CM of elliptic curves. (Assume · Sil. vol. 1 & facts about orders)

Outline:

I. Elliptic curves / $\mathbb{C}$ & rationality

II. Potentially good reduction & integrality of j.

III. Main thm. of CM & consequences (Grössencharakter, L-function)

IV. Ring class fields & abelian extensions

WARNING/ACHTUNG/ATTENTION:

- unedited notes. use at your own risk

Refs: Shimura, Lang, Silverman, Gross, Serre ...

I Elliptic curves / $\mathbb{C}$ & rationality.

Recall that an elliptic curve $E/\mathbb{C}$ has $\mathrm{End}(E) \cong \mathbb{Z}$ or an order $\mathcal{O}$ in a quadratic imaginary field K.

In the latter case, we say E has CM by K (or by $\mathcal{O}$)

If we have an isomorphism $\mathrm{End}\, E \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$, this determines an embedding $i : K \hookrightarrow \mathbb{C}$ s.t.

s.t.

$$\begin{tikzcd} \mathrm{End}\, E \otimes_{\mathbb{Z}} \mathbb{Q} \arrow[r, hook, "\text{canon.}"] \arrow[d, phantom, "\cong" rotate=90] & \mathrm{End}\, T_0 E \arrow[d, phantom, "\cong\ \text{canon.}"] \\ K \arrow[r, hook, "i"'] & \mathbb{C} \end{tikzcd}$$

commutes. (fix this once & for all)

Recall that every order $\mathcal{O} \subseteq \mathcal{O}_K$ is of the form $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ (count index)

Let $\mathrm{Cl}(\mathcal{O}) = \{\text{rk. 1 projective } \mathcal{O}\text{-modules}\}/_{\cong}$. This forms a group under $\otimes$.

Let $\mathrm{Ell}(\mathcal{O}) = \{\text{ell. curves } /\mathbb{C} \text{ w/ CM by } \mathcal{O}\}/_{\mathbb{C}-\cong}$.

Recall that every elt. of $\mathrm{Cl}(\mathcal{O})$ can be represented by an ideal $\mathfrak{a} \subseteq \mathcal{O}$ and that if Λ, Λ' are two projective $\mathcal{O}$-submodules of K, then $\Lambda \otimes_{\mathcal{O}} \Lambda' \cong \Lambda\Lambda'$. $\therefore$ $\mathfrak{a}^{-1} \cong \{\alpha \in K \mid \alpha\mathfrak{a} \subseteq \mathcal{O}\}$

Thm: There is a simply transitive action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$ s.t. $[\mathfrak{a}] \cdot [\mathbb{C}/\Lambda] = [\mathbb{C}/\mathfrak{a}^{-1}\Lambda]$.

Pf: Note that $\mathfrak{a}^{-1}\Lambda \subseteq \mathbb{C}$ is a lattice (it's a discrete sbgp. of $\mathbb{C}$ w/ $\mathbb{Z}$-rank ≥ 2)

To show this action is well-defined, we need to show that if $\mathbb{C}/\Lambda$ has CM by $\mathcal{O}$,

1) $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ has CM by $\mathcal{O}$

2) $\mathbb{C}/\mathfrak{a}^{-1}\Lambda \cong \mathbb{C}/(\mathfrak{a}')^{-1}\Lambda \iff \mathfrak{a} \cong \mathfrak{a}'$ as $\mathcal{O}$-modules

(note: If $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$, then clearly $\mathbb{C}/\mathfrak{a}^{-1}\Lambda \cong \mathbb{C}/\mathfrak{a}^{-1}\Lambda'$, as Λ & Λ' are homothetic)

Pf of 1): $\mathrm{End}(\mathbb{C}/\Lambda) \underset{\uparrow}{=} \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\} \underset{\uparrow}{=} \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a}^{-1}\Lambda \subseteq \mathfrak{a}^{-1}\Lambda\} = \mathrm{End}(\mathbb{C}/\mathfrak{a}^{-1}\Lambda)$

([AEC] VI 5.3)

since $\mathfrak{a}^{-1} \otimes \mathfrak{a} \cong \mathfrak{a}^{-1}\mathfrak{a}$
& we assume $\mathrm{End}\, \mathbb{C}/\Lambda = \mathcal{O}$,
so that $\mathcal{O}\Lambda \subseteq \Lambda$.

Pf of 2): $\mathbb{C}/\mathfrak{a}^{-1}\Lambda \cong \mathbb{C}/(\mathfrak{a}')^{-1}\Lambda \underset{\substack{\uparrow \\ ([\text{AEC}]\ \text{VI}.4.1.1)}}{\Leftrightarrow} \exists\, c \in \mathbb{C}^\times$ s.t. $\mathfrak{a}^{-1}\Lambda = c(\mathfrak{a}')^{-1}\Lambda \underset{\substack{\uparrow \\ \text{again use } \mathfrak{a}^{-1}\otimes\mathfrak{a}\cong\mathfrak{a}^{-1}\mathfrak{a} \\ \text{and } \mathcal{O}\Lambda\subseteq\Lambda}}{\Leftrightarrow} \Lambda = c\,\mathfrak{a}^{-1}\mathfrak{a}'\Lambda = c^{-1}\mathfrak{a}(\mathfrak{a}')^{-1}\Lambda$

This happens $\Leftrightarrow c\,\mathfrak{a}^{-1}\mathfrak{a}',\ c^{-1}\mathfrak{a}(\mathfrak{a}')^{-1} \subseteq \mathcal{O}$ (cf. first equality in pf. of 1)),

which is equivalent to $c \in K$ (since $\mathfrak{a}^{-1}\mathfrak{a}' \subseteq K$) and $\mathfrak{a} = c\,\mathfrak{a}' \Leftrightarrow \mathfrak{a} \cong \mathfrak{a}'$ as $\mathcal{O}$-modules
(in equiv of divisors)

Now we must show the action is simply transitive.

Actually, 2) above shows the action is faithful.

