Exercise 1.5

We change notation a little bit:
Let $K_n := \mathbb{Q}(\sqrt{n})$ for $n \in \mathbb{Z}$ and K_∞ = compositum of all quadratic ext'n of $\mathbb{Q}$

- Let p be any rational prime and p_∞ be a place of K_∞ above p.
  Then
  $$K_\infty/\mathbb{Q} = \text{splitting field of } \{X^2-n : n\in\mathbb{Z}\} \subseteq \mathbb{Q}[X]$$
  $$\Rightarrow K_\infty, p_\infty/\mathbb{Q}_p = \text{splitting field of } \{X^2-n : n\in\mathbb{Z}\} \subseteq \mathbb{Q}_p[X]$$
  $$\Rightarrow k_{\infty,p_\infty}/\mathbb{F}_p = \text{splitting field of } \underbrace{\{X^2-n : n\in\mathbb{Z}\} \subseteq \mathbb{F}_p[X]}_{(*)}.$$

  Note $(*)$ is a finite set of quadratic polynomials, so $k_{\infty,p_\infty}/\mathbb{F}_p$ is a finite extension, where k_{∞,p_∞} is the residue field of K_∞ at p_∞. Therefore, for any finite subextension $\mathbb{Q} \subseteq L \subseteq K_\infty$, let $p_L := p_\infty \cap L$, then the residue field extension $k_{L,p_L}/\mathbb{F}_p$ is finite of degree less than $[k_{\infty,p_\infty}:\mathbb{F}_p]$

- We now prove $E(K_\infty)_{tor}$ is finite. Suppose not, then for any $N>0$, $\exists$ a sequence of distinct points
  $$P_1 \in E(K_\infty)[m_1], \cdots, P_N \in E(K_\infty)[m_N], \quad m_i > 0.$$
  Then $\exists$ a finite subextension $\mathbb{Q} \subseteq L \subseteq K_\infty$ s.t.
  $$P_i \in E(L)[m] \quad \text{for a common } m = m_1 \cdots m_n.$$
  We find a "good" prime $\mathfrak{L}$ such that
  - E has good reduction at $\mathfrak{L}$
  - $\mathfrak{L} \nmid m$. (actually any $\mathfrak{L} + mN_E$ works)

  Then by [Silverman, VII.1.4], there is an injection
  $$E(L)[m] \hookrightarrow \tilde{E}(k_{L,\mathfrak{L}}) = E$$

Step 1:
We fix a priori a prime $\mathfrak{L}$ such that E is good reduction at $\mathfrak{L}$.
Let $P \in E(K_\infty)_{tor}$, then $\exists$ a finite subextension $\mathbb{Q} \subseteq L \subseteq K_\infty$ s.t. $P \in E(L)[m]$.
By [Silverman, VII.1.4], we have an injection
$$E(L)[m] \hookrightarrow \underbrace{\tilde{E}(k_{L,\mathfrak{L}})[m]}_{\text{of size bounded by } \#\tilde{E}(k_{\infty,\mathfrak{L}_\infty}) =: M \text{ independent of } L}.$$
Hence for m sufficiently large (indep of L) s.t. $m\tilde{E}(k_{\infty,\mathfrak{L}_\infty}) = 0$, (eg: $m \geq M$)

we see $E(L)[m] = 0$. This implies that $E(K_\infty)_{tor}$ has no torsion point of order m for $m \geq M$. //

Step 2. So it suffices to deal with "small m".

We start with a large prime p such that

1° E has good reduction at p

2° $p \nmid m$ for all $m < M$, for M in **Step 1**

We are now ready to show that $E(K_\infty)_{tor}$ is finite. Suppose not, then for any $N > 0$, $\exists$ a sequence of distinct nonzero points

$$P_1 \in E(K_\infty)[m_1], \cdots, P_N \in E(K_\infty)[m_N], \quad m_i < M \text{ for } i = 1, \cdots, N.$$

Then $\exists$ a finite subextension $\mathbb{Q} \subseteq L \subseteq K_\infty$ s.t.

$$P_i \in E(L)[m], \quad m = m_1 \cdots m_N.$$

We invoke [Silverman, VII.1.4] again for prime p, we see since $p \nmid m$,

$$E(L)[m] \hookrightarrow \underbrace{\tilde{E}(k_{L,\mathfrak{p}_L})}_{\text{size bounded by } \#\tilde{E}(k_{\infty,\mathfrak{p}_\infty})}$$

It is then impossible for $N > \#\tilde{E}(k_{\infty,\mathfrak{p}_\infty})$. //

So we have finished the proof. □

Exercise 1.6

Let $E/\mathbb{Q}$ be a fixed elliptic curve with Weierstrass equation

$$y^2 = f(x), \quad f(x) = x^3 + Ax + B \in \mathbb{Q}[x].$$

Let p be a rational prime and consider the point $Q_p := (p, \sqrt{f(\frac{1}{p})}) \in E(F_p)$ where $F_p := \mathbb{Q}(\sqrt{f(\frac{1}{p})})$ is an quadratic extension of $\mathbb{Q}$. More carefully, as

$$f(\tfrac{1}{p}) = \frac{1}{p^3} + \frac{A}{p} + B = \frac{1}{p^4}(1 + Ap^2 + Bp^3)p$$

we see $Q_p = (p, \frac{1}{p^2}\sqrt{p(1+Ap^2+Bp^3)}) \in E(F_p)$ with $F_p = \mathbb{Q}(\sqrt{p(1+Ap^2+Bp^3)})$.

(a) For p sufficiently large (say $p > C_1$), $Q_p \in E(F_p) \setminus E(\mathbb{Q})$. Indeed, suppose $Q_p \in E(\mathbb{Q})$, then $p(1+Ap^2+Bp^3)$ is a square, which implies that $Q_p \in E(\mathbb{Z})$ and further more by looking at the degree (power) of p, (?) in fact $Q_p \in E(\mathbb{Z})$ then. But by Siegal's finiteness theorem of integral points, $\#E(\mathbb{Z})$ is finite. So for sufficiently large prime p, $Q_p \in E(F_p) \setminus E(\mathbb{Q})$.

(b) We then show, for p sufficiently large, (say $p > C_2$), $E(F_p)_{tor} = E(\mathbb{Q})_{tor}$. Following Greenberg's note, I guess we need:

1° p is ramified in F_p: this is clear.

2° Then we let p sufficiently large such that E has good reduction at p (for example, $p >$ conductor of E). Then for $m \nmid p$, we have injections horizontally by [Silverman, VII.1.4]:

$$\begin{array}{ccc} E(\mathbb{Q})[m] & \hookrightarrow & \tilde{E}(\mathbb{F}_p) \\ \downarrow & & \| \text{ by } 1° \\ E(F_p)[m] & \hookrightarrow & \tilde{E}(\mathbb{F}_p) \end{array}$$

Then how does this imply $E(\mathbb{Q})[m] = E(F_p)[m]$?

3° For p-primary part, we take p sufficiently large such that $E(F_p)[p^\infty] = 0$. This can be done since we have a uniform upper bound for $E(K)_{tor}$ for any quadratic extn of K, by Mazel

(See for example : [Silverman, VIII.5.1]).

(c) Then granting (b), by taking $p > \max\{C_1, C_2\}$, we see $Q_p \in E(\mathbb{F}_p) \setminus E(\mathbb{Q})$ and hence a point of infinite order in $E(\mathbb{F}_p)$ but not in $E(\mathbb{Q})$. This shows $E(\mathbb{F}_p)$ has $\mathbb{Z}$-rank greater than that of $E(\mathbb{Q})$. □

Remark : In general it can be shown that :

Fact (arXiv: 1209.0933) : If E is an elliptic curve over a number field K and $m \geq 2$ is an integer, then

$$\#\{L/K \text{ finite extension} : [L:K] = m,\ rk_{\mathbb{Z}} E(L) > rk_{\mathbb{Z}} E(K)\} = \infty .$$

Actually this theorem is proved by :

- First reduced to case m is a prime number.
- Then by Siegal's theorem and "Hilbert irreducibility theorem" to prove the case $m \geq 5$ a prime number.
- Seperately deal with the ad-hoc case when $m = 2$ or 3. Here this exercise deals with the case $m = 2$, and $m = 3$ case is dealt with similarly, see proof of Corollary 2 in loc.cit. □

Doubt : (?) Can we get inspiration from the proof of Exercise 3.11 ?

