Algebra & Number Theory

Volume 4

2010

No. 8

On the minimal ramification problem for semiabelian groups

Hershy Kisilevsky, Danny Neftin and Jack Sonn

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 4:8(2010)

On the minimal ramification problem for semiabelian groups

Hershy Kisilevsky, Danny Neftin and Jack Sonn

It is now known that for any prime p and any finite semiabelian p-group G, there exists a (tame) realization of G as a Galois group over the rationals $\mathbb{Q}$ with exactly $d = \mathrm{d}(G)$ ramified primes, where $\mathrm{d}(G)$ is the minimal number of generators of G, which solves the minimal ramification problem for finite semiabelian p-groups. We generalize this result to obtain a theorem on finite semiabelian groups and derive the solution to the minimal ramification problem for a certain family of semiabelian groups that includes all finite nilpotent semiabelian groups G. Finally, we give some indication of the depth of the minimal ramification problem for semiabelian groups not covered by our theorem.

1. Introduction

Let G be a finite group. Let $d = \mathrm{d}(G)$ be the smallest number for which there exists a subset S of G with d elements such that the normal subgroup of G generated by S is all of G. One observes that if G is realizable as a Galois group $G(K/\mathbb{Q})$ with $K/\mathbb{Q}$ tamely ramified (e.g., if none of the ramified primes divide the order of G), then at least $\mathrm{d}(G)$ rational primes ramify in K (see, e.g., [Kisilevsky and Sonn 2010]). The *minimal ramification problem for* G is to realize G as the Galois group of a tamely ramified extension $K/\mathbb{Q}$ in which exactly $\mathrm{d}(G)$ rational primes ramify. This variant of the inverse Galois problem is open even for p-groups, and no counterexample has been found. It is known that the problem has an affirmative solution for all semiabelian p-groups, for all rational primes p [Neftin 2009; Kisilevsky and Sonn 2010]. A finite group G is *semiabelian* if and only if $G \in \mathcal{SA}$, where $\mathcal{SA}$ is the smallest family of finite groups satisfying (i) every finite abelian group belongs to $\mathcal{SA}$, (ii) if $G \in \mathcal{SA}$ and A is finite abelian, then any semidirect product $A \rtimes G$ belongs to $\mathcal{SA}$, and (iii) if $G \in \mathcal{SA}$, then every homomorphic image of G belongs to $\mathcal{SA}$. In this paper we generalize this result to arbitrary finite semiabelian groups by means of a "wreath product length" $\mathrm{wl}(G)$ of a finite semiabelian group G. When a

Kisilevsky's research was supported in part by a grant from the NSERC.
MSC2000: primary 11R32; secondary 20D15.
Keywords: Galois group, nilpotent group, ramified primes, wreath product, semiabelian group.

finite semiabelian group G is nilpotent, $\mathrm{wl}(G) = \mathrm{d}(G)$, which for nilpotent groups G equals the (more familiar) minimal number of generators of G. Thus the general result does not solve the minimal ramification problem for all finite semiabelian groups, but does specialize to an affirmative solution to the minimal ramification problem for nilpotent semiabelian groups. Note that for a nilpotent group G, $\mathrm{d}(G)$ is $\max_{p\,|\,|G|} \mathrm{d}(G_p)$ and not $\sum_{p\,|\,|G|} \mathrm{d}(G_p)$, where G_p is the p-Sylow subgroup of G. Thus, a solution to the minimal ramification problem for nilpotent groups does not follow trivially from the solution for p-groups.

2. Properties of wreath products

2.1. ***Functoriality.*** The family of semiabelian groups can also be defined using wreath products. Let us recall the definition of a wreath product. Here and throughout the text the actions of groups on sets are all right actions.

Definition 2.1. Let G and H be two groups that act on the sets X and Y, respectively. The (*permutational*) *wreath product* $H \wr_X G$ is the set $H^X \times G = \{(f, g) \mid f : X \to H, g \in G\}$ which is a group with respect to the multiplication

$$(f_1, g_1)(f_2, g_2) = (f_1 f_2^{g_1^{-1}}, g_1 g_2),$$

where $f_2^{g_1^{-1}}$ is defined by $f_2^{g_1^{-1}}(x) = f_2(x g_1)$ for any $g_1, g_2 \in G$, $f_1, f_2 : X \to H$, and $x \in X$. The group $H \wr_X G$ acts on the set $Y \times X$ by $(y, x) \cdot (f, g) = (y f(x), xg)$, for any $y \in Y$, $x \in X$, $f : X \to H$, $g \in G$.

Definition 2.2. The *standard* (or *regular*) *wreath product* $H \wr G$ is defined as the permutational wreath product with $X = G$, $Y = H$, and the right regular actions.

The functoriality of the arguments of a wreath product will play an important role in the sequel. The following five lemmas are devoted to these functoriality properties.

Definition 2.3. Let G be a group that acts on X and Y. A map $\phi : X \to Y$ is called a G-map if $\phi(xg) = \phi(x)g$ for every $g \in G$ and $x \in X$.

Note that for such ϕ, we also have $\phi^{-1}(y)g = \{xg \mid \phi(x) = y\} = \{x' \mid \phi(x' g^{-1}) = y\} = \{x' \mid \phi(x') = yg\} = \phi^{-1}(yg)$.

Lemma 2.4. *Let G be a group that acts on the finite sets X, Y and let A be an abelian group. Then every G-map $\phi : X \to Y$ induces a homomorphism $\tilde{\phi} : A \wr_X G \to A \wr_Y G$ by defining $(\tilde{\phi}(f, g)) = (\hat{\phi}(f), g)$ for every $f : X \to A$ and $g \in G$, where $\hat{\phi}(f) : Y \to A$ is defined by*

$$\hat{\phi}(f)(y) = \prod_{x \in \phi^{-1}(y)} f(x),$$

for every $y \in Y$. Furthermore, if ϕ is surjective then $\tilde{\phi}$ is an epimorphism.

