CHAPTER 14

Automorphism Groups

J. Donald MONK
University of Coloradó

Contents

HANDBOOK OF BOOLEAN ALGEBRAS
Edited by J.D. Monk, with R. Bonnet

0. Introduction

In this chapter we describe what is known about automorphism groups of BAs, exclusive of results concerning rigid BAs which are treated in other chapters in this Handbook. No characterization is known of those groups isomorphic to $\mathrm{Aut}\,A$ for some BA A. In Section 1 we show how the general study of automorphism groups can be reduced to several cases: automorphism groups of products of rigid BAs, of products of homogeneous BAs, and of BAs with no rigid or homogeneous elements. Section 2 is devoted to the study of the relative automorphism group $\mathrm{Aut}_A\,B = \{f \in \mathrm{Aut}\,B\colon f \restriction A \text{ is the identity}\}$, when B is obtained from A by adjoining a single element (and hence all Boolean combinations of it with elements of A). These groups turn out to be very simple to describe and work with. Section 3 does the same when B is obtained from A by adjoining finitely many elements; then the situation is more complicated. Finally, in Section 4 we discuss the size of automorphism groups. In the general case a fairly complete description of the relationship between $|A|$ and $|\mathrm{Aut}\,A|$ is known, but there are still open problems when we restrict attention to classes of BAs such as interval algebras or superatomic BAs. Section 4 can be read directly after Section 1.

1. General properties

Direct product decompositions of BAs enable us to break the analysis of automorphism groups into several cases. Most of the results of this section are taken from McKenzie and Monk [1975]. We begin with these considerations.

1.1. Lemma. *If $\langle A_i\colon i \in I\rangle$ is a system of similar algebras, then $\Pi_{i\in I}\,\mathrm{Aut}\,A_i$ can be isomorphically embedded in $\mathrm{Aut}\,\Pi_{i\in I}\,A_i$.*

Proof. For each $f \in \Pi_{i\in I}\,\mathrm{Aut}\,A_i$, each $i \in I$, and each $x \in \Pi_{i\in I}\,A_i$ let $(Ff)_x i = f_i x_i$. It is easily verified that F is the desired isomorphic embedding. □

Now we shall call BAs A, B *totally different* if, for all $a \in A^+$ and $b \in B^+$, we have $A \restriction a \not\cong B \restriction b$.

In several of the proofs below we shall use the following construction. Given a system $\langle A_i\colon i \in I\rangle$ of BAs, an index $j \in I$, and an element $a \in A_j$, we denote by $\xi_j a$ the element of $\Pi_{i\in I}\,A_i$ such that $(\xi_j a)_i = 0$ if $i \neq j$, while $(\xi_j a)_j = a$.

1.2. Theorem. *If $\langle A_i\colon i \in I\rangle$ is a system of pairwise totally different BAs, then*

$$\prod_{i\in I} \mathrm{Aut}\,A_i \cong \mathrm{Aut} \prod_{i\in I} A_i\,.$$

Proof. We show that the function F defined in the proof of Lemma 1.1 is onto. Let $g \in \mathrm{Aut}\,\Pi_{i\in I}\,A_i$; we want to find $f \in \Pi_{i\in I}\,\mathrm{Aut}\,A_i$ such that $Ff = g$. To do this, we need three auxiliary statements.

(1) If $i \in I$, $x \in \prod_{i \in I} A_i$, and $(gx)_i \neq 0$, then $x_i \neq 0$.

For, assume otherwise. Let $y = \xi_i(gx)_i$. Thus, $y \leq gx$, so $g^{-1}y \leq x$. Choose j so that $(g^{-1}y)_j \neq 0$; thus $j \neq i$. Now $\xi_j(g^{-1}y)_j \leq g^{-1}y \leq x$, so $\langle (g\xi_j a)_i : a \leq (g^{-1}y)_j \rangle$ is an isomorphism from $A_j \restriction (g^{-1}y)_j$ onto $A_i \restriction (g\xi_j(g^{-1}y)_j)_i$, a contradiction. So (1) holds.

