Séminaires & Congrès
13, 2006, p. 293–312

GALOIS THEORY OF ZARISKI PRIME DIVISORS

by

Florian Pop

Abstract. — In this paper we show how to recover a special class of valuations (which generalize in a natural way the Zariski prime divisors) of function fields from the Galois theory of the functions fields in discussion. These valuations play a central role in the birational anabelian geometry and related questions.

***Résumé* (Théorie de Galois des diviseurs premiers de Zariski).** — Dans cet article nous montrons comment retrouver une classe spéciale de valuations de corps de fonctions (qui généralisent naturellement les diviseurs premiers de Zariski) à partir de la théorie de Galois des corps de fonctions en question. Ces valuations jouent un rôle central en géométrie anabélienne birationnelle et pour d'autres questions connexes.

1. Introduction

The aim of this paper is to give a first insight into the way the pro-ℓ Galois theory of function fields over algebraically closed base fields of characteristic $\neq \ell$ encodes the Zariski prime divisors of the function fields in discussion. We consider the following context:

- ℓ is a fixed rational prime number.
- $K|k$ are function fields with k algebraically closed of characteristic $\neq \ell$.
- $K(\ell)|K$ is the maximal pro-ℓ Galois extension of K in some separable closure of K, and $G_K(\ell)$ denotes its Galois group.

It is a Program initiated by Bogomolov [**Bog**] at the beginning of the 1990's which has as ultimate goal to recover (the isomorphy type of) the field K from the Galois group $G_K(\ell)$. Actually, Bogomolov expects to recover the field K even from the

2000 *Mathematics Subject Classification.* — Primary 12E, 12F, 12G, 12J; Secondary 12E30, 12F10, 12G99.
Key words and phrases. — Anabelian geometry, function fields, valuations, Zariski prime divisors, Hilbert decomposition theory, pro-ℓ Galois theory.

Supported by NSF grant DMS-0401056.

Galois information encoded in $\mathrm{PGal}^{\mathrm{c}}_K$, which is the quotient of $G_K(\ell)$ by the second factor in its central series. Unfortunately, at the moment we have only a rough idea (maybe a hope) about how to recover the field K from $G_K(\ell)$, and not a definitive answer to the problem. Nevertheless, this program is settled and has a *positive answer,* in the case k is *an algebraic closure of a finite field,* Pop [**Popd**]; see also Bogomolov–Tschinkel [**BTb**] for the case of function fields of smooth surfaces with trivial fundamental group.

It is important to remark that ideas of this type were first initiated by Neukirch, who asked whether the isomorphism type of a number field F is encoded in its absolute Galois group. The final result in this direction is the celebrated result by Neukirch, Iwasawa, Uchida (with previous partial results by Ikeda, Komatsu, etc.) which roughly speaking asserts that the *isomorphy types of global fields are functorially encoded in their absolute Galois groups.* Nevertheless, it turns out that the result above concerning global fields is just a first piece in a very broad picture, namely that of *Grothendieck's anabelian geometry,* see Grothendieck [**Grob**], [**Groa**]. Grothendieck predicts in particular, that the finitely generated infinite fields are functorially encoded in their absolute Galois groups. This was finally proved by the author Pop [**Popc**], [**Popa**]; see also Spiess [**Spi**].

The strategy to prove the above fact is to first develop a "Local theory", which amounts of recovering local type information about a finitely generated field from its absolute Galois group. And then "globalize" the local information in order to finally get the field structure. The local type information consists of recovering the Zariski prime divisors of the finitely generated field. These are the discrete valuations which are defined by the Weil prime divisors of the several normal models of the finitely generated field in discussion.

In this manuscript, we will mimic the Local theory from the case of finitely generated infinite fields, and will develop a geometric pro-ℓ Local theory, whose final aim is to recover the so called quasi-divisorial valuations of a function field $K|k$ form $G_K(\ell)$ – notations as at the beginning of the Introduction. We remark that this kind of results played a key role in Pop [**Popd**], where only the case $k=\overline{\mathbb{F}}_p$ was considered.

We mention here briefly the notions introduced later and the main results proved later in the paper – notations as above.

