Contemporary Mathematics
Volume **00**, XXXX

information for the AMS-P logo

Regular Realization of Abelian Groups with Controlled Ramification

Pierre Dèbes

Abstract. We prove that given an arbitrary field K, a finite subset $D \subset \mathbb{P}^1(\overline{K})$ and a finite abelian group A, there exists an extension $F/K(T)$ that is regular over K, Galois of group A and such that the extension $\overline{K}F/\overline{K}(T)$ is unramified over each element of D.

1. Result and motivation

Theorem. *Let K be an arbitrary field and $D \subset \mathbb{P}^1(\overline{K})$ be a finite set. For each finite abelian group A, there exists an extension $F/K(T)$ that is regular over K, Galois of group A and such that the extension $\overline{K}F/\overline{K}(T)$ is unramified over each element of D.*

The above result is the goal of this Note. Our motivation initially lay in another problem of realization of groups as Galois groups called the Beckmann-Black problem. E. Black conjectures [**Bl2**] that, given an arbitrary field K, every Galois extension E/K is the specialization of a Galois branched cover of $\mathbb{P}^1$ defined over K and with the same Galois group G. In [**De**] we give a proof of the conjecture in the case the group G is abelian and K is an arbitrary field, which improves on previous results of Beckmann [**Be**] and Black [**Bl1**] where K was assumed to be a number field. Our construction starts with a Galois cover $f : X \to \mathbb{P}^1$ of group G defined over K as G-cover (*i.e.*, along with its automorphisms). Existence of such a cover is classical. However we require further in our proof that the cover has at least one unramified point $t_o \in \mathbb{P}^1(K)$. While this extra condition does not raise any difficulty when K is infinite, it appears that, to my knowledge, no such result on the regular realization of abelian groups with some prescription on the ramification was available in the literature for finite fields.

1991 *Mathematics Subject Classification.* Primary 12F12, 14H30; Secondary 14G20, 11Gxx..

2. Proof of the Theorem

2.1. A preliminary lemma. The following result will be used in the two cases of the proof of the Theorem.

LEMMA. *Let E/K be a finite Galois extension, $D \subset \mathbb{P}^1(\overline{K})$ be a finite set and $n \geq 1$ be an integer. There exist two polynomials $\alpha(T) \in E(T)$ and $\beta(T) \in K(T)$ satisfying the following conditions:*
(i) $\deg(\alpha) = r \geq 1$ *and* $\alpha(0) = 1$,
(ii) α is irreducible and separable over E,
(iii) The coefficient of T in $\alpha(T)$ is a primitive element of the extension E/K,
(iv) $\alpha(d^\gamma) \neq 0$ *for each $d \in D \setminus \{\infty\}$ and each $\gamma \in \mathrm{G}(\overline{K}/K)$,*
(v) $\deg(\beta) = r$,
(vi) $\alpha(T)$ and $\beta(T)$ are relatively prime in $E(T)$, and
(vii) $\beta(T)$ has a nth root in $K((T))$.

PROOF. If K is infinite, take $\alpha(T) = b_1 T + 1$ with b_1 a primitive element of E/K such that $-1/b_1$ is different from all the elements d^γ with $d \in D \setminus \{\infty\}$ and $\gamma \in \mathrm{G}(\overline{K}/K)$. The polynomial $\alpha(T)$ fulfills conditions (i)-(iv). As to conditions (v)-(vii), they are satisfied for any polynomial β of the form $bT+1$ with $b \in K \setminus \{0, b_1\}$.

Assume now that K is finite. Let r_o be an integer bigger than the degrees over E of all elements of $D \setminus \{\infty\}$. Then pick a polynomial $\alpha_o(T) \in E(T)$ of degree $r = nr_o$, irreducible and separable; this is clearly possible: each finite field has a (unique) extension of any given degree. Furthermore, one may take $\alpha_o(T)$ monic and, up to changing T by $T-a$ for some $a \in E$, assume that the coefficient of T^{r-1} in $\alpha_o(T)$ is a primitive element b_1 of E/K. Then the polynomial $\alpha(T) = T^r \alpha_o(1/T)$ satisfies conditions (i)-(iii). Condition (iv) holds as well since the roots of $\alpha(T)$ are of degree r over E. Finally take $\beta(T) = T^{nr_o}$; conditions (v)-(vii) are readily checked. □