Proof. Let us show the above $\tilde{\phi}$ is indeed a homomorphism. For this we claim $\tilde{\phi}((f_1, g_1)(f_2, g_2)) = \tilde{\phi}(f_1, g_1)\tilde{\phi}(f_2, g_2)$ for every $g_1, g_2 \in G$ and $f_1, f_2 : X \to A$. By definition:

$$\tilde{\phi}(f_1, g_1)\tilde{\phi}(f_2, g_2) = (\hat{\phi}(f_1), g_1)(\hat{\phi}(f_2), g_2) = (\hat{\phi}(f_1)\hat{\phi}(f_2)^{g_1^{-1}}, g_1 g_2),$$

while $\tilde{\phi}((f_1, g_1)(f_2, g_2)) = \tilde{\phi}(f_1 f_2^{g_1^{-1}}, g_1 g_2) = (\hat{\phi}(f_1 f_2^{g_1^{-1}}), g_1 g_2)$. We shall show that $\hat{\phi}(f_1 f_2) = \hat{\phi}(f_1)\hat{\phi}(f_2)$ and $\hat{\phi}(f^g) = \hat{\phi}(f)^g$ for every $f_1, f_2, f : X \to A$ and $g \in G$. Clearly this will imply the claim. The first assertion follows since

$$\hat{\phi}(f_1 f_2)(y) = \prod_{x \in \phi^{-1}(y)} f_1(x) f_2(x) = \prod_{x \in \phi^{-1}(y)} f_1(x) \prod_{x \in \phi^{-1}(y)} f_2(x) = \hat{\phi}(f_1)(y)\hat{\phi}(f_2)(y).$$

As to the second assertion we have

$$\hat{\phi}(f^g)(y) = \prod_{x \in \phi^{-1}(y)} f^g(x) = \prod_{x \in \phi^{-1}(y)} f(xg^{-1}) = \prod_{x'g \in \phi^{-1}(y)} f(x') = \prod_{x' \in \phi^{-1}(y)g^{-1}} f(x').$$

Since ϕ is a G-map we have $\phi^{-1}(y)g^{-1} = \phi^{-1}(yg^{-1})$ and thus

$$\hat{\phi}(f^g)(y) = \prod_{x \in \phi^{-1}(y)g^{-1}} f(x) = \prod_{x \in \phi^{-1}(yg^{-1})} f(x) = \hat{\phi}(f)^g(y).$$

This proves the second assertion and hence the claim. It is left to show that if ϕ is surjective then $\tilde{\phi}$ is surjective. Let $f' : Y \to A$ and $g' \in G$. Let us define an $f : X \to A$ that will map to f'. For every $y \in Y$ choose an element $x_y \in X$ for which $\phi(x_y) = y$ and define $f(x_y) := f'(y)$. Define $f(x) = 1$ for any $x \notin \{x_y \mid y \in Y\}$. Then clearly

$$\hat{\phi}(f)(y) = \prod_{x \in \phi^{-1}(y)} f(x) = f(x_y) = f'(y).$$

Thus, $\tilde{\phi}(f, g') = (\hat{\phi}(f), g') = (f', g')$ and $\tilde{\phi}$ is onto. □

Lemma 2.5. *Let B and C be two groups. Then there is a surjective $B \wr C$-map $\phi : B \wr C \to B \times C$ defined by $\phi(f, c) = (f(1), c)$ for every $f : C \to B, c \in C$.*

Proof. Let $(f, c), (f', c')$ be two elements of $B \wr C$. We check that $\phi((f, c)(f', c')) = \phi(f, c)(f', c')$. Indeed,

$$\begin{aligned}\phi((f, c)(f', c')) &= \phi(f f'^{c^{-1}}, cc') = (f(1) f'^{c^{-1}}(1), cc') = (f(1) f'(c), cc') \\ &= (f(1), c)(f', c) = \phi(f, c)(f', c').\end{aligned}$$

Note that the map ϕ is surjective: For every $b \in B$ and $c \in C$, one can choose a function $f_b : C \to B$ for which $f_b(1) = b$. One has $\phi(f_b, c) = (b, c)$. □

The following lemma appears in [Meldrum 1995, Part I, Chapter I, Theorem 4.13] and describes the functoriality of the first argument in the wreath product.

Lemma 2.6. *Let G, A, B be groups and $h : A \to B$ a homomorphism (resp. epimorphism). Then there is a naturally induced homomorphism (resp. epimorphism) $h_* : A \wr G \to B \wr G$ given by $h_*(f, g) = (h \circ f, g)$ for every $g \in G$ and $f : G \to A$.*

The functoriality of the second argument is given in [Neftin 2009, Lemma 2.15] whenever the first argument is abelian:

Lemma 2.7. *Let A be an abelian group and let $\psi : G \to H$ be a homomorphism (resp. epimorphism) of finite groups. Then there is a homomorphism (resp. epimorphism) $\tilde{\psi} : A \wr G \to A \wr H$ that is defined by $\tilde{\psi}(f, g) = (\hat{\psi}(f), \psi(g))$ with $\hat{\psi}(f)(h) = \prod_{k \in \psi^{-1}(h)} f(k)$ for every $h \in H$.*

These functoriality properties can now be joined to give a connection between different bracketing of iterated wreath products:

Lemma 2.8. *Let A, B, C be finite groups and A abelian. Then there are epimorphisms*

$$A \wr (B \wr C) \to (A \wr B) \wr C \to (A \times B) \wr C.$$

Proof. Let us first construct an epimorphism $h_* : (A \wr B) \wr C \to (A \times B) \wr C$. Define $h : A \wr B \to A \times B$ by

$$h(f, b) = \Bigl(\prod_{x \in B} f(x), b\Bigr),$$

for any $f : B \to A, b \in B$. Since A is abelian h is a homomorphism. For every $a \in A$, let $f_a : B \to A$ be the map $f_a(b') = 0$ for any $1 \neq b' \in B$ and $f_a(1) = a$. Then clearly $h(f_a, b) = (a, b)$ for any $a \in A$, $b \in B$ and hence h is onto. By Lemma 2.6, h induces an epimorphism $h_* : (A \wr B) \wr C \to (A \times B) \wr C$. To construct the epimorphism $A \wr (B \wr C) \to (A \wr B) \wr C$, we shall use the associativity of the permutational wreath product (see [Meldrum 1995, Theorem 3.2]). Using this associativity one has

$$(A \wr B) \wr C = (A \wr_B B) \wr_C C \cong A \wr_{B \times C} (B \wr_C C).$$

It is now left to construct an epimorphism:

$$A \wr (B \wr C) = A \wr_{B \wr C} (B \wr C) \to A \wr_{B \times C} (B \wr C).$$

By Lemma 2.5, there is a $B \wr C$-map $\phi : B \wr C \to B \times C$ and hence by Lemma 2.4 there is an epimorphism $A \wr_{B \wr C} (B \wr C) \to A \wr_{B \times C} (B \wr C)$. □

Let us iterate Lemma 2.8. Let $G_1, \ldots, G_n$ be groups. The *ascending iterated standard wreath product* of $G_1, \ldots, G_n$ is defined as

$$\bigl(\cdots((G_1 \wr G_2) \wr G_3) \wr \cdots\bigr) \wr G_n,$$

and the *descending iterated standard wreath product* of $G_1, \ldots, G_n$ is defined as

$$G_1 \wr (G_2 \wr (\cdots \wr (G_{n-1} \wr G_n) \cdots)).$$

These two iterated wreath products are not isomorphic in general, as the standard wreath product is not associative (as opposed to the permutation wreath product). We shall abbreviate and write $G_1 \wr (G_2 \wr \cdots \wr G_n)$ to refer to the descending wreath product and $(G_1 \wr \cdots \wr G_{r-1}) \wr G_r$ to refer to the ascending wreath product.

