CM of elliptic curves. (Assume S4, vol. 1 & facts about orders)

Outline:

I. Elliptic curves / $\mathbb{C}$ & rationality
II. Potentially good reduction & integrality of $j$.
III. Main theorem & consequences (Grossencharacter, $L$-function)
IV. Ring class fields & abelian extensions

WARNING/ACHTUNG/ATTENTION: * unedited notes, use at your own risk

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

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

Recall that an elliptic curve $E / \mathbb{C}$ has $\text{End}(E) \cong \mathbb{Z}$ 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 $\text{End}(E) \otimes \mathbb{Q} \cong K$, this determines an embedding $i : K \hookrightarrow C$ st.

St. $\text{End}(E) \otimes \mathbb{Q} \cong \text{End}(C)$ commutes. (fix this once $i$ for all)

$K \overset{i}{\longrightarrow} C$

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

Let $C_1(\mathcal{O}) = \tilde{\text{proj}}. 1$ projective $\mathcal{O}$-modules $\mathfrak{a}_1 / \mathfrak{a}_1$. This forms a group under $\otimes$.

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

Recall that every elt. of $C_1(\mathcal{O})$ can be represented by an ideal $\mathfrak{a} \subseteq \mathcal{O}$ and that if $\mathfrak{a}, \mathfrak{a}'$ are two projective $\mathcal{O}$-submodules of $K$, then $\mathfrak{a} \otimes \mathfrak{a}' \subseteq \mathfrak{a} \otimes \mathfrak{a}'$.

Thm: There is a simply transitive action of $C_1(\mathcal{O})$ on $\text{Ell}(\mathcal{O})$ st. $C_1[\mathfrak{a}_1/\mathfrak{a}] = [\mathfrak{e}/\mathfrak{a} \mathfrak{a}]$.

PF: Note that $\mathfrak{e}/\mathfrak{a} \mathfrak{a} \subseteq C$ is a lattice (it's a discrete subgroup of $C$ with $\mathbb{Z}$-rank $\geq 2$).

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

1) $C / \mathfrak{a} \mathfrak{a}$ has CM by $\mathcal{O}$
2) $C / \mathfrak{a} \mathfrak{a} \cong C / \mathfrak{a} \mathfrak{a}$ 

(Note: if $C / \mathcal{O} \cong C / \mathfrak{a} \mathfrak{a}$, then clearly $C / \mathfrak{a} \mathfrak{a} \cong C / \mathfrak{a} \mathfrak{a}$, as $\mathfrak{a} \mathfrak{a}$ are homothetic.)

Pf of 1): $\text{End}(C / \mathfrak{a}) = \{ \sigma \in C | \sigma \mathfrak{a} \subseteq \mathfrak{a} \} = \{ \sigma \in C | \sigma \mathfrak{a} \mathfrak{a} \subseteq \sigma \mathfrak{a} \mathfrak{a} \} = \text{End}(C / \mathfrak{a} \mathfrak{a})$

If we assume $C / \mathfrak{a} \mathfrak{a} = \mathcal{O}$, so that $\mathfrak{a} \mathfrak{a} \subseteq \mathfrak{a}$.
If of 2): \( \mathcal{O}/\mathcal{O}' = \mathcal{O}/(\mathcal{O}')/\mathcal{O} \leftrightarrow \exists \mathcal{C} \in \mathcal{C}^\times \text{ s.t. } \mathcal{C}/\mathcal{O}' = \mathcal{C}/(\mathcal{O}')/\mathcal{O} \leftrightarrow \mathcal{C}/\mathcal{O} \cong C \cdot \mathcal{C}/\mathcal{O}' = C \cdot \mathcal{C}/(\mathcal{O}')/\mathcal{O} \)

\[ (\text{[AEC]} \text{ VI.1.1}) \]

(again use \( C \cdot \mathcal{O}/\mathcal{O} \cong \mathcal{O}/\mathcal{O}' \))

This happens \( \Leftrightarrow C \cdot \mathcal{O}/\mathcal{O}' \subset \mathcal{O} \) (cf. first equality in pf. of 1)),

which is equivalent to \( C \in K \) since \( \mathcal{O}/\mathcal{O}' \subset \mathcal{O} \) and \( \mathcal{C}/\mathcal{O} \cong \mathcal{C}/\mathcal{O}' \) as \( \mathcal{O} \)-modules.

Now we must show the action is simply transitive.

Actually, 2) above shows the action is faithful.

Transitivity:

Any lattice \( \mathcal{C}/\mathcal{C} \) is isomorphic to a lattice contained in \( K \) if \( \mathcal{C}/\mathcal{C} \) has CM by \( \mathcal{O} \).

