$$\begin{array}{ccc} \mathrm{Div}^0(\mathrm{S}_1(N)'_{\mathrm{gd}}) & \xrightarrow{\langle d\rangle} & \mathrm{Div}^0(\mathrm{S}_1(N)'_{\mathrm{gd}}) \\ \downarrow & & \downarrow \\ \mathrm{Div}^0(\widetilde{\mathrm{S}}_1(N)') & \xrightarrow{\widetilde{\langle d\rangle}} & \mathrm{Div}^0(\widetilde{\mathrm{S}}_1(N)'). \end{array}$$

Show that the diamond operator in characteristic p on the moduli space and on the modular curve (cf. diagram (8.29)) are compatible in that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Div}^0(\widetilde{\mathrm{S}}_1(N)') & \xrightarrow{\widetilde{\langle d\rangle}} & \mathrm{Div}^0(\widetilde{\mathrm{S}}_1(N)') \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\widetilde{\langle d\rangle}_*} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array} \tag{8.39}$$

(d) Use part (b) and diagram (8.39) to complete the proof that diagram (8.34) commutes.

8.8 Fourier coefficients, L-functions, and Modularity

Recall that if E is an elliptic curve over $\mathbf{Q}$ then its analytic conductor was defined in Section 7.7 as the smallest N such that $X_0(N)$ surjects to E, and its algebraic conductor N_E was described in Section 8.3. Both conductors depend only on the isogeny class over $\mathbf{Q}$ of E. In this section we simply call the algebraic conductor the conductor en route to explaining why the two conductors are in fact equal and no longer need to be distinguished.

Theorem 8.8.1 (Modularity Theorem, Version a_p). *Let E be an elliptic curve over $\mathbf{Q}$ with conductor N_E. Then for some newform $f \in \mathcal{S}_2(\Gamma_0(N_E))$,*

$$a_p(f) = a_p(E) \quad \textit{for all primes } p.$$

This version of Modularity is most obviously related to Version $A_{\mathbf{Q}}$, the version that provides a map $A'_f \longrightarrow E$, since each version involves a newform f, and unsurprisingly the two f's are the same. But since A'_f is a variety rather than a curve, and our policy is to argue using only curves, we give instead a partial proof that Version $X_{\mathbf{Q}}$, providing a map $X_0(N) \longrightarrow E$, implies this version. The argument necessarily requires a little effort to extract f from $X_0(N)$ in consequence of avoiding varieties. Specifically, we prove

Theorem 8.8.2. *Let E be an elliptic curve over $\mathbf{Q}$ with conductor N_E, let N be a positive integer, and let*

$$\alpha : X_0(N) \longrightarrow E$$

be a nonzero morphism over $\mathbf{Q}$ *of curves over* $\mathbf{Q}$*. Then for some newform* $f \in \mathcal{S}_2(\Gamma_0(M_f))$ *where* $M_f \mid N$*,*

$$a_p(f) = a_p(E) \quad \textit{for all primes } p \nmid N_E N.$$

After proving this we will touch on the rest of the argument that Version $X_{\mathbf{Q}}$ of Modularity implies Version a_p, and on the more natural-seeming argument starting from Version $A_{\mathbf{Q}}$.

Proof. The route from $a_p(f)$ for some f to $a_p(E)$ is that

- $a_p(f)$ on A'_f is T_p for each f, by a variant of diagram (6.15), and a sum of factors A'_f over all f is isogenous to $\mathrm{Pic}^0(X_0(N))$, by a variant of Theorem 6.6.6,
- T_p on $\mathrm{Pic}^0(X_0(N))$ reduces to $\sigma_{p,*} + \sigma_p^*$ on $\mathrm{Pic}^0(\widetilde{X}_0(N))$, by the Eichler–Shimura Relation ($X_0(N)$ has good reduction at p because $p \nmid N$),
- $\sigma_{p,*}+\sigma_p^*$ on $\mathrm{Pic}^0(\widetilde{X}_0(N))$ commutes with $\tilde{\alpha}_*$ to become $\sigma_{p,*}+\sigma_p^*$ on $\mathrm{Pic}^0(\widetilde{E})$, by formulas (8.17) and (8.19) (E has good reduction at p because $p \nmid N_E$),
- and finally $\sigma_{p,*} + \sigma_p^*$ on $\mathrm{Pic}^0(\widetilde{E})$ is $a_p(E)$, by Proposition 8.3.2.