By iterating the epimorphism in Lemma 2.8 one obtains

Corollary 2.9. *Let $A_1, \dots, A_r$ be abelian groups. Then $(A_1 \wr \cdots \wr A_{r-1}) \wr A_r$ is an epimorphic image of $A_1 \wr (A_2 \wr \cdots \wr A_r)$.*

Proof. By induction on r. The cases $r = 1, 2$ are trivial; assume $r \geq 3$. By the induction hypothesis there is an epimorphism

$$\pi_1' : A_1 \wr (A_2 \wr \cdots \wr A_{r-1}) \to (A_1 \wr \cdots \wr A_{r-2}) \wr A_{r-1}.$$

By Lemma 2.6, π_1' induces an epimorphism $\pi_1 : (A_1 \wr (A_2 \wr \cdots \wr A_{r-1})) \wr A_r \to (A_1 \wr \cdots \wr A_{r-1}) \wr A_r$. Applying Lemma 2.8 with $A = A_1$, $B = A_2 \wr (A_3 \wr \cdots \wr A_{r-1})$, and $C = A_r$, one obtains an epimorphism

$$\pi_2 : A_1 \wr (A_2 \wr \cdots \wr A_r) \to (A_1 \wr (A_2 \wr \cdots \wr A_{r-1})) \wr A_r.$$

Taking the composition $\pi = \pi_1 \pi_2$ one obtains an epimorphism

$$\pi : A_1 \wr (A_2 \wr \cdots \wr A_r) \to (A_1 \wr \cdots \wr A_{r-1}) \wr A_r. \qquad \square$$

2.2. ***Dimension under epimorphisms.*** Let us examine how the "dimension" d behaves under the homomorphisms in Lemma 2.8 and Corollary 2.9. By [Kaplan and Lev 2003, Theorem 2.1], for any finite group G that is not perfect, i.e., $[G, G] \neq G$, where $[G, G]$ denotes the commutator subgroup of G, one has $\mathrm{d}(G) = \mathrm{d}(G/[G, G])$. According to our definitions, for a perfect group G, $\mathrm{d}(G/[G, G]) = \mathrm{d}(\{1\}) = 0$, but if G is nontrivial, $\mathrm{d}(G) \geq 1$. As nontrivial semiabelian groups are not perfect, this difference will not affect any of the arguments in the sequel.

Definition 2.10. Let G be a finite group and p a prime. Define $\mathrm{d}_p(G)$ to be the rank of the p-Sylow subgroup of $G/[G, G]$, i.e., $\mathrm{d}_p(G) := \mathrm{d}((G/[G, G])(p))$.

Note that if G is not perfect one has $\mathrm{d}(G) = \max_p(\mathrm{d}_p(G))$.

Let p be a prime. An epimorphism $f : G \to H$ is called d-preserving (resp. d_p-preserving) if $\mathrm{d}(G) = \mathrm{d}(H)$ (resp. $\mathrm{d}_p(G) = \mathrm{d}_p(H)$).

Lemma 2.11. *Let G and H be two finite groups. Then*:

$$H \wr G/[H \wr G, H \wr G] \cong H/[H, H] \times G/[G, G].$$

Proof. Applying Lemmas 2.6 and 2.7 one obtains an epimorphism

$$H \wr G \to H/[H, H] \wr G/[G, G].$$

By Lemma 2.8 (applied with $C = 1$) there is an epimorphism

$$H/[H,H] \wr G/[G,G] \to H/[H,H] \times G/[G,G].$$

Composing these epimorphisms one obtains an epimorphism

$$\pi : H \wr G \to H/[H,H] \times G/[G,G],$$

that sends an element $(f : G \to H, g) \in H \wr G$ to

$$\Big(\prod_{x \in G} f(x)[H,H], g[G,G]\Big) \in H/[H,H] \times G/[G,G].$$

The image of π is abelian and hence $\ker(\pi)$ contains $K := [H \wr G, H \wr G]$.

Let us show $K \supseteq \ker(\pi)$. Let $(f, g) \in \ker(\pi)$. Then $g \in [G,G]$ and $\prod_{x \in G} f(x) \in [H,H]$. As $g \in [G,G]$, it suffices to show that the element $f = (f, 1) \in H \wr G$ is in K. Let $g_1, \dots, g_n$ be the elements of G, and for every $i = 1, \dots, n$ let f_i be the function for which $f_i(g_i) = f(g_i)$ and $f(g_j) = 1$ for every $j \neq i$. One can write f as $\prod_{i=1}^n f_i$. Now for every $i = 1, \dots, n$, the function $f_{1,i} = f_i^{g_i^{-1}}$ satisfies $f_{1,i}(1) = f(g_i)$ and $f_{1,i}(g_j) = 1$ for every $j \neq 1$. Thus f_i is a product of an element in $[H^{|G|}, G]$ and $f_{i,1}$. So, f is a product of elements in $[H^{|G|}, G]$ and $f' = \prod_{i=1}^n f_{1,i}$. But $f'(1) = \prod_{x \in G} f(x) \in [H,H]$ and $f'(g_i) = 1$ for every $i \neq 1$ and hence $f' \in [H^{|G|}, H^{|G|}]$. Thus, $f \in K$ as required and $K = \ker \pi$. □

The following is an immediate conclusion:

Corollary 2.12. *Let G and H be two finite groups. Then*

$$\mathrm{d}_p(H \wr G) = \mathrm{d}_p(H) + \mathrm{d}_p(G)$$

for any prime p.

So, for groups A, B, C as in Lemma 2.8, we have

$$\mathrm{d}_p(A \wr (B \wr C)) = \mathrm{d}_p((A \times B) \wr C) = \mathrm{d}_p(A \times B \times C) = \mathrm{d}_p(A) + \mathrm{d}_p(B) + \mathrm{d}_p(C)$$

for every p. In particular, the epimorphisms in Lemma 2.8 are d-preserving.

The same observation holds for Corollary 2.9, so one has:

Lemma 2.13. *Let $A_1, \dots, A_r$ be finite abelian groups. Then*

$$\mathrm{d}_p(A_1 \wr (A_2 \wr \cdots \wr A_r)) = \mathrm{d}_p((A_1 \wr \cdots \wr A_{r-1}) \wr A_r) = \mathrm{d}_p(A_1 \times \cdots \times A_r)$$

are all $\sum_{i=1}^r \mathrm{d}_p(A_i)$ for any prime p.

