Solutions to selected exercises in R.Greenberg's Park City Note - Chapter 2

Ruichen XU December 2023

Exercise 2.1

(a) We write A as a direct limit of all finitely generated subgroups A_i, i.e. $A = \varinjlim A_i$. Then

$$\widehat{A} = \mathrm{Hom}(\varinjlim A_i, \mathbb{Q}_p/\mathbb{Z}_p) \cong \varprojlim \mathrm{Hom}(A_i, \mathbb{Q}_p/\mathbb{Z}_p) \quad -(*)$$

Here inside "$\varprojlim$", each $\mathrm{Hom}(A_i, \mathbb{Q}_p/\mathbb{Z}_p)$ is a finite p-group. Hence $\widehat{A}$ is pro-p. In particular, A is compact.

We also need to show such a profinite topology coincide with the compact open topology on $\widehat{A}$. Denote

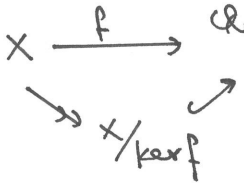
$$\varphi: \widehat{A} \longrightarrow \varprojlim \mathrm{Hom}(A_i, \mathbb{Q}_p/\mathbb{Z}_p)$$

be the canonical isomorphism. We show that if LHS has compact-open topology and RHS has profinite topology, then φ is an homeomorphism.

- φ is continuous
- φ is an open map.

This should not be very hard. (Left to the readers?)

(b) We first show X is p-primary. Since X is a pro-p group, it is compact. Noting that for any $f^* \in \widehat{X}$, $\ker f$ is open normal subgroup of X, hence it is of finite index in X. In other words, f factors through a finite group $X/\ker f$.



Now that X is pro-p, $X/\ker f$ is p-primary (?), which implies f is p-primary.

Next we show $\widehat{X}$ has discrete topology. Consider the coset ~~decomposition~~ decomposition $X/\ker f = \{a + \ker f : a \in X\}$, which is a finite set. Then one checks directly that

$$\{f\} = \bigcap_{a \in X/\ker f} \underbrace{V\big((\ker f + a), \{a\}\big)}_{:= \{f: X \to \mathbb{Q}_p/\mathbb{Z}_p : f(\overbrace{a+\ker f}^{\text{cpt}}) \subseteq \overbrace{a}^{\text{open}}\}}$$

that is, a finite intersection of open sets under the compact open topology of $\widehat{X}$, hence $\{f\}$ is open. This shows $\widehat{X}$ is discrete.

(c) Here in the computation, we invoked three important facts:

(i) A is a finite abelian p-group, then $\widehat{A} \cong A$.

(ii) If $A = \varprojlim A_i$ is a pro-p group, then $\widehat{A} = \varprojlim \widehat{A_i}$

(iii) If $A = \varinjlim A_i$ with each map $\varphi_i : A_i \longrightarrow A$ inclusions then $\widehat{A} = \varprojlim A_i$

The proofs of (i)–(iii) can be found in [Luis Ribes, Pavel Zalesskii, "Profinite groups" 2nd ed., §2.9].

Now we compute:

~~$\widehat{\mathbb{Z}_p} = \mathrm{Hom}(\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}, \mathbb{Q}_p/\mathbb{Z}_p)$~~

- $\widehat{\mathbb{Z}_p} = \left(\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}\right)^{\wedge} \overset{(ii)}{=} \varinjlim_n \left(\mathbb{Z}/p^n\mathbb{Z}\right)^{\wedge} \overset{(i)}{=} \varinjlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Q}_p/\mathbb{Z}_p$.
- $\widehat{\mathbb{Q}_p/\mathbb{Z}_p} = \left(\varinjlim_n \frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p\right)^{\wedge}$

$\overset{(iii)}{=} \varprojlim_n \left(\frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p\right)^{\wedge}$

$\overset{(i)}{=} \varprojlim_n \frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$,

as desired. □

Exercise 2.2

(a) As given by Greenberg,

$$H^1(\Gamma, A) \overset{\text{defined as}}{=\!=} \varinjlim_n H^1(\Gamma/\Gamma_n, A^{\Gamma_n})$$

where $\Gamma_n = \Gamma^{p^n}$, topologically generated by $\gamma_n := \gamma_0^{p^n}$, γ_0 is the topological generator of Γ. Then for the finite cyclic group $\Gamma/\Gamma_n = \langle \bar{\gamma}_n \rangle$, we have

$$H^1(\Gamma/\Gamma_n, A^{\Gamma_n}) = \frac{\ker(N_n)}{\mathrm{im}(\bar{\gamma}_n - 1)}, \text{ where } N_n := \sum_{i=1}^{p^n - 1} \bar{\gamma}_n^i : A^{\Gamma_n} \longrightarrow A^{\Gamma_n}.$$

- For n sufficiently large such that ~~Γ~~ $T^n A = 0$ (guaranteed by Exercise 3.1), we γ_n acts on A trivially, hence $\ker(N_n) = A^{\Gamma_n}$
- as $n \to \infty$, $\mathrm{im}(\bar{\gamma}_n - 1)$ tends to the entire $(\gamma_0 - 1)A$.

