Ruichen XU December 2023

Exercise 3.10 (by Luochen Zhao)

(throughout, we let $\widehat{A}$ to be the Pontragin dual of A).

Step 1: Let γ be the topological generator of Γ. We see since

$$(A^{\Gamma})^{\wedge} = \widehat{A}_{\Gamma} = \widehat{A}/(\gamma-1)\widehat{A},$$

as A^{Γ} is finite, $\widehat{A}/(\gamma-1)\widehat{A}$ is then finite. By [Greenberg, PC note, Thm 3.9], (i.e. the topological Nakayama's lemma), $\widehat{A}$ is a finitely generated torsion Λ-module

Step 2: We translate the condition $A^{\Gamma_{n+1}} = A^{\Gamma_n}$ into its dual, that is an exact sequence

$$0 \longrightarrow \frac{\gamma^{p^n}-1}{\gamma^{p^{n+1}}-1}\cdot A^{\vee} \longrightarrow A^{\vee}/(\gamma^{p^{n+1}}-1)A^{\vee} \xrightarrow{(*)} A^{\vee}/(\gamma^{p^n}-1)A^{\vee} \longrightarrow 0$$

here: the surjectivity $(*)$ follows from the natural inclusion $A^{\Gamma_n} \subseteq A^{\Gamma_{n+1}}$ and that $A^{\Gamma_{n+1}} = A^{\Gamma_n}$ implies that $(*)$ has trivial kernel, i.e.

$$\frac{\gamma^{p^n}-1}{\gamma^{p^{n+1}}-1}\cdot A^{\vee} \overset{(\star)}{=} (\gamma^{p^n}-1)A^{\vee} \otimes_{\Lambda} \Lambda/g = 0 \qquad \text{—— } (**)$$

where $g = \dfrac{\gamma^{p^{n+1}}-1}{\gamma^{p^n}-1} \in \Lambda$. We then note that:

- $(\gamma^{p^n}-1)A^{\vee}$ is a finitely generated Λ-module: indeed from Step 1 we see $A^{\vee}$ is so.
- $(g) \subseteq \max\mathrm{Spec}\,\Lambda$: to see this, we identify $\Lambda = \mathbb{Z}_p[[T]]$ with the power series ring $\mathbb{Z}_p[[T]]$ and $g = \dfrac{\omega_{n+1}(T)}{\omega_n(T)}$. Then one checks directly that $g \in (p, T)$ = the unique maximal ideal of $\mathbb{Z}_p[[T]]$.

So we apply the (abstract) Nakayama's Lemma on $(**)$ to see $(\gamma^{p^n}-1)A^{\vee} = 0$.

Finally, this implies $A^{\vee}/(\gamma^{p^n}-1)A^{\vee} = A^{\vee}$. Taking the Pontryagin dual again back, we see this is exactly $A = A^{\Gamma_n}$, as desired. $\square$

Remark: Here in $(\star)$, we used the property that for $f, g \in R$ and A an R-module, $fA/(fg)A \simeq fA \otimes R/g$.

Exercise 3.11

(a) We apply Exercise 3.10 : for any $m \in \mathbb{Z}_{>0}$, we use $A = E(F_\infty)[p^m]$, $n=1$, $\Gamma = Gal(F_\infty/F) \simeq \mathbb{Z}_p$ to see that since $A^\Gamma = E(F)[p^m]$ is finite, we get $E(F_\infty)[p^m] = E(F)[p^m]$. Since this holds for any m, take the direct limit we obtain $E(F_\infty)[p^\infty] = E(F)[p^\infty]$.

(b) To show $E(\mathbb{Q}_\infty)_{tor} = E(\mathbb{Q})_{tor}$, we consider two separated cases:

Case 1 : For $l \neq 2$, $E(\mathbb{Q}_\infty)[l^\infty] = E(\mathbb{Q})[l^\infty] = 0$.