(2) If $i, j \in I$, $i \neq j$, and $a \in A_i$, then $(g\xi_i a)_j = 0$.

This is immediate from (1).

(3) If $i \in I$, then $g\xi_i 1 = \xi_i 1$.

For, by (2) write $g\xi_i 1 = \xi_i a$ and $g^{-1}\xi_i(-a) = \xi_i b$. Then $\xi_i b = \xi_i b \cdot \xi_i 1 = g^{-1}\xi_i(-a) \cdot g^{-1}\xi_i a = 0$, so $b = 0$ and $a = 1$. So (3) holds.

Now define $f_i a = (g\xi_i a)_i$ for any $i \in I$ and $a \in A_i$. By (2) and (3) it is clear that $f \in \Pi_{i \in I} \operatorname{Aut} A_i$. To show that $Ff = g$, let $x \in \Pi_{i \in I} A_i$ and $i \in I$; we show that $(Ff)_x i = (gx)_i$. Now $(Ff)_x i = f_i x_i = (g\xi_i x_i)_i$. Since $\xi_i x_i \leq x$, we have $(g\xi_i x_i)_i \leq (gx)_i$. Also, $(x \cdot -\xi_i x_i)_i = 0$, so by (1) $(gx \cdot -g\xi_i x_i)_i = 0$, i.e. $(gx)_i \leq (g\xi_j x_j)_i$, as desired. □

Theorem 1.2 has several useful corollaries. Thus, if $\langle A_i : i \in I \rangle$ is a system of pairwise totally different rigid BAs, then $\Pi_{i \in I} A_i$ is rigid. If A and B are totally different and B is rigid, then $\operatorname{Aut}(A \times B) \cong \operatorname{Aut} A$. If A is infinite and homogeneous and B is rigid, then $\operatorname{Aut}(A \times B) \cong \operatorname{Aut} A$.

At least for complete BAs, the study of Aut A breaks into three cases by the next theorem.

1.3. THEOREM. *Let A be a complete BA. Then there exist B, C, D such that $A \cong B \times C \times D$, B is a product of homogeneous BAs, C is a product of rigid BAs, and D has no rigid or homogeneous direct factors. Furthermore,* $\operatorname{Aut} A \cong \operatorname{Aut} B \times \operatorname{Aut} C \times \operatorname{Aut} D$.

PROOF. Let $a = \Sigma\{x : \forall y \in (A \restriction x)^+ \, \exists z \in (A \restriction y)^+ \; (A \restriction z \text{ is homogeneous})$, and let b be defined similarly with "homogeneous" replaced by "rigid". Then $A \restriction a$, $A \restriction b$, $A \restriction (-a \cdot -b)$ may be taken for B, C, D. □

The decomposition in Theorem 1.3 is clearly unique. It is natural now to consider the three cases in 1.3 in turn, even for non-complete BAs. First, however, we give a general fact about isomorphism of direct powers which will be used below.

1.4. THEOREM. *Let $|I| \leq \kappa \geq |J|$, let A be a κ^+-complete BA, and suppose that $\langle a_{ij} : i \in I, j \in J \rangle$ is a system of elements of A such that $\forall i \in I \; \langle A_{ij} : j \in J \rangle$ is a partition of unity and $\forall j \in J \; \langle a_{ij} : i \in I \rangle$ is a partition of unity (we allow zeros in a partition of unity). For any $x \in {}^I\!A$ and any $j \in J$ let $(fx)_j = \Sigma_{i \in I} x_i \cdot a_{ij}$. Then f is an isomorphism from ${}^I\!A$ onto ${}^J\!A$.*

PROOF. We define the inverse g of f. For any $y \in {}^J A$ and $i \in I$ let $(gy)_i = \Sigma_{i \in J} y_j \cdot a_{ij}$. Then for any $y \in {}^J A$ and $j \in J$ we have

$$(fgy)_j = \sum_{i \in I} (gy)_i \cdot a_{ij} = \sum_{i \in I} y_j \cdot a_{ij} = y_j .$$

Thus, $fgy = y$, so $f \circ g$ is the identity. Similarly, $g \circ f$ is the identity. Clearly, $x \leq z$ implies that $fx \leq fz$ for $x, z \in {}^I A$, and analogously for g, so f is the desired isomorphism. □

1.1. *Products of rigid BAs*

The following simple lemma will be fundamental for what follows.

