

# Publications mathématiques de Besançon

## ALGÈBRE ET THÉORIE DES NOMBRES

Kentaro Mitsui

### Models of torsors under elliptic curves

2017, p. 79-108.

<[http://pmb.cedram.org/item?id=PMB\\_2017\\_\\_\\_\\_79\\_0](http://pmb.cedram.org/item?id=PMB_2017____79_0)>

© Presses universitaires de Franche-Comté, 2017, tous droits réservés.

L'accès aux articles de la revue « Publications mathématiques de Besançon » (<http://pmb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://pmb.cedram.org/legal/>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

*Publication éditée par le laboratoire de mathématiques  
de Besançon, UMR 6623 CNRS/UFC*

**cedram**

*Article mis en ligne dans le cadre du  
Centre de diffusion des revues académiques de mathématiques  
<http://www.cedram.org/>*

# MODELS OF TORSORS UNDER ELLIPTIC CURVES

by

Kentaro Mitsui

---

*Abstract.* — We study the special fibers of the minimal proper regular models of proper smooth geometrically integral curves of genus one over a complete discrete valuation field. We classify the configurations of their irreducible components when the residue field is perfect. As an application, we show the existence of separable closed points of small degree on the original curves when the residue field is finite. Finally, we extend this result under mild assumptions on the residue field and the degenerations of their Jacobians.

*Résumé.* — Nous étudions les fibres spéciales des modèles propres réguliers minimaux de courbes propres lisses géométriquement intègres de genre un sur un corps de valuation discrète complet. Nous classifions les configurations de leurs composantes irréductibles quand le corps résiduel est parfait. En guise d'application, nous montrons l'existence de points fermés séparables de petit degré des courbes originales quand le corps résiduel est fini. Finalement, nous étendons ce résultat sous des hypothèses faibles sur le corps résiduel et la dégénérescence de la jacobienne.

## 1. Introduction

Let  $K$  be a complete discrete valuation field. We denote the valuation ring of  $K$  by  $O_K$ , and the residue field of  $O_K$  by  $\bar{K}$ . Set  $C := \text{Spec } O_K$ , and  $\bar{C} := \text{Spec } \bar{K}$ . Let  $E_K$  be a  $K$ -elliptic curve. Choose  $\tau \in H^1(K, E_K)$ . We denote the  $K$ -torsor under  $E_K$  corresponding to  $\tau$  by  $X_K$ . Then  $X_K$  is a proper smooth geometrically integral  $K$ -curve. For a closed point  $x$  on  $X_K$ , we denote the residue field of  $X_K$  at  $x$  by  $k(x)$ . If  $k(x)/K$  is separable, then the closed point  $x$  is said to be *separable*. Take a minimal proper regular  $C$ -model  $X$  of  $X_K$ . Set  $\bar{X} := X \times_C \bar{C}$ . This paper is divided into two parts. We study the geometry of  $\bar{X}$  in the first part (§3) and separable closed points on  $X_K$  in the last part (§4).

In the first part, we classify the configurations of the irreducible components of  $\bar{X}$  when  $\bar{K}$  is perfect (see §3.8 for the dual graphs). The classification generalizes the case where

---

**2010 Mathematics Subject Classification.** — 11G20, 14G05, 11G07.

**Key words and phrases.** — elliptic curves, torsors, curves of genus one, models, degenerations, dual graphs, rational points.

$\bar{K}$  is algebraically closed, or  $X_K = E_K$  [12, §10.2.1]. If  $\bar{K}$  is algebraically closed, then the intersection matrix of the irreducible components of  $\bar{X}$  may be described by means of a Dynkin diagram. We obtain the dual graphs of the special fibers of proper regular  $C$ -models of  $X_K$  by studying birational morphisms between these models. Our classification is based on the classification of finite quotients of these dual graphs.

In the last part, we show the existence of a separable closed point on  $X_K$  of small degree. We denote the degree of a finite field extension  $l/k$  by  $[l : k]$ . The minimal positive integer among all degrees of zero-cycles on  $X_K$  is called the *index of  $X_K$* , and denoted by  $I(X_K)$ . Note that the equality

$$I(X_K) = \gcd\{[k(x) : K] \mid x \text{ is a closed point on } X_K\}$$

holds. In particular, for any closed point  $x$  on  $X_K$ , the relation  $I(X_K) \mid [k(x) : K]$  holds.

**Theorem 1.1.** — *We use the same notation as above. Then there exists a separable closed point  $x$  on  $X_K$  such that  $[k(x) : K] = I(X_K)$ .*

In the proof of the above theorem, we use the classification in the first part when  $\bar{K}$  is finite, i.e.,  $K$  is a local field (Remark 4.2). The order of  $\bar{X}$  in the abelian group  $H^1(K, E_K)$  is called the *period of  $X_K$* , and denoted by  $P(\bar{X})$ . We denote the Brauer group of a field  $k$  by  $\text{Br}(k)$ . If  $\text{Br}(K) = 0$ , or  $\bar{K}$  is finite, then  $P(\bar{X}) = I(X_K)$  ([11, §1, Thms. 1 and 3] and [15, p. 283, Cor.]). As a corollary, we obtain the following.

**Corollary 1.2.** — *We use the same notation as above. Assume that  $\text{Br}(K) = 0$ , or  $\bar{K}$  is finite. Then there exists a separable closed point  $x$  on  $X_K$  such that  $[k(x) : K] = P(\bar{X})$ .*

**Remark 1.3.** — Assume that  $\bar{K}$  is perfect. Then  $\text{Br}(K) = 0$  if and only if  $\text{Br}(\bar{K}) = 0$ , and there does not exist a non-trivial cyclic extension of  $\bar{K}$  [16, XII.3, Thm. 2].

A *global field* is a finite extension of  $\mathbb{Q}$  or  $k(t)$  where  $k$  is a finite field. When  $K$  is replaced by a global field, a statement analogous to the above corollary does not hold (Example 4.3). The conclusion of the above corollary does not hold in general when  $\bar{K}$  is not finite (Example 4.17). However, we prove Theorem 1.6 below in the case where  $E_K$  has good reduction or toric reduction (Definition 4.1).

**Definition 1.4.** — A field  $k$  is said to be *WC-trivial for elliptic curves* if  $H^1(l, E_l) = 0$  for any finite separable field extension  $l/k$  and any  $l$ -elliptic curve  $E_l$ .

**Example 1.5.** — A field  $k$  is WC-trivial for elliptic curves in the following cases:

1.  $k$  is separably closed;
2.  $k$  is finite [9, Thm. 1];
3.  $k$  is pseudo-algebraically closed [4, 11.2.5], e.g.,  $k$  is an infinite algebraic field extension of a finite field.

**Theorem 1.6.** — *We use the same notation as above. Assume that  $\bar{K}$  is perfect and WC-trivial for elliptic curves, and that, for any finite field extension  $\bar{K}/\bar{K}$ , there does not exist a Galois extension of  $\bar{K}$  with Galois group  $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ . Suppose that  $E_K$  has good reduction or toric reduction. Then there exists a separable closed point  $x$  on  $X_K$  such that  $[k(x) : K] = P(\bar{X})$ .*

**Example 1.7.** — Assume that  $\bar{K}$  is an algebraic field extension of a finite field. Then the assumptions on  $\bar{K}$  in Theorem 1.6 are satisfied (Example 1.5). If  $\bar{K}$  is not algebraically closed, then  $\text{Br}(K) = 0$  (Remark 1.3).

## 2. Notation and Convention

We denote the cardinality of a finite set  $S$  by  $|S|$ , and the trivial group by  $1$ . For  $n \in \mathbb{Z}_{>0}$ , we denote the cyclic group of order  $n$  by  $Z_n$ , the dihedral group of order  $2n$  by  $D_{2n}$ , the alternative group of degree  $n$  by  $A_n$ , and the symmetric group of degree  $n$  by  $S_n$ .

Let  $k$  be a field. For a Galois extension  $l/k$ , we denote the Galois group of  $l/k$  by  $G_{l/k}$ . A  $k$ -curve is a separated  $k$ -scheme of finite type of pure dimension one. Let  $Y$  be a proper  $k$ -scheme. For a coherent  $\mathcal{O}_Y$ -module  $F$  on  $Y$ , the *Euler–Poincaré characteristic* of  $F$  is defined as

$$\sum_{i \geq 0} (-1)^i \dim_k H^i(Y, F),$$

and denoted by  $\chi_k(F)$ . Take the normalization  $Y^\circ$  of  $Y$ . Set  $H^0(Y) := H^0(Y, \mathcal{O}_Y)$ , and  $h^0(Y) := \dim_k H^0(Y)$ . Assume that  $Y$  is a  $k$ -curve. The *arithmetic genus* of  $Y$  is defined as  $1 - \chi_k(\mathcal{O}_Y)$ , and denoted by  $p_a(Y)$ . When  $Y$  is a smooth geometrically integral  $k$ -curve, the arithmetic genus of  $Y$  is called the *genus* of  $Y$ , and denoted by  $g(Y)$ . For a line bundle  $L$  on  $Y$ , the *degree* of  $L$  is defined as  $\chi_k(L) - \chi_k(\mathcal{O}_Y)$ , and denoted by  $\deg_k L$  [12, 7.3.29].

Let  $Z$  be a scheme. We denote the reduction of  $Z$  by  $Z_{\text{red}}$ , the regular locus of  $Z$  by  $Z_{\text{reg}}$ , and the non-regular locus of  $Z$  by  $Z_{\text{sing}}$ . Let  $Y$  be a  $Z$ -scheme with structure morphism  $g: Y \rightarrow Z$ . We denote the group of  $Z$ -automorphisms of  $Y$  by  $\text{Aut}(Y/Z)$ . For a  $Z$ -scheme  $S = \text{Spec } k$ , we set  $Y(k) := \text{Hom}_Z(S, Y)$ . We denote the union of images of  $Y(k)$  by the same notation. Let  $Z'$  be a closed subscheme of  $Z$  with closed immersion  $h: Z' \rightarrow Z$ . We denote the closed subscheme  $Z' \times_Z Y$  of  $Y$  given by the base change of  $h$  via  $g$  by  $g^{-1}(Z')$ .

We use the notation  $K, \mathcal{O}_K, \bar{K}, C,$  and  $\bar{C}$  introduced in §1. Set  $C_K := \text{Spec } K$ .

## 3. Classification of Special Fibers

**3.1. Special Fibers.** — Let  $X_K$  be a proper regular  $K$ -curve. Take a proper regular  $C$ -model  $f_X: X \rightarrow C$  of  $X_K$ . Set  $\bar{X} := f_X^{-1}(\bar{C})$ . Then we have the canonical isomorphisms  $X_K = X \times_C C_K$  and  $\bar{X} = X \times_C \bar{C}$ , and the diagram of schemes and morphisms with Cartesian squares

$$\begin{array}{ccccc} X_K & \xrightarrow{X_K} & X & \xrightarrow{\bar{X}} & \bar{X} \\ \left\| \begin{array}{c} f_{X_K} \\ \text{open} \end{array} \right. & & \left\| \begin{array}{c} f_X \\ \text{open} \end{array} \right. & & \left\| \begin{array}{c} f_{\bar{X}} \\ \text{closed} \end{array} \right. \\ C_K & \xrightarrow{C_K} & C & \xrightarrow{\bar{C}} & \bar{C} \end{array}$$

where the upper horizontal arrows are the first projections, the left and right vertical arrows are the second projections, and the left and right lower horizontal arrows are the canonical open and closed immersions, respectively. We may regard  $\bar{X}$  as a divisor on  $X$ .

**Definition 3.1.** — A divisor  $D$  on  $X$  is said to be *vertical* if the support of  $D$  is contained in that of  $\bar{X}$ . We denote the set of vertical prime divisors on  $X$  by  $P(X)$ . Let  $D_1$  be a divisor on  $X$ , and  $D_2$  be a vertical divisor on  $X$ . We denote the *intersection number* of  $D_1$  and  $D_2$

by  $D_1 \cdot D_2$  [12, 9.1.12]. Set  $P^{(2)}(X) := \{Q \in P(X) \mid |Q| = 2\}$ . Take  $a = \{ \nu_1, \nu_2 \} \in P^{(2)}(X)$ . We denote the closed subscheme  $(\nu_1 \times_X \nu_2)_{\text{red}}$  of  $X$  by  $\bar{a}$ . For  $s \in \bar{a}$ , we define the *intersection number of  $a$  at  $s$*  by

$$i(a, s) := \dim_{\bar{K}} O_{X,s} / (O_{X,s}(-\nu_1) + O_{X,s}(-\nu_2)).$$

**Remark 3.2.** — If  $0 < D_2 \leq \bar{X}$ , then  $D_1 \cdot D_2 = \deg_{\bar{K}} O_X(D_1) / D_2$  [12, 9.1.12(d)]. If  $D_2 \in P(X)$ , then  $D_1 \cdot D_2 = \deg_{\bar{K}} O_X(D_1)$ , where  $\nu : D_2 \rightarrow X$  is the composite of the normalization  $D_2 \rightarrow D_2$  of  $D_2$  and the canonical closed immersion  $D_2 \rightarrow X$  [12, 9.1.14].

**Remark 3.3.** — For any  $a = \{ \nu_1, \nu_2 \} \in P^{(2)}(X)$ , the equality  $\nu_1 \cdot \nu_2 = \sum_{s \in \bar{a}} i(a, s)$  holds [12, 9.1.1 and 9.1.12(a)].

**Definition 3.4.** — We denote the open subscheme  $(\bar{X}_{\text{red}})_{\text{reg}}$  of  $\bar{X}_{\text{red}}$  by  $R(X)$ , and the closed subscheme  $(\bar{X}_{\text{red}})_{\text{sing}}$  of  $\bar{X}$  equipped with the reduced structure by  $S(X)$ . We write  $\bar{X} = \sum_{P(X)} n(\nu)$ , where  $n(\nu) \in \mathbb{Z}_{>0}$ . For  $\nu \in P(X)$ , the integer  $n(\nu)$  is called the *multiplicity of  $\nu$  in  $\bar{X}$* . We set  $m(\bar{X}) := \gcd\{n(\nu) \mid \nu \in P(X)\}$ . The integer  $m(\bar{X})$  is called the *multiplicity of  $\bar{X}$* . For  $\nu \in P(X)$ , we set  $m(\nu) := n(\nu) / m(\bar{X})$ .

**Remark 3.5.** — Since  $\bar{X}_{\text{red}}$  is a proper  $\bar{K}$ -curve, the set  $S(X)$  is finite.

Set  $P := P(X)$ ,  $P^{(2)} := P^{(2)}(X)$ ,  $S := S(X)$ , and  $m := m(\bar{X})$ .

**3.2. Dual Graphs.** — We introduce a graph that describes the multiplicities and intersection numbers of the elements of  $P$ . We give examples in §3.3.