So $H^1(\Gamma, A) = \varinjlim_n H^1(\Gamma/\Gamma_n, A^{\Gamma_n}) = A/(\gamma-1)A$.

(b) It is direct to see $A = \bigcup A^{\Gamma_n}$. For such an A, we again write it as $A = \varinjlim A_i$, where the colimit is over all finitely generated subgroups of A.

Then

$$\begin{aligned}
H^1(\Gamma, A) &\overset{\text{by defn}}{=\!=} \varinjlim_n H^1(\Gamma/\Gamma_n, A^{\Gamma_n}) \\
&= \varinjlim_n H^1(\Gamma/\Gamma_n, (\varinjlim_i A_i)^{\Gamma_n}) \qquad \left(\text{check: } A_i^{\Gamma_n} = \text{~~}A^{\Gamma_n} \cap A_i\right) \\
&= \varinjlim_n H^1(\Gamma/\Gamma_n, \varinjlim_i (A_i)^{\Gamma_n}) \\
&= \varinjlim_n \varinjlim_i H^1(\Gamma/\Gamma_n, A_i^{\Gamma_n}) \\
&= \varinjlim_i A_i/(\gamma-1)A_i \qquad \text{by Exercise 2.2(a)} \\
&= A/(\gamma-1)A, \qquad \text{as desired!}
\end{aligned}$$

(c) Consider the exact sequence

$$0 \longrightarrow A^\Gamma \longrightarrow A \xrightarrow{\gamma - 1} A \longrightarrow A/(\gamma-1)A \longrightarrow 0$$

and by (b), $H^1(\Gamma, A) = A/(\gamma-1)A$, note $H^0(\Gamma, A) = A^\Gamma = A^{\gamma-1}$. Taking $\mathbb{Z}_p$-cork along this sequence, we see $H^0(\Gamma, A)$ and $H^1(\Gamma, A)$ has the same $\mathbb{Z}_p$-corank. (not used $A \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r$ really). When $A \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r$, then (?) $A/(\gamma-1)A \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^s$ for $s \leq r$. Suppose $H^0(\Gamma, A) =$ finite, then it has $\mathrm{corank}_{\mathbb{Z}_p}$ zero. hence so does $H^1(\Gamma, A)$, which means $s = 0$, i.e. $H^1(\Gamma, A) = A/(\gamma-1)A = 0$.

□

Exercise 2.3 : We concentrate on $l \neq p$ case.

(a) Note that $A = \mathbb{Q}_p/\mathbb{Z}_p$ has trivial G_{K_v}-action

$$H^1(K_v, A) = \operatorname{Hom}_{cts}(G_{K_v}, \mathbb{Q}_p/\mathbb{Z}_p)$$
$$= \operatorname{Hom}_{cts}(G_{K_v}^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) \quad \text{since } \mathbb{Q}_p/\mathbb{Z}_p \text{ is abelian.}$$

Now by local class field theory, $G_{K_v}^{ab} \simeq \widehat{K_v^\times} = \underbrace{\widehat{\mathbb{Z}}}_{\text{given by the uniformizer}} \times \mathcal{O}_{K_v}^\times$ and $\mathcal{O}_{K_v}^\times \simeq \Delta \times \mathbb{Z}_l^{[K_v:\mathbb{Q}_l]}$ where Δ is a finite group, we see that

$$\operatorname{Hom}_{cts}(G_{K_v}^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Q}_p/\mathbb{Z}_p \times \text{a finite group}$$

where : • $\mathbb{Q}_p/\mathbb{Z}_p$ is from $\widehat{\mathbb{Z}}$-part, noting that $\widehat{\mathbb{Z}} = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$ and only the "$\mathbb{Z}_p$"-part contributes to "$\operatorname{Hom}_{cts}(G_{K_v}^{ab}, \mathbb{Q}_p/\mathbb{Z}_p)$".

• The "finite group" part comes from the possible p-primary part of Δ.

Therefore $\operatorname{corank}_{\mathbb{Z}_p} H^1(K_v, \mathbb{Q}_p/\mathbb{Z}_p) = 1$.