Remark : Note that the gap "$E(\mathbb{F}_p)_{tor} = E(\mathbb{Q})_{tor}$" is only used when showing Q_p is a point of infinite order in $E(\mathbb{F}_p)$. We can slightly get rid of the observation in (b) and prove the same thing.

$$\begin{aligned} & Q_p \text{ is of infinite order in } E(\mathbb{F}_p) \\ \Leftarrow\ & \forall\, m \in \mathbb{Z}_{>0},\ mQ_p \neq 0 \text{ in } E(\mathbb{F}_p) \\ \Leftarrow\ & \forall\, m \in \mathbb{Z}_{>0},\ mQ_p \notin E(\mathbb{Q}) . \end{aligned}$$

and the last condition can be checked by computations (not that straightforward), see [Gerhard Grey, Moshe Jarden, "Approx. theory and the rk of AV over large algebraic fields", Lemma 2.1]. □

Remark: We prove $E(F_p)_{tor} = E(\mathbb{Q})_{tor}$ for sufficiently large prime p.

To do this, we consider $Q_p = (p, \sqrt{f(p)}) \in E(F_p)_{tor} \setminus E(\mathbb{Q})_{tor}$. Then as $F_p \cap F_q = \mathbb{Q}$ when $F_p \neq F_q$, we see that $Q_p \notin E(F_q)_{tor}$ if $F_q \neq F_p$.

- Note that there are infinitely many distinct extensions $F_p/\mathbb{Q}$ as p running through all rational primes. Indeed, as we have see previously, p is ramified in F_p. Suppose there are only finitely many distinct extensions $F_p/\mathbb{Q}$, then an infinite number of prmies would ramify in a single $F_p/\mathbb{Q}$, which is absurd.

Now recall in Exercise 1.5 we have shown that $E(K)_{tor}$ is finite where K is the compositum of all quadratic extensions of $\mathbb{Q}$. So we see for $p \gg 0$, $E(F_p)_{tor} = E(\mathbb{Q})_{tor}$ since otherwise we could have infinitely many distinct points $Q_p \in E(F_p)_{tor} \subseteq E(K)_{tor}$.

As desired!

□

Exercise 1.7 (by Luochen Zhao) Recall $K =$ ~~[illegible]~~ a Galois extension of $\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2)^{\oplus n}$.

Exercises here are from Greenberg's Park City notes.
In 1.7, one is asked to prove

$$\mathrm{rank}(E(K)) = \mathrm{rank}(E(\mathbf{Q})) + \sum_F \mathrm{rank}(E(F)/E(\mathbf{Q})). \tag{0.1}$$

By the theory of elementary divisors, $\mathrm{rank}(E(K)/E(\mathbf{Q})) = \mathrm{rank}(E(K)) - \mathrm{rank}(E(\mathbf{Q}))$.
For abelian group L write $L_{\mathbf{Q}} = L \otimes \mathbf{Q}$. Now, we have the natural inclusion

$$i : \bigoplus_F E(F)_{\mathbf{Q}}/E(\mathbf{Q})_{\mathbf{Q}} \to E(K)_{\mathbf{Q}}/E(\mathbf{Q})_{\mathbf{Q}}. \tag{0.2}$$

We prove that the inverse arrow $j : y \mapsto \sum_F \frac{1}{|\mathrm{Gal}(K/F)|} \sum_{\sigma \in \mathrm{Gal}(K/F)} y^\sigma$ is an inverse.

- It is clear that $j \circ i = \mathrm{id}$.
- Counting alternatively, we find for any $y \in E(K)_{\mathbb{Q}}$,

$$\sum_F \frac{1}{|\mathrm{Gal}(K/F)|} \sum_{\sigma \in \mathrm{Gal}(K/F)} y^\sigma \tag{0.3}$$

$$= \frac{1}{2^{n-1}} \left[\sum_{\sigma \in \mathrm{Gal}(K/\mathbf{Q}), \sigma \neq 1} y^\sigma \#\{F \subset K \text{ quadratic}, \sigma|_F = \mathrm{id}\} + y \#\{F \subset K \text{ quadratic}\} \right] \tag{0.4}$$

$$= \frac{2^{n-1}-1}{2^{n-1}} \sum_{\sigma \in \mathrm{Gal}(K/\mathbf{Q}), \sigma \neq 1} y^\sigma + \frac{2^n - 1}{2^{n-1}} y = y \bmod E(\mathbf{Q})_{\mathbf{Q}}. \tag{0.5}$$

merging the two sums into one "$\sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q}), \sigma \neq 1}$".

K / $(\mathbb{Z}/2)^{\oplus(n-1)}$ / F / 2 / $\mathbb{Q}$

Here the second-to-last equality comes from the counting: the number of codimension-1 subspaces of $\mathbf{F}_2^n$ is $2^{n-1} - 1$; the number of quadratic fields fixed by a nontrivial σ correspond to codimension-1 subspaces of $\mathrm{Gal}(K/\mathbf{Q})$ containing σ.

So this shows $i \circ j = \mathrm{id}$.

Therefore, i is an isomorphism. So counting the rank$_{\mathbb{Z}_p}$ on both sides of (0.2) gives the desired result. □

Exercise 1.8

Similar to Exercise 1.5, we let K_∞ = the compositum of all quadratic extensions of $\mathbb{Q}$, let $K_n = \mathbb{Q}(\sqrt{n})$ for $n \in \mathbb{Z}$ and $K^{(n)} = \bigcup_{i=-n}^{n} K_n$. To show $\operatorname{rank}_{\mathbb{Z}} E(K_\infty)$ has to infinite, it suffices to show the sequence $\{\operatorname{rank}_{\mathbb{Z}} E(K^{(n)})\}_{n \in \mathbb{Z}_{>0}}$ tends to infinity as $n \to \infty$.

We invoke Exercise 1.7; since $\operatorname{Gal}(K^{(n)}/K) = (\mathbb{Z}/2\mathbb{Z})^{S_n}$, we have

$$\operatorname{rank}_{\mathbb{Z}} E(K^{(n)}) = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) + \sum_{i=-n}^{n}{}' \operatorname{rank}_{\mathbb{Z}} \left(\frac{E(K_n)}{E(\mathbb{Q})} \right) \qquad \text{—(*)}$$

where "Σ'" we mean choose one representative when $K_n = K_{n'}$ (eg: $n=2$ and $n=8$. $K_2 = K_8 = \mathbb{Q}(\sqrt{2})$, then only one "$K_2$" appears in this sum). Or to write in a more complicated way:

$$\sum_{i=-n}^{n}{}' = \sum_{\underbrace{\{-n \le j \le n : K_i \neq K_j \text{ for any } -n \le i < j\}}_{=: \mathcal{S}_n} \cap \{\underbrace{-n \le j \le n : [K_j : K] = 2}_{\text{i.e. } j \text{ is not a square}}\}}$$

with S_n summands)

By Exercise 1.6, there are infinitely many quadratic fields F such that $\operatorname{rank}_{\mathbb{Z}} E(F) > \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$. This implies $\operatorname{rank}_{\mathbb{Z}} E(K^{(n)}) \to \infty$ by gazing at (*) for sufficiently long time. Indeed to write more concisely,

$$\begin{aligned} \operatorname{rank}_{\mathbb{Z}} E(K^{(n)}) &\ge \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) + \sum_{i=-n}^{n}{}' \mathbb{1}\left\{ \operatorname{rank}_{\mathbb{Z}} \left(\frac{E(K_n)}{E(\mathbb{Q})} \right) \ge 1 \right\}(i) \\ &= \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) + \#\left\{ i \in \mathcal{S}_n : \operatorname{rank}_{\mathbb{Z}} \left(\frac{E(K_n)}{E(\mathbb{Q})} \right) \ge 1 \right\} \end{aligned}$$

and the latter $\#\{i \in \mathcal{S}_n : \cdots\} \to \infty$ as $n \to \infty$ by Exercise 1.6, so we are done. □

Remark: In Exercise 1.5 we have seen $E(K_\infty)_{\text{tor}}$ is finite. But through Exercise 1.6 to Exercise 1.8, we see $\operatorname{rank}_{\mathbb{Z}} E(K_\infty)$ is infinite, it is a quite interesting phenomenon. □

Exercise 1.9

We use arguments on [Greenberg, PC, p416]: let $n \geq 0$, we start with the layer F_n/F. It is a Galois extension with Galois group isomorphic to $G_n = \mathbb{Z}/p^n$. Then G_n acts on $E(F_n)$ and one can consider the finite dim'l rep. space $E(F_n) \otimes_{\mathbb{Z}} \mathbb{C}$, of dimension $\operatorname{rank}_{\mathbb{Z}} E(F_n)$ over $\mathbb{C}$.