Indeed, for $l \neq 2$, since E has good reduction at 2, we can consider for any $n \geq 0$, by [Silverman, VII.1.4], there is an injection

$$E(\mathbb{Q}_n)[l] \hookrightarrow \tilde{E}(\mathbb{F}_{2^{m(n)}}) \quad \text{——} \ (*)$$

where for $\mathbb{Q}_n/\mathbb{Q}$, the prime 2 has prime $\mathfrak{p}_n$ of $\mathbb{Q}_n$ lying above it with residue field $\mathbb{F}_{2^{m(n)}}$, $m(n) \geq 1$ depending on n. Now we use [Silverman, Exercise 5.13] to see inductively that for any $m \geq 0$,

$$\# \tilde{E}(\mathbb{F}_{2^{m+2}}) = \text{an even number} - \# \tilde{E}(\mathbb{F}_{2^{m+1}}) .$$

So since $\# E(\mathbb{F}_2)$ is 4, we see that $\# \tilde{E}(\mathbb{F}_{2^m})$ is an even number for any $m \geq 0$. Now the injection has righthand side order even and left hand side of possible order l, l^2 and zero. Since l is odd, this forces $E(\mathbb{Q}_n)[l] = 0$.

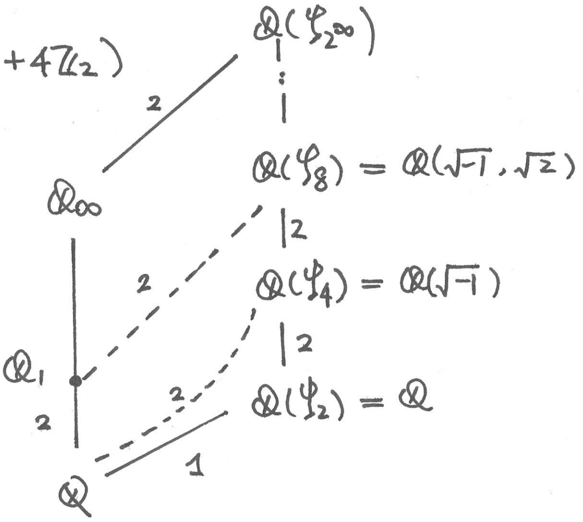
Now we have seen in particular that $E(\mathbb{Q})[l^\infty] = 0$. Moreover, by Exercise 1.15 (a), $E(\mathbb{Q}_\infty)[l^\infty]$ is finite, say they are $Q_1, \cdots, Q_N$ and WLOG we assume they are l-torsion. By such a finiteness result, we can choose a common $n \geq 0$ s.t. $Q_1, \cdots, Q_N \in E(\mathbb{Q}_n)[l^\infty]$. But as we have seen above, $E(\mathbb{Q}_n)[l] = 0$, so this forces $E(\mathbb{Q}_\infty)[l^\infty] = 0$. In particular, this gives $E(\mathbb{Q}_\infty)[l^\infty] = E(\mathbb{Q})[l^\infty] = 0$.

Exercise 3.11

(b0) There is a small gap on computing the first layer $\mathbb{Q}_1/\mathbb{Q}$. Here we are dealing with $\mathbb{Z}_2$-extension, which is a little bit subtle. Note:

<u>Fact</u>: $\mathbb{Z}_2^\times = (\mathbb{Z}/4)^\times \times (1+4\mathbb{Z}_2)$

We consider $\mathbb{Q}(\mu_{2^\infty})$ first:



As $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^\infty})/\mathbb{Q})$ has a order 2 ~~automorphism of~~ element being the complex conjugation, and $(\mathbb{Z}_2^\times)_{tor}$ is exactly of order 2, $\mathbb{Q}_\infty/\mathbb{Q}$ is the maximal real subfield of $\mathbb{Q}_\infty$. Passing to each layers, $\mathbb{Q}_n$ is the maximal real subfield of $\mathbb{Q}(\zeta_{2^{n+2}})$ for $n \geq 0$. In particular, $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$.