Let v be some valuation of $K(\ell)$, and for subfields Λ of $K(\ell)$ denote by $v\Lambda$ and Λv the value group, respectively residue field, of the restriction of v to Λ. And let $T_v \subseteq Z_v$ be the inertia, respectively decomposition, group of v in $G_K(\ell) = \mathrm{Gal}\big(K(\ell)|K\big)$.

First recall, see Section 3, A), that a Zariski prime divisor v of $K(\ell)$ is any valuation of $K(\ell)$ whose restriction $v|_K$ to K "comes from geometry", i.e., the valuation ring of $v|_K$ equals the local ring $\mathcal{O}_{X,x_v}$ of the generic point x_v of some Weil prime divisor of some normal model $X \to k$ of $K|k$. Thus $vK \cong \mathbb{Z}$ and $Kv|k$ is a function field satisfying $\mathrm{td}(Kv\,|\,k) = \mathrm{td}(K|k) - 1$. Now it turns out that Z_v has a "nice" structure as follows:

$$T_v \cong \mathbb{Z}_\ell \quad \text{and} \quad Z_v \cong T_v \times G_{Kv}(\ell) \cong \mathbb{Z}_\ell \times G_{Kv}(\ell).$$

We will call the decomposition groups Z_v of Zariski prime divisors v of $K(\ell)|k$ divisorial subgroups of $G_K(\ell)$ or of K.

Now in the case k is an algebraic closure of a finite field, it turns out that a *maximal subgroup of $G_K(\ell)$ which is isomorphic to a divisorial subgroup is actually indeed a divisorial subgroup of $G_K(\ell)$,* see [P4]; this follows nevertheless from Proposition 4.1 of this manuscript, as k has no no-trivial valuations in this case.

On the other hand, if k has positive Kronecker dimension (i.e., it is not algebraic over a finite field), then the situation becomes more intricate, as the non-trivial valuations of k play into the game. Let us say that a valuation v of $K(\ell)$ is a quasi-divisorial valuation, if it is minimal among the valuations of $K(\ell)$ having the properties: $\mathrm{td}(Kv\,|\,kv) = \mathrm{td}(K|k) - 1$ and $vK/vk \cong \mathbb{Z}$, see Definition 3.4, and Fact 5.5, 3). Note that the Zariski prime divisors of $K(\ell)$ are quasi-divisorial valuations of $K(\ell)$.

On the Galois theoretic side we make definitions as follows: Let Z be a closed subgroup of $G_K(\ell)$.

i) We say that Z a divisorial like subgroup of $G_K(\ell)$ or of K, if Z is isomorphic to a divisorial subgroup of some function field $L|l$ such that $\mathrm{td}(L|l) = \mathrm{td}(K|k)$, and l algebraically closed of characteristic $\neq \ell$.

ii) We will say that Z is quasi-divisorial, if Z is divisorial like and maximal among the divisorial like subgroups of $G_K(\ell)$.

Finally, for $t \in K$ a non-constant function, let K_t be the relative algebraic closure of $k(t)$ in K. Thus $K_t|k$ is a function field in one variable, and one has a canonical projection $p_t : G_K(\ell) \to G_{K_t}(\ell)$.

In these notations, the main results of the present manuscript can be summarized as follows, see Proposition 4.1, Key Lemma 4.2, and Proposition 4.6.

Theorem 1.1. — *Let $K|k$ be a function field with $\mathrm{td}(K|k) > 1$, where k is algebraically closed of characteristic $\neq \ell$. Then one has:*

(1) *A closed subgroup $Z \subset G_K(\ell)$ is quasi-divisorial $\iff$ Z is maximal among the subgroups Z' of $G_K(\ell)$ which have the properties:*
   i) *Z' contains closed subgroups isomorphic to $\mathbb{Z}_\ell^d$, where $d = \mathrm{td}(K|k)$.*
   ii) *Z' has a non-trivial pro-cyclic normal subgroup T' such that Z'/T' has no non-trivial Abelian normal subgroups.*

(2) *The quasi-divisorial subgroups of $G_K(\ell)$ are exactly the decomposition groups of the quasi-divisorial valuations of $K(\ell)$.*

(3) *A quasi-divisorial subgroup Z of $G_K(\ell)$ is a divisorial subgroup of $G_K(\ell)$ $\iff$ $p_t(Z)$ is open in $G_{K_t}(\ell)$ for some non-constant $t \in K$.*

