★ **Examples**: Problem 1:

Show that $\mathbb{Z}[\sqrt{-26}]$ has non-principal ideals of norm 30.

Claim 1: $\mathcal{O}_{-26}$ has 4 ideals of norm 30. Check the decomposition:

$p=2$ $(2) = (2, \sqrt{-26})^2 = \mathfrak{p}_2^2$

$p=3$ $-26 \equiv 1 \pmod 3$ $\rightarrow \mathfrak{p}_3 = (3, 1-\sqrt{-26})$ and $\mathfrak{p}_3 \neq \tilde{\mathfrak{p}}_3$

$p=5$ $-26 \equiv 4 = 2^2 (5)$ $\rightarrow \mathfrak{p}_5 = (5, 2-\sqrt{-26})$ and $\mathfrak{p}_5 \neq \tilde{\mathfrak{p}}_5$

$N(\mathfrak{p}_p) = p$ in all these cases.

Suppose I (ideal) is of norm 30. Then $I \mid \mathfrak{p}_2^r \mathfrak{p}_3^s \tilde{\mathfrak{p}}_3^t \mathfrak{p}_5^u \tilde{\mathfrak{p}}_5^v$ for some $r,s,t,u,v \geq 0$

Take norms. $30 = N(I) = 2^r 3^{s+t} 5^{u+v}$ for some exponenents.
Compute exponents. $\Rightarrow r=1, s+t=1, u+v=1$
$\Rightarrow 1.2.2 = 4$ possibilities

Claim (ii) $\mathbb{Z}[\sqrt{-26}]$ has only two principal ideals of norm 30.
$\gamma = a+b\sqrt{-26}$, $\longrightarrow |N(\gamma)| = \cancel{N(\gamma)}\ N((\gamma)) = 30$
means $a^2+26b^2 = 30$, get 4 solutions. $a=\pm 2$, $b=\pm 1$ $\rightarrow$ only two different ideals

Conclusion: $\exists$ non-principal ones!

Lecture 11: **The Ideal Class Group**

let $K = \mathbb{Q}(\theta)$ $|K:\mathbb{Q}| = n$ $R = \mathcal{O}_\theta$ with our running assumptions
1. a maximal ideal is invertible
2. $\exists$ a norm function for ideals
3. ideals are finitely generated as abelian groups.

This means $\mathcal{J}(R)$ is an abelian group.
For principal ideals, a similar thing is true, gives rise to the subgroup $\mathcal{P}(R)$ of principal ideals.

Definition: Two ideals, I, J in $\mathcal{J}(R)$ are equivalent, denoted $I \sim J$ if $\exists \lambda \in K^\times$ so that $I = (\lambda)_R J$

This leads us to define $CL(R) = \mathcal{J}(R)/\mathcal{P}(R)$ which is called the ideal class group of R.

The elements of $Cl(R)$ are $[I]$ equivalence classes of ideals.

Lecture 12: Long-Term Goal - arithmetic of number rings R
- unique factorisation into irreducibles (no longer true) replaced by unique prime ideal decomposition.
- need a grip on the units in R.
- still to capture the "ambiguity" of factorisation into irreducibles.

For the latter, introduced the (ideal) class group for $\mathcal{O}_K$.

$Cl(K) := Cl(\mathcal{O}_K) := \mathcal{J}(\mathcal{O}_K)/\mathcal{P}(\mathcal{O}_K)$ and its order called the <u>class number</u>, of $\mathcal{O}_K$.

[[Notation: $h_K := h_{\mathcal{O}_K} = \# Cl(K)$
for quadratic fields $K = \mathbb{Q}(\sqrt{d})$; $h_{\sqrt{d}} := h_{\mathcal{O}_K}$]]

We denote ideal class of an Ideal I in $\mathcal{J}(\mathcal{O}_K)$ by $[I]$.

<u>Proposition</u>: For $I, J \in \mathcal{J}(R)$, put $e = e_{Cl(R)}$ for identity in $Cl(R)$
- i) $[I] = e \iff I$ is principal
- ii) $[I] = [J] \iff \exists\ \alpha, \beta \in R\setminus\{0\}$, st $(\alpha) I = (\beta) J$
- iii) $[I . J] = [I].[J]$
- iv) $[I]^{-1} = [I^{-1}]$
- v) $[I]^m = e \iff I^m$ is principal

In order to get an upper bound on the class number, it is helpful to find relations among ideal classes, eg. by factorising principal ideals.

$(\alpha) = \mathfrak{p}.\mathfrak{q} \Rightarrow [\mathfrak{p}] = [\mathfrak{q}]^{-1}$

<u>Proposition</u>: If $K = \mathbb{Q}(\sqrt{d})$ we have
- i) $[\tilde{I}] = [I]^{-1}$
- ii) If $I.\tilde{J}$ is principal $\iff [I] = [J]$

<u>Problem</u>: For $R = \mathcal{O}_K = \mathbb{Z}[\sqrt{-29}]$
a) Show that R contains ideals $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5$ of norm 2, 3 and 5 resp. whose classes in $Cl(\mathcal{O}_K)$ are 2, 6 and 3 respectively.
b) R has an ideal of norm 11, whose class has order 6.

Solution: Using previous theorem, find
$-29 \equiv 3\ (4)$ hence $(2)_R = \mathfrak{p}_2^2$, $\mathfrak{p}_2 = (2, \sqrt{-29})$
$-29 \equiv 1^2\ (3)$ $(3)_R = \mathfrak{p}_3\tilde{\mathfrak{p}}_3$ $\mathfrak{p}_3 = (3, 1-\sqrt{-29})$
$-29 \equiv 1^2\ (5)$ $(5)_R = \mathfrak{p}_5\tilde{\mathfrak{p}}_5$ $\mathfrak{p}_5 = (5, 1-\sqrt{-29})$

Q: Are there any principal ideals of norm 2, 3 or 5?
[[No, otherwise $a^2 + 29b^2 = 2, 3, 5$ not possible in integers]]

Precise orders: $\mathfrak{p}_2$: its square is principal, but it is not principal itself.
$[\mathfrak{p}_2]$ is of order 2 (and norm = 2)

$\mathfrak{p}_5$: Instead of multiplying $\mathfrak{p}_5$ with itself and then checking if $\mathfrak{p}_5^2$ is principal, $\mathfrak{p}_5^3$ is principal, ..., we take a shortcut.

