13.4. ≈ 14.1.

(4) All of this is related to AG.

(Spec $\mathcal{O}_L$ / Spec $\mathcal{O}_K$ is a branched cover. These are curves.)

(5) There is a valuation theoretic version too.

Proof of theorem. At one point, will assume $A = \mathbb{Z}$ (or any PID, s.t. B is a free A-module). By CRT,

$$B/\mathfrak{p}B \cong B/\mathfrak{P}_1^{e_1} \oplus \cdots B/\mathfrak{P}_g^{e_g}.$$

Will prove:

(1) $[B/\mathfrak{p}B : A/\mathfrak{p}] = n$ (as $A/\mathfrak{p}$-modules)

(2) $[B/\mathfrak{P}_i^{e_i} : A/\mathfrak{p}] = e_i f_i$.

Proof of (1). (asserted before)

B is a free $A(=\mathbb{Z})$-module of rank n. (big theorem)
(This uses our hypothesis)

Write $B = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$

Let $\bar{a}_i = a_i \pmod{\mathfrak{p}B}$.

Claim. $\bar{a}_1, \ldots, \bar{a}_n$ is a basis for $[B/\mathfrak{p}B : A/\mathfrak{p}]$.

Proof. Note $B/\mathfrak{p}B = \mathbb{Z}\bar{a}_1 + \cdots + \mathbb{Z}\bar{a}_n$ spanning is clear.

To prove independence,

suppose $c_1\bar{a}_1 + \cdots + c_n\bar{a}_n = 0$ in $B/\mathfrak{p}B$. $c_i \in A/\mathfrak{p}$.

Choose arbitrary lifts of the c_i to d_i in A.

So, $d_1\bar{a}_1 + \cdots + d_n\bar{a}_n \in \mathfrak{p}B = (p)B$ | Use our assumption that $A = \mathbb{Z}$ is a PID.

$$\frac{d_1}{p}a_1 + \cdots + \frac{d_n}{p}a_n \in B.$$

But $B = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$, so each $\frac{d_n}{p}$ is an integer, so p divides all the d_n,

so the c_i are all 0 in $A/\mathfrak{p}$.

13.5. 214.2

(2). This is easy.

We saw in our discussion of norms that

$$B/\underline{p}_i \cong \underline{p}_i/\underline{p}_i^2 \cong \underline{p}_i^2/\underline{p}_i^3 \cong \cdots \underline{p}_i^{e_i-1}/\underline{p}_i^{e_i}$$

as $B/\underline{p}_i$-modules.

And so each has the same size.

So $\quad [B/\underline{p}_i^{e_i} : A/p] = e_i [B/\underline{p}_i : A/p]$

which equals $e_i f_i$ by definition.

Note. See Milne or Neukirch for a fancier proof which is valid when A is not a PID.

14.4.

(3). By CRT, $\mathcal{O}_L/p\mathcal{O}_L \cong \bigoplus_i \mathcal{O}_L/\mathfrak{p}_i^{e_i}$ as rings, and as $\mathbb{Z}/p\mathbb{Z}$-vector spaces.

Let $S_i = \{\alpha_1, \ldots, \alpha_{n_i}\}$ be a basis for $\mathcal{O}_L/\mathfrak{P}_i^{e_i}$ as a $\mathbb{Z}/p\mathbb{Z}$-vector space.

Then $T = \bigcup_{i=1}^{g} S_i$ is a basis for $\mathcal{O}_L/p\mathcal{O}_L$ over $\mathbb{Z}/p$.

Now different S_i's don't mix.

If $\beta_i \in S_i$ and $\beta_j \in S_j$ with $i \neq j$ then $\beta_i \cdot \beta_j = 0$.

This means $\left(\mathrm{Tr}_{\alpha,\alpha' \in T}(\alpha\alpha')\right)$ is a block matrix

$$\begin{pmatrix} \left(\mathrm{Tr}_{\alpha,\alpha'\in S_1}(\alpha\alpha')\right) & & 0 \\ & \ddots & \\ 0 & & \left(\mathrm{Tr}_{\alpha,\alpha'\in S_g}(\alpha\alpha')\right) \end{pmatrix}$$

and so can take a block determinant,

$$\det\left(\mathrm{Tr}_{\alpha,\alpha'\in T}(\alpha\alpha')\right) = \prod_{i=1}^{g} \det\left(\mathrm{Tr}_{\alpha,\alpha'\in S_i}(\alpha\alpha')\right)$$

i.e.

$$\mathrm{Disc}\left(\mathcal{O}_L/p\mathcal{O}_L \big/ \mathbb{Z}/p\mathbb{Z}\right) = \prod_{i=1}^{g} \mathrm{Disc}\left(\mathcal{O}_L/\mathfrak{p}_i^{e_i} \big/ \mathbb{Z}/p\mathbb{Z}\right)$$

as elements of $\mathbb{Z}/p\mathbb{Z}$.

14.3. **Theorem.** A prime $p \in \mathbb{Z}$ ramifies in $\mathcal{O}_L$ iff $p \mid \operatorname{Disc}(\mathcal{O}_L/\mathbb{Z})$.

A more general statement is true, but we didn't define the "relative discriminant".

Cor. Only finitely many primes ramify.

Proof. (following Rafe Jones) Write $p\mathcal{O}_L = \underline{P}_1^{e_1} \cdots \underline{P}_g^{e_g}$.

Show $p \mid \operatorname{Disc}(\mathcal{O}_L/\mathbb{Z}) \longleftrightarrow \operatorname{Disc}(\mathcal{O}_L/\mathbb{Z}) \equiv 0 \pmod p$ (clear)

$\xleftrightarrow{(2)} \operatorname{Disc}(\mathcal{O}_L/p\mathcal{O}_L \mid \mathbb{Z}/p\mathbb{Z}) = 0$ (in $\mathbb{Z}/p$)

$\xleftrightarrow{(3)} \prod_{i=1}^{g} \operatorname{Disc}(\mathcal{O}_L/\underline{P}_i^{e_i} / \mathbb{Z}/p\mathbb{Z}) = 0$

$\xleftrightarrow{(4)} e_i > 1$ for some i.

Proof.

(2). Let $\alpha_1, \dots, \alpha_n$ be an integral basis of $\mathcal{O}_L/\mathbb{Z}$.

We showed last time, $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ is a $\mathbb{Z}/p$-basis for $\mathcal{O}_L/p$.

Here $\bar{\alpha}_i = \alpha_i \pmod p$.

We have a ring homomorphism
$$\mathcal{O}_L \longrightarrow \mathcal{O}_L/p\mathcal{O}_L,$$
$$\alpha \longrightarrow \alpha + p\mathcal{O}_L$$

and so $\operatorname{Tr}(\bar{\alpha}_i \bar{\alpha}_j) = \overline{\operatorname{Tr}(\alpha_i \alpha_j)}$.

Just change the order in which you reduce mod p.

det(RHS) is $\operatorname{Disc}(\mathcal{O}_L/\mathbb{Z}) \bmod p$

det(LHS) is $\operatorname{Disc}(\mathcal{O}_L/p\mathcal{O}_L \mid \mathbb{Z}/p\mathbb{Z})$.

14.5. We want to prove $\mathrm{Disc}\left(\mathcal{O}_L/\underline{P}^e / \mathbb{Z}/p\mathbb{Z}\right) = 0$ if $e > 1$.
(converse later)

This is a question of nilpotents.

If $b \in \underline{P} \setminus \underline{P}^2$, then $b \neq 0$ in $\mathcal{O}_L/\underline{P}^e$
but $b^e = 0$ in $\mathcal{O}_L/\underline{P}^e$.

Let $\underset{\underset{\alpha_1}{\|}}{b}, \alpha_2, \dots, \alpha_\ell$ be a basis for $(\mathcal{O}_L/\underline{P}^e) \mid (\mathbb{Z}/p)$.

Claim. $\mathrm{Tr}(b\alpha_j) = 0$ for $j = 1, \dots, \ell$.

