REGULAR LIFTING OF COVERS
OVER AMPLE FIELDS

by

Dan Haran* and Moshe Jarden*

School of Mathematical Sciences, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

e-mail: haran@math.tau.ac.il   and   jarden@math.tau.ac.il

May 29, 2000

Introduction

Colliot-Thélène [CT] uses the technique of Kollár, Miyaoka, and Mori to prove the following result.

THEOREM A: *Let K be an ample field of characteristic 0, x a transcendental element over K, and G a finite group. Then there is a Galois extension F of $K(x)$ with Galois group G, regular over K. Moreover, F has a K-rational place φ.*

In fact, Colliot-Thélène proves a stronger version:

THEOREM B: *Given a Galois extension L/K with Galois group Γ which is a subgroup of G, one can choose F and φ so that the residue field extension of $F/K(x)$ under φ is L/K.*

Case $\Gamma = G$ of Theorem B means that K has the arithmetic lifting property of Beckmann and Black [BB].

As the results of Kollár, Miyaoka, and Mori are valid only in characteristic 0, Colliot-Thélène's proof works only in this case. Nonetheless, Theorem A holds in arbitrary characteristic ([Ha, Corollary 2.4] for complete fields, [Po1, Main Theorem A]; see also [Li] and [HV]). Moret-Bailly [MB], using methods of formal patching, extends Theorem B to arbitrary characteristic.

Here we use algebraic patching to prove Theorem B for arbitrary characteristic. In fact, the main ingredient of the proof is almost contained in [HJ1]. Therefore this note can be considered a sequel to [HJ1]; a large portion of it recalls the situation and facts considered there.

We also notice that if K is PAC and F is an *arbitrary* Galois extension of $K(x)$ with Galois group G, regular over K, then, *for every* Galois extension L/K with Galois group which is a subgroup of G, we can choose φ so that the residue field extension of $F/K(x)$ under φ is L/K. (After the first draft of this note has been written, P. Dèbes informed us that he also made this observation in [De, Remark 3.3].) This answers a question of Harbater. Notice that this stronger property does not hold for an arbitrary ample field K [CT, Appendix].

1

The idea (displayed in our Lemma 2.1) to use the embedding problem $G \ltimes G \to G$ in order to obtain the arithmetic lifting property has been used in [Po2]; we are grateful to F. Pop for making his notes available to us.

1. Embedding problems and decomposition groups

Let K/K_0 be a finite Galois extension with Galois group Γ. Let x be a transcendental element over K. Put $E_0 = K_0(x)$. Suppose that Γ acts (from the right) on a finite group G; let $\Gamma \ltimes G$ be the corresponding semidirect product and $\pi \colon \Gamma \ltimes G \to \Gamma$ the canonical projection. We call

$$(1) \qquad\qquad \pi \colon \Gamma \ltimes G \to \Gamma = \mathcal{G}(K/K_0)$$

a **finite constant split embedding problem**. A **solution** of (1) is a Galois extension F of E_0 such that $K \subseteq F$, $\mathcal{G}(F/E_0) = \Gamma \ltimes G$, and π is the restriction map $\mathrm{res}_K \colon \mathcal{G}(F/E_0) \to \mathcal{G}(K/K_0)$.

In [HJ1, Theorem 6.4] we reprove the following result of F. Pop [Po1]:

PROPOSITION 1.1: *Let K_0 be an ample field. Then each finite constant split embedding problem (1) has a solution F such that F has a K-rational place. (In particular, F/K is regular.)*

In this section we show that the proof of Proposition 1.1 in [HJ1] yields a stronger assertion.

