ with $f(\alpha) = 0$, then $p_\alpha \mid f$.

Proposition. Let L be a number field. Then $\alpha \in \mathcal{O}_L$ if and only if the minimal polynomial $p_\alpha(x) \in \mathbb{Q}[x]$ for the field extension $\mathbb{Q} \subseteq L$ is in fact in $\mathbb{Z}[x]$.

Lemma. We have

$$\operatorname{Frac} \mathcal{O}_L = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in \mathcal{O}_L, \beta \neq 0 \right\} = L.$$

In fact, for any $\alpha \in L$, there is some $n \in \mathbb{Z}$ such that $n\alpha \in \mathcal{O}_L$.

2 Norm, trace, discriminant, numbers

Proposition. For a field extension L/K and $a, b \in L$, we have $N(ab) = N(a)N(b)$ and $\mathrm{tr}(a+b) = \mathrm{tr}(a) + \mathrm{tr}(b)$.

Proposition. Let $p_\alpha \in K[x]$ be the minimal polynomial of α. Then the characteristic polynomial of m_α is

$$\det(xI - m_\alpha) = p_\alpha^{[L:K(\alpha)]}$$

Hence if $p_\alpha(x)$ splits in some field $L' \supseteq K(\alpha)$, say

$$p_\alpha(x) = (x - \alpha_1)\cdots(x - \alpha_r),$$

then

$$N_{K(\alpha)/K}(\alpha) = \prod \alpha_i, \quad \mathrm{tr}_{K(\alpha)/K}(\alpha) = \sum \alpha_i,$$

and hence

$$N_{L/K}(\alpha) = \left(\prod \alpha_i\right)^{[L:K(\alpha)]}, \quad \mathrm{tr}_{L/K} = [L : K(\alpha)]\left(\sum \alpha_i\right).$$

Corollary. Let $L \supseteq \mathbb{Q}$ be a number field. Then the following are equivalent:

(i) $\alpha \in \mathcal{O}_L$.

(ii) The minimal polynomial p_α is in $\mathbb{Z}[x]$

(iii) The characteristic polynomial of m_α is in $\mathbb{Z}[x]$.

This in particular implies $N_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and $\mathrm{tr}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Lemma. Let $L = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is not $0, 1$ and is square-free. Then

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2 \text{ or } 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{d})\right] & d \equiv 1 \pmod 4 \end{cases}$$

Theorem (Primitive element theorem)**.** Let $K \subseteq L$ be a separable field extension. Then there exists an $\alpha \in L$ such that $K(\alpha) = L$.

Lemma. The degree $[L : \mathbb{Q}] = n$ of a number field is the number of field embeddings $L \hookrightarrow \mathbb{C}$.

Corollary. Let $L/\mathbb{Q}$ be a number field. If $\sigma_1, \cdots, \sigma_n : L \to \mathbb{C}$ are the different field embeddings and $\beta \in L$, then

$$\mathrm{tr}_{L/\mathbb{Q}}(\beta) = \sum \sigma_i(\beta), \quad N_{L/\mathbb{Q}}(\beta) = \prod_i \sigma_i(\beta).$$

We call $\sigma_1(\beta), \cdots, \sigma_n(\beta)$ the *conjugates* of β in $\mathbb{C}$.

Lemma. Let $x \in \mathcal{O}_L$. Then x is a unit if and only if $N_{L/\mathbb{Q}}(x) = \pm 1$.

Corollary. If $x \in \mathcal{O}_L$ is such that $N(x)$ is prime, then x is irreducible.

Proposition. Let L/K be a separable extension. Then a K-bilinear form $L \times L \to K$ defined by $(x, y) \mapsto \mathrm{tr}_{L/K}(xy)$ is non-degenerate. Equivalent, if $\alpha_1, \cdots, \alpha_n$ are a K-basis for L, the Gram matrix $(\mathrm{tr}(\alpha_i\alpha_j))_{i,j=1,\cdots,n}$ has non-zero determinant.

Theorem. Let $\mathbb{Q}/L$ be a number field. Then there exists an integral basis for $\mathcal{O}_L$. In particular, $\mathcal{O}_L \cong \mathbb{Z}^n$ with $n = [L : \mathbb{Q}]$.