Thus, the first row of the matrix $\mathrm{Tr}(\alpha_i \alpha_j)$ will all be zeroes.

So the determinant $\left(= \mathrm{Disc}\left(\mathcal{O}_L/\underline{P}^e / \mathbb{Z}/p\mathbb{Z}\right)\right)$ will be 0.

Proof of claim. We know $(b\alpha_j)^e = 0$ for each j.

So, if M is the endomorphism $x \longrightarrow b\alpha_j x$, then $M^e = 0$.
(because $(b\alpha_j)^e x = 0$ for all x.)

The matrix M satisfies $X^e = 0$, so min poly of M divides X^e.

Recall linear algebra facts about the minimum and characteristic polynomials of a matrix.

(min. poly: min polynomial $f(t)$ s.t. $f(M) = 0$)

(char. poly.: $f(t) = \det(tI - M)$)

Then: (roots of min poly) = (roots of char poly)
= (eigenvalues of M)

also: (min poly.) | (char poly.) (Cayley - Hamilton)

* in this case we know the characteristic polynomial is
$f(t) = t^m$ for some m.

The t^{m-1} coefficient is the negative of the trace.

So $\mathrm{Tr}(M) = 0$.

<u>14.6</u>.

To show the converse:

$\mathcal{O}_L / \underline{P}$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$.

It is <u>separable</u> (D-F, Ch. 13, Cor 39)

And any finite separable extension has nonzero discriminant.

15.1. The factorization theorem.

Notation. Given $f(x) \in \mathbb{Z}[x]$ and $p \in \mathbb{Z}$, denote by $\bar{f}(x)$ the reduction in $\mathbb{Z}/p\mathbb{Z}[x]$.

Theorem. Let L be a number field, α a primitive element, $L = \mathbb{Q}(\alpha)$. Let $g(x) \in \mathbb{Z}[x]$ be the minimum polynomial. Suppose $p \nmid [\mathcal{O}_L : \mathbb{Z}[\alpha]]$ and that g is monic (i.e. $\alpha \in \mathcal{O}_L$).

Write $\bar{g} = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}$ in $\mathbb{Z}/p\mathbb{Z}[x]$ with $g_i \in \mathbb{Z}[x]$, $\bar{g}_i$ irred.

Then,

$$p\mathcal{O}_L = \underline{P}_1^{e_1} \cdots \underline{P}_r^{e_r}$$ is the factorization of p into primes, with

$$\underline{P}_i = (p, g_i(\alpha)) = p\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L.$$

Moreover, $f(\underline{P}_i \mid p) = \deg g_i$.

Proof. (Marcus's book)

Will show:

(1) For each i, $\underline{P}_i := (p, g_i(\alpha))$ is either $\mathcal{O}_L$, or $\mathcal{O}_L/\underline{P}_i$ is a field of order $p^{\deg g_i}$.

(In fact, as we'll see, $\mathcal{O}_L$ can't happen.)

(2) $\underline{P}_i + \underline{P}_j = \mathcal{O}_L$.

(3) $p\mathcal{O}_L \mid \underline{P}_1^{e_1} \cdots \underline{P}_r^{e_r}$.

15.2.

Assuming this: Rearrange so that $\underline{P}_1, \dots, \underline{P}_s \neq \mathcal{O}_L$,

$\underline{P}_{s+1}, \dots, \underline{P}_r = \mathcal{O}_L$.

Then, the $\underline{P}_i$ are primes lying over p. (since $p \in \underline{P}_i$, $\mathcal{O}_L/\underline{P}_i$ is a field)

We have $f(\underline{P}_i \mid p) = \deg g_i$, because $|\mathcal{O}_L/\underline{P}_i| = p^{\deg g_i}$.

By (2), all the $\underline{P}_i$ are distinct.

(3) shows $p\mathcal{O}_L \mid \underline{P}_1^{e_1} \cdots \underline{P}_s^{e_s}$ (ignore the ones that are just $\mathcal{O}_L$.)

So $p\mathcal{O}_L = \underline{P}_1^{d_1} \cdots \underline{P}_s^{d_s}$ with $d_i \le e_i$.

By e-f-g,

$$[L:\mathbb{Q}] = \sum_{i=1}^{s} d_i \cdot \deg g_i$$

But we know

$$[L:\mathbb{Q}] = \sum_{i=1}^{r} e_i \cdot \deg g_i \quad \text{(by our prime factorization)}$$

and so the d_i are equal to the e_i and none of the $\underline{P}$'s are $\mathcal{O}_L$.

Proof of (1), (2), (3).

(1). We have natural maps

$$\begin{array}{ccccc} \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}[x]/(p) & \longrightarrow & \mathbb{Z}[x]/(p, g_i(x)) \\ & & \wr\!\!\parallel & & \wr\!\!\parallel \\ & & \mathbb{F}_p[x] & \longrightarrow & \mathbb{F}_p[x]/\overline{g_i(x)} \end{array}$$

Because $\overline{g_i(x)}$ is irred / $\mathbb{F}_p$, this last is a field.

15.3.

Now if we had $\mathcal{O}_L = \mathbb{Z}[\alpha]$, would like to say

$$\mathcal{O}_L = \mathbb{Z}[\alpha] \longrightarrow \mathcal{O}_L/(p) \longrightarrow \mathcal{O}_L/(p, g_i(\alpha)) \cong \mathbb{F}_p[x]/\overline{g_i(x)}$$

but it is not evident that ~~you~~ all of $\mathcal{O}_L$ isn't in the kernel.

Also, don't necessarily have $\mathcal{O}_L = \mathbb{Z}[\alpha]$. (Can prove above. See Murty-Esmonde p.65)

Instead, look at

$$\Phi : \mathbb{Z}[x] \xrightarrow{\text{not nec. inj. or onto.}} \mathcal{O}_L \longrightarrow \mathcal{O}_L/\mathfrak{P}_i = \mathcal{O}_L/(p, g_i(\alpha)).$$
$$x \longrightarrow \alpha$$

Visibly, $(p, g_i(x)) \subseteq \ker \Phi$, and so $\ker \Phi$ is either $(p, g_i(x))$ or all of $\mathbb{Z}[x]$.

Claim. Φ is surjective.

Proof. The image is $\mathbb{Z}[\alpha] + \mathfrak{P}_i$ (as a union of $\mathfrak{P}_i$ cosets of $\mathcal{O}_L$).

WTS it's all of $\mathcal{O}_L$:

$[\mathcal{O}_L : \mathbb{Z}[\alpha] + p\mathcal{O}_L]$ divides both $[\mathcal{O}_L : \mathbb{Z}[\alpha]]$ and $[\mathcal{O}_L : p\mathcal{O}_L] = p^{[L:\mathbb{Q}]}$

but these are coprime.

So $[\mathcal{O}_L : \mathbb{Z}[\alpha] + p\mathcal{O}_L] = 1$, proves claim.

Now, so what? Get a surjection

$$\mathbb{Z}[x]/(p, g_i(x)) \longrightarrow \mathcal{O}_L/\mathfrak{P}_i$$

so $\mathcal{O}_L/\mathfrak{P}_i$ is trivial, or it is an isomorphism.

(Note: Previous arg. shows: ...

15.4.

Proof of (2). The $\bar{g}_i$ are distinct irreducibles in $\mathbb{F}_p[x]$.

We can therefore solve $\bar{h}\bar{g}_i + \bar{k}\bar{g}_j = 1$ in $\mathbb{F}_p[x]$

i.e. $hg_i + kg_j \equiv 1 \mod p$.

Evaluate at $x = \alpha$:

$$g_i(\alpha)h(\alpha) + g_j(\alpha)k(\alpha) \equiv 1 \pmod p$$

so that $1 \in (p, g_i(\alpha), g_j(\alpha)) = \underline{P}_i + \underline{P}_j$.

Proof of (3).

