

7.6 Function fields over \mathbf{Q}

Working over the complex numbers \mathbf{C} we have considered the universal curve E_j and the field containments

$$\mathbf{C}(j) \subset \mathbf{C}(j, E_j[N]) \subset \overline{\mathbf{C}(j)}.$$

Corollary 7.5.3 established that the extension $\mathbf{C}(j, E_j[N])/\mathbf{C}(j)$ is Galois with group $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. This section studies the situation when the underlying field is changed to the rational numbers \mathbf{Q} . The result will be that the Galois group enlarges to $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. Large enough subgroups correspond to intermediate fields that are the function fields of algebraic curves over the rational numbers. The next section will show that the intermediate fields $\mathbf{Q}(j, f_0)$ and $\mathbf{Q}(j, f_1)$ define $X_0(N)$ and $X_1(N)$ over \mathbf{Q} . The field $\mathbf{Q}(j, f_{1,0}, f_{0,1})$ defines $X(N)$ over the field $\mathbf{Q}(\mu_N)$ where μ_N is the group of complex N th roots of unity.

Since \mathbf{Q} is the prime subfield of \mathbf{C} , much of the algebraic structure from the previous section carries over. The equation defining E_j has its coefficients in $\mathbf{Q}(j)$. Viewing the curve as defined over this field means considering points $(x, y) \in \overline{\mathbf{Q}(j)}^2$ satisfying the equation. This includes the nonzero points of $E_j[N]$ over $\mathbf{C}(j)$ from before, and in the field containments

$$\mathbf{Q}(j) \subset \mathbf{Q}(j, E_j[N]) \subset \overline{\mathbf{Q}(j)}$$

the extension $\mathbf{Q}(j, E_j[N])/\mathbf{Q}(j)$ is again Galois. The only difference between the field theory over \mathbf{Q} and over \mathbf{C} will involve μ_N .

Consider the Galois group

$$H_{\mathbf{Q}} = \mathrm{Gal}(\mathbf{Q}(\mu_N, j, E_j[N])/\mathbf{Q}(j))$$

and the representation

$$\rho : H_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$$

describing how $H_{\mathbf{Q}}$ permutes $E_j[N]$. This is defined as before in terms of the ordered basis (P_τ, Q_τ) of $E_j[N]$ over $\mathbf{Z}/N\mathbf{Z}$ from (7.11), so that

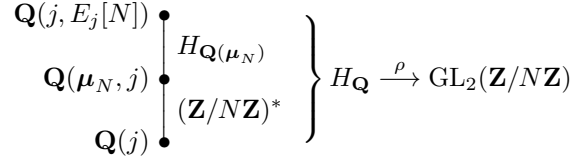
$$\begin{bmatrix} P_\tau^\sigma \\ Q_\tau^\sigma \end{bmatrix} = \rho(\sigma) \begin{bmatrix} P_\tau \\ Q_\tau \end{bmatrix}, \quad \sigma \in H_{\mathbf{Q}}.$$

Lemma 7.6.1. *The function $\det \rho$ describes how $H_{\mathbf{Q}}$ permutes μ_N ,*

$$\mu^\sigma = \mu^{\det \rho(\sigma)}, \quad \mu \in \mu_N, \quad \sigma \in H_{\mathbf{Q}}.$$

(Here μ^σ is μ acted on by σ while $\mu^{\det \rho(\sigma)}$ is μ raised to the power $\det \rho(\sigma)$.)

This is shown with the Weil pairing as in the proof of Corollary 7.5.3 (Exercise 7.6.1). To use the lemma, suppose $\sigma \in H_{\mathbf{Q}}$ fixes $E_j[N]$. This means

**Figure 7.3.** Fields and groups over \mathbf{Q}

that $\sigma \in \ker(\rho)$, so $\sigma \in \ker(\det \rho)$ and the lemma says that σ fixes μ_N . Thus $\mu_N \subset \mathbf{Q}(j, E_j[N])$ by Galois theory, showing that $H_{\mathbf{Q}}$ is in fact the Galois group of $\mathbf{Q}(j, E_j[N])$ over $\mathbf{Q}(j)$, the analog over \mathbf{Q} of the group H in the proof of Corollary 7.5.3. Consider the configuration of fields and groups in Figure 7.3. Since the field extension is generated by $E_j[N]$, now ρ clearly is injective, and by the lemma it restricts to

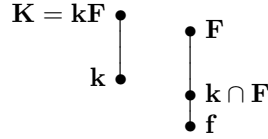
$$\rho : H_{\mathbf{Q}(\mu_N)} \longrightarrow \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}).$$

To analyze the images of $H_{\mathbf{Q}}$ and $H_{\mathbf{Q}(\mu_N)}$ under ρ , recall a result from Galois theory.

