Algebraic number theory

(20) Integral dependence & dimension
(21) Noetherian, Dedekind and discrete val. rings
(22) Ramification
(23) Number fields I : class number
(24) Number fields II : units
(25) Number fields III : discriminant
(26) Quadratic fields again
(27) Cyclotomic fields again
(28) Abelian extensions : class field theory
(29) Riemann and Dedekind ζ-fcns
(30) Dirichlet L-functions
(31) Local fields
(32) Adeles & ideles . Hecke L-functions

Key words in dio eqns

$f \in \mathbb{Z}[x_1, \dots, x_n]$, $\deg f = d$

$X(\mathbb{Q}) = \{\alpha \in \mathbb{Q}^n \mid f(\alpha) = 0\}$, $N_0 = |X(\mathbb{Q})|$; $X(\mathbb{C})$

$X(\mathbb{F}_p) = \{\alpha \in \mathbb{F}_p^n \mid f(\alpha) = 0\}$, $N_p = |X(\mathbb{F}_p)|$

Pblm 1 Understand N_0 ; more generally $X(\mathbb{Q})$ – finiteness properties

Pblm 2 Understand N_p, especially variation with p.

Pblm 3 Understand relation bet N_0 & N_p's – Hasse-Mink; Birch & S-D (Swinnerton-Dyer)

(1)

$n \backslash d$	1	2	3	4 ....
1	T	T	T	T
2	T	quadr rec & Legendre Th	Mordell Weil But when is $N_0 < \infty$	Mordell conj / Faltings th: $N_0 < \infty$ unless reduced to smaller d But $N_0 = ?$
3	T	quadr rec & Hasse-Minkowski principle		
4	T			
⋮				

conjecturally → N_0 small

N_0 big

conjectures depend on alg-geo of $X(\mathbb{C})$

(2)

$n \backslash d$	1	2	3	4 ....
1	T	quadr rec $N_p = 2 \Leftrightarrow p \in \cup$ arith prog	class field theory, Dirichlet L-fcns (e.g. $N_p = d$ for ∞ many p's & ; in "ab case" for $p \in \cup$ arith progr	
2	T		Riemann hypothesis for funct fields (Hasse-Weil) $[N_p = p + O(\sqrt{p})]$ But $N_p = ?$ ⇝ Hasse Weil L-fcn ⇝ Gauss sums	
3	T			
4	T			
5	T			

generalizes

Chevalley's theorem + homogenizing (p-divisibility properties of N_p) [e.g. $d < n \Rightarrow p \mid N_p$]

But $N_p = ?$ ⇝ Hasse-Weil L-fcns

...

Riemann ζ
(assoc to $\mathbb{Q}$)

Dedekind ζ_K
(assoc to # field K)

$\zeta_K = \prod L(s,\chi)$

Dirichlet L-fcns $L(s,\chi)$
(assoc to Dirichlet char mod m / $\mathbb{Q}$)

Hecke L-fcns
(assoc to "Grossencharacters" of a # field)

f.g. A-alg = f-type

(also say B finite $/A$ or f.g. A-mod)

20

Integral dependence and dimension

Def $A\subset B$ finite ext of rings if B is f.g. $\Rightarrow A$-mod. **Rem** $A\subset B, B\subset C$ fin $\Rightarrow A\subset C$ finite. B called f.g. if ... write $B = A[x_1,\dots,x_n]$, $x_i\in B$.

Def $A\subset B$ rings. An elt $x\in B$ is called *integral* $/A$ if $\exists a_i\in A$ s.t. $x^n + a_1x^{n-1}+\dots+a_n = 0$

Ex $t\in k[t]$ integral over $k[t^2,t^3]$, $\bar{y}$ integral over $k[x]$, $\bar{y}\in k[x,y]/(y^n+a_{n-1}(x)y^{n-1}+\dots+a_0(x))$

Key lemma M a fin gen A-mod, $\mathfrak{a}\subset A$ an ideal, $\varphi: M\to M$ homo with $\varphi(M)\subset \mathfrak{a}M$.

Then $\exists a_i\in\mathfrak{a}$ s.t. $\varphi^n + a_1\varphi^{n-1}+\dots+a_n I = 0$ in $\mathrm{End}_A(M)$.

Pf. Let $x_1,\dots,x_n$ gen of M, $\varphi(x_i) = \sum a_{ij}x_j$, $a_{ij}\in\mathfrak{a}$ so $\sum_j(\delta_{ij}\varphi - a_{ij})x_j = 0$. ~~Multiplying~~ Let $u_{ki}\in \mathrm{End}(M)$ s.t. (u_{ki}) is the adj of $(\delta_{ij}\varphi - a_{ij})$ [u_{ki} is a polin φ with coeff in A]. We get $\sum_{ij} u_{ki}v_{ij}x_j = 0$. But $\sum_i u_{ki}v_{ij} = \delta_{kj}d$ where $d = \det(v_{ij})$. So $dx_j = 0$ so $d(M) = 0$. Now we expand d.

Def A local ring is ...

Cor (Nakayama's lemma). If A is m-local and M is fin gen s.t. $\mathfrak{m}M = M$. Then $M = 0$

Pf: Apply Key l. to $\varphi = 1_M$ and note that $1+a_1+\dots+a_n\in A^*$.

Cor A m-loc, M f.g.$/A$, $x_1,\dots,x_n\in M$. Ass $\bar{x}_1,\dots,\bar{x}_n$ generate $M/\mathfrak{m}M$. $\Rightarrow x_1,\dots,x_n$ gen M [Pf: Apply Nak to $M/\sum Ax_i$]

Prop $A\subset B\ni x$. The foll are equiv:

1) x integral $/A$
2) $A[x]$ is a f.g. A-module
3) $A[x]\subset C$ = subring of B, f.g. as an A-module.
4) $\exists$ faithful $A[x]$-module M which is fin gen as an A-module.

([Pf. ind via $1)\Rightarrow 2)$])

Pf $1)\Rightarrow 2)\Rightarrow 3)\Rightarrow 4)$. To proove $4)\Rightarrow 1)$ take φ = mult by x in M.

Cor $A\subset B$; $x_i\in B$ integral $/A$ $(1\le i\le n)$. Then $A[x_1,\dots,x_n]$ is a f.g. A-module

(Cor) $A\subset B$ is finite iff f.g. & integral.

Cor $A\subset B$. The set C of integral elts of B over A is a subring of B [Pf. ...]

Cor $A\subset B$ integral, $B\subset C$ integral $\Rightarrow A\subset C$ integral.

Def A domain A is called *integrally closed* if $(\forall x\in Q(A)$, x integral $/A\Rightarrow x\in A)$.

(Ex $k[t^2,t^3]$ not int closed)

Cor A a domain. Then the ring $\bar{A}$ of elts of $Q(A)$ which are integral $/A$ is integrally closed (and called integr. closure of A).

Def C in ... is called the integr closure of A in B (by / any $x\in B$ integral $/C$ belongs to C)

(Prop) A fact $\Rightarrow A$ int. closed Pf .... (Cor) $k[x_1,\dots,x_n]$ int cl (Ex) $k[t]$ = int clos of $k[t^2,t^3]$.

Prop Let $A\subset B$ integral. Then

1) If $\mathfrak{b}\subset B$ ideal $\Rightarrow A/\mathfrak{b}\cap A\hookrightarrow B/\mathfrak{b}$ integral

2) If $S\subset A$ mult. closed $\Rightarrow S^{-1}A\hookrightarrow S^{-1}B$ integral

later we ... $k[x,y]/(y^2-x^3)$

Pf: 1) clear; 2) if $x\in B$, $x^n+a_1x^{n-1}+\dots+a_n = 0$. For $s\in S\Rightarrow (x/s)^n + (a_1/s)(x/s)^{n-1}+\dots+a_n/s^n = 0$.

Prop Let $A\subset B$ integral, both domains. Then A field $\Leftrightarrow B$ field.

Pf. "$\Rightarrow$" $x\neq 0$ $x^n+a_1x^{n-1}+\dots+a_n = 0\Rightarrow x(x^{n-1}+\dots+a_{n-1}) = -a_n$; "$\Leftarrow$" Let $x\in A\Rightarrow x^{-1}\in B$ integr$/A$ — $x^{-m}+a_1x^{-m+1}+\dots+a_n = 0\Rightarrow x^{-1}+a_1+a_2x+\dots+a_nx^{n-1} = 0\Rightarrow x^{-1}\in A$.

(Def) Residue field of A at a prime $A_p/pA_p = Q(A/p)$, ex $k[x,y]$ at (x) is at (y^2-x^3). $\mathbb{Z}$ at (0), (p) ...

Cor Let $A\subset B$ integral Then

1) If $q_1\subseteq q_2\subset B$ primes s.t. $q_1\cap A = q_2\cap A\Rightarrow q_1 = q_2$
2) If $q\subset B$ prime then q max $\Leftrightarrow q\cap A$ max.
3) $\forall p\subset A$ prime $\exists q\subset B$ prime s.t. $q\cap A = p$.

(*) a B-module M is faithful if $bM = 0\Rightarrow b = 0$. In other words $B\to \mathrm{End}_B(M)$ is injective.

(**) $A[x] = \{\sum a_ix^i \mid a_i\in A\}$. More generally $A[x_1,\dots,x_n] = \{\sum a_{i_1\dots i_n}x_1^{i_1}\cdots x_n^{i_n} \mid a_{i_1\dots i_n}\in A\}$.

(*) $\mathrm{End}(M)$ = homomorphisms $M\to M$; it is a non-comm ring. But the polyn in φ with coeff in A form a comm ring R so theory of determ (assumed known) from undergrad which extends to comm rings applies to R

field

Pf. For 1) if $p = q_i \cap A \Rightarrow (A/p)_p \to (B/q_1)_p$ integral [*] ....
For 2) $A/q\cap A \to B/q$ integral.....
For 3). $A_p \to B_p \ni 1 \neq 0$ & take $m \subset B_p$ max. Then $m \cap A_p = pA_p$ hence $m \cap A = p$.

(Prop) $A \subset B$ rings, C = integral clos of A in B & $S \subset A$ mult sys. Then $S^{-1}C$ = int. clos of $S^{-1}A$ in $S^{-1}B$.
Pf. Ass b/s int / $S^{-1}A$ so $(b/s)^n + (a_1/s_1)(b/s)^{n-1} + \dots + a_n/s_n = 0$. Mult by $(ts)^n$ where $t = s_1 \cdots s_n \Rightarrow$ bt integr / $A \Rightarrow bt \in C \Rightarrow b \in S^{-1}C$.

5) (Prop) Let A be an integral domain. Then A is integrally closed iff A_p is so for $\forall$ prime p, iff A_m is so for any max m.
(Lem) $f: M \to N$ inj, surj, bij iff f_p is so $\forall p$ iff f_m is so $\forall m$. (Ker & coker commutes with fract.)
~~[illegible]~~ Pf. Let C = int clos of A & $f: A \to C$. A int cl $\Leftrightarrow f: A \to C$ bij $\Leftrightarrow f_m : A_m \to C_m$ bij $\forall m$ (C_m = int cl of A_m so q-ed).

(Def) Let A be any ring. By $\dim A$ we underst the max n s.t $\exists$ primes $p_0 \subsetneq p_1 \subsetneq \dots \subsetneq p_n$ (chain of length n).

(Ex) $\dim(\text{field}) = 0$; $\dim \mathbb{Z} = 1$, $\dim k[x,y,z] \geq 3$ (we will see $= 3$) for we have $0 \subset (x) \subset (x,y) \subset (x,y,z)$

2) (Prop) $A \subset B$ integral $\Rightarrow \dim A = \dim B$.
Pf. Any chain in B $q_0 \subsetneq \dots \subsetneq q_m \Rightarrow q_0 \cap A \subsetneq \dots \subsetneq q_m \cap A$ so $\dim A \geq \dim B$. ($m = \dim B$)
Now let $p_0 \subsetneq \dots \subsetneq p_n \subset A$ ($n = \dim A$). We lift it inductively. Assume $\dots \subset p_i \subset p_{i+1}$, $\dots \subset q_i$.
Since $A/p_i \to B/q_i$ integr $\exists$ prime in B/q_i over $p_{i+1}/p_i \Rightarrow$ q.e.d.

3) (Th) (Noether normalis) k an infinite field, A a f.g. k-alg. $\exists\, y_1, \dots, y_d \in A$ alg ind/k s.t. A integral / $k[y_1, \dots, y_d]$ (holds also for k finite but diff arg!)

not needed

Pf. Induction on min number of gen. Ass O.K for $\leq n-1$ & $A = k[x_1, \dots, x_n]$. If $x_1, \dots, x_n$ alg ind/k, O.K. If not (after renumbering x_i) x_n alg / $k[x_1, \dots, x_{n-1}]$, $f(x_1, \dots, x_{n-1}; x_n) = 0$
Let F be the form of highest degree in f and put $x_i = x_i' + \lambda_i x_n$ ($i < n$) where $F(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$
$\Rightarrow x_n$ integral / $k[x_1', \dots, x_{n-1}']$ & apply induction. (L) F form $\neq 0$, k infinite $\Rightarrow F$ does not van.

2) (Prop) If in the stat above $A = k[x_1, \dots, x_M]/(f)$, $f \neq 0$ then we can take $d = M-1$.
Pf. Let F be the form of highest deg in f, put $x_i = x_i' + \lambda_i x_n$ ($i < n$) & $x_n = x_n'$ us...
This is an aut of $k[x_1, \dots, x_n]$. We may ass it is the ident. So $f = x_n^e + g_1(x_1, \dots, x_{n-1}) x_n^{e-1} + \dots$
So $\bar{x}_n \in A$ integral / $k[\bar{x}_1, \dots, \bar{x}_{n-1}]$. Now $\bar{x}_1, \dots, \bar{x}_{n-1}$ alg ind/k [if $h(\bar{x}_1, \dots, \bar{x}_{n-1}) = 0 \Rightarrow h = f \cdot g$ in $k[x_1, \dots, x_n]$ so f for $\deg_{x_n} h = 0$, $\deg_{x_n}(fg) \geq e$!].

8) (Prop) $\dim k[x_1, \dots, x_n] = n$
Pf. Ind on n. Let $d = \dim k[x_1, \dots, x_n]$, $0 = p_0 \subset p_1 \subset \dots \subset p_d$, $f \in p_1$, $f \neq 0$ $\Rightarrow f = \prod$ primes
replace f by a prime factor so ass f prime; $(f) \subset p_1 \Rightarrow p_1 = (f)$. We have
$\dim k[x_1, \dots, x_n]/p_1 = n-1$ so the chain $\frac{p_1}{p_1} \subset \dots \subset \frac{p_d}{p_1}$ has length $\leq n-1$ (ind hyp + prop 2)
so $d - 1 \leq n-1$ so $d \leq n$. On the other hand clearly $d \geq n$ $[0 \subset (x_1) \subset (x_1, x_2) \subset \dots \subset (x_1, \dots, x_n)]$

(Th) Let A be a domain f.g / k. Then $\dim A = \text{tr.deg}\, Q(A)/k$.
Pf (3) + (8)

~~[illegible]~~ Stop

[*] If $A \xrightarrow{u} B$ and $p \subset A$ prime we put $B_p := S^{-1}B$ where $S = u(A \setminus p)$.

(Th) (Hilbert's Nullstellensatz) k alg closed field, $a \subsetneq k[x_1, \dots, x_n]$ ideal $\Rightarrow \exists\, \alpha \in k^n$, $f(\alpha) = 0$ $\forall f \in a$
Pf. May ass $a = m$ max. Set $K = k[x_1, \dots, x_n]/m$. Noether normalis $\Rightarrow K$ integral / $k[z_1, \dots, z_s] \Rightarrow$ $k[z_1, \dots, z_s]$ field $\Rightarrow s = 0 \Rightarrow K \cong k \Rightarrow$ $L = k \Rightarrow$ Take $\alpha_i = \bar{x}_i$

21 Noetherian rings. Dedekind rings / Discrete valuation rings,

Def) An A-module M is called Noetherian if $\forall$ ascending chain of submod is stationary ($M_1 \subseteq M_2 \subseteq \cdots \Rightarrow \exists i$ s.t. $M_i = M_j$ $\forall j > i$). A ring is called Noeth if ...

(α) Prop) M is noeth iff any submod is fin gen [Pf: ...]

$\equiv$ Prop) $0 \to M' \to M \to M'' \to 0$ exact (i.e. $M'' = M/M'$). Then M Noeth $\Leftrightarrow$ M' & M'' Noeth

(β) Cor) A Noeth ring, M fin gen A-mod $\Rightarrow$ M Noeth [Pf: $M = A^n/N$]

don't need $\to$ Th) (Hilbert basis th.) A Noeth $\Rightarrow$ $A[x_1, \dots, x_N]$ Noeth.

Pf. Ind $\Rightarrow$ suff for $n = 1$. Put $B = A[x]$. Let $\underline{b} \subset B$ ideal. Let $\underline{a} = \{ a \in A \mid \exists f \in \underline{b}$ whose leading coeff is a i.e. $f = ax^n + \dots \}$. $\Rightarrow \underline{a} = (a_1, \dots, a_n) \Rightarrow \exists f_i = a_i x^{k_i} + \dots \in \underline{b}$

Let $k = \max k_i$, $\underline{b}' = (f_1, \dots, f_n) \subset \underline{b}$. Let $M = A + Ax + \dots + Ax^{k-1} \subset B$. (same as β...)

Claim: $\underline{b} = (\underline{b} \cap M) + \underline{b}'$ (this closes the pf for $\underline{b} \cap M$ is f.g. A-mod by (α) & (β))

$\supset$ clear; for $\subset$ induction on degrees. Let $f \in \underline{b} \Rightarrow f = ax^n + \dots \Rightarrow a = \sum u_i a_i$

$\Rightarrow f - \sum u_i f_i x^{n-k_i} \in \underline{b}$ and has degree $< n \overset{\text{ind}}{\Rightarrow} f - \sum u_i f_i x^{n-k_i} \in (\underline{b} \cap M) + \underline{b}' \Rightarrow f \in (\underline{b} \cap M) + \underline{b}'$

don't need $\to$ Cor) A Noeth, B fin gen A-alg $\Rightarrow$ B Noeth.
$k[x_1, \dots, x_N]$ Noeth.

$\equiv$ Prop) A Noeth $\Rightarrow$ $S^{-1}A$ Noeth [use $b = S^{-1}(b^c)$]

Prop) Let A be Noeth. Any rad ideal a (i.e. $a = \sqrt{a}$) can be uniquely written as $p_1 \cap \dots \cap p_r$, p_i primes. [p_i are called the components of a].

Pf: Call an ideal a irred if $a = b \cap c \Rightarrow a = b$ or $a = c$.

Claim 1: any$^+$ ideal = finite inters of irred$^+$ ones [Let Σ be the set of ideals$^+$ which are not finite inters of irr$^+$ id; if $\Sigma \neq \emptyset$ it has a max elt (by Noeth) a

$\Rightarrow a = b \cap c$, $a \subsetneq b$, $a \subsetneq c$ $^\heartsuit \Rightarrow b \notin \Sigma$, $c \notin \Sigma \Rightarrow a \notin \Sigma$ do]. Claim 2. Any irred radical ideal a is prime [passing to A/a can ass $a = (0)$. So let (0) be irred $xy = 0$ but $x \neq 0, y \neq 0$. Let $\mathrm{Ann}(x) \subset \mathrm{Ann}(x^2) \subset \cdots \Rightarrow \mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1}) \Rightarrow (x^n) \cap (y) = 0$ (check!)

$\Rightarrow (x^n) = 0 \Rightarrow x = 0$ do] Uniqueness easy.

$\equiv$ Prop) A Noeth, $a \subset A$ id $\Rightarrow \exists n$ $(\sqrt{a})^n \subset a$. ((0) radical)

Def) K a field. A discrete val is a (surj) map $v : K \to \mathbb{Z} \cup \{\infty\}$ s.t. $\begin{cases} v(x) = \infty \Leftrightarrow x = 0 \\ v(xy) = v(x) + v(y) \\ v(x+y) \geq \min(v(x), v(y)) \end{cases}$

ex) $K = \mathbb{Q}$, v = exponent of p in x. ; $K = k((x))$, v = order

$\equiv$ Prop) If $v : K \to \mathbb{Z} \cup \{\infty\}$ is a discr val $\Rightarrow A = \{ x \in K \mid v(x) \geq 0 \}$ is a local ring with max ideal $m = \{ x \in K \mid v(x) > 0 \}$. Moreover if $v(x) = 1 \Rightarrow$ any ideal has the form (x^n) (so A Noeth)

Pf: $v(1) = 0$. If $v(x) \geq 0 \Rightarrow 0 \leq v(x^2) = v((-x)^2) = 2v(-x) \Rightarrow v(-x) \geq 0 \Rightarrow A$ subring, easy

Def) A domain A is called DVR if $\exists$ val $v : Q(A) \to \mathbb{Z} \cup \{\infty\}$ s.t. $A = \{ x \in K \mid v(x) \geq 0 \}$

So a DVR is local, Noeth of dim = 1. Any $x \in A$ s.t. $v(x) = 1$ is called a parameter of A.

Th) A Noeth domain, A local, $\dim A = 1$, m its max id, $k = A/m$ (res field). Equiv:

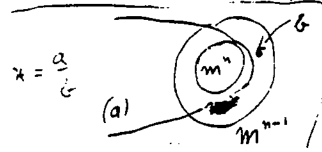
enough 1, 2, 5 equiv

1) A is DVR
2) A is integrally closed
3) m principal ($m = (x)$)
4) $\dim_k m/m^2 = 1$
5) $m = (x)$ & $\forall$ non-zero ideal has form (x^k).

$^+$ radical $\quad$ $^\heartsuit$ may ass b, c radical $\quad$ ($a = \sqrt{a} = \sqrt{b} \cap \sqrt{c}$)

Pf. 1)⇒2) Let $x \in Q(A)$, $x^n + a_1 x^{n-1} + \dots + a_n = 0$, $a_i \in A$. If $v(x) \geq 0$ O.K. If $v(x) < 0 \Rightarrow$
$\Rightarrow v(x^{-1}) > 0 \Rightarrow x^{-1} \in A \overset{:x^{n-1}}{\Rightarrow}$ $\underbrace{x + a_1 + a_2 x^{-1} + \dots + a_n x^{-n+1}}_{}= 0 \Rightarrow x \in A$ do.

2)⇒3) Let $0 \neq a \in m$. $\Rightarrow \underset{(\text{claim } m = (x))}{\sqrt{(a)} = m} \Rightarrow \exists n$ s.t. $m^n \subset (a)$, $m^{n-1} \not\subset (a)$. Choose $b \in m^{n-1} \setminus (a)$, $x = a/b \in Q(A)$. We have $x^{-1} \notin A$ (for $b \notin (a)$) $\Rightarrow x^{-1}$ not integral$/A$ so $x^{-1} m \not\subset m$ (for m is a faithfull $A[x^{-1}]$-module f.g. $/A$ (Theorem)). But $x^{-1} m \subset A$ (for $x^{-1} m = \frac{b}{a} m$ and $bm \subset m^n \subset (a)$) so $x^{-1} m = A$ so $m = xA = (x)$.



3)⇐4) by Nakayama. (Lect 2)

3)⇒5) Let $a \subset A$ ideal $\neq (0), (1)$. $\Rightarrow \sqrt{a} = m \overset{(x)}{=} \Rightarrow \exists n$ s.t. $(x^n) \subset a$ $\overset{Nak}{\Rightarrow} \exists n$ s.t. $a \subset (x^n)$, $a \not\subset (x^{n+1})$.
Choose $y \in a \setminus (x^{n+1})$ and write $y = \alpha x^n$ ($\alpha \in A$). $\Rightarrow \alpha \notin m = (x)$
$\Rightarrow \alpha$ invertible $\Rightarrow x^n \in a \Rightarrow$ $\Rightarrow a = (x^n)$.

5)⇒1) $(x^k) \neq (x^{k+1})$ by Nakayama so $\forall y \in A$, $(y) = (x^k)$ for exactly one k. Put $v(y) = k$ and $v(y/z) = v(y) - v(z)$. Check it is OK.

Def A Dedekind domain is a Noeth domain A integrally closed of $\dim A = 1$.

Prop Let A be Noeth (domain) of $\dim A = 1$. Equiv are:
1) A is integrally closed (i.e. A is Dedekind)
2) $\forall p \neq 0$ prime, A_p is a DVR. [Pf. Lect 2, (δ) and above Th.]

