

Abelian regular subgroups of the affine group and radical rings

By A. CARANTI (Povo), F. DALLA VOLTA (Milano)
and M. SALA (Cork)

In memory of Edit Szabó

Abstract. We establish a correspondence between abelian regular subgroup of the affine group, and commutative, associative algebra structures on the underlying vector space that are (Jacobson) radical rings.

As an application, we show that if the underlying field has positive characteristic, then an abelian regular subgroup has finite exponent if the vector space is finite-dimensional, while it can be torsion free if the dimension is infinite.

We also give an example of an abelian, regular subgroup of the affine group over an infinite-dimensional vector space, which intersects trivially the group of translations.

1. Introduction

CAI HENG LI has described in [Li03] the finite primitive permutation groups which contain an abelian regular subgroup. Among these we have

Mathematics Subject Classification: 20B10, 16N20.

Key words and phrases: affine group, abelian regular subgroups, (Jacobson) radical rings.

First author partially supported by MIUR-Italy via PRIN 2003018059 “Graded Lie algebras and pro- p -groups: representations, periodicity and derivations”. Second author partially supported by MIUR-Italy via PRIN “Group theory and applications”. First two authors are members of INdAM-GNSAGA.

the groups of affine type, where the translations form an abelian regular subgroup which is normal. Li notes that there might well be other (non normal) abelian regular subgroups in such groups, and as an example describes the abelian regular subgroups of the group of affine type that can be obtained as the split extension of an elementary abelian group of order 2^d by the symmetric group on $d + 1$ letters.

The goal of this note is to record a simple description of the abelian regular subgroups of the full affine group in terms of commutative, associative algebra structures that one can impose on the underlying vector space, so that the resulting ring is radical.

In Section 2 we establish the correspondence (Theorem 1). In Section 3 we give some examples.

As an application, we prove in Corollary 2 that if the underlying field has positive characteristic, then an abelian regular subgroup has finite exponent if the vector space is finite-dimensional. In Example 6 we show that if the dimension is allowed to be infinite, then an abelian regular subgroup can be torsion free.

An abelian regular subgroup of an affine group over a finite vector space must intersect the group of translations nontrivially. PÁL HEGEDŰS has given an example [Heg00] of a nonabelian, regular subgroup of an affine group over a finite vector space which has trivial intersection with the group of translations. In Corollary 5 we show that the same setting of Example 6 provides an example of an abelian, regular subgroup of the affine group over an infinite-dimensional vector space which has trivial intersection with the group of translations.

2. Abelian regular subgroups

Let F be an arbitrary field, and $(V, +)$ be a vector space of arbitrary dimension d over F .

Let $\text{GL}(V)$ be the group of invertible, F -linear maps on V , and N be the group of translations, that is,

$$N = \{ \nu(x) : x \in V \},$$

where $\nu(x) : z \mapsto z + x$. Let $\text{Aff}(V)$ be the affine group on V .

Clearly we have

Fact 1. N is a normal subgroup of $\text{Aff}(V)$. Every element of $\text{Aff}(V)$ can be written *uniquely* as a product of an element of $\text{GL}(V)$ and an element of N , so that we have the semidirect product decomposition

$$\text{Aff}(V) = \text{GL}(V)N.$$

We also write $\mathfrak{M}(V)$ for the F -algebra of F -linear maps on V .

Recall that a group G of permutations on a set Ω is said to be *regular* if, given any $\alpha \in \Omega$, then for each $\beta \in \Omega$ there exists a unique $g \in G$ such that $\alpha g = \beta$.

Clearly N is an abelian regular subgroup of $\text{Aff}(V)$. The next result describes them all.

Recall that a (*Jacobson*) *radical ring* [Jac64, Definition 2, p. 4] is a ring $(A, +, \cdot)$ in which every element is invertible with respect to the circle operation $x \circ y = x + y + x \cdot y$, so that (A, \circ) is a group. Equivalently, a ring is radical if it coincides with its Jacobson radical.

Theorem 1. *Let F be an arbitrary field, and $(V, +)$ a vector space of arbitrary dimension over F .*

There is a one-to-one correspondence between

- (1) *abelian regular subgroups T of $\text{Aff}(V)$, and*
- (2) *commutative, associative F -algebra structures $(V, +, \cdot)$ that one can impose on the vector space structure $(V, +)$, such that the resulting ring is radical.*

In this correspondence, isomorphism classes of F -algebras correspond to conjugacy classes under the action of $\text{GL}(V)$ of abelian regular subgroups of $\text{Aff}(V)$.

