NOTES ON RIEMANN'S EXISTENCE THEOREM

by Jeff Yelton

1 Algebraic Statement

For the following, k is always an algebraically closed field of characteristic 0. Let L be a finite Galois extension of the function field $k(x)$ with Galois group $G := \mathrm{Gal}(L/k(x))$. Consider $k(x)$ as the function field of the projective k-line whose set of points is given by

$$\mathbb{P}^1_k = k \cup \{\infty\}.$$

For each point $p \in \mathbb{P}^1_k$, we define an embedding θ_p of $k(x)$ into a power series ring $k((t))$ in the following manner: for $p \in k$, let $\theta_p : x \mapsto t + p$ (so that the uniformizing parameter is $x - p$), and for $p = \infty$, $\theta_p : x \mapsto t^{-1}$ (so that the uniformizing parameter is x^{-1}). We can extend each θ_p to an injection (not necessarily unique) ψ_p of L into a finite Galois extension of $k((t))$.

Now there is a simple description of all finite Galois extensions of $k((t))$: for any positive integer e, the only finite Galois extension of $k((t))$ is of the form $k((t^{1/e}))$ with cyclic Galois group generated by $\omega_e : t^{1/e} \mapsto \zeta_e t^{1/e}$. In the case above, we can consider the image $\theta_p(L)$ to lie in a particular finite Galois extension $k((t^{1/e}))/k((t))$ and define the Galois automorphism

$$g_p := \theta_p^{-1} \circ \omega_e \circ \theta_p \in G = \mathrm{Gal}(L/k(x)).$$

It can be shown that if g_p has order e' in G, then in fact, $\theta_p(L) \subset k((t^{1/e'}))$ so that we we may replace e with e' (which is the least possible choice of integer e). Now although the embedding θ_p is not unique, the group element g_p is unique up to conjugation – for a different embedding $\tilde{\theta}_p$, the corresponding Galois element $\tilde{g}_p$ will be $h^{-1} g_p h$, where $h = \theta_p^{-1} \circ \tilde{\theta}_p$. Thus, L and p determine a conjugation class of G, denoted C_p, all of whose elements have order $e =: e_p$ (the **ramification index** of L at p).

A **ramified point** or **branch point** of $L/k(x)$ is a point $p \in \mathbb{P}^1_k$ with $e_p > 1$ (equivalently with $C_p \neq \{1\}$).

Now we will assume that $k = \mathbb{C}$.

Definition 1.1. *A* ***ramification type*** *is an equivalence class of triples* $(G, P, \{C_p\}_{p\in P})$*, where* G *is a finite group,* P *is a finite subset of* $\mathbb{P}^1_k$ *and each* C_p *is a conjugacy class in* G *(they are not necessarily distinct), with the equivalence relation* $(G, P, \{C_p\}_{p\in P}) \sim (G', P', \{C'_p\}_{p\in P'})$ *if and only if* $P = P'$ *and there is an isomorphism* $G \to G'$ *mapping each* C_p *to* C'_p*.*

Theorem 1.2 (Riemann's Existence Theorem (Algebraic))**.** *Let* $(G, P, \{C_p\}_{p\in P})$ *be a ramification type, with* $P = \{p_1, ..., p_r\}$*. Then there exists a finite Galois extension* $L/\mathbb{C}(x)$ *with* $G = \mathrm{Gal}(L/\mathbb{C}(t))$ *of that ramification type if and only if there is a set of generators* $\{g_1, ..., g_r\}$ *of* G *with each* $g_i \in C_{p_i}$ *and* $g_1 g_2 ... g_r = 1$*.*

Corollary 1.3. *Every finite group is realizable as a Galois group over* $\mathbb{C}(x)$*.*

The above is an existence statement, which does not imply uniqueness of this Galois extension L, but now we will define a condition on the ramification type which will imply uniqueness of L.

