ANT Final Project: Modular Curves and Galois Covers

Jacob Lewis

December 7, 2007

Contents

1 Introduction **1**

2 Algebraic Curves **2**

2.1 Morphisms between Curves 3

2.2 Divisors on Curves 4

2.3 Galois Groups and Deck Transformations 5

2.4 Ramification and Hurwitz's Theorem 5

3 Modular Groups and Modular Curves **6**

3.1 Examples and Relationship with Elliptic Curves 7

4 Galois Coverings of Modular Curves **10**

References **11**

1 Introduction

Many concepts from algebraic number theory–particularly those which rely only on the fact that the ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain–have direct geometric analogues on algebraic curves. In Section 2, we will examine some of these analogues, such as unique factorization of ideals, ramification, and class groups. We will then specialize to modular curves, which are interesting to algebraic number theorists due to their relationship with families of elliptic curves. Section 3 defines what modular curves are, and Section 4 gives examples of Galois coverings of modular curves.

2 Function Fields of Curves and Analogies to Number Fields

Recall that for K a number field, its ring of algebraic integers $\mathcal{O}_K$ is a Dedekind domain. Recall also that in a Dedekind domain R, every nonzero prime ideal is maximal, every ideal has a unique (up to reordering of factors) decomposition as a product of prime ideals, and every fractional ideal of R in $\mathrm{Frac}(R)$ has an inverse. (Each of these, in fact, is equivalent to the statement that R is a Dedekind domain [DF, Thm. 16.15].)

We next recall some results about nonsingular projective curves. For details and proofs, see [Hart, §I.6]. Let C be a nonsingular projective curve over an algebraically closed field k, and $U = \operatorname{Spec} R$ an affine open subset of C. Then R is a noetherian ring of Krull dimension 1 over k which is integrally closed in its field of fractions $K(C)$, i.e. R is a Dedekind Domain. Moreover, $K(C)$ is a finitely generated field extension of k with transcendence degree 1, and up to isomorphism $K(C)$ does not depend on the choice of U. We call $K(C)$ the *function field* of C. Every finitely generated field extension of k with transcendence degree 1 is the function field of a nonsingular projective curve over k, and up to isomorphism the correspondence $C \mapsto K(C)$ is 1-to-1.

Points of C are in bijection with discrete valuation rings of $K(C)$ over k. The DVR corresponding to a point $p \in C$ is the *local ring* of p, denoted $\mathcal{O}_{C,p}$. The local ring can be defined as follows: choose an open affine $U = \operatorname{Spec} R \subset C$ containing p, and let $\mathfrak{p}$ be the prime ideal of R corresponding to p. Then $\mathcal{O}_{C,p} = R_\mathfrak{p}$ is the localization of R at $\mathfrak{p}$. We will denote the valuation on $\mathcal{O}_{C,p}$ by ν_p.

(If k is not algebraically closed, then the theory in this section still works, provided we modify the categories we are considering slightly. On the curve side, we restrict our attention to curves X on which the only globally defined functions are constant, i.e. $\mathcal{O}_X(X) = k$. On the function field side, we restrict to function fields$K$ over k such that k is algebraically closed in K, i.e. k is the set of elements of K which are algebraic over k. See [Lor, §VII.4] for details.)

Since C is projective, we can embed C into some projective space via some $\psi : C \hookrightarrow \mathbb{P}^N_k$. Let $I \subset k[x_0, x_1, \ldots, x_N] = S$ be the homogeneous ideal of $\psi(C)$, and let $g(r) = \deg_k \left(\frac{S}{I}\right)_r$ be the dimension of the r-th graded piece of the *homogeneous coordinate ring* S/I of $\psi(C)$. Then there exists a unique polynomial $P_{\psi(C)}(t) \in \mathbb{Z}[t]$ such that for all sufficiently large r, $g(r) = P_{\psi(C)}(r)$. We call $P_{\psi(C)}$ the *Hilbert polynomial* of $\psi(C)$. We define the *genus* $g(C)$ of C to be $1 - P_{\psi(C)}(0)$. As the name suggests, the genus of C does not depend on a choice of ψ. As we shall see, $g(C)$ is an important numerical invariant of C. When $k = \mathbb{C}$, the genus defined here agrees with the definition of genus of a Riemann surface as the number of "handles" of the C. The only genus zero curve is $\mathbb{P}^1_k$.