PROOF. Let T be an abelian regular subgroup of $\text{Aff}(V)$. Since T is regular, for each $x \in V$ there is a unique $\tau(x) \in T$ such that $0\tau(x) = x$. (Our affine maps act on the right.) Thus

$$T = \{ \tau(x) : x \in V \}. \tag{2.1}$$

Because of Fact 1, we can write $\tau(x)$ uniquely as

$$\tau(x) = \gamma(x)\nu(x), \tag{2.2}$$

where $\gamma(x) \in \text{GL}(V)$. We also introduce

$$\delta(x) = \gamma(x) - 1 \in \mathfrak{M}(V).$$

We have

$$\begin{aligned} \tau(x)\tau(y) &= \gamma(x)\nu(x)\gamma(y)\nu(y) \\ &= \gamma(x)\gamma(y)\nu(x)^{\gamma(y)}\nu(y) \\ &= \gamma(x)\gamma(y)\nu(x\gamma(y))\nu(y) \\ &= \gamma(x)\gamma(y)\nu(x + y + x\delta(y)). \end{aligned} \tag{2.3}$$

As T is abelian, we have $\tau(x)\tau(y) = \tau(y)\tau(x)$ for all $x, y \in V$. Therefore (2.3) yields

$$\gamma(x)\gamma(y)\nu(x + y + x\delta(y)) = \gamma(y)\gamma(x)\nu(y + x + y\delta(x))$$

for all $x, y \in V$. From Fact 1 we get

$$\nu(x + y + x\delta(y)) = \nu(y + x + y\delta(x))$$

for all $x, y \in V$. We get

Fact 2. $x\delta(y) = y\delta(x)$ for all $x, y \in V$.

As the left-hand side of $x\delta(y) = y\delta(x)$ is linear in x , so is the right-hand side. We obtain

Fact 3. $\delta : V \rightarrow \mathfrak{M}(V)$ is F -linear.

Since T is a group, we have $\tau(x)\tau(y) = \tau(z)$ for some $z \in V$. Because of (2.3) and Fact 1, we have $z = x + y + x\delta(y)$, so that

Fact 4. $\tau(x)\tau(y) = \tau(x + y + x\delta(y))$ for all $x, y \in V$.

Thus, again by (2.3) and Fact 1, $\gamma(x)\gamma(y) = \gamma(x + y + x\delta(y))$. We obtain, using Fact 3,

$$\begin{aligned} \gamma(x)\gamma(y) &= 1 + \delta(x) + \delta(y) + \delta(x)\delta(y) \\ &= \gamma(x + y + x\delta(y)) \\ &= 1 + \delta(x + y + x\delta(y)) \\ &= 1 + \delta(x) + \delta(y) + \delta(x\delta(y)), \end{aligned}$$

that is,

Fact 5. $\delta(x\delta(y)) = \delta(x)\delta(y)$ for all $x, y \in V$.

Now define on V a product operation by

$$x \cdot y = x\delta(y). \tag{2.4}$$

This product is commutative, by Fact 2. It is F -linear in both variables (in particular it distributes over $+$), for instance because $\delta(y) \in \mathfrak{M}(V)$ is an F -linear map, and because of Fact 3. The product is also associative as for all $x, y, z \in V$ one has, by definition (2.4) and Fact 5,

$$(xy)z = (x\delta(y))z = x\delta(y)\delta(z) = x\delta(y\delta(z)) = x\delta(yz) = x(yz).$$

Therefore $(V, +, \cdot)$ is an F -algebra.

We can now consider the circle operation “ \circ ” on V given by

$$x \circ y = x + y + xy, \tag{2.5}$$

which makes (V, \circ) into a monoid. The map

$$\begin{aligned} \tau : (V, \circ) &\rightarrow T \\ x &\mapsto \tau(x) \end{aligned}$$

is an isomorphism of monoids, because Fact 4 can be rewritten, according to Fact 5, (2.4) and (2.5), as $\tau(x)\tau(y) = \tau(x \circ y)$. Since T is a group, so is (V, \circ) . We have obtained

Fact 6. (V, \circ) is an abelian group, and the map

$$\begin{aligned} \tau : (V, \circ) &\rightarrow T \\ x &\mapsto \tau(x) \end{aligned}$$

is a group isomorphism.

We have thus proved that the ring $(V, +, \cdot)$ is radical.

We note also the following

Fact 7. $z\tau(x) = z \circ x$.