Recall some ideas from Section 6.6, given there for the group $\Gamma_1(N)$ and now modified for $\Gamma_0(N)$. The complex vector space $\mathcal{S}_2(\Gamma_0(N))$ has basis

$$\mathcal{B}'_2(N) = \bigcup_f \bigcup_n \bigcup_\sigma f^\sigma(n\tau)$$

where the first union is taken over equivalence class representatives of newforms $f \in \mathcal{S}_2(\Gamma_0(M_f))$ with M_f dividing N, the second over divisors n of N/M_f, and the third over embeddings $\sigma : \mathbf{K}_f \hookrightarrow \mathbf{C}$. Work over $\mathbf{C}$ now, identifying complex algebraic curves and Riemann surfaces, and identifying Picard groups and Jacobians. Then the Picard group associated to $\Gamma_0(N)$ is isogenous to a direct sum of Abelian varieties, both sides being viewed as complex tori,

$$\mathrm{Pic}^0(X_0(N)_{\mathbf{C}}) \longrightarrow \bigoplus_{f,n} A'_{f,\mathbf{C}},$$

and there exists a dual isogeny

$$\bigoplus_{f,n} A'_{f,\mathbf{C}} \longrightarrow \mathrm{Pic}^0(X_0(N)_{\mathbf{C}}).$$

The given map $\alpha : X_0(N) \longrightarrow E$ extends to

$$\alpha_{\mathbf{C}} : X_0(N)_{\mathbf{C}} \longrightarrow E_{\mathbf{C}},$$

viewed as a morphism of complex algebraic curves or as a holomorphic map of compact Riemann surfaces, a surjection in either case.

For any $p \nmid N_E N$ the diagram

$$\begin{array}{ccccc} \bigoplus_{f,n} A'_{f,\mathbf{C}} & \xrightarrow{\prod_{f,n}(a_p(f)-a_p(E))} & \bigoplus_{f,n} A'_{f,\mathbf{C}} & & \\ \downarrow & & \downarrow & & \\ \mathrm{Pic}^0(X_0(N)_{\mathbf{C}}) & \xrightarrow{T_p-a_p(E)} & \mathrm{Pic}^0(X_0(N)_{\mathbf{C}}) & \xrightarrow{\alpha_{\mathbf{C},*}} & \mathrm{Pic}^0(E_{\mathbf{C}}) \end{array} \tag{8.40}$$

has the following properties, to be proved in a moment:

(a) If $a_p(f) \neq a_p(E)$ then the top row surjects from $\bigoplus_n A'_{f,\mathbf{C}}$ to $\bigoplus_n A'_{f,\mathbf{C}}$.
(b) The square commutes.
(c) The composite map on the bottom row is zero.

If $a_p(f) \neq a_p(E)$ for some f and some $p \nmid N_E N$ then in the diagram for that p, mapping $\bigoplus_n A'_{f,\mathbf{C}}$ across the top row takes it to all of $\bigoplus_n A'_{f,\mathbf{C}}$ by property (a), and then mapping this down gives its isogenous image in $\mathrm{Pic}^0(X_0(N)_{\mathbf{C}})$. By property (b) the isogenous image also comes from mapping $\bigoplus_n A'_{f,\mathbf{C}}$ down the left side of the diagram and then halfway across the bottom row. Property (c) now shows that the isogenous image of $\bigoplus_n A'_{f,\mathbf{C}}$ lies in $\ker(\alpha_{\mathbf{C},*})$. Therefore, if for each f there exists a $p \nmid N_E N$ such that $a_p(f) \neq a_p(E)$ then all of $\mathrm{Pic}^0(X_0(N)_{\mathbf{C}})$ lies in $\ker(\alpha_{\mathbf{C},*})$. But $\alpha_{\mathbf{C},*}$ surjects, so this is impossible. That is, there is a newform f such that $a_p(f) = a_p(E)$ for all $p \nmid N_E N$, as we needed to prove.

Returning to diagram (8.40), to prove its property (a) let $a_p(f) \neq a_p(E)$. Recall that $a_p(f)$ is an algebraic integer, and $a_p(E)$ is a rational integer. Thus their difference δ satisfies a minimal monic polynomial with rational integer coefficients,

$$\delta^e + a_1\delta^{e-1} + \cdots + a_{e-1}\delta + a_e = 0, \quad a_1, \ldots, a_e \in \mathbf{Z},\ a_e \neq 0.$$

The resulting relation $\delta(\delta^{e-1} + a_1\delta^{e-2} + \cdots + a_{e-1}) = -a_e$ shows that δ is surjective on $A'_{f,\mathbf{C}}$ as desired, since $-a_e$ is.

