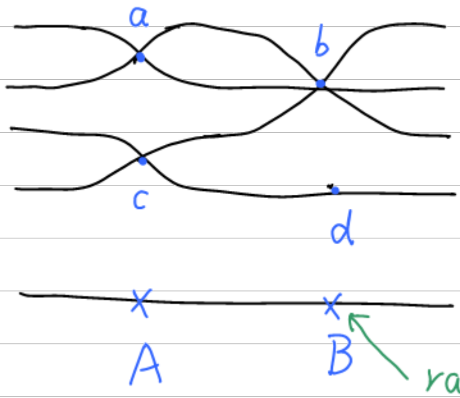
Belyi's Theorem

1. Ramification
2. Irreducible algebraic curves
3. Statement of Belyi's theorem
4. A one-side proof: (a) ⇒ (b)

1. Ramification



ramification points

$$\begin{tikzcd} S \arrow[d, "f"] \\ T \end{tikzcd} \qquad \begin{tikzcd} a \arrow[dr, "2"'] & & c \arrow[dl, "2"] \\ & A & \end{tikzcd} \qquad \begin{tikzcd} b \arrow[dr, "3"'] & & d \arrow[dl, "1"] \\ & B & \end{tikzcd}$$

$\mathrm{Ram}(f) = \{a, b, c\}$

$\mathrm{Branch}(f) = \{A, B\}$

$f(\mathrm{Ram}(f)) = \mathrm{Branch}(f)$

$f^{-1}(\mathrm{Branch}(f)) \subseteq \mathrm{Ram}(f)$

$$\begin{tikzcd} S \setminus \mathrm{Ram}(f) \arrow[d, "\text{covering map}"] \\ T \setminus \mathrm{Branch}(f) \end{tikzcd}$$

定义 B.3.1 设 $e \in \mathbb{Z}_{\geq 1} \sqcup \{\infty\}$.

- 若 e 有限, 按 $z \mapsto z^e$ 定义单位开圆盘到自身的连续满射 $f_e : \mathscr{D} \to \mathscr{D}$;
- 若 $e = \infty$, 按 $\tau \mapsto \exp(2\pi i \tau)$ 定义 $\mathscr{H} \sqcup \{\infty\}$ 到 $\mathscr{D}$ 的连续满射 f_e, 映 ∞ 为 0.

两种情形下都称 f_e 为 e 次**标准分歧复叠**.

定义 B.3.3 连续满射 $f : S \to T$ 具备以下性质时称为**分歧复叠**: 对每个 $t \in T$ 存在开邻域 $V \ni t$ 和 S 的一族无交开子集 $\{U_i\}_{i \in I}$ 使得 $f^{-1}(V) = \bigsqcup_{i \in I} U_i$, 而且对每个 $i \in I$, 皆存在 $e \in \mathbb{Z} \sqcup \{\infty\}$ 和从 $U_i \xrightarrow{f} V$ 到标准分歧复叠 f_e 的同胚, 使 t 对应到 $0 \in \mathscr{D}$.

定义–定理 B.3.4 设 $f : S \to T$ 是分歧复叠, 则对任意 $s \in S$ 及其邻域 U_1, 总存在开邻域 $U \ni s, U \subset U_1$ 使得 $f^{-1}(f(s)) \cap U = \{s\}$ 而 $U \setminus \{s\} \xrightarrow{f} f(U \setminus \{s\})$ 是复叠映射, 其次数 $e(s)$ 称为 f 在 s 处的**分歧指数**, 它只和 s 与 f 相关.

定义 B.3.5 设 $f : S \to T$ 为分歧复叠. 满足 $e(s) > 1$ 的点 $s \in S$ 称为**分歧点**. 全体分歧点构成 S 的子集 $\mathrm{Ram}(f)$.