Definition 1.4. *Let* $(G, P, \{C_p\}_{p\in P})$ *be a ramification type and write* $P = \{p_1, ..., p_r\}$*.*
a) We say that this ramification type is ***rigid*** *if there exist generators* $\{g_1, ..., g_r\}$ *of* G *with* $g_1 g_2 ... g_r = 1$ *and* $g_i \in C_{p_i}$ *such that if* $\{g'_1, ..., g'_r\}$ *is another such set of generators, there is a unique element* $g \in G$ *which conjugates each* g_i *to* g'_i*. (In particular, this implies that* G *has trivial center.)*
b) We say that this ramification type is ***weakly rigid*** *if there is a generating set* $\{g_1, ..., g_r\}$ *with the same properties such that for any other such generating set* $\{g'_1, ..., g'_r\}$*, there is an automorphism of* G *sending each* g_i *to* g'_i*.*

Note that since the g_i's generate G, if an automorphism exists that takes each g_i to g'_i, then that automorphism is unique. Thus, in the rigid case, the only automorphism of G leaving each C_i invariant is the unique inner automorphism in the definition.

Theorem 1.5. *If* $(G, P, \{C_p\}_{p\in P})$ *is a weakly rigid ramification type, then there extension* $L/\mathbb{C}(x)$ *implied by Riemann's Existence Theorem is unique up to isomorphism of* $\mathbb{C}(x)$*.*

Proof. Fix a weakly rigid ramification type, and let L and L' be two extensions with this ramifiction type. We may assume that $L_1, L_2 \subset L$ where

L is a finite Galois extension of $\mathbb{C}(x)$, and we want to show that $L_1 = L_2$. Let $G := \mathrm{Gal}(L/cc(x))$, $G_1 := \mathrm{Gal}(L_1/\mathbb{C}(x))$, and $G_2 := \mathrm{Gal}(L_2/\mathbb{C}(x))$ with $\rho_1 : G \twoheadrightarrow G_1$ and $\rho_2 : G \twoheadrightarrow G_2$ the restriction maps. Since all extensions are Galois, it will suffice to show that $\ker(\rho_1) = \ker(\rho_2)$. For each $p \in P$, denote the associated conjugacy classes of G, G_1, and G_2 by C_p, $C_p^{(1)}$, and $C_p^{(2)}$ respectively. There is compatibility such that for each $p \in P$, $\rho_1(C_p) = C_p^{(1)}$ and $\rho_2(C_p) = C_p^{(2)}$. By RET, there are generators $g_1, ...g_r$ with certain properties, and clearly, ρ_1 and ρ_2 map these generators to generators of G_1 and G_2 with the appropriate properties. Now since the ramification types are the same, there is an isomorphism $\phi : G_2 \to G_1$ which maps each $C_p^{(2)}$ to $C_p^{(1)}$. Thus, $\{\phi(\rho_2(g_1)), ..., \phi(\rho_2(g_r))\}$ is a generating set of G_1 with the appropriate properties. Since $\{\rho_1(g_1), ..., \rho_1(g_r)\}$ is also such a generating set for G_1 and we have weak rigidity, there must be an automorphism ψ of G_1 sending $\phi(\rho_2(g_i)) \mapsto \rho_1(g_i)$ for $1 \leq i \leq r$. Then $\psi \circ \phi$ is an isomophism $G_2 \to G_1$ such that $\rho_1 = \psi \circ \phi \circ \rho_2$, implying that $\ker(\rho_1) = \ker(\rho_2)$ as desired.

□

2 Proof of RET using the analytic statement

For this section, we again use $\mathbb{C}$ as our algebraically closed field, and write $\mathbb{P}^1$ for the complex projective line. The following is the analytic version of Riemann's Existence Theorem, which we will use in this section to prove the algebraic version of last section. The proof of this theorem requires some fairly deep analysis.

Theorem 2.1 (Riemann's Existence Theorem (Analytic))**.** *For Y a compact Riemann surface, $p_1, ..., p_s$ distinct points in Y, and $c_1, ..., c_s \in \mathbb{C}$, there is a $g \in \mathcal{M}(Y)$ with $g(p_i) = c_i$ for each i.*

To link this to the algebraic version of RET, we study finite coverings of $\mathbb{P}^1$ which are ramified at finitely many points. Equivalently, we study (topological) covering spaces $f : R \to \mathbb{P}^1 \backslash P$ for P a finite set of points, along with their compactifications $\bar{R}$. The field of meromorphic functions $\mathcal{M}(\bar{R})$ is a finite Galois extension of the field of meromorphic functions $\mathcal{M}(\mathbb{P}^1) = \mathbb{C}(x)$.