Find $\beta = 3+2\sqrt{-29}$, of norm $125 = 5^3$

$\Rightarrow \quad e = [(\beta)] = [\mathfrak{p}_5^a \tilde{\mathfrak{p}}_5^{3-a}]$

But also, $\beta \in \mathfrak{p}_5$, $\beta = 3+2\sqrt{-29} = 5-2(1+\sqrt{-29})$

and $\beta \notin \tilde{\mathfrak{p}}_5$ [[Otherwise $\beta + \tilde{\beta} = 6 \in \mathfrak{p}_5$ hence $1 \in \mathfrak{p}_5$ #]]

So $(\beta) = \mathfrak{p}_5^3$ and $[\mathfrak{p}_5]^3 = e$

Hence, as $\mathfrak{p}_5$ is not principal, get order of $[\mathfrak{p}_5] = 3$. (as must divide 3)

$\mathfrak{p}_3$: We 'understand' the ideal classes $\mathfrak{p}_2, \mathfrak{p}_5, \tilde{\mathfrak{p}}_5$.

$\Rightarrow$ Try to concoct elements of norm $2^? 5^? 3^{>0}$

Take $\gamma = 1+\sqrt{-29}$, of norm 30

$(\gamma) = \mathfrak{p}_2 \cdot \mathfrak{p}_3^a \tilde{\mathfrak{p}}_3^{1-a} \mathfrak{p}_5^b \tilde{\mathfrak{p}}_5^{1-b}$ with $0 \leq a, b \leq 1$.

Indeed, $\gamma \in \tilde{\mathfrak{p}}_3$, $\in \tilde{\mathfrak{p}}_5$ (not in $\mathfrak{p}_3, \mathfrak{p}_5$)

$\rightarrow (\gamma) = \mathfrak{p}_2 \tilde{\mathfrak{p}}_3 \tilde{\mathfrak{p}}_5$

$\underset{\text{in cl group}}{\Rightarrow} \quad = [\mathfrak{p}_2][\tilde{\mathfrak{p}}_3][\tilde{\mathfrak{p}}_5]$

order 2 order 3

$\Rightarrow [\tilde{\mathfrak{p}}_3]$ has order $\mathrm{lcm}(2,3) = 6$.

b) Try to find an element of norm $3 \cdot 11$

$\exists$ class of order 6

Simply take $\alpha := 2+\sqrt{-29}$

$\Rightarrow e = [(\alpha)] = [\tilde{\mathfrak{p}}_3^{(\sim)} \cdot \mathfrak{p}_{11}^{(\sim)}] = [\tilde{\mathfrak{p}}_3^{(\sim)}] \cdot [\mathfrak{p}_{11}^{(\sim)}]$

order 6 also has order 6.

<u>Goal</u>: h_K is finite

<u>Idea</u>: (Minkowski), "Geometry of Numbers"

list prime ideals ordered by norm, show that primes of norm beyond a certain bound ("Minkowski bound") do not contribute anything to the relations.

ecture 13: <u>Finiteness of Class Group</u>

Will need "Minkowski Bound."

To formulate, introduce <u>discriminant</u> of a polynomial.

<u>Definition</u>: $f(x) \in \mathbb{C}[X]$, $\deg f(x) = n$ with roots $\theta_1, \dots, \theta_n$.
Then the <u>discriminant</u> $\operatorname{discr}(f(x)) := \prod_{1 \leq i \leq j \leq n} (\theta_i - \theta_j)^2$

[[$f(x)$ has multiple roots $\Leftrightarrow$ $\operatorname{discr}(f(x)) = 0$]]

<u>Definition</u>: The <u>discriminant of a number field</u> $K = \mathbb{Q}(\theta)$ such that $\mathcal{O}_K \overset{*}{=} \mathbb{Z}[\theta]$ for some $\theta \in K$ is the discriminant of $p_\theta(x)$ [minimal polynomial of θ over $\mathbb{Q}$]

<u>Caveat</u>: $*$ is not always possible! [[Ex. $K = \mathbb{Q}(\sqrt[3]{10})$ does not have this property]]

But it is OK for quadratic fields. $\Delta_{\mathbb{Q}\sqrt{d}} = \begin{cases} 4d & \text{if } d \equiv 2,3 \ (4) \\ d & \text{if } d \equiv 1 \ (4) \end{cases}$

Check: minimal polynomial of $\theta = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \ (4)$ is $\left(x - \left(\frac{1+\sqrt{d}}{2}\right)\right)\left(x - \left(\frac{1-\sqrt{d}}{2}\right)\right)$

its discriminant is $\left(\frac{1+\sqrt{d}}{2} - \frac{1-\sqrt{d}}{2}\right)^2 = d$

<u>Definition</u>: Let $K = \mathbb{Q}(\theta)$ be a number field of degree $n = |K:\mathbb{Q}| = s + 2t$
where $s = \#\{\text{real embeddings of } K \text{ into } \mathbb{C}\}$
$t = \#\{\text{pairs of complex conjugate embeddings into } \mathbb{C}\}$

Then the <u>Minkowski Bound</u> for K is $B_K := \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \cdot \sqrt{|\Delta_K|} \in \mathbb{R}$

<u>Theorem</u>: (Minkowski)
For any number field K and any integral ideal $J \subset \mathcal{O}_K$. $(J \neq (0))$
There is a non-zero $\alpha \in J$ s.t. $\frac{|N_K(\alpha)|}{N(J)} \leqslant B_K$

<u>Corollary</u>: For each ideal class c in $Cl(\mathcal{O}_K)$ we can find a representative I which is an <u>integral</u> ideal in R such that $N(I) \leqslant B_K$.

<u>Proof (Corollary)</u>: We can choose in c^{-1} an <u>integral</u> ideal J representing it (up to multiplying by a principal ideal).
By theorem above, we can choose $\alpha \in J \setminus \{0\}$ such that $|N_K(\alpha)| \leqslant B_K N(J)$
Clearly $J \mid (\alpha)$, so $(\alpha) = J \cdot I$ for some integral ideal I.

This I satisfies the requirements: i) $I \in c$ [[$[I] = [J^{-1}(\alpha)] = [J^{-1}] = [J]^{-1} = (c^{-1})^{-1} = c$

ii) $N(I) \leqslant B_K$ [[$N(I)N(J) = N((\alpha)_K) = |N_K(\alpha)| \leqslant B_K \cdot N(J)$]] $\square$

Example: The class number of $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is 1.

Minkowski bound: $n=2$, $t=1$, $|\Delta_K| = 19$

field of degree 2 has 1 pair of complex embeddings (2 real embeddings or)

$f(x) = \prod(\text{real roots}) \prod(\text{complex roots})$

$t = \frac{\# \text{ complex roots}}{2}$

$$\rightarrow B_{\mathbb{Q}(\sqrt{-19})} = \left(\frac{4}{\pi}\right)^1 \cdot \frac{2!}{2^2} \underbrace{\sqrt{19}}_{\approx 4.5} \leqslant \frac{2}{3.14} \times 4.5 < 3$$

Now check ideals of norm $=2$

decomposing (2) into prime ideals. Since $d=-19 \equiv 5\ (8)$, we know (2) is a prime ideal, of ideal norm $2^2=4$.