Transitivity:

Any lattice $\Lambda \subseteq \mathbb{C}$ is homothetic to a lattice contained in K if $\mathbb{C}/\Lambda$ has CM by $\mathcal{O}$.
(divide by any nonzero $\lambda \in \Lambda$; then $\mathcal{O}\Lambda \subseteq \Lambda \Rightarrow \mathcal{O} \subseteq$ & they have the same $\mathbb{Z}$-rank)

"gap" { Note that $\operatorname{End}_{\mathcal{O}}\Lambda = \mathcal{O}$ since E has CM by $\mathcal{O}$.
Thus by Shimura, Prop. 4.11, Λ is a projective $\mathcal{O}$-module, so that given any $\mathbb{C}/\Lambda'$, we have $\mathbb{C}/\Lambda' \cong \mathbb{C}/(\Lambda'\Lambda^{-1})\Lambda$. □

<u>Cor</u>: Every ell. curve $E \in \mathrm{Ell}(\mathcal{O})$ has a model over a # fld.

<u>Pf</u>. If $\sigma \in \operatorname{Aut}(\mathbb{C})$ and E has CM by $\mathcal{O}$, then so does E^σ.

But there are only finitely many $\mathbb{C}$-isom classes of ell. curves, so $\{ j(E^\sigma) : \sigma \in \operatorname{Aut}\mathbb{C} \}$ is finite. (recall: $j(E^\sigma) = j(E)^\sigma$)

Thus $j(E) \in \overline{\mathbb{Q}}$. □

<u>Cor</u>: $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq \#\mathrm{Cl}(\mathcal{O})$ if $E \in \mathrm{Ell}(\mathcal{O})$

<u>Pf</u>. $\{j(E^\sigma)\} \hookrightarrow \mathrm{Ell}(\mathcal{O})$ & $\mathrm{Ell}(\mathcal{O})$ is a PHS for $\mathrm{Cl}(\mathcal{O})$ □

rationality of endomorphisms:

<u>Prop</u>: If $E \in \mathrm{Ell}(\mathcal{O})$, $\sigma \in \operatorname{Aut}(\mathbb{C})$, & $\alpha \in \mathcal{O}$, then

$$\begin{tikzcd} x \arrow[d, mapsto] & E(\mathbb{C}) \arrow[r, "{[\alpha]}"] \arrow[d] & E(\mathbb{C}) \arrow[d] & x \arrow[d, mapsto] \\ x^\sigma & E^\sigma(\mathbb{C}) \arrow[r, "{[\alpha^\sigma]}"'] & E^\sigma(\mathbb{C}) & x^\sigma \end{tikzcd}$$

commutes

i.e $[\alpha^\sigma] = [\alpha]^\sigma$. (Here $[\alpha]$ denotes the image of α under $\mathcal{O} \cong \operatorname{End} E$)

Pf: We want to show that the diagram

$$\begin{tikzcd}
\phi \arrow[d, mapsto] & \mathrm{End}(E) \arrow[r, hook] \arrow[d] & \mathrm{End}\, T_0 E \cong \mathbb{C} \arrow[d] & c \arrow[d, mapsto] \\
\phi^c & \mathrm{End}(E) \arrow[r, hook] & \mathrm{End}\, T_0 E \cong \mathbb{C} & c^\sigma
\end{tikzcd}$$

commutes.

But $([\alpha]^\sigma)^* \omega^\sigma = ([\alpha]^* \omega)^\sigma = (\alpha\omega)^\sigma = \alpha^\sigma \omega^\sigma = [\alpha^\sigma]^* \omega^\sigma$. ☐

Cor: If E/L has CM by $\mathcal{O}$, then every elt. of End E is defined over KL.

Pf: Klar! ☐

We proved that $\mathrm{Ell}(\mathcal{O})$ is a PHS for $\mathrm{Cl}(\mathcal{O})$. It is also a $\mathrm{Gal}(\bar{K}/K)$-set

CFT ⟹ ∃ surjection $r: \mathrm{Gal}(\bar{K}/K) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}) : \mathrm{Frob}_p \mapsto p \cap \mathcal{O}$ for $p \nmid$ cond $\mathcal{O}$ a prime of K. Hmm...

Thm: If $\sigma \in \mathrm{Gal}(\bar{K}/K)$, then $j(E)^\sigma = j(r(\sigma)\, E)$

Pf This will follow from the Main Thm. of CM ☐

II. Potentially good reduction & integrality of j.

We'll use the following:

Prop: If E/L ($L = \#$fld) has CM by K, then for $F = KL$, for any ℓ the representations $\rho_\ell : \mathrm{Gal}(\bar{F}/F) \to \mathrm{Aut}\, T_\ell E$ have abelian image.

Pf: Every endomorphism of E is defined over $F = KL$.

It will suffice to show that the representations $\mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{Aut}\, E[\ell^n]$ are abelian

By prev thm., $\mathrm{Gal}(\bar{F}/F)$-action commutes w/ $\mathcal{O}$-action on $E[\ell^n]$,

So really we have $\mathrm{Gal}(\bar{F}/F) \to \mathrm{Aut}_{\mathcal{O}} E[\ell^n]$

∴ suff. to show $E[\ell^n]$ is a projective $\mathcal{O}/(\ell^n)$-mod. of rk. 1, since then

$$\mathrm{Aut}_{\mathcal{O}} E[\ell^n] \cong \mathrm{Aut}_{\mathcal{O}/(\ell^n)} E[\ell^n] \underset{\uparrow}{\cong} (\mathcal{O}/(\ell^n))^\times \text{ is abelian}$$

$(\mathrm{Hom}_{\mathcal{O}/\ell^n}(E[\ell^n], \mathcal{O}/\ell^n) \otimes_{\mathcal{O}/\ell^n} E[\ell^n] \cong \mathrm{End}_{\mathcal{O}/\ell^n} E[\ell^n]$ check locally $)$

CMEC 4.

We can write $E \cong \mathbb{C}/\Lambda$ for $\Lambda \subseteq K$ an $\mathcal{O}$-module.

In fact, Λ is a projective $\mathcal{O}$-mod. of rank 1 (we proved this when we proved the fact that $\mathrm{Ell}(\mathcal{O})$ is a $\mathrm{Cl}(\mathcal{O})$-PHS). Thus $\Lambda/\ell^n\Lambda \cong \ell^{-n}\Lambda/\Lambda \cong$ $\cong E[\ell^n]$ is a proj. $\mathcal{O}/(\ell^n)$-module of rank 1. □.