3 Multiplicative structure of ideals

Proposition. Let $L/\mathbb{Q}$ be a number field, and $\mathcal{O}_L$ be its ring of integers. Then $\mathcal{O}_L$ is a Dedekind domain.

Lemma. Let $\mathfrak{a} \lhd \mathcal{O}_L$ be a non-zero ideal. Then $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$ and $\mathcal{O}_L/\mathfrak{a}$ is finite.

Lemma. Let $\mathfrak{p}$ be a prime ideal in a ring R. Then for $\mathfrak{a}, \mathfrak{b} \lhd R$ ideals, then $\mathfrak{ab} \subseteq \mathfrak{p}$ implies $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.

Lemma. Let $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$ a non-zero ideal. Then there is a subset of $\mathfrak{a}$ that is a product of prime ideals.

Proposition.

(i) Let $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$ be an ideal. If $x \in L$ has $x\mathfrak{a} \subseteq \mathfrak{a}$, then $x \in \mathcal{O}_L$.

(ii) Let $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$ be a *proper* ideal. Then

$$\{y \in L : y\mathfrak{a} \leq \mathcal{O}_L\}$$

contains elements that are not in $\mathcal{O}_L$. In other words,

$$\frac{\{y \in L : y\mathfrak{a} \leq \mathcal{O}_L\}}{\mathcal{O}_L} \neq 0.$$

Lemma. An $\mathcal{O}_L$ module $\mathfrak{q} \subseteq L$ is a fractional ideal if and only if there is some $c \in L^\times$ such that $c\mathfrak{q}$ is an ideal in $\mathcal{O}_L$. Moreover, we can pick c such that $c \in \mathbb{Z}$.

Corollary. Let $\mathfrak{q}$ be a fractional ideal. Then as an abelian group, $\mathfrak{q} \cong \mathbb{Z}^n$, where $n = [L : \mathbb{Q}]$.

Corollary. Let $\mathfrak{a} \leq \mathcal{O}_L$ be a proper ideal. Then $\{x \in L : x\mathfrak{a} \leq \mathcal{O}_L\}$ is a fractional ideal.

Proposition. Every non-zero fractional ideal is invertible. The inverse of $\mathfrak{q}$ is

$$\{x \in L : x\mathfrak{q} \subseteq \mathcal{O}_L\}.$$

Corollary. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \lhd \mathcal{O}_L$ be ideals, $\mathfrak{c} \neq 0$. Then

(i) $\mathfrak{b} \subseteq \mathfrak{a}$ if and only if $\mathfrak{bc} \subseteq \mathfrak{ac}$

(ii) $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{ac} \mid \mathfrak{bc}$

(iii) $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$.

Theorem. Let $\mathfrak{a} \lhd \mathcal{O}_L$ be an ideal, $\mathfrak{a} \neq 0$. Then $\mathfrak{a}$ can be written uniquely as a product of prime ideals.

Corollary. The non-zero fractional ideals form a group under multiplication. We denote this I_L. This is a free abelian group generated by the prime ideals, i.e. any fractional ideal $\mathfrak{q}$ can be written uniquely as $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{q_r}$, with $\mathfrak{p}_i$ distinct prime ideals and $a_i \in \mathbb{Z}$.

Moreover, if $\mathfrak{q}$ is an integral ideal, i.e. $\mathfrak{q} \lhd \mathcal{O}_L$, then $a_i, \cdots, a_r \geq 0$.

Theorem. The following are equivalent:

(i) $\mathcal{O}_L$ is a principal ideal domain

(ii) $\mathcal{O}_L$ is a unique factorization domain

(iii) cl_L is trivial.

4 Norms of ideals

Proposition. For any ideal $\mathfrak{a}$, we have $N(\mathfrak{a}) \in \mathfrak{a} \cap \mathbb{Z}$.

Proposition. Let $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_L$ be ideals. Then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

Proposition. Let $\mathfrak{a} \lhd \mathcal{O}_L$ be an ideal, $n = [L : \mathbb{Q}]$. Then

(i) There exists $\alpha_1, \cdots, \alpha_n \in \mathfrak{a}$ such that

$$\mathfrak{a} = \left\{\sum r_i\alpha_i : r_i \in \mathbb{Z}\right\} = \bigoplus_1^n \alpha_i\mathbb{Z},$$

and $\alpha_1, \cdots, \alpha_n$ are a basis of L over $\mathbb{Q}$. In particular, $\mathfrak{a}$ is a free $\mathbb{Z}$-module of n generators.