**Definition 3.6.** — The special fiber  $\bar{X}$  is said to be *of integral type* if the following condition is satisfied:

0. any  $\nu \in P$  is geometrically integral over  $\bar{K}$ .

We abbreviate *strongly normal crossing* to *snc*. The special fiber  $\bar{X}$  is said to be *of fundamental type* if  $\bar{X}$  is of integral type and satisfies the following conditions:

1. any  $\nu \in P$  is regular;
2.  $\bar{X}$  is a snc divisor;
3.  $S = \bar{X}(\bar{K})$ .

**Remark 3.7.** — Assume that  $\bar{K}$  is algebraically closed. Then  $\bar{X}$  is of integral type, and Condition 1 is satisfied. We set

$$L_1(X) := \sum_{\nu \in P} \nu_{\text{sing}}, \quad \text{and} \quad L_2(X) := \{x \in \bar{X}(\bar{K}) \mid \bar{X} \text{ is not snc at } x\}.$$

Then  $L_i(X)$  is a finite set for any  $i \in \{1, 2\}$ , and the following statement holds:  $\bar{X}$  is of fundamental type if and only if  $L_i(X) = \emptyset$  for any  $i \in \{1, 2\}$ . Set  $X_0 := X$ . For  $i \geq 0$ , we successively take the blowing-up  $X_{i+1} \rightarrow X_i$  of  $X_i$  along  $L_1(X_i)$  if  $L_1(X_i) \neq \emptyset$ . Then there exists  $i_1 \geq 0$  such that  $L_1(X_{i_1}) = \emptyset$  (see the proof of [12, 9.2.32]). For  $i \geq i_1$ , we successively take the blowing-up  $X_{i+1} \rightarrow X_i$  of  $X_i$  along  $L_2(X_i)$  if  $L_2(X_i) \neq \emptyset$ . Then there exists  $i_2 \geq i_1$  such that  $L_2(X_{i_2}) = \emptyset$  (see the proof of [12, 9.2.26]). Moreover, the equality

$L_1(X_i) = 0$  holds for any  $i \in \{i_0, \dots, i_1, \dots, i_2\}$  [12, 9.2.31]. Thus, the special fiber of  $X_{i_2}$  is of fundamental type.

**Definition 3.8.** — Assume that  $\bar{X}$  is of integral type. We define the *dual graph*  $D$  of  $\bar{X}/m$  as a graph consisting of vertices with multiplicities and edges, and satisfying Condition ( ) below. We denote the set of vertices of  $D$  by  $V$ , and the set of edges of  $D$  by  $E$ . For  $v \in V$ , we denote the multiplicity of  $v$  by  $m(v)$ . For  $F \subseteq E$ , we denote the set of vertices connected to an element of  $F$  by  $V(F)$ . For  $e \in E$ , we set  $V(e) := V(\{e\})$ . For  $W \subseteq V$ , we denote the set of edges connected to an element of  $W$  by  $E(W)$ . For  $v \in V$ , we set  $E(v) := E(\{v\})$ .

*Condition ( ):* there exists a bijection  $v(\bullet) : P \rightarrow V$  such that the following statements hold. For  $a \in P^{(2)}$ , we set  $[a] := \{e \in E \mid V(e) = v(a)\}$ .

1. For any  $a \in P$ , the equality  $m(v(a)) = m(a)$  holds.
2. The equality  $E = \bigcup_{a \in P^{(2)}} [a]$  holds, i.e., the graph  $D$  has no loop.
3. For any  $a = \{a_1, a_2\} \in P^{(2)}$ , the equality  $m(a_1) \cdot m(a_2) = |[a]|$  holds.

*Vertices.* We denote  $v \in V$  by a circle, and write  $m(v)$  at the center of the circle.

*Edges.* We denote  $e \in E$  by a line segment.

We denote the automorphism group of  $D$  by  $\text{Aut } D$ . Assume that  $\bar{X}$  is of fundamental type. We define a bijection  $e(\bullet) : S \rightarrow E$  in the following way. Since  $|[a]| = m(a)$  for any  $a \in P^{(2)}$ , we may choose a bijection  $s \mapsto [a]$  for each  $a \in P^{(2)}$ . Since  $S = \bigcup_{a \in P^{(2)}} [a]$ , the union of these bijections for all elements of  $P^{(2)}$  gives a bijection  $e(\bullet) : S \rightarrow E$ .

**Remark 3.9.** — For any  $a \in P^{(2)}$ , the inequality  $|[a]| \leq m(a)$  holds (Statement 3 and Remark 3.3). Moreover, the equality  $|[a]| = m(a)$  holds if and only if  $i(a, s) = 1$  for any  $s \in [a]$  (see Definition 3.1 for  $i(a, s)$ ).

**3.3. Curves of Genus One and Kodaira Symbols.** — In this subsection, we suppose that  $\bar{K}$  is perfect,  $X_K$  is a proper smooth geometrically integral  $K$ -curve of genus one, and  $X$  is minimal. We denote the Jacobian of  $X_K$  by  $E_K$ . Take a minimal proper regular  $C$ -model  $E$  of  $E_K$ . This model is unique up to unique  $C$ -isomorphism [12, 9.3.14]. Set  $\bar{E} := E \times_C \bar{C}$ , and  $N := |P|$ .

We denote the (extended) Kodaira symbol of  $\bar{E}$  by  $T_E$  [12, 10.2.1]. When  $\bar{K}$  is algebraically closed, we denote the Kodaira symbol of  $\bar{X}$  by  $mT$ . Then each  $T_E$  and  $T$  is equal to  $I_n$  ( $n \geq 0$ ),  $I_n^*$  ( $n \geq 0$ ), II, II\*, III, III\*, IV, or IV\*. In general, the symbol  $T_E$  is equal to one of the above symbols,  $I_{n,2}$  ( $n \geq 1$ ),  $I_{n,2}^*$  ( $n \geq 0$ ),  $I_{0,3}$ , or  $IV_2$ .

When  $\bar{K}$  is algebraically closed, we define a symbol  $D$  to denote the dual graph  $D$  of  $\bar{X}/m$  in the following way (Table 1). If  $N = 1$ , then we set  $D := A_0$ . Otherwise, we define  $D$  by the type of the affine Dynkin diagram corresponding to the dual graph  $D$  (without the multiplicities):  $A_n$  ( $n \geq 1$ ),  $D_n$  ( $n \geq 4$ ), or  $E_n$  ( $n = 6, 7, \text{ or } 8$ ).


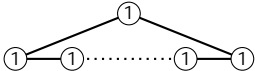
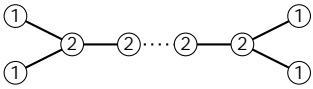
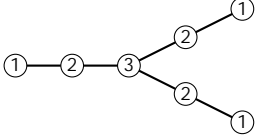
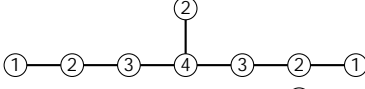
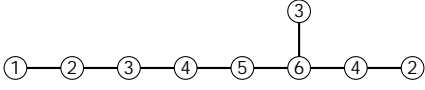
$D$	$D$	$N$	$\text{Aut } D$	$T$
$A_0$		1	1	$I_0, I_1, II$
$A_{n-1}$ ( $n \geq 2$ )		$n$	$D_{2n}$	$I_n$ III ( $n = 2$ ) IV ( $n = 3$ )
$D_{n-1}$ ( $n \geq 5$ )		$n$	$S_4$ ( $n = 5$ ) $D_8$ ( $n = 6$ )	$I_{n-5}$
$E_6$		7	$S_3$	IV
$E_7$		8	$Z_2$	III
$E_8$		9	1	II

Table 1. The dual graphs in the case where  $\bar{K}$  is algebraically closed (Definition 3.8).

**Remark 3.10.** — Assume that  $\bar{K}$  is algebraically closed. Then the following statements hold:

1. The equality  $T = T_E$  holds, and  $m$  is equal to the order of the element of the abelian group  $H^1(K, E_K)$  corresponding to  $X_K$  [13, 6.6].
2. If  $T = I_0$ , then  $P = \{ \}$ , and  $\bar{C}$  is a proper smooth  $\bar{C}$ -curve of genus one. Otherwise, for any  $P$ , the normalization of  $\bar{C}$  is  $\bar{C}$ -isomorphic to  $\mathbb{P}_{\bar{C}}^1$ .
3. An element  $P$  is not regular if and only if  $T = I_1$  or  $II$ . If these equivalent statements hold, then  $N = 1$ .
4. The special fiber  $\bar{X}$  is not of fundamental type if and only if  $T = I_1, II, III,$  or  $IV$ .
5. If  $P = \{ \}$ , then  $\dots = 0$ . Otherwise, the equality

$$1 \cdot 2 = \begin{cases} -2 & \text{if } 1 = 2, \\ 0, 1, \text{ or } 2 & \text{otherwise} \end{cases}$$

holds for any  $1 \in P$  and any  $2 \in P$ .

**3.4. Dual Graphs with Types and Degrees.** — We introduce a graph in the case where  $\bar{X}$  is not necessarily of integral type. In this graph, the vertices have two types (the first type and the second type), and the vertices and edges have degrees (Remark 3.14). We give examples in §3.8.

**Definition 3.11.** — Let  $z$  be a point on a locally Noetherian scheme  $Z$ . If the preimage of  $z$  under the normalization of  $Z$  consists of one point, then  $z$  is said to be *unibranch*.

**Definition 3.12.** — We define the *dual graph*  $D$  of  $\overline{X}/m$  (with types and degrees) as a graph consisting of two types of vertices with multiplicities and degrees and edges with degrees, and satisfying Condition ( ) below. We introduce the notation  $V, E, m(\bullet), V(\bullet),$  and  $E(\bullet)$  for  $D$  in the same way as in Definition 3.8. For  $v \in V$ , we denote the degree of  $v$  by  $d(v)$ . For  $e \in E$ , we denote the degree of  $e$  by  $d(e)$ . Set  $S_2 := \coprod_{a \in P^{(2)}} a$ .

*Condition ( ):* there exist bijections  $v(\bullet): P \rightarrow V$  and  $e(\bullet): S_2 \rightarrow E$  such that the following statements hold. For  $a \in P^{(2)}$ , we set  $[a] := \{e \in E \mid V(e) = v(a)\}$ .

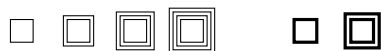
1. For any  $a \in P$ , the equalities  $m(v(a)) = m(a)$  and  $d(v(a)) = h^0(a)$  hold.
2. For any  $a \in P$ , the vertex  $v(a)$  is of the second type if and only if  $a$  has a unibranch singularity.
3. For any  $a \in P^{(2)}$  and any  $s \in a \subset S_2$ , the equality  $d(e(s)) = i(a, s)$  holds (see Definition 3.1 for  $i(a, s)$ ).
4. For any  $a \in P^{(2)}$ , the equality  $e([a]) = [a]$  holds.

*Vertices.* Take  $v \in V$ .

*Case 1:*  $v$  is of the first type. If  $d(v) = 4$ , then we denote  $v$  by a multi-circle whose number of circles is equal to  $d(v)$ . In the general case, we denote  $v$  by a thick circle, and specify the degree  $d(v)$ . Then we denote a vertex of  $D$  of the first type of degree  $2d(v)$  by a double thick circle. We write the multiplicity  $m(v)$  of  $v$  at the center of the circle.



*Case 2:*  $v$  is of the second type. We denote  $v$  by a multi-square in the same way as in Case 1, where we use squares instead of circles.



*Edges.* Take  $e \in E$ . If  $d(e) = 4$ , then we denote  $e$  by a multi-line segment whose number of line segments is equal to  $d(e)$ . In the general case, we denote  $e$  by a thick line segment, and specify the degree  $d(e)$ . Then we denote an edge of  $D$  with degree  $2d(e)$  by a double thick line segment.



**Remark 3.13.** — Statement 4 implies that  $E = \coprod_{a \in P^{(2)}} [a]$ , i.e., the graph  $D$  has no loop. Statements 3 and 4 imply that  $\sum_{e \in [a]} d(e) = 1 \cdot 2$  for any  $a = \{ \nu_1, \nu_2 \} \in P^{(2)}$  (Remark 3.3).

**Remark 3.14.** — If  $\overline{X}$  is of fundamental type, then all vertices are of the first type, all degrees are equal to one, and the graph (without types and degrees) coincides with that in Definition 3.8.



**3.5. Base Change.** — Choose an extension  $K/K$  between complete discrete valuation fields. We denote the valuation ring of  $K$  by  $O_K$ , and the residue field of  $O_K$  by  $\bar{K}$ . Set  $C_K := \text{Spec } K$ ,  $C := \text{Spec } O_K$ , and  $\bar{C} := \text{Spec } \bar{K}$ . We denote the canonical projection by  $\pi_C: C \rightarrow C$ , and the canonical homomorphism by  $\tau_C: \text{Aut}(C/C) \rightarrow \text{Aut}(\bar{C}/\bar{C})$ .

*Remark 3.15.* — Since  $O_K/O_K$  is an extension between complete discrete valuation rings, the morphism  $\pi_C$  is flat. Thus, the following statements are equivalent:

1.  $\pi_C$  is regular [7, 6.8.1 (iv)];
2. any fiber of  $\pi_C$  is geometrically regular [7, 6.7.6];
3. the canonical morphism  $\bar{\pi}_C: \bar{C} \rightarrow \bar{C}$  is an isomorphism, and both  $K/K$  and  $\bar{K}/\bar{K}$  are separable.

*Remark 3.16.* — If  $K/K$  is Galois (resp.  $\bar{K}/\bar{K}$  is Galois), then we obtain canonical isomorphisms  $\text{Aut}(C/C) = \text{Aut}(C_K/C_K) = G_{K/K}$  (resp.  $\text{Aut}(\bar{C}/\bar{C}) = G_{\bar{K}/\bar{K}}$ ).

*Example 3.17.* — The morphism  $\pi_C$  is regular (Remark 3.15), the field extension  $\bar{K}/\bar{K}$  is Galois (Remark 3.16), and the homomorphism  $\tau_C$  is surjective in the following cases:

- A.  $O_K$  is  $O_K$ -isomorphic to the completion of the strict Henselization of  $O_K$  [6, Cor. 5.6];
- B. the canonical morphism  $\bar{\pi}_C: \bar{C} \rightarrow \bar{C}$  is an isomorphism,  $K/K$  is a Galois extension, and  $\bar{K}/\bar{K}$  is a separable field extension.

In the following, we assume that  $\pi_C$  is regular (Remark 3.15).

*Lemma 3.18.* — Assume that  $K$  is finite over  $K$ . Then  $\pi_C$  is finite and étale.

*Proof.* — Since  $K$  is finite and separable over  $K$  (Remark 3.15), the finiteness of  $\pi_C$  follows from [14, §33, Lem. 1]. Since  $\pi_C$  is regular, the morphism  $\pi_C$  is étale (Remark 3.15).

