Lecture 9, 25.1.

Recall: For $0 \neq m \in \mathbb{Z}$ we defined

$$G_m := \{ x \in G_L \mid m^k x \in G \text{ for some } k \} = \{ \tfrac{y}{m^k} \mid y \in G, k \in \mathbb{N} \}$$

Lemma 5.16

a) G_m is an order containing G.

b) $[G_m : G] \mid m^k$ and $\gcd([G_L : G_m], m) = 1$

Proof of Lemma:

Clearly $G \subseteq G_m$. Show that G_m is a ring.

Let $x, y \in G_m$. Then $m^k x, m^l y \in G$ for some k, l. $\Rightarrow$

$m^{\max(k,l)}(x+y) \in G \Rightarrow x+y \in G_m$.

$m^{l+k} xy \in G \Rightarrow xy \in G_m$

So G_m a ring. Since $G_m \subseteq G_L$ by definition and G_L is a f.g. $\mathbb{Z}$-module and $\mathbb{Z}$ noetherian $\Rightarrow G_m$ f.g. $\mathbb{Z}$-module

$\Rightarrow G_m$ an order.

Let $\alpha_1, \dots, \alpha_n$ be a basis of G_m. For each i there is k_i s.t.

$m^{k_i} \alpha_i \in G$. Let $k := \max\{k_i\} \Rightarrow m^k \alpha_i \in G \; \forall i$

$\Rightarrow \quad m^k G_m \subseteq G \subseteq G_m$

$$\Rightarrow [G_m : G] \cdot [G : m^k G_m] = [G_m : m^k G_m] = m^{kn}.$$

Suppose $c := \gcd([G_L : G_m], m) \neq 1$. The there is $x \in G_L \setminus G_m$

$cx \in G_m \rightsquigarrow m^k c x \in G$ for some $k \underset{c \mid m}{\Rightarrow} m^{k+1} x \in G \Rightarrow x \in G_m$ ↯. $\square$

Now discuss how to obtain G_p. To this end, we first recall a few bits about prime ideals.

5.4 Review of prime ideals and radicals

R a commutative ring.

Lemma 5.17: For an ideal $P \subseteq R$ TFAE:

a) R/P is an integral domain

b) if $x, y \in R$ s.t. $xy \in P$, then $x \in P$ or $y \in P$.

$\square$

The set of all prime ideals is denoted by $\operatorname{Spec} R$.

Remark 5.18:

a) Maximal ideals are prime.

b) Ideals generated by a prime element are prime.

c) For an ideal $I \subseteq R$, $\operatorname{Spec}(R/I) \overset{1:1}{\longleftrightarrow} \{P \in \operatorname{Spec} R \mid P \supseteq I\}$.

d) If $\varphi: R \to S$ is a ring morphism, then φ induces a map

$$\begin{array}{ccc} \operatorname{Spec} S & & Q \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & & \varphi^{-1}(Q) \end{array}$$

Def 5.19: The radical of an ideal I of R is

$$\operatorname{rad}(I) := \{x \in R \mid x^n \in I \text{ for some } n \in \mathbb{N}\}$$

Lemma 5.20:

a) If $S \subseteq R$ is a multiplicatively closed subset, $0 \notin S$. Then for I an ideal in R the set $\{I \trianglelefteq R \mid I \cap S = \emptyset\}$ has a maximal element, and this is a prime ideal of R.

b) x nilpotent $\Leftrightarrow x \in \bigcap_{P \in \operatorname{Spec} R} P$

c) $\operatorname{rad}(I) = \bigcap_{\substack{P \in \operatorname{Spec} R \\ P \supseteq I}} P$. In particular, $\operatorname{rad}(I)$ is an ideal.

Proof (skipped because everyone said obvious...)

a) Let $\mathcal{M} := \{ I \trianglelefteq R \mid I \cap S = \emptyset \}$. Then $(0) \in \mathcal{M}$, so $\mathcal{M} \neq \emptyset$.

