Algebraic Number Theory

Lecture 11, 17th December 2021

Last lecture

$\mathfrak{a} \neq (0)$ be an ideal in $\mathcal{O}_K$.

$\mathcal{N}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = |\mathcal{O}_K/\mathfrak{a}|$, <u>absolute norm</u> of $\mathfrak{a}$.

$\mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$.

$$\mathcal{N} : J_K \longrightarrow \mathbb{Q}^\times_{>0}$$
$$\frac{\mathfrak{a}}{\mathfrak{b}} \longmapsto \frac{\mathcal{N}(\mathfrak{a})}{\mathcal{N}(\mathfrak{b})}$$

<u>Lemma 7.5</u> In every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$ there exists an $a \in \mathfrak{a}$, $a \neq 0$, with

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, \mathcal{N}(\mathfrak{a}).$$

<u>Theorem 7.6</u> The ideal class group $Cl_K = J_K/P_K$ is finite. Its order

$$h_K = |Cl_K|$$

is called the <u>class number</u> of K.

Proof sketch: 1) For any $M \in \mathbb{R}$ there are just fin. many $\mathfrak{a} \subset \mathcal{O}_K$ with $\mathcal{N}(\mathfrak{a}) \leq M$

2) For $M := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$ every class $[\mathfrak{a}] \in Cl_K$ contains an ideal $\mathfrak{a}_1 \in [\mathfrak{a}]$ with $\mathcal{N}(\mathfrak{a}_1) \leq M$.

Example 7.7 Let $K = \mathbb{Q}(\sqrt{-5})$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ has integral basis $\{1, \sqrt{-5}\}$ and $r = 0$, $s = 1$

$\tau_{1,2}: a + b\sqrt{-5} \mapsto a \pm b\sqrt{-5}$

$$d_K = \det\begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}^2 = (-2\sqrt{-5})^2 = -20.$$

$$\left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} = \frac{2}{\pi}\sqrt{20} \approx 2.85\ldots$$

Every class of Cl_K therefore contains an ideal $\mathfrak{a}$ with $N(\mathfrak{a}) \leq 2$. If $N(\mathfrak{a}) = 1$ then $\mathfrak{a} = \mathcal{O}_K$.

If $\underset{\substack{\| \\ |\mathcal{O}_K/\mathfrak{a}|}}{N(\mathfrak{a})} = 2$, then $2 \in \mathfrak{a}$, i.e $\mathfrak{a} \mid (2)$.

The prime factorization of (2) is

$$(2) = (\underbrace{2, 1+\sqrt{-5}}_{\mathfrak{p}})^2$$

and $N(\mathfrak{p}) = 2$. This shows that $(2, 1+\sqrt{-5})$ is the only ideal of norm 2.

This shows $h_K \leq 2$ and since $\mathbb{Z}[\sqrt{-5}]$ is not a PID/UFD we have $h_K > 1 \Rightarrow h_K = 2$.

A better bound for the norm is given by the following:

Theorem 7.8 (Minkowski bound)
Every class of Cl_K contains an integral ideal $\mathfrak{a} \subset \mathcal{O}_K$ with

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

Proof: Can be shown by proving a refinement of Thm 6.4, Lem 7.5 + Proof of Thm 7.6. (See Neukirch).

(In the example: $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} = \frac{2}{\pi}\sqrt{20}$ (same))

Class numbers for quadratic fields $K = \mathbb{Q}(\sqrt{d})$ (d squarefree)

$d<0$ (imaginary quadr. fields):

- Gauss class number problem (GCNP): For given $n \geq 1$ find all $d<0$ such that $h_{\mathbb{Q}(\sqrt{d})} = n$.
- Thm (Stark-Heegner theorem): For $n=1$ the only $d<0$ with $h_{\mathbb{Q}(\sqrt{d})}=1$ are

$$d \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\}.$$

- GCNP is solved for $n \leq 100$ (Watkins 2004)

$d>0$ (real quadratic fields):

<u>Conjecture</u> (Gauss) There are infinitely many $d>0$ with $h_{\mathbb{Q}(\sqrt{d})}=1$.

So far we do not even know if there are infinitely many number fields K with $h_K=1$.

There is also an "analytic" way to calculate the class number.