$\Rightarrow$ There is no ideal of norm 2 in $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$

Hence, the only generator of $Cl(\mathbb{Z}[\frac{1+\sqrt{-19}}{2}])$ is the class containing an ideal of norm 1. ie: $R (= \mathbb{Z}[\frac{1+\sqrt{-19}}{2}])$

Conclusion: Class group is trivial.

EXAM: We can even get the full structure of the class group.

Ex: $R = \mathbb{Z}[\sqrt{-14}]$ $n=2$, $t=1$, $\Delta_{Quot(R)} = -4 \cdot 14$, $K = Quot(R) = \mathbb{Q}(\sqrt{-14})$

$$\Rightarrow B_K = \frac{4}{\pi} \cdot \frac{2!}{2^2} 2\underbrace{\sqrt{14}}_{<3.73} < 5$$

This reduces the calculation to ideals of norm $\leqslant 4$.

norm $=2$ $\rightarrow (2) = \mathfrak{p}_2^2$ $\quad \mathfrak{p}_2 = (2, \sqrt{-14})$ $\quad$ norm $=2$

$=3$ $\rightarrow (3) = \mathfrak{p}_3 \tilde{\mathfrak{p}}_3$ $\quad \mathfrak{p}_3 = (3, 1-\sqrt{-14})$ $\quad$ split $\quad$ norm $=3$ [as for $\tilde{\mathfrak{p}}_3$]

$=4$ $\rightarrow$ only $\mathfrak{p}_2^2$ has norm $=4$

Hence: class group is, as a set, equal to $\{e, [\mathfrak{p}_2], [\mathfrak{p}_3], [\tilde{\mathfrak{p}}_3], [\mathfrak{p}_2^2]\}$

$[\mathfrak{p}_2^2] = [(2)] = e$ $\quad$ every principal ideal represents the trivial class

$\Rightarrow h_{\sqrt{-14}} \leqslant 4$

- Show $\mathfrak{p}_2, \mathfrak{p}_3, \tilde{\mathfrak{p}}_3$ are non-principal
- Show $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$, $(\Rightarrow h \geqslant 3)$
- Show $\mathfrak{p}_3^2$ is not principal (look at norms)

See Online

Conclusion: $h_{\sqrt{-14}} = 4$, $Cl(\mathbb{Z}[\sqrt{-14}]) \cong \mathbb{Z}/4\mathbb{Z}$ generated by $[\mathfrak{p}_3]$

not $\mathbb{Z}_2 \times \mathbb{Z}_2$

Lecture 14: Recall: Minkowski bound. K a number field with $n=[K:\mathbb{Q}]$ and s real embeddings, and t pairs of complex conjugate embeddings.
Then
$$B_K = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta_K|}$$

Ex: For $K=\mathbb{Q}(\sqrt{-29})$ we had seen
$[\mathfrak{p}_2]$ has order 2
$[\mathfrak{p}_3]$ has order 6
$[\mathfrak{p}_5]$ has order 3

Now use Minkowski: $t=1, n=2, \Delta_K = 4(-29)$

$$B_{\mathbb{Q}(\sqrt{-29})} = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2}\sqrt{4\cdot 29} = \frac{4}{\pi}\sqrt{29} < 7$$

$[\![4\times 5.4 < 7\times 3.14 \approx 21.98]\!]$

Now only need to consider ideals of norm <7

n	1	2	3	4	5	6
Ideals of norm n	R	$\mathfrak{p}_2$	$\mathfrak{p}_3$, $\tilde{\mathfrak{p}}_3$	$\mathfrak{p}_2^2$, (2)	$\mathfrak{p}_5$, $\tilde{\mathfrak{p}}_5$	$\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_2\tilde{\mathfrak{p}}_3$

$\Rightarrow h_{\sqrt{-29}} \leq 8$

We know that $6 \mid h_{\sqrt{-29}}$ (as $[\mathfrak{p}_3]$ has order 6)
$\Rightarrow h_{\sqrt{-29}} = 6 \Rightarrow Cl(\mathcal{O}_K) \cong \mathbb{Z}/6\mathbb{Z}$ (only one group of order 6)

Arithmetic of General Number Fields

General assumption: $K=\mathbb{Q}(\theta)$, $n=[K:\mathbb{Q}]$
$p_\theta(x) = x^n + p_{n-1}x^{n-1} + \dots + p_0$ the minimal polynomial of θ.

Basis of $\mathbb{Q}$-vector space K given by $\{1,\theta,\dots,\theta^{n-1}\}$

1. **Norms**: We had seen $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$, where $\alpha\in K$, $\sigma_i : K \hookrightarrow \mathbb{C}$

runs through the embeddings of K.

Another way: think of α as an endomorphism of K (multiplication by α)
$\hat{\alpha}: K \longrightarrow K$
$x \longmapsto \alpha x$

In particular, for $\alpha = \theta$ we have

$$\theta : 1 \longmapsto \theta$$
$$\theta \longmapsto \theta^2$$
$$\theta^{n-1} \longmapsto \theta^n \quad = -p_{n-1}\theta^{n-1} - \dots - p_0$$

We have an associated matrix, (using the given basis).

$$T = \begin{pmatrix} 0 & 1 & \cdots & & \\ 0 & 0 & 1 & \cdots & \\ \vdots & & & & \\ -p_0 & -p_1 & \cdots & & -p_{n-1} \end{pmatrix}$$

Take determinant $\det(T) = (-1)^n p_0$.

This agrees with previous definition of norm.

$N_K(\theta) = \prod \sigma_i(\theta)$

$\rightarrow p_\theta(x) = \prod_{i=1}^{n} (x - \sigma_i(\theta)) = x^n + \dots + \underbrace{(-1)^n \prod \sigma_i(\theta)}_{= p_0}$

<u>Define</u>: For any $\alpha \in K$, the norm is given by $\det(\hat{\alpha})$ where $\hat{\alpha}$ is the endomorphism "multiplication by α".

[[Recall that norm is multiplicative]]

<u>Proposition</u>: If $\alpha \in \mathbb{Q}$ then $N_K(\alpha - \theta) = p_\theta(\alpha)$

<u>Proof (sketch)</u> To $\widehat{\alpha - \theta}$ we get the associated matrix (wrt basis $\{1, \theta, \dots, \theta^{n-1}\}$)

$\alpha . I_n - T$ [[I_n = $n \times n$ identity matrix]]

$\rightarrow N_K(\alpha) = \det(\alpha I_n - T) =$ char. polynomial of $T|_\alpha$ $= p_\theta(\alpha)$.