In later sections of this paper, we will need to consider some singular curves. If C is a singular projective curve, there exists a unique (up to isomorphism) nonsingular projective curve $\tilde{C}$ (called the normalization of C) for which there exists a surjection $\tilde{C} \to C$ which induces an isomorphism between dense open subsets of $\tilde{C}$ and C. When we refer in this paper to the genus or function field of C, we will always mean the genus or function field of $\tilde{C}$.

2.1 Morphisms between Curves

Let $f : C \to D$ be a dominant morphism between two nonsingular projective curves. (In this context, the condition that f is dominant is equivalent to the condition that the image of f is not a point.) Then f induces a k-linear homomorphism $\phi_f : K(D) \to K(C)$. Conversely, given any k-linear homomorphism $\phi : K(D) \to K(C)$, there exists a dominant morphism $f : C \to D$ such that $\phi = \phi_f$. In other words, if we let $\mathscr{C}$ be the category whose objects are nonsingular projective curves and whose morphisms are dominant algebraic morphisms, then $\mathscr{C}$ is (contravariantly) equivalent to the category whose objects are finitely-generated transcendence-degree-one extensions of k with morphisms k-linear homomorphisms.

Note any k-linear homomorphism between two fields must be injective (since its kernel is a proper ideal), so a dominant morphism of curves $f : C \to D$ corresponds to an *extension* of fields $K(D) \hookrightarrow K(C)$. Further, since both have transcendence degree 1 over k, the extension $K(D) \hookrightarrow K(C)$ must be algebraic. If $U = \operatorname{Spec} R \subset D$ is an open affine subset of D, then $f^{-1}U = \operatorname{Spec} \overline{R}$, where $\overline{R}$ is the integral closure of R in $K(C)$. Since the extension of fields is algebraic, $\overline{R}$ is a finite R-module, and thus f is a finite morphism. Finite morphisms are closed, so $f(C)$ is closed in D. $f(C)$ is also dense in D, so we must have that $f(C) = D$–i.e. f is surjective. In other words, dominant morphisms of curves are *coverings* and correspond to *extensions* of function fields.

Now if $p \in U$ is a point corresponding to the prime ideal $\mathfrak{p} \subset R$, then $f^{-1}(p)$ is the closed subset of $V = f^{-1}(U)$ defined by the ideal $\mathfrak{p}\overline{R} \subset \overline{R}$. Since $\overline{R}$ is a Dedekind domain, we can factor $\mathfrak{p}\overline{R}$ uniquely as a product of primes of $\overline{R}$:

$$\mathfrak{p}\overline{R} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g} \tag{1}$$

Furthermore, $\sum_{i=1}^{g} e_i = [K(C) : K(D)]$. (This result is [Hart, Pro. II.6.9]. The proof uses the Chinese Remainder Theorem, and is analogous to the proof of [Stein, Thm. 9.2.2].)

2.2 Divisors on Curves

This result can be stated more elegantly in terms of divisors. A *divisor* on a nonsingular curve D is a formal $\mathbb{Z}$-linear sum of points. For $p \in D$, we will use the notation $[p]$ to denote the divisor corresponding to p. Any divisor can then be written as $E = \sum_{i=1}^{r} c_i[x_i]$ where $c_i \in \mathbb{Z}$ and $x_i \in D$. If all the points x_i are in $U = \operatorname{Spec} R$ and correspond to prime ideals $\mathfrak{q}_i$, then E corresponds to the fractional ideal $\prod \mathfrak{q}_i^{c_i}$. The *degree* of E is $\sum c_i$.

To any nonzero rational function $\alpha \in K(C)^*$, we can associate a divisor

$$(\alpha) = \sum_{p \in C} \nu_p(\alpha)[p] \tag{2}$$

To gain intuition into this definition, we can think of the case $k = \mathbb{C}$, where this reduces to an analysis problem. If we regard α as a meromorphic function on C, then $\nu_p(\alpha) > 0$ when $\alpha(p) = 0$ (and in this case $\nu_p(\alpha)$ is the order of vanishing of α at p), and $\nu_p(\alpha) < 0$ when α has a pole at p (and in this case $-\nu_p(\alpha)$ is the order of the pole). If α has neither a zero or a pole at p, then $\nu_p(\alpha) = 0$. Thus colloquially, (α) is the divisor of "zeroes minus poles" of α. Such a divisor is called *principal.* Principal divisors all have degree zero, and they form a subgroup of the group of divisors $\operatorname{Div} C$ on C. The quotient is called the *class group* of C, and is denoted $\operatorname{Cl}(C)$.

