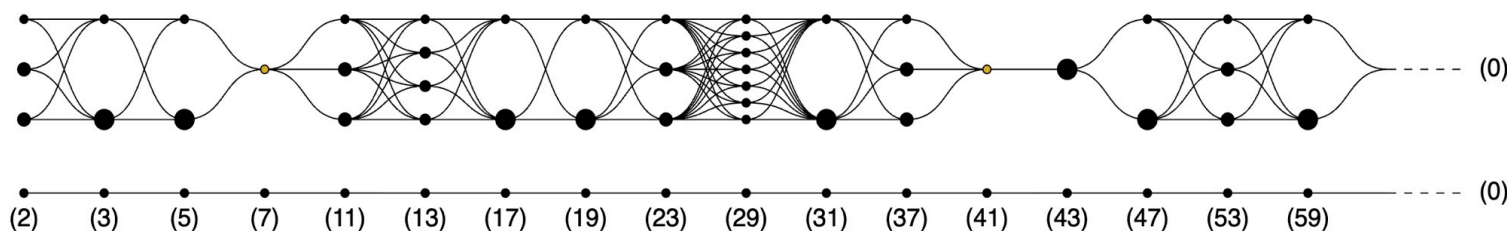


Algebraic Number Theory

University of Bonn
Summer 2026

Aleksander Horawa



LECTURE 1.

13/4

eCampus: V3A4/F4A1-4 - Algebraic Number Theory, password: Kummer

Tutorials: Mon 8-10, Wed 12-14 in 0.011

Sign up opens on eCampus: Tue, 8am

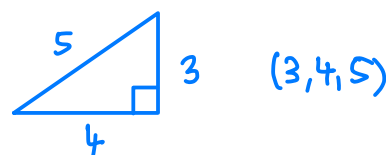
HWs: posted on Weds, due on Wed

HWO: posted this Wed, not submitted

Motivation of algebraic number theory: solve rational polynomial equations.

Example 1. Find all Pythagorean triples:

$$(x, y, z) \text{ coprime s.t. } \underbrace{x^2 + y^2}_{\text{mixes + and}} = z^2$$



Look at: $\underbrace{(x+iy)(x-iy)}_{\text{purely}} = z^2$ inside $\mathbb{Z}[i] \subseteq \mathbb{Q}(i)$.

Exercise: $\mathbb{Z}[i]$ is a UFD.

Exercise: $\mathbb{Z}[i]^{\times} = \{\pm 1, \pm i\}$.

$$\pi | z, \pi \in \mathbb{Z}[i] \text{ irreducible} \Rightarrow \pi^2 | z^2 \Rightarrow \pi^2 | (x+iy)(x-iy)$$

(If $\pi | x+iy, x-iy$, then $\pi | 2x, 2y$, so:

either $\pi | 2$, so $2 | z$ but then $x^2 + y^2 \equiv 0 \pmod{4} \Rightarrow 2 | x, y$ ↯
or $\pi | x, y$ ↯.)

$$\Rightarrow \pi^2 | x+iy \text{ or } \pi^2 | x-iy.$$

Thus, $x+iy = u \cdot \alpha^2$, $u \in \mathbb{Z}[i]^{\times} = \{\pm 1, \pm i\}$, $\alpha = m+in$, $m, n \in \mathbb{Z}$

$$\Rightarrow (x, y, z) = (\pm(m^2 - n^2), \pm 2mn, \pm(m^2 + n^2))$$

$$(3, 4, 5) = (+ (2^2 - 1), + 2 \cdot 2 \cdot 1, + (2^2 + 1^2))$$

21.
/ 1.

Example 2. Fermat's Last Theorem.

$\nexists (x, y, z)$ non-zero s.t. $\underbrace{x^n + y^n}_{\text{mixes + \&}} = z^n, n > 2.$

Suppose $p \geq 5$ prime ($n = 3, 4$ elementary).

Kummer's attempt to prove FLT (1847):

(*) $\underbrace{(x+y)(x+\omega_p y)(x+\omega_p^2 y) \dots (x+\omega_p^{p-1} y)}_{\text{purely } \cdot \nabla!} = z^p, \omega_p = e^{2\pi i/p}.$

As above, $x + \omega_p y = u \cdot \alpha^p$
 $u \in \mathbb{Z}[\omega_p]^\times,$
 $\alpha \in \mathbb{Z}[\omega_p].$

Exercise. $\mathbb{Z}[\omega_p]$ UFD $\Rightarrow$ no solutions.

(See HW 0.)

But ... $\mathbb{Z}[\omega_{23}]$ not a UFD. (Conjecturally, $\mathbb{Z}[\omega_p]$ only UFD for fin. many p .)

Exercise. $\omega := \omega_{23} \Rightarrow 2 \mid x \cdot y$ but $2 \nmid x, y$ for:

$$x := 1 + \omega^2 + \omega^4 + \omega^5 + \omega^6 + \omega^{10} + \omega^{11},$$

$$y := 1 + \omega + \omega^5 + \omega^6 + \omega^7 + \omega^9 + \omega^{11}.$$

(See HW 1.)

Using that 2 = irreducible, deduce $\mathbb{Z}[\omega_{23}] \neq$ UFD.

Kummer's idea: unique factorization holds for ideals of $\mathbb{Z}[\omega_p]$...

Ideal version of (*):

$$(x+y)(x+\omega_p y)(x+\omega_p^2 y) \dots (x+\omega_p^{p-1} y) = (z)^p$$

$$\Rightarrow (x+\omega_p y) = I^p, I = \text{ideal}.$$

If I was principal, $I = (\alpha)$, then $x + \omega_p y = u \cdot \alpha^p$

& can use similar argument to the UFD case.

In general: $K/\mathbb{Q}$ finite extension (number field), $K = \mathbb{Q}(\omega_p)$

$\mathcal{O}_K$ integral elements (ring of integers) $\mathcal{O}_K = \mathbb{Z}[\omega_p]$

The class group measures how far ideals of $\mathcal{O}_K$ are from being principal:

Def. Class group: $Cl(K) := \{\text{ideals of } \mathcal{O}_K\} / \{\text{principal ideals of } \mathcal{O}_K\}.$

Note: I principal $\Leftrightarrow [I] = 1 \in Cl(K)$;
 $Cl(K) = \{1\} \Leftrightarrow \mathcal{O}_K = PID \Rightarrow \mathcal{O}_K = UFD$.
 Note: $Cl(K)$ is an abelian gp. (HW1)

Thm. $h(K) := \#Cl(K) < \infty$ "class number".

* Understanding $Cl(K)$ & $h(K)$ is hard. *

Def. p regular if $p \nmid h(\mathbb{Q}(\omega_p))$.

$$(x + \omega_p y) = I^p \Rightarrow 1 = [(x + \omega_p y)] = [I^p] = [I]^p \quad (\text{in } Cl(K))$$

$$\Rightarrow [I] = 1 \quad (\text{in } Cl(K))$$

$\Rightarrow p$ regular

$$\Rightarrow I = (\alpha)$$

Overall, can deduce...

Thm (Kummer). $p \geq 5$ prime $\Rightarrow$ no non-zero solutions to $x^p + y^p = z^p$.

- Issue:
- $\exists \infty$ many irregular primes (37, 59, 67, ...),
 - not known if $\exists \infty$ many regular primes.

What is this course about?

K = finite extension of $\mathbb{Q}$ (number field)

e.g. $K = \mathbb{Q}(\omega_p)$

1. Ring of integers: $\mathcal{O}_K$.

Thm. $\mathcal{O}_{\mathbb{Q}(\omega_p)} = \mathbb{Z}[\omega_p]$.

2. Ideals & prime decomposition.

3. Splitting of primes in extensions L/K .

4. Class groups & finiteness of class group.

5. Unit group, $\mathcal{O}_K^\times$, is finitely generated.

6. Dedekind ζ -function, ζ_K , & class number formula:

- analytic formulas for elements in $\mathcal{O}_K^\times$?
- analytic formula for h_K ✓

7. L -functions? Local fields? Class field theory?

Prerequisites:

- Commutative algebra (rings, ideals, UFDs, PIDs, ...)
 - Galois theory
- Read appendices of Marcus, if needed!

Def. 1. A number field K is a finite field extension of $\mathbb{Q}$

Examples. $K = \mathbb{Q}(\sqrt[n]{m})$, $\mathbb{Q}(\omega_n)$, ... Note: $\mathbb{Q}(\sqrt[3]{-1}) = \mathbb{Q}(\omega_3)$ because
 $\omega_3 = \frac{-1 + \sqrt{-3}}{2}$.
 $n > 0$ "real" $n < 0$ "imaginary"

Def. 2. $\alpha \in K$ is integral if it is the root of a monic polynomial in $\mathbb{Z}[x]$.

Ring of integers: $\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ is integral}\}$.

Note: the monic polynomial need not be irreducible

(e.g. $\omega_n \in \mathcal{O}_{\mathbb{Q}(\omega_n)}$ even though $x^n - 1$ might be reducible).

Thm 3. $\alpha \in \mathcal{O}_K \Rightarrow$ the (monic)* min. poly. of α has coeffs in $\mathbb{Z}$.

*convention!

Fact 4. $f \in \mathbb{Z}[x]$ monic & $f = g \cdot h$ for $g, h \in \mathbb{Q}[x]$ monic $\Rightarrow g, h \in \mathbb{Z}[x]$.

Pf of Thm 3. Let $f \in \mathbb{Z}[x]$ monic, least degree s.t. $f(\alpha) = 0$.

Need to show f irreducible.

If $f = g \cdot h$ for $g, h \in \mathbb{Q}[x]$ non-constant

$\Rightarrow$ WLOG assume g, h monic

$\Rightarrow g, h \in \mathbb{Z}[x]$ & $0 = f(\alpha) = g(\alpha) \cdot h(\alpha)$
 (Fact 4)

$\Rightarrow g(\alpha)$ or $h(\alpha) = 0$ but $\deg(g), \deg(h) < \deg(f) \quad \nexists \quad \square$

Cor. 5. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

$m = \text{square-free integer} \ \& \ K = \mathbb{Q}(\sqrt{m}) \Rightarrow \mathcal{O}_K \supseteq \mathbb{Z}[\sqrt{m}]$.

$$\text{Cor. 6. } \mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \begin{cases} \mathbb{Z}[\sqrt{m}] & m \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{\sqrt{m}+1}{2}\right] & m \equiv 1 \pmod{4} \end{cases}$$

Pf. $\alpha = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ for $s \neq 0$ has min. poly

$$x^2 - 2rx + r^2 - ms^2 = 0$$

$$\Rightarrow \alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})} \Leftrightarrow 2r \in \mathbb{Z}, \ r^2 - ms^2 \in \mathbb{Z}.$$

$$r \in \mathbb{Z} \Rightarrow ms^2 \in \mathbb{Z} \Rightarrow s \in \mathbb{Z} \text{ b/c } m = \text{square-free}$$

$$r = \frac{r'}{2} \text{ for } r' \in \mathbb{Z} \Rightarrow (r')^2 - 4ms^2 \in 4\mathbb{Z}$$

$$\underline{\text{odd}} \Rightarrow s = \frac{s'}{2} \text{ } s' \text{ odd} \ \& \ (r')^2 - m(s')^2 \in 4\mathbb{Z}$$

$$\Rightarrow (r')^2 - m(s')^2 \equiv 0 \pmod{4}$$

$$\Rightarrow m \equiv 1 \pmod{4} \text{ b/c } r', s' \text{ odd}$$



Last time: • $K/\mathbb{Q}$ number field $\leadsto \mathcal{O}_K$ ring of integers.

Embeddings in $\mathbb{C}$. (Reminder from Galois theory.)

- $[K:\mathbb{Q}] = n \Rightarrow \# \text{Hom}(K, \mathbb{C}) = n$.
- More gen., K/F degree n & $\iota: F \hookrightarrow \mathbb{C}$
 $\Rightarrow \# \{ \tilde{\iota}: K \hookrightarrow \mathbb{C} : \tilde{\iota}|_F = \iota \} = n$.

Without using $\mathbb{C}$: $M = \text{normal closure of } K/F$

$$\begin{array}{c}
 K \\
 n | \\
 F
 \end{array}
 \begin{array}{c}
 \text{---} M \\
 \text{---}
 \end{array}
 \leadsto \# \{ \sigma: K \hookrightarrow M : \sigma|_F = \text{id}_F \} = n.$$

Examples. $\mathbb{Q}(\sqrt{n}) \hookrightarrow \mathbb{C}$
 $\sqrt{n} \mapsto \pm \sqrt{n}$

$$\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C} \\
 \sqrt[3]{2} \mapsto \sqrt[3]{2}, e^{\frac{2\pi i}{3}} \sqrt[3]{2}, e^{\frac{4\pi i}{3}} \sqrt[3]{2}$$

Caution.
 abstract number field
 vs. its embedding in $\mathbb{C}$.

$$\begin{array}{c}
 \mathbb{Q}(\sqrt[3]{2}, \omega_3) \hookrightarrow \mathbb{C} \\
 \sqrt[3]{2} \mapsto \sqrt[3]{2}, e^{\frac{2\pi i}{3}} \sqrt[3]{2}, e^{\frac{4\pi i}{3}} \sqrt[3]{2} \\
 \omega_3 \mapsto e^{2\pi i/3}, e^{4\pi i/3}
 \end{array}$$

Note: $M = \mathbb{Q}(\sqrt[3]{2}, \omega_3)$ is the normal closure of $\mathbb{Q}(\sqrt[3]{2})$.

$\text{Gal}(M/\mathbb{Q}) ? \cong S_3$

Recall : $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ is a ring. True in general !

Thm 1. TFAE for $\alpha \in K$:

- (1) $\alpha \in \mathcal{O}_K$
- (2) $\mathbb{Z}[\alpha]$ under $+$ is f.g.
- (3) $\forall \iota: K \hookrightarrow \mathbb{C}, \exists A \subseteq \mathbb{C}$ f.g. subgroup under $+$ s.t. $\iota(\alpha)A \subseteq A$.
- (4) $\exists \iota: K \hookrightarrow \mathbb{C}, \underline{\hspace{10cm}}$.

Pf. (1) $\Rightarrow$ (2) : α = root of monic poly in $\mathbb{Z}[x]$ of deg. n
 $\Rightarrow 1, \alpha, \dots, \alpha^{n-1}$ generate $\mathbb{Z}[\alpha]$

(2) $\Rightarrow$ (3) $\Rightarrow$ (4) : immediate.

(4) $\Rightarrow$ (1) : $a_1, \dots, a_n$ generate A

$$\Rightarrow \iota(\alpha) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = M \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad M \in M_{n \times n}(\mathbb{Z}) \quad (\text{b/c } \iota(\alpha) a_i \in A)$$

$$\Rightarrow (\iota(\alpha)I - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0$$

$$\Rightarrow \det(\iota(\alpha)I - M) = 0 \quad \therefore \alpha = \text{root of a monic poly} \in \mathbb{Z}[x]. \quad \square$$

Cor. 2. $\alpha, \beta \in \mathcal{O}_K \Rightarrow \alpha + \beta, \alpha\beta \in \mathcal{O}_K$, i.e. $\mathcal{O}_K$ is a ring.

Pf. $\mathbb{Z}[\alpha], \mathbb{Z}[\beta]$ finitely gen. $\Rightarrow \mathbb{Z}[\alpha, \beta]$ finitely gen.

& $\alpha + \beta, \alpha \cdot \beta \in \mathcal{O}_K$ by (4). $\square$

Next, work towards :

- $\mathcal{O}_{\mathbb{Q}(\omega_m)} = \mathbb{Z}[\omega_m]$
- In general, integral basis of $\mathcal{O}_K$.

Technical tools : norm, trace, discriminant.

Def 3. K/F , $\alpha \in K \rightsquigarrow m_\alpha: K \longrightarrow K$ F -linear map
 $x \longmapsto \alpha x$

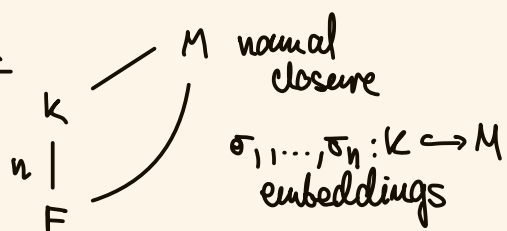
- trace of α : $T_{K/F}(\alpha) := \text{Tr}(m_\alpha) \in F$,
- norm of α : $N_{K/F}(\alpha) := \det(m_\alpha) \in F$.

write $T_K := T_{K/\mathbb{Q}}$
 $N_K := N_{K/\mathbb{Q}}$
 or even drop K
 when implicit!

Note: $f_\alpha(x) = \det(x \cdot \text{id} - m_\alpha)$ char. poly of m_α
 $= x^n - a_1 x^{n-1} + \dots + (-1)^n a_n$

$$\Rightarrow a_1 = \text{Tr}_{K/F}(\alpha), a_n = N_{K/F}(\alpha).$$

Thm. 4.



- $f_\alpha(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$,
- $T_{K/F}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$,
- $N_{K/F}(\alpha) = \sigma_1(\alpha) \cdot \dots \cdot \sigma_n(\alpha)$.

Pf. K $\beta_1, \dots, \beta_m$ basis of $K/F(\alpha)$

(Take $M = \mathbb{C}$ if you're scared)
 of normal closures.

$F(\alpha)$ $1, \alpha, \dots, \alpha^{d-1}$

F basis of $F(\alpha)/F$

$\rightsquigarrow \beta_1, \beta_1 \alpha, \dots, \beta_1 \alpha^{d-1}; \dots; \beta_m, \beta_m \alpha, \dots, \beta_m \alpha^{d-1}$
 basis of K/F

If $f(x) = \text{min. poly of } \alpha \text{ over } F$, then m_α block-diag. with blocks:

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & & \ddots & \\ & & & & 1 \\ -c_d & -c_{d-1} & \dots & & -c_1 \end{bmatrix}.$$

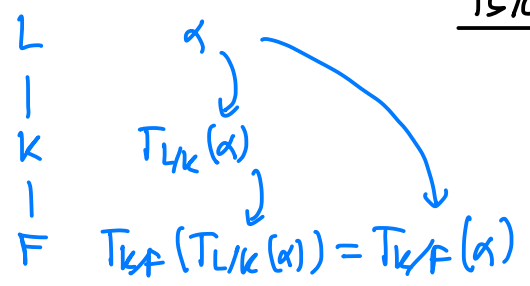
$$f(x) = x^d + c_1 x^{d-1} + \dots + c_d$$

$$\Rightarrow f_\alpha(x) = f(x)^m.$$

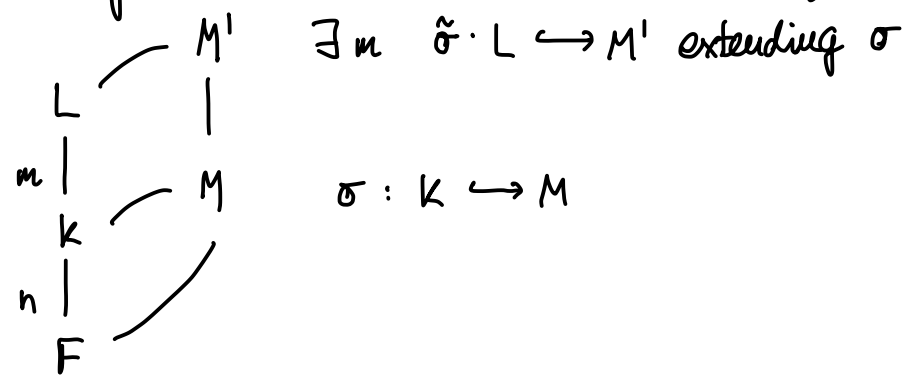
Recalling from Galois theory that $f(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$
 completes the proof. □

Cor. 5 (tower law). For fields $L/K/F$,

- $T_{K/F}(T_{L/K}(\alpha)) = T_{L/F}(\alpha)$,
- $N_{K/F}(N_{L/K}(\alpha)) = N_{L/F}(\alpha)$.



Pf. Check using Thm 4 & extensions of embeddings.



Cor 6. $\alpha \in \mathcal{O}_K \Rightarrow T_{K/F}(\alpha), N_{K/F}(\alpha) \in \mathcal{O}_F$.

Example. $K = \mathbb{Q}(\sqrt{m}) / F = \mathbb{Q}$

$$T(r + s\sqrt{m}) = 2r$$

$$N(r + s\sqrt{m}) = r^2 - ms^2$$

& we saw $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})} \Leftrightarrow T(\alpha), N(\alpha) \in \mathbb{Z}$.

$\Leftarrow$ not true in general

§. Discriminants.

$K/\mathbb{Q}$ degree n & $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ all emb.

Def 7. $\alpha_1, \dots, \alpha_n \in K \leadsto \text{disc}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$ discriminant

Thm 8. $\text{disc}(\alpha_1, \dots, \alpha_n) = \det(T(\alpha_i \alpha_j))$.

$$T := T_{K/\mathbb{Q}}$$

Pf. $[\sigma_j(\alpha_i)]_{i,j} \cdot [\sigma_i(\alpha_j)]_{i,j} = \left[\sum_k \sigma_k(\alpha_i \alpha_j) \right]_{i,j} \underset{\text{Thm 4}}{=} [T(\alpha_i \alpha_j)]_{i,j}$ □

Cor 9. $\text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$,

$\text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$ if $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$.

Thm 10. $\text{disc}(\alpha_1, \dots, \alpha_n) = 0 \Leftrightarrow \alpha_1, \dots, \alpha_n$ linearly dep. over $\mathbb{Q}$.

Pf. ' $\Leftarrow$ ' Clear by def.

' $\Rightarrow$ ' Rows of $T(\alpha_i \alpha_j)$ are lin. dep. (by Thm 8)

$$\Rightarrow 0 = \sum_{i=1}^n q_i T(\alpha_i \alpha_j) = T(\alpha \alpha_j) \text{ for } \alpha = \sum q_i \alpha_i, \forall j$$

Suppose for a contr. that $\alpha_1, \dots, \alpha_n$ lin. indep. ($\Rightarrow$ basis)

Then $\alpha \neq 0$ & $\alpha \alpha_1, \dots, \alpha \alpha_n$ lin. indep. too. ($\Rightarrow$ basis)

$$\Rightarrow 1 = \sum b_j (\alpha \alpha_j) \text{ but } n = T(1) = \sum b_j T(\alpha \alpha_j) = 0 \quad \blacktriangleleft \quad \square$$

Thm 11. $K = \mathbb{Q}(\alpha) \rightsquigarrow \alpha_i := \sigma_i(\alpha) \in \mathbb{C}$

$$\text{disc}(1, \alpha, \dots, \alpha^{n-1}) \stackrel{(1)}{=} \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 \stackrel{(2)}{=} \pm N(f'(\alpha))$$

$f = \text{min. poly of } \alpha / \mathbb{Q}; \quad \pm = + \Leftrightarrow n \equiv 0, 1 \pmod{4}.$

Pf. $\det(\sigma_i(\alpha_j^{-1})) = \det(\sigma_i(\alpha)^{j-1}) = \det(\alpha_i^{j-1})$ Vandermonde det.

$\Rightarrow (1).$ (Exercise.)

For (2), note: $\prod_{r < s} (\alpha_r - \alpha_s)^2 = \pm \prod_{r \neq s} (\alpha_r - \alpha_s)$

$$\text{Now, } N(f'(\alpha)) = \prod_{i=1}^n \sigma_i(f'(\alpha)) = \prod_{i=1}^n f'(\sigma_i(\alpha)) = \prod_{i=1}^n f'(\alpha_i).$$

Writing $f(x) = \prod_j (x - \alpha_j)$ over $\mathbb{C}$, get $f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$ ✓

Def. 12. $\text{disc}(\alpha) := \text{disc}(1, \alpha, \dots, \alpha^{n-1})$ if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.

Example. Thm 5 $\Rightarrow \text{disc}(\omega_p) = \pm p^{p-2}$. (Exercise.)

$\text{disc}(\omega_m)$ more complicated, but if $x^m - 1 = f(x) \cdot g(x)$, $g(x) \in \mathbb{Z}[x]$

$$\text{Thm 5} \Rightarrow m^{\varphi(m)} = \pm \text{disc}(\omega_m) \cdot \underbrace{N(\omega g(\omega))}_{\in \mathbb{Z}}$$

$$\Rightarrow \text{disc}(\omega_m) \mid m^{\varphi(m)}.$$

(Homework grading: see eCampus.)

Last time:

$$\begin{array}{c}
 \begin{array}{ccc}
 & M & \\
 K & \swarrow & \\
 n & | & \\
 F & \searrow & \\
 & \text{Galois} &
 \end{array}
 \end{array}
 \quad \sigma_1, \dots, \sigma_n : K \hookrightarrow M
 \quad \left\{ \begin{array}{l}
 \bullet \text{ trace : } T(\alpha) = T_{K/F}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha) \in F \\
 \bullet \text{ norm : } N(\alpha) = N_{K/F}(\alpha) = \sigma_1(\alpha) \cdot \dots \cdot \sigma_n(\alpha) \in F \\
 \bullet \text{ disc : } \alpha_1, \dots, \alpha_n \in K \\
 \text{disc}_{K/F}(\alpha_1, \dots, \alpha_n) := \det(\sigma_i(\alpha_j))^2 = \det(T(\alpha_i, \alpha_j)) \in F
 \end{array} \right.$$

(Assumed $F = \mathbb{Q}$, but not necessary.)

§. Additive structure of $\mathcal{O}_K$.

Goal: $\mathcal{O}_K$ = free ab. gp of rk $n = [K:\mathbb{Q}]$ (under $+$).

E.g. $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ gen. by 1 and $\begin{cases} \sqrt{m} & (m \equiv 1 \pmod{4}) \\ \frac{1+\sqrt{m}}{2} & (m \equiv 0 \pmod{4}) \end{cases}$

Idea: **Sandwich:** $\underbrace{A \subseteq B \subseteq C}_{\text{free rk } n} \Rightarrow B \text{ free of rk } n.$

Exercise. $\forall \alpha \in K \exists m \in \mathbb{Z} \text{ s.t. } m\alpha \in \mathcal{O}_K.$ (HW 2.)

$\Rightarrow \exists$ basis $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ of $K/\mathbb{Q}$.

$\Rightarrow \mathbb{Z}\langle \alpha_1, \dots, \alpha_n \rangle \subseteq \mathcal{O}_K$ free ab. gp of rk n .

$$\begin{array}{c}
 \mathbb{Z}\langle \alpha \rangle \oplus \dots \oplus \mathbb{Z}\langle \alpha_n \rangle \\
 \parallel \\
 \mathbb{Z}^n
 \end{array}$$

How to close the sandwich?

Thm 1. $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ basis of $K/\mathbb{Q}$, $d := \text{disc}(\alpha_1, \dots, \alpha_n)$

$\Rightarrow \mathcal{O}_K \subseteq \mathbb{Z}\langle \alpha_1/d, \dots, \alpha_n/d \rangle.$

In fact, any $\alpha \in \mathcal{O}_K$ is $\alpha = \frac{\sum m_i \alpha_i}{d}$, $m_i \in \mathbb{Z}$, $d \mid m_i^2$.

Pf. $\alpha \in \mathcal{O}_K \Rightarrow \alpha = x_1 \alpha_1 + \dots + x_n \alpha_n, \quad x_i \in \mathbb{Q}$

$$\Rightarrow \sigma_i(\alpha) = x_1 \sigma_i(\alpha_1) + \dots + x_n \sigma_i(\alpha_n) \quad \forall i$$

$$\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} = (\sigma_i(\alpha_j)) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \Rightarrow \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\sigma_i(\alpha_j))^{-1} \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}.$$

Say $\delta := \det(\sigma_i(\alpha_j))$ so $\delta^2 = d \in \mathbb{Z}$ (Cor. 2.9). Then:

- $\delta x_i \in \mathcal{O}_K \Rightarrow u_i := \delta x_i \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$,
- $u_i^2 / d = (d x_i)^2 / d = d x_i^2 = \delta^2 x_i^2 \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. □

Cor 2. $\mathcal{O}_K$ is a free ab. gp of rk n .

Def 3. $\text{disc}(K) := \text{disc}(\mathcal{O}_K) := \text{disc}(\alpha_1, \dots, \alpha_n)$ discriminant of K
where $\alpha_1, \dots, \alpha_n =$ any basis of $\mathcal{O}_K$.

Lemma 4. $\text{disc}(K)$ is well-defined.

Pf. $\beta_1, \dots, \beta_n$ different basis & $M =$ change of basis matrix

$$\Rightarrow \text{disc}(\alpha_1, \dots, \alpha_n) = \underbrace{\det(M)^2}_{\pm 1} \cdot \det(\beta_1, \dots, \beta_n).$$

Example.

$$\begin{aligned} \text{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{m})}) &= \begin{cases} \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 & m \equiv 1 \pmod{4} \\ \det \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 & m \equiv 0 \pmod{4} \end{cases} \\ &= \begin{cases} 4m & m \equiv 1 \pmod{4} \\ m & m \equiv 0 \pmod{4} \end{cases} \end{aligned}$$

In fact: $\beta_1, \dots, \beta_n = \mathcal{O}_K$ -basis $\Leftrightarrow \text{disc}(\beta_1, \dots, \beta_n) = \text{disc}(K)$.

Next goals:

- $\mathcal{O}_{\mathbb{Q}(\omega_n)} = \mathbb{Z}[\omega_n]$ (finally) ↗ $n = p^r$
- Generators of $\mathcal{O}_K$ in general. ↘ $(u, n) = 1 \rightarrow \mathbb{Q}(\omega_{un}) = \mathbb{Q}(\omega_n)\mathbb{Q}(\omega_u)$

Thm 5. For $K = \mathbb{Q}(\omega_{p^r})$, $\mathcal{O}_K = \mathbb{Z}[\omega_{p^r}]$.

Lemma 6. $\mathbb{Z}[1-\omega] = \mathbb{Z}[\omega]$ and $\text{disc}(1-\omega) = \text{disc}(\omega)$.

Pf. $\omega = 1 - (1-\omega)$ & apply Thm 2.11 (1):

$$\text{disc}(\omega) = \prod_{i < j} (\sigma_i(\omega) - \sigma_j(\omega))^2 = \prod_{i < j} (1 - \sigma_i(\omega) - (1 - \sigma_j(\omega)))^2 = \text{disc}(1-\omega). \quad \square$$

Lemma 7. $\prod_{\substack{p \nmid k \\ 1 \leq k \leq p^r}} (1 - \omega^k) = p$ for $\omega = \omega_{p^r}$.

$r=1$: $(1-\omega)(1-\omega^2) \dots (1-\omega^{p-1}) = p \rightarrow$ Use this in HWO! ▼

Pf. $f(x) := \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + \dots + x^{(p-1)p^{r-1}}$

$$\Rightarrow f(\omega^k) = 0 \text{ for } p \nmid k \Rightarrow f(x) = \prod (x - \omega^k) \text{ (equal degrees)}$$

Setting $x=1$ gives the result. □

Pf of Thm 5. Thm 1 $\Rightarrow \alpha \in \mathcal{O}_{\mathbb{Q}(\omega)}$ can be written as:

$$\alpha = \frac{u_1 + u_2(1-\omega) + \dots + u_n(1-\omega)^{n-1}}{d}$$

$$\begin{aligned} n &= \varphi(p^r) \\ u_i &\in \mathbb{Z} \\ d &= \text{disc}(1-\omega) = \text{disc}(\omega) \\ &= \text{power of } p. \end{aligned}$$

Suppose $\exists \alpha$ s.t. $d \nmid m_i$, same i . Then there is an element:

$$\beta := \frac{p \cdot m_i (1-\omega)^{i-1} + m_{i+1} (1-\omega)^i + \dots + m_n (1-\omega)^{n-1}}{p} \in \mathcal{O}_{\mathbb{Q}(\omega)}$$

$$\text{lemma 7} \Rightarrow p/(1-\omega)^n \in \mathbb{Z}[\omega] \quad \text{b/c } 1-\omega \mid 1-\omega^k$$

$$\Rightarrow p/(1-\omega)^i \in \mathbb{Z}[\omega] \Rightarrow \beta \cdot p/(1-\omega)^i \in \mathcal{O}_{\mathbb{Q}(\omega)}$$

$$\Rightarrow \frac{m_i}{1-\omega} \in \mathcal{O}_K \Rightarrow p = N(1-\omega) \mid N(m_i) = m_i^n \quad \text{lemma 11}$$

□

Next: $\mathcal{O}_{\mathbb{Q}(\omega_m)} = \mathbb{Z}[\omega_m]$ $\forall m$ using composita of fields.

$$\mathcal{O}_K \mathcal{O}_L \subseteq \mathcal{O}_{KL}$$

Caution: $\mathcal{O}_K \mathcal{O}_L \neq \mathcal{O}_{KL}$ in general!

$$\begin{array}{ccc} & & \\ & \swarrow & \searrow \\ \mathcal{O}_K \subseteq K & & L \supseteq \mathcal{O}_L \\ & \searrow & \swarrow \\ & \mathbb{Q} & \end{array}$$

$$\text{Exercise. } \frac{\sqrt{3} + \sqrt{7}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{3}, \sqrt{7})}.$$

HW 2

$$\text{but } \mathbb{Q}(\sqrt{3}) = \mathbb{Z}[\sqrt{3}], \mathbb{Q}(\sqrt{7}) = \mathbb{Z}[\sqrt{7}]$$

Thm 8. Let K, L be number fields with $K \cap L = \mathbb{Q}$. Then

$$\mathcal{O}_K \cdot \mathcal{O}_L \subseteq \mathcal{O}_{KL} \subseteq \frac{1}{\gcd(\text{disc}(K), \text{disc}(L))} \mathcal{O}_K \cdot \mathcal{O}_L.$$

Exercise. For $K = \mathbb{Q}(\sqrt{3})$, $L = \mathbb{Q}(\sqrt{7})$, neither equality holds!

HW 2

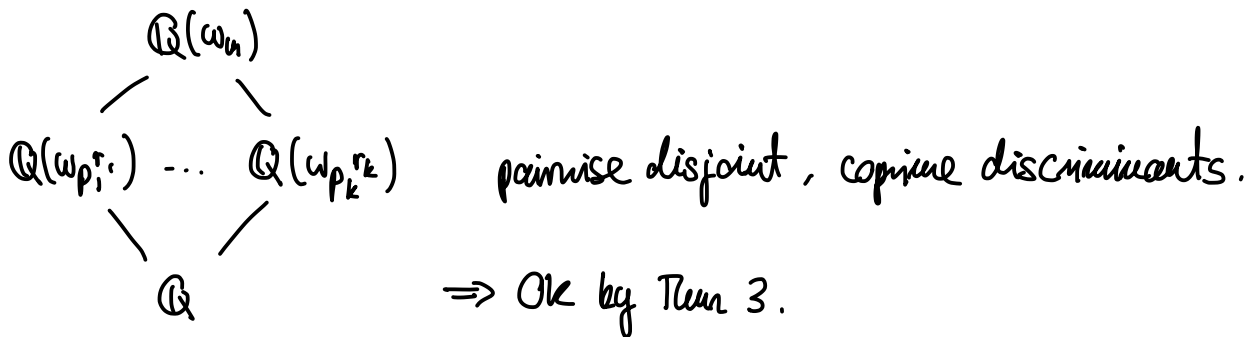
$$(\gcd(4 \cdot 3, 4 \cdot 7) = 4)$$

$$\text{Cor. 9. } \gcd(\text{disc}(K), \text{disc}(L)) = 1 \Rightarrow \mathcal{O}_{KL} = \mathcal{O}_K \cdot \mathcal{O}_L.$$

$$\text{Cor. 10. } \mathcal{O}_{\mathbb{Q}(\omega_m)} = \mathbb{Z}[\omega_m].$$

Pf. For $m = p^r$, this was Thm 5.

For $m = p_1^{r_1} \dots p_k^{r_k}$, we see $\omega_m = \omega_{p_1^{r_1}} \dots \omega_{p_k^{r_k}}$



Pf of Thm 8. $\alpha_1, \dots, \alpha_n$ basis of $\mathcal{O}_K$ $\leadsto \alpha_i \cdot \beta_j$ basis of $\mathcal{O}_K \cdot \mathcal{O}_L$
 $\beta_1, \dots, \beta_n$ basis of $\mathcal{O}_L$ & $\mathbb{Q}$ -basis of $K \cdot L$

For $\alpha \in \mathcal{O}_{KL}$, $\alpha \in KL$ so:

$$\alpha = \sum_{i,j} \frac{u_{ij}}{r} \alpha_i \cdot \beta_j \quad u_{ij}, r \in \mathbb{Z}, \gcd(r, \gcd(u_{ij})) = 1.$$

Claim: $r \mid \text{disc}(K)$. (By symmetry, $r \mid \text{disc}(L) \Rightarrow r \mid \gcd \checkmark$.)

$\sigma: K \hookrightarrow \mathbb{C}, \tau: L \hookrightarrow \mathbb{C} \leadsto \sigma\tau: KL \hookrightarrow \mathbb{C}$ extension

$$\Rightarrow \sigma\tau(\alpha) = \sum_{i,j} \frac{u_{ij}}{r} \sigma(\alpha_i) \tau(\beta_j).$$

$$\text{Set } x_i := \sum_{j=1}^n \frac{u_{ij}}{r} \tau(\beta_j) \leadsto \sum_{i=1}^n \sigma_k(\alpha_i) x_i = \sigma_k \tau(\alpha) \quad \forall \sigma_1, \dots, \sigma_n: K \hookrightarrow \mathbb{C}$$

$$(\sigma_k(\alpha_i)) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sigma_1 \tau(\alpha) \\ \vdots \\ \sigma_n \tau(\alpha) \end{pmatrix} \Rightarrow \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\sigma_k(\alpha_i))^{-1} \begin{pmatrix} \sigma_1 \tau(\alpha) \\ \vdots \\ \sigma_n \tau(\alpha) \end{pmatrix}$$

$$\Rightarrow d \cdot x_i = \sum_{j=1}^n \frac{d u_{ij}}{r} \beta_j \in \mathcal{O}_L \quad d := \text{disc}(\sigma_k(\alpha_i))^2 = \text{disc}(K)$$

$\Rightarrow$
as in proof
of Thm 1

$\in \mathbb{Z}$ b/c β_j $\mathbb{Z}$ -basis of $\mathcal{O}_L$

$$\Rightarrow r \mid \text{disc}(K) u_{ij} \quad \forall i, j$$

$$\Rightarrow r \mid \gcd(\text{disc}(K) u_{ij}) \Rightarrow r \mid \text{disc}(K).$$

LECTURE 4.

22/4

Last time: • $\mathcal{O}_K$ = free ab., rank n ; • $\mathcal{O}_{\mathbb{Q}(\omega_m)} = \mathbb{Z}[\omega_m] \quad \forall m$

Caution. Not every $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α .

$\mathbb{Z}[\alpha]$ = gen. by α as a ring
 $\Leftrightarrow \mathbb{Z}\langle 1, \alpha, \alpha^2, \dots, \alpha^{n-1} \rangle$
 = gen. by $1, \alpha, \dots, \alpha^{n-1}$ as a $\mathbb{Z}$ -module

Exercise. $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$. (HW 2.)

$\leadsto$ can't have $\mathbb{Z}$ -basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ in general...

But $K = \mathbb{Q}(\alpha) \Rightarrow \exists$ basis in terms of polynomials in α .

Here's the best we can do in general.

Thm 1. let $\alpha \in \mathcal{O}_K$ have degree n over $\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$. Then:

$\exists f_1, \dots, f_{n-1} \in \mathbb{Z}[x]$ monic, $\deg(f_i) = i$

$\exists$ unique $d_1 | \dots | d_{n-1}$ in $\mathbb{Z}$

s.t. $1, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}}$ basis of $\mathcal{O}_K$.