Very useful:

<u>Proposition</u>: For $a, b \in \mathbb{Q}$ we can compute $N_K(a + b\theta)$

$$N_K(a + b\theta) \overset{\text{mult.}}{=} \underbrace{N_K(-b)}_{=(-b)^n} N_K\left(-\frac{a}{b} - \theta\right)$$

$$\begin{pmatrix} -b & & \\ & -b & \\ & & b \ddots \end{pmatrix}$$

$$= (-b)^n p_\theta\left(-\frac{a}{b}\right)$$

<u>Example</u>: let θ be a root of $f(x) = x^3 - 4x + 14$ [[irreducible by eisenstein]]

so $K = \mathbb{Q}(\theta)$ is of degree 3, and we find

$N_K(a + b\theta) = (-b)^3 f\left(-\frac{a}{b}\right) = a^3 - 4ab^2 - 14b^3$

Discriminants: If $K = \mathbb{Q}(\theta)$ does not always imply $\mathcal{O}_K = \mathbb{Z}[\theta]$

Possible "deviations" are controlled by discriminant.
Only primes dividing Δ_K to a square can possibly be responsible for $\mathcal{O}_K \neq \mathbb{Z}[\theta]$

The discriminant $\Delta_K(\underline{\gamma})$ of a basis $\underline{\gamma} = (\gamma_1, \dots \gamma_n) \in K$ is given by $\det Q(\underline{\gamma})$ where

$$Q(\underline{\gamma}) = (\mathrm{Tr}_K(\gamma_i \gamma_j)_{1 \le i,j \le n})$$

$$= \begin{pmatrix} \mathrm{Tr}_K(\gamma_1\gamma_1) & \dots & \mathrm{Tr}_K(\gamma_1\gamma_n) \\ \vdots & & \\ \mathrm{Tr}_K(\gamma_n\gamma_1) & \dots & \mathrm{Tr}_K(\gamma_n\gamma_n) \end{pmatrix}$$

and $\mathrm{Tr}_K(\alpha) = \mathrm{trace}(\hat{\alpha}) \leftarrow$ same linear map as before
$= \underset{\text{trace}}{\text{matrix}}(A)$ where A is matrix associated to $\hat{\alpha}$.

[[Recall that trace of an endomorphism is independent of matrix]]

Proposition: i) $\Delta_K(\underline{\gamma}) \in \mathbb{Q}$, and if all $\gamma_i \in \mathcal{O}_K$, then actually $\Delta_K(\underline{\gamma}) \in \mathbb{Z}$.
ii) If $\underline{\delta} = M\underline{\gamma}$ for some $M \in M_n(\mathbb{Q})$, then $\Delta_K(\underline{\delta}) = \det(M)^2 \Delta_K(\underline{\gamma})$

Proof of ii) Calculate $MQ(\underline{\gamma})M^t$, $M = (m_{ij})_{i,j=1,\dots,n}$
with ijth entry $\displaystyle\sum_{k=1}^{n}\sum_{l=1}^{n} m_{ik}\mathrm{Tr}_K(\gamma_k\gamma_l)m_{jl} = \mathrm{Tr}_K\left(\sum_k\sum_l m_{ik}\gamma_k\gamma_l m_{jl}\right)$

$$= \mathrm{Tr}_K\Big(\underbrace{\sum_k m_{ik}\gamma_k}_{\delta_i}\underbrace{\sum_l m_{jl}\gamma_l}_{\delta_j}\Big) = \mathrm{Tr}_K(\delta_i\delta_j)$$

Now take determinants (use multiplicativity) □

Theorem: $\Delta_K(\{1, \theta, \dots, \theta^{n-1}\})$
$= (-1)^{n(n-1)/2} N_K(p_\theta'(\theta))$

lecture 15: ~~Lecture~~ Recall/Enhance discriminant of a system $\underline{\gamma} = \{\gamma_1, \dots, \gamma_n\} \in K$ $([K:\mathbb{Q}] = n)$, not necessarily a basis is given by $\det(\mathrm{Tr}(\gamma_i\gamma_j))_{1 \le i,j \le n} \in \mathbb{Q}$.

[[Possibly zero, eg if $\underline{\gamma}$ is not a basis]]

quadratic matrix

Then, if $\underline{\delta} = M\underline{\gamma}$ for $M \in M_n(\mathbb{Q})$, then
$\Delta_K(\underline{\delta}) = \det(\mathrm{Tr}(\delta_i\delta_j)) = \det(Q(\underline{\delta}))$
$= \det(MQ(\underline{\gamma})M^T) = \det(M)^2\Delta_K(\underline{\gamma})$

<u>Theorem:</u> Let $K = \mathbb{Q}(\theta)$, conjugates of θ denoted $\theta_1, \dots, \theta_n$. Then
$$\Delta_K(\{1, \theta, \dots, \theta^{n-1}\}) = \prod_{r<s} (\theta_r - \theta_s)^2$$
$$= (-1)^{\binom{n}{2}} \prod_{r=1}^{n} p_\theta'(\theta_r) = (-1)^{\binom{n}{2}} N_K(p_\theta'(\theta))$$

<u>Proof:</u> Express $Q(\{1, \theta, \dots, \theta^{n-1}\})$ in terms of $D = (\theta_i^{\,j-1})_{1 \le i,j \le n}$
$$= \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & & & \vdots \\ \vdots & & & & \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{pmatrix}$$ a Vander Monde matrix

★ <u>Exercise:</u> Check $\det(D) = (-1)^{\binom{n}{2}} \prod_{r<s} (\theta_r - \theta_s)$

$\left[n=2 \right.$ $\quad \begin{vmatrix} 1 & \theta_1 \\ 1 & \theta_2 \end{vmatrix} = \theta_2 - \theta_1$

$n=3$ $\quad \begin{vmatrix} 1 & \theta_1 & \theta_1^2 \\ 1 & \theta_2 & \theta_2^2 \\ 1 & \theta_3 & \theta_3^2 \end{vmatrix} = \begin{vmatrix} 1 & \theta & \theta_1^2 \\ 0 & \theta_2 - \theta_1 & \theta_2^2 - \theta_1^2 \\ 0 & \theta_3 - \theta_1 & \theta_3^2 - \theta_2^2 \end{vmatrix} =$ $\qquad c_3 \mapsto c_3 - \theta_1 c_2$

Now $Tr_K(\theta^i) = \sum_{r=1}^{n} \theta_r^i \qquad 0 \le i \le n-1$

and
$$D^T D = \begin{array}{l} \\ \\ i\text{th row} \rightarrow \\ \\ \end{array} \begin{pmatrix} 1 & \cdots & 1 \\ \theta_1 & \cdots & \theta_n \\ \theta_1^{i-1} & & \\ \theta_1^{n-1} & \cdots & \theta_n^{n-1} \end{pmatrix} \begin{array}{c} \begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{j-1} & \theta_1^{n-1} \\ 1 & & & & \\ 1 & & & & \\ 1 & \theta_n & \cdots & & \theta_n^{n-1} \end{pmatrix} \\ \uparrow j\text{th col} \end{array} = \left(\sum_{r=1}^{n} \theta_r^{i-1} \theta_r^{j-1} \right)_{i,j}$$

$$= \left(Tr(\theta^{i-1} \theta^{j-1}) \right)_{i,j}$$

Taking determinants we get

$LHS = \prod_{r<s} (\theta_r - \theta_s)^2$

$= \det(D^T D) = \det(D)^2 = \det\left(Tr(\theta^{i-1} \theta^{j-1})\right)$

$= \Delta_K(\{1, \dots, \theta^{n-1}\})$

= 1st equality

<u>Connection to $p_\theta'(x)$:</u>

Write $p_\theta(x) = \prod_{r=1}^{n} (x - \theta_r)$

Then $p_\theta'(x) = \sum_{r=1}^{n} \prod_{\substack{s=1 \\ s \ne r}}^{n} (x - \theta_s)$