Property (b) follows quickly from diagram (6.20) suitably modified from $\Gamma_1(N)$ to $\Gamma_0(N)$.

To prove property (c) switch back to working over $\mathbf{Q}$ and consider the following diagram:

$$\begin{array}{ccccc} \mathrm{Pic}^0(X_0(N)) & \xrightarrow{T_p-a_p(E)} & \mathrm{Pic}^0(X_0(N)) & \xrightarrow{\alpha_*} & \mathrm{Pic}^0(E) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_0(N)) & \xrightarrow{\sigma_{p,*}+\sigma_p^*-a_p(E)} & \mathrm{Pic}^0(\widetilde{X}_0(N)) & \xrightarrow{\tilde{\alpha}_*} & \mathrm{Pic}^0(\widetilde{E}) \\ {\scriptstyle 1}\downarrow & & & & \downarrow{\scriptstyle 1} \\ \mathrm{Pic}^0(\widetilde{X}_0(N)) & \xrightarrow{\tilde{\alpha}_*} & \mathrm{Pic}^0(\widetilde{E}) & \xrightarrow{\sigma_{p,*}+\sigma_p^*-a_p(E)} & \mathrm{Pic}^0(\widetilde{E}). \end{array} \tag{8.41}$$

The top row here is a restriction of the bottom row of diagram (8.40), and it suffices to prove that this restriction doesn't surject (Exercise 8.8.1). The top

left square commutes since it is essentially (8.38) from the Eichler–Shimura Relation, and the top right square commutes by Corollary 8.5.9. The bottom rectangle commutes because formulas (8.17) and (8.19) from earlier in the chapter show that $\sigma_{p,*}$ and σ_p^* commute with $\tilde{\alpha}_*$, and multiplication by $a_p(E)$ certainly commutes with the linear map $\tilde{\alpha}_*$ as well. The second map on the bottom row is zero by Proposition 8.3.2, making the bottom row zero and thus making the middle row zero. So the top row followed by the right vertical arrow to the second row is zero. But the vertical arrow surjects by Theorem 8.5.9. This shows that the top row can't surject, as desired. With properties (a), (b), and (c) of diagram (8.40) established, the proof of Theorem 8.8.2 is complete. □

For Version $X_{\mathbf{Q}}$ of Modularity to imply Version a_p, the newform f of Theorem 8.8.2 needs to have level $M_f = N_E$ and to have Fourier coefficients $a_p(f) = a_p(E)$ for all p.

Strong Multiplicity One shows that all the Fourier coefficients of f are rational integers. To see this, recall that if σ is any automorphism of $\overline{\mathbf{Q}}$ then the conjugate of f under σ is defined as

$$f^\sigma(\tau) = \sum_{n=1}^{\infty} a_n(f)^\sigma q^n.$$

According to Theorem 6.5.4 all conjugates of f are again newforms. In this case they are all equal to f itself because for all $p \nmid N$ and all σ,

$$a_p(f) = a_p(E) \implies a_p(f) \in \mathbf{Z} \implies a_p(f)^\sigma = a_p(f),$$

so that $f^\sigma = f$ by Strong Multiplicity One. This means that the Fourier coefficients of f are algebraic integers invariant under $\mathrm{Aut}(\overline{\mathbf{Q}})$, i.e., the Fourier coefficients are rational integers as claimed. Thus f has number field $\mathbf{K}_f = \mathbf{Q}$.

Obtaining Version a_p of Modularity from here requires results beyond the scope of this book, but we sketch the ideas. As quoted in Section 7.7, the Abelian variety A'_f, viewed as a variety over $\mathbf{Q}$, has dimension $[\mathbf{K}_f : \mathbf{Q}] = 1$, i.e., A'_f is an elliptic curve over $\mathbf{Q}$. The map $X_0(N) \longrightarrow \mathrm{Pic}^0(X_0(N)) \longrightarrow A'_f$ is defined over $\mathbf{Q}$, so we can run the proof of Theorem 8.8.2 again to show that there exists a newform g such that $a_p(g) = a_p(A'_f)$ for all but finitely many p. The proof in this case shows that $g = f$, so

$$a_p(f) = a_p(A'_f) \quad \text{for all but finitely many } p. \tag{8.42}$$

Carayol [Car86], building on the work of Eichler–Shimura, Langlands, and Deligne, showed that in fact $a_p(f) = a_p(A'_f)$ for all p, and the level of f is the conductor of A'_f, notated $M_f = N_f$, and this is also the analytic conductor of A_f. But also, the work so far gives an isogeny over $\mathbf{Q}$ from A'_f to E, so that $a_p(A'_f) = a_p(E)$ for all p and the conductor of A'_f is the conductor of E, that is, $N_f = N_E$. This gives $a_p(f) = a_p(E)$ for all p and $M_f = N_E$, i.e., Version a_p

of Modularity. It also shows that the analytic and algebraic conductors of E are the same. That is, the newform f associated to E has the same level as the smallest modular curve $X_0(N)$ that maps to E.