Examples • $\mathbb{Q}(\sqrt{m})$: $m = \square$ -free, basis of $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$: $\begin{cases} 1, \sqrt{m} & d_1=1 \quad m \equiv 1 \pmod{4} \\ 1, \frac{1+\sqrt{m}}{2} & d_1=2 \quad m \equiv 1 \pmod{4} \end{cases}$

• $\mathbb{Q}(\sqrt[3]{m})$: $m = \square$ -free, $\alpha = \sqrt[3]{m}$ (Exercise 2.41 in Marcus.)

properties of m	basis of $\mathcal{O}_{\mathbb{Q}(\alpha)}$	disc $(\mathbb{Q}(\alpha))$
$m = \square$ -free $\begin{cases} m \not\equiv \pm 1 \pmod{9} \\ m \equiv \pm 1 \pmod{9} \end{cases}$	$1, \alpha, \alpha^2 \quad d_1=d_2=1$ $1, \alpha, \frac{\alpha^2 \pm \alpha + 1}{2} \quad d_2=2$	$-27m^2$ $-3m^2$
$m = h \cdot k^2$ $k = \square$ -free $(h, h) = 1$ $\begin{cases} m \not\equiv \pm 1 \pmod{9} \\ m \equiv \pm 1 \pmod{9} \end{cases}$	$1, \alpha, \frac{\alpha^2}{k} \quad d_2=k$ $1, \alpha, \frac{\alpha^2 \pm k^2 \alpha + k^2}{3k} \quad d_2=3k$	$-27(hk)^2$ $-3(hk)^2$

• Exercise. Determine $\mathcal{O}_{\mathbb{Q}(\sqrt{m}, \sqrt{n})}$. (HW 2)

Pf of Thm 1. $d := \text{disc}(K) \rightsquigarrow F_j := \mathbb{Z} \left\langle \frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^{j-1}}{d} \right\rangle \subseteq K$
 $\bigcup_j$
 $\mathcal{O}_j := F_j \cap \mathcal{O}_K$ (free ab. gp of rk j)

Then ... $\mathbb{Z} = \mathcal{O}_1 \subseteq \mathcal{O}_2 \subseteq \dots \subseteq \mathcal{O}_{n-1} \subseteq \underbrace{\mathcal{O}_n = \mathcal{O}_K}_{\text{Thm 3.1}}$.

Goal: define d_i, f_i s.t. $1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{j-1}(\alpha)}{d_j}$ basis of $\mathcal{O}_j$

$j=1 \rightsquigarrow \mathcal{O}_1 = 1 \checkmark$

Suppose $j < n$ & $1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{j-1}(\alpha)}{d_{j-1}}$ basis of $\mathcal{O}_j$

$\rightsquigarrow$ want to define f_j & d_j to get basis of $\mathcal{O}_{j+1}$.

$F_{j+1} = \mathbb{Z} \left[\frac{1}{d}, \dots, \frac{\alpha^j}{d} \right] \xrightarrow{\pi} \mathbb{Z} \left[\frac{\alpha^j}{d} \right] \xleftarrow{\text{cyclic}} \text{"pick out deg. } j \text{ term"}$
 $\bigcup_j$
 $\mathcal{O}_{j+1} \xrightarrow{\pi} \pi(\mathcal{O}_{j+1}) \xleftarrow{\text{cyclic}}$
 $\beta \xrightarrow{\pi} \pi(\beta) \xleftarrow{\text{generator}}$

$\Rightarrow \mathcal{O}_{j+1} = \mathbb{Z} \left[1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{j-1}(\alpha)}{d_{j-1}}, \beta \right]$ (Exercise: convince yourself of this!)

WTS: β has the form: $\frac{f_j(\alpha)}{d_j}$ with $d_{j-1} \mid d_j$, $f_j \in \mathbb{Z}[x]$ deg j , monic.

Since $f_{j-1}(\alpha) = \alpha^{j+1} + \text{lower degree terms}$, $\pi(\alpha \cdot f_{j-1}(\alpha)) = \alpha^j$

$\Rightarrow \pi \left(\alpha \cdot \frac{f_{j-1}(\alpha)}{d_{j-1}} \right) = \frac{\alpha^j}{d_{j-1}} \Rightarrow \frac{\alpha^j}{d_{j-1}} = m \cdot \pi(\beta), \text{ some } m \in \mathbb{Z}.$
 $\in \pi(\mathcal{O}_{j+1}) = \mathbb{Z}[\pi(\beta)]$

let $d_j := m \cdot d_{j-1}$ so that $\pi(\beta) = \frac{\alpha^j}{d_j}$.

$$\Rightarrow \beta = \frac{f_j(\alpha)}{d_j} \text{ with } f_j(x) = x^j + \dots \in \mathbb{Q}[x] \text{ \& } \frac{d}{d_j} \cdot f_j \in \mathbb{Z}[x].$$

$$(d \cdot \beta \in \mathbb{Z}[\alpha_1, \dots, \alpha_i])$$

Need $f_j \in \mathbb{Z}[x]$.

$$\text{Set } \gamma := \frac{f_j(\alpha) - \alpha f_{j-1}(\alpha)}{d_{j-1}} \in \mathcal{O}_j \subseteq \mathcal{O}_K$$

$$\Rightarrow \gamma = \frac{g(\alpha)}{d_{j-1}} \text{ for } g \in \mathbb{Z}[x], \deg(g) < j \text{ (using our } \mathbb{Z}\text{-basis of } \mathcal{O}_j)$$

$$\Rightarrow f_j(x) - x f_{j-1}(x) = g(x) \quad (\text{b/c } [\mathbb{Q}(\alpha) : \mathbb{Q}] = d)$$

$$\Rightarrow f_j \in \mathbb{Z}[x]. //$$

Final piece: uniqueness of d_j .

Exercise. $d_j =$ smallest positive integer m s.t. $m \cdot \mathcal{O}_{j+1} \subseteq \mathbb{Z}[\alpha]$.

(HW 2)



Done with additive structure of $\mathcal{O}_K$:

- free abelian group of rank $n := [K : \mathbb{Q}]$,

- examples: $\rightarrow \mathcal{O}_{\mathbb{Q}(\sqrt{m})} =$ (two cases)

$$\rightarrow \mathcal{O}_{\mathbb{Q}(\omega_m)} = \mathbb{Z}[\omega_m]$$

$\rightarrow$ cubic fields

$\rightarrow$ biquadratic fields

- Thm 1: general result about $\mathbb{Z}$ -basis in terms of $\alpha \in \mathcal{O}_K$.

§ Prime decomposition of ideals in $\mathcal{O}_K$.

• HW 1, Q4 (b): $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ not a UFD

$\Rightarrow$ Instead, we want to show ideals factor into prime ideals.

• HW 1, Q4 (a): ideals don't factor in $\mathbb{Z}[\sqrt{3}]$

$\Rightarrow$ important to take all of $\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}\left[\frac{1+\sqrt{3}}{2}\right]$.

Def 2. A Noetherian integral domain R is a Dedekind domain if:

- R is integrally closed in $\text{Frac}(R)$ (normal),
- every non-zero prime is maximal ($\dim = 1$).

(Why is $R = \mathbb{Z}[\sqrt{3}]$ not a Dedekind domain?)

Thm 3. $\mathcal{O}_K$ is a Dedekind domain.

Pf. Integral domain b/c $\mathcal{O}_K \subseteq K$; normal by definition.

Noetherian: Cor. 3.2: $\mathcal{O}_K =$ free ab. gp of finite rk

$\Rightarrow I \trianglelefteq \mathcal{O}_K$ also free ab. gp of finite rk

$\Rightarrow$ f.g. as an ideal. $\checkmark$

$\dim \mathcal{O}_K = 1$: $0 \neq \mathfrak{p} \trianglelefteq \mathcal{O}_K$ prime. Want: $\mathcal{O}_K/\mathfrak{p}$ field.

Enough to show: $\mathcal{O}_K/\mathfrak{p}$ is finite (b/c every finite domain is a field).

This is true for every $0 \neq I \trianglelefteq \mathcal{O}_K$:

$\alpha \in I \Rightarrow n := N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and $n \in I$ by Thm 2.10

$\Rightarrow |\mathcal{O}_K/I| \leq |\mathcal{O}_K/n \cdot \mathcal{O}_K| = n^n.$

□

From now on, ideals are non-zero & $R =$ Dedekind domain, $K = \text{Frac}(R).$ L4. / 4.

Cor 4. $0 \neq I \trianglelefteq \mathcal{O}_K \Rightarrow |\mathcal{O}_K/I| < \infty$.

Corollary of
the proof!

Thm 5. $I \trianglelefteq R$ ideal $\Rightarrow \exists J \trianglelefteq R$ s.t. $I \cdot J$ is principal.

This will be a longer proof $\leadsto$ start with 2 lemmas.

Lemma 6. Every $I \trianglelefteq R$ contains a product of prime ideals.

Pf. Suppose not & take M = maximal ideal not containing such a product (R Noetherian!).

$M \neq \text{prime} \Rightarrow \exists r, s \in R \setminus M$ s.t. $r \cdot s \in M$

$\Rightarrow M + (r), M + (s) \supsetneq M$

$\Rightarrow$ contain products of primes

$\Rightarrow M \supseteq (M + (r)) \cdot (M + (s)) \supseteq \text{product of primes.} \quad \square$

Lemma 7. $I \trianglelefteq R \Rightarrow \exists \gamma \in K \setminus R$ s.t. $\gamma I \subseteq R$.

Pf. $0 \neq a \in I \leadsto (a) \supseteq \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r$ for prime ideals $\mathfrak{p}_i \subseteq R$.

Take r = minimal.

Now, $I \subseteq \mathfrak{p}$ for some prime $\mathfrak{p}$ (R Noetherian!)

$\mathfrak{p}_1 \dots \mathfrak{p}_r \Rightarrow \mathfrak{p}_i \subseteq \mathfrak{p}$ for some i ($\mathfrak{p}$ prime)

$\Rightarrow \mathfrak{p}_i = \mathfrak{p}$ ($\dim R = 1$)

WLOG $i=1$. r minimal $\Rightarrow (a) \not\subseteq \mathfrak{p}_2 \dots \mathfrak{p}_r$

(i.e. $I \subseteq \mathfrak{p}_1$)

$\Rightarrow \exists b \in \mathfrak{p}_2 \dots \mathfrak{p}_r \setminus (a)$.

Finally: $\gamma = b/a \in K \setminus R$ satisfies $\gamma I \subseteq R$:

$x \in I \subseteq \mathfrak{p}_1 \Rightarrow x \cdot b \in \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq (a) \Rightarrow \frac{x \cdot b}{a} \in R \quad \square \quad \text{L4.5.}$

Pf of Thm 5. $0 \neq \alpha \in I \rightsquigarrow \mathcal{I} := \{B \in R : BI \subseteq (\alpha)\} \neq 0$ 22/4
 clearly satisfies $I \cdot \mathcal{I} \subseteq (\alpha)$. ($\alpha \in \mathcal{I}$ at least)

Want: $I \cdot \mathcal{I} = (\alpha)$.

Consider $A = \frac{1}{\alpha} I \cdot \mathcal{I} \subseteq R$ & show $A = R$.

Else $A \subsetneq R$ & Lemma 7 $\Rightarrow \exists \gamma \in K \setminus R$ s.t. $\gamma A \subseteq R$.

Note: $\alpha \in I \Rightarrow \mathcal{I} \subseteq A \Rightarrow \gamma \mathcal{I} \subseteq \gamma A \subseteq R$

In fact: $\gamma \mathcal{I} \subseteq \mathcal{I}$. Indeed:

$$(\alpha) = \alpha R \supseteq \alpha \gamma A = \alpha \gamma \frac{1}{\alpha} I \cdot \mathcal{I} = \gamma \mathcal{I} \cdot I \Rightarrow \gamma \mathcal{I} \subseteq \mathcal{I} \text{ by def. of } \mathcal{I}.$$

Finally, if $\mathcal{I} = (\alpha_1, \dots, \alpha_m)$, then

$$\gamma \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \quad M \in M_{m \times m}(R)$$

$\Rightarrow$ char. poly of M shows γ is integral $\Rightarrow \gamma \in R$ (R normal) $\square$

Cor. 8. Ideal classes of R form a group. (HW1, Q3(d).)

Cor. 9. $A, B, C \subseteq R$ & $AB = AC \Rightarrow B = C$. "Cancellation law"

Pf. $\exists \mathcal{I}$ s.t. $A\mathcal{I} = (\alpha) \Rightarrow \alpha B = \alpha C \Rightarrow B = C$. $\square$

Cor. 10. $A, B \subseteq R$. $A \mid B \Leftrightarrow A \supseteq B$.

Pf. $A \mid B \Rightarrow A \supseteq B$ $\checkmark$

$A \supseteq B \Rightarrow$ fix $\mathcal{I}$ s.t. $A\mathcal{I} = (\alpha)$ & set $C := \frac{1}{\alpha} \mathcal{I} B \subseteq R$
 $\Rightarrow AC = B$. $\square$

Next time: ideals factor into prime ideals!

Last time: $R = \text{Dedekind domain}$ (Noetherian, normal, $\dim 1$)

• Cor. 4.9: $AB = AC \Rightarrow B = C$ for $A, B, C \trianglelefteq R$ "cancellation law"

• Cor. 4.10: $A \mid B \Leftrightarrow A \supseteq B$ for $A, B \trianglelefteq R$

Thm 1. $\forall I \trianglelefteq R \exists ! \mathfrak{p}_1, \dots, \mathfrak{p}_r$ prime s.t. $\mathfrak{p}_1 \cdots \mathfrak{p}_r = I$.

($r = \text{empty prod.}$)

Pf. Existence. Suppose not.

Let $M = \text{largest (proper) ideal not rep. as a product of primes.}$ (R Noetherian)
 $\subseteq \mathfrak{p}$ prime ideal.

$\Rightarrow M = \mathfrak{p} \cdot I$ for some I by Cor. 4.10

$\Rightarrow I \supseteq M$ & $I \neq M$ or else $R \cdot M = \mathfrak{p} \cdot M \Rightarrow R = \mathfrak{p}$ by Cor. 4.9

$\Rightarrow I \not\supseteq M \Rightarrow I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ by maximality of M

$\Rightarrow M = \mathfrak{p} \mathfrak{p}_1 \cdots \mathfrak{p}_r \quad \nsubseteq //$

Uniqueness. $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$

$\Rightarrow \mathfrak{p}_1 \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s$

$\Rightarrow \mathfrak{p}_1 \supseteq \mathfrak{q}_i$ some i ($\mathfrak{p}_1$ prime!)

$\Rightarrow \mathfrak{p}_1 = \mathfrak{q}_i$ ($\dim R = 1$)

$\Rightarrow \mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_{i-1} \mathfrak{q}_{i+1} \cdots \mathfrak{q}_s$ (Cor. 4.9.)

$\Rightarrow \dots \Rightarrow r = s$ & $\mathfrak{p}_i = \mathfrak{q}_i \forall i$ (after reordering)

□

Cor 2. Ideals in $\mathcal{O}_K$ factor uniquely into prime ideals.

Example. $K = \mathbb{Q}(\sqrt{5})$. We have:

$$(2) = (2, 1 + \sqrt{5})^2 \quad (\text{e.g. } (1 + \sqrt{5})^2 = -4 + 2\sqrt{5}, \text{ etc.})$$

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

$$\text{Primes } b/c \# \mathcal{O}_K/(2) = 4 \Rightarrow 1 \not\subseteq \underbrace{\mathcal{O}_K/(2, 1 + \sqrt{5})}_{\text{order 2}} \not\subseteq \mathcal{O}_K/(2), \text{ etc.}$$

Recall from HW 1: $2 \cdot 3 = 6 = (1 + \sqrt{5})(1 - \sqrt{5})$.

As ideals, can check:

$$(2, 1 + \sqrt{5})(3, 1 + \sqrt{5}) = (1 + \sqrt{5})$$

$$(2, 1 + \sqrt{5})(3, 1 - \sqrt{5}) = (1 - \sqrt{5})$$

$$\begin{aligned} \Rightarrow (2) \cdot (3) &= (2, 1 + \sqrt{5})^2 (3, 1 + \sqrt{5})(3, 1 - \sqrt{5}) \\ &= (1 + \sqrt{5})(1 - \sqrt{5}) \quad \underline{\text{no issue}} \end{aligned}$$

This is the prime fact. !

27/4

Given I, J , can define $\gcd(I, J)$ & $\text{lcm}(I, J)$ in the obv. way,
and observe $\gcd(I, J) = I + J$, $\text{lcm}(I, J) = I \cap J$.

Cor. 3. $I \trianglelefteq R$, $0 \neq \alpha \in I \Rightarrow \exists \beta \in I$ s.t. $I = (\alpha, \beta)$.

Pf. Find $\beta \in R$ s.t. $I = \gcd((\alpha), (\beta))$.

If $I = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}$, $\mathfrak{p}_i$ distinct primes

$\Rightarrow (\alpha) = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r} \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_s^{m_s}$ & want

$$\beta \in \bigcap_{i=1}^r (\mathfrak{p}_i^{n_i} - \mathfrak{p}_i^{n_i+1}) \cap \bigcap_{j=1}^s (R - \mathfrak{q}_j).$$

Chinese Remainder Thm: fix $\beta_i \in \mathfrak{p}_i^{n_i} - \mathfrak{p}_i^{n_i+1}$ $i=1, \dots, r$

$$\Rightarrow \exists \beta \in R \text{ sat. } \begin{aligned} \beta &\equiv \beta_i \pmod{\mathfrak{p}_i^{n_i+1}} & i=1, \dots, r \\ \beta &\equiv 1 \pmod{\mathfrak{q}_j} & j=1, \dots, s \end{aligned}$$

□

Recall: PID $\Rightarrow$ UFD. The converse is generally false ($\mathbb{Z}[x]$),
but true for Dedekind domains!

Cor. 4. R Dedekind domain $\Rightarrow$ PID $\Leftrightarrow$ UFD.

Pf. I ideal, $0 \neq \alpha \in I \Rightarrow I | (\alpha)$ by Cor. 4.9

Write $\alpha = p_1^{r_1} \dots p_n^{r_n}$ prime decomp.

$\Rightarrow (\alpha) = (p_1)^{r_1} \dots (p_n)^{r_n}$ prime decomp.

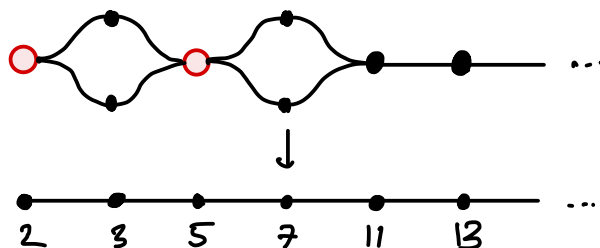
$\Rightarrow I = (p_1)^{s_1} \dots (p_n)^{s_n} = (p_1^{s_1} \dots p_n^{s_n})$ principal.
(unique fact.) $0 \leq s_i \leq r_i$

□

§ Splitting of primes in extensions. What happens to primes in L/K ?

$$\begin{array}{ccccccc}
 \mathbb{Z}[\sqrt{5}] \subseteq \mathcal{O}(\sqrt{5}) & (2) = (2, 1+\sqrt{5})^2 & (3) = (3, 1+\sqrt{5})(3, 1-\sqrt{5}) & \dots & (11) & \text{prime} \\
 | & | \text{"ramified"} & | \text{"split"} & & | & \text{"inert"} \\
 \mathbb{Z} \subseteq \mathbb{Q} & (2) & (3) & & (11) & \text{prime}
 \end{array}$$

$$\begin{array}{c}
 \text{Spec}(\mathbb{Z}[\sqrt{5}]) \\
 \downarrow \\
 \text{Spec}(\mathbb{Z})
 \end{array}$$



In general:

$$\begin{array}{c}
 L \supseteq \mathcal{O}_L \supseteq \mathfrak{P} \mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g} \quad \text{prime decomp. of } \mathfrak{P} \\
 | \qquad \qquad | \qquad \qquad | \\
 K \supseteq \mathcal{O}_K \supseteq \mathfrak{P}
 \end{array}$$

" $\mathfrak{P}_i$ lies above $\mathfrak{P}$ " / " $\mathfrak{P}$ lies below $\mathfrak{P}_i$ "
over under

Thm 5. TFAE:

- (1) $\mathfrak{P} \mid \mathfrak{P} \mathcal{O}_L$
- (2) $\mathfrak{P} \supseteq \mathfrak{P} \mathcal{O}_L$
- (3) $\mathfrak{P} \supseteq \mathfrak{P}$
- (4) $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P}$
- (5) $\mathfrak{P} \cap K = \mathfrak{P}$

Pf. (1) $\Leftrightarrow$ (2) by Cor. 4.10

(2) $\Leftrightarrow$ (3) b/c $\mathfrak{P}$ ideal

(3) $\Leftarrow$ (4) b/c $\mathfrak{P} \subseteq \mathcal{O}_L$

(4) $\Leftrightarrow$ (5) b/c $\mathfrak{P} \subseteq \mathcal{O}_L$

(3) $\Rightarrow$ (4). $\mathfrak{P} \cap \mathcal{O}_K \supseteq \mathfrak{P}$
maximal

& $1 \notin \mathfrak{P} \Rightarrow 1 \notin \mathfrak{P} \cap \mathcal{O}_K \Rightarrow \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P}$. $\square$

$\mathfrak{P}$ lies above $\mathfrak{P}$ etc.

Thm 6. Every prime $\mathfrak{P}$ of $\mathcal{O}_L$ lies above a unique prime of $\mathcal{O}_K$;
every prime $\mathfrak{P}$ of $\mathcal{O}_K$ lies under at least one prime of $\mathcal{O}_L$.

Pf. Claim 1. $\mathfrak{P} \cap \mathcal{O}_K$ is a prime

prime ideal $\checkmark$, $\neq \mathcal{O}_K$ b/c $1 \notin \mathfrak{P} \checkmark$,

$$\mathfrak{P} \cap \mathcal{O}_K \neq 0 \quad \text{b/c} \quad \mathcal{O}_K / \mathfrak{P} \cap \mathcal{O}_K \subseteq \underbrace{\mathcal{O}_L / \mathfrak{P}}_{\text{finite by Cor. 4.4}} \quad \checkmark$$

27/4

Claim 2. $\mathfrak{P} \mathcal{O}_L \neq \mathcal{O}_L$ i.e. $1 \notin \mathfrak{P} \mathcal{O}_L$

Lemma 4.7 $\Rightarrow \exists \gamma \in K \setminus \mathcal{O}_K$ s.t. $\gamma \mathfrak{P} \subseteq \mathcal{O}_K$

$$\Rightarrow \gamma \mathfrak{P} \mathcal{O}_L \subseteq \mathcal{O}_K \mathcal{O}_L = \mathcal{O}_L$$

& if $1 \in \mathfrak{P} \mathcal{O}_L$, then $\gamma \in \mathcal{O}_L$ $\hookrightarrow$

□

$$\begin{array}{ccc} L \supseteq \mathcal{O}_L \supseteq \mathfrak{P} \mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g} & \mathcal{O}_L / \mathfrak{P}_i & \\ | & | & \text{extension of finite fields} \\ K \supseteq \mathcal{O}_K \supseteq \mathfrak{P} & \mathcal{O}_K / \mathfrak{P} & \end{array}$$

Def 7. For $\mathfrak{P}$ above $\mathfrak{P}$, let:

$f(\mathfrak{P}/\mathfrak{P}) := [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{P}]$ inertial degree,

$e(\mathfrak{P}/\mathfrak{P}) :=$ exponent of $\mathfrak{P}$ in $\mathfrak{P} \mathcal{O}_L$ ramification index.

$$\text{Thm 8. } [L:K] = \sum_{i=1}^g f(\mathfrak{P}_i/\mathfrak{P}) \cdot e(\mathfrak{P}_i/\mathfrak{P}).$$

We will use norms of ideals to prove it...

Def 9. The absolute norm of $I \trianglelefteq \mathcal{O}_K$ is $\|I\| := \# \mathcal{O}_K/I$.

$$\text{Thm 10. (a) } \|I \cdot J\| = \|I\| \cdot \|J\|$$

$$(b) \|I \cdot \mathcal{O}_L\| = \|I\|^{[L:K]}, \quad L/K \text{ extension}$$

$$(c) \|(a)\| = |N_{K/\mathbb{Q}}(a)|, \quad a \in \mathcal{O}_K \setminus \{0\}$$

Examples.

(1) $\mathbb{Q}(\omega_{p^r})$?? Recall $\prod_{\substack{p \nmid k \\ 1 \leq k \leq p^r}} (1 - \omega^k) = p$ (Lemma 3.7)

$\mid$ $n = p^{r-1}(p-1)$ $\mid$

$\mathbb{Q}$ p & $(1 - \omega^k) = (1 - \omega) \underbrace{(1 + \omega + \dots + \omega^{k-1})}_{\in \mathbb{Z}[\omega]^\times \text{ unit! (Exercise)}}$

$$\Rightarrow (1 - \omega)^n = (p) \text{ as ideals of } \mathbb{Z}[\omega].$$

$$\Rightarrow (1 - \omega) \text{ must be prime by Thm 8!}$$

(2) $\mathbb{Q}(\alpha) \supseteq \mathbb{Z}[\alpha]$ $\alpha^3 = 2$ $(\alpha)^3$ $(\alpha+1)^3$
 $(5, \alpha+2) \cdot (5, \alpha^2+3\alpha-1)$
 $f=1 \quad \mid \quad f=2$
 (5)
 HW 3

$3 \mid$ $\mid$ $\mid$ $\mid$ (2) (3) (5) (2+1=3)

$\mathbb{Q} \supseteq \mathbb{Z}$

$$\begin{aligned}
 (\alpha+1)^3 &= 2 + 3\alpha^2 + 3\alpha + 1 \\
 &= 3(1 + \alpha + \alpha^2) \\
 &\quad \text{unit: } (\alpha-1)(1 + \alpha + \alpha^2) \\
 &= \alpha + \alpha^2 + 2 - 1 - \alpha - \alpha^2 = 1
 \end{aligned}$$

$$\mathbb{Q}(\alpha) \supseteq \mathbb{Z}[\alpha] \quad \alpha^3 = \alpha + 1$$

$$\mid$$

$$\mathbb{Q}$$

$$(23, \alpha-10)^2 \cdot (23, \alpha-3)$$

$$f=1 \quad \mid \quad f=1$$

$$(23)$$

HW 3

Demonstration (see eCampus for links):

- lmfdb.org
- galois-correspondence.org (by Sam Reiser).
- SageMath

Last time ...

$$\begin{array}{ccc}
 L \supseteq \mathcal{O}_L \supseteq \mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g} & \mathcal{O}_L/\mathfrak{p}_i & \\
 n \mid & \mid & \mid \\
 K \supseteq \mathcal{O}_K \supseteq \mathfrak{p} & \mathcal{O}_K/\mathfrak{p} & \text{extension of finite fields}
 \end{array}$$

Thm 8. $n = e_1 f_1 + \dots + e_g f_g.$

Thm 10. (a) $\|I \cdot J\| = \|I\| \cdot \|J\|$
 (b) $\|I \cdot \mathcal{O}_L\| = \|I\|^n$ for L/K degree n
 (c) $\|(\alpha)\| = |N_{K/\mathbb{Q}}(\alpha)|$, $\alpha \in \mathcal{O}_K \setminus \{0\}$

Def 9.

$$\|I\| := |\mathcal{O}_K/I|$$

Today: Prove Thms 8 & 10 simultaneously ... (You're in for a wild ride ...)

$$\text{Thm 10(a)} \Rightarrow \text{Thm 8 for } K/\mathbb{Q} \Rightarrow \text{Thm 10(b)} \Rightarrow \begin{cases} \text{Thm 8 for } L/K \\ \text{Thm 10(c)} \end{cases}$$

Pf of Thm 10(a). Enough to prove for I, J rel. prime & $I = \mathfrak{p}^n$.

- I, J relatively prime $\Rightarrow I \cdot J = I \cap J$ &
 $\Rightarrow \mathcal{O}_K/I \cap J \cong \mathcal{O}_K/I \times \mathcal{O}_K/J \Rightarrow \|I \cdot J\| = \|I\| \cdot \|J\|$
- $\|\mathfrak{p}^n\| = \|\mathfrak{p}\|^n$. Have
 $\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \dots \supseteq \mathfrak{p}^{n-1} \supseteq \mathfrak{p}^n$

and ... Exercise. $R/\mathfrak{p} \xrightarrow{\cong} \mathfrak{p}^k/\mathfrak{p}^{k+1}$

Pf of Thm 8 for $K/\mathbb{Q}$. $\mathfrak{p} = p\mathbb{Z}$

$$\begin{array}{c}
 p^n = \|p\mathcal{O}_K\| = \|\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}\| \underset{\text{Thm 10(a)}}{=} \|\mathfrak{p}_1\|^{e_1} \dots \|\mathfrak{p}_g\|^{e_g} = p^{f_1 e_1} \dots p^{f_g e_g} \\
 \uparrow \quad \quad \quad \uparrow \\
 \mathcal{O}_K/p\mathcal{O}_K \cong (\mathbb{Z}/p\mathbb{Z})^n
 \end{array}$$

□
16/1.

P of Thm 10(b). Enough to prove for $I = \mathfrak{p}$ prime, by (a).

Note: $\mathcal{O}_L / \mathfrak{p} \mathcal{O}_L = \mathcal{O}_K / \mathfrak{p}$ - vector space; ETS: dimension n .

$\dim \leq n$ $\alpha_1, \dots, \alpha_{n+1} \in \mathcal{O}_L$ are lin. dep. over $\mathcal{O}_K$ (HW 2, Exercise 1)

$$\Rightarrow \exists \beta_1, \dots, \beta_{n+1} \in \mathcal{O}_K \text{ s.t. } \beta_1 \alpha_1 + \dots + \beta_{n+1} \alpha_{n+1} = 0.$$

Can $\beta_i \equiv 0 \pmod{\mathfrak{p}} \forall i$? We need a gen. of Lemma 4.7 ...

Claim: $0 \neq B \subseteq A \subsetneq R$ ideals in Dedekind domain $\Rightarrow \exists \gamma \in K$ s.t. $\gamma B \subseteq R, \gamma B \not\subseteq A$.

Thm 4.5: $\exists C$ s.t. $BC = (\alpha) = \alpha R$

Then $BC \not\subseteq \alpha A \Rightarrow$ fix $\beta \in C$ s.t. $\beta B \not\subseteq \alpha A \Rightarrow \gamma = \beta/\alpha$ works. //
(cancellation law)

Claim with $A = \mathfrak{p}, B = (\beta_1, \dots, \beta_{n+1})$: if $B \subseteq A$, then use γ to get

$$0 = \underbrace{\gamma \beta_1}_{\in \mathcal{O}_K} \alpha_1 + \dots + \underbrace{\gamma \beta_{n+1}}_{\in \mathcal{O}_K} \alpha_{n+1} \quad \& \quad \gamma B \not\subseteq A.$$

$\Rightarrow$ WLOG $B \not\subseteq A \Rightarrow$ some $\beta_i \not\equiv 0 \pmod{\mathfrak{p}} \Rightarrow \dim \leq n$. //

$$\begin{array}{c} \text{dim} = n. \\ \begin{array}{c} L \\ n \mid \\ K \\ m \mid \\ \mathbb{Q} \end{array} \quad \begin{array}{c} \mathfrak{p} \mathcal{O}_L \\ \mid \\ \mathfrak{p} \\ \mid \\ \mathfrak{p} \mathbb{Z} \end{array} \mid \begin{array}{c} \mathcal{O}_L \\ \mid \\ \mathcal{O}_K \\ \mid \\ \mathbb{Q} \end{array} \end{array} \quad \begin{array}{l} \mathcal{O}_L = (\mathfrak{p}_1 \mathcal{O}_L)^{e_1} \dots (\mathfrak{p}_g \mathcal{O}_L)^{e_g} \\ \mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g} \end{array}$$

thm: $\dim_{\mathcal{O}_K/\mathfrak{p}_i} (\mathcal{O}_L / \mathfrak{p}_i \mathcal{O}_L) := n_i \leq n \quad \forall i$ (*)

Want: $n_i = n \quad \forall i$.

Thm 8 when $K = \mathbb{Q} \Rightarrow m = \sum e_i \cdot f_i$ (**)

$$p^{mn} = \|\mathfrak{p} \mathcal{O}_L\| = \prod_i \|\mathfrak{p}_i \mathcal{O}_L\|^{e_i} = \prod_i \|\mathfrak{p}_i\|^{n_i e_i} = \prod_i p^{f_i n_i e_i}$$

$$\Rightarrow mn = \sum f_i n_i e_i \stackrel{(*)}{\leq} \sum e_i f_i \cdot n \stackrel{(**)}{=} mn$$

$$\Rightarrow \text{holds} \Rightarrow n_i = n \quad \forall i.$$



Pf of Thm 8.

$$\|\beta\|^{[L:K]} \stackrel{(b)}{=} \|\beta \mathcal{O}_L\| = \|\beta_1^{e_1} \dots \beta_g^{e_g}\| \stackrel{(a)}{=} \prod_{i=1}^g \|\beta_i\|^{f_i e_i}$$

□

Pf of Thm 10(c).

$$\begin{array}{c} n \\ \mid \\ k \\ \mid \\ \mathbb{Q} \end{array} \xrightarrow{M} M \text{ normal closure} \Rightarrow \begin{array}{l} \bullet N(\alpha) = \prod_{\sigma} \sigma(\alpha) \\ \bullet \forall \sigma: k \hookrightarrow M \quad \|\sigma(\alpha) \mathcal{O}_M\| = \|\mathcal{O}_M\| \end{array}$$

$$\|N(\alpha) \mathcal{O}_M\| \stackrel{(b)}{=} \left\| \prod_{\sigma} \sigma(\alpha) \mathcal{O}_M \right\| = \prod_{\sigma} \|\sigma(\alpha) \mathcal{O}_M\| = \|\alpha \mathcal{O}_M\|^n \stackrel{(b)}{=} \|\alpha \mathcal{O}_k\|^{n \cdot n}$$

$N(\alpha)^{n \cdot n}$

□

Summary.

$$\begin{array}{c} L \\ \mid \\ n \\ \mid \\ k \end{array} \quad \begin{array}{c} \beta_1 \dots \beta_g \\ \downarrow \uparrow \\ f_1 \dots f_g \\ \beta \end{array} \quad \begin{array}{c} \beta_i^{e_i} \parallel \beta \mathcal{O}_L \\ f_i := [\mathcal{O}_L/\beta_i : \mathcal{O}_k/\beta] \end{array} \quad e_1 f_1 + \dots + e_g f_g = n$$

Example. $n = 2$: $1+1=2$, $1 \cdot 2 = 2$, $2 \cdot 1 = 2$

$$\begin{array}{c} L \\ \mid \\ k \end{array} \quad \begin{array}{c} \beta_1 \quad \beta_2 \\ \searrow \swarrow \\ \beta \end{array} \quad \beta \mathcal{O}_L = \beta_1 \cdot \beta_2 \quad \begin{array}{c} \beta \\ e=1 \mid f=2 \\ \beta \end{array} \quad \beta \mathcal{O}_L = \beta^2 \quad \begin{array}{c} \beta \\ e=2 \mid f=1 \\ \beta \end{array} \quad \beta \mathcal{O}_L = \beta^2$$

split inert ramified

HW 3 : $n=3$.

Suppose L/K Galois. Then for $\mathfrak{p}$ prime of K :

$$G := \text{Gal}(L/K) \subseteq \{ \text{primes of } L \text{ above } \mathfrak{p} \}$$

Check for $\mathfrak{P} / \mathfrak{p}$, $\sigma \in G$: $\sigma(\mathfrak{P})$ prime of L above $\mathfrak{p}$:

$$\sigma(\mathfrak{P}) \triangleq \sigma(\mathcal{O}_L) = \mathcal{O}_L \quad \& \quad \mathcal{O}_L / \sigma(\mathfrak{P}) \cong \mathcal{O}_L / \mathfrak{P} \Rightarrow \text{prime of } L,$$

$$\& \quad \sigma(\mathfrak{P}) \cap \mathcal{O}_K = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma(\mathfrak{p}) = \mathfrak{p}. \quad \Rightarrow \text{above } \mathfrak{p}.$$

Thm 1. This action is transitive.

Pf. Else: $\exists \mathfrak{P}, \mathfrak{P}' / \mathfrak{p}$ s.t. $\sigma(\mathfrak{P}) \neq \mathfrak{P}' \quad \forall \sigma \in G$.

Chinese remainder thm:

$$\exists \alpha \in \mathcal{O}_L \text{ s.t. } \begin{cases} (1) & \alpha \equiv 0 \pmod{\mathfrak{P}'} \\ (2) & \alpha \equiv 1 \pmod{\sigma(\mathfrak{P})} \quad \forall \sigma \in G \end{cases}$$

$$\Rightarrow N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma^{-1}(\alpha) \quad \left\{ \begin{array}{l} \in \mathcal{O}_K \cap \underbrace{\mathfrak{P}'}_{\sigma=id} = \mathfrak{P} \quad \text{by (1)} \\ \notin \mathcal{O}_K \cap \mathfrak{P} = \mathfrak{P} \quad \text{by (2)} \end{array} \right. \quad \begin{array}{l} \searrow \\ \square \end{array}$$

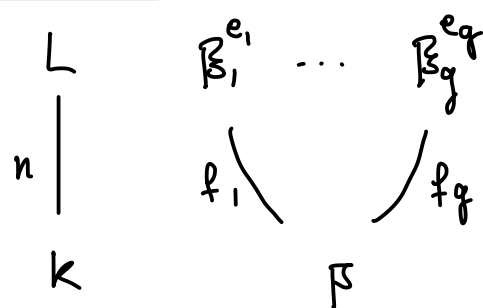
Cor 2. L/K Galois, $\mathfrak{P}, \mathfrak{P}' / \mathfrak{p} \Rightarrow e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{p}), f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{p})$.

In particular, $\mathfrak{p} \mathcal{O}_L = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e$ with inertial deg. f s.t. $n = pef$.

LECTURE 7.

4/5

Last time.



Default: get n primes.

Two ways a prime can

get fact: e_i or f_i & $e_i > 1$ is rare. (Thm 5.8)

$$f_i := [\mathcal{O}_L/\beta_i : \mathcal{O}_K/\beta] \rightsquigarrow e_1 f_1 + \dots + e_g f_g = n$$

(Thm 6.1)

& L/K Galois $\Rightarrow \text{Gal}(L/K) \subseteq \{\beta_1, \dots, \beta_g\}$ trans.

(Cor. 6.2)

$$\Rightarrow e_1 = \dots = e_g = e, f_1 = \dots = f_g = f; e \cdot f \cdot g = n$$

Exercise.

(TOWER LAW)



$\Rightarrow$

$$e(\beta/\mathfrak{q}) \cdot e(\mathfrak{q}/\beta) = e(\beta/\beta)$$

$$f(\beta/\mathfrak{q}) \cdot f(\mathfrak{q}/\beta) = f(\mathfrak{q}/\beta)$$

Def 1. β ramified in L if $e(\beta/\beta) > 1$ for some β/β .

Examples. • p ramified in $\mathbb{Q}(\omega_p)/\mathbb{Q}$

$$\text{disc}(\mathbb{Q}(\omega_p)) = p^?$$

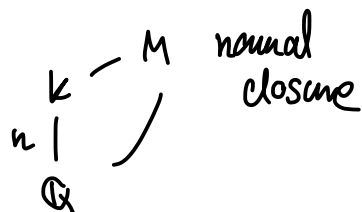
• $2, 3$ ramified in $\mathbb{Q}(\sqrt[3]{2})$

$$\text{disc}(\mathbb{Q}(\sqrt[3]{2})) = -2^2 \cdot 3^3$$

Thm 2. $p \in \mathbb{Z}$ ramified in $K \Rightarrow p \mid \text{disc}(K)$.

Converse also true & proved soon!

Pf. Recall def. of $\text{disc}(K)$:



$$\sigma_1, \dots, \sigma_n : K \hookrightarrow M$$

$$\alpha_1, \dots, \alpha_n \text{ } \mathbb{Z}\text{-basis of } \mathcal{O}_K$$

$$\Rightarrow \text{disc}(K) = \det(\sigma_i(\alpha_j))^2$$

$$\text{Suppose: } p \mathcal{O}_K = \beta_1^{e_1} \dots \beta_g^{e_g} = \beta_1 \cdot \underbrace{\beta_1^{e_1-1} \beta_2^{e_2} \dots \beta_g^{e_g}}_I \quad e_1 \geq 1$$

I

L7/1.

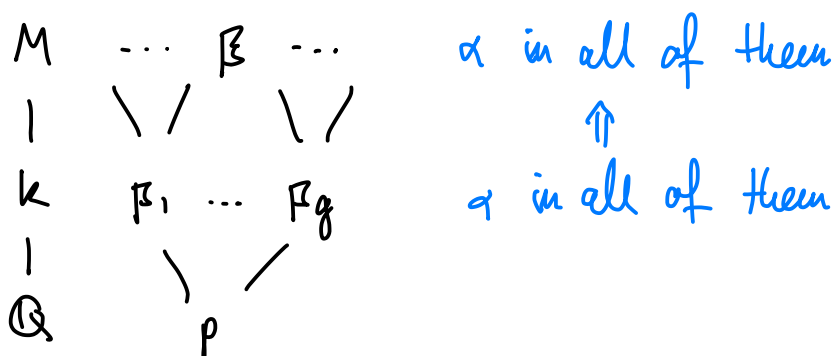
Take $\alpha \in I \setminus p\mathcal{O}_K$; then $\forall i, \alpha \in \mathfrak{p}_i$ and

$$\alpha = m_1 \alpha_1 + \dots + m_n \alpha_n \quad m_i \in \mathbb{Z}, \text{ not all div. by } p.$$

$\Rightarrow$ assume $p \nmid m_1$ & note:

$$\text{disc}(\alpha, \alpha_2, \dots, \alpha_n) = \underbrace{m_1^2}_{\text{not div. by } p} \cdot \text{disc}(K).$$

$\Rightarrow$ enough to show $p \mid \text{disc}(\alpha, \alpha_2, \dots, \alpha_n)$



Thm 6.1 $\Rightarrow \sigma(\alpha) \in \mathfrak{p} \quad \forall \sigma \in \text{Gal}(M/\mathbb{Q})$

$\Rightarrow \sigma_i(\alpha) \in \mathfrak{p} \quad \forall i$

$\Rightarrow \text{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}.$



Cor. 3. Say $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$ & $f =$ monic poly in $\mathbb{Z}[x]$ with $f(\alpha) = 0$
 $p \nmid N_{K/\mathbb{Q}} f'(\alpha) \Rightarrow p$ is unramified in K .

