Q: Why number fields?

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

\[ z^p = x^p - (-y)^p = (x+y)(x+S_p y) \cdots (x+S_p^{p-1} y) \text{ for } S_p = e^{2\pi i/p} \]

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

almost \( \Rightarrow \) \( x+S_p y \) is a \( p \)th power.

Kummer: This works when \( \mathbb{Z}[S_p] \) is “close” to a PID.

(He proved FLT for \( p<100 \) except for three such \( p \)’s.)

Upside: Studying bigger fields help understanding Diophantine equations over \( \mathbb{Q} \) or \( \mathbb{Z} \).

Number fields: by primitive elt thm.

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

finite extn \( \text{deg } h(x) = [F: \mathbb{Q}] = n \) \( \Rightarrow \) all the zeros are \( \alpha = \alpha_1, \ldots \alpha_n \)

Q: There are \( n \) embeddings

\[ \tau_1, \ldots, \tau_n : F \hookrightarrow \mathbb{Q}[x]/(h(x)) \hookrightarrow \mathbb{C} \]

\[ \tau_i (c_0 + c_1 x + \cdots + c_n x^n) := c_0 + c_1 \alpha_i + \cdots + c_n \alpha_i^{n-1} \]

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

real embedding \( \tau : \mathbb{Q}[x]/(x^2-3) \rightarrow \mathbb{R} \leq \mathbb{C} \)

\[ x \rightarrow \sqrt{3} \]

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

\[ \tau_2, \tau_3 : x \rightarrow \tau_2(\sqrt{3}), \tau_3(\sqrt{3}) \text{ complex conj of each other} \]

* In general, complex embeddings come in pairs.

* For \( \alpha \in F \), define its trace to be \( \text{Tr}_{F/\mathbb{Q}}(\alpha) = \tau_1(\alpha) + \cdots + \tau_n(\alpha) \in \mathbb{Q} \)

its norm to be \( \text{Nm}_{F/\mathbb{Q}}(\alpha) = \tau_1(\alpha) \cdots \tau_n(\alpha) \in \mathbb{Q} \)

* e.g. \( F = \mathbb{Q}(i) , \text{Nm}_{F/\mathbb{Q}}(x+iy) = (x+iy)(x-iy) = x^2 + y^2 \).

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

\[ \text{then, } \text{Tr}_{F/\mathbb{Q}}(\alpha) = -a_1, \text{ Nm}_{F/\mathbb{Q}}(\alpha) = (-1)^n a_n \]

* If \( \alpha \) is not the field generator,

* e.g. \( \alpha \in \mathbb{Q} , \text{Tr}_{F/\mathbb{Q}}(\alpha) = n \cdot \alpha , \text{Nm}_{F/\mathbb{Q}}(\alpha) = \alpha^n \)
Ring of integers:
\[ F = \mathbb{Q}(\alpha) \supseteq \mathcal{O}_F \]
Say \( \alpha \) is the zero of an irreducible polynomial with coefficients in \( \mathbb{Z} \).

1. Finite extension
2. \( \mathcal{O}_F \supseteq \mathbb{Z} \)

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

\( \mathcal{O}_F := \{ \beta \in F \mid \text{the minimal monic poly of } \beta \text{ in } \mathbb{Q}[x] \text{ has coeffs in } \mathbb{Z} \} \)
\[ = \{ \beta \in F \mid \beta \text{ is a zero of a monic poly with coeffs in } \mathbb{Z} \} \]

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

i.e. \( \exists \alpha_1, \ldots, \alpha_n \in \mathcal{O}_F \) s.t. \( \mathcal{O}_F = \mathbb{Z}_n + \cdots + \mathbb{Z} \alpha_n \)

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

Example: \( F = \mathbb{Q}(\sqrt{3}) \) for \( d \) square-free
\[ \mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod{4} \end{cases} \]
(check: \( \alpha = \frac{1+\sqrt{d}}{2} \) is a zero of \( (x - \frac{1+\sqrt{d}}{2})(x - \frac{1-\sqrt{d}}{2}) = x^2 - x + \frac{1-d}{4} \))

E.g. \( \mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}] \) and \( \mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \)

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

A: Often but not always. First counterexample: \( F = \mathbb{Q}(\sqrt{5}) \)

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 \( \mathcal{O}_F = \mathbb{Z}_n \alpha_1 + \cdots + \mathbb{Z} \alpha_n \)?

