S be finite set of primes, $2 \in S$. $W_S = \bigoplus_{p \notin S} \mu_{p^\infty}$.

Def An Euler system is a map $\phi : W_S \to \overline{\mathbb{Q}}^\times$ such that for $\zeta \in W_S$,

E1. $\phi(\zeta^{-1}) = \phi(\zeta)$; $\phi(\zeta^\sigma) = \phi(\zeta)^\sigma$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

E2. For $q \notin S$,

$$\prod_{\rho \in \mu_q} \phi(\rho\zeta) = \phi(\zeta^q).$$

E3. For $q \notin S$, ζ ord prime to q,

$$\phi(\rho\zeta) \equiv \phi(\zeta) \bmod \mathfrak{q}$$

for $\rho \in \mu_q$, $\mathfrak{q} | q$ prime of $\mathbb{Q}(\mu_q\zeta)^{(+)}$

[See few pages later, ϕ takes values in units.]

For $m \geq 1$ odd integer, define $\mathcal{H}_m = \mathbb{Q}(\mu_m)$, $H_m = \mathcal{H}_m^+$.
For $q \nmid m$ prime, $Fr_q \in \mathrm{Gal}(\mathcal{H}_m/\mathbb{Q})$ frobenius map at q, acts on ζ by $\zeta \mapsto \zeta^q$. $Fr_q \in \mathrm{Gal}(H_m/\mathbb{Q})$, $\zeta + \zeta^{-1} \mapsto \zeta^q + \zeta^{-q}$.
Let ϕ be an arbitrary Euler System. For $(m,S)=1$, $\zeta \in \mu_m$, E1 shows $\phi(\zeta) \in H_m$.

Lemma. $(m,S)=1$. q prime, $q \nmid m$, $q \notin S$. Then for $\zeta \in \mu_m$, $\rho \in \mu_q$, $\rho \neq 1$, we have

$$N_{H_{mq}/H_m} \phi(\rho\zeta) = \frac{\phi(\zeta)^{Fr_q}}{\phi(\zeta)}.$$

Lemma. $m \geq 1$, $(m,S)=1$. $q \nmid m$, $q \notin S$ prime. $n \geq 1$. For all $\zeta \in \mu_m$, $\eta \in \mu_{q^{n+1}}$ primitive q^{n+1}-root, we have

$$N_{H_{mq^{n+1}}/H_{mq^n}} \phi(\eta\zeta) = \phi(\eta^q \zeta^{Fr_q}).$$

For each $n \geq 0$, $\eta_n \in \mu_{q^{n+1}}$ primitive root, compatible under $\eta_n^q = \eta_{n-1}$ for $n \geq 1$.

Cor. Let $\tau_n = Fr_q^{-n}(\zeta)$. Let $v_n = \phi(\eta_{n-1}\tau_{n-1})$. Then

$$N_{H_{mq^{n+1}}/H_{mq^n}}(v_{n+1}) = v_n.$$

Example $a_1, \dots, a_r$ non-zero integers. $n_1, \dots, n_r$ integers with $\sum_1^r n_i = 0$.

S: set of primes, $2 \in S$, prime factors of $a_1 \dots a_r \in S$.

$W_S = \bigoplus_{p \notin S} \mu_{p^\infty}$. Define for $\zeta \neq 1 \in W_S$,

$$\phi(\zeta) = \prod_{j=1}^{r} \left(\zeta^{-a_j/2} - \zeta^{a_j/2}\right)^{n_j}.$$

Cyclotomic units are of this form. ($\phi(1) = \prod a_j^{n_j}$)

Cohomology Classes

Take $0 \to \mu_{p^m} \to \overline{\mathbb{Q}}^\times \xrightarrow{(\ )^{p^m}} \overline{\mathbb{Q}}^\times \to 0$.