Pf. Combine Thm 2 with Thm 2.11 (2). $\square$

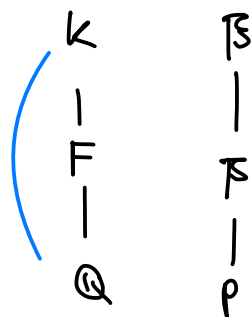
Cor. 4. Only finitely many primes of $\mathbb{Z}$ are ram. in K .

E.g. only $p \mid 4m$ can be ram. in $\mathbb{Q}(\sqrt{m})$.

Cor. 5. Only fin. many primes are ram. in K/F .

Pf.

fin.
many
ram.



Tower law:

$$\underbrace{e(\mathbb{P}/p)}_{>1} = \underbrace{e(\mathbb{P}/\mathfrak{P})}_{\leq} \cdot \underbrace{e(\mathfrak{P}/p)}_{>1}$$

HW 4: relative version
of Thm 2 using the
"different ideal".



Next: examples!

Thm 6. $m = \square$ -free, p prime, $K = \mathbb{Q}(\sqrt{m})$

$$(1) p | m \Rightarrow p \mathcal{O}_K = (p, \sqrt{m})^2 \quad (\text{ramified})$$

$$(2) p=2 \Rightarrow 2 \mathcal{O}_K = \begin{cases} (2, 1+\sqrt{m})^2 & m \equiv 3 \pmod{4} \quad (\text{ramified}) \\ (2, \frac{1+\sqrt{m}}{2})(2, \frac{1-\sqrt{m}}{2}) & m \equiv 1 \pmod{8} \quad (\text{split}) \\ \text{prime} & m \equiv 5 \pmod{8} \quad (\text{inert}) \end{cases}$$

$$(3) p \nmid 4m \Rightarrow p \mathcal{O}_K = \begin{cases} (p, n+\sqrt{m})(p, n-\sqrt{m}) & m \equiv n^2 \pmod{p} \quad \left(\frac{m}{p}\right) = 1 \\ \text{prime} & m \not\equiv \square \pmod{p} \quad \left(\frac{m}{p}\right) = -1 \end{cases}$$

Pf. Split/Ram. cases. E.g. for (1), calculate:

$$(p, \sqrt{m})^2 = (p^2, p\sqrt{m}, m) \subseteq p \mathcal{O}_K \text{ b/c } p|m \text{ \& contains } \gcd(p^2, m) = p$$

(Note: $(p, \sqrt{m})$ must then be prime by Thm 5.8.)

Other cases: similar calculations. Exercise. Do them! (HW 4)

Inert cases: Want: $\mathbb{P}/p \Rightarrow \mathcal{O}_K/\mathfrak{P} \not\cong \mathbb{F}_p$ i.e. $f \neq 1$
($\Rightarrow$ OK by Thm 5.8.)

(3) $m \not\equiv \square \pmod{p} \Rightarrow x^2 - m$ irreducible over F_p

but $x = \sqrt{m} \in \mathbb{Q}_K$ root $\Rightarrow \sqrt{m} \pmod{p}$ root in $\mathbb{Q}_K/p$
 $\Rightarrow \mathbb{Q}_K/p \neq F_p$.

(HW 4)

Exercise. For $p=2$, $m \equiv 5 \pmod{8}$, use $x^2 - x + \frac{1-m}{4}$ to finish (2). □

Rule. Quadratic residues $\left(\frac{p}{m}\right)$ related to splitting of p in $\mathbb{Q}(\sqrt{m})$.

Soon ... quadratic reciprocity using $\mathbb{Q}(\omega_q) \supseteq \mathbb{Q}(\sqrt{\pm q}) \supseteq \mathbb{Q}$, q prime.

Recall: $\mathbb{Q}(\omega_m)/\mathbb{Q}$ Galois $\Rightarrow p\mathbb{Z}[\omega_m] = (\mathfrak{p}_1 \dots \mathfrak{p}_g)^e$, $efg = \varphi(m)$.
 degree $\varphi(m)$

Thm 7. $m = p^k n$, $p \nmid n$

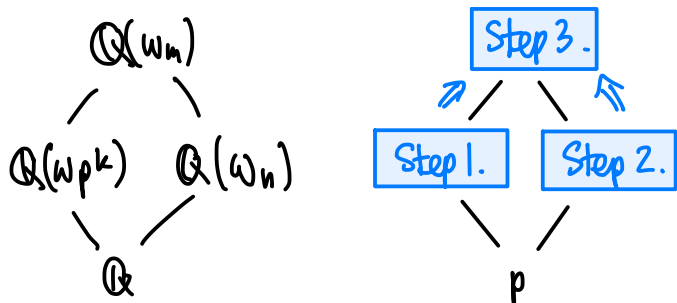
- $e = \varphi(p^k) = p^{k-1}(p-1)$
- $f = \text{order of } p \pmod{n}$, i.e. in $(\mathbb{Z}/n\mathbb{Z})^\times$

• Interesting.

• Useful, e.g. quadratic rec.

• Proof: illustrative of general phenomena.

Pf.



Step 1: Splitting of p in $\mathbb{Q}(\omega_{p^k})$ (if $k \geq 1$).

We saw this example in lecture 5:

$$p = u(1 - \omega_{p^k})^{\varphi(p^k)} \Rightarrow (p) = (1 - \omega_{p^k})^{\varphi(p^k)}$$

$$\Rightarrow \text{Thm 5.8 } e = \varphi(p^k), f = g = 1. \quad //$$

Step 2: Splitting of p in $\mathbb{Q}(\beta) = \mathbb{Q}(\omega_n)$, $p \nmid n$.

4/5

$\text{disc}(\mathbb{Q}(\omega_n)) \mid n^{\ell(n)}$ & $p \nmid n \Rightarrow p$ unram. by Thm 2 ($e=1$)

$$\Rightarrow p\mathbb{Z}[\omega_n] = \mathfrak{p}_1 \cdots \mathfrak{p}_g \quad \& \quad f \cdot g = \varphi(n).$$

Claim. f = order of $p \in (\mathbb{Z}/n\mathbb{Z})^\times =: d$

Recall: $\text{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$$(\omega_n \mapsto \omega_n^a) \longleftarrow a$$

Take $p \in (\mathbb{Z}/n\mathbb{Z})^\times$ & consider σ_p (which has order d).

$\leadsto$ We'll show $\sigma := \sigma_p$ has order f .

What is f ?

$\forall \beta = \beta_i/p, \mathbb{F}_\beta := \mathbb{Z}[\omega_n]/\beta$ degree f ext. of $\mathbb{F}_p$.

Recall: $\text{Gal}(\mathbb{F}_\beta/\mathbb{F}_p) \cong \mathbb{Z}/f\mathbb{Z}$ "Frobenius"

$$x \mapsto x^p \longleftarrow \tau$$

Want: order of σ = order of τ ; in fact $\forall a \in \mathbb{Z} \quad \sigma^a = 1 \Leftrightarrow \tau^a = 1$.

Clearly: $\sigma^a = 1 \Leftrightarrow \sigma^a(\omega_n) = \omega_n \Leftrightarrow \omega_n^{p^a} = \omega_n \Leftrightarrow p^a \equiv 1 \pmod{n}$

OTOH: $\tau^a = 1 \Leftrightarrow \tau^a(\omega_n) \equiv 1 \pmod{\mathfrak{p}} \Leftrightarrow \omega_n^{p^a} \equiv \omega_n \pmod{\mathfrak{p}}$

Thus need $p^a \equiv 1 \pmod{n} \Leftrightarrow \omega_n^{p^a} \equiv \omega_n \pmod{\mathfrak{p}}$.

$\Rightarrow$ clear even without mod p .

$\Leftarrow$ Write $p^a \equiv b \pmod{n}$, $1 \leq b \leq n$.

$$\text{Then } \omega_n^{p^a} = \omega_n^b \Rightarrow \omega_n^b \equiv \omega_n \pmod{\mathfrak{p}}$$

$$\Rightarrow \omega_n^{b-1} \equiv 1 \pmod{\mathfrak{p}} \quad (\omega_n \in \mathbb{Z}[\omega_n]^\times)$$

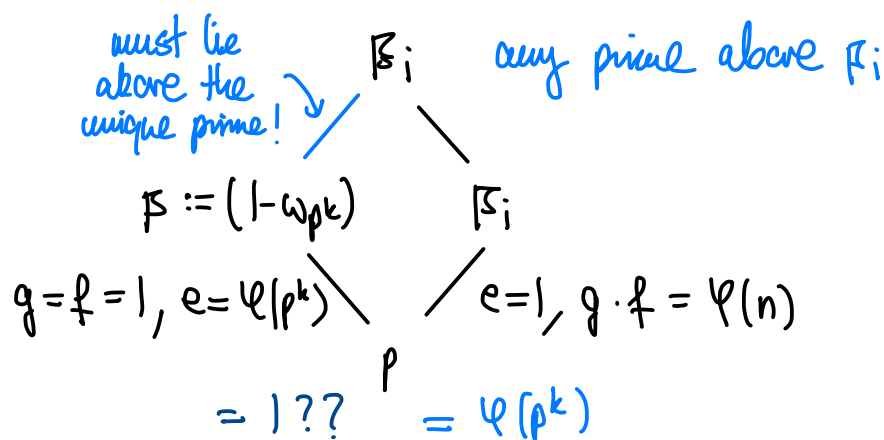
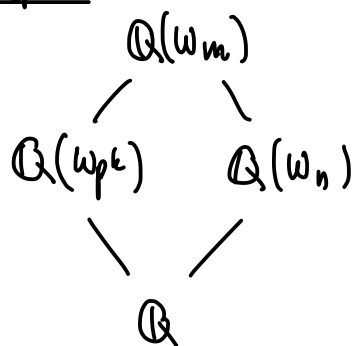
$$\text{Finally: } (1 - \omega_n)(1 - \omega_n^2) \cdots (1 - \omega_n^{n-1}) = n$$

so $b > 1$ implies $n \in \mathfrak{p}$ but then $n \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z} //$

5/17

Step 3.

4/5



Now: $e(K_i/p) = e(K_i/K) \cdot e(K/p) \geq v(p^k)$

$f(K_i/p) = f(K_i/K) \cdot f(K/p) \geq f$

$= 1?? \quad = f$

Finally: $v(p^k) \cdot v(n) = v(m) = \sum_i e(K_i/p) \cdot f(K_i/p)$

$\geq v(p^k) \cdot f \cdot g = v(p^k) \cdot v(n)$

$\Rightarrow$ equality holds & $= 1$ hold. □

- Key ideas:
- Split $K/\mathbb{Q}$ into unramified & ramified parts.
 - Study unram. part using $\text{Gal}(\mathbb{F}_K/\mathbb{F}_p)$.

More on this next!

Last time:

- p ram. in $K \Rightarrow p \mid \text{disc}(K)$ (Thm 7.2)
- Splitting of primes in $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\omega_m)$. (Thm 7.6, Thm 7.7)

§ Galois theory applied to prime decomposition.

Suppose K/F Galois, $G := \text{Gal}(K/F)$

$$\begin{array}{c} K \\ G \mid n \\ F \end{array} \quad \begin{array}{c} \mathbb{P}_1^{e_1} \dots \mathbb{P}_g^{e_g} \\ f_1 \mid f \\ F \end{array} \quad \begin{array}{l} \text{Thm 6.1. } G \curvearrowright \{\mathbb{P}_1, \dots, \mathbb{P}_g\} \text{ transitively} \\ \Rightarrow \text{Cor. 6.2. } e_1 = e, f_i = f \text{ \& } n = e f g. \\ \text{Stabilizers of } \mathbb{P}_i? \end{array}$$

Def. 1. Decomposition group. $G_{\mathbb{P}} := \{\sigma \in G \mid \sigma \mathbb{P} = \mathbb{P}\}$
 $= \text{Stab}_G(\mathbb{P})$

Immediate: $|G_{\mathbb{P}}| = e f$ (Orbit-stab. theorem: $n = |G_{\mathbb{P}}| \cdot g$)

The action $G \curvearrowright \mathcal{O}_K$ induces $G_{\mathbb{P}} \curvearrowright \mathcal{O}_K/\mathbb{P}$, fixing $\mathcal{O}_F/\mathbb{P}$.

Writing $\mathbb{F}_{\mathbb{P}} := \mathcal{O}_K/\mathbb{P}$, $\mathbb{F}_{\mathbb{P}} := \mathcal{O}_F/\mathbb{P} \hookrightarrow G_{\mathbb{P}} \longrightarrow \text{Gal}(\mathbb{F}_{\mathbb{P}}/\mathbb{F}_{\mathbb{P}})$.
 $\cong \mathbb{Z}/e\mathbb{Z}$ ($x \mapsto x^{||F||}$ generator)
 (Soon: surjective!)

Def 2. Inertia subgroup: $I_{\mathbb{P}} := \ker(G_{\mathbb{P}} \longrightarrow \text{Gal}(\mathbb{F}_{\mathbb{P}}/\mathbb{F}_{\mathbb{P}}))$
 $= \{\sigma \in G_{\mathbb{P}} \mid \sigma(\alpha) \equiv \alpha \pmod{\mathbb{P}} \forall \alpha \in \mathcal{O}_K\}$

(Surjectivity $\Leftrightarrow |I_{\mathbb{P}}| = e$!)

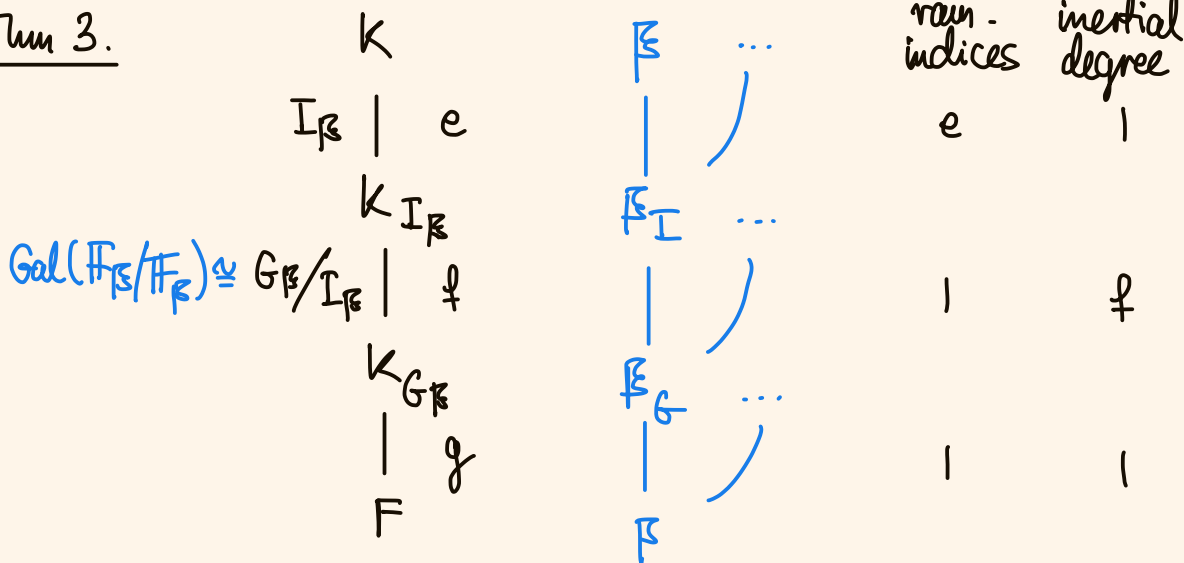
Fundamental Thm of Galois Theory:

$$\left\{ \begin{array}{l} H \leq \text{Gal}(K/F) \\ \text{subgroups} \end{array} \right\} \xleftrightarrow{(1-1)} \left\{ \begin{array}{l} F \subseteq M \subseteq K \\ \text{intermediate fields} \end{array} \right\}$$

$$H \longmapsto K_H := \{x \in K \mid \sigma x = x \ \forall \sigma \in H\}$$

$$\text{Gal}(K/M) \longleftrightarrow M$$

Thm 3.



Examples.

① $K = \mathbb{Q}(\omega_{23})$, ($p=2$ unram. b/c $2 \nmid 23$)

$$\mathbb{Q}(\omega_{23}) = K_{I_{\mathbb{F}}}$$

$$\mid 11$$

$$\mathbb{Q}(\sqrt{-23}) = K_{G_{\mathbb{F}}}$$

$$\mid 2$$

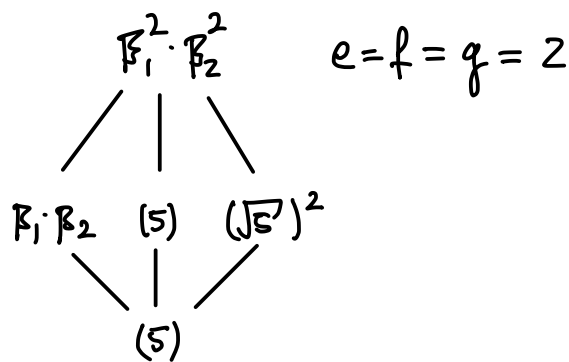
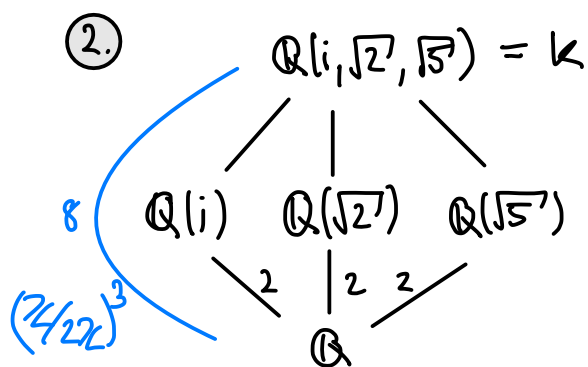
$$\mathbb{Q}$$

$\mathbb{F}_1$	$\mathbb{F}_2$
$\parallel \mid$	$\mid \parallel$
$(2, \frac{1+\sqrt{-23}}{2})$	$(2, \frac{1+\sqrt{-23}}{2})$
$\backslash \quad /$	
2	

Exercise.

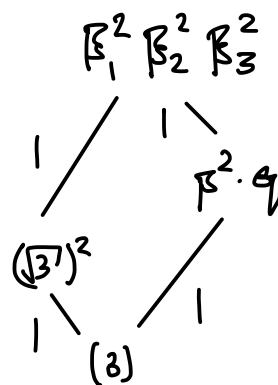
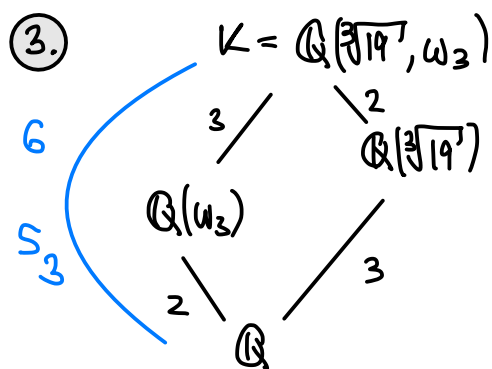
- Check this splitting.
- Deduce 2 irred. in $\mathbb{Z}[\omega_{23}]$.

Together with HW 1, Exercise 2, this finally shows $\mathbb{Z}[\omega_{23}]$ is not a UFD!



Thus... $K_{I(\mathbb{F}_i)} = \mathbb{Q}(i, \sqrt{2})$ (deg. 4 ext. in which (5) remains unram.)

$K_{G(\mathbb{F}_i)} =$ field with $e=f=1, g=2 : \mathbb{Q}(i) \& \mathbb{Q}(\sqrt{2}i)$



b/c: $e \geq 2, g \geq 2$
 $e \cdot f \cdot g = 6$

for some $\mathbb{F}_i, q$

Exercise:
check this!

Thus... $G_{\mathbb{F}_i}$ are fields of degree 3/ $\mathbb{Q}$ i.e. :

$\mathbb{Q}(\sqrt[3]{19}), \mathbb{Q}(\omega_3 \sqrt[3]{19}), \mathbb{Q}(\omega_3^2 \sqrt[3]{19})$.

and $G_{\mathbb{F}_i} = I_{\mathbb{F}_i}$ b/c $f=1$.

$\text{Gal}(K/\mathbb{Q})$ permutes them!

Def. 4. $\mathbb{P}$ prime of F , K/F degree n

- splits completely if $g=n$ ($e_i=f_i=1$)
- inert if $\mathbb{P} \cap K$ is prime, i.e. $g=e=1, f=n$
- totally ramified if $e=n$ ($g=f=1$)

Pf of Thm 3.

Recall: $|G_{\mathbb{P}}| = ef$, so $|G/G_{\mathbb{P}}| = g$, so $[K_{G_{\mathbb{P}}} : K] \stackrel{(*)}{=} g$.

Claim 1. $e(\mathbb{P}_G/\mathbb{P}) = f(\mathbb{P}_G/\mathbb{P}) = 1$.

Note: $\mathbb{P}$ = unique prime of $\mathcal{O}_K$ above $\mathbb{P}_G$

b/c $\text{Gal}(K/K_{G_{\mathbb{P}}}) \cong G_{\mathbb{P}}$ acts transitively & fixes $\mathbb{P}$.

$$\begin{aligned} \Rightarrow [K : K_{G_{\mathbb{P}}}] &= \underbrace{e(\mathbb{P}/\mathbb{P}_G)}_{\leq e} \cdot \underbrace{f(\mathbb{P}/\mathbb{P}_G)}_{\leq f} \\ \text{Thm 5.8} \quad \parallel \quad (*) & \\ n/g &= e \cdot f \end{aligned}$$

$$\Rightarrow e = e(\mathbb{P}/\mathbb{P}_G), f = f(\mathbb{P}/\mathbb{P}_G)$$

$$\Rightarrow 1 = e(\mathbb{P}_G/\mathbb{P}), 1 = f(\mathbb{P}_G/\mathbb{P}) \text{ by tower law //}$$

Claim 2. $f(\mathbb{P}/\mathbb{P}_I) = 1$, i.e. $\mathbb{F}_{\mathbb{P}} = \mathbb{F}_{\mathbb{P}_I}$.

$\bar{\alpha} \in \mathbb{F}_{\mathbb{P}} = \mathcal{O}_K/\mathbb{P}$ reduction of $\alpha \in \mathcal{O}_K$

$$\Rightarrow \alpha \in \mathcal{O}_K \text{ has min. poly over } \mathcal{O}_{K_{\mathbb{P}}} : f(x) = \prod_{\sigma \in I_{\mathbb{P}}} (x - \sigma(\alpha)) \in \mathcal{O}_{K_{\mathbb{P}}}[x]$$

$$\Rightarrow \overline{f(x)} = \prod_{\sigma \in I_{\mathbb{P}}} (x - \bar{\alpha}) \pmod{\mathbb{P}} \quad (\sigma(\alpha) \equiv \alpha \pmod{\mathbb{P}})$$

$$\Rightarrow \bar{\alpha} \in \mathbb{F}_{\mathbb{P}_I} \text{ b/c } \overline{f(x)} \in \mathbb{F}_{\mathbb{P}_I}[x] \quad (\bar{\alpha} \text{ fixed by all } \text{elts of } \text{Gal}(\mathbb{F}_{\mathbb{P}}/\mathbb{F}_{\mathbb{P}_I})) //$$

Have: $f(\mathbb{P}/\mathbb{P}_I) = 1$, $f(\mathbb{P}_I/\mathbb{P}_G) = f(\mathbb{P}/\mathbb{P}) = 1$.

$$\Rightarrow [K_{\mathbb{P}} : K_{G_{\mathbb{P}}}] \geq f \text{ but } G_{\mathbb{P}}/I_{\mathbb{P}} \hookrightarrow \text{Gal}(\mathbb{F}_{\mathbb{P}}/\mathbb{F}_{\mathbb{P}}) \cong \mathbb{Z}/f\mathbb{Z}$$

$$\Rightarrow [K_{\mathbb{P}} : K_{G_{\mathbb{P}}}] = f$$

$$\Rightarrow e(\mathbb{P}_I/\mathbb{P}_G) = 1 \text{ \& all follows.}$$

Cor. 5. $1 \longrightarrow I_{\mathbb{B}/\mathbb{F}} \longrightarrow G_{\mathbb{B}/\mathbb{F}} \longrightarrow \text{Gal}(\mathbb{F}_{\mathbb{B}}/\mathbb{F}_{\mathbb{F}}) \longrightarrow 1$
 $\sigma \longmapsto \bar{\sigma} \quad \text{is} \quad \mathbb{Z}/f\mathbb{Z}$

Cor. 6.

$$\begin{array}{c}
 K \\
 I_{\mathbb{B}} \mid e \\
 K_{I_{\mathbb{B}}} \\
 \text{Gal}(\mathbb{F}_{\mathbb{B}}/\mathbb{F}_{\mathbb{F}}) \cong G_{\mathbb{B}/I_{\mathbb{B}}} \mid f \\
 K_{G_{\mathbb{B}}} \\
 \mid g \\
 F
 \end{array}
 \left. \begin{array}{l}
 \text{Galois} \Rightarrow \\
 I_{\mathbb{B}} \trianglelefteq G \\
 \\
 \text{Galois} \Rightarrow \\
 (G_{\mathbb{B}} \trianglelefteq G)
 \end{array} \right\} \text{Galois}$$

$$\begin{array}{c}
 \mathbb{B}_1^e \dots \mathbb{B}_g^e \text{ totally ramified} \\
 \mid \quad \quad \mid \\
 \mathbb{B}_1 \dots \mathbb{B}_g \text{ inert} \\
 \mid f \quad \quad \mid f \\
 \mathbb{B}_1 \dots \mathbb{B}_g \text{ splits completely} \\
 \searrow \quad \swarrow \\
 \mathbb{B} \quad e=f=1
 \end{array}$$

E.g. this always holds if K/F abelian!

But this failed in Example (3) above.

Consider an intermediate field $F \subseteq M \subseteq K$:

$$\begin{array}{c}
 K \\
 \swarrow e' \quad \searrow \\
 e \mid \quad M_{I_{\mathbb{B}}} = K_{I_{\mathbb{B}}} M \\
 \mid K_{I_{\mathbb{B}}} \quad \mid f' \\
 f \mid \quad M_{G_{\mathbb{B}}} = K_{G_{\mathbb{B}}} M \\
 \mid K_{G_{\mathbb{B}}} \quad \mid g' \\
 g \mid \quad M \\
 F
 \end{array}$$

$$\begin{array}{c}
 \mathbb{B} \\
 \swarrow \quad \searrow \\
 \mid \quad \mathfrak{q}_{I_{\mathbb{B}}} \\
 \mid \mathbb{B}_{I_{\mathbb{B}}} \quad \mid \\
 \mid \mathbb{B}_{G_{\mathbb{B}}} \quad \mid \mathfrak{q}_G \\
 \mid \quad \mid \\
 \mid \quad \mathfrak{q} := \mathbb{B} \cap M \\
 \mathbb{B}
 \end{array}$$

We can use this to characterize $K_{G_{\mathbb{P}}}$ & $K_{I_{\mathbb{P}}}$ intrinsically!

Thm 7.

- (1) $K_{G_{\mathbb{P}}} =$ largest intermediate M s.t. $e(q/\mathbb{P}) = f(q/\mathbb{P}) = 1$
- (2) $K_{G_{\mathbb{P}}} =$ smallest intermediate M s.t. $\mathbb{P} =$ only prime of K above q
- (3) $K_{I_{\mathbb{P}}} =$ largest _____ s.t. $e(q/\mathbb{P}) = 1$
- (4) $K_{I_{\mathbb{P}}} =$ smallest _____ s.t. $\mathbb{P} =$ tot. ram. over $\mathbb{P}'$
(i.e. $e(\mathbb{P}/\mathbb{P}') = [L:M]$).

Pf. We checked in Thm 3 that $K_{G_{\mathbb{P}}}$ & $K_{I_{\mathbb{P}}}$ satisfy these properties.

Thus to prove the result, e.g.

$$\begin{aligned} (1) \quad M \text{ s.t. } e(q/\mathbb{P}) = f(q/\mathbb{P}) = 1 &\stackrel{\text{Tower Law}}{\Rightarrow} e = e', f = f' \\ &\Rightarrow [K : K_{G_{\mathbb{P}}}] = [K : M_{G_{\mathbb{P}}}] = e \cdot f \\ &\Rightarrow M_{G_{\mathbb{P}}} = M K_{G_{\mathbb{P}}} \supseteq K_{G_{\mathbb{P}}} \text{ must be } = \\ &\Rightarrow M \subseteq K_{G_{\mathbb{P}}} \quad // \end{aligned}$$

Exercise: prove (2), (3), (4) similarly. □

Cor. 8. $G_{\mathbb{P}/\mathbb{P}} \trianglelefteq G \Rightarrow \mathbb{P}$ splits comp. in $M \Leftrightarrow M \subseteq K_{G_{\mathbb{P}/\mathbb{P}}}$.

Next: use this to prove quadratic reciprocity.

Last time.

- K/F Galois with Galois group G , $G \curvearrowright \{\mathbb{P} \text{ above } \mathbb{P}\}$ transitively
- $\mathbb{P}$ above $\mathbb{P} \rightsquigarrow G_{\mathbb{P}} := \{\sigma \in G : \sigma \mathbb{P} = \mathbb{P}\}$ decomposition group

$$1 \longrightarrow I_{\mathbb{P}} \longrightarrow G_{\mathbb{P}} \twoheadrightarrow \text{Gal}(\mathbb{F}_{\mathbb{P}}/\mathbb{F}_{\mathbb{P}}) \longrightarrow 1$$

inertia subgroup

$\cong \mathbb{Z}/f\mathbb{Z}$

$x \mapsto x^{|\mathbb{P}|}$

$\mathbb{P}$	K	
	e	
$\mathbb{P}_I$	$K_{I_{\mathbb{P}}}$	Thm 8.7.
	f	= largest s.t. $e = 1$
$\mathbb{P}_G$	$K_{G_{\mathbb{P}}}$	inertia field
	g	= largest s.t. $e = f = 1$
$\mathbb{P}$	F	decomposition field

If also Galois, largest s.t. $\mathbb{P}$ unramified.

If Galois, largest s.t. $\mathbb{P}$ splits completely.

Simplest case: suppose $\text{Gal}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$ cyclic.

$$\mathbb{Z}/n\mathbb{Z} \left(\begin{array}{c} K \\ \frac{n}{d} \mid \mathbb{Z}/\frac{n}{d}\mathbb{Z} \\ K_d := K_{\mathbb{Z}/\frac{n}{d}\mathbb{Z}} \\ d \mid d \mid n \\ F \end{array} \right)$$

For $\mathbb{P}/\mathbb{P}$, have $n = e \cdot f \cdot g$ and:

- $K_{G_{\mathbb{P}}} = K_g$
- $K_{I_{\mathbb{P}}} = K_{fg}$

Example: $K = \mathbb{Q}(\omega_p)$ has $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$

p odd $\Rightarrow 2 \mid p-1 \Rightarrow K$ has a unique quadratic subfield K_2

Claim. $K_2 = \mathbb{Q}(\sqrt{\pm p'})$ where $\pm = +$ iff $p \equiv 1 \pmod{4}$.

Pf. Recall: $\text{disc}(\omega_p) = \pm p^{p-2}$ (Lecture 2)

$$\text{and } \text{disc}(w_p) = \det(\sigma_i(w_p^j))^2$$

$$\Rightarrow \det(\sigma_i(w_p^j)) = \sqrt{\pm p}^{p-2} \in \mathbb{Q}(w_p)$$

$$\Rightarrow \underbrace{\sqrt{\pm p} \cdot \sqrt{\pm p}^{p-3}}_{\in \mathbb{Q}} \in \mathbb{Q}(w_p) \Rightarrow \sqrt{\pm p} \in \mathbb{Q}(w_p) //$$

Thm 1. $p = \text{odd prime}$, $q \neq p$ prime, $d \mid p-1$

q splits completely in $K_d \Leftrightarrow q \equiv d^{\text{th}} \text{ power mod } p.$

$K = \mathbb{Q}(w_p)$
still!

Pf. $q \neq p \Rightarrow e=1$ and $p-1 = q \cdot f$

where $f = \text{order of } q \in (\mathbb{Z}/p\mathbb{Z})^\times$ (Thm 7.7.)

$$\{d^{\text{th}} \text{ powers mod } p\} \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

$$\begin{matrix} \text{ns} \\ \left(\begin{matrix} \text{unique} \\ \text{subgroup of} \\ \text{index } d \end{matrix} \right) \end{matrix} \hookrightarrow \begin{matrix} \text{ns} \\ \mathbb{Z}/(p-1)\mathbb{Z} \end{matrix}$$

$$\text{Thus: } q = d^{\text{th}} \text{ power mod } p \Leftrightarrow f \mid \frac{p-1}{d} = \frac{q \cdot f}{d}$$

$$\Leftrightarrow d \mid q$$

$$\Leftrightarrow K_d \subseteq K_q = K_{\mathbb{Q}_q}$$

$$\Leftrightarrow q \text{ splits comp. in } K_d.$$

Cor. 8.8.

□

Application: Quadratic Reciprocity (Elementary number theory!)

p odd prime, $n \in \mathbb{Z}$, $p \nmid n$

$$\leadsto \text{Legendre symbol: } \left(\frac{n}{p} \right) = \begin{cases} 1 & n \equiv \square \pmod{p} \\ -1 & n \not\equiv \square \pmod{p} \end{cases}$$

$$\text{E.g. } \left(\frac{1}{3} \right) = +1, \left(\frac{2}{3} \right) = -1.$$

Cor. 2. Quadratic reciprocity:

$$\begin{aligned} \bullet \quad q \neq 2, p : \left(\frac{q}{p} \right) &= \begin{cases} \left(\frac{p}{q} \right) & p \text{ or } q \equiv 1 \pmod{4} \\ -\left(\frac{p}{q} \right) & p \equiv q \equiv 3 \pmod{4} \end{cases} \quad (4) \\ \bullet \quad \left(\frac{2}{p} \right) &= \begin{cases} +1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases} \end{aligned}$$

- Conjectured by Euler & Legendre; Proved by Gauss in 1801.
- This approach: starting point of Class field theory, the Langlands program.

Pf. $q \neq 2, p$.

$$\left(\frac{q}{p} \right) = +1 \stackrel{\text{Thm 1}}{\iff} q \text{ splits (completely) in } F_2 = \mathbb{Q}(\sqrt{\pm p})$$

$$(\pm = + \text{ iff } p \equiv 1 \pmod{4})$$

$$\stackrel{\text{Thm 7.6}}{\iff} \pm p \equiv \square \pmod{q}$$

$$\iff \left(\frac{\pm p}{q} \right) = +1$$

$$\text{Moreover, } \left(\frac{\pm p}{q} \right) = \left(\frac{\pm 1}{q} \right) \cdot \left(\frac{p}{q} \right) \text{ and } \left(\frac{-1}{q} \right) = -1 \iff q \equiv 3 \pmod{4}. //$$

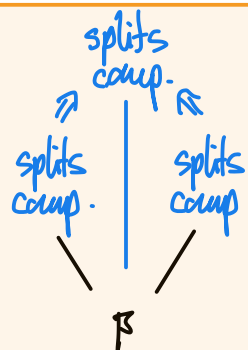
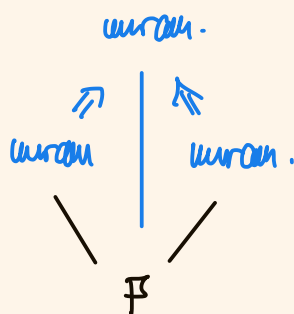
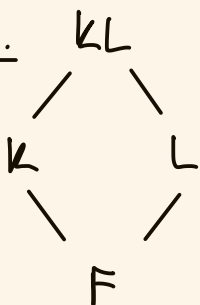
Exercise. $\left(\frac{2}{p} \right)$.

HW 5.



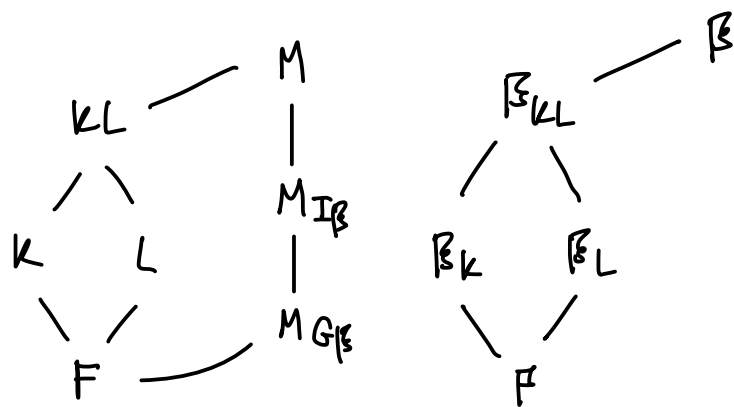
Consequences for non-Galois extensions.

Thm 3.



- $\mathfrak{p}$ unram. in K & $L \Rightarrow \mathfrak{p}$ unram. in KL
- $\mathfrak{p}$ spl. comp. in K & $L \Rightarrow \mathfrak{p}$ spl. comp. in KL

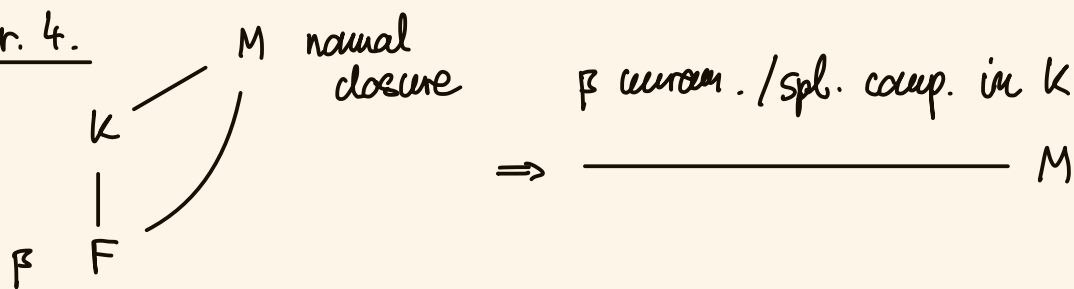
Pf. Consider $M = \text{normal closure of } KL$.



- $\beta_K, \beta_L / \beta$ unram. $\Rightarrow K, L \subseteq M_{I_\beta} \Rightarrow KL \subseteq M_{I_\beta} \Rightarrow \beta_{KL} / \beta$ unram. (Thm 8.7)
- $\beta_K, \beta_L / \beta$ spl. comp. $\Rightarrow K, L \subseteq M_{G_\beta} \Rightarrow KL \subseteq M_{G_\beta} \Rightarrow \beta_{KL} / \beta$ spl. comp. (Thm 8.7)

□

Cor. 4.



Pf. $\sigma_1, \dots, \sigma_n: K \hookrightarrow M$ embeddings

$\Rightarrow M = \sigma_1(K) \sigma_2(K) \dots \sigma_n(K)$ & use Thm 3.

□

Back to K/F Galois: Frobenius elements.

• For $\beta, \beta' / \beta$, how do $G_\beta, G_{\beta'} / I_\beta, I_{\beta'}$ compare?

Thm 6.1 $\Rightarrow \exists \sigma \in G$ s.t. $\beta' = \sigma \beta$ and then can check from def.:

$$G_{\beta'} = \sigma G_\beta \sigma^{-1}, \quad I_{\beta'} = \sigma I_\beta \sigma^{-1}.$$

• $\mathbb{F}/\mathbb{F}$ unram. in $K/F \Leftrightarrow \Gamma_{\mathbb{F}} = 1$

$$\Leftrightarrow G_{\mathbb{F}} \xrightarrow{\cong} \text{Gal}(\mathbb{F}_{\mathbb{F}}/\mathbb{F}_{\mathbb{F}}) \ni x \mapsto x^{||\mathbb{F}||}$$

$\downarrow$
 $\mathbb{Z}/f\mathbb{Z}$

Def. 5. $\mathbb{F}/\mathbb{F}$ unram.