<u>Remark</u>: In [Greenberg, LNM note], it is also needed to compute $\mathbb{Q}_2$: so we need to compute the maximal real subfield of $\mathbb{Q}(\zeta_{16})$, which is:

$$\mathbb{Q}_2 = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1}) = \mathbb{Q}(\cos\tfrac{\pi}{8}) = \mathbb{Q}\left(\frac{\sqrt{2+\sqrt{2}}}{2}\right).$$

again quite explicit.

<u>Remark</u>: This is a quite ad-hoc computation since $\mathbb{Z}_2^\times$ has torsion subgroup of order 2, similarly for $\mathbb{Z}_3^\times$, so the order 2 element is precisely corresponds to the complex conjugation. For $p \geq 5$,

$$\mathbb{Z}_p^\times = \mathbb{F}_p^\times \times (1+p\mathbb{Z}_p)$$

with $\mathbb{F}_p^\times$ of order $p-1$. Then $\underline{\mathbb{Q}_n \subseteq \mathbb{Q}(\zeta_{p^{n+1}})}$ (<u>note</u>: when $p=2$, we have $\mathbb{Q}_n \subseteq \mathbb{Q}(\zeta_{p^{n+2}})$) is of index $p-1$, contained in $\mathbb{Q}(\zeta_{p^{n+1}})^+$ but is even smaller. To make it more explicit, we can use [刘畅, 厦门大学硕士论文, 2021] to have a complete description of subfields of $\mathbb{Q}(\zeta_{p^n})$ using some Gauss sums / expontial sums to give the generator. □

Case 2: Then we need to show $E(\mathbb{Q})[2^\infty] = E(\mathbb{Q}(\sqrt{2}))[2^\infty]$, as $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$.

Similar to Exercises in Chapter 1, we choose another prime $l = 7$,

- note $l = 7$ splits completely in $\mathbb{Q}(\sqrt{2})$, we have the chain of injections as E has good reduction at 7

$$E(\mathbb{Q})[2^\infty] \hookrightarrow E(\mathbb{Q}(\sqrt{2}))[2^\infty] \hookrightarrow \tilde{E}(\mathbb{F}_7).$$

- Then we invoke extra informations:

  (i) $E(\mathbb{Q})_{tor}$ has order 8

  (ii) $\tilde{E}(\mathbb{F}_7)$ has order 8 ~~[illegible]~~ —— (※)

  So the injections here are injective maps.

Hence indeed $E(\mathbb{Q})[2^\infty] = E(\mathbb{Q}(\sqrt{2}))[2^\infty]$.

So combining the two cases, we see that indeed $E(\mathbb{Q})_{tor} = E(\mathbb{Q}_\infty)_{tor}$. $\square$

Remark:

(1) As remarked by Greenberg, the hypothesis is satisfied by the particular elliptic curve $y^2 + xy = y^3 - 115x + 392$. This example is used in [Greenberg, LNM, p137-141].

(2) Here different from the exercise, we add a new assumption (※) that $\tilde{E}(\mathbb{F}_7)$ has order 8. This seems indispensable as the same argument is used in [loc cit]. We note that $\tilde{E}(\mathbb{F}_7)$ has the Hasse bound

$$\# \tilde{E}(\mathbb{F}_7) \leq 2\sqrt{7} + 7 + 1 \cong 13.29$$

which is so large compared with 8. Actually, (※) gives

$$a_7 = \# \tilde{E}(\mathbb{F}_7) - 7 - 1 = 0$$

So this actually equivalent to an extra condition that E has good supersingular reduction at $p = 7$. This is indeed the case of the above example.

(3) But we know $E(\mathbb{Q})[2^\infty] = E(\mathbb{Q})_{tor}$ has order 8, embedded as a (normal) subgroup of $\tilde{E}(\mathbb{F}_7)$, so $\# \tilde{E}(\mathbb{F}_7)$ has to be a positive multiple of 8. Then the Hasse bound above forces $\# \tilde{E}(\mathbb{F}_7) = 8$, so we get the "extra" condition (※) for free! (hence E is good supersingular at $p = 7$). $\square$