Feedback:

- Many among those giving feedback consider the course to be very difficult.
- During class I got the impression that, unlike me, most consider the material to be rather easy.
- There is a gap between registered students and students attending the course.
- I want to anonymously collect the info about students attending class. Please mark your answer. Then place the paper face-down in front of you. I will collect it and shuffle it before looking at it, doing my best to give you anonimity.

Recall

- We have shown the following:

$$\begin{tikzcd} \text{Dedekind} \arrow[r] & A \arrow[r, hook] \arrow[d, hook] & B = \mathcal{O}_K(A) \arrow[d, hook] \\ & Q \arrow[r, hook] & K \end{tikzcd}$$

$Q = \mathrm{Frac}(A)$, $Q \hookrightarrow K$ finite separable

$\Rightarrow$ 1) B is Dedekind, A-f.t., contains Q-basis of K

2) if A is a PID, then $B \cong A^{[K:Q]}$.

- We have also seen the following:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook, dashed] \arrow[d, hook] \arrow[dr, hook, dashed] & \mathcal{O}_K \arrow[d, hook] \\ \mathbb{Q} \arrow[r, hook] & K \end{tikzcd}$$

$\mathcal{O}_K$ = unique maximal order in K, i.e., $\mathcal{O}_K$ unital subring s.t. $\mathcal{O}_K \cong \mathbb{Z}^{[K:\mathbb{Q}]}$

$\mathbb{Q} \hookrightarrow K$ finite extension

Theorem

$$\mathcal{O}_K = \mathcal{O}_K(\mathbb{Z})$$

Proof: exercise.

Relative Theory

Let $A \hookrightarrow Q \hookrightarrow K$ a finite sep. extension of the field of fractions of the Dedekind ring A.

Let $B = \mathcal{O}_K$. We obtain maps

$$\{\mathfrak{b} \lhd B\} \longrightarrow \{\mathfrak{a} \lhd A\}, \quad \mathfrak{b} \longmapsto \mathfrak{b} \cap A \qquad \text{"contraction"}$$

$$\{\mathfrak{a} \lhd A\} \longrightarrow \{\mathfrak{b} \lhd B\}, \quad \mathfrak{a} \longmapsto B.\mathfrak{a} = (\mathfrak{a}) \qquad \text{"extension"}$$

Lemma (proven last time — warm-up).

Let $\mathfrak{P} \lhd B$ prime. Then $A \cap \mathfrak{P} \lhd A$ is prime.

Proof:

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[d, dashed] \arrow[dr, hook, dashed, "\overline{\pi}"] & B \arrow[d, "\pi"] \\
A/_{\ker \overline{\pi}} \arrow[r, hook, dashed] & B/_{\mathfrak{P}}
\end{tikzcd}$$

$$\ker \overline{\pi} = \{a \in A : \pi(a) = 0\} = A \cap \mathfrak{P}$$

$\Rightarrow A \cap \mathfrak{P}$ is an ideal and $A/_{A \cap \mathfrak{P}}$ is isomorphic to a subring of $B/_{\mathfrak{P}}$.

The latter is a domain, hence so is every subring. ∎

Proposition:

The contraction is a surjective map between non-zero prime ideals.
Given $\mathfrak{p} \in \mathrm{Spec}(A)^*$, the fiber is exactly

$$\mathrm{Spec}_{\mathfrak{p}}(B) := \{\mathfrak{P} \in \mathrm{Spec}(B)^* : v_{\mathfrak{P}}(B.\mathfrak{p}) > 0\}.$$

primes lying above $\mathfrak{p}$, short: $\mathfrak{P} | \mathfrak{p}$

finite!

Lemma

Let $\mathfrak{p} \in \mathrm{Spec}(A)$. Then $B.\mathfrak{p}$ is proper.

Proof: If $\mathfrak{p} = \{0\}$, there is nothing to show ($1 \neq 0$ in B). So suppose $\mathfrak{p} \neq \{0\}$.

