12.1.

Back to number fields. (recap)

General setup

L/K finite ext of fields. (seperable)

$$\begin{array}{ccl} L & - & B \text{ — integral closure of } A \text{ in } L. \\ | & & \\ K & - & A \quad \text{integrally closed domain} \end{array}$$

Special case

$$\begin{array}{ccc} K & - & \mathcal{O}_K \\ | & & \\ \mathbb{Q} & - & \mathbb{Z} \end{array}$$

Some stuff is specialized to this case:

. norms, discriminants, ...

There are "relative notions".

Recap. In above, $\mathcal{O}_K$ is a Dedekind domain.

(1) noetherian

(2) integrally closed in its field of fractions

(3) every prime ideal $\neq (0)$ is maximal.

Thm. In above, A Dedekind $\Longrightarrow$ B is.

$\mathbb{Z}$ is, so $\mathcal{O}_K$ is also. Also finite ext'ns of $\mathbb{F}_q[t]$.

Thm. In a Dedekind domain, any ideal of B can be written uniquely as a product of number fields.

5.4. =12.2. **Theorem.** (Chinese Remainder)

Given a ring R, and ideals $\underline{a}_1 \ldots \underline{a}_n$ with $\underline{a}_i + \underline{a}_j = R$ if $i \neq j$.

Then,
$$R/\cap \underline{a}_i \cong \oplus R/\underline{a}_i.$$

Proof. Consider the homomorphism
$$R \longrightarrow \oplus R/\underline{a}_i$$
$$r \longrightarrow (r + \underline{a}_1, \ldots, r + \underline{a}_n).$$

Visibly, the kernel is $\cap \underline{a}_i$. So prove surjective.

Surjectivity for $n=2$.
We can write $1 = a_1 + a_2$ where $a_1 \in \underline{a}_1$, $a_2 \in \underline{a}_2$,

and so $a_1 \equiv 1 \pmod{\underline{a}_2}$, $\equiv 0 \pmod{\underline{a}_1}$ and vice versa

$$x a_1 + y a_2 \longrightarrow (y a_2, x a_1)$$
$$= (y, x) \text{ in } R/\underline{a}_1 \oplus R/\underline{a}_2$$

choose x, y anything you want.

$n > 2$. Similar story.
~~Write~~ Find $b_{1,2} \equiv 1 \pmod{\underline{a}_1}$ and $\equiv 0 \pmod{\underline{a}_2}$

$b_{1,3} \equiv 1 \pmod{\underline{a}_1}$ and $\equiv 0 \pmod{\underline{a}_3}$

$\vdots$

$b_{1,n} \equiv 1 \pmod{\underline{a}_1}$ and $\equiv 0 \pmod{\underline{a}_n}$

$$b_1 = b_{1,2} \cdot b_{1,3} \cdot \cdots \cdot b_{1,n} \equiv 1 \pmod{\underline{a}_1}$$
$$\equiv 0 \pmod{\underline{a}_i} \text{ for } i \neq 1.$$

Then $b_1 \longrightarrow (1, 0, 0, \cdots, 0)$.
Similarly can find elts mapping to $(0, 1, 0, 0, \cdots, 0)$ etc.
and these generate $\oplus R/\underline{a}_i$. ∎

(5.5.) = 12.3.

Prop. In a Dedekind domain R, if $\underline{a}_1 + \underline{a}_2 = R$ then $\underline{a}_1$ and $\underline{a}_2$ are coprime.

This is easy. If $\underline{a}_1 = \underline{p}\,\underline{b}_1$ for some $\underline{p}, \underline{b}_1$,

$$\underline{a}_2 = \underline{p}\,\underline{b}_2$$

then $\underline{a}_1 + \underline{a}_2 = \underline{p}\,\underline{b}_1 + \underline{p}\,\underline{b}_2 \subseteq \underline{p}$.

It goes the other way too.

If $\underline{a}_1 + \underline{a}_2 = \underline{a} < R$,

then $\underline{a}_1 \subseteq \underline{a}$, $\underline{a}_2 \subseteq \underline{a}$ and so $\underline{a}_1 = \underline{a} \cdot \underline{b}_1$, $\underline{a}_2 = \underline{a} \cdot \underline{b}_2$ for some $\underline{b}_1, \underline{b}_2$

(IMF, Prop. 69. containment $\longleftrightarrow$ divisibility.)

Prop. If $\underline{a}_1 \dots \underline{a}_n$ are pairwise coprime ideals, then

$$\underline{a}_1 \cdot \underline{a}_2 \cdots \underline{a}_n = \underline{a}_1 \cap \cdots \cap \underline{a}_n .$$

$\subseteq$ is obvious.

$\supseteq$: Do a simple induction, or:
if $a \in \underline{a}_1 \cap \cdots \cap \underline{a}_n$, then for each i, $\underline{a}_i \mid (a)$.
Since the $\underline{a}_i$'s are coprime, $\underline{a}_1 \cdots \underline{a}_n \mid (a)$.
i.e., $a \in \underline{a}_1 \cdots \underline{a}_n$.

So: CRT restated.