Starting instead from Version $A_{\mathbf{Q}}$ of Modularity, that is, starting from a map $\alpha : A'_f \longrightarrow E$, a more natural-looking proof that $a_p(f) = a_p(E)$ for all $p \nmid N_E M_f$ (where N_E is the conductor of E and M_f is the level of f) would set up a diagram analogous to (8.41),

$$\begin{array}{ccccc}
A'_f & \xrightarrow{a_p(f)-a_p(E)} & A'_f & \xrightarrow{\alpha} & E \\
\downarrow & & \downarrow & & \downarrow \\
\widetilde{A'_f} & \xrightarrow{\sigma_{p,*}+\sigma_p^*-a_p(E)} & \widetilde{A'_f} & \xrightarrow{\tilde{\alpha}} & \widetilde{E} \\
{\scriptstyle 1}\downarrow & & & & \downarrow{\scriptstyle 1} \\
\widetilde{A'_f} & \xrightarrow{\tilde{\alpha}} & \widetilde{E} & \xrightarrow{\sigma_{p,*}+\sigma_p^*-a_p(E)} & \widetilde{E}.
\end{array}$$

If $a_p(f) \neq a_p(E)$ then the top row is surjective, as is $E \longrightarrow \widetilde{E}$, but the bottom row is zero and hence the middle row is zero, giving a contradiction because all the rectangles commute. However, this argument makes use of the structure of A'_f as a variety over $\mathbf{Q}$, reduces the variety modulo p, and then makes further use of the structure of the reduction as a variety over $\mathbf{F}_p$, invoking algebraic geometry well beyond the scope of this book. By contrast our proof of Theorem 8.8.2 makes no reference to the variety structure of $\mathrm{Pic}^0(X_0(N))$, and it uses $\mathrm{Pic}^0(\widetilde{X}_0(N))$, the Picard group of the reduced curve, rather than reducing an Abelian variety.

Section 1.3 mentioned that some complex tori have complex multiplication, endomorphisms other than $\{[N] : N \in \mathbf{Z}\}$. This notion extends to algebraic elliptic curves, providing more examples of Modularity. For example the elliptic curve

$$E : y^2 = x^3 - d, \quad d \in \mathbf{Z},\ d \neq 0$$

has the order 3 automorphism $(x, y) \mapsto (\mu_3 x, y)$ over $\mathbf{Q}(\mu_3)$, and its ring of endomorphisms is isomorphic to $A = \mathbf{Z}[\mu_3]$. As in Exercise 8.3.6(b), $a_p(E) = 0$ for all $p \equiv 2 \pmod 3$ for which the displayed Weierstrass equation is minimal. The theory of complex multiplication in fact describes $a_p(E)$ for all p: there exist an integer $N \mid 12 \prod_{p|d} p$ and a character $\chi : (A/NA)^* \longrightarrow \mathbf{C}^*$ of order 6 such that $\chi(u) = u^{-1}$ for $u \in A^*$, $\chi(a) = (a/3)$ (Legendre symbol) for $a \in (\mathbf{Z}/N\mathbf{Z})^*$, and

$$a_p(E) = \tfrac{1}{6} \sum_{\substack{n \in A \\ |n|^2 = p}} \chi(n) n.$$

(See Chapter 2 of [Sil94] for proofs of these results, and see Exercise II.5.7 of [Kob93] for the case $d = -16$, giving $N = 3$.) The solution-counts of E are

the Fourier coefficients of the function

$$\theta_{2,\chi}(\tau) = \tfrac{1}{6} \sum_{n \in A} \chi(n) n e^{2\pi i |n|^2 \tau}, \quad \tau \in \mathcal{H}.$$

This function is a modular form of level $3N^2$ by the weight 2 version of Hecke's construction in Section 4.11. It is a normalized eigenform by an argument similar to the one in Section 5.9 for the weight 1 theta function. For the minimal choice of N, it is in fact a newform of level $3N^2 = N_E$, thus illustrating Version a_p of Modularity for these elliptic curves E. The elliptic curves E over $\mathbf{Q}$ with complex multiplication form a small class of examples—for example they have only a finite set of j-invariants—but they are important in number theory, and Shimura's proof of Version $X_{\mathbf{Q}}$ of Modularity for such curves [Shi71] provided evidence for the algebraic formulations of Modularity in general.

