12.1. Back to number fields. (recap)

General setup

$L \rightarrow B$ - $L/K$ finite ext of fields. (separable)

$\rightarrow$ integral closure of $A$ in $L$.

$K \rightarrow A$ - integrally closed domain

Special case

$K \rightarrow \mathcal{O}_K$ - Some stuff is specialized to this case:

- norms, discriminants, ...
- There are "relative notions:"

$\mathcal{O}_K \rightarrow \mathcal{O}$

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 $\Rightarrow B$ is.

$\mathcal{O}_K$ is, so $\mathcal{O}_K$ is also. Also finite ext/qs of $\mathbb{F}_q[T]$.

Thm. In a Dedekind domain, any ideal of $B$ can be written uniquely as a product of number fields.
\[ \text{Theorem (Chinese Remainder)} \]

Given a ring \( R \), and ideals \( a_1, \ldots, a_n \) with \( a_i + a_j = R \) if \( i \neq j \).

Then,
\[
\frac{R}{\cap a_i} \cong \bigoplus \frac{R}{a_i}.
\]

Proof. Consider the homomorphism
\[
R \longrightarrow \bigoplus \frac{R}{a_i}, \quad r \longrightarrow (r + a_1, \ldots, r + a_n).
\]

Visibly, the kernel is \( \cap a_i \). So prove surjective.

Surjectivity for \( n = 2 \).

We can write \( 1 = a_1 + a_2 \) where \( a_1 \in a_1, a_2 \in a_2 \),

and so \( a_1 \equiv 1 \pmod{a_2} \), \( 0 \equiv 0 \pmod{a_1} \) and vice versa
\[
xa_1 + ya_2 \longrightarrow (ya_2, xa_1)
\]
\[
= (y, x) \text{ in } \frac{R}{a_1} \oplus \frac{R}{a_2}
\]
choose \( x, y \) anything you want.

\( n > 2 \). Similar story.

Find \( b_{1,2} \equiv 1 \pmod{a_1} \) and \( 0 \equiv 0 \pmod{a_2} \)

\( b_{1,3} \equiv 1 \pmod{a_1} \) and \( 0 \equiv 0 \pmod{a_3} \)

\( \vdots \)

\( b_{1,n} \equiv 1 \pmod{a_1} \) and \( 0 \equiv 0 \pmod{a_n} \)

\( b_1 = b_{1,2} \cdot b_{1,3} \cdots b_{1,n} \equiv 1 \pmod{a_1} \)

\( = 0 \pmod{a_i} \) for \( i \neq 1 \).

Then \( b_1 \longrightarrow (1, 0, 0, \ldots, 0) \).

Similarly you findelts mapping to \((0,1,0,0,\ldots, 0)\) etc.

and these generate \( \bigoplus \frac{R}{a_i} \).
Prop. In a Dedekind domain, if \( a_1 + a_2 = \mathbb{R} \) then \( a_1 \) and \( a_2 \) are coprime.

This is easy. If \( a_1 = p \cdot b_1 \) for some \( p, b_1 \),
\[
a_2 = p \cdot b_2
\]
then \( a_1 + a_2 = p \cdot b_1 + p \cdot b_2 \subseteq p \).

It goes the other way too.

If \( a_1 + a_2 = a < \mathbb{R} \),
then \( a_1 \leq a, a_2 \leq a \) and so \( a_1 = a \cdot b_1 \) for some \( b_1, b_2 \),
\[
a_2 = a \cdot b_2
\]
(MF, Prop. 69. containment \( \leftrightarrow \) divisibility.)

Prop. If \( a_1 \ldots a_n \) are pairwise coprime ideals, then
\[
a_1 \cdot a_2 \ldots a_n = a_1 \cap \ldots \cap a_n.
\]

\( \mathbb{S} \) is obvious.

2: Do a simple induction, or:
if \( a = a_1 \cap \ldots \cap a_n \), then for each \( i \), \( a_i \mid (a) \).
Since the \( i \)'s are coprime, \( a_i \ldots a_n \mid (a) \).
i.e., \( a = a_1 \ldots a_n \).

So: CRT restated.