Let $f : R \to \mathbb{P}^1 \backslash P$ be such a covering. Around each $p \in \mathbb{P}^1$ we can construct a circular neighborhood small enough that no other point in P is in it. The intersection of this neighborhood with $\mathbb{P}^1 \backslash P$ is a small punctured circle D which is covered by $f^{-1}(D)$. Each connected component E of $f^{-1}(D)$ is

also a punctured circle. The restriction $f|_E : E \to D$ "looks like" the map from the punctured unit disk to itself defined by $z \mapsto z^e$ for some positive integer e (depending on p). Thus, the map $f|_E$ is of degree e, and the group of deck transformations of this map is cyclic of order e. The homeomorphism of E to itself defined by $z \mapsto \zeta_e z$ generates this group of deck transformations of $f|_E$. For all choices of connected component of $f^{-1}(D)$, the deck transformations obtained in this way are unique up to conjugation, so the point $p \in P$ defines a conjugacy class in the group of deck transformations $\mathrm{Deck}(f)$, which we denote by C_p.

For $f : R \to \mathbb{P}^1 \backslash P$ to be a covering space, for all $p \in \mathbb{P}^1 \backslash P$, the associated conjugacy class $C_p = \{1\}$. Of course, this may also be the case for some $p \in P$. We may extend $f : R \to \mathbb{P}^1 \backslash P$ to $f : \bar{R} \to \mathbb{P}^1$, where $\bar{R}$ is the compactification of R obtained by adding finitely many points. This is a finite covering of $\mathbb{P}^1$, which is said to be **unramified** at a point $p \in \mathbb{P}^1$ if $C_p = \{1\}$ and **ramified** at $p \in \mathbb{P}^1$ otherwise (the finite subset P contains all the ramified points). The group of deck transformations of f, which we will denote by G, is finite. After throwing all unramified points out of P, we see that the triple $(G, P, \{C_p\}_{p \in P})$ defines a ramification type, which we will call **the ramification type of** f.

Theorem 2.2. *Let $(G, P, \{C_p\}_{p \in P})$ be a ramification type with $P = \{p_1, ..., p_r\}$. Then there exists a finite Galois covering space $f : R \to \mathbb{P}^1 \backslash P$ of that type if and only if there is a set of generators $\{g_1, ..., g_r\}$ of G with each $g_i \in C_{p_i}$ and $g_1 g_2 ... g_r = 1$.*

Sketch of proof: For simplicity, we will assume that $p_r = \infty$.

First assume that the prescribed generators of G exist. Fix a basepoint of $\mathbb{P}^1 \backslash P$. Each generator g_i will be represented by a closed loop from the basepoint which goes around p_i counterclockwise but does surround any other points in P. One can define a Galois covering $f : R \to \mathbb{P}^1 \backslash P$ by directly constructing it or by thinking of it as a "quotient" of the universal covering space of $\mathbb{C} \backslash \{p_1, ..., p_{r-1}\}$.

To directly construct the Galois cover, define R as a set of points to be the cartesian product $(\mathbb{P}^1 \backslash P) \times G$ ($\#G$ "sheets" of $\mathbb{P}^1 \backslash P$) and defining the open neighborhoods to be such that the "sheet" corresponding to $g \in G$ gets close to the sheet corresponding to gg_i near the point p_i. In particular, this is done so that the loop circling p_i in $\mathbb{P}^{-1} \backslash P$ when lifted to R travels from the sheet corresponding to g to the sheet corresponding to gg_i. To see it as a "quotient" of a universal covering space, recall that the fundamental

group of the complex plane minus $r-1$ points is F_{n-1}, the free group on $n-1$ generators. Since G is generated by $\{g_1, ..., g_{r-1}\}$, it can be presented as a quotient of F_{r-1} by a normal subgroup, and therefore, there is a Galois covering space of $\mathbb{C}\backslash\{p_1, ..., p_{r-1}\}$ corresponding to that normal subgroup. Since $\mathbb{P}^1\backslash P = \mathbb{C}\backslash\{p_1, ..., p_{r-1}\}$, this is the desired Galois cover R.