LEMMA 1.2: *Let F be a solution of (1). Put $F_0 = F^\Gamma$. Let $\varphi \colon F \to \widetilde{K_0}$ be a K-place extending a K_0-place of E_0. Assume that φ is unramified in F/E_0 and let D_φ be its decomposition group in F/E_0. Then $\varphi(F) \supseteq K$ and the following assertions are equivalent:*
(a) *$\varphi(F) = K$ and $\Gamma = D_\varphi$;*
(b) *$\Gamma \supseteq D_\varphi$;*
(c) *$\varphi(F_0) = K_0$;*
(d) *$\varphi(F) = K$ and $\varphi(f^\gamma) = \varphi(f)^\gamma$ for each $\gamma \in \Gamma$ and $f \in F$ with $\varphi(f) \neq \infty$.*

Proof: As $K \subseteq F$, we have $K = \varphi(K) \subseteq \varphi(F)$. Since the inertia group of φ in F/E_0 is trivial, we have an isomorphism $\theta \colon D_\varphi \to \mathcal{G}(\varphi(F)/K_0)$ given by

$$(2) \qquad \varphi(f^\gamma) = \varphi(f)^{\theta(\gamma)}, \qquad \gamma \in D_\varphi,\ f \in F,\ \varphi(f) \neq \infty.$$

Hence $|D_\varphi| = [\varphi(F) : K_0] \geq [K : K_0] = |\Gamma|$. This gives (a) $\Leftrightarrow$ (b).

Since φ is unramified over E_0, the decomposition field F^{D_φ} is the largest intermediate field of F/E_0 mapped by φ into K_0, and hence (b) $\Leftrightarrow$ (c).

Clearly (d) $\Rightarrow$ (c). If $\varphi(F) = K$, apply (2) to $f \in K$ to see that $\theta(\gamma) = \gamma$ for all $\gamma \in D_\varphi$. Hence (a) $\Rightarrow$ (d). ∎

Remark 1.3: Let K_0 be an ample field and let F be a solution of (1). Suppose that F has a K-rational place extending K_0-places of E_0 and unramified over E_0 such that Γ is its decomposition group in F/E_0. Then F has infinitely many such places.

Indeed, put $F_0 = F^\Gamma$. Recall that F_0 is regular over K_0. By Lemma 1.2,
(a) the assumption is that there is a K_0-place $\varphi \colon F_0 \to K_0$ unramified over $K_0(x)$, and
(b) we have to show that there are infinitely many such places.
But (a) $\Rightarrow$ (b) is a property of an ample field. ∎

PROPOSITION 1.4: *Let K_0 be an ample field. Then each finite constant split embedding problem (1) has a solution F with a K-rational place of F extending a K_0-place of E_0 and unramified over E_0 such that Γ is its decomposition group in F/E_0.*

Proof: Put $E = K(x) = KK_0(x)$.

PART A: As in the proof of [HJ1, Theorem 6.4], we first assume that K_0 *is complete with respect to a non-trivial discrete ultrametric absolute value, with infinite residue field and K/K_0 is unramified.*

In this case [HJ1, Proposition 5.2] proves Proposition 1.1. Claim C of that proof shows that, for every $b \in K_0$ with $|b| > 1$, $x \to b$ extends to a K-homomorphism $\varphi_b \colon R \to K$, where R is the principal ideal ring $K\{\frac{1}{x-c_i} \mid i \in I\}$. From there it extends to a K-place $\varphi_b \colon Q \to K \cup \{\infty\}$ of the $Q = \mathrm{Quot}(R)$. Furthermore, [HJ1, Lemma 1.3(b)] gives an E-embedding $\lambda \colon F \to Q$. The compositum $\varphi = \varphi_b \circ \lambda$ is a K-rational place of

F. Excluding finitely many b's we may assume that φ is unramified over E_0. To verify that φ satisfies condition (d) of Lemma 1.2, we first recall the relevant facts from [HJ1].

(a) [HJ1, Proposition 5.2, Construction B] The group $\Gamma = \mathcal{G}(K/K_0)$ lifts isomorphically to $\mathcal{G}(E/E_0)$. By the choice of the c_i we have $\left(\frac{1}{x-c_i}\right)^\gamma = \frac{1}{x-c_i^\gamma}$, for each $\gamma \in \Gamma$. It follows that Γ continuously acts on R in the following way

$$\left(a_0 + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in} \left(\frac{1}{x-c_i}\right)^n\right)^\gamma = a_0^\gamma + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in}^\gamma \left(\frac{1}{x-c_i^\gamma}\right)^n.$$

This action induces an action of Γ on Q.