(b) Recall the corank lemma predicts

$$\operatorname{corank}_{\mathbb{Z}_p} H^1(K_v, \mathbb{Q}_p/\mathbb{Z}_p) = \text{[illegible]} + \operatorname{corank}_{\mathbb{Z}_p} H^0(K_v, \mathbb{Q}_p/\mathbb{Z}_p) + \operatorname{rk}_{\mathbb{Z}_p} H^0(K_v, \hat{A}(1))$$

• Since G_{K_v} acts on $\mathbb{Q}_p/\mathbb{Z}_p$ trivially, $H^0(K_v, \mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Q}_p/\mathbb{Z}_p$

• Note that $\hat{A}(1) = \operatorname{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) = \mathbb{Z}_p(1)$ since again G_{K_v} acts trivially on $\mathbb{Q}_p/\mathbb{Z}_p$. Hence $H^0(K_v, \hat{A}(1)) = \mathbb{Z}_p(1)^{G_{K_v}} = 0$ (Subtlety here !)

So combining with (a), the corank lemma is verified.

The $l = p$ case is similar :

• $\operatorname{Hom}_{cts}(G_{K_v}^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) = \underbrace{\mathbb{Q}_p/\mathbb{Z}_p}_{\text{from "}\widehat{\mathbb{Z}}\text{"-part}} \times \underbrace{(\mathbb{Q}_p/\mathbb{Z}_p)^{\oplus [K_v:\mathbb{Q}_p]}}_{\text{from "}\mathbb{Z}_p^{[K_v:\mathbb{Q}_p]}\text{"-part}} \times \text{finite group}$

So $\operatorname{corank}_{\mathbb{Z}_p} H^1(K_v, \mathbb{Q}_p/\mathbb{Z}_p) = 1 + [K_v : \mathbb{Q}_p]$.

• In the corank lemma, $H^0(K_v, \mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Q}_p/\mathbb{Z}_p$ again, and

$$H^0(K_v, \hat{A}(1)) = \mathbb{Z}_p(1)^{G_{K_v}} = 0 \quad \text{again.}$$

So this verifies the corank lemma again.

(c) For the nontrivial finite order char case, one can see [Greenberg, LNM, Lemma 2.3]. □

Exercise 2.4 :

(a) By Kummer theory, $H^1(K_v, \mu_{p^\infty}) = K_v^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$. As we know, $K_v^\times = \mathbb{Z} \times (\text{finite group}) \times \mathbb{Z}_\ell^{[K_v:\mathbb{Q}_\ell]}$, we see that

- When $\ell \neq p$, $\mathbb{Z}_\ell \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ since $\mathbb{Z}_\ell$ is p-divisible. Hence $H^1(K_v, \mu_{p^\infty}) \simeq \mathbb{Q}_p/\mathbb{Z}_p \times$ some finite group. Therefore it has $\mathbb{Z}_p$-corank one.
- When $\ell = p$, $\mathbb{Z}_p \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathbb{Q}_p/\mathbb{Z}_p$. Hence $H^1(K_v, \mu_{p^\infty}) = \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^{\oplus([K_v:\mathbb{Q}_p]+1)}$, which has $\mathbb{Z}_p$-corank $1+[K_v:\mathbb{Q}_p]$.

(b) Now we verify the corank Lemma : this time we needn't bother $\ell \neq p$ & $\ell = p$.

~~(i) When $\ell \neq p$, as we have seen in Exercise 2.3, $H^0(K_v, \mu_{p^\infty}) = \mathbb{Z}_p(1)$~~

For $A = \mu_{p^\infty}$, it suffices to consider two H^0 :

(i) $H^0(K_v, \mu_{p^\infty}) = \mu_{p^\infty}(K_v)$.
As $K_v^\times = \pi^{\mathbb{Z}} \times$ finite part $\times \mathbb{Z}_\ell^{[K_v:\mathbb{Q}_\ell]}$, we see $\mu_{p^\infty}(K_v)$ is finite, and hence $H^0(K_v, \mu_{p^\infty})$ has trivial $\mathbb{Z}_p$-corank.

(ii) For $H^0(K_v, \hat{A}(1))$, we need to first figure out $\hat{A}(1)$, by noting that
- $\mathrm{Hom}(\mu_{p^\infty}, \mathbb{Q}_p/\mathbb{Z}_p) =: \mathbb{Z}_p(-1)$ and $\mathbb{Z}_p(-1) \underset{\mathbb{Z}_p}{\otimes} \mathbb{Z}_p(1) = \mathbb{Z}_p$ with trivial G_{K_v}-action.

So $H^0(K_v, \hat{A}(1)) \simeq \mathbb{Z}_p$, which has $\mathbb{Z}_p$-rank one.

