# Lecture I: Number Fields 1

Thursday, May 24, 2018 9:58 PM

Q: Why number fields?

Early proof of Fermat's Last Theorem $x^p + y^p = z^p$ (p odd prime).

$\rightsquigarrow z^p = x^p - (-y)^p = (x+y)(x+\zeta_p y)\cdots(x+\zeta_p^{p-1}y)$ for $\zeta_p = e^{2\pi i/p}$

If the ring $\mathbb{Z}[\zeta_p]$ is a PID, can e.g. assume that $x, y$ coprime

almost $\Rightarrow x+\zeta_p^i y$ is a $p^{th}$ power.

Kummer: This works when $\mathbb{Z}[\zeta_p]$ is "close" to a PID.

(He proved FLT for $p<100$ except for three such $p$'s.)

Upshot: Studying bigger fields help understanding Diophantine equations over $\mathbb{Q}$ or $\mathbb{Z}$.

Number fields:

$F$ | finite ext'n $\mathbb{Q}$

by primitive elt thm.

Write $F = \mathbb{Q}(\alpha)$, where $\alpha$ is the zero of an irred. poly. $h(x) \in \mathbb{Q}[x]$

$\deg h(x) = [F:\mathbb{Q}] = n$ $\hookrightarrow$ all the zeros are $\alpha = \alpha_1, \dots, \alpha_n$

There are $n$ embeddings

$$\tau_1, \dots, \tau_n : F \simeq \mathbb{Q}[x]/(h(x)) \longrightarrow \mathbb{C}$$

$$\tau_i(c_0 + c_1 x + \dots + c_{n-1}x^{n-1}) := c_0 + c_1\alpha_i + \dots + c_{n-1}\alpha_i^{n-1}$$

E.g. $F = \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3-2)$

real embedding $\tau: \mathbb{Q}[x]/(x^3-2) \longrightarrow \mathbb{R} \subseteq \mathbb{C}$ — image lands in $\mathbb{R}$

$$x \longmapsto \sqrt[3]{2}$$

complex embeddings $\tau_2, \tau_3 : \mathbb{Q}[x]/(x^3-2) \longrightarrow \mathbb{C}$

$$x \overset{\tau_2}{\longmapsto} \zeta_3 \sqrt[3]{2}, \qquad x \overset{\tau_3}{\longmapsto} \zeta_3^{2}\cdot\sqrt[3]{2}$$

complex conj of each other

* In general, complex embeddings come in pairs.

- For $\alpha \in F$, define its trace to be $Tr_{F/\mathbb{Q}}(\alpha) := \tau_1(\alpha) + \dots + \tau_n(\alpha) \in \mathbb{Q}$

  its norm to be $Nm_{F/\mathbb{Q}}(\alpha) := \tau_1(\alpha)\cdots\tau_n(\alpha) \in \mathbb{Q}$

  e.g. $F = \mathbb{Q}(i)$, $Nm_{F/\mathbb{Q}}(x+iy) = (x+iy)(x-iy) = x^2+y^2$.

* If $F = \mathbb{Q}(\alpha)$ and $\alpha$ is the zero of irred. poly $h(x) = x^n + a_1 x^{n-1} + \dots + a_n$

then, $Tr_{F/\mathbb{Q}}(\alpha) = -a_1$, $Nm_{F/\mathbb{Q}}(\alpha) = (-1)^n a_n$.

- If $\alpha$ is not the field generator,

  e.g. $\alpha \in \mathbb{Q}$, $Tr_{F/\mathbb{Q}}(\alpha) = n\cdot\alpha$, $Nm_{F/\mathbb{Q}}(\alpha) = \alpha^n$

# Lecture I: Number Fields 2

Thursday, May 24, 2018 10:03 PM

Ring of integers:

$$\begin{array}{ccc} F = \mathbb{Q}(\alpha) & \supseteq & \mathcal{O}_F \\ | \text{ finite ext'n} & & | \\ \mathbb{Q} & \supseteq & \mathbb{Z} \end{array}$$

Say $\alpha$ is the zero of an irred. poly w/ coeffs in $\mathbb{Z}$.

Q: What's the best defn of $\mathcal{O}_F$?

* not $\mathbb{Z}[\alpha]$, b/c the choice of $\alpha$ is not canonical.

called the ring of integers of $F$ → $\mathcal{O}_F := \{\beta \in F ;$ the minimal monic poly. of $\beta$ in $\mathbb{Q}[x]$ has coeffs in $\mathbb{Z}\}$

$= \{\beta \in F ; \beta$ is a zero of a monic poly w/ coeffs in $\mathbb{Z}\}$

Fact: • $\mathcal{O}_F$ is a free $\mathbb{Z}$-module of rank $n = [F:\mathbb{Q}]$

i.e. $\exists\, \alpha_1, \cdots, \alpha_n \in \mathcal{O}_F$ s.t. $\mathcal{O}_F = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$

• For $\beta \in \mathcal{O}_F$, $Tr(\beta), Nm(\beta) \in \mathbb{Z}$.

Example: $F = \mathbb{Q}(\sqrt{d})$ for $d$ square-free

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4 \end{cases}$$

(check: $\alpha = \frac{1+\sqrt{d}}{2}$ is a zero of $\left(x - \frac{1+\sqrt{d}}{2}\right)\left(x - \frac{1-\sqrt{d}}{2}\right) = x^2 - x + \underbrace{\frac{1-d}{4}}_{\in\, \mathbb{Z}}$. )

E.g. $\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}]$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$

Example: $F = \mathbb{Q}(\zeta_n)$, $\zeta_n = e^{2\pi i/n}$ cyclotomic field; $\mathcal{O}_F = \mathbb{Z}[\zeta_n]$

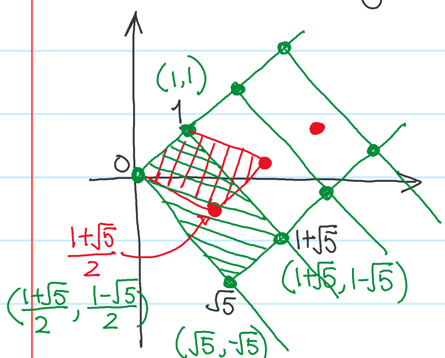
Q: Does there always exist $\alpha \in \mathcal{O}_F$ s.t. $\mathcal{O}_F = \mathbb{Z}[\alpha]$?