In a Dedekind domain, if $\underline{a} = \prod \underline{a}_i$ with the $\underline{a}_i$ coprime,

$$R/\underline{a} \cong \bigoplus_i R/\underline{a}_i . \qquad \text{(usual CRT!)}$$

12.4.

Norms.

Def. Let $\alpha \in L$. Then the norm from L to K, $N_{L/K}(\alpha)$ of α is the determinant of the endomorphism (as vector spaces over K)

$$L \longrightarrow L$$
$$x \longrightarrow \alpha x.$$

We have $N_{L/K}(x) = \prod_\sigma \sigma(x)$. σ: embeddings $L \hookrightarrow \bar{K}$.

Also, if α generates L/K with min poly

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \text{ then } a_0 = (-1)^n N_{L/K}(\alpha)$$

(write this as $\prod(x - \alpha_i) = 0$.)

The proof is as for the trace. (see 3.3-3.4 of lecture notes §1.2 of Neu. etc.)

If $K = \mathbb{Q}$ just talk about the norm $N(\alpha)$.

Def. Suppose that K is a number field and $\underline{a}$ is an ideal. Then its (absolute) norm is

$$N(\underline{a}) = [\mathcal{O}_K : \underline{a}].$$

There is a relative norm from L to K also. You get an ideal of $\mathcal{O}_K$.

Proposition. Let $\alpha \in \mathcal{O}_K$. Then

$$N(\alpha) = N((\alpha)).$$

Proof. Linear algebra. LHS is the determinant of the endomorphism $\times\alpha$. Here we have $\alpha\mathcal{O}_K \subseteq \mathcal{O}_K$,

so $\quad$ (det of this matrix) $= \left[\begin{array}{l}\text{original} \\ \text{lattice}\end{array} : \begin{array}{l}\text{image under} \\ \text{this endomorphism}\end{array}\right]$

i.e. exactly what we have above.

12.5.

Proposition. Norms are multiplicative, i.e.

$$N(\underline{a}\,\underline{b}) = N(\underline{a})\,N(\underline{b}).$$

Proof. (see also MF, Thm. 82)

If $\underline{a}, \underline{b}$ are coprime then

$$\mathcal{O}_K / \underline{a}\,\underline{b} = \mathcal{O}_K/\underline{a} \oplus \mathcal{O}_K/\underline{b} \quad \text{so obvious.}$$

In general, want to show

$$N(\mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r},$$

by CRT enough to show for prime powers.

We have $\mathcal{O}_K \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^e$.

All containments proper, because of unique factorization.

Claim. For each i, $\mathfrak{p}^i / \mathfrak{p}^{i+1}$ is an $\mathcal{O}_K/\mathfrak{p}$ - v.s. of dim 1.

~~[illegible]~~

~~[illegible]~~

~~[illegible]~~

Observe. (1) $\mathfrak{p}^i / \mathfrak{p}^{i+1}$ is indeed an $\mathcal{O}_K/\mathfrak{p}$ - v.s. (not 0).

Now, choose $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$

Consider

$$\mathcal{O}_K \longrightarrow \mathfrak{p}^i / \mathfrak{p}^{i+1}$$

$$x \longmapsto a \cdot x + \mathfrak{p}^{i+1}$$

The kernel is $\mathfrak{p}$, evidently.

It is surjective, because there are no ideals between $\mathfrak{p}^i$ and $\mathfrak{p}^{i+1}$.

(If we had such an ideal $\underline{b}$, would have $\mathcal{O}_K > \underline{b}\,\mathfrak{p}^{-i} > \mathfrak{p}$ but $\mathfrak{p}$ is maximal.

And so done.

13.1. Ideals in extensions.

$$
\begin{array}{ccc}
B & — & L \\
| & & \\
A & — & K \supseteq \mathfrak{p}
\end{array}
$$

<u>Question</u>. What does $\mathfrak{p}\mathcal{O}_L$ look like?

It has unique factorization, so write

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}. \qquad (*)$$

We say the $\mathfrak{P}_i$ <u>lie over</u> (or <u>divide</u> $\mathfrak{p}$.)

<u>Lemma</u>. $\mathfrak{P} \subseteq B$ lies over $\mathfrak{p} \subseteq A$ iff $\mathfrak{P} \cap A = \mathfrak{p}$.

<u>Proof</u>. $\longrightarrow$: By $(*)$, $\mathfrak{p} \subseteq \mathfrak{P}$, so $\mathfrak{p} \subseteq \mathfrak{P} \cap A$.

Conversely, $\mathfrak{P} \cap A$ is an ideal of A containing $\mathfrak{p}$ and not 1, so by maximality $\mathfrak{p} = \mathfrak{P} \cap A$.

$\longleftarrow$: $\mathfrak{p}B \subseteq \mathfrak{P}$, i.e., $\mathfrak{P}$ is a prime factor of $\mathfrak{p}B$.

<u>Definition</u>. If $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$:

If any $e_i \geq 1$, we say $\mathfrak{p}$ <u>ramifies</u> in B.

e_i is the <u>ramification index</u> of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Write $e(\mathfrak{P}_i | \mathfrak{p}) = e_i$.