(ii) For any such $\alpha_1, \cdots, \alpha_n$,

$$\Delta(\alpha_1, \cdots, \alpha_n) = N(\mathfrak{a})^2 D_L.$$

Lemma. Let M be a $\mathbb{Z}$-module (i.e. abelian group), and suppose $M \leq \mathbb{Z}^n$. Then $M \cong \mathbb{Z}^r$ for some $0 \leq r \leq n$.

Moreover, if $r = n$, then we can choose a basis $v_1, \cdots, v_n$ of M such that the change of basis matrix $A = (a_{ij}) \in M_{n\times n}(\mathbb{Z})$ is upper triangular, where

$$v_j = \sum a_{ij}e_i,$$

where $e_1, \cdots, e_n$ is the standard basis of $\mathbb{Z}^n$.

In particular,

$$|\mathbb{Z}^n/M| = |a_{11}a_{12}\cdots a_{nn}| = |\det A|.$$

Corollary. Suppose $\mathfrak{a} \lhd \mathcal{O}_L$ has basis $\alpha_1, \cdots, \alpha_n$, and $\Delta(\alpha_1, \cdots, \alpha_n)$ is square-free. Then $\mathfrak{a} = \mathcal{O}_L$ (and D_L is square-free).

Lemma. If $\alpha \in \mathcal{O}_L$, then

$$N(\langle\alpha\rangle) = |N_{L/\mathbb{Q}}(\alpha)|.$$

5 Structure of prime ideals

Lemma. Let $\mathfrak{p} \lhd \mathcal{O}_L$ be a prime ideal. Then there exists a unique $p \in \mathbb{Z}$, p prime, with $\mathfrak{p} \mid \langle p \rangle$. Moreover, $N(\mathfrak{p}) = p^f$ for some $1 \leq f \leq n$.

Theorem (Dedekind's criterion)**.** Let $\alpha \in \mathcal{O}_L$ and $g(x) \in \mathbb{Z}[x]$ be its minimal polynomial. Suppose $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$ has finite index, coprime to p (i.e. $p \nmid |\mathcal{O}_L/\mathbb{Z}[\alpha]|$). We write

$$\bar{g}(x) = g(x) \pmod{p},$$

so $\bar{g}(x) \in \mathbb{F}_p[x]$. We factor

$$\bar{g}(x) = \varphi_1^{e_1} \cdots \varphi_m^{e_m}$$

into distinct irreducibles in $\mathbb{F}_p[x]$. We define the ideal

$$\mathfrak{p}_i = \langle p, \tilde{\varphi}_i(\alpha) \rangle \lhd \mathcal{O}_L,$$

generated by p and $\tilde{\varphi}_i$, where $\tilde{\varphi}_i$ is any polynomial in $\mathbb{Z}[x]$ such that $\tilde{\varphi}_i \bmod p = \varphi_i$. Notice that if $\tilde{\varphi}'$ is another such polynomial, then $p \mid (\tilde{\varphi}_i - \varphi_i)$, so $\langle p, \tilde{\varphi}'(\alpha) \rangle = \langle p, \tilde{\varphi}(\alpha) \rangle$.

Then the $\mathfrak{p}_i$ are prime, and

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}.$$

Moreover, $f_i = \deg \varphi_i$, so $N(\mathfrak{a}) = p^{\deg \varphi_i}$.

Lemma. In $L = \mathbb{Q}(\sqrt{d})$,

(i) 2 splits in L if and only if $d \equiv 1 \pmod 8$;

(ii) 2 is inert in L if and only if $d \equiv 5 \pmod 8$;

(iii) 2 ramifies in L if $d \equiv 2, 3 \pmod 4$.

Corollary. If p is prime and $p < n = [L : \mathbb{Q}]$, and $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$ has finite index coprime to p, then p does *not* split completely in $\mathcal{O}_L$.