Ex. 1) Calculate $\mathrm{Branch}(f)$, where

$f : \mathbb{P}\mathbb{C}^1 \longrightarrow \mathbb{P}\mathbb{C}^1 \quad z \longmapsto z^3 + \frac{1}{z^3}$

2). Suppose $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ are maps between RSs, prove $\mathrm{Branch}(g \circ f) = \mathrm{Branch}(g) \cup g(\mathrm{Branch}(f))$

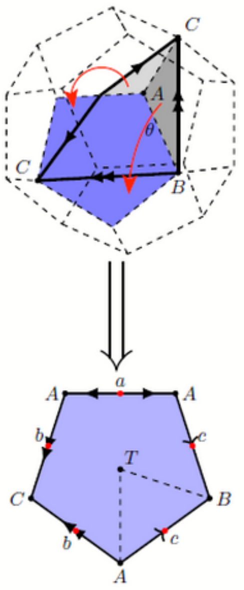


图 1.7

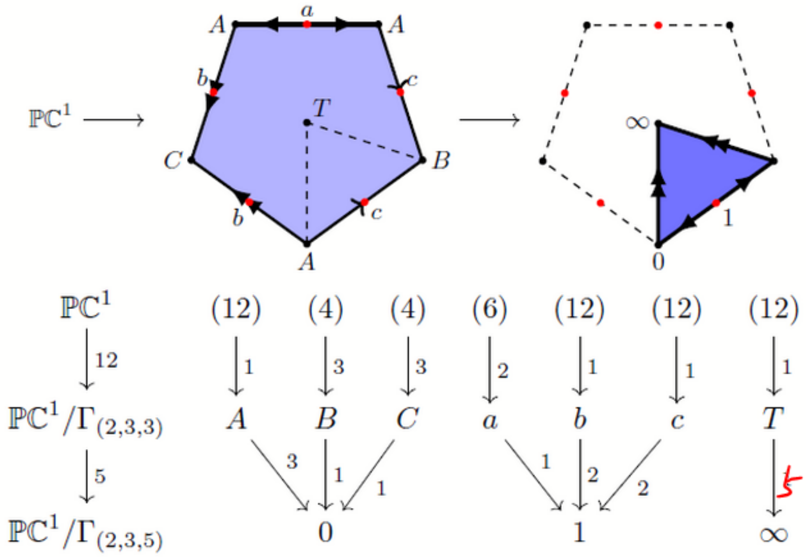


图 1.8 分歧点与分歧指标

(useless figure)

2. Irreducible algebraic curves

Remark 1.94 We have shown the equivalence between the following classes of objects:

(1) Compact Riemann surfaces S.

(2) *Function fields in one variable* (i.e. finite extensions of $\mathbb{C}(X)$).

(3) Irreducible algebraic curves $C : F(X, Y) = 0$.

RS $S \longrightarrow$ finite extensions of $\mathbb{C}(x)$

PET (primitive element theorem)

Irr alg curves $C: F(X,Y)=0$

Theorem 1.86 *Let*

$$F(X,Y) = p_0(X)Y^n + p_1(X)Y^{n-1} + \cdots + p_n(X)$$
$$= q_0(Y)X^m + q_1(Y)X^{m-1} + \cdots + q_m(Y)$$

be an irreducible polynomial. If $n \geq 1$ define

$$S_F^X = \{(x,y) \in \mathbb{C}^2 \mid F(x,y) = 0, F_Y(x,y) \neq 0, p_0(x) \neq 0\}$$

and, similarly, if $m \geq 1$ set

$$S_F^Y = \{(x,y) \in \mathbb{C}^2 \mid F(x,y) = 0, F_X(x,y) \neq 0, q_0(y) \neq 0\}$$

Then:

(i) S_F^X and S_F^Y are connected Riemann surfaces on which the coordinate functions $\mathbf{x}$ and $\mathbf{y}$ are holomorphic functions.

(ii) There exists a unique compact and connected Riemann surface $S = S_F$ that contains S_F^X and S_F^Y.

(iii) The coordinate functions $\mathbf{x}$ and $\mathbf{y}$ extend to meromorphic functions on S.

(iv) The branching points of $\mathbf{x}$ (resp. $\mathbf{y}$) lie in the finite set $S \setminus S_F^X$ (resp. $S \setminus S_F^Y$).

