SOLVABLE NOTES

MICHAEL MUSTY

Contents

I. Belyĭ Maps	1
II. Galois Groups and Coverings	1
III. An Algorithm to Produce Permutation Triples	2
III.1. Intro	2
III.2. Degree 4	3
III.3. Degree 8 Galois	6
III.4. The Non-Galois Story	9
III.5. The Algorithm	9
III.6. Graph of Examples	9
IV. Orders in Function Fields	9
IV.1. Intro	9
V. Computing Belyĭ Maps	9
V.1. Intro	9
V.2. Explicit Example	10
References	11

I. Belyĭ Maps

TODO: [transitive permutation triples] TODO: [function fields] TODO: [the solvable story and the analogy with number fields] TODO: [iterated quadratic extensions of function fields] TODO: [naming convention so we can refer to specific examples]

II. GALOIS GROUPS AND COVERINGS

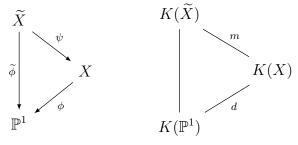
TODO: [describe how the iterative procedure leads us to a group theory question] TODO: [covering spaces via Rotman]

III. AN ALGORITHM TO PRODUCE PERMUTATION TRIPLES

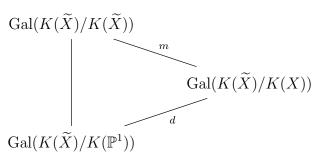
III.1. Intro. Let σ be a transitive permutation triple TODO: [link to previous section where this is defined]. Recall that this means

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3, \quad \sigma_\infty \sigma_1 \sigma_0 = 1,$$

and σ generates a transitive subgroup of S_d . As is described in TODO: [link], σ corresponds to a Belyĭ map $\phi: X \to \mathbb{P}^1$ of degree d. Given σ , we would like to describe all (Galois) Belyĭ maps $(\widetilde{X}, \widetilde{\phi})$ that are degree m covers of the given Belyĭ map (X, ϕ) . We will only be concerned with the particular case m = 2, but for now we remain in the more general setting. Put another way, $(\widetilde{X}, \widetilde{\phi})$ makes the diagrams



commute. According to Galois theory we have the following (upside down) diagram.



Let G, \widetilde{G}, H denote the Galois groups

$$G = \operatorname{Gal}(K(X)/K(\mathbb{P}^1))$$

$$\widetilde{G} = \operatorname{Gal}(K(\widetilde{X})/K(\mathbb{P}^1))$$

$$H = \operatorname{Gal}(K(\widetilde{X})/K(X)).$$

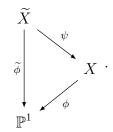
The above situation can be organized into an exact sequence of groups

$$1 \longrightarrow H \stackrel{\iota}{\longrightarrow} \widetilde{G} \stackrel{f}{\longrightarrow} G \longrightarrow 1.$$

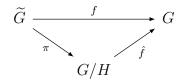
Now recall from section TODO: [link] that the groups \widetilde{G} and G are the monodromy groups for \widetilde{X} and X respectively. Thus, there is an action of \widetilde{G} on the md sheets of the covering $\widetilde{X} \to \mathbb{P}^1$ and there is an action

of G on the d sheets of the covering $X \to \mathbb{P}^1$. Identifying H with its image $\iota(H)$ in \widetilde{G} , we also have an action of H on the md sheets of the covering $\widetilde{X} \to \mathbb{P}^1$. To summarize, we can view $H \preceq \widetilde{G} \leq S_{md}$ and $G \leq S_d$. The groups \widetilde{G} and G are transitive since we only consider connected covers.

Moreover, the action of \widetilde{G} on the md sheets is required to factor through the diagram



To explain, the map $\psi:\widetilde{X}\to X$ is a m-sheeted cover and identifies the md sheets of \widetilde{X} into d blocks. From the exact sequence above, we have the diagram



with \hat{f} an isomorphism. Let $\tilde{g} \in f^{-1}(g)$ for some $g \in G$. According to the above diagrams, \tilde{G} must have a well-defined action on the d blocks realizing the element \tilde{g} as a permutation in S_d . MM: [more explanation?] Moreover, the action of \tilde{g} on blocks must agree with the action of g on $\{1, 2, \ldots, d\}$. That is, we must have

$$\hat{f}(\pi(\widetilde{g})) = f(\widetilde{g}) = g.$$

MM: [do we need to prove anything here? G-equivariant bijection?]