We have a decomposition as a direct sum of irreducible reps

$$E(F_n) \otimes_{\mathbb{Z}} \mathbb{C} \simeq \bigoplus_{\chi \in X(G_n)} V_\chi^{m_\chi(E)}$$

here since G_n is an abelian group, each rep space V_χ is one-dimensional and $m_\chi(E)$ is the multiplicity of χ in $E(F_n) \otimes_{\mathbb{Z}} \mathbb{C}$, $X(G_n)$ is the set of all characters of G_n, i.e. $X(G_n) := \{\chi : G_n \longrightarrow \mathbb{C}^\times$ continuous group homomorphism$\}$.

Then for $\mathbb{1} \in X(G_n)$ the trivial character, $m_{\mathbb{1}}(E) = \operatorname{rank}_{\mathbb{Z}} E(F)$. We then have

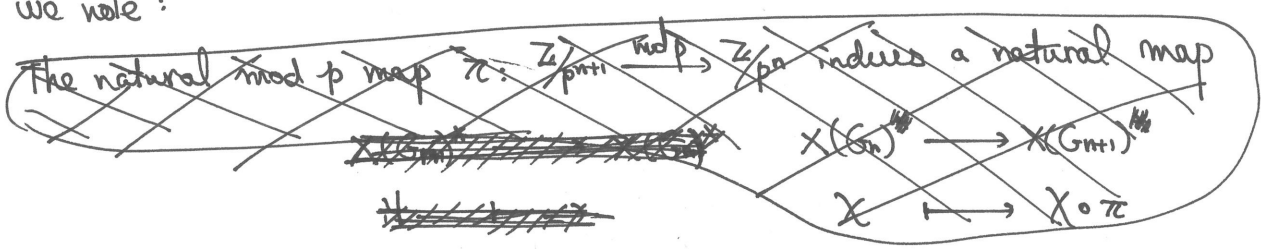
$$\operatorname{rank}_{\mathbb{Z}} E(F_n) = \operatorname{rank}_{\mathbb{Z}} E(F) + \sum_{\chi \in X(G_n)^*} m_\chi(E).$$

Then the entire story above holds for $E(F_{n+1})$, so we get

$$\operatorname{rank}_{\mathbb{Z}} E(F_{n+1}) = \operatorname{rank}_{\mathbb{Z}} E(F) + \sum_{\psi \in X(G_{n+1})^*} m_\psi(E).$$

Then we note:

- The natural mod p map $\pi : \mathbb{Z}/p^{n+1} \xrightarrow{\bmod p} \mathbb{Z}/p^n$ induces a natural map



- $X(G_n)$ is a group, that can be identified with $\mu_{p^n}(\mathbb{C})$. We choose a generator ζ_{p^n} for $\mu_{p^n}(\mathbb{C})$ and $\zeta_{p^{n+1}}$ for $\mu_{p^{n+1}}(\mathbb{C})$ such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. Under this identification, we seperate

$$\sum_{\psi \in X(G_{n+1})^*} m_\psi(E) = \sum_{\psi \in X(G_{n+1})^*_{\text{prim}}} m_\psi(E) + \sum_{\psi \in X(G_{n+1})^*_{\text{non}}} m_\chi(E)$$

where • $X(G_{n+1})^*_{\text{prim}}$ corresponds to those primitive roots of unities in $\mu_{p^{n+1}}(\mathbb{C})$ there are $\varphi(p^{n+1}) = p^n(p-1)$ many of them.

• $X(G_{n+1})^*_{\text{non}}$ corresponds to nonprimitive roots of unities in $\mu_{p^{n+1}}(\mathbb{C})$, it

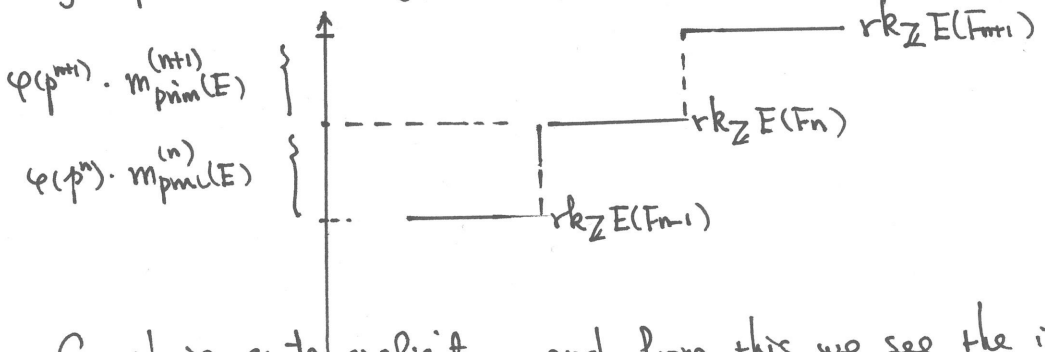
is in 1-1 correspondence with $\mu_{p^n}(\mathbb{C})$

For "primitive characters" (i.e. $\in X(G_{n+1})^*_{prim}$), they share the same multiplicity by Exercise 1.4. For nonprimitive character ψ that corresponding to $\chi \in X(G_n)^*$, we see $m_\chi(E) = m_\psi(E)$ by Exercise 1.3. Therefore,

$$\operatorname{rank}_{\mathbb{Z}} E(F_{n+1}) - \operatorname{rank}_{\mathbb{Z}} E(F_n) = m^{(n+1)}_{prim}(E) \cdot \varphi(p^{n+1}) \equiv 0 \mod \varphi(p^{n+1}),$$

as desired! □

Remark: Clearly $\operatorname{rank}_{\mathbb{Z}} E(F_{n+1}) \geq \operatorname{rank}_{\mathbb{Z}} E(F_n)$, so this exercise measures the jump at each stage:



So it is quite explicit, and from this we see the importance of the "primitive multiplicity" at each stage. There are discussion on p413–414, which are very worthy to read: assume $E/\mathbb{Q}$ has analytic order odd (i.e. $\omega(E(\mathbb{Q}) = -1$), ~~thus~~ of CM given by imaginary quadratic extn F. Then:

- $E/\mathbb{Q}$ good ordinary at p, then for F_∞^{ac}/F, $m^{(n)}_{prim} = 2$, for $n \gg 0$.
- $E/\mathbb{Q}$ good ss at p: $m^{(n)}_{prim} = 0$ or 2 for $n \gg 0$, depending just on the parity of n. (not ass $\omega(E(\mathbb{Q}) = -1$).

This is a more precise version of saying $\operatorname{rk}_{\mathbb{Z}} E(F_n^{ac})$ is unbounded under the above hypothesis, quite contary to the cyclotomic case, which is bounded. □

Remark: But for cyclotomic tower / line, as

$$\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}_n)) = \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}_{n_0})) \quad \text{for } n \geq n_0$$

can we describe n_0, does it depend on E or n_0? This is the theme of p417-422, with plenty of examples! □

Remark : In [Greenberg, PC, Thm 1.4], Greenberg stated :

Theorem : $E/\mathbb{Q}$, Σ finite set of prmes. Then $\mathrm{rk}_{\mathbb{Z}} E(L)$ is bounded as L varies over all finite abelian extns of $\mathbb{Q}$ unramified outside Σ.

Now we use the setup above to reformulate it :

- Theorem $\Leftarrow$ $m_\chi(E) = 0$ for all but finitely many one-dim characters with conductors only divisible by prmes in Σ. (i.e. $K_\chi/\mathbb{Q}$ unr. outside Σ)

  $\Uparrow$ Kato's observation (his side of IMC).

  $L(E/\mathbb{Q}, \chi, 1) \neq 0$

  and Rohrlich showed "$L(E/\mathbb{Q}, \chi, 1) \neq 0$" for a.e. all such characters χ in his "cyclotomic paper". (So at least we have seen the importance of Rohrlich's work on cyclotomic line?).

The anticyclotomic paper of Rohrlich is more complicated :

- $E/\mathbb{Q}$ with CM given by $\mathcal{O}_K \subseteq$ ring of integer K (so class number of K is one).

  Then consider K_∞^{ac}/K at a single prmie $\mathfrak{p}$. Then directly consider

$$E(K_\infty^{ac}) \otimes_{\mathcal{O}_K} \mathbb{C} =: V$$

  then $\mathrm{Gal}(K_\infty^{ac}/K) = \Gamma^{ac}$ acts on V.