Outline: If A was a PID, we could argue as follows. Let $\mathfrak{p} = A.p$ and suppose $B = B.p$. Since $A \subseteq B$, it follows that $1 = b.p$ for some $b \in B$. Moreover,

$$b = \frac{1}{p} \in \mathbb{Q} \cap B = A \Rightarrow 1 \in A.p = \mathfrak{p} \ \lightning$$

The argument to follow takes into account non-principality and instead of proving $1 \in \mathfrak{p}$, we ~~obtain~~ will use $B = B.\mathfrak{p}$ to show that $a \in \mathfrak{p}$ for some $a \in A - \mathfrak{p}$ $\lightning$

Since A is Dedekind, $\mathfrak{p} \neq \mathfrak{p}^2$ (unique factorization into prime ideals). Let

$$z \in \mathfrak{p} - \mathfrak{p}^2 \quad \Rightarrow z \neq 0.$$

Once more using prime factorization in A, there is $\mathfrak{a} \triangleleft A$ s.t. $A.z = \mathfrak{p}\mathfrak{a}$. Then $\mathfrak{a} \not\subseteq \mathfrak{p}$, since otherwise $A.z \subseteq \mathfrak{p}^2$ $\lightning$ So $\mathfrak{a}, \mathfrak{p}$ are coprime, i.e., $\mathfrak{a} + \mathfrak{p} = A$.

[Remark/exercise: $\mathfrak{a}, \mathfrak{b} \triangleleft A$ are coprime iff $\mathfrak{a}, \mathfrak{b}$ don't share prime divisors.]

$\Rightarrow \exists a \in \mathfrak{a}$ s.t. $a \equiv 1 \mod \mathfrak{p}$. Suppose $B.\mathfrak{p} = B$, then $B.a = B.\mathfrak{p}a \subseteq B.(A.z) = B.z$.

$\Rightarrow \exists b \in B$ s.t. $a = b.z$. Now $b = \frac{a}{z} \in B \cap \mathbb{Q} = A \Rightarrow a \in A.z \subseteq \mathfrak{p}$ $\lightning$

$\blacksquare$

Corollary:

Let $\mathfrak{p} \in \mathrm{Spec}(A)^{\times}$, then $\mathfrak{p} = B.\mathfrak{p} \cap A$.

Pf: $B.\mathfrak{p}$ is proper $\Rightarrow$ $B.\mathfrak{p} \cap A \subseteq A$ is proper, containing $\mathfrak{p}$.

$1 \notin B.\mathfrak{p}$

Proof of the proposition:

Let $\mathfrak{p} \in \mathrm{Spec}(A)^{\times}$, $\mathfrak{P} \in \mathrm{Spec}(B)$. Then

$$\mathfrak{p} = \mathfrak{P} \cap A \Leftrightarrow \mathfrak{p} \subseteq \mathfrak{P} \cap A \Leftrightarrow \mathfrak{p} \subseteq \mathfrak{P} \Leftrightarrow B.\mathfrak{p} \subseteq \mathfrak{P} \Leftrightarrow v_{\mathfrak{P}}(B.\mathfrak{p}) > 0.$$

$\mathfrak{p}$ max'l, $1 \notin \mathfrak{P}$

In particular, since $B.\mathfrak{p}$ is proper, the contraction is surjective.

Some terminology:

Let $\mathfrak{p} \in \mathrm{Spec}(A)^\times$, $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$. Then

- the ramification index of $\mathfrak{P}$ (at $\mathfrak{p}$) is $e_{\mathfrak{P}|\mathfrak{p}} := v_{\mathfrak{P}}(B.\mathfrak{p})$
- $k_{\mathfrak{p}} := A/\mathfrak{p}$ is the residue field at $\mathfrak{p}$
- $k_{\mathfrak{p}} \hookrightarrow k_{\mathfrak{P}} = B/\mathfrak{P}$ is finite extension (as B is A-f.t.) and the inertia degree of $\mathfrak{P}$ (at $\mathfrak{p}$) is $f_{\mathfrak{P}|\mathfrak{p}} := [k_{\mathfrak{P}} : k_{\mathfrak{p}}]$

Remarks: $\mathfrak{p}$ is unramified in B if $e_{\mathfrak{P}|\mathfrak{p}} = 1$ for all $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$.

