Gumm's Theorem and the Structure of Minimal Algebras

Marcus Kracht,
II. Mathematisches Institut,
Arnimallee 3,
D - 14195 Berlin

In this note we will show that Gumm's theorem on Abelian algebras can be strengthened in such a way that Pálfy's theorem on minimal algebras becomes a near consequence. This is surprising, at least after having a second look at the matter. For if one compares the proofs of the original theorems there is indeed a similarity between the two; however, it is not possible to see directly that a minimal algebra with more than 3 elements is Abelian. This results only after the completion of the classification of minimal algebras. So, Gumm's theorem is of no use here. Instead, there is a weaker property that can easily be derived for minimal algebras, which we call *1-Abelian*; and we can show that Gumm's theorem can be proved with *1-Abelian* replacing *Abelian*. It should be said here that few of the proofs are new; rather, the novelty is the arrangement of the facts that can be proved with them.

Definition 1 *An algebra $\mathfrak{A}$ is called 1-Abelian if it satisfies the term condition for all binary polynomials, that is, for all $f \in \mathrm{Pol}_2 \mathfrak{A}$ and $a, b, c, d \in A$*

$$(\dagger) \qquad f(a,c) = f(a,d) \text{ implies } f(b,c) = f(b,d).$$

Clearly, if $\mathfrak{A}$ is Abelian, it is also 1-Abelian. The property of being 1-Abelian has some easy consequences which we list in the following proposition.

Proposition 2 *Let $\mathfrak{A}$ be 1-Abelian. Then the following holds*

(i) *For all $f \in \mathrm{Pol}_{n+1} \mathfrak{A}$ and $\overline{a}, \overline{b} \in A^n$, $c, d \in A$:*

$$f(\overline{a}, c) = f(\overline{a}, d) \quad \text{implies} \quad f(\overline{b}, c) = f(\overline{b}, d)$$

(ii) *For all $f(\overline{x}, y) \in \mathrm{Pol}_{n+1} \mathfrak{A}$: if $f(\overline{a}, y)$ does not depend on y for some $\overline{a}$, then $f(\overline{x}, y)$ does not depend on y.*

Proof. It is clear that if $f \in \mathrm{Pol}_{n+1} \mathfrak{A}$ and $a, b, c, d \in A$ as well as $\overline{e} \in A^{n-1}$ then by (†) $f(a, c, \overline{e}) = f(a, d, \overline{e})$ implies $f(b, c, \overline{e}) = f(b, d, \overline{e})$. Thus the following implications hold:

$$\begin{array}{lc} & f(a_1, \ldots, a_n, c) = f(a_1, \ldots, a_n, d) \\ \Rightarrow & f(b_1, a_2, \ldots, a_n, c) = f(b_1, a_2, \ldots, a_n, d) \\ \Rightarrow & f(b_1, b_2, a_3, \ldots, a_n, c) = f(b_1, b_2, a_3, \ldots a_n, d) \\ \Rightarrow & \ldots \\ \Rightarrow & f(b_1, \ldots, b_n, c) = f(b_1, \ldots, b_n, d). \end{array}$$

(ii) Suppose that for all c, d $f(\overline{a}, c) = f(\overline{a}, d)$. Then by (i), for all $c, d, \overline{b}$ $f(\overline{b}, c) = f(\overline{b}, d)$. □

Recall that Gumm's Theorem states that an algebra is polynomially equivalent to a module over a ring iff it is Abelian and Malcev. Here we show the following theorem.

Theorem 3 *For an algebra $\mathfrak{A}$ the following are equivalent:*

(i) $\mathfrak{A}$ is Malcev and 1-Abelian.

(ii) $\mathfrak{A}$ is polynomially equivalent to a module over a ring.

Proof. (ii) $\Rightarrow$ (i). By Gumm's Theorem, since Abelian implies 1-Abelian. (i) $\Rightarrow$ (ii). We use the proof in [1], Claim 4, p. 49, to show that we have an Abelian group definable in $\mathfrak{A}$. As usual, pick an arbitrary element $0 \in A$ and put

$$\begin{aligned} x + y &= p(x, 0, y) \\ -x &= p(0, x, 0) \end{aligned}$$

where p is the Malcev polynomial. Then $x + 0 = 0 + x = x$. Now define the following polynomials.

$$\begin{aligned} \delta_1(x, y, z, u) &= p(p(x, 0, u), 0, p(y, u, z)) \\ \delta_2(x, u) &= p(x, u, p(u, x, 0)) \\ \delta_3(x, y, u) &= p(u, 0, p(x, u, y)) \end{aligned}$$

Since $\delta_1(0, b, 0, b) = b = \delta_1(0, b, 0, 0)$, $\delta_1(a, b, c, b) = \delta_1(a, b, c, 0)$, by (2.ii). Now

$$\delta_1(a, b, c, b) = p(p(a, 0, b), 0, p(b, b, c)) = (a + b) + c$$

and

$$\delta_1(a,b,c,0) = p(p(a,0,0),0,p(b,0,c)) = a + (b + c)$$

and hence $+$ is associative. Next, $\delta_2(0,a) = 0 = \delta_2(0,0)$ and so again by (2.ii) $\delta_2(a,a) = \delta_2(a,0)$ showing $a + (-a) = 0$. Finally, $\delta_3(0,0,b) = p(b,0,p(0,b,0)) = b + (-b) = 0$ and $\delta_3(0,0,0) = 0$ from which $a + b = \delta_3(a,b,0) = \delta_3(a,b,b) = b + a$, using (2.ii) once again.