For number field F, take $\mathrm{Gal}(\bar{F}/F)$-cohomology $H^i(F, \_)$.

$$0 \to \mu_{p^m}(F) \to F^\times \xrightarrow{(\ )^{p^m}} F^\times \to H^1(F, \mu_{p^m}) \to \underbrace{H^1(F, \overline{\mathbb{Q}}^\times)}_{0}$$

So $F^\times / F^{\times p^m} \simeq H^1(F, \mu_{p^m})$; $F^\times \otimes \mathbb{Z}_p \simeq H^1(F, \mu_{p^\infty})$.

For Euler system ϕ, m coprime to S, $\phi(\zeta_m) \in \mathbb{Q}(\mu_m)^\times$, so we construct corresponding class $c_m \in H^1(\mathbb{Q}(\mu_m), \mu_{p^\infty})$. The norm compatibility from lemmas become:

$$\mathrm{cores}^{\mathbb{Q}(\mu_{m\ell})}_{\mathbb{Q}(\mu_m)}(c_{m\ell}) = \begin{cases} c_m & \text{if } \ell \mid m \\ (1-\ell^{-1})\, c_m & \text{if } \ell \nmid m \end{cases}$$

$$(1 - \mathrm{Frob}_\ell^{-1})\, c_m$$

for good choice of ζ_m.

Rmk: Go to Galois rep, in place of μ_{p^∞}.

Values of Euler Systems.

Thm. For $\phi : W_S \to \overline{\mathbb{Q}}^\times$, the value $\phi(\eta) \in \mathbb{Q}(\eta)^+$ is a unit for all $\eta \neq 1$.

Let q be prime. Let $L/\mathbb{Q}$ be number field. L^{cyc}/L be the cyclotomic extension, and $L_n \subseteq L^{cyc}$ be the n^{th} level: $Gal(L^{cyc}/L) = \mathbb{Z}_q$, $Gal(L^{cyc}/L_n) = q^n \mathbb{Z}_q$.

Lemma. Let q be prime, $L/\mathbb{Q}$ finite. Suppose $z \in L^\times$ is a ~~unit~~ norm from L_n for all $n \geq 0$. Then for any prime $r \subseteq L$ not above q, $z \notin r$.

Pf. There are only finitely many primes of L^{cyc} above r: r is unramified in this extension. So the subgroup generated by Frob_r in $Gal(L^{cyc}/L) = \mathbb{Z}_p$ is non-trivial hence finite index. Index of $\langle \mathrm{Frob}_r \rangle$ = # primes of L^{cyc} above r.

Let $r_n \subseteq L_n$ be compatible system of primes above r. Since splitting is finite, inertia degree $[\mathcal{O}_{L_n}/r_n : \mathcal{O}_L/r]$ is unbounded as $n \to \infty$. Hence if z is norm from L_n, $z \in r$, then $z \in r_n^{f_n}$ so $\mathrm{ord}_r(z)$ is unbounded. Thus $\mathrm{ord}_r(z) = 0$.

Pf (Thm). $t = \mathrm{ord}(\eta)$. Let $q \mid t$, $t = t_1 q^{m+1}$ for $m \geq 0$, t_1 prime to q. So $\mu_t = \mu_{t_1} \oplus \mu_{q^{m+1}}$, $\exists\, \rho_m \in \mu_{q^{m+1}}$ primitive and $\zeta \in \mu_{t_1}$ such that $\eta = \rho_m \cdot \mathrm{Fr}_q^{-m}(\zeta)$. Then $\phi(\eta) \in H_{t_1 q^{m+1}}$ is a norm from $H_{t_1 q^n}$ for $n \geq m+1$. But $H_{t_1 q^{n+1}} / H_{t_1 q^{m+1}}$, $n \geq m$ is a $\mathbb{Z}_p$-extn (cyclotomic!) so for any $r \nmid q$, $\mathrm{ord}_r(\phi(\eta)) = 0$.