Take the base change  $f_X: X \rightarrow C$  of  $f_X$  via  $\pi_C$ , and the base change  $f_{\bar{X}}: X \rightarrow X$  of  $\pi_C$  via  $f_X$ . Set  $X_K := X_K \times_{C_K} C_K$ , and  $\bar{X} := f_{\bar{X}}^{-1}(\bar{C})$ . Then we have the followings:

1. the canonical isomorphisms  $X_K = X \times_C C_K$  and  $\bar{X} = X \times_C \bar{C}$ , and the diagram of schemes and morphisms with Cartesian squares

$$\begin{array}{ccccc} X_K & \xrightarrow{\pi_{X_K}} & X & \xrightarrow{\pi_X} & \bar{X} \\ \left| \begin{array}{c} f_{X_K} \\ \pi_{C_K} \end{array} \right. & & \left| \begin{array}{c} f_X \\ \pi_C \end{array} \right. & & \left| \begin{array}{c} f_{\bar{X}} \\ \pi_{\bar{C}} \end{array} \right. \\ C_K & \xrightarrow{\pi_{C_K}} & C & \xrightarrow{\pi_C} & \bar{C} \end{array}$$

where the upper horizontal arrows are the first projections, the left and right vertical arrows are the second projections, and the left and right lower horizontal arrows are the canonical open and closed immersions, respectively;

2. for  $W = C$  and  $X$ , the canonical isomorphisms  $W_K = W \times_W W_K$  and  $\overline{W} = W \times_W \overline{W}$ , and the diagram of schemes and morphisms with Cartesian squares

$$\begin{array}{ccccc} W_K & \xrightarrow{w_K} & W & \xrightarrow{w} & \overline{W} \\ \downarrow w_K & & \downarrow w & & \downarrow \overline{w} \\ W_K & \xrightarrow{w_K} & W & \xrightarrow{w} & \overline{W} \end{array}$$

where the upper horizontal arrows are the first projections, and the left and right vertical arrows are the second projections.

We have the diagram of groups and homomorphisms with commutative squares

$$\begin{array}{ccccc} \text{Aut}(C_K/C_K) & \xrightarrow{r_C} & \text{Aut}(C/C) & \xrightarrow{r_C} & \text{Aut}(\overline{C}/\overline{C}) \\ \downarrow b_K & & \downarrow b & & \downarrow \overline{b} \\ \text{Aut}(X_K/X_K) & \xrightarrow{r_X} & \text{Aut}(X/X) & \xrightarrow{r_X} & \text{Aut}(\overline{X}/\overline{X}) \end{array}$$

where the left horizontal arrows, the right horizontal arrows, and the vertical arrows are induced by the base changes via  $c_K$ ,  $\overline{c}$ , and  $f_X$ , respectively.

**Lemma 3.19.** — *The  $C$ -scheme  $X$  is a proper regular  $C$ -scheme.*

*Proof.* — Since  $X$  is proper over  $C$ , the scheme  $X$  is proper over  $C$ . Since  $C$  is regular over  $C$ , and  $X$  is regular, the scheme  $X$  is regular [7, 6.8.3 (iii) and 6.5.2 (ii)].

Set  $P := P(X)$ , and  $S := S(X)$ . We use the following fact [7, 4.6.4].

**Lemma 3.20.** — *Let  $k$  be a field,  $k$  be a separable field extension of  $k$ , and  $Z$  be a reduced  $k$ -scheme. Then the base change of  $Z$  via  $k/k$  is reduced.*

**Lemma 3.21.** — *Let  $k$  be a field,  $k$  be a separable field extension of  $k$ , and  $Z$  be a  $k$ -scheme locally of finite type with structure morphism  $f_Z: Z \rightarrow \text{Spec } k$ . The field extension  $k/k$  induces a morphism  $k: \text{Spec } k \rightarrow \text{Spec } k$ . Take the base change  $z: Z \rightarrow Z$  of  $k$  via  $f_Z$ . Then there exists a  $Z$ -isomorphism  $z^{-1}(Z_{\text{sing}}) = Z_{\text{sing}}$ .*

*Proof.* — Since  $z^{-1}(Z_{\text{sing}})$  is reduced (Lemma 3.20), we have only to show the equality  $z^{-1}(Z_{\text{sing}}) = Z_{\text{sing}}$  for the underlying sets. Thus, the lemma follows from [7, 6.7.4].

**Lemma 3.22.** — *For any  $P$ , there exists an  $X$ -isomorphism  $z^{-1}(P_{\text{sing}}) = (z^{-1}(P))_{\text{sing}}$ . Moreover, there exists an  $X$ -isomorphism  $z^{-1}(S) = S$ .*

*Proof.* — Since  $\overline{K}/\overline{K}$  is separable, the canonical morphism  $\overline{X}_{\text{red}} \rightarrow \overline{X}_{\text{red}} \times_{\overline{C}} \overline{C}$  is an isomorphism (Lemma 3.20). Thus, the lemma follows from Lemma 3.21.

**Lemma 3.23.** — *Let  $k$  be a field,  $k$  be a separable field extension of  $k$ , and  $Z$  be a  $k$ -scheme locally of finite type. Then the normalization of  $Z$  commutes with the base change via  $k/k$ , i.e., the following statement holds. Take the normalization  $z: Z \rightarrow Z$  of  $Z$ , and the base change  $z: Z \rightarrow Z$  of  $z$  via  $k/k$ . Then  $z$  is a normalization of  $Z$ .*

*Proof.* — Set  $W := \text{Spec } k$ , and  $W := \text{Spec } k$ . Since  $k/k$  is separable, the canonical morphism  $Z_{\text{red}} \rightarrow Z_{\text{red}} \times_W W$  is an isomorphism (Lemma 3.20). Thus, we may assume that both  $Z$  and  $Z$  are reduced. We denote the disjoint union of points of codimension zero on  $Z$  and  $Z$  by  $H$  and  $H$ , respectively. Then the normalizations of  $Z$  and  $Z$  are defined as the normalizations of  $Z$  and  $Z$  in  $H$  and  $H$ , respectively. Since  $k/k$  is separable, the ring  $I \otimes_k k$  is isomorphic to a product of a finite number of fields for any finitely generated field extension  $I/k$ . Thus, we obtain an isomorphism  $H \times_W W = H$ . Since  $W$  is regular over  $W$ , the lemma follows from [7, 6.14.5].

**Lemma 3.24.** — *Let  $k$  be a field,  $k$  be a field extension of  $k$ , and  $Z$  be a proper  $k$ -scheme. We define a  $k$ -scheme by  $Z := Z \times_{\text{Spec } k} \text{Spec } k$ . Then the following statements hold:*

1.  $H^i(Z, \mathcal{O}_Z) = H^i(Z, \mathcal{O}_Z) \otimes_k k$  for any  $i \geq 0$ ;
2. if  $k$  is separable over  $k$ , then  $h^0(Z) = h^0(Z)$ ;
3. if  $Z$  is geometrically integral over  $k$ , then  $h^0(Z) = 1$ .

*Proof.* — Statement 1 follows from the flat base change theorem of cohomology groups [12, 5.2.27]. Statement 2 follows from Statement 1 and Lemma 3.23. Statement 3 follows from [12, 3.2.14(c) and 3.3.21].

For any  $P \in X$ , we may regard  $\bar{X}^{-1}(P)$  as a Weil divisor on  $X$  since  $X$  is flat.

**Lemma 3.25.** — *The following statements hold.*

1. For any  $P \in X$ , there exists  $Q \in P$  such that  $\bar{X}^{-1}(P) = \sum_{Q \in P} Q$ . In particular, the equality  $m(\bar{X}) = m(\bar{X})$  holds (Definition 3.4).
2. The equality  $h^0(\bar{X}) = \sum_{Q \in P} h^0(Q)$  holds.
3. If  $\bar{X}$  is of integral type, then  $h^0(\bar{X}) = |Q|$ .

*Proof.* — Since  $\bar{X}^{-1}(P)$  is reduced (Lemma 3.20), Statement 1 holds. Statement 2 follows from Statement 1 and Lemma 3.24.2. Statement 3 follows from Statement 2 and Lemma 3.24.3.

**Lemma 3.26.** — *Assume that  $\bar{X}$  is of integral type. Take  $P \in X$ . Then  $\bar{X}^{-1}(P) \in P$ .*

*Proof.* — Since  $\bar{X}^{-1}(P) = \sum_{C \in P} \bar{C}$ , and  $\bar{X}$  is geometrically integral over  $\bar{K}$ , the lemma holds.

**Lemma 3.27.** — *For any divisor  $D_1$  on  $X$  and any vertical divisor  $D_2$  on  $X$ , the equality  $D_1 \cdot D_2 = \bar{X}^{-1}(D_1) \cdot \bar{X}^{-1}(D_2)$  holds.*

*Proof.* — The lemma follows from the Lemma 3.24.1.

**Remark 3.28.** — *When  $\bar{X}$  is of integral type, the multiplicities and intersection numbers of the elements of  $P$  may be determined by those of  $P$  (Lemmas 3.26 and 3.27).*

In the following, we study a relationship between the minimalities of the proper regular  $C$ -model  $X$  and the proper regular  $C$ -model  $X$  [12, 9.3.21]. Take a canonical divisor  $K_{X/C}$  of  $X/C$  [12, 9.1.34]. Set  $K_{X/C} := \bar{X}^{-1}(K_{X/C})$ .

**Lemma 3.29.** — *The following statements hold:*

1.  $K_{X/C}$  is a canonical divisor of  $X/C$  ;
2. if  $p_a(X_K) = 1$ , then the following statements hold:
  - (a)  $P$  is a  $(-1)$ -curve on  $X$  [12, 9.3.1] if and only if  $K_{X/C} \cdot P < 0$ ;
  - (b) the proper regular  $C$ -model  $X$  is minimal if and only if there does not exist a  $(-1)$ -curve on  $X$ .

*Proof.* — Statements 1, 2a, and 2b follow from [12, 6.4.9(b)], [12, 9.3.10(b)], and [12, 9.2.2], respectively.

**Proposition 3.30.** — *Assume that  $p_a(X_K) = 1$ . Then the proper regular  $C$ -model  $X$  of  $X_K$  is minimal if and only if the proper regular  $C$ -model  $X_K$  of  $X_K$  is minimal.*

*Proof.* — Let us show the if part. Assume that  $X$  is minimal. Take  $E = P$ . We have only to show that  $K_{X/C} \cdot E = 0$  (Lemma 3.29). Set  $E := \bar{X}^{-1}(E)$ . Take  $Q = P$  so that  $E = \bar{Q}$  (Lemma 3.25.1). Since  $K_{X/C} \cdot \bar{Q} = 0$  for any  $Q$  (Lemma 3.29.1 and 2), and  $K_{X/C} \cdot E = K_{X/C} \cdot \bar{Q}$  (Lemma 3.27), the inequality  $K_{X/C} \cdot E = 0$  holds, which concludes the proof of the if part.

Let us show the converse. Suppose that  $X$  is minimal, and that  $X_K$  is not minimal. We may take a  $(-1)$ -curve  $E = P$  on  $X_K$  (Lemma 3.29.2b). We denote  $\bar{X}(E)$  with the reduced structure by  $\bar{E}$ . Then  $\bar{E} = P$ , and  $\bar{E} = \bar{X}^{-1}(E)$ . Since  $K_{X/C} \cdot \bar{E} = 0$  (Lemma 3.29.2), the inequality  $K_{X/C} \cdot E = 0$  holds [12, 7.1.35 and 7.2.9] (Lemma 3.29.1), which contradicts the inequality  $K_{X/C} \cdot E < 0$  (Lemma 3.29.2a). Thus, the converse holds.

**3.6. Quotients.** — In the following subsections, we assume that  $K$  introduced in §3.5 is a finite Galois extension of  $k$ . Then both  $r_C$  and  $\tau_C$  are bijective (Lemma 3.18). We denote the  $C_K$ -action of  $G_K/k$  on  $C_K$  by  $c_{K/C_K}: G_K/k \rightarrow \text{Aut}(C_K/C_K)$ . Set  $c_{C/C} := r_C^{-1} \circ c_{K/C_K}$ ,  $\bar{c}_{C/C} := \tau_C \circ c_{C/C}$ ,  $x_{X/X} := b_{C/C}$ , and  $\bar{x}_{X/X} := \tau_X \circ x_{X/X}$ . For  $W = C, \bar{C}, C_K, X, \bar{X}$ , and  $X_K$ , we denote the structure morphism of the  $C$ -scheme  $W$  by  $f_{W/C}: W \rightarrow C$ . Then the base change of  $c_{C/C}$  via  $f_{W/C}$  is equal to  $c_W$ . Since  $c_W$  is finite (Lemma 3.18), we may take a quotient of  $c_W$  in the category of  $W$ -schemes, which is a quotient of  $c_W$  in the category of ringed spaces [3, V.4.1 (i)].

**Lemma 3.31.** — *The morphism  $c_W$  is a quotient morphism of  $c_W$  in both the category of  $W$ -schemes and the category of ringed spaces. In particular, the map between underlying topological spaces associated to  $c_W$  is a quotient map of the action on the underlying topological space of  $W$  induced by  $c_W$  in the category of topological spaces.*

*Proof.* — Since  $O_C$  is equal to the invariant subring of  $O_C$  with respect to the action induced by  $c_{C/C}$ , the case  $W = C$  holds (see the proof of [3, V.4.1]). We denote the constant  $W$ -group scheme induced by the group  $G_K/k$  by  $G_W$ . The  $W$ -action  $G_W \times_W W \rightarrow W$  of  $G_W$  on  $W$  induced by  $c_W$  and the second projection  $G_W \times_W W \rightarrow W$  induce a  $W$ -morphism

$$c_W: G_W \times_W W \rightarrow W, \quad (g, w) \mapsto (g \cdot w, w).$$

Since  $C/C$  is free [3, IV.3.2.1], the action  $W/W$  is free. Thus, the morphism  $W/W$  is an isomorphism [3, V.4.1 (iv)] (see [3, V.2 (b)] for the terminology *un couple d'équivalence*), which concludes the proof [3, IV.3.3].

**3.7. Quotients of Dual Graphs.** — We take a proper regular  $C$ -model  $X$  of  $X_K$  and a finite Galois extension  $K/K$  so that  $\bar{X}$  is of fundamental type.