(α) **Prop** Let A be DVR with parameter x. Then if $k = A/(x)$ $\Rightarrow \dim_k \frac{A}{(x^n)} = n$.
$\underbrace{k \hookrightarrow A \to k}_{id}$

don't need

Pf. Ex. seq. $0 \to \frac{(x^n)}{(x^{n+1})} \to \frac{A}{(x^{n+1})} \to \frac{A}{(x^n)} \to 0$. So suff $\dim \frac{(x^n)}{(x^{n+1})} = 1$. That ≤ 1 clear. That $\neq 0$ of Nakayama.

Ex $f \in k[x,y]$ irred polyn $f(0,0) = 0$ (i.e. $f \in (x,y)$) and $A = (k[x,y]/(f))_{(\bar{x},\bar{y})}$
Then A is a local domain of dim 1 (Lect 2, (α)). It is a DVR iff either $a := \frac{\partial f}{\partial x}(0,0) \neq 0$ or $b := \frac{\partial f}{\partial y}(0,0) \neq 0$. For if $f = ax + by +$ (higher terms) then $\frac{m}{m^2} \approx \frac{kx + ky}{k(ax + by)}$
because $m = (x,y)/(f)$, $m^2 = ((x,y)^2 + (f))/(f)$ so $\frac{m}{m^2} = \frac{(x,y)}{(x,y)^2 + (f)} = \frac{(x,y)}{(x,y)^2 + (ax+by)} = \frac{(x,y)/(x,y)^2}{((x,y)^2 + (ax+by))/(x,y)^2}$
so if $a \neq 0$, $\bar{y}$ is a par while if $b \neq 0$, $\bar{x}$ is a par.

Ex $A = (k[x,y]/(y^2 - x^3))_{(\bar{x},\bar{y})} \hookrightarrow k[t^2,t^3]_{(t^2,t^3)} \hookrightarrow k[t]_{(t)} =$ integral clos of A
not a DVR. $\quad x \mapsto t^2$, $y \mapsto t^3$

~~(++) A Noeth, $a \subset A$ ideal $\Rightarrow \exists n$ s.t. $(\sqrt{a})^n \subset a$. Pf: ...~~

~~(+) Lemma M f/g A-mod, A local with max id m. Ass $x_1, \dots, x_n \in M$ are s.t. $\bar{x}_1, \dots, \bar{x}_n$ gen M/mM as a $k = A/m$-vect sp. Then $x_1, \dots, x_n$ gen M.
Pf. $M' = \sum A x_i$. Then $m(M/M') = \frac{mM + M'}{M'} = \frac{M}{M'}$ so $\frac{M}{M'} = 0$ so $M = M'$.~~

($m_p \in \mathbb{N}$)

(ω) **Prop** A Dedekind dom $\underline{a} \subset A$ ideal. Set for each prime id $p \subset A$, $\underline{a}A_p = p^{m_p}A_p$ (OK bec A_p is DVR). Then $m_p = 0$ for almost all m_p & $\underline{a} = \prod p^{m_p}$. Call $m_p = m_p(\underline{a})$
In partic if $\underline{a}, \underline{b} \subset A$ ideals $\neq 0$ & $\underline{a} \subset \underline{b} \Rightarrow \exists\, \underline{c} \subset A$ s.t. $\underline{a} = \underline{b}\,\underline{c}$

<u>Pf</u> $m_p = 0$, almost all p bec in $\forall$ noeth ring $\forall$ rad id is $\cap$ of fin many primes (if not take max elt in set of rad id that are not $\cap$ of fin many pr. id.) Now if $\underline{a}' := \prod p^{m_p}$ we have $\underline{a}_p = \underline{a}'_p$ $\forall p$ so if $M = (\underline{a} + \underline{a}')/\underline{a}$ get $M_p = 0$ $\forall p$ so $M = 0$ so $\underline{a} = \underline{a}'$.

Def A Ded dom with fr. field K. Set $I = I(A)$ = free ab sgr gen by pr id of A (= set of non zero ideals, above prop) & $P = P(A) \subset I$ semigr of principal ideals. More gen if $c \in I$ let $I(c)$ = semigr of all $a \in I$ prime to c & $P_c^+ = \{(\alpha) \in P \mid \alpha \equiv 1 \bmod^* c\}$ where $\alpha \equiv 1 \bmod^* c$ means that "$m_p(c) > 0 \Rightarrow \alpha \equiv 1 \bmod p^{m_p(c)}$" & "$\sigma \in \mathrm{Hom}(K, \mathbb{R}) \Rightarrow \sigma\alpha > 0$". "totally pos"

Def Let I be <u>any</u> abelian semigr & $P \subset I$ <u>any</u> ab subsemigr. Call P full if
1) $x, y \in I$ & $x, xy \in P \Rightarrow y \in I$ & 2) $\forall x \in I, \exists y \in I$ s.t. $xy \in P$. Then may def a group $I/P := I/\sim$ where $x \sim y \Leftrightarrow \exists a, b \in P$ s.t. $ax = by$. [2) insures $\exists$ of inverse] [1) insures that $\exists$ bij bet full subgr of I containing P & subgr of I/P] (+)

Prop If A is Dedekind P is a full semigr of I & P_c^+ full in $I(C)$. The gr homo $I(c)/P_c^+ \to I/P$ is surj. (I/P called class gr; $I(c)/P_c^+$ ray class gr)

<u>Pf</u>. If $\underline{a} \in I(c)$ by Chin Rem th (++)

Ex If $A = \mathbb{Z}$, $c = m\mathbb{Z} \Rightarrow I(c)/P_c^+ \simeq (\mathbb{Z}/m\mathbb{Z})^*$
& ray classes in $\mathbb{Z}$ are arithm progr.

(equiv cl in $I(c)$ are called ray classes.)

(22) Ramification

(α) **Th** (Fin. of rel. int. clos) A int closed Noeth. dom, $K = Q(A)$, L/K fin sep., B = int clos of A in $L \Rightarrow B$ if finite A-module (So if A Dedekind $\Rightarrow B$ Dedekind)

<u>Pf</u>. Let $u_1, \dots, u_n \in L$ basis$/K$, Mult by some $a \in A \Rightarrow$ may ass $u_i \in B$. Let $v_1, \dots, v_n \in L$ s.t. $Tr(u_i v_j) = \delta_{ij}$ (by (17)). Claim $B \subset Av_1 + \dots + Av_n$ (& done) Write $b \in B$ as $b = \sum \lambda_i v_i$, $\lambda_i \in K$. Note $\forall \sigma \in \mathrm{Hom}_K(L, \bar{K}) \Rightarrow \sigma B = B$. So $Tr\, B \subset A$. So $Tr(u_i b) \in A$. But $Tr(u_i b) = \sum_j \lambda_j Tr(u_i v_j) = \lambda_i$. Done.

Prop Not as in (α), $S = A \setminus \{0\} \Rightarrow L = S^{-1}B$ [$K \to S^{-1}B$ integral, K field $\Rightarrow S^{-1}B$ field so $= L$]

(ε) **Th** Not as in (α). Ass L/K Galois. Let $p \subset A$ prime & $\mathfrak{P}, \mathfrak{P}' \subset B$ primes lying over p i.e. whose $\cap$ with A is p. Then $\exists\, \sigma \in G(L/K)$ s.t. $\sigma\mathfrak{P} = \mathfrak{P}'$.

<u>Pf</u>. Localizing may ass p max. Ass $\mathfrak{P} \neq \sigma\mathfrak{P}'$, $\forall \sigma \in G(L/K)$. Chinese rem th $\Rightarrow$
$\Rightarrow \exists\, x \in B$ s.t. $x \equiv 0 \bmod \mathfrak{P}$ & $x \equiv 1 \bmod \sigma\mathfrak{P}'$, $\forall \sigma$. As in (α) $\sigma B = B$ so $Nx = \prod \sigma x \in \mathfrak{P} \cap A = p$ (bec $x \in \mathfrak{P}$). But $x \notin \sigma\mathfrak{P}'$ $\forall \sigma$ so $\sigma x \notin \mathfrak{P}'$ $\forall \sigma$ so $Nx \notin \mathfrak{P}'$

(+) Use $A = \cap A_p$ [more gen, this is true for $\forall$ domain: $A = \cap A_m$, $m \in \mathrm{Max}\,A$. Pf: Let $x \in K$, $x \in \cap A_m$,

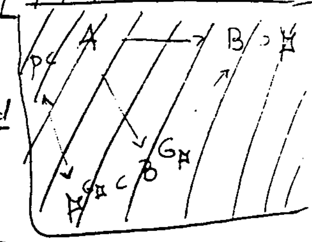
(+) If $P \subset I$ arbitrary semigr, I/P is only semigr.

(++) $\exists\, \alpha \in A$, $\alpha \equiv 0 \bmod \underline{a}$ & $\alpha \equiv 1 \bmod p^{m_p(c)}$ if $m_p(c) > 0$. So $(\alpha^2) \subset \underline{a}$ So by (ω) $\exists\, \underline{b} \in I$ s.t. $(\alpha^2) = \underline{a}\,\underline{b}$. Clearly α^2 tot pos so $\alpha^2 \equiv 1 \bmod^* c$ So axiom 2) in def of "full" is OK. So is ax 1). For "surj" use again Chinese

(Cor) Not as in (α) ⟹ over each pr in A $\exists$ only fin many pr in B [embed L in its Gal ext$/K$]

(β) (Def) Not as in (α), $p \subset A$ max, $\mathfrak{P} \subset B$ over it. Ass $L|K$ Galois with gr G.
Define <u>decompos gr</u> $G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$. Get $G_{\mathfrak{P}} \to G(B|\mathfrak{P}/A|p)$, $\sigma \mapsto \bar\sigma$.
~~Define decompos field as $L^{G_{\mathfrak{P}}}$. Clearly $B^{G_{\mathfrak{P}}} = B \cap L^{G_{\mathfrak{P}}}$ is the int clos of A in $L^{G_{\mathfrak{P}}}$ & $\exists!$ prime in $B^{G_{\mathfrak{P}}}$ lying over $\mathfrak{P}$ (namely $\mathfrak{P}^{G_{\mathfrak{P}}} = \mathfrak{P} \cap B^{G_{\mathfrak{P}}}$)~~

~~Prop Not as in (α)~~ Define <u>inertia gr</u> $T_{\mathfrak{P}} = \ker(G_{\mathfrak{P}} \to G(\frac{B}{\mathfrak{P}}/\frac{A}{p}))$.



(γ) (Def) Not as in (α) & ass A, B Dedekind. Define <u>ramif ind</u> $e_{\mathfrak{P}} := e(\mathfrak{P}/p)$ by formula $pB_{\mathfrak{P}} = \mathfrak{P}^{e(\mathfrak{P}/p)}B_{\mathfrak{P}}$ & <u>residue class degree</u> by $f_{\mathfrak{P}} = f(\mathfrak{P}/p) = [\frac{B}{\mathfrak{P}} : \frac{A}{p}]$. Define <u>norm</u> $N_{L|K}\mathfrak{P} = p^{f_{\mathfrak{P}}}$

Have 2 homo 1) $N_{L|K} : I(B) \to I(A)$ obtained by extending by linearity.
2) $I(A) \to I(B)$ obtained by extendg $p \mapsto pB$ by lin.
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \overset{\shortparallel}{\prod \mathfrak{P}_i^{e(\mathfrak{P}_i/p)}}$

Both are comp with compos of separ ext

Say p <u>splits completely</u> if $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$ $\forall \mathfrak{P}|p$ (wd for $\mathfrak{P} \cap A = p$)
p <u>ramifies</u> if $\exists \mathfrak{P}|p$ s.t. $e(\mathfrak{P}/p) \geq 2$.

(δ) (Prop) Not as in (γ) ~~& A, B Dedekind~~ Then $[L:K] = \sum_{\mathfrak{P}|p} e_{\mathfrak{P}} f_{\mathfrak{P}}$.

<u>Pf</u> May ass A a DVR. So B free A-mod of rank $n = [L:K]$

Write $pB = \prod \mathfrak{P}_i^{e_i}$. Chinese rem th ⟹ $B/pB \simeq \bigoplus B/\mathfrak{P}_i^{e_i}$ as $\frac{A}{p}$-vect sp.

~~($\mathfrak{a} = \prod$ ... more gen ... concede)~~

Now estimate $\dim_{A/p}$ & done [for $B/\mathfrak{P}^e$ use $B/\mathfrak{P}^e = B_{\mathfrak{P}}/\mathfrak{P}^e$ & filtr with powers of $\mathfrak{P}B_{\mathfrak{P}}$]

(Cor) Not as in (γ). For $\mathfrak{a} \in I(A)$, $N_{L|K}(\mathfrak{a}B) = \mathfrak{a}^{[L:K]}$ [Use above prop].

(ω) (Cor) Not as in (γ) & ass $L|K$ Galois with group G as in (β). Let $p = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ (write $e_i = e_{\mathfrak{P}_i}$, $f_i = f_{\mathfrak{P}_i}$). Then $e_1 = \cdots = e_r = e$; $f_1 = \cdots = f_r = f$ & $(N_{L|K}\mathfrak{P})B = \prod_{\sigma \in G} \sigma\mathfrak{P}_i = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^{ef}$ ($n = efr$) & $|G_{\mathfrak{P}_i}| = ef$

<u>Pf</u> By Th (ε) G oper trans on $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$ & isotr gr of $\mathfrak{P}_i$ is decomp gr $G_{\mathfrak{P}_i}$.
So $e_i = e$, $f_i = e$ & $n = efr$ (by (ε)) & $|G_{\mathfrak{P}_i}| = ef$ & ~~...~~ $N\mathfrak{P}_i = p^f$ so
$N_{L|K}\mathfrak{P}_i = p^f B = (\prod \mathfrak{P}_i^{e_i})^f = (\prod \mathfrak{P}_i)^{ef} = \prod_{\sigma \in G} \sigma\mathfrak{P}_i$

(·) (Prop) Notations as in (β) & (γ) (so A, B Ded & $L|K$ normal) (& finite res fields). Ass p prime in A, $\mathfrak{P} \subset B$, $\mathfrak{P}|p$. & ass $e(\mathfrak{P}/p) = 1$. Then $G_{\mathfrak{P}} \to G(\frac{B}{\mathfrak{P}}/\frac{A}{p})$ is an isomorphism.

<u>Pf</u> By (ω) both $G_{\mathfrak{P}}$ & $G(\frac{B}{\mathfrak{P}}/\frac{A}{p})$ have same cardin. So it is enough to prove homo $G_{\mathfrak{P}} \to G(\frac{B}{\mathfrak{P}}/\frac{A}{p})$ is ~~surjective~~ ~~...~~

<u>Spec Case</u> $r = 1$ (i.e. $G = G_{\mathfrak{P}}$) Let $\bar{x} \in \frac{B}{\mathfrak{P}}$ ~~be a gen of~~ ~~(sep clos of ...)~~ $\frac{B}{\mathfrak{P}}/\frac{A}{p}$.

injective. Assume $\sigma \in G_{\mathfrak{P}}$ is identity on ~~max sep ext of~~ $B/\mathfrak{P}$. By induction ~~...~~ σ is the identity on $B/\mathfrak{P}^n$ for all n. By $\bigcap \mathfrak{P}^n B_{\mathfrak{P}} = 0$ ⟹ $\sigma = \mathrm{id}$ on $B_{\mathfrak{P}}$ hence on B. qed//.

Express any elt of $\frac{B}{\mathfrak{P}^n}$ as $\theta + \pi\beta$ where $\mathfrak{P}B_{\mathfrak{P}} = (\pi)$
$\theta^{q-1} = 1$ (cf Hensel, $q = \#\frac{B}{\mathfrak{P}}$) and $\beta \in B/\mathfrak{P}^{n-1}$

(& all roots $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ of f in L lie in B)

image of $x \in B$. Set $f = \mathrm{Irr}(\alpha, K)$. Since $GB \subset B \Rightarrow$ coeff of $f \in B \cap K = A$. So $f = \prod (x - \alpha_i)$ in $B[x]$. So its red mod $\mathfrak{P}$, $\bar f = \prod (x - \bar\alpha_i)$ in $\frac{B}{\mathfrak{P}}[x]$. Let $\bar\sigma \in G(\frac{B}{\mathfrak{P}}/\frac{A}{p})$. Must have $\bar\sigma \bar\alpha = \bar\alpha_j$ for some j. L/K Gal $\Rightarrow$ $\exists\ \sigma \in G(L/K)$, $\sigma\alpha = \alpha_j$. Clearly σ induces $\bar\sigma$.

Gen. case r arbitrary. Idea: Replace K by $L^{G_\mathfrak{P}}$ ($\exists$! prime lying over p namely $\mathfrak{P} \cap B^{G_\mathfrak{P}}$) (appl to $L/L^{G_\mathfrak{P}}$) By (α) $G_\mathfrak{P}$ acts trans on primes in B lying over $\mathfrak{P} \cap B^{G_\mathfrak{P}} \subset B^{G_\mathfrak{P}}$; but $G_\mathfrak{P}$ acts triv on $\mathfrak{P}$. So $S = \{\mathfrak{P}\}$; one is left to check $\frac{A}{p} = \frac{B^{G_\mathfrak{P}}}{\mathfrak{P} \cap B^{G_\mathfrak{P}}}$; use smth. sim to pf. of (α)

(Def) Not as in (α), L/K Galois. Let $p \subset A$ prime & $\mathfrak{P} \subset B$, $\mathfrak{P} | p$. Ass p not ramif i.e. $e(\mathfrak{P}/p) = 1$ & A/p finite. Then by (16) $G(\frac{B}{\mathfrak{P}}/\frac{A}{p})$ is gen by Frob $\phi x = x^{\mathrm{card}\frac{A}{p}}$. By (7) $\exists$! aut den by $(\mathfrak{P}, L/K) \in G_\mathfrak{P}$ inducing ϕ. If L/K abelian all $(\mathfrak{P}, L/K)$ coincide. Call this $\sigma = (p, L/K) \in G$ the "Artin symbol". If let $N(p) = \mathrm{card}\,\frac{A}{p}$ (absolute norm) have $\sigma x \equiv x^{N(p)} \bmod \mathfrak{P}$, all $x \in B$, all $\mathfrak{P} | p$.

(Def) Ass not as in (α), L/K Galois abelian, Ass A/p finite $\forall$ prime & let $c \subset A$ be s.t. $\forall$ prime $p \subset A$, $p \nmid c$ is non-ramif (*). Then extend Artin symbol by linearity to sgr homo ("reciprocity map")

$$(-, L/K) : I(c) \to G(L/K)$$

Let $I(cB) \subset I(L)$ be the sgr of elts of $I(B)$ prime to cB.

Remark (**): if $b \in I(cB)$ then $(N_{L/K} b, L/K) = 1$ [Indeed, suff $b = \mathfrak{P}$ prime. But then $N_{L/K}\mathfrak{P} = p^f$ where $p = \mathfrak{P} \cap A$, $f = [\frac{B}{\mathfrak{P}} : \frac{A}{p}]$. So $(N_{L/K}\mathfrak{P}, L/K) = (p, L/K)^f$. But $(p, L/K)$ generates $G_\mathfrak{P} \simeq G(\frac{B}{\mathfrak{P}}/\frac{A}{p})$ & latter has order $f \Rightarrow$ done].

Remark if $p \subset A$ not ramif then: p splits compl. (ω) $\Leftrightarrow G_\mathfrak{P} = 1\ \forall \mathfrak{P}|p \Leftrightarrow (p, L/K) = 1$ (L/K abelian) Write $p = N\mathfrak{P}$ for some $\mathfrak{P}|p$

Write $L', \mathfrak{P}', B', \dots$ instead of $L^{G_\mathfrak{P}}, \mathfrak{P}^{G_\mathfrak{P}}, B^{G_\mathfrak{P}}, \dots$

Take $x \in B'$ & seek an elt $z \in A$ s.t. $z \equiv x \bmod \mathfrak{P}'$. Do as follows. By Cheb. $\exists\ y \in B'$ s.t. $y \equiv x \bmod \mathfrak{P}'$ & $y \equiv 1 \bmod \sigma^{-1}\mathfrak{P} \cap B'$, $\forall \sigma \in G \setminus G_\mathfrak{P}$. Hence in partic have $y \equiv x \bmod \mathfrak{P}$ & $\sigma y \equiv 1 \bmod \mathfrak{P}$, $\forall \sigma \in G \setminus G_\mathfrak{P}$

Set $z = N_{L'/K}\, y = y \cdot \prod_{\sigma \in (G \setminus G_\mathfrak{P})/G_\mathfrak{P}} \sigma y \equiv x \bmod \mathfrak{P}$ hence mod $\mathfrak{P}'$

$\cap B'$

$B \cap K = A$

qed//

(**) So have induced (semigr) homo $(-, L/K) : I(c)/N_{L/K} I(cB) \to G(L/K)$; but in gen $(P_i^+, L/K) \neq 1$!

(*) such a c exists in # field case as we shall see.

23) Number fields ~~[illegible]~~ I : class number

By 7, $\mathcal{O}$ is a free ab gr ($\mathbb{Z}$-module) of rk $[K:\mathbb{Q}]$

Def A number field means a fin ext K of $\mathbb{Q}$. One lets $\mathcal{O} := \mathcal{O}_K$ = int clos of $\mathbb{Z}$ in K. (called its ring of integers : it is Dedekind by 22, (α). Prime ideals of $\mathcal{O}_K$ are called primes of K. If $K \subset L$ # fields & p prime of K say p ramifies in L or splits compl in L (a.s.o.) if it does so in $\mathcal{O}_L$. Set $Cl(K) = I(\mathcal{O}_K)/P(\mathcal{O}_K)$, a.s.o. Have norm $N = N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ inducing $N : \mathcal{O}_K \to \mathbb{Z}$. cf 17. Also have $N : I(\mathcal{O}_K) \to I(\mathbb{Z})$. cf 22. Easy to see $N((a)) = (Na)$ (i.e $N(a\mathcal{O}_K) = Na\,\mathbb{Z}$) for $a \in \mathcal{O}_K$ [Indeed mult of both N's $\Rightarrow$ may ass $K/\mathbb{Q}$ normal & use Cor (ω) in 22 ; use also that $\alpha^n\mathbb{Z} = \beta^n\mathbb{Z}$, $\alpha,\beta \in \mathbb{Z} \Rightarrow \alpha\mathbb{Z} = \beta\mathbb{Z}$] Also easy to see for $\underline{a} \subset \mathcal{O}_K$ ideal have $N\underline{a} = (\#\mathcal{O}_K/\underline{a})\mathbb{Z}$ (set $N\underline{a} = \#\,\mathcal{O}_K/\underline{a}$) [by Chines rem th may ass $\underline{a} = \mathfrak{p}^n$; for this case compute dim as $\mathbb{F}_p$ - vect space].