Rmk: We could have waited to deduce this prop. from the Main Thm. of CM.

Thm: Let E/L ($L = \#$ fld.) have CM by K. Then E has everywhere potentially good reduction.

Pf: Prev prop. $\Rightarrow$ may replace L by a fin extn. & assume WLOG that $T_\ell E$ is an abelian $\mathrm{Gal}(\bar{L}/L)$-mod. $\forall \ell$.

Let v be a place of L and choose ℓ with $v | p \neq \ell$

To prove E has potentially good redn. at v, it will suffice to show (by the criterion of Néron-Ogg-Shafarevich) that inertia at v acts on $T_\ell E$ through a finite quotient.

Since $T_\ell E$ is abelian, we have a homom.
$$\begin{tikzcd} I_v^{ab} \arrow[r] \arrow[d, phantom, "\wr\|"' , "\text{CFT}"] & \mathrm{Aut}\, T_\ell E \arrow[d, phantom, "\wr\|"] \\ \mathcal{O}_{L_v}^\times & GL_2(\mathbb{Z}_\ell) \end{tikzcd}$$
(here I_v^{ab} is the image of I_v in $\mathrm{Gal}(\bar{L}/L)$)

But $\mathcal{O}_{L_v}^\times$ is an extension of a finite group by a pro-p gp &

$GL_2(\mathbb{Z}_\ell)$ is an extension of a finite group by a pro-ℓ gp. The rest is easy. □

Cor: If E has CM by $\mathcal{O}$, then $j(E) \in \mathcal{O}_{\bar{\mathbb{Q}}}$

Pf: [AEC] VII.5.5. □.

III. Main Thm. of CM & consequences. (Grössencharakter, L-function)

Preliminaries.

Let $\Lambda \subseteq K$ be a rk. 2 $\mathbb{Z}$-module (lattice). Then $\Lambda_p := \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p \subseteq K_p = K \otimes_{\mathbb{Z}} \mathbb{Q}_p$ is a $\mathbb{Z}_p$-lattice.

Exercise: Given a $\mathbb{Z}_p$-lattice $M_p \subseteq K_p$ $\forall p$ s.t $M_p = \mathcal{O}_{K,p}$ for a.a. p,

$\exists !$ lattice $\Lambda \subseteq K$ s.t. $\Lambda_p = M_p$ $\forall p$

Hint: $\Lambda = \bigcap_p (M_p \cap K)$ $\square$

Now given any idèle $s = (s_p) \in \mathbb{A}_K^\times$ with $s_p \in K_p$ and any lattice $\Lambda \subseteq K$, we can define by the exercise a lattice $s\Lambda$ by requiring $(s\Lambda)_p = s_p \Lambda_p$.

Moreover, we have $K/\Lambda \cong \bigoplus_p K_p/\Lambda_p$, so we can define "multiplication by s"

$K/\Lambda \underset{\cong}{\xrightarrow{\cdot s}} K/s\Lambda$ to be the sum of the maps $K_p/\Lambda_p \underset{\cong}{\xrightarrow{\cdot s_p}} K_p/s_p\Lambda_p$.

Thm: (Main Thm. of CM for ell. curves) Suppose $E/\mathbb{C}$ has CM by K. Choose $\Lambda \subseteq K$ such that $\xi : \mathbb{C}/\Lambda \to E$. Choose $\sigma \in \operatorname{Aut} \mathbb{C}$ and $s \in \mathbb{A}_K^\times$ s.t. $\sigma|_{K^{ab}} = [s, K]$. Then $\exists$ isom ξ' filling in the commutative diagram of isomorphisms

$$\begin{tikzcd}
K/\Lambda \arrow[r, "\xi"] \arrow[d, "s^{-1}"'] & E(\mathbb{C})_{tors} \arrow[d] & x \arrow[d, mapsto] \\
K/s^{-1}\Lambda \arrow[r, dashed, "\xi'"'] & E^\sigma(\mathbb{C})_{tors} & x^\sigma
\end{tikzcd}$$

Pf: Will be proved for ab. vars. ... eventually $\square$

We can get first of all the Grössencharakter.

Thm: Let $L \supseteq K$ be a # fld. & E/L an ell. curve w/ CM by K. Then there is a unique character $\alpha_E : \mathbb{A}_L^\times \to K^\times$ s.t if $x \in \mathbb{A}_L^\times$ and $s = N_{L/K} x$, then $\alpha(x)$ is unique s.t.

(a) $\alpha(x) \cdot \mathcal{O} = s\mathcal{O}$

(b) if $\Lambda \subseteq K$ is a projective $\mathcal{O}$-module & $\xi : \mathbb{C}/\Lambda \xrightarrow{\cong} E(\mathbb{C})$, then

$$\begin{tikzcd}
K/\Lambda \arrow[r, "\alpha(x)s^{-1}"] \arrow[d, "\xi"'] & K/\Lambda \arrow[d, "\xi"] \\
E(L^{ab}) \arrow[r, "{[x, L]}"'] & E(L^{ab})
\end{tikzcd}$$

Rmk: we showed earlier that $E(\mathbb{C})_{tors} \subseteq E(L^{ab})$

Pf: Let $\sigma \in \operatorname{Aut} \mathbb{C}$ s.t. $\sigma|_{L^{ab}} = (x, L)$, so $\sigma|_{K^{ab}} = (s, K)$

$\therefore$ MTCM $\Rightarrow$ $\exists\, \xi' : \mathbb{C}/s^{-1}\Lambda \xrightarrow{\cong} E(\mathbb{C})$ s.t.

$$\begin{tikzcd}
K/\Lambda \arrow[r, "s^{-1}"] \arrow[d, "\xi"'] & K/s^{-1}\Lambda \arrow[d, "\xi'"] \\
E(\mathbb{C}) \arrow[r, "\sigma"'] & E^{\sigma}(\mathbb{C}) = E(\mathbb{C})
\end{tikzcd}$$

commutes

Since $E^{\sigma}(\mathbb{C}) \cong E(\mathbb{C})$, $s^{-1}\Lambda$ & Λ are homothetic, so $\exists\, b = b(x) \in K^{\times}$

s.t. $b \cdot s^{-1}\Lambda = \Lambda$.