E.g. \( F = \mathbb{Q}(\sqrt{5}) \) \( \rightarrow \) two embeddings \( (\iota_1, \iota_2) : F \hookrightarrow \mathbb{R}^2 \)
\[ a + b\sqrt{5} \rightarrow (a + b\sqrt{5}, a-b\sqrt{5}) \]

\( \mathbb{Z}[\sqrt{5}] \hookrightarrow \mathbb{R}^2 \) becomes a lattice with
\[ (\text{fundamental area})^2 = (\sqrt{2} \cdot \sqrt{10})^2 = 20 \]

\( \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \hookrightarrow \mathbb{R}^2 \) becomes a lattice with
\[ (\text{fundamental area})^2 = \left(\frac{1}{2}\right)^2 \cdot 20 = 5 \]
A generalization of this picture: consider $\tau_1, \ldots, \tau_n : F \rightarrow \mathbb{C}$ all embeddings of $F$.

$$\text{disc}(\alpha_1, \ldots, \alpha_n) := \det \left( \begin{array}{c} \tau_1(\alpha_1) \cdots \tau_1(\alpha_n) \\ \vdots \vdots \\ \tau_n(\alpha_1) \cdots \tau_n(\alpha_n) \end{array} \right)^2$$

roughly the (fund. area)$^2$

but may not be positive in general.

**Exercise:** If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_F$, $\text{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$

**Definition:** When $\mathcal{O}_F = \mathbb{Z} \alpha_1 \oplus \cdots \oplus \mathbb{Z} \alpha_n$, we call $\text{disc}(\mathcal{O}_F) = \text{disc}(\alpha_1, \ldots, \alpha_n)$ the discriminant of $F$.

it is independent of the choices of $\alpha_1, \ldots, \alpha_n$.

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

**Fact:** If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_F$ is given so that $\text{disc}(\alpha_1, \ldots, \alpha_n)$ is square-free

then $\alpha_1, \ldots, \alpha_n$ form a basis of $\mathcal{O}_F$

(b/c $\text{disc}(\alpha_1, \ldots, \alpha_n) = \text{disc}(\mathcal{O}_F) \cdot [\mathcal{O}_F : \mathbb{Z} \alpha_1 \oplus \cdots \oplus \mathbb{Z} \alpha_n]^2$)

if square-free $\in \mathbb{Z}$ $\Rightarrow L$ has to be 1.

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

**Example:** $F = \mathbb{Q}(\alpha)$ with $\alpha^3 = \alpha + 1$, check $\text{disc}(1, \alpha, \alpha^2) = -23$ a prime number

$\Rightarrow \mathcal{O}_F = \mathbb{Z}[\alpha]$

**Example:** $F = \mathbb{Q}(3\sqrt{10})$, if we take $\alpha = \frac{1 + 3\sqrt{10} + 3\sqrt{100}}{3}$, $\text{disc}(1, \alpha, \alpha^2) = -3 \cdot 2 \cdot 5 \cdot 2$

so apriori $[\mathcal{O}_F : \mathbb{Z}[\alpha]]$ could be $1, 2, 5, 10, \text{ will see later it's actually 1}$. 
Lecture II: Factorization of Ideals

Thursday, May 24, 2018 10:15 PM

Yesterday: \( F \supseteq \mathbb{Q} \), \( \mathcal{O}_F = \{ \alpha \in F, \alpha \text{ is the zero of a monic poly w/ coeffs in } \mathbb{Z} \} \)

\[ \mathcal{O}_F \supseteq \mathbb{Z} \]