*Example 3.32.* — Whenever  $\bar{K}$  is perfect, we may always take such  $X$  and  $K$  in the following way. Take the completion  $\mathcal{O}$  of a strict Henselization of  $\mathcal{O}_K$  (Example 3.17.A). We denote the field of fractions of  $\mathcal{O}$  by  $K$ , and the residue field of  $\mathcal{O}$  by  $\bar{K}$ . Set  $C := \text{Spec } \mathcal{O}$ , and  $\bar{C} := \text{Spec } \bar{K}$ . The extension  $\mathcal{O}/\mathcal{O}$  induces a morphism  $\pi : C \rightarrow \bar{C}$ . Take the base change  $f_X : X \rightarrow C$  of  $f_X$  via  $\pi$ . Set  $X_0 := X$ . In the same way as in Remark 3.7, we take  $i_1 \in \mathbb{Z}$ ,  $i_2 \in \mathbb{Z}$ , and the successive blowing-ups  $\sigma_i : X_{i+1} \rightarrow X_i$  of  $X_i$  for  $i \geq i_0$ , where we set  $i_0 := \{i \in \mathbb{Z} \mid 0 \leq i < i_2\}$ . Set  $\bar{X}_{i_2} := X_{i_2} \times_C \bar{C}$ . Then  $\bar{X}_{i_2}$  is of fundamental type, and  $\text{Aut}(C/C)$  acts on  $X_0$ . We may show the following statements for any  $i \geq i_0$  by the induction on  $i$ :

1. we denote the center of  $\sigma_i$  by  $T_i$ ; then  $T_i$  is stable under the action of  $\text{Aut}(C/C)$ ;
2. the action of  $\text{Aut}(C/C)$  on  $X_i$  lifts to  $X_{i+1}$ .

Choose a finite Galois extension  $K/K$  in  $K$  so that  $\text{Aut}(C/C)$  trivially acts on  $P(X_{i_2})$  and  $S(X_{i_2})$ . The extension  $\mathcal{O}/\mathcal{O}$  induces a morphism  $\pi : C \rightarrow \bar{C}$ . Set  $X_0 := X$ ,  $X_0 := X$ , and  $\sigma_0 := \pi : X_0 \rightarrow X_0$ . Take the base change  $\sigma_0 : X_0 \rightarrow X_0$  of  $\pi$  via  $f_X$ . We may show the following statements for any  $i \geq i_0$  by the induction on  $i$ :

3. set  $\sigma_i := \sigma_i \circ \sigma_i$ , and  $T_i := \sigma_i(T_i)$ ; we equip  $T_i$  with the reduced structure; then  $\sigma_i^{-1}(T_i) = T_i$  over  $X_i$ ;
4. set  $T_i := (\sigma_i)^{-1}(T_i)$ ; take the blowing-up  $\sigma_i : X_{i+1} \rightarrow X_i$  of  $X_i$  along  $T_i$ , the blowing-up  $\sigma_i : X_{i+1} \rightarrow X_i$  of  $X_i$  along  $T_i$ , and the base change  $\sigma_{i+1} : X_{i+1} \rightarrow X_{i+1}$  of  $\sigma_i$  via  $\sigma_i$ ; then  $X_{i+1} = X_{i+1}$  over  $X_i$ ;
5. take the base change  $\sigma_{i+1} : X_{i+1} \rightarrow X_{i+1}$  of  $\sigma_i$  via  $\sigma_i$ ; then  $X_{i+1} = X_{i+1}$  over  $X_i$ .

In particular, for any  $i \geq i_0$ , the squares in the diagram

$$\begin{array}{ccccc}
 X_{i+1} & \xrightarrow{\sigma_{i+1}} & X_{i+1} & \xrightarrow{\sigma_{i+1}} & X_{i+1} \\
 \downarrow \sigma_i & & \downarrow \sigma_i & & \downarrow \sigma_i \\
 X_i & \xrightarrow{\sigma_i} & X_i & \xrightarrow{\sigma_i} & X_i
 \end{array}$$

are Cartesian, where we identify  $X_{i+1}$  and  $X_{i+1}$  with  $X_{i+1}$  and  $X_{i+1}$ , respectively. Set  $\bar{X}_{i_2} := X_{i_2} \times_C \bar{C}$ . Let us show that  $\bar{X}_{i_2}$  satisfies Conditions 0–3 in Definition 3.6. Since  $\text{Aut}(C/C)$  trivially acts on  $P(X_{i_2})$ , Condition 0 holds. Moreover, since  $\bar{X}_{i_2}$  is of fundamental type, Conditions 1 and 2 follow from Lemma 3.22. Since  $\text{Aut}(C/C)$  trivially acts on  $S(X_{i_2})$ , Condition 3 holds. Therefore, the special fiber  $\bar{X}_{i_2}$  is of fundamental type.

**Remark 3.33.** — Since  $\overline{X}_{i_2}$  is of fundamental type, the multiplicities and intersection numbers of the elements of  $P(X_{i_2})$  may be determined by those of  $P(X_{i_2})$  (Remark 3.28). Moreover, the projection  $S(X_{i_2}) \rightarrow S(X_{i_2})$  (Lemma 3.22) induces a bijection between the underlying sets.

**Definition 3.34.** — We use the notation  $D, \text{Aut } D, V, E, m(\bullet), V(\bullet), E(\bullet), v(\bullet): P \rightarrow V$ , and  $e(\bullet): S \rightarrow E$  for  $\overline{X}/m$  introduced in Definition 3.8. We have a homomorphism

$$\rho_D : \text{Aut}(\overline{X}/\overline{X}) \longrightarrow \text{Aut } D.$$

Set  $D := D \times_{\overline{X}/\overline{X}}$ , and  $G := \text{Im } \rho_D$ . For  $W \subset V$ , we denote the orbit of  $W$  by  $O(W)$ . For  $v \in V$ , we set  $O(v) := O(\{v\})$ . For  $F \subset E$ , we denote the orbit of  $F$  by  $O(F)$ . For  $e \in E$ , we set  $O(e) := O(\{e\})$ . We say that *the action fixes the center of  $e \in E$*  if there exists  $g \in G$  that fixes  $e$  and exchanges the two vertices in  $V(e)$ .

We define the *quotient  $D$  of  $D$  by  $G$*  as a graph consisting of two types of vertices with multiplicities and degrees and edges with degrees in the following way. We introduce the notation  $V, E, m(\bullet), d(\bullet), V(\bullet)$ , and  $E(\bullet)$  for  $D$  in the same way as in Definition 3.12.

*Vertices.* Take an orbit  $O$  of a vertex of  $D$ . Choose  $v \in O$ . The integer  $m(v)$  does not depend on the choice of  $v$ . We put a vertex  $\overline{O}$ , and set  $m(\overline{O}) := m(v)$ , and  $d(\overline{O}) := |O|$ . If the action does not fix the center of any edge in  $E(O)$ , then the vertex  $\overline{O}$  is of the first type. Otherwise, the vertex  $\overline{O}$  is of the second type. For  $W \subset V$ , we set  $\overline{W} := \{\overline{O(w)} \mid w \in W\}$ .

*Edges.* Take an orbit  $O$  of an edge of  $D$  with  $|V(\overline{O})| = 2$ . We put an edge  $\overline{O}$  so that  $V(\overline{O}) = \overline{V(O)}$ , and set  $d(\overline{O}) := |O|$ . For  $F \subset E$ , we set  $\overline{F} := \{\overline{O(f)} \mid f \in F \text{ and } |V(O(f))| = 2\}$ .

Set

$$E_1 := \{e \in E \mid \text{the action fixes the center of } e\},$$

and

$$E_2 := \{e \in E \mid |V(e)| = 2\}.$$

For  $i \in \{1, 2\}$ , we set  $S_i := (e)^{-1}(E_i)$ . Then the restriction  $e_i(\bullet): S_i \rightarrow E_i$  of  $e(\bullet)$  to  $S_i$  and  $E_i$  is bijective for any  $i \in \{1, 2\}$ . We denote the set of unibranch singularities on  $\overline{X}_{\text{red}}$  by  $S_1$  (Definition 3.11). Set  $S_2 := \bigcup_{a \in P(2)} a$ .

**Lemma 3.35.** — *The following statements hold.*

1. For any  $i \in \{1, 2\}$ , the equality  $\overline{X}^{-1}(S_i) = S_i$  holds.
2. The equality  $S_1 \cap S_2 = \emptyset$  holds.
3. The canonical morphism  $\bigcup_{a \in P(2)} a \rightarrow S_2$  is an isomorphism.
4. Any  $s \in S_2$  is a regular point on any  $\overline{X}^{-1}(P)$  with  $s \in P$ .
5. The equality  $S = S_1 \cup S_2$  holds if and only if any singularity on any  $\overline{X}^{-1}(P)$  is unibranch.

*Proof.* — Lemma 3.22 gives the equality  $\bar{X}^{-1}(S) = S$ . Choose  $s \in S$ . Take the two irreducible components  $S_1$  and  $S_2$  containing  $s$ . Set  $s := \bar{X}(s)$ . Then the following statements are equivalent:

- 1-1.  $s \in S_1$ ;
- 1-2. there exists  $g \in G_K / K$  such that  $\bar{X} / \bar{X}(g)$  fixes  $s$  and exchanges  $S_1$  and  $S_2$ ;
- 1-3.  $s \in S_1$ .

Moreover, the following statements are equivalent:

- 2-1.  $s \in S_2$ ;
- 2-2. the orbit of no element of  $P$  contains  $\{s_1, s_2\}$ ;
- 2-3.  $s \in S_2$ .

These equivalences prove the lemma.

**Definition 3.36.** — We use the notation introduced in Definition 3.34. Take the quotient maps  $q_P: P \rightarrow P$  and  $q_S: S_2 \rightarrow S_2$  of the action  $\bar{X} / \bar{X}$ . The maps  $q_V: V \rightarrow V, v \in \overline{O(v)}$  and  $q_E: E_2 \rightarrow E, e \in \overline{O(e)}$  are the quotient maps of the action  $D$ . Moreover, both  $v(\cdot)$  and  $e(\cdot)$  are equivariant with respect to the actions induced by  $\bar{X} / \bar{X}$  and  $D$ . Thus, there exist unique maps  $v(\cdot): P \rightarrow V$  and  $e(\cdot): S_2 \rightarrow E$  such that the squares in the two diagrams

$$\begin{array}{ccc}
 P & \xrightarrow{v(\cdot)} & V \\
 \left| \begin{array}{c} q_P \\ \downarrow \\ q_V \end{array} \right. & & \left| \begin{array}{c} q_S \\ \downarrow \\ q_E \end{array} \right. \\
 P & \xrightarrow{v(\cdot)} & V
 \end{array}
 \qquad
 \begin{array}{ccc}
 S_2 & \xrightarrow{e_2(\cdot)} & E_2 \\
 \left| \begin{array}{c} q_S \\ \downarrow \\ q_E \end{array} \right. & & \left| \begin{array}{c} q_S \\ \downarrow \\ q_E \end{array} \right. \\
 S_2 & \xrightarrow{e(\cdot)} & E
 \end{array}$$

are commutative. Since  $v(\cdot)$  and  $e(\cdot)$  are bijective, the maps  $v(\cdot)$  and  $e(\cdot)$  are bijective.

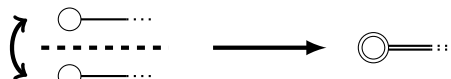
**Theorem 3.37.** — We use the notation introduced in Definitions 3.34 and 3.36. Then the graph  $D$  is the dual graph of  $\bar{X}/m$  with types and degrees by  $v(\cdot)$  and  $e(\cdot)$  (Definition 3.12).

*Proof.* — By Lemma 3.35.3, we may write  $S_2 = \coprod_{a \in P^{(2)}} a$ . Let us show that Statements 1–4 in Definition 3.12 hold for  $v(\cdot)$  and  $e(\cdot)$ . Statement 1 follows from Lemma 3.25.1 and 3. Take  $a \in P$ . Set  $v := v(a)$ . The vertex  $v$  is of the second type if and only if there exists  $e \in E_1$  such that  $v \in \overline{V(e)}$ . Thus, Statement 2 follows from the equality  $\bar{X}^{-1}(S_1) = S_1$  (Lemma 3.35.1). Let us show Statement 3. Take  $a \in P^{(2)}$  and  $s \in a \subset S_2$ . Since  $\bar{X}$  is of fundamental type, the equality  $|q_S^{-1}(s)| = i(a, s)$  holds (Lemmas 3.20 and 3.25.1). Since  $d(e(s)) = |q_E^{-1}(e(s))| = |q_S^{-1}(s)|$ , Statement 3 holds. Let us show Statement 4. Take  $a = \{s_1, s_2\} \subset P^{(2)}$ . Set  $A := \coprod_{a \in P_a} a, P_a := \{ \{s_1, s_2\} \subset P \mid q_P(\cdot) = \cdot \text{ for any } i \in \{1, 2\} \}$ , and  $A := \coprod_{a \in P_a} a$ . Then  $A = q_S(A), e_2(a) = [a]$  for any  $a \in P_a$ , and  $\coprod_{a \in P_a} q_E([a]) = [a]$  (see Definitions 3.8 and 3.12 for  $[\cdot]$ ). Thus, the equalities  $e(A) = e(q_S(A)) = q_E(e_2(A)) = [a]$  hold, which proves Statement 4.

**Example 3.38.** — We give examples of parts of  $D$  and  $D$  in several cases. Take a part of  $D_0$  of  $D$ . We write  $D_0$  on the left-hand side, and its image in  $D$  on the right-hand side, where the multiplicities are omitted for simplicity. We denote the vertices of  $D_0$  by  $O$ . Suppose that the following conditions are satisfied:

1.  $E(O) \subseteq E_2$  in all cases except (h);
2. there exists  $v_0 \in V$  such that  $O = O(v_0)$ .

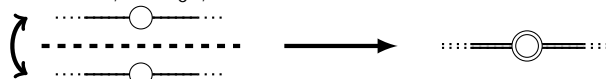
(a)  $|O| = 2$ , and  $|E(v_0)| = 1$ .



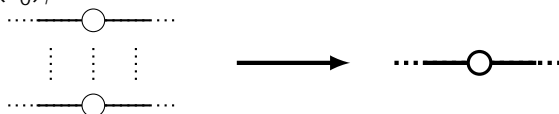
(b)  $|E(v_0)| = 1$ .



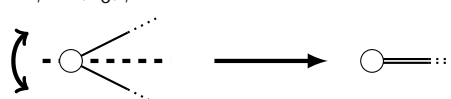
(c)  $|O| = 2$ ,  $|E(v_0)| = 2$ , and  $|\overline{E(v_0)}| = 2$ .



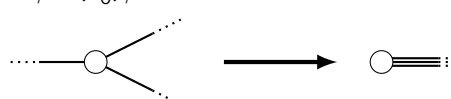
(d)  $|E(v_0)| = 2$ , and  $|\overline{E(v_0)}| = 2$ .



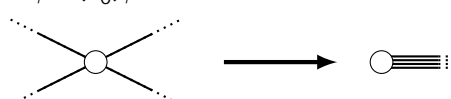
(e)  $|O| = 1$ ,  $|E(v_0)| = 2$ , and  $|\overline{E(v_0)}| = 1$ .



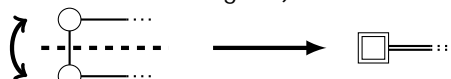
(f)  $|O| = 1$ ,  $|E(v_0)| = 3$ , and  $|\overline{E(v_0)}| = 1$ .