L (Hurwitz lemma) ("Generalized Euclid division") Let K be a # field. Then $\exists\, M \in \mathbb{Z}^+$ s.t. $\forall\, \alpha, \beta \overset{\neq 0}{\in} \mathcal{O} = \mathcal{O}_K$ $\exists$ integer t, $1 \le t \le M$ & $\exists\, \omega, \rho \in \mathcal{O}$ s.t.
$$t\alpha = \omega\beta + \rho \quad \& \quad |N(\rho)| < |N(\beta)|.$$

Pf. Let $\omega_1, \dots, \omega_n$ be $\mathbb{Z}$-basis of $\mathcal{O}$. Embed $\varphi : K \to \mathbb{Q}^n \subset \mathbb{R}^n$, $\varphi(\sum \lambda_i \omega_i) = (\lambda_1, \dots, \lambda_n)$ $\lambda_i \in \mathbb{Q}$. Let $|\ | : \mathbb{R}^n \to \mathbb{R}_+$ be $|(\lambda_1,\dots,\lambda_n)| = \max_i |\lambda_i|$. Clearly $\exists\, C > 0$ s.t. $z \in K \Rightarrow$ $|N(z)| \le C|\varphi(z)|^n$ [indeed $|N(z)| = |N(\sum \lambda_i \omega_i)| = |\prod_\sigma (\sum_i \lambda_i \sigma\omega_i)| \le \cdots$]. Choose integer $m > \sqrt[n]{C}$ & $M = m^n + 1$. Set $\gamma = \alpha/\beta \in K$. Want $\omega \in \mathcal{O}$, $\gamma \in K$ st $t\gamma = \omega + \delta$ with $|N(\delta)| < 1$. For $\forall\, \theta \in K$ $\theta = \sum \lambda_i \omega_i$, $\lambda_i \in \mathbb{Q}$ write $\theta = [\theta] + \{\theta\}$ where $[\theta] = \sum [\lambda_i]\omega_i$, $\{\theta\} = \sum \{\lambda_i\}\omega_i$, $[\lambda]$ = int part, $0 \le \{\lambda\} = \lambda - [\lambda] < 1$. Consider the $m^n + 1$ pts $\varphi(\{t\gamma\}) \in \mathbb{R}^n$, $1 \le t \le m^n + 1$. $\varphi(\{t\gamma\}) \in [0,1]^n$ = "unit cube". Divide $[0,1]^n$ into m^n cubes of side $1/m$. Pigeonhole principle $\Rightarrow \exists\, t_1 \neq t_2$ s.t. $\varphi(\{t_1\gamma\}), \varphi(\{t_2\gamma\}) \in$ same subcube. Consider $t_1\gamma = [t_1\gamma] + \{t_1\gamma\}$, $t_2\gamma = [t_2\gamma] + \{t_2\gamma\}$. Their diff is $(t_1 - t_2)\gamma = ([t_1\gamma] - [t_2\gamma]) + (\{t_1\gamma\} - \{t_2\gamma\})$. Write $[t_1\gamma] - [t_2\gamma] = \omega \in \mathcal{O}$ & $\{t_1\gamma\} - \{t_2\gamma\} = \delta \in K$. Note $|\varphi(\delta)| \le 1/m$. Get $|N(\delta)| \le C \cdot |\varphi(\delta)|^n \le C(1/m)^n < 1$. Also $t := t_1 - t_2$ satisfies $1 \le t \le m^n \le M$. (if $t_1 > t_2$)

δ instead of γ $\to$

$\overset{n}{m+1}$

Th Let K be a # field. Then $Cl(K)$ is finite [$h_K := |Cl(K)|$ called class #]

Pf Let $\underline{a} \subset \mathcal{O}_K$ be any ideal & $0 \neq \beta \in \underline{a}$ s.t. $|N(\beta)|$ minimum. By L above $\forall \alpha \in \underline{a}$ $\exists\, t$, $1 \le t \le M$ s.t. $t\alpha = \omega\beta$ for some $\omega \in \mathcal{O}_K$. So $M!\,\underline{a} \subset \beta\mathcal{O}$ (M ind of $\underline{a}$) Set $\underline{b} := \beta^{-1} M!\,\underline{a} \underset{id}{\subset} \mathcal{O}$. $\Rightarrow M!\,\underline{a} = \beta\,\underline{b}$. Since $\beta \in \underline{a} \Rightarrow M!\,\beta \in \beta\,\underline{b} \Rightarrow$ $M! \in \underline{b} \Rightarrow \exists$ only fin many poss for $\underline{b}$ ($\mathfrak{p}^e | \underline{b} \Rightarrow \mathfrak{p}^e | (M!)\mathcal{O}$). Since $\underline{a} \equiv \underline{b}$ mod $P(\mathcal{O})$ done.

(24) Number fields II: units

(Def) Let K be a # field. Set $U_K := \mathcal{O}_K^* \{$= inv elts of $\mathcal{O}_K\}$. Clearly $\mathrm{Tors}(U_K) = \{$roots of 1 in $K\}$. (gr of elts of finord)

(Th) (Dirichlet) U_K is a f.g. group.

(β) Pf Let $\mathrm{Hom}(K, \bar{\mathbb{Q}}) = \mathrm{Hom}(K, \mathbb{C}) = \{\overset{id}{\tau_1}, \dots, \tau_n\} = \{\overset{id}{\sigma_1}, \dots, \sigma_s, \sigma_{s+1}, \overline{\sigma_{s+1}}, \dots, \sigma_{s+t}, \overline{\sigma_{s+t}}\}$ where $\sigma_i(K) \subset \mathbb{R}$ for $1 \le i \le s$ & s max with this prop. ($n = [K:\mathbb{Q}] = s + 2t$). Let $\psi: K \to V := \mathbb{R}^s \times \mathbb{C}^t = \mathbb{R}^n = \mathbb{R}^{s+2t}$, $\psi(\alpha) = (\sigma_1\alpha, \dots, \sigma_{s+t}\alpha)$ (This is quite diff from φ in (23))

$\mathcal{O}_K \subset K \xrightarrow{\psi} \mathbb{R}^s \times \mathbb{C}^t$

$\cup \quad \cup$

$D_K \subset K^\times \xrightarrow{\psi} (\mathbb{R}^\times)^s \times (\mathbb{C}^\times)^t \xrightarrow{\lambda} \mathbb{R}^{s+t}$, μ

(γ) Claim 1 $\psi(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ (cf ++)

[Indeed, Let $\alpha = \{\alpha_1, \dots, \alpha_n\}$ be $\mathbb{Z}$-basis of $\mathcal{O}_K$. By (24)(β) $\det(\tau_i \alpha_j)_{1\le i,j\le n} \neq 0$.

$\Rightarrow \tau_1\alpha, \dots, \tau_n\alpha \in \mathbb{C}^n$, $\mathbb{C}$-lin ind i.e. $\sigma_1\alpha, \dots, \sigma_s\alpha, \sigma_{s+1}\alpha, \bar\sigma_{s+1}\alpha, \dots, \sigma_{s+t}\alpha, \bar\sigma_{s+t}\alpha$ $\mathbb{C}$-lin ind $\Rightarrow$

$\Rightarrow \sigma_1\alpha, \dots, \sigma_s\alpha, \mathrm{Re}\,\sigma_{s+1}\alpha, \mathrm{Im}\,\sigma_{s+1}\alpha, \dots, \mathrm{Re}\,\sigma_{s+t}\alpha, \mathrm{Im}\,\sigma_{s+t}\alpha$ $\mathbb{C}$-ind by +++, so $\mathbb{R}$-ind]

Let $\lambda: (\mathbb{R}^*)^s \times (\mathbb{C}^*)^t \to \mathbb{R}^{s+t}$ be def by $\lambda(\beta) = (\log|\beta_1|, \dots, \log|\beta_s|, 2\log|\beta_{s+1}|, \dots, 2\log|\beta_{s+t}|)$ & $\mu: K^* \to \mathbb{R}^{s+t}$, $\mu(\alpha) = \lambda(\psi(\alpha))$. Group homo. Note $\lambda^{-1}(\text{compact}) = \text{compact}$.

$(U_K^\wedge)$

Claim 2 $U_K \cap \mathrm{Ker}\,\mu = \{$roots of 1 in $K^*\}$ $^\Delta$ [Indeed if $\mu(\alpha) = 0 \Rightarrow |\tau\alpha| = 1, \forall \tau$, $\Rightarrow |\tau\alpha^n| = 1$ $\forall n \Rightarrow$ all conj of α^n have modulus 1, $\forall n \Rightarrow$ modulus of coeff of $\mathrm{Irr}(\alpha^n, \mathbb{Q})$ are bounded (indep of n) $\Rightarrow$ these polyn are in fin. # so $\exists$ one of them, f, s.t. α^n root of f for ∞ many $n \Rightarrow \exists n \neq m$ s.t. $\alpha^n = \alpha^m \Rightarrow$ qed]

Claim 3 $\mu(U_K)$ is a lattice in $\mathbb{R}^{s+t}$ [Indeed enough to check $\mu(U_K)$ discrete. Let $B = B(0,R) \subset \mathbb{R}^{s+t}$ ball of radius R about 0. $\Rightarrow \lambda^{-1}(\mu(U_K) \cap B) \subset \underbrace{\lambda^{-1}(B)}_{\text{compact}} \Rightarrow$

$\Rightarrow \lambda^{-1}(\mu(U_K) \cap B)$ bounded $\Rightarrow \lambda^{-1}(\mu(U_K) \cap B) \cap \psi(\mathcal{O}_K)$ finite (bec. $\psi(\mathcal{O}_K)$ lattice by Claim 1). But clearly $\lambda^{-1}(\mu(U_K) \cap B) \cap \psi(\mathcal{O}_K) \to \mu(U_K) \cap B$ surj.

So $\mu(U_K) \cap B$ finite, qed]

Now Claims 2 & 3 close pf.

(x) (Remark) In proof, if $u \in U_K \Rightarrow Nu = \pm 1 \Rightarrow |Nu| = 1$. But (the Σ of coord of) $\mu(u)$ is $\log|\sigma_1 u| + \dots + \log|\sigma_s u| + 2\log|\sigma_{s+1} u| + \dots + 2\log|\sigma_{s+t} u| = \log|Nu| = 0$. So $\mu(U_K) \subset \{(\xi_1, \dots, \xi_{s+t}) \in \mathbb{R}^{s+t} \mid \xi_1 + \dots + \xi_{s+t} = 0\}$ so rank $\mu(U_K) \le s+t-1$, so rank $U_K \le s+t-1$. Actually Dirichlet proved "=".

Δ hence $\mathrm{Ker}\,\mu$ is finite because if $\zeta_m \in K^*$ prim m-th root of 1, by (16) ζ_m has degree $\phi(m)$ over $\mathbb{Q}$. So $\phi(m) \le [K:\mathbb{Q}]$. This implies m bounded [Ex: $\phi(p^a) = p^{a-1}(p-1)$]

+++ Use fact: if $w \in \mathbb{C}^n$ then $\mathbb{C}w + \mathbb{C}\bar{w} = \mathbb{C}\,\mathrm{Re}\,w + \mathbb{C}\,\mathrm{Im}\,w$.

++ A lattice in $\mathbb{R}^n$ is a subgr of form $\mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$ $(m \le n)$ with $v_1, \dots, v_m$ $\mathbb{R}$-lin ind [Ex: A subgr of $\mathbb{R}^n$ is discrete $\Leftrightarrow$ a lattice ("discrete" means in usual top)]

May ass sgr $\Gamma \subset \mathbb{R}^n$ spans $\mathbb{R}^n$

choose $v_1, \dots, v_n \in \Gamma$ $\mathbb{R}$-lin indep; may ass v_i stand. basis, $\Gamma' = \sum \mathbb{Z}v_i = \mathbb{Z}^n$

Then Γ/Γ' finite bec $\Gamma \cap [0,1]^n$ finite. So Γ is fin gen of rank n. So Γ free of rank n.

(25) Number fields II : discriminant

$\begin{array}{c} K \\ \cup \end{array}$

(Def) Let $L|K$ be fin sep ext of deg n & $\alpha_1,\dots,\alpha_n \in L$. Set $\Delta(\alpha_1,\dots,\alpha_n) = \det(\mathrm{Tr}_{L|K}(\alpha_i\alpha_j))$. By (17) $\Delta \neq 0 \iff \alpha_1,\dots,\alpha_n$ basis

(α) (Prop) Ass $\alpha_1,\dots,\alpha_n$ & $\beta_1,\dots,\beta_n$ 2 basis & $\alpha_i = \sum \gamma_{ij}\beta_j$, $\gamma_{ij}\in K \Rightarrow \Delta(\alpha_1,\dots,\alpha_n) = (\det \gamma_{ij})^2 \Delta(\beta_1,\dots)$

Pf $\alpha_i\alpha_k = \sum_j \sum_\ell \gamma_{ij}\gamma_{k\ell}\beta_j\beta_\ell \Rightarrow \mathrm{Tr}(\alpha_i\alpha_k) = \sum_j\sum_\ell \gamma_{ij}\gamma_{k\ell}\mathrm{Tr}(\beta_j\beta_\ell)$. If $A = (\mathrm{Tr}(\alpha_i\alpha_j))$, $B = (\mathrm{Tr}(\beta_i\beta_j))$, $C = (\gamma_{ij}) \Rightarrow A = CB{}^tC \Rightarrow \det A = (\det C)^2 \det B$ qed//

(β) (Prop) If $\alpha_1,\dots,\alpha_n$ basis of $L|K$ & $\mathrm{Hom}_K(L,\bar K) = \{\sigma_1,\dots,\sigma_n\} \Rightarrow \Delta(\alpha_1,\dots,\alpha_n) = (\det(\sigma_i\alpha_j))^2$

Pf $\mathrm{Tr}(\alpha_i\alpha_j) = \sigma_1\alpha_i\sigma_1\alpha_j + \dots + \sigma_n\alpha_i\sigma_n\alpha_j$. Set $A = (\mathrm{Tr}(\alpha_i\alpha_j))$, $B = (\sigma_i\alpha_j)$. Then $A = {}^tBB \Rightarrow$ qed

(γ) (Prop) Ass $L = K(\beta)$ & $f = \mathrm{Irr}(f,K)$. Then $\Delta(1,\beta,\beta^2,\dots,\beta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L|K}(f'(\beta))$

Pf $\Delta(1,\beta,\dots,\beta^{n-1}) \underset{(\beta)}{=} (\det(\sigma_i\beta^j))^2 \underset{\text{Vandermonde}}{=} \left(\prod_{i<j}(\sigma_j\beta - \sigma_i\beta)\right)^2 = \prod_{i\neq j}(\sigma_j\beta - \sigma_i\beta)(-1)^{\frac{n(n-1)}{2}}$.

On other hand $f(x) = \prod_i (x - \sigma_i\beta)$ so $f'(x) = \sum (x-\sigma_1\beta)\cdots\widehat{(x-\sigma_i\beta)}\cdots(x-\sigma_n\beta)$. So $f'(\sigma_i\beta) = \prod_{i\neq j}(\sigma_i\beta - \sigma_j\beta)$ so $N(f'(\beta)) = \prod_i \sigma_i f'(\beta) = \prod_i f'(\sigma_i\beta) = \prod_{i\neq j}(\sigma_i\beta - \sigma_j\beta) \Rightarrow$ qed

(Def) Let K be a # field & $\underline{a} \subset \mathcal{O}_K$ ideal ($\Rightarrow \underline{a}$ free ab gr of rk $n = [K:\mathbb{Q}]$, bec it is so for $\underline{a} = A$ & $\forall$ id $\supset$ princ id ~~by Chin rem th~~). Let $\alpha_1,\dots,\alpha_n$ be a $\mathbb{Z}$basis of $\underline{a}$ & set $\Delta(\underline{a}) = \Delta(\alpha_1,\dots,\alpha_n)$; by (α) it doesn't depend on choice of α's. Call $\delta_K := \Delta(\mathcal{O}_K)$ the discrim of K. ($\delta_K \in \mathbb{Z}$ by (β))

(Prop) Let K be a # field, with discrim $\delta_K \in \mathbb{Z}$. Let p be a prime in $\mathbb{Q}$. $p \nmid \delta_K$ iff p does not ramify in K. In partic $\exists$ only fin many primes of $\mathbb{Q}$ that ramify.

Pf Ass p ramifies in $K \Rightarrow p\mathcal{O}_K = \mathfrak{P}^2\mathfrak{a}$ for ideals $\mathfrak{P}, \mathfrak{a} \subset \mathcal{O} = \mathcal{O}_K$, $\mathfrak{P}$ prime. $\exists\, \alpha \in \mathfrak{P}\mathfrak{a}$, $\alpha \notin p\mathcal{O} = \mathfrak{P}^2\mathfrak{a}$. Claim $\forall \beta \in \mathcal{O}$ have $p \mid \mathrm{Tr}(\alpha\beta)$ [Indeed suff to check $p \mid (\mathrm{Tr}(\alpha\beta))^p$. But $(\mathrm{Tr}(\alpha\beta))^p \equiv \mathrm{Tr}(\alpha^p\beta^p) \equiv 0 \mod (p\mathcal{O})$, because $\alpha^2 \in \mathfrak{P}^2\mathfrak{a}^2 \subset p\mathcal{O}$]

$p \mid \binom{p}{i}$

Since $\alpha \notin p\mathcal{O}$, its image $\bar\alpha \in \mathcal{O}/p\mathcal{O}$ is $\neq 0$. Complete it to an $\mathbb{F}_p$-basis $\bar\alpha_1 = \bar\alpha, \bar\alpha_2,\dots,\bar\alpha_n$ of $\mathcal{O}/p\mathcal{O}$, where $\alpha_i \in \mathcal{O}$. Let $\beta_1,\dots,\beta_n$ be a $\mathbb{Z}$basis of $\mathcal{O}$ & write $\alpha_i = \sum \gamma_{ij}\beta_j$. Get

$p \mid \Delta(\alpha_1,\dots,\alpha_n) \underset{(\alpha)}{=} (\det \gamma_{ij})^2 \Delta(\beta_1,\dots,\beta_n) \Rightarrow p \mid \Delta(\beta_1,\dots,\beta_n) = \delta_K$ qed//

bec $p \mid \mathrm{Tr}(\alpha_1\alpha_j)$; not div by p because (γ_{ij}) invert

Converse won't be proved

(δ) (Th) (Minkowski) 1) If $n = [K:\mathbb{Q}]$ & $d = |\delta_K|$ then $\exists\, 0 \neq \alpha \in \mathcal{O}_K$ s.t. $|N\alpha| \leq \frac{n!}{n^n}\left[\frac{4}{\pi}\right]^t d^{1/2}$ and t is as in (24)(β)

2) If $K \neq \mathbb{Q} \Rightarrow \exists$ primes of $\mathbb{Q}$ that ramify (hence $\delta_K \neq \pm 1$)

3) There $\exists$ only fin many K's with given value of δ_K

4) The quotient $[K:\mathbb{Q}]/\log|\delta_K|$ is bounded for all $K \neq \mathbb{Q}$.

Pf Note 1) ⟹ $d > 1$ (because $|N\alpha| \geq 1$) ⟹ 2). Also easy to see 1) ⟹ 4). So need to prove 1) & 3). Need:

(ε) (L) (Minkowski's lemma) Let $L \subset \mathbb{R}^n$ be a lattice of rank n & let F be a fundam. domain for L (cf. (+)). Let $C \subset \mathbb{R}^n$ be a closed convex(++) symmetric(+++) Lebesgue meas set(++++). If $\mathcal{V}(C) \geq 2^n \mathcal{V}(F)$ then $C \cap L \neq \{0\}$.

Pf. May ass $\mathcal{V}(C) > 2^n \mathcal{V}(F)$. Have $\frac{1}{2}C = \bigcup_{x \in L} (\frac{1}{2}C \cap (F+x))$ (disjoint) so $\mathcal{V}(\frac{1}{2}C) = \sum_{x\in L} \mathcal{V}(\frac{1}{2}C \cap (F+x)) = \sum_{x \in L} \mathcal{V}((\frac{1}{2}C - x) \cap F)$. Can't have all $\frac{1}{2}C - x$; $x \in L$ disjoint (would get last sum $\leq \mathcal{V}(F)$; but $\mathcal{V}(\frac{1}{2}C) = \frac{1}{2^n}\mathcal{V}(C)$ ⨳). So $\exists\, c_1, c_2 \in C$ & $x_1 \neq x_2 \in L$ s.t. $\frac{1}{2}c_1 - x_1 = \frac{1}{2}c_2 - x_2$, ⟹ $\underbrace{\frac{1}{2}(c_1 - c_2)}_{\cap\, C} = x_1 - x_2 \in L$ qed//

← because $-c_2 \in C$ by symm so $\frac{1}{2}c_1 + \frac{1}{2}(-c_2) \in C$ by conv.

Back to pf of (δ). 1) Use embedding $\psi: K \to \mathbb{R}^s \times \mathbb{C}^t = \mathbb{R}^n$ from (24)(β) & consider lattice $L = \psi(\mathcal{O}_K)$ (cf. (24)(γ)) & convex symm domain $C_a \subset \mathbb{R}^n$ def by

$$C_a = \{(\xi_1, \dots, \xi_s, z_1, \dots, z_t) \in \mathbb{R}^s \times \mathbb{C}^t \mid |\xi_1| + \dots + |\xi_s| + 2|z_1| + \dots + 2|z_t| \leq a\}, \ a > 0$$

(φ) Claim 1 $\mathcal{V}(C_a) = 2^s 4^{-t} (2\pi)^t \frac{1}{n!} a^n$ [exerc. in real analysis]

(ψ) Claim 2 If F fund dom for L ⟹ $\mathcal{V}(F) = 2^{-t} d^{1/2}$

[Indeed by (25), (β) d is the modulus of the square of

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

$$\begin{vmatrix} \sigma_1\alpha_1 & \cdots & \sigma_1\alpha_n \\ \vdots & & \\ \sigma_s\alpha_1 & \cdots & \sigma_s\alpha_n \\ \sigma_{s+1}\alpha_1 & \cdots & \sigma_{s+1}\alpha_n \\ \bar\sigma_{s+1}\alpha_1 & \cdots & \bar\sigma_{s+1}\alpha_n \\ \vdots & & \\ \sigma_{s+t}\alpha_1 & \cdots & \sigma_{s+t}\alpha_n \\ \bar\sigma_{s+t}\alpha_1 & \cdots & \bar\sigma_{s+t}\alpha_n \end{vmatrix} \overset{?}{=} i2^t \begin{vmatrix} \sigma_1\alpha_1 & \cdots & \sigma_1\alpha_n \\ \sigma_s\alpha_1 & \cdots & \sigma_s\alpha_n \\ \mathrm{Re}\,\sigma_{s+1}\alpha_1 & \cdots & \mathrm{Re}\,\sigma_{s+1}\alpha_n \\ \mathrm{Im}\,\sigma_{s+1}\alpha_1 & \cdots & \mathrm{Im}\,\sigma_{s+1}\alpha_n \\ \vdots & & \\ \mathrm{Re}\,\sigma_{s+t}\alpha_1 & \cdots & \mathrm{Re}\,\sigma_{s+t}\alpha_n \\ \mathrm{Im}\,\sigma_{s+t}\alpha_1 & \cdots & \mathrm{Im}\,\sigma_{s+t}\alpha_n \end{vmatrix} = 2^t \mathcal{V}(F) \cdot i^{?}$$

& done]

Now from (ε), (φ), (ψ) applied to $C = C_a$, $a^n = 4^t n!\, \pi^{-t} d^{1/2}$ ⟹ $\exists\, 0 \neq \psi(\alpha) \in C_a \cap L$. So $|\sigma_1\alpha| + \dots + |\sigma_s\alpha| + 2|\sigma_{s+1}\alpha| + \dots + 2|\sigma_{s+t}\alpha| \leq a$. But $|N\alpha|^{1/n} \underset{\uparrow}{\leq} \frac{1}{n}(|\sigma_1\alpha| + \dots + 2|\sigma_{s+t}\alpha|) \leq \frac{a}{n}$ ⟹ $|N\alpha| \leq \frac{a^n}{n^n}$ ⟹ qed//

geo mean ≤ arith mean

(++++) denote by $\mathcal{V}$ Lebesgue measure.

(+++) i.e. $x \in C \Rightarrow -x \in C$

(++) convex means $x, y \in C$, $0 \leq t \leq 1$ ⟹ $tx + (1-t)y \in C$

(+) $F = \{\sum \lambda_i w_i \mid 0 \leq \lambda_i \leq 1\}$ where $L = \sum \mathbb{Z} w_i$, $w_1, \dots, w_n$ $\mathbb{R}$lin ind.

Assume $K/\mathbb{Q}$ Galois to simplify

Pf of (δ 3). By 1) enough to prove $\exists$ only fin many K's with given degree n & discr δ. 2 cases $t \neq 0$ & $t = 0$. Analyse (say) $t=0$ so $n = s$.

Consider $D_a = \{(\xi_1, \dots, \xi_n) \in \mathbb{R}^n \mid |\xi_1| \le a \cdot d^{1/2}, |\xi_2| \le \frac{1}{2}, \dots, |\xi_n| \le \frac{1}{2}\}$

Condition $\underset{\substack{\| \text{obvious} \\ 2a \cdot d^{1/2}}}{V(D_a)} \ge 2^n V(F) \left(\overset{(4)}{=} 2^n d^{1/2}\right)$ is realized for, say, $a = 2^{n-1}$

So for $a = 2^{n-1}$ get by Mink's Lemma (ε) $\exists\ 0 \neq \phi(\alpha) \in D_a \cap L$ ($\alpha \in \mathcal{O}_K$) so $|\sigma_1 \alpha| \le a \cdot d^{1/2}$, $|\sigma_2 \alpha| \le \frac{1}{2}, \dots, |\sigma_n \alpha| \le \frac{1}{2}$. Since $1 \le |N\alpha| = |\sigma_1\alpha||\sigma_2\alpha|\cdots|\sigma_n\alpha|$ $\Rightarrow |\sigma_1 \alpha| \ge 2^{n-1}$. So $\alpha = \sigma_1 \alpha \neq \sigma_i \alpha$ for $i \neq 1$. So $K = \mathbb{Q}(\alpha)$. Now coeff of $f = \mathrm{Irr}(\alpha, \mathbb{Q})$ are $\in \mathbb{Z}$ & are symm fcns in $\sigma_1\alpha, \dots, \sigma_n\alpha$ so have abs value $\le$ const dep only on n & d $\Rightarrow \exists$ only fin many choices for f hence for K.