• 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. \((b/c \ Z[i] \text{ is Euclidean } \Rightarrow \text{PID} \Rightarrow \text{UFD})\)
  Fact: prime elements of \( \mathbb{Z}[i] \) up to mult. with \( \pm 1, \pm i \) are of the following forms
    (1) \( 1+i \) \( \Rightarrow Nm(1+i) = 2 \) (not a prime)
    (2) \( p \) for \( p \) a \( 4k+3 \) type prime \( \Rightarrow Nm(p) = p^2 \)
    (3) \( v+ iw \) for \( v^2 + w^2 = p \) a \( 4k+1 \) type prime \( \Rightarrow Nm(v+iw) = p \)
    * for each \( p \), there are precisely two such primes up to \( \{ \pm 1, \pm i \} \)
  \( (\text{Rmk: } Nm(\alpha) = p \Rightarrow \alpha \text{ is a prime elt in } \mathbb{Z}[i], \text{ but not conversely see here}) \)
  Eg. \( 2 = -i(1+i)^2, 3 = 3, 5 = (1+i)(1-i), \)
  \[ 7 = 7, 11 = 11, 13 = (2+3i)(2-3i), \ldots \]

* Non UFD example: \( F = \mathbb{Q}(\sqrt{39}) \), \( \mathcal{O}_F = \mathbb{Z}\left[\frac{1+\sqrt{39}}{2}\right] \) \( \leftarrow \) have smaller example even with \( d \equiv 2, 3 \pmod{4} \), so \( \mathcal{O}_F = \mathbb{Z}[i] \)

So UFD property fails for \( \mathcal{O}_F = \mathbb{Z}\left[\frac{1+\sqrt{39}}{2}\right] \)

Note: It's not entirely trivial to show that \( 2, 5, \frac{1+\sqrt{39}}{2}, \frac{1-\sqrt{39}}{2} \) are irreducible elements in \( \mathbb{Z}\left[\frac{1+\sqrt{39}}{2}\right] \)

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

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” solution to the problem.

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

So somehow “taking ideal \((x, y)\) is taking the gcd of \(x \& y\)”

Recall ideal multiplication: \( I = (a_1, \ldots, a_s), J = (b_1, \ldots, b_t) \)
  then \( I \cdot J = (a_1b_1, \ldots, a_sb_t, a_1b_1, \ldots, a_2b_t, \ldots, a_sb_t) \) \( \text{Eg. } (a)(b) = (ab) \)
Back to our example \(10 = 2 \cdot 5 = \frac{1 + \sqrt{39}}{2} \cdot \frac{1 - \sqrt{39}}{2}\). We should expect \((2) = (2, \frac{1 + \sqrt{39}}{2})(2, \frac{1 - \sqrt{39}}{2})\), \((5) = (5, \frac{1 + \sqrt{39}}{2})(5, \frac{1 - \sqrt{39}}{2})\)
and \(\left(\frac{1 + \sqrt{39}}{2}\right) = (2, \frac{1 + \sqrt{39}}{2})(5, \frac{1 + \sqrt{39}}{2})(\frac{1 - \sqrt{39}}{2}) = (2, \frac{1 - \sqrt{39}}{2})(5, \frac{1 - \sqrt{39}}{2})\)

Check: \((5, \frac{1 + \sqrt{39}}{2})(5, \frac{1 - \sqrt{39}}{2}) = (25, 5 \cdot \frac{1 + \sqrt{39}}{2}, 5 \cdot \frac{1 - \sqrt{39}}{2}, 10) = (5 = 25 - 2 \cdot 10, 25, 5 \cdot \frac{1 + \sqrt{39}}{2}, 5 \cdot \frac{1 - \sqrt{39}}{2}, 10) = (5)\)

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

**Theorem (Dedekind)** The ring of integers \(\mathcal{O}_F\) of a number field \(F\) is a Dedekind domain, 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' ideal.

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

**Fact:** Every ideal of \(\mathcal{O}_F\) can be generated by (at most) 2 elements.

**Slogan:** Work more with ideals, not just elts.

* Finding factorization in practice

\[ F \supseteq \mathcal{O}_F \supseteq (p) = p_1^{e_1} \cdots p_g^{e_g} \]

\[ \mathcal{O}_F / p_i \cong F_{p_i} \text{ for some } f_i \in \mathbb{Z} \]

\[ f_i \text{ inertia degree of } p_i \]

\[ g \text{ ramification index of } p_i \]

\[ g \text{ ramification degree of } p_i \]

\[ \text{or residual field degree} \]

Some notations:

* If \(e_i > 1\), say \(p_i\) is ramified

\(e_i = 1\), say \(p_i\) is unramified. \(\Leftrightarrow\) say \(p\) is unramified if all \(e_i = 1\).