2.2. Proof of the Theorem. One easily reduces to the case A is a cyclic group of prime power order. Indeed write A as the direct product of cyclic groups of prime power order. Assuming the result is true for cyclic groups of prime power order, realize a first cyclic factor over $K(T)$ with branch point set Δ_1 disjoint from D. Then realize a second cyclic factor over $K(T)$ with branch point set Δ_2 disjoint from $D \cup \Delta_1$ and proceed inductively. By construction, the obtained field extensions are linearly disjoint (since their branch point sets are pairwise disjoint). The compositum of these extensions is an extension $F/K(T)$ that is regular over K, Galois of group A and such that the extension $\overline{K}F/\overline{K}(T)$ is unramified over each element of D.

From now on, assume A is a cyclic group of order a prime power ℓ^m. Denote the characteristic of K by p. We distinguish two cases.

1st case: $\ell \neq p$ (including $p = 0$). Apart from condition "$F/K(T)$ unramified over each element of D", the result is then proved in Lemma 11.27 of [**Vo**] (which itself relies on some work of D. Saltman [**Sa**]). We will modify the proof to include the ramification condition. We explain below what changes should be made. Notation is that of [**Vo**;Lemma 11.27]; in particular $n = \ell^m$.

The construction starts with an extension of $K(\zeta_n)(T)$ associated with a polynomial of the form $Y^n - g(T)$ (where ζ_n is a primitive n-root of unity and $g(T) \in K(\zeta_n)[T]$ is a certain polynomial (see below)) and consists in showing that the associated cyclic cover of the T-line has a model over K (as G-cover). Only the polynomial $g(T)$ has to be changed in the proof in order to obtain the full conclusion of the Theorem in the considered case.

Set $\Gamma = \mathrm{G}(K(\zeta_n)/K)$ and for each $\gamma \in \Gamma$, select an integer $\chi(\gamma)$ such that $\gamma(\zeta_n) = \zeta_n^{\chi(\gamma)}$; take $\chi(1) = 1$. From the Lemma applied with $E = K(\zeta_n)$, there exists polynomials $\alpha(T) \in E(T)$ and $\beta(T) \in K(T)$ satisfying conditions (i)-(vii) of the Lemma. Then set

$$g(T) = \begin{cases} \prod_{\gamma\in\Gamma} \gamma(\alpha(T))^{\chi(\gamma^{-1})} & \text{if } \infty \notin D \\ \frac{\prod_{\gamma\in\Gamma} \gamma(\alpha(T))^{\chi(\gamma^{-1})}}{\beta(T)^{|\Gamma|}} & \text{if } \infty \in D \end{cases}$$

where each $\gamma \in \Gamma$ acts coefficientwise on polynomials in $K(\zeta_n)[T]$. The polynomial $g(T)$ generalizes the polynomial

$$\prod_{\gamma\in\Gamma} (1 + \gamma(b_1)T)^{\chi(\gamma^{-1})}$$

which is used in the proof of [**Vo**;Lemma 11.27]: $\alpha(T)$ replaces $1 + b_1T$.

It follows from conditions (ii) and (vi) of the Lemma that $\alpha(T)$ and $\alpha(T)/\beta(T)$ are not ℓ-powers in $\overline{K}[T]$. From condition (iii), the polynomials $\gamma(\alpha(T))$ $(\gamma \in \Gamma)$ are pairwise distinct. It follows that $g(T)$ is not a ℓ-power in $\overline{K}[T]$. Conclude that the polynomial $Y^n - g(T)$ is irreducible in $\overline{K}(T)[Y]$. The rest of the argument more or less follows [**Vo**] to conclude that the associated cover of the T-line is cyclic of order n and has a model over K as G-cover. For the convenience of the reader, we reproduce some details from [**Vo**].