So this verifies the corank lemma. □

Remark : Altogether, Exercise 2.3 & 2.4 verifies all interesting / useful case of the corank lemma :

- Exercise 2.3 : $A = \mathbb{Q}_p/\mathbb{Z}_p$ with trivial action & action by a finite order character $\psi : G_{K_v} \longrightarrow \mathbb{Z}_p^\times$.
- Exercise 2.4 : $A = \mu_{p^\infty} \simeq \mathbb{Q}_p/\mathbb{Z}_p$ as abstract groups but with the cyclotomic character ε_{cyc} (of of course infinite orders.).

□

Exercise 2.5

(a) Since $K_v(E[p^\infty])/K_v$ is an unramified extension, we have $K_v \subseteq K_v(E[p^\infty]) \subseteq K_v^{ur}$.

We use the inflation-restriction exact sequence:

$$0 \longrightarrow H^1(K_v(E[p^\infty])/K_v, E[p^\infty]) \longrightarrow H^1(K_v^{ur}/K_v, E[p^\infty]) \longrightarrow H^1(K_v^{ur}/K_v(E[p^\infty]), E[p^\infty]).$$

- First analyse the rightmost term: Since $Gal(K_v^{ur}/K_v(E[p^\infty]))$ acts on $E[p^\infty]$ trivially, $H^1(K_v^{ur}/K_v(E[p^\infty]), E[p^\infty]) = Hom(Gal(K_v^{ur}/K_v(E[p^\infty])), E[p^\infty])$. Now note:
  - $Gal(K_v^{ur}/K_v) \simeq \widehat{\mathbb{Z}} = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$
  - Let $K_{\infty,v}/K_v$ be the unique unramified $\mathbb{Z}_p$-extension of K_v (note $v \nmid p$),

(*) then we see $K_v(E[p^\infty]) \supseteq K_{\infty,v} \supseteq K_v$ with $\Delta := Gal(K_v(E[p^\infty])/K_{\infty,v})$ a finite cyclic group of order prime to p (borrowed from Greenberg's proof of Lemma 4.4 in PC note). So:

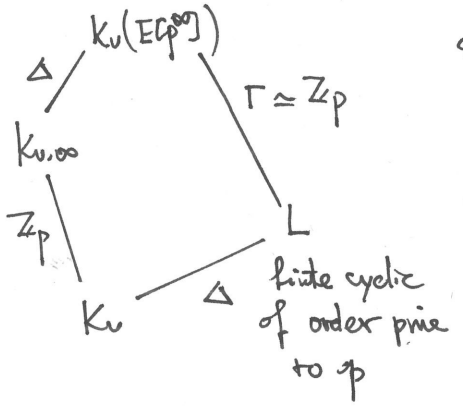
- we see $Gal(K_v^{ur}/K_v(E[p^\infty]))$ does not have pro-p part, hence $H^1(\cdots) = 0$.

- So to show the middle term is zero, it suffices to show the leftmost term is zero. (in fact, as we have seen, the two are isomorphic) ~~How we (note Exercise 2.2(c)), it suffices to show $H^0(K_v(E[p^\infty])/K_v, E[p^\infty])$ is~~

Note the following fact:

Fact: Let G be a profinite group and G_p be its pro-Sylow p-subgroup. Let A be a p-primary G-module. Then $H^1(G,A) = H^1(G_p, A)$.

So by (*), $H^1(K_v(E[p^\infty])/K_v, E[p^\infty]) = H^1(\Gamma, E[p^\infty])$ where $\Gamma \simeq \mathbb{Z}_p$ is characterized by (*). To show the latter is zero, by Exercise 2.2(c), it suffices to show $H^0(\Gamma, E[p^\infty]) = $ finite, yet it is nothing but $E(L)[p^\infty]$, which is indeed finite (for example, argue on the residue field of L).



(b) We consider the inflation-restriction exact sequence of $K_v^{ur}/L_v/K_v$:

$$0 \longrightarrow H^1(L_v/K_v, E(L_v)[p^\infty]) \longrightarrow H^1(K_v^{ur}/K_v, E[p^\infty]) \longrightarrow \cdots .$$

As seen in (a), $H^1(K_v^{ur}/K_v, E[p^\infty]) = 0$, so the leftmost term is zero.

(c) Not necessarily! Consider L_v/K_v to be a totally ramified degree $\not\equiv d$ extension with $p \mid d$. Then:

- Since $K_v(E[p^\infty])/K_v$ is unramified, $L_v \cap K_v(E[p^\infty]) = K_v$ and hence $E(L_v)[p^\infty] = E(K_v)[p^\infty]$. This implies that the Galois action of $\mathrm{Gal}(L_v/K_v)$ on $E(L_v)[p^\infty]$ is trivial.
- Then $H^1(L_v/K_v, E(L_v)[p^\infty]) = \mathrm{Hom}_{cts}\left(\mathrm{Gal}(L_v/K_v), E[p^\infty]\right)$. As the source has order p elements and $E[p^\infty]$ is pro-p, the $\mathrm{Hom}(-,-)$ could be nonzero.