- $B.\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$

Theorem (Degree formula)

Let $\mathfrak{p} \in \operatorname{Spec}(A)^*$, $K_\mathfrak{p} := B/B.\mathfrak{p}$. Then $K_\mathfrak{p}$ is a finite dimensional $k_\mathfrak{p}$-algebra and

$$[K:\mathbb{Q}] \overset{(i)}{=} \dim_{k_\mathfrak{p}}(K_\mathfrak{p}) \overset{(ii)}{=} \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}|\mathfrak{p}} \cdot f_{\mathfrak{P}|\mathfrak{p}}.$$

In particular, $|\operatorname{Spec}_\mathfrak{p}(B)| \leq [K:\mathbb{Q}]$

Proof of (ii): $\mathfrak{p} = B.\mathfrak{p} \cap A \Rightarrow k_\mathfrak{p} = A/\mathfrak{p} \hookrightarrow B/B.\mathfrak{p}$ and thus $B/B.\mathfrak{p}$ is a $k_\mathfrak{p}$-algebra.

B A-f.t. $\Rightarrow \dim_{k_\mathfrak{p}}(K_\mathfrak{p}) < \infty$.

Chinese-remainder theorem:

$$B/B.\mathfrak{p} \overset{(*)}{\cong} \bigoplus_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$$

as A-modules.

⌈Recall: the isomorphism in CRT is given by $x + B.\mathfrak{p} \mapsto (x + \mathfrak{P}_1^{e_{\mathfrak{P}_1|\mathfrak{p}}}, \ldots, x + \mathfrak{P}_s^{e_{\mathfrak{P}_s|\mathfrak{p}}})$ and hence is an isomorphism of A-modules ⌋

<u>Exercise</u>: Let e in $\mathbb{N}$. $\mathfrak{p} = \mathfrak{P}^e \cap A \iff 1 \leq e \leq e_{\mathfrak{P}|\mathfrak{p}}$.

Therefore $(*)$ is an isomorphism of $k_\mathfrak{p}$-vector spaces and the $B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$ are subspaces.

In particular,

$$\dim_{k_\mathfrak{p}}(K_\mathfrak{p}) = \sum_{\mathfrak{P}|\mathfrak{p}} \dim_{k_\mathfrak{p}}\left(B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}\right).$$

We show that

$$\dim_{k_\mathfrak{p}}\left(B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}\right) = e_{\mathfrak{P}|\mathfrak{p}} \cdot f_{\mathfrak{P}|\mathfrak{p}}.$$

If $e_{\mathfrak{P}|\mathfrak{p}} = 1$, then $B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}} = k_\mathfrak{P}$ and thus the statement follows by definition of $f_{\mathfrak{P}|\mathfrak{p}}$.

Suppose that $1 \leq e < e_{\mathfrak{P}|\mathfrak{p}}$ and $\dim_{k_\mathfrak{p}}\left(B/\mathfrak{P}^e\right) = e \cdot f_{\mathfrak{P}|\mathfrak{p}}$. We have an exact sequence of $k_\mathfrak{p}$-vector spaces

$$0 \longrightarrow \mathfrak{P}^e/\mathfrak{P}^{e+1} \longrightarrow B/\mathfrak{P}^{e+1} \longrightarrow B/\mathfrak{P}^e \longrightarrow 0,$$

thus $\dim_{k_\mathfrak{p}}\left(B/\mathfrak{P}^{e+1}\right) - \dim_{k_\mathfrak{p}}\left(\mathfrak{P}^e/\mathfrak{P}^{e+1}\right) = \dim_{k_\mathfrak{p}}\left(B/\mathfrak{P}^e\right)$.