We need to check $\mathrm{ord}_q(\phi(\eta)) = 0$. Here, $t = q^{m+1}$. In the tower $H_q \subseteq H_{q^2} \subseteq \dots$, q is totally ramified, non-split. For $t = q^{m+1}$,

$N_{H_{q^{m+1}}/H_q} \phi(\eta) = \phi(\rho_0)$ for some ρ_0 ($\rho_0 = \eta^{q^m}$). But

$N_{H_q/\mathbb{Q}} \phi(\rho_0)^2 = \prod_{\zeta \in \mu_q - 1} \phi(\zeta) = 1$ by E2. Hence η, ρ_0 are units.

Factorization Theorem.

Notation. p fixed odd prime. $F = \mathbb{Q}(\mu_{p^{m+1}})^+$, $m \geq 0$.
$t = p^a$, $a \geq m+1$. S finite set of primes, $2 \in S$, $p \notin S$.

$J_r = F(\mu_r)^+$, $\Delta_r = Gal(J_r/F)$, $r \geq 1$.
I: group of ideals of F, I_q: group of ideals above q. $I = \bigoplus_q I_q$
Z_S: sqfree positive integers prime to p, S. $Z_S' \subseteq Z_S$ products of primes $\equiv 1 \pmod t$.

Lemma. For $n \geq 1$, the map $F^\times/F^{\times t} \longrightarrow (J_n^\times / J_n^{\times t})^{\Delta_n}$ is an isomorphism.

Pf. $J^\times$ is totally real, so there are no tth roots of unity. So one has the exact sequence

$$1 \to J^\times \xrightarrow{\times t} J^\times \longrightarrow J^\times/J^{\times t} \to 1$$

Taking Galois cohomology gives the exact sequence

$$1 \to F^\times \xrightarrow{\times t} F^\times \to (J^\times/J^{\times t})^\Delta \longrightarrow H^1(\Delta, J^\times) \to \cdots$$

But $H^1(\Delta, J^\times) = 0$, so $F^\times/F^{\times t} \simeq (J^\times/J^{\times t})^\Delta$.

Lemma: For $n \in Z_S$, $q|n$ prime, we have $J_q \cap J_{n/q} = F$, $J_n = J_q J_{n/q}$. Primes of F above q have ramification index $q-1$ in J_n.

Cor. Suppose $n \in Z_S$, $n = q_1 \cdots q_k$. Then $\Delta_n \simeq \Delta_{q_1} \times \cdots \times \Delta_{q_k}$.

Δ_q is cyclic of order $q-1$. Let τ_q be a generator of Δ_q.
Consider elements of $\mathbb{Z}[\Delta_q]$: $N(q) = \sum_{\sigma \in \Delta_q} \sigma = \sum_{i=0}^{q-2} \tau_q^i$.
$D(q) = \sum_{i=0}^{q-2} i \cdot \tau_q^i$. ($D(q)$ depends on choice of τ_q).

Lemma: For $q \in Z_S$ prime, $(\tau_q - 1) D(q) = q - 1 - N(q)$.

For $n = q_1 \cdots q_k \in Z_S$, identify $\Delta_{q_i} \simeq Gal(J_n/J_{n/q_i}) \subseteq \Delta_n$.
So one can form $D(n) = D(q_1) \cdots D(q_k)$ in $\mathbb{Z}[\Delta n]$.
Let $\phi : W_S \to \overline{\mathbb{Q}}^\times$ be an Euler System. We extend Δ_n action to $\mathbb{Z}[\Delta n]$.

Prop. Let ρ be a primitive p^{m+1}-root of 1. For $n \in \mathbb{Z}_S^1$, let ξ_n be a primitive n^{th} root. The class of $\phi(\rho\xi_n)^{D(n)}$ in $J_n^{\times}/J_n^{\times t}$ is fixed by Δ_n.