Lemma 7.6.2 (Restriction Lemma). *Let \mathbf{k} and \mathbf{F} be extension fields of \mathbf{f} inside \mathbf{K} with \mathbf{F}/\mathbf{f} Galois. Suppose $\mathbf{K} = \mathbf{kF}$. Then \mathbf{K}/\mathbf{k} is Galois, there is a natural injection*

$$\mathrm{Gal}(\mathbf{K}/\mathbf{k}) \longrightarrow \mathrm{Gal}(\mathbf{F}/\mathbf{f}),$$

and the image is $\mathrm{Gal}(\mathbf{F}/(\mathbf{k} \cap \mathbf{F}))$.

**Figure 7.4.** Setup for the Restriction Lemma

Proof. The situation is shown in Figure 7.4. Any map $\sigma : \mathbf{K} \longrightarrow \overline{\mathbf{K}}$ fixing \mathbf{k} restricts to a map $\mathbf{F} \longrightarrow \overline{\mathbf{F}}$ fixing $\mathbf{k} \cap \mathbf{F}$. Since the extension $\mathbf{F}/(\mathbf{k} \cap \mathbf{F})$ is Galois, the restriction is an automorphism of \mathbf{F} and therefore σ is an automorphism of $\mathbf{K} = \mathbf{kF}$. This shows that \mathbf{K}/\mathbf{k} is Galois and that restriction gives a homomorphism

$$\mathrm{Gal}(\mathbf{K}/\mathbf{k}) \longrightarrow \mathrm{Gal}(\mathbf{F}/(\mathbf{k} \cap \mathbf{F})) \subset \mathrm{Gal}(\mathbf{F}/\mathbf{f}).$$

If the restriction of some σ fixes \mathbf{F} along with \mathbf{k} then it fixes \mathbf{K} and is trivial, so the restriction map injects. Since the fixed field of \mathbf{K} under $\text{Gal}(\mathbf{K}/\mathbf{k})$ is \mathbf{k} , the fixed field of \mathbf{F} under the restriction is $\mathbf{k} \cap \mathbf{F}$ and so restriction maps to all of $\text{Gal}(\mathbf{F}/\mathbf{k} \cap \mathbf{F})$. \square

One application of the lemma is implicit in Figure 7.3, where $(\mathbf{Z}/N\mathbf{Z})^*$ is displayed as $\text{Gal}(\mathbf{Q}(\mu_N, j)/\mathbf{Q}(j))$ (Exercise 7.6.2). For another, consider the situation shown in Figure 7.5.

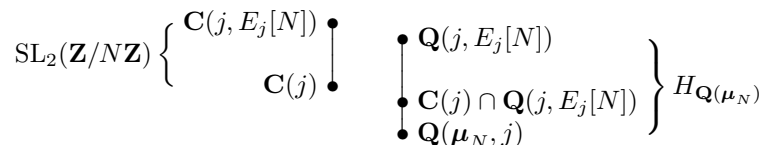


Figure 7.5. Applying the Restriction Lemma

The Restriction Lemma shows that $\text{SL}_2(\mathbf{Z}/N\mathbf{Z})$ injects into $H_{\mathbf{Q}(\mu_N)}$. But also ρ injects in the other direction, making the two groups isomorphic since they are finite,

$$\rho : H_{\mathbf{Q}(\mu_N)} \xrightarrow{\sim} \text{SL}_2(\mathbf{Z}/N\mathbf{Z}).$$

Now the lemma also shows that $\mathbf{C}(j) \cap \mathbf{Q}(j, E_j[N]) = \mathbf{Q}(\mu_N, j)$, and intersecting with $\overline{\mathbf{Q}}$ gives

$$\mathbf{Q}(j, E_j[N]) \cap \overline{\mathbf{Q}} = \mathbf{Q}(\mu_N).$$

Also, Figure 7.3 now shows that

$$|H_{\mathbf{Q}}| = |H_{\mathbf{Q}(\mu_N)}| |(\mathbf{Z}/N\mathbf{Z})^*| = |\text{SL}_2(\mathbf{Z}/N\mathbf{Z})| |(\mathbf{Z}/N\mathbf{Z})^*|.$$