Remarks

1) Similar proof $\Rightarrow \forall$ ideal $\mathfrak{a} \subset \mathcal{O}_K$ contains $\alpha \in \mathfrak{a}$ s.t. $|N\alpha| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t d^{1/2}\, N\mathfrak{a}$.

2) Writing $\mathfrak{a} = (\alpha)\mathfrak{b}$ get $N\mathfrak{a} = (N\alpha)(N\mathfrak{b})$ so $N\mathfrak{b} \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t d^{1/2}$. So any class in $Cl(\mathcal{O}_K)$ contains an ideal of norm $\le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t d^{1/2}$.

3) Discr compat with localis & completion. Since $\mathbb{Q}_p$ has only fin many ext K_p of fixed degree up to iso (p. 56) $\Rightarrow$ there are only fin many discriminants $\delta_{K_p} = \Delta(\mathcal{O}_{K_p})$ for such ext's so only fin many powers of p dividing such ext's. So if consider ext's K of $\mathbb{Q}$ of fixed degree n then $\forall p$ the exponent of p in δ_K is bounded by a const $C(n,p)$. So if you fix n & the primes dividing δ_K then you bound δ_K hence you find only fin many K's.

Hence:

Th (Hermite) $\exists$ only fin many # fields of fixed degree, unramif outside fin set of primes of $\mathbb{Q}$

(26) Quadratic fields again

(Def) "Quadratic field" means K s.t. $[K:\mathbb{Q}]=2$. Note K quadr $\Rightarrow \exists!\, d \in \mathbb{Z}$, sq free, s.t. $K = \mathbb{Q}(\sqrt{d})$. $K/\mathbb{Q}$ Galois, $G(K/\mathbb{Q}) = \{1, \sigma\}$, $\sigma\sqrt{d} = -\sqrt{d}$. Note $N: K \to \mathbb{Q}$, $N(a+b\sqrt{d}) = a^2 - db^2$, $Tr(a+b\sqrt{d}) = 2a$.

(α) (Prop) If $d \equiv 2,3\,(4) \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. If $d \equiv 1\,(4) \Rightarrow \mathcal{O}_K = \mathbb{Z}\left[-\frac{1}{2} + \frac{\sqrt{d}}{2}\right]$

Pf. Prove 1st that $\alpha \in \mathcal{O}_K \Leftrightarrow Tr\,\alpha,\ N\alpha \in \mathbb{Z}$ ["$\Rightarrow$" by (22); "$\Leftarrow$" $\alpha^2 - \underbrace{(\alpha+\sigma\alpha)}_{Tr\,\alpha}\alpha + \underbrace{\alpha\sigma\alpha}_{N\alpha} = 0$]

So $x + y\sqrt{d} \in \mathcal{O}_K$ $(x,y \in \mathbb{Q}) \Leftrightarrow 2x \in \mathbb{Z}$ & $x^2 - dy^2 \in \mathbb{Z} \Rightarrow 4dy^2 \in \mathbb{Z}$. Write $2y = m/n$ $_{(m,n)=1}$ $\Rightarrow d m^2 = z n^2 \Rightarrow (\forall$ prime $p \mid n \Rightarrow_{(m,n)=1} p^2 \mid d$ ✗ $) \Rightarrow 2y \in \mathbb{Z}$.

Write $2x = a$, $2y = b$, $a,b \in \mathbb{Z}$; $\Rightarrow a^2 - db^2 = 4(x^2 - dy^2) \equiv 0\,(4)$.

If $d \equiv 3\,(4) \Rightarrow a^2 - db^2 \equiv a^2 + b^2\,(4) \Rightarrow$ both a, b even $\Rightarrow$ done. Similar for $d \equiv 2\,(4)$.

If $d \equiv 1\,(4) \Rightarrow a^2 - db^2 \equiv a^2 - b^2\,(4) \Rightarrow a$ & b same parity $\Rightarrow \frac{a+b\sqrt{d}}{2} = \underbrace{\frac{a+b}{2}}_{\in \mathbb{Z}} + \underbrace{b}_{\in \mathbb{Z}}\left(-\frac{1}{2} + \frac{\sqrt{d}}{2}\right)$ qed

(β) (Prop) if $K = \mathbb{Q}(\sqrt{d})$ & δ_K = discrim $\Rightarrow$ $\delta_K = 4d$ if $d \equiv 2,3\,(4)$; $\delta_K = d$ if $d \equiv 1\,(4)$

Pf Just compute $\det(Tr(\alpha_i\alpha_j))$ where $\alpha_1 = 1, \alpha_2 = \sqrt{d}$ in 1st case & $\alpha_1 = 1$, $\alpha_2 = -\frac{1}{2} + \frac{\sqrt{d}}{2}$

(γ) (Prop) Let p be a prime $\in \mathbb{Z}$, odd, $K = \mathbb{Q}(\sqrt{d})$. p ramifies $\Leftrightarrow p \mid \delta_K$.
If $p \nmid \delta_K$ then p splits (completely) in $K \Leftrightarrow \left(\frac{d}{p}\right) = 1$

Pf Ass $d \equiv 2,3\,(4)$. Then $\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}] = \mathbb{F}_p[x]/(x^2 - \bar{d})$ as in (13),(α). As there if $\left(\frac{d}{p}\right) = -1 \Rightarrow x^2 - \bar{d}$ irr $\Rightarrow p\mathcal{O}_K$ prime. If $\left(\frac{d}{p}\right) = 1 \Rightarrow x^2 - \bar{d} = (x-\lambda)(x+\lambda)$, $\lambda \in \mathbb{F}_p$, $\lambda^2 = \bar{d}$ & the 2 factors are not assoc [bec $\lambda \neq -\lambda$, bec $\bar{2}\lambda \neq 0$ bec $\bar{2} \neq 0$ & $\bar{d} \neq 0$]. So $\mathbb{F}_p[x]/(x^2 - \bar{d})$ has 2 prime ideals $\Rightarrow \exists$ 2 prime id in $\mathbb{Z}[\sqrt{d}]$ containing p. $\Rightarrow$ OK

Ass $d \equiv 1(4)$. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$, $\alpha = -\frac{1}{2} + \frac{\sqrt{d}}{2}$. Since $Tr\,\alpha = -1$, $N\alpha = \frac{1-d}{4}$ so α sat $x^2 + x + \frac{1-d}{4} = 0$ & clearly this is $Irr(\alpha, \mathbb{Q})$ so if $d = 4k+1$ get $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(x^2+x-k)$ so $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[x]/(x^2+x-\bar{k})$; $x^2+x-\bar{k}$ irr $\Leftrightarrow 4x^2+4x-4\bar{k}$ irr $\Leftrightarrow (2x+1)^2 - \bar{d}$ irr $\Leftrightarrow y^2 - \bar{d}$ irr & do as above.

(δ) (Cor) Let $d \in \mathbb{Z}$, $K = \mathbb{Q}(\sqrt{d})$. Then $\{p \in \mathbb{Z} \mid p$ prime, p splits compl in $K\}$ (the set of primes lying in) is a finite union of arithmetic progressions.

Pf Cf (γ) + multiplic of $\left(\frac{?}{p}\right)$ & quadr reciprocity

Rem: this is the kind of stat generalized through "class field th".

(ε) (Prop) Let $K = \mathbb{Q}(\sqrt{d})$, $d < 0$. Then $U_K = \begin{cases} \{\pm 1, \pm i\} & \text{if } d = -1 \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } d = -3 \\ \{\pm 1\} & \text{otherwise} \end{cases}$ [Pf $z \in U_K \Leftrightarrow Nz = 1$ ($= a^2 - db^2$) aso]

(†) equiv, p is a norm $N\beta$, cf (22)(4)

Prop Let $K=\mathbb{Q}(\sqrt{d}), d>0$. Then $\mathcal{O}_K^* = \{\pm u^m \mid m\in\mathbb{Z}\}$ for some $u\in\mathcal{O}_K$, u not a root of 1.

Pf If r,s are as in (25) $r=2, s=0$ so rank $U_K \le 1$ cf (25)(α). Let's prove rank $=1$.
$u\in U_K \Leftrightarrow Nu=\pm 1$. So enough to find ∞ sol to "Pell's eqn":

(ε) **L** (Lagrange) $x^2-dy^2=1$ $(d>0)$ has ∞ many integral sol's.

Need:

(θ) **L** (Dirichlet) If $\xi\in\mathbb{C}\setminus\mathbb{Q} \Rightarrow \exists\,\infty$ many $\frac{x}{y}\in\mathbb{Q}$, $x,y\in\mathbb{Z}$, $(x,y)=1$ s.t. $\left|\frac{x}{y}-\xi\right|<\frac{1}{y^2}$.

Pf Enough to prove $(*)$ $\forall m\in\mathbb{N}\ \exists\, x_m, y_m\in\mathbb{Z}, (x_m,y_m)=1$ s.t. $\left|\frac{x_m}{y_m}-\xi\right|<\frac{1}{y_m m}$ $\underbrace{}_{1\le y_m\le m}$ [Indeed $\frac{1}{y_m m}\le\frac{1}{y_m^2}$ & $\left|\frac{x_m}{y_m}-\xi\right|\to 0$ as $m\to\infty$ so (x_m,y_m) must form an ∞ set]

To check $(*)$ divide $[0,1]$ into m equal segments & consider the $m+1$ #'s $0,\{\xi\},\{2\xi\},\dots,\{m\xi\}$ where $\{x\}=x-[x]$. By pigeon hole princ $\exists\ 0\le \ell<k\le m$ s.t. $|\{k\xi\}-\{\ell\xi\}|<\frac{1}{m}$. Get $|k\xi-[k\xi]-\ell\xi+[\ell\xi]|<\frac{1}{m}$. Get $\left[\left|\frac{[k\xi]-[\ell\xi]}{k-\ell}-\xi\right|\le\frac{1}{(k-\ell)m}\right]$ done, after making fr irr, which improves ineq.

(η) *Pf* of (ε) **Claim** $\exists\, M\in\mathbb{R}$ s.t. eqn $|x^2-dy^2|<M$ has ∞ sol in $\mathbb{Z}^2$.
[Indeed By (θ) have ∞ pairs $(x_m,y_m)=1$ s.t. $\left|\frac{x_m}{y_m}-\sqrt{d}\right|\underset{\Delta}{<}\frac{1}{y_m^2}$. Multiply by $\left|\frac{x_m}{y_m}+\sqrt{d}\right|$
Get $\left|\frac{x_m^2}{y_m^2}-d\right|\le\frac{1}{y_m^2}\left|\frac{x_m}{y_m}+\sqrt{d}\right|\underset{m\gg 0}{\le}\frac{1}{y_m^2}(2\cdot\sqrt{d}+1)$ because $\frac{x_m}{y_m}\to\sqrt{d}$ because Δ]

By Claim $\exists\, k, -M\le k\le M$ & $\exists\,\infty$ many pairs (x_m,y_m) s.t. $x_m^2-dy_m^2=k$. So $\exists\, m,n$ s.t. $x_m^2-dy_m^2=k=x_n^2-dy_n^2$ & $x_m\equiv x_n$ & $y_m\equiv y_n \mod (k)$ &

$\alpha\beta^\sigma\ne\pm k$ $\left(\frac{x_n}{y_n}\ne\frac{x_m}{y_m}\right)$ Set $\alpha=x_m-y_m\sqrt{d}$, $\beta=x_n-y_n\sqrt{d}$. Then $\alpha\beta^\sigma=(x_m-y_m\sqrt{d})(x_n+y_n\sqrt{d})=x_nx_m-y_ny_md+(x_ny_m-x_my_n)\sqrt{d}\equiv 0 \mod (k)$. So $\alpha\beta^\sigma=k(a+b\sqrt{d})$, $a,b\in\mathbb{Z}$. Taking $N:\mathbb{Q}(\sqrt{d})\to\mathbb{Q}$ get $k^2=N(\alpha)N(\beta^\sigma)=k^2N(a+b\sqrt{d})\Rightarrow N(a+b\sqrt{d})=1\Rightarrow a^2-b^2d=1$
Have $b\ne 0$ by) so $a+b\sqrt{d}$ is not a root of 1 $\Rightarrow$ done.
(the only real roots of 1 are ±1)

Prop p odd prime, $d\in\mathbb{Z}$, $K=\mathbb{Q}(\sqrt{d})$, $\sigma_q:=(q,\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ Artin symbol. Then $\sigma_q(\sqrt{d})=\left(\frac{d}{q}\right)\sqrt{q}$. Indeed $\sigma_q=id \underset{(22)\psi}{\Leftrightarrow} q$ splits completely $\underset{(\delta)}{\Leftrightarrow}\left(\frac{d}{q}\right)=1$. (This justifies calling the Artin symbol "the recipr. map"

[E.g. if Say $p,q\equiv 3(4)$ & $\left(\frac{p}{q}\right)=-1$. Have

$$\begin{array}{ccccc}
\sqrt{p}=\bar{x}\in\mathcal{O}_K=\mathbb{Z}[\sqrt{p}]=\mathbb{Z}[x]/(x^2-p) & \rightsquigarrow & \mathcal{O}_K/q\mathcal{O}_K=\mathbb{F}_q[x]/(x^2-\bar{p})\cong\mathbb{F}_{q^2}\ni\bar{x} \\
\downarrow \sigma_q & & \downarrow \ \sigma_q \bmod q=\mathrm{Frob}_q \\
-\sqrt{p}=-\bar{x}\in\mathbb{Z}[x]/(x^2-p) & & \mathbb{F}_q[x]/(x^2-\bar{p})\ni -\bar{x}=\bar{x}^q
\end{array}$$

Remark (η) may be proved "directly" using Minkowski's Lemma (25)(ε) applied to $L\Psi(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})\subset\mathbb{R}^2$ & $C_\varepsilon:=\{(\xi_1,\xi_2)\in\mathbb{R}^2 \mid |\xi_1|\le\varepsilon, |\xi_2|\le a/\varepsilon\}$
$\varepsilon\to 0$. $\left(V(C_\varepsilon)=a\ge 2^2 d^{1/2}\ge 4\sqrt{d} \Rightarrow \exists\,\alpha_\varepsilon\in\mathcal{O}\cap C_\varepsilon \Rightarrow |N\alpha_\varepsilon|\le\varepsilon\cdot\frac{a}{\varepsilon}=a\right)$

27 Cyclotomic fields again

Set as usual $\zeta_m = e^{2\pi i/m}$. Recall from 16 proof of β that $\Phi_m := \mathrm{Irr}(\zeta_m, \mathbb{Q}) \in \mathbb{Z}[x]$ & has degree $\varphi(m)$. Also $G(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$, $\sigma \mapsto j$, $\sigma\zeta_m = \zeta_m^j$.
(Note $\Phi_m \in \mathbb{Z}[x]$ also foll from gen theory in 22 : $\mathrm{Irr}(\text{integer}, \mathbb{Q}) \in \mathbb{Z}[x]$.

α Prop If $K = \mathbb{Q}(\zeta_m)$ then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$.

Pf (only case $m = p$ prime). In this case $f = \mathrm{Irr}(\zeta_p, \mathbb{Q}) = x^{p-1} + \dots + x + 1$. Set $\zeta = \zeta_p$.
Take $\alpha = a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2} \in \mathcal{O}_K$. Note $\mathrm{Tr}\,\zeta^j = -1$ if $j = 1, \dots, p-1$ (because ζ^j also prim root of 1 so has irr polyn f). Get $\mathrm{Tr}(\alpha\zeta^{-s}) =$
$= -a_0 - a_1 - \dots + (p-1)a_s - \dots - a_{p-2}$. So $\mathbb{Z} \ni \mathrm{Tr}(\alpha\zeta^{-s} - \alpha\zeta) = p a_s$ for $0 \le s \le p-2$.

Need:

β (L) If $\lambda = 1 - \zeta$ then $\underbrace{(\lambda)^{p-1}}_{N\lambda = p} = (p)$. [Indeed $x^{p-1} + \dots + 1 = \prod_{j=1}^{p-1}(x - \zeta^j)$. Setting $x = 1$ get $p = \prod_{j=1}^{p-1}(1 - \zeta^j)$. Enough to check $1 - \zeta \sim 1 - \zeta^j$. Clearly $1 - \zeta \mid 1 - \zeta^j$. But now we may interchange roles of ζ & ζ^j, bec ζ^j is also prim. So $1 - \zeta^j \mid 1 - \zeta$]

Pf of α continued. By above $p\alpha \in \mathbb{Z}[\zeta] = \mathbb{Z}[\lambda]$ so $p\alpha = b_0 + b_1\lambda + \dots + b_{p-2}\lambda^{p-2}$, $b_i \in \mathbb{Z}$.
Claim: $p \mid b_i$ for all i (this will close pf.) Ass not so ass $p \mid b_0, \dots, b_s$, $p \nmid b_{s+1}$ for some $\underset{s+1 \le p-2}{s \ge -1}$. Then dividing by λ^{s+1} get $\lambda \mid b_{s+1}$. Taking norms $\Rightarrow p \mid b_{s+1}$ ~~&~~. (+)

Prop If $K = \mathbb{Q}(\zeta_p)$, p prime $\Rightarrow |\delta_K| = p^{p-2}$ [By 25 γ, $|\delta_K| = |N(f'(\zeta))|$
$= |N((\zeta - \zeta^2)(\zeta - \zeta^3)\cdots(\zeta - \zeta^{p-1}))| \underset{L}{=} (N\lambda)^{p-2} \underset{L}{=} p^{p-2}$] So all primes $q \ne p$ are unr while by β p is ramif (totally) in K.

γ Prop if $K = \mathbb{Q}(\zeta_p)$ & $q \in \mathbb{Z}$ prime $\ne p$ then q splits completely in K $\Leftrightarrow q \equiv 1\ (p)$.

Pf. q splits compl in $K \overset{def}{\Leftrightarrow} \mathcal{O}_K/q\mathcal{O}_K$ has $p-1$ prime ideals $\Leftrightarrow$ (Because $\mathcal{O}_K/q\mathcal{O}_K =$
$\underset{α}{=} \mathbb{Z}[\zeta_p]/q\mathbb{Z}[\zeta_p] = \dfrac{\mathbb{Z}[x]/(x^{p-1} + \dots + 1)}{(q, x^{p-1} + \dots + 1)/(x^{p-1} + \dots + 1)} \simeq \mathbb{F}_q[x]/(x^{p-1} + \dots + \bar{1})$) $x^{p-1} + \dots + \bar{1} \in \mathbb{F}_q[x]$
splits into linear factors in $\mathbb{F}_q[x] \Leftrightarrow$ all roots of $x^p - \bar{1} \in \mathbb{F}_q[x]$ lie in $\mathbb{F}_q$.
If last happens, since {roots of $x^p - \bar{1}$} is a subgr of ord p of $\mathbb{F}_q^*$ which has ord $q - 1 \Rightarrow p \mid q-1 \Leftrightarrow p \equiv 1\,(q)$. Conversely, if $p \equiv 1\,(q)$, let $q - 1 = pm$ & let $\mathbb{F}_q^* = \langle\omega\rangle$. Then $1, \omega^m, \omega^{2m}, \dots, \omega^{(p-1)m}$ are distinct roots of $x^p - \bar{1} \in \mathbb{F}_q[x]$.

Prop If $K = \mathbb{Q}(\zeta_p) \Rightarrow (U_K)_{tors} = \{1, \zeta_p, \dots, \zeta_p^{p-1}\}$ [Indeed if $u \in U_K \Rightarrow u = \zeta_m^i$ for some $\underset{(i,m)=1}{m}$ so $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_p)$. One concludes by 16 β & its cor that $m = p$]

(+) Note that (λ) prime in $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ because if not then one contradicts $\underset{p-1}{[\mathbb{Q}(\zeta_p):\mathbb{Q}]} = \sum e_i f_i$

(δ) (Prop) Let $K=\mathbb{Q}(\zeta_p)$ & $n\in\mathbb{Z}$, $p\nmid n$ & $\sigma_n=(n\mathbb{Z}, K/\mathbb{Q})\in G(K/\mathbb{Q})$ the Artin symbol

Then $\sigma_n\zeta_p=\zeta_p^n$ [This is stronger than (γ) because we get $\sigma_q=id \Leftrightarrow q\equiv 1\ (p)$ But (γ) was proved "directly".]

Pf Enough to check for $n=q$ prime. Let $\tau_q\in G(K/\mathbb{Q})$, $\tau_q\zeta_p=\zeta_p^q$.

Enough to check $\tau_q w\equiv w^q\ (q)$ for all $w\in\mathbb{Z}[\zeta_p]$ (bec it then holds mod any $\mathfrak{P}\mid q$, $\mathfrak{P}\subset\mathcal{O}_K$)

Let $w=a_0+a_1\zeta_p+\dots+a_{p-2}\zeta_p^{p-2}$. Get $\tau_q w=a_0+a_1\zeta_p^q+\dots+a_{p-2}\zeta_p^{q(p-2)}\equiv$

$\equiv (a_0+a_1\zeta_p+\dots+a_{p-2}\zeta_p^{p-2})^q=w^q$ qed.

bec $a_i^q\equiv a_i\ (q)$
& $q\mid\binom{q}{j}$, $j\neq 0,q$

<u>Another pf. of quadratic reciprocity (without Gauss sums)</u>

Let p,q be odd primes, $p\neq q$. Set $K=\mathbb{Q}(\zeta_p)$. By pf of (β) have $p=(1-\zeta_p)\cdots(1-\zeta_p^{p-1})$. But $(1-\zeta_p^i)(1-\zeta_p^{p-i})=(1-\zeta_p^i)(1-\zeta_p^{-i})=-\zeta_p^{-i}(1-\zeta_p^i)^2 \Rightarrow$ $p=(-1)^{\frac{p-1}{2}}\zeta_p^b\prod_{i=1}^{(p-1)/2}(1-\zeta_p^i)^2$, $b\in\mathbb{Z}$. Since $(2,p)=1$, $\zeta_p^b=\zeta_p^{2c}$, $c\in\mathbb{Z}$ so $p^*:=(-1)^{\frac{p-1}{2}}p=\tau^2$, $\tau\in\mathbb{Z}[\zeta_p]$.[+] With notations of (δ)

$$\sigma_q\tau=\tau \Leftrightarrow \sigma_q\in G(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\tau)) \Leftrightarrow \sigma_q \text{ is a square in } G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \Leftrightarrow q \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^* \Leftrightarrow \left(\tfrac{q}{p}\right)=1$$

bec $G(\mathbb{Q}(\zeta_p)/\mathbb{Q})\simeq(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic so $G(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\tau))$ is the unique gr of index 2.

So $\sigma_q\tau=\left(\frac{q}{p}\right)\tau$.

Now $\sigma_q|_{\mathbb{Q}(\tau)}\in G(\mathbb{Q}(\tau)/\mathbb{Q})$ coincides with the Artin symbol $(q\mathbb{Z},\mathbb{Q}(\tau)/\mathbb{Q})$ (obvious functoriality: condition $\sigma_q x\equiv x^q \bmod \mathfrak{q}$ $\forall x\in\mathcal{O}_K$ $\Rightarrow$ $\sigma_q x\equiv x^q \bmod \mathfrak{q}\cap\mathcal{O}_{\mathbb{Q}(\tau)}$ $\forall x\in\mathcal{O}_{\mathbb{Q}(\tau)}$) so by Prop (μ) in (39) (which was not using quadr rec.) have $\sigma_q\tau=\left(\frac{p^*}{q}\right)\tau$. Conclude $\left(\frac{q}{p}\right)=\left(\frac{p^*}{q}\right)=\left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$

qed//

[+] so $\tau=\sqrt{p^*}$

(28) Abelian extensions$^{(++)}$: class field th.

that may be ϕ

(Def) Let K be a # field & S a set of primes of K. Den by $I(S)$ the semigr $I(\prod_{p\in S} p)$ of all ideals $\underline{a} \in I(\mathcal{O}_K)$ prime to S i.e. not div by any $p \in S$ (*)
For $\forall$ abel ext $L|K$ unramif outside S (i.e. $\forall p \notin S \Rightarrow p$ unr. in L) we have (22) (φ) the recipr. map (Artin map)

$$\mathcal{A}^S_{L|K} := (-, L|K) : I(S) \longrightarrow G(L/K)$$

Then $\operatorname{Ker} \mathcal{A}^S_{L|K}$ is a semigr $\subset I(S)$ (apriori not full: it satisfies axiom 2) in def of "full" but apriori not 1)). Call $\operatorname{Ker}\mathcal{A}^S_{L|K}$ the Artin kernel.