(divide by any nonzero \( \mathcal{C}/\mathcal{C} \) then \( \mathcal{C}/\mathcal{C} \supset \mathcal{O} \) if they have the same \( \mathcal{O} \)-rank)

Note that \( \text{End}_{\mathcal{O}} \mathcal{C}/\mathcal{C} = \mathcal{O} \) since \( \mathcal{O} \) has CM by \( \mathcal{O} \).

Thus, by Shimura, Prop. 4.11, \( \mathcal{C}/\mathcal{C} \) is a projective \( \mathcal{O} \)-module, so that given any \( \mathcal{O}/\mathcal{O}' \), we have \( \mathcal{O}/\mathcal{O}' \cong \mathcal{O}/(\mathcal{O}'\mathcal{O})/\mathcal{O} \).

\[ \square \]

Cor: Every ell. curve \( E \in \text{Ell}(\mathcal{O}) \) has a model over a \#-fold.

Pf: If \( \sigma \in \text{Aut}(\mathcal{O}) \) and \( E \) has CM by \( \mathcal{O} \), then \( \sigma \) does \( E/\mathcal{O} \).

But there are only finitely many \( \mathcal{O} \)-isom classes of ell. curves, so \( j(E/\mathcal{O}) : \sigma \in \text{Aut}(\mathcal{O}) \) is finite. (Recall \( j(E/\mathcal{O}) = j(E/\mathcal{O}) \))

Thus \( j(E/\mathcal{O}) \in \mathcal{O} \).

\[ \square \]

Cor: \( [\mathcal{O}(j(E/\mathcal{O})):\mathcal{O}] \leq \# \text{Cl}(\mathcal{O}) \) if \( E \in \text{Ell}(\mathcal{O}) \)

Pf: \( [\mathcal{O}(j(E/\mathcal{O})):\mathcal{O}] \in \text{Ell}(\mathcal{O}) \) if \( \text{Ell}(\mathcal{O}) \) is a PHS for \( \text{Cl}(\mathcal{O}) \)

\[ \square \]

Rationality of endomorphisms:

Prop: If \( E \in \text{Ell}(\mathcal{O}) \), \( \sigma \in \text{Aut}(\mathcal{O}) \), \( \mathcal{O} \in \mathcal{O} \), then \( \mathcal{E}(\mathcal{C}) \rightarrow \mathcal{E}(\mathcal{C}) \)

\[ \begin{array}{ccc}
\mathcal{E}(\mathcal{C}) & \xrightarrow{[\alpha]} & \mathcal{E}(\mathcal{C}) \\
\downarrow & & \downarrow \\
\mathcal{E}(\mathcal{C}) & \xrightarrow{\mathcal{E}(\mathcal{C})} & \mathcal{E}(\mathcal{C}) \\
\end{array} \]

commutes

\[ \therefore \mathcal{E}(\mathcal{C}) = \mathcal{E}(\mathcal{C}) \]

(Here \( \mathcal{E}(\mathcal{C}) \) denotes the image of \( \mathcal{C} \) under \( \mathcal{C} \in \text{End} E \) )
Pf: We want to show that the diagram
\[
\phi \colon \text{End}(E) \xrightarrow{\cong} \text{End} T_0 E \cong C^c \quad \phi
\]
\[
\downarrow \quad \downarrow \quad \quad \downarrow \quad \downarrow
\]
\[
\phi \colon \text{End}(E) \xrightarrow{\cong} \text{End} T_0 E \cong C^c \quad \text{commutes.}
\]

But \( (\alpha \omega)^\sigma \omega^\sigma = (\omega \alpha)^\sigma = \alpha^\sigma \omega^\sigma = \alpha^\omega (\omega^\sigma)^\sigma \).

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

Pf: Klar!

We proved that \( E/(\mathfrak{m}) \) is a PHS for \( Cl(\mathcal{O}) \). It is also a \( \text{Gal}(R/k) \)-set \( \mathcal{T} \rightarrow \mathfrak{m} \) surjection \( \nu \colon \text{Gal}(E/k) \rightarrow Cl(\mathcal{O}) \colon \mathfrak{p} \rightarrow \mathfrak{p} \cap \mathcal{O} \) for \( \mathfrak{p} \) prime of \( K \).

Thm: If \( \sigma \in \text{Gal}(E/k) \), then \( j(E)^\sigma = j((\sigma E) \cdot E) \).

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

II. Potentially good reduction & integrality of \( j \) :

We'll use the following:

Prop: If \( E/L \) (\( L = \# \mathfrak{m} ! \) ) has CM by \( K \), then for \( F = KL \), for any \( \ell \) the representations \( \rho_\ell \colon \text{Gal}(E/F) \rightarrow \text{Aut} T_\ell E \) have abelian image.

Pf: Every endomorphism of \( E \) is defined over \( F = KL \).

It will suffice to show that the representations \( \text{Gal}(E/F) \rightarrow \text{Aut} E[\mathfrak{m}] \) are abelian.

By prev thm., \( \text{Gal}(E/F) \)-action commutes w/ \( \mathfrak{m} \)-action on \( E[\mathfrak{m}] \).