We get

$$\begin{tikzcd}
K/\Lambda \arrow[r, "bs^{-1}"] \arrow[d, "\xi"'] & K/\Lambda \arrow[d, "\xi''"] \\
E(\mathbb{C}) \arrow[r, "\sigma"'] & E(\mathbb{C})
\end{tikzcd}$$

commutes for appropriate ξ''.

Let $\alpha(x)$ be the element of $K^{\times}$ corresponding to $\xi'' \xi^{-1}[b] \in (\operatorname{End} E) \otimes \mathbb{Q}$

Then the above diagram gives the commuting diagram

$$\begin{tikzcd}
K/\Lambda \arrow[r, "\alpha(x)s^{-1}"] \arrow[d, "\xi"'] & K/\Lambda \arrow[d, "\xi"] \\
E(L^{ab}) \arrow[r, "{(x,L)}"'] & E(L^{ab})
\end{tikzcd}$$

(since $\xi'' \circ b = [\alpha]\xi$)

Note that we must have $\alpha(x)\, s^{-1}\Lambda = \Lambda$ $\Rightarrow$ $\alpha(x)\mathcal{O} = s\mathcal{O}$.

$\alpha(x)$ is clearly unique $\in K^{\times}$ satisfying (b).

Also, it's straightforward to check that $\alpha(x)$ is indep. of Λ & ξ.

Moreover α is clearly a homom. by (b) & uniqueness. $\square$

This a is not the Grössencharakter, but will give rise to it.

Thm: $\alpha_E : \mathbb{A}_L^{\times} \to K^{\times}$ is the unique character s.t.

(a) $\ker \alpha$ is open

(b) $\alpha|_{L^{\times}} = N_{L/K}$

(c) α is unramified at $v \Leftrightarrow E$ has good redn. at v.

(d) If v is a good prime of E/L, then $[\alpha(\pi_v)]$ (which makes sense by (a) of prev. thm.) reduces to the Frobenius endom. ϕ_v at v.

Pf: (a)(b)(d) determine α uniquely

(b) is immediate from uniqueness of $\alpha(k)$, $k \in L^\times$

(a): It suffices to show $\ker \alpha$ contains an open subgroup.

We already showed $L(E[m])/L$ is a finite abelian extension, so CFT $\Rightarrow$

$\exists$ open $B_m \subseteq \mathbb{A}_L^\times$ s.t. $\mathbb{A}_L^\times / B_m \xrightarrow[\cong]{\text{rec}} \mathrm{Gal}(L(E[m])/L)$.

Set $U_m = \{ x \in B_m \mid (N_{L/K} x)_p \in (1 + m\mathcal{O}_p) \cap \mathcal{O}_p^\times \text{ for all } p \in \mathbb{Z} \text{ prime} \} \subseteq \mathbb{A}_L^\times$

Note that this is open since $(1+m\mathcal{O}_p) \cap \mathcal{O}_p^\times = \mathcal{O}_{K,p}^\times$ for a.a. p and in general $\mathcal{O}_p^\times$ has finite index in $\mathcal{O}_{K,p}^\times$ (use the exponential map). We'll show $\alpha|_{U_m} = 1$ (for suitable m)

Now choose $\xi : \mathbb{C}/\Lambda \xrightarrow{\cong} E(\mathbb{C})$, so that $m^{-1}\Lambda/\Lambda \cong E[m]$.

For any $t \in m^{-1}\Lambda/\Lambda$ and $x \in U_m$, we have by prev. thm.:

$$\xi(t) \underset{\uparrow}{=} \xi(t)^{[x,L]} = \xi(\alpha(x) N_{L/K} x^{-1} t) \underset{\uparrow}{=} \xi(\alpha(x) t)$$

since $x \in B_m$
so $[x,L]$ fixes $E[m]$

since $(N_{L/K} x)_p \equiv 1 \bmod m\mathcal{O}_p$
so acts as 1 on $t_p \in m^{-1}\Lambda_p/\Lambda_p$

$\therefore \alpha(x) \cdot (m^{-1}\Lambda/\Lambda) \subseteq m^{-1}\Lambda/\Lambda \Rightarrow (\alpha(x)-1)m^{-1}\Lambda \subseteq \Lambda \Rightarrow (\alpha(x)-1)\mathcal{O} \subseteq m\mathcal{O}$,

i.e. $\alpha(x) \in \mathcal{O}$ & $\alpha(x) \equiv 1 \bmod m\mathcal{O}$.

But prev. thm. $\Rightarrow \alpha(x)_p \mathcal{O}_p = (N_{L/K} x)_p \mathcal{O}_p = \mathcal{O}_p \ \forall p$, so $\alpha(x)\mathcal{O} = \mathcal{O}$, i.e. $\alpha(x) \in \mathcal{O}^\times$

Thus for appropriate choice of m, we get $\alpha(x) = 1$ ($\mathcal{O}^\times \subseteq \mathcal{O}_K^\times$ is finite)

(c): Let v be a prime of L. Choose $m \in \mathbb{Z}$ prime to v and $\xi : \mathbb{C}/\Lambda \to E(\mathbb{C})$

E has good reduction at $v \Leftrightarrow$ the inertia gp. I_v acts trivially on $E[m^n]$ for all n.

recall I_v acts through its quotient $I_v^{ab} \subseteq \mathrm{Gal}(L^{ab}/L)$.