So $p_\theta'(\theta_r) = \prod_{\substack{s=1 \\ s \ne r}}^{n} (\theta_r - \theta_s)$ ⟦All other summands have factors $(\theta_r - \theta_r)$, hence vanish⟧

$$\prod_{r=1}^{n} p_\theta'(\theta_r) = \prod_{r=1}^{n}\prod_{\substack{s=1\\ s\neq r}}^{n}(\theta_r-\theta_s) = \prod_{r<s}(\theta_r-\theta_s)\underbrace{\prod_{r>s}(\theta_r-\theta_s)}_{(-1)^{\binom{n}{2}}\prod_{r<s}(\theta_r-\theta_s)}$$

$$= (-1)^{\binom{n}{2}}\prod_{r<s}(\theta_r-\theta_s)^2$$

$\Rightarrow$ 2nd equality. $\square$

<u>Corollary:</u> $\Delta_K(\gamma)\neq 0 \iff \gamma$ is a basis of K.

<u>Proof:</u> Compare with basis $\underline{\theta}=\{1,\theta,\dots,\theta^{n-1}\}$ of $K=\mathbb{Q}(\theta)$. Write $\gamma = M\underline{\theta}$, some $M\in M_n(\mathbb{Q})$

Then $\Delta_K(\gamma) = \det(M)^2\Delta_K(\underline{\theta})$

each $\theta_r-\theta_s$ non zero

So $\Delta_K(\gamma)\neq 0 \iff \det(M)\neq 0$

$\iff \gamma$ is a basis of K.

<u>Calculating Discriminants</u>

i) Quadratic fields $K=\mathbb{Q}(\theta)$, $\theta=\sqrt{d}$, $p_\theta(x)=x^2-d$

$\rightsquigarrow p_\theta'(x)=2x$

$$\Delta_K(\{1,\theta\}) = (-1)^{\binom{2}{2}}(2\sqrt{d})(-2\sqrt{d}) = 4d$$

ii) Cubic fields $K=\mathbb{Q}(\theta)$, $\theta=\sqrt[3]{5}$, $p_\theta(x)=x^3-5$, $p_\theta'(x)=3x^2$

Then $\Delta_K(\{1,\theta,\theta^2\}) = (-1)^{\binom{3}{2}}N_K(3\theta^2)$

$$= -\underbrace{N_K(3)}_{3^{[K:\mathbb{Q}]}}\underbrace{N_K(-\theta)^2}_{=p_\theta(0)=-5} = -3^3(-5)^2 = -3^3\cdot 5^2$$

iii) $K=\mathbb{Q}(\theta)$, θ root of $f(x)=x^3-x+2$ [[irreducible]]

Hence $[K:\mathbb{Q}]=3$ and $p_\theta(x)=f(x)$

Moreover $f'(\theta)=3\theta^2-1$ [[Cannot decompose into linear factors]]

$$= \frac{3\theta^3-\theta}{\theta} = \frac{3(\theta-2)-\theta}{\theta} = \frac{2\theta-6}{\theta}$$

$$\Rightarrow \Delta_K(\{1,\theta,\theta^2\}) = -N_K\left(\frac{2\theta-6}{\theta}\right) = -\frac{N_K(-2)}{\underbrace{N_K(-\theta)}_{p_\theta(0)}}\underbrace{N_K(3-\theta)}_{p_\theta(3)}$$

$$= \frac{-2^3}{2}\cdot 26 = -2^3\cdot 13$$

Getting rid of our running assumptions.

(θ each ideal in $\mathcal{O}_K$ is finitely generated)

<u>Definition:</u> Let A be a subgroup of a $\mathbb{Q}$-vector space V, generated by a set B, which is a $\mathbb{Q}$-basis for V.

Then A is called a <u>full lattice</u> in V and B is a <u>generating set</u> for A.

<u>Ex:</u> $K=\mathbb{Q}(\theta)$ with $\theta\in\mathcal{O}_K$ [[can assume]] Then $\mathbb{Z}[\theta]$ has a <u>generating basis</u> $\{1,\dots,\theta^{n-1}\}$ and is a full lattice in $K=\mathbb{Q}+\mathbb{Q}\theta+\dots+\mathbb{Q}\theta^{n-1}$

Lecture 16: Recall: Minkowski bound for class # computations needs Δ_K. General # fields.

Ex: $K = \mathbb{Q}(\theta)$, with $\theta \in \mathcal{O}_K$. Then $\mathbb{Z}[\theta]$ has a generating basis, $\{1, \theta, \ldots, \theta^{n-1}\}$ and is a full lattice in $K (= \mathbb{Q}.1 + \mathbb{Q}.\theta + \cdots + \mathbb{Q}\theta^{n-1})$

Proposition: Every non-zero ideal $I \subset \mathcal{O}_K$ is generated by a basis of $K/\mathbb{Q}$.

Proof: ① I contains a $\mathbb{Q}$ basis of K.
[[take any $\mathbb{Q}$-basis $\{\partial_1, \ldots, \partial_n\}$ of K, can assume $\partial_i \in \mathcal{O}_K$, then multiply by $\beta \in I \setminus \{0\}$ so that $\{\beta\partial_1, \ldots, \beta\partial_n\}$ $(\subset I)$ is still a basis of K]]

② Any such $\mathbb{Q}$-basis B of K with $B \subset I$ has discriminant $\Delta_K(B) \in \mathbb{Z} \setminus \{0\}$
[[Since $B \subset \mathcal{O}_K$, get $\Delta_K(B) \in \mathbb{Z}$ (all entries in $Q(B)$ are traces)
as B is a basis, get $\neq 0$]]

③ Choose a basis $\{\gamma_1, \ldots, \gamma_n\} \subset I$ with minimal discriminant.
Then $I = \langle \gamma_1, \ldots, \gamma_n \rangle_{gp}$
[[Suppose not, then $\exists \alpha \in I \setminus \langle \gamma_1, \ldots, \gamma_n \rangle_{gp}$ and $\alpha = \sum_{j=1}^{n} q_j \gamma_j$, $q_j \in \mathbb{Q}$, not all $q_i \in \mathbb{Z}$.
say $q_1 \notin \mathbb{Z}$.
Then $\{\alpha - \lfloor q_n \rfloor \gamma_1, \gamma_2, \ldots, \gamma_n\}$ is also a basis for K, but has smaller absolute value for discriminant, # to minimality]]

Definition: A generating basis for $\mathcal{O}_K$ is called an integral basis for ~~$\mathcal{O}_K$~~ K.