So really we have \( \text{Gal}(E/F) \rightarrow \text{Aut}_\mathfrak{m} E[\mathfrak{m}] \).

It suff. to show \( E[\mathfrak{m}] \) is a projective \( (\mathcal{O}/(\mathfrak{m})) \)-mod. of rk. 1, since then

\[
\text{Aut}_\mathfrak{m} E[\mathfrak{m}] \cong \text{Aut}_{(\mathcal{O}/(\mathfrak{m}))} E[\mathfrak{m}] \cong (\mathcal{O}/(\mathfrak{m}))^\times \text{ is abelian}
\]

\[
(\text{Hom}_{\mathcal{O}/(\mathfrak{m})}(E[\mathfrak{m}], \mathcal{O}/(\mathfrak{m})) \otimes E[\mathfrak{m}] \cong \text{End}_{\mathcal{O}/(\mathfrak{m})} E[\mathfrak{m}] \text{ check locally } \)
\]
We can write $E \cong C/\Lambda$ for $\Lambda \leq K$ an $O$-module.

In fact, $\Lambda$ is a projective $O$-mod. of rank 1, (we proved this when we proved the fact that $E(0)$ is a $C(0)$-PHS). Thus $\Lambda/\Lambda^\omega \cong \Lambda^\omega/\Lambda \cong E[1] \cong$ a proj. $O/(p^n)$-module of rank 1.

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

**Thm:** Let $E(L = \# e_L)$ 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 $T\overline{E}$ is an abelian Gal$(L/E)$-mod. $\forall L$.

Let $v$ be a place of $L$ and choose $L$ with $v|p+1$.

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

Since $T\overline{E}$ is abelian, we have a homom. $I^0_v \to \text{Aut } T\overline{E}$. (Here $I^0_v$ is the image of $I_v$ in Gal$(E/L)$.)

But $O_v$ is an extension of a finite group by a pro-$p$ gp $O_v$,

$\text{GL}_2(O_v)$ is an extension of a finite group by a pro-$l$ gp. The rest is easy.

**Cor:** If $E$ has CM by $K$, then $j(E) \in O_K$.

**Pf:** [AEC] VII.5.5.

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

Preliminaries.

Let $\Lambda \leq K$ be a rk. 2 $Z$-module (lattice). Then $\Lambda_p = \Lambda \otimes \mathbb{Z}_p \leq \mathbb{Q}_p = \mathbb{Q}_p/\mathbb{Z}_p$ is a $\mathbb{Z}_p$-lattice.
Exercise: Given a $\mathbb{Z}_p$-lattice $M_p \subset K_p \forall p \ s.t. \ M_p = \mathcal{O}_{K_p}$ for a.a. $p$, 
\exists! lattice $\Lambda \subset K \ s.t. \ \Lambda_p = M_p \forall p$.

Hint: $\Lambda = \bigcap_{p} (M_p \cap K_p)$.

Now given any idèle $s = (s_p) \in \mathbb{A}_k^\times$ with $s_p \in K_p$ and any lattice $\Lambda \subset K$, we can define by the exercise a lattice $\Lambda$ 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 $s$" $K/\Lambda \overset{s} \rightarrow K/s \Lambda$ to be the sum of the maps $K_p/\Lambda_p \overset{s_p} \rightarrow K_p/s_p \Lambda_p$.

Thm: (Main Thm. of CM for ell. curves) Suppose $E/\mathbb{Q}$ has CM by $K$. Choose $\Lambda \subset K$ such that $\xi : \mathbb{A}_k \rightarrow E$. Choose $\phi \in \text{Aut} \mathbb{C}$ and $s \in \mathbb{A}_k^\times$ s.t. $\phi|_{k^\text{ab}} = [s, K]$.

Then $\exists$ isom $\xi'$ filling in the commutative diagram of isomorphisms:

$\begin{array}{ccc}
K/\Lambda & \xrightarrow{\xi} & E(\mathbb{C})_{\text{tor}} \times S \\
\downarrow s' & & \downarrow \\
K/s \Lambda & \xrightarrow{\xi'} & E(\mathbb{C})_{\text{tor}} \times S
\end{array}$

Proof: Will be proved for ab. vars. ... eventually.

We can get first of all the Grüssen character.