Now assume the existence of this Galois cover $R \to \mathbb{P}^1\backslash P$ with the prescribed ramification type. Since the covering is Galois, we may define

$$G = \pi_1(\mathbb{P}^1\backslash P)/\pi_1(R) \cong \mathrm{Gal}(R/(\mathbb{P}^1\backslash P)).$$

Then for $1 \leq i \leq r-1$, define each g_i to be the loop circling the point p_i counterclockwise. It is clear from above discussions that each $g_i \in C_{p_i}$. Furthermore, the g_i's do generate G since any covering space of the complex plane minus $r-1$ points must be a "quotient" of the universal covering space of it, whose fundamental group is generated by these paths. Finally, one can define $g_r := (g_1 ... g_{r-1})^{-1}$ and see that it's a counterclockwise loop around ∞ whose associated conjugacy class is C_∞, so we have a group G with the desired properties.

□

Now we can construct an atlas on the compactification $\bar{R}$ of the cover R so that $\bar{R}$ is a Riemann surface and $f : \bar{R} \to \mathbb{P}^1$ is an analytic map. The deck transformations can now be considered analytic isomorphisms of $\bar{R}$. Then for every deck transformation $g \in \mathrm{Deck}(f)$, we can define a map $\iota_g : \mathcal{M}(\bar{R}) \to \mathcal{M}(\bar{R})$ given by $\iota_g(h) = h \circ g^{-1}$ for all meromorphic functions h on $\bar{R}$. Clearly ι_g leaves any constant function fixed, and since all deck transformations g respect the map $f : \bar{R} \to \mathbb{P}^1$, ι_g also leaves f fixed. It is clear that ι_g also preserves addition and multiplication of meromorphic functions. Therefore, we may consider ι_g to be an automorphism of the field $\mathcal{M}(\bar{R})$ fixing the subfield $\mathbb{C}(f)$, so $\iota_g \in \mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(f))$. Thus we have a map from the group of deck transformations to $\mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(f))$ which is clearly a group homomorphism

$$\iota : \mathrm{Deck}(\bar{R}) \to \mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(f)).$$

To prove the algebraic version of RET given in the last section, we will need to show that this is in fact an isomorphism.

To prove surjectivity, let H be the image of ι. Then the fixed field of H consists of all meromorphic functions $h : \bar{R} \to \mathbb{P}^1$ with the property that

$h = h \circ g$ for all $g \in \mathrm{Deck}(f)$. For any point $z \in \mathbb{P}^1 \backslash P$, since the group of deck transformations acts transitively on all the points in the inverse image $f^{-1}(z)$, h must take the same value on all of them, call it $\tilde{h}(z)$. For a small enough open neighborhood U of z, its inverse image will be the disjoint union of open sets homeomorphic to U, on each of which $\tilde{h} = h \circ f^{-1}$. Since h and f^{-1} are analytic, so is $\tilde{h}$, and $\tilde{h}$ can be extended to a meromorphic function on all of $\mathbb{P}^1$ with the property that $h = \tilde{h} \circ f$. Since the meromorphic functions on $\mathbb{P}^1$ are just $\mathbb{C}(x)$ (where we may think of x as the "identity function"), it is clear that $h \in \mathbb{C}(f)$. Therefore, the fixed field of the subgroup H of the Galois group is only $\mathbb{C}(f)$, and so H is the whole Galois group and ι is surjective.

To prove injectivity, suppose that g is a deck transformation such that ι_g is the trivial automorphism of $\mathcal{M}(\bar{R})$. Choose any point $a \in \bar{R}$. If we let $z := f(a)$, then $f^{-1}(z)$ is a finite set of points in $\bar{R}$, so we may use the analytic version of RET (Theorem 2.1) to choose a function $h \in \mathcal{M}(\bar{R})$ which takes different values on each point of $f^{-1}(z)$. Since g permutes the points in $f^{-1}(z)$, $g(a) \in f^{-1}(z)$ and $h(g(a)) = \iota_g(h)(g(a)) = (h \circ g^{-1} \circ g)(a) = h(a)$. But since h takes different values on distinct points in $f^{-1}(z)$, the fact that $h(g(a)) = h(a)$ implies that $g(a) = a$. Since this is true for all points $a \in \bar{R}$, we see that h is the identity deck transformation, so ι is injective.