Example: $F = \mathbb{Q}(\sqrt[3]{10})$, $\mathcal{O}_F = \mathbb{Z}\left[\sqrt[3]{10}, \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}\right] = \mathbb{Z}\left[\frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}\right]$

A: Often but not always. First counterexample: $F = \mathbb{Q}(\beta)$

Q: How to visualize $\mathcal{O}_F$? How do we know if $\mathcal{O}_F = \mathbb{Z}[\alpha]$ for some given $\alpha$?

or more generally if $\mathcal{O}_F = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$?




E.g. $F = \mathbb{Q}(\sqrt{5}) \rightsquigarrow$ two embeddings $(\tau_1, \tau_2) : F \hookrightarrow \mathbb{R}^2$

$a + b\sqrt{5} \mapsto (a + b\sqrt{5}, a - b\sqrt{5})$

$\mathbb{Z}[\sqrt{5}] \hookrightarrow \mathbb{R}^2$ becomes a lattice with

$(\text{fundamental area})^2 = (\sqrt{2}\cdot\sqrt{10})^2 = 20$

$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \hookrightarrow \mathbb{R}^2$ becomes a lattice with

$(\text{fundmental area})^2 = \left(\frac{1}{2}\right)^2 \cdot 20 = 5$

# Lecture I: Number Fields 3

Thursday, May 24, 2018 10:13 PM

A generalization of this picture: consider $\tau_1, \cdots, \tau_n : F \hookrightarrow \mathbb{C}$ all embeddings of F.

$$\rightsquigarrow \operatorname{disc}(\alpha_1, \cdots, \alpha_n) := \det \begin{pmatrix} \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \tau_n(\alpha_1) & \cdots & \tau_n(\alpha_n) \end{pmatrix}^2$$

roughly the $(\text{fund. area})^2$ but may not be positive in general.

Exercise: If $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_F$, $\operatorname{disc}(\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}$

<u>Defn</u>: When $\mathcal{O}_F = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$, we call $\operatorname{disc}(\mathcal{O}_F) = \operatorname{disc}(\alpha_1, \cdots, \alpha_n)$ the <u>discriminant</u> of F, it is independent of the choices of $\alpha_1, \cdots, \alpha_n$.

<u>Exercise</u>. For $F = \mathbb{Q}(\sqrt{d})$, d squarefree,
$$\operatorname{disc}(\mathcal{O}_F) = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2,3 \pmod 4 \end{cases}$$

<u>Fact</u>: If $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_F$ is given so that $\operatorname{disc}(\alpha_1, \cdots, \alpha_n)$ is square-free then $\alpha_1, \cdots, \alpha_n$ form a basis of $\mathcal{O}_F$

$$\Big( \text{b/c } \underbrace{\operatorname{disc}(\alpha_1, \cdots, \alpha_n)}_{\text{if square-free}} = \underbrace{\operatorname{disc}(\mathcal{O}_F)}_{\text{in } \mathbb{Z}} \cdot [\mathcal{O}_F : \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n]^2$$

$\Rightarrow$ ↳ has to be 1.

(In the example of $F = \mathbb{Q}(\sqrt{5})$ above, $\operatorname{disc}(1, \sqrt{5}) = 20 = \operatorname{disc}(\mathcal{O}_F) \cdot 2^2$)

<u>Example</u>: $F = \mathbb{Q}(\alpha)$ with $\alpha^3 = \alpha + 1$, check $\operatorname{disc}(1, \alpha, \alpha^2) = -23$ a prime number
$\Rightarrow \mathcal{O}_F = \mathbb{Z}[\alpha]$

<u>Example</u>: $F = \mathbb{Q}(\sqrt[3]{10})$, if we take $\alpha = \frac{1 + \sqrt[3]{10} + \sqrt[3]{100}}{3}$, $\operatorname{disc}(1, \alpha, \alpha^2) = -3 \cdot 2^2 \cdot 5^2$
so apriori $[\mathcal{O}_F : \mathbb{Z}[\alpha]]$ could be 1, 2, 5, 10 will see later it's actually 1.

# Lecture II: Factorization of Ideals 1

Thursday, May 24, 2018 10:15 PM

Yesterday: $\begin{matrix} F & \supseteq & \mathcal{O}_F \\ | & & | \\ \mathbb{Q} & \supseteq & \mathbb{Z} \end{matrix}$ , $\mathcal{O}_F = \{\alpha \in F, \alpha$ is the zero of a monic poly w/ coeffs in $\mathbb{Z}\}$

• Factorization in $\mathcal{O}_F$

Over $\mathbb{Z}$, every positive integer is a unique product of prime numbers, up to permuting the factors.

But this property may not hold for general $\mathcal{O}_F$

Example: $\mathbb{Z}[i]$ is a UFD. (b/c $\mathbb{Z}[i]$ is Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD)

Fact. prime elements of $\mathbb{Z}[i]$ up to mult. with $\pm 1, \pm i$ are of the following forms

(1) $1+i$ $\longrightarrow Nm(1+i) = 2$

(2) $p$ for $p$ a $4k+3$ type prime $\longrightarrow Nm(p) = p^2$ ← norm not a prime

(3) $\left.\begin{matrix} v+iw \\ v-iw \end{matrix}\right\}$ for $v^2+w^2=p$ a $4k+1$ type prime $\longrightarrow Nm(v \pm iw) = p$

for each $p$, there are precisely two such primes up to $\{\pm 1, \pm i\}$

(Rmk: $Nm(\alpha) = p \Rightarrow \alpha$ is a prime elt in $\mathbb{Z}[i]$, but not conversely ~ see here)

E.g. $2 = -i(1+i)^2$, $3=3$, $5 = (1+2i)(1-2i)$,

$7 = 7$, $11 = 11$, $13 = (2+3i)(2-3i)$, ...