Proposition: Suppose A, B are full lattices in an n-dimensional $\mathbb{Q}$-vectorspace V, with generating bases $\{\alpha_j\}_{1 \leq j \leq n}$, $\{\beta\}_{1 \leq j \leq n}$ (respectively), and $A \supset B$.

Express $\beta_j = \sum_{i=1}^{n} m_{ji} \alpha_i \quad (1 \leq j \leq n)$ with $m_{ji} \in \mathbb{Z}$, ie. $\underline{\beta} = M \underline{\alpha}$

$M \in GL_n(\mathbb{Z})$.
Then, i) $\#(A/B) = |\det M|$
ii) $A = B \Leftrightarrow |\det M| = 1$

Idea of proof: Think 'fundamental theorem of f.g. abelian groups'
The group A/B has a set of generators $\{\alpha_i\}_i$ and a set of relations given by $\{\sum_{i=1}^{n} m_{ji} \alpha_i\}_j$. By applying suitable row and column operations we can bring M into diagonal form D, preserving the determinant (at least up to sign), can read off the size of A/B by taking $|\det(D)| = |\det(M)|$
$=$ product of diagonal terms of D $=$ product of torsion coefficients □

Corollary: For K (of degree $n/\mathbb{Q}$) and $\{\alpha_i\}_i$, $\{\beta_j\}_j$ of K
i) $\Delta_K(\{\beta_j\}_{j=1}^{k}) = \det(M)^2 \Delta_K(\{\alpha_i\}_{i=1}^{n})$
ii) In particular, Δ depends only on the group generated by some basis.

ie. We can write $\underset{\substack{\uparrow\\ \text{group}}}{\Delta_K(B)} = \Delta_K(\{\beta_1, \dots, \beta_n\})$ for $B = \langle \beta_1, \dots, \beta_n \rangle_{gp}$

<u>Note</u>: If $A \supset B$, as in proposition, we get $\Delta_K(B) = \#(A/B)^2 \Delta_K(A)$.
(discriminant of <u>smaller</u> lattice (here B) is <u>larger</u>)

<u>Definition</u>: The discriminant $\Delta_K := \Delta_K(\mathcal{O}_K)$ is defined as the discriminant of any integral basis for K.
[ie. any generating basis for $\mathcal{O}_K$]

<u>Corollary</u>: $\#(\mathcal{O}_K/I)$ is finite for any non-zero ideal $I \subset \mathcal{O}_K$.

<u>Definition</u>: The <u>ideal norm</u> of $I \subset \mathcal{O}_K$ is given by $N(I) = \#(\mathcal{O}_K/I)$

<u>Lemma</u>: The ideal norm is strictly multiplicative.
[mult. use chinese remainder theorem. $R/IJ \simeq R/I \times R/J$ for I, J coprime.
Strict multiplication: one shows $\mathcal{O}_K/\mathfrak{p} \simeq \mathfrak{p}/\mathfrak{p}^2$ for $\mathfrak{p}$ prime]

Consistency check with previous definition:
eg. $d = 2, 3$; $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.
Any ideal I can be written $I = \langle \alpha, \beta \rangle_{gp}$ $\alpha = a + b\sqrt{d}$ $\beta = e + f\sqrt{d}$

$$\Rightarrow \begin{pmatrix} \alpha & \beta \\ \tilde{\alpha} & \tilde{\beta} \end{pmatrix} = \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} \begin{pmatrix} a & e \\ b & f \end{pmatrix}$$

$$\text{Hence, } \#(\mathcal{O}_K/I) = \left|\det \begin{pmatrix} a & e \\ b & f \end{pmatrix}\right| = \frac{\left|\det \begin{pmatrix} \alpha & \beta \\ \tilde{\alpha} & \tilde{\beta} \end{pmatrix}\right|}{\left|\det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}\right|} = \frac{|\alpha\tilde{\beta} - \tilde{\alpha}\beta|}{|2\sqrt{d}|}$$

OTOH: $m = \gcd(\alpha\tilde{\alpha}, \beta\tilde{\beta}, \alpha\tilde{\beta} + \beta\tilde{\alpha})$, then we get

$$m^2 = \#(\mathcal{O}_K/m\mathcal{O}_K) = \#\left(\mathcal{O}_K/\langle m, \tilde{\alpha}\beta \rangle_{gp}\right) = \frac{\left|\det \begin{pmatrix} m & \tilde{\alpha}\beta \\ m & \alpha\tilde{\beta} \end{pmatrix}\right|}{2\sqrt{d}}$$
$$= m\,\#(\mathcal{O}_K/I) \quad \square$$

→ How to check whether, given $\theta \in \mathcal{O}_K$, one has $\mathbb{Z}[\theta] = \mathcal{O}_K$ or not?

<u>Theorem</u>: Suppose $S = \langle \gamma_1, \dots, \gamma_n \rangle \subset \mathcal{O}_K$ is a basis of K.
Then for each prime $p \mid \#(\mathcal{O}_K/S)$ one has:
i) $p^2 \mid \Delta_K(S)$
ii) there is an element $\alpha \in S$, ie. $\alpha = \sum m_i \gamma_i$, $(m_i \in \mathbb{Z})$
such that
- $\frac{\alpha}{p} \in \mathcal{O}_K \setminus S$
- $\begin{cases} 0 \leq |m_i| < p/2 & \text{if } p \text{ odd} \\ 0 \leq m_i \leq 1 & \text{if } p = 2 \end{cases}$

[Note: first bullet point excludes $\alpha = 0$]

Proof (i) Since $p^2 | \#(\mathcal{O}_K/S)^2$, we also have $p^2 | \#(\mathcal{O}_K/S)^2 \Delta_K(\mathcal{O}_K) = \Delta_K(S)$

ii) Use Cauchy's theorem for finite group: if p prime divides $\#G$ for a finite group G, then $\exists$ element $g \in G$ of order p.
Here $\exists$ element β of order p in $\mathcal{O}_K/S$. We can modify $\beta = \sum r_i \gamma_i$, $r_i \in \mathbb{Q}$ subtracting multiples of $p \rightarrow$ coefficients in $(-p/2, p/2)$

Lecture 17: How to decide, for $\theta \in K$, whether $\mathbb{Z}[\theta] = \mathcal{O}_K$?