* We say \(p\) splits completely if \(e_i = f_i = 1\) for all \(i\), i.e., \(p\mathcal{O}_F = p_1 \cdots p_n\) for \(n = [F : \mathbb{Q}]\).

\(p\) is inert if \(g = 1\) & \(e_i = 1\). i.e. \((p)\) is a prime ideal in \(\mathcal{O}_F\).

**Fact:** \(p\) is ramified in \(F \iff p \mid \text{disc}(\mathcal{O}_F)\), so only finitely many prime ramifies.

* E.g., \(F = \mathbb{Q}(\sqrt{d})\), square free \(\Rightarrow\) odd prime \(p\) ramifies \(\iff p \mid \text{Id}\)

\(p = \{2, \text{ramifies} \iff d \equiv 2, 3 (\text{mod} 4)\} \)
Lecture II: Factorization of Ideals

Thursday, May 24, 2018 10:29 PM

Theorem 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 \( \bar{h}(x) = h_1(x)^{e_1} \cdots h_g(x)^{e_g} \) 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 \( \bar{h}_i(x) \in \mathbb{F}_p[x] \)

So \( Nm(p, h_i(\alpha)) = p^{deg h_i} = p^{f_i} \)

Theorem \( n = \sum_{i=1}^{g} e_i f_i \)

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

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

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

\( \mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{39}}{2}] \) so \( [\mathcal{O}_F : \mathbb{Z}[\alpha]] = 2 \) \( \Rightarrow \) our theorem works for \( p = 2 \) \( \quad \text{(Remark: if we had used} \alpha = \frac{1-\sqrt{39}}{2} \text{instead, our theorem would work for all} \ p) \)

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 \( (5) = (5, \frac{1+\sqrt{39}}{2})(5, \frac{1-\sqrt{39}}{2}) \)?

Obviously, \( (5, \sqrt{39}+1) \leq (5, \frac{1+\sqrt{39}}{2}) \)

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

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

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

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

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

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

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

\( \Rightarrow (p) = (b+ic)(b-ic) \))
Last time: F number field, \( \mathcal{O}_F \) ring of integers, \( n = [F: \mathbb{Q}] \)

* Every non-zero proper ideal of \( \mathcal{O}_F \) can be uniquely written as the product of prime ideals.

Goal: explain \( \mathcal{O}_F^p = (x+y)(x+\zeta_p y) \cdots (x+\zeta_p^{p-1} y) \)

Fact: For \( \mathcal{O}_F \), \( \text{PID} \iff \text{UFD} \)

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

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

\[ I \sim J \iff \alpha \cdot I = \beta \cdot J \text{ for some } \alpha, \beta \in \mathcal{O}_F \setminus \{0\} \]

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

\[
\begin{align*}
(3, 1 + \sqrt{-5}) \cdot (1 + \sqrt{-5}) &= (3 + 3\sqrt{-5}, 6) \Rightarrow ((3, 1+\sqrt{-5}) = [(2, 1+\sqrt{-5})] \\
(2, 1+\sqrt{-5}) \cdot 3 &= (6, 3 + 3\sqrt{-5})
\end{align*}
\]

Group structure: identity: \( [I] = [\alpha] \) for any \( \alpha \in \mathcal{O}_F \setminus \{0\} \)
multiplication: \( [I] \cdot [J] = [IJ] \)
inverse: For \( [I] \), pick \( \chi \in I \Rightarrow (\chi) = I \cdot J \)

Then \( [\mathcal{O}_F] = [I] \cdot [J] \Rightarrow [J] = [I]^{-1} \)

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

(not true for general Dedekind domain, e.g. \( A = \mathbb{C}[x,y] / (y^2 - (x^3 - x)) \)

\( \text{Cl}(A) \) is in bijection w/ cplx pts on \( y^2 = x^3 - x \).