$\therefore$ <u>NTS:</u> $\dim_{k_\mathfrak{p}}\left(\mathfrak{P}^e/\mathfrak{P}^{e+1}\right) = f_{\mathfrak{P}|\mathfrak{p}}$. $(**)$

Proof of (**):

We first explain why $\mathfrak{P}^e/\mathfrak{P}^{e+1} \subseteq B/\mathfrak{P}^{e+1}$ is a $k_\mathfrak{p}$-subspace. It is clear that it is an additive subgroup. Moreover, if $a \in A$ and $x \in \mathfrak{P}^e$, then $a.x \in \mathfrak{P}^e$ and hence

$$(a+\mathfrak{p}).(x+\mathfrak{P}^{e+1}) = a.x + \mathfrak{P}^{e+1} \in \mathfrak{P}^e/\mathfrak{P}^{e+1}.$$

this is how $k_\mathfrak{p} \curvearrowright B/\mathfrak{P}^{e+1}$

The same argument shows that $\mathfrak{P}^e/\mathfrak{P}^{e+1}$ is a $k_\mathfrak{P}$-vector space.

⚠ caveat: $B/\mathfrak{P}^{e+1}$ is <u>not</u> a $k_\mathfrak{P}$-vector space.

Thus it suffices to show that $\dim_{k_\mathfrak{P}}\left(\mathfrak{P}^e/\mathfrak{P}^{e+1}\right) = 1$.

Let $M \subseteq \mathfrak{P}^e/\mathfrak{P}^{e+1}$ a $k_\mathfrak{P}$-subspace, then it is in particular a B-submodule.

The B-submodules of $\mathfrak{P}^e/\mathfrak{P}^{e+1}$ are in 1-1-correspondence with the B-submodules I of B (i.e., ideals) satisfying $\mathfrak{P}^{e+1} \subseteq I \subseteq \mathfrak{P}^e$.

Prime factorization of ideals in B implies that $I \in \{\mathfrak{P}^e, \mathfrak{P}^{e+1}\}$.

$\blacksquare$

Proof of (i) if A is a PID:

In this case, B is free over A of rank $[K:\mathbb{Q}]$ and so is $B.\mathfrak{p}$.
Let $(z_1,\dots,z_d)$ an A-basis of B and suppose $\mathfrak{p} = A.a$ (A is a PID). Then $(a.z_1,\dots,a.z_d)$ is an A-basis of $B.\mathfrak{p}$.

Claim:
$(z_1+B.\mathfrak{p},\dots,z_d+B.\mathfrak{p})$ are a $k_\mathfrak{p}$-basis of $B/B.\mathfrak{p}$

Indeed, $B/B.\mathfrak{p}$ is generated by $(z_1+B.\mathfrak{p},\dots,z_d+B.\mathfrak{p})$. We have to prove linear independence.

Suppose $a_1,\dots,a_d \in A$ s.t. $a_1.z_1+\dots+a_d.z_d \in B.\mathfrak{p}$, i.e., $\exists r_1,\dots,r_d \in A$

$$a_1.z_1+\dots+a_d.z_d = r_1 a.z_1 + \dots + r_d a.z_d$$

$z_1,\dots,z_d$ lin. indep. over A

$\Rightarrow a_i = r_i a \in \mathfrak{p}$ and thus $a_i.z_i \in B.\mathfrak{p}$ $\blacksquare$

What if A is not a PID?

Outline

We localize at $S = A - \mathfrak{p}$, to obtain $A_\mathfrak{p}$, $\underbrace{B_\mathfrak{p} := S^{-1}B}_{\text{"localization of } B \text{ at } \mathfrak{p}\text{"}}$. Note that

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[d, two heads] \arrow[dr, dotted, "\varphi"] & A_\mathfrak{p} \arrow[d, two heads] \\
k_\mathfrak{p} \arrow[r, "\sim"] & A_\mathfrak{p}/A_\mathfrak{p}\cdot\mathfrak{p}
\end{tikzcd}$$

$$\ker\varphi = A \cap A_\mathfrak{p}\cdot\mathfrak{p} = \mathfrak{p}$$

and, as we will see, we obtain an isomorphism

$$B/B.\mathfrak{p} \cong B_\mathfrak{p}/B_\mathfrak{p}\cdot\mathfrak{p}$$

of $k_\mathfrak{p}$-algebras. We show that $B_\mathfrak{p} = \mathcal{O}_K(A_\mathfrak{p})$ and, using that $A_\mathfrak{p}$ is a PID, the claim follows.