(Th1) $\mathcal{A}^S_{L|K}$ surj & $\exists\, c \in I(\mathcal{O}_K)$, $\operatorname{Supp} C = S$ (cf (+)) s.t. $P^+_c \subset \operatorname{Ker}\mathcal{A}^S_{L|K}$.
In partic $\operatorname{Ker}\mathcal{A}^S_{L|K}$ is full & have $\underline{\text{gr}}$. iso $I(c)/\operatorname{Ker}\mathcal{A}^S_{L|K} \xrightarrow{\sim} G(L|K)$.
Moreover $\operatorname{Ker}\mathcal{A}^S_{L|K}/P^+_c$ is gen by $N_{L|K} I(c\mathcal{O}_L)$. So have

$$\frac{I(c)/P^+_c}{\langle N_{L|K} I(c\mathcal{O}_L)\rangle} \xrightarrow{\sim} G(L|K)$$

Obs. This shows that the primes $p \in I(c)$ that split completely in L are precisely the primes lying in a finite union of ray classes

(Th2) The map $L/K \mapsto \operatorname{Ker}\mathcal{A}^S_{L|K}$ establishes a bij between I{ abelian ext of K (in $\bar{K}$) unramif outside S } and II{ full semigr of $I(S)$ that contain a suitable P^+_c for some $C \in I(\mathcal{O}_K)$, $\operatorname{Supp} c = S$ }. This corresp reverses inclus.

(Obs) 1) If a semigr $\Gamma \in$ II corresponds to $L|K \in$ I say $L|K$ is a class field for Γ.
2) Note that P (= semigr of princ ideals $\in I(\mathcal{O}_K)$) belongs to II for $S=\phi$ (++)
The class field to P is called Hilbert class field of K & is den by $H(K)=H$
Note H/K unramif, $[H:K] = |Cl(K)|$, more precisely $Cl(K) \xrightarrow{\sim} G(H/K)$.
3) Similarly P^+ (= semigr of pr id $\alpha\mathcal{O}_K$, $\alpha \in \mathcal{O}_K$, α totally positive i.e. $\sigma\alpha > 0$, $\forall \sigma \in \operatorname{Hom}(K, \mathbb{R})$) belongs to II for $S=\phi$ (is the minimal elt). The class field to P^+ is then the max abelian non-ram ext$^{(\oplus)}$ of K & is den by $H^+ = H^+(K)$ (so $H^+(K) \supset H(K)$). By def & (Th1) $I/P^+ \simeq G(H^+/K)$.
4) If $S \neq \phi$ arb, II has no minimal elt, so I has no max elt! For each $c \in I(\mathcal{O}_K)$ $\operatorname{Supp} c = S$ the corr class field is called the ray class field of c, denoted H^+_c.

(++) $P \supset P^+_c$ for $c = \mathcal{O}_K$. / (+++) we stress that "abel ext" are "finite Galois ext with abel Gal grp"

(*) if $S=\phi$ set $\prod_{p\in S} p \overset{def}{=} \mathcal{O}_K$ so $I(S) = I(\mathcal{O}_K)$

(+) i.e. The primes that divide c are precisely those in S. So $I(c) = I(S)$

(⊕) or Hilbert$^+$ class field /

Have $I(S)/P_c^+ \xrightarrow{\sim} G(H_c^+/K)$. So picture is

$$K - H - H^+ - H_c^+ - H_{c'}^+ \qquad \text{if } c' \subset c$$

Gal Groups: I/P (for $K - H$), I/P^+ (for $K - H^+$), $I(S)/P_c^+$ (for $K - H_c^+$)

clear at least for suitable c (not for any C !)

(Ex) Case $K = \mathbb{Q}$, $H = H^+ = \mathbb{Q}$, $H^+_{m\mathbb{Z}} = \mathbb{Q}(\zeta_m)$. (Cor) $\forall$ ab ext of $\mathbb{Q}$ contained in some $\mathbb{Q}(\zeta_m)$ $\Leftarrow$ Kronecker-Weber Th.

In gen $\forall L \in \underline{I}$ is contained in some H_c^+. Any such c is called Artin conductor.

(Rem) Strategy of pfs (cf Artin) It is suff to prove (in order to prove Th 1 & 2)

a) (surj of Artin map): $\mathcal{A}^S_{L|K}$ surj for $\forall$ ab ext $L|K$ unr outside S.

b) (universal norm index th): $\left[\frac{I(c)}{P_c^+} : \langle N_{L|K} I(c\mathcal{O}_L)\rangle\right] \le [L:K]$ for any $L|K$ as in a) & $\forall c \in I(\mathcal{O}_K)$, Supp $c = S$.

c) (existence of Artin conductor): for any ab ext $L|K$ unr outside S, $\exists\, c \in I(\mathcal{O}_K)$, Supp $c = S$ s.t. $\operatorname{Ker} \mathcal{A}^S_{L|K} \supset P_c^+$.

d) (unicity of class fields): If $\operatorname{Ker} \mathcal{A}^S_{L_1|K} = \operatorname{Ker} \mathcal{A}^S_{L_2|K}$ for 2 ab ext L_1, L_2 unr out $S \Rightarrow L_1 = L_2$

e) (existence th for cl fields): For $\forall$ full semigr Γ containing a P_c^+ $\exists$ ab ext $L|K$ unr out S s.t. $\Gamma = \operatorname{Ker} \mathcal{A}^S_{L|K}$.

[We shall prove later a), b), d) but not c) & e)]
Need: zeta fcns for a), d) & L-fcns for b)

c) & e) are proved algebraically by adjoining suitable roots of 1, applying cycl Th + Kummer th & going back.

(29) Riemann & Dedekind Zeta functions ζ & ζ_K

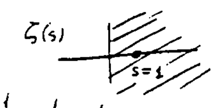
Def For $n \in \mathbb{Z}^+$ & $s \in \mathbb{C}$ set $n^s = e^{(\log n)s} \in \mathbb{C}^*$. So $|n^s| = n^{\mathrm{Re}\, s}$. Write $s = x+iy$, $x,y \in \mathbb{R}$

(α) **Th** (Convergence of Dirichlet series) Let $(a_n)_{n\geq 1}$ be a seq $a_n \in \mathbb{C}$. Assume $\sum_{n\leq T} a_n = O(T^r)$ for some $r \geq 0$ (cf (+)). Then $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges unif (++) in any compact subset of $\{\mathrm{Re}\, s > r\}$ (hence is hol in s on $\{\mathrm{Re}\, s > r\}$.)

Pf. Analysis.

Ex $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$ conv & is hol on $\{\mathrm{Re}\, s > 1\}$. Also $f(s) := 1 - \frac{1}{2^s} + \frac{1}{3^s} - \cdots$ conv & is hol on $\{\mathrm{Re}\, s > 0\}$.

(β) **Prop** $(s-1)\zeta(s)$ extends (*) to a hol fcn on $\{\mathrm{Re}\, s > 0\}$. So (equiv) $\zeta(s)$ extends (O) to mer fcn on $\{\mathrm{Re}\, s > 0\}$ with 1 pole of ord 1 at $s=1$.



Pf. $\left(1 - \frac{2}{2^s}\right)\zeta(s) = \left(1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots\right) - 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \cdots\right) \overset{(\nabla)}{=} 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} \cdots =: f(s)$

$\left(1 - \frac{3}{3^s}\right)\zeta(s) = \left(1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots\right) - 3\left(\frac{1}{3^s} + \frac{1}{6^s} + \frac{1}{9^s} + \frac{1}{12^s} \cdots\right) \overset{(\nabla)}{=} 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \cdots =: g(s)$

for $\mathrm{Re}\, s > 1$. By (α) f & g are hol on $\{\mathrm{Re}\, s > 0\}$. By

$$\zeta(s) = \frac{f(s)}{1 - \frac{2}{2^s}} = \frac{g(s)}{1 - \frac{3}{3^s}} \quad (\mathrm{Re}\, s > 1)$$

& fact that $1 - \frac{2}{2^s}$, $1 - \frac{3}{3^s}$ have only $s=1$ as common zero $(\nabla\nabla)$ & this is a simple 0 $(\nabla\nabla\nabla)$ ⇒ done (!)

Now to define zeta fcn of Dedekind need:

(γ) **L** Let K be a # field $[K:\mathbb{Q}] = N$. Then ∃ constant $\gamma \in \mathbb{R}$ with the foll prop. For any div class $\mathscr{C} \subset I(\mathcal{O}_K)$ (**) we have $\#\{\underline{a} \in \mathscr{C} \mid N\underline{a} \leq T\} = \gamma \cdot T + O_{\mathscr{C}}(T^{1-\frac{1}{N}})$ (!!)

Pf (vague idea only). Let $\underline{b}_0 \in I$ s.t. $\underline{a}_0 \underline{b}_0 \in P$, $\underline{a}_0 \in \mathscr{C}$. Then we have bij

$\{\underline{a} \in \mathscr{C} \mid N\underline{a} \leq T\} \xrightarrow{\sim} \{(\alpha) \subset \underline{b}_0 \mid |N\alpha| \leq (N\underline{b}_0) \cdot T\} \simeq \underbrace{\{\alpha \in \underline{b}_0 \mid |N\alpha| \leq (N\underline{b}_0)T\}/U_K}_{\text{to estimate this use "Minkowski" th.}}$

$\underline{a} \longmapsto \underline{a}\underline{b}_0$

(if U_K finite our # is $|U_K|^{-1} \cdot \#\{\alpha \in \underline{b}_0 \mid |N\alpha| \leq (N\underline{b}_0)T\}$ a.s.o. if U_K infinite more subtle...)

(**) i.e. $\mathscr{C}$ = equiv class wrt $\underline{a}_1 \sim \underline{a}_2 \Leftrightarrow \exists\, \alpha_1, \alpha_2 \in \mathcal{O}_K$ s.t. $\alpha_1 \underline{a}_1 = \alpha_2 \underline{a}_2$; i.e. $\mathscr{C}$ fibre of $I(\mathcal{O}_K) = I \to \underbrace{I/P}_{Cl(K)}$

(*) but not by the original series

$(\nabla\nabla\nabla)$ look at derivative

(!) $s=1$ is really a pole for ζ bec. if ζ were hol at $s=1$ we would get $f(1)=0$ which is not so $f(1) = (1-\frac{1}{2}) + (\frac{1}{3} - \frac{1}{4}) + \cdots > 0$

$(\nabla\nabla)$ Eq $n^s = 1$ has sol's $s \in \left\{\frac{2k\pi i}{\log n} \mid k \in \mathbb{Z}\right\}$

(∇) for $\mathrm{Re}\, s > 1$ where everything is abs conv by (α) I can change order of summation

---

(+) If $f, g : [a, \infty) \to \mathbb{R}$ (or $: \mathbb{N} \to \mathbb{R}$). Say $f = O(g)$ if $\exists\, C \in \mathbb{R}_+$ s.t $|f| \leq C \cdot g$

(O) The "Riem zeta fcn" (introduced by Euler).

(++) but not absolutely.

(!!) $O_{\mathscr{C}}(T^r)$ means a fcn $\in O(T^r)$ that depends on $\mathscr{C}$.

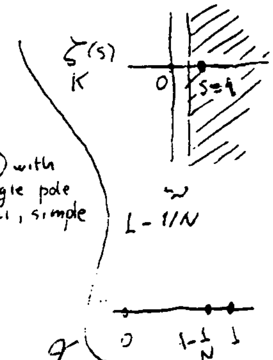
(ζ) (Rem) More is true: $\forall\, \mathfrak{c} \in I(\mathcal{O}_K)$ $\exists$ const $\gamma_{\mathfrak{c}}^{+} \in \mathbb{R}$ s.t. $\forall$ ray class $\mathcal{R} \subset I(\mathfrak{c})$ (i.e. fibre of $I(\mathfrak{c}) \to I(\mathfrak{c})/P_{\mathfrak{c}}^{+}$) we have $\#\{\underline{a} \in \mathcal{R} \mid N\underline{a} \le T\} = \gamma_{\mathfrak{c}}^{+} \cdot T + O_{\mathcal{R}}(T^{1-\frac{1}{N}})$.

(Def) Let K be a # field, $[K:\mathbb{Q}] = N$. Define the Dedekind zeta fn by
$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j_n}{n^s}$, $j_n = \{\underline{a} \in I(\mathcal{O}_K) \mid N\underline{a} = n\}$; by (L) $\sum_{n \le T} j_n \le h_K \gamma T + O(T^{1-\frac{1}{N}}) = O(T)$ so by (α) ζ_K conv. Σ is hol on $\{\operatorname{Re} s > 1\}$. May write
$\zeta_K(s) = \sum_{\underline{a} \in I} \frac{1}{N\underline{a}^s}$, $\operatorname{Re} s > 1$ (no order of Σ specified because positive terms so abs. conv) (also clearly $\zeta_{\mathbb{Q}} = \zeta$).

(ε) (Prop) $(s-1)\zeta_K(s)$ extends to a hol fcn on $\{\operatorname{Re} s > 1 - \frac{1}{N}\}$, $N = [K:\mathbb{Q}]$.
(equiv ζ_K mer for $\operatorname{Re} s > 1-\frac{1}{N}$, with only 1 pole at $s=1$, which is simple).

Pf For $\operatorname{Re} s > 1$ have (setting $h = h_K$, the class #):

$$\zeta_K(s) \overset{(\nabla)}{=} \underbrace{\sum_{n=1}^{\infty} \frac{j_n - h\gamma}{n^s}}_{\text{by } (\alpha)\,\&\,(\gamma) \text{ conv \& hol for } \operatorname{Re} s > 1-\frac{1}{N}} + \underbrace{h\gamma\zeta(s)}_{\text{extends to mer fcn on } \operatorname{Re} s > 0,\ \text{cf } (\beta) \text{ with a single pole at } s=1,\ \text{simple}}$$



(L) $a_1, a_2, \ldots \in \mathbb{C}$, $|a_i| < 1$ & $\sum_{i=1}^{\infty} |a_i| < \infty$. Then $\prod_{i=1}^{\infty} (1-a_i)^{-1} = 1 + \sum_{j=1}^{\infty} \sum_{r_1, \ldots, r_j \ge 1} a_1^{r_1} \cdots a_j^{r_j}$
(Moreover both sum & pr absolutely converge & order of factors & terms doesn't matter).
Pf. Analysis

(Prop) Let K be a # field. Then for $\operatorname{Re} s > 1$ have (denoting by $X = \mathcal{I} = \mathcal{I}(\mathcal{O}_K)$ the set of prime ideals)

$$\zeta_K(s) = \sum_{\underline{a} \in I} \frac{1}{N\underline{a}^s} = \prod_{\mathfrak{p} \in X} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1}$$
, both Σ, Π absol. conv & indep of order

Pf. By (L) must check $\sum_{\mathfrak{p} \in X} |N\mathfrak{p}^{-s}| < \infty$. Have $\sum_{\mathfrak{p} \in X} |N\mathfrak{p}^{-s}| = \sum_{\mathfrak{p} \in X} N\mathfrak{p}^{-\operatorname{Re} s} \le \sum_{\underline{a} \in I} N\underline{a}^{-\operatorname{Re} s} \underset{\uparrow}{<} \infty$ (bec $\zeta_K(s)$ conv for $\operatorname{Re} s > 1$)
Similarly, for any set of primes $Y \subset X$, let $[Y] \subset I$ be the semigr gen by Y then define:

(a) (Prop) $\zeta_{K,Y}(s) := \sum_{\underline{a} \in [Y]} \frac{1}{N\underline{a}^s} = \prod_{\mathfrak{p} \in Y} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1}$ for $\operatorname{Re} s > 1$ (both members converge absol & order of factors/terms irrelevant) & give a hol fcn on $\{\operatorname{Re} s > 1\}$.

(t) (Def) If $\zeta_{K,Y}^{n}(s)$ may be extended to a mer fcn in a nbhd of $s=1$ having a pole of ord m at $s=1$ we say Y has <u>polar density</u> m/n. Here $m, n \in \mathbb{Z}_+$.

(∇) $\operatorname{Re} s > 1 \Rightarrow$ abs conv $\Rightarrow$ may interchange ord of summation

(b) **Prop** Let K be a # field & Y a set of primes, $Y\subset X$ (X = set of all primes).

1) If Y finite $\Rightarrow$ Y has polar density 0 [because each "Euler factor" $\frac{1}{1-\frac{1}{\mathbb{N}p^s}}$ is hol for $\operatorname{Re} s>0$]

2) If $Y=X$ $\Rightarrow$ Y has pol dens 1 [because $\zeta_{K,X}=\zeta_K$ has a pole of ord 1, (29)(ε)]

3) If $Y\subset Z\subset X$ & $Z\setminus Y$ has pol dens 0 then (Y has pol dens $\theta \Leftrightarrow X$ has pol dens θ). [Indeed $\zeta_{K,Z}=\zeta_{K,Y}\cdot\zeta_{K,Z\setminus Y}$ & by hyp $\exists\, m$ st $\zeta^m_{K,Z\setminus Y}$ is hol around $s=1$ $\Rightarrow$ easily]

4) If ($\forall p\in Y \Rightarrow \mathbb{N}p$ is not prime)$^{++}$, then Y has polar dens 0 [indeed let's check $\zeta_{K,Y}(s)$ extends hol to $\{\operatorname{Re} s>\frac12\}$. Have $\zeta_{K,Y}=\prod_{p\in Y}\left(1-\frac{1}{\mathbb{N}p^s}\right)^{-1}$; each $\mathbb{N}p$ is a power of a prime in $\mathbb{Z}$, at least a square, & each prime in $\mathbb{Z}$ occurs at most $[K:\mathbb{Q}]$ times. So splitting Y according to primes of $\mathbb{Z}$ $\Rightarrow$ $\zeta_{K,Y}$ = prod of $[K:\mathbb{Q}]$ subprod, & each subprod is expressible as $\sum \frac{a_n}{n^s}$ with ~~$\sum_{n\le T} a_n$ bounded by the similar argu~~ ~~…~~ & done by (29)(α)]

(c) **Th** Let L/K be a normal ext of # fields. Then the set $Y_{L/K}$ of primes of k that split completely in L has polar density $1/[L:K]$. (In partic $Y_{L/K}$ is infinite, with ∞ complement in the set of all primes.)

Pf Let $Y=Y_{L/K}$ & let Z be the set of primes of L lying over primes of Y. $\forall p\in Y$, $\exists\, n:=[L:K]$ primes $\mathfrak{P}\in Z$ lying over p & $\mathbb{N}p=\mathbb{N}\mathfrak{P}$ (because $f(\mathfrak{P}/p)=1 \Rightarrow$ $\Rightarrow \mathcal{O}_K/p=\mathcal{O}_L/\mathfrak{P}$). So $\zeta_{L,Z}=\zeta^n_{K,Y}$. Let X = set of all primes in L & $R\subset X$ the primes lying over ramif. primes. Then $\forall \mathfrak{P}\in X\setminus(Z\cup R)$ $\Rightarrow$ $\mathbb{N}\mathfrak{P}$ not prime (indeed suf that $N_{L/K}\mathfrak{P}$ not prime in $\mathcal{O}_K$. But $N_{L/K}\mathfrak{P}=p^{f(\mathfrak{P}/p)}$, $p=\mathfrak{P}\cap\mathcal{O}_K$. Recall that by normality (i.e. Galois) all primes over p have same f & same e. Since $\mathfrak{P}\notin Z \Rightarrow p\notin Y \Rightarrow$ either $e\neq1$ or $f\neq 1$. Since $\mathfrak{P}\notin R \Rightarrow e=1$. So $f\neq 1$, qed). By Prop (b) 4) $X\setminus(Z\cup R)$ has pol dens 0. By (b) 2), 3) $\Rightarrow$ $Z\cup R$ has pol dens 1. By (b) 1) & 3) $\Rightarrow$ Z has pol dens 1 $\Rightarrow$ $\zeta^\nu_{L,Z}$ has a pole of ord ν at $s=1$ (for some ν) $\Rightarrow$ $\Rightarrow \zeta^{n\nu}_{K,Y}$ has a pole of ord ν $\Rightarrow$ Y has pol dens $\frac{\nu}{\nu n}=\frac1n$ qed

(d) **Th** Let L_1/K, L_2/K be 2 normal ext of # fields, cont in $\overline{K}$. Let $Y_i=Y_{L_i/K}$ be the set of primes in K that split compl. in L_i. Ass $Y_1\setminus Y_2$ & $Y_2\setminus Y_1$ are finite. Then $L_1=L_2$ (hence also $Y_1=Y_2$).

Pf Let $Y=Y_1\cap Y_2\cap R_{12}$ (where R_{12} = pr of K that ramif in L_1L_2). Then any $p\in Y$ splits completely in L_1L_2 [because if $\mathfrak{P}$ prime in L_1L_2 above p and $\sigma\in G_{\mathfrak{P}}$ (= decomp. gr) $\subset G(L_1L_2/K)$ $\Rightarrow$ $\sigma|_{L_i}\in G_{\mathfrak{P}_i}\in G(L_i/K)$,

~~$\zeta(s) = 1+\frac{1}{4^s}+\frac{1}{9^s}+\dots$ so $\sum_{n\le T} a_n$ (for this Dir series) = # squares less than T $\le T^{1/2}$~~

$^{++}$ equivalently $\deg p\geq 2$, where $\deg p = f(p/p\cap\mathbb{Z})$

Let (f_p) fam of nat #'s. Call $n\in\mathbb{Z}$ an f-power if $v_p(n)\equiv 0 \mod f_p$

$a_n\in\{0,1\}$ & $a_n=0$ if n not an f-power. So $\sum_{n\le T} a_n = \#\{f\text{-powers} \le T\} \le \#\{\text{squares} \le T\} = O(T^{1/2})$

$\{f\text{-powers} \le T\} \to \{\text{squares} \le T\}$, $\prod_p p^{f_p g_p} \mapsto \prod_p p^{2g_p}$ if $f_p\geq 2$ for all p

$\mathfrak{P}_i = \mathfrak{P} \cap \mathcal{O}_{L_i}$. But $G_{\mathfrak{P}_i} = 1$ bec p splits compl in L_i so $\sigma|_{L_i} = id$ $i=1,2$

$\Rightarrow \sigma = id \in G(L_1L_2/K)$. So $G_{\mathfrak{P}} = 1$. So p splits compl in L_1L_2.

Let $\Upsilon_{12} = \Upsilon_{L_1L_2/K}$ = set of primes of K that split compl in L_1L_2 - We just saw $\Upsilon \subset \Upsilon_{12}$. But also clearly $\Upsilon_{12} \subset \Upsilon_1 \cap \Upsilon_2$. Th ($\gamma$) applied to L_i gives Υ_i has pol density $1/[L_i:K]$. Th (γ) appl to L_1L_2 gives Υ_{12} has pol density $1/[L_1L_2:K]$. By (β 2), 3), since $\Upsilon_1, \Upsilon_2, \Upsilon_{12}$ differ by finite sets $\Rightarrow$ $[L_1:K] = [L_2:K] = [L_1L_2:K]$. $\Rightarrow$ $L_1 = L_2$.

(e) Rem The above already proves the "unicity of class fields" (28) for the primes in $\mathrm{Ker}\, \omega^S_{L/S}$ are precisely the primes $\notin S$ that split completely in L.

(f) Th Let L/K be a nor ext of # fields & $H \triangleleft G(L/K)$ a nor. subgr. Let S be a fin set of primes of K s.t. L/K unramif outside S. Then $\{ p$ prime in $K \mid p \notin S, \exists \mathfrak{P}$ prime in L, $\mathfrak{P} \mid p$, $(\mathfrak{P}, L/K) \in H \}$ has polar density $|H| / |G(L/K)|$.

Pf For $\mathfrak{P} \mid p, p \notin S$ we have $(\mathfrak{P}, L/K) \in H \underset{\text{Galois corr}}{\Leftrightarrow} (\mathfrak{P}, L/K)|_{L^H} = 1 \in G(L^H/K) \Leftrightarrow$ $(\mathfrak{P}, L^H/K) = 1 \Leftrightarrow \mathfrak{P}$ splits compl in L^H & apply (γ) to L^H/K.

$(\mathfrak{P}, L/K)|_{L^H} = (\mathfrak{P}, L^H/K)$ clearly functorial (use def $\sigma x \equiv x^{Np} \bmod \mathfrak{P}$)

(g) Rem (f) proves the "surj of Artin map" in (28)

Rem (c) proves that $\exists \infty$ many primes $\equiv 1 (4)$ & ∞ many $\equiv 3 (4)$ [Take $\mathbb{Q}(i)/\mathbb{Q}$]

$\exists \infty$ many primes $\equiv 1\,(p)$ where p given prime [Take $\mathbb{Q}(\zeta_p)/\mathbb{Q}$] (27)

More generally: Dirichlet's th says $\exists \infty$ many primes $\equiv a\,(m)$ if $(a,m)=1$ (to prove this one needs L-fcns of $\mathbb{Q}$ not ζ_K-fcns for K!)