If $I_1 \subseteq I_2 \subseteq \ldots \subseteq$ is a chain in $\mathcal{M}$, then $\bigcup_{i \in \mathbb{N}} I_i \in \mathcal{M}$, and this is an upper bound $\Rightarrow$ $\mathcal{M}$ has a maximal element P by Zorn's Lemma.

Need to show that P is prime: Suppose $xy \in P$ but $x, y \notin P$. Then $(x, P), (y, P) \supsetneq P$. Hence, by maximality of P, $(x, P) \cap S \neq \emptyset \neq (y, P)$.

$\Rightarrow rx + p = s, \quad r'y + p' = s'$

for some $s, s' \in S$, $p, p' \in R$, $r, r' \in R$.

Since S multiplicatively closed $\Rightarrow$

$$S \ni ss' = (rx + p)(r'y + p') = rr'xy + rxp' + pr'y + pp' \in P \ \lightning$$

$\Rightarrow x \in P$ or $y \in P \Rightarrow P$ prime

b) $x^n = 0$ for some $n \Rightarrow x \cdot x^{n-1} = 0 \in P \Rightarrow x \in P$ or $x^{n-1} \in P \Rightarrow$ inductively $x \in P$
$\Rightarrow x \in \bigcap P$.

Suppose $x \in R$ not nilpotent. Consider $S := \{ x^n \mid n \in \mathbb{N} \}$. By a) there is $P \in \operatorname{Spec} R$, $P \cap S = \emptyset$. $\Rightarrow x \notin P$.

c) Under $\pi : R \to R/I$, $\operatorname{rad}(I)$ corresponds precisely to the nilpotent elements in R/I, hence by b:

$$\pi(\operatorname{rad}(I)) = \bigcap_{P \in \operatorname{Spec} R/I} P$$

$$\Rightarrow \quad \operatorname{rad}(P) = \bigcap_{\substack{P \in \operatorname{Spec} R \\ P \supseteq I}} P$$

$\square$

5.5 Primes in an order

Back to an order $\mathcal{O}$.

Prop 5.21:

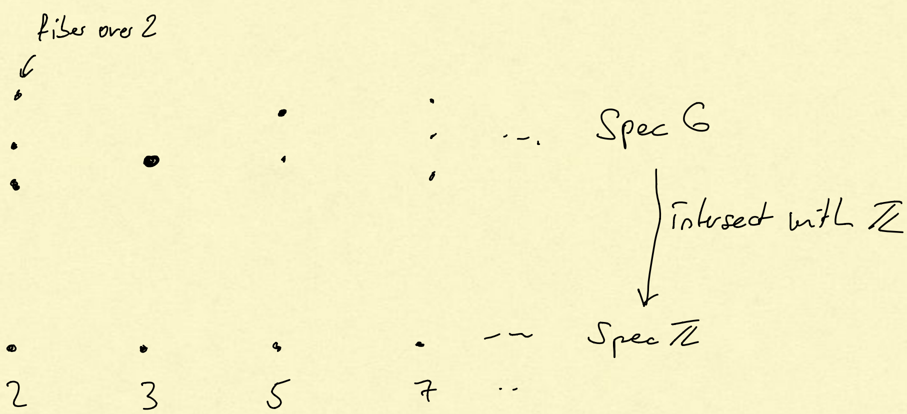
a) For every $P \in \operatorname{Spec} \mathcal{O}$, $P \cap \mathbb{Z} = (p) \in \operatorname{Spec} \mathbb{Z}$ (one says "P lies over p")

b) $\{\text{Primes above } p\} \overset{1:1}{\longleftrightarrow} \operatorname{Spec} \mathcal{O}/p\mathcal{O}$.

c) Every non-zero prime ideal of $\mathcal{O}$ is already maximal
($\mathcal{O}$ is "one-dimensional").

d) For every prime number $p \in \mathbb{Z}$ there is at least one and there are at most $\dim_{\mathbb{Q}} L$ many primes $P \in \operatorname{Spec} \mathcal{O}$ above p.