(g)  $|O| = 1$ ,  $|E(v_0)| = 4$ , and  $|\overline{E(v_0)}| = 1$ .



(h)  $|E(v_0)| = 2$ ,  $|\overline{E(v_0)}| = 1$ , and there exists  $e \in E$  such that  $V(e) = O$  (in this case, the action fixes the center of the edge  $e$ ).



**3.8. Curves of Genus One and Dual Graphs.** — We use the notation introduced in §3.3 and Example 3.32. Set  $\overline{X} := f_X^{-1}(\overline{C})$ . We denote the Kodaira symbol of  $\overline{X}$  by  $mT$  (see Remark 3.33), the symbol of the dual graph of  $\overline{X}/m$  by  $D$ , the dual graph of  $\overline{X}_{i_2}/m$



by  $D$ , and the birational morphisms by  $\sigma : X_{i_2} \rightarrow X$  and  $\tau : X_{i_2} \rightarrow X$ . Set  $I_P := \{i \in \mathbb{Z} / 1 \leq i < N\}$ , and  $I_P := I_P \cup \{N\}$ . We write  $P = \{s_i\}_{i \in I_P}$  where  $h^0(s_i) = h^0(s_{i+1})$  for any  $i \in I_P$ .

Assume that  $T = I_1, II, III$ , or  $IV$ . Then  $\overline{X} = m \rightarrow P$  (Lemma 3.25.1). We may write  $S = \{s_i\}$  and  $S = \{s_i\}$  (Lemma 3.22). For  $i \in I_P$ , we denote the restriction of  $\sigma$  to the strict transform of  $s_i$  by  $\sigma_i$ , and set  $s_i := \sigma_i^{-1}(s)$ . We denote the set of prime divisors on  $X_{i_2}$  contained in the exceptional locus of  $\sigma$  by  $P$ . Since the multiplicities of the elements of  $P$  in  $\overline{X}$  are different from each other, any element of  $P$  is stable under the action of  $\overline{X} / \overline{X}$ .

In the following, we introduce two symbols  $T$  and  $D$  to denote the type of  $\overline{X}/m$  and the dual graph  $D$  of  $\overline{X}/m$  with types and degrees (Definition 3.12), respectively (Tables 2–7; see Tables 8 and 9 for the changes from  $T$  and  $D$  to  $T$  and  $D$ , respectively). We use the following symbols for  $T$  ( $n \in \mathbb{Z}_{>0}$ ,  $r \in \mathbb{Z}_{>0}$ , and  $r \mid n$ ):

$$I_0, I_n^r (n-1), I_{n,2}^r (n-1), I_{n,2,2}^r (2r \mid n > 0), II, III, III_2, IV, IV_2, IV_3, \\ I_n, I_{n,2}, I_{n,2,2}, I_{n,2,3}, I_{0,3}, I_{n,4}, II, III, III_2, IV, IV_2, IV_3.$$

For each  $n$ , we set  $I_n := I_n^1$ ,  $I_{n,2} := I_{n,2}^1$ , and  $I_{n,2,2} := I_{n,2,2}^1$ . The symbol  $D$  is an analogue to the symbol of a (twisted) affine Dynkin diagram. The original symbols are the followings:

$$A_u^{(1)} (u-1), B_u^{(1)} (u-3), C_u^{(1)} (u-2), D_u^{(1)} (u-4), E_u^{(1)} (6-u-8), F_4^{(1)}, G_2^{(1)}, \\ B_u^{(2)} (u-2), C_u^{(2)} (u-3), BC_u^{(2)} (u-1), F_4^{(2)}, G_2^{(3)}.$$

We use the following symbols ( $r \geq 1$ ):

$$A_{u,r}^{(1)} (u-0), B_u^{(1)} (u-3), C_{u,r}^{(1)} (u-1), C_{u,r}^{[1]} (u-0), C_{u,r}^{[1]} (u-0), D_u^{(1)} (u-4), \\ E_u^{(1)} (6-u-8), F_4^{(1)}, G_2^{(1)}, \\ B_u^{(2)} (u-2), C_u^{(2)} (u-2), C_u^{[2]} (u-2), BC_u^{(2)} (u-1), BC_u^{[2]} (u-1), F_4^{(2)}, G_2^{(3)}.$$

For each  $u$ , we set  $A_u^{(1)} := A_{u,1}^{(1)}$ ,  $C_u^{(1)} := C_{u,1}^{(1)}$ ,  $C_u^{[1]} := C_{u,1}^{[1]}$ , and  $C_u^{[1]} := C_{u,1}^{[1]}$ . We determine  $D$  by Lemmas 3.22, 3.25, and 3.27.

*Case 0:*  $T = I_0$ . The equalities  $N = 1$ ,  $h^0(s_1) = 1$ , and  $S = \emptyset$  hold. We set  $T := I_0$ , and  $D := A_0^{(1)}$ .

*Case 1:*  $T = I_1$ . The equalities  $N = 1$  and  $h^0(s_1) = 1$  hold.

A.  $D$  is trivial. The equality  $|s_1| = 2$  holds. We set  $T := I_1$ , and  $D := A_0^{(1)}$ .

B. otherwise. The equality  $|s_1| = 1$  holds. We set  $T := I_{1,2}$ , and  $D := C_0^{(1)}$ .

*Case 2:*  $T = II$ . The equalities  $N = 1$ ,  $h^0(s_1) = 1$ , and  $|s_1| = 1$  hold. We set  $T := II$ , and  $D := C_0^{(1)}$ .

$D$	$D$	$N$	$G$	$T$
$A_0^{(1)}$	$\textcircled{1}$	1	1	$I_0, I_1$
$C_0^{(1)}$	$\boxed{1}$	1	$Z_2$	$I_{1,2}$
$C_1^{(1)}$	$\textcircled{1} \text{---} \textcircled{1}$	2	1	III
$C_{0,2}^{(1)}$	$\boxed{\textcircled{1}}$	1	$Z_2$	III <sub>2</sub>
$A_2^{(1)}$	$\begin{array}{c} \textcircled{1} \\ \diagdown \quad \diagup \\ \textcircled{1} \text{---} \textcircled{1} \end{array}$	3	1	IV
$C_1^{(1)}$	$\textcircled{1} \text{---} \boxed{1}$	2	$Z_2$	IV <sub>2</sub>
$C_{0,3}^{(1)}$	$\boxed{\boxed{1}}$	1	$Z_3, S_3$	IV <sub>3</sub>

Table 2. The dual graphs in Cases 0–4.

Case 3:  $T = \text{III}$ . The equality  $N = 1$  or  $2$  holds. For any  $i \in I_P$ , the equality  $|S_i| = 1$  holds.

A.  $N = 2$ . The equality  $|S_1| \cdot |S_2| = 2$  holds. For any  $i \in \{1, 2\}$ , the equality  $h^0(S_i) = 1$  holds. We set  $T := \text{III}$ , and  $D := C_1^{(1)}$ .

B.  $N = 1$ . The equality  $h^0(S_1) = 2$  holds. We set  $T := \text{III}_2$ , and  $D := C_{0,2}^{(1)}$ .

Case 4:  $T = \text{IV}$ . The equality  $N = 1, 2,$  or  $3$  holds. For any  $i \in I_P$ , the equality  $|S_i| = 1$  holds.

A.  $N = 3$ . For any  $\{i, j\} \in P^{(2)}$ , the equality  $|S_i \cap S_j| = 1$  holds. For any  $i \in \{1, 2, 3\}$ , the equality  $h^0(S_i) = 1$  holds. We set  $T := \text{IV}$ , and  $D := A_2^{(1)}$ .

B.  $N = 2$ . The equality  $|S_1| \cdot |S_2| = 2$  holds. For any  $i \in \{1, 2\}$ , the equality  $h^0(S_i) = i$  holds. We set  $T := \text{IV}_2$ , and  $D := C_1^{(1)}$ .

C.  $N = 1$ . The equality  $h^0(S_1) = 3$  hold. We set  $T := \text{IV}_3$ , and  $D := C_{0,3}^{(1)}$ .

In the other cases, the special fiber  $\overline{X}$  is of fundamental type. We study these cases by the method developed in §3.7.

Case 5:  $T = I_n$  ( $n \geq 2$ ). Since  $\text{Aut } D = D_{2n}$ , we have an isomorphism  $G = Z_r$  or  $D_{2r}$ , where  $r \mid n$ . Set  $u := n/r$ .

A.  $G = Z_r$ . The equality  $N = u$  holds. For any  $\sigma \in P$ , the equality  $h^0(S_\sigma) = r$  holds. We set  $T := I_n^r$ , and  $D := A_{u-1,r}^{(1)}$ .

B.  $G = D_{2r}$ . We denote the subset of  $G$  consisting of rotations of the cycle  $D$  by  $H$ . Then  $H$  is a normal subgroup of  $G$ , and  $H = Z_r$ . Set  $Y := X/H$ , and  $G := G/H$ . Then the special fiber of  $Y$  is of type  $I_n^r$ ,  $G = Z_2$ ,  $G$  acts on  $Y$ , and  $X = Y/G$ . By  $M$  we denote the number of elements of  $P(Y)$  that are fixed by the action of  $G$ . Then  $M = 0, 1,$  or  $2$ . The equality  $M = 1$  holds if and only if  $u$  is odd.


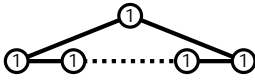


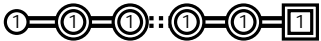


$D$	$D$	$N$	$G$	$T$
$A_{0,n}^{(1)}$ $u = 1$		1	$Z_n$	$I_n^n$
$A_{u-1,r}^{(1)}$ $u \geq 2$		$u$	$Z_r$	$I_n^r$
$C_{0,n}^{(1)}$ $u = 1$		1	$D_{2n}$	$I_{n,2}^n$
$C_{\frac{u}{2},r}^{(1)}$ $u: \text{even}$		$\frac{u}{2} + 1$	$D_{2r}$	$I_{n,2}^r$
$C_{\frac{u-1}{2},r}^{(1)}$ $u: \text{odd}$		$\frac{u+1}{2}$	$D_{2r}$	$I_{n,2}^r$
$C_{0,\frac{n}{2}}^{(1)}$ $u = 2$		1	$D_n$	$I_{\frac{n}{2},2,2}^n$
$C_{\frac{u}{2}-1,r}^{(1)}$ $u: \text{even}$		$\frac{u}{2}$	$D_{2r}$	$I_{n,2,2}^r$

Table 3. The dual graphs in Case 5. The inequality  $n \geq 2$  holds (if  $2 \nmid n$ , then  $C_{0,n}^{(1)} = C_{0,\frac{n}{2}}^{(1)}$ ). The thick circles, squares, and segments are of degree  $r$ . The double thick circles, squares, and segments are of degree  $2r$ .

- (a)  $M > 0$ . We set  $T := I_{n,2}^r$ . If  $N = 1$ , then we set  $D := C_{0,n}^{(1)}$ . If  $N > 0$ , and  $M = 2$ , then we set  $D := C_{\frac{u}{2},r}^{(1)}$ . Otherwise, we set  $D := C_{\frac{u-1}{2},r}^{(1)}$ .
- (b)  $M = 0$ . In this case, the reduction  $\bar{X}_{\text{red}}$  has two unibranch singularities. We set  $T := I_{n,2,2}^r$ . If  $u = 2$ , then we set  $D := C_{0,\frac{n}{2}}^{(1)}$  or  $C_{0,n}^{(1)}$ . Otherwise, we set  $D := C_{\frac{u}{2}-1,r}^{(1)}$ .

Case 6:  $T = I_{n-5}$  ( $n \geq 5$ ).

- A.  $n = 5$ . Since  $\text{Aut } D = S_4$ , we have an isomorphism  $G = 1, Z_2, Z_3, Z_4, Z_2^2, S_3, D_8, A_4$ , or  $S_4$ . If  $N = 5$  (resp.  $N = 4$ , resp.  $N = 3$ , and  $h^0(\mathcal{N}) = 2$ , resp.  $N = 3$ , and  $h^0(\mathcal{N}) = 3$ , resp.  $N = 2$ ), we set  $T := I_0$  (resp.  $I_{0,2}$ , resp.  $I_{0,2,2}$  or  $I_{0,2,3}$ , resp.  $I_{0,3}$ , resp.  $I_{0,4}$ ), and  $D := D_4^{(1)}$  (resp.  $B_3^{(1)}$ , resp.  $B_2^{(2)}$  or  $C_2^{(2)}$ , resp.  $G_2^{(1)}$ , resp.  $BC_1^{(2)}$ ).
- B.  $n \geq 6$ . Since  $\text{Aut } D = D_8$ , we have an isomorphism  $G = 1, Z_2, Z_4, Z_2^2$ , or  $D_8$ .
  - (a)  $N = n - 2$ . If  $N = n$  (resp.  $N = n - 1$ , resp.  $N = n - 2$ ), then we set  $T := I_{n-5}$  (resp.  $I_{n-5,2}$ , resp.  $I_{n-5,2,2}$ ), and  $D := D_{n-1}^{(1)}$  (resp.  $B_{n-2}^{(1)}$ , resp.  $B_{n-3}^{(2)}$ ).

$D$	$D$	$N$	$G$	$T$
$D_{n-1}^{(1)}$		$n$	$1$	$I_{n-5}$
$B_{n-2}^{(1)}$		$n - 1$	$Z_2$	$I_{n-5,2}$
$B_2^{(2)}$ (= $C_2^{(2)}$ ) $n = 5$		$3$	$Z_2, Z_2^2$	$I_{0,2,2}$ (= $I_{0,2,3}$ )
$B_{n-3}^{(2)}$ $n \geq 6$		$n - 2$	$Z_2, Z_2^2$	$I_{n-5,2,2}$
$C_{\frac{n-1}{2}}^{(2)}$ $n \geq 7$ $n$ : odd		$\frac{n+1}{2}$	$Z_2$	$I_{n-5,2,3}$
$C_{\frac{n}{2}-1}^{(2)}$ $n$ : even		$\frac{n}{2}$	$Z_2$	$I_{n-5,2,3}$
$G_2^{(1)}$ $n = 5$		$3$	$Z_3, S_3$	$I_{0,3}$
$BC_1^{(2)}$ $n = 5$		$2$	$Z_2^2, Z_4, D_8,$ $A_4, S_4$	$I_{0,4}$
$BC_{\frac{n-3}{2}}^{(2)}$ $n \geq 7$ $n$ : odd		$\frac{n-1}{2}$	$Z_2^2, Z_4, D_8$	$I_{n-5,4}$
$BC_{\frac{n}{2}-2}^{(2)}$ $n$ : even		$\frac{n}{2} - 1$	$Z_2^2, Z_4, D_8$	$I_{n-5,4}$

Table 4. The dual graphs in Case 6. The inequality  $n \geq 5$  holds.