For cyclic groups $A_1, \dots, A_r$, $\mathrm{d}_p(A_1 \wr (A_2 \wr \cdots \wr A_r))$ is simply the number of cyclic groups among $A_1, \dots, A_r$ whose p-part is nontrivial. Thus:

Corollary 2.14. *Let $C_1, \dots, C_r$ be finite cyclic groups and $G = C_1 \wr (C_2 \wr \cdots \wr C_r)$. Then* $\mathrm{d}(G) = \max_{p \mid |G|} \mathrm{d}\big(C_1(p) \wr (C_2(p) \wr \cdots \wr C_r(p))\big)$.

Let us apply Lemma 2.8 in order to connect between descending iterated wreath products of abelian and cyclic groups:

Proposition 2.15. *Let $A_1, \dots, A_r$ be finite abelian groups and let A_i have invariant factors $C_{i,j}$ for $j = 1, \dots, l_i$, i.e., $A_i = \prod_{j=1}^{l_i} C_{i,j}$ and $|C_{i,j}|$ divides $|C_{i,j+1}|$ for $i = 1, \dots, r$ and $j = 1, \dots, l_i - 1$. There is an epimorphism from the descending iterated wreath product $\tilde{G} := \wr_{i=1}^{r} \wr_{j=1}^{l_i} C_{i,j}$ (where the groups $C_{i,j}$ are ordered lexicographically: $C_{1,1}, C_{1,2}, \dots, C_{1,l_1}, C_{2,1}, \dots, C_{r,l_r}$) to $G := A_1 \wr (A_2 \wr \cdots \wr A_r)$.*

Proof. Assume $A_1 \neq \{0\}$ (otherwise A_1 can be simply omitted). Let us prove the assertion by induction on $\sum_{i=1}^{r} l_i$. Let $G_2 = A_2 \wr (A_3 \wr \cdots \wr A_k)$. Write $A_1 = C_{1,1} \times A_1'$. By Lemma 2.8, there is an epimorphism

$$\pi_1 : C_{1,1} \wr (A_1' \wr G_2) \to (C_{1,1} \times A_1') \wr G_2 = A_1 \wr G_2 = G.$$

By applying the induction hypothesis to $A_1', A_2, \dots, A_r$, there is an epimorphism π_2' from the descending iterated wreath product $\tilde{G}_2 = \wr_{j=2}^{l_1} C_{1,j} \wr (\wr_{i=2}^{r} \wr_{j=1}^{l_i} C_{i,j})$ to $A_1' \wr G_2$. By Lemma 2.7, π_2' induces an epimorphism $\pi_2 : C_{1,1} \wr \tilde{G}_2 \to C_{1,1} \wr (A_1' \wr G_2)$. Taking the composition $\pi = \pi_2 \pi_1$, we obtain the required epimorphism: $\pi : \tilde{G} = C_{1,1} \wr \tilde{G}_2 \to G$. □

Remark 2.16. Note that

$$\mathrm{d}_p(\tilde{G}) = \sum_{i=1}^{r} \sum_{j=1}^{l_i} \mathrm{d}_p(C_{i,j}) = \sum_{i=1}^{r} \mathrm{d}_p(A_i) = \mathrm{d}_p(G)$$

for every p and hence π is d-preserving.

Therefore, showing G is a d-preserving epimorphic image of an iterated wreath product of abelian groups is equivalent to showing G is a d-preserving epimorphic image of an iterated wreath product of finite cyclic groups.

3. Wreath length

The following lemma is essential for the definition of wreath length:

Lemma 3.1. *Let G be a finite semiabelian group. Then G is a homomorphic image of a descending iterated wreath product of finite cyclic groups, i.e., there are finite cyclic groups $C_1, \dots, C_r$ and an epimorphism $C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$.*

Proof. By Proposition 2.15 it suffices to show G is an epimorphic image of a descending iterated wreath product of finite abelian groups. We prove this by induction on $|G|$, the case $G = \{1\}$ being trivial. By Theorem 2.3 of [Dentzer 1995], we have $G = A_1 H$ with A_1 an abelian normal subgroup and H a proper semiabelian subgroup of G. First, there is an epimorphism

$$\pi_1 : A_1 \wr H \to A_1 H = G.$$

By induction there are abelian groups $A_2, \dots, A_r$ and an epimorphism $\pi_2' : A_2 \wr (A_3 \wr \cdots \wr A_r) \to H$. By Lemma 2.6, π_2' can be extended to an epimorphism $\pi_2 : A_1 \wr (A_2 \wr \cdots \wr A_r) \to A_1 \wr H$. So, by taking the composition $\pi = \pi_1 \pi_2$ one obtains the required epimorphism $\pi : A_1 \wr (A_2 \wr \cdots \wr A_r) \to G$. □

Definition 3.2. Let G be a finite semiabelian group. Define the *wreath length* $\mathrm{wl}(G)$ of G to be the smallest positive integer r such that there are finite cyclic groups $C_1, \dots, C_r$ and an epimorphism $C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$.

Let $\tilde{G} = C_1 \wr (C_2 \wr \cdots \wr C_r)$ and $\pi : \tilde{G} \to G$ an epimorphism. Then, by Corollary 2.14,

$$\mathrm{d}(G) \le \mathrm{d}(\tilde{G}) \le r.$$

In particular $\mathrm{d}(G) \le \mathrm{wl}(G)$.

Proposition 3.3. *Let $C_1, \dots, C_r$ be nontrivial finite cyclic groups. Then*

$$\mathrm{wl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) = r.$$

Let $\mathrm{dl}(G)$ denote the derived length of a (finite) solvable group G, i.e., the smallest positive integer n such that the n-th higher commutator subgroup of G (the n-th element in the derived series $G = G^{(0)} \ge G^{(1)} = [G, G] \ge \cdots \ge G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \ge \cdots$) is trivial. In order to prove this proposition we will use the following lemma:

Lemma 3.4. *Let $C_1, \dots, C_r$ be nontrivial finite cyclic groups. Then*

$$\mathrm{dl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) = r.$$

Proof. It is easy (by induction) to see that $\mathrm{dl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) \le r$. We turn to the reverse inequality. By Corollary 2.9, it suffices to prove it for the ascending iterated wreath product $G = (C_1 \wr \cdots \wr C_{r-1}) \wr C_r$. We prove this by induction on r. The case $r = 1$ is trivial. Assume $r \ge 1$. Write $G_1 := (C_1 \wr \cdots \wr C_{r-2}) \wr C_{r-1}$ so that $G = G_1 \wr C_r$. By the induction hypothesis, $\mathrm{dl}(G_1) = r - 1$. View G as the semidirect product $G_1^r \rtimes C_r$. For any $g \in G_1$, the element $t_g := (g, g^{-1}, 1, 1, \dots, 1) \in G_1^r$ lies in $[G_1^r, C_r]$ and hence in $[G_1^r, C_r] \le G' \le G_1^r$. Let $H = \{t_g \mid g \in G_1\}$. The projection map $G_1^r \to G_1$ onto the first copy of G_1 in G_1^r maps H onto G_1. Since $H \le G'$, the projection map also maps G' onto G_1. Now $\mathrm{dl}(G_1) = r - 1$ by the induction hypothesis. It follows that $\mathrm{dl}(G') \ge r - 1$, whence $\mathrm{dl}(G) \ge r$. □