Now, Given $\mathfrak{P} | \mathfrak{p}$, $B/\mathfrak{P}$ and $A/\mathfrak{p}$ are both <u>fields</u>.

Moreover, we have an <u>injective</u> map

$$
\begin{aligned}
A/\mathfrak{p} &\hookrightarrow B/\mathfrak{P} \\
a + \mathfrak{p} &\longmapsto a + \mathfrak{P}
\end{aligned}
$$

injective because kernel is $\mathfrak{p} + \mathfrak{P} = \mathfrak{P}$.

B is a finitely generated A-module, so $B/\mathfrak{P}$ is a f.g. $A/\mathfrak{p}$-module.

i.e. if $B = Ab_1 \oplus Ab_2 \oplus \cdots \oplus Ab_n$,

then $B/\mathfrak{P} = (A/\mathfrak{p}) b_1 \pmod{\mathfrak{P}} + \cdots + (A/\mathfrak{p}) b_n \pmod{\mathfrak{P}}$

but no longer necessarily direct.

13.2.

Put another way,

$$B/\mathfrak{p}B = (A/\mathfrak{p})\,b_1 \oplus \cdots \oplus (A/\mathfrak{p})\,b_n.$$ (spanning is clear. independence to be shown.)

and we have a natural injection $B/\underline{P} \hookrightarrow B/\mathfrak{p}B$,

because $\mathfrak{p}B \subseteq \underline{P}$.

Thus $B/\underline{P}$ is a finite field extension of $A/\mathfrak{p}$.

and $[B/\underline{P} : A/\mathfrak{p}] \leq [L:K]$.

Def. $[B/\underline{P} : A/\mathfrak{p}]$ is the residue class degree of $\underline{P}$ over $\mathfrak{p}$. Write it $f(\underline{P}\,|\,\mathfrak{p})$.

Theorem. (e-f-g) A : Ded. domain with f.f. K. L/K finite separable, B = int. closure of A in L.

Let $\mathfrak{p} \subseteq A$ and $\mathfrak{p}B = \underline{P}_1^{e_1} \cdots \underline{P}_g^{e_g}$,

where each $\underline{P}_i$ has ramification index e_i and residue class degree f_i.

Then,
$$[L:K] = \sum_{i=1}^{g} e_i f_i.$$

Note. Will show, if L/K is Galois, that all the e_i are equal, and all the f_i are equal, so
$$[L:K] = efg.$$

Example. $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $B = \mathbb{Z}[i]$.

Then $(2) = (1+i)^2$ so $e((1+i)\,|\,(2)) = 2$.

(3) = still prime, so $e((3)\,|\,(3)) = 1$

$f((3)\,|\,(3)) = 2$.

Here $\mathbb{Z}[i]/(3) \cong \mathbb{F}_9$.

$(5) = (2+i)(2-i)$, and $e = f = 1$,

$$\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}[i]/(2-i) \cong \mathbb{Z}/(5) = \mathbb{F}_5.$$

13.3.

Example.

Let $L = \mathbb{Q}(\theta)$, where $\theta^3 - \theta - 1 = 0$. $\mathrm{Disc}(L) = -23$.

$3\mathcal{O}_L = (3)$ still prime so $f(5|5) = 3$.

$5\mathcal{O}_L = \mathfrak{p}_1 \cdot \mathfrak{p}_2$, where $f(\mathfrak{p}_1|5) = 1$ $f(\mathfrak{p}_2|5) = 2$.

$59\mathcal{O}_L = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$ where $f(\mathfrak{p}_i|59) = 1$.
(Yes, 59 is the first one

$23\mathcal{O}_L = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2$. This is the only prime that ramifies.

Cool facts. (1) $\left(\frac{-23}{p}\right) = -1 \longleftrightarrow p = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ as above.

$\left(\frac{-23}{p}\right) = 1 \longleftrightarrow p = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$ or it's still prime.

$\left(\frac{-23}{p}\right) = 0 \longleftrightarrow p$ is partially ramified.

(2) You can have $p = \mathfrak{p}^3$ but not in this field.
First example. Let $L = \mathbb{Q}(\theta)$, $\theta^3 - \theta^2 + \theta + 1$. $\mathrm{Disc}(L) = -44$
Then $(2) = \mathfrak{p}^3$. (And $(11) = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2$.)

(3) You can predict the densities.
If L is cubic and not Galois,

$p\mathcal{O}_L$ = prime w/ probability $\frac{1}{3}$

$= \mathfrak{p}_1 \cdot \mathfrak{p}_2$ with $f(\mathfrak{p}_1|p) = 1$, $f(\mathfrak{p}_2|p) = 2$ prob. $\frac{1}{2}$

$= \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$ with prob. $\frac{1}{6}$

ramified if and only if $p \mid \mathrm{Disc}(L)$.

Same probabilities: Let g be a random elt. of $\mathrm{Sym}(3)$.

3-cycle with prob. $\frac{1}{3}$.

2-cycle with prob. $\frac{1}{2}$.

trivial with prob. $\frac{1}{6}$.

Connection: Chebotorev density theorem (to come)