Classical Iwasawa Theory

Fix an odd prime p (to simplify things).

Notation: μ_m = the group of m^{th} roots of unity in $\bar{\mathbb{Q}}$

$K_n = \mathbb{Q}(\mu_{p^{n+1}})$, $K_0 = \mathbb{Q}(\mu_p)$.

$Cl(K_n)$ = ideal class group

$A_n = Cl(K_n)_p$ = Sylow p-subgroup of $Cl(K_n)$

$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \cdots$

Let $K_\infty = \bigcup_{n=0}^{\infty} K_n = \mathbb{Q}(\mu_{p^\infty})$.

Themes:

- Behavior of the A_n's as n varies is related to the behavior of $\zeta(1-m)$ as m varies, $m \geq 1$.

(Kummer, Herbrand-Ribet, Iwasawa, Mazur-Wiles, ...)

Recall that
$$\zeta(1-m) = \frac{-B_m}{m}$$
where B_m is the m^{th} Bernoulli number.

We begin with the case of $n=0$:

$K_0 = \mathbb{Q}(\mu_p)$

$\Delta = G_0 = Gal(K_0/\mathbb{Q})$

There is a natural isomorphism

$$\omega : \Delta \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$$

given by $\delta \in \Delta$, $\omega(\delta) = \delta|_{\mu_p} \in \mathrm{Aut}(\mu_p) \cong GL_1(\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p^\times$.

As one should think of ω as a 1-dimensional character of Δ.

We also have

$$\mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$$

$$\mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times .$$

There exists a homom.

$$(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}_p^\times$$

which we regard as a homom.

$$\omega : \Delta \to \mathbb{Z}_p^\times .$$

$A_0 = Cl(K_0)_p$ (usually A_0 has exponent p)

Δ acts on A_0 : $A_0 = \oplus A_0^{(\omega^i)}$ where $A_0^{(\omega^i)} = \{ a \in A_0 : \delta(a) = \omega^i(\delta) a \ \ \forall \delta \in \Delta \}$.

The characters of Δ are $\{ \omega^i : 0 \le i < p-1 \}$.

(This decomposition of A_0 is valid as long as A_0 is a $\mathbb{Z}_p[\Delta]$-module.)

$$A_0^{(\omega^0)} = 0$$

$$A_0^{(\omega^1)} = 0$$

Herbrand-Ribet: Assume i is odd and j is even, $j \geq 2$

$i \not\equiv 1 \pmod{p-1}$, $j \not\equiv 0 \pmod{p-1}$, $i+j \equiv 1 \pmod{p-1}$

(i.e., $\omega^i \omega^j = \omega$). Then $A^{(\omega^i)} \neq 0$ iff

$\zeta(1-j) \equiv 0 \pmod{p\mathbb{Z}_p}$ (i.e., p divides the numerator

of $\zeta(1-j)$.)

Kummer Congruences: If $j_1, j_2 \geq 2$, even. If $j_1 \equiv j_2 \not\equiv 0 \pmod{p-1}$,

then $\zeta(1-j_1) \equiv \zeta(1-j_2) \pmod{p\mathbb{Z}_p}$.

Note if $j \equiv 0 \pmod{p-1}$, then $\zeta(1-j)$ has a p in the denominator,

so we are using that if $j \not\equiv 0 \pmod{p-1}$ then $\zeta(1-j) \in \mathbb{Z}_p$.

Example: $p = 37$ $p \mid B_{32}$. So $\zeta(1-32) \equiv 0 \pmod{p\mathbb{Z}_p}$.

So we have $A_0^{(\omega^5)} \neq 0$.

$\zeta(1-j) \equiv 0 \pmod{p\mathbb{Z}_p}$ iff $j \equiv 32 \pmod{p-1}$.

$A_0^{(\omega^i)} = 0$ for all odd i, $i \not\equiv 5 \pmod{p-1}$.

$A_0^{(\omega^i)} = 0$ for all even i.

$\dim_{\mathbb{F}_p}(A_0) = 1$ and so $A_0 \cong A_0^{(\omega^5)} \cong \mathbb{Z}/p\mathbb{Z}$.

Interpretation in terms of Galois extensions of K_0: (still w/ $p = 37$)

Let L_0 = p-Hilbert class field of K_0, $Gal(L_0/K_0) \cong A_0$

$$\begin{tikzcd} L_0 \arrow[d, dash, "\mathbb{Z}/p\mathbb{Z}"] \\ K_0 \arrow[d, dash, "\Delta"] \\ \mathbb{Q} \end{tikzcd}$$

i.e., we have an exact sequence

$$1 \to \mathrm{Gal}(L_0/K_0) \to \mathrm{Gal}(L_0/\mathbb{Q}) \to \Delta \to 1$$

i.e, a group extension.