$\therefore$ E has good redn. at v $\Leftrightarrow \overset{(\forall n \in \mathbb{Z}_+)}{\vee}\ \xi(t)^{\sigma} = \xi(t)\ \ \forall \sigma \in I_v^{ab}$ & $t \in m^{-n}\Lambda/\Lambda$

$$\Leftrightarrow \underset{\displaystyle \xi(\alpha(x) N_{L/K}x^{-1} t)}{\underset{\parallel}{\xi(t)^{[x,L]}}} = \xi(t) \quad \forall x \in \mathcal{O}_{L_v}^{\times} \subseteq \mathbb{A}_L^{\times} \ \ \& \ \ t \in m^{-n}\Lambda/\Lambda .$$

(*) Now we claim that $N_{L/K}x^{-1}$ acts trivially on $m^{-n}\Lambda/\Lambda$ for all n:

Since $\mathcal{O}_p \neq \mathcal{O}_{K,p}$ for only finitely many p and $\mathcal{O}_p^{\times} \subseteq \mathcal{O}_{K,p}^{\times}$ always has finite index, $\exists k$ s.t. $m^{-kn} \in \mathcal{O}_p^{\times}$ $\forall n$ & $p \nmid m$, so $m^{-kn}\Lambda_p/\Lambda_p = m^{-n}\Lambda_p/\Lambda_p = 0$

Thus $m^{-n}\Lambda/\Lambda \cong \bigoplus_{p|m} m^{-n}\Lambda_p/\Lambda_p$. But for $p \mid m$, $(N_{L/K}x^{-1})_p = 1$. QED

Hence we have: E has good redn. at v $\Leftrightarrow \xi(\alpha(x)t) = \xi(t)\ \forall x \in \mathcal{O}_{L_v}^{\times} \subseteq \mathbb{A}_L^{\times}$ & $t \in m^{-n}\Lambda/\Lambda$.

$\Leftrightarrow \alpha(x) \equiv 1 \bmod m^{kn}\mathcal{O}\ \ \forall x \in \mathcal{O}_{L_v}^{\times} \Leftrightarrow \alpha(x) = 1\ \ \forall x \in \mathcal{O}_{L_v}^{\times}$,

i.e., α is unram. at v.

(d): Let v be a good prime for E/L and again choose m prime to v & $\xi : \mathbb{C}/\Lambda \xrightarrow{\cong} E(\mathbb{C})$

Claim (*) above shows that $\underset{(\forall n)}{\wedge}$ $\xi(t)^{\overset{\text{Frob}_v}{\uparrow}} = \xi(\alpha(\pi_v)t) = [\alpha(\pi_v)]\xi(t)\ \ \forall t \in m^{-n}\Lambda/\Lambda$

$\text{Frob}_v = [\pi_v, L]$

Denote by $\tilde{E}/k(v)$ the reduction of E at v, and let $\underset{x \mapsto \tilde{x}}{E(L^{ab}) \xrightarrow{\overset{\text{map of } D_v\text{-mods.}}{\downarrow}} \tilde{E}(\overline{k(v)})}$ be

the reduction map. Then $\widetilde{\xi(t)^{\text{Frob}_v}} = \phi_v(\widetilde{\xi(t)})$.

Also denote the (injective) map $\text{End}\, E \hookrightarrow \text{End}\, \tilde{E} : \phi \mapsto \tilde{\phi}$. This satisfies $\widetilde{\phi(x)} = \tilde{\phi}(\tilde{x})$.

$\nwarrow$(comes from Néron mapping property; injective because

$$\begin{tikzcd} \text{End}\, E \arrow[r, hook] \arrow[d] & \text{End}\, T_\ell E \arrow[d, equal] \\ \text{End}\, \tilde{E} \arrow[r, hook, "?"] & \text{End}\, T_\ell \tilde{E} \end{tikzcd}$$

for $v \nmid \ell$)

Hence $\phi_v(\widetilde{\xi(t)}) = \widetilde{[\alpha(\pi_v)]}(\widetilde{\xi(t)})\ \ \forall t \in m^{-n}\Lambda/\Lambda$, so done (since

$\text{End}\, \tilde{E} \hookrightarrow \text{End}\, T_\ell \tilde{E}$ for $v \nmid \ell$)

$\square$

We can now (finally!) talk about the Grössencharakter & L-function ...

For any place (possibly infinite) p of $\mathbb{Q}$ and number field L, set $L_v = L \otimes_{\mathbb{Q}} \mathbb{Q}_p$

If $L \supseteq K$, define the local norm $\mathbb{N}_p : L_p \to K_p$.

Now suppose E/L has CM by K and that $L \overset{?}{\supseteq} K$. Let $\alpha = \alpha_E$.

Define
$$\chi_p = \chi_{E,p} : \mathbb{A}_L^\times \to K_p^\times$$
$$x \mapsto \alpha(x) \cdot \mathbb{N}_p(x_p)^{-1}$$

Then by (a) & (b) of the prev. thm., χ_p is a continuous idèle class character.

If p is finite, $K_p^\times$ is totally disconnected, so χ_p is trivial on $(\mathbb{A}_L^\times / L^\times)^\circ$, so

CFT $\Rightarrow$ we can view χ_p as a $K_p^\times$-valued character of $\mathrm{Gal}(L^{ab}/L)$

Recall that T_pE is a $\underset{\text{(generic)}}{{}_\wedge}$ rank 1 $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$-module, so we can view $\rho_p : \mathrm{Gal}(\bar{L}/L) \to \underset{\overset{\cong}{\mathrm{Aut}(T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)}}{K_p^\times}$.

<u>Thm</u>: $\chi_p = \rho_p$

<u>Pf</u>: We only need to check this on Frob_v for $v \nmid p$ a good prime of E.

This is just (d) of the prev. thm. (note: $\alpha|_{\mathcal{O}_{L_v}^\times} = \chi_p|_{\mathcal{O}_{L_v}^\times}$). □

For $p = \infty$, we get $\chi_\infty : \mathbb{A}_L^\times / L^\times \to (K \otimes \mathbb{R})^\times = \mathbb{C}$. This is a Grössen charakter.