(This definition of the class group–which applies in a much more general context–agrees exactly with the definition of the class group $\operatorname{Cl}(\mathcal{O}_K)$ of fractional ideals of the ring of integers of a number field.)

If $f : C \to D$ is a morphism of nonsingular curves, and E is a divisor on D, we can define a divisor f^*E on C as follows: if p is a point in $U = \operatorname{Spec} R$ corresponding to the prime ideal $\mathfrak{p}$ as above, $\mathfrak{p}$ splits in $\overline{R}$ as in Equation 1, and if $p_i \in V = f^{-1}U = \operatorname{Spec} \overline{R}$ are the points corresponding to $\mathfrak{p}_i$, then

$$f^*[p] = \sum_{i=1}^{g} e_i[p_i] \tag{3}$$

Now we extend linearly:

$$f^*\left(\sum_{i=1}^{r} c_i[x_i]\right) = \sum_{i=1}^{r} c_i f^*[x_i] \tag{4}$$

Then our result above says

$$\deg f^*E = [K(C) : K(D)] \deg E \tag{5}$$

We will also call $[K(C) : K(D)]$ the *degree* of f.

2.3 Galois Groups and Deck Transformations

Now $\sigma \in \operatorname{Aut}(K(C)/K(D))$ induces an isomorphism $g_\sigma : C \to C$ such that $f = f \circ g$. So elements of $\operatorname{Aut}(K(C)/K(D))$ correspond to deck transformations of the covering $C \to D$. Hence $\operatorname{Aut}(K(C)/K(D))$ acts on each fiber of f. As in the case of number fields, if $K(C)/K(D)$ is Galois, then the action is transitive on each fiber, and coefficients of the $[p_i]$ in $f^*[p]$ agree.

2.4 Ramification and Hurwitz's Theorem

For simplicity in this section we will assume that k has characteristic zero. For $p \in D$ and $f : C \to D$ as above, write $f^*[p] = \sum_{q\in f^{-1}(p)}^{g} e_q[q]$. We say f is *ramified* at q if $e_q > 1$, and we call e_q the *ramification index* of q. f is ramified at only finitely many points, and so the *ramification divisor* $R = \sum_{q\in C}(e_q - 1)[q]$ is well defined. Hurwitz's Theorem states that

$$2g(C) - 2 = \deg f\,(2g(D) - 2) + \deg R \tag{6}$$

¿From this we can draw two immediate corollaries: the degree of R must be even, and $g(C)$ must be greater than or equal to $g(D)$.

Hurwitz's Theorem relies on k being algebraically closed. If k is not algebraically closed, it may be that not all of the ramification points are defined over k. Thus when working over a non-algebraically closed field one must be careful about fields of definition when analyzing ramification. For example, for a covering of curves over $\mathbb{Q}$, Hurwitz's Theorem may not hold, but after base-changing to a number field over which all ramification is defined, the theorem will hold. We will see an example of this later. The requirement that the characteristic of k is zero is stronger than necessary–as long as the extension $K(C)/K(D)$ is separable and the characteristic of k does not divide any ramification index e_q (in which case we say f is *tamely ramified*) Hurwitz's Theorem will still hold.

3 Modular Groups and Modular Curves

The curves about which we will be primarily concerned in the remainder of this paper are *modular curves*. We will now give an overview of the definition of these curves, and we will try to give a glimpse into why they are important objects. For details, see [St]. Modular curves will *a priori* be curves defined over $k = \mathbb{C}$, although in fact they will be defined over $\mathbb{Q}$ as well. Roughly speaking, a modular curve is a compactification of a quotient of the upper half-plane $\mathbb{H}$ by an action of a *congruence group*.

One important class of congruence groups are the *principal congruence groups*. These are defined as

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cong \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

for N a positive integer called the *level* of the group. A general *congruence group* is a subgroup of $\mathrm{PSL}_2(\mathbb{R})$ commensurable to $PSL_2(\mathbb{Z})$ and containing some principal congruence subgroup.

One of the most interesting classes of congruences subgroups for our purposes is

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) \mid c \cong 0 \pmod{N} \right\}$$

and for $l \mid N$, the subgroup $\Gamma_0(N) + l$ of $\mathrm{PSL}_2(\mathbb{R})$ generated by $\Gamma_0(N)$ and

$$\mu_l = \begin{pmatrix} 0 & \sqrt{l} \\ -\frac{1}{\sqrt{l}} & 0 \end{pmatrix}$$

(μ_l is an *Atkin-Lehner* involution.) Note $\Gamma_0(1) = PSL_2(\mathbb{Z})$.