E.g. Klein quartic $F(X,Y) = X^3Y + Y^3 + X$

$$S_F^X = \{(x,y)\in\mathbb{C}^2 \mid F(x,y)=0,\ x^3+3y^2\neq 0,\ 1\neq 0\}$$
$$S_F^Y = \{(x,y)\in\mathbb{C}^2 \mid F(x,y)=0,\ 3x^2+1\neq 0,\ y\neq 0\}$$
$$S_F^X \cup S_F^Y = \{(x,y)\in\mathbb{C}^2 \mid F(x,y)=0\} - \{(0,0)\}$$

$$\begin{array}{ccc} S_F^X & & S_F \\ \downarrow & \Rightarrow & \downarrow \\ \mathbb{CP}^1 - \{\text{finite pts}\} & & \mathbb{CP}^1 \end{array}$$

Rmk: 1. S_F is generally not the corresponding proj variety ? projective Don't understand it now

2. If the corresponding proj variety is RS (no singularity) Riemann Surface
$\Rightarrow$ it's the required one.

Def (defined over $K \subseteq \mathbb{C}$)

We shall say that a Riemann surface S *is defined over a field* $K \subset \mathbb{C}$ (or that K is a *field of definition of* S) if $S \simeq S_F$ for some irreducible polynomial $F(X,Y) = \sum a_{ij}X^iY^j$ with coefficients $a_{ij} \in K$.

$$S \simeq S_F \qquad F(X,Y) = \sum a_{ij} X^i Y^j \quad a_{ij} \in K.$$

E.g Elliptic curve over $\mathbb{Q}$

(1) S_{F_1}: $F_1(X,Y) = Y^2 - [X^3 - 1]$

(2) S_{F_2}: $F_2(X,Y) = Y^2 - [X^3 - \pi^3]$

Reason: $\downarrow$ (x,y)

S_{F_1}: $F_1(W,Z) = Z^2 - [W^3 - 1]$ $\downarrow$

$$\left(\frac{y}{\pi\sqrt{\pi}}\right)^2 - \left[\left(\frac{x}{\pi}\right)^3 - 1\right] = 0 \quad \text{well-defined} \left(\frac{x}{\pi}, \frac{y}{\pi\sqrt{\pi}}\right)$$

3. Claim of Belyi's theorem

Philosophy: functions reflect properties of space.
- topology
- geometry
- arithmetic

Theorem 3.1 (Belyi's Theorem) *Let S be a compact Riemann surface. The following statements are equivalent:*

(a) *S is defined over $\overline{\mathbb{Q}}$.*

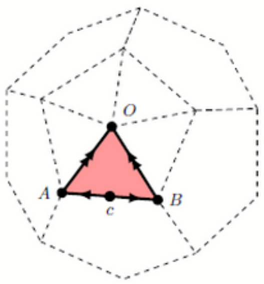
(b) *S admits a morphism $f : S \longrightarrow \mathbb{P}^1$ with $\underline{\text{at most}}$ three branching values.*
Rmk

defined over $\overline{\mathbb{Q}}$ $\Leftrightarrow$ admits a Belyi fct.

Rmk $n := \#\mathrm{Branch}(f)$
- when $n = 0, 1, 2$, $S \cong \mathbb{P}^1$;
- when $n = 3$, we can assume $\mathrm{Branch}(f) = \{\infty, 0, 1\}$

Eg. of (b).

1) $\mathbb{P}\mathbb{C}^1 \xrightarrow{\pi} \mathbb{P}\mathbb{C}^1/\Gamma \cong \mathbb{P}\mathbb{C}^1$ (Of course $\mathbb{P}\mathbb{C}^1$ is defined over $\overline{\mathbb{Q}}$)

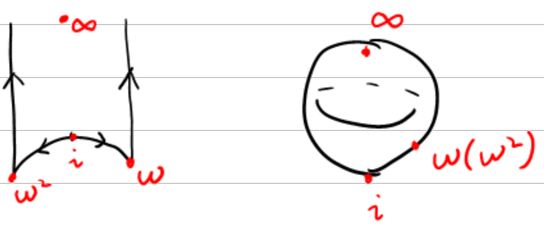


$$\begin{array}{cccc}
\mathbb{P}\mathbb{C}^1 & A, B, \cdots (12) & c, \cdots (20) & O, \cdots (30) \\
\pi \Big\downarrow 60 & \Big\downarrow 5 & \Big\downarrow 3 & \Big\downarrow 2 \\
\mathbb{P}\mathbb{C}^1/\Gamma_{(2,3,5)} & 0 & 1 & \infty
\end{array}$$