Δ acts on $\mathrm{Gal}(L_0/K_0)$ by inner automorphisms. Thus,

$\mathrm{Gal}(L_0/K_0) \simeq A_0$ as $\mathbb{Z}_p[\Delta]$-modules.

Δ acts on $\mathrm{Gal}(L_0/K_0) \simeq \mathbb{Z}/p\mathbb{Z}$ by ω^5.

<u>Kummer Theory Interpretation</u>: ($p = 37$ still)

Let $c \in A_0$, $c = \mathrm{cl}(I)$ where I = fractional ideal of $\mathcal{O}_{K_0}$.

$c\,\bar{c} = c_0$ = identity of A_0

We can choose I so that $I\bar{I} = (1)$.

$I^p = (\alpha)$ where $\alpha \in K_0$. We can choose α so that $\alpha\bar{\alpha} = 1$.

We can even choose α so that

$$\alpha(K_0^\times)^p \in \left(K_0^\times/(K_0^\times)^p\right)^{(\omega^5)}$$

Let $M_0 = K_0(\sqrt[p]{\alpha})$. This is unramified away from p.

By Kummer theory we have $\mathrm{Gal}(M_0/K_0) \simeq \mathbb{Z}/p\mathbb{Z}$.

M_0 is Galois over $\mathbb{Q}$.

$$\begin{tikzcd}
M_0 \arrow[d, dash, "\mathbb{Z}/p\mathbb{Z}"] \\
K_0 \arrow[d, dash, "\Delta"] \\
\mathbb{Q}
\end{tikzcd}$$

Δ acts on $\mathrm{Gal}(M_0/K_0)$ by inner automorphisms by $\omega\omega^{-5} = \omega^{32}$

In summary, for $p = 37$ we have

$$\begin{tikzcd}
L_0 \arrow[dr, dash, "\omega^5"'] & & M_0 \arrow[dl, dash, "\omega^{32}"] \arrow[dr, dash] & \\
& K_0 \arrow[dr, dash] \arrow[dd, dash, "\Delta"'] & & M_0^+ \arrow[dl, dash, "\omega^{32}"] \\
& & K_0^+ \arrow[dl, dash] & \\
& \mathbb{Q} & &
\end{tikzcd}$$

$K_0^+ = \mathbb{Q}(\cos(\frac{2\pi}{p}))$ = max. real subfield.

$$\mathrm{Gal}(M_0^+/K_0^+) \simeq \mathbb{Z}/p\mathbb{Z}$$

$$M_0 = M_0^+ K_0 .$$

ω^{32} factors through $\mathrm{Gal}(K_0^+/\mathbb{Q})$

$p = 37$ divides $\zeta(1-32)$ gives fields L_0, M_0 with these Galois actions.

<u>Example:</u> $p = 691$

$p \mid B_{12}$ and $p \mid B_{200}$

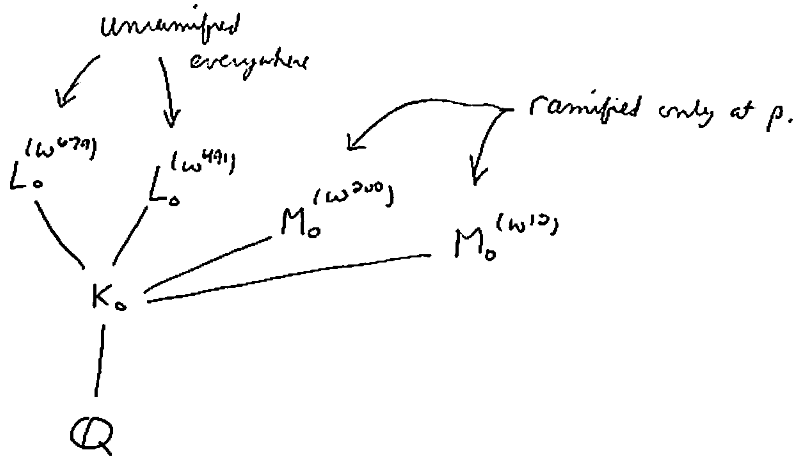
$K_0 = \mathbb{Q}(\mu_p)$

$A_0 = Cl(K_0)_p \simeq A_0^{(\omega^{679})} \oplus A_0^{(\omega^{491})}$

and $A_0^{(\omega^i)} = 0$ for all other ω^i.

$A_0^{(\omega^{679})} \cong \mathbb{Z}/p\mathbb{Z}$.