Any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{R})$ acts on $\mathbb{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

The action extends to one on $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1_{\mathbb{Q}}$, and for any congruence group Υ, the quotient $\overline{\mathbb{H}}/\Upsilon$ will be compact. In fact, it will be a projective algebraic curve over $\mathbb{C}$, albeit typically singular. This is what we mean by a modular curve.

The modular curves which are quotients of $\Gamma(N)$ we denote $X(N)$; the modular curves for $\Gamma_0(N)$ we call $X_0(N)$, and the modular curves for $\Gamma_0(N)+l$ we call $X_0(N) + l$.

In the case where a modular curve $X = \overline{\mathbb{H}}/\Upsilon$ has genus zero, its function field is purely trancendental, and so we can write $K(X) \simeq \mathbb{C}(t)$. We call t a *hauptmodul* for Υ. Choosing t corresponds to fixing an parametrization $\mathbb{P}^1_{\mathbb{C}} \to X$ given by $p \mapsto t(p)$, and t becomes an affine parameter on $\mathbb{P}^1$. Of course, since $\mathbb{P}^1_{\mathbb{C}}$ has many automorphisms, choosing a hauptmodul involves making a choice. Note in general X will be singular, so this parametrization will not be an isomorphism, but it will be the normalization. In what follows, we will often find it convenient to abuse notation and identify a modular curve with its normalization. We will sometimes refer to these as a "singular model" and a "nonsingular model" for the modular curve.

We can view t as a function from $\mathbb{H} \to \mathbb{C}$ which is invariant under the action of Υ. Then, we can expand t in a Laurent series in the variable $q = e^{2\pi i \tau}$, where τ is the natural parameter on $\mathbb{H}$. This is called a *q-series expansion* for t. q-series expansions for particular choices of hauptmoduls have been worked out explicitly in the literature on this subject. See for example [CN, Table 4]. By abuse of terminology, when X has genus zero, we say Υ is a *genus zero group.*

If $\Upsilon \subset \Upsilon'$ are two congruence subgroups, then the identity map on $\overline{\mathbb{H}}$ induces a covering $\overline{\mathbb{H}}/\Upsilon \to \overline{\mathbb{H}}/\Upsilon'$. For example, if $M|N$, then $\Gamma_0(N) \subset \Gamma_0(M)$, and hence $X_0(N)$ covers $X_0(M)$.

3.1 Examples and Relationship with Elliptic Curves

For any $\tau \in \mathbb{H}$ we can define an elliptic curve $E_\tau \simeq \mathbb{C}/\langle 1, \tau \rangle$. So $X_0(1) \simeq \mathbb{P}^1_{\mathbb{C}}$ precisely parametrizes isomorphism classes of elliptic curves (together with one other point–the orbit $\mathbb{P}^1_{\mathbb{Q}}$–corresponding to a singular curve). The standard choice of hauptmodul on $X_0(1)$ is the classical elliptic invariant j. The q-series for j begins

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \dots \tag{7}$$

If E_τ is put into Weierstrass form $y^2 = x^3 + ax + b$, then

$$j(\tau) = \frac{1728 \cdot 4a^3}{4a^3 + 26b^2} \tag{8}$$

For a natural number n, the identity map on $\mathbb{C}$ induces an n to 1 map $E_{n\tau} \to E_\tau$ with kernel generated by τ. We call two elliptic curves C_1, C_2 *n-isogenous* if there exists a homomorphism between them with kernel cyclic of order n (such a homomorphism is called an *isogeny*). Since the kernel must be contained in the n-torsion subgroup of C_1, we can always arrange for an n-isogeny to be induced by the identity as above. I.E., C_1 and C_2 are n-isogenous if and only if $C_1 \simeq E_\tau$ and $C_2 \simeq E_{n\tau}$ for some $\tau \in \mathbb{H}$. Let $\tau' = -\frac{1}{n\tau}$, and note that $E_\tau \simeq E_{n\tau'}$ and $E_{n\tau} \simeq E_{\tau'}$. Thus if there exists an n-isogeny $C_1 \to C_2$, there also exists a (dual) n-isogeny $C_2 \to C_1$.