III.2. Degree 4.

Example III.2.1. TODO: [m=2, d=4, the Galois story] Up to isomorphism, there is only one degree 2 Belyĭ map $\phi: X \to \mathbb{P}^1$ corresponding to the permutation triple

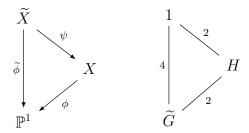
$$\sigma = ((12), (12), (1)(2)).$$

From σ (and the above discussion) we would like to find all $\tilde{\sigma}$ corresponding to degree m=2 covers of X that are Galois Belyĭ maps.

Notes

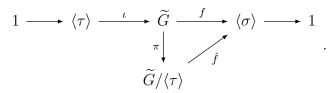
that is, $\widetilde{X} \to \mathbb{P}^1$ is degree 4 with monodromy \widetilde{G} having order 4.

That is, $\widetilde{\sigma}$ correspond to Belyĭ maps $(\widetilde{X},\widetilde{\phi})$ and monodromy groups \widetilde{G} making the diagrams



commute. Since m=2, H is an order 2 subgroup of S_4 that identifies 4 sheets to 2 sheets. Thus $H=\langle \tau \rangle$ with $\tau=(1\,2)(3\,4),\,\tau=(1\,3)(2\,4),$ or $\tau=(1\,4)(2\,3)$. We choose $\tau=(1\,3)(2\,4)$ so that the identification of sheets corresponds to reducing the sheets modulo 2 (labeling them 1,2,3,4). This identifies the 4 sheets into 2 blocks $\{\boxed{1\,3},\boxed{2\,4}\}$.

Moreover, by assuming \widetilde{X} Galois, we get $H \leq \widetilde{G}$. Also, $G = \langle \sigma \rangle = S_2 \cong \mathbb{Z}/2\mathbb{Z}$. Thus, we are looking for all permutation triples $\widetilde{\sigma} \in S_4^3$ that generate a (transitive) order 4 monodromy group $\widetilde{G} \leq S_4$ sitting in the exact sequence



Now we have the combinatorial task of pulling back σ under the map f.

Notes

One thing that makes me nervous is that we do not know the group \widetilde{G} a priori. If we have \widetilde{G} in hand (from a transitive group database or by some other means) with $\langle \tau \rangle \trianglelefteq \widetilde{G}$, then pulling back σ under f is nothing more than finding all $\widetilde{\sigma}$ that map to σ in the quotient (once this quotient is identified with $\langle \sigma \rangle$). MM: [When we don't have \widetilde{G} , how do we prove that identifying sheets via τ yields all possible $\widetilde{\sigma}$?]

The first requirement for any element in a preimage of f is that it has a well-defined action on the set of blocks $\{13, 24\}$ obtained from τ . For instance, (1234) does not have a well-defined action on these blocks. The only other requirement is that the action on blocks agrees with the permutation we are pulling back. MM: [more explanation?]

In our example, $\sigma_{\infty} = (1)(2)$. Then $f^{-1}(\sigma_{\infty})$ is precisely the $\widetilde{\sigma_{\infty}} \in S_4$ with a well-defined action on $B = \{\boxed{13}, \boxed{24}\}$ such that the action of $\widetilde{\sigma_{\infty}}$ on B agrees with the action of σ_{∞} on $\{1, 2\}$. Thus

$$f^{-1}(\sigma_{\infty}) = \{(1)(3)(2)(4), (13)(24)\} = \{(1)(2)(3)(4), (13)(24)\}.$$