- (b)  $n/2 \leq N \leq n-3$ . We set  $T := I_{n-5,2,3}$ . If  $n$  is odd, then we set  $D := C_{\frac{n-1}{2}}^{(2)}$ . Otherwise, we set  $D := C_{\frac{n}{2}-1}^{(2)}$ .
- (c) otherwise. We set  $T := I_{n-5,4}$ . If  $n$  is odd, then we set  $D := BC_{\frac{n-3}{2}}^{(2)}$ . Otherwise, we set  $D := BC_{\frac{n}{2}-2}^{(2)}$ .

Case 7:  $T = IV$ . Since  $\text{Aut } D = S_3$ , we have an isomorphism  $G = 1, Z_2, Z_3$ , or  $S_3$ . If  $G = 1$ , then we set  $T := IV$ , and  $D := E_6^{(1)}$ . If  $G = Z_2$ , then we set  $T := IV_2$ , and  $D := F_4^{(1)}$ . Otherwise, we set  $T := IV_3$ , and  $D := G_2^{(3)}$ .

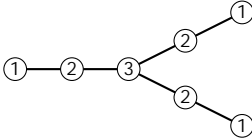
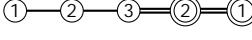

$D$	$D$	$N$	$G$	$T$
$E_6^{(1)}$		7	1	IV
$F_4^{(1)}$		5	$Z_2$	$IV_2$
$G_2^{(3)}$		3	$Z_3, S_3$	$IV_3$

Table 5. The dual graphs in Case 7.

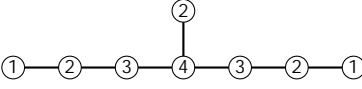
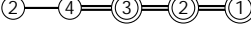
$D$	$D$	$N$	$G$	$T$
$E_7^{(1)}$		8	1	III
$F_4^{(2)}$		5	$Z_2$	$III_2$

Table 6. The dual graphs in Case 8.

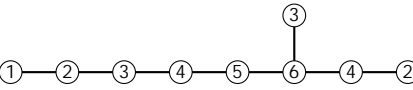
$D$	$D$	$N$	$G$	$T$
$E_8^{(1)}$		9	1	II

Table 7. The dual graph in Case 9.

$T$	$I_0$	$I_n (n \geq 1)$	II	III	IV	
$T$	$I_0$	$I_n^r, I_{n,2}^r, I_{n,2,2}^r$	II	III, III <sub>2</sub>	IV, IV <sub>2</sub> , IV <sub>3</sub>	
$T$	$I_n (n \geq 0)$			II	III	IV
$T$	$I_n, I_{n,2}, I_{n,2,2}, I_{n,2,3}, I_{0,3} (n = 0), I_{n,4}$			II	III, III <sub>2</sub>	IV, IV <sub>2</sub> , IV <sub>3</sub>

Table 8. The changes from  $T$  to  $T$ . The relation  $r/n$  holds.

Case 8:  $T = III$ . Since  $\text{Aut } D = Z_2$ , we have an isomorphism  $G = 1$  or  $Z_2$ . If  $G = 1$ , then we set  $T := III$ , and  $D := E_7^{(1)}$ . Otherwise, we set  $T := III_2$ , and  $D := F_4^{(2)}$ .

Case 9:  $T = II$ . Since  $\text{Aut } D = 1$ , we have an isomorphism  $G = 1$ . We set  $T := II$ , and  $D := E_8^{(1)}$ .

$D$	$A_0$	$A_{n-1} (n \geq 2)$			
$D$	$A_0^{(1)}, C_0^{(1)}$	$A_{\frac{n}{r}-1, r}^{(1)}$	$C_{\frac{n}{2r}, r}^{(1)}$	$C_{\frac{n-r}{2r}, r}^{(1)}$	$C_{\frac{n}{2r}-1, r}^{(1)}$
$D$	$D_{n-1} (n \geq 5)$				
$D$	$D_{n-1}^{(1)}, B_{n-2}^{(1)}, G_2^{(1)}$	$(n = 5), B_{n-3}^{(2)}$	$C_{\frac{n-1}{2}}^{(2)}$	$C_{\frac{n}{2}-1}^{(2)}$	$BC_{\frac{n-3}{2}}^{(2)}, BC_{\frac{n}{2}-2}^{(2)}$
$D$	$E_6$		$E_7$	$E_8$	
$D$	$E_6^{(1)}, F_4^{(1)}, G_2^{(3)}$	$E_7^{(1)}, F_4^{(2)}$		$E_8^{(1)}$	

Table 9. The changes from  $D$  to  $D$ . The relation  $r \mid n$  holds.

**Lemma 3.39.** — *Let  $k$  be a perfect field, and  $Z$  be a  $k$ -scheme. Then the following statements hold:*

1.  $Z$  is reduced if and only if  $Z$  is geometrically reduced over  $k$ ;
2. assume that  $Z$  is locally of finite type; then  $Z$  is regular if and only if  $Z$  is smooth over  $k$ .

*Proof.* — Statements 1 and 2 follow from [7, 4.6.11] and [8, 17.15.2], respectively.

In the above classification, we obtain the following (Lemmas 3.22, 3.24, and 3.39).

**Proposition 3.40.** — *Take  $P$  and the normalization  $\tilde{P}$  of  $P$ . Then the following statements hold.*

1. If  $T = \mathbb{A}_0^n$ , then  $P = \{ \text{pt} \}$ , and  $\tilde{P}$  is a proper smooth geometrically integral  $H^0(\mathbb{A}_0^n, \mathbb{Z})$ -curve of genus one. Otherwise, the normalization of  $P$  is a proper smooth geometrically integral  $H^0(\mathbb{A}_0^n, \mathbb{Z})$ -curve of genus zero.
2. If  $T = \mathbb{A}_n^n (n \geq 1)$ , then  $P = \{ \text{pt} \}$ ,  $|\text{sing}| = 1$ , and  $|\text{sing}^{-1}(\text{pt})| = 2$  ( $\text{sing}$  consists of one non-unibranch singularity). If  $T = \mathbb{A}_{n,2,2}^n (2 \mid n > 0)$ , then  $P = \{ \text{pt} \}$ ,  $|\text{sing}| = 2$ , and  $|\text{sing}^{-1}(\text{pt})| = 2$  ( $\text{sing}$  consists of two unibranch singularities). Otherwise, if  $\text{sing} = \emptyset$ , then  $|\text{sing}| = |\text{sing}^{-1}(\text{pt})| = 1$  ( $\text{sing}$  consists of one unibranch singularity).

#### 4. Separable Closed Points

**4.1. Special Fibers, Indices, and Separable Closed Points.** — Take a separable closure  $K^{\text{sep}}$  of  $K$ . For a field extension  $K'/K$  in  $K^{\text{sep}}$ , we set  $G_{K'} := G_{K^{\text{sep}}/K}$ . Let  $E_K$  be a  $K$ -elliptic curve.

**Definition 4.1.** — Take a proper regular  $C$ -model  $f_E: E \rightarrow C$  of  $E_K$ . The  $K$ -elliptic curve  $E_K$  is said to *have good reduction* if  $E$  is smooth over  $C$ . The  $K$ -elliptic curve  $E_K$  is said to *have toric reduction* if the identity component of the special fiber of the Néron model of  $E_K$  is a  $\overline{C}$ -torus. The  $K$ -elliptic curve  $E_K$  is said to *have potentially good* (resp. *potentially toric reduction*) if there exists a finite separable field extension  $K'/K$  such that the  $K'$ -elliptic curve  $E_K \times_K K'$  has good (resp. toric reduction).

*Proof of Theorem 1.1.* — Take a minimal proper regular  $C$ -model  $f_X: X \rightarrow C$  of  $X_K$ . Set  $\bar{X} := f_X^{-1}(\bar{C})$ , and  $l := l(X_K)$ . We may take a divisor  $D$  on  $X_K$  of degree  $l$ . The Riemann–Roch theorem gives the equality

$$\dim_K H^0(X_K, \mathcal{O}_{X_K}(D)) = l$$

[12, 7.3.33]. Thus, we may take an effective divisor  $\sum_{y \in S} a_y [y]$  of degree  $l$ , where  $S$  is a finite set of closed points on  $X_K$ ,  $a_y \in \mathbb{Z}_{>0}$  for any  $y \in S$ , and  $[y]$  is the prime divisor with support  $y$ . Then  $\sum_{y \in S} a_y [k(y) : K] = l$ , and  $l \mid [k(y) : K]$  for any  $y \in S$ . Thus, we may write  $S = \{z\}$ , and the equalities  $a_z = 1$  and  $[k(z) : K] = l$  hold. We have to show that there exists a separable closed point  $x$  on  $X_K$  such that  $[k(x) : K] = l$ . If  $\bar{K}$  is infinite, then it follows from [5, 8.4(2) and (3)].

Assume that  $\bar{K}$  is finite. We use the notation  $H^0(\cdot)$ ,  $h^0(\cdot)$ ,  $R(X)$ ,  $P(X)$ , and  $n(\cdot)$  introduced in §2 and Definition 3.4. Take  $P(X)$ , and the normalization  $\bar{\cdot}$  of  $\cdot$ . We denote the index of  $\bar{\cdot}_{\text{reg}}$  by  $l(\bar{\cdot}_{\text{reg}})$  (see §1). Since  $H^0(\bar{\cdot}) = k(x)$  for any closed point  $x$  on  $\bar{\cdot}$ , the relation  $h^0(\bar{\cdot}) \mid l(\bar{\cdot}_{\text{reg}})$  holds. For any finite field  $k$  and any proper smooth geometrically integral  $k$ -curve  $C_k$  of genus zero (resp. of genus one), the inequality  $|C_k(k)| \geq 3$  (resp.  $|C_k(k)| \geq 1$ ) holds since  $C_k$  is  $k$ -isomorphic to  $\mathbb{P}_k^1$  (resp. a  $k$ -elliptic curve) ([17, II.3.3(a)] and Example 1.5.2). Thus, Proposition 3.40 shows that  $l(\bar{\cdot}_{\text{reg}}) \mid h^0(\bar{\cdot})$ , which implies that  $l(\bar{\cdot}_{\text{reg}}) \mid h^0(\bar{\cdot})$ . Therefore, the equality  $l(\bar{\cdot}_{\text{reg}}) = h^0(\bar{\cdot})$  holds. Since  $l = \gcd_{P(X)} \{n(\bar{\cdot}) \cdot l(\bar{\cdot}_{\text{reg}})\}$  [5, 8.2(b)], the equality

$$l = \gcd_{P(X)} \{n(\bar{\cdot}) \cdot h^0(\bar{\cdot})\}$$

holds. Thus, by the classification of the special fibers in §3.8, there exists  $\bar{\cdot} \in P(X)$  such that  $n(\bar{\cdot}) \cdot h^0(\bar{\cdot}) = l$ , and  $(R(X))(\bar{\cdot}) = h^0(\bar{\cdot})$  (Proposition 3.40). Therefore, the theorem follows from [5, 8.4(3)].

**Remark 4.2.** — In the above proof, the result in §3.8 is applied in the case where  $\bar{K}$  is finite.

**Example 4.3.** — The following statement holds [18, Thm. 2]: for any global field  $K$ , any  $K$ -elliptic curve  $E_K$ , and any  $P \in \mathbb{Z}_{>0}$ , there exists  $\bar{\cdot} \in H^1(K, E_K)$  such that  $P(\bar{\cdot}) = P$ , and  $l(X_K) = P(\bar{\cdot})^2$ , where  $X_K$  is the  $K$ -torsor under  $E_K$  corresponding to  $\bar{\cdot}$ . In particular, for any closed point  $x$  on  $X_K$ , the relation  $P(\bar{\cdot})^2 \mid [k(x) : K]$  holds.

### 4.2. Case of Good Reduction. —

**Theorem 4.4.** — *Suppose that  $\bar{K}$  is perfect and WC-trivial for elliptic curves. Assume that  $E_K$  has good reduction. Take  $\bar{\cdot} \in H^1(K, E_K)$ . Then there exists a separable field extension  $L/K$  of degree  $P(\bar{\cdot})$  such that  $\bar{\cdot}|_L = 0$ .*

*Proof.* — By the induction on  $P(\bar{\cdot})$ , we may assume that  $P(\bar{\cdot})$  is a prime number. Take the  $K$ -torsor  $X_K$  under  $E_K$  corresponding to  $\bar{\cdot}$ , a minimal proper regular  $C$ -model  $f_X: X \rightarrow C$  of  $X_K$ , and the completion  $\mathcal{O}$  of a strict Henselization of  $\mathcal{O}_K$  (Example 3.17.A). We denote the field of fractions of  $\mathcal{O}$  by  $K$ . Set  $C := \text{Spec } \mathcal{O}$ ,  $E := E \times_C C$ ,  $X := X \times_C C$ , and  $m := P(\bar{\cdot}|_K)$ . Then  $E$  and  $X$  are minimal proper regular  $C$ -models of their generic fibers (Proposition 3.30). Since  $E$  is smooth over  $C$ , the Kodaira symbol of the special fiber of  $X$  is equal to  $m I_0$  (Remark 3.10.1). Since  $\bar{K}$  is perfect, the  $\bar{K}$ -scheme  $\bar{X}_{\text{red}}$  is a

$\bar{K}$ -torsor under a  $\bar{K}$ -elliptic curve  $\bar{E}_0$  [13, 8.1–8.2]. Moreover, the equality  $m(\bar{X}) = m$  holds (Lemma 3.25.1; see Definition 3.4 for  $m(\bar{X})$ ). Since  $\bar{K}$  is WC-trivial for elliptic curves, there exists a  $\bar{C}$ -isomorphism  $\bar{X}_{\text{red}} = \bar{E}_0$ . Thus, there exists a separable field extension  $L/K$  of degree  $m$  such that  $X_K(L) = \emptyset$  [5, 8.4(3)], which gives the equality  $\chi(L) = 0$ . Since  $P(\chi) = 1$ , the inequality  $m = 1$  holds. Since  $P(\chi)$  is a prime number, and  $m = P(\chi_K) / P(\chi)$ , the equality  $m = P(\chi)$  holds, which concludes the proof.

**4.3. Case of Toric Reduction.** — In this subsection, we use the rigid analytic uniformization of  $E_K$ . Assume that  $E_K$  has potentially toric reduction. For a  $K$ -scheme  $Z_K$  locally of finite type, we denote the analytification of  $Z_K$  by  $Z_K^{\text{an}}$ . Take the uniformization  $u_K : T_K^{\text{an}} / E_K^{\text{an}} = T_K^{\text{an}} / \Gamma_K^{\text{an}}$  of  $E_K$ , where  $T_K$  is a  $K$ -torus, and  $\Gamma_K$  is a  $K$ -lattice of  $T_K$ . The  $K$ -lattice  $\Gamma_K$  is associated with a  $G_K$ -module  $\Gamma_Z$  whose underlying group is isomorphic to  $Z$ . Let  $K'/K$  be a field extension in  $K^{\text{sep}}$ . For a module  $M$ , we denote the  $G_K$ -module associated with  $M$  with trivial action of  $G_K$  by  $M_K$ . The  $K$ -torus  $T_K$  (resp. the  $K$ -lattice  $\Gamma_K$ ) is said to *split over  $K$*  if  $T_K \times_K K' = G_{m,K}$  as  $K$ -group schemes (resp.  $\Gamma_Z = \Gamma_{Z,K}$  as  $G_K$ -modules).