Let $v \in K(\zeta_n)((T))$ such that $v^n = \alpha(T)$ (such a v exists since $\alpha(0) = 1$) and $w \in K((T))$ such that $w^n = \beta(T)$ (w exists from the Lemma (condition (vii)). Then

$$u = \begin{cases} \prod_{\gamma\in\Gamma} \gamma(v)^{\chi(\gamma^{-1})} & \text{if } \infty \notin D \\ \frac{\prod_{\gamma\in\Gamma} \gamma(v)^{\chi(\gamma^{-1})}}{w^{|\Gamma|}} & \text{if } \infty \in D \end{cases}$$

lies in $K(\zeta_n)((T))$ and satisfies $u^n = g(T)$. The extension $K(\zeta_n)(T,u)/K(\zeta_n)(T)$ is Galois of degree n and is regular over $K(\zeta_n)$. Its Galois group is the cyclic group $<\omega>$ generated by the $K(\zeta_n)(T)$-automorphism ω determined by $\omega(u) = \zeta_n u$.

Each $\gamma \in \Gamma$ acts on $K(\zeta_n)(T,u)$ *via* its action on $K(\zeta_n)((T))$. For this action, we have

$$\gamma(u) = u^{\chi(\gamma)} f(T) \text{ with } f(T) \in K(\zeta_n)(T)$$

This is a straightforward computation using $\chi(\gamma_1\gamma_2) = \chi(\gamma_1)\chi(\gamma_2)$ [mod n] and $v^n \in K(\zeta_n)(T)$; in particular $\chi(\gamma)\chi(\gamma^{-1}) = 1$ [mod n]. Hence Γ leaves $K(\zeta_n)(T,u)$ invariant. Furthermore we have $(\gamma\omega)(u) = (\omega\gamma)(u)$. Indeed, with $m = \chi(\gamma)$ we obtain

$$(\gamma\omega)(u) = \zeta^m u^m f(T) = \omega(u)^m f(T) = \omega(u^m f(T)) = (\omega\gamma)(u)$$

Let Γ_o be the group of $K(T)$-automorphisms of $K(\zeta_n)(T,u)$ induced by elements of Γ and let Λ be the group generated by Γ_o and ω. We have the diagram

$$\begin{array}{ccc} K(\zeta_n)(T,u)^{\Gamma_o} & \overset{\Gamma_o}{\text{———}} & K(\zeta_n)(T,u) \\ \Big| & & \Big| {<}\omega{>} \\ K(T) & \overset{\Gamma}{\text{———}} & K(\zeta_n)(T) \end{array}$$

Clearly $(K(\zeta_n)(T,u))^\Lambda = K(T)$ whence $|\Lambda| = |\Gamma_o| \cdot |{<}\omega{>}|$. It follows that Λ is the direct product of Γ_o and ${<}\omega{>}$. Conclude that the field $(K(\zeta_n)(T,u))^{\Gamma_o}$ is Galois over $K(T)$ with Galois group isomorphic to ${<}\omega{>}$.

Consider the cover of $\mathbb{P}^1$ associated with the extension $(K(\zeta_n)(T,u))^{\Gamma_o}/K(T)$. Its branch points are contained in the set

$$\begin{cases} \{t \in \overline{K} | g(t) = 0\} \cup \{\infty\} & \text{if } \infty \notin D \\ \{t \in \overline{K} | g(t) = 0\} & \text{if } \infty \in D \end{cases}$$

From condition (iv) of the Lemma, no point $d \in D$ is a branch point of the cover.

2nd case: $\ell = p$. Here again, apart from the ramification condition, the result is fairly classical. We will modify the proof of Lemma 24.42 in [**FrJa**] to include the ramification condition.

From the Lemma applied to $E = K$ and $n = 1$, there exists a polynomial $\alpha \in K(T)$ satisfying conditions (i)-(iv) of this lemma. Then set $\mathcal{O} = K[T, 1/\alpha(T)]$ and $U = \mathrm{Spec}(\mathcal{O})$. From condition (iv) of the Lemma, U is an open subset of $\mathbb{P}^1_K$ such that $D \subset U(\overline{K})$.