This follows from

$$z\tau(x) = z(1 + \delta(x))\nu(x) = z + z\delta(x) + x = z \circ x.$$

Fact 7 shows that $\tau(x)$ is also a translation, but with respect to “ \circ ”, while $\nu(x)$ is a translation with respect to “ $+$ ”. (But note that (V, \circ) need not be the additive group of a vector space, see e.g. Example 1 in the next section.)

Conversely, suppose $(V, +, \cdot)$ is a radical ring. For $x \in V$ define a map $\tau(x)$ on V by $\tau(x) : y \mapsto y \circ x$, with “ \circ ” as in (2.5). Reversing the above arguments, one sees that $T = \{\tau(x) : x \in V\}$ is an abelian regular subgroup of $\text{Aff}(V)$ then.

We now pass to the statement about the isomorphism and conjugacy classes.

Suppose first that $(V, +, \cdot)$ and $(V, +, *)$ are two commutative, associative F -algebra structures on the vector space structure $(V, +)$, such that they are radical rings. Suppose there is an F -algebra isomorphism

$$\varphi : (V, +, \cdot) \rightarrow (V, +, *).$$

In particular, $\varphi \in \text{GL}(V)$. For $x, y \in V$ we have two circle operations

$$\begin{cases} x \circ y = x + y + x \cdot y, \\ x \diamond y = x + y + x * y, \end{cases}$$

Since φ is an algebra isomorphism it follows

$$\begin{aligned} (x \circ y)\varphi &= (x + y + x \cdot y)\varphi \\ &= (x\varphi) + (y\varphi) + (x\varphi) * (y\varphi) \\ &= x\varphi \diamond y\varphi. \end{aligned} \tag{2.6}$$

Let $T_1 = \{\tau_1(x) : x \in V\}$ and $T_2 = \{\tau_2(x) : x \in V\}$ be the corresponding subgroups, so that

$$\begin{cases} z\tau_1(x) = z \circ x, \\ z\tau_2(x) = z \diamond x. \end{cases}$$

Now for $x, y \in V$ we have, according to Fact 7 and to (2.6),

$$y\varphi^{-1}\tau_1(x)\varphi = (y\varphi^{-1} \circ x)\varphi = y \diamond x\varphi = y\tau_2(x\varphi).$$

Thus for all $x \in V$ we have $\tau_2(x\varphi) = \varphi^{-1}\tau_1(x)\varphi$, so that $T_2 = \varphi^{-1}T_1\varphi$.

Conversely, if $T_2 = \varphi^{-1}T_1\varphi$ for some $\varphi \in \text{GL}(V)$, let $\psi : V \rightarrow V$ be the bijection such that

$$\varphi^{-1}\tau_1(x)\varphi = \tau_2(x\psi)$$

for all $x \in V$. We have

$$0\varphi^{-1}\tau_1(x)\varphi = 0\tau_1(x)\varphi = x\varphi = 0\tau_2(x\psi) = x\psi,$$

so that $\varphi = \psi$.

Now for $x, y \in V$ we have, according to Fact 6,

$$\begin{aligned} \tau_2(x\varphi \diamond y\varphi) &= \tau_2(x\varphi)\tau_2(y\varphi) \\ &= \varphi^{-1}\tau_1(x)\tau_1(y)\varphi \\ &= \varphi^{-1}\tau_1(x \circ y)\varphi \\ &= \tau_2((x \circ y)\varphi), \end{aligned}$$

so that

$$(x \circ y)\varphi = x\varphi \diamond y\varphi,$$

and reversing the argument of (2.6) one gets that

$$\varphi : (V, +, \cdot) \rightarrow (V, +, *)$$

is an isomorphism of F -algebras. □

As an application, we get

Corollary 2. *Let F be a field of positive characteristic p , and let $(V, +)$ be a finite dimensional vector space over F .*

Then every abelian regular subgroup of $\text{Aff}(V)$ has finite exponent, which is a power of p .

The result does not hold when V is allowed to be infinite dimensional. In Example 6 in the next section we give an example of an abelian regular subgroup which is torsion free.

PROOF. We first prove that any F -algebra $(V, +, \cdot)$, which is radical as a ring, is nilpotent. Clearly V is non-unital, because -1 would have no inverse with respect to \circ , as $(-1) \circ a = -1$ for all $a \in V$. Now a non-unital finite-dimensional F -algebra A need not be an Artinian ring, as an ideal need not be an F -subspace. (Think of the one-dimensional \mathbf{Q} -algebra

$\mathbf{Q}a$, where $a^2 = 0$. Its ideals correspond to the additive subgroups of \mathbf{Q} .) However, A can be embedded in the standard way in a unital F -algebra B of dimension one more. If A is radical, then A is the Jacobson radical of the artinian ring B , and so A is nilpotent.