(b) [HJ1, (7) on p. 334] The above mentioned action of Γ on Q defines an action of Γ on the Q-algebra

$$N = \mathrm{Ind}_1^G Q = \left\{ \sum_{\theta \in G} a_\theta \theta \mid a_\theta \in Q \right\}$$

in the following way:

$$\left(\sum_{\theta \in G} a_\theta \theta\right)^\gamma = \sum_{\theta \in G} a_\theta^\gamma \theta^\gamma \qquad a_\theta \in Q, \ \gamma \in \Gamma.$$

Furthermore, the field F is a subring of N [HJ1, p. 332] and Γ acts on it by restriction from N [HJ1, Proof of Proposition 1.5, Part A].

(c) The embedding $\lambda \colon F \to Q$ is just the restriction to F of the projection

$$\sum_{\theta \in G} a_\theta \theta \mapsto a_1$$

from $N = \mathrm{Ind}_1^G Q \to Q$ [HV, Proposition 3.4].

(d) The place $\varphi_b \colon Q \to K \cup \{\infty\}$ is induced from the evaluation homomorphism $\varphi_b \colon R \to K$ given by [HJ1, Remark 3.5]

$$\varphi_b \left(a_0 + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in} \left(\frac{1}{x-c_i}\right)^n\right) = a_0 + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in} \left(\frac{1}{b-c_i}\right)^n.$$

In order to prove condition (d) of Lemma 1.2 it suffices to show that both λ and φ_b are Γ-equivariant.

4

Let $f = \sum_{\theta \in G} a_\theta \theta \in F \subseteq N$. Then, by (b) and (c),

$$\lambda(f^\gamma) = \lambda\Big(\sum_{\theta \in G} a_\theta^\gamma \theta^\gamma\Big) = a_1^\gamma = \Big(\lambda\Big(\sum_{\theta \in G} a_\theta \theta\Big)\Big)^\gamma = \lambda(f)^\gamma.$$

Furthermore, let $r = a_0 + \sum_{i \in I} \sum_{n=1}^\infty a_{in}\big(\frac{1}{x-c_i}\big)^n \in R$. By (a) and (d),

$$\varphi_b(r^\gamma) = \varphi_b\Big(a_0^\gamma + \sum_{i \in I} \sum_{n=1}^\infty a_{in}^\gamma \big(\frac{1}{x - c_i^\gamma}\big)^n\Big) = a_0^\gamma + \sum_{i \in I} \sum_{n=1}^\infty a_{in}^\gamma \big(\frac{1}{b - c_i^\gamma}\big)^n$$

$$= \Big(a_0 + \sum_{i \in I} \sum_{n=1}^\infty a_{in}\big(\frac{1}{b - c_i}\big)^n\Big)^\gamma = \varphi_b(r)^\gamma.$$

Thus φ_b is Γ-equivariant.

PART B: K_0 *is an arbitrary ample field.* As in the proof of [HJ1, Theorem 6.4] let $\hat{K}_0$ be the field of Laurent series over K_0. Then $\hat{K} = K\hat{K}_0$ is an unramified extension of $\hat{K}_0$ with Galois group Γ and infinite residue field.

By Part A, $\hat{K}_0(x)$ has a Galois extension $\hat{F}$ which contains $\hat{K}(x)$, such that $\mathcal{G}(\hat{F}/\hat{K}_0(x)) = \Gamma \ltimes G$ and the restriction map $\mathcal{G}(\hat{F}/\hat{K}_0(x)) \to \mathcal{G}(K/K_0)$ is the projection $\pi \colon \Gamma \ltimes G \to \Gamma$. Furthermore, there is $b \in \hat{K}_0$ such that the place $x \to b$ of $\hat{K}_0(x)$ extends to an unramified $\hat{K}$-place $\hat{\varphi} \colon \hat{F} \to \hat{K}$ and $\hat{\varphi}(\hat{F}^\Gamma) = \hat{K}_0$. Put $m = |G|$.

Use Weak Approximation to find $y \in \hat{F}^\Gamma$ mapped by the m distinct extensions of $x \to b$ to $\hat{F}^\Gamma$ into m distinct elements of the separable closure of $\hat{K}_0$; then $\hat{F}^\Gamma = \hat{K}_0(x, y)$.

