Answer to a question on $A'$-groups arisen from the study of Steinitz classes

Alessandro Cobbe · Maurizio Monge

Received 7 July, 2013 / Accepted 2 June, 2014 / Published online: 22 July 2014
© Fondation Carl-Herz and Springer International Publishing Switzerland 2014

Abstract In this short note we provide an answer to a question in group theory raised in [2]. In that paper the author describes the set of realizable Steinitz classes for so-called $A'$-groups of odd order, obtained by iterating some direct and semidirect products. It is clear from the definition that $A'$-groups are solvable $A$-groups, but the author left as an open question whether or not the converse is true. In this note we prove the converse when only two prime numbers divide the order of the group and we show that it is false in general, by exhibiting a family of counterexamples of metabelian $A'$-groups whose order is divisible by exactly three primes. Steinitz classes which are realizable for the groups in this family are computed and we verify that they form a group.

Résumé Dans cette note, nous répondons à une question de théorie des groupes posée dans [2]. Dans cet article, l’auteur décrit l’ensemble des classes de Steinitz réalisables pour les $A'$-groupes d’ordre impair, obtenus par produits directs et semidirects à partir des groupes abéliens. Il découle de leur définition que les $A'$-groupes sont des $A$-groupes résolubles, et l’auteur pose la question de savoir si la réciproque est vraie. Nous répondons positivement à cette question lorsque l’ordre du groupe est divisible par deux nombres premiers, et nous montrons que la réponse est négative en général, en produisant une famille de contre-exemples via des groupes métabéliens d’ordre divisible par exactement trois nombres premiers. Les classes de Steinitz réalisables pour les groupes de cette famille sont calculées et nous vérifions qu’elles forment un groupe.

Keywords Steinitz classes · $A'$-groups · Class groups of algebraic number fields · Solvable groups · Metabelian groups

Mathematics Subject Classification 20F16

A. Cobbe (✉) · M. Monge
Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy
e-mail: a.cobbe@sns.it
M. Monge
e-mail: maurizio.monge@sns.it
1 Introduction

Let $K/k$ be an extension of number fields with rings of integers $\mathcal{O}_K$ and $\mathcal{O}_k$ respectively. Then there exists an ideal $I$ of $\mathcal{O}_k$ such that

$$\mathcal{O}_K \cong \mathcal{O}_k^{[K:k]−1} \oplus I$$

as $\mathcal{O}_k$-modules where the ideal $I$ is determined up to principal ideals. Its class in the ideal class group $\text{Cl}(\mathcal{O}_k)$ of $\mathcal{O}_k$ is called the Steinitz class of the extension and is denoted by $\text{st}(K/k)$. For a fixed number field $k$ and a finite group $G$ one can consider the set of classes which arise as Steinitz classes of tame Galois extensions with Galois group $G$, i.e., as the set

$$\mathcal{R}_t(k, G) = \{ c \in \text{Cl}(k) : \exists K/k \text{ Galois and tame, } \text{Gal}(K/k) \cong G, \ c = \text{st}(K/k) \}.$$  

A description of $\mathcal{R}_t(k, G)$ is not known in general, but there are a lot of known results for some particular groups. These results lead to the conjecture that $\mathcal{R}_t(k, G)$ is always a subgroup of the ideal class group, which however has not yet been proved in general. In [2] the author defined $A'$-groups in the following way and proved the above conjecture for all $A'$-groups of odd order.

**Definition 1.1** We define $A'$-groups inductively:

1. Finite abelian groups are $A'$-groups.
2. If $G$ is an $A'$-group and $H$ is a finite abelian group of order prime to that of $G$, then $H \rtimes \mu G$ is an $A'$-group, for any action $\mu$ of $G$ on $H$.
3. If $G_1$ and $G_2$ are $A'$-groups, then $G_1 \times G_2$ is an $A'$-group.

Let us recall the definition of $A$-groups; see [4,5] for some general results about $A$-groups.