Pf. Define $\kappa_{n,q} = D(n)(\tau_q - 1)$, $q \in \mathbb{Z}_S^1$. We prove prop by induction on k, $n = q_1 \cdots q_k$. For $n = q$, $q \equiv 1 \pmod t$ prime,
$\phi(\rho\xi_q)^{[q-1]} \in J_n^{\times t}$, $[q-1] \in \mathbb{Z}[\Delta_n]$. But $q-1 = \kappa_{q,q} + N(q)$. So,
$\phi(\rho\xi_q)^{\kappa_{q,q}} \equiv \phi(\rho\xi_q)^{-N(q)} \bmod J^{\times t}$. Note now that $\phi(\rho\xi_q)^{N(q)}$ is just the norm ~~of~~ $H_{p^{m+1}q}$ to $H_{p^{m+1}}$. So,

$$\phi(\rho\xi_q)^{N(q)} = \phi(\rho)^{Fr_q - 1}!$$

But also observe $q \equiv 1 \bmod t$, so $q \equiv 1 \bmod p^{m+1}$. Hence Fr_q acts trivially. So $\phi(\rho\xi_q)^{\kappa_{q,q}} \equiv 1 \bmod J^{\times t}$ which means τ_q (hence Δ_q) acts trivially on the class of $\phi(\rho\xi_q)^{D(q)}$ in $J^{\times}/J^{\times t}$.
Now say $n = q_1 \cdots q_k$ and prop is true for all n with $< k$ factors
$\xi_n = \xi_{q_1} \cdots \xi_{q_k}$, product of primitive roots. Since $\tau_{q_1} \cdots \tau_{q_k}$ generate Δ_n, we show $\phi(\xi_n\rho)^{\kappa_{n,q_i}} \in J_n^{\times t}$ for all i. Set $D_i(n) = \prod_{j \neq i} D(q_j)$.

We have,

$$\phi(\rho\xi_n)^{\kappa_{n,q_i}} \equiv \left(\phi(\rho\xi_n)^{D_i(n)}\right)^{q_i - 1 - N(q_i)} \bmod J_n^{\times t}$$

$t \mid q_i - 1$.

$$\equiv \phi(\rho\xi_n)^{-D_i(n)N(q_i)} \bmod J_n^{\times t}.$$

But now $\phi(\rho\xi_n)^{N(q_i)} = \phi(\rho\xi_n/\xi_{q_i})^{Fr_{q_i} - 1}$, so

$$\phi(\rho\xi_n)^{D_i(n)N(q_i)} \equiv \phi(\rho\xi_n/\xi_{q_i})^{(Fr_{q_i}-1)D_i(n)}$$

By induction hypothesis, $Fr_{q_i} - 1$ acts trivially on $\phi(\rho\xi_n/\xi_{q_i})^{D_i(n)}$ mod $J_n^{\times t}$, so we have $\phi(\rho\xi_n)^{\kappa_{n,q_i}} \in J_n^{\times t}$, proving the prop.

<u>Lemma</u>: Let $q \in Z_S^1$ be prime. There is a natural homomorphism

$$l_q' : (\mathcal{O}_F / q\mathcal{O}_F)^\times \longrightarrow I_q / t I_q \,,$$

$\mathrm{Gal}(F/\mathbb{Q})$-equivariant, and $\ker(l_q') = (\mathcal{O}_F/q\mathcal{O}_F)^{\times t}$.

<u>Rmk</u>: l_q' depends on the choice of generator τ_q. Lemma depends on the fact that primes above q are tamely ramified in J_q/F.

<u>Pf</u>: $q \equiv 1 \bmod t$, so q splits completely in F ($\mathrm{Fr}_q = 1$). So I_q is a free $\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$-module of rank 1.

J_q/F has degree $q-1$, and all primes over q are totally ramified (also tamely ramified). Residue field of $\mathfrak{q}|q$ is $\mathbb{F}_q$. From ramification theory, $\sigma \longmapsto \pi_{\mathfrak{q}}/\sigma(\pi_{\mathfrak{q}})$ is an isomorphism $\Delta_q \xrightarrow{\sim} \mathbb{F}_{\mathfrak{q}}^\times$, independent of choice of uniformizer $\pi_{\mathfrak{q}}$.

$$\begin{tikzcd}
 & J_q \arrow[d, dash] \\
\mathfrak{q} \arrow[d, dash] & F \arrow[d, dash] \\
q & \mathbb{Q}
\end{tikzcd}$$

τ_q maps to a primitive root $r_{\mathfrak{q}} = \pi_{\mathfrak{q}}^{1-\tau_q}$.