Picture



Proof:

a) $P \cap \mathbb{Z} = \varphi^{-1}(P) \in \operatorname{Spec} \mathbb{Z}$, where $\varphi: \mathbb{Z} \hookrightarrow \mathcal{O}$ is the inclusion.

b) $\operatorname{Spec} \mathcal{O}/p\mathcal{O} \cong \{P \in \operatorname{Spec} \mathcal{O} \mid P \supseteq p\mathcal{O}\}$. If $P \supseteq p\mathcal{O}$, then $P \cap \mathbb{Z} \supseteq p\mathcal{O} \cap \mathbb{Z} \supseteq p\mathbb{Z}$.
Since $P \cap \mathbb{Z} \in \operatorname{Spec} \mathbb{Z}$ and $(p) \in \operatorname{Spec} \mathbb{Z}$ is maximal, $P \cap \mathbb{Z} = p\mathbb{Z}$.
Conversely, if $P \cap \mathbb{Z} = (p) \rightsquigarrow P \supseteq p\mathcal{O}$.

c) Let $P \cap \mathbb{Z} = (p)$. Then $\mathcal{O}/p$ is a $\mathbb{Z}/(p) = \mathbb{F}_p$-module, generated by $n = \dim_{\mathbb{Z}} \mathcal{O} = \dim_{\mathbb{Q}} L$ elements.
$\rightsquigarrow \dim_{\mathbb{F}_p} \mathcal{O}/p = n < \infty$. $\Rightarrow \mathcal{O}/p$ is a finite-dimensional $\mathbb{F}_p$-algebra

Moreover, since P prime $\Rightarrow G/P$ is an integral domain.

Then G/P is already a field because:

<u>Claim</u>: If A is a finite-dimensional algebra over a field K and A is an integral domain, then A is already a field.

<u>Proof</u>: Let $0 \neq a \in A$. The multiplication map $A \to A, x \mapsto ax$ is a vector space endomorphism. It is injective since A is an integral domain $\Rightarrow$ it is surjective $\Rightarrow \exists x \in A: ax = 1$ $\square$

$\Rightarrow P$ maximal.

d) $pG \neq G \Rightarrow G/pG \neq 0 \Rightarrow$ has a maximal (and thus) a prime ideal.

G/pG is a $\mathbb{Z}/(p) = \mathbb{F}_p$-module of dimension $\leq n = \dim_{\mathbb{Q}} L$ (in fact $=$).

By b, all prime ideals of G/pG are maximal.

Let $M_1, \dots, M_r$ be distinct maximal ideals of G/pG

By Chinese Remainder

$$G/pG \twoheadrightarrow G/M_1 \times \dots \times G/M_r$$

surjective morphism of $\mathbb{Z}/(p) = \mathbb{F}_p$-algebras

$$\Rightarrow r \leq \dim_{\mathbb{F}_p} G/pG \leq n$$

$\square$

<u>Remark 5.22</u>: The proposition is just a special case of the general behavior of primes in integral ring extensions.

5.6 The round-2 algorithm (theory)

Remember: The goal is to find the p-maximal overorder $\mathcal{O}_p$ for $p^2 \mid d_{\mathcal{O}}$.

Generalizing Thm 3.68:

Lemma 5.23:

If $0 \neq I \subseteq \mathcal{O}$ is an ideal, then I is a free $\mathbb{Z}$-module of dimension n.

Proof:

$\mathcal{O}$ is free of dimension n by definition. Since $\mathcal{O}$ noetherian, I is a f.g. $\mathbb{Z}$-module; obviously torsion-free, thus free by Thm 3.66.