FACTS ABOUT DENSITIES

$Y \subset X = \{p \mid p \text{ prime in } \mathbb{Z}\}$

Def Y has polar density $r \in \mathbb{Q}_+$ if $\exists\, m, n \in \mathbb{Z}$, $r = \frac{m}{n}$, $\zeta^n_{\mathbb{Q},Y}$ can be mer. cont around $s=1$ w/ pole of ord m. | here $\zeta_{\mathbb{Q},Y}(s) := \prod_{p \in Y} \left(1 - \frac{1}{p^s}\right)^{-1}$

Def Y has Dirichlet density $r \in \mathbb{R}_+$ if

$$\lim_{\substack{s \in \mathbb{R} \\ s \downarrow 1}} \frac{\sum_{p \in Y} \frac{1}{p^s}}{\sum_{p \in X} \frac{1}{p^s}} = r$$

Def Y has natural density $r \in \mathbb{R}_+$ if

$$\lim_{N \to \infty} \frac{\#\{p \in Y \mid p \le N\}}{\#\{p \in X \mid p \le N\}} = r$$

<u>Facts</u>

$$\begin{tikzcd}[column sep=small]
Y \text{ has polar density } r \arrow[dr, Rightarrow, shift left] & & Y \text{ has natural density } r \arrow[dl, Rightarrow, shift left] \\
& Y \text{ has Dir. density } r \arrow[ul, Rightarrow, shift left, "\not" description, "1"] \arrow[ur, Rightarrow, shift left, "\not" description, "2"'] &
\end{tikzcd}$$

1, 2 follow from the foll fact: $Y = \{p \in X \mid 1^{st} \text{ digit of } p \text{ is } 1\}$ has Dir. density $\log_{10} 2$ (Bombieri) but no natural density (PNT) & no polar density (b/c $\log_{10} 2 \notin \mathbb{Q}$).

(30) Dirichlet L-functions L & L_K

(Def) Recall that for any finite gr G we set $\hat{G} = Hom(G, \mathbb{C}^*)$. Write $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Embed naturally $\widehat{\mathbb{Z}_m^*} \hookrightarrow Map(\mathbb{Z}, \mathbb{C})$ by letting $\chi(n) = 0$ $\forall \chi \in \widehat{\mathbb{Z}_m^*}$, $\forall$ n not prime to m. For $\chi \in \widehat{\mathbb{Z}_m^*}$ define

$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ (by (29) (α) it is conv & hol on $\{Re\ s > 1\}$ because $|\chi(1)+\dots+\chi(n)| \le |\chi(1)|+\dots+|\chi(n)| \le n$ so $\sum_{n\le T} \chi(n) = O(T)$) As in (30) (L) & (α)

$L(s,\chi) = \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, $Re\ s > 1$. In partic $L(s,1) = \zeta(s) \prod_{p|m}(1 - \frac{1}{p^s})$.

So

(α) (Prop) $L(s,1)$ extends to mer fcn on $Re\ s > 0$ with simple pole at $s=1$ [(29) (β)]

(β) (Prop) For $\chi \ne 1$, $L(s,\chi)$ extends to hol fcn on $Re\ s > 0$

Pf $\sum_{n\le T} \chi(n)$ is a periodic (+) fcn in T, hence is $O(1)$ & apply (29) (α)

(γ) (Prop) (Link bet ζ_K & L). Ass $K = \mathbb{Q}(\zeta_m)$, set $G = G(K/\mathbb{Q})$, consider iso $(\mathbb{Z}/m\mathbb{Z})^* \simeq G(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ & hence iso $\hat{G} \simeq \widehat{\mathbb{Z}_m^*}$. Let Y be the set of primes of K prime to m. Then

1) $\zeta_{K,Y}(s) = \prod_{\chi \in \hat{G}} L(s,\chi)$, $Re\ s > 1$

2) $L(1,\chi) \ne 0$ for $\chi \ne 1$

Pf. Give pf only in case $\longrightarrow$ $m = p$ prime (in general similar).

For each prime $q \in \mathbb{Z}$, $q \ne p$ let $f_q = f(\mathfrak{q}_i/q)$, $g_q = r$ where $q\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_r$

(so $f_q g_q = p-1$) By (27) (δ) if $\sigma_q = (q, K/\mathbb{Q})$ then $\sigma_q \zeta_p = \zeta_p^q$. So

$f_q = (\text{order of } \sigma_q \text{ in } G(K/\mathbb{Q})) = (\text{order of } q \text{ in } (\mathbb{Z}/p\mathbb{Z})^*)$

$\langle \sigma_q \rangle = $ decomp gr $\qquad G(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^*$

So $\chi(q)$ is a f_q-root of 1 [because $(\chi(q))^{f_q} = \chi(q^{f_q}) = \chi(1) = 1$] & moreover if χ vary in $\hat{G}$ $\Rightarrow$ $\chi(q)$ vary through whole set of f_q-roots of 1

Indeed look at homo $\hat{G} \longrightarrow \underbrace{\{f_q\text{-roots of } 1\}}_{\mu_{f_q}} \subset \mathbb{C}^*$, $\chi \mapsto \chi(q)$ (++)

(+) $\chi(n) + \chi(n+1) + \dots + \chi(n+m) = 0$ $\forall n$, because more gen, if G fin gr & $\chi \in \hat{G}$ $\Rightarrow$ ($\chi \ne 1 \Rightarrow \sum_{g\in G} \chi(g) = 0$); bec if $\chi(g_0) \ne 1$ then $\chi(g_0)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(g_0 g) = \sum_{g\in G}\chi(g)$).

(++) This is surj b/c if $\zeta \in \mu_{f_q}$ $\exists$ $\chi' : \langle \hat{q} \rangle \to \mathbb{C}^\times$, $\chi'(q) = \zeta$
Can prolong χ' to $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ b/c $\mathbb{C}^\times$ divisible

For each ω, $\chi(q)=\omega$ exactly r_q times as $\chi \in \hat{G}$.

So $\left[x^{f_q} - \dfrac{1}{q^{f_q s}}\right]^{r_q} = \left[\prod_{\omega^{f_q}=1} \left(x - \dfrac{\omega}{q^s}\right)\right]^{r_q} = \prod_{\chi\in\hat G}\left(x - \dfrac{\chi(q)}{q^s}\right)$

So $\zeta_{K,Y}(s) \overset{def}{=} \prod_{\substack{q\neq p \\ q \text{ prin } \mathbb{Z}}} \left(1-\dfrac{1}{q^{f_q s}}\right)^{-r_q} \underset{\text{above}}{=} \prod_{q\neq p}\prod_{\chi\in\hat G}\left(1-\dfrac{\chi(q)}{q^s}\right)^{-1} = \prod_{\chi\in\hat G} L(s,\chi)$

which proves ass 1)

To check 2), copy above equality

> Can be replaced by: if $L(1,\chi)=0$ for some $\chi\neq 1$ then $\prod_{\chi\in\hat G} L(s,\chi)$ holo at $s=1$ so $\zeta_{K,Y}$ holo at $s=1$, so Y has polar density 0; but Y has pol dens $=1$. ✗

$\therefore\ \underline{I} = \prod_{\chi\in\hat G} L(s,\chi) \underset{\text{for } \operatorname{Re} s>1}{=} \prod_{q\neq p}\left(1-\dfrac{1}{q^{f_q s}}\right)^{-r_q} \underset{\substack{\text{If } s\in\mathbb{R}\\ s>1}}{\geqslant} \prod_{q\equiv 1(p)}\left(1-\dfrac{1}{q^s}\right)^{-(p-1)} = \underline{II} \geqslant 1$

[each factor $(1-\frac{1}{q^{f_q s}})^{-r_q}\in\mathbb{R}$ & is >1)
note also that for $q\equiv 1(p)$, $f_q=1$, $r_q=p-1$]

Now if $L(1,\chi)=0$ for some $\chi\neq 1$ $\Rightarrow$
$\Rightarrow L(s,\chi)$ would have a zero at $s=1$ cancelling the simple pole of $L(s,1)$ (α), hence by (α) & (β), $\underline{I}$ would be hol for $\operatorname{Re} s>0$. In partic for $s\in\mathbb{R}$, $s>1$, $s\to 1$, $\underline{II}$ would tend to a finite limit. But $(\underline{II})^{1/p-1} \underset{\substack{\text{for } s\in\mathbb{R}\\ s>1}}{=} \zeta_{\mathbb{Q},\{q\equiv 1(p)\}}(s)$ $\not\to$ [not as in (29)(b)]. Since by (129)(c), $\{q\equiv 1(p)\}$ has polar density >0 [because $\{q\equiv 1(p)\}$ is precisely the set of primes of $\mathbb{Q}$ splitting in $\mathbb{Q}(\zeta_p)$, by (27),(γ)] $\Rightarrow \zeta^{\nu}_{\mathbb{Q},\{q\equiv 1(p)\}}(s)$, $\operatorname{Re} s>1$ has a mer ext around $s=1$ with a genuine pole at $s=1$ (for some $\nu\in\mathbb{Z}_+$)

$\Rightarrow \lim_{\substack{s\in\mathbb{R}\\ s>1\\ s\to 1}} \zeta^{\nu}_{\mathbb{Q},\{q\equiv 1(p)\}}(s) \to \infty$ ✗ DONE.

(δ) **Th** (Dirichlet) For each $m\in\mathbb{Z}$, $a\in\mathbb{Z}_m^*$ the set $Y_a=\{q\in\mathbb{Z}_+ \text{ prime} \mid q\equiv a(m)\}$ has "Dir. density" $\dfrac{1}{\varphi(m)}$ which by def means

$$\lim_{\substack{s\in\mathbb{R}\\ s>1\\ s\to 1}} \frac{\sum_{q\in Y_a}\frac{1}{q^s}}{\sum_{\text{all } q\in Y}\frac{1}{q^s}} = \frac{1}{\varphi(m)} \qquad (\text{in partic } \#Y=\infty)$$

Pf. Set $G=(\mathbb{Z}/m\mathbb{Z})^*$, $Y=\{\text{set of all primes in } \mathbb{Z} \text{ not dividing } m\}$, $J=\{\text{set of integers prime to } m\}$ = free sub semigr on Y

$\phi: J\to G$ canonical mor of semigr, $\hat G = \operatorname{Hom}(G,\mathbb{C}^*)$

So by def, for $n\in J$ have $\chi(n)=\chi(\phi(n))$

For $\operatorname{Re} s > 1$ have

$$\underbrace{\sum_{\chi\in\hat G}\chi(a^{-1})\sum_{q\in Y}\frac{\chi(q)}{q^s}}_{\parallel} \overset{\text{may change ord of summ by abs conv}}{=} \sum_{q\in Y}\frac{1}{q^s}\sum_{\chi\in\hat G}\chi(a^{-1}\phi(q)) = |G|\sum_{\phi(q)=a}\frac{1}{q^s}$$

$g\in G \Rightarrow \sum_{\chi\in G}\chi(g) = \begin{cases} 0 & \text{if } g\neq 1\\ |G| & \text{if } g=1\end{cases}$

$$\sum_{q\in Y}\frac{1}{q^s} + \sum_{\substack{\chi\in\hat G\\ \chi\neq 1}}\chi(a^{-1})\sum_{q\in Y}\frac{\chi(q)}{q^s}$$

Enough if prove that $\sum_{q\in Y}\frac{\chi(q)}{q^s}$, $\chi\neq 1$, stays bounded for $s\in\mathbb{R}$, $s>1$, $s\to 1$. (+) ~~extends to hol fcn on a nbhd of $\{|s-1|<\varepsilon\}$~~

~~Notation: for f,g hol fcns on $\{\operatorname{Re}s>1\}$ write $f\sim g$ if $f-g$ extends to a hol fcn on a nbhd of $s=1$.~~ Since by (δ) $L(1,\chi)\neq 0$ we shall be done if we check for $\chi\neq 1$

(ε) Claim $\sum_{q\in Y}\frac{\chi(q)}{q^s} \approx \log L(s,\chi)$ (++) (for any χ).

[Indeed (♡) $-\log(1-x) = x+\frac{x^2}{2}+\frac{x^3}{3}+\cdots$ for $|x|<1$ get

$$\log L(s,\chi) = \log\prod_{q\in Y}\left(1-\frac{\chi(q)}{q^s}\right)^{-1} = \sum_{q\in Y}\sum_{n\geq 1}\frac{\chi(q)^n}{nq^{ns}} = \sum_{q\in Y}\frac{\chi(q)}{q^s} + \underbrace{\sum_{q\in Y}\sum_{n\geq 2}\frac{\chi(q)^n}{nq^{ns}}}_{A(s)}$$

But $|A(s)| \leq \sum_{q\in Y}\sum_{n\geq 2}\frac{1}{nq^{ns}} \leq \sum_q\sum_{n\geq 2}\frac{1}{q^{ns}} = \sum_q\frac{1}{q^{2s}}\frac{1}{1-\frac{1}{q^s}} \leq$

$$\leq \frac{1}{1-\frac{1}{2^s}}\sum_q\frac{1}{q^{2s}} \leq \frac{1}{1-\frac{1}{2^s}}\zeta(2s) \quad \text{qed} // \;]$$

(η) Remark: Let Z be a set of primes in $\mathbb{Z}$. Ass Z has polar density m/n. Then Z has Dir. density m/n. Indeed if $\zeta^n_{\mathbb{Q},Z}(s)$ extends to a mer fcn around $s=1$ with pole of ord m then $\zeta^n_{\mathbb{Q},Z}(s) = (s-1)^{-m}g(s)$, g hol around $s=1$, $g(1)\neq 0$. Taking log get $n\log\zeta_{\mathbb{Q},Z}(s) \approx m\log\frac{1}{s-1}$. Similarly $\log\zeta_{\mathbb{Q}} \approx \log\frac{1}{s-1}$. As in (ε) $\log\zeta_{\mathbb{Q},Z}(s) \approx \sum_{q\in Z}\frac{1}{q^s}$, $\log\zeta_{\mathbb{Q}}(s) \approx \sum_{\text{all } q}\frac{1}{q^s}$. Combining get

$$\frac{m}{n}\sum_{\text{all } q}\frac{1}{q^s} \approx \sum_{q\in Z}\frac{1}{q^s} \Rightarrow \text{qed}//$$

(+) Make notation $f\approx g$ $[f,g:(1,1+\varepsilon)\to\mathbb{C}]$ if $f-g(s)$ stays bounded as $s\in\mathbb{R}$, $s>1$, $s\to 1$. So what we want is $\sum_q\frac{\chi(q)}{q^s}\approx 0$, $\chi\neq 1$

(++) log is of course multivalued. But if $L: \overset{c}{\cap}(a,b)\subset\mathbb{R} \to \mathbb{C}^*$ is continuous then $\log\circ L: (a,b)\to\mathbb{C}$ makes sense as a usual, unival fcn if I fix a branch of log around $L(c)$. So s real here is crucial!

(♡) To be able to assume throughout the same branch need to mk sure $L(s,\chi)$ does not wind around 0 as $s\in\mathbb{R}$, $s\downarrow 1$. For $\chi\neq 1$ clear

~~Lemma*: Assume L is meromorphic. Then $\exists\,\varepsilon'<\varepsilon$ ... $\{z\in\mathbb{C} \mid |z-1|<\varepsilon\}$ and $\exists$ halfline $H=\{1+\lambda z_0 \mid \lambda\in[0,\infty)\}$, $z_0\in\mathbb{C}$, s.t. $L((0,\varepsilon'))\cap H=\emptyset$. Same for $L: D^*\to\mathbb{C}$, $r\in\mathbb{R}$. If L as above can define $\log\circ L: (0,\varepsilon')\to\mathbb{C}$ where $\log: \mathbb{C}\setminus H\to\mathbb{C}$ is the branch s.t. $-\log(1-x) = x+\frac{x^2}{2}+\frac{x^3}{3}+\cdots$ on $\{x \mid |x|<1\}$.~~ Cor

(φ) **Def** Let K be a # field (of deg N), $c \in I(\mathcal{O}_K)$, $\phi: I(c) \to G := I(c)/P_c^+$ natural semigr homo. Let $\chi \in \hat{G}$. Set for $\underline{a} \in I(c)$, $\chi(\underline{a}) := \chi(\phi(\underline{a}))$. Def:
$L_K(s,\chi) := \sum_{\underline{a} \in I(c)} \frac{\chi(\underline{a})}{N\underline{a}^s}$ (generalizes $L(s,\chi)$ above that corr to $K=\mathbb{Q}$, $c = m\mathbb{Z}$, $\phi: I(m) \to (\mathbb{Z}/m\mathbb{Z})^*$)

As for ζ_K & L (+), the series above conv & hol for $\mathrm{Re}\, s > 1$, $L_K(s,\chi) = \prod_{p \in Y} \left(1 - \frac{\chi(p)}{Np^s}\right)^{-1}$ for $\mathrm{Re}\, s > 1$, $Y = \{\text{prime id, pr to } c\}$, $L_K(s,1)$ extends to mer fcn on $\{\mathrm{Re}\, s > 1 - \frac{1}{N}\}$ with 1 pole, simple at 1 (+) & $L_K(s,\chi)$, $\chi \neq 1$ extends hol to $\{\mathrm{Re}\, s > 1 - \frac{1}{N}\}$.
As in (30)(ε) $\log L_K(s,\chi) \approx \sum_{p \in Y} \frac{\chi(p)}{Np^s}$. As for analogue of property $L(1,\chi) \neq 0$ for $\chi \neq 1$ ((δ) above) this is more subtle; for (δ) we used the explicit form of Artin map for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. In what foll give an alternat pf in more gen case of L_K; we prove simult. the univ norm index th.

(ψ) **Prop** K a # field, L/K normal extension, $G := \frac{I(c)}{P_c^+}$, $N := \langle N_{L/K} I(c\mathcal{O}_L) \rangle \subset G$. Then:
1) [Non-van of L_K at $s=1$] If $1 \neq \chi \in \widehat{G/N} \subset \hat{G}$ $\Longrightarrow$ $L_K(1,\chi) \neq 0$
2) [Universal Norm Index Ineq] $[G : N] \leq [L:K]$

Pf Write (for $\chi \neq 1$) $L_K(s,\chi) = (s-1)^{m(\chi)} g(s,\chi)$, $g(s,\chi)$ hol around 1, $g(1,\chi) \neq 0$
Get
$$\underbrace{\log\frac{1}{s-1} - \sum_{\substack{\chi \in \widehat{G/N} \\ \chi \neq 1}} m(\chi) \log\frac{1}{s-1}}_{= \log\frac{1}{s-1}\left[1 - \sum_{\substack{\chi \neq 1 \\ \chi \in \widehat{G/N}}} m(\chi)\right]} \approx \sum_{\chi \in \widehat{G/N}} \log L_K(s,\chi) \underset{(\varphi)}{\approx} \sum_{\chi \in \widehat{G/N}} \sum_{p \in Y} \frac{\chi(p)}{Np^s} = \sum_{\chi \in \widehat{G/N}} \sum_{a \in G/N} \sum_{p \in Y} \chi(a) \frac{1}{Np^s} =$$
$$= \sum_{a \in G/N} \left(\sum_{\chi \in \widehat{G/N}} \chi(a) \right) \sum_{p \in Y} \frac{1}{Np^s} = |G/N| \sum_{\substack{p \in Y \\ \phi(p) \in N}} \frac{1}{Np^s} \underset{\approx}{>}^{(++)}$$
$$\underset{\approx}{>} |G/N| \sum_{p \in Y_{L/K}} \frac{1}{Np^s} \approx \frac{|G/N|}{[L:K]} \sum_{\substack{\mathfrak{P} \\ f(\mathfrak{P}/\mathfrak{P}\cap\mathcal{O}_K) = 1}} \frac{1}{N\mathfrak{P}^s} \underset{(29)(\delta)4 \,\&\, (\theta)}{\approx} \frac{|G/N|}{[L:K]} \sum_{\mathfrak{P}} \frac{1}{N\mathfrak{P}^s} \underset{(\varphi)}{\approx} \frac{|G/N|}{[L:K]} \log\frac{1}{s-1}$$

Get $m(\chi) = 0$ because $m(\chi) \in \mathbb{Z}_+$. But then get $\frac{|G/N|}{[L:K]} \leq 1$.

(++) $f \underset{\approx}{>} g$ means $f - g(s)$ is bounded from below for $s \in \mathbb{R}$, $s > 1$, $s \to 1$. In our case we have $\underset{\approx}{>}$ bec $\forall p \in Y_{L/K}$ (i.e. (29)(c) any prime of K that splits completely in L) is the norm of a prime of L by definition $\mathfrak{P}$

(∇)(29)(ε) & hsy of (30)

(+) $L_K(s,1)$ differs from ζ_K by fin many Euler factors

(ω) **Cor** (uses ∃ of class fields (28)). K a # field, $c \in I(\mathcal{O}_K)$, $G = I(c)/P_c^+$. Then
1) $L_K(1,\chi) \neq 0$, $\forall \chi \in \hat{G}$, $\chi \neq 1$
2) The set of primes in each ray class (i.e. coset of P_c^+ in $I(c)$) has Dir. dens $\frac{1}{|G|}$.

Pf Take $L = H_c^+$ in (ψ). Then $N = 0 \Rightarrow$ 1st stat. 2nd stat foll ex. as in (δ)

30 bis Dirichlet's class # formula

Recall from (29) p. 45

(L) Let K be a # field of deg N over $\mathbb{Q}$. Then $\exists\ \gamma \in \mathbb{R}$, $\forall$ div class $\mathscr{C} \subset I(\mathcal{O}_K)$ we have $\#\{\underline{a} \in \mathscr{C} \mid N\underline{a} \leq T\} = \gamma \cdot T + O_{\mathscr{C}}(T^{1-\frac{1}{N}})$.

(Rem) (p. 45): if $\zeta_K(s) = \sum_{n \geq 1} \frac{j_n}{n^s} \Rightarrow \zeta_K(s) = \underbrace{\sum_{n\geq 1} \frac{j_n - h\gamma}{n^s}}_{\text{hol for } \mathrm{Re}\, s > 1-\frac{1}{N}} + h\gamma\zeta(s)$

(P_1) Notations as above

$$\gamma = \frac{2^{t+s}\pi^t \operatorname{reg}(\mathcal{O}_K)}{w\ |\delta_K|^{1/2}}$$

where s = # real emb's, t = # pairs of non-real emb's, w = # roots of 1 in K, $\operatorname{reg}(\mathcal{O}_K) = \operatorname{vol}(H/\Lambda_U)/\sqrt{s+t}$, H = hyperplane $y_1 + \cdots + y_{s+t} = 0$ in $\mathbb{R}^{s+t}$, Λ_U = (image of U_K via $K^\times \xrightarrow{\psi} (\mathbb{R}^\times)^s \times (\mathbb{C}^\times)^t \xrightarrow{\lambda} \mathbb{R}^{s+t}$, cf (24) p 35)

Pf. Not given: geo of #'s, see Marcus

Next: amplification of (30), p 49 (same pf in loc cit $K = \mathbb{Q}(\zeta_m)$)

(P_2) Let $K \subset \mathbb{Q}(\zeta_m)$, $G = G(K|\mathbb{Q}) \twoheadleftarrow G(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$ so $\hat{G} \subset \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$

Let Υ = {primes in K coprime to m}. Then

$$\zeta_{K,\Upsilon}(s) = \prod_{\chi \in \hat{G}} L(s,\chi)$$

(P_3) $$h = \gamma^{-1}\Big[\prod_{q|m}(1-\tfrac{1}{q})(1-\tfrac{1}{q^{f_q}})^{-r_q}\Big] \prod_{\substack{\chi\in\hat{G} \\ \chi \neq 1}} L(1,\chi),$$ for $K \subset \mathbb{Q}(\zeta_m)$ as in P_2

Pf By (Rem) above $h\gamma = \lim_{s \downarrow 1} \frac{\zeta_K(s)}{\zeta(s)}$. Now by ($P_2$) get

$$\frac{\zeta_K(s)}{\zeta(s)} = \frac{\prod_{q|m}(1-\frac{1}{q^{f_q}})^{-r_q} \cdot \prod_{1\neq\chi\in\hat{G}} L(s,\chi)\cdot L(s,1)}{\zeta(s)} \Rightarrow \gamma(\text{RHS in } P_3) \ \square.$$

(Rem) For any $z_0 \in \mathbb{C}$, $|z_0| = 1$, $z_0 \neq 1$, we denote by $\log(1-z_0) \in \mathbb{C}$ the value of the log of $1-z_0$ obtained by moving on a path where in $\{z \mid |z|<1\}$ we take the branch $\log(1-z) = -\sum \frac{z^n}{n}$.

i.e. $\log(1-z_0) \overset{\text{def}}{=} \lim_{\substack{z\to z_0\\ |z|<1,\ z/z_0\in\mathbb{R}}} \log(1-z) \overset{\text{def}}{=} \lim_{\substack{z\to z_0\\ |z|<1\\ z/z_0\in\mathbb{R}}} \left(-\sum_{n\geq 1} \frac{z^n}{n}\right)$.