For $\alpha \in \mathcal{O}_F$, $(\alpha, q) = 1$, we have $\alpha \bmod \mathfrak{q} = r_{\mathfrak{q}}^{a_{\mathfrak{q}}(\alpha)}$ for some $a_{\mathfrak{q}}(\alpha) \in \mathbb{Z}/(q-1)\mathbb{Z}$. We define the map

$$l_q'(\alpha \bmod q\mathcal{O}_F) = \sum_{\mathfrak{q}|q} (a_{\mathfrak{q}}(\alpha) \bmod t)\cdot \mathfrak{q}.$$

Then l_q' has the desired properties.

Galois action

$$\begin{aligned}
l_q'(\sigma\alpha) &= \sum (a_{\mathfrak{q}}(\sigma\alpha) \bmod t)\, \mathfrak{q} \\
&= \sum (a_{\sigma^{-1}\mathfrak{q}}(\alpha) \bmod t)\, \mathfrak{q} \\
&= \sum (a_{\mathfrak{q}}(\alpha) \bmod t)\, \sigma\mathfrak{q}.
\end{aligned}$$

Kernel = t^{th} powers, when $a_{\mathfrak{q}} = 0 \bmod t$ so $\alpha \equiv t^{th}$ power mod $\mathfrak{q}$ $\forall \mathfrak{q}$.

For $x \in F^\times/F^{\times t}$, write
$$(x) = \sum_r \mathrm{ord}_r(x)\cdot r \bmod tI,$$
$$(x)_q = \sum_{\mathfrak{q}|q} \mathrm{ord}_{\mathfrak{q}}(x)\, \mathfrak{q} \bmod t I_q.$$

Let S_q be subgroup of $F^\times/F^{\times t}$, $(\ )_q = 0$.

For $q \in \mathbb{Z}_s^1$ prime, there is homomorphism

$$S_q \longrightarrow \mathcal{B}/\mathcal{B}^t, \quad \mathcal{B} = (\mathcal{O}_F/q\mathcal{O}_F)^\times.$$

compose with $\mathcal{B}/\mathcal{B}^t \longrightarrow I_q/tI_q$, one has map $l_q : S_q \to I_q/tI_q$

ρ: fixed, primitive p^{M+1} root of 1.

<u>Def</u>. $R_\phi(\xi_n) \in F^\times/F^{\times t}$ corr. to $\phi(\rho\xi_n)^{D(n)}$ mod $J_n^{\times t}$. $n \in \mathbb{Z}_s^1$.

<u>Thm</u> (Factorization) Let $n = q_1 \cdots q_k \in \mathbb{Z}_s^1$. ξ_n be primitive n^{th} root, and $\xi_n = \prod \xi_{q_i}$. We have

$$(R_\phi(\xi_n))_q = 0 \quad \text{for } q \neq q_1 \cdots q_k,$$

and for $q = q_i$,

$$(R_\phi(\xi_n))_{q_i} = l_{q_i}(R_\phi(\xi_n/\xi_{q_i})).$$

$(\xi_n/\xi_{q_i} \in S_{q_i})$

<u>Pf</u>. For $q \neq q_1 \cdots q_k$, q is unr. in J_n/F. $\phi(\rho\xi_n)^{D(n)}$ ~~$R_\phi(\xi_n)$~~ is a unit in J_n, so $(R_\phi(\xi_n))_q = 0$.

Assume $q = q_i$. q is unr. in $J_{n/q}/\mathbb{Q}$. Fr_q: Frobenius over q, in $Gal(J_{n/q}/\mathbb{Q})$. $q \equiv 1 \pmod t$, so $Fr_q \in Gal(J_{n/q}/F)$.