It is clear that χ_E has type $(1,0)$ w.r.t. $i : K \hookrightarrow \mathbb{C}$ (the embedding from the beginning)

Some general nonsense about L-functions:

All Grössen charaktere $\psi : \mathbb{A}_L^\times \to \mathbb{C}^\times$ have an L-function $L(\psi, s) = \prod_{v \in S} (1 - \psi(\pi_v) \underset{\overset{\uparrow}{(q_v = \# k(v))}}{q_v^{-s}})^{-1}$,

where S = set of finite places of L where ψ is unramified

We can also define an L-function for an elliptic curve E over a # fld L:

$$L(E/L, s) = \prod_{\substack{v \text{ finite} \\ \text{place of } L}} L_v(E/L, q_v^{-s})^{-1}, \text{ where}$$

$$L_v(E/L, T) := \det(1 - \phi_v T \mid T_\ell E^{I_v}) = \begin{cases} \det \phi_v T^2 - \mathrm{tr}\,\phi_v T + 1 & E \text{ good at } v \\ 1 - T & E \text{ split mult at } v \\ 1 + T & E \text{ non-split mult.} \\ 1 & E \text{ additive at } v \end{cases} \in \mathbb{Z}[T]$$

Thm: Let E/L have CM by K

(a) If $L \supseteq K$, then $L(E/L, s) = L(\chi_E, s) L(\bar{\chi}_E, s)$

(b) If $L \not\supseteq K$, then $L(E/L, s) = L(\chi_E, s)$ (where χ_E is the Grössencharakter of KL associated to E/KL).

Pf: (a): Since E has potentially good reduction at all v, its reduction is everywhere either good or additive. Since χ_E & $\bar{\chi}_E$ are unramified at $v \Leftrightarrow E$ has good reduction at v, need to prove (for v good prime for E)

$$\left.\begin{array}{l} \text{(i) } \operatorname{tr} \phi_v = \chi_E(\pi_v) + \overline{\chi_E(\pi_v)} \\ \text{(ii) } \det \phi_v = \chi_E(\pi_v) \overline{\chi_E(\pi_v)} \end{array}\right\} \begin{array}{l} (\operatorname{tr}\phi_v \text{ \& } \det \phi_v \text{ can be calculated on } T_\ell E \\ \quad \text{for any } v \nmid \ell) \end{array}$$

(i): follows from the fact that $\chi_\ell = \rho_\ell$ (pick ℓ = split in K, e.g.)

(ii): can proceed as in (i), or note that $\chi_E \bar{\chi}_E = \mathbb{N}$ since χ_E has type $(1,0)$, then use that $\det \phi_v = \deg \phi_v = q_v = \mathbb{N}(\pi_v)$.

(b): this will be more work. Set $F = KL$ and let σ be the nontrivial elt. of $\mathrm{Gal}(F/L)$

Claim: if a prime v of L is ramified in F, then E has bad reduction at $w|v$.

Pf: $\exists \alpha \in \mathcal{O}$ s.t $\alpha^\sigma = \alpha$, so that $[\alpha]^\sigma \neq [\alpha]$.

If the reduction $\tilde{E}$ of E at w is good, we get an injection (as before) $\operatorname{End} E \hookrightarrow \operatorname{End} \tilde{E}$. But since v is ramified, we have that $k(w) = k(v)$ and σ fixes w; thus it must be that $\widetilde{[\alpha]}^\sigma = \widetilde{[\alpha]}$ $\Rightarrow\Leftarrow$.

Thus if v is ramified in F with $w|v$, E has additive reduction at v, so that $L_v(E/L, T) = 1$. E also has bad reduction at w, so χ_E is ramified at w.

$\therefore$ only need to worry about Euler factors at primes unramified in F.

Also note that if v is unramified in F and $w|v$, then E is unramified at $v \Leftrightarrow E_F$ is unramified at w (unram. base change doesn't change reduction type), so we only need consider Euler factors at good primes v.

Claim: if w, w' are the primes of F over v (possibly w = w'), then

$$\chi_E(\pi_w^\sigma) = \chi_E(\pi_{w'}) \overset{\downarrow}{\underset{\uparrow}{=}} \chi_E(\pi_w)^\sigma = \overline{\chi_E(\pi_w)}$$

Pf: $[\chi_E(\pi_{w'})]$ is the unique endomorphism of E reducing to the Frobenius endomorphism $\phi_{w'}$ at w'. So is $[\chi_E(\pi_w)^\sigma] = [\chi_E(\pi_w)]^\sigma$ QED.

(Rmk. thus in fact $\overline{\chi_E} = \chi_E \circ \sigma$.)

Thus if v is split, we have $\mathrm{tr}\,\phi_v = \mathrm{tr}\,\phi_w = \mathrm{tr}\,\phi_{w'} = \chi_E(\pi_w) + \overline{\chi_E(\pi_w)} =$

$= \chi_E(\pi_w) + \chi_E(\pi_{w'})$ and $\det \phi_v = q_v = q_w = q_{w'} = \chi_E(\pi_w)\overline{\chi_E(\pi_w)} = \chi_E(\pi_w)\chi_E(\pi_{w'})$

$\therefore$ $L_v(E/L,T) = (1-\chi_E(\pi_w)T)(1-\chi_E(\pi_{w'})T)$ (if E has good redn at v)

If v is inert w/ w|v, then we have $\chi_E(\pi_w) = \overline{\chi_E(\pi_w)}$ so that

$[\chi_E(\pi_w)] \in \mathbb{Z} \subseteq \mathrm{End}\,E \Rightarrow \widetilde{[\chi_E(\pi_w)]} = \phi_w = \pm q_v \in \mathbb{Z} \subseteq \mathrm{End}\,\tilde{E}$.

Note that $\phi_v^2 = \phi_w = \pm q_v$. We claim that $\phi_w = -q_v$. If not, then we have $\phi_v \in \mathbb{Z}$ as well (otherwise $\mathbb{Q}[\phi_v, \hat{\phi}_v] \cong \mathbb{Q}(\sqrt{q_v})$ is real quadratic w/ non-trivial endomorphism $\phi_v \mapsto \hat{\phi}_v$, but $\phi_v\hat{\phi}_v = q_v$ ⇒⇐). As before, let $[\alpha] \neq [\alpha]^\sigma$ be an endomorphism of $E_{\mathbb{F}}$ not defined over L, so that $\widetilde{[\alpha]} \neq \widetilde{[\alpha]}^\sigma = \widetilde{[\alpha]}^{\mathrm{Frob}_v}$.

We also have that $\phi_v \widetilde{[\alpha]} = \widetilde{[\alpha]}^{\mathrm{Frob}_v} \phi_v$, but since $\phi_v \in \mathbb{Z}$, it commutes w/ every endomorphism, so that $\widetilde{[\alpha]} = \widetilde{[\alpha]}^{\mathrm{Frob}_v}$ ⇒⇐. Thus $\phi_w = -q_v$.