$A_0^{(\omega^{491})} \cong \mathbb{Z}/p\mathbb{Z}$



<u>Galois Cohomology Interpretation</u>: ($p = 37$ again)

Consider $\mu_p^{\otimes i} = \mathbb{Z}/p\mathbb{Z}$ with $G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acting on $\mu_p^{\otimes i}$

by $G_{\mathbb{Q}} \twoheadrightarrow \Delta \xrightarrow{\omega^i} (\mathbb{Z}/p\mathbb{Z})^\times$

$$H^1(G_{\mathbb{Q}}, \mu_p^{\otimes i}) \underset{\sim}{\xrightarrow{res.}} H^1(G_{K_0}, \mu_p^{\otimes i})^\Delta$$
$$\qquad\qquad\qquad\qquad\qquad \parallel$$
$$\qquad\qquad\qquad\qquad\qquad \mathrm{Hom}(G_{K_0}, \mu_p^{\otimes i})^\Delta$$

$$H^1_{un}(\mathbb{Q}, \mu_p^{\otimes i}) \xrightarrow[\sim]{res} H^1_{un}(K_0, \mu_p^{\otimes i})^{\Delta},$$
$$\parallel$$
$$\mathrm{Hom}_{\Delta}(\mathrm{Gal}(L_0/K_0), \mu_p^{\otimes i})$$

In other words,

$$H^1_{un}(\mathbb{Q}, \mu_p^{\otimes i}) \cong \mathrm{Hom}_{\Delta}(\mathrm{Gal}(L_0/K_0), \mu_p^{\otimes i})$$

However, $\mathrm{Gal}(L_0/K_0) \cong \mu_p^{\otimes 5}$, so

$$H^1_{un}(\mathbb{Q}, \mu_p^{\otimes i}) \simeq \mathrm{Hom}_{\Delta}(\mu_p^{\otimes 5}, \mu_p^{\otimes i}) = \begin{cases} 0 & \text{if } \omega^i \neq \omega^5 \\ \mathbb{Z}/p\mathbb{Z} & \text{if } \omega^i = \omega^5 \end{cases}$$

Let $\Sigma = \{p, \infty\}$. $\quad j$ even

$$H^1_{\Sigma\text{-ram}}(\mathbb{Q}, \mu_p^{\otimes j}) = \begin{cases} 0 & \text{if } \omega^j \neq \omega^{32} \text{ or } \omega^0 \\ \mathbb{Z}/p\mathbb{Z} & \text{if } \omega^j = \omega^{32} \text{ or } \omega^0. \end{cases}$$

<u>Herbrand - Ribet Theorem:</u> With the same setup as in the statement before: is equivalent to

$$H^1_{un}(\mathbb{Q}, \mu_p^{\otimes i}) \neq 0$$

or

$$H^1_{\Sigma\text{-ram}}(\mathbb{Q}, \mu_p^{\otimes j}) \neq 0.$$

Let $G_n = Gal(K_n/\mathbb{Q})$ where we recall $K_n = \mathbb{Q}(\mu_{p^{n+1}})$.

If $g \in G_n$, then $g(\zeta) = \zeta^{a_g}$ for all $\zeta \in \mu_{p^{n+1}}$. Define

$\chi_n : G_n \xrightarrow{\sim} (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ by $\chi_n(g) = a_g + p^{n+1}\mathbb{Z}$, or we could

equivalently say $\chi_n(g) = g|_{\mu_{p^{n+1}}} \in Aut(\mu_{p^{n+1}}) = GL_1(\mathbb{Z}/p^{n+1}\mathbb{Z}) = (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$.

We may also be interested in

(since $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ is cyclic)

$$Hom(G_n, (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times) = \{ \chi_n^i \mid 0 \le i \le p^n(p-1) \}$$

<u>$p=37$:</u> $A_n = Cl(K_n)_p \cong \mathbb{Z}/p^{n+1}\mathbb{Z}$.

$|A_n| = p^{n+1}$.

G_n acts on A_n by a homom. $\varphi_n : G_n \to Aut(A_n) = (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$.

where $\varphi_n = \chi_n^{i_n}$, $0 \le i_n < p^n(p-1)$.

$p | B_{32}$

$(n=0,\ \chi_0 = \omega,\ \varphi_0 = \omega^5,\ G_0 = \Delta)$

$n=1$: $\varphi_1 = \chi_1^{1049}$, $\chi_1\varphi_1^{-1} = \chi_1^{284}$, $p^2 | B_{284}$.

Suppose $m \ge n \ge 0$. We have two maps

$$J_{m/n} : A_n \to A_m$$
$$(cl(I) \to cl(I\mathcal{O}_{K_m}))$$

This map turns out to be injective.

$$N_{m/n} : A_m \to A_n$$
$$(cl(I) \to cl(Nm_{K_m/K_n}(I))).$$

This map is surjective.

The action of G_m on A_m determines the action of G_n on A_n. Greenberg p59.

Hence, $i_m \equiv i_n \pmod{p^n(p-1)}$.