Thm: Let $L \supset K$ be a # fld. $\xi : E/L$ an ell. curve w/ CM by $K$. Then there is a unique character $\alpha : \Lambda_{L}^\times \rightarrow K^\times$ s.t. if $x \in \Lambda_{L}$ and $s = N_{L/K}^\times$, then $\alpha(x)$ is unique s.t. 
(a) $\alpha(x) \cdot 0 = s \cdot 0$
(b) if $\Lambda \subset K$ is a projective $\mathcal{O}$-module & $\xi : E/L \overset{\xi} \rightarrow E(\mathbb{C})$, then

$\begin{array}{ccc}
K/\Lambda & \overset{\text{Quadr.}} \rightarrow & K/\Lambda \\
\downarrow \xi & & \downarrow \xi \\
E(\mathbb{C})_{\text{tor}} & \rightarrow & E(\mathbb{L}_{\text{ab}}) \\
\text{[x] - 1}
\end{array}$

Remark: We showed earlier that $E(\mathbb{C})_{\text{tor}} \subset E(\mathbb{L}_{\text{ab}})$.
Let $\sigma \in \text{Aut}(C)$ s.t. $\sigma|_{\mathfrak{m}} = (x,\mathfrak{m})$, so $\sigma|_{\mathfrak{m}}(a) = (s, K)$

\[ MT(N) \Rightarrow \exists \xi: C/\mathfrak{m} \to C/\mathfrak{m} \text{ s.t.} \]

\[ K/\mathfrak{m} \xrightarrow{\xi} K/\mathfrak{m} \]

\[ \xi \downarrow \quad \downarrow \xi' \quad \text{commutes} \]

\[ E(C) \to E(C) \]

\[ E(C) = E(C) \]

Since $E(C) = E(C)$, $\mathfrak{m} \not\in \mathfrak{m}$ are homothetic, so $\exists b = b(x) \in K^x$

s.t. $b \cdot \mathfrak{m} = \mathfrak{m}$.

We get $K/\mathfrak{m} \xrightarrow{\text{b}^{-1}} K/\mathfrak{m}$ commutes for appropriate $\xi''$.

\[ \xi \downarrow \quad \downarrow \xi'' \]

\[ E(C) \to E(C) \]

Let $\alpha(x)$ be the element of $K^x$ corresponding to $\xi''\xi^{-1}[b] \in (\text{End}(E)) \otimes \mathfrak{m}$.

Then the above diagram gives the commuting diagram

\[ K/\mathfrak{m} \xrightarrow{\alpha(x)\xi^{-1}} K/\mathfrak{m} \]

\[ \xi \downarrow \quad \downarrow \xi \]

\[ E(C) \to E(C) \]

(since $\xi''\xi^{-1}b = [\alpha][\xi]$)

Note that we must have $\alpha(x) \cdot \mathfrak{m} = \mathfrak{m} \Rightarrow \alpha(x) = s(0)$.

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

Also, it's straightforward to check that $\alpha(x)$ is indep. of $\mathfrak{m}$ $\xi$.

Moreover $\alpha$ is clearly a homom. by (b) $\xi$ uniqueness.

This $\alpha$ is not the Grössencharakter, but will give rise to it.

Thm: $\alpha: \mathbb{A}_C \to K^x$ is the unique character s.t.

(a) $\ker \alpha$ is open

(b) $\alpha|_{L^x} = N_{L/K}$
(c) $\alpha$ is unramified at $v \iff E$ has good reduction 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. $\phi_v$ at $v$.

**Pf:** (a),(b),(d) determine $\alpha$ 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 $\implies$

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

Set $U_m = \{ x \in B_m \mid (N_{L/k}x)_p \in (1 + m \mathfrak{o}_p) \cap \mathfrak{o}_p^{\times} \text{ for all } p \text{ prime}. \}

Note that this is open since $(1 + m \mathfrak{o}_p) \mathfrak{o}_p^{\times} = \mathfrak{o}_p^{\times}$ for all $p$ and in general $\mathfrak{o}_p^{\times}$ has finite index in $\mathfrak{o}_k^{\times}$ (use the exponential map). We'll show $\alpha_{|U_m} = 1$ ($\text{for suitable } m$).

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

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

$\xi(t) = \xi(t)^{\mathfrak{m}_L} = \xi(\mathfrak{m}_L)$ since $x \in B_m$

$\text{so } [x,L] \text{ fixes } E[m]$.

Since $(N_{L/k}x)_p \equiv 1 \mod m \mathfrak{o}_p$, so acts as $1$ on $t_p \in m^{-1}\Lambda/\Lambda$.

Thus $\alpha(x) \cdot (m^{-1}\Lambda) \subseteq m^{-1}\Lambda \implies (\alpha(x)-1) \cdot m^{-1}\Lambda \subseteq \Lambda \implies (\alpha(x)-1) \cdot 0 \equiv 0 \mod m \mathfrak{o}_p$.

i.e. $\alpha(x) \in \mathfrak{o}_p$ and $\alpha(x) \equiv 1 \mod m \mathfrak{o}_p$.

But prev. thm. $\implies (\alpha(x))_p (0 \mathfrak{o}_p = \mathfrak{o}_p \forall \mathfrak{p}$ so $\alpha(x) \cdot 0 \equiv 0 \mod m \mathfrak{o}_p$.

Thus for appropriate choice of $m$, we get $\alpha(x) = 1$ ($\mathfrak{o}_k^{\times}$ is finite).