* Non UFD example: $F = \mathbb{Q}(\sqrt{-39})$, $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-39}}{2}]$ ← have smaller example even with $d \equiv 2,3 \pmod 4$ (so $\mathcal{O}_F = \mathbb{Z}[\sqrt{-d}]$) but will work with this later

$10 = 2 \cdot 5 = \frac{1+\sqrt{-39}}{2} \cdot \frac{1-\sqrt{-39}}{2}$

So UFD property fails for $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-39}}{2}]$

Note: It's not entirely trivial to show that $2, 5, \frac{1+\sqrt{-39}}{2}, \frac{1-\sqrt{-39}}{2}$ are irred. elts in $\mathbb{Z}[\frac{1+\sqrt{-39}}{2}]$

The similar factorization $10 = 2 \cdot 5 = (3+i)(3-i)$ does not contradict that $\mathbb{Z}[i]$ is a UFD b/c $2 \cdot 5 = (1+i)(1-i) \cdot (1+2i)(1-2i)$

$(3+i) \cdot (3-i) = (1-i)(1+2i) \cdot (1+i)(1-2i)$

Remedy: consider the factorization of the ideal (15) into the product of prime ideals

(I think the name "ideal" comes from that this is the "ideal" sol'n to the problem.)

Recall that in $\mathbb{Z}$, $(4,6) = (2)$ or more generally $(m,n) = (\gcd(m,n))$

So somehow "taking ideal $(x,y)$" $\approx$ "taking the gcd of $x$ & $y$"

Recall ideal multiplication: $I = (a_1, \cdots, a_s)$, $J = (b_1, \cdots, b_t)$

then $I \cdot J = (a_1b_1, \cdots, a_1b_t, a_2b_1, \cdots, a_2b_t, \cdots, a_sb_t)$ E.g. $(a)(b) = (ab)$

# Lecture II: Factorization of Ideals 2

Thursday, May 24, 2018 10:20 PM

Back to our example $10 = 2\cdot 5 = \frac{1+\sqrt{-39}}{2}\cdot\frac{1-\sqrt{-39}}{2}$

should expect $(2) = \left(2, \frac{1+\sqrt{-39}}{2}\right)\left(2, \frac{1-\sqrt{-39}}{2}\right)$, $(5) = \left(5, \frac{1+\sqrt{-39}}{2}\right)\left(5, \frac{1-\sqrt{-39}}{2}\right)$

and $\left(\frac{1+\sqrt{-39}}{2}\right) = \left(2, \frac{1+\sqrt{-39}}{2}\right)\left(5, \frac{1+\sqrt{-39}}{2}\right)$, $\left(\frac{1-\sqrt{-39}}{2}\right) = \left(2, \frac{1-\sqrt{-39}}{2}\right)\left(5, \frac{1-\sqrt{-39}}{2}\right)$

<u>check</u>. $\left(5, \frac{1+\sqrt{-39}}{2}\right)\left(5, \frac{1-\sqrt{-39}}{2}\right) = \left(25, 5\cdot\frac{1+\sqrt{-39}}{2}, 5\cdot\frac{1-\sqrt{-39}}{2}, 10\right)$

$= \left(5 = 25 - 2\cdot 10, 25, 5\cdot\frac{1+\sqrt{-39}}{2}, 5\cdot\frac{1-\sqrt{-39}}{2}, 10\right) = (5)$

The upshot is: instead of factoring elts, we should factor ideals.

<u>Theorem</u> (Dedekind) The ring of integers $\mathcal{O}_F$ of a number field $F$ is a <u>Dedekind domain</u>, i.e. an integral domain in which every nonzero proper ideal factors into a product of prime ideals (and such factorization is unique.)

($\Rightarrow$ every non-zero prime ideal is a max'l ideal)

In the example above, $(5) = \left(5, \frac{1+\sqrt{-39}}{2}\right)\left(5, \frac{1-\sqrt{-39}}{2}\right)$ is the prime ideal factorization of $(5)$.

<u>Fact</u>: Every ideal of $\mathcal{O}_F$ can be generated by (at most) 2 elements

<u>Slogan</u>. Work more with ideals, not just elts.

- <u>Finding factorization in practice</u>

$$\begin{array}{ccccc} F & \supseteq & \mathcal{O}_F & (p) = p\mathcal{O}_F = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g} \\ | & & | & | \\ \mathbb{Q} & \supseteq & \mathbb{Z} & \supseteq (p) \leftarrow \text{prime number} \end{array}$$

$e_i$: <u>ramification index</u> or <u>ramification degree</u>

$\mathcal{O}_F/\mathfrak{p}_i \cong \mathbb{F}_{p^{f_i}}$ for some $f_i \in \mathbb{N}$

$f_i$. <u>inertia degree</u> of $\mathfrak{p}_i$ or <u>residual field degree</u>

<u>Some notations</u>.

* If $e_i > 1$, say $\mathfrak{p}_i$ is <u>ramified</u>.

$e_i = 1$, say $\mathfrak{p}_i$ is <u>unramified</u>. $\rightsquigarrow$ say $p$ is <u>unramified</u> if all $e_i = 1$.

* We say $p$ <u>splits completely</u> if $e_i = f_i = 1$ for all $i$, i.e. $p\mathcal{O}_F = \mathfrak{p}_1\cdots\mathfrak{p}_n$ for $n = [F:\mathbb{Q}]$

$p$ is <u>inert</u> if $g = 1$ & $e_1 = 1$. i.e. $(p)$ is a prime ideal in $\mathcal{O}_F$

<u>Fact</u>: $p$ is ramified in $F \iff p \mid \mathrm{disc}(\mathcal{O}_F)$ <u>so only finitely many prime ramifies</u>.