For each $\widetilde{\sigma_{\infty}} \in f^{-1}(\sigma_{\infty})$ we can indeed check that the action of $\widetilde{\sigma_{\infty}}$ on blocks is given by (13)(24) (i.e. $\widetilde{\sigma_{\infty}}$ fixes each block). Similarly, for $\sigma_0 = \sigma_1 = (12)$ we have that

$$f^{-1}(\sigma_0) = f^{-1}(\sigma_1) = \{(1\,2\,3\,4), (1\,2)(3\,4), (1\,4\,2\,3), (1\,4)(2\,3)\}.$$

That is, each $\widetilde{\sigma}_i \in f^{-1}(\sigma_i)$ for $i \in \{0, 1\}$ acts on blocks by $(\boxed{13}\boxed{24})$.

Thus we have the following possibilities for the preimages of $\sigma_0 = \sigma_1 = (1 \, 2)$ and $\sigma_{\infty} = (1)(2)$ under f:

$$(1234), (12)(34), (1423), (14)(23) \mapsto (12)$$
$$(13)(24), (1)(2)(3)(4) \mapsto (1)(2)$$

and we can sort through these possibilities to see which ones correspond to degree 4 (Galois) Belyĭ maps according to TODO: [link]. If $\widetilde{\sigma_{\infty}} = (1)(2)(3)(4)$, then the condition that

$$\widetilde{\sigma_{\infty}}\widetilde{\sigma_1}\widetilde{\sigma_0} = (1)(2)(3)(4)$$

allows for only the single possibility $\widetilde{\sigma_0}=(1\,2\,3\,4)$ and $\widetilde{\sigma_1}=(1\,4\,2\,3)$ (up to simultaneous conjugation). MM: [should we prove that simultaneous conjugation does not mess up our convention of identifying sheets mod 2?] In this case $\widetilde{G}\cong \mathbb{Z}/4\mathbb{Z}$. If $\widetilde{\sigma_\infty}=\tau$, then there are two possibilities up to simultaneous conjugation. One possibility is

$$\widetilde{\sigma} = ((1\,2\,3\,4), (1\,2\,3\,4), (1\,3)(2\,4))$$

with $\widetilde{G} \cong \mathbb{Z}/4\mathbb{Z}$. The other possibility is

$$\widetilde{\sigma} = ((12)(34), (14)(32), (13)(24))$$

with $\widetilde{G} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

In summary, there are 3 permutation triples $\tilde{\sigma}$ (up to isomorphism) corresponding to degree 4 Galois Belyĭ maps that factor through the

degree 2 Belyĭ map corresponding to σ . They are as follows: TODO: [make a table?]

$$\Big((1\,2\,3\,4),(1\,4\,2\,3),(1)(2)(3)(4)\Big),\Big((1\,2\,3\,4),(1\,2\,3\,4),(1\,3)(2\,4)\Big),\Big((1\,2)(3\,4),(1\,4)(3\,2),(1\,3)(2\,4)\Big).$$

III.3. Degree 8 Galois.

Example III.3.1. TODO: [Galois degree 2 covers of 4T1-441] Let

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) = ((1 \, 2 \, 3 \, 4), (1 \, 4 \, 2 \, 3), (1)(2)(3)(4)).$$

We organize $f^{-1}(\sigma)$ in the following table.

$f^{-1}\Big((1234)\Big)$	$f^{-1}\Big((1423)\Big)$	$f^{-1}\Big((1)(2)(3)(4)\Big)$
(1234)(5678)	(1832)(4765)	(1)(2)(3)(4)(5)(6)(7)(8)
(1674)(2385)	(1436)(2587)	(15)(26)(37)(48)
(1634)(2785)	(1472)(3658)	
(1678)(2345)	(1476)(2583)	
(1274)(3856)	(1836)(2547)	
(1238)(4567)	(1432)(5876)	
(1278)(3456)	(1872)(3654)	
(1638)(2745)	(1876)(2543)	
(16785234)	(18725436)	
(12385674)	(14765832)	
(12785634)	(18365472)	
(16385274)	(18325476)	
(12345678)	(14725836)	
(16745238)	(18765432)	
(16345278)	(14365872)	
(12745638)	(14325876)	