Frobenius of $\mathbb{F}/\mathbb{F}$: $\phi := \phi_{\mathbb{F}/\mathbb{F}} \in G_{\mathbb{F}} \subseteq G$ such that $\phi(\alpha) \equiv \alpha^{||\mathbb{F}||} \pmod{\mathbb{F}}$.

Note : $\phi_{\sigma\mathbb{F}/\mathbb{F}} = \sigma \phi_{\mathbb{F}/\mathbb{F}} \sigma^{-1} \quad \forall \sigma \in G.$

Associated with $\mathbb{F}$, $\phi_{\mathbb{F}} := \phi_{\mathbb{F}/\mathbb{F}}$ for any $\mathbb{F}/\mathbb{F}$ is well-defined up to conj.,
i.e. defines a conjugacy class.

In particular, $G = \text{abelian} \Rightarrow \phi_{\mathbb{F}}$ well-defined :

unique element such that $\phi_{\mathbb{F}}(\alpha) \equiv \alpha^{||\mathbb{F}||} \pmod{\mathbb{F} \cap K}.$

Note: $\text{order}(\phi_{\mathbb{F}/\mathbb{F}}) = f(\mathbb{F}/\mathbb{F})$ by definition.

Example. For $K = \mathbb{Q}(\omega_m)/\mathbb{Q}$, $p \nmid m$, what is ϕ_p ? We already saw it!

$$\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

$$\sigma_k: \omega_m \mapsto \omega_m^a \longleftarrow a$$

$$\text{i.e. } \sum a_i \omega_m^i \mapsto \sum a_i \omega_m^{ki}$$

Claim. $\phi_p = \sigma_p.$

$$\text{Indeed, } \sigma_p\left(\sum_i a_i \omega_i\right) = \sum_i a_i \omega_i^p \equiv \left(\sum_i a_i \omega_i\right)^p \pmod{p\mathbb{Z}[\omega]} \quad \checkmark$$

Key step in proof of Thm 7.7 : $f(\mathbb{F}/\mathbb{F}) = \text{order of } \sigma_p,$

which now follows from the claim!

Direchlet Theorem on primes in arithmetic progressions:

$$\forall a \in (\mathbb{Z}/m\mathbb{Z})^\times \quad \exists \infty \text{ many } p \text{ s.t. } p \equiv a \pmod{m}.$$

$$\Rightarrow \forall \sigma \in \text{Gal}(\mathbb{Q}(\omega_m)/\mathbb{Q}) \quad \exists \infty \text{ many } p \text{ s.t. } \sigma = \phi_p \quad !$$

"Class field theory" $\Rightarrow \forall K/\mathbb{Q}$ abelian $\forall \sigma \in \text{Gal}(K/\mathbb{Q})$

$$\exists \infty \text{ many } p \text{ s.t. } \sigma = \phi_p.$$

What if K/F not Galois?

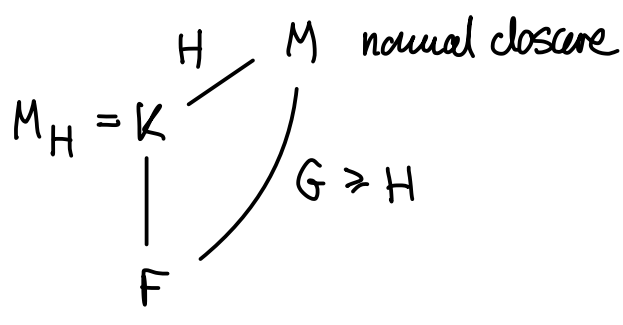


Diagram illustrating field extensions and Galois groups:

```

    graph TD
      F --> K
      F --> B
      K --> B
      K -- G --> H
      B -- "normal closure" --> H
  
```

Labels: $\phi := \phi_{B/F} \in G_B \subseteq G$, $\uparrow$ (Cor. 4.) $\uparrow$ unram.

Consider $H \backslash G = \{H\sigma \mid \sigma \in G\} \ni \langle \phi \rangle = G_B$

$$H\sigma \longmapsto H\sigma\phi$$

Decompose $H \backslash G$ into $\langle \phi \rangle$ orbits:

$$\{H\sigma_1, H\sigma_1\phi, \dots, H\sigma_1\phi^{m_1-1}\} \perp \{H\sigma_2, H\sigma_2\phi, \dots, H\sigma_2\phi^{m_2-1}\} \\ \perp \dots \perp \{H\sigma_g, H\sigma_g\phi, \dots, H\sigma_g\phi^{m_g-1}\}.$$

Thm 6. $\mathbb{P} \cap K = \sigma_1 \dots \sigma_g$ for $\sigma_i := \sigma_i \mathbb{P} \cap K$
& $f(\sigma_i/\mathbb{P}) = m_i$.

Pf: next time.

Last time:

- Splitting of primes in $\mathbb{Q}(\omega_p) \supset \mathbb{Q}(\sqrt{\pm p}) \supset \mathbb{Q} \Rightarrow$ quadratic reciprocity.
- **Frobenius**: K/F Galois, $\mathbb{P}/\mathbb{P}$ unramified

$$G_{\mathbb{P}} \xrightarrow{\cong} \text{Gal}(\mathbb{F}_{\mathbb{P}}/\mathbb{F}_{\mathbb{P}}) \cong \mathbb{Z}/f\mathbb{Z}$$

$$\phi := \phi_{\mathbb{P}/\mathbb{P}} \mapsto x \mapsto x^{|\mathbb{F}|}$$

i.e. $G_{\mathbb{P}}$ = cyclic, generated by ϕ of order f .

- In this case: $e=1$, f = order of ϕ , $g = n/f$.

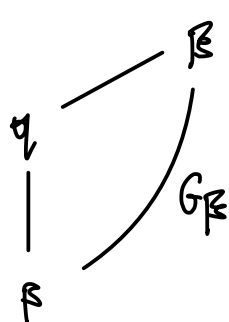
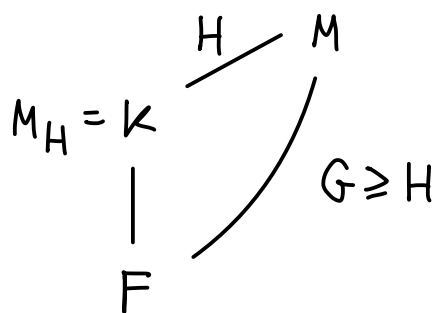
$\Rightarrow$ splitting of $\mathbb{P}$:

$$G/G_{\mathbb{P}} = G/\langle \phi \rangle \xleftrightarrow{1-1} \{ \text{primes above } \mathbb{P} \},$$

$$\sigma \langle \phi \rangle \mapsto \sigma \mathbb{P}$$

$$\{ \sigma, \sigma\phi, \dots, \sigma\phi^{f-1} \} \quad \& \quad f = f(\sigma\mathbb{P}/\mathbb{P}) \quad \forall \sigma.$$

- What if K/F not Galois? Let M/K Galois closure; $\mathbb{P}$ unram. in M .



$$G/G_{\mathbb{P}} \longleftrightarrow \{ \mathbb{P} \text{ above } \mathbb{P} \}$$

$$q_{\sigma} := \sigma\mathbb{P} \cap K \quad \forall \sigma \in G$$

$$q_{\sigma} = q_{\sigma'} \text{ if } \sigma(\sigma')^{-1} \in H$$

b/c H fixes K !

$$\Rightarrow H \backslash G/G_{\mathbb{P}} = \{ H\sigma G_{\mathbb{P}} : \sigma \in G \} \xleftrightarrow{1-1} \{ q \text{ above } \mathbb{P} \}$$

$$\text{"double cosets"} = \{ H\sigma_1 G_{\mathbb{P}}, \dots, H\sigma_g G_{\mathbb{P}} \} \longleftrightarrow \{ q_1, \dots, q_g \}$$

What is $f(q_i/\mathbb{P})$?

Consider :

$$\begin{array}{ccc}
 H \backslash G & \longrightarrow & H \backslash G / G_{\mathbb{F}} \\
 H \sigma & \longmapsto & H \sigma G_{\mathbb{F}} \\
 H \sigma_i, H \sigma_i \phi, \dots, H \sigma_i \phi^{f_i-1} & \longrightarrow & H \sigma_i G_{\mathbb{F}} = H \sigma_i \langle \phi \rangle
 \end{array}$$

$f_i \mid f = \text{order of } \phi$

Thm 9.6. $\mathbb{F} \cap K = \mathbb{F}_1 \dots \mathbb{F}_g$ for $\mathbb{F}_i := \sigma_i \mathbb{F} \cap K$, $f_i(\mathbb{F}_i / \mathbb{F}) = f_i$.

Pf. Checked already: $\{\mathbb{F}_i \text{ above } \mathbb{F}\} = \{\mathbb{F}_1, \dots, \mathbb{F}_g\}$.

Claim. $f(\mathbb{F}_i / \mathbb{F}) \geq f_i \forall i$.

Then: $[K:F] = \sum_{i=1}^g f(\mathbb{F}_i / \mathbb{F}) \cdot 1 \geq \sum_{i=1}^g f_i = |H \backslash G| = [K:F]$

Thm 5.8

proves equality holds & we're done.

Write $\mathbb{F}_i = \sigma_i \mathbb{F} \cap K$, $f = f_i$, $\sigma = \sigma_i \leadsto \mathbb{F}_i = \sigma \mathbb{F} \cap K$ & want $f(\mathbb{F}_i / \mathbb{F}) \geq f$.

Note: $\phi(\sigma \mathbb{F} / \mathbb{F}_i) = \phi(\sigma \mathbb{F} / \mathbb{F})^{f(\mathbb{F}_i / \mathbb{F})}$.

unique such that
unique such that

$$x \mapsto x^{\|\mathbb{F}_i\|} \bmod \sigma \mathbb{F} \quad x \mapsto x^{\|\mathbb{F}\|} \bmod \sigma \mathbb{F}$$

& $\|\mathbb{F}_i\| = |G_K / \mathbb{F}_i| = |G_F / \mathbb{F}|^{f(\mathbb{F}_i / \mathbb{F})} = \|\mathbb{F}\|^{f(\mathbb{F}_i / \mathbb{F})}$

Thus: $H \ni \phi(\sigma \mathbb{F} / \mathbb{F}_i) = (\sigma \phi(\mathbb{F} / \mathbb{F}) \sigma^{-1})^{f(\mathbb{F}_i / \mathbb{F})}$

$$= \sigma \phi^{f(\mathbb{F}_i / \mathbb{F})} \sigma^{-1} \quad (\phi = \phi(\mathbb{F} / \mathbb{F}))$$

$\Rightarrow \sigma \phi^{f(\mathbb{F}_i / \mathbb{F})} \sigma^{-1} \in H \Rightarrow H \sigma \phi^{f(\mathbb{F}_i / \mathbb{F})} = H \sigma$

$\Rightarrow f \leq f(\mathbb{F}_i / \mathbb{F})$ as we wanted.

Homework:

- Apply Thm 9.6 to splitting in $K = \mathbb{Q}(\sqrt[n]{m})$.
- Generalize $\phi_{\mathbb{P}/\mathbb{P}}$ & Thm 9.6 to ramified primes.

Another thing I promised to do...

Thm 1. $p \mid \text{disc}(K) \Rightarrow p$ ramified in K .

This $\Leftrightarrow$ holds by Thm 7.2.

Rf. $\alpha_1, \dots, \alpha_n$ basis of $\mathcal{O}_K \Rightarrow \text{disc}(K) = \det T(\alpha_i \alpha_j)$ (Thm 2.8)

Assumption: $\det T(\alpha_i \alpha_j) \equiv 0 \pmod{p}$

$$\Rightarrow \exists m_1, \dots, m_n \in \mathbb{Z} \text{ s.t. } \sum_{i=1}^n m_i T(\alpha_i \alpha_j) \equiv 0 \pmod{p} \quad \forall j$$

(not all 0 mod p)

$$\Rightarrow \alpha := \sum_{i=1}^n m_i \alpha_i \text{ satisfies } T(\alpha \alpha_j) \equiv 0 \pmod{p} \quad \forall j$$

$$\Rightarrow T(\alpha \mathcal{O}_K) \subseteq p\mathbb{Z}^{(*)} \text{ but } \alpha \notin p\mathcal{O}_K \text{ (not all } m_i \equiv 0 \pmod{p}).$$

Suppose p unram. in $K \Rightarrow p\mathcal{O}_K = \mathfrak{P}_1 \dots \mathfrak{P}_g$, $\mathfrak{P}_i$ distinct.

$$\text{Now, } \alpha \in \mathfrak{P}_i \quad \forall i \Rightarrow \mathfrak{P}_1 \dots \mathfrak{P}_g \mid \alpha \mathcal{O}_K$$

$$\Rightarrow p\mathcal{O}_K \mid \alpha \mathcal{O}_K$$

$$\Rightarrow p\mathcal{O}_K \supseteq \alpha \mathcal{O}_K \ni \alpha \quad \nsubseteq$$

Thus, $\alpha \notin \mathfrak{P}$ for some $\mathfrak{P}$ of K over p .

Let M = normal closure of K

$\Rightarrow p$ unram. in M as well (Cor. 9.4)

Also, for $\mathfrak{P}$ of M above $\mathfrak{P}$, $\alpha \notin \mathfrak{P}$. (else $\alpha \in \mathfrak{P} \cap K = \mathfrak{P}$)

$$\begin{aligned} \text{Now: } T_{M/\mathbb{Q}}(\alpha \theta_M) &= T_{K/\mathbb{Q}} T_{M/K}(\alpha \theta_M) = T_{K/\mathbb{Q}}(\alpha T_{M/K}(\theta_M)) \\ &\subseteq T_{K/\mathbb{Q}}(\alpha \theta_K) \\ &\stackrel{(*)}{\subseteq} p\mathbb{Z}. \end{aligned}$$

Fix $\beta \in \mathcal{O}_M$ s.t. $\beta \notin \mathfrak{P}$, $\beta \in \mathfrak{P}' \quad \forall \mathfrak{P}'$ prime of M above p , $\mathfrak{P}' \neq \mathfrak{P}$.

Claim. $\forall \gamma \in \mathcal{O}_M$

$$(1) \quad T_{M/\mathbb{Q}}(\alpha \beta \gamma) \in \mathfrak{P}$$

$$(2) \quad \sigma(\alpha \beta \gamma) \in \mathfrak{P} \quad \forall \sigma \in G - G_{\mathfrak{P}}$$

$G := \text{Gal}(M/\mathbb{Q})$
 $G_{\mathfrak{P}}$ decap. group of $\mathfrak{P}$

$$\text{Indeed: (1): } T_{M/\mathbb{Q}}(\alpha \beta \gamma) \in p\mathbb{Z} \subseteq \mathfrak{P} \quad \checkmark$$

$$(2): \beta \in \sigma^{-1}\mathfrak{P} \quad \forall \sigma \in G - G_{\mathfrak{P}} \Rightarrow \sigma(\beta) \in \mathfrak{P} \quad \checkmark //$$

$$\begin{aligned} \text{Claim} \Rightarrow & \boxed{T_{M/\mathbb{Q}}(\alpha \beta \gamma)} \stackrel{\in \mathfrak{P} \quad (1)}{=} \sum_{\sigma \in G} \sigma(\alpha \beta \gamma) = \sum_{\sigma \in G_{\mathfrak{P}}} \sigma(\alpha \beta \gamma) + \boxed{\sum_{\sigma \in G - G_{\mathfrak{P}}} \sigma(\alpha \beta \gamma)} \stackrel{\in \mathfrak{P} \quad (2)}{=} \\ \Rightarrow & \sum_{\sigma \in G_{\mathfrak{P}}} \sigma(\alpha \beta \gamma) \in \mathfrak{P} \quad \forall \gamma \in \mathcal{O}_L. \end{aligned}$$

$$\text{Reducing mod } \mathfrak{P}: \sum_{\sigma \in G_{\mathfrak{P}}} \overline{\sigma(\alpha \beta \gamma)} = 0 \quad \forall \gamma \in \mathbb{F}_{\mathfrak{P}}$$

$$\alpha, \beta \notin \mathfrak{P} \Rightarrow \alpha \cdot \beta \notin \mathfrak{P} \Rightarrow \overline{\alpha \beta} \neq 0 \text{ in } \mathbb{F}_{\mathfrak{P}}$$

$$\Rightarrow \sum_{\overline{\sigma} \in \text{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p)} \overline{\sigma}(x) = 0 \quad \forall x \in \mathbb{F}_{\mathfrak{P}}$$

This is a contradiction: k field, $\sigma_1, \dots, \sigma_f: k \rightarrow k$ distinct
 $\Rightarrow \sigma_1, \dots, \sigma_f$ are k -linearly independent.

Else: say $\sum_{i=1}^n a_i \sigma_i = 0$ shortest lin. comb. (*)

$$\Rightarrow \forall x, y \quad \sum_i a_i \sigma_i(xy) = \sum_i a_i \sigma_i(x) \sigma_i(y) = 0 \quad (*) (xy)$$

$$\Rightarrow \forall x \quad \sum_i a_i \sigma_i(x) \sigma_i = 0$$

$$\& \forall x \quad \sum_i a_i \sigma_n(x) \sigma_i = 0 \quad (*) \cdot \sigma_n(x)$$

$$\Rightarrow \forall x \quad \sum_{i=1}^{n-1} a_i (\sigma_n(x) - \sigma_i(x)) \sigma_i = 0 \quad \text{shorter linear comb.}$$

$$\Rightarrow \forall x \quad \sigma_n(x) = \sigma_i(x) \Rightarrow \sigma_n = \sigma_i \quad \forall i \quad \square$$

One more result I skipped... (but used implicitly)

$K = F(\alpha), \alpha \in \mathcal{O}_K$ with min. poly $f(x)$ over $\mathcal{O}_F$

$\downarrow$
 F

... determined by
 $\downarrow$
 $\mathbb{F}$
 $\overline{f(x)} \in \mathbb{F}_{\mathbb{F}}[x] !$

Thm 2. If $p \nmid |\mathcal{O}_K/\mathcal{O}_F[\alpha]|$ (e.g. $\mathcal{O}_K = \mathcal{O}_F[\alpha]$) & $\mathbb{F}$ is above p ,

then factorization of $\overline{f(x)} = \overline{f_1(x)}^{e_1} \cdots \overline{f_g(x)}^{e_g}$ in $\mathbb{F}_{\mathbb{F}}[x]$ gives

$$\mathbb{F} \mathcal{O}_K = \mathbb{F}_1^{e_1} \cdots \mathbb{F}_g^{e_g} \text{ with } \mathbb{F}_i = \mathbb{F} \mathcal{O}_K + \mathcal{O}_K q_i(\alpha), \\ f(\mathbb{F}_i/\mathbb{F}) = \deg(q_i(x)).$$

(Pf: skipped.)

Example. $K = \mathbb{Q}(\sqrt{m})/\mathbb{Q}$ (c.f. Thm 7.6)

$$x^2 - m \pmod{p} \begin{cases} \xrightarrow{x^2 \quad p \nmid m} (x-n)(x+n) & m \equiv n^2 \pmod{p} \\ \xrightarrow{\text{ined.}} \end{cases}$$

(p odd)

$$p \mathcal{O}_K = \mathbb{F}^2, \quad \mathbb{F} = (p, \sqrt{m})$$

$$p \mathcal{O}_K = \mathbb{F}_1 \mathbb{F}_2, \quad \mathbb{F}_i = (p, \sqrt{m} \pm n)$$

$$p \mathcal{O}_K \text{ prime}$$

Done with splitting of primes in extensions!

One can use what we learned so far to prove the following ...

Thm 3 (Kronecker-Weber). $\rightarrow \text{Gal}(K/\mathbb{Q}) = \text{abelian group}$

Every abelian extension $K/\mathbb{Q}$ is contain in $\mathbb{Q}(\omega_m)$ for some m .

This is proved in a series of exercises in chapter 4 of Marcus.

Recall: $\omega_m = e^{2\pi i/m}$ = value of $e^{2\pi i z}$ at $z = \frac{1}{m}$.

Hilbert's 12th problem. (1900)

For any number field F , find special functions whose values generate any abelian extension of F

Note: $\omega_m \in \mathbb{Z}[\omega_m]^\times \Rightarrow$ related goal: construct units in abelian ext. of F
(c.f. Stark's conjecture).

Resolved for $F = \mathbb{Q}(\sqrt{m})$, $m < 0$: (imaginary quadratic)

theory of complex multiplication & elliptic functions.

Lots of ongoing research in other cases:

- $F = \mathbb{Q}(\sqrt{m})$, $m > 0$: (real quadratic)

- $\rightarrow$ Damanik-Venk (2021): conjectural attempt (complex-analytic).

- $\rightarrow$ Dasgupta-Kakde (2021): successful p-adic resolution.

- $F = \mathbb{Q}(\sqrt[3]{m})$ (complex cubic)

- Bergeron-Charollois-Garcia (2023): conjectural attempt (complex-analytic)

- Monday : Q & A session
→ complete the eCampus survey by Friday!
- Monday, June 8 : evaluation survey, completed in class.

Summary.

K = number field,
 $[K:\mathbb{Q}] = n$

$\mathcal{O}_K$ = ring of integers

Thm. $\mathcal{O}_K$ free of rank n .

Caution:
 $\mathcal{O}_K$ not always $\mathbb{Z}[\alpha]$!

Tools to study them:

$$N_{K/\mathbb{Q}}: K \rightarrow \mathbb{Q}$$

$$T_{K/\mathbb{Q}}: K \rightarrow \mathbb{Q}$$

For M = normal closure of $K/\mathbb{Q}$,

$$\sigma_1, \dots, \sigma_n: K \hookrightarrow M:$$

$$N_{K/\mathbb{Q}}(x) = \sigma_1(x) \cdot \dots \cdot \sigma_n(x)$$

$$T_{K/\mathbb{Q}}(x) = \sigma_1(x) + \dots + \sigma_n(x)$$

Also: $\alpha_1, \dots, \alpha_n$ $\mathbb{Z}$ -basis of $\mathcal{O}_K$

$$\begin{aligned} \text{disc}(K) &:= \det(\sigma_i(\alpha_j))^2 \\ &= \det(T_{K/\mathbb{Q}}(\alpha_i \alpha_j)) \end{aligned}$$

Note: there's an "ideal norm"

$$\|I\| := \mathcal{O}_K/I$$

& we proved: $\|(\alpha)\| = |N_{K/\mathbb{Q}}(\alpha)|$.

Example.

$$K = \mathbb{Q}(\alpha) \quad \alpha^3 = 2$$

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

$$= \mathbb{Z}\langle 1, \alpha, \alpha^2 \rangle \ni a + b\alpha + c\alpha^2$$

$$M = \mathbb{Q}(\alpha, \omega_3) \quad \text{b/c roots of } x^3 - 2$$

$$\text{are } \alpha, \alpha\omega_3, \alpha\omega_3^2.$$

$$K \longrightarrow M$$

$$\begin{array}{ccc} \alpha & \xrightarrow{\sigma_1} & \alpha & \sigma_1(a + b\alpha + c\alpha^2) \\ \alpha & \xrightarrow{\sigma_2} & \omega_3 \alpha & \parallel \\ \alpha & \xrightarrow{\sigma_3} & \omega_3^2 \alpha & a + b\sigma_1(\alpha) + c\sigma_1(\alpha)^2 \end{array}$$

$$\begin{aligned} N_{K/\mathbb{Q}}(x) &= \sigma_1(x) \cdot \sigma_2(x) \cdot \sigma_3(x) \\ &= x^3 + 2b^3 + 4c^3 - 6abc \end{aligned}$$

$$\begin{aligned} T_{K/\mathbb{Q}}(x) &= 3a + b(\alpha + \alpha\omega + \alpha\omega^2) \\ &\quad + c(\alpha^2 + (\alpha\omega)^2 + (\alpha\omega^2)^2) \\ &= 3a \quad \text{b/c } 1 + \omega + \omega^2 = 0 \end{aligned}$$

$$\begin{aligned} \text{disc}(K) &= \det \begin{pmatrix} \text{Tr}(1) & \text{Tr}(\alpha) & \text{Tr}(\alpha^2) \\ \text{Tr}(\alpha) & \text{Tr}(\alpha^2) & \text{Tr}(\alpha^3) \\ \text{Tr}(\alpha^2) & \text{Tr}(\alpha^3) & \text{Tr}(\alpha^4) \end{pmatrix} \\ &= \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{pmatrix} \end{aligned}$$

$$= -108 = -2^2 \cdot 3^3$$

$$\|(\alpha)\| = \left| \frac{\mathbb{Z}\langle 1, \alpha, \alpha^2 \rangle}{(\alpha)} \right| = \left| \frac{\mathbb{Z}}{2\mathbb{Z}} \right| = 2$$

$$N(\alpha) = \alpha \cdot \omega_3 \alpha \cdot \omega_3^2 \alpha^2 = \alpha^3 = 2$$

But $T_{K/\mathbb{Q}}(I) := \{T_{K/\mathbb{Q}}(x) : x \in I\}$, etc.

$$\begin{aligned} T_{K/\mathbb{Q}}(6) &= \{T_{K/\mathbb{Q}}(a \cdot (a+b\alpha+c\alpha^2)) : a,b,c \in \mathbb{Z}\} \\ &= \{T_{K/\mathbb{Q}}(a^2 + b^2\alpha + 2c\alpha^2) : a,b,c \in \mathbb{Z}\} = 6\mathbb{Z} \\ &= T_{K/\mathbb{Q}}(\alpha)\mathbb{Z} = 0. \end{aligned}$$

Thm. K, L with $K \cap L = \mathbb{Q}$

$$\Rightarrow \mathcal{O}_K \cdot \mathcal{O}_L \subseteq \mathcal{O}_{KL} \subseteq \frac{1}{\gcd(\text{disc}(K), \text{disc}(L))} \mathcal{O}_K \cdot \mathcal{O}_L.$$

Note: inductively extends to more fields!

$\mathcal{O}_K \neq \text{PID}$ b/c $\mathcal{O}_K$ Dedekind domain



Note: $\mathcal{O}_K \neq \text{UFD}$ in general!

Our current example is a UFD :

But $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\omega_{23})$, $\mathbb{Q}(\sqrt[3]{-23})$

are all non-examples.

Thm. Ideals in $\mathcal{O}_K$ factor uniquely into prime ideals.

Consequence: for any p prime, $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ for some $\mathfrak{p}_i$ prime.

Thm. $e_1 f_1 + \dots + e_g f_g = n$ where $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$.

Thm. If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ & $f(x) = \text{min. poly of } \alpha$, then:

$$\overline{f(x)} \equiv \prod_{i=1}^g \overline{f_i(x)}^{e_i} \pmod{p} \iff p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g} \quad \begin{aligned} \mathfrak{p}_i &= (p, g_i(\alpha)) \\ f_i &= \deg g_i(x). \end{aligned}$$

Example. $K = \mathbb{Q}(\alpha)$, $f(x) = x^3 - 2$

• $p=2$: $x^3 - 2 \equiv x^3 \pmod{2} \Rightarrow 2\mathbb{Z}[\alpha] = (2, \alpha)^3 = (\alpha)^3$
 $\uparrow$
 $(2 = \alpha^3)$

• $p=3$: $x^3 - 2 \equiv x^3 + 1 = (x+1)(x^2 - x + 1) \pmod{3}$
 $\equiv (x+1)(x^2 + 2x + 1)$
 $= (x+1)(x+1)^2 = (x+1)^3$

$\Rightarrow 3\mathbb{Z}[\alpha] = (3, \alpha+1)^3$

• $p=5$: $x^3 - 2 = ?$

Roots? $x=0 \rightsquigarrow -2$ x
 $x=1 \rightsquigarrow 1-2 = -1$ x
 $x=2 \rightsquigarrow 8-2 = 6$ x
 $x=3 \rightsquigarrow 27-2 = 25 \equiv 0$ $\checkmark$
 $x=4 \rightsquigarrow (-1)^3 - 2 = -3$ x
 $\equiv -1$

$x^3 - 2 = (x-3)(\underbrace{x^2 + 3x + 4}_{\text{no roots}}) \pmod{5}$

$\Rightarrow 5\mathbb{Z}[\alpha] = (\underbrace{5, \alpha-3}_{f=1}) \cdot (\underbrace{5, \alpha^2 + 3\alpha + 4}_{f=2})$ $(1 \cdot 1 + 1 \cdot 2 = 3)$

• $p=7$: $x^3 - 2$ has no roots mod 7 (check by hand)

$\Rightarrow 7\mathbb{Z}[\alpha]$ is prime with $f=3$.

• $p=31$: $x^3 - 2$ has 3 roots $\Rightarrow \mathbb{Z}[\alpha] = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$, all with $f=1$.

Rem. $p \mid \text{disc}(K/\mathbb{Q}) \Leftrightarrow p$ is ramified in $K/\mathbb{Q}$.

Exactly $p=2, 3$ ramify in $\mathbb{Q}(\sqrt[3]{2})$!

Galois theory applied to splitting.

K/F Galois, $G := \text{Gal}(K/F)$, $\mathbb{P}/\mathbb{P}$ prime

$$\leadsto G_{\mathbb{P}} := \{\sigma \in G \mid \sigma \mathbb{P} = \mathbb{P}\} \cong I_{\mathbb{P}} := \{\sigma \in G_{\mathbb{P}} \mid \sigma(x) \equiv x \pmod{\mathbb{P}} \forall x\}$$

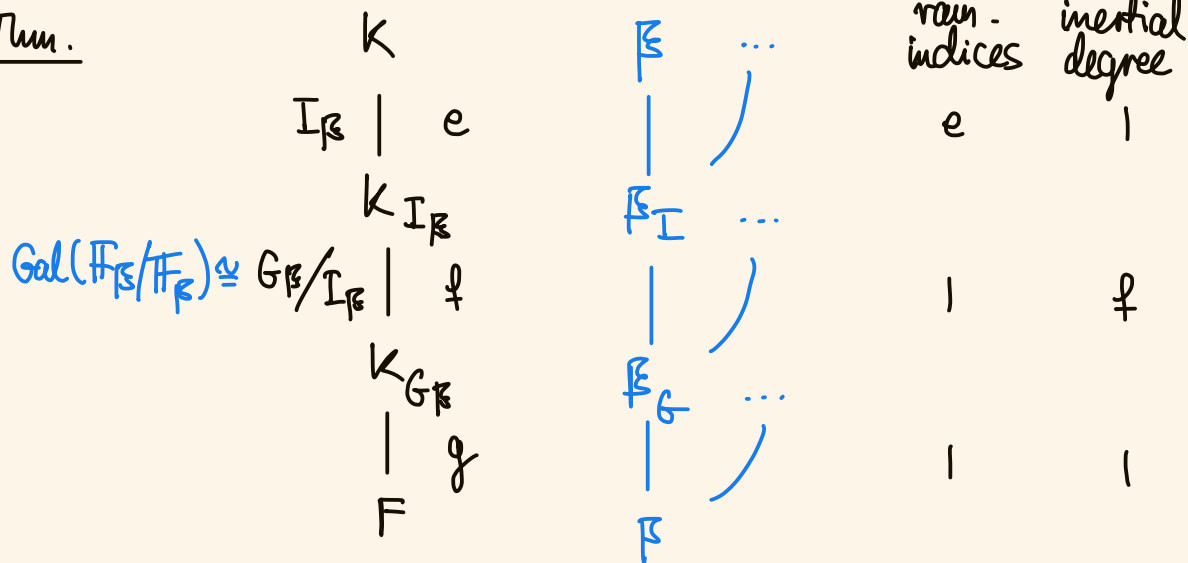
$$G_{\mathbb{P}}/I_{\mathbb{P}} \xrightarrow{\cong} \text{Gal}(\mathbb{F}_{\mathbb{P}}/\mathbb{F}_{\mathbb{P}})$$

$$|I_{\mathbb{P}}| = e, |G_{\mathbb{P}}| = e \cdot f$$

$$\sigma \longmapsto \sigma \pmod{\mathbb{P}}$$

$$e \cdot f \cdot g = n$$

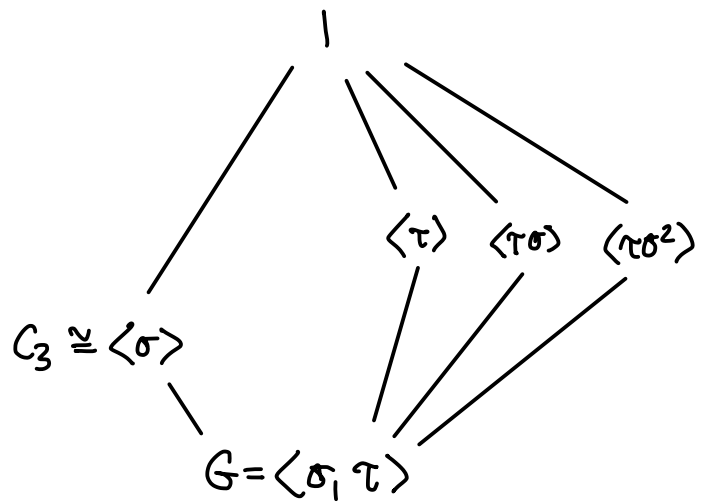
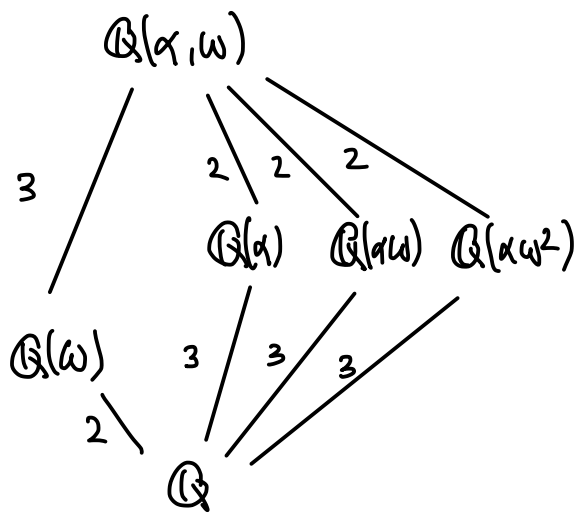
Thm.



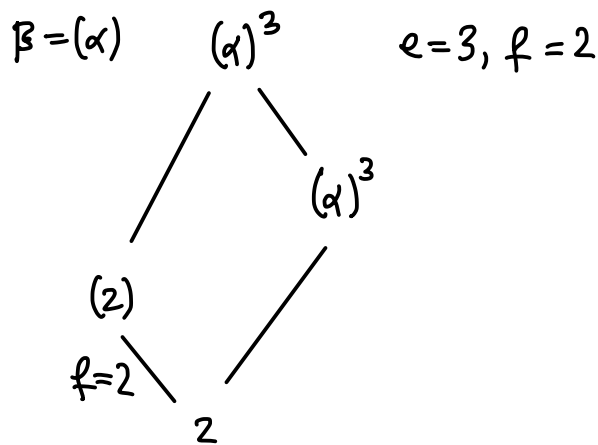
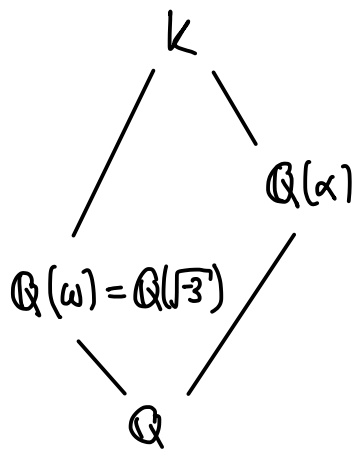
Example. $K = \mathbb{Q}(\alpha, \omega)$, $\alpha^3 = 2$, $\omega^3 = 1$, (normal closure of $\mathbb{Q}(\sqrt[3]{2})$)

Galois group.

element	$\alpha \mapsto ?$	$\omega \mapsto ?$	element of S_3
id	α	ω	(1)
σ	$\omega \alpha$	ω	(123)
σ^2	$\omega^2 \alpha$	ω	(132)
τ	α	ω^2	(23)
$\tau \sigma$	$\omega^2 \alpha$	ω^2	(13)
$\tau \sigma^2$	$\omega \alpha$	ω^2	(12)



p=2.

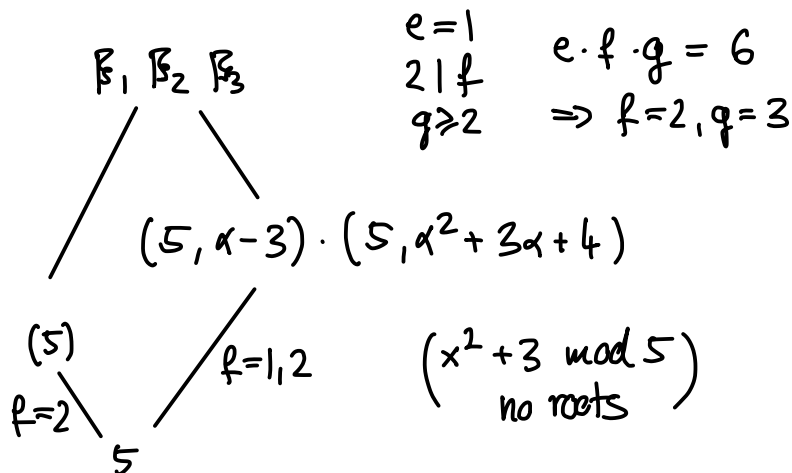
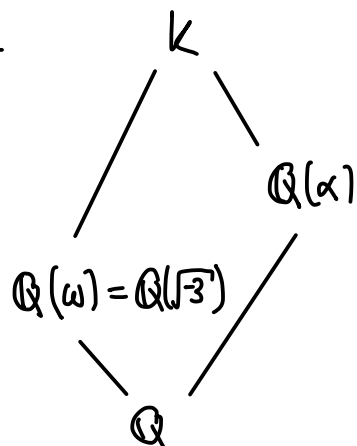


$$\Rightarrow \begin{aligned} & \bullet |G_B| = e \cdot f = 6 \Rightarrow G_B = G \Rightarrow K_{G_B} = \mathbb{Q} \\ & \bullet |I_B| = e = 3 \Rightarrow I_B = \langle \sigma \rangle \Rightarrow K_{I_B} = \mathbb{Q}(\omega) \end{aligned}$$

p=3. p tot. ram. in both $\mathbb{Q}(\omega)$ & $\mathbb{Q}(\alpha) \Rightarrow$ tot. ram. in K

$$\Rightarrow G_B = I_B = G \text{ \& } K_{G_B} = K_{I_B} = \mathbb{Q}$$

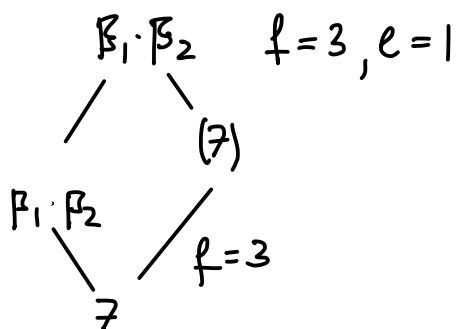
p=5.



• $|G_{B_i}| = e \cdot f = 2 \Rightarrow K_{G_{B_i}}$ are the three groups $\langle \tau \rangle, \langle \tau\sigma \rangle, \langle \tau\sigma^2 \rangle$
& correspond to $\mathbb{Q}(\alpha), \mathbb{Q}(\alpha\omega), \mathbb{Q}(\alpha\omega^2)$.

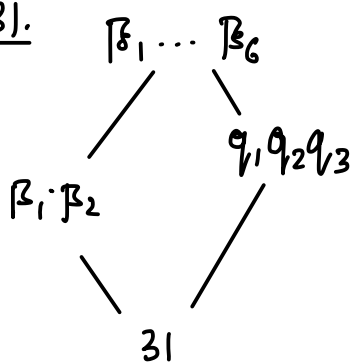
• $|I_{B_i}| = e = 1 \Rightarrow K_{I_{B_i}} = K$ always.

p=7.

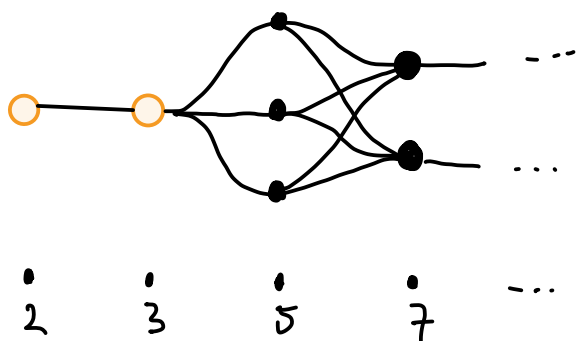


$|G_{B_i}| = 3 \Rightarrow G_{B_i} = \langle \sigma \rangle$
 $K_{G_{B_i}} = \mathbb{Q}(\omega)$

p=31.