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

$E$ has good reduction at $v \iff$ the inertia $\mathfrak{I}_v$ acts trivially on $E[mn]$ for all $n$.

Recall $\mathfrak{I}_v$ acts through its quotient $\mathfrak{l}_v^{\mathfrak{i}b} \subseteq \text{Gal}(L_{\mathfrak{i}b}/L)$.
\[
(\forall n \in \mathbb{Z}^+) \\
\vdash E \text{ has good reduc. at } v \iff x(t) = x(t) \quad \forall x \in \mathcal{L}_E \quad \forall t \in m^{-n} \wedge \Lambda \\
\iff x(t) \upharpoonright [x, L] = x(t) \quad \forall x \in \mathcal{O}_v \subseteq \mathcal{A}_E \quad \forall t \in m^{-n} \wedge \Lambda \\
\quad \implies x(\alpha(x) N_{L/F}^{-1} t).}
\]

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

Since \(\alpha_p \neq \sigma_p\) for only finitely many \(p\) and \(\mathcal{O}_E \subseteq \mathcal{O}_{K_p}\) always has finite index, \(\exists k \text{ s.t. } m^{-k} \subseteq \mathcal{O}_p\) \(\forall n \geq p \times m\), so \(m^{-k} \wedge \Lambda_p = m^{-k} \wedge \Lambda_p = 0\).

Thus \(m^{-n} \wedge \Lambda = \bigoplus_{p \mid m} m^{-n} \wedge \Lambda_p \). But for \(p \mid m\), \((N_{E/K}^{-1})_p = 1\). QED

Hence we have: \(E\) has good reduc. at \(v \iff \exists x(\alpha(x) t) = x(t) \forall x \in \mathcal{O}_v \subseteq \mathcal{A}_E \quad \forall t \in m^{-n} \wedge \Lambda\).

\(\iff \alpha(x) \equiv 1 \mod m^k \forall x \in \mathcal{O}_v \iff \alpha(x) = 1 \forall x \in \mathcal{O}_v \),

i.e., \(x\) is unram. at \(v\).

(d): Let \(v\) be a good prime for \(E/L\) and again choose \(m\) prime to \(v\).

Claim (*) above shows that \(x(t) \upharpoonright \mathcal{F}_{E_v} = x(\alpha(x) t) = [\alpha(x)] (x(t)) \forall t \in m^{-n} \wedge \Lambda\)

\((\forall \mathcal{F}_{E_v} \uparrow \mathcal{F}_L) = [\alpha(x)] \mathcal{F}_L \quad \forall t \in m^{-n} \wedge \Lambda\),

Denote by \(\tilde{E}/\mathcal{O}(v)\) the reduction of \(E\) at \(v\), and let \(E(\mathcal{O}(v)) \rightarrow \tilde{E}/\mathcal{O}(v)\) be the reduction map. Then \(x(t) \upharpoonright \mathcal{F}_{E_v} = \tilde{x}(x(t)) \).

Also denote the (injective) map \(\text{End } E \rightarrow \text{End } \tilde{E} : \psi \mapsto \tilde{\psi}\). This satisfies \(\tilde{\psi}(x) = \tilde{x}(\psi(x))\).

\(\text{End } E \rightarrow \text{End } \tilde{E} \text{ for } v \notin \mathcal{P}\)

Hence \(\tilde{x}(x(t)) = \tilde{\alpha}(\tilde{x}(x)) (\tilde{x}(t)) \forall t \in m^{-n} \wedge \Lambda\), so done (since
We can now (finally!) talk about the Grössencharakter $\chi$-L-function...

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

If $L \subseteq K$, define the local norm $N_p : L_p \to K_p$.

Now suppose $E/L$ has CM by $K$ and that $L \subseteq K$. Let $\alpha = \alpha_E$.

Define $\chi_p = \chi_{E,p} : \mathbb{A}_L^\times \to K_p^\times$

\[ x \mapsto \alpha(x).N_p(x)^{-1} \]

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

If $p$ is finite, $K_p^\times$ is totally disconnected, so $\chi_p$ is trivial on $(\mathbb{A}_C^\times/L_p^\times)^0$, so $CFL \Rightarrow$ we can view $\chi_p$ as a $K_p^\times$-valued character of $\text{Gal}(L_p/K_p)$.

Recall that $T_pE$ is a rank 1 $O_\mathbb{Z}_p^\times$-module, so we can view $\rho_p : \text{Gal}(L/K) \to K_p^\times$.

\[
\text{Thm : } \chi_p = \rho_p
\]

If: We only need to check this on $\text{Frob}_v$ for $v \mid p$ a good prime of $E$.

This is just (d) of the prev. thm. (note: $\chi|_{\mathbb{C}_L^\times} = \chi_p|_{\mathbb{C}_L^\times}$).