- E.g. $F = \mathbb{Q}(\sqrt{d})$, $d$ square free $\Rightarrow \begin{cases} \text{odd prime } p \text{ ramifies} \iff p \mid d \\ p = 2 \text{ ramifies} \iff d \equiv 2,3 \pmod 4 \end{cases}$

# Lecture II: Factorization of Ideals 3

Thursday, May 24, 2018 10:29 PM

**Thm** Assume
- $F = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_F$ and $p \nmid [\mathcal{O}_F : \mathbb{Z}[\alpha]]$
- $h(x) \in \mathbb{Z}[x]$ is the minimal poly of $\alpha$, and $\bar{h}(x) \in \mathbb{F}_p[x]$ is its reduction
- $\bar{h}(x)$ factors as $(\bar{h}_1(x))^{e_1} \cdots \bar{h}_g(x))^{e_g}$ in $\mathbb{F}_p[x]$

Then $(p) = p\mathcal{O}_F = (p, h_1(\alpha))^{e_1} \cdots (p, h_g(\alpha))^{e_g}$ in $\mathcal{O}_F$, where $h_i(x) \in \mathbb{Z}[x]$ is any lift of $\bar{h}_i(x) \in \mathbb{F}_p[x]$

$\deg \bar{h}_1$ = inertia degree $f_1$

So $Nm(p, h_i(\alpha)) = p^{\deg \bar{h}_i} = p^{f_i}$

**Theorem**: $n = \sum_{i=1}^{g} e_i f_i$

"Proof" $Nm(p\mathcal{O}_F) = |Nm_{F/\mathbb{Q}}(p)| = p^n$

$\prod_{i=1}^{g} Nm(p, f_i(\alpha))^{e_i} = \prod_{i=1}^{g} (p^{f_i})^{e_i}$

E.g. $F = \mathbb{Q}(\sqrt{-39})$. $\alpha = \sqrt{-39}$, so $h(x) = x^2 + 39$.

$\mathcal{O}_F = \mathbb{Z}\left[\frac{1+\sqrt{-39}}{2}\right]$ so $[\mathcal{O}_F : \mathbb{Z}[\alpha]] = 2$ $\Rightarrow$ our theorem works for $p \neq 2$

(Rmk: if we had used $\alpha = \frac{1+\sqrt{-39}}{2}$ instead, our thm would work for all p)

Say we look at $p=5$: $h(x) = x^2 + 39 \equiv x^2 - 1 = (x+1)(x-1) \mod 5$

So $(5) = (5, \sqrt{-39}+1)(5, \sqrt{-39}-1)$

Look a little different from $(5) = \left(5, \frac{1+\sqrt{-39}}{2}\right)\left(5, \frac{1-\sqrt{-39}}{2}\right)$?

Obviously, $(5, \sqrt{-39}+1) \subseteq \left(5, \frac{1+\sqrt{-39}}{2}\right)$

conversely, $\frac{1+\sqrt{-39}}{2} = 5 \cdot \frac{1+\sqrt{-39}}{2} - 2 \cdot (1+\sqrt{-39}) \in (5, 1+\sqrt{-39})$

E.g. $F = \mathbb{Q}(i)$, $\mathcal{O}_F = \mathbb{Z}[i]$, for $\alpha = i$, its min. poly is $h(x) = x^2+1$ b/c $2 = (1+i)(1-i)$

For $p=2$, $h(x) = x^2+1 \equiv (x+1)^2 \mod 2 \Rightarrow (2) = (2, 1+i)^2 = (1+i)^2$ $\boxed{\text{inertia deg} = 2}$

$p$ $4k+3$ type prime, $h(x) = x^2+1 \mod p$ is irred. so $(p)$ is a prime ideal.

$p$ $4k+1$ type prime, $h(x) = x^2+1 \equiv (x-\bar{a})(x+\bar{a}) \mod p$ for some $\bar{a} \in \mathbb{F}_p$

$\Rightarrow (p) = (p, i-a)(p, i+a)$ for $a \in \mathbb{Z}$ a lift of $\bar{a}$

(some more work $\Rightarrow \exists\, b, c$ s.t. $b^2 + c^2 = p$ & $b+ic \equiv c(i+a) \mod p$

$\Rightarrow (p) = (b+ic)(b-ic)$ )

# Lecture III: Ideal Class Group 1

Thursday, May 24, 2018 10:50 PM

Last time: $F$ number field, $\mathcal{O}_F$ ring of integers, $n = [F:\mathbb{Q}]$

* Every nonzero proper ideal of $\mathcal{O}_F$ can be uniquely written as the product of prime ideals

"Goal: explain $z^p = (x+y)(x+\zeta_p y)\cdots(x+\zeta_p^{p-1}y)$"

Fact: For $\mathcal{O}_F$, PID $\Leftrightarrow$ UFD

Q: How far is $\mathcal{O}_F$ from being a PID?

Define the ideal class group to be $Cl(\mathcal{O}_F)$ = equivalence classes of ideals

$I \sim J \Leftrightarrow \alpha \cdot I = \beta \cdot J$ for some $\alpha, \beta \in \mathcal{O}_F - \{0\}$.

E.g. $F = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}]$

$(3, 1+\sqrt{-5}) \cdot (1+\sqrt{-5}) = (3+3\sqrt{-5}, 6)$

$(2, 1+\sqrt{-5}) \cdot 3 = (6, 3+3\sqrt{-5})$ $\Rightarrow [(3, 1+\sqrt{-5})] = [(2, 1+\sqrt{-5})]$

Group structure: identity: $[(1)] = [(\alpha)]$ for any $\alpha \in \mathcal{O}_F - \{0\}$

multiplication: $[I]\cdot[J] = [IJ]$ as in $6 \in (\mathbb{Z})$ $\Rightarrow 6 = 2\cdot 3$

inverse: For $[I]$, pick $n \in I$ $\Rightarrow (n) = I \cdot J$

Then $\underbrace{[(n)]}_{\text{identity}} = [I]\cdot[J] \Rightarrow [J] = [I]^{-1}$

Theorem. For a number field $F$, $Cl(\mathcal{O}_F)$ is a finite (abelian) group.