Proof of Proposition 3.3. We first observe that $\mathrm{wl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) \le r$ by definition. If $C_1 \wr (C_2 \wr \cdots \wr C_r)$ were a homomorphic image of a shorter descending iterated wreath product $C_1' \wr (C_2' \wr \cdots \wr C_s')$, then by Lemma 3.4,

$$s = \mathrm{dl}(C_1' \wr (C_2' \wr \cdots \wr C_s')) \ge \mathrm{dl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) = r > s,$$

a contradiction. □

Combining Proposition 3.3 with Corollary 2.14 we have:

Corollary 3.5. *Let $C_1, \dots, C_r$ be finite cyclic groups and $G = C_1 \wr (C_2 \wr \cdots \wr C_r)$. Then* $\mathrm{wl}(G) = \mathrm{d}(G)$ *if and only if there is a prime p for which $p \mid |C_1|, \dots, |C_r|$.*

All examples of groups G with $\mathrm{wl}(G) = \mathrm{d}(G)$ arise from Corollary 3.5:

Proposition 3.6. *Let G be a finite semiabelian group. Then* $\mathrm{wl}(G) = \mathrm{d}(G)$ *if and only if there is a prime p, finite cyclic groups $C_1, \dots, C_r$ for which $p \mid |C_i|$, $i = 1, \dots, r$, and a* d*-preserving epimorphism $\pi : C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$.*

Proof. Let $d = \mathrm{d}(G)$. The equality $d = \mathrm{wl}(G)$ holds if and only if there are finite cyclic groups $C_1, C_2, \dots, C_d$ and an epimorphism $\pi : \tilde{G} = C_1 \wr (C_2 \wr \cdots \wr C_d) \to G$. Assume the latter holds. Clearly $d \le \mathrm{d}(\tilde{G})$ but by Corollary 2.14 applied to $\tilde{G}$ we also have $\mathrm{d}(\tilde{G}) \le d$. It follows that π is d-preserving. Since $\mathrm{d}(G) = \max_p(\mathrm{d}_p(G))$, there is a prime p for which $d = \mathrm{d}_p(G)$ and hence $\mathrm{d}_p(\tilde{G}) = d$. Thus, $p \mid |C_i|$ for all $i = 1, \dots, r$.

Let us prove the converse. Assume there is a prime p, finite cyclic groups $C_1, \dots, C_r$ for which $p \mid |C_i|$, $i = 1, \dots, r$, and a d-preserving epimorphism $\pi : \tilde{G} := C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$. Since $p \mid |C_i|$, it follows that $\mathrm{d}_p(\tilde{G}) = r$. As $\mathrm{d}_p(\tilde{G}) \le \mathrm{d}(\tilde{G}) \le r$, it follows that $\mathrm{d}(G) = \mathrm{d}(\tilde{G}) = r$. In particular $\mathrm{wl}(G) \le r = \mathrm{d}(G)$ and hence $\mathrm{wl}(G) = \mathrm{d}(G)$. □

Remark 3.7. Let G be a semiabelian p-group. By [Neftin 2009, Corollary 2.15], G is a d-preserving image of an iterated wreath product of abelian subgroups of G (following the proof one can observe that the abelian groups were actually subgroups of G). So, by Proposition 2.15, G is a d-preserving epimorphic image of $\tilde{G} := C_1 \wr (C_2 \wr \cdots \wr C_k)$ for cyclic subgroups $C_1, \dots, C_k$ of G. By applying Proposition 3.6 one obtains $\mathrm{wl}(G) = \mathrm{d}(G)$.

Remark 3.8. Throughout the proof of [Neftin 2009, Corollary 2.15] one can use the minimality assumption posed on the decompositions to show directly that the abelian groups $A_1, \dots, A_r$, for which there is a d-preserving epimorphism $A_1 \wr (A_2 \wr \cdots \wr A_r) \to G$, can be actually chosen to be cyclic.

We generalize Remark 3.7 to nilpotent groups:

Proposition 3.9. *Let G be a finite nilpotent semiabelian group. Then* $\mathrm{wl}(G) = \mathrm{d}(G)$.

Proof. Let $d = \mathrm{d}(G)$. Let $p_1, \dots, p_k$ be the primes dividing $|G|$ and let P_i be the p_i-Sylow subgroup of G for every $i = 1, \dots, k$. So, $G \cong \prod_{i=1}^k P_i$. By Remark 3.7, there are cyclic p_i-groups $C_{i,1}, \dots, C_{i,r_i}$ and a d-preserving epimorphism $\pi_i : C_{i,1} \wr (C_{i,2} \wr \cdots \wr C_{i,r_i}) \to P_i$ for every $i = 1, \dots, k$. In particular for any $i = 1, \dots, k$, $r_i = \mathrm{d}(P_i) = \mathrm{d}_p(G) \le d$. For any $i = 1, \dots, k$ and any $d \ge j > r_i$, set $C_{i,j} = \{1\}$. For any $j = 1, \dots, d$ define $C_j = \prod_{i=1}^k C_{i,j}$.

We claim G is an epimorphic image of $\tilde{G} = C_1 \wr (C_2 \wr \cdots \wr C_d)$. To prove this claim it suffices to show every P_i is an epimorphic image of $\tilde{G}$ for every $i = 1, \ldots, k$. As $C_{i,j}$ is an epimorphic image of C_j for every $j = 1, \ldots, d$ and every $i = 1, \ldots, k$, one can apply Lemmas 2.6 and 2.7 iteratively to obtain an epimorphism $\pi_i' : \tilde{G} \to C_{i,1} \wr (C_{i,2} \wr \cdots \wr C_{i,r})$ for every $i = 1, \ldots, k$. Taking the composition $\pi_i' \pi_i$ gives the required epimorphism and proves the claim. As G is an epimorphic image of an iterated wreath product of $\mathrm{d}(G)$ cyclic groups one has $\mathrm{wl}(G) \le \mathrm{d}(G)$ and hence $\mathrm{wl}(G) = \mathrm{d}(G)$. □

Example 3.10. Let $G = D_n = \langle \sigma, \tau \mid \sigma^2 = 1, \tau^n = 1, \sigma\tau\sigma = \tau^{-1} \rangle$ for $n \ge 3$. Since G is an epimorphic image of $\langle \tau \rangle \wr \langle \sigma \rangle$ and G is not abelian we have $\mathrm{wl}(G) = 2$. On the other hand $\mathrm{d}(G) = \mathrm{d}(G/[G, G])$ is 1 if n is odd and 2 if n is even. So, $G = D_3 = S_3$ is the minimal example for which $\mathrm{wl}(G) \ne \mathrm{d}(G)$.

