CRITICAL ALGEBRAS AND THE FRATTINI CONGRUENCE

Emil W. Kiss and Samuel M. Vovsi

Abstract. In this note we show that if two critical algebras generate the same congruence-permutable variety, then the varieties generated by their proper sections also coincide.

1. Introduction

Let A be a finite algebra. The *sections* of A are the homomorphic images of the subalgebras of A. A section is called *proper* if it differs from A. The class of all proper sections of A is denoted by $(\mathbf{HS}-1)A$. An algebra is called *critical* if it is finite, and does not belong to the variety generated by its proper sections.

In 1971, Bryant [1] proved that if A and B are two critical groups generating the same variety, then the varieties generated by $(\mathbf{HS}-1)A$ and $(\mathbf{HS}-1)B$ are also the same, thus solving Problem 25 from Hana Neumann's book [10]. There naturally arose the question whether an analogous result is valid for other types of algebraic structures. The answer turned out to be in the affirmative, e.g., for group representations over a field (see [11]) and for associative algebras over $GF(p)$ (Mal'tsev [9]). On the other hand, for arbitrary associative rings the question has remained open for a rather long time.

It was proved in [12] that Bryant's theorem is valid not only for rings but in a much more general setting, namely, for arbitrary multioperator groups. Surprisingly, the proof was almost a literal repetition of that in [1]. The reason why this proof was not found earlier was mainly of psychological character. The group-theoretic arguments in [1] were essentially based on the properties of the Frattini subgroup, but the analogous notion of the Frattini subalgebra did not work for rings and other algebras. The basic idea of [12] was that, instead of the Frattini subalgebra, one should use a much less known concept of the *Frattini ideal.*

These results showed that Bryant's theorem may hold even more generally, and its natural form is yet to be determined. In this note we prove that it is true for algebras from any congruence-permutable variety.

Theorem. *Let A and B be critical algebras contained in a congruence-permutable variety. If* $\operatorname{var} A = \operatorname{var} B$*, then* $\operatorname{var}(\mathbf{HS}-1)A = \operatorname{var}(\mathbf{HS}-1)B$.

This theorem contains, of course, the cited results from [1], [9] and [12]. The proof is a combination of ideas from [1], [12], [7] with only a few minor additions (like Lemma 2). We

Key words and phrases. Critical algebra, congruence-permutable variety.

The research of the first author has been supported by the Hungarian National Foundation for Scientific Research (OTKA), grant number 1903

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

are grateful to Ralph McKenzie who drew our attention to the possibility of putting these ideas together.

2. Proof of the theorem

First we fix our terminology and notation. Let A be an algebra. If $B \leq A$ (B is a subalgebra of A) and θ is a congruence of A, then by $B[\theta]$ we denote the union of all θ-classes intersecting B. Clearly, this is a subalgebra containing B, and if α is any homomorphism from A with kernel θ, then we have $B[\theta] = \alpha^{-1}\alpha(B)$. We say that θ *is contained in* B if B is a union of θ-classes (that is, $B[\theta] = B$). It is straightforward that the join of all congruences contained in B is still contained in B, so there exists a largest such congruence, which is denoted by $\phi_B(A)$.

Let $(\mathbf{S}-1)A$ denote the class of all proper subalgebras of A, and $(\mathbf{H}-1)A$ the class of all proper homomorphic images of A. An algebra A is called $\mathbf{H}$-*critical* or $\mathbf{S}$-*critical* if it is finite, and is not contained in $(\mathbf{H}-1)A$ or $(\mathbf{S}-1)A$, respectively. It may happen that the algebra A has no proper subalgebras. Such algebras A are considered $\mathbf{S}$-critical, and therefore we make the convention that the variety generated by the empty set of algebras is the empty set. It is important to distinguish this case from the one, when A has only singletons as proper subalgebras, see statement (b) of Proposition 1 below. With this convention, the statement "each locally finite variety is generated by its critical algebras" remains true for trivial varieties.