So we are done if such a local field extension L_v/K_v exists. This can be done by constructing a Lubin-Tate tower of extensions $K_{v,n}/K_v$, and choose primes p and ℓ appropately such that $p \mid \ell - 1$. $\left(\because [K_{v,n}/K_v] = (\ell-1)\ell^{n-1}\right)$.

Exercise 2.6 :

Again we use inflation–restriction exact sequences :

(1) $\overline{K_v}$ / K_v^{tame} / K_v gives

$$0 \longrightarrow H^1(K_v^{tame}/K_v, E[p^\infty]) \longrightarrow H^1(K_v, E[p^\infty]) \longrightarrow H^1(K_v^{tame}, E[p^\infty]).$$

Now note that $\mathrm{Gal}_{K_v^{tame}}$ is pro-l and $E[p^\infty]$ is pro-p, the rightmost term vanishes, so $H^1(K_v, E[p^\infty]) \cong H^1(K_v^{tame}/K_v, E[p^\infty])$.

(2) Then K_v^{tame} / K_v^{ur} / K_v gives

$$0 \longrightarrow H^1(K_v^{ur}/K_v, E[p^\infty]) \longrightarrow H^1(K_v^{tame}/K_v, E[p^\infty]) \hookrightarrow H^1(K_v^{tame}/K_v^{ur}, E[p^\infty])^{\mathrm{Gal}(K_v^{ur}/K_v)}$$

$$\downarrow$$

$$H^2(K_v^{ur}/K_v, E[p^\infty]).$$

Then : • $H^1(K_v^{ur}/K_v, E[p^\infty]) = 0$ by Exercise 2.5 and the rightmost term is zero since $\hat{\mathbb{Z}}$ has cohomological dimension 1.

therefore $H^1(K_v^{tame}/K_v, E[p^\infty]) \cong \underbrace{H^1(K_v^{tame}/K_v^{ur}, E[p^\infty])^{\mathrm{Gal}(K_v^{ur}/K_v)}}_{(*)}$.

So our main focus is on $(*)$.

• Note $\mathrm{Gal}(K_v^{tame}/K_v^{ur})$ acts on $E[p^\infty]$ trivially. $(*) = \mathrm{Hom}\left(\mathrm{Gal}(K_v^{tame}/K_v^{ur}), E[p^\infty]\right)^{\mathrm{Gal}(K_v^{ur}/K_v)}$.

• Then since $\mathrm{Gal}(K_v^{tame}/K_v^{ur}) \simeq \prod_{q \neq l} \mathbb{Z}_q$ with Galois action as cyclotomic characters (i.e. $\mathrm{Gal}(K_v^{tame}/K_v^{ur}) \simeq \prod_{q \neq l} \mathbb{Z}_q(1)$ as Galois module), we see

$$(*) = \mathrm{Hom}_{cts}(\mathbb{Z}_p(1), E[p^\infty])^{\mathrm{Gal}(K_v^{ur}/K_v)} \quad (\because \text{throwing away non pro-}p \text{ part})$$

$$= \{P \in E[p^\infty] : \sigma P = \varepsilon_{cyc}(\sigma) \cdot P, \ \forall \sigma \in \mathrm{Gal}(K_v^{ur}/K_v)\}.$$

Therefore the main claim here is that this set is a finite set.

Here we use Dr. Luochen ZHAO's great arguments :

Exercise 2.6 (The key step by Luochen Zhao)

$$\mathrm{Hom}(\mathbf{Z}_p, E[p^\infty])^{\hat{\mathbf{Z}}} = \{P \in E[p^\infty] : \text{ for all } \sigma \in \hat{\mathbf{Z}},\ P^\sigma = \chi(\sigma)P\} =: X. \tag{0.5}$$

For the sake of absurdity, suppose the set X is infinite. We claim that a contradiction arises if, fixing a topological generator $\sigma \in \mathbf{Z}_p \subset \hat{\mathbf{Z}}$, there exists infinitely many points $Q \in E[p^\infty]$ with $Q^\sigma = Q$. If this is so, we know that if L/K is the unramified subextension with $\mathrm{Gal}(L/K) \simeq \prod_{v \nmid p} \mathbf{Z}_v$, then $E[p^\infty](L)$ has infinitely many points. As $\mathrm{Gal}(L/K) \to \mathrm{Aut}(E[p^\infty]) = \mathrm{GL}_2(\mathbf{Z}_p)$ has finite image, we conclude that $E[p^\infty](L) = E[p^\infty](L')$ for some finite subextension L'/K of L. This shows that $E[p^\infty](L')$ is infinite, contradicting the finiteness of the residue field of L'.