For $a \in \mathbf{N}$ and $x \in V$, we write

$$a \circ x = \underbrace{x \circ \dots \circ x}_{a \text{ times}}.$$

One proves easily by induction

$$a \circ x = \sum_{i=1}^a \binom{a}{i} x^i.$$

In particular

$$p \circ^j x = x^{p^j}. \quad (2.7)$$

Suppose $V^n = 0$ for some n . If $p^j \geq n$ for some j , then $V^{p^j} = 0$, so that by (2.7), and Fact 6, the corresponding T has exponent dividing p^j . \square

3. Examples and comments

We begin with some examples in which V is finite, so that all algebra structures $(V, +, \cdot)$, which are radical as rings, are nilpotent. In this section we use the notation of the proof of Theorem 1.

The first example is here as folklore.

Example 1. When F is the field with 2 elements, and V has dimension 2 over F , the affine group is isomorphic to the symmetric group $\text{Sym}(4)$ on four letters. We write $V = \{0, a, b, a + b\}$ for the underlying vector space. The other abelian regular subgroups of $\text{Sym}(4)$ are the three cyclic subgroups, which correspond to the ring structures on $(V, +)$ defined by

- $a^2 = b, b^2 = 0, ab = 0$;
- $a^2 = 0, b^2 = a, ab = 0$;
- $a^2 = b^2 = ab = a + b$.

For instance in the first case we obtain the cyclic group (T, \circ) where

- $2 \circ a = a + a + b = b,$
- $3 \circ a = b + a + ab = a + b,$
- $4 \circ a = a + b + a + (a + b)a = b + b = 0.$

The three cyclic subgroups are conjugate here, and the three rings are isomorphic.

A generalization of this for an arbitrary prime p is given by the following

Example 2. Let p be an arbitrary prime, and take V to have dimension p over the field F with p elements. Then one can define a suitable ring structure on V by declaring a base of V in the form

$$a, a^2, \dots, a^p,$$

and letting $a^{p+1} = 0$. The corresponding group T is abelian of type $(p^2, \underbrace{p, \dots, p}_{p-2})$, where the cyclic component of order p^2 is generated by a (one has $p \circ a = a^p$), and those of order p are generated by a^2, \dots, a^{p-1} .

The following non trivial ring structure on V satisfies $xyz = 0$ for all $x, y, z \in V$.

Example 3. Let F be the field with 2 elements, and $(V, +, \cdot)$ be the exterior algebra over a vector space of dimension k , spanned by e_1, \dots, e_k , truncated at length 2. That is, V has basis

$$e_1, \dots, e_k, e_1 \wedge e_2, \dots, e_{k-1} \wedge e_k,$$

and satisfies $x^2 = 0$.

This is relevant to the question whether N normalizes all abelian regular subgroups T . Note first the following interpretation of our product in terms of the action of T on N .

Lemma 3. $[\nu(x), \tau(y)] = \nu(xy)$.

PROOF.

$$\begin{aligned} [\nu(x), \tau(y)] &= \nu(x)^{-1} \nu(x)^{\gamma(y)} \\ &= \nu(-x) \nu(x(1 + \delta(y))) \\ &= \nu(-x + x + xy) = \nu(xy). \end{aligned} \quad \square$$

By assumption, T normalizes N . Now N normalizes T if and only if $\nu(xy) \in T$ for all x, y , that is, $\delta(xy) = 0$, that is $xyz = 0$ for all $x, y, z \in V$. So in Example 3, N normalizes T . However, in the following example N does not normalize T , as there is a nonzero threefold product.

Example 4. Let F be the field with 2 elements, and $(V, +, \cdot)$ be the exterior algebra over a vector space of dimension three, spanned by e_1, e_2, e_3 . That is, V has basis

$$e_1, e_2, e_3, e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_3.$$

Clearly $x^2 = 0$ for all x , but $e_1 \wedge e_2 \wedge e_3 \neq 0$.

In Examples 3 and 4, the ring is an exterior algebra over the field F with two elements, or a quotient thereof. In characteristic 2, algebras that are quotients of exterior algebras correspond to elementary abelian regular subgroups of the affine group.

Before considering an example when V is infinite, let us define, for a prescribed F -algebra structure $(V, +, \cdot)$,

$$U = \ker(\delta) = \{x \in V : x \cdot y = 0 \text{ for all } y \in V\}.$$

Clearly we can choose the algebra structure on the finite dimensional vector space $(V, +)$ so that U has arbitrary dimension, for instance as in the next example.