We have $\underline{P}_1^{e_1} \cdots \underline{P}_r^{e_r} = (p, g_1(\alpha))^{e_1} \cdots (p, g_r(\alpha))^{e_r}$

$$\subseteq (p, g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r}).$$

Claim. This ideal is just $(p) = p\mathcal{O}_L$. (in which case we're done.)

Need to show $g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r}$ is a multiple of p.

~~Mod p, it reduces to~~ $\cancel{g_1(\alpha)^{e_1} g_2(\alpha)}$

Mod p, we have $\overline{g_1(x)}^{e_1} \cdots \overline{g_r(x)}^{e_r} = \overline{g(x)}$,

so $g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r} - g(\alpha) = $ (multiple of p),

and $g(\alpha) = 0$. So we are done.

15.5.

Examples of prime decomposition.

Let $L = \mathbb{Q}(\sqrt{D})$ with $D \equiv 3 \pmod 4$.

Then $\mathcal{O}_L = \mathbb{Z}[\sqrt{D}]$, a min poly. is $x^2 - D = 0$.

By Theorem, (note $[\mathcal{O}_L : \mathbb{Z}[\sqrt{D}]] = 1$ — hypothesis is empty)

$$p\mathcal{O}_L = \begin{cases} \text{prime} & \longleftrightarrow \quad x^2 - D \text{ irred.}/\mathbb{F}_p \longleftrightarrow \left(\frac{D}{p}\right) = -1. \\ \underline{p} \cdot \underline{p}' & \longleftrightarrow \quad x^2 - D \text{ factors }/\mathbb{F}_p \longleftrightarrow \left(\frac{D}{p}\right) = 1. \\ \underline{p}^2 & \longleftrightarrow \quad x^2 - D = (x-a)^2 \text{ in } \mathbb{F}_p \\ & \qquad \longleftrightarrow p \mid D, \text{ i.e. } \left(\frac{D}{p}\right) = 0. \end{cases}$$

(exercise. do for any D)

<u>Ex</u>. Let $L = \mathbb{Q}(i)$, choose $\alpha = 3i$.

The min poly of α is $x^2 + 9$.

Mod 3, $x^2 + 9 \equiv x^2$.

If the method applied, we would say (3) ramifies.

But (3) is prime.

<u>Problem</u>. $\mathcal{O}_L / \mathbb{Z}[\alpha] = \mathcal{O}_L / 3\mathbb{Z}[i]$ has 9 elements.

<u>Note</u>. If $p \mid [\mathcal{O}_L : \mathbb{Z}[\alpha]]$ then $p^2 \mid \mathrm{Disc}(\mathbb{Z}[\alpha]/\mathbb{Z})$.

So you can check that a given α is okay for all but finitely many p.

<u>Note</u>. Not all rings of integers have a power basis!

16.1. Fractional ideals and the class group.

The motivating result.

Given $\begin{array}{ccc} L & - & B \\ | & & \\ K & - & A \end{array}$. Given an ideal $\mathfrak{a}$ in B.
Then there exists an ideal $\mathfrak{a}' \in B$
s.t. $\mathfrak{a}\mathfrak{a}'$ is principal.

Proved in MF, Theorem 67.

Cheating proof. Pick some $\alpha \in \mathfrak{a}$.
If you like, can choose α in A even.
(Take its norm)

Then $(\alpha) \subseteq \mathfrak{a}$. So $\mathfrak{a} \mid (\alpha)$.
By unique factorization $(\alpha) = \mathfrak{a}\mathfrak{a}'$ for some $\mathfrak{a}'$.

We can think of $\dfrac{\mathfrak{a}'}{\alpha} := \{ x \in L : \alpha x \in \mathfrak{a}' \}$ as an inverse to $\mathfrak{a}$. So, $\mathfrak{a} \cdot \dfrac{\mathfrak{a}'}{\alpha} = (1) = B$.

Need to make this precise.

Def. (fractional ideals)
Let B be a Dedekind domain with fraction field L.
A fractional ideal of B is a (nonzero) submodule $\mathfrak{a}$ of L
such that, equivalently:

(1) $d\mathfrak{a} \subseteq B$ for some $d \in B$.

(2) $\mathfrak{a}$ is finitely generated as a B-module.

The difference between an ideal and a fractional ideal:
A fractional ideal lives in L, not necessarily B.
But it is closed only under multiplication by B.
"Real" ideals are sometimes called integral ideals.

Exercise. Prove $(1) \longleftrightarrow (2)$.

Def. If $b \in L$ then $(b) = bB$ is the principal fractional ideal generated by b.

(If $b \in B$ it is an integral ideal.)

Define products as with integral ideals.

Check, e.g. that $(b)(b') = (bb')$

(product of two princ. frac. ideals also princ.)

~~Next~~

Theorem. Let B be a Dedekind domain. Then,

(1) all fractional ideals are invertible.

(i.e. given $\underline{a}$ there exists $\underline{a}^{-1}$ with $\underline{a} \cdot \underline{a}^{-1} = B$.)

(2) So, $I(B) :=$ {all fractional ideals} forms a group.

(3) Every fractional ideal decomposes uniquely as a product of primes (with neg. exponents allowed)

(4) So, $I(B)$ is the free abelian group on the set of primes.

(5) $P(B) :=$ {all principal fractional ideals} also forms a group, a subgroup of $I(B)$.

Proof. (1) Given $\underline{a}$ and $a \in \underline{a}$, find $\underline{a}'$ with $\underline{a}\,\underline{a}' = (a)$.

Define $\underline{a}^{-1} := \frac{1}{a}\underline{a}' = \left\{ \frac{x}{a} : x \in \underline{a}' \right\}$.

This is a fractional ideal. (The $\frac{1}{a}$ is along for the ride.)

In fact this was a bit sloppy. Only proved when $\underline{a}$ is an integral ideal!

(—)

Know, $d\underline{a}$ is an integral ideal for some $d \in B$
(one of our two definitions)

Find $(d\underline{a})'$ with $(d\underline{a})(d\underline{a})' = a$ for some $a \in d\underline{a}$

Then $\frac{1}{a}(d\underline{a})'$ is an inverse for $d\underline{a}$

and so $\frac{d}{a}(d\underline{a})'$ is an inverse for $\underline{a}$.

(2) easy.

(3). Follows from unique factorization for integral ideals.

Choose d with $d\underline{a} \subseteq B$, so $d\underline{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$ $(r_i, s_i \geq 0)$

$(d) = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$

Then $\underline{a} = \mathfrak{p}_1^{r_1 - s_1} \cdots \mathfrak{p}_m^{r_m - s_m}$.

What if we looked at $d'\underline{a} \subseteq B$ for some other d'?

Use unique factorization of $dd'\underline{a}$.

(Ex. Work out the details.)

(4), (5) easy.

Ex. In $\mathbb{Z}$, $\left(\frac{3}{4}\right) = (3)(2)^{-2}$.

Indeed, all ideals are principal
and so are fractional ideals, because $(a)^{-1} = (a^{-1})$.

Remark. (1) is not true, e.g. in nonmaximal orders.

We have $P(B) \subseteq I(B)$.

Def. $Cl(B) := I(B)/P(B)$ is called the (ideal) class group.

Its order is called the class number. ("if" finite)

If $B = \mathcal{O}_L$, write $Cl(L)$ too.

Also write $h_L = h(L) = \# Cl(\mathcal{O}_L)$.

Represents failure of L to be a PID.

