Math 538, Lecture 5 24/1/2024

(1) PS1, PS2 on website
(2) commutative algebra supplement

Last time: Unique factorisation in $\mathcal{O}_K$

K = # field, $\mathcal{O}_K$ = ring of integers

Thm: (1) Every ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ has a unique representation in the form

$$\mathfrak{a} = \prod_{\mathfrak{p} \trianglelefteq \mathcal{O}_K} \mathfrak{p}^{e_\mathfrak{p}}$$

($\mathfrak{p}$ primes, $e_\mathfrak{p} \in \mathbb{Z}_{\geq 0}$, almost all 0)

(2) Every fractional ideal has a unique such representation, $e_\mathfrak{p} \in \mathbb{Z}$

"Correct" generalization to K of the fundamental theorem of arithmetic.

Cor: In the monoid of ideals of $\mathcal{O}_K$, $\mathfrak{a} | \mathfrak{b}$ iff $\mathfrak{a} \supset \mathfrak{b}$.

Today: Extension of primes

Key tool in understanding primes of K was studying prime $\mathfrak{p} \cap \mathbb{Z}$ of $\mathbb{Q}$.

Proof of unique factorization transported structure from $\mathbb{Q}$ to K

Next: general extension L/K of # fields

Lemma: Let $\mathfrak{P}$ be a prime of L. Then $\mathfrak{p} = \mathfrak{P} \cap K = \mathfrak{P} \cap \mathcal{O}_K$ is a prime of K, the unique prime of K contained in $\mathfrak{P}$.

Pf: Same as for $K/\mathbb{Q}$. (HW)

Def: In this situation say $\mathfrak{P}$ lies above $\mathfrak{p}$, write $\mathfrak{P} \mid \mathfrak{p}$.

(strictly speaking $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$)

$\Rightarrow$ prime ideals of L which lie above $\mathfrak{p}$ are exactly the prime divisors of $\mathfrak{p}\mathcal{O}_L$

Also, the $\mathcal{O}_L$-module $\mathcal{O}_L/\mathfrak{P}$ is annihilated by $\mathfrak{p}$
$\Rightarrow k_{\mathfrak{P}} \overset{\text{def}}{=} \mathcal{O}_L/\mathfrak{P}$ is a $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$-module

Call $k_{\mathfrak{p}}$, $k_{\mathfrak{P}}$ the residue fields of $\mathfrak{p}, \mathfrak{P}$..

__Def:__ $q_{\mathfrak{p}} = \# k_{\mathfrak{p}}$ is the size of the residue field

$f(\mathfrak{P}/\mathfrak{p}) \overset{\text{def}}{=} [k_{\mathfrak{P}} : k_{\mathfrak{p}}] = \dim_{k_{\mathfrak{p}}} k_{\mathfrak{P}}$ is called the residue index or inertial degree..

__Prop:__ $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$, i.e. there exist primes of L above $\mathfrak{p}$.
(Ex.)

Say $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ with $\mathfrak{P}_i$ distinct.

__Def:__ $e(\mathfrak{P}_i/\mathfrak{p}) \overset{\text{def}}{=} e_i$ is called the ramification index. If some $e_i > 1$, say $\mathfrak{p}$ ramifies in L

Also write f_i for $f(\mathfrak{P}_i/\mathfrak{p})$.

<u>Lemma:</u> Let $\mathfrak{P} \triangleleft \mathcal{O}_L$ be prime. Then for all $e \geq 1$, $\mathcal{O}_L/\mathfrak{P}^e$ is a dvr: a local ring and a PID

<u>Pf:</u> The ideals of $\mathcal{O}_L/\mathfrak{P}^e$ correspond to the ideals of $\mathcal{O}_L$ containing $\mathfrak{P}^e$, i.e. to the ideals

$$\{\mathfrak{P}^j\}_{j=0}^{e}.$$ So $\mathfrak{P}/\mathfrak{P}^e$ is the unique prime.

Choose $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Then its image in $\mathcal{O}_L/\mathfrak{P}^e$ generates a proper ideal not contained in $\mathfrak{P}^2/\mathfrak{P}^e$. So it must be $\mathfrak{P}/\mathfrak{P}^e$.

<u>Conclusion:</u> $\mathfrak{P}^j/\mathfrak{P}^e = (\bar{\pi})^j$ $\qquad \bar{\pi}$ = image of π.

<u>Example:</u> $F[[\{x^r : r \in \mathbb{Q}_{\geq 0}\}]] = \varinjlim_{n \to \infty} F[[x^{1/n}]]$

is not of this type.

Thm: Recall $n = [L:K]$. Then for any $p \lhd \mathcal{O}_K$

$$n = \sum_{i=1}^{g} f_i e_i$$

Pf: Calculate

$\dim_{k_p}(\mathcal{O}_L / p\mathcal{O}_L)$ in two ways

RHS: P_i are maximal ideals, so if $i \neq j$ $P_i + P_j = (1)$
$\Rightarrow P_i^{e_i} + P_j^{e_j} = (1)$. Next, $\bigcap_{i=1}^{g} P_i^{e_i} = p\mathcal{O}_L$ (both sides have same factorisation: if Q is a prime of L, r larger than order of Q in both sides, reduce mod Q^r)

$\Rightarrow$ (CRT) $\mathcal{O}_L / p\mathcal{O}_L \cong \bigoplus_{i=1}^{g} \mathcal{O}_L / P_i^{e_i}$

As a k_p-vsp, $\mathcal{O}_L / P_i^{e_i}$ is filtered by subspaces $\{P_i^j / P_i^{e_i}\}_{j=0}^{e_i}$.