  Check : V as a complex rep of $\Gamma^{ac} = \mathbb{Z}_p$ is admissible. Hence

$$V = \bigoplus_\rho V(\rho)$$

  with ρ distinct characters of $\mathrm{Gal}(K_\infty^{ac}/K)$ and $V(\rho)$ finite dim'l subspace of V on which $\mathrm{Gal}(K_\infty^{ac}/K)$ acts via ρ. The question is : $\dim_{\mathbb{C}} V(\rho) = ?$.

  $\Uparrow$ clue in Rohrlich's introduction

Rovich's main theorem | $\mathrm{ord}_{s=1} L(s,\chi) = \begin{cases} 0 & \text{if } W(\chi) = 1 \\ 1 & \text{if } W(\chi) = -1 \end{cases}$ ← new phenomenon in anticyclotomic case.

(for a.e. characters χ in "$\mathcal{X}$") | "corresponding to cyc. case"

(in Rovich's paper, general anti tower at a finite set of places $\mathcal{P}$, instead of a single "$\mathfrak{p}$".)

Exercise 1.10

(a) We start with $L = F$, i.e. consider only the anticyclotomic $\mathbb{Z}_p$-extension F_∞^{ac}/F.

- Then consider a "good" prime $\mathfrak{q} \in \mathbb{Q}$ such that
  1° E has good reduction @ $\mathfrak{q}$.
  2° $\mathfrak{q}$ remains inert in F. Hence (by "Hint") $\mathfrak{q}$ splits completely in F_∞^{ac}/F.

  The condition in 2° implies that for any n, $\mathfrak{q}_n := \mathfrak{q}_\infty \cap F_n^{ac}$ has residue field isomorphic to $\mathbb{F}_{q^2}$.

  Note: There are infinitely many such good prime $\mathfrak{q}$: indeed, by density theorem, there are infinitely many inert primes in F. Requiring 1° only rules out finitely many of them dividing DN_E, where D is the discriminant of F (so $F = \mathbb{Q}(\sqrt{D})$) and N_E is the conductor of E.

- We first prove that $E(F_\infty^{ac})[m : m \text{ prime to } \mathfrak{q}]$ is finite. This is almost the same argument as Exercise 1.15.1:
  $\forall\, P \in E(F_\infty^{ac})_{tor}$ with order m prime to $\mathfrak{q}$, then $P \in E(F_{n_p}^{ac})[m]$ for a certain layer n_p. By [Silverman, VII.1.4],

$$E(F_{n_p}^{ac})[m] \hookrightarrow \widetilde{E}(k_{\mathfrak{q}_{n_p}}) = \widetilde{E}(\mathbb{F}_{q^2})$$

  (size bounded indep. of n_p)

  Hence $E(F_\infty^{ac})_{tor}[m : m \text{ prime to } \mathfrak{q}]$ is finite. Otherwise $\forall N$, $\exists$ distinct points $P_1, \cdots, P_N \in E(F_\infty^{ac})_{tor}$ of order $m_1, \cdots, m_N$. Then $\exists\, n$ s.t.

$$P_i \in E(F_n^{ac})[m] \quad \text{for all } i = 1, \cdots, N, \quad m = m_1 \cdots m_N.$$

  Hence $\{P_1, \cdots, P_N\} \hookrightarrow \widetilde{E}(\mathbb{F}_{q^2})$. This is impossible if we take $N > \#\widetilde{E}(\mathbb{F}_{q^2})$. //

$m: \mathfrak{g} \mid m$

~~$m \neq \mathfrak{g}$~~

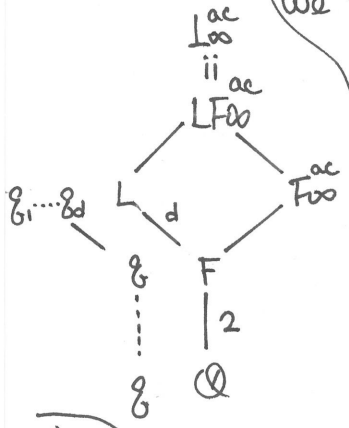
- We then show that $E(F_\infty^{ac})[$~~$\mathfrak{g}$~~$]$ is finite.

  This is easy since there are infinitely many good prmie "$\mathfrak{g}$" (i.e. (odd) primes satisfying $1^\circ - 2^\circ$. So we freely change to another good prmie $\mathfrak{g}'$ and run preirous arguments, to see $E(F_\infty^{ac})[n: n$ prmie to $\mathfrak{g}']$ is finite, and hence the remaing $E(F_\infty^{ac})[m: \mathfrak{g} \mid m]$ is finite, as desired. //

(b) Now we prove the exercise for general finite extension L/F and $L_\infty^{ac} := LF_\infty^{ac}$ as a $\mathbb{Z}_p$-extension of L.

The only problem is the existence (and infinitude) of "good prmies". As we have seen, $\exists$ infinitely many prmies $\mathfrak{g}$ that is inert in F, split completely in F_∞^{ac}. To make them split completely further in L_∞^{ac}, we should require:

(*) $\mathfrak{g}$ is inert in F and for $\mathfrak{g}$ as prmies in F, they splits completely in L.



⚠ to prove the general case, we do not need to pose such strong requirements

So if prmies $\mathfrak{g}$ satisfying (*) are infinite, then ruling out those where E has bad reduction, we have infinitely many prmies s.t.

1° E has good reduction at $\mathfrak{g}$

2° $\mathfrak{g}$ splits completely in L_∞^{ac}/F, regarding $\mathfrak{g}$ as a prmie of F.

We note that $L_\infty^{ac}/F_\infty^{ac}$ is a finite extension of degree $\leq [L:F]$. So for "good prmies" in (a), $\mathfrak{g}$ splits completely in F_∞^{ac}, hence the residue field of $\mathfrak{g}_\infty$ is the finite field $\mathbb{F}_{\mathfrak{g}^2}$. Taking a step forward, for prmies $\widetilde{\mathfrak{g}}_\infty$ of L_∞^{ac} above $\mathfrak{g}_\infty$, it has residue field contained in $\mathbb{F}_{\mathfrak{g}^{2[L:F]}}$

Then we can run the arguments in (a) by replacing F_n^{ac} by L_n^{ac}, F_∞^{ac} by L_∞^{ac} and $\widetilde{E}(\mathbb{F}_{\mathfrak{g}^2})$ by $\widetilde{E}(\mathbb{F}_{\mathfrak{g}^{2[L:F]}})$. //

□

On Iwasawa theory of elliptic curves in $\mathrm{PGL}_2(\mathbb{Z}_p)$-extension

Asked 1 month ago Modified 25 days ago Viewed 224 times

Let E be an elliptic curve over the rationals $\mathbb{Q}$. We consider the Galois representation attached to E by acting on its p-adic Tate module $T_p(E)$,

$$\rho_E : G_K \to \mathrm{Aut}(T_p(E)) \cong \mathrm{GL}_2(\mathbb{Z}_p).$$

Then it cuts out a field $M := \overline{\mathbb{Q}}^{\ker(\rho_E)}$, whose Galois group over $\mathbb{Q}$ is isomorphic to the image of ρ_E. A theorem of Serre tells us that if E has no CM, then $\mathrm{im}(\rho_E)$ is a finite index subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ and strictly equals to $\mathrm{GL}_2(\mathbb{Z}_p)$ for all but finitely many primes p. So for simplicity, we take sufficiently large odd prime p to guarantee ρ_E has full image.

Further $\widetilde{\rho_E} : G_K \to \mathrm{PGL}_2(\mathbb{Z}_p)$. Then similarly consider $K := \overline{\mathbb{Q}}^{\ker(\widetilde{\rho_E})}$. We assume E has no CM and p sufficiently large so that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{Z}_p)$.

Ultimate Goal: The group of torsion points $E(K)_{\mathrm{tors}}$ is a finite group.

A crucial step in proving this (from my naive thought) is to ensure that

Claim 1: there exist infinitely many primes "good primes" q such that the residue field for any prime of K lying above q is finite.

This post is asking how to prove (or disprove) this boldface claim 1?

My "attempt" is to imitate the proof of the following claim in the anticyclotomic $\mathbb{Z}_p$-extension case.

Claim 2: Let F be an imaginary quadratic field and F_∞^{ac} is its anticyclotomic $\mathbb{Z}_p$-extension. Then for any prime of F which is inert in $F/\mathbb{Q}$ must split completely in F_∞^{ac}/F.

Then since there are infinitely many inert primes in F (by density arguments), we have infinitely many primes that "has finite residue field in F_∞^{ac}".