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

It is clear that $\chi_E$ has type $(1,0)$ with respect to $i : K \hookrightarrow \mathbb{C}$ (the embedding from the beginning).

Some general nonsense about $L$-functions:

All Grössencharaktere $\chi : \mathbb{A}_C^\times \to \mathbb{C}^\times$ have an $L$-function $L(\chi, s) = \prod_{v \in S} (1 - \chi(v_v)q_v^{-s})^{-1}$, where $S$ = set of finite places of $L$ where $\chi$ is unramified.

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

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

where $L_v(E/L, T) := \det (1 - \text{Fr}_v T | T_E^I_v) = \begin{cases} \det \text{Fr}_v T^2 - T \Phi(T) + 1 & \text{E good at } v \\ 1 - T & \text{E split mult. at } v \\ 1 + T & \text{E nonsplit mult. } \mathbb{Z}[T] \\ 1 & \text{E additive at } v \end{cases}$
Thus: Let $E/L$ have CM by $K$

(a) If $L \cong K$, then $L(E/L, \sigma) = \mathbb{L}((\chi_E, s)) \mathbb{L}((\overline{\chi}_E, s))$
(b) If $L \not\cong K$, then $L(E/L, \sigma) = \mathbb{L}((\chi_E, s))$ (where $\chi_E$ 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 $\chi_E \not\equiv \overline{\chi}_E$ are unramified at $v \in \mathbb{S}$, $E$ has good reduction at $v$, need to prove (for $v$ good prime for $E$)

(i) $\text{tr} \phi_v = \chi_E(\pi_v) + \overline{\chi}_E(\pi_v)$
(ii) $\det \phi_v = \chi_E(\pi_v)\overline{\chi}_E(\pi_v)$

(i): follows from the fact that $\chi_E = \rho_p$ (pick $l = \text{split in } K$, e.g.)

(ii): can proceed as in (i), or note that $\chi_E\overline{\chi}_E = 1_N$ since $\chi_E$ has type $(1,0)$,

then use that $\det \phi_v = \text{deg } \phi_v = q_v = N(\pi_v)$

(l): This will be more work. Set $F = KL$ and let $\sigma$ be the nontrivial elt. of $\text{Gal}(E/L)$

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

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

If the reduction $\bar{E}$ of $E$ at $w$ is good, we get an injection (as before)

End $E \rightarrow \text{End } \bar{E}$. But since $v$ is ramified, $w$ has bad reduction at $v$.

and $\sigma$ fixes $w$; thus $\sigma$ must be that $[\sigma]^{G} = [\alpha] \Rightarrow \sigma$.

Thus if $v$ is ramified in $F$ with $w|v$, $E$ has additive reduction at $v$.

So that $Lv(E/L, T) = 1$. $E$ also has bad reduction at $w$, so $\chi_E$ is ramified at $w$.

\[ \vdots \] 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 $v \Rightarrow E_F$ 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
\[ X_E(\pi_w) = X_E(\pi_{w'}) \Downarrow X_E(\pi_w) = X_E(\pi_{w'}) \]

**Proof:** \([X_E(\pi_w)]\) is the unique endomorphism of $E$ reducing to the Frobenius endomorphism $\phi_w$ at $w$. So is $\left[ X_E(\pi_w)^{\sigma} \right] = \left[ X_E(\pi_w) \right]^{\sigma}$ \(\blacksquare\).

(Rmk. thus in fact $\overline{X_E} = X_E^{\sigma}.\)

Thus, if $v$ is split, we have \(\text{tr} \phi_v = \text{tr} \phi_w = \text{tr} \phi_{w'} = X_E(\pi_w) + X_E(\pi_{w'}) = X_E(\pi_w) + X_E(\pi_{w'})\) and \(\det \phi_v = q_v = q_w = q_{w'} = X_E(\pi_w)X_E(\pi_{w'}) = X_E(\pi_w)X_E(\pi_{w'})\)

\[
\therefore L_v(E/L, T) = (1 - X_E(\pi_w)T)(1 - X_E(\pi_{w'})T) \quad \text{(if $E$ has good reduc at $v$)}
\]

If $v$ is inert in $w' \mid v$, then we have $X_E(\pi_w) = \overline{X_E(\pi_w)}$ so that

\[ [X_E(\pi_w)] \in \mathbb{Z} \leq \text{End } E \Rightarrow [X_E(\pi_w)] = \phi_w = q_v e \mathbb{Z} \leq \text{End } E.\]

Note that $\phi_v^2 = \phi_w = q_v$. We claim that $\phi_w = q_v$. If not, then we have $\phi_v \in \mathbb{Z}$ as well (otherwise $\alpha[\phi_v, \phi_v] \cong \mathbb{Q}(q_v)$ is real quadratic with non-trivial endomorphism $\phi_v \mapsto \phi_v$, but $\phi_{w'} = q_v \neq q_v$). As before, let $[\alpha] \neq [\alpha]^\sigma$ be an endomorphism of $E_F$ not defined over $L$, so that $[\alpha] \neq [\alpha]^\sigma = [\alpha]^{F_{w'}}$. We also have that $[\phi_v][\alpha] = [\alpha]^{F_{w'}}[\phi_v]$, but since $\phi_v \in \mathbb{Z}$, it commutes with every endomorphism, so that $[\alpha] = [\alpha]^{F_{w'}}$. Thus $\phi_w = q_v$.

