Part II — Number Fields

Definitions

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

Definition (Field extension)**.** A *field extension* is an inclusion of fields $K \subseteq L$. We sometimes write this as L/K.

Definition (Degree of field extension)**.** Let $K \subseteq L$ be fields. Then L is a vector space over K, and the *degree* of the field extension is

$$[L : K] = \dim_K(L).$$

Definition (Finite extension)**.** A *finite field extension* is a field extension with finite degree.

Definition (Number field)**.** A *number field* is a finite field extension over $\mathbb{Q}$.

Definition (Algebraic integer)**.** Let L be a number field. An *algebraic integer* is an $\alpha \in L$ such that there is some monic $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$. We write $\mathcal{O}_L$ for the set of algebraic integers in L.

Definition (Integrality)**.** Let $R \subseteq S$ be rings. We say $\alpha \in S$ is *integral over* R if there is some monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$.

We say S is *integral over* R if all $\alpha \in S$ are integral over R.

Definition (Finitely-generated)**.** We say S is *finitely-generated* over R if there exists elements $\alpha_1, \cdots, \alpha_n \in S$ such that the function $R^n \to S$ defined by $(r_1, \cdots, r_n) \mapsto \sum r_i \alpha_i$ is surjective, i.e. every element of S can be written as a R-linear combination of elements $\alpha_1, \cdots, \alpha_n$. In other words, S is finitely-generated as an R-module.

Notation. If $\alpha_1, \cdots, \alpha_r \in S$, we write $R[\alpha_1, \cdots, \alpha_r]$ for the subring of S generated by $R, \alpha_1, \cdots, \alpha_r$. In other words, it is the image of the homomorphism from the polynomial ring $R[x_1, \cdots, x_n] \to S$ given by $x_i \mapsto \alpha_i$.

2 Norm, trace, discriminant, numbers

Definition (Norm and trace)**.** Let L/K be a field extension, and $\alpha \in L$. We write $m_\alpha : L \to L$ for the map $\ell \mapsto \alpha\ell$. Viewing this as a linear map of L vector spaces, we define the *norm* of α to be

$$N_{L/K}(\alpha) = \det m_\alpha,$$

and the *trace* to be

$$\mathrm{tr}_{L/K}(\alpha) = \mathrm{tr}\, m_\alpha.$$

Notation. Write $\mathcal{O}_L^\times = \{x \in \mathcal{O}_L : x^{-1} \in \mathcal{O}_L\}$, the units in $\mathcal{O}_L$.

Definition (r and s)**.** We write r for the number of field embeddings $L \hookrightarrow \mathbb{R}$, and s the number of pairs of non-real field embeddings $L \hookrightarrow \mathbb{C}$. Then

$$n = r + 2s.$$

Alternatively, r is the number of real roots of p_α, and s is the number of pairs of complex conjugate roots.

Notation.

$$\Delta(\alpha_1, \cdots, \alpha_n) = \det(\mathrm{tr}_{L/K}(\alpha_i\alpha_j)).$$

Definition (Integral basis)**.** Let $L/\mathbb{Q}$ be a number field. Then a basis $\alpha_1, \cdots, \alpha_n$ of L is an *integral basis* if

$$\mathcal{O}_L = \left\{\sum_{i=1}^n m_i\alpha_i : m_i \in \mathbb{Z}\right\} = \bigoplus_1^n \mathbb{Z}\alpha_i.$$

In other words, it is simultaneously a basis for L over $\mathbb{Q}$ and $\mathcal{O}_L$ over $\mathbb{Z}$.

Definition (Discriminant)**.** The *discriminant* D_L of a number field L is defined as

$$D_L = \Delta(\alpha_1, \cdots, \alpha_n)$$

for any integral basis $\alpha_1, \cdots, \alpha_n$.

3 Multiplicative structure of ideals

Definition (Ideal multiplication)**.** Let $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_L$ be ideals. Then we define the product $\mathfrak{ab}$ as

$$\mathfrak{ab} = \left\{ \sum_{i,j} \alpha_i \beta_j : \alpha_i \in \mathfrak{a}, \beta_j \in \mathfrak{b} \right\}.$$

We write $\mathfrak{a} \mid \mathfrak{b}$ if there is some ideal $\mathfrak{c}$ such that $\mathfrak{ac} = \mathfrak{b}$, and say $\mathfrak{a}$ *divides* $\mathfrak{b}$.

Definition (Prime ideal)**.** Let R be a ring. An ideal $\mathfrak{p} \subseteq R$ is *prime* if $R/\mathfrak{p}$ is an integral domain. Alternatively, for all $x, y \in R$, $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

In this course, we take the convention that a prime ideal is *non-zero*. This is not standard, but it saves us from saying "non-zero" all the time.

Definition (Dedekind domain)**.** A ring R is a *Dedekind domain* if

(i) R is an integral domain.

(ii) R is a Noetherian ring.

(iii) R is integrally closed in $\operatorname{Frac} R$, i.e. if $x \in \operatorname{Frac} R$ is integral over R, then $x \in R$.