4. A ramification bound for semiabelian groups

Theorem 4.1. *Let G be a finite semiabelian group. Then there exists a tamely ramified extension $K/\mathbb{Q}$ with $G(K/\mathbb{Q}) \cong G$ in which at most $\mathrm{wl}(G)$ primes ramify.*

The proof relies on the splitting lemma from [Kisilevsky and Sonn 2010]: Let ℓ be a rational prime, K a number field, and $\mathfrak{p}$ a prime of K that is prime to ℓ. Let $I_{K,\mathfrak{p}}$ denote the group of fractional ideals prime to $\mathfrak{p}$, let $P_{K,\mathfrak{p}}$ denote the subgroup of principal ideals that are prime to $\mathfrak{p}$, and let $P_{K,\mathfrak{p},1}$ be the subgroup of principal ideals (α) with $\alpha \equiv 1 \pmod{\mathfrak{p}}$. Let $\bar{P}_{\mathfrak{p}}$ denote $P_{K,\mathfrak{p}}/P_{K,\mathfrak{p},1}$. The ray class group $Cl_{K,\mathfrak{p}}$ is defined to be $I_{K,\mathfrak{p}}/P_{K,\mathfrak{p},1}$. Now, as $I_{K,\mathfrak{p}}/P_{K,\mathfrak{p}} \cong Cl_K$, one has the short exact sequence

$$1 \longrightarrow \bar{P}_{\mathfrak{p}}^{(\ell)} \longrightarrow Cl_{K,\mathfrak{p}}^{(\ell)} \longrightarrow Cl_K^{(\ell)} \longrightarrow 1, \tag{4-1}$$

where $A^{(\ell)}$ denotes the ℓ-primary component of an abelian group A. Let us describe a sufficient condition for the splitting of (4-1). Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \in I_{K,\mathfrak{p}}$, and let $\tilde{\mathfrak{a}}_1, \ldots, \tilde{\mathfrak{a}}_r$ be their classes in $Cl_{K,\mathfrak{p}}^{(\ell)}$ with images $\bar{\mathfrak{a}}_1, \ldots, \bar{\mathfrak{a}}_r$ in $Cl_K^{(\ell)}$, so that $Cl_K^{(\ell)} = \langle \bar{\mathfrak{a}}_1 \rangle \times \langle \bar{\mathfrak{a}}_2 \rangle \times \cdots \times \langle \bar{\mathfrak{a}}_r \rangle$. Let $\ell^{m_i} := |\langle \bar{\mathfrak{a}}_i \rangle|$ and let $a_i \in K$ satisfy $\mathfrak{a}_i^{\ell^{m_i}} = (a_i)$, for $i = 1, \ldots, r$.

Lemma 4.2 [Kisilevsky and Sonn 2006]. *Let $\mathfrak{p}$ be a prime of K and let $K' = K(\sqrt[\ell^{m_i}]{a_i} \mid i = 1, \ldots, r)$. If $\mathfrak{p}$ splits completely in K' then the sequence (4-1) splits.*

The splitting of (4-1) was used in [Kisilevsky and Sonn 2010] to construct cyclic ramified extensions at one prime only. Let $m = \max\{1, m_1, \ldots, m_r\}$. Let U_K denote the units in $\mathbb{O}_K$.

Lemma 4.3 [Kisilevsky and Sonn 2010]. *Let $K'' = K(\mu_{\ell^m}, \sqrt[\ell^m]{\xi}, \sqrt[\ell^{m_i}]{a_i} \mid \xi \in U_K, i = 1, \ldots, r)$ and let $\mathfrak{p}$ be a prime of K which splits completely in K''. Then there is a cyclic ℓ^m-extension of K that is totally ramified at $\mathfrak{p}$ and is not ramified at any other prime of K.*

Corollary 4.4. *Let K be a number field, n a positive integer. Then there exists a finite extension K''' of K such that if $\mathfrak{p}$ is any prime of K that splits completely in K''', then there exists a cyclic extension L/K of degree n in which $\mathfrak{p}$ is totally ramified and $\mathfrak{p}$ is the only prime of K that ramifies in L.*

Proof. Let $n = \prod_\ell \ell^{m(\ell)}$ be the decomposition of n into primes. Let K''' be the composite of the fields $K'' = K''(\ell)$ in Lemma 4.3 ($m = m(\ell)$). Let $L(\ell)$ be the cyclic extension of degree $\ell^{m(\ell)}$ yielded by Lemma 4.3. The composite $L = \prod L(\ell)$ has the desired property. □

Proof of Theorem 4.1. By definition, G is a homomorphic image of a descending iterated wreath product of cyclic groups $C_1 \wr (C_2 \wr \cdots \wr C_r)$, $r = \mathrm{wl}(G)$. Without loss of generality $G \cong C_1 \wr (C_2 \wr \cdots \wr C_r)$ is itself a descending iterated wreath product of cyclic groups. Proceed by induction on r. For $r = 1$, G is cyclic of order, say, N. If p is a rational prime $\equiv 1 \pmod N$, then the field of p-th roots of unity $\mathbb{Q}(\mu_p)$ contains a subfield L cyclic over $\mathbb{Q}$ with Galois group G and exactly one ramified prime, namely p. Thus the theorem holds for $r = 1$.

Assume $r > 1$ and the theorem holds for $r - 1$. Let $K_1/\mathbb{Q}$ be a tamely ramified Galois extension with $G(K_1/\mathbb{Q}) \cong G_1$, where G_1 is the descending iterated wreath product $C_2 \wr (C_3 \wr \cdots \wr C_r)$, such that the ramified primes in K_1 are a subset of $\{p_2, \ldots, p_r\}$. By Corollary 4.4, there exists a prime $p = p_1$ not dividing the order of G which splits completely in K_1''', the field supplied for K_1 by Corollary 4.4, and let $\mathfrak{p} = \mathfrak{p}_1$ be a prime of K_1 dividing p. By Corollary 4.4, there exists a cyclic extension L/K_1 with $G(L/K_1) \cong C_1$ in which $\mathfrak{p}$ is totally ramified and in which $\mathfrak{p}$ is the only prime of K_1 which ramifies in L.

