Intro to Wed.

On Monday, we proved Dedekind domains admit unique factorization of ideals into prime ideals.

proof keys: combination of Noetherian condition and fact that maximal / prime ideals are "invertible" (i.e. set $\mathfrak{p}^{-1} = \{ x \in K \mid x\mathfrak{p} \subseteq \mathcal{O} \}$

and $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$, but $\mathfrak{p}$ maximal so $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathcal{O}$.)

Can we place this in larger framework where we have group law under multiplication of such sets?

The ideals of $\mathcal{O}_K$ may be multiplied, but they have no multiplicative inverses.

useful to consider <u>fractional</u> ideals : finitely generated $\mathcal{O}_K$-submodules $\mathfrak{a} \neq 0$ in K.

(since $\mathcal{O}_K$ Noetherian, a non-zero submodule $\mathfrak{a}$ is a fractional ideal of K

$\iff \exists\ c \in \mathcal{O}_K\ (\neq 0)$ s.t. $c \cdot \mathfrak{a} \subseteq \mathcal{O}_K$, is an ideal.

So this justifies the name.)

$\Rightarrow$: generators $x_1, \dots, x_n$ for $\mathfrak{a}$ in K can be written as $x_i = \frac{y_i}{c}$, common denom $c \in \mathcal{O}_K\ \forall i$.

$\Leftarrow$: $\mathfrak{a} = c^{-1} \cdot \mathfrak{b}$ for integral ideal $\mathfrak{b}$ so $\mathfrak{a}$ is finitely generated since $\mathcal{O}_K$ Noetherian

⟶ DO EXAMPLES FIRST ⟶

(fractional)

Proposition : The fractional ideals form an (abelian) gp under multiplication of ideals.

(So elts of product are finite sums of products, as before).

identity elt. in the gp. is ideal $\mathcal{O}_K = (1)$, and given fractional ideal $\mathfrak{a}$, its inverse is $\mathfrak{a}^{-1} = \{ x \in K \mid x \cdot \mathfrak{a} \subseteq \mathcal{O}_K \}$. (*)

pf : Just need to check inverses. If $\mathfrak{a}$ integral, then write $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ and then $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$ since $\mathfrak{p}^{-1}\mathfrak{p} \supsetneq \mathfrak{p}$ (Lemma 2) so $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$ (maximality of $\mathfrak{p}$)

Why is $\mathfrak{b} = \mathfrak{a}^{-1}$ as defined above in this case?

since $\mathfrak{b}\mathfrak{a} = \mathcal{O}_K$, then $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. If $x \in \mathfrak{a}^{-1}$ so $x \cdot \mathfrak{a} \subseteq \mathcal{O}_K$

then $x\,\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b} \Rightarrow x \in \mathfrak{b}$ since $\mathfrak{a}\mathfrak{b} = \mathcal{O}_K$. ✓

here $(c\mathfrak{a})^{-1}$ and $\mathfrak{a}^{-1}$ as defined in (*)

If $\mathfrak{a}$ fractional, $\exists\ c \in \mathcal{O}_K$ with $c \cdot \mathfrak{a} \subseteq \mathcal{O}_K$, so since $(c\mathfrak{a})^{-1} = c^{-1} \cdot \mathfrak{a}^{-1}$ is inverse of $c\mathfrak{a}$

where c really denotes principal ideal (c)

then $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$ as desired.

Examples : (0) any integral ideal is fractional

(1) Given elt $\alpha = \frac{a}{b} \in K$ then $\alpha \mathcal{O}_K$ is fractional, since $b \cdot \alpha \subseteq \mathcal{O}_K$

or equally simply, its a 1-dim'l $\mathcal{O}_K$-submodule of K.

" principal fractional ideals "

(2) $\mathfrak{p}^{-1} := \{ x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}_K \}$ is fractional.

clearly, it is an $\mathcal{O}_K$-module. Any non-zero elt. of $\mathfrak{p}$ serves as common denominator of elements of $\mathfrak{p}^{-1}$.

Corollary : Every fractional ideal $\mathfrak{a}$ admits unique factorization as product of (finitely many) prime ideals having integer exponents. (Equivalently, the gp of fractional ideals is free gp. with generators in bijection with (non-zero) prime ideals of $\mathcal{O}_K$.)

Consider the following exact sequence

$$1 \to \underbrace{\mathcal{O}_K^\times}_{\text{units}} \to \underbrace{K^\times}_{\text{principal fractional ideals}} \to \underbrace{J_K}_{\text{gp. of fract. ideals}} \to J_K/K^\times \to 1$$

Neukirch : unit gp. measures ~~expansion~~ contraction in moving from numbers/elts $\to$ ideals $K^\times \to J_K$

"class gp" $J_K/K^\times$ measures expansion in moving from numbers $\to$ ideals.