Now it's easy to finish proving the algebraic version of RET. Let $L/\mathbb{C}(x)$ be a finite Galois extension. Then the finite subset $P \subset \mathbb{P}^1$ is the set of primes of the ring $\mathbb{C}[x]$ (or of the ring $\mathbb{C}[x^{-1}]$) which are ramify. We construct the Galois cover more or less as follows: let $F(x, y)$ be the polynomial of degree n in $\mathbb{C}(x)[y]$ for which L is a splitting field. Let R' be the subset of $\mathbb{C}^{n+1}$ consisting of tuples $(z, \alpha_1(z), ..., \alpha_n(z))$, where $z \in \mathbb{P}^1 \backslash P$ and $\alpha_1(z), ..., \alpha_n(z)$ are the roots of the the polynomial $F(z, y)$ (note that these roots are *distinct*), and let $f' : (z, \alpha_1(z), ..., \alpha_n(z)) \mapsto z$. Then we let R be a connected component of R', and $f' : R \to \mathbb{P}^1 \backslash P$ is our Galois cover. The group $\mathrm{Deck}(f)$ permutes the $\alpha_i(z)$'s. For each small enough neighborhood U of any point $z \in \mathbb{P}^1 \backslash P$ and each permutation $\sigma \in \mathrm{Gal}(f)$ of the roots, there is an analytic isomorphism of U onto a homeomorphic neighborhood of $(z, \alpha_{\sigma(1)}(z), ..., \alpha_{\sigma(n)}(z))$ given by $w \mapsto (w, \psi_1(w), ..., \psi_n(w))$, with $\psi_i(z) = \alpha_{\sigma(i)}(z)$ for $i = 1, ..., n$. If the neighborhood U is chosen small enough, these homeomorphic images corresponding to each permutation in $\mathrm{Deck}(f)$ are disjoint, so $f : R \to \mathbb{P}^1 \backslash P$ is a covering space.

For each i, define $h_i \in \mathcal{M}(R)$ to be the function sending

$$(z, \alpha_1(z), ..., \alpha_i(z), ..., \alpha_n(z)) \mapsto \alpha_i(z).$$

Then $F(f, h_i) \equiv 0$, so h_i is a root of the polynomial $F \in \mathbb{C}(f)[y]$. Furthermore, the h_i's generate $\mathcal{M}(R)$ over $\mathbb{C}(f)$. To see this, recall the isomorphism given by ι given above and assume that for some deck transformation g, the field automorphism ι_g fixes all of the h_i's. This means that for all i, $h_i(g^{-1}(z, \alpha_1(z), ..., \alpha_i(z), ..., \alpha_n(z)) = h_i(z, \alpha_1(z), ..., \alpha_i(z), ..., \alpha_n(z))$, so that the second through $(n+1)$th coordinates are fixed under g^{-1}. But since g^{-1} is a deck transformation and f projects onto the first coordinate, we see that the first coordinates are fixed under g^{-1} also, so g^{-1} (and hence g) is the identity deck transformation. So any ι_g which fixes all of the h_i is the identity automorphism, which implies that the h_i's generate the field extension. Thus, if we identify f with x, $\mathcal{M}(\bar{R}) = L$. One can see that at each prime that ramifies in this field extension, viewed as a point $p_i \in \mathbb{P}^1$, we can construct a $g_i \in \mathrm{Deck}(R) \cong \mathrm{Gal}(L/\mathbb{C}(x)) =: G$ as in the proof of Theorem 2.2, so that the g_i's generate G, each $g_i \in C_{p_i}$, and $g_1 g_2 ... g_r = 1$.

To sum up, we are able to start with a ramification type $(G, P, \{C_p\}_{p \in P})$ and, by Theorem 2.2, get a finite Galois cover $f : R \to \mathbb{P}^1 \backslash P$ with that ramification type if and only if G has the prescribed set of generators. Then, using the analytic version of RET, we are able to show that, given the covering space with that ramification type, the Galois group of the covering space is isomorphic to $\mathrm{Gal}(\mathcal{M}(\bar{R})/\mathcal{M}(\mathbb{P}^1))$, which is isomorphic to a field extension L of $\mathbb{C}(x)$ whose Galois group has that ramification type. Conversely, given any finite Galois extension $L/\mathbb{C}(x)$ of a certain ramificatinon type, we can construct a finite Galois cover of $\mathbb{P}^1 \backslash P$ whose group of deck transformations is isomorphic to $\mathrm{Gal}(L/\mathbb{C}(x))$, and we can define generators $g_1, ..., g_r$ with the desired properties. Thus, we have proven the algebraic statement of RET.