Let $\alpha_1, \dots, \alpha_n$ be a basis of $\mathcal{O}$. Let $0 \neq x \in I$. Then $x\alpha_1, \dots, x\alpha_n \in I$.

These are linearly independent $\Rightarrow \dim_{\mathbb{Z}} I \geq n$.

Since $I \subseteq \mathcal{O} \Rightarrow \dim_{\mathbb{Z}} I \leq \dim_{\mathbb{Z}} \mathcal{O} = n \Rightarrow \dim_{\mathbb{Z}} I = n$.

$\square$

Prop 5.24:

Let $I \subseteq \mathcal{O}$ be an ideal. Then

$$[I/I] := \{ x \in \overset{\overset{Q(\mathcal{O})}{\shortparallel}}{L} \mid xI \subseteq I \}$$

is an order in L containing $\mathcal{O}$. It is called the ring of multipliers of I.

Proof: Since I is an ideal, $\mathcal{O} \subseteq [I/I]$. Let $x, y \in [I/I]$. Then $xI \subseteq I$, $yI \subseteq I$, hence $xyI \subseteq I$ and $(x+y)I \subseteq I \Rightarrow xy, x+y \in [I/I]$.

I is a free $\mathbb{Z}$-module of rank n by Lemma 5.23.

$\rightsquigarrow N := [\mathcal{O} : I]$ is finite. Then $N \cdot \mathcal{O} \subseteq I \rightsquigarrow N = N \cdot 1 \in I$

Hence,

$$[I/I] = \{ x \in L \mid xI \subseteq I \} \subseteq \{ x \in L \mid x \cdot N \subseteq I \} \subseteq \{ x \in L \mid x \cdot N \subseteq \mathcal{O} \}$$

$$= \frac{1}{N} \cdot \mathcal{O} \leftarrow \text{this is a free } \mathbb{Z}\text{-module of the same dimension as } \mathcal{O}, \text{ in particular finitely generated.}$$

This implies that $[I/I]$ is a f.g. $\mathbb{Z}$-module $\Rightarrow [I/I]$ is an order. $\square$

Def 5.25:

Let $p \in \mathbb{Z}$ be a prime number. The p-radical of G is

$$\mathrm{rad}_p(G) := \mathrm{rad}(pG) \overset{\text{Lemma 5.20}}{=} \bigcap_{\substack{P \in \mathrm{Spec}\, G \\ P \supseteq pG}} P \;\; = \prod_{\substack{P \in \mathrm{Spec}\, G \\ P \supseteq pG}} P$$

because all P maximal by Lemma 5.21, thus pairwise coprime.

Corollary 5.26:

$\mathrm{mul}_p(G) := [\mathrm{rad}_p(G)/\mathrm{rad}_p(G)]$ is an order containing G and $[\mathrm{mul}_p(G) : G] = p^k$ for some $k \leq n$. In particular, $\mathrm{mul}_p(G)$ is contained in G_p, the p-maximal overorder of G.

dim $\mathbb{Q}L$

We call $\mathrm{mul}_p(G)$ the p-multiplier of G.

Proof: First part from Prop 5.24. For second part note that if $x \in \mathrm{mul}_p G$, then $x \cdot \mathrm{rad}_p G \subseteq \mathrm{rad}_p G \subseteq G$ by definition. Since $p \in \mathrm{rad}_p G$

$\Rightarrow p \cdot \mathrm{mul}_p G \subseteq G \Rightarrow \mathrm{mul}_p G \subseteq \frac{1}{p} G$.

We have

$$p^n = [\tfrac{1}{p}G : G] = [\tfrac{1}{p}G : \mathrm{mul}_p G] \cdot [\mathrm{mul}_p G : G] \Rightarrow [\mathrm{mul}_p G : G] \text{ divides } p^n.$$

$\square$

Thm 5.27 (p-maximality criterion) $G_p = G \iff \mathrm{mul}_p G = G$.

Before we prove this, note what this implies: