Extension of Dedekind domains

Reminder: most of the US goes off Daylight Saving Time this weekend.
In particular, all times for this class will shift from UTC-7 to UTC-8.

Reminder: voting in the US election concludes Tuesday, November 3 (and in the AMS election Sunday, November 1).

Integral closures in a separable field extension

$\mathcal{O}_K$ = Dedekind domain, K = Frac $\mathcal{O}_K$ (e.g. $\mathbb{Z}$, $\mathbb{Q}$)

can be removed

L/K finite separable field extension, (e.g. L = # field

$\mathcal{O}_L$ = integral closure of $\mathcal{O}_K$ in L $\mathcal{O}_L = \overline{\mathbb{Z}} \cap L$)

Prop $\mathcal{O}_L$ is also a Dedekind domain.

Pf need to show:

- $\mathcal{O}_L$ is an integral domain ✓
- $\mathcal{O}_L$ is noetherian trace pairing $L \times L \to K$ is nondegenerate $\Rightarrow \mathcal{O}_L \leq$ f.g. $\mathcal{O}_K$-module
- $\mathcal{O}_L$ integrally closed in K ✓
- every nonzero prime is maximal

$\mathfrak{P} \subseteq \mathcal{O}_L$ nonzero prime, $\mathfrak{P} \cap \mathcal{O}_K$ nonzero prime $\Rightarrow$ maximal

$\mathcal{O}_L/(\mathfrak{P})$ finite algebra over $\mathcal{O}_K/\mathcal{O}_K \cap \mathfrak{P}$ field
integral

Extension of a prime ideal

L/K finite separable field extension
$\mathcal{O}_K$ = Dedekind domain, $\operatorname{Frac}\mathcal{O}_K = K$
$\mathcal{O}_L$ = integral closure of $\mathcal{O}_K$ in L

$\mathfrak{p} \subseteq \mathcal{O}_K$ nonzero prime

Note: $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$

(e.g. $\pi \in \mathfrak{p} - \mathfrak{p}^2$, so $\pi\mathcal{O}_K = \mathfrak{p}\mathfrak{a}$, $\mathfrak{p} \nmid \mathfrak{a}$, so $\mathfrak{p} + \mathfrak{a} = \mathcal{O}_K$

$b + s = 1$

$s \notin \mathfrak{p}$

$s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi\mathcal{O}_K$

if $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$, then $s\mathcal{O}_L = s\mathfrak{p}\mathcal{O}_L \subseteq \pi\mathcal{O}_L$ so $s = \pi x$ for $x \in \mathcal{O}_L \cap K = \mathcal{O}_K$ $\Rightarrow$ ↯

$\Rightarrow$ $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_r^{e_r}$ prime factorization $(r > 0)$

The $\mathfrak{q}_i$ are precisely those nonzero prime ideals $\mathfrak{q}$ of $\mathcal{O}_L$ for which $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$

Ramification

$$\mathfrak{p} O_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

e_i = *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$

$\mathfrak{q}_i$ is *ramified* if $e_i > 1$.

Examples

$\mathcal{O}_K = \mathbb{Z}$, $K = \mathbb{Q}$

- $L = \mathbb{Q}(i)$ $\mathcal{O}_L = \mathbb{Z}[i]$

$$\underset{(p)}{p}\,\mathcal{O}_L = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{if } p \equiv 1 \mod 4 \quad \mathfrak{p}_1 \neq \mathfrak{p}_2 \\ p\,\mathcal{O}_L & \text{if } p \equiv 3 \mod 4 \\ (1+i)^2 & p = 2 \end{cases}$$

e.g. $5\mathcal{O}_L = (2+i)(2-i)$ $\quad \frac{2+i}{2-i} = \frac{(2+i)^2}{5} = \frac{3}{5} + \frac{4}{5}i \notin \mathbb{Z}[i]$

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

similarly for $L = \mathbb{Q}(\zeta_3)$ get ramification above $p = 3$

$L = \mathbb{Q}(\zeta_p)$ - ramification only above p.