$e = f = 1 \Rightarrow G_{B_i} = I_{B_i} = \{1\}$
 $\Rightarrow K_{G_{B_i}} = K_{I_{B_i}} = K$.



CLASS ON WEDNESDAY: ONLINE ON ZOOM!

(I'm at a conference.)

Rough plan going forward: $\leq$ instead of $=$

- Finiteness of the class group $Cl(K)$ & the unit group $\mathcal{O}_K^\times$.
- Distribution of ideals.
- The Dedekind zeta function & the class number formula.

Recall ...

Def 1. Class group of K

HW 3, Ex. 4

$$Cl(K) := \left\{ \text{ideals of } \mathcal{O}_K \right\} / \sim = \left\{ \text{fractional ideals of } K \right\} / \left\{ \text{principal fractional ideals of } K \right\}$$

$$I \sim J \text{ if } \alpha I = \beta J, \alpha, \beta \in \mathcal{O}_K \setminus \{0\}$$

Goal: $Cl(K)$ is finite.

It's a group! (Inverses: Thm 4.5.)

Thm 2. $\exists \lambda > 0$ (dep. on K) s.t. $\forall I \subseteq \mathcal{O}_K \exists \alpha \in I$ s.t.

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \lambda \cdot \|I\|.$$
(λ indep. of I !)Pf. $\alpha_1, \dots, \alpha_n$ basis of $\mathcal{O}_K$, $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ embeddings

$$\lambda := \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(\alpha_j)|.$$

For I , take $m \in \mathbb{N}$ s.t. $m^n \leq \|I\| \leq (m+1)^n$.The set: $\left\{ \sum_{j=1}^n m_j \alpha_j : m_j \in \mathbb{Z}, 0 \leq m_j \leq m \right\}$ has $(m+1)^n \geq \|I\|$ elements $\Rightarrow$ two must be congruent mod I $\Rightarrow$ let α be their difference: $\alpha = \sum m_j \alpha_j$, $|m_j| \leq m$.

L12/1.

$$\begin{aligned}
 \text{Then } |N_{K/\mathbb{Q}}(\alpha)| &= \prod_{i=1}^n |\sigma_i(\alpha)| \leq \prod_{i=1}^n \sum_{j=1}^n |a_j| |\sigma_i(\alpha_j)| \\
 &\leq \prod_{i=1}^n \sum_{j=1}^n |a_j| |\sigma_i(\alpha_j)| \\
 &= |a|^\eta \cdot \lambda \\
 &\leq \|I\| \cdot \lambda.
 \end{aligned}$$

□

Cor. 3. Every ideal class contains $\mathfrak{f}$ with $\|\mathfrak{f}\| \leq \lambda$ for λ as above.

Pf. $C \in \text{Cl}(K) \leadsto C^{-1} \in \text{Cl}(K) \leadsto I \in C^{-1}$ any ideal in the class

$\Rightarrow$ let $\alpha \in I$ as in Thm 2: $|N(\alpha)| \leq \lambda \cdot \|I\|$.

Then $(\alpha) \subseteq I \Rightarrow (\alpha) = I \cdot \mathfrak{f}$ for some $\mathfrak{f}$ & $\mathfrak{f} \in C$ ($1 = [I] \cdot [\mathfrak{f}]$)

$$\begin{aligned}
 \Rightarrow |N(\alpha)| &= \|(\alpha)\| = \|I \cdot \mathfrak{f}\| = \|I\| \cdot \|\mathfrak{f}\| \quad (\text{Thm 5.10}) \\
 &\quad \wedge \\
 &\quad \lambda \cdot \|I\|
 \end{aligned}$$

$$\Rightarrow \|\mathfrak{f}\| \leq \lambda.$$

□

Cor. 4. $|\text{Cl}(K)| < \infty$.

Def 5. $h(K) := |\text{Cl}(K)|$ class number.

Pf. For $\mathfrak{f} \in \text{Cl}(K)$, $\mathfrak{f} = \prod \mathfrak{p}_i^{n_i} \Rightarrow \|\mathfrak{f}\| = \prod \|\mathfrak{p}_i\|^{n_i}$

$\Rightarrow$ fin. many $\mathfrak{f}$ with $\|\mathfrak{f}\| \leq \lambda$.

□

To compute $\text{Cl}(K)$, consider all such $\mathfrak{f}$ & figure out coincidences between the classes ... $\leadsto$ Useful to make λ smaller!

Consider $\sigma_1, \dots, \sigma_r: K \hookrightarrow \mathbb{R}$, $\tau_1, \bar{\tau}_1, \dots, \tau_s, \bar{\tau}_s: K \hookrightarrow \mathbb{C}$ ($\tau_i \neq \bar{\tau}_i$)

so that $r + 2s = n$.

E.g. For $K = \mathbb{Q}(\sqrt{m})$, $m < 0: r=0, s=1$
 $m > 0: r=2, s=0$

Thm 6. (Minkowski bound). Every ideal class of R contains $\mathfrak{f}$ with

$$\|\mathfrak{f}\| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\text{disc}(K)|}.$$

↓
Minkowski constant (gets small fast!)

Examples

① $K = \mathbb{Q}(\sqrt{2})$. $n=2, s=0, \text{disc}(K) = 8$

$$\Rightarrow \|\mathfrak{f}\| \leq \frac{2!}{2^2} \left(\frac{4}{\pi}\right)^0 \sqrt{8} = \sqrt{2} < 2$$

$$\Rightarrow \mathcal{C}(K) = \{1\}$$

② $K = \mathbb{Q}(\sqrt{-5})$. $n=2, s=1, \text{disc}(K) = -20$

$$\Rightarrow \|\mathfrak{f}\| \leq \frac{2!}{2^2} \left(\frac{4}{\pi}\right)^1 \sqrt{20} = \frac{4\sqrt{5}}{\pi} < 3$$

$\Rightarrow$ every ideal class contains $\mathfrak{f}$ with $\|\mathfrak{f}\| \in \{1, 2\}$.

Enough to consider $\|\mathfrak{f}\| = 2 \rightarrow \mathfrak{f} = (2, 1+\sqrt{-5})$ with $\mathfrak{f}^2 = 2\mathcal{O}_K$

Can $\mathfrak{f} = (2, 1+\sqrt{-5})$ be principal? No!

$$\text{If } \mathfrak{f} = (\alpha) \Rightarrow |N(\alpha)| = \|(\alpha)\| = 2 \Rightarrow N(\alpha) = \pm 2$$

$$\Rightarrow \alpha = a + b\sqrt{-5} \text{ implies } a^2 + 5b^2 = \pm 2 \quad \text{No!}$$

$$\text{Thus: } \mathcal{C}(K) = \{1, [(2, 1+\sqrt{-5})]\} \quad \& \quad h(K) = 2.$$

HW 7. Application of this, similar to lecture 1:
 $y^2 = x^3 + 5$.

③ $K = \mathbb{Q}(\omega_5)$ $n=4, s=2, \text{disc}(\omega_5) = 5^3$

$$\Rightarrow \|\mathfrak{f}\| \leq \frac{4!}{4^4} \cdot \left(\frac{4}{\pi}\right)^2 \cdot 5\sqrt{5} = \frac{15\sqrt{5}}{\pi^2} < 2$$

$$\Rightarrow \mathcal{C}(K) = \{1\}.$$

More examples: exercises!

Cor 7. $|\text{disc}(K)| > 1$ when $K \neq \mathbb{Q}$.

Thus there are no unramified extensions of $\mathbb{Q}$!

How to prove Thm 6?

Recall: $\sigma_1, \dots, \sigma_r, \tau_1, \bar{\tau}_1, \dots, \tau_s, \bar{\tau}_s$ $n = r + 2s$

$$\leadsto K \longrightarrow \mathbb{R}^r \oplus \mathbb{C}^s \cong \mathbb{R}^n \quad \mathbb{C} \cong \mathbb{R}^2 \text{ via } z \mapsto (\operatorname{Re} z, \operatorname{Im} z)$$

$$\alpha \longmapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha)) \in \mathbb{R}^r \oplus \mathbb{C}^s$$

$$= (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Re} \tau_1(\alpha), \operatorname{Im} \tau_1(\alpha), \dots, \operatorname{Re} \tau_s(\alpha), \operatorname{Im} \tau_s(\alpha)) \in \mathbb{R}^n$$

Thm 8. The map $K \longrightarrow \mathbb{R}^n$ sends $\mathcal{O}_K$ to a lattice $\Lambda_K \subseteq \mathbb{R}^n$
(i.e. the $\mathbb{Z}$ -span of an $\mathbb{R}$ -basis of $\mathbb{R}^n$) with covolume $\frac{1}{2^s} \sqrt{|\operatorname{disc}(K)|}$.

Pf. Let $\alpha_1, \dots, \alpha_n =$ basis of $\mathcal{O}_K$. Its image in $\mathbb{R}^n$ is

$$v_j := (\sigma_1(\alpha_j), \dots, \sigma_r(\alpha_j), \operatorname{Re} \tau_1(\alpha_j), \operatorname{Im} \tau_1(\alpha_j), \dots, \operatorname{Re} \tau_s(\alpha_j), \operatorname{Im} \tau_s(\alpha_j)) \quad j=1, \dots, n$$

& elementary col. operations transform this to a matrix

$$\frac{1}{(2i)^s} \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & \bar{\tau}_1(\alpha_1) & \dots & \tau_s(\alpha_1) & \bar{\tau}_s(\alpha_1) \\ \vdots & & & & & & & \\ \sigma_1(\alpha_n) & \dots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & \bar{\tau}_1(\alpha_n) & \dots & \tau_s(\alpha_n) & \bar{\tau}_s(\alpha_n) \end{pmatrix}$$

& $\det^2 = \frac{1}{2^{2s}} \cdot \operatorname{disc}(K)$. The result follows:

- $\det \neq 0 \Rightarrow$ lattice

- $|\det| =$ covolume of the lattice. □

Covolume of lattice $\Lambda \subseteq \mathbb{R}^n = \operatorname{vol}(\mathbb{R}^n / \Lambda)$

= volume of fundamental parallelepiped F : $\mathbb{R}^n = \bigsqcup_{\lambda \in \Lambda} (F + \lambda)$

$$\left\{ \sum_{i=1}^n a_i v_i : 0 \leq a_i < 1 \right\} \text{ for } v_i = \mathbb{Z}\text{-basis of } \Lambda.$$

Cor. 9. The image of K is dense in $\mathbb{R}^n$.

Now, if $\Delta' \subseteq \Delta$ sublattice, $\Delta/\Delta' = \text{finite group}$ &

$$\text{vol}(\mathbb{R}^n/\Delta') = \text{vol}(\mathbb{R}^n/\Delta) \cdot |\Delta/\Delta'|.$$

Thus, for $I \subseteq \mathcal{O}_K$, get lattice $\Delta_I \subseteq \Delta_K$ &

$$\text{vol}(\mathbb{R}^n/\Delta_I) = \frac{1}{2^s} \sqrt{|\text{disc}(K)|} \|I\|.$$

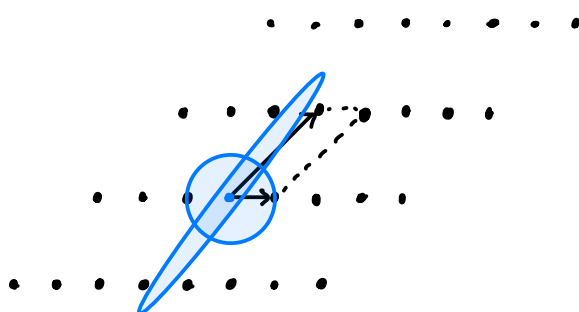
Norm on $\mathbb{R}^n$ obtained from norm on $\mathbb{R}^r \times \mathbb{C}^s$:

$$N(x) = x_1 \cdots x_r (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2).$$

Then for $\alpha \in \mathcal{O}_K$ mapping to $x \in \Delta_K$, $N(x) = N_{K/\mathbb{Q}}(\alpha)$.

Thm 10. Every n -dim'l lattice $\Delta \subseteq \mathbb{R}^n$ contains a nonzero point x with

$$|N(x)| \leq \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^s \text{vol}(\mathbb{R}^n/\Delta).$$



volume?
What radius do I need before
I must hit a lattice point?

Cor. 11. • Every ideal $I \subseteq \mathcal{O}_K$ contains a non-zero α with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\text{disc}(K)|} \cdot \|I\|.$$

• Thm 6.

OK, so it remains to prove Thm 10 now, which is purely about lattices.

Minkowski proved something stronger!

Lemma 12. (Minkowski's Thm). $\Lambda \subseteq \mathbb{R}^n$ lattice

$E \subseteq \mathbb{R}^n$ convex, measurable, centrally symmetric subset with

(1) $\text{vol}(E) > 2^n \cdot \text{vol}(\mathbb{R}^n/\Lambda)$, or

(2) $\text{vol}(E) \geq 2^n \cdot \text{vol}(\mathbb{R}^n/\Lambda)$ & E also compact

$\Rightarrow E \cap (\Lambda \setminus \{0\}) \neq \emptyset$

$$x \in E \Rightarrow -x \in E$$

$$x, y \in E \Rightarrow x - y \in E$$

w.r.t. Lebesgue measure on $\mathbb{R}^n$

closed & bounded

Pf. $F =$ fundamental parallelotope for $\Lambda \Rightarrow \mathbb{R}^n = \bigsqcup_{\lambda \in \Lambda} (\lambda + F)$

$$\Rightarrow \frac{1}{2}E = \bigsqcup_{\lambda \in \Lambda} \left(\frac{1}{2}E \right) \cap (\lambda + F) \quad (\text{intersect with } \frac{1}{2}E)$$

$$\Rightarrow \text{vol}(F) \stackrel{\text{assumption}}{<} \frac{1}{2^n} \text{vol}(E) = \text{vol}\left(\frac{1}{2}E\right) \stackrel{\text{countably additive}}{=} \sum_{\lambda \in \Lambda} \text{vol}\left(\left(\frac{1}{2}E\right) \cap (\lambda + F)\right)$$

$$\text{translate by } \lambda \stackrel{\text{translate by } \lambda}{=} \sum_{\lambda \in \Lambda} \text{vol}\left(\left(\frac{1}{2}E\right) - \lambda \cap F\right)$$

$$\stackrel{\text{If } \frac{1}{2}E - \lambda \text{ all disjoint,}}{=} \text{vol}\left(\bigcup_{\lambda \in \Lambda} \left(\frac{1}{2}E\right) - \lambda \cap F\right) \leq \text{vol}(F) \quad \hookleftarrow$$

Thus $\frac{1}{2}E - \lambda$ not all disjoint; take $\frac{1}{2}E - \lambda$ & $\frac{1}{2}E - \mu$ that intersect.

Then $\lambda - \mu \in \Lambda \setminus \{0\}$ and we claim $\lambda - \mu \in E$:

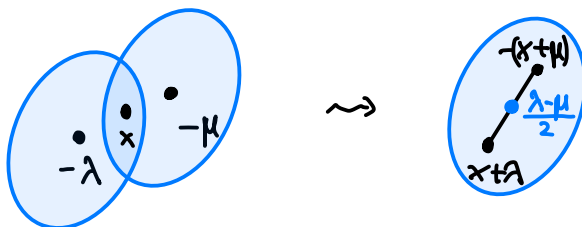
$$x \in \left(\frac{1}{2}E - \lambda\right) \cap \left(\frac{1}{2}E - \mu\right)$$

$$x + \lambda, x + \mu \in \frac{1}{2}E$$

$$x + \lambda, -(x + \mu) \in \frac{1}{2}E \Rightarrow x + \lambda - t(2x + \lambda + \mu) \in \frac{1}{2}E \quad t \in [0, 1]$$

$$\Rightarrow x + \lambda - \frac{1}{2}(2x + \lambda + \mu) = \lambda - \frac{1}{2}(\lambda + \mu) = \frac{1}{2}(\lambda - \mu) \in \frac{1}{2}E$$

$$\Rightarrow \lambda - \mu \in E \quad \checkmark$$



This proves (1). TBC on Wednesday ...

Last time:

- Finiteness of the class group.
- We're trying to prove a better bound (Minkowski bound):
Every ideal class of R contains $\mathfrak{f}$ with $\|\mathfrak{f}\| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\text{disc}(K)|}$.
- We reduced it to a general result about lattices:

Thm 10. Every n -dim'l lattice $\Lambda \subseteq \mathbb{R}^n$ contains a nonzero point x with

$$|N(x)| \leq \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^s \text{vol}(\mathbb{R}^n/\Lambda).$$

- Finally, we proved (1) of the following lemma:

Lemma 12. (Minkowski's Thm). $\Lambda \subseteq \mathbb{R}^n$ lattice
 $E \subseteq \mathbb{R}^n$ convex, measurable, centrally symmetric subset with
 (1) $\text{vol}(E) > 2^n \cdot \text{vol}(\mathbb{R}^n/\Lambda)$, or
 (2) $\text{vol}(E) \geq 2^n \cdot \text{vol}(\mathbb{R}^n/\Lambda)$ & E also compact
 $\Rightarrow E \cap (\Lambda \setminus \{0\}) \neq \emptyset$

Pf of (2). Note that (1) $\Rightarrow \bigcup_{x_m} (1 + \frac{1}{m})E \cap (\Lambda \setminus \{0\}) \neq \emptyset$ for $m=1, 2, \dots$

$\Rightarrow x_m \in \Lambda$ bounded ($\in 2E$) $\Rightarrow$ fin. many distinct x_m b/c Λ is discrete

$\Rightarrow$ some $x \in (1 + \frac{1}{m})E \cap \Lambda$ for ∞ many $m \Rightarrow x \in \overline{E} \Rightarrow x \in E$. □

Cor. 1. Suppose $\exists A = \text{compact, convex, centr. symm. with } \text{vol}(A) > 0$ &

$$a \in A \Rightarrow |N(a)| \leq 1.$$

Then every $\Lambda \subseteq \mathbb{R}^n$ lattice contains $x \neq 0$ with

$$|N(x)| \leq \frac{2^n}{\text{vol}(A)} \cdot \text{vol}(\mathbb{R}^n / \Lambda).$$

Pf. Apply Minkowski's Thm with $E = t \cdot A$ where

$$t^n = \frac{2^n}{\text{vol}(A)} \cdot \text{vol}(\mathbb{R}^n / \Lambda).$$

to get $x = t \cdot a \in \Lambda \setminus \{0\}$, $a \in A$, s.t.

$$|N(x)| = |N(t \cdot a)| = t^n |N(a)| \leq t^n \quad \checkmark.$$

□

Pf of Thm 12.10. We will use Cor. 1 with A defined by

$$|x_1| + \dots + |x_r| + 2(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \dots + \sqrt{x_{r+2s-1}^2 + x_{r+2s}^2}) \leq n.$$

• A is convex Exercise: check this.

• $a \in A \Rightarrow |N(a)| \leq 1$?

$$\sqrt[n]{|N(a)|} \leq \frac{|x_1| + \dots + |x_r| + 2(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \dots + \sqrt{x_{r+2s-1}^2 + x_{r+2s}^2})}{n} \leq 1$$

geometric mean $\leq$ arithmetic mean

• Claim. $\text{vol}(A) = \frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s$. This will prove Thm 12.10.

More generally, for $r, s, t > 0$:

$$V_{r,s}(t) := \text{vol} \left\{ |x_1| + \dots + |x_r| + 2(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \dots + \sqrt{x_{r+2s-1}^2 + x_{r+2s}^2}) \leq t \right\}.$$

Note: $V_{r,s}(t) = t^{r+2s} \cdot V_{r,s}(1) \Rightarrow$ enough to compute

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

If $r > 0$, we have

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

$$\Rightarrow V_{r,s}(1) = \dots = \frac{2^r}{(r+2s)(r+2s-1) \dots (2s+1)} V_{0,s}(1).$$

Next, for $s > 0$, we have

$$\begin{aligned} V_{0,s}(1) &= \iint_{x^2+y^2 \leq \frac{1}{4}} V_{0,s-1}(1-2\sqrt{x^2+y^2}) dx dy \\ &= \int_0^{2\pi} \int_0^{1/2} V_{0,s-1}(1-2r) r dr d\theta \quad (\text{polar coordinates}) \\ &= V_{0,s-1}(1) \cdot 2\pi \cdot \int_0^{1/2} (1-2r)^{2(s-1)} r dr \\ &= V_{0,s-1}(1) \cdot \frac{\pi}{2} \int_0^1 u^{2(s-1)} (1-u) du \quad u = 1-2r \\ &= V_{0,s-1}(1) \cdot \frac{\pi}{2} \left(\frac{1}{2s-1} - \frac{1}{2s} \right) \\ &= V_{0,s-1}(1) \cdot \frac{\pi}{2} \frac{1}{(2s)(2s-1)} \end{aligned}$$

$$\Rightarrow V_{0,s}(1) = \left(\frac{\pi}{2}\right)^s \cdot \frac{1}{(2s)!}.$$



Next: study the unit group $\mathcal{O}_K^\times$.

Example: $K = \mathbb{Q}(\sqrt{m})$.

$$u = a + b\sqrt{m} \in \mathcal{O}_K \text{ is a unit} \Rightarrow N(u) \in \mathbb{Z}^\times = \{\pm 1\} \\ \Rightarrow a^2 - mb^2 = \pm 1.$$

① $m < 0$: finitely many solutions.

E.g. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ (HW 1)

② $m > 0$: infinitely many solutions!

E.g. $(1 + \sqrt{2})(1 - \sqrt{2}) = 1 - 2 = -1 \Rightarrow 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$
has infinite order!

$$\text{In fact, } \mathbb{Z}[\sqrt{2}]^\times = \{\pm 1\} \times \{(1 + \sqrt{2})^k : k \in \mathbb{Z}\} \\ \cong (\text{finite group}) \times \mathbb{Z}.$$

Thm 2. $\mathcal{O}_K^\times \cong W \times V$ where

- $W = \left\{ \text{roots of } 1 \text{ in } K \right\}$, finite group

- $V \cong \mathbb{Z}^{r+s-1}$ i.e. $V = \{u_1^{k_1} \dots u_{r+s-1}^{k_{r+s-1}} : k_i \in \mathbb{Z}\}$
for some $u_1, \dots, u_{r+s-1} \in \mathcal{O}_K^\times$ basis.

Example. $K/\mathbb{Q}$ degree 4 with $r=0 \Rightarrow \mathcal{O}_K^\times = \{\theta \cdot u^k : \theta = \text{root of } 1, k \in \mathbb{Z}\}$

For $K = \mathbb{Q}(\omega_5)$, $\theta = \pm \omega_5^i$ and $u = 1 + \omega_5$.

Want: play the same game as with $\mathcal{O}_K$ above...

Key: log turns $\cdot$ to $+$, so apply $\log|\cdot|$:

$$\mathcal{O}_K^\times \xrightarrow{\log} \mathbb{R}^{r+s}$$

$$u \longmapsto (\log|\sigma_1(u)|, \dots, \log|\sigma_r(u)|, 2\log|\tau_1(u)|, \dots, 2\log|\tau_s(u)|)$$

Note:

$$(1) \log(uv) = \log(u) + \log(v) \Rightarrow \text{group hom.}$$

$$(2) \log(\mathcal{O}_K^\times) \subseteq H \subseteq \mathbb{R}^{r+s} \text{ with } H = \{y_1 + \dots + y_{r+s} = 0\}$$

$$\text{b/c } N(u) = \pm 1 \Rightarrow \log|N(u)| = 0,$$

(3) the map log factors as

$$\begin{array}{ccc} \mathcal{O}_K^\times & \xrightarrow{\log} & \mathbb{R}^{r+s} \quad (\log|x_1|, \dots, \log|x_r|, \log|x_{r+1}^2 + x_{r+2}^2|, \dots, \log|x_{r+2s-1}^2 + x_{r+2s}^2|) \\ \downarrow & & \uparrow \log \\ \mathcal{O}_K \setminus \{0\} & \longrightarrow & \Lambda_K \setminus \{0\} \subseteq \mathbb{R}^{r+2s} \quad x_1, \dots, x_r, x_{r+1}, \dots, x_{r+2s} \end{array}$$

$\Rightarrow$ for $B \subseteq \mathbb{R}^{r+s}$ bounded, $\log^{-1}(B)$ is finite.

Lemma 3. (i) $\ker(\log) = W = \{\text{roots of unity in } K\}$

(ii) $\text{im}(\log) = \text{lattice in } \mathbb{R}^{r+s}$ (not of full rank)

Pf. For (i), use (3): $\ker(\log) = \log^{-1}\{1\}$ finite

$\Rightarrow \ker(\log)$ consists of elts of finite order, i.e. roots of 1;
conversely, any root of 1 is clearly in the kernel.

For (ii), use (3) again: $\log(\mathcal{O}_K^\times)$ has the property that every bounded subset is finite.

Exercise. $G \subseteq \mathbb{R}^m$ s.t. every bounded subset is finite $\Rightarrow G$ is a lattice.

This proves (ii). □

Let $\Lambda_u := \log(\mathcal{O}_K^\times) \subseteq \mathbb{R}^{r+s}$ unit lattice.

Since $\Lambda_u \subseteq H$ by (2) above, $d := \text{rank}(\Lambda_u) \leq r+s-1$.

Moreover, $\mathcal{O}_K^\times \cong W \times V$ with $V \cong \Lambda_u \cong \mathbb{Z}^d$.

Need to prove $d = r+s-1$: many units exist!

First, a random looking lemma, producing elements of $\mathcal{O}_K$.

Lemma 4. For $1 \leq k \leq r+s$, $\alpha \in \mathcal{O}_K$, $\exists \beta \in \mathcal{O}_K$ s.t.

$$\bullet |N_{\mathbb{Q}}^K(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc}(K)|}$$

$$\bullet \log(\alpha) = (a_1, \dots, a_{r+s}), \log(\beta) = (b_1, \dots, b_{r+s})$$

$$\Rightarrow b_i < a_i \quad \forall i \neq k.$$

Pf. Minkowski's Thm 12.12:

Choose $0 < c_i < e^{a_i}$ $i \neq k$, $c_1 \dots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc}(K)|}$

& E defined by $|x_1| \leq c_1, \dots, |x_r| \leq c_r$

$$x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \dots, x_{n-1}^2 + x_n^2 \leq c_{r+s}.$$

Then $\text{vol}(E) = 2^r \pi^s c_1 \dots c_{r+s} = 2^n \text{vol}(\mathbb{R}^n / \Lambda_K)$.

$\Rightarrow E$ contains $x \in \Lambda_K$ non-zero & we take $\beta \in \mathcal{O}_K$ corresp. to it. □

TBC next week!

Last time ...

- Minkowski bound :

$$\left\{ \mathfrak{f} : \|\mathfrak{f}\| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\text{disc}(K)|} \right\} \longrightarrow \text{cl}(K).$$

- Working towards ... Dirichlet unit theorem:

Thm 13.2. $\mathcal{O}_K^\times \cong \{ \text{roots of } 1 \text{ in } K \} \times \mathbb{Z}^{r+s-1}$.

We defined $\log : \mathcal{O}_K^\times \longrightarrow \mathbb{R}^{r+s}$ & showed

$\ker \log = \text{roots of } 1$

$\text{im } \log = \text{lattice of } n_K \text{ } n \leq r+s-1$.

$\Rightarrow$ need $n \geq r+s-1$.

Lemma 13.4. For $1 \leq k \leq r+s$, $\alpha \in \mathcal{O}_K$, $\exists \beta \in \mathcal{O}_K$ s.t.

$$\bullet |N_{\mathbb{Q}}^K(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc}(K)|}$$

$$\bullet \log(\alpha) = (a_1, \dots, a_{r+s}), \log(\beta) = (b_1, \dots, b_{r+s})$$

$$\Rightarrow b_i < a_i \quad \forall i \neq k.$$

We now use this to prove many units exist.

Lemma 1. For $1 \leq k \leq r+s$, $\exists u_k \in \mathcal{O}_K^\times$ s.t.

$$\log(u_k) = (y_1, \dots, y_{r+s}) \text{ s.t. } y_i < 0 \text{ for } i \neq k.$$

Pf. $\alpha_1 \in \mathcal{O}_K \setminus \{0\} \rightsquigarrow \alpha_2 \rightsquigarrow \alpha_3 \rightsquigarrow \dots$
any Lemma 4 Lemma 4

$\Rightarrow$ sequence (α_j) s.t. $\forall i \neq k, \log(\alpha_{j+1})_i < \log(\alpha_j)_i$
 & $N(\alpha_j)$ bounded.

$\Rightarrow \|(\alpha_j)\| = |N(\alpha_j)|$ bounded & $\exists$ finite many ideals with bounded norm

$\Rightarrow (\alpha_j) = (\alpha_h)$ for some $j < h$

$\Rightarrow \alpha_j = u \cdot \alpha_h, u \in \mathcal{O}_K^\times$. This is the unit u_k . □

Overall, get $u_1, \dots, u_{r+s}$ s.t.

$$\log(u_k)_j = \begin{cases} < 0 & j \neq k, \\ > 0 & j = k. \end{cases} \quad \text{b/c } \sum_j \log(u_k)_j = 0$$

Lemma 2. $A = (a_{ij}) \in \mathbb{R}^{m \times m}$ s.t. $a_{ii} > 0, a_{ij} < 0 \ i \neq j$ & $\sum_{i=1}^m a_{ij} = 0$
 $\Rightarrow A$ has rank $m-1$.

Pf. The first $m-1$ columns are linearly independent:

$$t_1 v_1 + \dots + t_{m-1} v_{m-1} = 0, \quad v_j = j^{\text{th}} \text{ column}, t_j \in \mathbb{R} \text{ not all } 0$$

$\Rightarrow$ WLOG assume some $t_k = 1$ & other $t_j \leq 1$

Then look at k^{th} row:

$$0 = \sum_{j=1}^{m-1} t_j a_{kj} \geq \sum_{j=1}^{m-1} a_{kj} > \sum_{j=1}^m a_{kj} = 0. \quad \text{□}$$

This finally proves Thm 13.2 (Dirichlet's unit theorem)!

Know: $\mathcal{O}_K \cong \mathbb{Z}^{2r+s}, \mathcal{O}_K^\times \cong \mathbb{Z}^{r+s+1} \times (\text{finite}),$

$h(K) = |\text{Cl}(K)| < \infty$ & can compute it in practice.

EVALUATIONS:

- LINK ON eCampus
- course ID: V3A4-F4A1-4
- Passwork: nostus 56x90u

Next goal: give a formula for the class number $h := h(K)$.

Q: How are ideals distributed among the classes? $C_1, \dots, C_h$

$$\{I \trianglelefteq \mathcal{O}_K : \|I\| \leq t\}$$

$$\{I \in C_1 : \|I\| \leq t\} \sqcup \dots \sqcup \{I \in C_h : \|I\| \leq t\}$$

$$i(t) := \#\{I : \|I\| \leq t\}, \quad i_C(t) := \#\{I \in C : \|I\| \leq t\}$$

$$\Rightarrow i(t) = i_{C_1}(t) + \dots + i_{C_h}(t).$$

Thm 3. $\exists k$ (dep. on K , but not on C) s.t. $i_C(t) = k \cdot t + O(t^{1-\frac{1}{h}})$.

In particular:

- $\frac{i_C(t)}{t} \rightarrow k$ as $t \rightarrow \infty$

- $i(t) = \boxed{h} \cdot k \cdot t + O(t^{1-\frac{1}{h}})$; so $\frac{i(t)}{t} \rightarrow h \cdot k$ as $t \rightarrow \infty$.

$\hookrightarrow$ This will lead to our formula for h !

Moreover, there is an explicit formula for k .

It will involve the following:

- r, s
- $w = \#W = \#\{\text{roots of } 1 \text{ in } K\}$
- $\text{disc}(K)$
- $\text{reg}(K)$: regulator of K , related to $V \subseteq \mathcal{O}_K^\times$ the free part
 $\underset{\substack{\|V\| \\ \geq r+s-1}}$

To prove the unit theorem, we used $G_K^x \xrightarrow{\log} \mathbb{R}^{r+s}$.

For basis $u_1, \dots, u_{r+s-1}$ of $V \subseteq G_K^x$, and

embeddings $\sigma_1, \dots, \sigma_r, \tau_1, \bar{\tau}_1, \dots, \tau_s, \bar{\tau}_s : K \hookrightarrow \mathbb{C}$,

consider $(r+s-1) \times (r+s)$ matrix

$$M := \begin{pmatrix} \log |\sigma_1(u_1)| & \dots & \log |\sigma_r(u_1)| & 2 \log |\tau_1(u_1)| & \dots & 2 \log |\tau_s(u_1)| \\ \vdots & & & & & \vdots \\ \log |\sigma_1(u_{r+s-1})| & \dots & \log |\sigma_r(u_{r+s-1})| & 2 \log |\tau_1(u_{r+s-1})| & \dots & 2 \log |\tau_s(u_{r+s-1})| \end{pmatrix} \begin{matrix} \rightarrow \text{sum} = 0 \\ \vdots \\ \rightarrow \text{sum} = 0 \end{matrix}$$

(b/c $N(u_i) = 1$)

Def 4. $\text{reg}(K) := |\det(\text{matrix obtained from } M \text{ by removing any column})|$.

Thm 5.
$$h_K = \frac{2^{r+s} \pi^s \text{reg}(K)}{w \cdot \sqrt{|\text{disc}(K)|}}$$

$$\#\{ \|I\| < t \} \sim h_K \cdot h \cdot t \text{ as } t \rightarrow \infty$$

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

• $m < 0 \Rightarrow \text{reg}(K) = 1 \rightsquigarrow h_K = \frac{2\pi}{w \cdot \sqrt{-\text{disc}(K)}} \quad V = \text{trivial}$

• $m > 0 \Rightarrow V = \langle u \rangle$ & we may assume $\sigma_1(u) > 1 \Rightarrow \text{reg}(K) = \log u$
(If $\sigma_1(u) < 1$, replace u by u^{-1} .)

$$w = \{\pm 1\} \rightsquigarrow h_K = \frac{2 \log(u)}{\sqrt{\text{disc}(K)}}.$$

Pts of Tum 3 & 4: Same techniques as Minkowski bound & Dirichlet's unit thm.
We will skip them for now... See Chapter 6 of Marcus.

Goal remains: Formula for h .

Big reveal: the function which will give the formula...

$$\begin{aligned} \text{Def. 6. } \zeta_K(s) &:= \sum_{I \in \mathcal{O}_K} \frac{1}{\|I\|^s} \quad \text{for } \operatorname{Re}(s) > 1 && \text{Dedekind } \zeta\text{-function} \\ &= \sum_{n=1}^{\infty} \frac{j_n}{n^s} && j_n = \#\{I : \|I\| = n\} \end{aligned}$$

Example. $K = \mathbb{Q} \rightsquigarrow \zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$ Riemann ζ -function.

We want to first establish analytic properties of $\zeta_K(s)$.

In general: Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$, $s = x + iy \in \mathbb{C}$, $a_n \in \mathbb{C}$.

Lemma 7. Suppose $\sum_{n \leq t} a_n$ is $O(t^r)$ for some $r \geq 0$.

Then $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $x > r$ & is holomorphic on $\{s \in \mathbb{C} \mid \operatorname{Re}(s) > r\}$.

Corollary 8. $\zeta_K(s)$ converges to a holomorphic function on $\operatorname{Re}(s) > 1$.

Pf. Apply Lemma 7 together with Tum 3. $\square$

Next: extend it a little bit; to $\operatorname{Re}(s) > 1 - \frac{1}{n}$, with a pole at $s = 1$.

10/6

Last time: new topic

- Def. 14.6 $\zeta_K(s) = \sum_I \frac{1}{\|I\|^s}$ for $\operatorname{Re}(s) > 1$.

• Lemma 14.7. $\sum_{n=1}^t a_n = O(t^r) \Rightarrow \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges to hdo. fun. on $\{ \operatorname{Re}(s) > r \}$.

$\Rightarrow$ Cor. 8. $\zeta_k(s)$ defines hdo. function on $\text{Re}(s) > 1$.

Pf of Lemma 14.7.

Enough to show: uniform convergence on compact subsets.

For each s , we estimate the sum $\sum_{n=y}^M \frac{a_n}{n^s}$ by $A_k := \sum_{n=1}^k a_n$:

$$\sum_{n=n_1}^M \frac{a_n}{n^s} = \sum_{n=n_1}^M \left(\frac{A_n - A_{n-1}}{n^s} \right) = \frac{A_{n_1}}{n_1^s} - \frac{A_{n_1-1}}{n_1^s} + \sum_{n=n_1}^{M-1} A_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right)$$

From $O(t^n)$, $\exists B$ s.t. $|A_n| \leq B \cdot n^n \quad \forall n$, so:

$$\left| \sum_{n=n_1}^M \frac{a_n}{h^s} \right| \leq B \left(\frac{M^r}{|M^s|} + \frac{(n-1)^r}{|n^s|} + \sum_{n=n_1}^{M-1} n^r \underbrace{\left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right|} \right)$$

$$\leadsto \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| \leq |s| \int_n^{n+1} \frac{dt}{t^{s+1}} = \int_n^{n+1} \frac{dt}{t^{x+1}} \leq \frac{|s|}{n^{x+1}} \quad (s = x + iy).$$

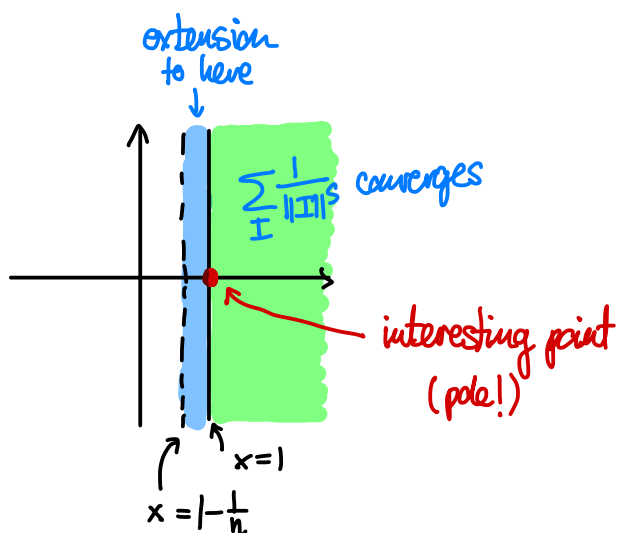
$$\Rightarrow \left| \sum_{n=m}^M \frac{a_n}{n^s} \right| \leq B \left(\underbrace{M^{r-x}}_0 + \underbrace{m^{r-x}}_0 + |s| \underbrace{\sum_{n=m}^{M-1} n^{r-x-1}}_0 \right) \quad \text{for } x > r$$

$$\text{as } M \rightarrow \infty \quad \text{as } n \rightarrow \infty \quad \text{as } n, M \rightarrow \infty$$

b/c

$$\sum_{n=m}^{\infty} n^{r-x-1} \leq \int_{m-1}^{\infty} t^{r-x-1} = \frac{(m-1)^{r-x}}{x-r} \quad (m > 1)$$

Thus, $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for $\sigma > \sigma_c$, uniformly on compact subsets. □



In fact $\zeta_k(s)$ extends to all of $\mathbb{C}$, but this requires more work...

Lemma 1. $\zeta(s)$ extends to $\text{Re}(s) > 0$ to a meromorphic function whose only pole is $s=1$, with residue equal to 1.

Pf. Cute trick! Consider

$$\begin{aligned} f(s) &= 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \dots \quad \text{converges on } \sigma > 0 \text{ by lemma 14.7} \\ &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots - \frac{2}{2^s} \left(1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots \right) \\ &= (1 - 2^{1-s}) \zeta(s) \end{aligned}$$

$$\Rightarrow \zeta(s) = \frac{f(s)}{1 - 2^{1-s}} \quad \text{meromorphic on } \sigma > 0 \text{ with poles at most at } 1 - 2^{1-s} = 0 \leadsto s = 1 + k \frac{2\pi i}{\log 2}, \quad k \in \mathbb{Z}.$$

Residue at $s=1$?

$$f(1) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \dots = \log(2)$$

$$\lim_{s \rightarrow 1} (s-1) \cdot \zeta(s) = \lim_{s \rightarrow 1} \frac{s-1}{1-2^{1-s}} \cdot \log(2) \stackrel{\text{L'Hopital}}{=} \frac{1}{\log 2} \cdot \log 2 = 1.$$

Why doesn't it have the extra poles?

$$g(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \dots \quad \text{conv. for } x > 0 \text{ by Lemma 14.7}$$

$$= (1 - 3^{1-s}) \zeta(s)$$

$$\Rightarrow \zeta(s) = \frac{g(s)}{1 - 3^{1-s}} \quad \text{meromorphic on } x > 0 \text{ \& only c\&mon pole with above is } s = 1.$$

□

Ok, we now proceed with general k , $[k: \mathbb{Q}] = n$.