We denote the group of  $K^{\text{sep}}$ -automorphisms of the  $K^{\text{sep}}$ -group scheme  $G_{m,K^{\text{sep}}}$  by  $\text{Aut}_{K^{\text{sep}}} G_{m,K^{\text{sep}}}$ . Then  $\text{Aut}_{K^{\text{sep}}} G_{m,K^{\text{sep}}} = Z_2$ . Choose an isomorphism  $T_K : T_K \times_K K^{\text{sep}} = G_{m,K^{\text{sep}}}$  between  $K^{\text{sep}}$ -group schemes. The action of  $G_K$  on  $K^{\text{sep}}$  induces  $K$ -actions  $T_K$  and  $\Gamma_{G_{m,K}}$  of  $G_K$  on  $T_K \times_K K^{\text{sep}}$  and  $G_{m,K^{\text{sep}}}$ , respectively. We define a  $K^{\text{sep}}$ -action  $T_K : G_K \rightarrow \text{Aut}_{K^{\text{sep}}} G_{m,K^{\text{sep}}}$  of  $G_K$  on  $G_{m,K^{\text{sep}}}$  by  $T_K(g) := T_K \circ T_K(g) \circ T_K^{-1} \circ \Gamma_{G_{m,K}}^{-1}(g)$ . Take the field extension  $M/K$  corresponding to  $\text{Ker } T_K$ . Then  $G_{M/K} = 1$  or  $Z_2$ , and  $M$  is minimum among the field extensions of  $K$  in  $K^{\text{sep}}$  over which  $T_K$  splits.

Take a Galois extension  $M'/K$  in  $K^{\text{sep}}$  so that  $M' = M$ . Fix an isomorphism  $T_{M'} = G_{m,M'}$  between  $M'$ -group schemes, which induces an isomorphism  $T_K(M') = (M')^\times$  between groups. For  $g \in G_{M'/K}$ , we denote the image of  $a \in (M')^\times$  (resp.  $a \in T_K(M')$ ) under  $g$  by  $ga$  (resp.  $g \cdot a$ ), and set

$$e(g) := \begin{cases} 1 & \text{if the image of } g \text{ in } G_{M'/K} \text{ is equal to the identity,} \\ -1 & \text{otherwise.} \end{cases}$$

Then  $g \cdot a = ga^{e(g)}$  for any  $g \in G_{M'/K}$  and any  $a \in T_K(M') = (M')^\times$ . Take a generator  $q$  of  $\Gamma_Z$ . Note that the valuation of  $q$  is not equal to zero.

**Lemma 4.5.** — *The relation  $q \in K^\times$  holds. In particular, the lattice  $\Gamma_Z$  splits over  $M$ .*

*Proof.* — Set  $M := K^{\text{sep}}$ . Take  $g \in G_K$ . Since  $g \cdot \Gamma_Z = \Gamma_Z$ , we may take  $e_g \in Z$  so that  $g \cdot q = q^{e_g}$ . Since  $g \cdot q = gq^{e(g)}$ , the equality  $q^{e_g} = gq^{e(g)}$  holds. Taking the valuations of both sides, we obtain the equality  $e_g = e(g)$ . Thus, the equality  $gq = q$  holds, which concludes the proof.

The exact sequence of  $G_K$ -modules

$$0 \longrightarrow \Gamma_Z \longrightarrow T_K(K^{\text{sep}}) \longrightarrow E_K(K^{\text{sep}}) \longrightarrow 0$$

induces a long exact sequence of abelian groups

$$H^1(K, \Gamma_Z) \longrightarrow H^1(K, T_K) \xrightarrow{u_K} H^1(K, E_K) \xrightarrow{\kappa} H^2(K, \Gamma_Z) \longrightarrow H^2(K, T_K).$$



Set  $\mathcal{O} := \sum_{z \in Z_K} \mathcal{O}_K$ , and  $\mathcal{O}/Z := \sum_{z \in Z_K} (\mathcal{O}/Z)_K$ . Since  $\mathcal{O}$  is divisible, the equality  $H^i(K, \mathcal{O}) = 0$  holds for any  $i \geq 0$ . Thus, the exact sequence of  $G_K$ -modules

$$0 \longrightarrow \mathcal{O} \longrightarrow \mathcal{O} \longrightarrow \mathcal{O}/Z \longrightarrow 0$$

induces an isomorphism

$$i_K^i: H^i(K, \mathcal{O}/Z) \xrightarrow{\cong} H^{i+1}(K, \mathcal{O})$$

for any  $i \geq 0$ . We denote the image of  $g \in G_K$  in  $G_{M/K}$  by  $\bar{g}$ . Since the action of  $G_M$  on  $\mathcal{O}/Z$  is trivial (Lemma 4.5), we have a canonical isomorphism

$$H^1(M, \mathcal{O}/Z) = \text{Hom}(G_M, \mathcal{O}/Z).$$

Thus, the restriction morphism

$$H^1(K, \mathcal{O}/Z) \longrightarrow H^1(M, \mathcal{O}/Z)^{G_{M/K}}$$

induces a homomorphism

$$\bar{\cdot}: H^1(K, \mathcal{O}/Z) \longrightarrow \text{Hom}(G_M, \mathcal{O}/Z)^{G_{M/K}},$$

where  $(\bar{g} \cdot)(h) = g(g^{-1}hg)$  for any  $g \in G_K$ , any  $h \in G_M$ , and any  $\cdot \in \text{Hom}(G_M, \mathcal{O}/Z)$  [17, 1.2.6].

Take  $H^1(K, E_K)$ . Put  $\mathfrak{k} := (\text{Gal}(L/K))^{-1} \cdot \mathfrak{k}$ , and  $\mathfrak{k} := \text{Ker } \bar{\cdot}$ . Since  $\bar{g} \cdot = \cdot$  for any  $g \in G_K$ , the equality  $g^{-1}\mathfrak{k}g = \mathfrak{k}$  holds for any  $g \in G_K$ . Thus, the subgroup  $\mathfrak{k}$  of  $G_K$  is normal, which implies that the field extension  $L/K$  corresponding to  $\mathfrak{k}$  is Galois. Therefore, we may take  $L$  as  $M$  introduced above. We denote the order of  $\bar{\cdot}$  in  $\text{Hom}(G_M, \mathcal{O}/Z)$  by  $P(\cdot)$ .

**Lemma 4.6.** — *The field  $M$  is a cyclic extension of  $K$  of degree  $P(\cdot)$ .*

*Proof.* — The lemma follows from the isomorphisms  $G_M/\mathfrak{k} = \text{Im } \bar{\cdot} = Z_{P(\cdot)}$ .

**Proposition 4.7.** — *The following statements hold:*

1.  $G_M/M = Z_{P(\cdot)}$ , and  $G_{M/K} = 1$  or  $Z_2$ ;
2. if  $P(\cdot) = 2$ , and  $G_{M/K} = Z_2$ , then  $G_{M/K} = Z_4$  or  $Z_2^2$ ;
3.  $\bar{\cdot}_M = 0$ .

*Proof.* — Statement 1 follows from Lemma 4.6. Statement 2 follows from Statement 1. Since  $T_K$  splits over  $M$ , the equality  $H^1(M, T_K) = 0$  holds, which implies that  $\bar{\cdot}_M$  is injective. The equality  $\bar{\cdot}_M = 0$  gives the equality  $\bar{\cdot}_M(\bar{\cdot}_M) = 0$ . Thus, Statement 3 holds.

**Proposition 4.8.** — *Assume that  $2 \nmid P(\cdot)$ . Then there exists a field extension of  $K$  in  $M$  of degree  $P(\cdot)$ . Moreover, for any field extension  $K'/K$  in  $M$  of degree  $P(\cdot)$ , the equality  $\bar{\cdot}_{K'} = 0$  holds.*

*Proof.* — The first statement follows from Proposition 4.7.1 and Sylow’s theorem. The composite of the restriction homomorphism and the corestriction homomorphism

$$H^1(K, E_K) \longrightarrow H^1(M, E_K) \longrightarrow H^1(K, E_K)$$

is equal to the multiplication by  $[M : K]$  [17, I.2.4]. Thus, the last statement follows from the facts  $[M : K] = [M : K] / 2$  and  $\int_M = 0$  (Proposition 4.7.1 and 3).

Since  $T_K$  splits over  $M$ , we have a  $G_{M/K}$ -equivariant isomorphism  $E_K(M) = T_K(M) / Z$ . We denote the image of  $a \in T_K(M)$  in  $E_K(M)$  by  $\bar{a}$ . The element  $\int_M$  may be represented by  $\{\bar{a}g\}_g \in Z^1(G_{M/K}, E_K(M))$ .

**Proposition 4.9.** — Assume that  $G_{M/K} = Z_2$ , and  $G_{M/K} = Z_2$  or  $Z_4$ . Then  $\int_M = 0$ .

*Proof.* — Take a generator  $g$  of  $G_{M/K}$ . We may assume that  $M = M$ , and take  $e \in Z$  so that

$$a \cdot a^{-1} \cdot {}^2a \cdot {}^3a^{-1} = q^e.$$

Taking the valuations of both sides, we obtain the equality  $e = 0$ , which implies that

$$a \cdot a^{-1} \cdot {}^2a \cdot {}^3a^{-1} = 1.$$

Thus, we may take  $\int_M \in H^1(K, T_K)$  so that  $\int_M = u_K(\int_M)$ . Since  $T_K$  splits over  $M$ , the equality  $H^1(M, T_K) = 0$  holds, which implies that  $\int_M = 0$ . Therefore, the equality  $\int_M = 0$  holds.

**Lemma 4.10.** — The trace map  $\text{Tr}_{k/K} : k \rightarrow K$  is surjective for any Galois extension  $k/K$  of degree 2.

*Proof.* — Take  $a \in k$ . We denote the characteristic of  $k$  by  $p_k$ . If  $p_k = 2$ , then  $\text{Tr}_{k/K}(a/2) = a$ . Assume that  $p_k = 2$ . Take the generator  $g$  of  $G_{k/K}$ . We may take  $b \in k$  so that  $b = b + 1$ . Then  $\text{Tr}_{k/K}(ab) = a$ , which concludes the proof.

**Lemma 4.11.** — Let  $F$  be a finite Galois extension of  $K$  of degree  $d$ . We denote the valuation ring of  $F$  by  $O_F$ , the residue field of  $O_F$  by  $\bar{F}$ , and the norm map by  $N_{F/K} : F \rightarrow K$ . Assume that  $\bar{F}/\bar{K}$  is a Galois extension of degree  $d$ , and that both norm map and trace map of  $\bar{F}/\bar{K}$  are surjective. Then  $N_{F/K}(O_F^\times) = O_K^\times$ . Moreover, the group  $K^\times / N_{F/K}(F^\times)$  is isomorphic to  $Z_d$ , and generated by the image of a uniformizer of  $O_K$ .

*Proof.* — We denote the maximal ideal of  $O_K$  and  $O_F$  by  $\mathfrak{m}_K$  and  $\mathfrak{m}_F$ , respectively. Let us consider the diagram of abelian groups with commutative squares and horizontal exact sequences

$$\begin{array}{ccccccc} 1 & \longrightarrow & 1 + \mathfrak{m}_F & \longrightarrow & O_F^\times & \longrightarrow & \bar{F}^\times & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & 1 + \mathfrak{m}_K & \longrightarrow & O_K^\times & \longrightarrow & \bar{K}^\times & \longrightarrow & 1 \end{array}$$

where the vertical arrows are the norm maps. We denote the norm map and the trace map of  $\bar{F}/\bar{K}$  by  $N_{\bar{F}/\bar{K}}$  and  $\text{Tr}_{\bar{F}/\bar{K}}$ , respectively. Take a uniformizer  $\pi$  of  $O_K$ . Then  $\pi$  is a uniformizer of  $O_F$  since  $[F : K] = d = [\bar{F} : \bar{K}]$ . For  $i \in \mathbb{Z}_{>0}$ , the isomorphism  $O_K / \mathfrak{m}_K^i \cong O_F / \mathfrak{m}_F^i$ ,  $a \mapsto a^i$  induces an isomorphism  $\bar{K} / \mathfrak{m}_K^i / \mathfrak{m}_K^{i+1} \cong \bar{K} / \mathfrak{m}_F^i / \mathfrak{m}_F^{i+1}$ . For any  $a \in O_F$  and any  $i \in \mathbb{Z}_{>0}$ , the equality

$$N_{F/K}(1 + a^i) \equiv 1 + i(\text{Tr}_{\bar{F}/\bar{K}} \bar{a}) \pmod{\mathfrak{m}_K^{i+1}}$$

holds, where  $\bar{a}$  is the image of  $a$  in  $\bar{F}$ . Thus, since  $\text{Tr}_{\bar{F}/\bar{K}}$  is surjective, the left vertical arrow is surjective. Since  $N_{\bar{F}/\bar{K}}$  is surjective, the right vertical arrow is surjective. Therefore, the middle vertical arrow is surjective.

Let us consider the diagram of abelian groups with commutative squares and horizontal exact sequences

$$\begin{array}{ccccccc} 1 & \longrightarrow & /O_F^\times & \longrightarrow & /F^\times & \longrightarrow & /Z & \longrightarrow & /1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & /O_K^\times & \longrightarrow & /K^\times & \longrightarrow & /Z & \longrightarrow & /1 \end{array}$$

where the left and middle vertical arrows are the norm maps, the right vertical arrow is the multiplication by  $d$ , and the third horizontal arrows are the valuations. Since the left vertical arrow is surjective, the cokernel of the middle arrow is isomorphic to that of the right vertical arrow, which concludes the proof.

**Proposition 4.12.** — Assume that the following conditions are satisfied:

1.  $E_K$  has toric reduction;
2.  $\bar{K}$  is perfect;
3. there does not exist a Galois extension of  $\bar{K}$  with Galois group  $Z_2^2$ ;
4. the norm map of  $\bar{F}/\bar{K}$  is surjective for any Galois extension  $\bar{F}/\bar{K}$  of degree 2;
5.  $G_{M/K} = Z_2^2$ ;
6.  $P(\ ) = 2$ .

Then there exists a field extension  $K'/K$  in  $M$  of degree 2 such that  $v_{K'} = 0$ .