So

$$\dim_{k_p} \mathcal{O}_L / P_i^{e_i} = \sum_{j=0}^{e_i - 1} \dim_{k_p} P_i^j / P_i^{j+1}$$

$$P_i^j / P_i^{j+1} = (\bar{\pi})^j / (\bar{\pi})^{j+1} \cong \mathcal{O}_L / P_i \quad \leftarrow \dim = f_i$$

(in $\mathcal{O}_L / P_i^{e_i}$, mult by $\bar{\pi}$ gives isom P_i^j / P_i^{j+1} and P_i^{j+1} / P_i^{j+2}.)

$\Rightarrow \dim_{k_p} \mathcal{O}_L / P_i^{e_i} = e_i \cdot f_i \Rightarrow \dim_{k_p} \mathcal{O}_L / p\mathcal{O}_L = \sum_i e_i f_i$

LHS: If $K=\mathbb{Q}$, $\mathfrak{p}=p\mathbb{Z}$ have $\mathcal{O}_L \cong \mathbb{Z}^n$ as $\mathbb{Z}$-mod.
so $\mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{Z}^n/p\mathbb{Z}^n \cong (\mathbb{Z}/p\mathbb{Z})^n \Rightarrow \dim_{\mathbb{F}_p} \mathcal{O}_L/p\mathcal{O}_L = n$

In general, $\mathcal{O}_L$ need not be a free $\mathcal{O}_K$-module
solution: localise at $\mathfrak{p}$

Pass to $\mathcal{O}_{K,\mathfrak{p}}$ has $\mathfrak{p}$ as the unique maximal ideal
($\mathcal{O}_{K,\mathfrak{p}}$ = subring of K generated by $\mathcal{O}_K$, $\{\alpha^{-1} : \alpha \in \mathcal{O}_K \setminus \mathfrak{p}\}$)

$\Rightarrow$ ideals of $\mathcal{O}_{K,\mathfrak{p}}$ are powers of $\mathfrak{p}$.
$\Rightarrow$ $\mathcal{O}_{K,\mathfrak{p}}$ is a PID (ideals are generated by π^j as in lemma)

Now $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_L[S^{-1}]$, $S = \mathcal{O}_K \setminus \mathfrak{p}$
is a torsion-free $\mathcal{O}_{K,\mathfrak{p}}$-module (torsion-free as ab gp, all ideals of $\mathcal{O}_{K,\mathfrak{p}}$ are cofinite)
so it is free, so
$$\mathcal{O}_L[S^{-1}] \cong \mathcal{O}_{K,\mathfrak{p}}^m \quad (\$)$$
as an $\mathcal{O}_{K,\mathfrak{p}}$-module.

Further localize by inverting every element of $\mathbb{Z}$

$\mathcal{O}_L[\mathbb{Z}^{-1}] = L$, $\mathcal{O}_K[\mathbb{Z}^{-1}] = K$ ($\forall \alpha \in K$ $\exists d \in \mathbb{Z}$ s.t. $d\alpha \in \mathcal{O}_K$)

$\Rightarrow$ $L \cong K^m$ as K-module $\Rightarrow$ $m = n$

Finally, every $s \in S$ is invertible in $\mathcal{O}_K/p$, so

$$\mathcal{O}_L/p\mathcal{O}_L \cong (\mathcal{O}_L/p\mathcal{O}_L)[S^{-1}] \cong \mathcal{O}_L[S^{-1}]/p\mathcal{O}_L[S^{-1}]$$

$$\cong \mathcal{O}_{K,p}^n / p\,\mathcal{O}_{K,p}^n \cong (\mathcal{O}_{K,p}/p)^n \cong (\mathcal{O}_K/p)^n.$$

$\Rightarrow$ $\dim_{\mathcal{O}_K/p} \mathcal{O}_L/p\mathcal{O}_L = n.$ $\blacksquare$

Or: Have abstract notion of "Dedekind domain".

Thm: If $\mathcal{O}$ is a Dedekind domain, M f.g. $\mathcal{O}$-mod then have ideals $\mathfrak{a}_i, \mathfrak{b}_j$ s.t.

$$M \cong \bigoplus_i \mathfrak{a}_i \oplus \bigoplus_j \mathcal{O}/\mathfrak{b}_j$$

$\mathfrak{a}_i$: really ideal classes.

Analogy: ① Riemann surfaces $\mathcal{O}_K$
(1d complex manifolds, holomorphic fcns
$K \leftrightarrow$ meromorphic fcns)

② Algebraic curves (1d projective varieties)
$\mathcal{O}_K \leftrightarrow$ regular function
$K \leftrightarrow$ rational functions

Extension $\begin{matrix} L \\ \updownarrow \\ K \end{matrix}$ $\longleftrightarrow$ non-constant map of surfaces $\begin{matrix} S_1 \\ \downarrow \\ S_2 \end{matrix}$

primes $\leftrightarrow$ points