16.4. Example. Let $L = \mathbb{Q}(\sqrt{-23})$, $\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$.

Consider $\underline{a} = \left(2, \frac{1+\sqrt{-23}}{2}\right)$. Has norm 2. (explain why)

$$\underline{a}^2 = \left(4, 1+\sqrt{-23}, \tfrac{1}{4}(-22+2\sqrt{-23})\right)$$
$$= \left(4, 1+\sqrt{-23}, \tfrac{-11}{2} + \tfrac{1}{2}\sqrt{-23}\right).$$

Note: Twice #3 is $-11+\sqrt{-23}$
add 12. Get second.

$$= \left(4, \tfrac{-11}{2} + \tfrac{1}{2}\sqrt{-23}\right)$$
$$= \left(4, \tfrac{-3}{2} + \tfrac{1}{2}\sqrt{-23}\right).$$

norm of second elt:
$\frac{1}{4}(9+23) = 8.$
Doesn't give us 4.

$$\underline{a}^3 = \left(4, \tfrac{-3}{2} + \tfrac{1}{2}\sqrt{-23}\right)\left(2, \tfrac{1+\sqrt{-23}}{2}\right)$$
$$= \left(8, -3+\sqrt{-23}, 2+2\sqrt{-23}, \tfrac{1}{4}(-3+\sqrt{-23})(1+\sqrt{-23})\right)$$
$$= \left(8, -3+\sqrt{-23}, 2+2\sqrt{-23}, \tfrac{1}{4}(-26-2\sqrt{-23})\right)$$
$$= \left(8, -3+\sqrt{-23}, 2+2\sqrt{-23}, \tfrac{3}{2} - \tfrac{\sqrt{-23}}{2}\right).$$

Note: $(\#4)\cdot(-4) = \#2$. So can remove #2.
$\#4 \cdot 4$ is $6 - 2\sqrt{-23}$
subtract from 8: can get #3.

$$= \left(8, \tfrac{3}{2} - \tfrac{\sqrt{-23}}{2}\right)$$

Now $\left(\frac{3}{2} - \frac{\sqrt{-23}}{2}\right)\left(\frac{3}{2} + \frac{\sqrt{-23}}{2}\right)$

$$= \tfrac{1}{4}(3^2+23) = 8.$$

Bingo. $\underline{a}^3 = \left(\frac{3}{2} + \frac{\sqrt{-23}}{2}\right)$.

16.5,

This proves $\mathbb{Z}/3\mathbb{Z} \subseteq Cl(\mathcal{O}_L)$.

In fact, $Cl(\mathcal{O}_L) = \mathbb{Z}/3\mathbb{Z}$, but how would we show that?

One <u>formula</u>. If $L = \mathbb{Q}(\sqrt{-D})$ D a fund. disc., not $-3, -4$,

then
$$h(-D) = \frac{\sqrt{|D|}}{\pi} \cdot \sum_{m=1}^{\infty} \left(\frac{-D}{m}\right) \cdot \frac{1}{m}.$$

So, e.g.
$$h(-23) = \underbrace{\frac{\sqrt{23}}{\pi}}_{1.526} \cdot \underbrace{\left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} - \frac{1}{7} \cdots\right.}_{\text{This part is } 1.907\ldots}$$

So $2.91\ldots$ so far!

Also have
$$h(-D) = \frac{-1}{|D|} \cdot \sum_{m=1}^{D} m \left(\frac{-D}{m}\right).$$

(Try it!)

In general,
$$h_K = \frac{\#(\text{roots of unity}) \cdot \sqrt{|\mathrm{Disc}(K)|}}{2^{r_1} \cdot (2\pi)^{r_2} \cdot \mathrm{Regulator}(K)} \cdot \lim_{s \to 1} (s-1)\, \zeta_K(s)$$

$$\zeta_K(s) = \sum_{\mathfrak{a} \trianglelefteq \mathcal{O}_K} (N\mathfrak{a})^{-s}.$$

Prototype for BSD.

Now, guess: if $\left(\frac{-D}{m}\right)$ is "random" then $h(-D) \approx \frac{\sqrt{D}}{\pi}$.

Ex. $h(-163) = \frac{\sqrt{163}}{\pi} \cdot \left(1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8} + \frac{1}{9} \cdots\right)$

so far, $0.9206\ldots$

17.1. Finiteness of the class number.

(Recall definitions)

<u>Theorem</u>. Let $h(K) := \mathcal{I}(K)/P(K)$.

Then $h(K)$ is finite.

How do we prove that?

Theorem. (N. 1.6.2) Suppose $[K:\mathbb{Q}] = n$ and $\mathfrak{a} \subseteq \mathcal{O}_K$.
Let $\Delta_K = \mathrm{Disc}(\mathcal{O}_K/\mathbb{Z})$ and let $2s = \#$ embeddings $K \hookrightarrow \mathbb{C}$.
Then $\mathfrak{a}$ contains a nonzero element a s.t.

$$|N_{K/\mathbb{Q}}(a)| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s N(\mathfrak{a})\,|\Delta_K|^{1/2}.$$

<u>Corollary</u>. With the same notation, any element of the class group is represented by some integral ideal $\mathfrak{a}$, s.t.

$$|N(\mathfrak{a})| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \cdot |\Delta_K|^{1/2}.$$ (the <u>Minkowski bound</u>)

<u>Proof of</u> cor.

Given an elt. of the class group, choose an arbitrary representative $\mathfrak{a}_1$, ~~such that~~ and $\gamma \in \mathcal{O}_K$ ($\gamma \neq 0$) s.t. $\mathfrak{b} := \gamma\mathfrak{a}_1^{-1} \subseteq \mathcal{O}_K$.

(Note: In fact, can choose $\mathfrak{a}_1$ s.t. $\mathfrak{a}_1^{-1}$ is integral.)

Then there exists $a \in \mathfrak{b}$ with

$$|N(a)| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s N(\mathfrak{b})\,|\Delta_K|^{1/2},$$

~~but N(b) = N(γ)/N(a)~~

Note, $\mathfrak{b} \mid (a)$, so $(a)\mathfrak{b}^{-1}$ is an integral ideal,

$$N(a\mathfrak{b}^{-1}) = \frac{|N(a)|}{N(\mathfrak{b})} \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |\Delta_K|^{1/2}$$ <u>AWD</u>.

17.2.

Now, $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \cdot |\Delta_K|^{1/2}$ is fixed for any given K, so finiteness of the class number follows from:

<u>Proposition</u>. Given any M and K,

$$\{\underline{a} \subseteq \mathcal{O}_K : N(\underline{a}) < M\} \text{ is finite.}$$

<u>Proof</u>. By writing $\underline{a} = \underline{p}_1^{m_1} \cdots \underline{p}_r^{m_r}$, $N(\underline{a}) = \prod N(\underline{p}_i)^{m_i}$, it is enough to show this for <u>prime</u> ideals.

The set of primes $p < M$ is finite, and there are finitely many primes $\underline{P}$ over p, all with $N(\underline{P}) \geq p$, and so <u>we're done</u>.

<u>Remark</u>. In fact, $\{\underline{a} \subseteq \mathcal{O}_K : N(\underline{a}) < M\} < M(1+\log M)^{[K:\mathbb{Q}]}$.

<u>Corollary of corollary</u>. Given any number field K,

$$|\Delta_K| \geq \left(\frac{n^n}{n!}\right)^2 \cdot \left(\frac{\pi}{4}\right)^{2s}.$$

<u>Proof</u>. The cor. says that $1 \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \cdot |\Delta_K|^{1/2}$.

<u>Theorem</u>. There do not exist any unramified extensions of $\mathbb{Q}$.

<u>Proof</u>. Because $p \mid \mathrm{Disc}(K) \longrightarrow p$ ramifies in K,

ETS $$a_n := \left(\frac{n^n}{n!}\right)^2 \cdot \left(\frac{\pi}{4}\right)^{n} > 1.$$

We have $$\frac{a_{n+1}}{a_n} = \left[\frac{\left(\frac{n+1}{n}\right)^{n} \cdot (n+1)}{(n+1)}\right]^2 \cdot \left(\frac{\pi}{4}\right) = \left(\frac{\pi}{4}\right)\left(1+\frac{1}{n}\right)^n > 1.$$

(use some calculus)

In fact, by Stirling,

$$|\mathrm{Disc}(K)| \geq \left(e^2 \cdot \frac{\pi}{4} + o(1)\right)^n .$$

Remark. There do exist unramified extensions of fields other than $\mathbb{Q}$. In fact:

Def. For a number field K, the Hilbert class field is the largest algebraic extension H of K such that

(1) H/K is Galois with abelian Galois group;

(2) H/K is unramified.