*Proof.* — Condition 5 implies that  $G_{M/M} = Z_2$ , and  $G_{M/K} = Z_2$  (Proposition 4.7.1). Moreover, we may write  $G_{M/K} = \{e, \sigma_1, \sigma_2, \sigma_3\}$ , where  $e$  is the identity, and  $\sigma_3$  is the generator of  $G_{M/M}$ . For  $i \in \{1, 2, 3\}$ , we set  $a_i := a_{\sigma_i}$ , denote the subgroup generated by  $\sigma_i$  by  $G_i$ , and denote the fixed subfield of  $G_i$  by  $K_i$ . Then  $K_3 = M$ . For any  $a \in T_K(M)$ , the equalities  $\sigma_1 \cdot a = \sigma_1 a^{-1}$ ,  $\sigma_2 \cdot a = \sigma_2 a^{-1}$ , and  $\sigma_3 \cdot a = \sigma_3 a$  hold.

Take  $i \in \{1, 2\}$ . We may take  $e_i \in Z$  so that

$$a_i \cdot \sigma_i a_i^{-1} = q^{e_i}.$$

Taking the valuations of both sides, we obtain the equality  $e_i = 0$ , which implies that  $a_i \in K_i^\times$ . We denote the norm map by  $N_i: (M)^\times \rightarrow K_i^\times$ , and the image of  $K_i^\times$  and  $\text{Im } N_i$  in  $E_K(M)$  by  $Z_i$  and  $B_i$ , respectively. Set  $H_i := Z_i/B_i$ . Since the homomorphisms

$$Z^1(G_i, E_K(M)) \longrightarrow /Z_i, \quad (\bar{b}_g)_g \in G_i \longrightarrow /b_i$$

and

$$B^1(G_i, E_K(M)) \longrightarrow /B_i, \quad (\bar{b}_g)_g \in G_i \longrightarrow /b_i$$

are bijective, the homomorphism

$$H^1(G_i, E_K(M)) \longrightarrow /H_i, \quad (\bar{b}_g)_g \in G_i \longrightarrow /b_i$$

is bijective, where  $b_i$  is the image of  $\overline{b_i}$  in  $H_i$ .

Since

$$a_1 \cdot {}_1a_2^{-1} = a_3 = a_2 \cdot {}_2a_1^{-1} \pmod{Z},$$

the equalities

$$a_1 \cdot {}_2a_1 = a_2 \cdot {}_1a_2 \pmod{Z}$$

and

$$a_3^2 = a_1 \cdot {}_2a_1^{-1} \cdot a_2 \cdot {}_1a_2^{-1} = a_1 \cdot {}_3a_1^{-1} \cdot a_2 \cdot {}_3a_2^{-1} \pmod{Z}$$

hold. For  $i \in \{1, 2\}$ , we set  $b_i := a_i^2 \cdot (a_1 \cdot {}_i a_1)^{-1}$ . We set  $b_e := 1$ ,  $b_3 := a_3^2 \cdot (a_1 \cdot {}_3 a_1^{-1})^{-1}$ , and  $a := a_2$ . Then  $b_1 = 1$ ,  $b_2 = a \cdot {}_1 a^{-1}$ ,  $b_3 = a \cdot {}_3 a^{-1}$ , and the cohomology class of  $(\overline{b_g})_g \in G_{M/K}$  is equal to 2. By Condition 6, we may take  $b \in M$  so that  $b \cdot {}_1 b = 1$ ,  $b \cdot {}_2 b = a \cdot {}_1 a^{-1}$ , and  $b \cdot {}_3 b^{-1} = a \cdot {}_3 a^{-1}$ . The last equality implies that we may take  $e_3 \in Z$  so that

$$a \cdot b^{-1} = {}_3(a \cdot b^{-1}) \cdot q^{e_3}.$$

Taking the valuations of both sides, we obtain the equality  $e_3 = 0$ . Thus, we may take  $c \in M$  so that  $a = bc$ . Since  $N_1 b = 1$ , the equality  $N_1 a = N_1 c$  holds.

We may assume that  $v_{K_i} = 0$  for any  $i \in \{1, 2\}$ . Then  $\overline{a_i} \in B_i$  for any  $i \in \{1, 2\}$ , which implies that  $a_i \in \text{Im } N_i$  for any  $i \in \{1, 2\}$ . By  $v: (M)^\times \rightarrow Z$  we denote the valuation of  $M$  with  $\text{Im } v = Z$ . Condition 1 implies that  $M$  is unramified over  $K$ , which implies that  $M$  is unramified over  $K_i$  for any  $i \in \{1, 2\}$ . Thus, Condition 4 implies that  $\text{Im } N_i = v^{-1}(2Z) \subset K_i^\times$  (Lemmas 4.10 and 4.11), which implies that  $v(a_i) \in 1 + 2Z$ , and  $v(N_1 a) \in 2 + 4Z$ . Conditions 2 and 3 imply that  $v(K^\times) = 2v(K_i^\times)$ , which implies that  $v(M^\times) = 2v((M)^\times) = 2Z$  and  $v(N_1 M^\times) = 4Z$ . Since  $N_1 a = N_1 c$ ,  $v(q) \in 2Z$ ,  $v(N_1 a) \in 2 + 4Z$ , and  $v(N_1 c) \in 4Z$ , we conclude that  $v(q) \in 2 + 4Z$ . The equality  $a_1 \cdot {}_2 a_1 = a_2 \cdot {}_1 a_2$  shows that  $2(v(a_1) - v(a_2)) \in v(q)Z$ . Since  $v(a_1) - v(a_2) \in 2Z$ , we conclude that  $v(a_1) - v(a_2) \in v(q)Z$ . Thus, the equality  $a_3 = a_1 \cdot {}_1 a_2^{-1}$  implies that  $v(a_3) \in v(q)Z$ .

Since  $\text{Im } N_1 = v^{-1}(2Z) \subset K_1^\times$ , we may assume that  $v(a_1) = 1$ . Since  $a_e = 1$ ,  $v(a_1) - v(a_2) \in v(q)Z$ , and  $v(a_3) \in v(q)Z$ , we may assume that  $a_e = 1$ ,  $v(a_2) = 1$ , and  $v(a_3) = 0$ . For any  $g \in G_{M/K}$  and any  $h \in G_{M/K}$ , we may take  $e_{g,h} \in Z$  so that

$$a_{gh} = a_g \cdot (g \cdot a_h) \cdot q^{e_{g,h}}.$$

Since  $v(a_{gh}) = v(a_g) + v(g \cdot a_h)$ , the equality  $e_{g,h} = 0$  holds, which implies that  $a_{gh} = a_g \cdot (g \cdot a_h)$ . Thus, we may take  $H^1(K, T_K) = 0$  so that  $\text{res} = u_K(\text{res})$ . Since  $H^1(M, T_K) = 0$ , the equality  $\text{res}_M = 0$  holds. Therefore, the equality  $\text{res}_M = 0$  holds, which concludes the proof.

**Example 4.13.** — The conclusion of Proposition 4.12 does not hold without Condition 3. Note that Conditions 1–4 are used only in the last two paragraphs of the above proof. Assume that there exists a finite Galois extension  $\overline{F}/\overline{K}$  with  $G_{\overline{F}/\overline{K}} = Z_2^2$ . Then we may take an unramified Galois extension  $M/K$  with  $G_{M/K} = Z_2^2$ . We may write  $G_{M/K} = \{e, \sigma_1, \sigma_2, \sigma_3\}$ , where  $e$  is the identity. For  $i \in \{1, 2, 3\}$ , we denote the subgroup generated by  $\sigma_i$  by  $G_i$ , and the fixed subfield of  $G_i$  by  $K_i$ . Take a uniformizer  $\pi$  of  $O_K$ . Set  $M := K_3$ , and  $q := \pi^4$ . We may take a  $K$ -torus  $T_K$  and a  $K$ -elliptic curve  $E_K$  that satisfy the following conditions:  $T_K$  does not split over  $K$ ,  $T_K$  splits over  $M$ , and  $E_K^{\text{an}} = T_K^{\text{an}} / \pi^{\text{an}}$ , where  $\pi^{\text{an}}$  is the lattice of  $T_K$  induced by  $\{q^i \mid i \in Z\}$  ( $(K^{\text{sep}})^\times = T_K(K^{\text{sep}})$ ). Then  $E_K$  has toric reduction since  $M$  is unramified over  $K$ . Set  $a_e := 1$ ,  $a_{\sigma_1} := \pi$ ,  $a_{\sigma_2} := \pi^3$ ,  $a_{\sigma_3} := \pi^2$ , and  $c := \{\overline{a_g}\}_g \in G_{M/K}$ . Then

$c \in Z^1(G_{M/K}, E_K(M))$ . We define  $\alpha \in H^1(K, E_K)$  as the cohomology class represented by  $c$ . By the above proof, we conclude that  $P(\alpha) = 2$ , and  $\alpha|_{K_i} = 0$  for any  $i \in \{1, 2, 3\}$ .

**Theorem 4.14.** — Assume that the following conditions are satisfied:

1.  $E_K$  has toric reduction;
2.  $\bar{K}$  is perfect;
3. for any finite field extension  $\bar{K}'/\bar{K}$ , there does not exist a Galois extension of  $\bar{K}'$  with Galois group  $Z_2^2$ ;
4. for any finite field extension  $\bar{K}'/\bar{K}$  and any Galois extension  $\bar{F}'/\bar{K}'$  of degree 2, the norm map of  $\bar{F}'/\bar{K}'$  is surjective.

Take  $\alpha \in H^1(K, E_K)$ . Then there exists a separable field extension  $L/K$  of degree  $P(\alpha)$  such that  $\alpha|_L = 0$ .

*Proof.* — By the induction on  $P(\alpha)$ , we may assume that  $P(\alpha)$  is a prime number. If  $P(\alpha) = 2$ , then Proposition 4.8 concludes the proof. Otherwise, by Proposition 4.7, we may assume that  $G_{M/K} = Z_2$ , and  $G_{M'/K} = Z_4$  or  $Z_2^2$ . Thus, Propositions 4.9 and 4.12 conclude the proof.

#### 4.4. Periods and Separable Closed Points. —

**Definition 4.15.** — A field  $k$  is said to be of dimension  $\geq 1$  if one of the following equivalent conditions is satisfied [17, II.3.1, Prop. 5]:

1. for any finite separable field extension  $L/k$ , the Brauer group of  $L$  is trivial;
2. for any finite separable field extension  $L/k$ , the norm map of any finite Galois extension of  $L$  is surjective.

We use the following fact (see the proof of [2, Thm. 27]).

**Lemma 4.16.** — Let  $k$  be a field. Assume that  $k$  is perfect and WC-trivial for elliptic curves. Then  $k$  is of dimension  $\geq 1$ .

*Proof of Theorem 1.6.* — Lemma 4.16 implies that  $\bar{K}$  is of dimension  $\geq 1$ . Thus, the theorem follows from Theorems 4.4 and 4.14.

**Example 4.17.** — A field  $k$  is said to be *quasi-finite* if the absolute Galois group of  $k$  is isomorphic to the profinite completion of  $\mathbb{Z}$ . The WC-triviality for elliptic curves of  $\bar{K}$  is necessary in Theorem 1.6: there exist a complete discrete valuation field  $K$  with perfect quasi-finite residue field, a  $K$ -elliptic curve  $E_K$  with ordinary good reduction, and a non-trivial  $K$ -torsor  $X_K$  under  $E_K$  such that  $P(X_K)^2 \nmid [k(x) : K]$  for any separable closed point  $x$  on  $X_K$  ([10, §4, p. 678] or [1]).

*Acknowledgments.* — The author thanks the referee for helpful comments. He thanks Professor Qing Liu for discussion on indices (§4.1), and l’Institut de Mathématiques de Bordeaux, Université Bordeaux 1 for warm hospitality. This work was supported by the Grant-in-Aid for Young Scientists (B) (25800018) from the JSPS (the Japan Society for the Promotion of Science), the Grant-in-Aid for Scientific Research (S) (24224001) from the JSPS, and the JSPS Program for Advancing Strategic International Networks to Accelerate the Circulation of Talented Researchers based on OCAMI (Osaka City University Advanced Mathematical Institute).

## References

- [1] V. Ī. Andriĭ uk, “The order and index of a principal homogeneous space of an elliptic curve over a general local field”, *Ukr. Mat. Zh.* **27** (1975), p. 62-63.
- [2] P. L. Clark, “The period-index problem in WC-groups IV: a local transition theorem”, *J. Théor. Nombres Bordx.* **22** (2010), no. 3, p. 583-606.
- [3] M. Demazure & A. Grothendieck (eds.), *Schémas en groupes I–III*, Lecture Notes in Mathematics, vol. 151, 152, 153, Springer, 1970, Séminaire de Géométrie Algébrique du Bois Marie 1962–1964 (SGA 3), Avec la collaboration de M. Artin, J.E. Bertin, P. Gabriel, M. Raynaud et J.-P. Serre, xv+564, ix+654, vii+529 pages.
- [4] M. D. Fried & M. Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3., vol. 11, Springer, 2008, Revised by Jarden, xxiv+792 pages.
- [5] O. Gabber, Q. Liu & D. Lorenzini, “The index of an algebraic variety”, *Invent. Math.* **192** (2013), no. 3, p. 567-626.
- [6] S. Greco, “Two theorems on excellent rings”, *Nagoya Math. J.* **60** (1976), p. 139-149.
- [7] A. Grothendieck, “Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas (Seconde partie)”, *Publ. Math., Inst. Hautes Étud. Sci.* **24** (1965), p. 1-231.
- [8] ———, “Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas (Quatrième partie)”, *Publ. Math., Inst. Hautes Étud. Sci.* **32** (1967), p. 1-361.
- [9] S. Lang, “Algebraic groups over finite fields”, *Am. J. Math.* **78** (1956), p. 555-563.
- [10] S. Lang & J. Tate, “Principal homogeneous spaces over abelian varieties”, *Am. J. Math.* **80** (1958), p. 659-684.
- [11] S. Lichtenbaum, “The period-index problem for elliptic curves”, *Am. J. Math.* **90** (1968), p. 1209-1223.
- [12] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, 2002, xv+576 pages.
- [13] Q. Liu, D. Lorenzini & M. Raynaud, “Néron models, Lie algebras, and reduction of curves of genus one”, *Invent. Math.* **157** (2004), no. 3, p. 455-518.
- [14] H. Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, 1989, Translated from the Japanese by M. Reid, xiv+320 pages.
- [15] J. S. Mil ne, “Weil-Châtelet groups over local fields”, *Ann. Sci. Éc. Norm. Supér.* **3** (1970), p. 273-284.

- 
- [16] J.-P. Serre, "Espaces fibrés algébriques (d'après André Weil)", in *Séminaire Bourbaki, Vol. 2*, Société Mathématique de France, 1995, p. 305-311 (Exp. No. 82).
- [17] ———, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author, x+210 pages.
- [18] S. Sharif, "Period and index of genus one curves over global fields", *Math. Ann.* **354** (2012), no. 3, p. 1029-1047.

---

Kentaro Mitsui, Department of Mathematics, Graduate School of Science, Kobe University, Hyogo 657-8501, Japan • *E-mail* : [mitsui@math.kobe-u.ac.jp](mailto:mitsui@math.kobe-u.ac.jp)