(not true for general Dedekind domain, e.g. $A = \mathbb{C}[x,y]/(y^2-(x^3-x))$
$Cl(A)$ is in bijection w/ cplx pts on $y^2 = x^3 - x$.)

Note: $Cl(\mathcal{O}_F)$ = trivial $\Leftrightarrow$ $\mathcal{O}_F$ is a PID/UFD

Q: Why do we care?

E.g. Early proof of Fermat's Last Theorem $x^p + y^p = z^p$ ($p$ odd prime).

$\rightsquigarrow z^p = x^p - (-y)^p = (x+y)(x+\zeta_p y)\cdots(x+\zeta_p^{p-1}y)$ for $\zeta_p = e^{2\pi i/p}$

Kummer: If $\mathbb{Z}[\zeta_p]$ is a PID, (or if $p \nmid \# Cl(\mathbb{Z}[\zeta_p])$)
then there's no non-triv sol'n to $x^p + y^p = z^p$

Rmk: (1) $\mathbb{Z}[\zeta_p]$ is PID only when $p \le 19$ (odd primes)

(2) $p \nmid \# Cl(\mathbb{Z}[\zeta_p])$ holds for many primes (for odd primes $<100$, except 37, 59, 67)

# Lecture III: Ideal Class Group 2

Friday, May 25, 2018 12:37 PM

Q: How large are the groups $Cl(\mathcal{O}_F)$?

Thm (Brauer-Siegel) For d square-free, as $d \to \infty$, $\# Cl(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}) \sim O(\sqrt{d})$

(Gauss Conjecture, proved indep. by Heegner, Baker, and Stark)

There are only 9 imag. quad fields which are PID.

$-d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$

(Mark Watkins found complete list of imag. quad. fields with class number $\leqslant 100$)

Q: How do we compute $Cl(\mathcal{O}_F)$ in practice?

* F has $r_1$ real embeddings : $\tau_1, \cdots, \tau_{r_1} : F \hookrightarrow \mathbb{R}$

$r_2$ pairs of complex embeddings, $\tau_{r_1+1}, \tau_{r_1+2} = \overline{\tau_{r_1+1}}, \cdots, \tau_{r_1+2r_2-1}, \tau_{r_1+2r_2} = \overline{\tau_{r_1+2r_2-1}} : F \hookrightarrow \mathbb{C}$

$\Rightarrow n = r_1 + 2r_2$

| $F$ | $n$ | $r_1$ | $r_2$ |
|---|---|---|---|
| $\mathbb{Q}(\sqrt{d})$; $d>0$ | 2 | 2 | 0 |
| $\mathbb{Q}(\sqrt{d})$; $d<0$ | 2 | 0 | 1 |
| $\mathbb{Q}(\sqrt[3]{2})$ | 3 | 1 | 1 |
| $\mathbb{Q}(\zeta_n)$, $n>2$ | $\varphi(n)$ | 0 | $\frac{\varphi(n)}{2}$ |

* Recall from Lecture 1 the def'n of $\mathrm{disc}(\mathcal{O}_F)$: if $\mathcal{O}_F = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$

$$\mathrm{disc}(\mathcal{O}_F) := \det \begin{pmatrix} \tau_1(\alpha_1) & \cdots & \tau_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \tau_1(\alpha_n) & \cdots & \tau_n(\alpha_n) \end{pmatrix}^2 \in \mathbb{Z}$$

Theorem (Minkowski) Every element of the ideal class group contains a nonzero ideal I of norm

$$\mathrm{Nm}(I) := \#(\mathcal{O}_F/I) \leqslant \sqrt{|\mathrm{disc}(\mathcal{O}_F)|} \cdot \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}$$

$\leftarrow$ pair of cplx embeddings

More on norm of ideals: • $\mathrm{Nm}((\alpha)) = |\mathrm{Nm}_{F/\mathbb{Q}}(\alpha)|$ for $\alpha \in \mathcal{O}_F - \{0\}$

• $\mathrm{Nm}(I) = 1 \Leftrightarrow I = (1) = \mathcal{O}_F$

• $\mathrm{Nm}(IJ) = \mathrm{Nm}(I) \cdot \mathrm{Nm}(J)$

• There are finitely many ideals of norm $\leqslant$ a given number, so Thm $\Rightarrow$ finiteness of $Cl(\mathcal{O}_F)$.

This statement fails for elements!

(e.g. $\exists$ $\infty$'ly many $x+\sqrt{2}y$ s.t. $\mathrm{Nm}(x+\sqrt{2}y) = x^2-2y^2 = 1$)

# Lecture III Ideal Class Group 3

Thursday, May 31, 2018 1:40 PM

Example. Compute $Cl(\mathcal{O}_F)$ for $F=\mathbb{Q}(\sqrt{-14})$

$\mathcal{O}_F=\mathbb{Z}[\sqrt{-14}]$ with min. poly $h(x)=x^2+14$, disc $\mathcal{O}_F=-56$

Minkowski bound $=\sqrt{56}\cdot\frac{4}{\pi}\cdot\frac{2!}{2^2}\approx 4.76$

$\Rightarrow$ Suffices to look at the factorizations of 2 & 3

For $p=2$, $h(x)\equiv x^2 \bmod 2 \Rightarrow (2)=(2,\sqrt{-14})^2$

For $p=3$, $h(x)=x^2+14\equiv x^2-1=(x+1)(x-1) \bmod 3 \Rightarrow (3)=(3,\sqrt{-14}+1)(3,\sqrt{-14}-1)$

So we see from this that $\# Cl(\mathcal{O}_F)\leq 4$, at best represented by

$(1)$, $(2,\sqrt{-14})$, $(3,\sqrt{-14}+1)$, $(3,\sqrt{-14}-1)$

Possible structures of $Cl(\mathcal{O}_F)$: $\{1\}$, $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}/4$, $\mathbb{Z}/2\times\mathbb{Z}/2$

