7.6 Function fields over $\mathbb{Q}$

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

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

Corollary 7.5.3 established that the extension $\mathbb{C}(j, E_j[N])/\mathbb{C}(j)$ is Galois with group $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})$. This section studies the situation when the underlying field is changed to the rational numbers $\mathbb{Q}$. The result will be that the Galois group enlarges to $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. 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 $\mathbb{Q}(j, f_0)$ and $\mathbb{Q}(j, f_1)$ define $X_0(N)$ and $X_1(N)$ over $\mathbb{Q}$. The field $\mathbb{Q}(j, f_1, 0, f_0)$ defines $X(N)$ over the field $\mathbb{Q}(\mu_N)$ where $\mu_N$ is the group of complex $N$th roots of unity.

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

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

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

Consider the Galois group

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

and the representation

$$\rho : H_\mathbb{Q} \rightarrow \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

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

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

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

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

(Here $\mu^\sigma$ is $\mu$ acted on by $\sigma$ while $\mu^{\det \rho(\sigma)}$ is $\mu$ 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 $\sigma \in H_\mathbb{Q}$ fixes $E_j[N]$. This means
that $\sigma \in \ker(\rho)$, so $\sigma \in \ker(\det \rho)$ and the lemma says that $\sigma$ fixes $\mu_N$. Thus $\mu_N \subset \mathbb{Q}(j, E_j[N])$ by Galois theory, showing that $H_{\mathbb{Q}}$ is in fact the Galois group of $\mathbb{Q}(j, E_j[N])$ over $\mathbb{Q}(j)$, the analog over $\mathbb{Q}$ 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 $\rho$ clearly is injective, and by the lemma it restricts to $\rho : H_{\mathbb{Q}(\mu_N)} \longrightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

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

**Lemma 7.6.2 (Restriction Lemma).** Let $k$ and $F$ be extension fields of $f$ inside $K$ with $F/f$ Galois. Suppose $K = kF$. Then $K/k$ is Galois, there is a natural injection
\[ \text{Gal}(K/k) \longrightarrow \text{Gal}(F/f), \]
and the image is $\text{Gal}(F/(k \cap F))$.

**Proof.** The situation is shown in Figure 7.4. Any map $\sigma : K \longrightarrow \overline{K}$ fixing $k$ restricts to a map $F \longrightarrow \overline{F}$ fixing $k \cap F$. Since the extension $F/(k \cap F)$ is Galois, the restriction is an automorphism of $F$ and therefore $\sigma$ is an automorphism of $K = kF$. This shows that $K/k$ is Galois and that restriction gives a homomorphism
\[ \text{Gal}(K/k) \longrightarrow \text{Gal}(F/(k \cap F)) \subset \text{Gal}(F/f). \]
If the restriction of some $\sigma$ fixes $F$ along with $k$ then it fixes $K$ and is trivial, so the restriction map injects. Since the fixed field of $K$ under $\text{Gal}(K/k)$ is $k$, the fixed field of $F$ under the restriction is $k \cap F$ and so restriction maps to all of $\text{Gal}(F/k \cap F)$.

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

\[ \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \left\{ \begin{array}{c} C(j, E_j[N]) \bullet \quad Q(j, E_j[N]) \\ C(j) \bullet \quad C(j) \cap Q(j, E_j[N]) \\ Q(\mu_N, j) \end{array} \right\} H_{\mathbb{Q}(\mu_N)} \]

\textbf{Figure 7.5. Applying the Restriction Lemma}

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

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

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

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

Also, Figure 7.3 now shows that

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

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

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

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

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

$K \cap \overline{Q} = \mathbb{Q} \iff K \cap Q(\mu_N) = \mathbb{Q}$

$\iff \det \rho : K \rightarrow (\mathbb{Z}/N\mathbb{Z})^*$ surjects.

Summing up the results of this section,
Theorem 7.6.3. Let $H_Q$ denote the Galois group of the field extension $Q(j, E_j[N])/Q(j)$. There is an isomorphism

$$\rho : H_Q \xrightarrow{\sim} \text{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Let $K$ be an intermediate field and let $K$ be the corresponding subgroup of $H_Q$. Then

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

Thus $K$ is the function field of an algebraic curve over $Q$ 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 $\text{Gal}(Q(\mu_N,j)/Q(j)) \cong (\mathbb{Z}/N\mathbb{Z})^*$ 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 $Q$ and then restates the Modularity Theorem algebraically.

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

$$K_0 = Q(j, f_0), \quad K'_0 = Q(j, jN), \quad K_1 = Q(j, f_1),$$

analogous to the function fields $C(j, f_0) = C(j, jN)$ and $C(j, f_1)$ 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 $H_Q$ corresponding to $K_0$, $K'_0$, and $K_1$ satisfy (Exercise 7.7.1)

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

running through all such matrices in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$, so in fact $K_0 = K'_0$. Thus $\det \rho : K_j \to (\mathbb{Z}/N\mathbb{Z})^*$ 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