We now construct the infinitely many Q's with $Q^\sigma = Q$. Let $\langle , \rangle$ be the Weil pairing $E[p^\infty] \times E[p^\infty] \to \mu_{p^\infty}$. For all $Q \in E[p^\infty]$ and $\sigma \in \hat{\mathbf{Z}}$, we have

$$\langle P^\sigma, Q^\sigma \rangle = \langle P, Q \rangle^\sigma = \chi(\sigma)\langle P, Q \rangle. \tag{0.6}$$

If $P \in X$, we find $\langle P, Q^\sigma - Q \rangle = 0$. Now, suppose further that P has exactly order p^n, and choose Q to be in $E[p^n]$, by the nondegeneracy of the Weil pairing we conclude that $Q^\sigma - Q \in (\mathbf{Z}/p^n)P$; say $Q^\sigma - Q = \lambda P$ for some $\lambda \in \mathbf{Z}_{>0}$. Now, form the point

$$Q' = (\chi(\sigma) - 1)Q - \lambda P, \tag{0.7}$$

for which we have

$$Q'^\sigma = (\chi(\sigma) - 1)(Q + \lambda P) - \lambda\chi(\sigma)P = Q'. \tag{0.8}$$

Clearly, if we choose Q to be of order n, then Q' is of order at least $n - \mathrm{ord}_p(\chi(\sigma) - 1)$. The infinitude of P then guarantees that we can make n as large as possible, and therefore we have infinite many points in $E[p^\infty]$ fixed by σ.

Exercise 2.7

We use the corank lemma to see

$$\operatorname{corank}_{\mathbb{Z}_p} H^1(K_v, E[p^\infty]) = 2[K_v:\mathbb{Q}_p] + \operatorname{corank}_{\mathbb{Z}_p} H^0(K_v, E[p^\infty]) + \operatorname{rk}_{\mathbb{Z}_p} H^0(K_v, \widehat{E[p^\infty]}(1)).$$

Now $H^0(K_v, E[p^\infty]) = E(K_v)[p^\infty]$ is finite, since $E(K_v)$ is a finitely generated $\mathbb{Z}_p$-mod so $\operatorname{corank}_{\mathbb{Z}_p}\left(H^0(K_v, E[p^\infty])\right) = 0$. The difficulty is on the rightmost term:

- $\widehat{E[p^\infty]}(1) = \mathrm{Hom}_{\mathrm{cts}}\left(E[p^\infty], \mu_{p^\infty}\right)$, here both $E[p^\infty]$ and μ_{p^∞} are equipped with G_{K_v}-action, so the $\mathrm{Hom}_{\mathrm{cts}}$-space is so as well. As [Greenberg, PC note, p428-429], by choosing a basis, we write the action ρ_E of G_{K_v} on $E[p^\infty]$ by a matrix which is "triangular", i.e. $\rho_E = \begin{pmatrix} \varphi & * \\ 0 & \psi \end{pmatrix}$, where
  - φ is the action of G_{K_v} on $\ker\left(\pi : E[p^\infty] \longrightarrow \overline{E}[p^\infty]\right)$.
  - ψ is the inflated action of G_{k_v} on $\overline{E}[p^\infty]$, which is trivial on I_{K_v}.

  The Weil pairing implies that $\det(\rho_E) = \varphi.\psi = \varepsilon_{cyc}$, i.e. the cyclotomic character. Note that the action of G_{K_v} on μ_{p^∞} is by ε_{cyc}. we see G_{K_v} acts on $\widehat{E[p^\infty]}(1)$ by $\begin{pmatrix} \varphi^{-1}\varepsilon_{cyc} & * \\ & \psi^{-1}\varepsilon_{cyc} \end{pmatrix}$
- So now we try to see $H^0(K_v, \widehat{E[p^\infty]}(1))$, which is the G_{K_v}-fixed part of the above $\widehat{E[p^\infty]}(1)$. Then if we can show $\varphi \neq \varepsilon_{cyc}$ always holds, then $\widehat{E[p^\infty]}(1)^{G_{K_v}} = 0$, hence $\operatorname{rk}_{\mathbb{Z}_p}$ is zero.

~~Still stuck here, I do not know how~~

[Indeed, if $\varphi = \varepsilon_{cyc}$, then since $\varphi.\psi = \varepsilon_{cyc}$, ψ would be the trivial character. But this is impossible since ψ is inflated from the action of G_{k_v} on $\overline{E}[p^\infty]$, and the latter couldn't be trivial (?). (Doubts !!)]