The Frattini subalgebra $\Phi(A)$ of A is the intersection of all maximal (proper) subalgebras of A. It may happen that $\Phi(A)$ is empty. If A has no maximal subalgebras, we set $\Phi(A) = A$. Now we introduce the concept of the *Frattini congruence of A,* which will play an important role in what follows. It is denoted by $\phi(A)$, and is defined to be the intersection of all $\phi_M(A)$, where M runs over all maximal subalgebras of A. In other words, $\phi(A)$ is the largest congruence of A that is contained in all maximal subalgebras. If A has no maximal subalgebras at all, we define $\phi(A) = 1_A$.

In groups, the Frattini subgroup of a factor-group behaves nicely, as the following well-known observation shows.

Claim. *Let $\alpha : G \to H$ be an onto homomorphism of finite groups, and denote by Φ' the complete inverse image of $\Phi(H)$ in G. Then we have*

(a) $\Phi(G) \leq \Phi'$ *(hence $H/\Phi(H)$ is a homomorphic image of $G/\Phi(G)$).*
(b) $\Phi(G) = \Phi' \iff \mathrm{Ker}(\alpha) \leq \Phi(G) \iff H/\Phi(H) \cong G/\Phi(G)$.

The proof is straightforward, but one has to use the fact that the inverse image of a maximal subalgebra under an onto homomorphism is also a maximal subalgebra. This is clear for groups, but not true for general algebras (consider an onto homomorphism from the three element chain as a distributive lattice to the two element lattice). Fortunately, we can generalize this claim for the case, when the Frattini congruence permutes with all other congruences.

Lemma 1. *Let $\alpha : C \to D$ be an onto homomorphism of finite algebras, and denote by ϕ' the complete inverse image of $\phi(D)$ in C. Then we have*

(a) *If $\phi(C)$ permutes with* $\mathrm{Ker}(\alpha)$, *then $\phi(C) \leq \phi'$ (hence $D/\phi(D)$ is a homomorphic image of $C/\phi(C)$).*

(b) $\phi(C) = \phi' \iff \mathrm{Ker}(\alpha) \le \phi(C) \implies D/\phi(D) \cong C/\phi(C)$.
(c) *If* $\phi(C)$ *permutes with* $\mathrm{Ker}(\alpha)$*, and* $D/\phi(D) \cong C/\phi(C)$*, then* $\mathrm{Ker}(\alpha) \le \phi(C)$.

The key to proving this lemma is the following observation.

Lemma 2. *Let* $\alpha : C \to D$ *be an onto homomorphism, and assume that* $\phi(C)$ *permutes with* $\mathrm{Ker}(\alpha)$*. If* M *is a maximal subalgebra of* D*, then* $\phi(C)$ *is contained in* $\alpha^{-1}(M)$*.*

Proof. Assume otherwise, then $N' \supsetneqq N$, where $N = \alpha^{-1}(M)$, $\phi = \phi(C)$, and $N' = N[\phi]$. Hence $\alpha(N') \supsetneqq M$, and by the maximality of M we have $\alpha(N') = D$. Thus for every $a \in C$ there exists $b \in N'$ such that $a\ \theta\ b$, where θ is the kernel of the homomorphism α. By the definition of N', there is an element $c \in N$ with $b\ \phi\ c$. Since θ and ϕ permute, there exists some $d \in C$ such that $c\ \theta\ d$ (that is, $\alpha(c) = \alpha(d)$) and $d\ \phi\ a$. Since $N = \alpha^{-1}(M)$ and $c \in N$, we get $d \in N$, whence $a \in N'$.

Thus $C = N'$. But this is impossible, because N, as a complete inverse image of the proper subalgebra M, must be proper in C and so it is contained in some maximal subalgebra S of C. Hence $N' = N[\phi] \subseteq S$, showing $C \neq N'$. □

To prove Lemma 1, notice that ϕ' is the largest congruence of C that is contained in the inverse image of every maximal subalgebra of D. Thus Lemma 2 proves the inequality in (a). We clearly have that $C/\phi' \cong D/\phi(D)$, and therefore the statement in parentheses follows from the standard homomorphism theorem. We get the two statements concerning $C/\phi(C) \cong D/\phi(D)$ as well, since the algebra C is finite.