Theorem: Suppose $\mathcal{O}_K \supsetneq S = \langle \gamma_1, \dots, \gamma_n \rangle$ full lattice.
Then $p | \#(\mathcal{O}_K/S) \Rightarrow p^2 | \Delta_K(S)$

ii) $\exists \alpha \in S$, $\alpha = \sum_{i=1}^n m_i \gamma_i$ $(m_i \in \mathbb{Z})$ st
- $\frac{\alpha}{p} \in \mathcal{O}_K \setminus S$
- $\begin{cases} 0 \leq m_i < p/2 & , p \text{ odd} \\ 0 \leq m_i \leq 1 & , p = 2 \end{cases}$

Ex: $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{5}$
Show: $\mathbb{Z}[\theta] = \mathcal{O}_K$

Proof: Minimal polynomial of θ: $p_\theta(x) = x^3 - 5 \Rightarrow [K:\mathbb{Q}] = 3$ as $p_\theta(x)$ irreducible.
and $\{1, \theta, \theta^2\}$ is a basis of $K/\mathbb{Q}$.
For $\alpha = a + b\theta + c\theta^2$ get
$Tr_K(\alpha) = 3a$, $N_K(\alpha) = a^3 + 5b^3 + 25c^3 - 15abc$

Already seen: $\Delta_K(\{1, \theta, \theta^2\}) = -5^2 \cdot 3^3$

Now suppose $\mathbb{Z}[\theta] \subsetneq \mathcal{O}_K$, then p (as in theorem) $\in \{3, 5\}$, and
$\alpha = a + b\theta + c\theta^2$ such that $\frac{\alpha}{p} \notin S = \langle 1, \theta, \theta^2 \rangle$, but $\frac{\alpha}{p} \in \mathcal{O}_K$.

and $0 \leq |a|, |b|, |c| \leq p/2$

Case $p = 5$: Suppose $\frac{\alpha}{5} \in \mathcal{O}_K$, $|a|, |b|, |c| \in \{0, 1, 2\}$

Now we can use combination of properties of N_K and Tr_K, of $\alpha/5$ and related numbers to get $\alpha = 0$, contradicting $\frac{\alpha}{5} \in \mathcal{O}_K \setminus S$

Trace: $Tr(\alpha/5) \underset{\substack{\uparrow \\ \text{trace is} \\ \text{linear}}}{=} \frac{1}{5} Tr(\alpha) = \frac{3a}{5} \in \mathbb{Z}$ $\Rightarrow 5 | a \Rightarrow a = 0$

know it must be

So $\alpha = b\theta + c\theta^2 = \theta(b + c\theta)$

From $\frac{\alpha}{5} \in \mathcal{O}_K$, $\theta \in \mathcal{O}_K$ get $\frac{\alpha}{5}\theta \in \mathcal{O}_K$

and $\frac{b\theta^2}{5} = \underbrace{\frac{\alpha\theta}{5}}_{\in \mathcal{O}_K} - \underbrace{\frac{c\theta^3}{5}}_{\in \mathcal{O}_K} \in \mathcal{O}_K$

$\theta^3 = 5$

So $N_K\left(\frac{b\theta^2}{5}\right) \in \mathbb{Z}$

$$= \frac{N_K(b)N(-\theta)^2}{N_K(5)} = \frac{b^3}{5^3}\underbrace{p_\theta(0)^2}_{-5} \Rightarrow \frac{b^3}{5} \in \mathbb{Z} \Rightarrow 5 \mid b$$

$\Rightarrow \quad \alpha = c\theta^2$

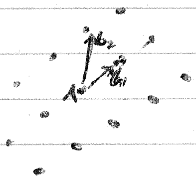
$N_K(\alpha/5) \in \mathbb{Z} \qquad = \frac{N_K(c\theta^2)}{5^3} = \frac{c^3 p_\theta(0)^2}{5^3} = \frac{c^3}{5} \Rightarrow c = 0$

So $\alpha = 0$ $\square$

Case $p=3$ is similar.

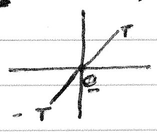
<u>Minkowski's Theorem</u>

<u>Def:</u> Let $\Lambda \subset \mathbb{R}^n$ be a full lattice with basis $\{b_1, \dots, b_n\}$. Then the fundamental domain for $\lambda \in \Lambda$ (and $\{b_i\}_i$) is
$D_\lambda := \{\lambda + \sum_{i=1}^n a_i b_i \mid 0 \leq a_i < 1\}$ in $\mathbb{R}^2$



<u>Note:</u> All lattice translates D_λ, $\lambda \in \Lambda$ cover $\mathbb{R}^n$ precisely.

<u>Theorem (Minkowski)</u> $\Lambda \subset \mathbb{R}^n$ full lattice with fundamental domain $D (= D_\lambda, \lambda \in N)$
Furthermore, let T be <u>convex</u> and a centrally symmetric subset $\subset \mathbb{R}^n$.



[centrally symmetric: $t \in T \Rightarrow -t \in T$
convex: $a, b \in T \Rightarrow \mu a + (1-\mu)b \in T$ for $0 \leq \mu \leq 1$]

In particular, $0 \in T$. If $\mathrm{vol}(T) > 2^n \mathrm{vol}\, D$, then there exists a $\lambda \in \Lambda \cap T$ different from 0.

<u>Proof (Idea)</u> "intuitively clear". There are overlaps among the lattice translates of any $S \subset \mathbb{R}^n$ with $\mathrm{vol}(S) > \mathrm{vol}(D)$. ie: $\exists \underbrace{s_1 \neq s_2}_{\in S}, \underbrace{\lambda_1 \neq \lambda_2}_{\in \Lambda}$ st $s_1 + \lambda_1 = s_2 + \lambda_2$

Use as follows:
- $\alpha \in T \Rightarrow -\alpha \in T$
- $\alpha, \beta \in T \Rightarrow \frac{1}{2}(\alpha - \beta) \in T$
- Take $S = \frac{1}{2}T = \{t/2 \mid t \in T\}$, by assumption we get $\mathrm{vol}(S) = \frac{1}{2^n}\mathrm{vol}(T) > \mathrm{vol}(D)$.

$\xRightarrow{\text{above}} \exists s_1, s_2 \in S, \ s_1 - s_2 \in \Lambda \setminus \{0\}$ $\square$

Apply this to #fd K, $[K:\mathbb{Q}]=n=s+2t$, $s=\#\{\text{real embs}\}$
$t=\#\{\text{pairs of complex embeddings}\}$

$\sigma: K \to \mathbb{R}^s \times \mathbb{C}^t$
$\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \dots, \sigma_{s+t}(\alpha))$ $\mathbb{R}^2$ - a real vector space.