(3) Every embedding $\sigma : K \hookrightarrow \mathbb{R}$ extends to an embedding $H \hookrightarrow \mathbb{R}$.

(The infinite valuations are unramified)

Theorem. H is a finite extension of K, and There exists a canonical homomorphism

$$Cl(\mathcal{O}_K) \xrightarrow{\sim} \mathrm{Gal}(H/K).$$

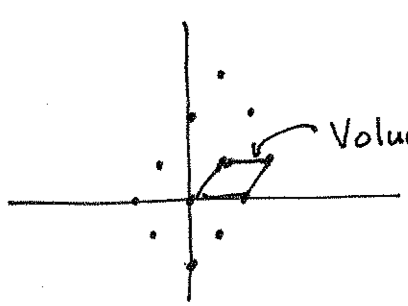
First theorem of class field theory.

Sketch of proof.

(1) There is an embedding of K into $\mathbb{R}^n$ ($n = [K:\mathbb{Q}]$) where $\mathcal{O}_K$ is a lattice, and any ideal $\underline{a} \subseteq \mathcal{O}_K$ is a lattice. Moreover, the "covolume" is $2^{-s} N(\underline{a}) \cdot |\Delta_K|^{1/2}$.

(s = # pairs of complex embeddings.

Example. $K = \mathbb{Q}(\sqrt{-3})$.

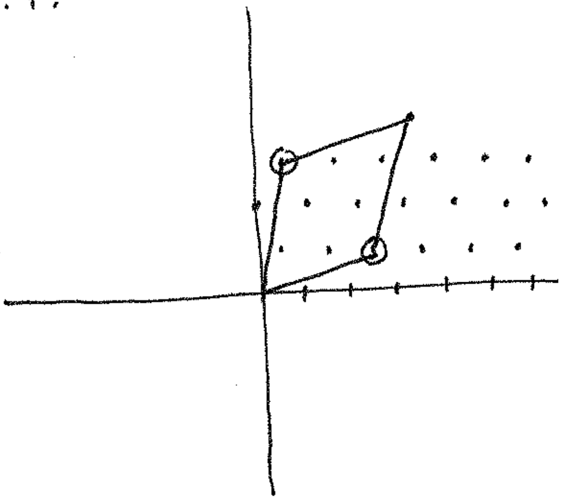


Covolume of $\mathcal{O}_K$ is $2^{-1} \cdot 1 \cdot \sqrt{|-3|}$. (matches).

Now, draw the ideal $\left(\frac{1+3\sqrt{-3}}{2}\right)$. (do it)

($\rightarrow$)

17.4.



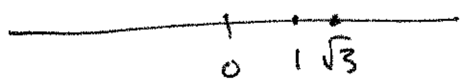
$$\left(\frac{1+3\sqrt{-3}}{2}\right)\cdot\left(\frac{1-\sqrt{-3}}{2}\right)$$
$$=\frac{1}{4}\left[1+9+2\sqrt{-3}\right]$$
$$=\frac{5}{2}+\frac{1}{2}\sqrt{-3}.$$

$$N\left(\frac{1+3\sqrt{-3}}{2}\right)=\left(\frac{1+3\sqrt{-3}}{2}\right)\left(\frac{1-3\sqrt{-3}}{2}\right)$$
$$=\frac{1}{4}(1+27)=7.$$

and $\left|\frac{1+3\sqrt{-3}}{2}\right|^2\cdot\sin(60^\circ)=7$ also.

If K is not imaginary quadratic, be more creative.

<u>Ex</u>. $K=\mathbb{Q}(\sqrt{3})$.



<u>not</u> a lattice.

(2) Minkowski's lattice point theorem.

Let $\Lambda \subseteq \mathbb{R}^n$ be a "full" lattice.

$T \subseteq \mathbb{R}^n$ convex, symmetric, and compact.

Then, if $\mathrm{Vol}(T) \geq 2^n \mathrm{Vol}(\Lambda)$, T contains a nonzero element of Λ.

(1) + (2) proves the theorem!

17.5 (probably postpone)

18.1. Recall: Main theorem; N. 1.6.2 (17.1), (i) from 17.3.

Def. Let V be a real vector space of dim. n.

A lattice $\Lambda \subseteq V$ is an additive subgroup

$$\mathbb{Z}e_1 + \dots + \mathbb{Z}e_r \quad , \text{ where the } e_i \text{ are linearly independent over } \mathbb{R}.$$

The e_i form a basis for the lattice.

If $r = n$ the lattice is full.

Prop. (Ex.) Λ is a lattice iff it is free of rank n and $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = V$. (equivalent characterization)

Prop. Λ is a lattice iff it is free of rank n and it is discrete.

(i.e., given $v \in \Lambda$, $\exists\ \varepsilon > 0$ s.t. $|v' - v| < \varepsilon \Rightarrow v' = v$.

Ex. Prove it. (takes some work)

For any $\lambda_0 \in \Lambda$ a full lattice we have a fundamental parallelepiped

$$D_{\lambda_0} := \{ \lambda_0 + \sum_{i=1}^{n} a_i e_i \ , \quad 0 \le a_i < 1 \}.$$

(a fundamental domain for Λ acting on $\mathbb{R}^n$ by addition).

Def. The volume (or covolume) of the lattice is $\mathrm{Vol}(D_{\lambda_0})$.

An alternative definition: Quotient measure, induced by Lebesgue measure and the projection $\mathbb{R}^n \to \mathbb{R}^n/\Lambda$.

($\mathbb{R}^n/\Lambda$ is compact.

So Λ is cocompact.)

18.2. Lattices and determinants:

If $\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$ where $e_i = \sum_{j=1}^{n} a_{ij} v_j$,

then we have $\mathrm{Vol}(\Lambda) = |\det(a_{ij})|$,

assuming $\mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_n$ is normalized to have volume 1.

(e.g. if $v_1 = (1, 0, 0, \ldots)$
$v_2 = (0, 1, 0, \ldots)$
etc. in $\mathbb{R}^n$).

Note also. If $e_1', \ldots, e_n'$ is another basis for Λ, the change of basis matrix is invertible, in $GL_2(\mathbb{Z})$.

So $\mathrm{Vol}(\Lambda)$ is independent of a choice of basis.

18.3.

Lemma. Let $S \subseteq V = \mathbb{R}^n$ measurable.

Λ full lattice in V.

If $\mu(S) > \mathrm{Vol}(\Lambda)$ then we can find $\alpha, \beta \in S$, $\alpha \neq \beta$, and $\beta - \alpha \in \Lambda$.

Proof. Think of this as obvious. (draw a picture)
(Prove the mapping $S \subseteq V \to V/\Lambda$ is not injective.)

A proof. Write $S = \bigcup_{\lambda_0 \in \Lambda} (S \cap D_{\lambda_0})$

By countable additivity $\mu(S) = \sum_{\lambda_0 \in \Lambda} \mu(S \cap D_{\lambda_0})$.

Now, $\sum_{\lambda_0 \in \Lambda} \mu((S \cap D_{\lambda_0}) - \lambda_0) = \mu(S) > \mathrm{Vol}(\Lambda)$.

This means, for some λ_0 and λ_0',

$(S \cap D_{\lambda_0}) - \lambda_0 \cap (S \cap D_{\lambda_0'}) - \lambda_0' \neq \phi$.

i.e. $\alpha - \lambda_0 = \beta - \lambda_0'$ for some $\alpha, \beta \in S$. QED.

Minkowski's lattice point theorem:

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice.

Let $T \subseteq \mathbb{R}^n$ be a set which is

convex (when $\alpha, \beta \in T$, the line joining them is in T)

symmetric ($\alpha \in T \to -\alpha \in T$).

If $\mu(T) > 2^n \mathrm{Vol}(\Lambda)$, then T contains a nonzero $\lambda \in \Lambda$.