Now consider the map $\phi_n : \mathbb{H} \to \mathbb{P}^2$ given by $\tau \mapsto [j(\tau), j(n\tau), 1] = [x, y, z]$. We claim $X_0(n)$ is the closure of the image of ϕ_n. $\phi_n(\tau) = \phi_n(\tau')$ if and only if

$$\tau' = \frac{a\tau + b}{c\tau + d} \ , \ n\tau' = \frac{\alpha n\tau + \beta}{\gamma n\tau + \delta}$$

for some

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$$

Examining these equations, we see that

$$\begin{pmatrix} na & nb \\ c & d \end{pmatrix} = \pm \begin{pmatrix} n\alpha & \beta \\ n\gamma & \delta \end{pmatrix}$$

which is possible if and only if $\tau' = \frac{a\tau+b}{c\tau+d}$, for

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(n) \ .$$

Thus $X_0(n)$ parametrizes (ordered) pairs of n-isogenous elliptic curves.

The genus of $X_0(n)$ for many small n can be found in [Cohn]. The equation $\Phi_n(x, y) = 0$ for $X_0(n)$ on the affine patch $z = 1$ is the classical modular equation for $\Gamma_0(n)$. Because it is symmetric in x and y, it can be written as a polynomial in terms of the elementary symmetric functions $\pi = xy$, $\sigma = x + y$. Let $\Phi_n^{+n}(\pi, \sigma)$ be the corresponding polynomial such that $\Phi_n^{+n}(xy, x + y) = \Phi_n(x, y)$. Note that

$$(j(\tau)j(n\tau), j(\tau) + j(n\tau)) = (j(\tau')j(n\tau'), j(\tau') + j(n\tau'))$$

if and only if $(j(\tau), j(n\tau)) = (j(\tau'), j(n\tau')$ or $(j(n\tau'), j(\tau'))$, which will occur if and only if $\tau' = \frac{a\tau+b}{c\tau+d}$ for some

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(n) + n \ .$$

We may thus view $\Phi_n^{+n}(\pi, \sigma) = 0$ as the defining equation for $X_0(n) + n$. Hence we see that $X_0(n) + n$ parametrizes unordered pairs of n isogenous elliptic curves.

The map $(x, y) \mapsto (xy, x + y)$ is precisely the two-to-one covering coming from the fact that $\Gamma_0(n)$ is an index 2 subgroup of $\Gamma_0(n)$. Ramification points of this covering are points where $x = y$. These correspond to elliptic curves which are n isogenous to themselves. Classically, such points were called "singular moduli," although this terminology can be somewhat confusing due to the fact that although $X_0(n)$ is typically singular, these "singular moduli" are not in general singular points of the curve. The number of such "singular moduli" is determined by Hurwitz's Theorem.

Note that instead of thinking of $X_0(n)$ as parametrizing pairs of elliptic curves, we could instead think about $X_0(n)$ as parametrizing elliptic cuves with marked cyclic subgroups of order n. In fact, most modular curves can be thought about in this way, as parametrizing families of elliptic curves with some extra structure. If X is the modular curve corresponding to some $\Upsilon \subset \mathrm{PSL}_2(\mathbb{Z})$, and we think of X as parametrizing elliptic curves with some extra structure, then the covering $X \to X_0(1)$ is the "forgetful map" which corresponds to forgetting the extra structure, and only considering the elliptic curves themselves.

4 Galois Coverings of Modular Curves

Although in principle one can calculate Φ_n and Φ_n^{+n} to determine what $X_0(n)$ and $X_0(n)+n$ are, in practice this is quite difficult and cumbersome, because the coefficients in these defining polynomials grow very large very quickly. In practice, a better way to study a given modular curve is often to use a galois cover from this curve to another better-understood modular curve.

An especially useful case is when some $\Gamma_0(N)+l$ is genus zero. In this case, since $\Gamma_0(N)$ has index 2 in $\Gamma_0(N)+l$, we have a presentation of (a nonsingular model for) $X_0(N)$ as a degree 2 cover of $\mathbb{P}^1_{\mathbb{C}}$ (i.e. $X_0(N)$ is *hyperelliptic*). Such a covering is necessarily galois, since $K(X_0(N))$ is then isomorphic to the splitting field of $y^2 - f(x) \in \mathbb{C}(x)[y]$, where $f(x) \in \mathbb{C}[x]$ is squarefree. It is a fact that when $g(X_0(N)) \leq 5$, $X_0(N)$ is hyperelliptic, although the hyperelliptic presentation may not be induced by an Atkin-Lehner involution (the first example where this does not occur is $N = 37$). The study of these hyperelliptic presentations goes back to the work of Fricke in the 19th century, and is still an active area of research today. Nice examples and explanation can be found in [Cohn], [HM].