The proof goes by induction on m. Take for F_1 the splitting field over $K(T)$ of the polynomial $Y^p - Y - 1/\alpha(T)$. This polynomial has no root in $\overline{K}(T)$. Indeed assume on the contrary that u/v is a root of $Y^p - Y - 1/\alpha(T)$ with $u, v \in \overline{K}[T]$ relatively prime. We obtain

$$v^p = \alpha(u^p - uv^{p-1})$$

From condition (ii), α is irreducible and separable over K. Therefore α necessarily divides v in $\overline{K}[T]$. Simplifying by α in the equality above leads to v^{p-1} divides u^p in $\overline{K}[T]$, a contradiction since $p \geq 2$. Therefore, from additive Kummer's theory (*e.g.* [**La**;Ch.8 §6]), the polynomial $Y^p - Y - 1/\alpha(T)$ is irreducible over $\overline{K}(T)$ and the extension $F_1/K(T)$ is a cyclic extension of degree p, regular over K. Furthermore, the extension $\overline{K}F_1/\overline{K}(T)$ is unramified above each element $t \in \overline{K}$ which is not a pole of $1/\alpha(T)$. In particular, no element of D can be a branch point of the extension $\overline{K}F_1/\overline{K}(T)$.

Suppose next given a cyclic extension $F_m/K(T)$ of degree p^m, regular over K and such that the extension $\overline{K}F_m/\overline{K}(T)$ is unramified over each element of D. Denote by $\widetilde{\mathcal{O}}$ the integral closure of $\mathcal{O}$ in F_m. Also denote the trace function relative to the extension $F_m/K(T)$ by Tr. For each $b \in \widetilde{\mathcal{O}}$, $\mathrm{Tr}(b) \in \mathcal{O}$.

We claim that there exists an element $b_o \in \widetilde{\mathcal{O}}$ such that $\mathrm{Tr}(b_o)(d) \neq 0$ for each $d \in D$. Indeed, by induction hypothesis, the field extension $F_m/K(T)$ and so the ring extension $\widetilde{\mathcal{O}}/\mathcal{O}$ are unramified at each element $d \in D$. Since the ring $\mathcal{O}$ is a p.i.d., the discriminant ideal of $\widetilde{\mathcal{O}}/\mathcal{O}$ is a principal ideal and $\widetilde{\mathcal{O}}$ is a free $\mathcal{O}$-module of rank p^m. More specifically, if $\{x_1, \ldots, x_{p^m}\} \subset \widetilde{\mathcal{O}}$ is a basis of the $\mathcal{O}$-module $\widetilde{\mathcal{O}}$, then the discriminant ideal is generated by

$$\Delta(T) = \det\left((\mathrm{Tr}(x_i x_j))_{i,j}\right)$$

From above, $\Delta(d) \neq 0$ for each $d \in D$. It follows then that for each $d \in D$ at least one of the elements $\mathrm{Tr}(x_i x_j)$ does not vanish at d. This shows that for each $d \in D$, the $\mathcal{O}$-module

$$V_d = \{x \in \widetilde{\mathcal{O}} | \mathrm{Tr}(x)(d) = 0\}$$

is properly contained in $\widetilde{\mathcal{O}}$. The claim follows from the fact that, since $\mathcal{O}$ is infinite, $\widetilde{\mathcal{O}}$ cannot be the union of the finitely many proper sub-modules V_d with $d \in D$.

Set $b = b_o/\mathrm{Tr}(b_o)$ and $\mathcal{P}(b) = b^p - b$; $\mathcal{P}(x) = x^p - x$ is the Artin-Schreier operator. Then $\mathrm{Tr}(b) = 1$ and $\mathrm{Tr}(\mathcal{P}(b)) = \mathrm{Tr}(b)^p - \mathrm{Tr}(b) = 0$. Let σ be a generator of the cyclic group $\mathrm{G}(F_m/K(T))$; from the regularity of the extension F_m/K, σ extends to a generator of the Galois group $\mathrm{G}(\overline{K}F_m/\overline{K}(T))$. From the additive form of Hilbert's Theorem 90 [**La**;Ch.8 §6], there exists $a \in F_m$ such that $a^\sigma - a = b^p - b$. Furthermore, a can be taken to be

$$a = -\mathcal{P}(b)b^\sigma - \mathcal{P}(b + b^\sigma)b^{\sigma^2} - \cdots - \mathcal{P}(b + b^\sigma + \cdots + b^{\sigma^{p^m-2}})b^{\sigma^{p^m-1}}$$

Since b_o is integral over $\mathcal{O} = K[T, 1/\alpha(T)]$, the possible poles of b_o (viewed as a function on the smooth projective model C_m of $\overline{K}F_m$) lie above roots of α (*via* the restriction map T). The same is true for each conjugate $b_o^{\sigma^i}$ of b_o ($i = 0, \ldots, p^m - 1$). In particular, no pole of any of the $b_o^{\sigma^i}$ ($i = 0, \ldots, p^m - 1$) lies above some element of D. Since $\mathrm{Tr}(b_o)(d) \neq 0$ for each $d \in D$, the same is true for all the b^{σ^i} ($i = 0, \ldots, p^m - 1$). Conclude from the form of a that no pole of a lies above some element of D.