$\equiv i_0 \equiv 5 \pmod{p-1}$. $(p-1 = 36$ still$)$

$\{i_n\}$ converges p-adically.

$$\lim_{n\to\infty} i_n = 13 + 20(37) + 30(37)^2 + \cdots$$

$\shortparallel$

(the unique zero of $\mathcal{L}_p(\omega^{32}, s)$)

$$\begin{tikzcd}
L_n \arrow[dr, dash] & & M_n \arrow[dl, dash] \\
& K_n \arrow[d, dash, "G_n"] & \\
& \mathbb{Q} &
\end{tikzcd}$$

$L_n =$ p-Hilbert class field of K_n

$Gal(L_n/K_n) \cong A_n \simeq \mathbb{Z}/p^{n+1}\mathbb{Z}$

G_n acts on $Gal(L_n/K_n)$ by $\chi_n^{i_n}$

$Gal(M_n/K_n) \simeq \mathbb{Z}/p^{n+1}\mathbb{Z}$

M_n is Σ-ramified where $\Sigma = \{p, \infty\}$.

G_n acts on $Gal(M_n/K_n)$ by $\chi_n \chi_n^{-i_n} = \chi_n^{1-i_n}$.

$K_\infty = \bigcup K_n = \mathbb{Q}(\mu_{p^\infty})$

$G_\infty = Gal(K_\infty/\mathbb{Q}) = \varprojlim G_n$

$\chi_\infty : G_\infty \longrightarrow \mathbb{Z}_p^\times$.

$\chi_\infty(g) = g|_{\mu_{p^\infty}} \in Aut(\mu_{p^\infty}) \simeq \mathbb{Z}_p^\times$.

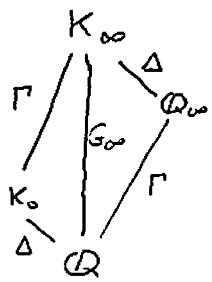
$\mu_{p^\infty} = \varinjlim \mu_{p^n}$, $\mathbb{Z}_p(1) = \varprojlim \mu_{p^n}$.

$\mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)$

Apply χ_∞^{-1}:

$$G_\infty \simeq \Delta \times \Gamma.$$

where $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $\Gamma \simeq 1+p\mathbb{Z}_p \simeq \mathbb{Z}_p$ as topological groups.



$\mathbb{Q}_\infty = \mathbb{Q}^{cycl}$ = cyclotomic $\mathbb{Z}_p$-ext. of $\mathbb{Q}$.

How does G_∞ act on $A_\infty = \varinjlim_n A_n \simeq \mathbb{Q}_p/\mathbb{Z}_p$

or $X_\infty = \varprojlim_n A_n \simeq \mathbb{Z}_p$?

The action is given by $\varphi_\infty : G_\infty \to \mathbb{Z}_p^\times$, where

$\varphi_\infty = \lim_{n\to\infty} \chi^{i_n}$.

$\chi = \chi_\infty = \chi|_\Delta \, \chi|_\Gamma$. where $\chi|_\Delta = \omega$ and $\chi|_\Gamma = \kappa$ (as our definition of κ) $\kappa : \Gamma \xrightarrow{\sim} 1+p\mathbb{Z}_p$.

We can define κ^s for any $s \in \mathbb{Z}_p$.

$$\varphi_\infty = \lim_{n\to\infty} \chi^{i_n} = \lim_{n\to\infty} \omega^{i_n}\kappa^{i_n}$$

$$= \omega^s \kappa^t$$

where $t = \lim_{n\to\infty} i_n \in \mathbb{Z}_p$.

How to study the A_n's:

$X_\infty = \varprojlim_n A_n$ is isomorphic to a Galois group

Let $L_\infty = \bigcup L_n$, so L_∞/K_∞ is a Galois ext. and

$\mathrm{Gal}(L_\infty/K_\infty) \simeq \varprojlim_n \mathrm{Gal}(L_n/K_n)$ where if $m \geq n \geq 0$,

$$\begin{tikzcd}
L_m \arrow[d, dash] \arrow[dr, dash] & \\
L_n \arrow[dr, dash] & K_m \arrow[d, dash] \\
& K_n
\end{tikzcd}$$

$$\begin{tikzcd}
\mathrm{Gal}(L_m/K_m) \arrow[r, "\sim"] \arrow[d, "\mathrm{res}_{m/n}"'] \arrow[dr, phantom, "\circlearrowleft"] & A_m \arrow[d, "N_{m/n}"] \\
\mathrm{Gal}(L_n/K_n) \arrow[r, "\sim"] & A_n
\end{tikzcd}$$

Note that this explains the earlier remark that the norm map is surjective.

$$X_\infty = \varprojlim_n A_n \simeq \varprojlim_n \mathrm{Gal}(L_n/K_n) \simeq \mathrm{Gal}(L_\infty/K_\infty).$$

$(p=37)$

$$\begin{tikzcd}
L_\infty \arrow[dr, dash, "X_\infty"'] & & M_\infty^{(\omega^{32})} \arrow[dl, dash] \\
& K_\infty \arrow[d, dash, "G_\infty \simeq \Delta \times \Gamma"] & \\
& \mathbb{Q} &
\end{tikzcd}$$

$X_\infty = \mathrm{Gal}(L_\infty/K_\infty) \simeq \mathbb{Z}_p \quad (p=37).$

L_∞ = maximal abelian, everywhere unramified, pro-p extension of K_∞

G_∞ acts on X_∞ by $\varphi_\infty = \omega^s \kappa^t$.