Now $\mathfrak{p}$ has $|G_1|$ distinct conjugates $\{\sigma(\mathfrak{p}) \mid \sigma \in G(K_1/\mathbb{Q})\}$ over K_1. For each $\sigma \in G(K_1/\mathbb{Q})$, the conjugate extension $\sigma(L)/K_1$ is well-defined, since $K_1/\mathbb{Q}$ is Galois. Let M be the composite of the $\sigma(L)$, $\sigma \in G(K_1/\mathbb{Q})$. For each σ, $\sigma(L)/K_1$ is cyclic of degree $|C_1|$, ramified only at $\sigma(\mathfrak{p})$, and $\sigma(\mathfrak{p})$ is totally ramified in $\sigma(L)/K_1$. It now follows (see, e.g., [Kisilevsky and Sonn 2010, Lemma 1]) that the fields $\{\sigma(L) \mid \sigma \in G(K_1/\mathbb{Q})\}$ are linearly disjoint over K_1, hence $G(M/\mathbb{Q}) \cong C_1 \wr G_1 \cong G$. Since the only primes of K_1 ramified in M are $\{\sigma(\mathfrak{p}) \mid \sigma \in G(K_1/\mathbb{Q})\}$, the only rational primes ramified in M are $p_1, p_2, \ldots, p_n$. □

Corollary 4.5. *The minimal ramification problem has a positive solution for all finite semiabelian groups G for which* $\mathrm{wl}(G) = \mathrm{d}(G)$. *Precisely, any finite semiabelian group G for which* $\mathrm{wl}(G) = \mathrm{d}(G)$ *can be realized tamely as a Galois group over the rational numbers with exactly* $\mathrm{d}(G)$ *ramified primes.*

By Proposition 3.9, we have:

Corollary 4.6. *The minimal ramification problem has a positive solution for all finite nilpotent semiabelian groups.*

5. Arithmetic consequences

In this section we examine some arithmetic consequences of a positive solution to the minimal ramification problem. Specifically, given a group G, the existence of infinitely many minimally tamely ramified G-extensions $K/\mathbb{Q}$ is reinterpreted in some cases in terms of some open problems in algebraic number theory. We will be most interested in the case $\mathrm{d}(G) = 1$.

Proposition 5.1. *Let q and ℓ be distinct primes. Let $K/\mathbb{Q}$ be a cyclic extension of degree $n := [K : \mathbb{Q}] \geq 2$ with $(n, q\ell) = 1$. Suppose that $K/\mathbb{Q}$ is totally and tamely ramified at a unique prime $\mathfrak{l}$ dividing ℓ. Then q divides the class number h_K of K if and only if there exists an extension L/K satisfying the following*:

(1) *$L/\mathbb{Q}$ is a Galois extension with* nonabelian *Galois group $G = G(L/\mathbb{Q})$.*

(2) *The degree $[L : K] = q^s$ is a power of q.*

(3) *$L/\mathbb{Q}$ is (tamely) ramified only at primes over ℓ.*

Proof. First suppose that q divides h_K. Let K_0 be the q-Hilbert class field of K, i.e., K_0/K is the maximal unramified abelian q-extension of K. Then $K_0/\mathbb{Q}$ is a Galois extension with Galois group $G := G(K_0/\mathbb{Q})$, and $H := G(K_0/K) \simeq (C_K)_q \neq 0$, the q-part of the ideal class group of K. Then $[G, G]$ is contained in H. If $[G, G] \subsetneq H$, then the fixed field of $[G, G]$ would be an abelian extension of $\mathbb{Q}$ which contains an unramified q-extension of $\mathbb{Q}$, which is impossible. Hence $[G, G] = H \neq 0$ and so G is a nonabelian group, and $L = K_0$ satisfies (1), (2), and (3) of the statement.

Conversely suppose that there is an extension L/K satisfying (1), (2), and (3) of the statement. Since $H = G(L/K)$ is a q-group, there is a sequence of normal subgroups $H = H_0 \supset H_1 \supset H_2 \cdots \supset H_s = 0$ with H_i/H_{i+1} a cyclic group of order q. Let L_i denote the fixed field of H_i so that $K = L_0 \subset \cdots \subset L_s = L$. Let m be the largest index such that $L_m/\mathbb{Q}$ is totally ramified (necessarily at ℓ). If $m = s$, then $L/\mathbb{Q}$ is totally and tamely ramified at ℓ and so the inertia group $T(\mathfrak{L}/(\ell)) = G$, where in this case $\mathfrak{L}$ is the unique prime of L dividing ℓ. Since $L/\mathbb{Q}$ is tamely ramified it follows that $T(\mathfrak{L}/(\ell))$ is cyclic, but this contradicts the hypothesis that G is nonabelian. Therefore it follows that $m < s$, and so L_{m+1}/L_m is unramified and therefore q must divide the class number h_{L_m}. Then a result of [Iwasawa 1956] implies that q divides all of the class numbers $h_{L_{m-1}}, \ldots, h_{L_0} = h_K$. $\square$

We now apply this to the case that $G \neq \{1\}$ is a quotient of the regular wreath product $C_q \wr C_p$ where p and q are distinct primes. Then $\mathrm{d}(G) = 1$.

The existence of infinitely many minimally tamely ramified G-extensions $L/\mathbb{Q}$ would by Proposition 5.1 imply the existence of infinitely many cyclic extensions $K/\mathbb{Q}$ of degree $[K : \mathbb{Q}] = p$ ramified at a unique prime $\ell \neq p, q$ for which q divides the class number h_K. (If there were only finitely many distinct such cyclic extensions $K/\mathbb{Q}$, then the number of ramified primes ℓ would be bounded, and there would be an absolute upper bound on the possible discriminants of the distinct fields $L/\mathbb{Q}$. By Hermite's theorem, this would mean that the number of such G-extensions $L/\mathbb{Q}$ would be bounded).

The question of whether there is an infinite number of cyclic degree p extensions (or even one) of $\mathbb{Q}$ whose class number is divisible by q is in general open at this time.

For $p=2$, it is known that there are infinitely many quadratic fields (see [Ankeny and Chowla 1955]), with class numbers divisible by q, but it is not known that this occurs for quadratic fields with prime discriminant.

This latter statement is also a consequence of Schinzel's hypothesis as is shown in [Plans 2004]. There is also some numerical evidence that the heuristic of Cohen-Lenstra should be statistically independent of the primality of the discriminant [Jacobson et al. 1995; te Riele and Williams 2003]. If this were true, then one would expect that there is a positive density of primes ℓ for which the cyclic extension of degree p and conductor ℓ would have class number divisible by q.