We conclude with an interesting example. In [HM], it is shown that $X_0(28) + 7$ has genus zero, and the galois covering $X_0(28) \to X_0(28) + 7$ is ramified over $\pm\sqrt{-7}, \frac{1\pm\sqrt{-7}}{2}, \frac{-1\pm\sqrt{-7}}{2}$. Hence we see that the ramification is defined over $\mathbb{Q}(\sqrt{-7})$, that $X_0(28)$ has hyperelliptic presentation $y^2 = (x^2+7)(x^2+x+2)(x^2-x+2)$, and by Hurwitz that $X_0(28)$ has genus 2.

We can also deduce from [HM] that the Atkin-Lehner involution μ_{28} is given in this hyperelliptic presentation by $x \mapsto \frac{x+3}{x-1}$, $y \mapsto \frac{8y}{(x-1)^3}$. The galois covering $X_0(28) \to X_0(28) + 28$ can then be defined by

$$\pi_{28} : (x, y) \mapsto (x, y) + \mu_{28}((x, y)) = \left(\frac{x^2+3}{x-1}, \frac{y(x+1)(x^2-4x+7)}{(x-1)^3}\right)$$

Ramification will occur when $\mu_2 8(x, y) = (x, y)$, i.e. for (x, y) such that

$$\begin{aligned} x &= \frac{x+3}{x-1} \\ y &= \frac{8y}{(x-1)^3} \\ y^2 &= (x^2+7)(x^2+x+2)(x^2-x+2) \end{aligned}$$

The first equation implies $x = 3, -1$. If $x = -1$, the second equation becomes $y = -y$, so then $y = 0$. But $(-1, 0)$ doesn't satisfy the third equation, so the only ramification occurs when $x = 3$. From the third equation, we see that in these cases $y = \pm 16\sqrt{7}$. So by Hurwitz, since $\deg R = 2$, $X_0(28) + 28$ must have genus 1. The ramification is defined over $\mathbb{Q}(\sqrt{7})$. (So a good field to work over when study modular curves of level 28 is $\mathbb{Q}(i, \sqrt{7})$).

We can also compute from these data a singular model for $X_0(28) + 28$ as the image of π_{28}. This can be done using elimination theory: over an affine patch of $X_0(28)$ where $x \neq 1$, the graph of π_{28} is the variety defined by the equations

$$\begin{aligned} 0 &= y^2 - (x^2+7)(x^2+x+2)(x^2-x+2) && (9) \\ 0 &= (x-1)u - (x^2+3) && (10) \\ 0 &= (x-1)^3 v - y(x+1)(x^2-4x+7) && (11) \\ 0 &= t(x-1) - 1 && (12) \end{aligned}$$

in $\mathbb{A}^5$ with coordinates (t, x, y, u, v). The image of $\pi_2 8$ is the (closure of) the image of this variety under the projection onto the $\mathbb{A}^2$ with coordinates (u, v). So we need only eliminate t, x, y from the ideal generated by the right-hand-sides of Equations 9, 10, 11. Doing so, we have that (a singular model for) $X_0(28) + 28$ has hyperelliptic presentation

$$v^2 = (u-4)^2(u+1)(u+2)\left(u^2 - u + 2\right) \tag{13}$$

A similar computation in the first nontrivial case ($N = 22$) can be found in [Elkies].

References

[Cohn] H. Cohn, "Fricke's Two-Valued Modular Equations." *Math. of Computation* 51 #184 (1988).

[CN] J.H. Conway and S.P. Norton, "Monstrous Moonshine." *Bull. London Math. Soc.* 11 (19279), 208-339.

[DF] D.S. Dummit and R.M. Foote, *Abstract Algebra*, 3rd ed. Wiley and Sons, 2004.

[Elkies] N. Elkies, "Elliptic Curves in Nature."
`http://www.math.harvard.edu/~elkies/nature.html`.

[Hart] R. Hartshorne, *Algebraic Geometry.* GTM 52.

[HM] T. Hibino and N. Murabayashi, "Modular Equations of Hyperelliptic $X_0(N)$ and an application." *Acta Arithmetica* 82 #3 (1997).

[Lor] D. Lorenzini, *An Invitation to Arithmetic Geometry.* GSM 9.

[Stein] W. Stein, *Algebraic Number Theory, A Computational Approach.* Nov. 26, 2007 ed.

[St] G. Stevens, *Arithmetic on Modular Curves.* Progress in Math 20.