So to sum up, $\operatorname{corank}_{\mathbb{Z}_p} H^1(K_v, E[p^\infty]) = 2[K_v:\mathbb{Q}_p]$.

Exercise 2.8

We consider

$$0 \longrightarrow \ker\theta \longrightarrow H^1(\mathbb{Q}, E[p^\infty]) \xrightarrow{\theta} \prod_{\ell \text{ prime}} H^1(\mathbb{Q}_\ell, E[p^\infty]) \quad \text{—— (*)}$$

- For the middle term, by Kumer theory we have $\kappa: E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(\mathbb{Q}, E[p^\infty])$
  By assumption, $\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 3$, hence $\operatorname{corank}_{\mathbb{Z}_p} H^1(\mathbb{Q}, E[p^\infty]) \geq 3$.
- The hardest part is the rightmost term. We have:

$$H^1(\mathbb{Q}_\ell, E[p^\infty]) = \begin{cases} \text{finite}, & \text{when } \ell \neq p,\ E \text{ has good reduction @ } \ell \text{ (Exercise 2.6)} \\ (?), & \text{when } \ell \neq p,\ E \text{ has bad reduction @ } \ell. \\ \text{has } \operatorname{corank}_{\mathbb{Z}_p} \text{ equals to } 2, & \text{when } \ell = p \end{cases}$$

Guess: @ bad places, $H^1(\mathbb{Q}_\ell, E[p^\infty])$ is finite as well. (?)

Putting @ κ into (*), as $\ker(\theta\circ\kappa) \hookrightarrow \ker\theta$ by the injectivity of κ, to show $\ker\theta$ is infinite, it suffices to show $\ker(\theta\circ\kappa)$ is infinite. The adapted sequence of (*) is

$$0 \longrightarrow \ker(\theta\circ\kappa) \longrightarrow \underbrace{E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}_{\| \ (\mathbb{Q}_p/\mathbb{Z}_p)^{\oplus r}} \xrightarrow{\theta\circ\kappa} \prod_{\ell \text{ prime}} H^1(\mathbb{Q}_\ell, E[p^\infty]) \quad \text{—— (**)}$$

We spot that there is No nontrivial group homomorphism $\eta: \mathbb{Q}_p/\mathbb{Z}_p \to A$ where A is a finite group, so actually $\theta\circ\kappa$ factors through $H^1(\mathbb{Q}_p, E[p^\infty])$:

$$0 \to \ker(\theta\circ\kappa) \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\theta\circ\kappa} \prod_{\ell} H^1(\mathbb{Q}_\ell, E[p^\infty]) \quad \text{—— (***)}$$
$$\theta\circ\kappa \searrow \quad \uparrow$$
$$H^1(\mathbb{Q}_p, E[p^\infty])$$

then we take $\operatorname{corank}_{\mathbb{Z}_p}(-)$ along this new sequence (***) to see

$$\operatorname{corank}_{\mathbb{Z}_p}(\ker(\theta\circ\kappa)) \geq \operatorname{cork}_{\mathbb{Z}_p}\left(E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right) - \operatorname{cork} H^1(\mathbb{Q}_p, E[p^\infty]) = r-2$$

So when $r \geq 3$, we see $\operatorname{corank}_{\mathbb{Z}_p}(\ker(\theta\circ\kappa))$ is positive, hence $\ker(\theta\circ\kappa)$ is infinite, as desired!

Remark: So a weaker Guess' suffices: @ bad places, $H^1(\mathbb{Q}_\ell, E[p^\infty])$ does not provide positive $\mathbb{Z}_p$-rank.

Exercise 2.10

We use the inflation – restriction exact sequence

$$0 \longrightarrow H^1\left(M/k, E[n]\right) \longrightarrow H^1(k, E[n]) \longrightarrow H^1(M, E[n])^{\mathrm{Gal}(M/k)} \longrightarrow H^2\left(M/k, E[n]\right).$$

$\bar{k}$

$M := k(E[n])$

k

Then: • $H^i(M/k, E[n])$ are finite for $i = 1, 2$, since $\mathrm{Gal}(M/k)$ and $E[n]$ are both finite.

Hence to show $H^1(k, E[n])$ has infinitely many element of order p, it is sufficient to prove it for $H^1(M, E[n])^{\mathrm{Gal}(M/k)}$.

Now note that G_M acts trivially on $E[n]$, so $H^1(M, E[n]) = \mathrm{Hom}(G_M, E[n])$. But then how to find infinitely many elements of order p in it that is fixed by $\mathrm{Gal}(M/k)$?

Exercise 2.11

We first write $n = p_1^{e_1} \cdots p_g^{e_g}$. Then $E[n] = \prod_{i=1}^{g} E[p_i^{e_i}]$. Inductively taking $H^1(K_\Sigma/k, -)$, we see it suffices to show that for any p and n, $H^1(K_\Sigma/k, E[p^n])$ is finite.