18.4. (–19)

Proof. Apply the lemma to the lattice $2\Lambda := \{2 \cdot v : v \in \Lambda\}$.
$\mathrm{Vol}(2\Lambda) = 2^n \mathrm{Vol}(\Lambda)$,
so if $\mu(T) > 2^n \mathrm{Vol}(\Lambda)$ there exist $\alpha, \beta \in T$ with
$\alpha - \beta \in 2\Lambda$.

By symmetry, $-\beta \in T$.
By convexity, $\frac{\alpha - \beta}{2} \in T$. It's also in Λ. Q.E.D.

Note. If T is compact, can prove for $\mu(T) \geq 2^n \mathrm{Vol}(\Lambda)$.
Can cook up counterexamples when less.

Ideals and lattices.

Let $[K : \mathbb{Q}] = n$.
Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.
So is an ideal, because it's a submodule of $\mathcal{O}_K$.
So is a fractional ideal, because d times it is an ideal for some $d \in \mathbb{Z}$.

Want to regard it in $\mathbb{R}^n$.
Suppose K has r real embeddings $\sigma_1, \ldots, \sigma_r$ $K \hookrightarrow \mathbb{R}$
$2s$ complex ones $\sigma_{r+1}, \ldots \sigma_{r+s}$ and their complex conjugates.
$n = r + 2s$ by Galois theory.

Then define $\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \xrightarrow{\sim} \mathbb{R}^n$ (as vector spaces)
(non-canonically!
$\mathbb{C} \xrightarrow{\sim} \mathbb{R}^2$
$1 \longrightarrow (1, 0)$
$i \longrightarrow (0, 1)$.)

$\alpha \longrightarrow (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \ldots, \sigma_{r+s}(\alpha))$.

18.5. (-19)

Example. $K = \mathbb{Q}(\sqrt[3]{2})$ with $r = 1$ and $s = 1$.

$$\sigma(1) = (1, \underbrace{1, 0}_{1+0i})$$

$$\sigma(\sqrt[3]{2}) = \left(\sqrt[3]{2}, \frac{-1}{2}\cdot\sqrt[3]{2}, \frac{\sqrt{3}}{2}\cdot\sqrt[3]{2}\right)$$

$$\sigma(\sqrt[3]{4}) = \left(\sqrt[3]{4}, \frac{-1}{2}\cdot\sqrt[3]{4}, \frac{\sqrt{3}}{2}\cdot\sqrt[3]{4}\right)$$

so that $\sigma(\underbrace{\mathbb{Z}[\sqrt[3]{2}]}_{\text{This is } \mathcal{O}_K}) = \mathbb{Z}\sigma(1) + \mathbb{Z}\sigma(\sqrt[3]{2}) + \mathbb{Z}\sigma(\sqrt[3]{4})$.

Theorem. Let $\underline{a} \subseteq \mathcal{O}_K$. Then $\sigma(\underline{a})$ is a full lattice under the injection $\sigma: \mathcal{O}_K \hookrightarrow \mathbb{R}^n$, with

$$\mathrm{Vol}(\sigma(\underline{a})) = 2^{-s}\cdot \mathbb{N}(\underline{a})\cdot |\Delta_K|^{1/2}.$$

Remarks. We know that $\mathbb{N}(\underline{a})$ must appear here, because $\mathbb{N}(\underline{a}) = [\mathcal{O}_K : \underline{a}]$, which implies that if $\underline{a} = M\mathcal{O}_K$ (as real n-dim vector spaces)

then $\mathrm{Vol}(\underline{a}) = |\det(M)|\,\mathrm{Vol}(\mathcal{O}_K)$

and $\dfrac{\mathrm{Vol}(\underline{a})}{\mathrm{Vol}(\mathcal{O}_K)} = [\mathcal{O}_K : \underline{a}]$.

We are also not surprised to see $|\Delta_K|^{1/2}$.

We had $\Delta_K = \det(\sigma_K(\alpha_i))^2$ where $\{\alpha_i\}$ are an integral basis.

Indeed, if K is totally real then we are done.

18.6. (-19) If K is not totally real?

Consider the matrix

$$A = \begin{bmatrix} \sigma_1(a_1) & \cdots & \sigma_r(a_1) & \mathrm{Re}(\sigma_{r+1}(a_1)) & \mathrm{Im}(\sigma_{r+1}(a_1)) & \cdots & \mathrm{Im}(\sigma_{r+s}(a_1)) \\ \vdots & & & & & & \\ \sigma_1(a_n) & \cdots & & & & & \end{bmatrix}$$

By construction $\mathrm{Vol}(\sigma(\underline{a})) = |\det A|$.

Do some column operations: Replace

$(\mathrm{Re}(\sigma_{r+1}(a_1)), \ \mathrm{Im}(\sigma_{r+1}(a_1)))$

with $(\mathrm{Re}(\sigma_{r+1}(a_1)) + i \cdot \mathrm{Im}(\sigma_{r+1}(a_i)),$
$\mathrm{Re}(\sigma_{r+1}(a_1)) - i \cdot \mathrm{Im}(\sigma_{r+1}(a_i)))$:

Add $i \cdot (\text{Col } r+2)$ to $(\text{Col } r+1)$.
Then ~~subtract~~ replace $(\text{Col } r+2)$ with
$-2i(\text{Col } r+2)$
$+ (\text{Col } r+1)$.

This multiplies the determinant by $-2i$.
Repeating s times, get

$$B = \begin{bmatrix} \sigma_1(a_1) & \cdots & \sigma_r(a_1) & \sigma_{r+1}(a_1) & \overline{\sigma_{r+1}(a_1)} & \cdots & \sigma_{r+s}(a_1) & \overline{\sigma_{r+s}(a_1)} \\ \vdots & & & & & & & \\ \sigma_1(a_n) & \cdots & & & & & & \end{bmatrix}$$

with $\det B = (-2i)^s \det A$.

18.7. (-19) We therefore compute that

~~Vol(σ(O_K))~~

$$\mathrm{Vol}(\sigma(\underline{a})) = |\det A| = 2^{-s} \cdot |\det B|$$
$$= 2^{-s} \cdot \mathrm{Disc}(a_1, \dots, a_n)^{1/2}$$
$$= 2^{-s} \cdot \left([\mathcal{O}_K : \underline{a}]^2 \cdot |\mathrm{Disc}(\mathcal{O}_K/\mathbb{Z})| \right)^{1/2}$$
$$= 2^{-s} \cdot N(\underline{a}) \cdot |\Delta_K|^{1/2}. \quad \underline{\text{QED}}.$$

Now what? Recall, we aim to prove $\exists\, a \in \underline{a}$ s.t.

$$|N_{K/\mathbb{Q}}(a)| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s N(\underline{a})\, |\Delta_K|^{1/2}.$$

Relate the <u>norm</u> to <u>volume</u> of a b<u>a</u>ll.
or some other convex set.

Try this.
- For $\vec{x} \in \mathbb{R}^r \oplus \mathbb{C}^s$, define

$$\|\vec{x}\| = \underbrace{\sum_{i=1}^{r} |x_i|}_{\text{real abs. value}} + \underbrace{\sum_{i=r+1}^{r+s} 2|z_i|}_{\text{complex abs value}},$$

and $S(t) := \{ \vec{x} \in V : \|\vec{x}\| \leq t \}$.

Then, $S(t)$ is:
- <u>symmetric</u> (obvious)
- <u>compact</u> (because it is closed and bounded)
- <u>convex</u>, because (ex: check), for $c \in [0,1]$,

$$\|(1-c)\vec{x} + c\vec{y}\| \leq (1-c)\|\vec{x}\| + c\|\vec{y}\| \leq \max(\|\vec{x}\|, \|\vec{y}\|)$$

Also, $\mathrm{Vol}(S(t)) = t^n \cdot \mathrm{Vol}(S(1))$.

