Lecture 20 (15.1)

Recall from Prop 5.21 that if $P \subseteq R$ is a non-zero prime ideal, then $P \cap \mathbb{Z} = (p)$ for a prime number p (we say that P is lying over p).

Lemma 8.25

If P is lying over p, then $N(P) = p^k$ for some $k \le n = \dim_{\mathbb{Q}} L$.

Proof: We have $pR \subseteq P \Rightarrow [R:P] = N(P)$ divides $[R:pR]$.

R/pR is an $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ - vector space, and from Prop 5.21 we know that $\dim_{\mathbb{F}_p} R/pR \le n$.

Hence, $[R:pR] = p^l$ for some $l \le n$. $\Rightarrow [R:P] = p^k$ for some $k \le l$. □

The following is very important:

Lemma 8.26

In every non-zero ideal $I \subseteq R$ there is an element $0 \neq \omega \in I$ with

$$|N_{L|\mathbb{Q}}(\omega)| \le \underbrace{\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_L|}}_{=:M_L} \cdot N(I)$$

Minkowski bound

Proof: As in Exescise 7.1: for $\lambda \in \mathbb{R}_{>0}$ consider the set

$$E_\lambda := \left\{ x \in \mathbb{R}^{r+2s} \;\middle|\; |x_1| + \dots + |x_r| + \sqrt{2}(x_{r+1}^2 + x_{r+2}^2)^{1/2} + \dots + \sqrt{2}(x_{r+2s-1}^2 + x_{r+s}^2)^{1/2} \le \lambda \right\}$$

If $\omega \in G$ and $j(\omega) \in E_\lambda$, then by definition of E_λ and j:

$$|\sigma_1(\omega)| + \dots + |\sigma_r(\omega)| + \sqrt{2}\Big((\sqrt{2}\,\mathrm{Re}\,\sigma_{r+1}(\omega))^2 + (\sqrt{2}\,\mathrm{Im}\,\sigma_{r+1}(\omega)\Big)^2 + \overset{\text{up to } \sigma_{r+s}}{\dots} \le \lambda$$

$$\Rightarrow |\sigma_1(\omega)| + \dots + |\sigma_r(\omega)| + \sqrt{2}\left(2|\sigma_{r+1}(\omega)|^2\right)^{1/2} + \dots \le \lambda$$

$$\Rightarrow |\sigma_1(\omega)| + \dots + |\sigma_r(\omega)| + 2|\sigma_{r+1}(\omega)| + \dots \le \lambda$$

$$\Rightarrow \sum_{i=1}^{n=r+2s} |\sigma_i(\omega)| \le \lambda \qquad \left(\text{recall } \sigma_{r+i} = \overline{\sigma_{r+s+i}}\right)$$

$$\Rightarrow |N_{L|\mathbb{Q}}(\omega)|^{1/n} = \left(\prod_{i=1}^{n} |\sigma_i(\omega)|\right)^{1/n} \underset{\substack{\text{inequality of geometric} \\ \text{and arithmetic mean}}}{\le} \frac{1}{n}\sum_{i=1}^{n} |\sigma_i(\omega)| \le \frac{1}{n}\lambda$$

2

$$\Rightarrow |N_{L|\mathbb{Q}}(\omega)| \leq n^{-n}\lambda^n.$$

One can compute that

$$vol(E_\lambda) = \frac{2^r \pi^s}{n!}\lambda^n$$

Let $\Lambda := j(I) \subseteq \mathbb{R}^{r+2s}$, a lattice with $d(j(I)) = d(j(R))\cdot[R:I] = \sqrt{|d_L|}\cdot N(I)$

Choose

$$\lambda := \left(n!\left(\frac{4}{\pi}\right)^s d(\Lambda)\right)^{1/n}$$

Then

$$vol(E_\lambda) \leq 2^n d(\Lambda).$$

Hence, by Minkowski's theorem (Thm 6.18), there is a non-zero $\omega \in I$ with $j(\omega) \in E_\lambda$

By above, we have

$$|N_{L|\mathbb{Q}}(\omega)| \leq n^{-n}\lambda^n = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s d(\Lambda) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_L|}\cdot N(I).$$

□

<u>Prop 8.27</u> 7

Every ideal class of R has a representative $I \subseteq R$ such that $N(I) \leq M_L$.

<u>Proof:</u>

Let J be a non-zero fractional ideal. There exists $0 \neq r \in R$ such that $C := rJ^{-1} \subseteq R$.

By Lemma 8.26 there is $0 \neq \omega \in C$ with $N(C)\, M_L \geq |N_{L|\mathbb{Q}}(\omega)|$.