In a Dedekind domain, if \( a = \bigcap a_i \) with the \( a_i \) coprime,
\[
\frac{\mathbb{R}}{a} \cong \bigoplus_{i} \frac{\mathbb{R}}{a_i}. \quad \text{(usual CRT!)}
\]
12.4. Norms.

*Def.* Let \( \mathcal{L} \) be a \( k \)-vector space. Then the norm of \( \mathcal{L} \) is the determinant of the endomorphism (as vector spaces over \( K \))

\[
\mathcal{L} \rightarrow \mathcal{L},
\begin{align*}
x & \mapsto \mathcal{L}.
\end{align*}
\]

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

Also, if \( \mathcal{L} \) generates \( L/K \) with min poly

\[
x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0,
\]

then \( a_0 = (-1)^n N_{L/K}(x) \)

(write this as \( \prod(x - \alpha_i) = a_0 \).)

The proof is as for the trace. (see 3.3-3.4 of lecture notes 41.2 of Neu. ete.)

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

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

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

There is a relative norm from \( L \) to \( K \) also.

You get an ideal of \( \mathcal{O}_K \).

Proposition. Let \( \mathcal{O} \in \mathcal{O}_K \). Then

\[
N(\mathcal{O}) = N((\mathcal{O})).
\]

Proof. Linear algebra. LHS is the determinant of the endomorphism \( \mathcal{O} \). Here we have \( \mathcal{O} \cap \mathcal{O}_K \subseteq \mathcal{O}_K \),

so \( \det \text{ of this matrix} = \prod \text{original image under lattice of this endomorphism} \)

i.e. exactly what we have above.
Proposition. Norms are multiplicative, i.e.
\[ N(ab) = N(a)N(b). \]

Proof. (see also MF, Thm. 8.2)

If \( a, b \) are coprime then
\[ \mathcal{O}_K/ab = \mathcal{O}_K/a \oplus \mathcal{O}_K/b \] so obvious.

In general, want to show
\[ N(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = N(p_1)^{e_1} \cdots N(p_r)^{e_r}, \]
by CRT enough to show for prime powers.

We have \( \mathcal{O}_K = \mathbb{Z} p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \).
All containments proper, because of unique factorization.

Claim. For each \( i, p_i/p_{i+1} \) is an \( \mathcal{O}_K/p \)-v.s. of dim 1.

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

Now, choose \( a \in \mathcal{O}_K \setminus p_i/p_{i+1} \).
Consider \( \mathcal{O}_K \rightarrow p_i/p_{i+1} \).

\[ ax \rightarrow a \cdot x + p_{i+1} \]

The kernel is \( p_i \), evidently.
It is surjective, because there are no ideals between \( p_i \) and \( p_{i+1} \).
(If we had such an ideal \( \mathfrak{b} \),
would have \( \mathcal{O}_K \supset \mathfrak{b} p_i^{-1} \supset p_i \)
but \( p \) is maximal.

And so done.
13.1. Ideals in extensions.

Question. What does \( pO_L \) look like?

It has unique factorization, so write

\[
pO_L = P_1^{e_1} \cdots P_g^{e_g}. \tag{\*}
\]

We say the \( P_i \) lie over (or divide \( p \)).

Lemma. \( P \in B \) lies over \( p \in A \) iff \( P \cap A = p \).

Proof. \( \rightarrow \) By (\*), \( p \leq P \), so \( p \subseteq P \cap A \).

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

\( \leftarrow \) : \( pB \leq P \), i.e., \( P \) is a prime factor of \( pB \).

Definition. If \( pO_L = P_1^{e_1} \cdots P_g^{e_g} \):

If any \( e_i \geq 1 \), we say \( p \) \( \text{ramifies in } B \).

\( e_i \) is the \( \text{ramification index of } \mathfrak{g}P_i \) over \( p \).

Write \( e(P_i \mid p) = e_i \).

Now, given \( p \mid p \), \( B/\mathfrak{p} \) and \( A/\mathfrak{p} \) are both fields.

Moreover, we have an \( \text{injective map} \)

\[
A/\mathfrak{p} \longrightarrow B/\mathfrak{p},
\]

\( a + \mathfrak{p} \longrightarrow a + \mathfrak{p} \)(injective because kernel is \( \mathfrak{p} \) and \( \mathfrak{p} + \mathfrak{p} = \mathfrak{p} \)).

\( B \) is a finitely generated \( A \)-module, so

\( B/\mathfrak{p} \) is a \( f. q. \) \( A/\mathfrak{p} \)-module.

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

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

but no longer necessarily direct.
13.2.
Put another way, \[ B/\mathfrak{p}B = (A/\mathfrak{p}) b_1 \oplus \ldots \oplus (A/\mathfrak{p}) b_n, \]
spanning is clear, (independence to be shown.)
and we have a natural injection \[ \mathbb{B}/\mathfrak{p} \longrightarrow B/\mathfrak{p}B, \]
because \( \mathfrak{p}B \subseteq \mathfrak{B} \).
Thus \( \mathbb{B}/\mathfrak{p} \) is a finite field extension of \( A/\mathfrak{p} \).
and \( [B/\mathfrak{p} : A/\mathfrak{p}] \leq [L:K] \).
Def. \( [B/\mathfrak{p} : A/\mathfrak{p}] \) is the residue class degree of \( \mathfrak{p} \) over \( \mathfrak{p} \). Write it \( f(\mathfrak{p} | \mathfrak{p}) \).

Theorem. \((e-f-g)\) \( A \) : Ded. domain with f.f. \( K \).
\( L/K \) finite separable, \( B = \text{int. closure of } A \text{ in } L \).
Let \( \mathfrak{p} \in A \) and \( \mathfrak{p}B = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_g^{e_g} \),
where each \( \mathfrak{P}_i \) 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
\[ [L:K] = e \cdot f \cdot g. \]

Example. \( K = \mathbb{Q}, L = \mathbb{Q}(i), B = \mathbb{Z}[i]. \)
Then \( (2) = (1+i)^2 \), so \( e(\mathbb{Q}(1+i) | (2)) = 2 \).
\( (3) = \text{still prime, so } e(\mathbb{Q}(3) | (3)) = 1 \).
\( f(\mathbb{Q}(3) | (3)) = 2. \)
Here \( \mathbb{Z}[i]/(3) \cong \mathbb{F}_3 \).
\( (5) = (2+i)(2-i), \) and \( e = f = 1, \)
\[ \mathbb{Z}[i]/(2+i) \cong \mathbb{Z}[i]/(2-i) \]
\[ \cong \mathbb{Z}/(5) = \mathbb{F}_5. \]
Example.

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

30L = (3) still prime so \( f(5/15) = 3 \).

510L = \( p_1 \cdot p_2 \), where \( f(p_1 | 15) = 1 \) \( f(p_2 | 15) = 2 \).

590L = \( p_1 \cdot p_2 \cdot p_3 \), where \( f(p_i | 159) = 1 \).

(Yes, 59 is the first one.)

230L = \( p_1^2 \cdot p_2 \). This is the only prime that ramifies.

Cool facts,

\[
\left( \frac{-23}{p} \right) = -1 \quad \Rightarrow \quad p = p_1 \cdot p_2 \quad \text{as above.}
\]

\[
\left( \frac{-23}{p} \right) = 1 \quad \Rightarrow \quad p = p_1 \cdot p_2 \cdot p_3 \quad \text{or it's still prime.}
\]

\[
\left( \frac{-23}{p} \right) = 0 \quad \Rightarrow \quad p \quad \text{is partially ramified.}
\]

(2) You can have \( p = p_3^2 \) but not in this field.

First example. Let \( L = \mathbb{Q}(\theta) \), \( \theta^3 - \theta^2 + \theta + 1 \). Disc (L) = -4\( \chi \).

Then \((2) = \theta^3 \). (And \((11) = p_1^2 \cdot p_2 \).)

(3) You can predict the densities.

If \( L \) is cubic and not Galois,

\( pL \) = prime w/ probability \( \frac{1}{3} \)

= \( p_1 \cdot p_2 \) with \( f(p_1 | p) = 1 \), \( f(p_2 | p) = 2 \) prob. \( \frac{1}{2} \)

= \( p_1 \cdot p_2 \cdot p_3 \) with prob. \( \frac{1}{6} \)

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

Same probabilities: Let \( g \) be a random elt. of 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)