Claim: $Cl(\mathcal{O}_F)=\mathbb{Z}/4\mathbb{Z}$

Note that $(2,\sqrt{-14})^2=(2)$ so $[(2,\sqrt{-14})]$ is expected to be the element of order 2

Will prove: ① $(2,\sqrt{-14})$ is not a principal ideal

② $[(3,\sqrt{-14}+1)]^2=[(2,\sqrt{-14})]$

For ①, if $(2,\sqrt{-14})=(\alpha)$ for $\alpha\in\mathcal{O}_F$

$\Rightarrow Nm(2,\sqrt{-14})=|Nm_{F/\mathbb{Q}}(\alpha)|$

note: $Nm(2,\sqrt{-14})^2=Nm(2)=|Nm_{F/\mathbb{Q}}(2)|=4$

So $Nm_{F/\mathbb{Q}}(\alpha)=2$. Say $\alpha=a+b\sqrt{-14}\Rightarrow a^2+14b^2=2$ not possible.

For ②, it's equivalent to show $[(3,\sqrt{-14}+1)]^2[(2,\sqrt{-14})]=[(1)]$

i.e. $(3,\sqrt{-14}+1)^2(2,\sqrt{-14})$ is principal.

$=(9,3+3\sqrt{-14},-13+2\sqrt{-14})(2,\sqrt{-14})$

$=(9,\underbrace{16+\sqrt{-14}}_{-2+\sqrt{-14}},\underbrace{-13+2\sqrt{-14}}_{=2(-2+\sqrt{-14})-9})(2,\sqrt{-14})$

$=(9,-2+\sqrt{-14})(2,\sqrt{-14})$

$=(18,9\sqrt{-14},-4+2\sqrt{-14},-2\sqrt{-14}-14)$

$9\sqrt{-14},-4+2\sqrt{-14} \to 16+\sqrt{-14}$

$18, 16+\sqrt{-14} \to -2+\sqrt{-14}$

note: $(-2+\sqrt{-14})(-2-\sqrt{-14})=18$

$\Rightarrow =(-2+\sqrt{-14})$ is principal.

Example. Compute $Cl(\mathcal{O}_F)$ for $F=\mathbb{Q}(\sqrt{-39})$,

$\mathcal{O}_F=\mathbb{Z}[\alpha]$, $\alpha=\frac{1+\sqrt{-39}}{2}$ with min poly $h(x)=\left(x-\frac{1+\sqrt{-39}}{2}\right)\left(x-\frac{1-\sqrt{-39}}{2}\right)=x^2-x+10$

$\mathrm{disc}(\mathcal{O}_F)=-39$.

Minkowski bound $=\sqrt{39}\cdot\frac{4}{\pi}\cdot\frac{2!}{2^2}=3.97$.

It suffices to look at the factorization of 2 & 3

For $p=2$, $\bar{h}(x)\equiv x^2-x=x(x-1)\pmod 2\Rightarrow (2)=(2,\alpha)(2,\alpha-1)$

For $p=3$, $\bar{h}(x)\equiv x^2+2x+1=(x+1)^2\pmod 3\Rightarrow (3)=(3,\alpha+1)^2$

So we see from this that $\#Cl(\mathcal{O}_F)\le 4$, at best rep'd by $(1),(2,\alpha),(2,\alpha-1),(3,\alpha+1)$

Possibilities of the structure of $Cl(\mathcal{O}_F)$: $\{1\}$, $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}/4$, $\mathbb{Z}/2\times\mathbb{Z}/2$

Claim. $Cl(\mathcal{O}_F)\simeq\mathbb{Z}/4\mathbb{Z}$

① Show that $(3,\alpha+1)$ is not a principal ideal

Note: $Nm(3,\alpha+1)^2=Nm(3)=|Nm_{F/\mathbb{Q}}(3)|=9 \Rightarrow Nm(3,\alpha+1)=3$

But there's no element in $\mathcal{O}_F$ with norm 3, indeed,

if $Nm\left(\frac{a+\sqrt{-39}\cdot b}{2}\right)=3$ for $a,b\in\mathbb{Z}$ w/ same parity

$\Rightarrow a^2+39b^2=12$ No such $a$ & $b$

So $(3,\alpha+1)$ represents a non-trivial elt in $Cl(\mathcal{O}_F)$.

and thus an element of order 2 in $Cl(\mathcal{O}_F)$, as $[(3)]=[(3,\alpha+1)]^2$

② Check that $(2,\alpha)^2\cdot(3,1+\alpha)$ is a principal ideal

$$=(4,2\alpha,\alpha^2=\alpha-10)\cdot(3,1+\alpha)$$

$=\alpha-10$
$=\alpha+2-4\cdot 3$

$$=(4,\alpha+2)\cdot(3,\alpha+1)$$

$$=(12,\underbrace{3\alpha+6,4\alpha+4}_{\text{gives } \alpha-2},\alpha^2+3\alpha+2=4\alpha-8)$$

Note: $(\alpha-2)(\alpha+1)=\alpha^2-\alpha-2=-12$

So $(2,\alpha)^2\cdot(3,1+\alpha)=(\alpha-2)$.