<u>Definition 7.9</u> The <u>Dedekind zeta function</u> of a number field K is defined by

$$\zeta_K(z) = \sum_{\substack{0\neq \mathfrak{a}\subseteq \mathcal{O}_K \\ \text{ideal}}} \frac{1}{N(\mathfrak{a})^z}.$$

<u>Remark 7.10</u>

i) $\zeta_K(z)$ converges abs. for $z\in\mathbb{C}$ with $\mathrm{Re}(z)>1$.

ii) ζ_K has an analytic continuation to $\mathbb{C}$ with a simple pole only at $z=1$.

iii) Due to the unique prime ideal factorization in $\mathcal{O}_K$ (Thm. 4.4) we have the Euler product

$$\zeta_K(z) = \prod_{\substack{(0)\neq \mathfrak{p}\subseteq \mathcal{O}_K \\ \text{prime}}} \frac{1}{1-N(\mathfrak{p})^{-z}}.$$

iv) In the case $K=\mathbb{Q}$ we have

$$\zeta_K(z)=\zeta(z)=\sum_{m>0}\frac{1}{m^z}=\prod_{p \text{ prime}}\frac{1}{1-p^{-z}}.$$

The connection to the class number is given due to the following result.

Theorem 7.10 (Analytic class number formula)

The residue of ζ_K at $z=1$ is given by

$$\lim_{z\to 1}(1-z)\zeta_K(z) = \frac{2^r (2\pi)^s h_K R_K}{\omega_K \sqrt{|d_K|}},$$

$$\lim_{z\to 1}(1-z)\zeta_K(z) = \operatorname{Res}_{z=1}\zeta_K(z)$$

r: # real emb
s: # pair of compl. emb.

where R_K = Regulator of K (will be part of Section 9)

ω_K = # roots of unity in K.

$$\left(K=\mathbb{Q}:\ \operatorname{Res}_{z=1}\zeta(z)=1 = \frac{2\cdot 1\cdot 1}{2\cdot 1}\right)$$

§ 8 Fermat's Last Theorem

Recall: For $n \geq 1$ the Fermat equation is

$$x^n + y^n = z^n. \qquad (FE)$$

We are interested in non-trivial ($x \cdot y \cdot z \neq 0$) solutions for (FE) with $x, y, z \in \mathbb{Z}$.

$n=1$: trivial

$n=2$: There are infinitely many non-trivial solutions (HW1, Ex4)

$n \geq 3$: Fermat claimed: There are no non-trivial solutions.
"Fermat's last theorem" (FLT)

Notice: Since $x^{ab} + y^{ab} = z^{ab} \Leftrightarrow (x^a)^b + (y^a)^b = (z^a)^b$ it suffices to consider the case $n=4$ in (FE) or n being an odd prime.

Theorem 8.1 (Fermat)
There are no nonzero solutions $x, y, z \in \mathbb{Z}$ for

$$x^4 + y^4 = z^2.$$

In particular FLT is true for $n=4$.

Proof: HW4. Use HW1 by writing $(x^2)^2 + (y^2)^2 = z^2$. $\square$

From now we assume $n = p \geq 3$ is an odd prime.

Let $\zeta_p = e^{\frac{2\pi i}{p}}$ be a primitive p-th root of unity.

Then $t^p - 1 = (t-1)(t-\zeta_p)(t-\zeta_p^2)\cdots(t-\zeta_p^{p-1})$.

in particular setting $t = -\frac{x}{y}$ and multiplying with $(-y)^p$ gives the factorization

$$x^p + y^p = \prod_{j=0}^{p-1} (x + \zeta_p^j y)$$

in the number field $K = \mathbb{Q}(\zeta_p)$.

One can show:
- The minimal polynomial of ζ_p is $1 + x + \ldots + x^{p-1}$, i.e $[K:\mathbb{Q}] = p-1$.
- We have $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

To prove FLT: show that $z^p = \prod_{j=0}^{p-1}(x + \zeta_p^j y)$ is not possible in $\mathcal{O}_K$ for $x \cdot y \cdot z \neq 0$.

This was done by Kummer for regular primes.

<u>Definition 8.2</u> A prime p is called <u>regular</u> if $p \nmid h_{\mathbb{Q}(\zeta_p)}$.