Note. If we defined $\|\vec{x}\|$ a little differently, would still get such.

20.1.

($\mathcal{O}_K$ has r real embs.
s complex)

Last time:

Embeded $\mathcal{O}_K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$ (as $\mathbb{R}$-vector spaces)

$$a \longrightarrow (\sigma_1(a), \dots, \sigma_r(a), \sigma_{r+1}(a), \dots, \sigma_{r+s}(a))$$

where we had $\mathrm{Vol}(\sigma(\underline{a})) = 2^{-s} N(\underline{a}) \, |\Delta_K|^{1/2}$.

We defined $S(t) := \{ \vec{x} \in \mathbb{R}^r \times \mathbb{C}^s : \|\vec{x}\| \le t \}$,

where $\|\vec{x}\| = \sum_{i=1}^{r} |x_i| + \sum_{i=r+1}^{r+s} 2|z_i|$

and observed that $S(t)$ is symmetric, compact, and convex.

We observed, by AM-GM, that

$$N_{K/\mathbb{Q}}(a) \le \frac{1}{n^n} \cdot \|a\|^n.$$

(This is done adequately on 18.2)

Suppose $\mathrm{Vol}(S(t)) \ge 2^n \, \mathrm{Vol}(\sigma(\underline{a}))$.

Then, by MCBT, there is $a \in \underline{a}$ with $a \ne 0$, $\|a\| \le t$.

~~This implies~~

18.8. (-19) (→ 20.2)

with $\sigma : K \hookrightarrow V = \mathbb{R}^n = \mathbb{R}^r \oplus \mathbb{C}^s$,

$$\alpha \longrightarrow (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \ldots, \sigma_{r+s}(\alpha))$$

and $N_{K/\mathbb{Q}}(\alpha) = |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)| \cdot |\sigma_{r+1}(\alpha)|^2 \cdots |\sigma_{r+s}(\alpha)|^2$.

The A.M - GM inequality says,

$$\left[|\sigma_1(\alpha)| \cdots |\sigma_{r+s}(\alpha)|^2\right]^{1/n} \le \frac{|\sigma_1(\alpha)| + \cdots + |\sigma_r(\alpha)| + 2|\sigma_{r+1}(\alpha)| + \cdots + 2|\sigma_{r+s}(\alpha)|}{n}$$

i.e., $N_{K/\mathbb{Q}}(\alpha) \le \frac{1}{n^n} \cdot \|\alpha\|^n$.

Have $\mathrm{Vol}(S(t)) = t^n \cdot \mathrm{Vol}(S_n(1))$.

Suppose we compute that. Can finish the proof! (note: inequality was proved.)

→ (20.2). ~~Then~~ If $\mathrm{Vol}(S(t)) \ge 2^n \mathrm{Vol}(\sigma(\underline{a}))$,

then there exists $\alpha \in \underline{a}$ with $\alpha \ne 0$ and $\|\alpha\| < t$.

Lemma. $\mathrm{Vol}(S(t)) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{t^n}{n!}$.

Assuming this:

If $2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{t^n}{n!} \ge 2^n \mathrm{Vol}(\sigma(\underline{a}))$, (*)

then there is $\alpha \in \underline{a}$ with $\alpha \ne 0$, for which

$$N_{K/\mathbb{Q}}(\alpha) \le \frac{1}{n^n} \cdot \|\alpha\|^n \le \frac{1}{n^n} \cdot t^n.$$

Choosing t^n with equality in (*), writing $\mathrm{Vol}(\sigma(\underline{a})) = 2^{-s} N(\underline{a}) |\Delta_K|^{1/2}$,

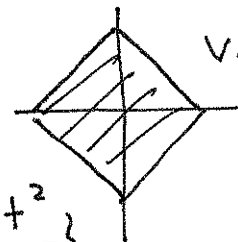
$$N_{K/\mathbb{Q}}(\alpha) \le \frac{1}{n^n} \cdot 2^n \cdot 2^{-s} N(\underline{a}) |\Delta_K|^{1/2} \cdot n! \cdot 2^{-r} \cdot \left(\frac{2}{\pi}\right)^s$$

$$= \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s N(\underline{a}) |\Delta_K|^{1/2}$$ which was enough to prove 1.6.2, and thus

18.9. 20.3 Left to show:

Proposition. $\mathrm{Vol}(S(1)) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{1}{n!}$.

Some pictures: $r=2, s=0$: $\{(x,y) \in \mathbb{R}^2 : |x| + |y| \le t\}$.



$\mathrm{Vol} = 2t^2$.

$r=0, s=1$: $\{(x,y) \in \mathbb{R}^2 : \cancel{4}x^2 + y^2 \le \frac{t^2}{4}\}$.

(i.e., $2\sqrt{x^2+y^2} \le t$). Vol. $\frac{\pi}{4} \cdot t^2$.

Finally we have to do it.

Write $V_{r,s}(1) = \mathrm{Vol}(S(1))$ in $\mathbb{R}^r \times \mathbb{C}^s$.

Prove by induction on r and then s:

$$V_{r,s}(1) = 2\int_0^1 V_{r-1,s}(1-x)\,dx$$

$$= 2\int_0^1 (1-x)^{r-1+2s}\, V_{r-1,s}(1)\,dx$$

$$= 2 \cdot V_{r-1,s}(1) \cdot \int_0^1 (1-x)^{r-1+2s}\,dx$$

$$= \frac{2 \cdot V_{r-1,s}(1)}{r+2s}$$

$$= \frac{2 \cdot \left(2^{r-1}\left(\frac{\pi}{2}\right)^s \cdot \frac{1}{(n-1)!}\right)}{n} \quad \text{(induction)}$$

$$= 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{1}{n!}.$$

18.10. (≈20:4) For s,

$$V_{0,s}(1) = \iint_{x^2+y^2 \le \frac{1}{4}} V_{0,s-1}\left(1 - 2\sqrt{x^2+y^2}\right) dx\, dy$$

$$= 2\pi \int_{r \le \frac{1}{2}} V_{0,s-1}(1-2r)\, r\, dr$$

$$= 2\pi\, V_{0,s-1}(1) \cdot \int_0^{1/2} (1-2r)^{2(s-1)}\, r\, dr$$

Let $u = 1 - 2r$

$$= \frac{\pi}{2} V_{0,s-1}(1) \int_0^1 u^{2(s-1)} (1-u)\, du$$

$$= \frac{\pi}{2} \cdot \left(\frac{\pi}{2}\right)^{s-1} \cdot \frac{1}{(2s-2)!} \cdot \frac{1}{(2s)(2s-1)}.$$

Proof follows by induction.

<u>So, we're done:</u>

1. Minkowski's convex body theorem.
   Any convex, symm body of volume $\ge 2^n \operatorname{Vol}(\Lambda)$ contains a nonzero $\lambda \in \Lambda$.

2. Ideals as lattices.
   There is a natural embedding $\mathfrak{a} \hookrightarrow \mathbb{R}^n$ with
   $$\operatorname{Vol}(\sigma(\mathfrak{a})) = 2^{-s} N(\mathfrak{a}) |\Delta_K|^{1/2}.$$

3. Comparison: $|N(\alpha)| \le \frac{1}{n^n} \cdot \|\alpha\|$ for a natural $\|\cdot\|$,
   for which
   $$S(t) = \{\vec{v} : \|\vec{v}\| \le t\}$$ has volume $2^r \left(\frac{\pi}{2}\right)^s \cdot \frac{t^n}{n!}$.

4. Shows $\mathfrak{a}$ contains α with
   $$|N(\alpha)| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \cdot N(\mathfrak{a}) |\Delta_K|^{1/2}.$$

5. Any elt. of the ideal class group is represented by an $\mathfrak{a}$ with
   $$|N(\mathfrak{a})| \le \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_K|^{1/2}.$$

6. Only finitely many $\mathfrak{a}$ with this bound $\Rightarrow$ we're done!

20.5.