Thus there exist polynomials $f \in \hat{K}_0[X, Z]$, $g \in \hat{K}_0[X, Y]$, elements $z \in \hat{F}$, $y \in \hat{F}^\Gamma$, and elements $b, c \in \hat{K}_0$, such that the following conditions hold:

(3a) $\hat{F} = \hat{K}_0(x, z)$, $f(x, Z) = \mathrm{irr}(z, \hat{K}_0(x))$; we may therefore identify $\mathcal{G}(f(x, Z), \hat{K}_0(x))$ with $\mathcal{G}(\hat{F}/\hat{K}_0(x))$;

(3b) $\hat{F}^\Gamma = \hat{K}_0(x, y)$, whence $\hat{F} = \hat{K}(x, y)$, and $g(x, Y) = \mathrm{irr}(y, \hat{K}_0(x))$; therefore $g(X, Y)$ is absolutely irreducible;

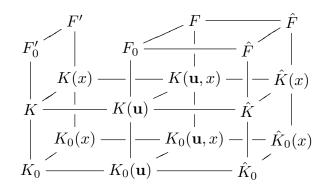(3c) $\mathrm{discr} g(b, Y) \neq 0$ and $g(b, c) = 0$.

All of these objects depend on only finitely many parameters from $\hat{K}_0$. So, there are $u_1, \dots, u_n \in \hat{K}_0$ So, let $u_1, \dots, u_n$ be elements of $\hat{K}_0$ such that the following conditions hold:

(4a) $F = K_0(\mathbf{u}, x, z)$ is a Galois extension of $K_0(\mathbf{u}, x)$, the coefficients of $f(X, Z)$ lie in $K_0[\mathbf{u}]$, $f(x, Z) = \mathrm{irr}(z, K_0(\mathbf{u}, x))$, and $\mathcal{G}(f(x, Z), K_0(\mathbf{u}, x)) = \mathcal{G}(f(x, Z), \hat{K}_0(x))$;

(4b) the coefficients of g lie in $K[\mathbf{u}]$; hence $g(x, Y) = \mathrm{irr}(y, K_0(\mathbf{u}, x))$; furthermore, $K_0(\mathbf{u}, x, y) = F^\Gamma$;

(4c) $b, c \in K_0[\mathbf{u}]$ and $\mathrm{discr} g(b, Y) \neq 0$ and $g(b, c) = 0$.

Since $\hat{K}_0$ has a K-rational place, namely, $x \to 0$, the field $\hat{K}_0$ and therefore also $K_0(\mathbf{u})$ are regular extensions of K_0. Thus, $\mathbf{u}$ generates an absolutely irreducible variety $U = \mathrm{Spec}(K_0[\mathbf{u}])$ over K_0. By Bertini-Noether [FJ, Proposition 8.8] the variety U has a nonempty Zariski open subset U' such that for each $\mathbf{u}' \in U'$ the K_0-specialization $\mathbf{u} \to \mathbf{u}'$ extends to a K-homomorphism $': K[\mathbf{u}, x, z, y] \to K[\mathbf{u}', x, z', y']$ such that the following conditions hold:

(5a) $f'(x, z') = 0$, the discriminant of $f'(x, Z)$ is not zero, and $F' = K_0(\mathbf{u}', x, z')$ is the splitting field of $f'(x, Z)$ over $K_0(\mathbf{u}', x)$; in particular $F'/K_0(\mathbf{u}', x)$ is Galois;

(5b) $g'(X, Y)$ is absolutely irreducible and $g'(x, y') = 0$; so $g'(x, Y) = \mathrm{irr}(y', K(\mathbf{u}', x))$; furthermore, $K_0(\mathbf{u}', x, y') = (F')^\Gamma$;

(5c) $b', c' \in K_0[\mathbf{u}']$ and $\mathrm{discr} g'(b', Y) \neq 0$ and $g'(b', c') = 0$.

As K_0 is existentially closed in $\hat{K}_0$, and since $\mathbf{u} \in U(\hat{K}_0)$, there is $\mathbf{u}' \in U(K_0)$. Now repeat the end of the proof of [HJ1, Lemma 6.2] (from "By (5a), the homomorphism..." to conclude that F' is a solution of (1).