The proof of Claim 2 may date back to Iwasawa in the second section of his article "*On the μ-invariants of $\mathbb{Z}_\ell$-extensions (1973)*". A sketch of proof goes like this:

> Let q be a prime coprime to p that is inert in F, write $\mathfrak{q}$ for the unique prime of F lying above q, then $\mathfrak{q}$ is unramified in the n-th layer F_n^{ac}. Let $\mathfrak{q}_n$ be a prime of F_n^{ac} lying above $\mathfrak{q}$ and Z_n be the decomposition group of it for the Galois extension

$F_n^{\mathrm{ac}}/\mathbb{Q}$. Then since q is unramified in F_n^{ac} and is inert in F, Z_n is a cyclic group of $G_n := \mathrm{Gal}(F_n^{\mathrm{ac}}/\mathbb{Q})$ such that $G_n = Z_n H_n$, where $H_n := \mathrm{Gal}(F_n^{\mathrm{ac}}/F)$. As G_n is a dihedral group of order $2p^n$, it follows that Z_n is a cyclic group of order two satisfying $Z_n \cap H_n = 1$. However, $Z_n \cap H_n$ is nothing but the decomposition group of $\mathfrak{q}_n$ for the extension F_n^{ac}/F, hence $\mathfrak{q}$ splits completely in F_n^{ac}.

Then to imitate the proof above, we need to know the parallel facts on general $\mathrm{PGL}_2(\mathbb{Z}_p)$-extensions $K/\mathbb{Q}$, for example:

1. Specify all intermediate fields of the $\mathrm{PGL}_2(\mathbb{Z}_p)$-extension $K/\mathbb{Q}$. This is equivalent to classifying all closed subgroups of $\mathrm{PGL}_2(\mathbb{Z}_p)$ and figuring out which of them are open.

   Maybe we can try some congruence subgroups? Let Γ_n be the group of matrices in $\mathrm{GL}_2(\mathbb{Z}_p)$ that are congruence to identity matrix modulo p^n, and let $\overline{\Gamma_n}$ be its image of $\mathrm{PGL}_2(\mathbb{Z}_p)$. Do these groups work and are these all such subgroups? (I got hints from here.)

2. The properties of the Galois groups of intermediate fields are good for us to run a similar argument as the anticyclotomic case. In this process, we hope to get a sufficient condition $(\star)$ for such "good primes" (that satisfying Claim 1).

   Follow Greenberg's hint, maybe a common property for finite dihedral groups and $\mathrm{PGL}_2(\mathbb{Z}_p)$ is that g and g^{-1} are conjugate for any group element g. Unfortunately, I cannot see how this property is used in the above proof of anticyclotomic case either.

3. There are infinitely many primes satisfying the sufficient condition $(\star)$ in 2.

   Following Greenberg's hint, I guess that the primes q such that E has good supersingular reduction satisfies the abstract sufficient condition $(\star)$. Then a result of N. Elkies shows that there are infinitely many good supersingular primes. Yet I cannot see how such good supersingular properties are used in the abstract discussion of $\mathrm{PGL}_2(\mathbb{Z}_p)$-extensions. Since I am not able to do 2, figuring out 3 is impossible.

So though there is a rough three-step roadmap, I got stuck on each step. So I am here to ask if there is any way out.

Some further remarks:

- This entire problem is motivated by solving Exercise 1.12 of Ralph Greenberg's IAS/Park City note "*Introduction to Iwasawa Theory for Elliptic Curves*". The hints above by Greenberg is taken from here.

- The **Claim 2** seems to work for anticyclotomic $\mathbb{Z}_p$-extension $\mathcal{F}_\infty^{\mathrm{ac}}$ for any CM field $\mathcal{F}/\mathcal{F}^+$.
- Even if all the problems in this post are solved, we still cannot get the full proof of Greenberg's Exercise 1.12 that $E(K)_{\mathrm{tors}}$ is finite since we haven't touched the CM elliptic curves. An exercise in Silverman's book tells us that in this case, ρ_E has abelian image in $\mathrm{GL}_2(\mathbb{Z}_p)$, and hence $\widetilde{\rho_E}$ has abelian image in $\mathrm{PGL}_2(\mathbb{Z}_p)$. Then in this CM elliptic curve case, it seems that we need a classification of abelian subgroups of $\mathrm{PGL}_2(\mathbb{Z}_p)$ as "Step 0" and try to run the argument above.

Or am I so stupid that missed some easy solution to this exercise? Actually, I feel like I am quite good at making things unnecessarily complicated and as a result, obtaining nothing valuable during my Ph.D. study up to now. Quite frustrated. :(

So sorry for such a long post, and thank you all for commenting and answering! :)

EDIT: Even Further Remarks: I found Greenberg's Exercise 1.16 was focusing on the CM case.

- In Greenberg's Exercise 1.16, he considered a particular elliptic curve $y^2 = x^3 - x$ with CM $\mathbb{Z}[\sqrt{-1}]$. Let $F = \mathbb{Q}(\sqrt{-1})$. Then he asked the reader to show K contains F_∞^{ac} and $[K : F_\infty^{\mathrm{ac}}] < \infty$. This example (though I am still trying to prove) may inspire us to show that maybe (I am not sure at all) K contains an anticyclotomic extension of finite index and then use the **Claim 2** directly to conclude?
- When searching for references, I found arXiv: 2008.04960, where the authors said in the second paragraph of the introduction that **the $\mathrm{PGL}(2)$-extension does not contain the cyclotomic extension**. This (though still I am trying to prove it) may further provide some evidence on that certain "anticyclotomic line" appears in $K/\mathbb{Q}$?

nt.number-theory elliptic-curves iwasawa-theory

Share Cite Edit Close Delete Flag

edited Nov 22 at 10:38

asked Nov 22 at 5:41

Hetong Xu

2 There exists no $\mathbf{Z}_p$ extension (cyclotomic or anticyclotomic or whatever) contained in a PGL_2 extension, just by elementary group theory: $\mathbf{Z}_p$ is not a quotient of $PGL_2(\mathbf{Z}_p)$. This is precisely *why* the PGL2 extensions are studied: because they are the first obvious example of p-adic Lie extensions which are "essentially" nonabelian, having no nontrivial abelian extensions inside them. – David Loeffler Nov 22 at 14:25

@DavidLoeffler Thank you so much for your comment and sorry for the late reply. I managed to see the group theory fact you mentioned. Then inspired by your comment, I realized that I mixed up the CM case and the non-CM case, which seems to be completely different. In the CM case, the image of ρ_E is an abelian subgroup of $\mathrm{PGL}_2(\mathbb{Z}_p)$, which could be quite small, and as Greenberg pointed out, it contains a F_∞^{ac} "of finite index". (I have somehow managed to show this after struggling for two days, at least for $y^2 = x^3 - x$.) – Hetong Xu Nov 24 at 7:46

... Yet for the non-CM case, the image of ρ_E is (except for finitely many prime p) the entire PGL2, which makes the story completely different. I hope I got this right this time, though still I have no idea how to get the ultimate goal proved. – Hetong Xu Nov 24 at 7:49

1 Answer

Sorted by: Highest score (default)

0

It seems that I have obtained some positive results, but I couldn't believe my "solution" is correct since I haven't completely followed Greenberg's hints.

Throughout, p is an odd prime.

Let's focus on the non-CM case only, and suppose p is sufficiently large so that $\tilde{\rho}_E$ has full image $\mathrm{PGL}_2(\mathbb{Z}_p)$. For "small primes", the image is of finite index in $\mathrm{PGL}_2(\mathbb{Z}_p)$, so it doesn't harm.

Recall that we have the tower of extensions

$$\mathbb{Q} \subseteq K := \overline{\mathbb{Q}}^{\ker \tilde{\rho}_E} \subseteq M := \overline{\mathbb{Q}}^{\ker \rho_E} = \mathbb{Q}(E[p^\infty]).$$

Our goal is to understand $K/\mathbb{Q}$. To imitate the anticyclotomic $\mathbb{Z}_p$-case, we observe that there is a short exact sequence of abstract groups

$$0 \to \mathrm{PSL}_2(\mathbb{Z}_p) \to \mathrm{PGL}_2(\mathbb{Z}_p) \xrightarrow{\det} \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 = \{1,-1\} \to 0,$$

and $\mathrm{PGL}_2(\mathbb{Z}_p) = \mathrm{PSL}_2(\mathbb{Z}_p) \rtimes C_2$, where C_2 is a cyclic group of order two. So we have a quadratic extension $F/\mathbb{Q}$ such that $\mathrm{Gal}(K/F) \cong \mathrm{PSL}_2(\mathbb{Z}_p)$. Actually from the construction we see that F is nothing but the fixed field of $\overline{\mathbb{Q}}$ by $\ker(\det \circ \tilde{\rho}_E)$.