These possibilities combine to yield $512 = 16^2 \cdot 2$ possible $\widetilde{\sigma}$. Of these 512 possibilities, only 32 have $\widetilde{\sigma_\infty}\widetilde{\sigma_1}\widetilde{\sigma_0} = \mathrm{id}_{S_8}$. Of these 32, only 24 generate a transitive order 8 subgroup of S_8 . MM: [include some of these lists?] Finally, if we identify triples that are simultaneously conjugate or in the same orbit under the S_3 action on triples, we get the following list of 3 possibilities for $\widetilde{\sigma}$ organized by \widetilde{G} :

$$\widetilde{G} \cong \mathbb{Z}/8\mathbb{Z} \\
\left((16785234), (14325876), id_{S_8} \right) \\
\left((16785234), (18365472), (15)(26)(37)(48) \right) \\
\widetilde{G} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\
\left((1234)(5678), (1836)(2547), (15)(26)(37)(48) \right)$$

Example III.3.2. TODO: [Galois degree 2 covers of 4T1-442] Let

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) = ((1234), (1234), (13)(24)).$$

We organize $f^{-1}(\sigma)$ in the following table.

$f^{-1}(\sigma_0)$	$f^{-1}(\sigma_1)$	$f^{-1}(\sigma_{\infty})$
(1, 2, 3, 4)(5, 6, 7, 8)	(1, 2, 3, 4)(5, 6, 7, 8)	(1,3)(2,4)(5,7)(6,8)
(1,6,7,4)(2,3,8,5)	(1,6,7,4)(2,3,8,5)	(1,3)(2,8)(4,6)(5,7)
(1,6,3,4)(2,7,8,5)	(1,6,3,4)(2,7,8,5)	(1,7)(2,4)(3,5)(6,8)
(1,6,7,8)(2,3,4,5)	(1,6,7,8)(2,3,4,5)	(1,7)(2,8)(3,5)(4,6)
(1, 2, 7, 4)(3, 8, 5, 6)	(1, 2, 7, 4)(3, 8, 5, 6)	(1,3,5,7)(2,4,6,8)
(1,2,3,8)(4,5,6,7)	(1, 2, 3, 8)(4, 5, 6, 7)	(1,3,5,7)(2,8,6,4)
(1, 2, 7, 8)(3, 4, 5, 6)	(1, 2, 7, 8)(3, 4, 5, 6)	(1,7,5,3)(2,4,6,8)
(1,6,3,8)(2,7,4,5)	(1,6,3,8)(2,7,4,5)	(1,7,5,3)(2,8,6,4)
(1, 6, 7, 8, 5, 2, 3, 4)	(1, 6, 7, 8, 5, 2, 3, 4)	
(1, 2, 3, 8, 5, 6, 7, 4)	(1, 2, 3, 8, 5, 6, 7, 4)	
(1, 2, 7, 8, 5, 6, 3, 4)	(1, 2, 7, 8, 5, 6, 3, 4)	
(1,6,3,8,5,2,7,4)	(1,6,3,8,5,2,7,4)	
(1, 2, 3, 4, 5, 6, 7, 8)	(1, 2, 3, 4, 5, 6, 7, 8)	
(1, 6, 7, 4, 5, 2, 3, 8)	(1, 6, 7, 4, 5, 2, 3, 8)	
(1,6,3,4,5,2,7,8)	(1,6,3,4,5,2,7,8)	
(1, 2, 7, 4, 5, 6, 3, 8)	(1, 2, 7, 4, 5, 6, 3, 8)	

These possibilities combine to yield 2048 possible $\tilde{\sigma}$. Of these, 128 have $\tilde{\sigma_{\infty}}\tilde{\sigma_{1}}\tilde{\sigma_{0}}=\mathrm{id}_{S_{8}}$. Of these, 120 generate a transitive subgroup of S_{8} . Of these 120 transitive groups, 24 have order equal to 8. Finally, after identifying triples up to simultaneous conjugation in S_{8} and the S_{3} action on triples, we get the following list of 3 possibilities for $\tilde{\sigma}$ organized by \tilde{G} :

$$\begin{split} \widetilde{G} &\cong \mathbb{Z}/8\mathbb{Z} \\ \hline & \left((16785234), (16785234), (1357)(2864) \right) \\ & \left((16785234), (12745638), (1753)(2468) \right) \\ \hline & \widetilde{G} &\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \hline & \left((1234)(5678), (1638)(2745), (17)(28)(35)(46) \right) \end{split}$$

MM: [3 things to mention here. . .