Note: \( \text{Cl}(\mathcal{O}_F) = \text{trivial} \iff \mathcal{O}_F \) 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),

\[
\begin{align*}
z^p &= x^p - (-y)^p = (x+y)(x+\zeta_p y) \cdots (x+\zeta_p^{p-1} y) \\
&\quad \text{for } \zeta_p = e^{2\pi i/p}
\end{align*}
\]

Kummer: If \( \mathbb{Z}[\zeta_p] \) is a PID, or if \( p \neq \#\text{Cl}(\mathbb{Z}[\zeta_p]) \)

then there's no non-triv soln to \( x^p + y^p = z^p \)

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

(2) \( p \neq \#\text{Cl}(\mathbb{Z}[\zeta_p]) \) holds for many primes (for odd primes \( < 100 \), except \( 37, 59, 67 \))
Q: How large are the groups $\text{Cl}(\mathcal{O}_F)$?

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

(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 $\leq 100$)

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

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

$2r_2$ pairs of complex embeddings, $\tau_{r_1+1}, \tau_{r_1+2}, \tau_{r_1+2}, \ldots, \tau_{r_1+2r_2-1}, \tau_{r_1+2r_2} = \tau_{r_1+1}^{-1}: F \to \mathbb{C}$

$\Rightarrow n = r_1 + 2r_2$

<table>
<thead>
<tr>
<th>$F$</th>
<th>$n$</th>
<th>$r_1$</th>
<th>$r_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Q}(\sqrt{d}), d &gt; 0$</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>$\mathbb{Q}(\sqrt{d}), d &lt; 0$</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$\mathbb{Q}(\sqrt{-2})$</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\mathbb{Q}(\sqrt{n}), n &gt; 2$</td>
<td>$\varphi(n)$</td>
<td>0</td>
<td>$\frac{\varphi(n)}{2}$</td>
</tr>
</tbody>
</table>

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

$$\det \begin{pmatrix}
\tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\
\vdots & \ddots & \vdots \\
\tau_n(\alpha_1) & \cdots & \tau_n(\alpha_n)
\end{pmatrix} \in \mathbb{Z}$$

Theorem (Minkowski): Every element of the ideal class group contains a non-zero ideal $I$ of norm

$$\text{Nm}(I) := \# \mathcal{O}_F/I \leq \sqrt{|\text{disc}(\mathcal{O}_F)|} \cdot \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \text{ pair of cpx. embeddings}$$

More on norm of ideals:

$\bullet \text{Nm}(\alpha) = |\text{Nm}_{F/Q}(\alpha)|$ for $\alpha \in \mathcal{O}_F - \{0\}$

$\bullet \text{Nm}(I) = 1 \iff I = (1) = \mathcal{O}_F$

$\bullet \text{Nm}(IJ) = \text{Nm}(I) \cdot \text{Nm}(J)$

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

This statement fails for elements!

(e.g. only many $x + \sqrt{2}y$ s.t. $\text{Nm}(x + \sqrt{2}y) = x^2 - 2y^2 = 1$)
Example. Compute \( \text{Cl}(\mathcal{O}_F) \) for \( F = \mathbb{Q}(\sqrt[4]{14}) \)

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

Minkowski bound \( \approx \sqrt{56 \cdot \frac{4}{\pi} \cdot \frac{2^4}{2^2}} \approx 4.76 \)

\[\Rightarrow \text{Suffices to look at the factorizations of } 2 \text{ & } 3\]

For \( p=2 \), \( h(x) = x^2 \mod 2 \Rightarrow (2) = (2, \sqrt[4]{14})^2 \)

For \( p=3 \), \( h(x) = x^2 + 14 \equiv x^2 - 1 = (x+1)(x-1) \mod 3 \Rightarrow (3) = (3, \sqrt[4]{14} + 1)(3, \sqrt[4]{14} - 1) \)

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

\[
(1), (2, \sqrt[4]{14}), (3, \sqrt[4]{14} + 1), (3, \sqrt[4]{14} - 1)
\]

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

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

Note that \( (2, \sqrt[4]{14})^2 = (2) \) so \([2, \sqrt[4]{14}]\) is expected to be the element of order 2