$M_\infty^{(\omega^{32})}$ = maximal abelian Σ-ramified pro-p-extension of K_∞. such that Δ acts on $\mathrm{Gal}(M^{(\omega^{32})}/K_\infty)$ by ω^{32}.

$\mathrm{Gal}(M_\infty^{(\omega^{32})}/K_\infty) \simeq \mathbb{Z}_p$. Γ acts on $\mathrm{Gal}(M_\infty^{(\omega^{32})}/K_\infty)$ by

κ^{1-t}.

$\Lambda = \mathbb{Z}_p[[\Gamma]] = \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$ $\qquad$ $\Gamma/\Gamma^{p^n} = \mathrm{Gal}(K_n/K_0)$, $\Gamma = \mathrm{Gal}(K_\infty/K)$

$\Gamma = \overline{\langle\gamma\rangle}$, $\gamma \in \Gamma$, $\gamma|_{K_1} \neq 1$

X_∞ is a Λ-module. In fact, X_∞ is a torsion Λ-module,

$$X_\infty \simeq \Lambda/(\gamma - \kappa^t(\gamma))$$

Back to a general prime p.

$\Gamma \simeq \mathbb{Z}_p$

$\Gamma \supseteq \Gamma^p \supseteq \Gamma^{p^2} \supseteq \cdots$

$\Gamma/\Gamma^{p^n} \simeq \mathbb{Z}/p^n\mathbb{Z}$

$$\begin{array}{c} K_\infty \\ \Big| \, \Gamma \\ K \end{array} \quad \Rightarrow \quad K_\infty = \bigcup_{n \geq 0} K_n \quad \text{with } \mathrm{Gal}(K_n/K) \simeq \Gamma/\Gamma^{p^n}.$$

L_∞ = max. ab. everywhere unram. pro-p ext of K_∞.

$L_\infty = \bigcup_{n\geq 0} L_n$ where L_n = p-Hilbert class field of K_n.

$$X = \mathrm{Gal}(L_\infty/K_\infty) = \varprojlim \mathrm{Gal}(L_n/K_n).$$

Since $\mathrm{Gal}(L_n/K_n) \simeq Cl(K_n)_p$, we would like to get information about these class groups by studying X.

We will work under the following assumption: there is only one prime of K ramified in K_∞/K and that prime is totally ramified in K_∞/K. (it is enough for the prime to be ramified in K_1/K.)

<u>Example:</u> $K = \mathbb{Q}(\mu_p)$, $K_\infty = \mathbb{Q}(\mu_{p^\infty})$, p odd

$$\mathrm{Gal}(K_\infty/K) = \Gamma \simeq 1 + p\mathbb{Z}_p$$

$$\begin{array}{c} K_n = \mathbb{Q}(\mu_{p^{n+1}}) \\ | \\ K = \mathbb{Q}(\mu_p) \\ | \\ \mathbb{Q} \end{array}$$

p totally ramified, so any prime of K over p must be totally ramified in K_n.

Consider again the diagram

$$\begin{tikzcd} L_\infty \arrow[d, dash, "X"] \arrow[dd, dash, bend right, "\mathcal{G}"'] \\ K_\infty \arrow[d, dash, "\Gamma"] \\ K \end{tikzcd}$$

So we have the group extension:

$$1 \to X \to \mathcal{G} \to \Gamma \to 1.$$

Let $\gamma \in \Gamma$ be a topological generator, i.e., $\Gamma = \overline{\langle \gamma \rangle}$.

Pick $\tilde{\gamma} \in \mathcal{G}$ a lifting of γ. If $x \in X$, then $\gamma(x) = \tilde{\gamma} x \tilde{\gamma}^{-1}$.

Let $\mathcal{G}'$ be the commutator subgroup of $\mathcal{G}$.

<u>Claim:</u> $\mathcal{G}' = X^{\gamma - 1} = \{ \gamma(x) x^{-1} \mid x \in X \}$

Note that $\gamma(x) x^{-1} = \tilde{\gamma} x \tilde{\gamma}^{-1} x^{-1} \in \mathcal{G}'$ and so $X^{\gamma-1} \subseteq \mathcal{G}'$.