To finish the proof of (b), assume first that $\phi(C) = \phi'$. Since $\mathrm{Ker}(\alpha)$ is contained in the inverse image of every subalgebra of D, we have $\mathrm{Ker}(\alpha) \le \phi'$ by the description of ϕ' above. Hence $\mathrm{Ker}(\alpha) \le \phi(C)$. Now assume that $\mathrm{Ker}(\alpha) \le \phi(C)$. Then these two congruences permute, so by (a) it is sufficient to show that $\phi' \le \phi(C)$. Let M be a maximal subalgebra of C. Then $\mathrm{Ker}(\alpha)$ is contained in M, hence $M = \alpha^{-1}\alpha(M)$. Thus $\alpha(M)$ is a proper (and of course maximal) subalgebra of D, and we have shown that every maximal subalgebra of C is the inverse image of a maximal subalgebra of D, proving $\phi' \le \phi(C)$. □

Now we are able to give a rather straightforward generalization of Theorem 3.5 of [1]. We present its proof for the sake of completeness. Notice that the only places where we use congruence permutability are the references to Lemma 1(a,c).

Proposition 1. *Let* A *and* B *be* $\mathbf{S}$*-critical algebras in a congruence-permutable variety. If* $\mathrm{var}\, A = \mathrm{var}\, B$*, then*

(a) $A/\phi(A) \cong B/\phi(B)$.
(b) $\mathrm{var}\,(\mathbf{S}-1)A = \mathrm{var}\,(\mathbf{S}-1)B$ *(in particular,* $(\mathbf{S}-1)A$ *is empty if and only if* $(\mathbf{S}-1)B$ *is empty).*

Proof. Since A and B are finite, it follows that $A = \alpha(R)$, where α is an onto homomorphism, and $R \le D_1 \times \cdots \times D_n$ is a subdirect product of some subalgebras $D_1, \ldots, D_n$ of B. Choose R to have minimal possible order, and denote by θ the kernel of α. We show that

$$\theta \le \phi(R)\,. \tag{1}$$

If R has no proper subalgebras, then $\phi(R) = 1_R$ and (1) holds. Otherwise, by the definition of $\phi(R)$, if (1) fails, then there exists a maximal subalgebra N of R not containing θ. Thus

$N < N[\theta] = \alpha^{-1}\alpha(N)$, and as N is maximal, we have $\alpha^{-1}\alpha(N) = R$. On the other hand, by the minimality of R, the image $\alpha(N)$ of N must be proper in A, hence $\alpha^{-1}\alpha(N)$ is a proper subalgebra of R. This contradiction proves (1). Now statement (b) of Lemma 1 implies that

$$R/\phi(R) \cong A/\phi(A)\,. \tag{2}$$

Next we prove (a). By symmetry, it is enough to show that $B/\phi(B) \in \mathbf{H}\{A/\phi(A)\}$. We have $A \in \operatorname{var} R$, $R \in \operatorname{var} B$, and $\operatorname{var} A = \operatorname{var} B$. Thus $\operatorname{var} R = \operatorname{var} B$ and, as B is $\mathbf{S}$-critical, $R \notin \operatorname{var}(\mathbf{S}-1)B$. Therefore $B = D_i$ for some i, whence $B \in \mathbf{H}\{R\}$. By (2) and statement (a) of Lemma 1 we get that $B/\phi(B) \in \mathbf{H}\{R/\phi(R)\} = \mathbf{H}\{A/\phi(A)\}$.

Finally we prove (b). By symmetry, it suffices to show that $\operatorname{var}(\mathbf{S}-1)A \subseteq \operatorname{var}(\mathbf{S}-1)B$. Since A is a homomorphic image of R, we have $\operatorname{var}(\mathbf{S}-1)A \subseteq \operatorname{var}(\mathbf{S}-1)R$, hence it is sufficient to show that $\operatorname{var}(\mathbf{S}-1)R \subseteq \operatorname{var}(\mathbf{S}-1)B$.