$z \in F^\times$ rep. $R_\phi(\xi_n)$. There is $\beta \in J_n^\times$ s.t. $z = \dfrac{\phi(\rho\xi_n)^{D(n)}}{\beta^t}$.

We want $(z)_q$. $\mathfrak{q} | q$ in F, $\mathfrak{q}' | \mathfrak{q}$ in J_n

Then,

$$(R_\phi(\xi_n))_q = \sum_{\mathfrak{q}|q} \frac{t}{1-q} c_{\mathfrak{q}'} \cdot \mathfrak{q} \pmod{tI_q}$$

$c_{\mathfrak{q}'} = \text{ord}_{\mathfrak{q}'}(\beta)$

Let $\pi_{\mathfrak{q}}$ be local parameter of J_q above $\mathfrak{q}$. Then $\pi_{\mathfrak{q}}$ is also local parameter at $\mathfrak{q}'$.

$$\beta = \pi_{\mathfrak{q}}^{c_{\mathfrak{q}'}} \cdot \alpha_{\mathfrak{q}} \quad , \ \mathrm{ord}_{\mathfrak{q}'}(\alpha_{\mathfrak{q}}) = 0.$$

We have $\alpha_{\mathfrak{q}}^{1-\tau_q} \equiv 1 \pmod{\mathfrak{q}}$ because $J_n/J_{n/q}$ is T.R.

$\gamma_{\mathfrak{q}} := \pi_{\mathfrak{q}}^{1-\tau_q}$. computation shows

$$\beta^{1-\tau_q} \equiv \gamma_q^{c_{q'}} \pmod{q'},$$

so $c_{\mathfrak{q}'}$ is the $\mathfrak{q}$-component of $l_q'(\beta^{1-\tau_q})$.

<u>Computing $\beta^{1-\tau_q}$</u>:

$$\beta^{(1-\tau_q)t} = \phi(\rho\xi_n)^{(N(q)+1-q)D(n/q)},$$

Now, (E2) $\phi(\rho\xi_n)^{N(q)} = \phi(\rho\xi_n/\xi_q)^{Fr_q - 1}$

Let $z_q = \phi(\rho\xi_n/\xi_q)^{D(n/q)}/\beta_q^t \in F^\times$ be prime to q.

z_q represents $R\phi(\xi_n/\xi_q)$. $Fr_q \in \mathrm{Gal}(J_{n/q}/\mathbb{Q})$ fixes F,

so

$$\phi(\rho\xi_n/\xi_q)^{D(n/q)\cdot(Fr_q - 1)} = \beta_q^{t(Fr_q-1)}.$$

$$\beta^{(1-\tau_q)t} = \beta_q^{(Fr_q-1)t} \cdot \phi(\rho\xi_n)^{(1-q)D(n/q)}$$

$$\cancel{\beta(1-\tau} \quad \beta^{(1-\tau_q)} = \beta_q^{(Fr_q-1)} \phi(\rho\xi_n)^{\left(\frac{1-q}{t}\right)D(n/q)}.$$

(E3) $\phi(\rho\xi_n) \equiv \phi(\rho\xi_n/\xi_q) \pmod{\mathfrak{q}'}$.

So,

$$\beta^{1-\tau_q} \equiv \beta_q^{q-1} \cdot \phi(\rho\xi_n/\xi_q)^{D(n/q)\left(\frac{1-q}{t}\right)} \pmod{\mathfrak{q}'}.$$

$$\equiv z_q^{\frac{1-q}{t}} \pmod{\mathfrak{q}'}.$$

$c_{q'}$: q component of $\ell_q'(\beta^{1-\tau_q})$

$= q$ comp. of $\ell_q'\left(z_q^{\left(\frac{1-q}{t}\right)}\right)$

$= q$ comp. of $\ell_q\left(R_\phi(\xi_n / \xi_q)\right) \times \left(\frac{1-q}{t}\right)$.