Among other things, one uses in the proof some ideas by Ware and Arason–Elman–Jacob, see e.g. Engler–Nogueira [**EN**] for $\ell = 2$, Engler–Koenigsmann [**EK**] in the case $\ell \neq 2$, and/or Efrat [**Efr**] in general. And naturally, one could use here Bogomolov [**Bog**], Bogomolov–Tschinkel [**BTa**]. We would also like to remark that this kind of assertions – and even stronger but more technical ones – might be obtained by employing the local theory developed by Bogomolov [**Bog**], and Bogomolov–Tschinkel [**BTa**].

Concerning applications: Proposition 4.1 plays an essential role in tackling Bogomolov's Program in the case the base field k is an algebraic closure of a global field (and hopefully, in general); and Proposition 4.6 is used in a proof of the so called Ihara/Oda–Matsumoto Conjecture. (These facts will be published soon).

Acknowledgments

I would like to thank the referee for the careful reading of the manuscript and the several suggestions which finally lead to the present form of the manuscript.

2. Basic facts from valuation theory

A) On the decomposition group (See e.g. [End], [Bou], [ZS].)— Consider the following context: $\tilde{K}|K$ is some Galois field extension, and v is a valuation on $\tilde{K}$. For every subfield Λ of $\tilde{K}$ denote by $v\Lambda$ and Λv the valued group, respectively the residue field of Λ with respect to (the restriction of) v on Λ. We denote by $p = \mathrm{char}(\tilde{K}v)$ the residue characteristic. Further let Z_v, T_v, and V_v be respectively the decomposition group, the inertia group, and the ramification group of v in $\mathrm{Gal}(\tilde{K}|K)$, and K^V, K^T, and K^Z the corresponding fixed fields in $\tilde{K}$.

Fact 2.1. — The following are well known facts from Hilbert decomposition, and/or ramification theory for general valuations:

1) $\tilde{K}v\,|\,Kv$ is a normal field extension. We set $G_v := \mathrm{Aut}(\tilde{K}v\,|\,Kv)$. Further, $V_v \subset T_v$ are normal subgroups of Z_v, and one has a canonical exact sequence

$$1 \to T_v \to Z_v \to G_v \to 1\,.$$

One has $v(K^T) = v(K^Z) = vK$, and $Kv = K^Z v$. Further, $K^T v\,|\,Kv$ is the separable part of the normal extension $\tilde{K}v\,|\,Kv$, thus it is the maximal Galois sub-extension of $\tilde{K}v\,|\,Kv$. Further, $K^V\,|\,K^T$ is totally tamely ramified.

2) Let $\mu_{\tilde{K}v}$ denote the group of roots of unity in $\tilde{K}v$. There exists a canonical pairing as follows: $\Psi_{\tilde{K}} : T_v \times v\tilde{K}/vK \to \mu_{\tilde{K}v}$, $(g, vx) \mapsto (gx/x)v$, and the following hold: The left kernel of $\Psi_{\tilde{K}}$ is exactly V_v. The right kernel of $\Psi_{\tilde{K}}$ is trivial if $p = 0$, respectively equals the Sylow p-group of $v\tilde{K}/vK$ if $p > 0$. In particular, T_v/V_v is Abelian, V_v is trivial if $\mathrm{char}(K) = 0$, respectively equals the unique Sylow p-group of T_v if $\mathrm{char}(K) = p > 0$. Further, $\Psi_{\tilde{K}}$ is compatible with the action of G_v.

3) Suppose that $v' \leq v$ is a coarsening of v, i.e., $\mathcal{O}_v \subseteq \mathcal{O}_{v'}$. Then denoting $v_0 = v/v'$ the valuation induced by v on $\tilde{K}v'$, and by Z_{v_0} its decomposition group in $G_{v'} = \mathrm{Aut}(\tilde{K}v'|Kv)$, one has: $T_v \subseteq Z_v$ are the preimages of $T_{v_0} \subseteq Z_{v_0}$ in $Z_{v'}$ via the canonical projection $Z_{v'} \to G_{v'}$. In particular, $T_{v'} \subseteq T_v$ and $Z_v \subseteq Z_{v'}$.