Denote by π_i the natural projection of R onto D_i. It is enough to show that if M is a maximal subalgebra of R, then $\pi_i(M) \in (\mathbf{S}-1)B$ for each i. If D_i is a proper subalgebra of B, there is nothing to prove. If $D_i = B$, then we have an onto homomorphism $\pi_i : R \to B$. We have already proved that $R/\phi(R) \cong B/\phi(B)$, so statement (c) in Lemma 1 shows that $\operatorname{Ker}(\pi_i) \leq \phi(R)$. But $\phi(R)$ is contained in the maximal subalgebra M, so $\pi_i(M)$ is a proper subalgebra of B. □

The monolith (smallest nontrivial congruence) of a monolithic (that is, subdirectly irreducible) algebra A is denoted by $\mu(A)$. We recall the lemma from [7] (which is a generalization of a result of Kovács and Newman [8]).

Lemma 3. *Let $\mathcal{C}$ be a finite set of finite subdirectly irreducible algebras that is closed under monolithic sections. Assume that $\mathcal{V} = \operatorname{var}(\mathcal{C})$ is congruence modular. If A is a subdirectly irreducible algebra in $\mathcal{V}$, then*

$$A/\mu(A) \in \operatorname{var}\{D/\mu(D) \mid D \in \mathcal{C}\}\,.$$

Proposition 2. *Let A and B be monolithic algebras in a congruence-modular variety. If* $\operatorname{var} A = \operatorname{var} B$, *then* $\operatorname{var}(\mathbf{H}-1)A \subseteq \operatorname{var}(\mathbf{HS}-1)B$.

Proof. Our assertion is equivalent to

$$A/\mu(A) \in \operatorname{var}(\mathbf{HS}-1)B\,. \tag{3}$$

Denote by $\mathcal{C}$ the class of all monolithic sections of B. Since B is monolithic, we have $B \in \mathcal{C}$ and $\operatorname{var} B = \operatorname{var}\mathcal{C}$, whence $A \in \operatorname{var}\mathcal{C}$. Since each $D/\mu(D)$ is a proper section of B, we obtain (3) by applying Lemma 3. □

Since every critical algebra is both $\mathbf{S}$-critical and $\mathbf{H}$-critical, and since every non-singleton $\mathbf{H}$-critical algebra is monolithic, our theorem follows directly from Propositions 1 and 2.

3. Discussion

Congruence modularity. The theorem holds for any congruence-distributive variety (by Jónsson's lemma [6]). Since we have proved Proposition 2 for the congruence-modular case, the following question arises naturally.

Problem. *Does the theorem hold for congruence-modular varieties?*

As we have pointed out, it would be sufficient to generalize Lemma 1. The Frattini congruence is nilpotent in the case of groups, and even solvable congruences permute with all other congruences in modular varieties. It is of course not true that the Frattini congruence is always solvable in the general case (think of congruence-distributive varieties). We do not think that Lemma 1 holds either, but a suitable weaker form might.

For *multioperator groups* one can prove the following improvement of Proposition 2: if A and B are $\mathbf{H}$-critical multioperator groups such that $\operatorname{var} A = \operatorname{var} B$, then $\mu(A) \cong \mu(B)$ and $\operatorname{var}(\mathbf{H}-1)A = \operatorname{var}(\mathbf{H}-1)B$ (see [1], [12]). It may be interesting to know if this fact, which is a natural counterpart of Proposition 1, can be generalized to arbitrary congruence-modular (or at least congruence-permutable) varieties (with the first assertion stated in terms of similar and isomorphic congruences described in Chapter 10 of Freese-McKenzie [4] and in Day-Kiss [2]).

Finally we take the opportunity to call attention to the following related problem of Ralph Freese [3], for which the Frattini congruence could be a useful tool: is it true that all subvarieties of finitely generated congruence-modular varieties are also finitely generated?