But $|\text{SL}_2(\mathbf{Z}/N\mathbf{Z})| |(\mathbf{Z}/N\mathbf{Z})^*| = |\text{GL}_2(\mathbf{Z}/N\mathbf{Z})|$, so the representation ρ surjects,

$$\rho : H_{\mathbf{Q}} \xrightarrow{\sim} \text{GL}_2(\mathbf{Z}/N\mathbf{Z}).$$

This lets us specify which intermediate fields of $\mathbf{Q}(j, E_j[N])/\mathbf{Q}(j)$ correspond to algebraic curves over \mathbf{Q} . Let \mathbf{K} be an intermediate field and let the corresponding subgroup of $H_{\mathbf{Q}}$ be $K = \text{Gal}(\mathbf{Q}(j, E_j[N])/\mathbf{K})$, as in Figure 7.6.

Recall that $\det \rho$ describes how $H_{\mathbf{Q}}$ permutes μ_N . This gives the equivalences

$$\begin{aligned} \mathbf{K} \cap \overline{\mathbf{Q}} = \mathbf{Q} &\iff \mathbf{K} \cap \mathbf{Q}(\mu_N) = \mathbf{Q} \\ &\iff \det \rho : K \longrightarrow (\mathbf{Z}/N\mathbf{Z})^* \text{ surjects.} \end{aligned}$$

Summing up the results of this section,

$$\left. \begin{array}{c} \mathbf{Q}(j, E_j[N]) \\ \mathbf{K} \\ \mathbf{Q}(j) \end{array} \right\} K \Bigg\} H_{\mathbf{Q}} \xrightarrow{\rho} \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$$

Figure 7.6. Subgroup and fixed field

Theorem 7.6.3. *Let $H_{\mathbf{Q}}$ denote the Galois group of the field extension $\mathbf{Q}(j, E_j[N])/\mathbf{Q}(j)$. There is an isomorphism*

$$\rho : H_{\mathbf{Q}} \xrightarrow{\sim} \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}).$$

Let \mathbf{K} be an intermediate field and let K be the corresponding subgroup of $H_{\mathbf{Q}}$. Then

$$\mathbf{K} \cap \overline{\mathbf{Q}} = \mathbf{Q} \iff \det \rho : K \longrightarrow (\mathbf{Z}/N\mathbf{Z})^* \text{ surjects.}$$

Thus \mathbf{K} is the function field of an algebraic curve over \mathbf{Q} if and only if $\det \rho$ surjects.

The last statement in the theorem follows from Theorem 7.2.5.

Exercises

7.6.1. Prove Lemma 7.6.1.

7.6.2. Justify the relation $\mathrm{Gal}(\mathbf{Q}(\mu_N, j)/\mathbf{Q}(j)) \cong (\mathbf{Z}/N\mathbf{Z})^*$ shown in Figure 7.3.

7.7 Modular curves as algebraic curves and Modularity

This section defines the modular curves $X_0(N)$ and $X_1(N)$ as algebraic curves over \mathbf{Q} and then restates the Modularity Theorem algebraically.

Consider three intermediate fields of the extension $\mathbf{Q}(j, E_j[N])/\mathbf{Q}(j)$,

$$\mathbf{K}_0 = \mathbf{Q}(j, f_0), \quad \mathbf{K}'_0 = \mathbf{Q}(j, j_N), \quad \mathbf{K}_1 = \mathbf{Q}(j, f_1),$$

analogous to the function fields $\mathbf{C}(j, f_0) = \mathbf{C}(j, j_N)$ and $\mathbf{C}(j, f_1)$ of the modular curves $X_0(N)$ and $X_1(N)$ as complex algebraic curves. The subgroups K_0 , K'_0 , and K_1 of $H_{\mathbf{Q}}$ corresponding to \mathbf{K}_0 , \mathbf{K}'_0 , and \mathbf{K}_1 satisfy (Exercise 7.7.1)

$$\rho(K_0) = \rho(K'_0) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \right\}, \quad \rho(K_1) = \left\{ \pm \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \right\}, \quad (7.13)$$

running through all such matrices in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, so in fact $\mathbf{K}_0 = \mathbf{K}'_0$. Thus $\det \rho : K_j \longrightarrow (\mathbf{Z}/N\mathbf{Z})^*$ surjects for $j = 0, 1$, and so by Theorem 7.6.3 the

A First Course in Modular Forms

Diamond, F.; Shurman, J.

2005, XVI, 450 p. 57 illus., Hardcover

ISBN: 978-0-387-23229-4