In the $\mathrm{PSL}_2(\mathbb{Z}_p)$-extension K/F, we have many finite subextensions. We consider the quotient $\mathrm{PSL}_2(\mathbb{Z}/p^n)$ of $\mathrm{PSL}_2(\mathbb{Z}_p)$. It gives a finite subextension of F_n of K/F such that

$$\mathrm{Gal}(F_n/K) \cong \mathrm{PSL}_2(\mathbb{Z}/p^n), \quad \mathrm{Gal}(F_n/\mathbb{Q}) \cong \mathrm{PSL}_2(\mathbb{Z}/p^n) \rtimes C_2 \cong \mathrm{PGL}_2(\mathbb{Z}/p^n). \quad (*$$

> **Pity 1**: I still have no idea about the classification of closed/open subgroups of $\mathrm{PSL}_2(\mathbb{Z}_p)$ or $\mathrm{PGL}_2(\mathbb{Z}_p)$. But knowing some of these is sufficient to get this exercise done.

Then the story is similar to the anticyclotomic $\mathbb{Z}_p$-extension. But still, an important property need to be established:

"*Property* $(\dagger)$": Let $\mathfrak{q}$ be a prime of F not lying above p, then $\mathfrak{q}$ is unramified in the $\mathrm{PSL}_2(\mathbb{Z}_p)$-extension K/F.

To imitate the $\mathbb{Z}_p$-extension case, it seems that we still need to know the closed subgroups of $\mathrm{PSL}_2(\mathbb{Z}_p)$. But here note that the extension K/F arises from the elliptic curve E. We use:

Property (Neron-Ogg-Shafarevich): with notations above, $\mathfrak{q}$ is unramified in $F(E[p^\infty])$ if (and only if) E has good reduction at $\mathfrak{q}$.

Then since $K \subseteq M = \mathbb{Q}(E[p^\infty]) \subseteq F(E[p^\infty])$, we see that at least **for prime $\mathfrak{q}$ where E/F has good reduction**, $\mathfrak{q}$ is unramified in K.

> **Pity 2**: I cannot show the "*Property* $(\dagger)$" for abstract $\mathrm{PSL}_2(\mathbb{Z}_p)$-extension of number fields.

Now let q be a rational prime that is

- not equal to p, odd
- inert in $F/\mathbb{Q}$,
- E has good (*not necessarily supersingular*) reduction at q.

then by [Silverman, AEC, Proposition 5.4(a)], for any prime $\mathfrak{q}$ of F over q, E has good reduction at $\mathfrak{q}$, and hence $\mathfrak{q}$ is unramified in K. Obviously there are infinitely many such rational primes q.

Then we are finally ready to run the proof of **Claim 2** quoted in my question, replacing the intermediate fields "F_n^{ac}" there by F_n here. The similar structure of Galois groups in $(*)$ helps us to conclude.

Edit: I was a little bit cheating here. Let me write some details here.

Let $\mathfrak{q}_n/\mathfrak{q}/q$ be the primes in the tower $F_n/F/\mathbb{Q}$. Then since $\mathfrak{q}/q$ is inert and $\mathfrak{q}_n/\mathfrak{q}$ is unramified, the decomposition group $Z(\mathfrak{q}_n/q)$ is cyclic of **even** order. Then by counting $\#\mathrm{PSL}_2(\mathrm{p}^n) = p^{3n-2}(p^2-1)/2$ (citing here), we see that $Z(\mathfrak{q}_n/\mathfrak{q})$ is of order at most $(p^2-1)/2$. (**Here we used the assumption that p is odd**). Hence the ramification index e_n and f_n satisfies $e_n f_n \leq (p^2-1)/2$, which is bounded independent of n. This implies that the residue field of q in K is finite.

Remark: So here is still a little bit difference between the dihedral group case and the PGL_2 case.

I hope that I haven't made mistakes in the proof. Here I would like to add a proof of Prof. David Loeffler's hint that $\mathrm{PGL}_2(\mathbb{Z}_p)$ has no quotient isomorphic to $\mathbb{Z}_p$.

We assume $p \geq 5$. For primes $p = 2$ and $p = 3$, actually I am not quite certain.

Proof: Suppose $\mathrm{PGL}_2(\mathbb{Z}_p) \twoheadrightarrow \mathbb{Z}_p$, then quotienting out $p\mathbb{Z}_p$, we obtain $\mathrm{PGL}_2(\mathbb{F}_p) \twoheadrightarrow \mathbb{F}_p$. This means (by counting the cardinality of the two groups $\mathrm{PGL}_2(\mathbb{F}_p)$ and $\mathrm{PGL}_2(\mathbb{F}_p)$) that we would have a normal subgroup H of $\mathrm{PGL}_2(\mathbb{F}_p)$ of order p^2-1. We show next that this would not happen.

The key is the fact:

Fact of Galois: When $p \geq 5$, $\mathrm{PSL}_2(\mathbb{F}_p)$ is a simple group. (See K. Conrad's note here.)

This is the only place in the proof that we use the assumption $p \geq 5$. Suppose H is a normal subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$, then by the simplicity result of Galois, $H \cap \mathrm{PSL}_2(\mathbb{F}_p)$ would be either trivial or the entire $\mathrm{PSL}_2(\mathbb{F}_p)$.

- If $H \cap \mathrm{PSL}_2(\mathbb{F}_p) = \mathrm{PSL}_2(\mathbb{F}_p)$. Then $H \supseteq \mathrm{PSL}_2(\mathbb{F}_p)$. As $\mathrm{PSL}_2(\mathbb{F}_p)$ is of index two in $\mathrm{PGL}_2(\mathbb{F}_p)$, we see that either $H = \mathrm{PSL}_2(\mathbb{F}_p)$ or $H = \mathrm{PGL}_2(\mathbb{F}_p)$.
- If $H \cap \mathrm{PSL}_2(\mathbb{F}_p) = 1$, then $H \cdot \mathrm{PSL}_2(\mathbb{F}_p) = \mathrm{PGL}_2(\mathbb{F}_p)$. By the second isomorphism theorem,

  $$\mathrm{PGL}_2(\mathbb{F}_p)/H \cong H \cdot \mathrm{PSL}_2(\mathbb{F}_p)/H \cong \mathrm{PSL}_2(\mathbb{F}_p)/H \cap \mathrm{PSL}_2(\mathbb{F}_p) \cong \mathrm{PSL}_2(\mathbb{F}_p).$$

  So H is a normal subgroup of order 2, strictly smaller than $p^2 - 1$.

So we are done.

I doubt if it is correct for $p = 2$. For $p = 3$, maybe it follows form a more direct computation since $\mathrm{PSL}_2(\mathbb{F}_3)$ is just the alternating group A_4.(Again here.)

Share Cite Edit Delete Flag edited Nov 28 at 7:42 answered Nov 25 at 9:05

Hetong Xu

It is very hard to classify open subgroups of PGL_2. In the final part, it should also be true for $p = 2$. – stupid boy Nov 25 at 19:21

Exercise 1.12 We follow Greenberg's (& Wan's) hint to consider the supersingular primes. The subtlety is to show that for supersingular primes $\ell \geq 5$, $\ell \neq p$, the residue field for any prime of K lying above ℓ is finite.

The condition "$\ell \geq 5$" guarantees $a_\ell = 0$ (here a_ℓ is the Hasse invariant of E at ℓ) by Exercise 2.12. Then the Eichler–Shimura relation (or the Hecke polynomial argument) tells us that as endomorphisms,

$$\rho_E(\mathrm{Frob}_\ell)^2 + \ell = 0 \quad \text{in} \quad GL_2(\mathbb{Z}_p)$$

for $\rho_E : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow GL(T_p E) \cong GL_2(\mathbb{Z}_p)$. Then moding the center of $GL_2(\mathbb{Z}_p)$, we see $\overline{\rho_E}(\mathrm{Frob}_\ell)^2 = 1$ in $PGL_2(\mathbb{Z}_p)$.

