Cheatsheet: Algebraic Number Theory I

Thursday 9th May, 2019

Let K be a **number field**, that is, K is a finite algebraic extension of $\mathbb{Q}$; $n = [K : \mathbb{Q}]$ is the **degree** of K. Equivalently, $K \cong \mathbb{Q}(x)/(f(x))$ for some monic irreducible polynomial $f \in \mathbb{Q}[x]$ of degree n. If $f(\alpha) = 0$, we write $K = \mathbb{Q}(\alpha)$. As a vector space, $\mathbb{Q}(\alpha)$ is isomorphic to $\{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\}$. If $\alpha_1, \ldots, \alpha_n$ are the roots of f, we define **embeddings**

$$\tau_i : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}, \qquad \alpha \mapsto \alpha_i, \qquad (i = 1, \ldots, n).$$

For any $z \in K$, its **trace** and **norm** are defined respectively as

$$Tr_{K/\mathbb{Q}}(z) = \sum_{i=1}^{n} \tau_i(z) \qquad \text{and} \qquad N_{K/\mathbb{Q}}(z) = \prod_{i=1}^{n} \tau_i(z)\,.$$

A **ring of integers** of K is the set

$$\mathcal{O}_K = \{z \in K : f(z) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}.$$

We denote the units of $\mathcal{O}_K$ (i.e., the invertible elements) by $\mathcal{O}_K^\times$. We have the equivalence

$$z \in \mathcal{O}_K^\times \qquad \Longleftrightarrow \qquad N_{K/\mathbb{Q}}(z) = \pm 1\,.$$

Let $\{v_1, \ldots, v_n\}$ be any $\mathbb{Q}$-basis for K (e.g. $\{1, \alpha, \ldots, \alpha^{n-1}\}$). We define

$$\mathrm{disc}(v_1, \ldots, v_n) := \det([\tau_i(v_j)]_{i,j})^2 = \det([Tr_{K/\mathbb{Q}}(v_i v_j)]_{i,j})$$

Any non-zero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ has an integral basis: $\mathfrak{a} = \mathbb{Z}a_1 \oplus \ldots \oplus \mathbb{Z}a_n$ for some $a_1, \ldots, a_n \in \mathfrak{a}$. We define the **discriminant of an ideal** $\mathfrak{a}$ as $\mathrm{disc}(\mathfrak{a}) := \mathrm{disc}(a_1, \ldots, a_n)$. In particular, if $\{w_1, \ldots, w_n\}$ constitutes an integral basis of $\mathcal{O}_K$, we set

$$\mathrm{disc}(K) := \mathrm{disc}(\mathcal{O}_K) := \mathrm{disc}(w_1, \ldots, w_n)\,.$$

We then have

$$\mathrm{disc}(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})^2 \mathrm{disc}(K) = (\mathcal{O}_K : \mathfrak{a})^2 \mathrm{disc}(K)$$

for any non-zero ideal $\mathfrak{a}$. The number $\mathfrak{N}(\mathfrak{a}) := \#(\mathcal{O}_K/\mathfrak{a})$ is the **absolute norm** of an ideal $(0) \neq \mathfrak{a} \lhd \mathcal{O}_K$.

An ideal $\mathfrak{p} \lhd \mathcal{O}_K$ is a **prime ideal** if

$$\mathfrak{p} \neq \{0\}, \mathcal{O}_K \qquad \text{and} \qquad (ab \in \mathfrak{p} \;\Rightarrow\; a \in \mathfrak{p} \text{ or } b \in \mathfrak{p})\,,$$

or equivalently (as an ideal of $\mathcal{O}_K$) $\mathfrak{p}$ is maximal among the proper ideals of $\mathcal{O}_K$.

The ideals of $\mathcal{O}_K$ do not form a group (no inverses), but fractional ideals do. A **fractional ideal** of K is a finitely generated $\mathcal{O}_K$-submodule of K not equal to $\{0\}$, i.e.,

$$\mathfrak{f} = (a_1, \ldots, a_m)\mathcal{O}_K := a_1\mathcal{O}_K + \ldots + a_m\mathcal{O}_K \qquad \text{for some } \; a_1, \ldots, a_m \in K\backslash\{0\},\; m \in \mathbb{N}\,.$$

Its inverse (with respect to $\mathfrak{fg} = \{\sum_{i=1}^{k} a_i b_i : a_i \in \mathfrak{f}, b_i \in \mathfrak{g}, k \in \mathbb{N}\}$, with the identity element $\mathcal{O}_K$) is

$$\mathfrak{f}^{-1} = \{x \in K : x\mathfrak{f} \subseteq \mathcal{O}_K\}\,.$$

Every fractional ideal $\mathfrak{f}$ may be written uniquely as $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$ where the product is taken over all prime ideals of $\mathcal{O}_K$ and $\nu_\mathfrak{p} \in \mathbb{Z}$ with $\nu_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$.

The fractional ideal

$$\mathfrak{d}^{-1} := \{x \in K : Tr_{K/\mathbb{Q}}(x\mathcal{O}_K) \subseteq \mathbb{Z}\}$$

defines the **inverse different** of $K/\mathbb{Q}$.

Two fractional ideals $\mathfrak{f}, \mathfrak{g}$ are equivalent if there exists $0 \neq a \in K$ such that $\mathfrak{g} = (a)\mathfrak{f}$, i.e. $\mathfrak{f}$ and $\mathfrak{g}$ are equal up to multiplication by **principal fractional ideals**; the equivalence classes are called **ideal classes**, the set Cl_K of ideal classes is the **ideal class group** of K, and $h_K = \#\mathrm{Cl}_K$ is the **class number** of K. Cl_K is a finite abelian group.