$\mathbb{Q}(\zeta_n)$ - ramification only above $p \mid n$ ($n \not\equiv 0, 1 \mod 4$)

$L = \mathbb{Q}[x]/(x^3 - x - 1)$ ramification above 23.

$L = \mathbb{Q}(\zeta_p)$ $\quad (1 - \zeta_p)^{p-1} \sim p$

$p \neq 2$

Inertia degree

$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ $\mathfrak{p}$ $\mathcal{O}_K$ prime

$f_i := [\underbrace{\mathcal{O}_L/\mathfrak{q}_i}_{\text{residue field of } \mathfrak{q}_i} : \mathcal{O}_K/\mathfrak{p}]$

e.g. $K = \mathbb{Q}(i)$

$\mathfrak{p} = (p)$ $\begin{cases} p \equiv 1 \bmod 4, \text{ two factors with } e_i = 1, f_i = 1 \\ p \equiv 3 \bmod 4, \text{ one factor with } e = 1, f = 2 \end{cases}$

$\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}/(5)$

$\mathbb{Z}[i]/(3) \not\cong \mathbb{Z}/(3)$

$p = 2$, one factor with $e = 2$, $f = 1$

$\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}/(2)$

The fundamental identity

L/K separable

$$p\mathcal{O}_L = q_1^{e_1} \cdots q_r^{e_r} \implies \sum_{i=1}^{r} e_i f_i = n = [L:K]$$

- Pf [for $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, can see this by computing norms

$$\mathrm{Norm}(p\mathcal{O}_L) = p^n \qquad \mathrm{Norm}(q_i) = p^{f_i}$$

]

Chinese remainder theorem: want to count dimensions of both sides as $(\mathcal{O}_K/p)$-vector spaces

$$\boxed{\underbrace{\mathcal{O}_L/_{p}\mathcal{O}_L}_{\overset{?}{=}n} \cong \bigoplus_{i=1}^{r} \underbrace{\mathcal{O}_L/q_i^{e_i}}_{\overset{?}{=}e_i f_i}}$$

Proof of the fundamental identity

why is $\dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n$?

need to show: if $\alpha_1, \ldots \alpha_m \in \mathcal{O}_L$ s.t.
$\bar{\alpha}_1, \ldots \bar{\alpha}_m \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ form a basis over $\mathcal{O}_K/\mathfrak{p}$,
then $\alpha_1 \ldots \alpha_m$ form a basis for L/K.

why is $\dim(\mathcal{O}_K/\mathfrak{p})\ \mathcal{O}_L/\mathfrak{q}_i^{e_i} = e_i f_i$?

For $e_i = 1$ true by definition; otherwise
pick $\pi \in \mathfrak{q}_i - \mathfrak{q}_i^2$ show that $1, \pi, \ldots \pi^{e_i - 1}$ form a basis of $\mathcal{O}_L/\mathfrak{q}_i^{e_i}$ over $\mathcal{O}_K/\mathfrak{p}$

Examples revisited

A criterion for computing ramification/inertia degrees

Say $\alpha \in \mathcal{O}_L$ s.t. $L = K(\alpha)$

$g(x) \in \mathcal{O}_K[x]$ minimal polynomial.

For $\mathfrak{p} \subset \mathcal{O}_K$ not dividing conductor of $\mathcal{O}_K(\alpha)$ in $\mathcal{O}_L$

(i.e. $\{\beta \in \mathcal{O}_K : \beta\, \mathcal{O}_L \subseteq \mathcal{O}_K(\alpha)\}$)

can factor $\mathfrak{p}\mathcal{O}_L$ by factoring

$\bar{g}(x) \in \mathcal{O}_K/(\mathfrak{p})[x]$ $\qquad$ $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$

$= \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}$ $\qquad$ $e_i = e_i$

$f_i = \deg(\bar{g}_i)$

(e.g. for $\mathbb{Z}[i]$, $x^2+1 \bmod p$)

Ramification and discriminants