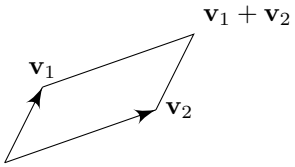
Theorem. $p \mid D_L$ if and only if p ramifies in $\mathcal{O}_L$.

6 Minkowski bound and finiteness of class group

Lemma (Minskowski's lemma)**.** Let $\Lambda = \mathbb{Z}\mathbf{v}_1 + \mathbb{Z}\mathbf{v}_2 \subseteq \mathbb{R}^2$ be a lattice, with $\mathbf{v}_1, \mathbf{v}_2$ linearly independent in $\mathbb{R}$ (i.e. $\mathbb{R}\mathbf{v}_1 + \mathbb{R}\mathbf{v}_2 = \mathbb{R}^2$). We write $\mathbf{v}_i = a_i\mathbf{e}_1 + b_i\mathbf{e}_2$. Then let

$$A(\Lambda) = \text{area of fundamental parallelogram} = \left|\det \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}\right|,$$

where the fundamental parallelogram is the following:



Then a closed disc S around 0 contains a non-zero point of Λ if

$$\text{area}(S) \geq 4A(\Lambda).$$

In particular, there exists an $\alpha \in \Lambda$ with $\alpha \neq 0$, such that

$$0 < |\alpha|^2 \leq \frac{4A(\Lambda)}{\pi}.$$

Proposition.

(i) If $\alpha = a + b\sqrt{\lambda}$, then as a complex number,

$$|\alpha|^2 = (a + b\sqrt{\lambda})(a - b\sqrt{\lambda}) = N(\alpha).$$

(ii) For $\mathcal{O}_L$, we have

$$A(\mathcal{O}_L) = \frac{1}{2}\sqrt{|D_L|}.$$

(iii) In general, we have

$$A(\mathfrak{a}) = \frac{1}{2}\sqrt{|\Delta(\alpha_1, \alpha_2)|},$$

where α_1, α_2 are the integral basis of $\mathfrak{a}$.

(iv) We have

$$A(\mathfrak{a}) = N(\mathfrak{a})A(\mathcal{O}_L).$$

Proposition (Minkowski bound)**.** For all $[\mathfrak{a}] \in \text{cl}_L$, there is a representative $\mathfrak{b}$ of $[\mathfrak{a}]$ (i.e. an ideal $\mathfrak{b} \leq \mathcal{O}_L$ such that $[\mathfrak{b}] = [\mathfrak{a}]$) such that

$$N(\mathfrak{b}) \leq c_L = \frac{2\sqrt{|D_L|}}{\pi}.$$

Lemma. For every $n \in \mathbb{Z}$, there are only finitely many ideals $\mathfrak{a} \leq \mathcal{O}_L$ with $N(\mathfrak{a}) = m$.

Theorem. The class group cl_L is a finite group, and the divisors of ideals of the form $\langle p \rangle$ for $p \in \mathbb{Z}$, p a prime, and $0 < p < c_L$, collectively generate cl_L.

Theorem. Let $L = \mathbb{Q}(\sqrt{d})$ with $d < 0$. Then $\mathcal{O}_L$ is a UFD if

$$-d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Moreover, this is actually an "if and only if".

Proposition. Suppose $\Lambda \subseteq \mathbb{R}^n$ is a subgroup. Then Λ is a discrete subgroup of $(\mathbb{R}^n, +)$ if and only if

$$\Lambda = \left\{ \sum_1^m n_i \mathbf{x}_i : n_i \in \mathbb{Z} \right\}$$

for some $\mathbf{x}_1, \cdots, \mathbf{x}_m$ linearly independent over $\mathbb{R}$.

Theorem (Minkowski's theorem)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice, and P be a fundamental domain. We let $S \subseteq \mathbb{R}^n$ be a measurable set, i.e. one for which $\mathrm{vol}(S)$ is defined.

(i) Suppose $\mathrm{vol}(S) > \mathrm{covol}(\Lambda)$. Then there exists distinct $\mathbf{x}, \mathbf{y} \in S$ such that $\mathbf{x} - \mathbf{y} \in \Lambda$.