- 4T1-442 to 8T2-442 unramified.
- Notice that 8T1-882 does not factor through 4T1-442 even though it seems like it should be possible at first.
- We have identified a size 2 passport...should probably prove something about these always showing up and make sure attempts to optimize algorithm don't eliminate these...

1

Example III.3.3. TODO: [Galois degree 2 covers of 4T2-222] Let

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) = ((1234), (1234), (13)(24)).$$

We organize $f^{-1}(\sigma)$ in the following table.

$f^{-1}(\sigma_0)$	$f^{-1}(\sigma_1)$	$f^{-1}(\sigma_{\infty})$
(1,2)(3,4)(5,6)(7,8)	(1,4)(2,3)(5,8)(6,7)	(1,3)(2,4)(5,7)(6,8)
(1,2)(3,8)(4,7)(5,6)	(1,4)(2,7)(3,6)(5,8)	(1,3)(2,8)(4,6)(5,7)
(1,6)(2,5)(3,4)(7,8)	(1,8)(2,3)(4,5)(6,7)	(1,7)(2,4)(3,5)(6,8)
(1,6)(2,5)(3,8)(4,7)	(1,8)(2,7)(3,6)(4,5)	(1,7)(2,8)(3,5)(4,6)
(1, 2, 5, 6)(3, 4, 7, 8)	(1,4,5,8)(2,3,6,7)	(1,3,5,7)(2,4,6,8)
(1, 2, 5, 6)(3, 8, 7, 4)	(1,4,5,8)(2,7,6,3)	(1,3,5,7)(2,8,6,4)
(1,6,5,2)(3,4,7,8)	(1,8,5,4)(2,3,6,7)	(1,7,5,3)(2,4,6,8)
(1,6,5,2)(3,8,7,4)	(1,8,5,4)(2,7,6,3)	(1,7,5,3)(2,8,6,4)

These possibilities combine to yield 512 possible $\widetilde{\sigma}$. Of these, 64 have $\widetilde{\sigma_{\infty}}\widetilde{\sigma_{1}}\widetilde{\sigma_{0}}=\mathrm{id}_{S_{8}}$. Of these, 56 generate a transitive subgroup of S_{8} and all 56 have order 8. Finally, after identifying triples up to simultaneous conjugation in S_{8} and the S_{3} action on triples, we get the following list of 3 possibilities for $\widetilde{\sigma}$ organized by \widetilde{G} :

$$\widetilde{G} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\left((12)(34)(56)(78), (1458)(2367), (1753)(2864) \right)$$

$$\widetilde{G} \cong D_{8}$$

$$\left((12)(34)(56)(78), (14)(27)(36)(58), (1753)(2468) \right)$$

$$\widetilde{G} \cong Q_{8}$$

$$\left((1256)(3478), (1458)(2367), (1357)(2864) \right)$$

III.4. The Non-Galois Story.

Example III.4.1. TODO: [m = 2, d = 4, the non-Galois story] MM: [maybe do non-Galois in a different section...]

Example III.4.2. TODO: [m = 3...]

III.5. **The Algorithm.** We now formally describe an algorithm to compute all Galois degree 2 covers of a given Belyĭ map.

Algorithm III.5.1 (Brute Force).

Proof. \Box

III.6. Graph of Examples.