It is not hard to see that $X^{\gamma-1}$ is a normal subgroup of $\mathcal{G}'$ (use that X is abelian) so we can consider $\mathcal{G}/X^{\gamma-1}$.

$$1 \to X/X^{\gamma-1} \to \mathcal{G}/X^{\gamma-1} \to \Gamma \to 1$$

In fact, this is a central extension. $\mathcal{G}/X^{\gamma-1}$ is abelian, which gives $\mathcal{G}' \subseteq X^{\gamma-1}$ and so we have the claim.

$$\begin{tikzcd}
L_\infty \arrow[d, dash] \arrow[d, bend left=60, dash, "\mathcal{G}' = X^{\gamma-1}"] \arrow[dd, bend right=60, dash, "X"'] \\
L_\infty^{(0)} \arrow[d, dash] \arrow[ddd, bend left=60, dash, "\mathcal{G}/\mathcal{G}' = \text{abelian!}"] \\
K_\infty \arrow[d, dash, "\Gamma"'] \\
K
\end{tikzcd}$$

$L_\infty^{(0)}$ = max. ab ext of K in L_∞

So now we will concentrate on the picture

$$\begin{tikzcd}[column sep=small]
 & L_\infty^{(0)} \arrow[dl, dash, "I"'] \arrow[d, dash] \\
L_0 \arrow[dr, dash] & K_\infty \arrow[d, dash] \\
 & K
\end{tikzcd}$$

(L_0 fixed field of I)

Since there is only one prime ramifying in K_∞/K and $L_\infty^{(0)}/K_\infty$ is unramified, the fact that this group $\mathcal{G}/\mathcal{G}'$ is abelian gives that there is only one inertia group. I.

L_0/K is an abelian, pro-p unramified extension of K.

Hence, $L_0 \subseteq$ p-Hilbert class field of K and so L_0/K is finite. In fact, $L_0 =$ p-Hilbert class field of K.

$$\begin{tikzcd}[column sep=small]
 & L_\infty^{(0)} \arrow[dl, dash, "I"'] \arrow[dr, dash, "H"] & \\
L_0 \arrow[dr, dash] & & K_\infty \arrow[dl, dash, "\Gamma"] \\
 & K &
\end{tikzcd}$$

$I \cap H = \{ id \}$.

$\Rightarrow L_\infty^{(0)} = L_0 K_\infty$

$L_0 \cap K_\infty = K$

$$\mathrm{Gal}(L_\infty^{(0)}/K) \simeq \mathrm{Gal}(L_0/K) \times \Gamma$$

$$\Rightarrow H \simeq \mathrm{Gal}(L_0/K) \simeq Cl(K)_p. = X/X^{\gamma - 1}.$$

$$\begin{tikzcd}
L_\infty \arrow[d, dash, "X"'] \\
K_\infty \arrow[d, dash, "\Gamma^{p^n} = \langle \overline{\gamma^{p^n}} \rangle"] \\
K_n \arrow[d, dash] \\
K \arrow[uu, dash, bend left=60, "\Gamma"]
\end{tikzcd}$$

Our assumption remains valid when we replace K by K_n,

and so

$$Cl(K_n)_p \simeq Gal(L_n/K_n) \simeq X/X^{\gamma^{p^n}-1}.$$

Thus, from X we can recover all the groups $Cl(K_n)_p$.

Switch to additive notation now and let $T = \gamma - 1$, i.e,

$T x = x^{\gamma-1} = \gamma(x) - x = (\gamma-1)x$.

$A_n = Cl(K_n)_p \simeq X/((1+T)^{p^n}-1)X$.

<u>Special Case</u>: Assume $Cl(K)_p = 0$.

This means that $X = TX$.

<u>Claim</u>: This implies $X = 0$. (i.e, $Cl(K_n)_p = 0 \quad \forall n \geq 0$)

$X = TX \Rightarrow X = TX = T^2 X = T^3 X = \cdots$

But X is a pro-p group, abelian.

Assume X is a finite abelian nontrivial p-group.

$$T : X \to X$$
$$x \mapsto (\gamma-1)x$$

If $X \neq 0$, then $\ker T \neq 0 \Rightarrow TX \neq X \Rightarrow T^n X = 0$

for n large enough. So if X is finite we are done.

Now just assume $X \neq 0$ (not necessarily finite anymore)

Pick an open subgroup U of X. Then X/U is a finite p-group.

Hence $T^n X \subseteq U$ for large enough n.

But U is any open subgroup. So $X = TX \Rightarrow X = 0$

because we can take intersections of opens, which is zero.

Example: ① $\mathbb{Q}_\infty/\mathbb{Q}$

$Cl(\mathbb{Q}_n)_p = 0 \quad \forall n.$

② $K_n = \mathbb{Q}(\mu_{p^{n+1}})$

If $Cl(K_0)_p = 0$, then $Cl(K_n)_p = 0 \quad \forall n > 0.$

(p is a regular prime)

Let $\Lambda = \mathbb{Z}_p[[T]]$. This is a complete Noetherian ring, and many other nice properties. $\mathfrak{m} = (p, T)$ = maximal ideal, Λ is compact.