Semigroups. We do not know if Proposition 1 or the theorem holds for semigroups. However, consider the following example. Let B_n be the semigroup consisting of all $n \times n$ matrix units plus the zero matrix (so B_n has $n^2 + 1$ elements). It is (congruence-)simple for each n. However, if I is the ideal of $R = B_2 \times B_2$ consisting of all pairs with at least one zero component, then $(B_2 \times B_2)/I \cong B_4$. Since B_2 is a subsemigroup of B_4, we have $\operatorname{var} B_2 = \operatorname{var} B_4$, hence B_4 is not critical.

So *finite simple semigroups need not be critical, and two finite simple semigroups generating the same variety need not be isomorphic.* This example also shows that Lemma 1(a) (without the assumption that the Frattini congruence permutes with $\operatorname{Ker}(\alpha)$) fails for semigroups. Indeed, we have $\phi(B_n) = 0$ (since B_n is simple having a proper subsemigroup). We show that $\phi(R) = \theta(I)$ (the congruence corresponding to the ideal I). Let M be a maximal subsemigroup of R. Then $M \cup I$ is also a subsemigroup. If $M \cup I = R$, then M contains $R \setminus I$. An easy calculation shows that $R \setminus I$ generates R, so $M = R$, contradicting the maximality of M. Thus $M \cup I = M$, showing $I \subseteq M$. Thus $\phi(R) \geq \theta(I)$. On the other hand $R/I \cong B_4$ is simple, so $\theta(I)$ is a maximal congruence, and R does have proper subsemigroups, so $\phi(R) < 1$, and therefore indeed $\phi(R) = \theta(I)$. Now consider the first projection $R \to B_2$. Lemma 1(a) fails for this homomorphism, since $B_2 \cong B_2/\phi(B_2)$ is not a homomorphic image of the simple semigroup $R/\phi(R) \cong B_4$.

This example shows very clearly how the argument proving Proposition 1 fails in the general case. In the first part of that argument we prove that $B/\phi(B)$ is a homomorphic image of $A/\phi(A)$. Here we use only that B is $\mathbf{S}$-critical and R is minimal. Both conditions are satisfied in the example. Indeed, the identity $xyzx = xzyx$ holds in every subsemigroup of $B = B_2$, but not in B_2, hence B is $\mathbf{S}$-critical. If S is a subsemigroup of R whose image is still the full $A = B_4$, then every element of $R \setminus I$ must be in S, and therefore $S = R$, since $R \setminus I$ generates R. Thus R is minimal.

Notice that Lemma 1(a) fails for a nice homomorphism (a projection on a direct product), and that the Frattini congruence of a direct product is a skew congruence (and not the product of the Frattini congruences of the factors, as it is the case for finite groups). By Corollary 4.5 of Gumm [5], the projection kernels of a direct product permute with all the congruences in the congruence-modular case, so R cannot be a direct product in a modular counterexample.

Simple algebras. According to the main result of Valeriote [13], every finite Abelian algebra has only trivial subalgebras. Therefore such algebras are critical. Nonabelian simple algebras in congruence-modular varieties are also critical by the Generalized Jónsson's Theorem (see Theorem 10.1 in [4]). Thus Proposition 1(a) contains the following well-known (see Theorem 12.4 in [4]) fact: If two finite simple algebras generate the same congruence-permutable variety, and one of them has a proper subalgebra, then they are isomorphic.

We complement the example of simple semigroups above by the following well-known observation showing that *two simple* **and** *critical algebras generating the same variety need not be isomorphic.* Recall that if G is a group, then a G-set (or G-act, or G-polygon) is a set X on which G acts (say, on the right) as a permutation group, not necessarily faithfully. It is considered as a unary algebra whose set of basic operations can be identified with the elements of G. If H is a subgroup of G, then G acts by right multiplication on the set of right cosets modulo H. This G-set is denoted by G/H. We shall denote by $c(H)$ the intersection of all conjugates of H in G.

The following facts are well-known and easy to check.

(1) For any given group G the class of all G-sets is a variety. Its subvarieties are in one-to-one correspondence with the normal subgroups of G. The subvariety corresponding to a normal subgroup N is defined by the identities $xh = x$ for $h \in N$.
(2) If H is a subgroup of G, then the variety generated by G/H corresponds to the normal subgroup $c(H)$ of G.
(3) If H is a subgroup of G, then the congruence lattice of G/H is isomorphic to the lattice of all subgroups of G containing H.
(4) If H and K are two subgroups of G, then G/H and G/K are isomorphic G-sets iff H and K are conjugate subgroups of G.