(ii) Suppose $\mathbf{0} \in S$, and S is symmetric around 0, i.e. $\mathbf{s} \in S$ if and only if $-\mathbf{s} \in S$, and S is convex, i.e. for all $\mathbf{x}, \mathbf{y} \in S$ and $\lambda \in [0, 1]$, then

$$\lambda \mathbf{x} + (1 - \lambda)\mathbf{y} \in S.$$

Then suppose either

(a) $\mathrm{vol}(S) > 2^n \,\mathrm{covol}(\Lambda)$; or

(b) $\mathrm{vol}(S) \geq 2^n \,\mathrm{covol}(\Lambda)$ and S is closed.

Then S contains a $\gamma \in \Lambda$ with $\gamma \neq 0$.

Lemma.

(i) $\sigma(\mathcal{O}_L)$ is a lattice in $\mathbb{R}^n$ of covolume $2^{-s}|D_L|^{\frac{1}{2}}$.

(ii) More generally, if $\mathfrak{a} \lhd \mathcal{O}_L$ is an ideal, then $\sigma(\mathfrak{a})$ is a lattice and the covolume

$$\mathrm{covol}(\sigma(\mathfrak{a})) = 2^{-s}|D_L|^{\frac{1}{2}} N(\mathfrak{a}).$$

Proposition. Let $\mathfrak{a} \lhd \mathcal{O}_L$ be an ideal. Then there exists an $\alpha \in \mathfrak{a}$ with $\alpha \neq 0$ such that

$$|N(\alpha)| \leq c_L N(\mathfrak{a}),$$

where

$$c_L = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |D_L|^{\frac{1}{2}}.$$

Corollary. Every $[\mathfrak{a}] \in \mathrm{cl}_L$ has a representative $\mathfrak{a} \in \mathcal{O}_L$ with $N(\mathfrak{a}) \leq c_L$.

Theorem (Dirichlet)**.** The class group cl_L is finite, and is generated by prime ideals of norm $\leq c_L$.

7 Dirichlet's unit theorem

Theorem (Dirichlet unit theorem)**.** We have the isomorphism

$$\mathcal{O}_L^\times \cong \mu_L \times \mathbb{Z}^{r+s-1},$$

where

$$\mu_L = \{\alpha \in L : \alpha^N = 1 \text{ for some } N > 0\}$$

is the group of roots of unity in L, and is a finite cyclic group.

Theorem (Pell's equation)**.** There are infinitely many $x + y\sqrt{d} \in \mathcal{O}_L$ such that $x^2 - dy^2 = \pm 1$.

Theorem (Dirchlet's unit theorem for real quadratic fields)**.** Let $L = \mathbb{Q}(\sqrt{d})$. Then there is some $\varepsilon_0 \in \mathcal{O}_L^\times$ such that

$$\mathcal{O}_L^\times = \{\pm\varepsilon_0^n : n \in \mathbb{Z}\}.$$

We call such an ε_0 a *fundamental unit* (which is not unique). So

$$\mathcal{O}_L^\times \cong \{\pm 1\} \times \mathbb{Z}.$$

Theorem (Dirichlet unit theorem)**.** We have the isomorphism

$$\mathcal{O}_L^\times \cong \mu_L \times \mathbb{Z}^{r+s-1},$$

where

$$\mu_L = \{\alpha \in L : \alpha^N = 1 \text{ for some } N > 0\}$$

is the group of roots of unity in L, and is a finite cyclic group.

Lemma.

(i) If $d = -1$, then $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \mathbb{Z}/4\mathbb{Z}$.

(ii) If $d = -3$, then let $\omega = \frac{1}{2}(1 + \sqrt{d})$, and we have $\omega^6 = 1$. So $\mathbb{Z}[\omega]^\times = \{1, \omega, \cdots, \omega^5\} \cong \mathbb{Z}/6\mathbb{Z}$.

(iii) For any other $d < 0$, we have $\mathcal{O}_L^\times = \{\pm 1\}$.

8 L-functions, Dirichlet series*

Theorem (Euclid)**.** There are infinitely many primes.

Theorem (Dirichlet's theorem)**.** Let $a, q \in \mathbb{Z}$ be coprime. Then there exists infinitely many primes in the sequence

$$a, a+q, a+2q, \cdots,$$

i.e. there are infinitely many primes in any such arithmetic progression.

Proposition.

(i) The Riemann zeta function $\zeta(s)$ converges for $\mathrm{Re}(s) > 1$.