**Definition 1.2** An $A$-group is a finite group with the property that all of its Sylow subgroups are abelian.

Clearly (see [2, Proposition 1.2]) every $A'$-group is a solvable $A$-group, though it was asked whether the converse is true. In this short note we find a family of counterexamples for this question. In the last section we show how the techniques from [2] can also be applied for the calculation of the realizable Steinitz classes for these groups, showing in particular that $\mathcal{R}_t(k, G)$ is still a subgroup of the ideal class group and confirming the general conjecture.

2 Solvable $A$-groups which are not $A'$-groups

We start showing a positive result when only two primes divide the order of an $A$-group.

**Proposition 2.1** An $A$-group $G$ having order divisible by at most two different primes is an $A'$-group.

**Proof** Indeed, let $G$ be an $A$-group with order divisible only by the primes $p$ and $q$; it is always solvable by Burnside Theorem. By Hall-Higman Theorem [4, Satz VI.14.16] a solvable $A$-group has derived length at most equal to the number of distinct prime divisors of the order, so in our case $G$ has derived length at most 2 and $G'$ is abelian. If the derived length is 1 then $G$ is abelian, so we are reduced to considering the case of derived length exactly 2.
We will consider the unique subgroup $K_p$ such that $K_pG'/G'$ is the $p$-Sylow of $G/G'$ and $K_p \cap G'$ is the $q$-Sylow of $G'$ and we will show that it is normal in $G$. By Schur-Zassenhaus Theorem it is an $A'$-group, being the semidirect product of an abelian $q$-group by an abelian $p$-group. We construct analogously $K_q$, with $p$ and $q$ exchanged. Then

$$K_p \cap K_q \cap G' = 1$$

since it is contained both in the $p$-Sylow and in the $q$-Sylow of $G'$. Analogously, we also have

$$(K_pG' \cap K_qG')/G' = K_pG'/G' \cap K_qG'/G' = 1$$

and it follows that $K_p \cap K_q \subseteq G'$, and hence we have that $K_p \cap K_q = 1$. We also see that

$$K_pK_q \cap G' = G',$$

since $K_pK_q \cap G'$ is a subgroup containing both the $p$-Sylow and the $q$-Sylow subgroup of $G'$. Similarly

$$K_pK_qG'/G' = G/G'$$

and hence we deduce that $K_pK_q$ is all of $G$. Therefore $K_p$ and $K_q$ are direct factors of $G$, since, as announced above, we will prove that they are normal. Since $K_p$ and $K_q$ are $A'$-groups, we conclude that $G$ is an $A'$-group by rule 3.

To construct $K_p$, let us quotient out the $q$-Sylow $S_q$ of $G'$, obtaining the group $\tilde{G} = G/S_q$. The inverse image of the $p$-Sylow of $G/G'$ under the projection

$$G/S_q \longrightarrow G/G'$$

is the $p$-Sylow $\tilde{P}$ of $\tilde{G} = G/S_q$. Therefore the $p$-Sylow $\tilde{P}$ of $\tilde{G}$ is a normal subgroup of $\tilde{G}$. So we have the exact sequence

$$1 \rightarrow \tilde{P} \rightarrow \tilde{G} \rightarrow \tilde{G}/\tilde{P} \rightarrow 1,$$

and furthermore $\tilde{G}'$ is equal to $G'/S_q$ because $S_q \subseteq G'$, and is contained in $\tilde{P}$, since $\tilde{G}/\tilde{P}$ is abelian.

Now $\tilde{G}'$ has a complementary factor in $\tilde{P}$ which is invariant under the action by conjugation of the $q$-group $\tilde{G}/\tilde{P}$ by $[3$, Theorem 2.3, Chap. 5], so let us assume $\tilde{P} = \tilde{G}' \times F_p$, say. Clearly $F_p$ is a $p$-group which is normal in $\tilde{G}$, and $F_p\tilde{G}'/\tilde{G}'$ is the $p$-Sylow of $\tilde{G}/\tilde{G}' = G/G'$. So if we put $K_p$ to be the preimage of $F_p$ under the projection $G \longrightarrow \tilde{G}$, we have that $K_p$ is normal in $G$, $K_pG'/G'$ is the $p$-Sylow of $G/G'$, and $K_p \cap G'$ is the $q$-Sylow $S_q$ of $G'$, being the preimage of $F_p \cap \tilde{G}' = 1$. \hfill $\Box$

For any triple $p, q, r$ of distinct primes we construct now a counterexample which is a metabelian group. For any integer $n$ let $C_n$ be the cyclic group of $n$ elements.