Hence $\phi_v$ satisfies $X^2 + q_v$, which therefore must be its characteristic polynomial \(\therefore\) since the char poly has conjugate roots: \(\det \left( \frac{m}{n} - \phi_v \right) = \frac{1}{n} \deg (m - n\phi_v) \geq 0 \quad \forall \frac{m}{n} \in \mathbb{Q} \)

In particular, \(\det \phi_v = q_v = X_E(\pi_w)\) and \(\text{tr} \phi_v = 0\).

In conclusion, we have shown:

\[
L_v(E/L, T) = \begin{cases} 
(1 - X_E(\pi_w)T)(1 - X_E(\pi_{w'})T) & \text{E good at } v = w', w' \\
(1 - X_E(\pi_w)T^2) & \text{E good at } v = w \text{ (split)} \\
1 & \text{E bad at } v.
\end{cases}
\]

So: \(L(E/L, s) = \prod_{w'' \mid w} L_v(E/L, q_{w''}^{-s}) = \prod_{w' \mid w} (1 - X_E(\pi_w)^{-s}) q_w^{-s} = L(E, s) \quad \text{(note } q_{w''}^2 = q_{w'} \text{ if } v \text{ inert}) \quad \square\).
Cor: $L(E/L,s)$ has analytic continuation and functional equation of the form

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

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

Pf: Follows from the thm. of properties of $\chi_E$.

Remark: (1) Let $E/L$ have CM by $K \not= \mathbb{Q}$. If $p \in O_\mathbb{A}$ is split in $K_1$, the homomorphism

$$\chi_p: \mathbb{A}_F^\times \rightarrow K_1^\times \cong \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times$$

splits as a sum of two characters $\chi_p = \varphi_p \otimes (\chi_p)^{(1 \neq \sigma \in \text{Gal}(F/L))}$. Using the pf of the thm., one can show that in this case $\varphi_p \cong \text{Ind}_F^K \varphi_p$.

(2) In the proof of the thm., we saw that when $v$ is inert in $F \not= \mathbb{Q}$, we have $\text{tr} q_v = 0$, so that $E$ is supersingular at such primes.

(3) In general, if $E/L$ has CM by $K$ and good reduction at $\mathfrak{p} \mid p$, then $E$ has supersingular reduction at $\mathfrak{p}$ if and 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 previous 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 Grössencharacters).

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 $h_E : E \to E/\text{Aut} E$ (defined over $L$). Note that $E/\text{Aut} E \cong \mathbb{P}_L^1$.

If $E \cong E'$ (over $K$), get canonical $L$-isom. $E/\text{Aut} E = E'/\text{Aut} E'$, i.e., $h_E \eta = h_{E'} \eta$ for all $\eta \in E$.

If $E$ has Weierstrass equation $y^2 = 4x^3 - q_2 x - q_3$, the Weber function can be expressed as

$$h(x, y) = \begin{cases} \left(\frac{q_2 x}{q_3} \right)^x \left(\frac{q_3}{q_2} \right)^x & j(E) \neq 0, 1728 \\ \left(\frac{q_3}{q_2} \right)^x & j(E) = 1728 \\ \left(\frac{q_2}{q_3} \right)^x & j(E) = 0 \end{cases}$$

This gives a map $E \to \mathbb{P}_L^1$.

Then: Suppose $E$ has CM by $0 \leq K$ and let $\xi : E/\mathbb{Q} \to E(C)$ for $\Lambda \in K$.

Let $\Lambda \in K$ and set

$$W = \{ w \in \Lambda \mid \exists \xi = \lambda, w = u \} \quad \text{(does not depend on $\Lambda \in K$)}$$

Then $K(\xi(E), h(\xi(w)))$ is the subfield of $K^\Lambda$ corresponding to $K^\Lambda W \subseteq \Lambda^\Lambda$.

Proof: Note $W \cong K^\Lambda$ and is open. Let $F \subseteq K^\Lambda$ be the field with $\Lambda^\Lambda / F \cong \text{Im}(E/K)$.

Choose any $o \in \text{Aut} E$ fixing $K$ and let $\sigma \in \text{Aut} E$ be s.t. $o|Kab = [\xi, K]$.

The Main Thm. of CM $\Rightarrow \exists \xi : E/\mathbb{Q} \to E(C)$ s.t. $\ldots$

We need that $\sigma|E = 1 \iff \sigma|K(\xi(E), h(\xi(w))) = 1$.