Condition (5c) ensures that the place $x \to b'$ of $K_0(x)$ is unramified in in $(F')^\Gamma$, hence in F', and extends to a K_0-rational place of $(F')^\Gamma$. This ends the proof by Lemma 1.2.   ∎

2. Lifting property over ample fields

Let Γ be a subgroup of a finite group G. Let Γ act on G by the conjugation in G

$$g^\gamma = \gamma^{-1} g \gamma.$$

and consider the semidirect product $\Gamma \ltimes G$. To fix notation, $\Gamma \ltimes G = \{(\gamma, g) \mid \gamma \in \Gamma, g \in G\}$ and the multiplication on $\Gamma \ltimes G$ is defined by

$$(\gamma_1, g_1)(\gamma_2, g_2) = (\gamma_1 \gamma_2, g_1^{\gamma_2} g_2).$$

Notice that $\Gamma \ltimes G \cong \Gamma \times G$ by $(\gamma, g) \mapsto (\gamma, \gamma g)$. However, the above presentation gives a different splitting of the projection $\Gamma \times G \to \Gamma$. In particular, we have an epimorphism $\rho \colon \Gamma \ltimes G \to G$ given by $(\gamma, g) \mapsto \gamma g$. Let N denote its kernel.

LEMMA 2.1: *Let K_0 be a field, K a Galois extension of K_0 with Galois group Γ, and x a transcendental element over K_0. Assume that (1) has a solution $\hat{F}$ with a K-rational place $\hat{\varphi}$ of F extending a K_0-place of $K_0(x)$ and unramified over $K_0(x)$ such that Γ is its decomposition group in $F/K_0(x)$. Let $F = \hat{F}^N$ and let φ be the restriction of $\hat{\varphi}$ to F. Then*

(6a) *F is a Galois extension of $K_0(x)$ and $\mathcal{G}(F/K_0(x)) \cong G$;*

(6b) *F/K_0 is a regular extension;*

(6c) *φ represents a prime divisor $\mathfrak{p}$ of F/K_0 with decomposition group Γ in $F/K_0(x)$ and residue field K.*

Proof: By assumption, $\hat{F}$ is a Galois extension of $K_0(x)$ containing K, with Galois group $\Gamma \ltimes G$ such that the restriction $\mathcal{G}(\hat{F}/K_0(x)) \to \mathcal{G}(K/K_0)$ is the projection $\Gamma \ltimes G \to \Gamma$, and $\hat{F}/K$ is regular. Furthermore, $\hat{\varphi} \colon \hat{F} \to K$ is a K-place unramified over $K_0(x)$, with decomposition group $\Delta = \{(\gamma, 1) \mid \gamma \in \Gamma\} \cong \Gamma$ in $\hat{F}/K_0(x)$ and residue field extension K/K_0. In particular, $\hat{F}$ is regular over K.

From the definition of F we get (6a) and $\rho(\Delta) = \Gamma \leq G$ is the decomposition group of the restriction $\varphi \colon F \to K$ of $\hat{\varphi}$ to F. As $|\Delta| = [K : K_0]$, the residue field of φ is K. As $\Gamma \ltimes G = NG$, the fields $F = \hat{F}^N$ and $K(x) = \hat{F}^G$ are linearly disjoint over $K_0(x)$. Therefore F is regular over K_0. ∎

Lemma 2.1 together with Proposition 1.4 and Remark 1.3 yield the following result, originally proved by Colliot-Thélène [CT, Theorem 1] in characteristic 0:

THEOREM 2.2: *Let K_0 be an ample field, G a finite group, Γ a subgroup, K a Galois extension of K_0 with Galois group Γ, and x a transcendental element over K_0. Then there is F that satisfies (6a), (6b) and*

(6d) *there are infinitely many prime divisors $\mathfrak{p}$ of F/K_0 with decomposition group Γ in $F/K_0(x)$ and residue field K.*

Remark 2.3: In case of $\Gamma = G$, Theorem 2.2 says that an ample field K_0 has the so-called **arithmetic lifting property** of Beckmann-Black [BB]. ∎

If K_0 is a PAC field, an even stronger property holds.