For $p=3$ it has been proved in [Bhargava 2005] that there are infinitely many cubic fields $K/\mathbb{Q}$ for which 2 divides their class numbers. That there are infinitely many cyclic cubics with prime squared discriminants whose class numbers are even (or more generally divisible by some fixed prime q) seems out of reach at this time.

In our view, there is significant arithmetic interest in solving the minimal ramification problem for other groups. See also [Harbater 1994; Jones and Roberts 2008; Rabayev 2009].

References

[Ankeny and Chowla 1955] N. C. Ankeny and S. Chowla, "On the divisibility of the class number of quadratic fields", *Pacific J. Math.* **5** (1955), 321–324. MR 19,18f Zbl 0065.02402

[Bhargava 2005] M. Bhargava, "The density of discriminants of quartic rings and fields", *Ann. of Math.* (2) **162**:2 (2005), 1031–1063. MR 2006m:11163 Zbl 1159.11045

[Dentzer 1995] R. Dentzer, "On geometric embedding problems and semiabelian groups", *Manuscripta Math.* **86**:2 (1995), 199–216. MR 96c:12006 Zbl 0836.12002

[Harbater 1994] D. Harbater, "Galois groups with prescribed ramification", pp. 35–60 in *Arithmetic geometry* (Tempe, AZ, 1993), edited by N. Childress and J. W. Jones, Contemp. Math. **174**, Amer. Math. Soc., Providence, RI, 1994. MR 96a:12008 Zbl 0815.11053

[Iwasawa 1956] K. Iwasawa, "A note on class numbers of algebraic number fields", *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258. MR 18,644d Zbl 0074.03002

[Jacobson et al. 1995] M. J. Jacobson, Jr., R. F. Lukes, and H. C. Williams, "An investigation of bounds for the regulator of quadratic fields", *Experiment. Math.* **4** (1995), 211–225. MR 97d:11173 Zbl 0859.11057

[Jones and Roberts 2008] J. W. Jones and D. P. Roberts, "Number fields ramified at one prime", pp. 226–239 in *Algorithmic number theory*, edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, Berlin, 2008. MR 2010b:11152 Zbl 05279289

[Kaplan and Lev 2003] G. Kaplan and A. Lev, "On the dimension and basis concepts in finite groups", *Comm. Algebra* **31**:6 (2003), 2707–2717. MR 2004f:20060 Zbl 1038.20020

[Kisilevsky and Sonn 2006] H. Kisilevsky and J. Sonn, "Abelian extensions of global fields with constant local degree", *Math. Res. Lett.* **13**:4 (2006), 599–605. MR 2007e:11130 Zbl 1158.11045

[Kisilevsky and Sonn 2010] H. Kisilevsky and J. Sonn, "On the minimal ramification problem for ℓ-groups", *Compos. Math.* **146**:3 (2010), 599–606. MR 2644928 Zbl 1197.11150

[Meldrum 1995] J. D. P. Meldrum, *Wreath products of groups and semigroups*, Pitman Monographs and Surveys in Pure and Applied Mathematics **74**, Longman, Harlow, 1995. MR 97j:20030 Zbl 0833.20001

[Neftin 2009] D. Neftin, "On semiabelian p-groups", preprint, 2009. arXiv 0908.1472v2

[Plans 2004] B. Plans, "On the minimal number of ramified primes in some solvable extensions of $\mathbb{Q}$", *Pacific J. Math.* **215**:2 (2004), 381–391. MR 2005d:12005 Zbl 1064.11072

[Rabayev 2009] D. Rabayev, *Polynomials with roots mod n for all n*, Master's Thesis, Technion, 2009.

[te Riele and Williams 2003] H. te Riele and H. Williams, "New computations concerning the Cohen–Lenstra heuristics", *Experiment. Math.* **12** (2003), 99–113. MR 2005d:11183 Zbl 1050.11096

Communicated by Hendrik W. Lenstra
Received 2009-12-20 Revised 2010-06-24 Accepted 2010-08-01

kisilev@mathstat.concordia.ca *Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve Blvd West, Montreal, QC H3G 1M8, Canada*

neftind@tx.technion.ac.il *Department of Mathematics, Technion – Israel Institute of Technology, 32000 Haifa, Israel*
http://www.technion.ac.il/~neftind/

sonn@math.technion.ac.il *Department of Mathematics, Technion – Israel Institute of Technology, 32000 Haifa, Israel*
http://www.math.technion.ac.il/~sonn/

Algebra & Number Theory

www.jant.org

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA
Dave Benson	University of Aberdeen, Scotland
Richard E. Borcherds	University of California, Berkeley, USA
John H. Coates	University of Cambridge, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France
Brian D. Conrad	University of Michigan, USA
Hélène Esnault	Universität Duisburg-Essen, Germany
Hubert Flenner	Ruhr-Universität, Germany
Edward Frenkel	University of California, Berkeley, USA
Andrew Granville	Université de Montréal, Canada
Joseph Gubeladze	San Francisco State University, USA
Ehud Hrushovski	Hebrew University, Israel
Craig Huneke	University of Kansas, USA
Mikhail Kapranov	Yale University, USA
Yujiro Kawamata	University of Tokyo, Japan
János Kollár	Princeton University, USA
Hendrik W. Lenstra	Universiteit Leiden, The Netherlands
Yuri Manin	Northwestern University, USA
Barry Mazur	Harvard University, USA
Susan Montgomery	University of Southern California, USA
Shigefumi Mori	RIMS, Kyoto University, Japan
Andrei Okounkov	Princeton University, USA
Raman Parimala	Emory University, USA
Victor Reiner	University of Minnesota, USA
Karl Rubin	University of California, Irvine, USA
Peter Sarnak	Princeton University, USA
Michael Singer	North Carolina State University, USA
Ronald Solomon	Ohio State University, USA
Vasudevan Srinivas	Tata Inst. of Fund. Research, India
J. Toby Stafford	University of Michigan, USA
Bernd Sturmfels	University of California, Berkeley, USA
Richard Taylor	Harvard University, USA
Ravi Vakil	Stanford University, USA
Michel van den Bergh	Hasselt University, Belgium
Marie-France Vignéras	Université Paris VII, France
Kei-Ichi Watanabe	Nihon University, Japan
Andrei Zelevinsky	Northeastern University, USA
Efim Zelmanov	University of California, San Diego, USA

PRODUCTION

ant@mathscipub.org

Silvio Levy, Scientific Editor

Andrew Levy, Production Editor

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2010 is US $140/year for the electronic version, and $200/year (+$30 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
http://www.mathscipub.org
A NON-PROFIT CORPORATION
Typeset in LaTeX

Copyright ©2010 by Mathematical Sciences Publishers

Algebra & Number Theory

Volume 4 No. 8 2010