X is a Λ-module. (X is a $\mathbb{Z}_p$-module because it is a pro-p group, and T acts on X and so X is a $\mathbb{Z}_p[T]$-module.) However, in this topology $T^n x \to 0$ as $n \to \infty$ in X, i.e., T is topologically nilpotent and so we can let a power series act on x.)

In fact, X is a f.g. Λ-module. The reason is that X/TX is finite (it corresponds to $Cl(K)_p$). Suppose $x_1, \ldots, x_n \in X$ are chosen so that their images in X/TX generate X/TX as a $\mathbb{Z}_p$-module. Let $Y = \Lambda x_1 + \cdots + \Lambda x_n \subseteq X$. Y is compact because

Λ is. Y is a Λ-submodule of X and $Y + TX = X$

Consider $Z = X/Y$. We have $TZ = Z$. Hence $Z = 0$ as was shown before and so $X = Y$.

Moreover, X is a f.g. torsion module. The reason:

$$\Lambda/T \simeq \mathbb{Z}_p$$

$$rk_\Lambda(X) \leq rk_{\Lambda/T}(X/TX)$$

One uses a localization arg. to get, but X/TX is finite and so $rk_{\Lambda/T}(X/TX) = 0 \Rightarrow X$ is Λ-torsion.

__Theorem (Iwasawa '59):__ Let K_∞/K be an arbitrary $\mathbb{Z}_p$-extension. Then there exist integers λ, μ, ν s.t.

$$|Cl(K_n)_p| = p^{\lambda n + \mu p^n + \nu}$$

for n sufficiently large.

__Definition of λ and μ:__

Let $X = Gal(L_\infty/K_\infty)$ where L_∞ is the max. ab unram. pro-p extension of K_∞. (or $X = \varprojlim_n A_n$ where $A_n = Cl(K_n)_p$.)

X is a f.g. torsion Λ-module. One can prove that $Y = X_{\mathbb{Z}_p\text{-torsion}}$ has bounded exponent ($Y = X[p^t]$ for some $t \geq 0$) and $X/Y \simeq \mathbb{Z}_p^{\lambda}$.

$\Lambda/p\Lambda \simeq \mathbb{F}_p[[T]] = \text{PID}$

$X[p] \simeq (\Lambda/p\Lambda)^{\mu_1} \times (\text{finite})$

$X[p^2]/X[p] \simeq (\Lambda/p\Lambda)^{\mu_2} \times (\text{finite})$

$$\mu = \sum_{i=1}^{t} rk_{\Lambda/p\Lambda}\left(X[p^i]/X[p^{i-1}] \right)$$

λ = can be defined as the dimension of $X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

$A_\infty = \lim_{n \to \infty} A_n$

(assume $\mu = 0$)

Then $A_\infty \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$ and $X/Y \simeq \mathbb{Z}_p^\lambda$. Thus,

$X \simeq \mathbb{Z}_p^\lambda \times (\text{finite})$

<u>Conjecture (Iwasawa)</u>: Let $K_\infty = K_\infty^{cycl.}$. Then $\mu = \mu(K_\infty/K) = 0$.

<u>Thm (Ferrero-Washington)</u>: This conjecture is true if K is an abelian extension of $\mathbb{Q}$.

If $\mu = 0$, then $A_n \underset{\uparrow}{\approx} (\mathbb{Z}/p^n\mathbb{Z})^\lambda$

roughly isom. ← Can be off by kernel and cokernel that are bounded.

$\mu > 0 \Leftrightarrow \dim_{\mathbb{Z}/p\mathbb{Z}}(A_n[p]) \geq p^n - \text{constant}$ for all n.

<u>Remark</u>: $\mu(K_\infty/K) > 0$ is possible if $K_\infty \neq K_\infty^{cycl}$. This can happen

possibly if there exists ∞'ly many primes v of K which split completely in K_∞/K. Greenberg pg 20

Let K be any number field. Let $\tilde{K}$ be the compositum of all $\mathbb{Z}_p$-extensions of K. One has

$$\mathrm{Gal}(\tilde{K}/K) \simeq \mathbb{Z}_p^{r_2+1+\delta}$$

where $r_2 = \#$ of complex primes of K and $\delta \geq 0$.

<u>Leopoldt conj:</u> $\delta = 0$. (Known when the extension $\mathrm{Gal}(K/\mathbb{Q})$ is abelian)

Suppose $r_2 > 0$ and p splits completely in $K/\mathbb{Q}$ and $K_\infty = K_\infty^{cycl}$.

$$\begin{tikzcd}
L_\infty \arrow[dr, dash] \arrow[dd, dash, "X"'] & \\
& \tilde{K} \arrow[dl, dash, "\mathbb{Z}_p^{r_2+\delta}"] \\
K_\infty \arrow[d, dash, "\Gamma"] & \\
K &
\end{tikzcd}$$

<u>Claim:</u> $\tilde{K} \subseteq L_\infty$.