(iv) Every proper prime ideal is maximal.

Definition (Fractional ideal)**.** A *fractional ideal* of $\mathcal{O}_L$ is a subset of L that is also an $\mathcal{O}_L$ module and is finitely generated.

Definition (Integral/honest ideal)**.** If we want to emphasize that $\mathfrak{a} \lhd \mathcal{O}_L$ is an ideal, we say it is an *integral or honest ideal*. But we never use "ideal" to mean fractional ideal.

Definition (Invertible fractional ideal)**.** A fractional ideal $\mathfrak{q}$ is *invertible* if there exists a fractional ideal $\mathfrak{r}$ such that $\mathfrak{qr} = \mathcal{O}_L = \langle 1 \rangle$.

Definition (Class group)**.** . The *class group* or *ideal class group* of a number field L is

$$\mathrm{cl}_L = I_L / P_L,$$

where I_L is the group of fractional ideals, and P_L is the subgroup of principal fractional ideals.

4 Norms of ideals

Definition (Norm of ideal)**.** Let $\mathfrak{a} \lhd \mathcal{O}_L$ be an ideal. We define

$$|N(\mathfrak{a})| = |\mathcal{O}_L/\mathfrak{a}| \in \mathbb{N}.$$

5 Structure of prime ideals

Definition (Ramification indices)**.** Let $\langle p\rangle = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}$ be the factorization into prime ideals. Then $e_1, \cdots, e_m$ are the *ramification indices*.

Definition (Ramified prime)**.** We say p is *ramified* if some $e_i > 1$.

Definition (Inert prime)**.** We say p is *inert* if $m = 1$ and $e_m = 1$, i.e. $\langle p\rangle$ remains prime.

Definition (Splitting prime)**.** We say p *splits completely* if $e_1 = \cdots = e_m = 1 = f_1 = \cdots = f_m$. So $m = n$.

6 Minkowski bound and finiteness of class group

Definition (Discrete subset)**.** A subset $X \subseteq \mathbb{R}^n$ is *discrete* if for every $x \in X$, there is some $\varepsilon > 0$ such that $B_\varepsilon(x) \cap X = \{x\}$. This is true if and only if for every compact $K \subseteq \mathbb{R}^n$, $K \cap X$ is finite.

Definition (Lattice)**.** If $\operatorname{rank} \Lambda = n = \dim \mathbb{R}^n$, then Λ is a *lattice* in $\mathbb{R}^n$.

Definition (Covolume and fundamental domain)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice, and $\mathbf{x}_1, \cdots, \mathbf{x}_n$ be a basis of Λ, then let

$$P = \left\{ \sum_{i=1}^n \lambda_i \mathbf{x}_i : \lambda_i \in [0,1] \right\},$$

and define the *covolume* of Λ to be

$$\operatorname{covol}(\Lambda) = \operatorname{vol}(P) = |\det A|,$$

where A is the matrix such that $\mathbf{x}_i = \sum a_{ij} \mathbf{e}_j$.

We say P is a *fundamental domain* for the action of Λ on $\mathbb{R}^n$, i.e.

$$\mathbb{R}^n = \bigcup_{\gamma \in \Lambda} (\gamma + P),$$

and

$$(\gamma + P) \cap (\mu + P) \subseteq \partial(\gamma + P).$$

In particular, the intersection has zero volume.

7 Dirichlet's unit theorem

Definition (Regulator)**.** The *regulator* of a number field L is

$$R_L = \operatorname{covol}(\ell(\mathcal{O}_L^\times) \subseteq \mathbb{R}^{r+s-1}).$$

8 L-functions, Dirichlet series*

Definition (Riemann zeta function)**.** The *Riemann zeta function* is defined as

$$\zeta(s) = \sum_{n \geq 1} n^{-s}$$

for $s \in \mathbb{C}$.

Definition (Dirichlet series)**.** A *Dirichlet series* is a series of the form $\sum a_n n^{-s}$, where $a_1, a_2, \cdots \in \mathbb{C}$.

Definition (Zeta function)**.** Let $L \supseteq \mathbb{Q}$ be a number field, and $[L : \mathbb{Q}] = n$. We define the *zeta function of* L by

$$\zeta_L(s) = \sum_{\mathfrak{a} \lhd \mathcal{O}_L} N(\mathfrak{a})^{-s}.$$

Definition (L-function)**.** We define the *L-function* by

$$L(\chi, s) = \prod_{p \text{ prime}} (1 - \chi(p) p^{-s})^{-1}.$$

Definition (Dirichlet character)**.** A function $\chi : \mathbb{Z} \to \mathbb{C}$ is a *Dirichlet character of modulus D* if there exists a group homomorphism

$$w : \left(\frac{\mathbb{Z}}{D\mathbb{Z}}\right)^{\times} \to \mathbb{C}^{\times}$$

such that

$$\chi(m) = \begin{cases} w(m \bmod D) & \gcd(m, D) = 1 \\ 0 & \text{otherwise} \end{cases}.$$

We say χ is *non-trivial* if ω is non-trivial.