Map further to

$\alpha \mapsto (\sigma_1(\alpha), \dots, Re(\sigma_{s+1}(\alpha)), Im(\sigma_{s+1}(\alpha)), \dots)$
$K \mapsto \mathbb{R}^{s+2t}$

<u>Prop</u>: $I < \mathcal{O}_K$ ideal $\Rightarrow$ $\sigma(I)$ is a full lattice in $\mathbb{R}^n$; and
$vol(D_I) = 2^{-t} N(I) \sqrt{\Delta_K}$

Idea: Pass to $(\sigma_1(\alpha), \dots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \dots)$
$\rightsquigarrow$ gives $(-2i)^t$ as "difference factor."

The new presentation then gives $det = ((\sigma(\alpha_j)) = \dots = \Delta_K())$.

Minkowski bound now from comparing "balls" (wrt a certain norm) in $\mathbb{R}^s \times \mathbb{C}^t$
$\mathbb{R}^s \times \mathbb{C}^t \longrightarrow 2^s \left(\frac{\pi}{2}\right)^t \frac{\rho^n}{n!}$ (ρ = 'radius for balls')

Important Material not covered

<u>Dirichlet Unit Theorem</u>

$$\mathcal{O}_K^* = \underbrace{\mathbb{Z}/n\mathbb{Z}}_{\substack{\text{roots of } 1 \\ \text{inside } K}} \times \mathbb{Z}^{s+t-1}$$

Ex: $\mathbb{Q}(\sqrt{d})$, $d>1$ $\Rightarrow s=2$, $t=0$
$\Rightarrow$ get $\underset{\pm 1}{\mathbb{Z}/2\mathbb{Z}} \times \mathbb{Z}$ generated by fundamental unit.

<u>Class number formula</u>

for $\mathbb{Q}(\sqrt{\Delta})$ Δ discriminant

$$h_\Delta = -\frac{1}{\log u} \sum_{r=1}^{\Delta/2} \left(\frac{\Delta}{r}\right) \log\left(\sin \frac{\pi r}{\Delta}\right)$$

Ex: $d=5$

$\left(\frac{\Delta}{r}\right)=1$ $r=1$ $\rightsquigarrow \log(\sin(\frac{\pi}{5})) \approx -0.53\dots$

$\left(\frac{\Delta}{r}\right)=-1$ $r=2$ $\rightsquigarrow \log(\sin(\frac{2\pi}{5})) \approx -0.05$

$\log\left(\frac{1+\sqrt{5}}{2}\right) \approx 0.46\dots$

PC

Prime Decomposition in General # Fields

Useful for computing class #

Dedekind's Theorem: Suppose $\mathcal{O}_K = \mathbb{Z}[\theta]$ and $f_\theta(x)$ the minimal polynomial of θ. For any prime p, one has, after reducing mod p, the factorisation $\overline{f_\theta}(x) = \overline{g_1}(x) \dots \overline{g_r}(x)$

$g_i(x) \in \mathbb{Z}[x]$ irreducible and monic.

Then we have the prime decomposition $(p) = (p, g_1(\theta)) \dots (p, g_r(\theta))$ of respective norms $p^{\deg(g_j(x))}$

$\quad\quad\quad /\!/ f(x)$

<u>Sheet 10 q 8</u>: Take θ, a root of x^3+3x-1. Factorise $(2\theta-3)$, $(\theta-7)$, $(3\theta^2+2)$ and $3(\theta-7, \theta^2-\theta-9)$

$K = \mathbb{Q}(\theta)$, we are given $\mathcal{O}_K = \mathbb{Z}[\theta]$.

$$N_K = (2\theta-3) = N_K(-2)\, N_K(3/2-\theta) = (-2)^3 \cdot \left((3/2)^3 + 3/2 \cdot 3 - 1\right) = -55$$

$$N_K(\theta-7) = -f(-7) = -3 \cdot 11^2$$

$$N_K(3\theta^2+2) = \frac{N_K(\theta(3\theta^2+2))}{N_K(\theta)} = \frac{N_K(\overbrace{3(1-3\theta)+2\theta}^{=3-7\theta})}{N_K(\theta)}$$

$$= \frac{N_K(7)\, N_K(3/7-\theta)}{N_K(\theta)} = \dots = 125 = 5^3$$

Primes to check: 3, 5, 11

mod 3: $\overline{f}(x) = X^3 - \overline{1} = (X-\overline{1})^3$
$\Rightarrow (3) = \underbrace{(3, \theta-1)}_{=\mathfrak{p}_3}{}^3$, $\mathfrak{p}_3$ of norm 3

mod 5: $\overline{f}(x) = (x+\overline{1})(x-\overline{3})^2$
$\Rightarrow (5) = \underset{\text{norm} = 5^1}{(5, \theta-1)} \cdot \underset{\text{norm} = 5^1}{(5, \theta-3)}^2 \leftarrow \mathfrak{p}_5'$ $\quad \mathfrak{p}_5$

mod 11: $\overline{f}(x) = (x-\overline{7})(x^2 - \overline{7}x + \overline{8})$
$(11) = \underset{\mathfrak{p}_{11} \text{ of norm } 11}{(11, \theta-7)}(11, \theta^2-7\theta+8)$ $\quad \mathfrak{p}_{11}'$ of norm 11^2

So $(2\theta-3) \overset{?}{\in} \mathfrak{p}_5$: $(2(\theta+1)-5) \Rightarrow \mathfrak{p}_5 \mid (2\theta-3)$ $\leftarrow$ norm $= -5 \cdot 11$

$\Rightarrow (2\theta-3) = \mathfrak{p}_5 \mathfrak{p}_{11}$

Inverse: $((2\theta-3)^{-1}) = \mathfrak{p}_5^{-1}\mathfrak{p}_{11}^{-1} = \dfrac{(\mathfrak{p}_5')^2}{(5)} \cdot \dfrac{(\mathfrak{p}_{11}')}{(11)} = \dfrac{1}{(55)}(\mathfrak{p}_5')^2 \mathfrak{p}_{11}'$

w = up there 5

Now $3(\theta-7, \theta^2-\theta-9)$

$= 3(\theta-7, \theta^2-\theta-9-(\theta-7)(\theta+6))$

$= 3(\theta-7, 33)$

$[N(\theta-7) = -3 \cdot 11^2]$

$\xRightarrow{\text{short calculation}} (\theta-7)$ has factors $\mathfrak{p}_3 \cdot \mathfrak{p}_{11}^2$

Also $(33) = \mathfrak{p}_3^3 \cdot \mathfrak{p}_{11} \cdot \mathfrak{p}_{11}'$

$= 3(\gcd(\mathfrak{p}_3\mathfrak{p}_{11}^2, \mathfrak{p}_3^3 \cdot \mathfrak{p}_{11}\mathfrak{p}_{11}') = 3\mathfrak{p}_3\mathfrak{p}_{11} = \mathfrak{p}_3^4\mathfrak{p}_{11}$

with inverse $\frac{\mathfrak{p}_3^2}{(3^2)} \frac{\mathfrak{p}_{11}'}{(11)}$