Thm 2. • $\zeta_k(s)$ meromorphic for $x > 1 - \frac{1}{n}$,
holomorphic except for a simple pole at $s = 1$.

• For $x > 1$, have the expressions:

$$\zeta_k(s) = \sum_{\mathbf{I}} \frac{1}{\|\mathbf{I}\|^s} = \prod_{\mathbf{P}} \left(1 - \frac{1}{\|\mathbf{P}\|^s}\right)^{-1}.$$

• CLASS NUMBER FORMULA:

$$\operatorname{Res}_{s=1} \zeta_k(s) = h(k) \cdot k \quad \text{for } k = \frac{2^{r+s} \pi^s \operatorname{reg}(k)}{w \cdot \sqrt{|\operatorname{disc}(k)|}}.$$

This Dirichlet series knows about the class group, the unit group, ...!

Pf. Recall:

$$\zeta_k(s) = \sum_{n=1}^{\infty} \frac{j_n}{n^s} = \sum_{n=1}^{\infty} \frac{j_n - hk}{n^s} + hk \zeta(s).$$

$$j_n = \#\{\|\mathbf{I}\| = n\}$$

$$\text{Now, } \sum_{n=1}^t j_n - hk = i(t) - thk = O(t^{1-\frac{1}{n}}) \text{ by Thms 14.3 / 14.5}$$

$$\Rightarrow \sum_{n=1}^{\infty} \frac{j_n - hk}{n^s} \text{ converges to a hdo fun. on } x > 1 - \frac{1}{n}.$$

Lemma 14.7

$\Rightarrow \zeta_K(s)$ converges to a mer. fun. on $x > 1 - \frac{1}{n}$, with Lemma 1

$$\operatorname{Res}_{s=1} \zeta_K(s) = 0 + h \cdot K \cdot \operatorname{Res}_{s=1} \zeta(s) = h \cdot K.$$

Finally, we note:

$$\begin{aligned} \prod_{\mathfrak{p}} \left(1 - \frac{1}{\|\mathfrak{p}\|^s}\right)^{-1} &= \prod_{\mathfrak{p}} \left(1 + \|\mathfrak{p}\|^s + \|\mathfrak{p}\|^{2s} + \dots\right)^{-1} \\ &= \prod_{\mathfrak{I}} (\|\mathfrak{I}\|^{-1})^s \end{aligned}$$

is exactly the unique factorization into primes of ideals $\mathfrak{I}$. □

Exercise: sort out convergence issues in final part of the argument.

In other words: $\frac{\zeta_K(s)}{\zeta(s)}$ is holomorphic at $s=1$, and its value is $h \cdot K$.

To make this usable in practice, we will study this quotient shortly (next week).

Today, we give a few other applications of Item 2.

We want to measure "density" of

$$A \subseteq \{\text{primes of } \mathcal{O}_K\}.$$

Given A , define $[A] = \{\mathfrak{I} \trianglelefteq \mathcal{O}_K : \mathfrak{p} \mid \mathfrak{I} \Rightarrow \mathfrak{p} \in A\}$

$$\leadsto \zeta_{K,A}(s) = \sum_{\mathfrak{I} \in [A]} \frac{1}{\|\mathfrak{I}\|^s} = \prod_{\mathfrak{p} \in A} \left(1 - \frac{1}{\|\mathfrak{p}\|^s}\right)^{-1}, \quad \operatorname{Re}(s) > 1 \quad (\text{Lemma 14.7})$$

Def. 3. A has **polar density** $\delta(A) = \frac{m}{n}$ if $\zeta_{K,A}$ extends to a meromorphic function in a nbhd of $s=1$, with pole of order m .

Polar density might not exist! (It means what you think it means...)

Examples. • $A = \{\text{all primes}\} \Rightarrow \zeta_{k,A} = \zeta_k \Rightarrow \delta(A) = 1$ by Thm 2.

• Similarly: $\delta(\{\text{all but fin. many primes}\}) = 1$

• $A = \{\text{finite set}\} \Rightarrow \zeta_{k,A}$ holomorphic $\Rightarrow \delta(A) = 0$

$$\text{Exercise. } \delta(A) = \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in A} \frac{1}{\|\mathfrak{p}\|^s}}{\sum_{\mathfrak{p}} \frac{1}{\|\mathfrak{p}\|^s}} \quad \text{Dirichlet density}$$

Lemma 4. Suppose A contains no $\mathfrak{p}$ s.t. $\|\mathfrak{p}\| \in \mathbb{Z}$ prime. Then $\delta(A) = 0$.

Pf. Claim. $\zeta_{k,A}(s)$ holomorphic for $\text{Re}(s) > \frac{1}{2}$.

$$\zeta_{k,A}(s) = \prod_{\mathfrak{p} \in A} \left(1 - \frac{1}{\|\mathfrak{p}\|^s}\right)^{-1} \quad \begin{array}{l} \& \text{each } \|\mathfrak{p}\| = p^f \quad f \geq 2 \\ \& \text{at most } n \text{ primes above } p \end{array}$$

$$\leq \zeta(2s)^n$$

the sums $\sum_{n \leq t} a_n$ are bounded by the sums for $\zeta(2s)^n$

But $\zeta(2s)$ converges for $s > \frac{1}{2}$ by Lemma 1 $\Rightarrow$ we're done. □

Thm 5. k/F Galois, degree n

$$\delta(\{\text{primes of } F \text{ which split completely in } k\}) = \frac{1}{n}.$$

Example. In a quadratic extension:

• 50% primes split $\left(\frac{m}{p}\right) = +1$

• 0% primes ramify

• 50% primes are inert $\left(\frac{m}{p}\right) = -1$

Exercise. Investigate this for cubic fields!

(HW 9)

Pf of Thm 5.

$$\left. \begin{array}{lcl} K & B = \{ \text{primes above } A \} \ni \mathfrak{B} & \cdot f(\mathfrak{B}/\mathfrak{P}) = 1 \\ n & | & \Rightarrow \|\mathfrak{B}\| = \|\mathfrak{P}\| \\ F & A = \{ \text{split completely} \} \ni \mathfrak{P} & \cdot e(\mathfrak{B}/\mathfrak{P}) = 1 \\ & & \cdot g(\mathfrak{P}) = n \end{array} \right\} \sum_{F,A}^n = \sum_{K,B}$$

$\therefore$ Claim. $\sum_{K,B}$ has a pole of order 1 at $s=1$

Note: if $\mathfrak{B}$ prime of K & $\|\mathfrak{B}\| = \text{prime } p$

$\Rightarrow$ either p ram. in F or $f(\mathfrak{B}/\mathfrak{P}) = 1$ so $e(\mathfrak{B}/\mathfrak{P}) = 1$.

Thus: $\{ \text{primes of } K \} \setminus B = \underbrace{\{ \mathfrak{B} : \|\mathfrak{B}\| \neq \text{prime} \}}_{s=0 \text{ by Lemma 4}} \cup \underbrace{\{ \text{finite set} \}}_{s=0}$

$$\Rightarrow \delta(B) = \delta(\{ \text{primes of } K \}) = 1. //$$

□

Cor. 6. K/F any ext., $M = \text{normal closure}$

$$\Rightarrow \delta(\{ \text{primes of } F \text{ which split comp. in } K \}) = 1/[M:F].$$

Pf. $\mathfrak{P}$ splits comp. in $K \Leftrightarrow \mathfrak{P}$ splits comp. in M .

Cor. 9.4

□

Cor. 7. $H \trianglelefteq \text{Gal}(K/F) \Rightarrow \delta(\{ \mathfrak{P} : \phi_{\mathfrak{B}/\mathfrak{P}} \in H \}) = |H|/|G|.$

Pf. (H normal $\Rightarrow \phi_{\mathfrak{B}/\mathfrak{P}} \in H \Leftrightarrow \phi_{\mathfrak{B}'/\mathfrak{P}} \in H \quad \forall \mathfrak{B}, \mathfrak{B}'/\mathfrak{P}$)

Thm 9.6: Splitting of $\mathfrak{P}$ in K_H determined by Frobenius;

in part.: $\phi_{\mathfrak{B}/\mathfrak{P}} \in H \Leftrightarrow \mathfrak{P}$ splits comp. in H . Ok by Thm 5.

□

E.g. for $K = \mathbb{Q}(\omega_m)$, $F = \mathbb{Q}$:

$$H \leq (\mathbb{Z}/m\mathbb{Z})^\times \rightsquigarrow \delta(\{ p \in \mathbb{Z} : \bar{p} \in H \}) = |H|/\varphi(m).$$

Last time:

- Dedekind ζ -function $\zeta_K(s)$ extends to $\operatorname{Re}(s) > 1 - \frac{1}{n}$ with simple pole at $s=1$.
- Class number formula: $\operatorname{Res}_{s=1} \zeta_K(s) = h \cdot k$, $k = \frac{2^{r+s} \pi^s \operatorname{reg}(K)}{w \cdot \sqrt{|\operatorname{disc}(K)|}}$

In other words, $\beta := \lim_{s \rightarrow 1} \frac{\zeta_K(s)}{\zeta(s)} = h \cdot k$ so $h = \beta/k$.

Question: Can we evaluate β directly?

Answer: Yes, when $K/\mathbb{Q}$ is abelian.

Def 1. For $G = \text{abelian}$, a **character** is a group hom. $\chi: G \rightarrow \mathbb{C}^\times$.

We write $\hat{G} := \{ \chi: G \rightarrow \mathbb{C}^\times \}$ (which also forms a group).

Recall: • for $\mathfrak{p} \mid p$ unram. in $K/\mathbb{Q}$, we defined Frobenius $\phi_{\mathfrak{p}} \in \operatorname{Gal}(K/\mathbb{Q})$ (Def. 9.5)
• for $K/\mathbb{Q}$ abelian, $\phi_p := \phi_{\mathfrak{p}}$ is indep. of $\mathfrak{p} \mid p$.

Def 2. For $K/\mathbb{Q}$ abelian with Galois group G & $\chi: G \rightarrow \mathbb{C}^\times$:

- define $\chi(p) := \chi(\phi_p)$ for $p \nmid \operatorname{disc}(K)$,
- extend to multiplicative fun. $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ with $\chi(n) = 0$ if $(n, \operatorname{disc}(K)) \neq 1$.

Then the **Dirichlet L-function** of χ is defined as:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \nmid \operatorname{disc}(K)} \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} \quad \text{for } \operatorname{Re}(s) > 1$$

(convergent for $\operatorname{Re}(s) > 1$ b/c $\chi(n) = \text{root of unity} \Rightarrow |\chi(n)| = 1$
& use Lemma 14.7 again)

Example. When $K = \mathbb{Q}(\zeta_m)$, $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$,

$$\phi_p \longmapsto p.$$

Thus, we may take $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ Dirichlet character mod m

$\Rightarrow L(s, \chi)$ recovers classical notion of Dirichlet L-function.

(Since by Kronecker-Weber Thm 10.3, any $K/\mathbb{Q}$ abelian in $K \subseteq \mathbb{Q}(\zeta_m)$,
for m , all of our $L(s, \chi)$ are in fact of this form.)

The key result is ...

Thm 3. For $K/\mathbb{Q}$ abelian,

$$\zeta_K(s) = \prod_{\chi \in \hat{G}} L(s, \chi) \cdot \prod_{p \mid \text{disc}(K)} (1 - p^{-f_p s})^{-g_p} \quad \text{for } \text{Re}(s) > 1,$$

where $f_p := f(\mathbb{F}/\mathbb{F}_p)$ for any $\mathbb{F} \mid p$ & $g_p := \#\{\mathbb{F} \mid p\}$.

$$\text{In particular: } \frac{\zeta_K(s)}{\zeta(s)} = \prod_{p \mid \text{disc}(K)} \frac{1 - p^{-s}}{(1 - p^{-f_p s})^{g_p}} \cdot \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} L(s, \chi).$$

Pf. We compare Euler factors at p unramified:

$$\prod_{\mathbb{F} \mid p} (1 - \#\mathbb{F}|p|^{-s})^{-1} = (1 - p^{-f_p s})^{-g_p} \stackrel{?}{=} \prod_{\chi \in \hat{G}} (1 - \chi(p) p^{-s})^{-1}.$$

Note that:

- for $G = \mathbb{Z}/n\mathbb{Z}$ cyclic, $\hat{G} \cong \mu_n = \{n^{\text{th}} \text{ roots of } 1\}$
 $\chi \mapsto \chi(1)$
- for G general, $G = \text{product of cyclic groups } \mathbb{Z}/n_i\mathbb{Z}$,
 $\hat{G} = \text{product of } \mu_{n_i}$.

Recall: $\text{order}(\phi_p) = f_p$ (by def.; see discussion after Def. 9.4).

and $|G| = n = g_p \cdot f_p$ b/c $e_p = 1$ (unramified).

Thus $\chi(p)^{f_p} = \chi(\phi_p)^{f_p} = 1$ i.e. $\chi(\phi_p) \in \mu_{f_p}$, each occurs g_p times.

$$\begin{aligned} \text{Conclusion: } \prod_{\chi \in \hat{G}} (1 - \chi(p) p^{-s})^{-1} &= \prod_{\zeta \in \mu_{f_p}} (1 - \zeta \cdot p^{-s})^{-g_p} \\ &= (1 - p^{-f_p s})^{-g_p} \quad \left(\prod_{\zeta \in \mu_{f_p}} (1 - \zeta x) = 1 - x^{f_p} \right) \end{aligned}$$

For p ramified, $\prod_{p \mid \text{disc}(K)} (1 - p^{-f_p s})^{-g_p}$ is the product of Euler factors of $\zeta_K(s)$.

Finally, for the last claim, note that for $\chi = \text{trivial}$

$$L(s, 1) = \prod_{p \nmid \text{disc}(K)} (1 - p^{-s})^{-1} = \zeta(s) \cdot \prod_{p \mid \text{disc}(K)} (1 - p^{-s}).$$

□

OK, so to control $\beta = \lim_{s \rightarrow 1} \frac{\zeta_K(s)}{\zeta(s)}$, need to study $L(s, \chi)$ at $s=1$ for $\chi \neq 1$.

Lemma 4. For $\chi \neq 1$, $L(s, \chi)$ analytic for $s > 0$.

Pf. Claim. $\chi \neq 1 \Rightarrow \sum_{g \in G} \chi(g) = 0$.

Indeed, let $g_0 \in G$ s.t. $\chi(g_0) \neq 1$, and note

$$\sum_{g \in G} \chi(g) = \sum_g \chi(g_0 g) = \chi(g_0) \cdot \sum_{g \in G} \chi(g). \quad //$$

Thus, $\left| \sum_{n=1}^t \chi(n) \right| \leq \sum_{g \in G} |\chi(g)| = O(1)$ & use Lemma 14.7.

□

Cor. 5. $h = \mathfrak{p}/k$ where

$$\mathfrak{p} = \prod_{\mathfrak{p} | \text{disc}(k)} \frac{1 - \mathfrak{p}^{-1}}{(1 - \mathfrak{p}^{-f_{\mathfrak{p}}})^{\mathfrak{g}_{\mathfrak{p}}}} \cdot \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} L(1, \chi).$$

Finally, we evaluate $L(1, \chi)$ explicitly to get formula for h .

Recall: $k \subseteq \mathbb{Q}(\zeta_m) \Rightarrow \chi \in \hat{G}$ is a character of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Thm 6. $1 \neq \chi : (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ character

$$L(1, \chi) = -\frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \cdot \log(1 - e^{-2\pi i k/m}),$$

$$\text{where } \tau_k(\chi) := \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) \cdot e^{2\pi i a k/m} \quad \text{Gauss sum}.$$

Pf. For $\text{Re}(s) > 1$:

$$\begin{aligned} L(s, \chi) &= \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) \sum_{\substack{\bar{n}=a \\ n \geq 1}} \frac{1}{n^s} \\ &= \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) \sum_{n=1}^{\infty} \frac{\frac{1}{m} \sum_{k=0}^{m-1} e^{2\pi i (\frac{a-n}{m})k}}{n^s} = \begin{cases} 1 & \bar{n}=a \\ 0 & \text{o/w} \end{cases} \\ &= \frac{1}{m} \sum_{k=0}^{m-1} \tau_k(a) \cdot \sum_{n=1}^{\infty} \frac{e^{-2\pi i \frac{nk}{m}}}{n^s}. \end{aligned}$$

$$\text{Now: } \tau_0(a) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) = 0 \quad \text{b/c } \chi \neq 1 \quad (\text{as above})$$

$$\& \text{ for } 1 \leq k \leq m-1, \sum_{n=1}^{\infty} \frac{e^{-2\pi i \frac{nk}{m}}}{n^s} \text{ converges for } \text{Re}(s) > 0 \quad (\text{Lemma 14.7})$$

& its value at $s=1$ is $\sum_{n=1}^{\infty} \frac{e^{-2\pi i \frac{nk}{m}}}{n} = -\log(1 - e^{-2\pi i \frac{k}{m}})$. □

Next: further simplifications!

Def 7. For $d|m$, $(\mathbb{Z}/m\mathbb{Z})^{\times} \twoheadrightarrow (\mathbb{Z}/d\mathbb{Z})^{\times}$ & we say $\chi' \bmod d$ *induces* $\chi \bmod m$ by composition with this map.

$$\begin{array}{ccc} & & \downarrow \chi' \\ & \searrow \chi & \downarrow \chi' \\ & & \mathbb{C}^{\times} \end{array}$$

In this case: $L(1, \chi) = \prod_{\substack{p|m \\ p \nmid d}} \left(1 - \frac{\chi'(p)}{p}\right) \cdot L(1, \chi')$.

Def 8. $\chi \bmod m$ is *primitive* if χ not induced by any $\chi' \bmod d|m$

Lemma 9. If χ is primitive: $\tau_k(\chi) = \begin{cases} \overline{\chi}(k) \cdot \tau_1(\chi) & (k, m) = 1, \\ 0 & \text{o/w} \end{cases}$

Pf. First part is immediate & general:

$$\begin{aligned} \tau_k(\chi) &= \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^{\times}} \chi(a) \cdot e^{2\pi i a k / m} \\ &= \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^{\times}} \chi(a k^{-1}) \cdot e^{2\pi i a / m} \quad (a \mapsto a k^{-1}) \\ &= \overline{\chi}(k) \cdot \tau_1(\chi). \end{aligned}$$

For the second part, note that χ must be non-trivial on

$$\ker((\mathbb{Z}/m\mathbb{Z})^{\times} \rightarrow (\mathbb{Z}/d\mathbb{Z})^{\times}) \quad \forall d|m$$

(else: induced by a char. mod d !).

For $d = m/(k, m)$, we have $\chi(b) \neq 1$ for some $b \equiv 1 \bmod d$, $b \in (\mathbb{Z}/m\mathbb{Z})^{\times}$.

Then $b k \equiv k \bmod m \Rightarrow e^{2\pi i b k / m} = e^{2\pi i k / m}$

$$\begin{aligned}
\Rightarrow \tau_k(\chi) &= \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(a) \cdot e^{2\pi i a k / n} \\
&= \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(ab) e^{2\pi i a b k / n} \quad (a \mapsto ab) \\
&= \chi(b) \tau_k(\chi) \\
\Rightarrow \tau_k(\chi) &= 0.
\end{aligned}$$

□

We write $\tau(\chi) := \tau_1(\chi)$ for simplicity. Then by Thm 6 & Lemma 9 :

$$\begin{aligned}
L(1, \chi) &= - \frac{\tau(\chi)}{n} \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \bar{\chi}(k) \log(1 - \omega^{-k}) \\
&= - \frac{\chi(-1) \tau(\chi)}{n} \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \bar{\chi}(k) \log(1 - \omega^k) \quad (k \mapsto -k)
\end{aligned}$$

Exercise. $\log(1 - \omega^k) = \log 2 + \log \sin \frac{k\pi}{n} + \left(\frac{k}{n} - \frac{1}{2}\right)\pi i.$

$$= - \frac{\chi(-1) \tau(\chi)}{n} \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \bar{\chi}(k) \left(\log \sin \frac{k\pi}{n} + \frac{k\pi i}{n} \right).$$

(because $\sum_k \bar{\chi}(k) = 0$)

Finally : $\chi(-1) = 1 \Rightarrow \sum_k \bar{\chi}(k) k = 0 \quad (k \mapsto -k)$
even

$\chi(-1) = -1 \Rightarrow \sum_k \bar{\chi}(k) \log \sin \frac{k\pi}{n} = 0 \quad (k \mapsto -k)$
odd

$$\text{Thus } L(1, \chi) = \begin{cases} - \frac{\tau(\chi)}{n} \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \bar{\chi}(k) \log \sin \frac{k\pi}{n} & \chi \text{ even,} \\ \frac{\pi i \tau(\chi)}{n^2} \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \bar{\chi}(k) k & \chi \text{ odd.} \end{cases}$$

Exercises. • $|\tau(\chi)|^2 = m$ when $\chi = \text{primitive mod } m$.

• For χ odd, $\sum_{\substack{k \in (\mathbb{Z}/m\mathbb{Z})^\times \\ k < m/2}} \chi(k) k = \frac{m}{\chi(2)-2} \sum_{k < \frac{m}{2}} \chi(k)$.

HW 9.

Overall, get explicit formula:

Thm 10. χ primitive mod $m \geq 3$. Then:

$$|L(1, \chi)| = \begin{cases} \frac{2}{\sqrt{m}} \left| \sum_{\substack{k \in (\mathbb{Z}/m\mathbb{Z})^\times \\ k < m/2}} \chi(k) \log \sin \frac{k\pi}{m} \right| & \chi \text{ even.} \\ \frac{\pi}{|2-\chi(2)|\sqrt{m}} \left| \sum_{\substack{k \in (\mathbb{Z}/m\mathbb{Z})^\times \\ k < m/2}} \chi(k) \right| & \chi \text{ odd.} \end{cases}$$

last time: explicit class number formula

- $h(k) = \mathfrak{f}/k$ for $\mathfrak{f} = \prod_{p \mid \text{disc}(k)} \frac{1-p^{-1}}{(1-p^{-\frac{1}{2}})^{g_p}} \cdot \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} L(1, \chi).$
- for χ induced by $\chi' \bmod d \mid m$: $L(1, \chi) = \prod_{\substack{p \mid m \\ p \nmid d}} \left(1 - \frac{\chi'(p)}{p}\right) \cdot L(1, \chi').$
- for χ primitive:

$$|L(1, \chi)| = \begin{cases} \frac{2}{\sqrt{m}} \left| \sum_{\substack{k \in (\mathbb{Z}/m\mathbb{Z})^\times \\ k < m/2}} \chi(k) \log \sin \frac{k\pi}{m} \right| & \chi \text{ even} \\ \frac{\pi}{|2-\chi(2)|\sqrt{m}} \left| \sum_{\substack{k \in (\mathbb{Z}/m\mathbb{Z})^\times \\ k < m/2}} \chi(k) \right| & \chi \text{ odd} \end{cases}$$

Upshot: really explicit formula for $h(k)$!

Example. The quadratic case: $K = \mathbb{Q}(\sqrt{d})$, $n = |\text{disc}(K)|$, $G = \text{Gal}(K/\mathbb{Q})$
 $\Rightarrow$ can check unique non-trivial $\chi \in \hat{G}$ gives χ is primitive mod m :

$$\chi(p) = \left(\frac{d}{p}\right) = \begin{cases} 1 & d \equiv \square \bmod p \\ -1 & d \not\equiv \square \bmod p \end{cases} \quad p \nmid m \text{ odd},$$

$$\chi(2) = \begin{cases} 1 & d \equiv 1 \pmod{8} \\ -1 & d \equiv 5 \pmod{8} \end{cases} \quad m \text{ odd}.$$

Moreover: $d > 0 \Rightarrow \chi$ even, $d < 0 \Rightarrow \chi$ odd.

Exercise. Check this & deduce the following result.

HW9.

Thm 1. $h := h(\mathbb{Q}(\sqrt{d}))$ is explicitly given by:

$$\frac{1}{\log(u)} \left| \sum_{\substack{k \in (\mathbb{Z}/u\mathbb{Z})^\times \\ k < u/2}} \chi(k) \log \sin \frac{k\pi}{u} \right| \quad d > 0, u = \text{fundamental unit}$$

$$\frac{1}{2 - \chi(2)} \left| \sum_{\substack{k \in (\mathbb{Z}/u\mathbb{Z})^\times \\ k < u/2}} \chi(k) \right| \quad d < 0, d \neq -1, -3.$$

You can really use these to compute h ! (See HW.)

Example.

$$\begin{aligned} \underline{d = -5.} \quad h &= \frac{1}{2} \left| \chi(1) + \chi(3) + \chi(7) + \chi(9) \right| \\ &= \frac{1}{2} \left| \left(\frac{-5}{1}\right) + \left(\frac{-5}{3}\right) + \left(\frac{-5}{7}\right) + \left(\frac{-5}{9}\right) \right| \\ &= \frac{1}{2} \left| 1 + 1 + 1 + 1 \right| \\ &= 2 \quad \text{as expected} \end{aligned}$$

$$\begin{aligned} \underline{d = 2.} \quad h &= \frac{1}{\log(1+\sqrt{2})} \left| \chi(1) \log \sin \frac{\pi}{8} + \chi(3) \log \sin \frac{3\pi}{8} \right| \\ &= \log \left(\frac{\sin \frac{3\pi}{8}}{\sin \frac{\pi}{8}} \right) / \log(1+\sqrt{2}) \\ &= 1 \end{aligned}$$

An introduction to class field theory.

For the explicit class number formula, we used the following:

(1) There's a Frobenius map for m s.t. $p \nmid m \Rightarrow p$ unram. (e.g. $m = \text{disc}(K)$)

$$\phi: \{p \nmid m\} \longrightarrow \text{Gal}(K/\mathbb{Q})$$

$$p \longmapsto \phi_p := \phi_{\mathbb{F}/p} \text{ any } \mathbb{F}/p.$$

& we extended it to $n \in \mathbb{Z}_{\geq 1}$ multiplicatively; we can interpret it as:

$$\phi: I_{\mathbb{Q}}^m := \{n\mathbb{Z} : n \text{ coprime to } m\} \longrightarrow \text{Gal}(K/\mathbb{Q}).$$

(2) This map must have large kernel ... In fact, we recall that $K \subseteq \mathbb{Q}(\zeta_m)$,

and so $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times / H$ and so $\phi(n\mathbb{Z}) \equiv 1$ if $n > 0$ & $n \equiv 1 \pmod{m}$.

Writing $P_{\mathbb{Q}}^{m,0} := \{n\mathbb{Z} : n > 0 \text{ \& } n \equiv 1 \pmod{m}\}$, we in fact get

$$I_{\mathbb{Q}}^m / P_{\mathbb{Q}}^{m,0} \overset{\text{Ex.}}{\cong} (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})} \text{Gal}(K/\mathbb{Q}).$$

If we instead took $P_{\mathbb{Q}}^m := \{n\mathbb{Z} : n \equiv 1 \pmod{m}\}$, then get

$$I_{\mathbb{Q}}^m / P_{\mathbb{Q}}^m \overset{\text{Ex.}}{\cong} (\mathbb{Z}/m\mathbb{Z})^\times / \{\pm 1\}.$$

Goal. Study all abelian extensions of $F = \text{any number field}$.

Def 2. Let $\sigma_1, \dots, \sigma_r: F \hookrightarrow \mathbb{C}$ be the real emb. of F (if any exist).

A modulus is a formal product $m = m_f \cdot m_\infty$ where

where $m_f \trianglelefteq \mathcal{O}_F$ (so $m_f = \prod \mathfrak{p}_i^{n_i}$) and $m_\infty = \sigma_1^{\epsilon_1} \dots \sigma_r^{\epsilon_r}$ for $\epsilon_i \in \{0, 1\}$.

Example: both m & m_∞ are moduli for $F = \mathbb{Q}$.

Def 3. $m = \text{modulus} = m_f m_\infty$

- $I_F^m := \{ \text{a fractional ideal} \cdot a \text{ coprime to } m_f \}$
- $P_F^m := \{ a \in \mathcal{O}_K : a \equiv 1 \pmod{m_f} \text{ \& } \forall \sigma_i | m_\infty, \sigma_i(a) > 0 \}$
 $\underbrace{\sigma_i | m_\infty}_{\epsilon_i = 1}$

Then the ray class group of modulus m is $\mathcal{C}(m) := I_F^m / P_F^m$.

Exercise. Use $|\mathcal{C}(F)| < \infty$ to deduce $|\mathcal{C}(m)| < \infty$.

(HW10)

Exercise. For $F = \mathbb{Q}$, $\mathcal{C}(m) \cong (\mathbb{Z}/m\mathbb{Z})^\times / \{ \pm 1 \}$

$$\mathcal{C}(m_\infty) \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

(HW10)

For $F = \mathbb{Q}$, K/F abelian, $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times / H$ for some H .

If K/F abelian & $m = \text{modulus div. by all ram. primes}$, then have

$$\begin{aligned} \phi : I_F^m &\longrightarrow \text{Gal}(K/F) && \text{Artin map} \\ \mathfrak{P} &\longmapsto \phi_{\mathfrak{P}} := \phi_{\mathfrak{P}/\mathbb{P}} \quad \text{any } \mathfrak{P}/\mathbb{P} \end{aligned}$$

Thm 5. (Artin reciprocity).

- The Artin map is surjective.
 - $\exists m$ s.t. $P_F^m \subseteq \ker(\phi)$.
- $$\Rightarrow \phi : \boxed{I_F^m / P_F^m} \longrightarrow \text{Gal}(K/F)$$

Thus, $\text{Gal}(K/F)$ is isom. to a quotient of $\mathcal{C}(m)$ via ϕ .

Def 6. • A class group C is a quotient $\mathcal{C}(m)/H$.

- A class field for C is an extension K/F such that $\phi : C \xrightarrow{\cong} \text{Gal}(K/F)$.

Thm 7. For any class group, there is a unique class field.

Exercise. K/F abelian, $G = \text{Gal}(K/F)$

- For each $\chi \in \hat{G}$, can define $L(s, \chi)$.
- We have: $\zeta_K(s) = \zeta_F(s) \cdot \prod_{\chi \neq 1} L(s, \chi)$.

Analogue of Thm 16.3.

(HW 10)

Prop: When $m = 1$, note that $\text{Cl}(m) = \text{Cl}(F)$.

Its class field is called the **Hilbert class field**: maximal unram. ext. of F .

Note that $\mathbb{Q}$ has no unram. ext & indeed $\text{Cl}(\mathbb{Q}) = \{1\}$.

Q: Can class fields be constructed explicitly?

(1) $F = \mathbb{Q}$. Yes: Kronecker-Weber theorem.

(2) $F = \mathbb{Q}(\sqrt{m})$, $m < 0$. Yes: theory of complex multiplication.

(3) $F = \text{any other field}$: wide open!

This is Hilbert's 12th problem from Lecture 10.

We will not prove Thms 6 & 7, they are very hard.

References: • Lang, Algebraic Number Theory,

• Neukirch, _____,

• Cox, Primes of the form $x^2 + ny^2$ (for (2) above).

Last time...

- Proved class number formula:

$$h(K) \cdot K = \frac{\zeta_K(s)}{\zeta(s)} \Big|_{s=1}.$$

- Explicitly computed RHS for $K/\mathbb{Q}$ abelian:

$$K \subseteq \mathbb{Q}(\zeta_m) \text{ \& } \frac{\zeta_K(s)}{\zeta(s)} = \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} L(s, \chi), \quad \chi = \text{Dirichlet char. mod } m.$$

Very explicit formula for $K/\mathbb{Q}$ quadratic. (Thm 17.1.)

- Discussed statements of class field theory:

Q: What are all the abelian extensions of F ?

A: They correspond to "class fields".

Application to distributions of primes (Marcus, Chapter 8).

Thm 1 (Chebotarev density). K/F Galois with group G , $\sigma \in G$ fixed

$$\delta \left(\left\{ \mathfrak{p} \text{ prime of } F, \text{ unram. in } K : \phi(\mathfrak{K}/\mathfrak{p}) = \sigma \text{ for some } \mathfrak{K}/\mathfrak{p} \right\} \right) = \frac{|\{\text{conj. of } \sigma\}|}{|G|}.$$

- Proved before class field theory, but modern proof uses it.
- For $K = \mathbb{Q}(\zeta_m) / F = \mathbb{Q}$, recovers Dirichlet's Thm on primes in arithmetic prog.:
for $(a, m) = 1$, $\delta \left(\{ p : p = a + mn \text{ some } n \in \mathbb{N} \} \right) = \frac{1}{m} > 0.$
- Generalizes Thm 15.5: $\frac{1}{n}$ of primes split completely ($\Leftrightarrow \sigma = 1$).
- For cubic fields, can be used to prove all the predictions you made in HW 9 about densities of splittings of primes!

We needed to extend L-functions to study $s=1$. In fact, more is true!

C = class group, $\chi: C \rightarrow \mathbb{C}^\times$ character, $\chi \neq 1$ Hecke character
(+ generalization to ∞ order characters. "Großencharakter").

Thm 2 (Hecke). $L(s, \chi)$ defined for $\operatorname{Re}(s) > 1$ extends to a holomorphic function on $\mathbb{C}$, with functional equation relating s to $1-s$.

This result was later reproved in John Tate's thesis, using a modern approach that gave lots of generalizations.

This will be the subject of Toshio Kakei's seminar next semester.

What's next in the course?

① What about K/F not abelian? Artin representations & L-functions.

Motivation of "Langlands program".

② Local fields: Decomposition group $G_{\mathbb{F}/\mathbb{F}}$ & inertia group $I_{\mathbb{F}/\mathbb{F}}$ should be studied purely locally: "one prime at a time".

③ Local-to-global: arithmetic of number fields (e.g. class groups, L-functions) via local field, using the adeles & ideles.

References for ① : • My notes on Artin L-functions.

• Sorensen, From classical L-functions to modern reciprocity laws.

↳ contains pf of Thm 1 above using L-functions.

Generalization of Dirichlet characters to any Galois extension.

Def 3. K/F Galois, $G = \text{Gal}(K/F)$

An Artin representation is a representation (i.e. group homomorphism)

$$\rho : G \longrightarrow \text{GL}(V_\rho) \cong \text{GL}_n(\mathbb{C}).$$

If K/F abelian & ρ irreducible $\Rightarrow \rho = \chi$ Hecke char. (1-dim'l).

In this case, we defined:

$$L(s, \chi) = \prod_{\mathfrak{p} \text{ unram.}} L_{\mathfrak{p}}(s, \chi), \quad L_{\mathfrak{p}}(s, \chi) := (1 - N_{\mathfrak{p}}^{-s} \chi(\phi_{\mathfrak{p}}))^{-1},$$

where $\phi_{\mathfrak{p}} := \phi_{\mathfrak{K}/\mathfrak{p}}$ for any $\mathfrak{K}/\mathfrak{p}$ (indep. b/c K/F abelian).

Def. 4. For $\mathfrak{p}$ unram. in K/F , let $\phi_{\mathfrak{p}} := \phi_{\mathfrak{K}/\mathfrak{p}}$, any $\mathfrak{K}/\mathfrak{p}$,
and define: $L_{\mathfrak{p}}(s, \rho) := \det(I - N_{\mathfrak{p}}^{-s} \rho(\phi_{\mathfrak{p}}))^{-1}$

Note: $\phi_{\mathfrak{p}}$ defined up to conjugation $\Rightarrow \det$ is well-defined.

What about ramified primes? In HW 5, Exercise 4, we defined:

$$[\phi_{\mathfrak{K}/\mathfrak{p}}] \in G_{\mathfrak{K}}/I_{\mathfrak{K}} \text{ (coset) } (\text{Frobenius}).$$

Claim. Let $V^{I_{\mathfrak{K}}} := \{v \in V : \rho(\sigma)v = v \ \forall \sigma \in I_{\mathfrak{K}}\}$.

Then we can define $\rho([\phi_{\mathfrak{K}/\mathfrak{p}}]) \in \text{GL}(V^{I_{\mathfrak{K}}})$.

Pf. Let $[\phi_{\mathfrak{K}/\mathfrak{p}}] = \phi \cdot I_{\mathfrak{K}}$, $\phi \in G_{\mathfrak{K}}$.

Then for $v \in V^{I_{\mathfrak{K}}}$, $\sigma \in I_{\mathfrak{K}}$:

$$\rho(\sigma) \rho(\phi) v = \rho(\phi) \underbrace{\rho(\phi^{-1} \sigma \phi)}_{\substack{\in I_{\mathfrak{K}} \\ \text{b/c } I_{\mathfrak{K}} \trianglelefteq G_{\mathfrak{K}}}} v = \rho(\phi) v$$

$\Rightarrow$ have a map $\rho(\phi) : V^{\mathbb{I}_{\mathbb{F}}} \longrightarrow V^{\mathbb{I}_{\mathbb{F}}}$ & $\rho([\phi_{\mathbb{F}/\mathbb{F}}]) := \rho(\phi)$.

If $\phi \mathbb{I}_{\mathbb{F}} = \phi' \mathbb{I}_{\mathbb{F}}$, then $\phi^{-1} \phi' \in \mathbb{I}_{\mathbb{F}}$ and

$$\rho(\phi)^{-1} \rho(\phi') = \rho(\phi^{-1} \phi') = \text{id}_{V^{\mathbb{I}_{\mathbb{F}}}} \Rightarrow \text{well-defined.} //$$

Def. 5. For $\mathfrak{p}$ = any prime of F , choose $\mathbb{F}/\mathbb{F}$ above & define:

$$L_{\mathfrak{p}}(s, \rho) := \det(I - \|\mathfrak{p}\|^{-s} \rho([\phi_{\mathbb{F}/\mathbb{F}}]))^{-1}.$$

local factor of the Artin L-function of ρ at $\mathfrak{p}$

(Note: $\mathfrak{p}$ unram. $\Rightarrow \mathbb{I}_{\mathbb{F}} = 1 \Rightarrow V^{\mathbb{I}_{\mathbb{F}}} = V \Rightarrow$ recovers Def. 4.)

Def. 6. The Artin L-function of $\rho : \text{Gal}(K/F) \longrightarrow \text{GL}(V)$ is defined as

$$L(s, \rho) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, \rho).$$

Prop. 7. The product above converges absolutely for $\text{Re}(s) > 1$.

Pf. Enough to take product for $\mathfrak{p}$ unram.

Suppose $\rho(\phi_{\mathbb{F}})$ has eigenvalues $\lambda_{\mathfrak{p},1}, \dots, \lambda_{\mathfrak{p},n}$:

since $\text{order}(\rho(\phi_{\mathbb{F}})) \mid |G|$, $\lambda_{\mathfrak{p},i}$ are roots of unity $\Rightarrow |\lambda_{\mathfrak{p},i}| = 1$.

Moreover, $\det(1 - \|\mathfrak{p}\|^{-s} \rho(\phi_{\mathbb{F}})) = \prod_{i=1}^n (1 - \lambda_{\mathfrak{p},i} \|\mathfrak{p}\|^{-s}).$

Absolute conv. of product is equivalence to abs. conv. of $\ln$, i.e.

$$\sum_{\mathfrak{p} \text{ unram.}} \ln \left(\frac{1}{\det(1 - \rho(\phi_{\mathbb{F}}) \|\mathfrak{p}\|^{-s})} \right) = \sum_{\mathfrak{p} \text{ unram.}} \sum_{i=1}^n \ln \left(\frac{1}{1 - \lambda_{\mathfrak{p},i} \|\mathfrak{p}\|^{-s}} \right)$$

$$= \sum_{\mathfrak{p} \text{ unram.}} \sum_{i=1}^n \sum_{k=1}^{\infty} \frac{\lambda_{\mathfrak{p},i}^k}{k} \|\mathfrak{p}\|^{-ks}$$

& we again use Lemma 14.7

Note: when $\mathcal{P} = \mathcal{K}$ is 1-dimensional (Hecke character),

$$L(\mathcal{P}, s) = L(\mathcal{K}, s).$$

Why are we bothering with these? We will now work towards ...

$$\text{Thm 8. } k/F \text{ Galois} \Rightarrow \frac{\zeta_k(s)}{\zeta_F(s)} = \prod_{\substack{\mathcal{P} \neq 1 \\ \text{ired. rep.} \\ \text{of } \text{Gal}(k/F)}} L(s, \mathcal{P})^{\dim \mathcal{P}}.$$

In particular, for $k/\mathbb{Q}$ non-abelian, class number formulae can be studied using $L(s, \mathcal{P})$ at $s=1$ (if we extend it there ...).

We need some basic properties first ...

Exercise.