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

Then $h_E(E(\xi(w)^\sigma)) = h_{E'}(\xi(\xi(w))^\sigma) = h_{E'}(\xi(w))^\sigma$.

Since $h_{E'}$ is the Weber function of $E'$, since $h_E$ is the Weber function of $E'$. 
But we have $E(\xi(w)^\sigma) = E(\xi'(s^{-1}w)) = \xi(w)$, so that $h_E(\xi(w)) = h_E(\xi(w))^\sigma$.

Thus $\sigma|_{k(j(E), h_E(\xi(w)))} = 1$.

Conversely, if $\sigma|_{k(j(E), h_E(\xi(w)))} = 1$, $j(E) = j(E)^\sigma$, so $\xi(w) \cong \xi(w)^\sigma$.

$\Rightarrow s^{-1}w \cong w$ as $\sigma$-equiv. $\Rightarrow \exists \mu \in K^x$ s.t. $\mu s^{-1}w = w$.

So we can define $g : E^\sigma \rightarrow E$ s.t.

$E/\xi(w)\cong E/\xi(w)^\sigma$.

Again using properties of Weber functions, get that

$h_E(\xi(w)) = h_E(\xi'(w))$, so $\xi(w)$ and $\xi'(w)$ differ by an automorphism of $E$, say $\xi'(w) = \alpha \xi(w)^\sigma$.

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

so that $(\alpha \mu s^{-1})w = w$. Thus $s \in K^x$.

$\Rightarrow \sigma|_E = \text{id}$.

Recall that $\text{Gal}(E)$ has a simply transitive action of $C_1(0)$ and an action of $\text{Gal}(E/K)$.

There is also a surjection: $\pi : \text{Gal}(E/K) \rightarrow C_1(0)$.

For $p \in C_1$, $C_1(0)$ (if p is conductor 0)

**Cor:**

(a) $k_{ab} = k(j(E), h_E(\xi(w)))$

(b) $j(E)^\sigma = j(E^\sigma)$ for $\sigma \in \text{Gal}(E/K)$. Also, $k(j(E))$ is the ring class field of $K$ of conductor $C = \text{cond}(E)$. (If $C = \sigma$, this is the Hilbert class field.)

(c) $[k(j(E)) : k] = [K : \text{Gal}(E/K)] = \#C_1(0)$

(d) If $\{A_i : 1 \leq i \leq \#C_1(0)\}$ is a set of representatives for $C_1(0)$, then $j(A_i)^{\sigma} = j(A_i)$ is a complete set of conjugates for $j(E)$ over $A_i$ (or $K$).
Pf: (a): check that \( \bigcap_{u \in W(u)} K^x W(u) = K^x K_\infty^x. \)

Note that we already know \([K(j(\ell)) : K] \leq [\Delta(j(\ell)) : \Delta] \leq \#Cl(\ell)\),
so clearly (b) \(\Rightarrow\) (c) \(\Rightarrow\) (a).

(b): take \(u = 0\) in the prev thm., so \(W(u) = K_\infty^x \times \prod_p B_p^x \).

then the theory of ray class fields \(\Rightarrow K^x W\) is the kernel

\[ A_k^x \xrightarrow{rec} \text{Gal}(K^{ab}/K) \xrightarrow{\rho} \text{Cl}(\ell), \text{and also of } A_k^x \xrightarrow{rec} \text{Gal}(K(j(\ell))/K) \]

We already know from the Main Thm. that \(j(\ell)^{Frob_p} = j(\ell)^{[\pi_p, K]} = \)

\[ = j\left( (\pi_p^{-1}\ell)^{\ell} \right) = j\left( (\ell \pi_p^{-1})^\ell \right) = j\left( \ell^{\ell \pi_p^{-1}} \right) \quad \forall \ell \text{ conductor } \ell. \]

D.

Cor: If \(E\) has CM by \(\mathcal{O}_K\) and \(\mathfrak{c} \subseteq \mathcal{O}_K\) is an ideal, then \(K(j(\ell), h(E[\mathfrak{c}]))\) is

the ray class field of \(K\) of conductor \(\mathfrak{c}\). (Here \(E[\mathfrak{c}] = \{x \in E(\mathbb{C}) \mid [\mathfrak{c}]x = 0 \forall x \in \mathfrak{c}\} \))

Pf: Check that \(\bigcap_{u \in W(u)} K^x W(u) = K^x U(\mathfrak{c})\), where \(U(\mathfrak{c})\) is the subgroup

\[ \{ s \in A_k^x \mid s_p \in B_p^x, \forall p \text{ such that } s_p \equiv 1 (\mathfrak{c} \mathcal{O}_{E_p}^x \text{ ) the primes } p \} =: U(\mathfrak{c}) \subseteq A_k^x. \]

D.