Notice that indeed we only used that $\mathfrak{A}$ is 1-Abelian. In the next step we show that all polynomials are affine; the rest is standard. The ring will be defined as usual, and it follows indeed that $\mathfrak{A}$ is equivalent to a module over that ring. So, take a $f \in \mathrm{Pol}_n\,\mathfrak{A}$ and put $g(\overline{x}) = f(\overline{x}) - f(\overline{0})$. A proof of the next claim will complete the proof of the theorem.

Claim 4 *$g(\overline{x})$ is linear. Moreover, for the functions $g_i(\overline{x}) = g(0,\ldots,x_i,\ldots,0)$ we have*

$$g(\overline{x}) = \sum_{i=1}^{n} g_i(\overline{x})$$

Proof. Consider the function

$$h(\overline{x}) = g(\overline{x}) - \sum_{i=1}^{n} g_i(\overline{x}).$$

Since

$$\begin{aligned} h(0,\ldots,0,x_i,0,\ldots,0) &= g(0,\ldots,0,x_i,0,\ldots,0) - \sum_{i=0}^{n} g_i(0,\ldots,0,x_i,0,\ldots,0) \\ &= g_i(\overline{x}) - g_i(\overline{x}) \\ &= 0 \end{aligned}$$

we find that h does not depend on x_i, by (2.ii). □

Recall that an algebra $\mathfrak{A}$ is called **minimal** if its unary polynomials are either constant or bijective. It is trivial to see that if $\mathfrak{A}$ has two elements it is minimal and likewise if it contains only unary bijective polynomials (plus, of course, the constant ones). The remaining case is covered by Pálfys Theorem stated below. It is a rather direct consequence of Theorem 3 and the following fact, which corresponds to Step 1 on p. 152 in [2]. (The proof performed there is due to B. Jónsson.)

Lemma 5 *Let $\mathfrak{A}$ be a finite minimal algebra with $\sharp A > 2$. Then every binary operation which depends on both arguments is a quasigroup operation, that is, $f(a,c) = f(a,d)$ implies $c = d$.*

Furthermore, if $\mathfrak{A}$ is not unary, there is a binary polynomial depending on both arguments, by Corollary 4.2 of [1].

Lemma 6 *Suppose that $\mathfrak{A}$ is a finite minimal algebra and $\sharp A > 2$. Then $\mathfrak{A}$ is 1-Abelian.*

Proof. Consider a binary polynomial $f(x,y)$. (†) is trivially satisfied if f depends on just one variable. For suppose $f(a,c) = f(a,d)$; if f does not depend on its first argument, then $f(b,c) = f(a,c) = f(a,d) = f(b,d)$. If, however, f does not depend on its second argument, then $f(b,c) = f(b,d)$ by definition. If f depends on both variables then $f(a,c) = f(a,d)$ implies $c = d$ by the previous lemma and so $f(b,c) = f(b,d)$ for every b. □

Lemma 7 *Suppose that $\mathfrak{A}$ is a finite minimal algebra, $\sharp A > 2$ and that $\mathfrak{A}$ is not unary. Then $\mathfrak{A}$ is Malcev.*

Proof. By assumption, there is a poynomial which is not unary; so there is binary polynomial f depending on both arguments. f is a quasigroup operation and A finite; so $\langle A, f\rangle$ and a fortiori $\mathfrak{A}$ is Malcev. □

Theorem 8 (Pálfy) *Suppose that $\mathfrak{A}$ is a finite, non-unary minimal algebra and $\sharp A > 2$. Then $\mathfrak{A}$ is polynomially equivalent to a finite vector space.*

Proof. From Lemma 6 and Lemma 7 it follows in conjunction with Theorem 3 that $\mathfrak{A}$ is polynomially equivalent to a module over a ring. Since multiplication by an element $r \neq 0$ of the ring must be bijective by the minimality of $\mathfrak{A}$ the ring has no zero divisors; it is therefore a field since it is finite. □

In the light of these results it seems that 1-Abelian behaves much the same as Abelian and is equivalent to it in presence of a Malcev polynomial. We do not believe that 1-Abelian algebras are necessarily Abelian but we have not found a counterexample.

References:

[1] D. Hobby, R. McKenzie: *The Structure of Finite Algebras.* Contemporary Mathematics, AMS vol. 76, 1988.

[2] Th. Ihringer: *Allgemeine Algebra.* Teubner Verlag, Stuttgart, 1988.