Now let G be a finite nonabelian simple group. Embed each Sylow subgroup of G into a maximal subgroup of G. These maximal subgroups cannot all have the same index, therefore G has two maximal subgroups H and K that are not conjugate. Then G/H and G/K generate the same variety, they are clearly simple, critical, and are not isomorphic.

The theorem fails for G-sets. By the remarks on G-sets above, it is sufficient to find a finite group G and two subgroups H and K such that $c(H) = c(K) = 1$, (hence G/H and G/K generate the same variety as $G/1$), H is maximal (so $(\mathbf{HS} - 1)(G/H)$ is trivial, and hence G/H is critical), K is not maximal (so $(\mathbf{HS} - 1)(G/K)$ is nontrivial), and finally G/K is critical. This last condition is ensured, for example, if there is only one subgroup L of G strictly between K and G, and L contains a nontrivial normal subgroup of G (then

G/K has no proper subalgebras, and its only nontrivial factor is in a proper subvariety). These conditions can be realized, for example, when $G = A_4$ (the alternating group), L is its Klein-subgroup, H is a subgroup of order three, and K is a subgroup of order two.

There is a way to avoid the references to the facts above. The following nice idea has been shown to us by Keith Kearnes. Take G to be the symmetric group of degree four, with A (corresponding to G/H) being its normal action on a four element set. Realize G as the rotation group of the usual three-dimensional cube, let B be the set of all faces of the cube regarded as a G-set (corresponding to G/K). The only nontrivial congruence θ of B has three classes (pairs of opposite faces of the cube). The three-element G-set B/θ cannot be faithful, so var(B/θ) is a proper nontrivial variety of G-sets. Thus B is critical.

References

1. Bryant, R. M., *On S-critical groups*, Quart. J. Math. Oxford **22** (1971), 91–101.
2. Day, A., Kiss, E. W., *Frames and rings in congruence modular varieties*, Journal of Algebra **109** (1987), 479–507.
3. Freese, R., *On Jónsson's theorem*, Algebra Universalis **18** (1984), 70–76.
4. Freese, R., McKenzie, R., *Commutator theory for congruence modular varieties*, London Math. Soc. Lecture Notes Series, vol. 125, Cambridge University Press, 1987.
5. Gumm, H. P., *Geometrical methods in congruence modular algebras*, Memoirs of the AMS **45** (1983).
6. Jónsson, B., *Algebras whose congruence lattices are distributive*, Math. Scand. **21** (1967), 110–121.
7. Kiss, E. W., *On the Loewy rank of infinite algebras*, Algebra Universalis **29** (1992), 437–440.
8. Kovács, L. G., Newman, M. F., *On critical groups*, J. Austral Math. Soc. (1966), 237–250.
9. Mal'tsev, Yu. M., *Cross varieties of algebras*, DAN SSSR **278** (1984), 1060–1063.
10. Neumann, H., *Varieties of Groups*, Springer–Verlag, Berlin, 1967.
11. Vovsi, S. M., *On locally finite varieties of group representations*, Izv. VUZ Mat., 1971, No. 6, 16–27.
12. Vovsi, S. M., *On critical multioperator groups*, Sibirsk. Mat. Zh. **30** (1989), 213–215.
13. Valeriote, M. A., *Finite simple Abelian algebras are strictly simple*, Proceedings of the AMS **108** (1990), 49–57.

Emil W. Kiss: Lóránd Eötvös University, Department of Algebra and Number Theory, Múzeum körút 6–8, 1088. Budapest, HUNGARY

E-mail address: `ewkiss@ludens.elte.hu`

Samuel M. Vovsi: Trenton State College, Department of Mathematics and Statistics, Trenton, NJ 08650, USA

E-mail address: `vovsi@math.rutgers.edu, vovsi@math.trenton.edu`