Now let λ be a place of K above ℓ, and Gal_{K_λ} be the decomposition group, $k_\lambda = \mathcal{O}_K/\lambda$ be the residue field, then there is a commutative diagram

$$(*) \quad \begin{array}{ccc} \mathrm{Gal}_{K_\lambda} & \hookrightarrow & PGL(E[p^\infty]) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(k_\lambda/\mathbb{F}_\ell) & \hookrightarrow & PGL(\widetilde{E}[p^\infty](k)) \end{array} \qquad \text{"local field"}$$

(note that the inertia I_λ acts trivially on $\widetilde{E}[p^\infty](k)$). Then (regard $\mathrm{Frob}_\ell \in G_{K_\lambda}$), we see $\overline{\rho_E}(\mathrm{Frob}_\ell)^2 = 1$, i.e. $\overline{\rho_E}(\mathrm{Frob}_\ell)$ has order 2. Wandering around the diagram $(*)$, we can see that $k_\lambda/\mathbb{F}_\ell$ is indeed of order 2, hence in particular finite, as desired. (?)

□

Doubt (?): Some details need to be added!

Exercise 1.13

Proof: One sees immediately that it suffices to show inductively that for any $n \in \mathbb{Z}_{\geq 0}$,

$$E(F_n)[p] = 0 \quad \text{implies} \quad E(F_{n+1})[p] = 0 .$$

- Suppose otherwise, $E(F_{n+1})[p] \neq 0$. Let Q be a nonzero point in $E(F_{n+1})[p]$. Let $\mathrm{Gal}(F_{n+1}/F_n) \simeq \mathbb{Z}/p$ generated by σ. Then

$$\begin{array}{cccc} Q, & [2]Q, & \cdots, & [p-1]Q \\ \sigma Q, & [2]\sigma Q, & \cdots, & [p-1]\sigma Q, \\ \vdots & & & \\ \sigma^{p-1}Q, & [2]\sigma^{p-1}Q, & \cdots, & [p-1]\sigma^{p-1}Q \end{array} \qquad \text{—— } (\bigstar)$$

are $p(p-1)$ points in $E(F_{n+1})[p]$, and they are <u>distinct</u>: in fact, Suppose $Q = [m]\sigma^i Q$ for some $1 \leq m \leq p-1$ and $0 \leq i \leq p-1$, then

$$\sigma^{-i}Q = [m]Q \qquad \text{—— } (*) .$$

But it would give

$$Q = \sigma^{-pi}Q \underset{(*)}{=} [m^p]Q \underset{\substack{\text{Fermat's little} \\ \text{theorem: } m^p \equiv m \bmod p}}{=\!=} [m]Q .$$

It implies $m \equiv 1 \bmod p$ and then $(*)$ becomes $Q = \sigma^i Q$. Note that $\mathrm{Gal}(F_{n+1}/F_n)$ is a cyclic group of order p, so σ^i is another generator. This means $Q \in E(F_{n+1})[p]^{\mathrm{Gal}(F_{n+1}/F_n)} = E(F_n)[p] = 0$, contradiction to our choice of Q. So points in $(\bigstar)$ are all distinct.

- Together with the point O, we have found $p^2 - p + 1$ distinct points in $E(F_{n+1})[p]$. Regard $E(F_{n+1})[p]$ as a Galois module, i.e. a $\mathbb{Z}[\mathrm{Gal}(F_{n+1}/F_n)]$ module, then it means the <u>cyclic module generated by Q has at least $p^2 - p + 1$ elements</u>. Recall $E[p] \simeq \mathbb{Z}/p \times \mathbb{Z}/p$ also as $\mathbb{Z}[\mathrm{Gal}(F_{n+1}/F_n)]$-module. by "Lagrange theorem", we can take $R \in E[F_{n+1})[p]$ not in $(\bigstar)$ and nonzero, and hence a new sequence

$$R, \ \sigma R, \ \cdots \ \sigma^{p-1}R, \text{ altogether } p \text{ distinct point}$$

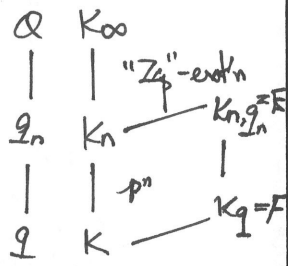
not in $(\bigstar)$. So we have constructed $p^2 + 1$ points in $E(F_{n+1})[p]$, absurd! □

Exercise 1.14 :

23 $\mathbf{Z}_p$-extensions II

23.1 Ramification in a $\mathbf{Z}_p$-extension

Let K be a number field and K_∞/K a $\mathbf{Z}_p$-extension. Let $\Gamma = \mathrm{Gal}(K_\infty/K)$. We will fix an isomorphism $\Gamma \simeq \mathbf{Z}_p$ i.e. a topological generator γ for Γ.



Theorem 23.1. *Let $\mathfrak{q}$ be a prime of K that ramifies in K_∞. Then*

1. *$\mathfrak{q}$ must lie above p.*
2. *For n large enough, any prime of K_n lying over $\mathfrak{q}$ is totally ramified in K_∞/K_n.*

Further, at least one prime of K (lying over p) must ramify in K_∞/K.

Proof. Firstly, at least one prime of K must ramify in K_∞ since K_∞/K is an infinite abelian extension and the maximal totally unramified abelian extension of K is finite. Let $\mathfrak{q}$ be such a prime and let $\mathfrak{Q}$ be a prime of K_∞ over $\mathfrak{q}$. The inertia group $I(\mathfrak{Q}/\mathfrak{q})$ is a nontrivial closed subgroup of Γ, hence must equal Γ^{p^n} for some integer $n \geq 0$. Let $\mathfrak{q}_n$ denote the prime of K_n lying under $\mathfrak{Q}$. Then $\mathfrak{q}_n$ is totally ramified in K_∞/K_n, hence the same is true for all other primes of K_n lying over $\mathfrak{q}$. It only remains to show that $\mathfrak{q}$ must lie over p. Firstly it is clear that $\mathfrak{q}$ cannot be archimedean, for then $I(\mathfrak{Q}/\mathfrak{q})$ is of order 2 and $\mathbf{Z}_p$ has no closed subgroups of finite index. So we may suppose that $\mathfrak{q}$ lies over a finite prime q. We may also suppose without loss that $\mathfrak{q}$ is totally ramified in K_∞ since this may be achieved by replacing K by K_n. (K_∞/K_n is also a $\mathbf{Z}_p$-extension.)

Suppose $q \neq p$. Let m be a positive integer, and let F denote the completion of K at $\mathfrak{q}$ and E that of K_m at $\mathfrak{q}_m$. The extension E/F is then a tamely (and totally) ramified Galois extension of local fields, of degree p^m. By the lemma below, $p^m = [K_m : K]$ must divide $N_{K/\mathbf{Q}}(\mathfrak{q}) - 1$, which gives a contradiction for m large enough. □

This lemma is precisely Greenberg's hint:

Lemma 23.2. *Let F be a finite extension of $\mathbf{Q}_p$, E/F a finite Galois extension that is tamely ramified (i.e. such that the ramification degree of E/F is prime to p.) Then the ramification degree $e(E/F)$ divides $|\mathcal{O}_E/\mathfrak{m}_E| - 1$, where $\mathcal{O}_E$, $\mathfrak{m}_E$ denote the ring of integers of E and its maximal ideal respectively. In particular, if E/F is also totally ramified, $[E : F]$ divides $|\mathcal{O}_F/\mathfrak{m}_F| - 1$.*

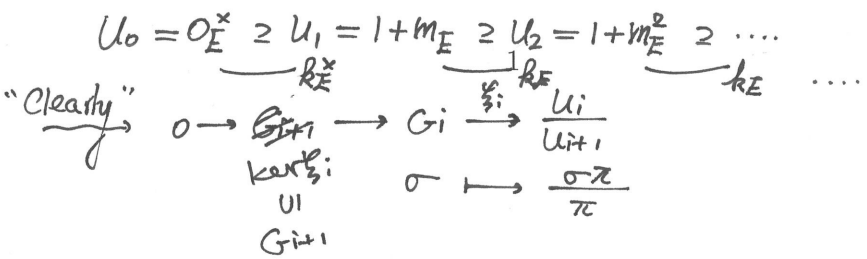
Proof. We first recall some facts about higher ramification groups. Let F be as in the statement of the lemma and E any finite Galois extension of F with Galois group $G = \mathrm{Gal}(E/F)$. For $i \geq -1$, define subgroups G_i of G (the higher ramification groups) by

$$G_i = \{\sigma \in G : \sigma x \equiv x \mod \mathfrak{m}_E^{i+1} \text{ for all } x \in \mathcal{O}_E\}.$$

Thus $G_{-1} = G$, G_0 is the inertia subgroup and the G_i give a filtration on G. Further for i large enough, $G_i = 0$. Let U_0 be the unit group of $\mathcal{O}_E$ and let $U_i = 1 + \mathfrak{m}_E^i$, so that the U_i give a descending filtration on U_0. Let $\sigma \in G_i$ and let π be a uniformizer of $\mathcal{O}_E$. Then $\sigma\pi \equiv \pi \mod \pi^{i+1}$, hence $\sigma\pi/\pi \equiv 1 \mod \pi^i$ i.e. $u := \sigma\pi/\pi \in U_i$. Further, if $\tau \in G_i$ also, then

$$\frac{\tau\sigma\pi}{\pi} = \frac{\tau\pi}{\pi}\frac{\sigma\pi}{\pi}\frac{\tau u}{u}.$$

Since $\tau u \equiv u \mod \pi^{i+1}$, we have $\tau u/u \in U_{i+1}$. Thus the map $\sigma \mapsto \sigma\pi/\pi$ induces a homomorphism of G_i into U_i/U_{i+1}. Clearly G_{i+1} is in the kernel of this homomorphism.