Example III.6.1. TODO: [graph of examples]

IV. Orders in Function Fields

IV.1. **Intro.** Following [5], we will start with the general setting with data (A, K, L) where A is a commutative domain, $K = \operatorname{Frac}(A)$, and L a finite extension of K. Given such a triple (A, K, L), we associate a subring $B \subset L$ such that $L = \operatorname{Frac}(B)$. TODO: [define order] TODO: [define maximal order] TODO: [define ring of integers]

V. Computing Belyi Maps

V.1. **Intro.** We begin by explaining a bit about the task of computing Belyĭ maps in general. TODO: [reference the various methods for computing maps in general and in specific cases too....] For a (much) more detailed account see [7].

TODO: [Explain the special setting we are in]

V.2. Explicit Example. We now explain an explicit example. Let $K = \overline{\mathbb{Q}}$. Let $X_0 = \mathbb{P}^1$ over K. Up to isomorphism, there is a unique degree 2 Belyĭ map $\varphi : X_1 \to X_0$. Let $K(X_0)$ be the function field of X_0 which is $K(x_0)$ (the rational function field). To write down an equation for X_1 , we must specify the ramification values (branch points) on X_0 . We can do this by recording the ramification values in a divisor $D^0 \in \text{Div}(X_0)$. For the degree 2 Belyĭ map, we get to choose 2 branch points on X_0 , say 0 and ∞ so that $D^0 = 0 - \infty$.

MM: [mention how this comes to us from previous section]

Next, we find $f_0 \in K(X_0)$ such that the quadratic function field extension

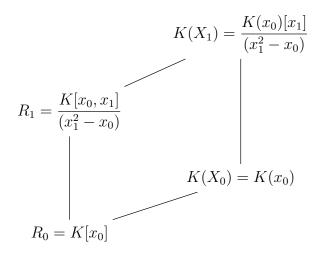
$$K(X_1) := \frac{K(X_0)[x_1]}{(x_1^2 - f_0)}$$

corresponds to φ .

MM: [write down explicitly the correspondence?]

MM: [explain choices involved in choosing f... i.e. up to square and such that $\operatorname{div}(f)$ has property...]

We get that $f_0 = x_0$ and X_1 is the projective closure of the affine curve defined by the equation $x_1^2 - x_0$. On the function field side, we have the following diagram.



Let $\mathfrak{p}_0 = (x_0, x_1)$. We can see that we have the right ramification since

$$(x_0) = \mathfrak{p}_0^2$$

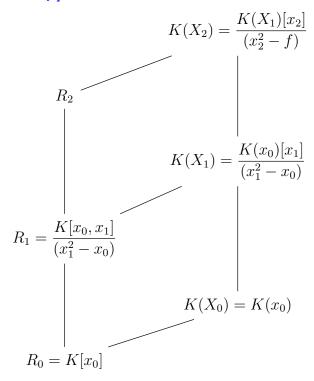
 $(1/x_0) = \mathfrak{p}_0^{-2}$

and the discriminant of R_1 is $4x_0$. What are the primes above $(x_0 - 1)$? Well, $(x_0 - 1) = \mathfrak{p}_1\mathfrak{p}_2$ where

$$\mathfrak{p}_1 = (x_0 - 1, x_1 - 1)$$
$$\mathfrak{p}_2 = (x_0 - 1, x_1 + 1).$$

Now...

MM: [In summary,]



References

- 1. Gennadii Vladimirovich Belyi, On galois extensions of a maximal cyclotomic field, Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya **43** (1979), no. 2, 267–276.
- 2. David Steven Dummit and Richard M Foote, *Abstract algebra*, vol. 3, Wiley Hoboken, 2004.
- 3. Alexandre Grothendieck, Esquisse d'un programme, London Mathematical Society Lecture Note Series (1997), 5–48.
- 4. Michael Klug, Michael Musty, Sam Schiavone, and John Voight, *Numerical calculation of three-point branched covers of the projective line*, LMS Journal of Computation and Mathematics 17 (2014), no. 01, 379–430.
- 5. Dino Lorenzini, An invitation to arithmetic geometry, vol. 9, American Mathematical Soc., 1996.
- 6. Jean-Pierre Serre, Topics in galois theory, CRC Press, 2007.
- 7. Jeroen Sijsling and John Voight, On computing belyi maps, arXiv preprint arXiv:1311.2529 (2013).