Fact 2.2. — Let ℓ be a rational prime number. In the notations and the context from Fact 2.1 above, suppose that K contains the ℓ^∞ roots of unity, and fix once for all an identification of the Tate ℓ-module of $\mathbb{G}_{m,K}$ with $\mathbb{Z}_\ell(1)$, say

$$\imath : \mathbb{T}_\ell \to \mathbb{Z}_\ell(1).$$

And let the Galois extensions $\tilde{K}|K$ considered at Fact 2.1 satisfy $K^{\ell,\mathrm{ab}} \subseteq \tilde{K} \subseteq K(\ell)$, where $K^{\ell,\mathrm{ab}}$ is the maximal Abelian extension of K inside $K(\ell)$. Finally, we consider valuations v on $\tilde{K}$ such that Kv has characteristic $\neq \ell$. Then by the discussion above we have: $V_v = \{1\}$, and further: $v\tilde{K}$ is the ℓ-divisible hull of vK; and the residue field extension $\tilde{K}v\,|\,Kv$ is separable and also satisfies the properties above we asked for $\tilde{K}|K$ to satisfy.

1) For $n = \ell^e$, there exists a unique sub-extension $K_n|K^T$ of $\tilde{K}|K^T$ such that $K_n|K^Z$ is a Galois sub-extension of $\tilde{K}|K^Z$, and $vK_n = \frac{1}{n}\,vK^T = \frac{1}{n}\,vK$. On the other hand, the multiplication by n induces a canonical isomorphism $\frac{1}{n}\,vK \,/\, vK \cong vK/n$. Therefore, the pairing $\Psi_{\tilde{K}}$ gives rise to a non-degenerate pairing

$$\Psi_n : T_v/n \times vK/n \to \mu_n \xrightarrow{\imath} \mathbb{Z}/n(1),$$

hence to isomorphisms $\theta^{v,n} : vK/n \to \mathrm{Hom}(T_v, \mu_n)$, $\theta_{v,n} : T_v/n \to \mathrm{Hom}(vK, \mu_n)$. In particular, taking limits over all $n = \ell^e$, one obtains a canonical isomorphism of G_v-modules

$$\theta_v : T_v \to \mathrm{Hom}\big(vK, \mathbb{Z}_\ell(1)\big).$$

2) Next let $\mathcal{B} = (vx_i)_i$ be an $\mathbb{F}_\ell$-basis of the vector space $vK\,/\,\ell$. For every x_i, choose a system of roots $(\alpha_{i,n})_n$ in $\tilde{K}$ such that $\alpha_{i,n}^\ell = \alpha_{i,n-1}$ (all $n > 0$), where $\alpha_{i,0} = x_i$. Then setting $K^0 = K[(\alpha_{i,n})_{i,n}] \subset \tilde{K}$, it follows that v is totally ramified in $K^0|K$, and vK^0 is ℓ-divisible. Therefore, $K^0v = Kv$, and the inertia group of v in $\tilde{K}|K^0$ is trivial. In particular, T_v has complements in Z_v, and $T_v \cong \mathbb{Z}_\ell^{\mathcal{B}}(1)$ as G_v-modules.

3) Since by hypothesis $\mu_{\ell^\infty} \subseteq K$, the action of G_v on $\mathbb{Z}_\ell^{\mathcal{B}}(1) \cong T_v$ is trivial. In particular, setting $\delta_v := |\mathcal{B}| = \dim_{\mathbb{F}_\ell}(vK/\ell)$ we finally have:

$$Z_v \cong T_v \times G_v \;\cong\; \mathbb{Z}_\ell^{\delta_v} \times G_v.$$

B) Two results of F. K. Schmidt. — In this subsection we will recall the pro-ℓ form of two important results of F. K. Schmidt and generalizations of these like the ones in Pop [**Popb**], The local theory, A. See also Endler–Engler [**EE**].

Let ℓ be a fixed rational prime number. We consider fields K of characteristic $\neq \ell$ containing the ℓ^∞ roots of unity. For such a field K we denote by $K(\ell)$ a maximal pro-ℓ Galois extension of K. Thus the Galois group of $K(\ell)|K$ is the maximal pro-ℓ