We now return to the proof of the lemma. Without loss we may assume that E/F is totally ramified (replacing F by its maximal unramified extension in E.) We claim that with this assumption the homomorphism $G_i/G_{i+1} \to U_i/U_{i+1}$ is injective. Indeed, suppose $\sigma \in G_i$ is such that $\sigma\pi/\pi \equiv 1 \mod \pi^{i+1}$. Then $\sigma\pi \equiv \pi \mod \pi^{i+2}$. Let $u \in U$ be a unit and let u_0 be a unit in F such that $u \equiv u_0 \mod \pi$. (Such a u_0 exists since E/F is totally ramified.) Then $u = u_0 + \pi t$ for some $t \in \mathcal{O}_E$ and

$$\sigma u - u = (\sigma\pi)(\sigma t) - \pi t = (\sigma\pi - \pi)(\sigma t) + \pi(\sigma t - t) \equiv 0 \mod \pi^{i+2}.$$

It follows then that for any $x \in \mathcal{O}_E$, $\sigma x \equiv x \mod \pi^{i+2}$, so that $\sigma \in G_{i+1}$ as claimed.

Now for $i \geq 1$, U_i/U_{i+1} is a finite p-group. Since G_i/G_{i+1} has order prime to p and injects into U_i/U_{i+1}, we must have $G_i = G_{i+1}$. Since $G_i = 0$ for large i, it follows that $G_1 = 0$ as well. Thus the inertia group G_0 is isomorphic to a subgroup of $U_0/U_1 \simeq (\mathcal{O}_E/\mathfrak{m}_E)^\times \simeq (\mathcal{O}_F/\mathfrak{m}_F)^\times$, from which the lemma follows. □

We will say that $K_{\cdot}/K_{\cdot}$ [illegible]

Exercise 1.15 :

1. We first show $A := E(F_\infty)_{tors}[m : m+p]$ is finite :

- Recall two facts for general $\mathbb{Z}_p$-extensions F_∞/F :
  (1) At least one prime of F above p is ramified in F_∞/F. ([Ochiai, Thm 2.6])
  (2) We can take a sufficiently large n_0 s.t. all ramified pmies of F_∞/F_{n_0} are totally ramified.

  Note that F_∞/F_{n_0} is also a $\mathbb{Z}_p$-extension, from now on we may assume v is a prime of F above p that is totally ramified in F_∞/F.

- Let $P \in A$, ie. $P \in E(F_\infty)_{tors}[m : m+p]$. Then $\exists$ a natural number n_p s.t. $P \in E(F_{n_p})[m]$ for some $m+p$. Recall [Silverman, VIII.1.4], since E has good reduction at p, there is an injection

$$E(F_{n_p})[m] \hookrightarrow \tilde{E}(k_{v_{n_p}}) = \tilde{E}(k_v)$$

  here $k_{v_{n_p}}$ is the residue field of v_{n_p}, where v_{n_p} is a place of F_{n_p} above v. The last equality follows from that v_{n_p}/v is totally ramified. The key is that $\tilde{E}(k_v)$ is finite with size independent of P.

- So the proof is done. In fact, suppose $\exists\, \infty$ distinct points in A, ie. $\forall N$, $\exists$ distinct $P_1, \cdots, P_N \in A$. then $P_i \in E(F_{n_i})[m_i]$ for $n_i := n_{p_i}$. We choose

$$n := \max(n_i : i = 1, \cdots, N)$$
$$m := \text{product of } m_1, \cdots, m_N, \quad (\text{then } m+p)$$

  then $P_1, \cdots, P_N$ are distinct points in $E(F_n)[m] \hookrightarrow \tilde{E}(k_v)$. This is impossible if we choose N large enough. (eg: $N > \#\tilde{E}(k_v)$).

So we have finished the proof. □

Remark : Compare with Exercise 1.10 where we can prove $E(F_\infty^{ac})_{tor} =$ finite, the good thing for anticyc $\mathbb{Z}_p$-extn is that we have "infinitely many good primes" to work with, while here we only have pmie p and we have to pose a priori the condition that E is good @ p.

(b) Now we give an example that B can be infinite. Before that, we recall the following fact on Iwasawa theory of CM elliptic curves.
(cf. de Shalit "Iwasawa theory of elliptic curves w/ CM" (1987))

Setup: • Let E be an elliptic curve $/\mathbb{Q}$ with CM, $\mathcal{O}_K$, ring of integers of an imaginary quadratic ext'n of $\mathbb{Q}$. We Regard E as an elliptic curve over K. For any ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, we define

$$E[\mathfrak{a}] = \mathfrak{a}\text{-torsion points of } E(\bar{K}).$$

where $\mathfrak{a}$ is identified with a bunch of endomorphisms of E via $\iota: \mathcal{O}_K \xrightarrow{\sim} \mathrm{End}(E)$.

• Let N be the conductor of E/K.

Fact 1: Let $\mathfrak{g}, \mathfrak{m}$ be two coprime (integral) ideals of K, ~~then~~ $(N, \mathfrak{m}) = 1$, then: ① $K(E[\mathfrak{m}])$ and $K(E[\mathfrak{g}])$ are linearly disjoint over K

② $\mathrm{Gal}(F(E[\mathfrak{m}])/F) \simeq (\mathcal{O}_K/\mathfrak{m})^\times$.

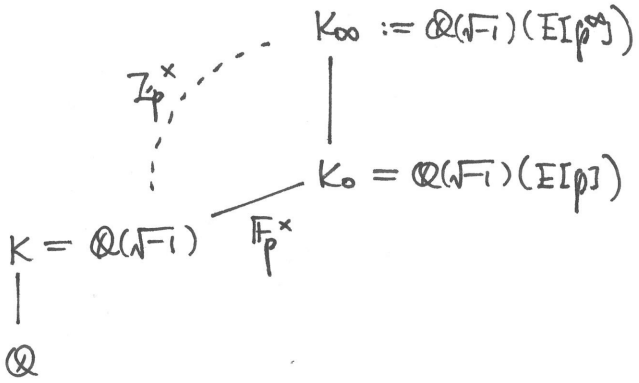
(cf. de Shalit, Chapt. 2, (1.7)).

Now we start with $E: y^2 = x^3 - x$. it has CM $\mathbb{Z}[\sqrt{-1}] \subseteq K := \mathbb{Q}(\sqrt{-1})$, with conductor 32, i.e. it has bad reduction at prime 2 only. Following the hint, let $p \equiv 1 \bmod 4$, then:

• p splits completely in K, say $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$

• E has good reduction at $\mathfrak{p}$.

Now consider the field extension and use Fact 1 to compute the degree:



• $\mathrm{Gal}(K_\infty/K) \simeq \varprojlim_n \mathrm{Gal}(K(E[p^n])/K) = \varprojlim_n (\mathcal{O}_K/p^n)^\times = \mathcal{O}_{K,p}^\times \simeq \mathbb{Z}_p^\times$

• $\mathrm{Gal}(K_0/K) \simeq (\mathcal{O}_K/\mathfrak{p})^\times \simeq \mathbb{F}_p^\times$

So K_∞/K_0 is a $\mathbb{Z}_p$-extension of K_0.

Then we further regard E as an elliptic curve over K_0 such that E has good reduction at $\mathfrak{p}$. Then

$$E(K_\infty)[p^\infty] \supseteq E(K_\infty)[\mathfrak{p}^\infty] = E[\mathfrak{p}^\infty] \text{ is infinite} \quad .$$

as desired. □