在 $0, 1, \infty$ 处分歧, π is a Belyi fct

图 1.2 例: 正十二面体

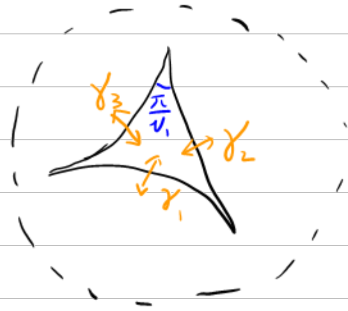
2) $\mathcal{H}^*/\Gamma(N) \xrightarrow{\pi} \mathcal{H}^*/SL_2(\mathbb{Z}) \xrightarrow[\sim]{j} \mathbb{P}\mathbb{C}^1$



The ramification points here are called elliptive points.
"Why modular form / modular space is an arithmetic object"

3) $\mathbb{D}/K \longrightarrow \mathbb{D}/\Gamma$

$\underbrace{\mathbb{D}/K}_{}$ $\downarrow$ to make $\mathbb{D}/K$ cpt



$\Gamma_1 := \langle \gamma_1\gamma_2, \gamma_2\gamma_3, \gamma_3\gamma_1 \rangle$

4. a one-side proof: (a) $\Rightarrow$ (b)

(1) an example

e.g. for S_{F_λ} $\quad F_\lambda$: $Y^2 = X(X-1)(X-\lambda)$ $\quad \lambda \in \mathbb{Q} \cap (0,1)$

① F_λ is defined over $\overline{\mathbb{Q}}$

② x: ramified at $\infty, 0, 1, \lambda$.

③ adjustment: $P_\lambda \circ x$ ramified at 3 points, where

$\lambda = \frac{m}{m+n}$ $\qquad P_\lambda(x) = \dfrac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n$

$$\begin{array}{ccccccc}
S_{F_\lambda} & & & & & & \\
\downarrow x & \Downarrow & \Downarrow & \Downarrow & \Downarrow & & \\
\mathbb{P}^1 & 0 & 1 & \lambda & \infty & & a \\
\downarrow P_\lambda & \searrow & \swarrow & \downarrow & \downarrow & & \Downarrow ? \\
\mathbb{P}^1 & 0 & & 1 & \infty & & P_\lambda(a)
\end{array}$$

$0 = P_\lambda'(a) = \dfrac{(m+n)^{m+n}}{m^m n^n} [ma + n(1-a)] a^{m-1} (1-a)^{n-1} \Rightarrow a = 0, 1, \lambda$

Thm. (Belyi's Theorem) Suppose S is a cpt RS, then TFAE:

(a) S is defined over $\overline{\mathbb{Q}}$.

(b0) $\exists f: S \to \mathbb{P}^1$ with $\mathrm{Branch}(f) = \{\infty, 0, 1\}$.

(b1) $\exists f: S \to \mathbb{P}^1$ with $\# \mathrm{Branch}(f) \leq 3$

(b2) $\exists f: S \to \mathbb{P}^1$ with $\mathrm{Branch}(f) \subseteq \mathbb{Q} \cup \{\infty\}$.

(b3) $\exists f: S \to \mathbb{P}^1$ with $\mathrm{Branch}(f) \subseteq \overline{\mathbb{Q}} \cup \{\infty\}$

Sketch

$$\begin{tikzcd}
 & (b0) \arrow[d, shift left] \\
 & (b1) \arrow[u, shift left, "Rmk"] \arrow[d, shift left] \\
(a) \arrow[ddr, "\text{Verify}", "(3)"'] & \\
 & (b2) \arrow[uu, shift left, "(2)(5)"] \arrow[d, shift left] \\
 & (b3) \arrow[u, shift left, "(4)"]
\end{tikzcd}$$

(2) : (b2) $\Rightarrow$ (b1)

Use induction.