Since $\omega \in C \Rightarrow (\omega) \subseteq C \Rightarrow C \mid (\omega)$, i.e. $\exists$ an ideal $I \subseteq R$ with $IC = (\omega)$ (see Exercise 10.1). Now

$$M_L \geq |N_{L|\mathbb{Q}}(\omega)|\cdot N(C)^{-1} \overset{8.23, 8.24}{=} N((\omega))\cdot N(C^{-1}) \overset{8.24}{=} N((\omega)\cdot C^{-1}) = N(I)$$

We have

$$I \subseteq R,\ N(I) \leq M_L,\ I = \omega C^{-1} = \omega r^{-1} J$$

$$\Rightarrow I \equiv J \bmod P_R, \text{ i.e. } I = J \text{ in } Cl_R.$$

□

Let $I \subseteq R$ be a non-zero ideal with factorization $I = P_1^{\nu_1} \cdots P_r^{\nu_r}$. Then

$$N(I) = \prod_{i=1}^{r} p_i^{k_i \nu_i},$$

where $N(P_i) = p_i^{k_i}$, see Lemma 8.25. If $N(I) \leq M_L$, then

$$\prod_{i=1}^{r} p_i^{k_i \nu_i} \leq M_L$$

Hence, there can only be finitely many such I! Prop 8.27 thus implies:

Thm 8.28

The class group Cl_R is finite. □

Remark 8.29

The above also gives an idea how to compute Cl_R:

1. Compute the Minkowski bound M_L and find all primes $p_1, \ldots, p_r \leq M_L$.
2. Determin the prime ideals $P_{i,j}$ of R lying above the p_i, i.e. factorize $p_i R$ (only finitely many ideals).
3. Determine all products (including powers) of the P_{ij} whose norm is $\leq M_L$. This will give representatives of all elements of Cl_R. ⑧
4. Find the relations between the representatives: this is essentially about testing if ideals are principal, namely:

   ideals $I, J \subseteq R$ are equal in $Cl_R \iff IJ^{-1} = \alpha R$ for some $\underline{\alpha \in K}$.

   Since IJ^{-1} is a fractional ideal, there is $r \in R \setminus \{0\}$ such that $rIJ^{-1} =: C \subseteq R$.

   Then

   $$I = J \text{ in } Cl_R \iff C = r\alpha R \text{ for some } \alpha \in K$$

   Since $C \subseteq R \Rightarrow \gamma := r\alpha \in R$, so

   $$I = J \text{ in } Cl_R \iff C = (\gamma) \text{ for some } \underline{\gamma \in R}.$$

   The following lemma helps to test this.

Lemma 8.30

An ideal $C \subseteq R$ is principal iff there is $\gamma \in C$ such that $N(C) = |N_{L|\mathbb{Q}}(\gamma)|$.

Proof: If $C = (\gamma)$, then $N(C) = |N(\gamma)|$ by Lemma 8.23. Conversely, assume that $\gamma \in C$ with $N(C) = |N_{L|\mathbb{Q}}(\gamma)|$. Since $(\gamma) \subseteq C \Rightarrow C \mid (\gamma)$, hence there is an ideal C' with $C = (\gamma) C'$.

$$|N_{L|\mathbb{Q}}(\gamma)| = N(C) \overset{8.23}{=} N((\gamma)) N(C') = |N_{L|\mathbb{Q}}(\gamma)| N(C') \Rightarrow [R : C'] = N(C') = \underline{1}$$

$$\Rightarrow C' = R \Rightarrow C = (\gamma). \quad \square$$

The condition $|N(\gamma)| = N(C)$ will be some Diophantine equation which can be difficult to check for solvability (but there are effective algorithms).

Exercise 10.3 has some very simple examples of class groups.

Two basic problems:

1. understand how prime number split into prime ideals in R
2. find relations.

8.4 Ramification theory

To have some fun, we consider a more general situation again: R is a Dedekind domain with fraction field K, $L \supseteq K$ is a finite separable extension and S is the integral closure of R in S. Standard application will be $R = \mathbb{Z}$, L a number field $\rightsquigarrow S = \mathcal{O}_L$.

Lemma 8.31

S is a Dedekind domain, and $S \cap K = R$.

Proof:
S is integrally closed by Lemma 3.31. By Thm 3.47, S is a finitely generated R-module, hence noetherian since R is noetherian. If $0 \neq Q \in \operatorname{Spec} S$, then $Q \cap R = P \in \operatorname{Spec} R$ since $Q \cap R = \varphi^{-1}(Q)$, where $\varphi : R \to S$ is the inclusion. Since $R \subseteq S$ is finite, $R/P \subset S/Q$ is finite. Since R one-dimensional, R/P is a field, so S/Q is an integral domain which is a finite-dimensional algebra over a field $\Rightarrow S/Q$ is a field by sub-claim in proof of Prop 5.21c.
$\Rightarrow Q$ maximal $\Rightarrow S$ one-dimensional. $\square$

Elements of $S \cap K$ are integral over R and contained in $K \Rightarrow$ contained in R since R is integrally closed. $\square$

Remark 8.32

In general it is not true that S is a *free* R-module. This holds for example if S is a PID (see Thm 3.68).

Lemma 8.33

For $0 \neq P \in \operatorname{Spec} R$ and $Q \in \operatorname{Spec} S$ the following are equivalent:

a) $P \subseteq Q$, b) $Q \mid PS$, c) $P = Q \cap R$

In this case we say that Q is *lying over* P.

Proof: $a \Leftrightarrow b$ is Exercise 10.1a. If $P \subseteq Q$, then $P \subseteq Q \cap R$. Since $Q \cap R \in \operatorname{Spec} S$, must have $P = Q \cap R$ since R one-dimensional. If $P = Q \cap R$, clearly $P \subseteq Q$. $\square$