Let $a, b$ be integers such that

$$qr | p^a - 1 \text{ and } pr | q^b - 1,$$

or equivalently such that

$$\text{ord}_{qr}(p) | a \text{ and } \text{ord}_{pq}(q) | b.$$

Let $\mathbb{F}_p^\times$ and $\mathbb{F}_q^\times$ respectively be the fields with $p^a$ and $q^b$ elements. Then the multiplicative groups $\mathbb{F}_p^\times$ and $\mathbb{F}_q^\times$ act naturally as automorphisms on the additive groups $\mathbb{F}_p^\times$ and $\mathbb{F}_q^\times$. If

$$\phi : C_q \hookrightarrow \mathbb{F}_p^\times \text{ and } \psi : C_p \hookrightarrow \mathbb{F}_q^\times$$

$\bigcirc$ Springer
are embeddings, we can consider the semidirect products

\[ H_1 = \mathbb{F}_p^+ \rtimes \phi C_q, \quad H_2 = \mathbb{F}_q^+ \rtimes \psi C_p. \]

Let us also consider embeddings

\[ \rho_1 : C_r \hookrightarrow \mathbb{F}_p^+, \quad \rho_2 : C_r \hookrightarrow \mathbb{F}_q^+. \]

Since \( \mathbb{F}_p^+ \) and \( \mathbb{F}_q^+ \) are abelian groups, the actions induced by \( C_r \) on \( \mathbb{F}_p^+ \) and \( \mathbb{F}_q^+ \) commute with those of \( C_q \) and \( C_p \), so \( \rho_1, \rho_2 \) induce an action of \( C_r \) on \( H_1 \) and \( H_2 \) which is trivial on \( C_p \) and \( C_q \).

We define

\[ G = (H_1 \times H_2) \rtimes_{\rho_1, \rho_2} C_r, \]

where \( C_r \) acts on \( H_j \) via \( \rho_j \), for \( j = 1, 2 \). Let

\[ \iota_j : C_j \longrightarrow G \quad \text{for} \quad j = p, \ q, \ r, \]

be the canonical injections of \( C_p, C_q \) and \( C_r \) into \( G \) given by the definition of \( G \) as a semidirect product.

**Proposition 2.2** The group \( G = (H_1 \times H_2) \rtimes_{\rho_1, \rho_2} C_r \) is a metabelian A-group which is not an \( A' \)-group.

**Proof** Indeed, \( G \) is metabelian because \( \mathbb{F}_p^+ \rtimes \mathbb{F}_q^+ \) is a normal abelian subgroup with abelian quotient isomorphic to \( C_q \times C_p \times C_r \).

To show that \( G \) cannot be obtained by applying rule 2 in the inductive definition of the \( A' \)-groups, we prove that no Sylow subgroup is normal. Since \( (r, p) = 1 \), a \( p \)-Sylow \( P \) is contained in \( H_1 \times H_2 \), and if \( P \) is normal then \( H_2 \cap P \) would be normal in \( H_2 \) too. However a \( p \)-Sylow in \( \mathbb{F}_q^+ \rtimes C_p \) is isomorphic to \( C_p \) and clearly cannot be normal, or it would be complemented by the normal subgroup isomorphic to \( \mathbb{F}_q^+ \). \( H_2 \) would be abelian, which is not the case. The same holds for the \( q \)-Sylow of \( H_1 \), and similarly an \( r \)-Sylow of \( G \), which is isomorphic to \( C_r \), cannot be normal unless \( G \cong (H_1 \times H_2) \times C_r \) and all elements of order \( r \) would be contained in the center of \( G \), which is not the case.