Example 5. Let $0 \leq e < d$, and we choose $(V, +, \cdot)$ to be the quotient of the ideal of the polynomial ring $F[x_0, x_1, \dots, x_e]$ generated by x_0, x_1, \dots, x_e modulo the relations

$$\begin{cases} x_0^{d-e+1}, \\ x_0 x_i, & \text{for } i > 0, \\ x_j x_i, & \text{for } i, j > 0. \end{cases}$$

Then V has dimension d , while U has basis $x_0^{d-e}, x_1, \dots, x_e$, and thus $\dim(U) = e + 1$.

Now U corresponds to the intersection $N \cap T$, as

$$\begin{aligned} N \cap T &= \{\nu(x) : \tau(x) = \nu(x)\} \\ &= \{\nu(x) : \delta(x) = 0\} \\ &= \{\nu(x) : x \in U\}. \end{aligned} \tag{3.1}$$

Using Lemma 3, one recovers the well-known fact

Lemma 4. *Let N be the group of translations in the affine group $\text{Aff}(V)$, and let T be an abelian regular subgroup. Then*

$$N \cap T = C_N(T) = C_T(N). \tag{3.2}$$

When V , and thus $\text{Aff}(V)$, is finite, then $U \neq 0$, as $(V, +, \cdot)$ is nilpotent, so that the subgroup of (3.2) is nontrivial. (Alternatively, $C_N(T)$ is nontrivial, as T is a finite p -group acting on the finite p -group N ; here p is the characteristic of the underlying field.) In other words, an abelian regular subgroup of the affine group over a finite vector space intersects the group of translations nontrivially.

It also follows from Example 5 that when V is finite, then $N \cap T$ has arbitrary order, different from 1.

PÁL HEGEDŰS has given an example [Heg00] of a nonabelian, regular subgroup of an affine group over a finite vector space which has trivial intersection with the group of translations.

Now we consider the following

Example 6. Let $(V, +, \cdot)$ be the maximal ideal $tF[[t]]$ of the F -algebra $F[[t]]$ of formal power series over an arbitrary field F . This is a radical ring. Since $F[[t]]$ is a domain, we have $U = 0$ here.

It follows from (3.1) that in this example the abelian regular subgroup T intersects trivially the group N of translations.

Also, T is torsion-free. If F is a field of positive characteristic p , then the group N of translations has exponent p . Thus $\text{Aff}(V)$ has two rather different abelian regular subgroups here.

Summing up, we have

Corollary 5.

- (1) *In the affine group over a finite vector space, an abelian regular subgroup intersects the group of translations nontrivially.*
- (2) *There is an example [Heg00] of a nonabelian, regular subgroup of an affine group over a finite vector space which has trivial intersection with the group of translations.*

- (3) *There is an example (Example 6 above) of an abelian, regular subgroup of the affine group over an infinite vector space which has trivial intersection with the group of translations.*

References

- [Heg00] PÁL HEGEDŰS, Regular subgroups of the affine group, *J. Algebra* **225**, no. 2 (2000), 740–742.
- [Jac64] NATHAN JACOBSON, Structure of rings, American Mathematical Society Colloquium Publications, Vol. 37, Revised edition, *American Mathematical Society, Providence, R.I.*, 1964.
- [Li03] CAI HENG LI, The finite primitive permutation groups containing an abelian regular subgroup, *Proc. London Math. Soc.* (3) **87**, no. 3 (2003), 725–747.

A. CARANTI
DIPARTIMENTO DI MATEMATICA
UNIVERSITÀ DEGLI STUDI DI TRENTO
VIA SOMMARIVE 14
I-38050 POVO (TRENTO)
ITALY

E-mail: caranti@science.unitn.it
URL: <http://science.unitn.it/~caranti/>

FRANCESCA DALLA VOLTA
DIPARTIMENTO DI MATEMATICA E APPLICAZIONI
EDIFICIO U5
UNIVERSITÀ DEGLI STUDI DI MILANO-BICOCCA
VIA BICOCCA DEGLI ARCIMBOLDI 8
I-20126 MILANO
ITALY

E-mail: francesca.dallavolta@unimib.it
URL: <http://www.matapp.unimib.it/~dallavolta/>

MASSIMILIANO SALA
BOOLE CENTRE FOR RESEARCH IN INFORMATICS
UNIVERSITY COLLEGE CORK
CORK
IRELAND

E-mail: msala@bcri.ucc.ie

(Received October 26, 2005; revised April 11, 2006)