Hence ϕ_v satisfies $X^2 + q_v$, which therefore must be its characteristic polynomial (∵ since the char poly has conjugate roots: $\det(\frac{m}{n} - \phi_v) =$

$= \frac{1}{n^2}\deg(m - n\phi_v) \geq 0 \ \forall \frac{m}{n} \in \mathbb{Q}$)

In particular, $\det \phi_v = q_v = -\chi_E(\pi_v)$ and $\mathrm{tr}\,\phi_v = 0$.

In conclusion, we have shown:

$$L_v(E/L,T) = \begin{cases} (1-\chi_E(\pi_w)T)(1-\chi_E(\pi_{w'})T) & \text{E good at } v = ww' \\ (1-\chi_E(\pi_w)T^2) & \text{E good at } v = w \text{ (inert)} \\ 1 & \text{E bad at } v. \end{cases}$$

So: $L(E/L,s) = \prod_v L_v(E/L, q_v^{-s}) = \prod_{w \nmid \mathrm{cond}\,\chi_E} (1-\chi_E(\pi_w)q_w^{-s}) = L(\chi_E, s)$ (note $q_v^2 = q_w$ if v inert)

□.

<u>Cor</u>: $L(E/L, s)$ has analytic continuation & functional equation of the form

$$\Lambda(E/L, s) = w(E)\Lambda(E/L, s), \quad w(E) = \pm 1$$

where $\Lambda(E/L, s)$ is a suitable "completed" L-function.

Pf: Follows from the thm. & properties of χ_E. □

<u>Rmk</u>: (1) Let E/L have CM by $K \notin L$. If $p \in \mathbb{Q}$ is split in K, the homomorphism

$\chi_p : \mathbb{A}_F^\times \to K_p^\times \cong \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times$ splits as a sum of two characters $\chi_p \cong \psi_p \oplus (\psi_p \circ \sigma)$ $(1 \neq \sigma \in \mathrm{Gal}(F/L))$.

Using the pf of the thm., one can show that in this case $\rho_p \cong \mathrm{Ind}_F^L \psi_p$.

(2) In the proof of the thm., we saw that when v is inert in F & good for E, we have $\mathrm{tr}\, \phi_v = 0$, so that E is supersingular at such primes.

(3) In general, if E/L has CM by K and good reduction at $\mathfrak{P} | p$, then E has supersingular reduction at $\mathfrak{P}$ if & only if p is either inert or ramified in K (see Lang, Ch. 13, §4, Thm. 12)

IV. Ring class fields & abelian extensions

In the prev. section, we showed how the Main Thm. of CM gives arithmetic info of E/L w/ CM by K in terms of the arithmetic of K (in particular its Grössen charaktere). In this section, we show how the Main Thm. of CM gives arithmetic info. about K in terms of the arithmetic of elliptic curves E/L w/ CM by K.

If E/L is an elliptic curve over $L = K(j(E))$, define the Weber function of E as the map $h = h_E : E \to E/\mathrm{Aut}\,E$ (defined over L). Note that $E/\mathrm{Aut}\,E \cong \mathbb{P}^1_L$.

If $E \cong E'$ (over $\mathbb{C}$), get canonical L-isom. $E/\mathrm{Aut}\,E = E'/\mathrm{Aut}\,E'$, i.e. "$h_E \eta = h_{E'}\ \forall \eta : E' \cong E$"

If E has Weierstrass equation $y^2 = 4x^2 - g_2 x - g_3$, the Weber function can be expressed as

$$h(x,y) = \begin{cases} (g_2 g_3/\Delta)x & j(E) \neq 0, 1728 \\ (g_2^2/\Delta)x^2 & j(E) = 1728 \\ (g_3/\Delta)x^3 & j(E) = 0 \end{cases} \qquad \text{(this gives a map } E \to \mathbb{P}^1_L\text{)}$$

<u>Thm</u>: Suppose E has CM by $\mathcal{O} \subseteq K$ and let $\xi : \mathbb{C}/\Lambda \xrightarrow{\cong} E(\mathbb{C})$ for $\Lambda \subseteq K$.

Let $u \in K/\Lambda$ and set

$$W = W(u) = \{ s \in \mathbb{A}_K^\times \mid s\Lambda = \Lambda \ \&\ su = u \} \quad \text{(does not depend on } \Lambda \subseteq K\text{)}$$

Then $K(j(E), h(\xi(u)))$ is the subfield of K^{ab} corresponding to $K^\times W \subseteq \mathbb{A}_K^\times$.

<u>Pf</u>: Note $W \supseteq K_\infty^\times$ and is open. Let $F \subseteq K^{ab}$ be the field with $\mathbb{A}_K^\times / K^\times W \xrightarrow{\cong} \mathrm{Gal}(F/K)$.

Choose any $\sigma \in \mathrm{Aut}\,\mathbb{C}$ fixing K & let $s \in \mathbb{A}_K^\times$ be s.t. $\sigma|_{K^{ab}} = [s, K]$

The Main Thm. of CM $\Rightarrow \exists\ \xi' : \mathbb{C}/s^{-1}\Lambda \to E^\sigma(\mathbb{C})$ s.t. ...

We need that $\sigma|_F = 1 \Leftrightarrow \sigma|_{K(j(E), h(\xi(u)))} = 1$

If $\sigma|_F = 1$, then $s \in W$, so $s^{-1}\Lambda = \Lambda$ & hence $j(E) \cong j(E)^\sigma$. Let $\varepsilon = \xi(\xi')^{-1} : E^\sigma \cong E$.

Then $h_E(\varepsilon(\xi(u)^\sigma)) \underset{\uparrow}{=} h_{E^\sigma}(\xi(u)^\sigma) = h_E(\xi(u))^\sigma$

since $h_E\varepsilon$ is the Weber function of E^σ

since h_E^σ is the Weber function of E^σ

But we have $\varepsilon(\xi(u)^\sigma) \underset{\substack{\uparrow \\ \text{def. of } \xi' \\ \text{from MTCM}}}{=} \varepsilon(\xi'(s^{-1}u)) \underset{\substack{\uparrow \\ \text{def. of } \varepsilon \text{ \& } \\ s \in W}}{=} \xi(u)$, so that $h_E(\xi(u)) = h_E(\xi(u))^\sigma$.