To conclude we just need to show that \( G \) is not a direct product, so it also cannot be obtained applying rule 3. Suppose \( G = G_1 \times G_2 \). Then exactly one of \( G_1, G_2 \) has order divisible by \( r \), so assume \( r \mid |G_1| \), and we have that \( G_1 \) contains all \( r \)-Sylow subgroups, so in particular \( \iota_r(C_r) \subseteq G_1 \). Then \( G_2 \) is contained in the centralizer of \( \iota_r(C_r) \), which considering the definition of \( G \) we can see to be

\[ \iota_r(C_r)G_2 \iota_r(C_r) \cong C_r \times C_q \times C_r. \]

However, \( r \nmid |G_2| \). If \( p \nmid |G_2| \), we would have \( \iota_p(C_p) \subseteq G_2 \) and \( \iota_p(C_p) \) would be the \( p \)-Sylow, and hence a characteristic subgroup of \( G_2 \), and consequently normal in \( G \), which is absurd. Since we can prove similarly that \( q \nmid |G_2| \) we obtain \( G_2 = 1 \).

We remark that some of the smallest counterexamples are those obtained by putting \((p, q, r; a, b)\) respectively equal to \((5, 2, 3; 2, 4)\) and \((13, 3, 2; 1, 3)\). The groups produced have orders respectively 12, 000 and 27, 378, and are already a bit too far away to be found via a brute force computer search, as was performed by the author of [2].
3 Realizable Steinitz classes

Let $k$ be a number field and $G$ be a finite group. For any $\tau \in G$, let $N_G(\tau)$ be the normalizer of the subgroup of $G$ generated by $\tau$ and let

$$\varphi_\tau : N_G(\tau) \rightarrow (\mathbb{Z}/o(\tau)\mathbb{Z})^\times$$

be defined by $\varphi_\tau(\sigma) = \alpha$, where $\sigma \tau \sigma^{-1} = \tau^\alpha$ and $o(\tau)$ is the order of $\tau$. Furthermore, let

$$\psi_{k,\tau} : \text{Gal}(k(\zeta_{o(\tau)})/k) \rightarrow (\mathbb{Z}/o(\tau)\mathbb{Z})^\times$$

be the cyclotomic character. Then we call $E_{k,G,\tau}$ the fixed subfield of $v_{k,\tau}^{-1}(\varphi_\tau(N_G(\tau)))$ in $k(\zeta_{o(\tau)})$ and we define $\mathcal{W}(k, G)$, a subgroup of $\text{Cl}(k)$ in one of the following equivalent ways (see [1, Proposition 2.8 and Definition 2]):

(i) $\mathcal{W}(k, G) = \prod_{\tau \in G^*} W(k, E_{k,G,\tau})^{(\frac{o(\tau)-1}{2})\#G/o(\tau)^\times}$

(ii) $\mathcal{W}(k, G) = \prod_{\ell \mid \#G} \prod_{\sigma \in G(\ell)^*} W(k, E_{k,G,\sigma})^{(\frac{s-1}{2})\#G/o(\sigma)^\times}$

where the first product in (ii) ranges over all prime numbers $\ell$ dividing the order of $G$, $G(\ell)^*$ is the set of all non-trivial elements of $G$ whose order is a power of $\ell$. For any extension $K/k$ of number fields, we have $W(k, K) = N_{K/k}(\text{Cl}(K))$.

In [1, Theorem 2.10] it has been shown that $R_t(k, G) \subseteq \mathcal{W}(k, G)$ and that there is an equality whenever $G$ is an $A'$-group of odd order [1, Theorem 4.3]. So it is a natural question to investigate whether the equality holds for the solvable $A'$-groups constructed above, which are not $A'$-groups, when $p, q, r$ are all odd prime numbers.