- If $\mathcal{P}_1 \cong \mathcal{P}_2$, then $L(s, \mathcal{P}_1) = L(s, \mathcal{P}_2)$
- $L(s, \mathcal{P}_1 \oplus \mathcal{P}_2) = L(s, \mathcal{P}_1) \cdot L(s, \mathcal{P}_2)$ "additive"

(HW10)

$$G \begin{pmatrix} L \\ | \\ H \leq G \\ | \\ K = LH \\ | \\ F \end{pmatrix}$$

Three ways to get reps of G :

- ① For $\rho_0: G \rightarrow GL(W)$, restriction of ρ "from F to k "
 "from $\text{Gal}(L/F)$ to $\text{Gal}(L/k)$ "
 (bottom field increases)
- $$H \hookrightarrow G \xrightarrow{\rho_0} GL(W)$$
- $$\rho := \text{Res}_k^F \rho_0 := \text{Res}_H^G \rho_0$$

- ② If $H \trianglelefteq G$, i.e. k/F Galois, and $\rho_0: \text{Gal}(k/F) \rightarrow GL_n(\mathbb{C})$,
 $G \twoheadrightarrow G/H \xrightarrow{\rho_0} GL_n(\mathbb{C})$

$\rho := \text{Inf}_k^L \rho_0 := \text{Inf}_{G/H}^G \rho_0$ inflation of ρ_0 "from k to L " / "from $\text{Gal}(k/F)$ to $\text{Gal}(L/F)$ "
 (top field increases)

Prop 9. $L(\text{Inf}_K^L \rho_0, s) = L(\rho_0, s).$

Pf. Exercise. (HW 10). $\square$

Cor 10. Suppose $\rho: \text{Gal}(K/F) \rightarrow \mathbb{C}^\times$ is a 1-dimensional Artin rep.
Then $L(\rho, s)$ is a Hecke L-function.

Pf. $G \xrightarrow{\rho} \mathbb{C}^\times \Rightarrow \rho = \text{Inf } \chi$ where χ is a character
of an abelian ext. $M/\mathbb{Q}$, $M := M_{[G, G]}$.
 $G^{\text{ab}} =: G/[G, G] \xrightarrow{\chi} \mathbb{C}^\times$

$\square$

③ For any $H \leq G$ & $\rho_0: H \rightarrow \text{GL}(W)$

induction of ρ_0 : $\text{Inf}_H^G \rho_0 := \text{Inf}_K^F \rho_0 := \text{GL}(V)$

"from $\text{Gal}(L/K)$ to $\text{Gal}(L/F)$ "
"from K to F "

$$V = \{ f: G \rightarrow W : f(hx) = \rho_0(h) f(x) \ \forall h \in H, x \in G \}$$

(bottom field increases)

w/ action of G on V : $\rho(g) f(x) = f(xg).$

(Exercise. $\dim V = [G:H] \cdot \dim W.$)

Prop 11. $L(\text{Inf}_K^F \rho_0, s) = L(\rho_0, s).$

Last time:

- Artin rep. $\rho: \text{Gal}(K/F) \longrightarrow \text{GL}_n(\mathbb{C}) \rightsquigarrow L(\rho, s)$ Artin L-function
- Aiming to prove ... (Thm 18.8)

$$\zeta_K(s) = \zeta_F(s) \cdot \prod_{\substack{\rho \neq 1 \\ \text{irred.}}} L(s, \rho)^{\dim \rho} = \prod_{\rho \text{ irred.}} L(s, \rho)^{\dim \rho}.$$

A crash course on representations of finite groups.

$G =$ finite group

Def 1. A **representation** of G is a pair (ρ, V)

- $V =$ f.d. complex vector space,
- $\rho: G \longrightarrow \text{GL}(V)$ homomorphism

Its **dimension** is $\dim(V)$.

• Often, you just call V or ρ the representation of G .

• When $\dim V = n$ & you choose a basis:

$$\text{GL}(V) \cong \text{GL}_n(\mathbb{C}).$$

Examples.

- 1-dim'l reps are characters $\chi: G \longrightarrow \mathbb{C}^\times$
(they always factor through G^{ab}).

- $G = S_3$, $V = \mathbb{C}^3$, $\rho: S_3 \longrightarrow \text{GL}(V)$ by permuting the axes
 $\sigma \longmapsto (e_i \mapsto e_{\sigma(i)})$

Then $U := \left\{ \begin{pmatrix} x \\ x \\ x \end{pmatrix} \right\} = \text{span}\{e_1 + e_2 + e_3\}$ is preserved by S_3 ,

$W := \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : x+y+z=0 \right\} = \text{span}\{e_1 - e_2, e_2 - e_3\}$ is preserved by S_3 ,

and hence $V \cong U \oplus W$ as representations of S_3 !

Note: because $(123)(e_1 - e_2) = (e_2 - e_3)$, W has no invariant subspace.

Def 2. • Given reps V, W of G , the **direct sum** $V \oplus W$ is a rep. of G
 • A rep. V is **irreducible** if it contains no subspace $0 \subsetneq W \subsetneq V$ invariant under G (**subrepresentation**).

Thm 3. Any rep. V of G admits a decomposition
 $V \cong V_1 \oplus \dots \oplus V_r$ into irreducible reps V_i .

As above
for S_3 !

Three ways to get new reps:

- **Restriction** to $H \leq G$: given (ρ, V) rep. of G , the composition:

$$\begin{array}{ccc} H & \hookrightarrow & G \xrightarrow{\rho} GL(V) \\ & \searrow & \uparrow \\ & & \text{Res}_H^G \rho \end{array}$$

- **Inflation** from $G \twoheadrightarrow G/H$: given (ρ, V) rep. of G/H , the composition:

$$\begin{array}{ccc} G & \twoheadrightarrow & G/H \xrightarrow{\rho} GL(V) \\ & \searrow & \uparrow \\ & & \text{Inf}_{G/H}^G \rho \end{array}$$

- **Induction** from $H \leq G$: given (ρ, V) rep. of H , define

$$\bullet \text{Ind}_H^G V := \{ f: G \rightarrow V : f(hx) = \rho(h) f(x) \quad \forall h \in H, x \in G \}$$

$$\bullet \text{Ind}_H^G \rho : G \longrightarrow GL(\text{Ind}_H^G V)$$

$$g \longmapsto (f \longmapsto f g)$$

$$f g(x) := f(xg).$$

Note: • $f g(hx) = f(hxg) = \rho(h) f(xg) = \rho(h) f g(x)$ ✓

$$\bullet \dim \text{Ind}_H^G V = [G:H] \cdot \dim V.$$

Example. The irred. 2-dim'l rep. W of S_3 is actually ism. to $W \cong \text{Ind}_{\langle (123) \rangle}^{S_3} \chi$, $\chi((123)) = e^{2\pi i/3}$.

Exercise. Check this. (HW 11.)

Finally, need to know some interactions between them.

Thm 4. (Frobenius Reciprocity).

$$\text{Hom}_G(\text{Ind}_H^G W, V) \cong \text{Hom}_H(W, \text{Res}_H^G V).$$

(Ind & Res are adjoint functors)

Thm 5. (Schur's Lemma).

$$V, W \text{ irreducible} \Rightarrow \dim \text{Hom}_G(V, W) = \begin{cases} 1 & V \cong W \\ 0 & V \not\cong W \end{cases}$$

Cor. 6. $\text{Ind}_{\{e\}}^G \mathbb{1} \cong \bigoplus_{V \text{ irred.}} V^{\oplus \dim V}$.

In particular, $|G| = \sum_{V \text{ irred.}} (\dim V)^2$.

Exercise. Use this to classify all irreps of S_3 .

$$6 = \underset{\mathbb{1}}{1} + \underset{\chi}{1} + \underset{W}{2^2} \quad \ddots$$

Finally, we need to know how induction interacts with restriction.

Def. 7. $\rho : H \rightarrow GL(V)$ rep. of $H \leq G$, $\sigma \in G$

$\rightarrow \sigma_* \rho : \sigma^{-1} H \sigma \rightarrow GL(\sigma_* V)$ *conjugate representation*

is $\sigma_* V := V$ w/ action given by

$$\sigma^{-1} H \sigma \xrightarrow{\cong} H \xrightarrow{\rho} GL(V)$$

$$\tau \longmapsto \sigma \tau \sigma^{-1}$$

Thm 8. (Mackey decomposition). $\Gamma, H \leq G$ and suppose

$$H \backslash G / \Gamma = \{ H \sigma_1 \Gamma, \dots, H \sigma_g \Gamma \}.$$

$$\Rightarrow \text{Res}_{\Gamma}^G \text{Ind}_H^G \rho \xrightarrow{\cong} \bigoplus_{i=1}^g \text{Ind}_{\Gamma \cap \sigma_i^{-1} H \sigma_i}^{\Gamma} (\sigma_{i,*} \rho)$$

$$f \longmapsto (f \sigma_1, \dots, f \sigma_g)$$

$$f^{\sigma_i}(\gamma) := f(\sigma_i \gamma) \text{ for } \gamma \in \Gamma$$

We're ready to do Artin reps again!

$$\rho: \text{Gal}(K/F) \rightarrow GL(V) \text{ Artin rep.}$$

$$\leadsto L(s, \rho) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, \rho), \text{Re}(s) > 1 \text{ Artin } L\text{-function}$$

$$\text{Then: } \bullet \rho_1 \cong \rho_2 \Rightarrow L(s, \rho_1) = L(s, \rho_2)$$

$$\bullet L(s, \rho_1 \oplus \rho_2) = L(s, \rho_1) \cdot L(s, \rho_2)$$

$$\bullet L(s, \text{Ind}_{G/H}^G \rho) = L(s, \rho) \text{ for } G \left(\begin{array}{c} L \\ \vdots \\ 1 \\ \vdots \\ k \\ \vdots \\ 1 \\ \vdots \\ F \end{array} \right)^H \text{ all Galois}$$

Exercises!

$$\text{Prop 18.11. } L(s, \text{Ind}_H^G \rho) = L(s, \rho) \text{ for } G = \text{Gal}(L/F), H = \text{Gal}(L/K).$$

Pf. We want to check this for Euler factors at $\mathfrak{p}$ for all $\mathfrak{p}$.

Choose $\mathbb{F} / \mathfrak{f}$ in L/F & recall that

$$\phi_{\mathfrak{f}} := \phi_{\mathbb{F}/\mathfrak{f}} \in G_{\mathbb{F}} / I_{\mathbb{F}} \text{ acts on } (\text{Ind } V)^{I_{\mathbb{F}}}.$$

$$\begin{aligned} \leadsto L_{\mathfrak{f}}(s, \text{Ind } \rho) &:= \det(1 - \phi_{\mathfrak{f}} \|_{\mathbb{F}}^{-s}; (\text{Ind } V)^{I_{\mathbb{F}}}) \\ &= \det(1 - \phi_{\mathfrak{f}} \|_{\mathbb{F}}^{-s}; (\text{Res}_{G_{\mathbb{F}}} \text{Ind } V)^{I_{\mathbb{F}}}). \end{aligned}$$

Hence we will apply Mœchey's decomp. thm (Thm 8).

$$H \backslash G / G_{\mathbb{F}} = \{ H \sigma_1 G_{\mathbb{F}}, \dots, H \sigma_g G_{\mathbb{F}} \}$$

$$\rightarrow \text{Res}_{G_{\mathbb{F}}} \text{Ind } \rho = \bigoplus_{i=1}^g \text{Ind}_{G_{\mathbb{F}} \cap \sigma_i^{-1} H \sigma_i}^{G_{\mathbb{F}}} (\sigma_i)_* \rho.$$

$$= \bigoplus_{i=1}^g (\sigma_i)_* \left(\text{Ind}_{\sigma_i G_{\mathbb{F}} \sigma_i^{-1} \cap H}^{\sigma_i G_{\mathbb{F}} \sigma_i^{-1}} \rho \right)$$

$$\text{Now, } \sigma_i G_{\mathbb{F}} \sigma_i^{-1} = G_{\mathbb{F}_i}, \quad \sigma_i I_{\mathbb{F}} \sigma_i^{-1} = I_{\mathbb{F}_i}, \quad \sigma_i \phi_{\mathbb{F}/\mathbb{F}} \sigma_i^{-1} = \phi_{\mathbb{F}_i/\mathbb{F}}.$$

Therefore, we get:

$$L_{\mathbb{F}}(s, \text{Ind } \rho) = \prod_{i=1}^g \det \left(1 - \phi_{\mathbb{F}_i/\mathbb{F}} \|\rho\|^{-s}; \left(\text{Ind}_{G_{\mathbb{F}_i} \cap H}^{G_{\mathbb{F}_i}} \rho \right)^{I_{\mathbb{F}_i}} \right)$$

The key result is Exercise 4 from Sheet 5.

$$\begin{aligned} H \backslash G / G_{\mathbb{F}} &\xleftrightarrow{'1-1'} \{ \text{primes } \mathfrak{q} \text{ of } k \text{ above } \mathbb{F} \}, \\ H \sigma_i G_{\mathbb{F}} &\longmapsto \mathfrak{q}_i := \mathbb{F}_i \cap k. \end{aligned}$$

Thus the Euler factors on RHS are:

$$L_{\mathfrak{q}_i}(s, \rho) = \det \left(1 - \phi_{\mathbb{F}_i/\mathfrak{q}_i} \|\rho\|^{-s}; \rho^{I_{\mathbb{F}_i/\mathfrak{q}_i}} \right).$$

Moreover, recall that $\phi_{\mathbb{F}_i/\mathbb{F}}^{\mathfrak{f}_i} = \phi_{\mathbb{F}_i/\mathfrak{q}_i}$, $\|\rho\| = \|\rho\|^{\mathfrak{f}_i}$ for $\mathfrak{f}_i = \mathfrak{f}(\mathfrak{q}_i/\mathbb{F})$.

Claim. $\det \left(1 - \phi_i t; \left(\text{Ind}_{G_{\mathfrak{q}_i}}^{G_{\mathbb{F}_i}} \rho \right)^{I_{\mathbb{F}_i}} \right)$

$$= \det \left(1 - \phi_i^{\mathfrak{f}_i} t; \rho^{I_{\mathfrak{q}_i}} \right).$$

$$G_{\mathfrak{q}_i} = G_{\mathbb{F}_i} \cap H$$

$$\phi_i := \phi_{\mathbb{F}_i/\mathbb{F}}$$

Another application of Mackey (Thm 8):

$$G_{q_i} \backslash G_{\mathbb{F}_i} / I_{\mathbb{F}_i} \xleftrightarrow{(1)} \{ 1, \phi_i, \dots, \phi_i^{f_i-1} \}$$

$$\left(\text{Ind}_{G_{q_i}}^{G_{\mathbb{F}_i}} V \right)^{I_{\mathbb{F}_i}} = \left(\bigoplus_{i=0}^{f_i-1} (\phi_i)_* V \right)^{I_{\mathbb{F}_i}} = \bigoplus_{i=0}^{f_i-1} V^{I_{q_i}}$$

~> What is the matrix of ϕ_i acting on this direct sum?

$$\begin{bmatrix} 0 & I & & \\ & 0 & I & \\ & & \ddots & \\ A & & & 0 \end{bmatrix} \quad A = \text{matrix of } \phi_i^{f_i} \text{ acting on } V^{I_{q_i}}$$

Thus in Claim:

$$\text{LHS} = \det \begin{pmatrix} I & -tI & & \\ & I & -tI & \\ & & \ddots & -tI \\ -At & & & I \end{pmatrix} = \det(I - A \cdot t^{f_i}) = \text{RHS}.$$

□

Pf of Thm 18.8.

$$\zeta_L(s) \stackrel{18.11}{=} L(s, \text{Ind}_{\mathbb{F}_1 \mathbb{F}_2}^G \mathbb{1}) \stackrel{\text{Cor. 6}}{=} L(s, \bigoplus_{\mathfrak{p} \text{ ir.}} \mathfrak{p}^{\dim \mathfrak{p}}) = \prod_{\mathfrak{p} \text{ ir.}} L(s, \mathfrak{p})^{\dim \mathfrak{p}}$$

$$= \zeta_k(s) \cdot \prod_{\substack{\mathfrak{p} \neq 1 \\ \text{red.}}} L(s, \mathfrak{p})^{\dim \mathfrak{p}}.$$

□

Next time: Can $L(s, \mathfrak{p})$ be continued to a holo. fun. on $\mathbb{C}$?

Last time:

$$\zeta_K(s) = \zeta_F(s) \cdot \prod_{\mathfrak{p} \neq 1} L(s, \rho), \quad \rho \text{ irrep. of } \text{Gal}(K/F)$$

For $K/\mathbb{Q}$ any Galois extension,

$$h_K \cdot K = \lim_{s \rightarrow 1} \frac{\zeta_K(s)}{\zeta(s)} = \prod_{\mathfrak{p} \neq 1} L(1, \rho)$$

if we can analytically continue $L(s, \rho)$.

Artin's initial idea was to reduce to the abelian case.

Tool from representation theory:

 α representation ρ of G is determined by its **character**

$$G \ni g \longmapsto \chi_\rho(g) := \text{Tr}(\rho(g)) \in \mathbb{C}.$$

Note: $\chi_{\rho_1 \oplus \rho_2} = \chi_{\rho_1} + \chi_{\rho_2}$,• we write $\text{Ind}_H^G \chi_\rho := \chi_{\text{Ind}_H^G \rho}$.• if $\dim \rho = 1$, $\chi_\rho(g) = \rho(g)$ (the character of a character is the character).Thm 1 (Brauer). For each $\rho : G \rightarrow \text{GL}(V)$ rep., $\exists$ abelian subgroups H_i , characters $\chi_i \in \hat{H}_i$, $a_i \in \mathbb{Z}$ s.t.

$$\chi_\rho = \sum_i a_i \cdot \text{Ind}_{H_i}^G \chi_i.$$

Cor 2 (Artin). Any Artin L-function is a ratio of Hecke L-functions:

$$L(s, \rho) = \prod_i L(s, \chi_i)^{a_i}, \quad \chi_i = \text{Hecke character}$$

Pf. Combine Brauer's Thm 1 w/ Prop. 18.11. $\square$

Cor 3 (Artin). $L(s, \rho)$ admits meromorphic continuation to $s \in \mathbb{C}$.

Pf. Combine Thm 2 w/ Hecke's Thm 18.2.

(Only meromorphic because $a_i \in \mathbb{Z}$.) $\square$

- In fact, we know that $L(1, \chi) \neq 0$ for $\chi =$ Hecke characters:
and hence deduce:

$$L(1, \rho) = \prod_i L(1, \chi_i)^{a_i} \text{ is well-defined \& non-zero.}$$

However, since H_i, χ_i, a_i are generally not explicit, it is hard to get an explicit CNF this way...

- Nonetheless, can deduce Chebotarev Density Thm (Thm 18.1)
(see Sorensen's book.)
- One of the biggest open problems in number theory is...

Conj. (Artin). $L(s, \rho)$ for $\rho \neq 1$ is holomorphic on $\mathbb{C}$.

What is the Langlands program?

For K/F abelian, we use class field theory:

characters of $\text{Gal}(K/F) \leftrightarrow$ characters of ray class fields,

———— $\text{Gal}(K/\mathbb{Q}) \leftrightarrow$ Dirichlet characters.

Can we make this non-abelian?

① Class fields can be interpreted in terms of the ring A_F of adèles.

(A lot about them is Kolyva's seminar next semester!)

$$\leadsto \chi: \underbrace{\text{Gal}(K/F)}_{\text{abelian}} \longrightarrow \underbrace{\mathbb{C}^\times}_{\text{GL}_1(\mathbb{C})} \longleftrightarrow \pi: \text{GL}_1(A_F) \longrightarrow \underbrace{\mathbb{C}^\times}_{A_F^\times}$$

② Maybe ...

$$\rho: \text{Gal}(K/F) \longrightarrow \text{GL}_n(\mathbb{C}) \overset{??}{\longleftrightarrow} \text{representations } \pi \text{ of } \text{GL}_n(A_F)$$

"automorphic representations"

$$\text{s.t. } L(\rho, s) = L(\pi, s).$$

This is (a part of) the Langlands program.

③ Thm (Godement-Jacquet, 1971). $L(\pi, s)$ admits hol. cont. to $\mathbb{C}$.

Thus ② would prove Artin's conj.!

What do we know for $n=2$?

Suppose $\rho: \text{Gal}(K/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{C})$ irred. is "odd"

$$\det(\rho(\text{complex conj.})) = -1.$$

Thm (Deligne-Wintenberger, 2008).

$\exists$ modular form f of wt 1 s.t. $L(\rho, s) = L(f, s)$.

In particular, $L(\rho, s)$ is holomorphic on $\mathbb{C}$.

(Serre's conjecture.)

Learning seminar next semester (by me!):

modular forms & elliptic curves.

(Maybe also this at the end...)

Homework 11: all about Artin reps of $\text{Gal}(K/\mathbb{Q}) \cong S_3$.

In particular, you'll prove

- Artin's conjecture in this case,
 - some consequence of all this for class numbers.
-

The rest of the course: completions & local fields.

References: • Neukirch, Algebraic Number Theory, Chapter II
• Lang, Algebraic Number Theory, Chapter II

Main idea: pick your favourite prime p of K & "focus on it".

§ The p -adic numbers. $p = \text{prime}$, fixed

Idea: Write numbers as a power series in p :

$$f \in \mathbb{N} \leadsto f = a_0 + a_1 p + a_2 p^2 + \dots + a_n p^n \quad \text{"polynomial in } p"$$
$$a_i \in \{0, 1, \dots, p-1\} = \mathbb{F}_p$$

Computed using division by p with remainder:

$$f = a_0 + p f_1$$

$$f_1 = a_1 + p f_2$$

$$\vdots$$

$$f_{n-1} = a_{n-1} + p f_n$$

$$f_n = a_n$$

Notation: $f = a_0, a_1, a_2 \dots a_n$.

Example.

$216 = 0,0011011$	(2-adic)	$216 = 2^3 + 2^4 + 2^6 + 2^7$
$216 = 0,0022$	(3-adic)	$216 = 2 \cdot 3^3 + 2 \cdot 3^4$
$216 = 1,331$	(5-adic)	$216 = 1 + 3 \cdot 5 + 3 \cdot 5^2 + 5^3$

How would we write down -1 this way?

$$\begin{aligned}
 -1 &= (p-1) + p \cdot (-1) \\
 -1 &= (p-1) + p \cdot (-1) \quad \leadsto \quad -1 = p-1 + (p-1)p + (p-1)p^2 + \dots \\
 -1 &= (p-1) + p \cdot (-1) \quad (p-1), (p-1)p, (p-1)p^2, \dots \text{ infinite series!} \\
 &\vdots
 \end{aligned}$$

Def. 4. A p -adic integer is a formal infinite series

$$a_0 + a_1 p + a_2 p^2 + \dots \quad a_i \in \{0, 1, \dots, p-1\}.$$

Their set is denoted by $\mathbb{Z}_p$.

Prop 5. The residue classes $a \in \mathbb{Z}/p^n\mathbb{Z}$ can be uniquely rep. as

$$\begin{aligned}
 a &= a_0 + a_1 p + a_2 p^2 + \dots + a_{n-1} p^{n-1} \pmod{p^n} \\
 a_i &\in \{0, 1, \dots, p-1\}.
 \end{aligned}$$

Pf. Induction on n :

- Clear for $n=1$.
- Assume for $n-1$. Then $a \equiv a_0 + a_1 p + \dots + a_{n-2} p^{n-2} \pmod{p^{n-1}}$ (unique)
 $\Rightarrow a = a_0 + a_1 p + \dots + a_{n-2} p^{n-2} + q p^{n-1}$, some $q \in \mathbb{Z}$ (unique)
 & if $q \equiv a_{n-1} \pmod{p}$, this a_{n-1} is uniquely determined & works. $\square$

Thus, there is a map $\mathbb{Z} \rightarrow \mathbb{Z}_p$:

$f \mapsto$ its p -adic expansion.

Def. 6. The set of p -adic numbers $\mathbb{Q}_p$ consists of "Laurent series in p "

$$\sum_{v=-m}^{\infty} a_v p^v = a_{-m} p^{-m} + \dots + a_{-1} p^{-1} + a_0 + a_1 p + \dots$$

Then there is a canonical mapping

$$\mathbb{Z}_{(p)} \longrightarrow \mathbb{Z}_p$$

$$\cap \quad \cap$$

$$\mathbb{Q}_{(p)} \longrightarrow \mathbb{Q}_p$$

$$(p, gh) = 1 \quad p^{-m} \frac{g}{h} = f \longmapsto p^{-m} (p\text{-adic exp. of } \frac{g}{h})$$

Example. $\frac{1}{1-p} = 1 + p + p^2 + \dots$

To define addition & mult. of p -adic numbers, think instead about compatible sequences of res. classes mod p^n

Cor. 7. There is an isomorphism:

$$\mathbb{Z}_p \xrightarrow{\cong} \varprojlim_n \mathbb{Z}/p^n \mathbb{Z}$$

$$f = \sum_{v=0}^{\infty} a_v p^v \longmapsto (\overline{s}_n)_{n \in \mathbb{N}}, \quad \overline{s}_n := \sum_{v=0}^{n-1} a_v p^v \pmod{p^n}$$

In particular, $\mathbb{Z}_p$ is a ring & $\mathbb{Q}_p = \text{Frac}(\mathbb{Z}_p)$ is a field.

Pf. Apply Prop. 5 for both surjectivity (existence) & injectivity (uniqueness). $\square$

Application. Diophantine equations:

Does $F(x_1, \dots, x_n) = 0$ for $F \in \mathbb{Z}[x_1, \dots, x_n]$ have an integer solution?

Weaken this by asking: does $F \equiv 0 \pmod{m}$ have a solution mod m for all m ?

Chinese remainder theorem: $\Leftrightarrow F \equiv 0 \pmod{p^v}$ has a solution $\forall v, p$.

Prop. 8. $F \equiv 0 \pmod{p^v}$ has a solution $\forall v \geq 1$

$\Leftrightarrow F = 0$ has a solution in $\mathbb{Z}_p$.

Pf. Exercise using

Cor. 7. $\square$

§ The p -adic absolute value.

<u>p-adic expansion</u>	<u>vs.</u>	<u>decimal expansion</u>
$a_0 + a_1 p + a_2 p^2 + \dots$	$p \longleftrightarrow \frac{1}{10}$	$a_0 + a_1 \left(\frac{1}{10}\right) + a_2 \left(\frac{1}{10}\right)^2 + \dots$
$a_i \in \{0, \dots, p-1\}$		$a_i \in \{0, \dots, 9\}$
does <u>not</u> converge classically b/c $ p > 1$		converges classically b/c $ \frac{1}{10} < 1$

Idea: introduce a different absolute value which makes p small!

Def 9. • Write $\mathbb{Q}^* \ni a = p^m \cdot \frac{b}{c}$, $m \in \mathbb{Z}$, $p \nmid b, c$ & define

p -adic abs. value $|a|_p = p^{-m}$ (e.g. $|p|_p = p^{-1} < 1$).
 $|0|_p = 0$

• Also define

p -adic valuation $v_p(a) = m \rightsquigarrow |a|_p = p^{-v_p(a)}$.
 $v_p(0) = \infty$

Note: $|\cdot|_p$ is a (non-archimedean) norm on $\mathbb{Q}$:

(1) $|a|_p = 0 \Leftrightarrow a = 0$

(2) $|ab|_p = |a|_p |b|_p$

(3) $|a+b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$
non-archimedean norm

One can show: any norm on $\mathbb{Q}$ is $|\cdot|^s$ or $|\cdot|_p^s$ for some $s > 0$.

Write $|\cdot| = |\cdot|_\infty$ to make notation clear.

Last time:

• Introduced $\mathbb{Z}_p = \{ \text{formal power series } \sum_{v=0}^{\infty} a_v p^v, a_v \in \{0, \dots, p-1\} \} \cong \mathbb{Z}$
 (Hensel's def.) $\cong \varprojlim_{n \in \mathbb{N}} (\mathbb{Z}/p^n \mathbb{Z})$ (p -adic integers)

$\mathbb{Q}_p = \{ \text{Laurent series} \} = \text{Frac}(\mathbb{Z}_p)$ (p -adic numbers)

• Introduced $|\cdot|_p = p$ -adic absolute value on $\mathbb{Q}$,
 $|\cdot|_{\infty} = |\cdot| = \text{usual absolute value}.$

Another way to define $\mathbb{Q}_p$: completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$.
 (Kürschale)

$R := \{ \text{Cauchy sequences } (x_n) \text{ in } \mathbb{Q} \text{ w.r.t. } |\cdot|_p \}$ $\xleftarrow{(x)_n \longleftarrow x} \mathbb{Q}$
 $\mathcal{I} := \{ \text{null-sequences } (x_n) : |x_n|_p \rightarrow 0 \}$

Def 1. $\mathbb{Q}_p := R/\mathcal{I}$ New definition! Soon: equivalent to the old.

Note: $\mathbb{Z}_p^{\text{old}} \xrightarrow{\omega} R \xrightarrow{\omega} R/\mathcal{I} =: \mathbb{Q}_p$
 $\sum_{v=0}^{\infty} a_v p^v \mapsto (x_n)_n, \quad x_n := \sum_{v=0}^{n-1} a_v p^v$ partial sum

Cauchy b/c for $n > m$, $|x_n - x_m|_p = \left| \sum_{v=m}^{n-1} a_v p^v \right|_p \leq \max_{m \leq v \leq n-1} \{ |a_v p^v|_p \} \leq \frac{1}{p^m}.$

Given $x = (x_n) \in \mathbb{Q}_p$, define $|x|_p := \lim_{n \rightarrow \infty} |x_n|_p$ which exists b/c R is complete,
 and is indep. of class in $R/\mathcal{I}$ chosen.

Note that $|x_n|_p \in \{0\} \cup p^{\mathbb{Z}} \subseteq \mathbb{R}$ discrete

$\Rightarrow |x|_p = \lim |x_n|_p$ for large $n \gg 0$.

Thus $v_p: \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{\infty\}$ extends as well: $v_p(x) = v_p(x_n)$ for $n \gg 0$.

Finally, $|x|_p = p^{-v_p(x)} \quad \forall x \in \mathbb{Q}_p$ again.

Prop. 2. The field $\mathbb{Q}_p$ is complete w.r.t. to $|\cdot|_p$ (i.e. Cauchy seq. converge).

(The pf is the same as for $\mathbb{R}$.)

Prop. 3. The subset $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ is a subring of $\mathbb{Q}_p$, the closure w.r.t. $|\cdot|_p$ of $\mathbb{Z}$ in $\mathbb{Q}_p$.

Pf. $|x+y|_p \leq \max\{|x|_p, |y|_p\} \Rightarrow$ closed under $+$
 $|xy|_p \leq |x|_p |y|_p \Rightarrow$ closed under $\cdot$ } $\Rightarrow$ subring

$\{x_n\}$ Cauchy seq. in $\mathbb{Z}$, $x := \lim_{n \rightarrow \infty} x_n \in \mathbb{Q}_p$

$\leadsto |x_n|_p \leq 1 \Rightarrow |x|_p = \lim_{n \rightarrow \infty} |x_n|_p \leq 1 \Rightarrow x \in \mathbb{Z}_p$.

Conversely, $x = \lim_{n \rightarrow \infty} x_n \in \mathbb{Z}_p$ for $x_n \in \mathbb{Q}$ Cauchy;

then $|x|_p \leq 1$ & we saw $|x|_p = |x_n|_p$ for $n \gg 0$

i.e. $x_n = \frac{a_n}{b_n}$ with $p \nmid b_n$, $n \gg 0$.

Choose $\forall n \gg 0$, $y_n \in \mathbb{Z}$ s.t. $b_n y_n \equiv a_n \pmod{p^n}$

$\Rightarrow |x_n - y_n|_p \leq p^{-n} \Rightarrow x = \lim y_n \in \text{closure of } \mathbb{Z}$. □

(In other words: $\mathbb{Z}_p = \{(x_n) \in \mathbb{R} : x_n \in \mathbb{Z}\} / \sim$.)

Now, clearly, $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x|_p = 1\}$ $|x|_p \leq 1$ & $|x^{-1}|_p \leq 1$

Moreover, $\mathbb{Q}_p^\times = p\mathbb{Z} \times \mathbb{Z}_p^\times$:

$x \mapsto (p^{v_p(x)}, x \cdot p^{-v_p(x)})$

$p^u u \mapsto (p^u, u)$

Prop. 4. The non-zero ideals of $\mathbb{Z}_p$ are $p^n \mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq n\}$, $n \geq 0$,
and $\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z} / p^n \mathbb{Z}$.

Pf. $\mathfrak{a} \neq 0$ ideal of $\mathbb{Z}_p$, $x \in \mathfrak{a}$ element of largest possible norm (≤ 1 still)
 $p^n u$, $u \in \mathbb{Z}_p^\times$, $n \geq 0$

Then $\mathfrak{a} \supseteq p^n \mathbb{Z}_p$ and any $y \in \mathfrak{a}$ has $|y|_p \leq |x|_p = p^{-n}$,

i.e. $v_p(y) \geq v_p(x) = n$.

$$\Rightarrow y = p^m \cdot v, m \geq n \text{ \& } v \in \mathbb{Z}_p^\times \Rightarrow y = p^n \cdot (p^{m-n} \cdot v) \in p^n \mathbb{Z}_p.$$

$\in \mathbb{Z}_p$

$$\Rightarrow \mathfrak{a} = p^n \mathbb{Z}_p.$$

Now, consider: $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}_p / p^n \mathbb{Z}_p$
 $a \longmapsto a \bmod p^n$

$$\cdot \ker \varphi = \{a \in \mathbb{Z} : a \equiv 0 \bmod p^n\} = p^n \mathbb{Z}$$

$$\cdot \varphi \text{ surjective: } \forall x \in \mathbb{Z}_p \exists a \in \mathbb{Z} \text{ s.t. } |x - a|_p \leq \frac{1}{p^n} \text{ by Prop 3}$$

$$\Rightarrow x - a \in p^n \mathbb{Z}_p \Rightarrow x \equiv a \bmod p^n \mathbb{Z}_p \checkmark.$$

Thus φ gives the desired $\mathbb{Z} / p^n \mathbb{Z} \xrightarrow[\cong]{\varphi} \mathbb{Z}_p / p^n \mathbb{Z}_p$. □

Prop. 5. $\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}_p / p^n \mathbb{Z}_p \cong \varprojlim_n \mathbb{Z} / p^n \mathbb{Z}$ is an isom.
 $x \longmapsto (x \bmod p^n)_n$

Pf. $\cdot x \longmapsto 0 \Rightarrow x \in p^n \mathbb{Z}_p \forall n \geq 1 \Rightarrow |x|_p \leq \frac{1}{p^n} \forall n \geq 1 \Rightarrow |x|_p = 0 \Rightarrow x = 0.$

$$\cdot \text{An elt. } (s_n) \in \varprojlim_n \mathbb{Z} / p^n \mathbb{Z} \text{ is given by } s_n = \sum_{v=0}^{n-1} a_v p^v \text{ by Prop. 20.5.}$$

We saw this sequence is Cauchy so defines $x \in \mathbb{Z}_p$ mapping to (s_n) . □

Cor. 6. Old & new definitions of $\mathbb{Z}_p$ & $\mathbb{Q}_p$ agree.

Pf. Prop. 5 & Cor. 20.7: $\mathbb{Z}_p^{\text{old}} \cong \varprojlim \mathbb{Z}/p^n \mathbb{Z}$. $\square$

§. Absolute values. Both $|\cdot|_\infty$ & $|\cdot|_p$ are "absolute values":

Def. 7 K field

An **absolute value** on K is a function $|\cdot|: K \rightarrow \mathbb{R}_{\geq 0}$

$$(1) |x| \geq 0 \quad \& \quad = 0 \Leftrightarrow x = 0,$$

$$(2) \forall x, y \in K, |x \cdot y| = |x| |y|,$$

$$(3) |x+y| \leq |x| + |y| \quad \text{"triangle inequality"}$$

It is **non-archimedean (NA)** if it satisfies:

$$(3') |x+y| \leq \max\{|x|, |y|\} \quad \text{"strong triangle inequality"} \quad (\text{Note: } (3') \Rightarrow (3).)$$

Example. $|\cdot|_p$ is non-arch.: $|p^m \frac{a}{b} - p^n \frac{c}{d}|_p = p^{-\min\{m, n\}} = \max\{|p^m \frac{a}{b}|_p, |p^n \frac{c}{d}|_p\}.$

$|\cdot|_\infty$ is arch.: $|1+2| = 3 > 2 = \max\{1, 2\}.$

Assume: $|\cdot| \neq \text{trivial}$, i.e. not $|x| = 1 \forall x \neq 0$.

Def 8 $|\cdot|, |\cdot|'$ **equivalent** if $|\cdot|' = |\cdot|^s$ for some $s > 0$

Note: $|\cdot|$ defines a metric $d(x, y) := |x - y|$, and

$|\cdot|, |\cdot|'$ equivalent $\Leftrightarrow$ the topological spaces are equal.

Thm 9. (Approximation Thm). K field

$|\cdot|_1, \dots, |\cdot|_s$ non-trivial, pairwise inequiv. abs. values

$$x_1, \dots, x_s \in K, \varepsilon > 0 \Rightarrow \exists x \in K \text{ s.t. } |x - x_i|_i < \varepsilon \quad \forall i.$$

Pf. $|\cdot|_1$ & $|\cdot|_s$ inequiv. $\Rightarrow \exists \alpha \in K$ s.t. $|\alpha|_1 < 1, |\alpha|_s \geq 1$

$$\exists \beta \in K \text{ s.t. } |\beta|_1 \geq 1, |\beta|_s < 1$$

$$\Rightarrow y := \beta/\alpha \text{ s.t. } |y|_1 > 1, |y|_s < 1.$$

Claim. $\exists z \in K$ s.t. $|z|_1 > 1, |z|_j < 1, j=2, \dots, s$.

Proof by induction:

• $s=2$ ✓

• Say OK for $j=2, \dots, s-1$ with $z \in K$.

• If $|z|_s \leq 1$, then take $z^n y$ for y as above & n large:

$$* |z|_1^n |y|_1 > 1,$$

$$* \underbrace{|z|_j^n}_{<1} \underbrace{|y|_j}_{??} < 1, \quad j=2, \dots, s-1 \text{ for } n \text{ large,}$$

$$* |z|_s^n |y|_s < 1 \cdot 1 = 1.$$

• If $|z|_s > 1$, then take $t_n := \frac{z^n}{1+z^n}$ which ...

$$\rightarrow 1 \text{ for } |\cdot|_1 \text{ & } |\cdot|_s$$

$$\rightarrow 0 \text{ for } |\cdot|_j \quad j=2, \dots, s-1$$

For n large, $t_n \cdot y$ will work. //

Ok, so now take the z from Claim. Then again:

$$\frac{z^n}{1+z^n} \begin{cases} \rightarrow 1 & \text{in } |\cdot|_1 \\ \rightarrow 0 & \text{in } |\cdot|_j, \quad j=1, \dots, s-1 \end{cases}$$

For each $i=1, \dots, s$, choose $z_i \in K$ close to 1 at $|\cdot|_i$, close to 0 at $|\cdot|_j \quad j \neq i$

$$\Rightarrow x = z_1 x_1 + \dots + z_s x_s \in K \text{ works.} \quad \square$$

Thm 10 (Ostrowski). Every absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ or $|\cdot|_\infty$.

- One-side A4 page notecard will be allowed on the exam.
- Mike Deas will give next 3 lectures; Last 2 lectures $\rightarrow$ office hours.
- Final HW to be posted on Wed.

Last time: • New definition of $\mathbb{Q}_p$: completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\} = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p \mid v_p(x) = 0\} = \{x \in \mathbb{Q}_p \mid |x|_p = 1\}$$

- Equivalent to old definition:

$$\mathbb{Z}_p^{\text{new}} \cong \varprojlim \mathbb{Z}/p^n \mathbb{Z} \cong \varprojlim \mathbb{Z}/p^n \mathbb{Z} \cong \mathbb{Z}_p^{\text{old}}.$$

- Approximation Theorem 21.9: ultimate form of Chinese Remainder Theorem

$$\left. \begin{array}{l} p_1, \dots, p_n \text{ primes} \\ r_1, \dots, r_n \in \mathbb{Z}_{\geq 1} \\ x_1, \dots, x_n \in \mathbb{Z} \end{array} \right\} \leadsto \begin{array}{l} \exists x \in \mathbb{Z} \text{ s.t. } x \equiv x_i \pmod{p_i^{r_i}} \\ \text{i.e. } |x - x_i|_{p_i} \leq p_i^{-r_i} < \varepsilon \end{array}$$

Thm 21.10. (Ostrowski's Thm).

Every absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ or $|\cdot|_\infty$.

Pf. Case 1. $|n| \leq 1$ for all $n \in \mathbb{Z}_{\geq 1}$

$\exists n \neq 1$ s.t. $|n| < 1$ b/c non-trivial $\Rightarrow \exists$ prime p s.t. $|p| < 1$ (divisor of n)

Then $\mathfrak{o} := \{a \in \mathbb{Z} : |a| < 1\}$ is an ideal s.t. $p\mathbb{Z} \subseteq \mathfrak{o} \subsetneq \mathbb{Z}$

& $p\mathbb{Z}$ maximal $\Rightarrow p\mathbb{Z} = \mathfrak{o}$.