Thus $\sigma|_{K(j(E),\, h(\xi(u)))} = 1$.

Conversely, if $\sigma|_{K(j(E),\, h(\xi(u)))} = 1$, $j(E) = j(E)^\sigma$, so $\mathbb{C}/\Lambda \cong \mathbb{C}/s^{-1}\Lambda$

$\Rightarrow s^{-1}\Lambda \cong \Lambda$ as $\mathcal{O}$-mods. $\Rightarrow \exists\, \mu \in K^\times$ s.t. $\mu s^{-1}\Lambda = \Lambda$.

$\therefore$ can define $\delta : E^\sigma \to E$ s.t.

$$\begin{tikzcd} \mathbb{C}/s^{-1}\Lambda \arrow[r, "\xi'"] \arrow[d, "\mu"'] & E^\sigma(\mathbb{C}) \arrow[d, "\delta"] \\ \mathbb{C}/\Lambda \arrow[r, "\xi"'] & E(\mathbb{C}) \end{tikzcd}$$

Commutes

Again using properties of Weber functions, get that

$h_E(\delta(\xi(u)^\sigma)) = h_E(\xi(u))$, so $\delta(\xi(u)^\sigma)$ and $\xi(u)$ differ by an automorphism of E, say $\xi(u) = [\alpha]\, \delta(\xi(u)^\sigma)$

Now note that $\delta(\xi(u)^\sigma) = \delta(\xi'(s^{-1}u)) = \xi(\mu s^{-1}u)$ so $\xi(u) = \xi(\alpha\mu s^{-1}u)$,

so that $(\alpha\mu s^{-1})\Lambda = \Lambda$ and $(\alpha\mu s^{-1})u = u \Rightarrow (\alpha\mu s^{-1}) \in W \Rightarrow s \in K^\times W$.

$\Rightarrow \sigma|_F = \mathrm{id}$. $\square$.

Recall that $\mathrm{Ell}(\mathcal{O})$ has a simply transitive action of $\mathrm{Cl}(\mathcal{O})$ & an action of $\mathrm{Gal}(\bar{K}/K)$.

There is also a surjection: $r : \mathrm{Gal}(\bar{K}/K) \twoheadrightarrow \mathrm{Cl}(\mathcal{O})$.

$\mathrm{Frob}_\mathfrak{p} \mapsto \mathfrak{p} \cap \mathcal{O}$ (if $\mathfrak{p} \nmid \mathrm{cond}\, \mathcal{O}$)

<u>Cor</u>: (a) $K^{ab} = K(j(E), h_E(E_{\text{tors}}))$

(b) $j(E)^\sigma = j(r(\sigma)E)$ $\forall\, \sigma \in \mathrm{Gal}(\bar{K}/K)$. Also, $K(j(E))$ is the ring class field of K of conductor $c = \mathrm{cond}\, \mathcal{O}$. (If $\mathcal{O} = \mathcal{O}_K$, this is the Hilbert class field.)

(c) $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}] = \#\mathrm{Cl}(\mathcal{O})$

(d) If $\{\Lambda_i\}_{i=1}^{\#\mathrm{Cl}(\mathcal{O})}$ is a set of representatives for $\mathrm{Cl}(\mathcal{O})$, then $\{j(\Lambda_i)\}_{i=1}^{\#\mathrm{Cl}(\mathcal{O})}$ is a complete set of conjugates for $j(E)$ over $\mathbb{Q}$ (or K)

<u>Pf</u>: (a): check that $\bigcap_{u} K^\times W(u) = K^\times K_\infty^\times$.

Note that we already know $[K(j(E)):K] \leq [\mathbb{Q}(j(E)):\mathbb{Q}] \leq \# \mathrm{Cl}(\mathcal{O})$,

so clearly (b) $\Rightarrow$ (c) & (d)

(b): take $u=0$ in the prev thm., so $W(u) = K_\infty^\times \times \prod_p \mathcal{O}_p^\times$.

then the theory of ring class fields $\Rightarrow$ $K^\times W$ is the kernel

of $\mathbb{A}_K^\times \xrightarrow{\mathrm{rec}} \mathrm{Gal}(K^{ab}/K) \xrightarrow{r} \mathrm{Cl}(\mathcal{O})$, and also of $\mathbb{A}_K^\times \xrightarrow{\mathrm{rec}} \mathrm{Gal}(K(j(E))/K)$

We already know from the Main Thm. that $j(\Lambda)^{\mathrm{Frob}_\mathfrak{p}} = j(\Lambda)^{[\pi_\mathfrak{p}, K]} =$

$= j(\pi_\mathfrak{p}^{-1}\Lambda) = j((\mathfrak{p} \cap \mathcal{O})^{-1}\Lambda) = j(r(\mathrm{Frob}_\mathfrak{p}) \cdot \Lambda)$ $\forall\, \mathfrak{p} \nmid \mathrm{cond}\, \mathcal{O}$. $\square$.

<u>Cor</u>: If E has CM by $\mathcal{O}_K$ and $\mathfrak{a} \subseteq \mathcal{O}_K$ is an ideal, then $K(j(E), h(E[\mathfrak{a}]))$ is the ray class field of K of conductor $\mathfrak{a}$. (Here $E[\mathfrak{a}] = \{x \in E(\overline{L}) \mid [\alpha](x) = 0 \ \forall \alpha \in \mathfrak{a}\}$)

<u>Pf</u>: Check that $\bigcap_{u \in \mathfrak{a}^{-1}\Lambda/\Lambda} K^\times W(u) = K^\times \cdot U(\mathfrak{a})$, where $U(\mathfrak{a})$ is the subgroup

$\{s \in \mathbb{A}_K^\times \mid s_p \in \mathcal{O}_{K,p}^\times \ \& \ s_p \equiv 1 \ (\mathfrak{a}\mathcal{O}_{K,p}) \ \forall \text{ primes } p\} =: U(\mathfrak{a}) \subseteq \mathbb{A}_K^\times$ $\square$.