More on unique factorization in rings of integers

HW1 due Thursday 10/15: please submit via CoCalc. (If you have trouble, PM me on Zulip.)
See Zulip/Homework Q&A for clarifications.

Supplementary problem solving sessions: see Zulip/General announcements.

Discriminant of an integral basis

$K = \#$ field $\alpha_1 \dots \alpha_n \in K$ basis of K as $\mathbb{Q}$-vec. space

discriminant $d(\alpha_1 \dots \alpha_n) = \det \big(\overbrace{\sigma_j \alpha_i}^{A}\big)_{ij}^2 \in \mathbb{Q}$ invariant under $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$

$\sigma_1 \dots \sigma_n : K \hookrightarrow \overline{\mathbb{Q}}$

Equivalently, $d(\alpha \dots \alpha_n) = \det \left(Trace_{K/\mathbb{Q}}(\alpha_i \alpha_j)\right)_{ij}$

b/c $Trace_{L/K}(\alpha_i \alpha_j) = \sum_k (\sigma_k \alpha_i)(\sigma_k \alpha_j)$

$= (A^T A)_{ij}$

Comparison of integral bases and their discriminants

Note: if $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, then $d(\alpha_1 \dots \alpha_n) \in \mathbb{Z}$.

Observation: If $\mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n \subseteq \mathbb{Z}\beta_1 + \dots + \mathbb{Z}\beta_n$

then $d(\alpha_1 \dots \alpha_n) = d(\beta_1 \dots \beta_n)\, c^2$

$$c = [\mathbb{Z}\beta_1 + \dots + \mathbb{Z}\beta_n : \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n]$$

Corollary: Any prime factor of $[\mathcal{O}_K : \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n]$ if $\alpha_1 \dots \alpha_n \in \mathcal{O}_K$ appears at least twice in prime factorization of $d(\alpha_1 \dots \alpha_n)$.

Statement of unique factorization for Dedekind domains

A Dedekind domain is an integral domain which is

- noetherian and
- integrally closed in its fraction field
- such that every nonzero prime ideal is maximal.

Example: $\mathcal{O}_K$ where $K = \#$ field

Lemma from last time

R = Dedekind domain

Theorem Every nonzero ideal of R can be written as a product of prime ideals uniquely up to order.

Lemma For $I \subset R$ nonzero ideal, $\exists$ nonzero primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ s.t. $I \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$

The "multiplicative inverse" of a prime ideal

R = Dedekind domain

Lemma: Let $\mathfrak{p} \subset R$ be a nonzero prime ideal.

Define $\mathfrak{p}^{-1} = \{x \in \mathrm{Frac}(R) : x\mathfrak{p} \subseteq R\}$.

Then for any nonzero ideal I of R

$$I\mathfrak{p}^{-1} = \langle \sum_i a_i x_i : a_i \in I, x_i \in \mathfrak{p}^{-1} \rangle \neq I.$$

In particular, $\boxed{\mathfrak{p}^{-1} \neq R}$.

Pf: Prove this first. Pick $a \in \mathfrak{p}$, $a \neq 0$. Apply previous lemma

$\mathfrak{p} \supseteq (a) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $= \mathfrak{p}$, $b \in$

get $a^{-1} b \in \mathfrak{p}^{-1}$.

The "multiplicative inverse" of a prime ideal (contd.)

Suppose $I\mathfrak{p}^{-1} = I$ $\quad \alpha_1 \ldots \alpha_n$ generators of I

For $x \in \mathfrak{p}^{-1}$: $\quad x\alpha_i = \sum a_{ij}\alpha_j \quad a_{ij} \in R$.

Cayley-Hamilton

$$\Rightarrow \det(xI_n - (a_{ij})) = 0$$

R integrally closed

$$\Rightarrow x \in R \Rightarrow \mathfrak{p}^{-1} = R \supsetneq$$

Existence of prime factorizations

Suppose existence fails. Since R is noetherian, can find a maximal counterexample I.

Pick a maximal ideal $\mathfrak{p} \supseteq I$.

By previous lemma, $I \subsetneq \underbrace{I\mathfrak{p}^{-1}}_{=\mathfrak{p}_1 \cdots \mathfrak{p}_r} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$

Then $I = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r$

$= I\mathfrak{p}^{-1}\mathfrak{p}$

Uniqueness of prime factorizations

Say $\mathcal{I} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$

where $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are nonzero primes.

Since $\mathfrak{p}_1$ is prime, $\mathfrak{p}_1 \subseteq \mathfrak{q}_j$ for some j

$=$ b/c both maximal

$$\mathfrak{p}_1^{-1}\mathcal{I} = \mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \cancel{\mathfrak{q}_j} \cdots \mathfrak{q}_s$$

Continue until one side is exhausted.

Fractional ideals

$K = \#$ field

A <u>fractional ideal</u> of K is a <u>nonzero</u> finitely generated $\mathcal{O}_K$-submodule of K.

(an ideal of $\mathcal{O}_K$ as <u>integral</u> ideals)

<u>Prop</u> The fractional ideals form an abelian group under multiplication, with identity $(1) = \mathcal{O}_K$, and $I^{-1} = \{x \in K : xI \subseteq \mathcal{O}_K\}$.

& unique factorization into primes.

The ideal class group of a number field

$J_K = \{$ fractional ideals $\}$

$P_K = \{$ principal fractional ideals $\}$

class group $\quad \mathcal{C}l_K = J_K / P_K$

A fundamental exact sequence

$$
\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^* \arrow[r] \arrow[rr, bend left, "\text{zero}"] & K^\times \arrow[r] \arrow[rr, bend right, "\text{zero}"'] & J_K \arrow[r] & Cl_K \arrow[r] & 1.
\end{tikzcd}
$$

$$\alpha \longrightarrow (\alpha)$$