THEOREM 2.4: *Let K_0 be a PAC field, G a finite group, F a function field of one variable over K_0, and E a subfield of F such that F/E is Galois with Galois group G. Let Γ be a subgroup of G and K a Galois extension of K_0 with Galois group Γ. Then there are infinitely many prime divisors $\mathfrak{p}$ of F/K_0 with decomposition group Γ in F/E and residue field K.*

Proof: By definition, F is a regular extension of K_0. In particular, F is linearly disjoint from K over K_0. Hence,

$$\mathcal{G}(FK/E) = \mathcal{G}(FK/F) \times \mathcal{G}(FK/EK) \cong \Gamma \times G.$$

Consider the subgroup $\Delta = \{(\gamma, \gamma) \in \Gamma \times G \,|\, \gamma \in \Gamma\}$ of $\mathcal{G}(FK/E)$. It satisfies the following conditions:

(7a) $\Delta \cdot (\Gamma \times 1) = \Gamma \times \Gamma$ and $\Delta \cap (\Gamma \times 1) = 1$.

(7b) $\Delta \cdot (1 \times G) = \Gamma \times G$ and $\Delta \cap (G \times 1) = 1$.

Denote the fixed field of Δ in FK by D and the fixed field of the subgroup Γ of $G = \mathcal{G}(F/E)$ by F_0. Condition (7) translates via Galois theory to the following one:

(8a) $D \cap F = F_0$ and $DF = FK$.

(8b) $D \cap EK = E$ and $DK = FK$.

As F/K_0 is regular, so is FK/K. Hence, by (8b), D/K_0 is a regular extension. Since K_0 is PAC, there exist infinitely many K_0-places $\varphi \colon D \to K_0$. Use (8b) to extend

8

each such φ to a K-place $\psi\colon FK \to K$. As $[FK : D] = |\Delta| = |\Gamma| = [K : K_0]$, D is the decomposition field of ψ in FK/E. By (8a), F_0 is the decomposition field of $\psi|_F$ in F/E. ∎

COROLLARY 2.5: *Let K_0 be a PAC field, E a function field of one variable over K_0, and G a finite group. For $i = 1, \ldots, n$ let Γ_i be a subgroup of G and K_i a Galois extension of K_0 with Galois group Γ_i. Then E has a Galois extension F such that*

(9a) $\mathcal{G}(F/E) \cong G$.

(9b) *F/K_0 is a regular extension.*

(9c) *For each i there exists a prime divisor $\mathfrak{p}_i$ of F/K_0 with decomposition group over E equal to Γ_i and with residue field K_i. Moreover, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct.*

Proof: The existence of F with the properties (9a) and (9b) is well known [HJ2, Theorem 2]. Now apply Theorem 2.4 successively to Γ_i and K_i instead of to Γ and K. ∎

References

[BB]   E.V. Black, *Deformations of dihedral 2-group extensions of fields,* Transactions of the AMS **351** (1999), 3229–3241.

[CT]   J.-L. Colliot-Thélène, *Rational connectedness and Galois cover of the projective line,* a preprint.

[De]   P. Dèbes, *Galois Covers with Prescribed Fibers: The Beckmann-Black Problem,* Ann. Scuola Norm. Sup. Pisa **28** (1999), 273–286.

[FJ]   M. D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

[Ha]   D. Harbater, *Galois coverings of the arithmetic line,* in: Lecture Notes in Mathematics **1240**, 165–195, Springer-Verlag 1987.

[HJ1]   D. Haran and M. Jarden, *Regular split embedding problems over complete valued fields,* Forum Mathematicum **10** (1998), 329–351 .

[HJ2]   D. Haran and M. Jarden, *Regular split embedding problems over function fields of one variable over ample fields,* Journal of Algebra, **208** (1998), 147–164.

[HV]   D. Haran and H. Völklein, *Galois groups over complete valued fields,* Israel Journal of Mathematics, **93** (1996), 9–27.

[Li]   Q. Liu, *Tout groupe fini est un groupe de Galois sur $\mathbb{Q}_p(T)$, d'après Harbater,* Contemporary Mathematics **186** (1995), 261–265.

[MB]   L. Moret-Bailly, *Construction de revêtements de courbes pointées,* preprint, June 1999.

[Po1]   F. Pop, *Embedding problems over large fields,* Annals of Mathematics **144** (1996), 1–34.

[Po2]   F. Pop, *On the BB theory,* an unpublished note, 2 pages.