$\mathcal{O}_K$: arb. Dedekind domain, then can't say much. But if $\mathcal{O}_K$: ring of ints. of $K/\mathbb{Q}$ then we get finiteness results. Their study forms remainder of our first unit.

Want to prove first that class gp. $J_K / K^\times$ is finite.

Do this by counting problem with lattices. Define "absolute norm" of ideal $\mathfrak{a}$ by $N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$.

so by theory of free-modules over P.I.D., then this index is finite.

Recall that same pf showing $\mathcal{O}_K$ is free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$ shows any $\mathcal{O}_K$-submodule in K is free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$ (Prop. 2.10 in Neukirch)

This generalizes notion of norm of element:

If $\alpha \in \mathcal{O}_K$, then

$$N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$$

pf: If $\omega_1, \dots, \omega_n$ is integral basis for $\mathcal{O}_K$ as $\mathbb{Z}$-module, then $\alpha\omega_1, \dots, \alpha\omega_n$ is a basis for $(\alpha) = \alpha \cdot \mathcal{O}_K$

Write $\alpha\omega_i = \sum_j a_{ij}\omega_j$. Then $N_{K/\mathbb{Q}}(\alpha) = \det(T_\alpha) = \det(a_{ij})$

But (a_{ij}) matrix also gives change of basis from (α) to $\mathcal{O}_K$, so by classification of modules over a P.I.D., ~~the~~ is $[\mathcal{O}_K : (\alpha)] = N((\alpha))$.
$|\det(a_{ij})|$

Proposition: if $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ is prime factorization, then $N(\mathfrak{a}) = N(\mathfrak{p}_1)^{\nu_1} \cdots N(\mathfrak{p}_r)^{\nu_r}$, and hence "absolute norm" is multiplicative function on ideals: $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

pf: Chinese remainder thm gives $\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r}$

which immediately reduces to case where $\mathfrak{a}$ is power of single prime ideal.
(proof of CRT identical to one over integers) (3.6 in Neukirch)

Now $N(\mathfrak{p}^\nu) \overset{\text{def}}{=} [\mathcal{O}_K : \mathfrak{p}^\nu] = [\mathcal{O}_K:\mathfrak{p}][\mathfrak{p}:\mathfrak{p}^2]\cdots[\mathfrak{p}^{\nu-1}:\mathfrak{p}^\nu]$

so done if we can show $\mathfrak{p}^i/\mathfrak{p}^{i+1} \simeq \mathcal{O}_K/\mathfrak{p}$ $\forall\ i = 1,\dots,\nu-1$.

Know $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$, by uniqueness of prime factorization. Take elt $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, consider ideal $\mathfrak{b} = (a) + \mathfrak{p}^{i+1}$ then $\mathfrak{p}^{i+1} \subsetneq \mathfrak{b} \subseteq \mathfrak{p}^i$

Claim: $\mathfrak{p}^i = \mathfrak{b}$ pf: else $\mathfrak{b}\mathfrak{p}^{-i}$ is a proper divisor of $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$ and $\mathfrak{p}$ maximal. ↯.

So $a \pmod{\mathfrak{p}^{i+1}}$ is one-dim'l basis for $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ as $\mathcal{O}_K/\mathfrak{p}$ vector space, i.e. $\mathfrak{p}^i/\mathfrak{p}^{i+1} \simeq \mathcal{O}_K/\mathfrak{p}$ as desired.

So absolute norm N is group homomorphism (upon extending definition to fractional ideals)

$$N : J_K \longrightarrow \mathbb{R}_+^\times$$

Thm: $J_K/K^\times$ is finite gp. (Its order is called "class number of K")

pf: Given non-zero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ then $\mathfrak{p} \cap \mathbb{Z} = (p)$ ← meaning $p\cdot\mathbb{Z}$, p: rational prime

and $\mathcal{O}_K/\mathfrak{p}$ is finite extension of field $\mathbb{Z}/p\mathbb{Z}$ so is a finite field itself, say with p^f elements some f.

i.e. $N(\mathfrak{p}) = p^f$. Moreover the $\mathcal{O}_K$ ideal $p\cdot\mathcal{O}_K = \mathfrak{p}_1^{\nu_1}\cdots\mathfrak{p}_r^{\nu_r}$ so only finitely many prime ideals can have $\mathfrak{p} \cap \mathbb{Z} = p\cdot\mathbb{Z}$ (which implies $\mathfrak{p} \mid p\cdot\mathcal{O}_K$.)

$\Rightarrow$ Only finitely many prime ideals have absolute norm bounded by fixed constant