[Suppose $f: S \to \mathbb{P}^1$ ramified at $\{\infty, 0, 1, \lambda_1, \cdots, \lambda_n\} \subset \mathbb{Q} \cup \{\infty\}$
need construct $g: S \to \mathbb{P}^1$ ramified at $\{\infty, 0, 1, \mu_1, \cdots, \mu_{n-1}\} \subset \mathbb{Q} \cup \{\infty\}$]

$$\begin{array}{llllll}
S & & & & & \\
\downarrow f & \Downarrow & \Downarrow & \Downarrow\ \Downarrow\ \Downarrow & & \\
\mathbb{P}^1 & \{\infty, 0, 1\} & \lambda_1 & \lambda_2, \cdots, \lambda_n & & \\
\downarrow T / \frac{1}{1-T} / \frac{1}{T}\ (\in \mathrm{Aut}(\mathbb{P}^1)) & \downarrow & \downarrow & \downarrow\ \downarrow\ \downarrow & & \\
\mathbb{P}^1 & \{\infty, 0, 1\} & \lambda_1' & \lambda_2', \cdots, \lambda_n' & & \lambda_1' \in \mathbb{Q} \cap (0,1) \\
\downarrow P_{\lambda_1'} & \downarrow\ \downarrow\ \swarrow & \swarrow & \downarrow\ \downarrow\ \downarrow & & \\
\mathbb{P}^1 & \infty\ \ 0\ \ 1 & & P_{\lambda_1'}(\lambda_2') \cdots P_{\lambda_1'}(\lambda_n') & &
\end{array}$$

(g = composite $S \to \mathbb{P}^1$ of the three vertical maps)

Eg. of (2) $F: y^2 = x(x-1)(x+1)(x-\frac{5}{3})$

$$\begin{array}{llllll}
S_F & & & & & \\
\downarrow x & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow \\
\mathbb{P}^1 & \infty & 0 & 1 & \frac{5}{3} & -1 \\
\downarrow \frac{1}{T} & \searrow & \swarrow & \downarrow & \downarrow & \downarrow \\
\mathbb{P}^1 & \infty & 0 & 1 & \frac{3}{5} & -1 \\
\downarrow P_{\frac{3}{5}} & \downarrow & \downarrow & \swarrow & \swarrow & \downarrow \\
\mathbb{P}^1 & \infty & 0 & 1 & & -\frac{5^5}{3^3} \\
\downarrow \frac{1}{1-T} & & & & & \downarrow \\
\mathbb{P}^1 & \infty & 0 & 1 & & \frac{27}{3152} \\
\downarrow P_{\frac{27}{3152}} & \downarrow & \downarrow & \swarrow & & \swarrow \\
\mathbb{P}^1 & \infty & 0 & 1 & &
\end{array}$$

$\lambda = \frac{3}{5} = \frac{3}{3+2}$ $\quad m=3 \quad n=2$

$P_{\frac{3}{5}}(T) = \frac{5^5}{3^3 2^2} T^3 (1-T)^2$

$P_{\frac{27}{3152}}(T) = \frac{3152^{3152}}{27^{27} 3125^{3125}} T^{27} (1-T)^{3125}$

$f(x,y) = P_{\frac{27}{3152}}\left(\frac{1}{1 - P_{\frac{3}{5}}(\frac{1}{x})}\right)$

(3): (a) $\Rightarrow$ (b3)

$$\left[\begin{array}{l} S \cong S_F \qquad F(X,Y) = \sum a_{ij} X^i Y^j \in \overline{\mathbb{Q}}[X,Y] \text{ irr} \\ \text{Verify } \; x : S_F \longrightarrow \mathbb{P}^1 \text{ only ramified in } \overline{\mathbb{Q}} \cup \{\infty\}. \end{array}\right]$$

$x|_{S_F^X} : S_F^X \longrightarrow \mathbb{C}$ is unramified, so

the possible ramified points:

① ∞

② $x : p_0(X) = 0$ $\qquad F(X,Y) = p_0(X)Y^n + \cdots p_n(X)$

③ $x \quad (\{(x,y) \mid F(x,y) = F_Y(x,y) = 0\})$

(4): (b3) $\Rightarrow$ (b2)

$$\left[\begin{array}{l} \text{Suppose } f : S \to \mathbb{P}^1 \text{ ramified at } \{\infty, 0, 1, \lambda_1, \cdots, \lambda_n\} \subset \overline{\mathbb{Q}} \cup \{\infty\} \\ \text{need construct } g : S \to \mathbb{P}^1 \text{ ramified at } \{\infty, 0, 1, \mu_1, \cdots, \mu_n\} \subset \mathbb{Q} \cup \{\infty\} \end{array}\right]$$