Will prove: \( 1. (2, \sqrt[4]{14}) \) is not a principal ideal

\( 2. ([3, \sqrt[4]{14} + 1])^2 = [2, \sqrt[4]{14}] \)

For \( 1. \), if \( (2, \sqrt[4]{14}) = (\alpha) \) for \( \alpha \in \mathcal{O}_F \)

\[ \Rightarrow \text{Nm} (2, \sqrt[4]{14}) = \left| \text{Nm}_{\mathbb{Q}}(\alpha) \right| \]

Note: \( \text{Nm}(2, \sqrt[4]{14})^2 = \text{Nm}(2) = \left| \text{Nm}_{\mathbb{Q}}(2) \right| = 4 \)

So \( \text{Nm}_{\mathbb{Q}}(\alpha) = 2 \). Say \( \alpha = a + b\sqrt[4]{14} \Rightarrow a^2 + 14b^2 = 2 \) not possible.

For \( 2. \), it’s equivalent to show \([3, \sqrt[4]{14} + 1]^2 [2, \sqrt[4]{14}] = [1]\)

i.e. \( (3, \sqrt[4]{14} + 1)^2 (2, \sqrt[4]{14}) \) is principal.

\[
= (9 + 3\sqrt[4]{14}, -13 + 2\sqrt[4]{14}) (2, \sqrt[4]{14}) \\
= (9 + 16\sqrt[4]{14}, -13 + 2\sqrt[4]{14}) (2, \sqrt[4]{14}) \\
= (9 + 16\sqrt[4]{14} - 2\sqrt[4]{14} - 9) \\
= (9, -2 + \sqrt[4]{14}) (2, \sqrt[4]{14}) \\
= (18, 9\sqrt[4]{14}, -4 + 2\sqrt[4]{14}, -2\sqrt[4]{14} - 14) \\
\Rightarrow -2 + \sqrt[4]{14} \quad \text{note} (-2 + \sqrt[4]{14})(-2 - \sqrt[4]{14}) = 18 \quad \text{is principal.} \]
Example. Compute $\text{Cl}(\mathcal{O}_F)$ for $F = \mathbb{Q}(\sqrt{-39})$.

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

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

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

So we see that $\# \text{Cl}(\mathcal{O}_F) \leq 4$, at best shoot by $(1), (2, \alpha), (2, \alpha-1), (3, \alpha + 1)$

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

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

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

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

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

if $\text{Nm}\left(\frac{a + \sqrt{-39}b}{2}\right) = 3$ 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 $\text{Cl}(\mathcal{O}_F)$.

and thus an element of order 2 in $\text{Cl}(\mathcal{O}_F)$, $a_0[3] = [(3, \alpha + 1)]^2$

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

$= \alpha - 10$

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

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

$= (12, 3\alpha + 6, 4\alpha + 4, \alpha^2 + 3\alpha + 2 = 4\alpha - 8)$

$\Rightarrow$ gives $\alpha - 2$

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

$\Rightarrow \text{Cl}(\mathcal{O}_F) \cong \mathbb{Z}/4\mathbb{Z}$.

Exercise. Show explicitly that $(2, \alpha)^4 = (\alpha + 2)$.
• 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 $r = r_1 + 2r_2 - 1$ multiplicatively independent units of infinite order: there are units with infinite order $s.t.$

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

($u_i, \ldots, u_r$ multi. indep. means $u_i^{n_i} \cdots u_r^{n_r} = 1 \iff \text{all } n_i = 0$)

Abstractly, $\mathcal{O}_F^\times \cong \mathbb{Z}^{r_1 + r_2 - 1} \times (\mu(F))$ 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, $\mathcal{O}_F^\times = \{ u \in \mathcal{O}_F : s.t. Nm(u) \in \{ \pm 1 \} \}$

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

Example: (Pell’s equation) $x^2 - dy^2 = 1$ for $d \in \mathbb{N}_1$ square-free

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

So a soln to Pell’s equation $\Rightarrow$ a unit $x + y\sqrt{d} \in (\mathbb{Z}[\sqrt{d}])^\times$

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

By Dirichlet’s theorem, $\mathcal{O}_F^\times = \{ 1 \} \times \gamma^{2z}$, with $\gamma = a + b\sqrt{d}$ $\ a, b \in \mathbb{Z}_{>0}$

Pell’s equation has a fundamental soln $(x_0, y_0)$

$\Rightarrow a + b\sqrt{d} \iff Nm(a + b\sqrt{d}) = 1$

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

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

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

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

The fundamental soln to $x^2 - 10y^2 = 1$ comes from

$(3 + \sqrt{10})^2 = 19 + 6\sqrt{10} \Rightarrow$ fundamental soln $(19, 6)$.