Then we run a Kummerian argument:

$$0 \longrightarrow E[p^n] \longrightarrow E[p^\infty] \xrightarrow{\times p^n} E[p^\infty] \longrightarrow 0$$

and take $H^1(K_\Sigma/k, -)$:

$$0 \longrightarrow \frac{E[p^\infty]^G}{p^n E[p^\infty]} \longrightarrow H^1(K_\Sigma/k, E[p^n]) \longrightarrow H^1(K_\Sigma/k, E[p^\infty])[p^n] \longrightarrow 0$$

where $G = \mathrm{Gal}(K_\Sigma/k)$. Then we note:

- Since $E[p^\infty]/p^n E[p^\infty] \simeq \mathbb{Z}/p^n \times \mathbb{Z}/p^n$ is finite, the leftmost term is finite.
- The rightmost term is studied in Exercise 2.9, where we have seen $H^1(K_\Sigma/k, E[p^\infty])$ is a cofinitely generated $\mathbb{Z}_p$-module. Hence its p^n-torsion part is finite. (?)

Therefore, the middle term $H^1(K_\Sigma/k, E[p^n])$ is indeed finite. □

Exercise 2.12

Note : Here in the setup, $\widetilde{E}$ is an elliptic curve over a finite field k_v of characteristic p. So it is a priori smooth. In this exercise we are studying whether it is ordinary or supersingular.

In Greenberg's note : (p412) if $\widetilde{E}(\overline{k_v})$ has points of order p, then it is called ordinary, otherwise supersingular.

(a) Key observations are geometric interpretations of the Hasse invariant of $\widetilde{E}$, in fact.

$$a_v = 1 + |k_v| - |\widetilde{E}(k_v)| = 1 + \deg(Fr_v) - \deg(1 - Fr_v) = \mathrm{trace}(Fr_v).$$

This implies $[a] = Fr_v + \widehat{Fr_v}$, where $\widehat{Fr_v}$ is the dual isogeny of Fr_v.

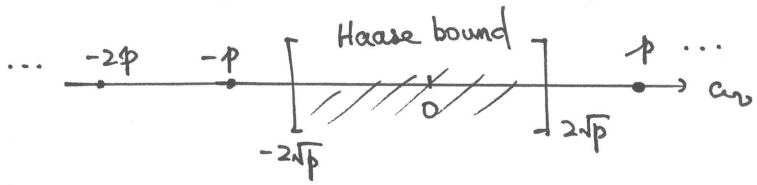
Then $a_v \equiv 0 \bmod p \iff \widehat{Fr_v}$ is inseperable [Silverman, III.5.5)

$\iff \widetilde{E}$ is supersingular [Silverman, V.3.1a(ii)]

since $\widehat{Fr_v} = [a] - Fr_v$. (This is actually the argument hidden in [Silverman, p150])

Hence, $\widetilde{E}$ is ordinary iff $p \nmid a_v$.

(b) Now $k_v = \mathbb{F}_p$, we have the Hasse bound that $|a_v| \le 2\sqrt{p}$, which is strictly smaller than p when $p \ge 5$. If $\widetilde{E}$ is supersingular, $p \mid a_v$ by (a). So this forces $a_v = 0$.

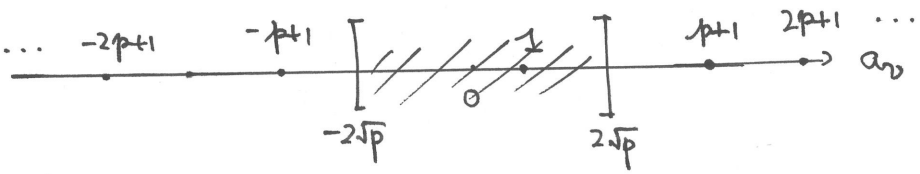


(c) $\widetilde{E}(k_v)$ has a point of order p

$\iff p \mid |\widetilde{E}(k_v)|$

$\iff a_v \equiv 1 \bmod p$ since $a_v := 1 + |k_v| - |\widetilde{E}(k_v)|$.

Now $k_v = \mathbb{F}_p$, then again by the Hasse bound, $|a_v| \le 2\sqrt{p}$



So when $p \ge 7$, $a_v \equiv 1 \bmod p \iff a_v = 1$. □

Remark : Note the relation of (c) and that $\widetilde{E}$ is ordinary : $\widetilde{E}$ is ordinary means that $\widetilde{E}(\overline{k_v})$ has a point of order p. (c) is stronger : $\widetilde{E}(k_v)$ has points of order p.