Denote $\quad B_1(f) = \mathrm{Branch}(f) \setminus \mathbb{Q} \cup \{\infty\} := \{\lambda_1, \cdots \lambda_m\}$

$B_2(f) = \mathrm{Branch}(f) \cap (\mathbb{Q} \cup \{\infty\})$

Let $m_f(T) \in \mathbb{Q}[T]$ be the minimal polynomial of $B_1(f)$

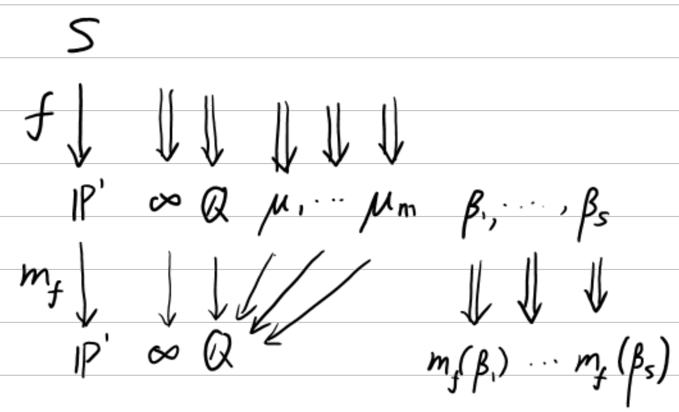
$$\left[\begin{array}{l} \text{Induction on } \deg m_f(T): \\ \qquad \text{construct } g : S \to \mathbb{P}^1 \text{ s.t. } \deg m_g(T) < \deg m_f(T) \\ \qquad\qquad\qquad\qquad \text{or} \rightarrow B_1(g) = \emptyset \\ \qquad\qquad\qquad\qquad \text{By convention } m_g(T) = 0 \end{array}\right]$$

Claim: $\quad \deg m_{m_f \circ f} < \deg m_f$

Let $\Phi := \{\beta_1, \cdots \beta_s\}$ be the roots of m_f'

then $B_1(m_f \circ f) = \{m_f(\beta_1), \cdots, m_f(\beta_s)\} \setminus \mathbb{Q}$

Notation: Let $p(T) \in \mathbb{Q}[T]$ be the minimal polynomial of $\Phi \setminus \mathbb{Q}$



We have

$$\deg m_{m_f \circ f} \leq \deg p \overset{\text{def of min poly}}{\leq} \deg m_f' < \deg m_f$$

$$\left\{\begin{array}{l} \deg \min(m_f(\beta_i)) \leq \deg \min(\beta_i) \\ \beta_i = \sigma(\beta_j) \quad \Rightarrow m_f(\beta_i) = \sigma(m_f(\beta_j)) \end{array}\right.$$

E.g. of (4) $\qquad S_F: \; y^2 = x(x-\sqrt{2})(x-\sqrt[3]{11})$

$$\begin{array}{ccccccccc}
S_F & & & & & & & & \\
\downarrow x & & \Downarrow & \Downarrow & \Downarrow & \Downarrow & & & \\
\mathbb{P}^1 & & \infty & 0 & \sqrt{2} & \sqrt[3]{11} & \beta_3 & \beta_4 & \\
\downarrow (T^2-2)(T^3-11) & & \downarrow & \downarrow & \downarrow & \swarrow & \Downarrow & \Downarrow & \\
\mathbb{P}^1 & & \infty & 6 & 0 & & m_x(\beta_3) & m_x(\beta_4) & \frac{2733}{64} \\
\downarrow & & \downarrow & \downarrow & \downarrow & & \searrow & \swarrow & \downarrow \\
\mathbb{P}^1 & & \infty & 373248 & 388494 & & 0 & & \frac{42257943}{128}
\end{array}$$