Theorem 8.3 (Kummer 1850)

i) If $n = p \geq 3$ is a regular prime then there are no non-trivial solutions to (FE).

i) A prime p is regular if and only if it does not divide the numerator of the Bernoulli numbers B_k for $k = 2, 4, \ldots, p-3$.

$$\left(\sum_{k \geq 0} \frac{B_k}{k!} X^k := \frac{X}{e^X - 1} \right)$$

Remark 8.4

i) Setting $h_p := h_{\mathbb{Q}(\zeta_p)}$ we have $h_p = 1$ for $p \leq 19$ and $h_{23} = 3$, $h_{37} = 37$, $h_{59} = 3 \cdot 59 \cdot 233$, $h_{67} = 67 \cdot 12739$.

All primes ≤ 100 are regular except for 37, 59 and 67.

ii) Conjecturally there are infinitely many regular primes (~60% of all primes). We know that there are infinitely irregular primes.

The reason regular primes are "special" is given by the following.

Lemma 8.5 Let $K = \mathbb{Q}(\zeta_p)$, $\mathfrak{a} \subset \mathcal{O}_K$ an ideal. If p is regular and $\mathfrak{a}^p$ is principal, then $\mathfrak{a}$ is also principal.

Proof: If $\mathfrak{a}^p$ is principal, then $[\mathfrak{a}^p] = [1]$ in Cl_K. But if $p \nmid |Cl_K| = h_K$, then we also need to have $[\mathfrak{a}] = [1]$, i.e $\mathfrak{a}$ is principal.

From now $\zeta := \zeta_p$.

Lemma 8.6

i) In $\mathbb{Z}[\zeta]$ the numbers $1-\zeta, 1-\zeta^2, \ldots, 1-\zeta^{p-1}$ are all associated and $1+\zeta$ is a unit.

ii) $p = u(1-\zeta)^{p-1}$ for some unit $u \in \mathbb{Z}[\zeta]^\times$ and $(1-\zeta)$ is the only prime ideal in $\mathbb{Z}[\zeta]$ dividing p.

Proof: See Keith Conrad: "FLT for regular primes" $\square$

Proof sketch/beginning of Thm 8.3 i):

We assume that $p \geq 3$ is a regular prime and

$$x^n + y^n = z^n$$

for coprime x, y, z with $x \cdot y \cdot z \neq 0$.

There are two cases: Case I: $p \nmid xyz$

Case II: $p \mid xyz$

We just sketch the first part of Case I.

The equation

$$z^p = x^p + y^p = \prod_{j=1}^{p-1} (x + \zeta^j y)$$

gives an equation of ideals

$$(z)^p = \prod_{j=1}^{p-1} (x + \zeta^j y). \qquad (*)$$

First we show that the ideals $(x + \zeta^j y)$ are relatively prime ideals. For $0 \leq j < j' \leq p-1$ a common factor $\mathfrak{p}$ of $(x + \zeta^j y)$ and $(x + \zeta^{j'} y)$ is also a factor of the difference

$$x + \zeta^j y - x - \zeta^{j'} y = \zeta^j y (1 - \zeta^{j'-j}) \underset{\text{Lemma 8.6 i)}}{=} v y (1 - \zeta)$$

for some unit $v \in \mathbb{Z}[\zeta]^\times$.

$$y(1-\zeta) \mid yp \implies \mathfrak{b} \mid (yp) \quad ((yp) \subseteq \mathfrak{b})$$

Lem. 8.6 ii)

We also have $\mathfrak{b} \mid (z)^p$ by (*). (assume $p \nmid xyz$)

Since yp and z^p are relatively prime we get that $\mathfrak{b} = (1) = \mathbb{Z}[\zeta]$, i.e. the $(x+\zeta^j y)$ are relatively prime.

By (*) and the unique prime factorization we get that $(j=1)$

$$(x+\zeta y) = \mathfrak{a}^p$$

for some ideal $\mathfrak{a}$.

p is <u>regular</u> and therefore

Lemma 8.5 $\implies$ $\underset{(t)}{\overset{\mathfrak{a}}{\shortparallel}}$ is a principal ideal. $t \in \mathbb{Z}[\zeta]$

$$\implies \quad x+\zeta y = u t^p \quad \text{for some unit } u \in \mathbb{Z}[\zeta]$$

One then shows with a bit more work that such an t can not exist if $p \nmid x \cdot y$.