Version a_p of the Modularity Theorem rephrases in terms of L-functions. Recall from Chapter 5 that if $f \in \mathcal{S}_2(\Gamma_0(N))$ is a newform then its L-function is

$$L(s, f) = \sum_{n=1}^{\infty} a_n(f) n^{-s} = \prod_p (1 - a_p(f) p^{-s} + \mathbf{1}_N(p) p^{1-2s})^{-1}, \tag{8.43}$$

with convergence in a right half plane. For any elliptic curve E over $\mathbf{Q}$ let $\mathbf{1}_E$ be the trivial character modulo the conductor N of E as in Section 8.3. The *Hasse–Weil L-function of E*, encoding all the solution-counts $a_p(E)$, is

$$L(s, E) = \prod_p (1 - a_p(E) p^{-s} + \mathbf{1}_E(p) p^{1-2s})^{-1}.$$

From Section 8.3 we have the definitions

$$a_p(E) = 1, \qquad a_{p^e}(E) = p^e + 1 - |\widetilde{E}(\mathbf{F}_{p^e})|, \quad e \geq 1$$

and the recurrence

$$a_{p^e}(E) = a_p(E) a_{p^{e-1}}(E) - \mathbf{1}_E(p) p a_{p^{e-2}}(E), \quad e \geq 2.$$

One more definition,

$$a_{mn}(E) = a_m(E) a_n(E), \quad (m, n) = 1,$$

completes the analogy between the values $a_n(E)$ and the Fourier coefficients $a_n(f)$ of a newform. As in Chapter 5, the L-function of an elliptic curve is now

$$L(s, E) = \sum_{n=1}^{\infty} a_n(E) n^{-s} = \prod_p (1 - a_p(E) p^{-s} + \mathbf{1}_E(p) p^{1-2s})^{-1}. \tag{8.44}$$

Half plane convergence of $L(s, E)$ can be established as well by estimating $a_p(E)$. But this is unnecessary since comparing the products in (8.43) and (8.44) shows that Version a_p of Modularity is equivalent to

Theorem 8.8.3 (Modularity Theorem, Version L). *Let E be an elliptic curve over $\mathbf{Q}$ with conductor N_E. Then for some newform $f \in \mathcal{S}_2(\Gamma_0(N_E))$,*

$$L(s, f) = L(s, E).$$

Faltings's Isogeny Theorem (Corollary 5.2 in Chapter 2 of [CS86]), a deep result, now shows that this Version L of Modularity implies

Theorem 8.8.4 (Modularity Theorem, strong Version $A_{\mathbf{Q}}$). *Let E be an elliptic curve over $\mathbf{Q}$ with conductor N_E. Then for some newform $f \in \mathcal{S}_2(\Gamma_0(N_E))$ the Abelian variety A'_f is also an elliptic curve over $\mathbf{Q}$ and there exists an isogeny over $\mathbf{Q}$*

$$A'_f \longrightarrow E.$$

To see this, suppose that by Version L we have $L(s, f) = L(s, E)$. Then f has rational coefficients, making A'_f an elliptic curve. Equation (8.42) shows that $L(s, A'_f)$ and $L(s, f)$ have the same Euler product factors for all but finitely many primes p. So the same is true of $L(s, A'_f)$ and $L(s, E)$, and now Faltings's Theorem gives an isogeny $A'_f \longrightarrow E$.