Hence $\lambda = \mathrm{cork}_{\mathbb{Z}_p} X \geq r_2$.

Let $\wp$ be a prime of K lying over p. We have $K_\wp = \mathbb{Q}_p$

and

$$\begin{array}{c} \tilde{K}_{\wp} \\ | \\ (K_\infty^{cycl})_{\wp} = \mathbb{Q}_p^{cycl} \\ | \\ K_{\wp} \simeq \mathbb{Q}_p \end{array}$$

$$\mathrm{Gal}(\tilde{K}_{\wp}/K_{\wp}) \cong \mathbb{Z}_p^2$$

$$\begin{tikzcd}
 & \mathbb{Q}_p^{unr}\mathbb{Q}_p^{cycl} \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "\mathbb{Z}_p^2"] & \\
\mathbb{Q}_p^{unr} \arrow[dr, dash, "\mathbb{Z}_p"'] & & \mathbb{Q}_p^{cycl} \arrow[dl, dash, "\mathbb{Z}_p"] \\
 & \mathbb{Q}_p &
\end{tikzcd}$$

local CFT

$$\mathrm{Gal}(\tilde{K}_{\wp}/K_{\wp}) \simeq \mathbb{Z}_p^2 \Rightarrow \tilde{K}_p \subseteq \mathbb{Q}_p^{unr}\mathbb{Q}_p^{cycl}.$$

$$\begin{array}{ccc} \tilde{K}_p & \subseteq & \mathbb{Q}_p^{unr}\mathbb{Q}_p^{cycl} \\ \cup| & & \cup| \\ \mathbb{Q}_p^{cycl} & & \mathbb{Q}_p^{cycl} \end{array} \quad \leftarrow \text{unramified}$$

$\rightarrow$ $\tilde{K}_{\wp}/\mathbb{Q}_p^{cycl}$ is unramified. $\Rightarrow \lambda \geq r_2$.

Suppose now $r_2 = 0$, i.e., K is totally real. Leopoldt's conjecture says

$\tilde{K} = K_\infty^{cycl}$.

<u>Conjecture</u>: $\lambda(K_\infty/K) = 0$. (and $\mu(K_\infty/K) = 0$)

$\Rightarrow$ X is a finite group.

$X = \varprojlim_n A_n \Rightarrow |A_n|$ is bounded.

Let $K = \mathbb{Q}(\sqrt{254})$ and $p = 3$. $A_0 = \mathbb{Z}/3\mathbb{Z}$, $A_1 = \mathbb{Z}/9\mathbb{Z}$, $A_2 = \mathbb{Z}/27\mathbb{Z}$,

$A_4 \simeq \mathbb{Z}/3^5\mathbb{Z}$, $A_5 \simeq \mathbb{Z}/3^5\mathbb{Z}$, $A_6 \simeq \mathbb{Z}/3^5\mathbb{Z}$, ...

$A_n \simeq \mathbb{Z}/3^5\mathbb{Z}$ for all $n \geq 4$. In fact, one has

$\varinjlim_n A_n = 0$, $X = \varprojlim_n A_n \simeq \mathbb{Z}/3^5\mathbb{Z}$, $\lambda = 0$, $\mu = 0$.

We now give a sketch of the proof of Iwasawa's theorem under the following simplifying assumptions: Assume that only one prime is ramified in K_∞/K and that it is totally ramified. Assume $X \simeq \mathbb{Z}_p^\lambda$.

We saw before that $A_n \simeq X/(\gamma^{p^n}-1)X$ for all n.

$$\left| X/(\gamma^{p^n}-1)X \right| \sim \det(\gamma^{p^n}-1 : X \to X)$$

up to p-adic unit

$\sim$ product of eigenvalues of $\gamma^{p^n}-1$.

Let $\alpha_1, \ldots, \alpha_\lambda$ be the eigenvalues of γ. The eigenvalues of $\gamma - 1$ are $\alpha_1 - 1, \ldots, \alpha_\lambda - 1$.

$|\alpha_i - 1|_p < 1$ (action is topologically nilpotent)

$$\det(\gamma^{p^n} - 1) = \prod_{i=1}^{\lambda} (\alpha_i^{p^n} - 1) \sim \prod_{i=1}^{\lambda} \log_p(\alpha_i^{p^n}) \quad \text{for } n \gg 0$$

$$= (p^n)^\lambda \left(\prod_{i=1}^{\lambda} \log_p \alpha_i \right) \leftarrow \text{indep. of } n!$$

$$= p^{\lambda n + \nu} \quad \text{for some constant } \nu \text{ and all } n \gg 0.$$

Thus, $|A_n| = p^{\lambda n + \nu}$.