Define F_{m+1} to be $F_m(x)$ where x is a zero of the polynomial $Y^p - Y - a$. It follows from $a^\sigma - a = b^p - b$ that the extension F_{m+1} is a proper extension (of degree p) of F_m and that the extension $F_{m+1}/K(T)$ is cyclic of order p^{m+1} and regular over K. This is proved for example [**FrJa**;Ch.24 §8]. For the convenience of the reader, we reproduce the argument.

The first point is that the polynomial $Y^p - Y - a$ has no zero in $\overline{K}F_m$. Indeed otherwise, $Y^p - Y - a = \prod_{i=0}^{p-1}(Y - x - i)$ is totally split in $F_m[Y]$. Then we have

$$\begin{aligned} 0 &= ((x^\sigma)^p - x^\sigma - a^\sigma) - (x^p - x - a) \\ &= (x^\sigma - x)^p - (x^\sigma - x) - (a^\sigma - a) \\ &= (x^\sigma - x)^p - (x^\sigma - x) - (b^p - b) \end{aligned}$$

Since b is a root of $Y^p - Y - (b^p - b)$ there exists an integer i such that $x^\sigma - x = b + i$. Applying the trace function Tr to both sides yields $0 = 1$, a contradiction. This proves the claim. It follows then from [**La**;Ch.8 §6] that the polynomial $Y^p - Y - a$ is irreducible in $\overline{K}F_m$.

The second point consists in extending σ to a $K(T)$-automophism of F_{m+1}. It follows from $a^\sigma - a = b^p - b$ that $x + b$ is a zero of $Y^p - Y - a^\sigma$. Thus there exists a $K(T)$-automorphism σ' of F_{m+1} that extends σ and maps x to $x + b$.

We are left with proving that σ' has order p^{m+1}. An easy induction shows that $(\sigma')^j(x) = x + \sigma^{j-1}b + \sigma^{j-2}b + \cdots + b$ $(j \geq 1)$. Therefore

$$(\sigma')^{p^m}(x) = x + \mathrm{Tr}(b) = x + 1$$

Conclude that σ' is indeed an automorphism of order p^{m+1}.

To finish the second case of the proof, it remains to show that the extension $\overline{K}F_{m+1}/\overline{K}(T)$ is unramified over each element $d \in D$. The branch points of the extension $\overline{K}F_{m+1}/\overline{K}F_m$ are necessarily poles of a (viewed as a function on the smooth projective model C_m of $\overline{K}F_m$). Thus by construction, the extension $\overline{K}F_{m+1}/\overline{K}F_m$ is unramified above each point of C_m lying above some element $d \in D$. Conclude from the induction hypothesis that the extension $\overline{K}F_{m+1}/\overline{K}(T)$ is unramified over each element $d \in D$.

References

[Be] S. Beckmann, *Is every extension of $\mathbb{Q}$ the specialization of a branched covering?*, J. Algebra **164** (1994), 430–451.

[Bl1] E. Black, *Arithmetic lifting of dihedral extensions*, J. Algebra **203** (1998), 12–29.

[Bl2] E. Black, *On semidirect products and arithmetic lifting property*, J. London Math. Soc. (to appear).

[De] P. Dèbes, *Some arithmetic properties of algebraic covers*, preprint.

[FrJa] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin Heildelberg, 1986.

[La] S. Lang, *Algebra*, Addison-Wesley, Reading, 1967.

[Sa] D. Saltman, *Generic Galois extensions and problems in field theory*, Advances in Math. **43** (1982), 250–283.

[Vo] H. Völklein, *Groups as Galois Groups - an Introduction*, Cambridge Univ. Press, 1996.

Mathématiques, Université Lille, 59655 Villeneuve d'Ascq Cedex, France

E-mail address: Pierre.Debes@univ-lille1.fr