**Proposition 3.1** Let $p, q, r$ be odd prime numbers, let $G$ be defined as in the previous section and let $k$ be a number field. Then

$$R_t(k, G) = \mathcal{W}(k, G).$$

**Proof** As mentioned above, the inclusion

$$R_t(k, G) \subseteq \mathcal{W}(k, G)$$

is true in general and was proved in [1, Theorem 2.10]. To reverse the inclusion, we will use the notation and will rely on the main results of [1].

We note that $G$ can be written as a semidirect product of the form $H \rtimes G$, where

$$H = \mathbb{F}_{p^a}^+ \times \mathbb{F}_{p^b}^+ \quad \text{and} \quad G = C_p \times C_q \times C_r.$$

Let $\pi : G \rightarrow G$ be the usual projection. Then by [1, Theorem 3.5] and [1, Proposition 4.3] (applied to $G$), we obtain

$$R_t(k, G) \supseteq \mathcal{W}(k, G)^{\#H} \prod_{\ell \mid \#H} \prod_{\tau \in H(\ell)^*} W(k, E_{k,G,\tau})^{((\ell-1)/2)(\#G/o(\tau))}.$$  

So it suffices to show that

$$\mathcal{W}(k, G) \subseteq \mathcal{W}(k, G)^{\#H} \prod_{\ell \mid \#H} \prod_{\tau \in H(\ell)^*} W(k, E_{k,G,\tau})^{((\ell-1)/2)(\#G/o(\tau))}. \quad (1)$$
For any prime number $\ell$ dividing $\#G$, the $\ell$-Sylow subgroups of $G$ have exponent $\ell$, i.e., for all $\tau \in G[\ell]^*$, the order of $\tau$ is exactly $\ell$. So let $\tau \in G$ be of order $\ell$. Then we have two possibilities.

Firstly, suppose that $\pi(\tau)$ is of order $\ell$. Then for any element $\sigma$ of the normalizer of $\tau$, we have $\sigma \tau \sigma^{-1} = \tau^i$ for some $i$. Hence also $\pi(\sigma)\pi(\tau)\pi(\sigma)^{-1} = \pi(\tau)^i$ and, since $G$ is abelian, we can conclude that $i = 1$. Therefore the normalizer of $\tau$ is equal to its centralizer and so from the definition of $E_{k,G,\tau}$, it is clear that $E_{k,G,\tau} = k(\zeta_\ell)$. Therefore we easily obtain

$$W(k, E_{k,G,\tau})((\ell-1)/2)(\#G/\ell) \subseteq W(k, G)^{\#H}.$$  

Suppose that $\pi(\tau) = 1$. In this case $\tau \in H$ and we clearly have

$$W(k, E_{k,G,\tau})(((\ell-1)/2)(\#G/\ell) = W(k, E_{k,G,\tau})(((\ell-1)/2)(\#G/o(\tau)).$$

Therefore, in any case we have shown that $W(k, E_{k,G,\tau})(((\ell-1)/2)(\#G/\ell)$ is contained in the subgroup on the right hand side of the inclusion (1). This concludes the proof if we recall the definition of $W(k, G)$.

In particular this proves that $R_t(k, G)$ is a group. It is also straightforward to verify that $G$ is very good, according to the definition given in [1].

References

1. Caputo, L., Cobbe, A.: An explicit candidate for the set of Steinitz classes of tame Galois extensions with fixed Galois group of odd order. Proc. Lond. Math. Soc. 107(2), 391–413 (2013)
2. Cobbe, A.: Steinitz classes of tamely ramified galois extensions of algebraic number fields. J. Number Theory 130(5), 1129–1154 (2010)
3. Gorenstein, D.: Finite groups, 2nd edn, pp. xvii+519. Chelsea Publishing Co., New York (1980)
4. Huppert, B.: Endliche Gruppen I, vol. 134 of Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen. Springer (1967)
5. Taunt, D.: On $a$-groups. In: Mathematical Proceedings of the Cambridge Philosophical Society, vol 45, pp. 24–42. Cambridge Univ Press, (1949)