Some open problems + connections with class numbers.
(Also: next time: computing class groups)

Theorem. (Dirichlet) If $D < -4$, then

$$\#Cl(\mathbb{Q}(\sqrt{-D})) = \sqrt{D} \cdot \frac{1}{\pi} \cdot \sum_{n \geq 1} \left(\frac{-D}{n} \right).$$

So, on average, $\#Cl(\mathbb{Q}(\sqrt{-D})) \approx \sqrt{D}$.

Classical conjectures. (Gauss)

If $-D < 0$, then

$$\overset{h(-D) =}{\#Cl(\mathbb{Q}(\sqrt{-D}))} = 1 \longleftrightarrow D = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Also, $\lim_{D \to \infty} h(-D) = \infty$.

Took until Baker, Heegner, Stark (~1970) to prove.

Interesting related facts:

(1) $\left(\frac{-163}{p} \right) = -1$ for $p = 2, 3, 5, \ldots, 37$.
First prime to split is 41.

(2) Let $f(n) = n^2 + n + 41$.
Represents for small n: 41, 43, 47, ~~~~53, 61, 71, 83, 97, 113, 131, 151, 173, 197, ...
For $0 \leq n \leq 39$, get primes.

(3) $e^{\pi\sqrt{163}} = 262,537,412,640,768,743.999\,999\,999\,999\,25\ldots$

Also mention: * Real quadratic fields
* Cohen-Lenstra.
* 3-ranks.

21.1. Finding class groups.

Have a complete set of representatives of the class group $\underline{a}$, with

$$N(\underline{a}) \le \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_K|^{1/2}. \quad \text{(Call RHS} = B_K.)$$

Example. Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha + 1$.

Compute $h(K)$.

Computation $\Rightarrow$ $\Delta_K = -31$. $\quad n = 3$ and $s = 1$.

$$B_K = \frac{3!}{3^3} \cdot \left(\frac{4}{\pi}\right) \cdot \sqrt{31} = 1.575\ldots$$

So K is a PID.

Ex. $K = \mathbb{Q}(\sqrt{-19})$. $\quad \Delta_K = -19$.

$$B_K = \frac{2!}{2^2} \cdot \left(\frac{4}{\pi}\right) \sqrt{19} = 2.77\ldots$$

Check all ideals of norm 2.

Is there an ideal of norm 2?

How does $2\mathcal{O}_K$ factor?

Have $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where α is a root of $x^2 - x + 5$.

$x^2 + x + 1$ is irred over $\mathbb{F}_2$. (neither 0 nor 1 a root)

So (2) is inert and $N_{K/\mathbb{Q}}((2)) = 4$.

So there is no ideal of $\mathcal{O}_K$ of norm 2; K is a PID.

Ex. $K = \mathbb{Q}(\sqrt{-5})$ $\quad \Delta_K = -20$.

$$B_K = \frac{1}{2} \cdot \left(\frac{4}{\pi}\right) \cdot \sqrt{20} = 2.84\ldots$$

Check ideals of norm 2.

What is $2\mathcal{O}_K$? It ramifies, because $2 \mid 20$.

Note $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for α a root of $x^2 + 5$. $\quad x^2 + 5 = (x+1)^2$.

So (2) is $\underline{p}^2$ with $\underline{p} = (2, 1 + \sqrt{-5})^2$.

21.2.

Is $\mathfrak{p}$ principal?

If $(2, 1+\sqrt{-5}) = (\gamma)$ then $N((\gamma)) = 2 = N(\gamma)$

i.e. if $\gamma = a + b\sqrt{-5}$, $N(\gamma) = a^2 + 5b^2 = 2$.

(not possible)

So $h(K) = 2$ and $Cl(K) \cong \mathbb{Z}/2\mathbb{Z}$.

Ex. $K = \mathbb{Q}(\sqrt{-163})$.

$$B_K = \frac{1}{2} \cdot \left(\frac{4}{\pi}\right) \cdot \sqrt{163} = 8.127\ldots$$

(think about this. HW)

Ex. $K = \mathbb{Q}(\zeta_7)$ (cyclotomic field.) $[K : \mathbb{Q}] = 6$.

$\mathcal{O}_K = \mathbb{Z}[\zeta_7]$, $\Delta_K = -16807 = -7^5$.

All the embeddings are complex. (no real 7th root of 1.)

$$B_K = \frac{6!}{6^6} \cdot \left(\frac{4}{\pi}\right)^3 \cdot \sqrt{16807} = 4.1295\ldots$$

Ideals of norm 2? Look at $x^6 + x^5 + x^4 + \cdots + 1 \mod 2$.

no solutions.

~~So it is~~ Can it have a quadratic factor?

Would be $x^2 + 1$ or $x^2 + x + 1$.

not irreducible

~~[illegible]~~ So 2 is either prime or

2 is $\mathfrak{p} \cdot \mathfrak{p}'$ with $\mathfrak{p}, \mathfrak{p}'$ of degree 3.

(in fact the former)

So no ideals of norm 2 or 4.

Look at 3: Polynomial is irreducible.

So no ideals of norm 3.

21.3. Exercise. Prove $Cl(\mathbb{Q}(\sqrt{-23})) = \mathbb{Z}/2 \times \mathbb{Z}/2$.

Theorem. (Ankeny + Chowla, 1953).

Suppose $d = 3^g - a^2$ squarefree with g even.

where $2 | x$ and $0 < a < (2 \cdot 3^{g-1})^{1/2}$.

Then $g \mid h(-d)$.

Proof. We have $3^g = a^2 + d$. x is coprime to 3, (b/c d is squarefree)

mod 3, $0 \equiv a^2 + d$.

~~But~~ $-d$ is a quadratic residue mod 3, so the polynomial $x^2 + d$ factors.

$(x^2 + d = x^2 - a^2.)$

This says $3 = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ in $\mathbb{Q}(\sqrt{d})$.

Let m be minimal s.t. $\mathfrak{p}_1^m$ is principal.

By way of contradiction show $m < g$. $\mathfrak{p}_1^m = (\alpha)$.

We have $2 | g$, $2 | a$, so $d \equiv 1 \pmod 4$.

So $\alpha = u + v\sqrt{-d}$ where $u, v \in \mathbb{Z}$.

Then, $(3^m) = \mathfrak{p}_1^m \cdot \mathfrak{p}_2^m = (u + v\sqrt{-d})(u - v\sqrt{-d}) = u^2 + v^2 d$

i.e. $3^m = u^2 + v^2 d$.

We have $d > 3^{g-1}$ by our assumed upper bound on a.

But if $m < g$, $3^{g-1} \geq u^2 + v^2 d$ and so $v = 0$.

This means $\mathfrak{p}_1^m = (u)$ and $\mathfrak{p}_2^m = (u)$

but $\mathfrak{p}_1^m = \mathfrak{p}_2^m \Rightarrow \mathfrak{p}_1 = \mathfrak{p}_2$, contradiction.

21.4. So $\mathfrak{p}_1, \cdots \mathfrak{p}_1^{g-1}$ not principal.

$$\text{But } 3^g = a^2 + d = (a + \sqrt{-d})(a - \sqrt{-d})$$
$$= \mathfrak{p}_1^g \cdot \mathfrak{p}_2^g.$$

In fact $(a + \sqrt{-d}) = \mathfrak{p}_1^g$ and
$(a - \sqrt{-d}) = \mathfrak{p}_2^g$ or vice versa.

ETS $a + \sqrt{-d}$, $a - \sqrt{-d}$ are <u>coprime</u>.

If they have a common factor $\underline{b}$
then $2a \in \underline{b}$
$3^g \in \underline{b}$ so $1 \in \underline{b}$.

So $\mathfrak{p}_1$ <u>is</u> principal. Q.E.D.

Also. <u>Lemma</u>. The number of such squarefree d is $\geq \frac{1}{25} 3^{g/2}$.

(Proof. Do a simple sieve)

<u>Cor.</u> For any g, There are infinitely many IQF with $g \mid h(-d)$.