Version L of the Modularity Theorem shows that the half plane convergence, analytic continuation, and functional equation of $L(s, f)$ from Theorem 5.10.2 now apply to $L(s, E)$. This is important because the continued $L(s, E)$ is conjectured to contain sophisticated information about the group structure of E. Specifically, since $E(\mathbf{Q})$ is a finitely generated Abelian group it takes the form

$$E(\mathbf{Q}) \cong T \oplus \mathbf{Z}^r,$$

where T is the torsion subgroup and r is the rank. The rank is much harder to compute than the torsion. However,

Conjecture 8.8.5 (Weak Birch and Swinnerton-Dyer Conjecture). *Let E be an elliptic curve defined over $\mathbf{Q}$. Then the order of vanishing of $L(s, E)$ at $s = 1$ is the rank of $E(\mathbf{Q})$. That is, if $E(\mathbf{Q})$ has rank r then*

$$L(s, E) = (s - 1)^r g(s), \quad g(1) \neq 0, \infty.$$

The original half plane of convergence of $L(s, E)$ is $\{\mathrm{Re}(s) > 2\}$, and the functional equation then determines $L(s, E)$ for $\mathrm{Re}(s) < 0$, but the behavior of $L(s, E)$ at the center of the remaining strip $\{0 \leq \mathrm{Re}(s) \leq 2\}$ is what conjecturally determines the rank of $E(\mathbf{Q})$. The Birch and Swinnerton-Dyer Conjecture would give an algorithm for finding all rational points on elliptic curves, and it would give an effective method for finding imaginary quadratic fields with a given class number. For more on the Birch and Swinnerton-Dyer Conjecture see [Tat02], Appendix C.16 of [Sil86], or Chapter 17 of [Hus04].

Exercise

8.8.1. Let $\beta_{\mathbf{C}}$ denote the map of the bottom row of diagram (8.40),

$$\beta_{\mathbf{C}} : \mathrm{Pic}^0(X_0(N)_{\mathbf{C}}) \xrightarrow{\alpha_* \circ (T_p - a_p(E))} \mathrm{Pic}^0(E_{\mathbf{C}}).$$

Augment $\beta_{\mathbf{C}}$ to get a map of complex algebraic curves,

$$\gamma_{\mathbf{C}} : X_0(N) \longrightarrow \mathrm{Pic}^0(X_0(N)_{\mathbf{C}}) \xrightarrow{\beta_{\mathbf{C}}} \mathrm{Pic}^0(E_{\mathbf{C}}) \longrightarrow E_{\mathbf{C}}.$$

Here the first stage is $P \mapsto [(P)-(P_0)]$ where $P_0 \in X_0(N)_{\mathbf{C}}$ is a base point, and the third stage is $[\sum(Q_i)] \mapsto \sum Q_i$. Since $\gamma_{\mathbf{C}}$ is a composite of holomorphic maps, it is holomorphic as a map of Riemann surfaces and therefore it is a morphism as a map of complex algebraic curves.

(a) Show that if $\gamma_{\mathbf{C}}$ is zero then $\beta_{\mathbf{C}}$ is zero. (A hint for this exercise is at the end of the book.)

(b) Assume that the base point P_0 in part (a) has algebraic coordinates. Show that $\gamma_{\mathbf{C}}$ is defined over $\overline{\mathbf{Q}}$ as follows. It suffices to show that $\gamma_{\mathbf{C}}^{\sigma} = \gamma_{\mathbf{C}}$ for all $\sigma \in \mathrm{Aut}(\mathbf{C}/\overline{\mathbf{Q}})$. Compute that for any $P \in X_0(N)_{\mathbf{C}}$ and any σ,

$$\gamma_{\mathbf{C}}(P^{\sigma}) = \gamma_{\mathbf{C}}(P)^{\sigma} = \gamma_{\mathbf{C}}^{\sigma}(P^{\sigma}).$$

Since P^{σ} can be any point of $X_0(N)_{\mathbf{C}}$, this gives the result.

(c) Let β denote the map of the top row of diagram (8.41),

$$\beta : \mathrm{Pic}^0(X_0(N)) \xrightarrow{\alpha_* \circ (T_p - a_p(E))} \mathrm{Pic}^0(E).$$

This is the restriction of $\beta_{\mathbf{C}}$ to $\overline{\mathbf{Q}}$-points. Consider the corresponding restriction of $\gamma_{\mathbf{C}}$, viewed as a morphism over $\overline{\mathbf{Q}}$ of algebraic curves over $\overline{\mathbf{Q}}$ according to part (b),

$$\gamma : X_0(N) \longrightarrow \mathrm{Pic}^0(X_0(N)) \xrightarrow{\beta} \mathrm{Pic}^0(E) \longrightarrow E.$$

Use the maps of curves γ and $\gamma_{\mathbf{C}}$ to show that if β does not surject then $\beta_{\mathbf{C}}$ is zero. This was used in proving property (c) of diagram (8.40). The result is immediate from quoting that as morphisms from varieties to curves, β and $\beta_{\mathbf{C}}$ are both constant or surjective, but the argument in this exercise uses only the algebraic geometry of curves.