$B_1(x) = \{\sqrt{2}, \sqrt[3]{11}\}$

$m_x(T) = (T^2-2)(T^3-11)$

$m_x'(T) = T(T-2)(2T^2+7T+14)$

$\Phi = \{\beta_1, \beta_2, \beta_3, \beta_4\}$

$= \{0, 2, \frac{1}{4}(-7 \pm 3\sqrt{7}i)\}$

$f := m_x \circ x$

$B_1(f) = \{\beta_3, \beta_4\}$

$m_f(T) = 32T^2 - 2733T + 388494$

$m_f'(T) = 64T - 2733$

$\Phi' = \{\frac{2733}{64}\}$

(5): (b2) $\Rightarrow$ (b1)

[Suppose $f: S \to \mathbb{P}^1$ ramified at $\{\infty, 0, 1, \lambda_1, \cdots, \lambda_n\} \subset \mathbb{Q} \cup \{\infty\}$

need construct $g: S \to \mathbb{P}^1$ ramified at $\{\infty, 0, 1\}$]

[Idea: find a "good ramified fct" $G(T) = \prod_{i=1}^{n} (x-\lambda_i)^{a_i}$ $\quad a_i \in \mathbb{N} - \{0\}$

$\uparrow$ Ram$(G) \subseteq \{\lambda_1, \cdots \lambda_n\}$]

① Suppose Branch$(f) \subseteq \mathbb{Z} \cup \{\infty\}$

② Let $\quad y_i := \dfrac{1}{\prod_{j \neq i} (\lambda_i - \lambda_j)} \qquad V := \prod_{j>i} (\lambda_j - \lambda_i) \qquad a_i := V y_i$

③ Verified: i) $a_i \in \mathbb{N} - \{0\} \quad \Rightarrow \quad G(\lambda_i) = 0$ or ∞

ii) $\sum a_i = 0 \quad \Rightarrow \quad G(\infty) = 1$

$$a_n = \prod_{n>j>i} (\lambda_j - \lambda_i) = \begin{vmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-2} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & \lambda_{n-1} & \cdots & \lambda_1^{n-2} & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{vmatrix} \qquad a_{n-1} = \begin{vmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-2} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & \lambda_{n-2} & \cdots & \lambda_{n-2}^{n-2} & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ 1 & \lambda_n & \cdots & \lambda_n & 0 \end{vmatrix}$$

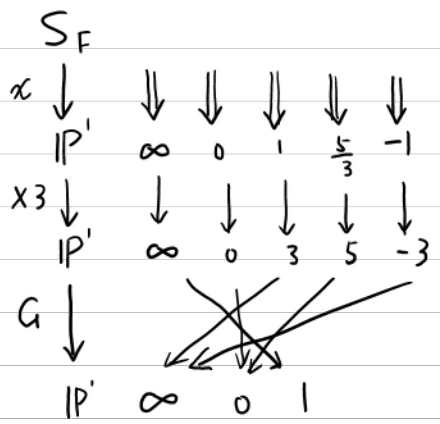
$$\Rightarrow \sum a_i = \begin{vmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-2} & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{n-2} & 1 \end{vmatrix} = 0$$

iii) Ram$(G) \subseteq \{\lambda_1, \cdots \lambda_n\}$

$$\frac{G'(T)}{G(T)} = \left(\log G(T)\right)' = \sum_{i=1}^{n} \frac{a_i}{x-\lambda_i} = \sum_{i=1}^{n} \frac{V y_i}{x-\lambda_i} = \frac{V}{\prod_{i=1}^{n}(x-\lambda_i)}$$

$$\Rightarrow G'(T) = V \prod_{i=1}^{n} (x-\lambda_i)^{a_i - 1}$$

Eg. of (5) $F: y^2 = x(x-1)(x+1)\left(x-\frac{5}{3}\right)$



$\{\lambda_1, \dots \lambda_4, \infty\} = \{-3, 0, 3, 5, \infty\}$

$V = \prod_{j>i} (\lambda_j - \lambda_i) = 4320$

$\{y_1, y_2, y_3, y_4\} = \{-\frac{1}{144}, \frac{1}{45}, -\frac{1}{36}, \frac{1}{80}\}$

$\{a_1, a_2, a_3, a_4\} = \{-30, 96, -120, 54\}$

$$G(x) = \frac{x^{96}(x-5)^{54}}{(x+3)^{30}(x-3)^{120}}$$

$$G'(x) = 4320 \frac{x^{95}(x-5)^{53}}{(x+3)^{29}(x-3)^{119}}$$