Then for ζ a root of 1

$$\log(1-\zeta) = \lim_{\substack{z\to\zeta\\ |z|<1\\ z/z_0\in\mathbb{R}}} \left(-\sum_{n\geq 1}\frac{z^n}{n}\right) \underset{\uparrow}{=} -\sum_{n\geq 1}\frac{\zeta^n}{n}.$$

Abel's th: if a power series $\underbrace{}_{\text{w/ real or } \mathbb{C}\text{-coeff \& real variable}}$ has radius of conv 1 & is convergent @ 1 (or −1) then it is continuous there; apply this to $\sum a_n z_0^n t^n$.

See Ross' book in UTM, p. 148 →

Note $\sum_{n\geq 1}\frac{\zeta^n}{n}$ conv b/c $\sum_{n\leq T}\zeta^n = O(T^0)$

(P4) $L(1,\chi) = -\frac{1}{m}\sum_{k=1}^{m-1} \tau_k(\chi)\log(1-\zeta_m^{-k})$, $\tau_k(\chi) := \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)\zeta_m^{ak}$

$(\chi\neq 1)$ $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$ (Gauss sum)

Pf. For $\mathrm{Re}\, s > 1$

$$L(s,\chi) = \sum_{n\geq 1}\frac{\chi(n)}{n^s} = \sum_{a\in\mathbb{Z}_m^\times}\chi(a)\sum_{\hat{n}=a}\frac{1}{n^s} = \sum_{a\in\mathbb{Z}_m^\times}\chi(a)\sum_{n\geq 1}\frac{\frac{1}{m}\sum_{k=0}^{m-1}\zeta_m^{(a-n)k}}{n^s}$$

$$= \frac{1}{m}\sum_{k=0}^{m-1}\tau_k(\chi)\sum_{n\geq 1}\frac{\zeta_m^{-nk}}{n^s} \underset{\substack{\uparrow\\ \tau_0=0\\ +\\ \text{Rem above}}}{=} -\frac{1}{m}\sum_{k=1}\tau_k(\chi)\log(1-\zeta_m^{-k}) \ \square.$$

$P_3 + P_1 + P_4$

Th h = expression depending on $t, s, \mathrm{reg}(\mathcal{O}_K), w, |\delta_K|, f_q$ (for $q\,|\,m$), (also $\tau_k(\chi)$, $\log(1-\zeta_m^{-k})$) if $K\subset\mathbb{Q}(\zeta_m)$.

Rem (not to be checked). If $K=\mathbb{Q}(\sqrt{d})$, d square free, $m := |\delta_K|$ then

1) if $d>0$ get $h = \frac{1}{\log(u)}\left|\sum_{\substack{k\in\mathbb{Z}_m^\times\\ k<m/2}}\chi(k)\log\sin\frac{k\pi}{m}\right|$ for some $\chi\in\widehat{\mathbb{Z}_m^\times}$ (the unique char corr to $G(K/\mathbb{Q})$ ...)

where $U_K = \langle \pm 1, -u\rangle$.

2) if $d<0$, $d\neq -1,-3$ we get $h = \frac{1}{2-\chi(2)}\left|\sum_{\substack{k\in\mathbb{Z}_m^\times\\ k<m/2}}\chi(k)\right|$

Computation of γ for K quadratic imaginary.

Let $\mathfrak{a}_0 \in \mathscr{C}$. Fix $\mathfrak{b}_0 \in I(\mathcal{O}_K)$, $\mathfrak{a}_0\mathfrak{b}_0 = (\alpha)$, $\alpha \in \mathcal{O}_K$. Get

$$\{\mathfrak{a} \in \mathscr{C} \mid N\mathfrak{a} \le T\} \simeq \{\beta \in \underbrace{\alpha^{-1}\mathfrak{b}_0}_{\text{lattice in } \mathbb{C}} \mid \underbrace{N\beta \le \frac{T}{N\mathfrak{a}_0}}_{|\beta| \le \text{const}.\, T^{1/2}}\}/\overset{\text{fin gr, known}}{U_K}$$

$$\beta\mathfrak{a}_0 \longleftarrow\!\shortmid\ \beta$$

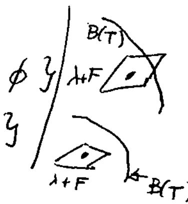
So I'm reduced$^{♡}$ to the foll

(L) Let $L \subset \mathbb{C}$ be a lattice, F a fund dom, $B(T) = \{z \in \mathbb{C} \mid |z| \le T\}$

Then $\#(L \cap B(T)) = \dfrac{\pi}{\mathrm{Vol}(F)} T^2 + O(T)$.

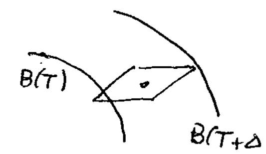
Pf. Let $n(T) = \#(L \cap B(T))$, $n_+(T) = \#\{\lambda \in L \mid (F+\lambda) \cap B(T) \neq \emptyset\}$

$n_-(T) = \#\{\lambda \in L \mid (F+\lambda) \subset B(T)\}$



So $n_-(T) \le n(T) \le n_+(T)$ (*)

Let $\Delta =$ ~~length of~~ $\mathrm{diam}(F)$. Then $n_+(T) \le n_-(T+\Delta)$ (**)



So by (*) & (**)

get $n_+(T-\Delta) \le n(T) \le n_-(T+\Delta)$

so $\underset{\pi(T-\Delta)^2}{\underset{\|}{\mathrm{Vol}(B(T-\Delta))}} \le n_+(T-\Delta)\mathrm{Vol}(F) \le n(T)\,\mathrm{vol}(F) \le n_-(T+\Delta)\mathrm{Vol}(F) \le \underset{\pi(T+\Delta)^2}{\underset{\|}{\mathrm{Vol}(B(T+\Delta))}}$

So $\dfrac{\pi}{\mathrm{Vol}\,F}(T^2 - 2T\Delta + \Delta^2) \le n(T) \le \dfrac{\pi}{\mathrm{Vol}(F)}(T^2 + 2T\Delta + \Delta^2)$

So $n(T) - \dfrac{\pi}{\mathrm{Vol}(F)} T^2 = O(T)$

♡ not going to do the details but note that $\mathrm{Vol}(F)$ in (L) rel to δ_K !!

31 Local fields.

Def A metric space is set X & fcn $d: X\times X \to \mathbb{R}_+$ called $\underbrace{\text{distance}}_{\text{metric co}}$ s.t. $d(x,y)=d(y,x)$, $d(x,z)\le d(x,y)+d(y,z)$, $d(x,y)=0 \iff x=y$.
Seq $x_n\in X$ called Cauchy if $\forall \varepsilon>0\ \exists N$ s.t. $n,m\ge N \Rightarrow d(x_n,x_m)\le\varepsilon$. A seq $x_n\to x_0$ iff… (called conv)
X called complete if $\forall$ Cauchy seq is conv.
Given X one may construct "completion" $\hat X = \{$set of Cauchy seq $(x_n)_n\}/\sim$
$[(x_n)_n\sim(y_n)_n$ if $\forall\varepsilon>0\ \exists N$ s.t. $n\ge N\Rightarrow d(x_n,y_n)<\varepsilon]$ & metric $\hat d$ on $\hat X$ & emb $X\to\hat X$ (s.t. $\hat X$ compl)
$[\hat d((x_n),(y_n)) = \lim_n d(x_n,y_n)$, which $\exists$ bec $\mathbb{R}$ is complete!$]$ [to see $\hat X$ complete use diag. trick].

Def(*) If K field, $v: K\to\mathbb{Z}$ discr. val, def metric (on K) $d(x,y) := |x-y|_v$ where $|x|_v := c^{-v(x)}$ (†), $c>1$.
($|\ |_v$ called abs value (**)). Then $\hat K$ has nat str of field & if $\hat v:\hat K\to\mathbb{Z}$ def by
$\hat v((x_n)) = \lim_n v(x_n) = v(x_m)$ for $m\gg 0 \Rightarrow \hat d(x,y) = |x-y|_{\hat v}$, $\hat v$ discr val. If $A,\hat A$
& $p,\hat p$ are val rings & id of $v,\hat v \Rightarrow \hat A =$ compl of A, $\hat p =$ compl of p & $\frac{A}{p}\simeq\frac{\hat A}{\hat p}$

Ex $K=\mathbb{Q}$, $v \leftrightarrow A=\mathbb{Z}_{p\mathbb{Z}}$ denote $\mathbb{Z}_p$, $\mathbb{Q}_p$ the compl of $A,\mathbb{Q}$. [Ex: $\mathbb{Z}_p = \{\sum_{i=0}^{\infty} a_i p^i,\ a_i\in\mathbb{Z},\ 0\le a_i<p\}$]

(α) Prop K compl discr val field, $A=$ val ring of K, L/K fin sep ext, $B=$ int clos of A in L
(Dedekind by (22),(α)). Then B is DVR ($\iff$ has 1 max id only). Moreover L is complete.
Pf. Let $p\subset A$ max id. Write $pB = P_1^{r_1}\cdots P_m^{r_m}$, P_i primes in B, distinct. Ass $m\ge 2$.
Get by Chin rem th $B/p^nB \simeq B/P_1^{nr_1}\times\cdots\times B/P_m^{nr_m} \ni e_n := (1,0,\dots,0)$. Get
syst of elts $\bar b_n\in B/p^nB$, $b_n\in B$ s.t. $b_{n+1}-b_n\in p^nB$. Since $e_n^2=e_n\Rightarrow b_n^2-b_n\in p^nB$
Now if take A-basis of B get product metric on B & B complete. Clearly b_n Cauchy
so $b_n\to b\in B$, $b^2=b \Rightarrow b(1-b)=0$, B integral $\Rightarrow b=0$ or $b=1 \Rightarrow e_n = \begin{smallmatrix}\to 0\\ \to 1\end{smallmatrix}$ ✗.
To check L complete, write $B=\oplus Ae_i$. Clearly B complete wrt "product metric" (***)

(β) Prop (Hensel Lemma) K compl discr val field, $A=$ its val ring, $p\subset A$ the max id
Let $f\in A[x]$. Ass $a_0\in A$ is s.t. $f(a_0)\equiv 0\ (p)$, $f'(a_0)\not\equiv 0\ (p)$. Then
$\exists a\in A$, $a\equiv a_0\ (p)$ s.t. $f(a)=0$ [i.e. one can lift simple roots of f from $\frac{A}{p}$ to A].
Pf. Construct seq $a_n\in A$ s.t. $a_{n+1}\equiv a_n\ (p^n)$ & $f(a_n)\equiv 0\ (p^n)$ by ind. Ass have
a_n. Set $a_{n+1} = a_n+\pi^n b$, $p=\pi A$, $b\in A$ & try to find b. Have $f(a_{n+1}) =$
$= f(a_n+\pi^n b) \equiv f(a_n) + f'(a_n)\pi^n b \mod(\pi^{n+1})$ If $f(a_n) = \pi^n c$, $c\in A$ take $b = -\frac{c}{f'(a_n)}$
$[f'(a_n)\equiv f'(a_0) \mod p$ by ind so $f'(a_n)\notin p]$.

Def Ass we are in sit of (α) & let p, P be the max id of A,B. Say L/K is
unram, ramif if p is so [unramif $\overset{\Leftrightarrow}{\scriptstyle def}$ $e(P/p)=1$, ramif $\Leftrightarrow e\ge 2$]. Say L/K is
totally ramif if $f(P/p)=1$ [equiv, by (22)(δ), if $e(P/p) = [L:K]$].
Notation: $e(L/K)$, $f(L/K)$ instead of $e(P/p)$, $f(P/p)$.

(†) If $A=$ val ring of v & $p\subset A$ max id we also write $|\ |_p$ in place of $|\ |_v$.

(*) By "loc field" here we mean field + discr val, which is complete.
so —″— = compl discr val field. We shall use the latter term

(**) It sat $|x|=0\Rightarrow x=0$, $|xy|=|x||y|$, $|x+y|\le\max\{|x|,|y|\}$. (called non-arch abs value).

(***) But latter is equiv to "valuation metric" bec if $pA = P^r \Rightarrow$
$\oplus p^n Ae_i = p^nB = P^{nr}$.

(γ) Def From now on assume our K (compl discr val field) has ch 0 & (its res field has) ch $p>0$. For any $\alpha \in \bar{K}$ define $|\alpha| \in \mathbb{R}_+$ as foll: take any $\alpha \in L \subset \bar{K}$, $[L:K]<\infty$ & set $|\alpha| = p^{-\frac{v_{\mathfrak{P}}(\alpha)}{v_{\mathfrak{P}}(p)}}$ (so $|p| = p^{-1}$).

Note $p \in \mathfrak{p}$ = max id of val ring A of K & $\mathfrak{P}$ = max id of int cl B of A in L. ($\Rightarrow |\alpha|$ does not dep on L!). It was essential that B is local, cf (α)!

(δ) Obs In sit (γ), if $\alpha \in \bar{K}$ then all conj α' of α over K have $|\alpha| = |\alpha'|$ [Indeed may take $L|K$ normal, $\alpha \in L$. Then $\forall \sigma \in G(L|K)$, $\sigma B = B$ so $v_{\mathfrak{P}} \circ \sigma = v_{\mathfrak{P}}$]

(μ) Obs In sit (γ) if $\alpha \in L \subset \bar{K}$, L/K fin, we have $|\alpha| = |N_{L|K}\, \alpha|^{1/[L:K]}$ [B_y]

Prop Assume sit in (α) Assume $L|K$ totally ramif. Let $\pi \in L$ be s.t. $v_{\mathfrak{P}}(\pi) = 1$ ($\mathfrak{P}$ = max of B)(*). Then $f := \mathrm{Irr}(\pi, K)$ is an Eisenstein pol of degree $n = [L:K] = e(\mathfrak{P}|p)$, i.e. $f = x^n + a_{n-1}x^{n-1} + \dots + a_0$, $v_{\mathfrak{p}}(a_i) \geq 1$, $v_{\mathfrak{p}}(a_0) = 1$. So also $L = K(\pi)$.

[Pf. If $\pi_K \in K$, $v_p(\pi_K) = 1 \Rightarrow |\pi| = |\pi_K|^{1/e}$. All coeff of f are hom polyn in conj of π so have $v_p \geq 1$. If $\deg f = d$ then $|a_0| = |\prod_{i=1}^{d} \sigma_i \pi| \underset{\text{Obs (δ)}}{=} |\pi|^d = |\pi_K|^{\frac{d}{e}}$ ($\mathrm{Hom}_K(K(\pi), \bar{K}) = \{\sigma_1, \dots, \sigma_d\}$)

$\Rightarrow v_{\mathfrak{p}}(a_0) = \frac{d}{e} \Rightarrow d = e$ & $v_{\mathfrak{p}}(a_0) = 1$ qed]

Prop (Converse of above). If K compl discr val field, val ring $= A$, $f \in A[x]$ Eisenstein polyn, $\alpha \in \bar{K}$ root of $f \Rightarrow L := K(\alpha)/K$ is totally ramified.

Pf f Eisenstein $\Rightarrow f$ irr in $K[x]$ (10) $\Rightarrow f = \mathrm{Irr}(\alpha, K)$. As above, if $f = x^n + \dots + a_0$ then $|\pi_K| = |a_0| = |\alpha|^n$ so $e := e(K(\alpha)/K) \geq n$. Since always $e \leq n$ get $e = n$, done.

(ε) Prop 1) ∃ a unique unramif extension of degree f of $\mathbb{Q}_p$: it is $\mathbb{Q}_p(\zeta_{p^f-1})$ where ζ_{p^f-1} is a primitive p^f-1-root of 1 [Hence by (22)(η) $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^f-1})/\mathbb{Q}_p) \simeq \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ is gen by $\zeta \mapsto \zeta^p$]

2) Any ext $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$, ζ_m a prim m-th root of 1, $p \nmid m$ is unramif.

3) $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is totally ramif of degree $p-1$.

Pf. 3) foll as in (27)(β). 1) ⇒ 2) because $p \nmid m \Rightarrow \exists f$ s.t. $m \mid p^f - 1$ [take f = ord of p in $(\mathbb{Z}/m\mathbb{Z})^*$]

1) Let $L/\mathbb{Q}_p$ be unramif of degree f. Let B = val ring of L & max id $= \mathfrak{P}$. $\Rightarrow \frac{B}{\mathfrak{P}} = \mathbb{F}_{p^f}$. Hensel lemma (β) applied to $x^{p^f-1} - 1 \Rightarrow$ each elt of $\mathbb{F}_{p^f}^*$ lifts to a p^f-1-root of 1 in B. So $\mathbb{Q}_p(\zeta_{p^f-1}) \subset L$. So get = by considering degrees. To conclude 1) need to show ∃ $K/\mathbb{Q}_p$ unramif of given degree f. Let $\mathbb{F}_{p^f} = \mathbb{F}_p(\alpha)$, $f = \mathrm{Irr}(\alpha, \mathbb{F}_p) = x^f + \bar{a}_{f-1}x^{f-1} + \dots + \bar{a}_0$, $a_i \in \mathbb{Z}_p$. Then $F := x^f + a_{f-1}x^{f-1} + \dots + a_0 \in \mathbb{Z}_p[x]$ is irr$/\mathbb{Q}_p[x]$ (because primitive & irr $/\mathbb{Z}_p[x]$ bec if reducible $/\mathbb{Z}_p[x] \Rightarrow F = G \cdot H$, G, H monic ⇒ f reducible ↯). Let $\alpha \in \bar{\mathbb{Q}}_p$ be root of F. Then $K := \mathbb{Q}_p(\alpha)$ has res field $\mathbb{F}_{p^f}$ so it is unramif by equality $n = ef$.

Prop ∀ fin ext $L/\mathbb{Q}_p$, ∃ $\mathbb{Q}_p \subset K \subset L$ s.t. $K/\mathbb{Q}_p$ urm & $L|K$ tot ramif [Pf: Hensel ⇒ $\zeta_{p^f-1} \in L$; set $K = \mathbb{Q}_p(\zeta_{p^f-1})$]

(*) call such a π a parameter of L

OK

(ω) **Def** $\mathbb{Q}_p^{ur} := \bigcup_{\substack{K/\mathbb{Q}_p \\ \text{fin, unramif}}} K = \bigcup_{\substack{\zeta^m = 1 \\ p \nmid m}} \mathbb{Q}_p(\zeta)$ it is discr. val field (<u>not</u> complete); $\mathbb{Z}_p^{ur}$:= its val ring

Res field $= \overline{\mathbb{F}}_p$

Frob $\in G(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ lifts to $\phi \in G(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$, $\phi\zeta = \zeta^p$.

By (ε) red mod p map $T = \left\{ \substack{\text{roots of 1 in } \overline{\mathbb{Q}}_p \\ \text{of ord prime to } p} \right\} \subseteq \mathbb{Q}_p^{ur} \to \overline{\mathbb{F}}_p^*$ is bij so $\exists$ inverse $\theta: \overline{\mathbb{F}}_p^* \to T (\in \mathbb{Q}_p^{ur})$ called Teichmuller character.

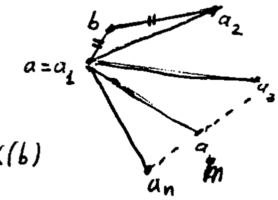
Clearly: any $\alpha \in \widehat{\mathbb{Z}_p^{ur}}$ written uniquely as $\sum \theta(\lambda_i) p^i$, $\lambda_i \in \overline{\mathbb{F}}_p$ where $\theta(0) \overset{def}{=} 0$.

Similarly one proves

Prop If $K/\mathbb{Q}_p$ finite and $\pi \in K$ parameter. Then any $\alpha \in K$ may be written uniquely as $\sum_{i=m}^{\infty} a_i \pi^i$, $m \in \mathbb{Z}$, $a_i^{p^f} = a_i$, $f = f(K/\mathbb{Q}_p)$; so $a_i = 0$ or a_i is $p^f - 1$ root of 1.

(φ) **Prop** (Krasner's lemma) In the setting of (δ) (i.e. K compl discr val of char 0, $c > 1$ fixed). Assume $a, b \in \overline{K}$. Let $a_1 = a, a_2, \dots, a_n \in \overline{K}$ the conjugates of a/K. Ass $|b - a| < |a_i - a|$, $i \neq 1$. Then $K(a) \subset K(b)$.

<u>Pf</u> Ass $K(a) \not\subset K(b)$ i.e. $a \notin K(b)$



May Ass $a_1 = a, a_2, \dots, a_m$ $(2 \le m \le n)$ are the conj of a over $K(b)$

So $\exists\ \sigma \in \mathrm{Hom}_{K(b)}(K(b,a), \overline{K})$, $\sigma a = a_2$. So $\sigma(b - a) = b - a_2$ so $b - a$ & $b - a_2$ are conj$/K(b)$

Get by (δ) that $|b - a| = |b - a_2|$ So get

$$|a_2 - a| \le \max\{|a_2 - b|, |b - a|\} = |b - a| \overset{hyp}{<} |a_2 - a| \quad \text{↯}.$$

In ψ f, g monic

(ψ) **Prop** (Continuity of roots wrt coeff) In the setting of (δ) denote for $\forall f \in K[x]$, $f = \sum_{i=1}^{n} a_i x^i$ (monic & deg f), $|f| := \max_i |a_i|$.

1) $\forall$ root $\alpha \in \overline{K}$ of $f \Rightarrow |\alpha| \le C(|f|)$ where C is a ct depending only on $|f|$, not on f.

more correctly $C(|f|, n)$ where $C: \mathbb{R}_+ \times \mathbb{N} \to \mathbb{R}_+$, $C(-, n)$ increasing, $C \geq 1$

2) Let $f \in K[x]$ have degree n & distinct roots. Then $\forall \varepsilon > 0$ $\exists \delta$ s.t. $\forall g \in K[x]$ of deg n with $|f - g| < \delta \Rightarrow (\forall$ root α_i of f $\exists!$ root β_i of g s.t. $|\alpha_i - \beta_i| < \varepsilon)$

<u>Pf</u> 1) $a_n \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0 \Rightarrow$ (divide by α^n) $a_n + \frac{a_{n-1}}{\alpha} + \frac{a_{n-2}}{\alpha^2} + \dots + \frac{a_0}{\alpha^n} = 0$. Ass 1) fails.

$\Rightarrow \exists$ sequences $a_i^{(\nu)}$ s.t. $|a_i^{(\nu)}|$ bounded & seq $\alpha^{(\nu)}$ of roots s.t. $|\alpha^{(\nu)}| \to \infty$. Then $\frac{|a_i^{(\nu)}|}{|\alpha^{(\nu)}|^i} \to 0$. Get $a_n = 0$ ↯

2) Let β a root of g. Get

$$|f(\beta)| = |f(\beta) - g(\beta)| \le |f - g|\, C(|g|)^n \underset{\nabla}{\le} |f - g| \cdot C(|f|)^n$$

by 1) applied to g ; if $|f - g| \le |f|$

$f = a_n \prod (x - \alpha_i)$; $\|$; $|a_n| |\prod_i (\beta - \alpha_i)|$

$|g| \le \max\{|f|, |f - g|\} \le |f|$ if $|f - g| \le |f|$

$\Rightarrow$ one of the $|\beta - \alpha_i|$ must be small; & only one can because if 2 of them $|\beta - \alpha_i|$, $|\beta - \alpha_j|$ are small so is $|\alpha_i - \alpha_j|$ ↯, bec $\alpha_i \neq \alpha_j$ fixed

(η) **Cor** In the setting of (δ) if $f \in K[x]$ is an irreducible pol $\Rightarrow$ $\exists\ \delta$ s.t. $\forall$ $g \in K[x]$ of degree n with $|f - g| < \delta \Rightarrow g$ irred & $\forall$ root α of g $\exists!$ root α of f s.t. $K(\alpha) = K(\beta)$

<u>Pf</u> (φ), (ψ) [g follows irred because $K(\alpha) = K(\beta)$ so each root of g has degree n]

(θ) Prop Let K be a fin ext of $\mathbb{Q}_p$, $\mathcal{O} \subset K$ the val ring, $\mathfrak{p} \subset \mathcal{O}$ the max ideal $\mathcal{O}^* = \mathcal{O} \setminus \mathfrak{p}$. As usual. Then $\mathcal{O}, \mathfrak{p}, \mathcal{O}^*$ are compact & K is locally comp.
Pf. Enough to check $\mathcal{O}$ compact (bec $\mathfrak{p}$ & $\mathcal{O}$ open hence also closed hence $\mathcal{O}^*$ closed) By pf of (α) $\mathcal{O}$ isometric to prod $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$. So enough $\mathbb{Z}_p$ compact. In a metric space enough check $\forall$ seq $\exists$ conv. subseq. Let $x_n \in \mathbb{Z}_p$, $x_n = \sum \alpha_{ni} p^i$ $0 \le \alpha_{ni} < p$, $\alpha_{ni} \in \mathbb{Z}$. $\exists$ subseq $x_n^{(1)}$ s.t α_{n0} constant. This subseq cont a subseq $x_n^{(2)}$ s.t α_{n1} const a.s.o. Get subs. $x_n^{(1)}, x_n^{(2)}, \dots$. Consider diag subseq $y_n := x_n^{(n)}$. It converges to $\sum \alpha_i p^i$ where α_i is the constant i-digit of $x_i^{(i)}$.