$\Rightarrow$ The ideal class $[(2,\alpha)]$ in the class gp satisfies $[(2,\alpha)]^2=[(3,1+\alpha)]^{-1}\neq[(1)]$

$\Rightarrow Cl(\mathcal{O}_F)\cong\mathbb{Z}/4\mathbb{Z}$. & $([(2,\alpha)]^2)^2=[(1)]$

Exercise. Show explicitly that $(2,\alpha)^4=(\alpha+2)$

# Lecture IV: Unit Groups 1

Thursday, May 24, 2018 10:44 PM

- Structure of unit group $\mathcal{O}_F^\times$:

Let $F$ have $r_1$ real embeddings and $r_2$ pairs of complex embeddings

**Theorem** (Dirichlet) The group $\mathcal{O}_F^\times$ is finitely generated with $r = r_1 + r_2 - 1$ multiplicatively independent units of infinite order: there are units with infinite order s.t.

$$\mathcal{O}_F^\times = \{ z u_1^{n_1} \cdots u_r^{n_r} : z \text{ is a root of unity in } F;\ n_i \in \mathbb{Z} \}$$

($u_1, \cdots, u_r$ mult. indep. means $u_1^{n_1} \cdots u_r^{n_r} = 1 \Rightarrow$ all $n_i = 0$)

Abstractly, $\mathcal{O}_F^\times \cong \mathbb{Z}^{r_1+r_2-1} \times \mu(F) \longleftarrow$ roots of unity in $F$

**Rmk**: $r_1 + r_2 - 1 = 0$ only if $F = \mathbb{Q}$ or an imaginary quadratic field

So if $F \neq \mathbb{Q}$ or imag. quad. field, $\mathcal{O}_F^\times$ is infinite!

**Rmk**: Dirichlet thm holds for $\mathbb{Z}[\alpha]$ for any algebraic integer $\alpha$.

**Note**: $u \in \mathcal{O}_F^\times$ is a unit $\Rightarrow uv = 1 \Rightarrow Nm(u) \cdot Nm(v) = 1 \Rightarrow Nm(u) \in \{\pm 1\}$

In fact, $\mathcal{O}_F^\times = \{ u \in \mathcal{O}_F \text{, s.t. } Nm(u) \in \{\pm 1\} \}$

Caveat: for $\alpha \in F$ & $Nm(\alpha) = 1$ does not mean $\alpha \in \mathcal{O}_F^\times$. e.g. $\alpha = \frac{3+4i}{5}$ $Nm_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) = 1$.

**Example**: (Pell's equation) $x^2 - dy^2 = 1$ for $d \in \mathbb{N}_{>1}$ square-free

$\rightsquigarrow (x + y\sqrt{d})(x - y\sqrt{d}) = 1$

So a sol'n to Pell's equation $\rightsquigarrow$ a unit $x + y\sqrt{d} \in (\mathbb{Z}[\sqrt{d}])^\times$

Roughly, solving Pell's equation $\longleftrightarrow$ finding the units in $\mathbb{Z}[\sqrt{d}]$.

By Dirichlet's theorem, $\mathcal{O}_F^\times = \{\pm 1\} \times \gamma^{\mathbb{Z}}$, with $\gamma = a + b\sqrt{d}$ $a, b \in \mathbb{Z}_{>0}$

Pell's equation has a fundamental sol'n $(x_0, y_0)$

$\longrightarrow a + b\sqrt{d}$ if $Nm(a + b\sqrt{d}) = 1$

$\longrightarrow (a + b\sqrt{d})^2$ if $Nm(a + b\sqrt{d}) = -1$

all other sol'ns come from $\pm(x_0 + y_0\sqrt{d})^r$ for $r \in \mathbb{Z}$

E.g. The sol'ns to $x^2 - 10y^2 = 1$ are $(x,y) = (19,6), (721,228), (27379,8658), \cdots$

$F = \mathbb{Q}(\sqrt{10})$, $\mathcal{O}_F = \mathbb{Z}[\sqrt{10}]$, $\gamma = 3 + \sqrt{10}$; $Nm(\gamma) = (3+\sqrt{10})(3-\sqrt{10}) = -1$

The fundamental sol'n to $x^2 - 10y^2 = 1$ comes from

$(3+\sqrt{10})^2 = 19 + 6\sqrt{10} \rightsquigarrow$ fundamental sol'n $(19,6)$.

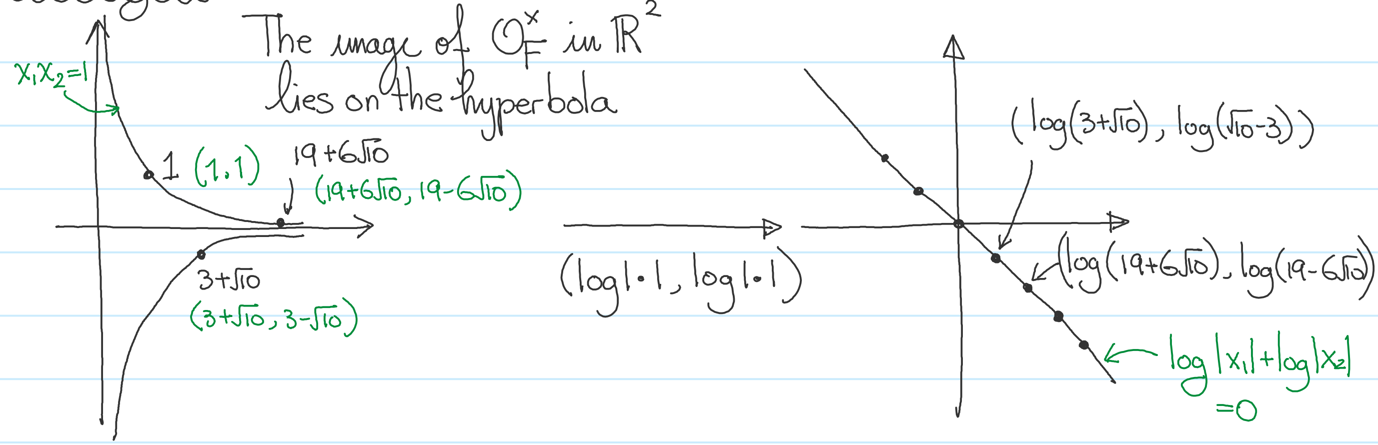
Note: $(19+6\sqrt{10})^2 = 721 + 228\sqrt{10}$ and $(19+6\sqrt{10})^3 = 27379 + 8658\sqrt{10}, \cdots$

# Lecture IV: Unit Groups 2

Thursday, May 24, 2018 10:50 PM

Visualize it: $F \hookrightarrow \mathbb{R}^2 \quad a+b\sqrt{10} \mapsto (a+b\sqrt{10}, a-b\sqrt{10})$

The image of $\mathcal{O}_F^\times$ in $\mathbb{R}^2$ lies on the hyperbola




Note: the fundamental unit could be large, e.g. $F=\mathbb{Q}(\sqrt{94})$, $u = 2143295 + 221064\sqrt{94}$

Example: $F=\mathbb{Q}(\zeta_n)$, $[F:\mathbb{Q}] = \varphi(n) = \#(\mathbb{Z}/n)^\times$ Assume $n>2$

$\mathcal{O}_F = \mathbb{Z}[\zeta_n]$ cyclotomic units $\mathcal{O}_F^\times$.