Note: $(19 + 6\sqrt{10})^2 = 721 + 228\sqrt{10}$ and $(19 + 6\sqrt{10})^3 = 27379 + 8658\sqrt{10}, \ldots$
Lecture IV: Unit Groups 2

Thursday, May 24, 2018 10:50 PM

Visualize: \( F \hookrightarrow \mathbb{R}^2 \) with \( a + b \sqrt{\alpha} \mapsto (a + b \sqrt{\alpha}, a - b \sqrt{\alpha}) \)

The image of \( \mathcal{O}_F \) in \( \mathbb{R}^2 \) lies on the hyperbola.

Note: the fundamental unit could be large, e.g., \( \mathcal{F} = \mathcal{O}(\sqrt{\alpha}) \), \( u = 2143295 + 221064 \sqrt{\alpha} \).

Example: \( \mathcal{F} = \mathcal{O}(\mathbb{Z}[\zeta_n]) \), \( [\mathcal{F} : \mathcal{O}] = \varphi(n) = \#(\mathbb{Z}/n) \).
Assume \( n > 2 \).

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

When \( n > 3 \), all embeddings of \( \mathcal{F} \) are complex \( \Rightarrow \frac{1}{2} \varphi(n) \) pair of embeddings.

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

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

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

\[
\frac{\zeta_n - 1}{\zeta_n - 1} = \frac{(\zeta_n^i)^{j-1} - 1}{\zeta_n^i - 1} = 1 + \zeta_n + \zeta_n^2 + \ldots + \zeta_n^{j-1} \in \mathcal{O}_F
\]

Yet \( \frac{\zeta_n - 1}{\zeta_n - 1} = (-\zeta_n^i) \frac{\zeta_n^i - 1}{\zeta_n - 1} \)

so up to roots of unity, these two are essentially the same.

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

\( \Rightarrow [\mathcal{O}_F^\times : \langle \frac{\zeta_n^i - 1}{\zeta_n - 1} : 1 \leq i \leq \frac{n}{2}, \gcd(i, n) = 1 \rangle] \) 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 \( \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \) when \( \Re(s) > 1 \).

\( \zeta(s) \) 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.
Dedekind zeta function for a number field $F$

$$\zeta_F(s) = \sum_{I \in \mathcal{O}_F, \text{nonzero ideal}} \frac{1}{N(I)^s} = \prod_{p \text{ prime idele}} \frac{1}{1 - N(p)^{-s}} \quad \text{Res} > 1$$

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

- meromorphic cont. 
  - function $\zeta_{\mathbb{Q}(i)}(s) \in \mathbb{C}$ for $s \in \mathbb{C} \setminus \{s \mid \text{Res } s = \frac{1}{2}\}$
- Special value: $$\zeta_{\mathbb{Q}(i)}(s) \sim \frac{\Gamma(\frac{s}{2}) \Gamma(s)}{\pi^{\frac{s}{2}} (2\pi)^s \Gamma(s - \frac{1}{2})}$$ near $s = 1$ has arithmetic info.

E.g. $F = \mathbb{Q}(\sqrt{-d})$

$$\lim_{s \to 1} (s-1) \zeta_F(s) = \frac{2\pi \cdot \# \mathcal{O}_F^*}{\# \mathcal{O}_F^* (\mathcal{O}_F)} = \left\{ \begin{array}{ll} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{if } d \equiv 2,3 \mod 4 \end{array} \right.$$ 2 unless $d = 1$ or $3$

Special values of generalized zeta functions are related to important arithmetic 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., $\mathcal{O}_F^*$ is infinite
* $F = \mathbb{Q}(\sqrt{-19})$ has class number 1 but not a Euclidean domain