(ii) The function
$$\zeta(s) - \frac{1}{s-1}$$
extends to a holomorphic function when $\mathrm{Re}(s) > 0$.

In other words, $\zeta(s)$ extends to a meromorphic function on $\mathrm{Re}(s) > 0$ with a simple pole at 1 with residue 1.

(iii) We have the expression
$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$$
for $\mathrm{Re}(s) > 1$, and the product is absolutely convergent. This is the *Euler product*.

Lemma. If there is a real number $r \in \mathbb{R}$ such that
$$a_1 + \cdots + a_N = O(N^r),$$
then
$$\sum a_n n^{-s}$$
converges for $\mathrm{Re}(s) > r$, and is a holomorphic function there.

Theorem.

(i) $\zeta_L(s)$ converges to a holomorphic function if $\mathrm{Re}(s) > 1$.

(ii) *Analytic class number formula*: $\zeta_L(s)$ is a meromorphic function if $\mathrm{Re}(s) > 1 - \frac{1}{n}$ and has a simple pole at $s = 1$ with residue
$$\frac{|\operatorname{cl}_L| 2^r (2\pi)^s R_L}{|D_L|^{1/2} |\mu_L|},$$
where cl_L is the class group, r and s are the number of real and complex embeddings, you know what π is, R_L is the regulator, D_L is the discriminant and μ_L is the roots of unity in L.

(iii)
$$\zeta_L(s) = \prod_{\mathfrak{p} \lhd \mathcal{O}_L \text{ prime ideal}} (1 - N(\mathfrak{p})^{-s})^{-1}.$$
This is again known as the *Euler product*.

Proposition. χ_D, as defined for $L = \mathbb{Q}(\sqrt{d})$ is a Dirichlet character of modulus D.

Lemma. Let χ be any non-trivial Dirichlet character. Then $L(\chi, s)$ is holomorphic for $\text{Re}(s) > 0$.

Corollary. For quadratic characters χ_D, we have
$$L(\chi_D, 1) \neq 0.$$

Proposition.

(i) We have $[L : \mathbb{Q}] = \varphi(q)$, where
$$\varphi(q) = |(\mathbb{Z}/q\mathbb{Z})^\times|.$$

(ii) $L \supseteq \mathbb{Q}$ is a Galois extension, with
$$\text{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^\times,$$
where if $r \in (\mathbb{Z}/q\mathbb{Z})^\times$, then r acts on $\mathbb{Q}(w_Q)$ by sending $\omega_q \mapsto \omega_q^r$. This is what plays the role of quadratic reciprocity for cyclotomic fields.

(iii) The ring of integers is
$$\mathcal{O}_L = \mathbb{Z}[\omega_q] = \mathbb{Z}[x]/\Phi_q(x),$$
where
$$\Phi_q(x) = \frac{x^q - 1}{\prod_{d|q, d\neq q} \Phi_d(x)}$$
is the qth cyclotomic polynomial.

(iv) Let p be a prime. Then p ramifies in $\mathcal{O}_L$ if and only if $p \mid D_L$, if and only if $p \mid q$. So while D might be messy, the prime factors of D are the prime factors of q.

(v) Let p be a prime and $p \nmid q$. Then $\langle p \rangle$ factors as a product of $\varphi(q)/f$ distinct prime ideals, each of norm p^f, where f is the order of p in $(\mathbb{Z}/q\mathbb{Z})^\times$.

Proposition. We have
$$\zeta_{\mathbb{Q}(\omega_q)}(s) = \prod_{i=1}^{\varphi(q)} L(\chi_i, s) \cdot (\text{corr. factor}) = \zeta_{\mathbb{Q}}(s) \prod_{i=2}^{\varphi(q)} L(\chi_i, s) \cdot (\text{corr. factor})$$
where the correction factor is a finite product coming from the primes that divide q.

Corollary. If χ is any non-trivial Dirichlet character, then $L(\chi, 1) \neq 0$.

Theorem (Dirichlet, 1839)**.** Let $a, q \in \mathbb{N}$ be coprime, i.e. $\gcd(a, q) = 1$. Then there are infinitely many primes in the arithmetic progression
$$a, a + q, a + 2q, a + 3q, \cdots .$$