When $n \geq 3$, all embeddings of $F$ are complex $\rightsquigarrow \frac{1}{2}\varphi(n)$ pair of embeddings

For $i \in \mathbb{Z}$, $\gcd(i,n)=1$, we have an unit

$$\frac{\zeta_n^i - 1}{\zeta_n - 1} = 1 + \zeta_n + \cdots + \zeta_n^{i-1} \in \mathcal{O}_F = \mathbb{Z}[\zeta_n]$$

$\exists j \in \mathbb{Z}$ s.t. $ij \equiv 1 \pmod n$

$$\frac{\zeta_n - 1}{\zeta_n^i - 1} = \frac{(\zeta_n^i)^j - 1}{\zeta_n^i - 1} = 1 + \zeta_n^i + \zeta_n^{2i} + \cdots + \zeta_n^{(j-1)i} \in \mathcal{O}_F$$

$$\Rightarrow \frac{\zeta_n^i - 1}{\zeta_n - 1} \in \mathcal{O}_F^\times$$

Yet $\dfrac{\zeta_n^{-i} - 1}{\zeta_n - 1} = (-\zeta_n^{-i}) \dfrac{\zeta_n^i - 1}{\zeta_n - 1}$ so up to roots of unity, these two are essentially the same

Fact: When $n = p^r$ is a prime power, $\left\{ \frac{\zeta_n^i - 1}{\zeta_n - 1} ; 1 \leq i \leq \frac{n}{2}, \gcd(i,n)=1 \right\}$ are mult. indep.

$\Rightarrow \left[\mathcal{O}_F^\times : \left\langle \frac{\zeta_n^i - 1}{\zeta_n - 1} ; 1 \leq i \leq \frac{n}{2}, \gcd(i,n)=1 \right\rangle\right]$ is finite

but this could fail if $n$ is not a prime power, e.g. $n=55$

Digression on Dedekind zeta function

- Recall Riemann zeta function $\zeta(s) = \sum_{n \geq 0} \frac{1}{n^s}$ when $\mathrm{Re}(s) > 1$

  $\zeta(s)$ has a meromorphic continuation to $s \in \mathbb{C}$ with a simple pole @ $s=1$

  s.t. $\zeta(s) \sim \frac{1}{s-1}$ near $s=1$.

  & functional equation $\zeta(s) \leftrightarrow \zeta(1-s)$ & Riemann hypothesis

# Lecture IV Unit Groups 3

Thursday, May 31, 2018 2:12 PM

Dedekind zeta function for a number field $F$

$$\zeta_F(s) = \sum_{\substack{0 \neq I \subset \mathcal{O}_F \\ \text{nonzero ideal}}} \frac{1}{Nm(I)^s} = \prod_{\wp \text{ prime ideal}} \frac{1}{1 - Nm(\wp)^{-s}} \qquad \mathrm{Re}\, s > 1$$

e.g. $$\zeta_{\mathbb{Q}(i)}(s) = \frac{1}{1-2^{-s}} \cdot \prod_{p\ 4k+3} \frac{1}{1-(p^2)^{-s}} \cdot \prod_{p\ 4k+1} \left(\frac{1}{1-p^{-s}}\right)^2$$

$2 = Nm(1+i)$, $p^2 = Nm(p)$, $(p) = \wp_1 \wp_2$ with $Nm(\wp_i) = p$

- meromorphic cont. & function eq'n $s \leftrightarrow 1-s$
  & Riemann Hypothesis: zeros of $\zeta_F(s) \in \mathbb{Z}_{\leq 0} \cup \{s \mid \mathrm{Re}\, s = \frac{1}{2}\}$
- Special value: $\zeta_F(s) \sim \frac{(*)}{s-1}$ near $s=1$ ; $(*)$ has arithmetic info.

E.g. $F = \mathbb{Q}(\sqrt{-d})$ $$\lim_{s\to 1} (s-1)\zeta_F(s) = \frac{2\pi \cdot \# cl(\mathcal{O}_F)}{\# \mathcal{O}_F^\times \cdot \sqrt{disc(\mathcal{O}_F)}}$$

$\# \mathcal{O}_F^\times = 2$ unless $d = 1$ or $3$

$disc(\mathcal{O}_F) = \begin{cases} d & \text{if } -d \equiv 1 \pmod 4 \\ 4d & \text{if } -d \equiv 2,3 \pmod 4 \end{cases}$

class number formula $\rightarrow$

$F = \mathbb{Q}(\sqrt{d})$ $$\lim_{s\to 1} (s-1)\zeta_F(s) = \frac{4 \cdot \# cl(\mathcal{O}_F) \cdot \log|u|}{2 \cdot \sqrt{disc(\mathcal{O}_F)}}$$

$u$: generator of $\mathcal{O}_F$

Special values of generalized zeta functions are related to important arithm. invariants.

Somewhat surprising result

Thm: (Weinberger 1973) Assume GRH (Generalized Riemann Hypothesis)
If $F$ is not imag. quad. field & $F$ is a PID $\Rightarrow$ $F$ is Euclidean.

* The proof uses that when $F \neq \mathbb{Q}$ or imag. quad, $\mathcal{O}_F^\times$ is infinite

* $F = \mathbb{Q}(\sqrt{-19})$ has class number 1 but not a Euclidean domain