For $a \in \mathbb{Z}$, $a = p^n b$, $p \nmid b$, $b \notin \mathfrak{o}$ so $|b| = 1$ and

$$|a| = |p^n b| = |p|^n.$$

Picking s s.t. $|p|^s = p^{-1}$, we have $|\cdot|^s = |\cdot|_p$. //

Case 2. $|n| > 1$ same $n \in \mathbb{Z}_{\geq 1}$.

($|\cdot|$ usual absolute value on $\mathbb{Q}$)

Let $b \in \mathbb{Z}_{\geq 1}$ smallest s.t. $|b| > 1$. (Eventually $b=2$ & this holds $\forall n \in \mathbb{Z}_{\geq 1}$.)

Write $|b| = b^s$, same $s > 0$.

For $n \geq 1$, consider the base- b expansion:

$$(*) \quad n = a_0 + a_1 b + \dots + a_r b^r, \quad 0 \leq a_j < b, \quad r \geq 0, \quad a_r \geq 1.$$

Minimality of $b \Rightarrow |a_i| \leq 1 \quad \forall i$

$$\Rightarrow |n| \leq \sum_{i=0}^r |a_i| |b|^i \leq \sum_{i=0}^r |b|^i \leq \frac{|b|^r}{1 - 1/|b|}$$

For $C = \frac{1}{1 - 1/|b|} > 0$, $|n| \leq C \cdot |b|^r = C b^{rs} \leq C n^s$ (b/c $b^r \leq n$).

$$\Rightarrow |n^k| \leq C n^{sk} \Rightarrow |n| \leq C^{1/k} n^s \xrightarrow{k \rightarrow \infty} |n| \leq n^s = |n|_{\infty}^s \quad (**)$$

WTS: $|n| \geq |n|_{\infty}^s$; enough to prove $|n| \geq C' n^s$ and proceed as above.

Using $(*)$ again $b^{r+1} > n \geq b^s$, and

$$\begin{aligned} b^{s(r+1)} &= |b|^{r+1} = |b^{r+1}| = |b^{r+1} - n + n| \leq |b^{r+1} - n| + |n| \\ &\stackrel{(**)}{\leq} (b^{r+1} - n)^s + |n| \end{aligned}$$

$$\begin{aligned} \Rightarrow |n| &\geq (b^{r+1})^s - (b^{r+1} - n)^s = (b^{r+1})^s \left(1 - \left(1 - \frac{n}{b^{r+1}} \right)^s \right) \\ &\geq n^s \cdot \underbrace{\left(1 - \left(1 - \frac{1}{b} \right)^s \right)}_{C'} \end{aligned}$$

$\Rightarrow |n| \geq C' \cdot n^s$, as we wanted. //

Thus, $|n| = |n|_{\infty}^s \quad \forall n \geq 1$, and hence $|\cdot| = |\cdot|_{\infty}^s$. □

Note: proof of Case 2 was updated compared to the lecture. In the lecture, (following Neukirch), we had assumed $|n| \geq 1 \quad \forall n \geq 1$ which needs to be proved.

§ Discretely valued rings & fields. Generalization of $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

Def. 1. A NA absolute value $|\cdot|$ on K is **discrete** if $\exists \alpha \in (0,1)$ s.t.

$$\text{Im } |\cdot| = \alpha^{\mathbb{Z}} \cup \{0\}. \leadsto K \text{ is a discrete valued field (d.v.f.)}$$

- Then the associated **valuation** is $v(x) = \log_{\alpha} |x| \in \mathbb{Z} \cup \{\infty\}$.
- The **valuation ring** is $\mathcal{O}_K = \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$,
& its **prime ideal** is $\mathfrak{p} := \{x \in K : v(x) \geq 1\}$.

Def. 2. K with absolute value $|\cdot|$

$\leadsto \hat{K} := \{\text{Cauchy seq.}\} / \{\text{null sequences}\}$ **completion** w.r.t. $|\cdot|$,
equipped with $|(x_n)| := \lim_n |x_n|$ absolute value

We have $K \hookrightarrow \hat{K}$ & K is **complete** if this is an isomorphism.
 $x \mapsto (x, x, \dots)$

Def. 3. • A **discrete valuation ring (d.v.r.)** is a domain A with a $\mathbb{Z}_{\geq 0}$ -valued valuation v .

- Its **prime ideal** is $\mathfrak{p} := \{a \in A : v(a) \geq 1\}$; it is principal,
generated by a **uniformizer** $\pi \in A$.
- Its **residue field** is $k(A) := A/\mathfrak{p}$.
- The **completion** of A is $\hat{A} := \varprojlim A/\pi^n A$ and A is **complete** if the
natural map $A \rightarrow \hat{A}$ is an isomorphism.

Prop. 4.

(1) $K = \text{complete dvr} \rightsquigarrow \hat{O}_K = \text{complete dvr}$
and $\hat{O}_K$ is complete as a topological space

(2) $A = \text{complete dvr} \rightsquigarrow \text{Frac}(A) = \text{complete dvr}$
and $\hat{O}_{\text{Frac}(A)} = \hat{O}_A$.

(3) $A = \text{dvr with unif. } \pi \rightsquigarrow \text{image of } \pi \text{ in } \hat{A} \text{ is a uniformizer}$
 $\forall n \geq 1 \quad A/\pi^n A \xrightarrow{\cong} \hat{A}/\pi^n \hat{A}$

In particular, $k(\hat{A}) \cong k(A)$.

Pf. The same proofs as for $\mathbb{Z}_p$ & $\mathbb{Q}_p$: Exercise. $\square$

Example. $\mathbb{Z}$ with $v_p \rightsquigarrow \hat{\mathbb{Z}} = \mathbb{Z}_p, \hat{\mathbb{Q}} = \mathbb{Q}_p, \mathbb{Z}/p^n \mathbb{Z} \cong \mathbb{Z}_p/p^n \mathbb{Z}_p$.

Example. $K = \text{number field}, \mathcal{O}_K \ni \mathfrak{p}$ prime ideal

$\rightsquigarrow$ For $x \in \mathcal{O}_K, x \neq 0, x\mathcal{O}_K = \mathfrak{p}^v \cdot \mathfrak{q}_1^{r_1} \dots \mathfrak{q}_n^{r_n}, v \geq 0, \mathfrak{q}_i \neq \mathfrak{p}$
 $\Rightarrow v_{\mathfrak{p}}(x) := v = \text{power of } \mathfrak{p} \text{ in fact. of } x\mathcal{O}_K$.

Then: $v_{\mathfrak{p}}$ discrete valuation on $\mathcal{O}_K \rightsquigarrow v_{\mathfrak{p}}$ discrete valuation on $K = \text{Frac}(\mathcal{O}_K)$

$\rightsquigarrow K_{\mathfrak{p}} := \text{completion of } K \text{ wrt } |\cdot|_{\mathfrak{p}} := \|\mathfrak{p}\|^{-v_{\mathfrak{p}}(\cdot)}$

$$\hat{\mathcal{O}}_{K_{\mathfrak{p}}} \cong \varprojlim_n \mathcal{O}_K / \mathfrak{p}^n \mathcal{O}_K.$$

This generalizes $\mathbb{Q}_p$ and $\mathbb{Z}_p$!

Slogan: Study $\mathfrak{p}/p$ (e.g. $e(\mathfrak{p}/p), f(\mathfrak{p}/p), G_{\mathfrak{p}/p} \cong \Gamma_{\mathfrak{p}/p}$)
in terms of the extension $K_{\mathfrak{p}}/\mathbb{Q}_p$!

What are the possible absolute values on K ?

- (1) Any embedding $\sigma: K \hookrightarrow \mathbb{R}$, $\tau: K \hookrightarrow \mathbb{C}$ induces absolute value
 $|x|_\sigma := |\sigma(x)|$, $|x|_\tau := |\tau(x)| = \sqrt{\tau(x) \cdot \overline{\tau(x)}}$ ($\tau, \bar{\tau}$ induce the same)
- (2) Any prime ideal $\mathfrak{p}$ induces $|\cdot|_{\mathfrak{p}}$ as above.

Def. 5. A **place** v of K is either a prime ideal $\mathfrak{p}$, $\sigma: K \hookrightarrow \mathbb{R}$,
or $\{\tau, \bar{\tau}\}$ for $\tau: K \hookrightarrow \mathbb{C}$.

Each place has an associated absolute value $|\cdot|_v$, and completion K_v .

- Approximation theorem 21.9 still applies! (Upgrade of Chinese remainder thm.)
- Ostrowski's Thm for $K = \mathbb{Q}$: these are all the absolute values!

Goal: Prove this for any K .

If $|\cdot|_K = \text{any abs. value on } K \Rightarrow \text{restriction to } \mathbb{Q} \text{ is } |\cdot|_v \text{ for some } v.$

Moreover, $\hat{K}$ is then a finite extension of $\mathbb{Q}_v = \begin{cases} \mathbb{Q}_p & v = \mathfrak{p}, \\ \mathbb{R} & v: \mathbb{Q} \hookrightarrow \mathbb{R} \text{ "}\infty\text{"} \end{cases}$

Thm 6 (Ostrowski). $K = \text{field complete w.r.t. arch. abs. value}$

Then $\exists \sigma: K \hookrightarrow \mathbb{R} \text{ or } \mathbb{C} \text{ s.t. } |a| = |\sigma(a)|^s \forall a \text{ for some } s > 0.$

Pf. Omitted – see Neukirch, Thm II.4.2. $\square$

Goal. What are all the finite extensions of $\mathbb{Q}_p$? (Or a complete def in general.)

→ How do polynomials factor over $\mathbb{Z}_p$?

Thm 7. (Hensel's Lemma).

A : complete dvr with uniformizer π & $k := A/\pi A$ res. field

$f(x) \in A[x]$ polynomial, $\bar{f}(x) \in k[A]$ reduction mod π

$\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$ in $k[x] \Rightarrow \exists g(x), h(x) \in A[x]$ s.t.

$\bar{g}, \bar{h}$ coprime to each other

- $f(x) = g(x) \cdot h(x)$
- reduce to $\bar{g}(x), \bar{h}(x)$ mod π ,
- $\deg g(x) = \deg \bar{g}(x)$.

Example. $x^{p-1} - 1$ in $\mathbb{Z}_p[x]$ splits into distinct linear factors over $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$

$\Rightarrow$ splits into distinct linear factors over $\mathbb{Z}_p$

$\Rightarrow \mathbb{Z}_p$ contains all $(p-1)^{\text{th}}$ roots of unity!

Last time :

- proof of Ostrowski's Thm 20.10 : any $|\cdot|$ on $\mathbb{Q}$ is equiv. to $|\cdot|_p$ or $|\cdot|_\infty$.
 $\rightarrow$ Issue with proof when $|\cdot| = \text{arch.}$: resolved in new version of notes.
 The argument is still similar, but a bit longer - see lecture notes.
- discrete valued fields/rings & their completions :

$$K \text{ number field} \leadsto |\cdot|_v = \begin{cases} |\cdot|_p & v = p \text{ prime} \\ |\cdot|_\sigma & \sigma: K \hookrightarrow \mathbb{C} \end{cases}$$

$$\leadsto K_v = \begin{cases} \text{finite ext. of } \mathbb{Q}_p & p \text{ above } p \\ \mathbb{R} \text{ or } \mathbb{C} & \sigma: K \hookrightarrow \mathbb{R} \text{ or } \tau: K \hookrightarrow \mathbb{C} \end{cases}$$

Goal. What are the extensions of $\mathbb{Q}_p$?

- Hensel's Lemma 22.7 : reducibility in $k[x]$ lifts to reducibility in $A[x]$.

Pf of Hensel's Lemma 22.7. Suppose $\bar{f}(x) = \bar{g}(x) \bar{h}(x)$ in $k[x]$.

Let $g_0(x), h_0(x) =$ any lift of $\bar{g}(x), \bar{h}(x)$ to $A[x]$ with same degrees.

Then : $f(x) \equiv g_0(x) h_0(x) \pmod{\pi}$, $\deg g_0(x) = \deg \bar{g}(x)$ ($\deg \bar{f} \leq \deg f$)

$$\deg h_0(x) \leq \deg f(x) - \deg \bar{g}(x)$$

Claim by induction. $\exists p_i(x), q_i(x)$ s.t. $\deg p_i(x) < \deg \bar{g}(x)$

$$\deg q_i(x) \leq \deg \bar{f}(x) - \deg \bar{g}(x)$$

$$\text{and } g_n(x) := g_0(x) + \pi p_1(x) + \pi^2 p_2(x) + \dots + \pi^n p_n(x)$$

$$h_n(x) := h_0(x) + \pi q_1(x) + \pi^2 q_2(x) + \dots + \pi^n q_n(x)$$

satisfy : $f(x) \equiv g_n(x) \cdot h_n(x) \pmod{\pi^{n+1}}$.

If we prove the claim, we can simply take $g(x) = \lim_n g_n(x)$, $h(x) = \lim_n h_n(x)$.
b/c A is complete!

Pf of Claim. $n=0$ ✓

Suppose $f(x) \equiv g_n(x) \cdot h_n(x) \pmod{\pi^{n+1}}$ as above.

$$\text{Let } d_n(x) := \frac{f(x) - g_n(x) \cdot h_n(x)}{\pi^{n+1}} \in A[x].$$

We need to prove:

$$f(x) \equiv (g_n(x) + \pi^{n+1} p_{n+1}(x)) (h_n(x) + \pi^{n+1} q_{n+1}(x)) \pmod{\pi^{n+2}}$$

$$\Leftrightarrow f(x) - g_n(x) h_n(x) \equiv \pi^{n+1} (p_{n+1}(x) h_n(x) + q_{n+1}(x) h_n(x)) \pmod{\pi^{n+2}}$$

$$\Leftrightarrow d_n(x) \equiv p_{n+1}(x) h_n(x) + q_{n+1}(x) g_n(x) \pmod{\pi},$$

$$\Leftrightarrow d_n(x) \equiv p_{n+1}(x) \overset{III}{h_0(x)} + q_{n+1}(x) \overset{III}{g_0(x)} \pmod{\pi}.$$

$k[x]$ Euclidean domain $\Rightarrow \exists \bar{a}(x), \bar{b}(x) \in k[x]$ s.t. $\bar{a} \cdot \bar{g} + \bar{b} \cdot \bar{h} = 1$

$\Rightarrow$ pick lifts $a(x), b(x) \in A[x]$ & let

$$r_{n+1}(x) = d_n(x) b(x), \quad s_{n+1}(x) = d_n(x) \cdot a(x).$$

Then: $r_{n+1}(x) \cdot h_0(x) + q_{n+1}(x) \cdot g_0(x) \equiv d_n(x) \pmod{\pi},$

and the only issue is that we may have $\deg r_{n+1} \geq \deg \bar{g},$
 $\deg s_{n+1} > \deg f - \deg \bar{g}.$

Ok, so divide by $\bar{g}$ in $k[x]$:

$$\overline{r_{n+1}}(x) = \overline{d_n}(x) \bar{b}(x) = \bar{\alpha}(x) \bar{g}(x) + \bar{\beta}(x) \quad \bar{\alpha}, \bar{\beta} \in k[x]$$

$$\deg \bar{\beta} < \deg \bar{g}.$$

& take lifts $\alpha, \beta \in R[x]$ of $\bar{\alpha}, \bar{\beta} \in k[x]$

$$\Rightarrow r_{n+1}(x) = d_n(x) b(x) \equiv \alpha(x) g(x) + \beta(x) \pmod{\pi}$$

$$\Rightarrow \beta(x) h_0(x) + (\alpha(x) h_0(x) + q_{n+1}(x)) g_0(x) \equiv d_n(x) \pmod{\pi}$$

Since now $\deg \beta = \deg \bar{\beta} < \deg \bar{g}$, we can safely take $p_{n+1}(x) = \beta(x)$.

Finally, we play the same game to find q_{n+1} with $\deg \leq \deg f(x) - \deg \bar{q}(x)$. □

Thm 1. $F = \text{complete w.r.t } |\cdot|$, K/F any finite extension of $\deg. n$

$\Rightarrow |\cdot|$ extends uniquely to an absolute value on K/F , K is complete, and this extension is given by

$$|\alpha| = \sqrt[n]{|N_{K/F}(\alpha)|}, \quad \alpha \in K.$$

Pf. 1.1 archimedean: Ostrowski's Thm 21.6 $\Rightarrow F = \mathbb{R}$ or $\mathbb{C}$

$\Rightarrow$ only non-trivial case is $K = \mathbb{C} / F = \mathbb{R}$, and then

$$|z| = \sqrt[2]{|N_{\mathbb{C}/\mathbb{R}}(z)|} = \sqrt[2]{z \cdot \bar{z}}$$

1.1 NA.

Lemma. Let $\mathcal{O}_F = \text{valuation ring of } F = \{x \in F : |x| \leq 1\}$,

and $\mathcal{O}_K := \{\text{integral closure of } \mathcal{O}_F \text{ in } K\}$.

Then: $\mathcal{O}_K = \{\alpha \in K : N_{K/F}(\alpha) \in \mathcal{O}_F\}$.

Note: false for number fields.

We saw: $\alpha \in K$ integral $\Rightarrow N_{K/F}(\alpha) \in \mathcal{O}_F$.

Conversely, say $N_{K/F}(\alpha) \in \mathcal{O}_F$.

$\Rightarrow f(x) \in F[x]$ min poly of α , has constant coeff $N_{K/F}(\alpha)$ of $\mathcal{O}_F$
& we want $f(x) \in \mathcal{O}_F[x]$.

Otherwise, say $\pi^n f(x) \in \mathcal{O}_F[x]$ with $n \geq 1$ has reduction

$0 \neq \bar{f}_n(x) \in k[x]$ & constant term 0, degree $< \deg(f(x))$

Thus, $\bar{f}_n(x) = x^d \cdot \bar{h}(x)$ for $d \geq 1$ and $\bar{h}$ coprime to x .

Hensel's lemma $\Rightarrow \pi^n f(x) = g(x) \cdot h(x)$ with $g, h \in \mathcal{O}_K[x]$

and $g(x) \equiv x^d \pmod{\pi}$, $h(x) \equiv \bar{h}(x) \pmod{\pi}$,

$\deg g(x) = d < \deg f(x)$

Since $f(x)$ is irreducible, $\deg g(x) = 0$ $\nless$.

Existence. Clearly, $|\cdot|_K$ extends $|\cdot|$, $|\alpha\beta|_K = |\alpha|_K |\beta|_K$, and

$$|\alpha|_K = 0 \Leftrightarrow N_{K/F}(\alpha) = 0 \Leftrightarrow \alpha = 0.$$

Strong triangle inequality: $0 \neq x, y \in K$, $|x|_K \leq |y|_K \Rightarrow |x+y|_K \leq |y|_K$.

Let $z = \frac{x}{y}$ so that $|z|_K \leq 1 \Rightarrow |N_{K/F}(z)| \leq 1$

$$\Rightarrow N_{K/F}(z) \in \mathcal{O}_F$$

$\stackrel{(i)}{\Rightarrow} z \in K$ integral over $\mathcal{O}_F$

$\Rightarrow z+1 \in K$ integral over $\mathcal{O}_F$

$$\stackrel{(i)}{\Rightarrow} N_{K/F}(z+1) \in \mathcal{O}_F$$

$$\Rightarrow |z+1|_K \leq 1$$

$$\Rightarrow |x+y|_K \leq |y|_K \quad \checkmark$$

Uniqueness. Say $|\cdot|'$ another extension, $\mathcal{O}_K' = \{\alpha \in K : |\alpha|' \leq 1\}$

$\leadsto \mathfrak{p}, \mathfrak{p}'$ maximal ideals in $\mathcal{O}_K, \mathcal{O}_K'$ (i.e. $|\cdot| < 1, |\cdot|' < 1$).

Claim. $\mathcal{O}_K \subseteq \mathcal{O}_K'$.

Else, $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_K'$ and $f(x) = x^d + \dots + a_d$ min. poly of α over F

$\Rightarrow a_1, \dots, a_d \in \mathcal{O}_F$, and $\alpha \notin \mathcal{O}_K' \Rightarrow |\alpha| > 1 \Rightarrow \alpha^{-1} \in \mathfrak{p}'$

$\Rightarrow 1 = -a_1 \alpha^{-1} - \dots - a_d (\alpha^{-1})^d \in \mathfrak{p}' \quad \nlessdot //$

Thus $\mathcal{O}_K \subseteq \mathcal{O}_K'$, i.e. $|\alpha| \leq 1 \Rightarrow |\alpha|' \leq 1$.

If $|\cdot|, |\cdot|'$ not equivalent, then by Approximation Thm 21.9,

$\exists \alpha \in K$ s.t. $|\alpha| \leq 1$ & $|\alpha|' > 1$; contradiction.

Hence $|\cdot|' = |\cdot|^s$, $s > 0$, and $s = 1$ b/c they agree on F . //

Completeness. Follows from the general result...

Lemma. F complete w.r.t. $|\cdot|$, $V = n$ -dimensional v.sp./ F

$\Rightarrow$ for any basis $e_1, \dots, e_n \in V$, the max norm

$$\|x_1 v_1 + \dots + x_n v_n\| := \max\{|x_1|, \dots, |x_n|\}$$

is equivalent to any norm on V , and V is complete via the homeomorphism

$$K^n \xrightarrow{\cong} V$$

$$(x_1, \dots, x_n) \longmapsto x_1 v_1 + \dots + x_n v_n.$$

See Neukirch, Prop. II.4.9 for the pf. □

Cor. 2. K field of characteristic 0

$K/\mathbb{Q}_p$ finite extension $\Leftrightarrow K$ is a complete discrete value field
with finite residue field ("local field")

Pf. ' $\Rightarrow$ ' Thm 1 + residue field is finite extension of $\mathbb{F}_p$:

If $\bar{x}_1, \dots, \bar{x}_n \in k := k(\mathcal{O}_K) = \mathcal{O}_K/\pi$ linearly indep.

$\Rightarrow$ lifts $x_1, \dots, x_n \in \mathcal{O}_K$ linearly indep.

(Clear out powers of π in linear comb. in $\mathcal{O}_K$ & reduce mod π .)

' $\Leftarrow$ ' Say residue field has char. p

$\Rightarrow$ restriction of $|\cdot|$ on K to $\mathbb{Q}$ is equiv. to $|\cdot|_p$ by Ostrowski's Thm 21.10.

Since K is complete, it contains $\mathbb{Q}_p$.

The fact that $[K:\mathbb{Q}_p] < \infty$ follows from local compactness of K (omitted.) $\square$

This immediately motivates the following definitions.

Def. 3. For $K/F/\mathbb{Q}_p$ finite

- the **inertial degree**: $f(K/F) := [k(\mathcal{O}_K) : k(\mathcal{O}_F)]$

- the **ramification index**: $e(K/F) := e \in \mathbb{Z}_{\geq 1}$, where:

$\mathfrak{P} \subseteq \mathcal{O}_K, \mathfrak{p} \subseteq \mathcal{O}_F$ maximal ideals $\mapsto \mathfrak{P} \mathcal{O}_K = \mathfrak{p}^e$ for some e .

Note: there's only one prime in $\mathcal{O}_K \Rightarrow$ no "g" as for number fields.

Thm 4. $[K:F] = e(K/F) \cdot f(K/F)$.

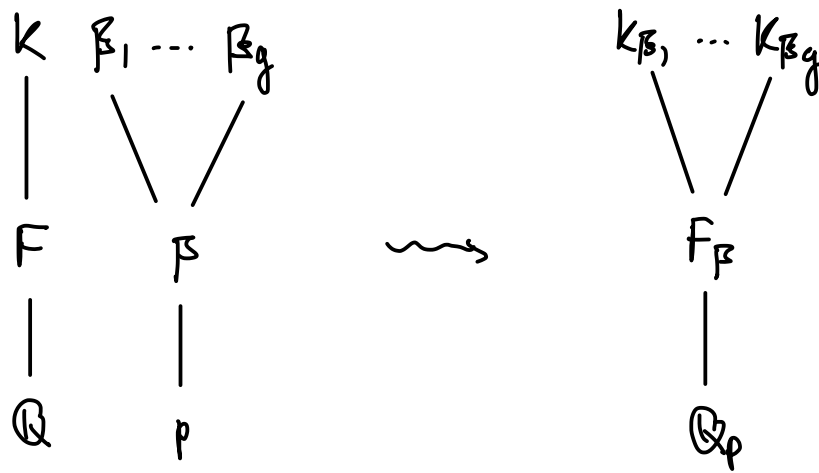
Pf. Our favorite Thm 5.8: for K/F number fields, $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ above $\mathfrak{p}$

$$[K:F] = \sum_{i=1}^g e(\mathfrak{P}_i/\mathfrak{p}) \cdot f(\mathfrak{P}_i/\mathfrak{p}).$$

The proof works for Dedekind domains $\Rightarrow$ apply it to $\mathcal{O}_K$ & $\mathcal{O}_F$ in our setting; since $q=1$, we get the result. □

Summary of applications to number fields.

K/F extension of number fields, $\mathfrak{p}$ prime of F



Then :

$$(1) \quad K \otimes_F F_{\mathfrak{p}} \cong K_{\mathfrak{p}_1} \times \dots \times K_{\mathfrak{p}_g} \quad (\text{to be proved soon!})$$

$$(2) \quad f(\mathfrak{p}_i/\mathfrak{p}) = f(K_{\mathfrak{p}_i}/F_{\mathfrak{p}}) ; \text{ in fact, we know that (prop. 22.4) :}$$

$$\begin{array}{ccc} \mathcal{O}_{K_{\mathfrak{p}_i}} / \pi \mathcal{O}_{K_{\mathfrak{p}_i}} & \cong & \mathcal{O}_K / \mathfrak{p}_i =: \mathbb{F}_{\mathfrak{p}_i} \\ f(K_{\mathfrak{p}_i}/F_{\mathfrak{p}}) \downarrow & & \downarrow f(\mathfrak{p}_i/\mathfrak{p}) \\ \mathcal{O}_{F_{\mathfrak{p}}} / \pi \mathcal{O}_{F_{\mathfrak{p}}} & \cong & \mathcal{O}_F / \mathfrak{p} =: \mathbb{F}_{\mathfrak{p}} \end{array}$$

$$(3) \quad e(\mathfrak{p}_i/\mathfrak{p}) = e(K_{\mathfrak{p}_i}/F_{\mathfrak{p}}) \text{ because}$$

$$\mathfrak{p} \mathcal{O}_K = \prod \mathfrak{p}_j^{e_j}$$

$$\Rightarrow \beta \mathcal{O}_{K_{\beta_i}} = \beta_i^{e_i} \cdot \prod_{j \neq i} \beta_j^{e_j} = \beta_i^{e_i} \quad \text{in } \mathcal{O}_{K_{\beta_i}}.$$

$$\left(\text{b/c } \forall \beta_i(\alpha) = 0 \text{ for } \alpha \in \beta_j \Rightarrow \subseteq \mathcal{O}_{K_{\beta_i}}^\times \right)$$

(4) Say K/F Galois. Then we defined for β/β :

$$G_{\beta/\beta} := \{ \sigma \in \text{Gal}(K/F) : \sigma(\beta) = \beta \}$$

$\cup$
 $\cup$

$$I_{\beta/\beta} := \ker \left(G_{\beta/\beta} \twoheadrightarrow \text{Gal}(\mathbb{F}_{\beta}/\mathbb{F}_K) \right).$$

We will prove that :

$$G_{\beta/\beta} \xrightarrow{\cong} \text{Gal}(K_{\beta}/F_K).$$

ψ

$$\sigma \longmapsto \text{induced automorphism } \sigma \text{ on the completion}$$

such that

$$G_{\beta/\beta} \xrightarrow{\cong} \text{Gal}(K_{\beta}/F_K)$$

$\text{red. map.} \searrow \quad \swarrow \text{red. map.}$

$$\text{Gal}(\mathbb{F}_{\beta}/\mathbb{F}_K)$$

We will prove these facts next time!

Last time:

- Thm 23.1: F = complete w.r.t. $|\cdot|$, K = finite ext. of F
 $\Rightarrow \exists!$ extension of $|\cdot|$ to K & K is complete.
- Stated results about splitting of primes in number fields via local fields.

Today: Prove those results.

K/F number fields

$|\cdot|_v$ = absolute value on $F \rightarrow$ How can we extend it to K ?

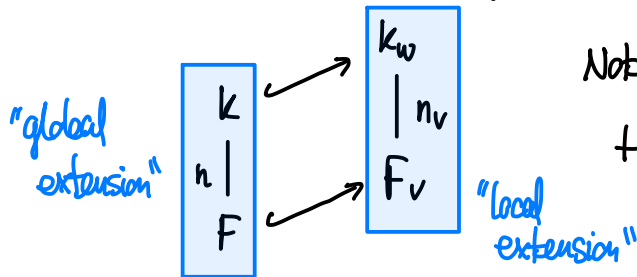
Note: $|\cdot|_v$ gives completion F_v w/ absolute value $|\cdot|_v$

$\rightarrow$ By Thm 23.1, can extend it to $|\cdot|_{\bar{v}}$ on $\bar{F}_v$.

Given $\tau: K \hookrightarrow \bar{F}_v$, get an extension:

$$|\alpha|_w = |\tau(\alpha)|_{\bar{v}}.$$

Then can also consider K_w = completion of K w.r.t. w :



Note: $K_w = \tau(K) \cdot F_v$ because

the right hand side contains K & is complete.

Of course, by Thm 23.1, $|\alpha|_w = \sqrt[n_v]{|N_{K_w/F_v}(\alpha)|_v}$.

How many choices of w ? One for each $\tau: K \hookrightarrow \bar{F}_v$.

For $\sigma \in \text{Gal}(\bar{F}_v/F_v)$, get $K \xrightarrow{\tau} \bar{F}_v \xrightarrow{\sigma} \bar{F}_v \rightsquigarrow \tau' := \sigma \circ \tau$

and we call such τ' *conjugate* to τ over F_v .

Thm 1. (Extension Thm).

- (i) Every extension of v to w arises as $w = \bar{v} \circ \tau$ for some $\tau: K \hookrightarrow \bar{F}_V$.
 (ii) $\bar{v} \circ \tau' \& \bar{v} \circ \tau$ are equal $\Leftrightarrow \tau, \tau'$ are conjugate over F_V .

Pf. (i) $w = \text{extension}$, $K_w = \text{localization with valuation } w$

$\Rightarrow w$ is the unique extension of v from F_V to K_w
 (Thm 23.1)

$\therefore$ choosing any embedding $K_w \xrightarrow{\tau} \bar{F}_V$, $\bar{v} \circ \tau$ has to coincide with w .

Now, $K \subseteq K_w \Rightarrow$ restriction of τ to K gives the desired $w = \bar{v} \circ \tau$ //

(ii) $\tau, \sigma \circ \tau$ conjugate embeddings, $\sigma \in \text{Gal}(\bar{F}_V/F_V)$

$\Rightarrow \bar{v} = \bar{v} \circ \sigma$ on $\bar{F}_V$ by uniqueness $\Rightarrow \bar{v} \circ \tau = \bar{v} \circ \sigma \circ \tau$ $\checkmark$
 (Thm 23.1)

$\bar{v} \circ \tau' = \bar{v} \circ \tau$ for $\tau, \tau': K \hookrightarrow \bar{F}_V \Rightarrow$

$$\begin{array}{ccc} K & \xrightarrow{\tau} & \bar{F}_V \\ & \searrow \tau' & \parallel \\ & & F_V \end{array} \rightsquigarrow \sigma: \tau(K) \rightarrow \tau'(K) \text{ automorphism} \\ \text{s.t. } \sigma = \tau' \circ \tau^{-1}$$

$\rightsquigarrow$ extend σ to F_V -isom. $\sigma: \tau(K)F_V \rightarrow \tau'(K)F_V$:

$\tau(K) \subseteq \tau(K)F_V$ is dense $\Rightarrow$ any $x \in \tau(K)F_V$ is $x = \lim_n x_n$, $x_n \in \tau(K)$

& define $\sigma(x) = \lim_n \sigma(x_n)$, $\sigma(x_n) \in \tau'(K)$

$\in \tau'(K)F_V$.

The map $x \mapsto \sigma(x)$ is indep. of choice of (x_n) & yields:

$$\tau(K)F_V \xrightarrow[\cong]{\sigma} \tau'(K)F_V \text{ over } F_V.$$

Extend it to $\bar{F}_V \xrightarrow[\cong]{\tilde{\sigma}} \bar{F}_V$ over F_V to get desired $\tilde{\sigma} \in \text{Gal}(\bar{F}_V/F_V)$. $\square$

Concrete variant:

$K = F(\alpha)$, $\alpha = \text{root of irred. } f(x) \in F[x]$

$\leadsto f(x) = f_1(x)^{m_1} \cdots f_g(x)^{m_g}$ factorization in $F_v[x]$

(Recall: by Hensel's Lemma, can check this over residue field $F_v[x]$)

$\leadsto$ this featured in splitting of primes, e.g. Thm from Lecture 11.)

$\Rightarrow K = F(\alpha) \xrightarrow{\tau_i} \overline{F_v}$ embedding
 $\alpha \longmapsto \text{root } \alpha_i \text{ of } f_i(x), i = 1, \dots, g$

Cor. 2. The valuations $w_1, \dots, w_g$ extending v correspond to the irred. factors $f_i(x)$.

In fact, we get $\tau_i: K_{w_i} \xrightarrow{\cong} F_v(\alpha_i)$, $\alpha_i = \text{root of } f_i(x)$.

For $w = \text{valuation of } K \text{ extending } v = \text{valuation of } F$, write $v|w$.

E.g. for $v = v_p$ & $w = w_p$ for $p|P$, $v_p|w_p$.

Cor. 3. There is an isomorphism:

$$K \otimes_F F_v \xrightarrow{\cong} \prod_{w|v} K_w.$$

$$a \otimes b \longmapsto (a \cdot b)_w \quad \text{via} \quad \begin{matrix} a \in K \hookrightarrow K_w \\ b \in F_v \hookrightarrow K_w \end{matrix} \leadsto a \cdot b \in K_w$$

Pf. Say $\alpha \in K$ s.t. $K = F(\alpha)$ & take $f(x) \in F[x]$ min. poly of α .

$\leadsto$ by Cor. 2, each $w|v$ corresp. to factor $f_w(x)$ of $f(x)$ in $F_v[x]$.

Fix alg. closure $\overline{F_v}$, embed each K_w in $\overline{F_v}$, and let

$\alpha_w := \text{image of } \alpha \in K \text{ under } K \hookrightarrow K_w$.

Then $K_w = F_v(\alpha_w)$ inside $\overline{F_v}$, and $f_w = \text{min. poly of } \alpha_w \text{ over } F_v$.

Thus, we have a commutative diagram:

$$\begin{array}{ccc}
 F_v[x]/(f(x)) & \xrightarrow{\cong} & \prod_{w|v} F_v[x]/(f_w(x)) \quad (\text{Chinese remainder thm}) \\
 \parallel & & \downarrow \cong \\
 F[x]/(f(x)) \otimes_F F_v & \hookrightarrow & F_v[x]/(f_v(x)) \cong F_v(\alpha_w) = k_w \\
 \parallel & & \\
 k \otimes_F F_v & \longrightarrow & \prod_{w|v} k_w
 \end{array}$$

□

Cor. 4. $[k:F] = \sum_{w|v} [k_w:F_v] = \sum_{w|v} e(k_w/F_v) f(k_w/F_v).$

→ Recovers Thm 5.8!

Example. $K = \mathbb{Q}(\sqrt{m})$, p odd, $m = \square$ -free

Exercise. There's three non-isomorphic quadratic extensions of $\mathbb{Q}_p$, p odd:

- For $a \not\equiv \square \pmod{p}$, $\mathbb{Q}_p(\sqrt{a})$ unique unramified (indep. of a).
- Two ramified extensions:

$$\mathbb{Q}_p(\sqrt{p}), \quad \mathbb{Q}_p(\sqrt{ap}).$$

• p inert in $K \Rightarrow K_p \cong \mathbb{Q}_p(\sqrt{a})$ (b/c $m \not\equiv \square \pmod{p}$)

• p splits in K , $p = \beta_1 \beta_2 \Rightarrow K_{\beta_i} \cong \mathbb{Q}_p$ for $i=1,2$

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \times \mathbb{Q}_p.$$

• p ramified in K , β above $p \Rightarrow p|m$

$$K_{\beta} \cong \begin{cases} \mathbb{Q}_p(\sqrt{p}) \\ \mathbb{Q}_p(\sqrt{ap}) \end{cases} \quad \begin{array}{l} \frac{m}{p} \equiv \square \pmod{p}, \\ \frac{m}{p} \not\equiv \square \pmod{p}. \end{array}$$

§ Galois Theory applied to valuation splitting.

K/F finite Galois extension of ... $\begin{cases} \text{global fields} & (\text{number fields}) \\ \text{local fields} & (\text{finite ext. of } \mathbb{Q}_p) \end{cases}$

$G := \text{Gal}(K/F)$, v = discrete valuation on F

Prop. 5. G acts transitively on $\{w|v\}$.

Pf. $w, w' =$ two ext. of v to K

Not conjugate $\Rightarrow \{w \circ \sigma \mid \sigma \in G\}$ disjoint from $\{w' \circ \sigma \mid \sigma \in G\}$

By Approximation Thm 21.9, $\exists \alpha \in L$ s.t.

$$|\sigma(\alpha)|_w < 1 \quad \& \quad |\sigma(\alpha)|_{w'} > 1 \quad \forall \sigma \in G,$$

$$\Rightarrow |N_{K/F}(\alpha)|_v = \left| \prod_{\sigma \in G} \sigma(\alpha) \right|_v = \begin{cases} \prod |\sigma(\alpha)|_w < 1 \\ \prod |\sigma(\alpha)|_{w'} > 1 \end{cases} \quad \begin{matrix} \nwarrow \\ \nearrow \end{matrix}$$

□

Def. 6. The decomposition group of $w|v$ is

$$G_w = G_w(K/F) := \{\sigma \in \text{Gal}(K/F) : w \circ \sigma = w\}.$$

The inertia subgroup is

$$I_w = I_w(K/F) := \{\sigma \in G_w : \sigma \alpha \equiv \alpha \pmod{\mathfrak{P}_w}\},$$

$$\text{where } \mathfrak{P}_w := \{x \in K : |x|_w < 1\}.$$

For global fields,

$$w = w_{\mathfrak{p}}, v = v_{\mathfrak{p}} \text{ for } \mathfrak{p} | \mathfrak{P} \rightsquigarrow G_w = G_{\mathfrak{p}} \supseteq I_{\mathfrak{p}} = I_w \quad \checkmark$$

For local fields, $G_w = G$ b/c $\exists!$ $w|v$ (Thm 23.1).

$$I_w =: I.$$

Thm 7. For K/F number fields, $G := \text{Gal}(K/F)$, $\mathbb{R}|\mathbb{P}$, $w = w|_{\mathbb{P}}$, $v = v|_{\mathbb{P}}$

- $G_w(K/F) \cong \text{Gal}(K_w/F_v)$,
- $I_w(K/F) \cong I(K_w/F_v)$.

Pf. Claim: $G_w(K/F) = \{\sigma \in \text{Gal}(K/F) : \text{continuous w.r.t. topology } |\cdot|_w\}$.

' $\subseteq$ ' is clear.

' $\supseteq$ ' If σ continuous, $|x|_w < 1 \Rightarrow |\sigma(x)|_w = |x|_{w \circ \sigma} < 1$.

$$\begin{aligned} \text{b/c } |x|_w < 1 &\Rightarrow x^n \text{ null-sequence in } |\cdot|_w \\ &\Rightarrow \sigma(x)^n \text{ null-sequence in } |\cdot|_w \\ &\Rightarrow x^n \text{ null-sequence in } |\cdot|_{w \circ \sigma} \\ &\Rightarrow |x|_{w \circ \sigma} < 1. \end{aligned}$$

Thus w & $w \circ \sigma$ induce the same topology

$\Rightarrow$ they are equivalent

$\Rightarrow$ equal b/c $w|_F = (w \circ \sigma)|_F \Rightarrow \sigma \in \text{Gal}(K/F)$. //

Finally, $K \subseteq K_w$ is dense $\Rightarrow$ every $\sigma \in G_w(K/F)$ extends uniquely to a continuous F_v -aut. $\tilde{\sigma} : K_w \rightarrow K_w$ and

$$\tilde{\sigma} \in I(K_w/F_v) \Leftrightarrow \sigma \in I_w(K/F).$$



LECTURE 25.

15/7

Final lecture: next week, office hours in MZ 4.027, during lecture times.

Exam 1: 25/7

Exam 2: 14/7

Introduction to local class field theory by Dr. Mike Daas.