Cor $\mathbb{Q}_p$ has only fin many extensions of fixed degree $\subset \overline{\mathbb{Q}_p}$
Pf (η) + (θ).

Prop The completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}_p}$ w.r.t. $|\ |$ ($K = \mathbb{Q}_p$ in (γ)) is alg. closed [Easy: take a polyn $f \in \mathbb{C}_p[x]$, take $f_i \in \overline{\mathbb{Q}_p}[x]$, $|f - f_i| \to 0$. Claim $\exists$ seq $\alpha_i \in \overline{\mathbb{Q}_p}$ of roots of f_i which is Cauchy: to check this use same estimate as in (ψ)]

Def Some remarkable homomorph. 1) If $R = \mathbb{Z}_p$ or $\widehat{\mathbb{Z}_p^{ur}}$ & $p \neq 2$ then have homomorph inverse to each other $\log = \log_p : 1 + pR \to pR$, $\exp = \exp_p : pR \to 1 + pR$ $(1 + pR < R^*)$ def by $\log(1+\alpha) := \alpha - \frac{\alpha^2}{2} + \frac{\alpha^3}{3} - \cdots$ & $\exp \alpha = 1 + \frac{\alpha}{1!} + \frac{\alpha^2}{2!} + \frac{\alpha^3}{3!} + \cdots$ [they converge & have right codom bec $v_p(\alpha^n/n) \geq v_p(\alpha^n/n!) \geq n - v_p(n!) \geq n - [\frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots] \geq n - \frac{n}{p-1}$]
May extend log to $\overset{\text{contin}}{\text{homolog}}$ $: R^* \to pR$ by $\log \alpha = \frac{1}{m} \log(\alpha^m)$ where $p \nmid m$ & $\alpha^m \equiv 1\ (p)$.
Clearly $\mathrm{Ker}(\log : R^* \to pR) = \{$ roots of 1 of ord prime to $p\}$. If want to pass to $\mathbb{C}_p$ get log & exp give gr. iso. $\{\alpha \in \mathbb{C}_p^* ; |\alpha - 1| < p^{-1/(p-1)}\} \simeq \{\alpha \in \mathbb{C}_p ; |\alpha| < p^{-1/(p-1)}\}$ given by same series. [Actually log may be prol. uniquely to a cont homo $\mathbb{C}_p^* \to \mathbb{C}_p$ that sends p to 0, called Iwasawa log: exercise (?!)].

Fesenko, Kato (B for ab var) → 2) If $R = \widehat{\mathbb{Z}_p^{ur}}$ define Cont homo $\psi : R^* \to R$, $\psi(\alpha) = \frac{1}{p} \log\left(\frac{\phi(\alpha)}{\alpha^p}\right)$ where $\phi : R \to R$ is lift of Frob, cf (ω) (well def bec $\frac{\phi(\alpha)}{\alpha^p} \in 1 + pR$). Claim $\mathrm{Ker}\, \psi = \{$all roots of 1 in $R^*\}$
[Indeed $\psi(\alpha) = 0 \Rightarrow \phi(\alpha) = \alpha^p$. Since $\{\alpha \in R^* \mid \phi(\alpha) = \alpha^p\} \supset \{$roots of 1 of ord. prime to $p\} \xrightarrow{\sim} \overline{\mathbb{F}}_p^*$, enough to check that if $\phi(\alpha) = \alpha^p$ & $\alpha \equiv 1\ (p)$ then $\alpha = 1$. Write $\alpha = 1 + a_m p^m + a_{m+1} p^{m+1} + \cdots$ where $a_i \in \{0\} \cup \{$roots of 1$\}$ ($a_m \neq 0$). Then $\phi(\alpha) = 1 + a_m^p p^m + a_{m+1}^p p^{m+1} + \cdots$. But $\alpha^p = 1 + a_m p^{m+1} + \cdots$ $\Rightarrow a_m = 0$ ⨳] Note: if set $\delta : R \to R$, $\delta\alpha = \frac{\phi(\alpha) - \alpha^p}{p}$ (analogue of deriv)
$$\psi(\alpha) = \frac{\delta\alpha}{\alpha^p} - \frac{p}{2}\left(\frac{\delta\alpha}{\alpha^p}\right)^2 + \frac{p^2}{3}\left(\frac{\delta\alpha}{\alpha^p}\right)^3 - \cdots$$

(32) Adeles & Ideles. Hecke L-functions

(α) (Def) Let K be a # field. For $\forall$ prime $\mathfrak{p}$ of K let $K_{\mathfrak{p}}$ be the completion of K wrt $|\ |_{\mathfrak{p}}$ (recall $|\alpha|_{\mathfrak{p}} = p^{-v_{\mathfrak{p}}(\alpha)/v_{\mathfrak{p}}(p)}$ where $\mathfrak{p}\cap\mathbb{Z}=(p)$). Let M_K be the union $\{\text{primes of } K\} \cup \left(\mathrm{Hom}(K,\bar{\mathbb{Q}})/{\text{complx conj}}\right)$. Its elts den. by $v\in M_K$ (are called places). Denote by $|\ |_v$ either $|\ |_{\mathfrak{p}}$ if $v=\mathfrak{p}$ or $|\alpha|_v = |\sigma\alpha|_\infty$ if $v=\sigma\in\mathrm{Hom}_{\mathbb{Q}}(K,\bar{\mathbb{Q}})$ ($|\sigma\alpha|_\infty$ is usual norm of complex #). Set $N_v=[K_v:\mathbb{Q}_{v_0}]$ (where if $v=\mathfrak{p}\Rightarrow v_0=p$ & if $v=\sigma$ then $\mathbb{Q}_{v_0}=\mathbb{R}$ & K_v is either $\mathbb{R}$ or $\mathbb{C}$ according to whether $\sigma(K)\subset\mathbb{R}$ or not). Set $\|\alpha\|_v = |\alpha|_v^{N_v}$ for $\alpha\in K$. Let $\mathcal{O}_v := \mathcal{O}_{K_v}$ be the val ring of K_v ($=\{\alpha\in K_v \mid |\alpha|_v\le 1\}$) if v is a prime and $\mathcal{O}_v=K_v$ if $v=\sigma$.

(Obs) If A = integr clos of $\mathbb{Z}$ in K (i.e. $A=\mathcal{O}_K$). Then $N_{\mathfrak{p}} \overset{\text{def}}{=} [K_{\mathfrak{p}}:\mathbb{Q}_p] \overset{(22)\delta}{=} e(\hat{A}_{\mathfrak{p}}/\mathbb{Z}_p)f(\hat{A}_{\mathfrak{p}}/\mathbb{Z}_p) \overset{\text{clear}}{=}$ $= e(A_{\mathfrak{p}}/\mathbb{Z}_{p\mathbb{Z}})f(A_{\mathfrak{p}}/\mathbb{Z}_{p\mathbb{Z}}) \overset{\text{def}}{=} e_{\mathfrak{p}}f_{\mathfrak{p}}$. In partic by (22)δ again, $\sum_{\mathfrak{p}|p} N_{\mathfrak{p}} = [K:\mathbb{Q}]$. More generally if $K\subset L$ # fields & $\mathfrak{p},\mathfrak{P}$ primes of K, L, $\mathfrak{P}|\mathfrak{p}$ then $[L_{\mathfrak{P}}:K_{\mathfrak{p}}] = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$ (same arg.).

(β) (Prop)(+) Let $K\subset L$ be # fields, $v\in M_K$; then $\forall\alpha\in L \Rightarrow \mathrm{Tr}_{L/K}\alpha = \sum_{w|v}\mathrm{Tr}_{L_w/K_v}\alpha$, $N_{L/K}\alpha=\prod_{w|v}N_{L_w/K_v}\alpha$

Pf. Ass first $v=\mathfrak{p}\subset A:=\mathcal{O}_K$ & $w\leftrightarrow\mathfrak{P}\subset B=\mathcal{O}_L$. Then, using red mod $\mathfrak{p}^n$ & trick in pf of (31)(α) we get $\hat{B}_{\mathfrak{p}} \simeq \prod_{\mathfrak{P}|\mathfrak{p}}\hat{B}_{\mathfrak{P}}$ [where $\wedge$ on left is completion in product metric of $B_{\mathfrak{p}} = \oplus A_{\mathfrak{p}}e_i$, e_i basis of A-mod B & $\wedge$ on the right is compl in val. metric] Next define Tr & N for fin dim K-alg (that need not be fields) as Tr & det of matrix of mult by an elt (++). Then Prop follows for primes. If $v=\sigma\in\mathrm{Hom}(K,\mathbb{C})$ & $w=\tau\in\mathrm{Hom}(L,\mathbb{C})$ extends σ then may ass σ = inclusion $K\subset\bar{K}\subset\mathbb{C}$ & get $\mathrm{Tr}_{L/K}\alpha \overset{\text{def}}{=} \sum_\tau \tau\alpha = \sum_{\tau\text{ real}}\tau\alpha + \sum_{\substack{\tau\text{ complex}\\ \text{taken mod conj}}}(\tau\alpha+\bar{\tau}\alpha) = \sum \mathrm{Tr}_{L_w/K_v}\alpha$ & same for N.

(γ) (Cor) (Product formula) Let K be a # field (notations as in (α)). Then for $\alpha\in K$ get $\prod_{v\in M_K}\|\alpha\|_v = 1$.

Pf. For $K=\mathbb{Q}$, clear: $\prod_{v_0\in M_{\mathbb{Q}}}\|k\|_{v_0} = \overbrace{|k|_\infty}^{k}\cdot\overbrace{\prod_{p\text{ prime}}p^{-v_p(k)}}^{k^{-1}} = 1$ for $k\in\mathbb{Z}_+$, hence for $k\in\mathbb{Q}$.

For K arb we have

$$\prod_{v\in M_K}\|\alpha\|_v \underset{(\alpha)}{=} \prod_{v\in M_K}|\alpha|_v^{N_v} \underset{(31)(\beta)}{=} \prod_{v_0\in M_{\mathbb{Q}}}\prod_{v|v_0}|N_{K_v/\mathbb{Q}_{v_0}}\alpha|_{v_0} \overset{(\beta)}{=} \prod_{v_0\in M_{\mathbb{Q}}}|N_{K/\mathbb{Q}}\alpha|_{v_0} = 1$$

(++) & check this coincides with prev. def for field ext.

(+) if v, w are primes we know what $w|v$ means., if they are embeddings this means w prolongs v.

(containg $M_{K,\infty} = \mathrm{Hom}(K,\bar{\mathbb{Q}})/_{\text{conj}} =: \{v \in M_K \mid v|\infty\}$)

Def (Adeles) Let K be a # field. For $S \subset M_K$ finite set $\mathbb{A}_S := \mathbb{A}_{K,S} := \prod_{v\notin S} \mathcal{O}_v \times \prod_{v\in S} K_v$. $\mathbb{A} = \mathbb{A}_K = \bigcup_S \mathbb{A}_{K,S} \subset \prod_{v\in M_K} K_v$. Called adele ring. Give $\mathbb{A}_S$ prod top (weakest top s.t. proj are cont.). By Tychonov's th ($\prod$ compact = compact) $\Rightarrow$ $\mathbb{A}_S$ locally comp. Make $\mathbb{A}$ top space (ring!) by letting $\mathbb{A}_S$ be open $\Rightarrow$ $\mathbb{A}$ loc. comp.

Embed $K \to \mathbb{A}$ diagonally. Set $\mathbb{A}_\infty := \mathbb{A}_{M_{K,\infty}} = \prod_{v\nmid\infty} \mathcal{O}_v \times \underbrace{\prod_{v|\infty} K_v}_{\mathbb{R}^s \times \mathbb{C}^t}$

(a_1) **Prop** K discrete in $\mathbb{A}$.

Pf. Ass it's not so $\exists\, x^{(n)} \in k$, $x^{(n)} \to 0$ in $\mathbb{A}$. $\Longrightarrow$ $x^{(n)} \in \mathbb{A}_S$ for some S & $x^{(n)} \to 0$ in $\mathbb{A}_S$. So $|x^{(n)}|_v \le 1$ $\forall v \notin S$ & $|x^{(n)}|_v \to 0$ as $n\to\infty$ $\forall v \in M_K$ (not unif in v!). This contradicts prod. formula.

(a_2) **Prop** $\mathbb{A} = K + \mathbb{A}_\infty$.

Pf Let $a = (a_v)_v \in \mathbb{A}$. Let $v_1,\dots,v_u$ be (all places) s.t. $v_i \nmid \infty$ & $|a_v|_v > 1$. Ass $v_i | p_i \in \mathbb{Z}$ prime. Choose n_i s.t. $|p_i^{n_i} a_v| \le 1$. Set $m = \prod p_i^{n_i}$. Then $|m a_{v_i}| \le 1$ so $m a_{v_i} \in \mathcal{O}_K$. By Chin rem th $\exists\, x \in \mathcal{O}_K$ s.t. $|m a_{v_i} - x|_{v_i} \le |m|_{v_i}$, $\forall i$. So $|a_{v_i} - \frac{x}{m}|_{v_i} \le 1$. Since for $\forall$ other $v \nmid \infty$ have $a_v \in \mathcal{O}_v$, $\frac{x}{m} \in \mathcal{O}_v$ get $|a_v - \frac{x}{m}|_v \le 1$ for $v \ne v_i$, $v\nmid\infty$ as well so $a - \frac{x}{m} \in \mathbb{A}_\infty$ qed.

(a_3) **Prop** $\mathbb{A}/K$ is compact & have surj homo $\mathbb{A}/K \twoheadrightarrow (\mathbb{R}^s \times \mathbb{C}^t)/\psi(\mathcal{O}_K)$ [not cf (24)].

Pf. Enough to check that $\forall a \in \mathbb{A}$ has a repres mod K in $\prod_{v\nmid\infty} \mathcal{O}_v \times F_\infty$ where F_∞ fund dom of $\psi(\mathcal{O}_K)$ in $\mathbb{R}^s \times \mathbb{C}^t$ (not. as in (24)(β)). By above prop $\mathbb{A}/K = (K + \mathbb{A}_\infty)/K = \mathbb{A}_\infty / K \cap \mathbb{A}_\infty = (\prod_{v\nmid\infty} \mathcal{O}_v \times \mathbb{R}^s \times \mathbb{C}^t)/\mathcal{O}_K$ & done.

(Ideles)
Def Let K be a # field. For $\forall$ finite set $S \subset M_K$, $S \supset M_{K,\infty}$ set $J_S = J_{K,S} := \prod_{v\notin S} \mathcal{O}_v^* \times \prod_{v\in S} K_v^*$, $J = J_K := \bigcup J_{K,S}$. Called idele gr.
Locally compact. (Top NOT ind by $\mathbb{A}$). Let $K^* \to J$ be diag. emb. Set $J_\infty := \prod_{v\nmid\infty} \mathcal{O}_v^* \times (\mathbb{R}^*)^s \times (\mathbb{C}^*)^t$

(i_1) **Prop** K^* discrete in J, [same arg as for $\mathbb{A}$]

(i_2) **Prop** $[J : K^* J_\infty] < \infty$; more precisely $J/K^* J_\infty \simeq I/P$ (= div cl gr of K)

Pf Define $J \longrightarrow I/P$ by $a = (a_v)_v \longmapsto [\prod_{v\nmid\infty} \mathfrak{p}_v^{n_v}]$ where $\mathfrak{p}_v \subset \mathcal{O}_K$ corr to v & $n_v = v_{\mathfrak{p}_v \mathcal{O}_v}(a_v)$. Easy to check induces iso.

(Def) Have a $\overset{\text{cont}}{\text{can}}$ homo $\mathcal{J} \to \mathbb{R}^+$, $a=(a_v)_v \mapsto \overbrace{\prod_{v\in M_K}}^{\text{"}} \|a_v\|_v$. Set $\mathcal{J}^0$ = its kernel. (closed)

By prod. formula $K^* \subset \mathcal{J}^0$. Set $C_K = \mathcal{J}/K^*$ (gr. of idele classes).

$C_K^0 = \mathcal{J}^0/K^* \underset{\substack{\text{closed}\\ \text{subgr}}}{\hookrightarrow} C_K$. By ($i_2$) have nat $\overset{\text{surj}}{}$homo $C_K \twoheadrightarrow J/P = Cl(k)$.

(i_3) (Prop) $C_K^0 = \mathcal{J}^0/K^*$ is compact [Pf: Lang p.141; it generalizes Dirichlet's unit th.]

(i_4) (Prop) For $\forall c \in I(\mathcal{O}_K)$ $\exists$ nat surj $\mathcal{J}/K^* \to I(c)/P_c^+$ [ψ]

(Def) $K \subset L$ # fields. Define $Tr_{L/K}: \mathbb{A}_L \to \mathbb{A}_K$, $N_{L/K}: \mathcal{J}_L \to \mathcal{J}_K$ by

$T_{L/K}\, a := (\sum_{w|v} Tr_{L_w/K_v} a_w)_v$, $N_{L/K}\, a = (\prod_{w|v} N_{L_w/K_v} a_w)_v$. They are comp

with $Tr_{L/K}: L \to K$, $N_{L/K}: L^* \to K^*$ by (β) so they induce $Tr_{L/K}: \frac{\mathbb{A}_L}{L} \to \frac{\mathbb{A}_K}{K}$,

$N_{L/K}: C_L \to C_K$. Next – reformulation of class field th in idele-th. terms:

(g_1) (Th) Let L/K be an abelian $\overset{\text{(of \# fields)}}{\text{extension}}$. Then for $c \in I(\mathcal{O}_K)$ any Artin conductor

of L/K consider map $a \mapsto (a, L/K)$ defined as the composition

$\mathcal{J} \to \mathcal{J}/K^* \xrightarrow{(i_4)} I(c)/P_c^+ \xrightarrow{(\ ,L/K)} G(L/K)$. Then

this map does not dep on c, is surj (of course) & has

kernel $= K^* N_{L/K} \mathcal{J}_L$. So get gr iso

$$C_K/N_{L/K} C_L \simeq \mathcal{J}_K/K^* N_{L/K} \mathcal{J}_L \simeq G(L/K)$$

Pf Lang p. 207

(g_2) (Th) The map $L \mapsto N_{L/K} C_L$ is a bij bet ab ext L/K & open subgr that reverses inclusions. (Here K, a # field).

Pf Lang p. 208

(l_1) (Th) Let L/K be an ab ext. Then for any $v \in M_K$, $v \nmid \infty$. the map $K_v^* \to G(L/K)$ def by $\lambda \mapsto ((1,\dots,1,\lambda,1,\dots), L/K)$ is surj onto the decomp gr G_v & has kernel $N_{L_w/K_v} L_w^*$ (w any div of v). So $K_v^*/N_{L_w/K_v} L_w^* \simeq G_v$. (denote this by $(\lambda, L/K)$)

(l_2) (Th) Let K be a # field & v a prime. The ab ext of L/K are in bij with open subgr of K_v^*. Bij is given by $E/K_v \mapsto N_{L_w/K_v} E^*$ where

---

ψ Construction: Let $\mathcal{J}_c = \{a \in \mathcal{J} \mid a_v \equiv 1 \mod^* c_v$ (i.e. $\equiv 1$ for v prime & $a_v > 0$ if $v = \sigma \in Hom(K,\mathbb{R})$ $\}$. First one proves $\mathcal{J}_c/\mathcal{J}_c \cap K^* \xrightarrow{\sim} \mathcal{J}/K^*$ (this generalises Chinese rem th). Then one has a nat surj $\mathcal{J}_c/\mathcal{J}_c \cap K^* \to I(c)/P_c^+$ (obvious).

(i.e. χ trivial on some J_S for S finite) (*)

Def Let K be a # field. By a Hecke character (or Grossenchar.) one underst a homo $\chi : J \to \mathbb{C}^*$ trivial on K^* & s.t. $\chi_v(\mathcal{O}_v^*) = 1$ for all but fin. many $v \in M_K$, where χ_v is compos $K_v^* \to J \xrightarrow{\chi} \mathbb{C}^*$. [Say χ unram at v if $\chi_v(\mathcal{O}_v^*) = 1$; define conductor $c(\chi)$ (+) to be product of ramified v.

Define, for $\mathfrak{p}$ prime of K, $\chi(\mathfrak{p}) = \begin{cases} 0 & \text{if } \mathfrak{p} \mid c(\chi) \\ \chi(\pi) & \text{if } v = \mathfrak{p} \nmid c(\chi) \text{ \& } \pi \text{ par of } \mathcal{O}_v \end{cases}$

Extend def to $\chi(\mathfrak{a})$, $\mathfrak{a} \in I(\mathcal{O}_K)$ (i.e. $\mathfrak{a}$ ideals in $\mathcal{O}_K$). Get $\chi : I(\mathcal{O}_K) \to \mathbb{C}^*$ (+++)

Define Hecke L-fcn formally.

$$L_K(s,\chi) = \sum_{\mathfrak{a} \in I} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} = \sum_{\mathfrak{a} \in I(c(\chi))} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} = \prod_{\mathfrak{p} \nmid c(\chi)} (1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-}$$

Assuming $|\chi(\mathfrak{p})| \le N\mathfrak{p}^{\nu} \Rightarrow L_K(s,\chi)$ conv for $\mathrm{Re}\, s > 1 + \nu$.

Ex 1) $\forall$ character $\chi : I(c)/P_c^+ \to \mathbb{C}^*$ gives a Grossench. $\tilde{\chi} : J/K^* \to \mathbb{C}^*$ by compos. with surj $J/K^* \to I(c)/P_c^+$ (64).
E.g. if $K = \mathbb{Q}$, $c = m\mathbb{Z} \Rightarrow I(c)/P_c^+ = (\mathbb{Z}/m\mathbb{Z})^*$, so Dirichlet char $\in \widehat{(\mathbb{Z}/m\mathbb{Z})}$ give in partic. Grossench. [explicitly $\tilde{\chi}_p(up^i) = \chi(p)^i$ for $p \nmid m$, $u \in \mathbb{Z}_p^*$; for $p \mid m$, however, definition of $\tilde{\chi}$ goes through iso $J/\mathbb{Q}^* \simeq J_{m\mathbb{Z}} / J_{m\mathbb{Z}} \cap \mathbb{Q}^*$. For ∞, clearly $\tilde{\chi}_\infty = 1$]

2) The map $\chi : I(\mathbb{Z}[\omega]) \to \mathbb{C}^*$ at the end of (13) comes from a Grossenchar. (∇) [$\chi : J \to \mathbb{C}^*$ defined by $\chi_\pi(u\pi^i) = \begin{cases} -\pi & \text{if } \pi \in \mathbb{Z}[\omega] \text{ prime} \equiv 2\ (3) \\ \pi & \text{if } \pi \in \mathbb{Z}[\omega] \text{ primary prime} \equiv 1\ (3) \end{cases}$
but for the other places $(1-\omega)$ & ∞ not obvious!]. Note χ not of finite order & $\chi_\infty \ne 1$

(∇) won't check it here.

(*) Of course χ may be recaptured from χ_v by $\chi(x) = \prod_v \chi_v(x_v)$.

(+) so $c(\chi) \leftrightarrow$ minimum S s.t. χ trivial on J_S. / (++) of fin. order

(+++) sometimes say this associated χ comes from a Grossenchar.