1.5. LEMMA. *Let $a, b \in A^+$, $a \neq b$, and let f be an isomorphism from $A \upharpoonright a$ onto $A \upharpoonright b$. Then there exist disjoint non-zero $c \leq a$, $d \leq b$ such that $fc = d$.*

PROOF. If $a \not\leq b$ we let $c = a \cdot -b$, $d = f(a \cdot -b)$, while if $b \not\leq a$ we let $c = f^{-1}(b \cdot -a)$, $d = b \cdot -a$. □

This lemma has two immediate corollaries worth mentioning. If $f \in \operatorname{Aut} A$ is non-trivial (i.e. not the identity), then there is an $a \in A^+$ with $a \cdot fa = 0$; hence, $A \cong B \times B \times C$, where $B = A \upharpoonright a$ and $C = A \upharpoonright (-a \cdot -fa)$. If A is rigid, then $A \upharpoonright a \not\cong A \upharpoonright b$ for any two distinct elements $a, b \in A$.

It can also be shown that for an BA A, Aut A has a non-trivial center iff $A \cong B \times B \times C$ for some non-trivial rigid B and some C such that B and C are totally different; see MCKENZIE and MONK [1975, Theorem 1.16].

From Lemma 1.5 it follows in particular that if Aut A is non-trivial, then it has an element of order 2 – hence not every group is the automorphism group of a BA. This result can be generalized as follows.

1.6. THEOREM. *Let A be an infinite BA, and G the direct sum of $|A|$ copies of the two-element group. Then* $\operatorname{Aut}(A \times A)$ *has a subgroup isomorphic to G. In the case where A is rigid,* $\operatorname{Aut}(A \times A)$ *is actually isomorphic to G.*

PROOF. For each $a \in A$, let f_a be the automorphism of $A \times A$ pictured as follows:

$$\begin{aligned}(x, y) &\mapsto (x \cdot a, x \cdot -a, y \cdot a, y \cdot -a)\\ &\mapsto (y \cdot a, x \cdot -a, x \cdot a, y \cdot -a)\\ &\mapsto (y \cdot a + x \cdot -a, x \cdot a + y \cdot -a) .\end{aligned}$$

If $a, b \in A$ and $a \neq b$, say $a \cdot -b \neq 0$, then $f_b(a, 0) = (a \cdot -b, a \cdot b) \neq (0, a) = f_a(a, 0)$, so $f_a \neq f_b$. Clearly, f_a has order 2, and $f_a \circ f_b = f_b \circ f_a = f_{a \triangle b}$ for any a, $b \in A$. Hence, $\{f_a : a \in A\}$ is isomorphic to G.

Now let A be rigid, and let g be any automorphism of $A \times A$. Say $g(1, 0) = (a, b)$, and then choose c so that $g(c, 0) = (a, 0)$. The mapping

$x \mapsto (x, 0) \mapsto_g (y, 0) \mapsto y$ is an isomorphism of $A \upharpoonright c$ onto $A \upharpoonright a$, so by the above remarks, $a = c$. Thus, $g(a, 0) = (a, 0)$ and $g(1, 0) = g(a, 0) + g(-a, 0)$, so $g(-a, 0) = (0, b)$, and the above remarks give $b = -a$. Also by the same arguments, $g(0, 1) = (-a, a)$, $g(0, a) = (0, a)$, $g(0, -a) = (-a, 0)$. Hence,

$$\begin{aligned} g(x, y) &= g(x \cdot a + x \cdot -a,\ y \cdot a + y \cdot -a) \\ &= g(x \cdot a, 0) + g(x \cdot -a, 0) + g(0, y \cdot a) + g(0, y \cdot -a) \\ &= (x \cdot a, 0) + (0, x \cdot -a) + (0, y \cdot a) + (y \cdot -a, 0) \\ &= f_{-a}(x, y), \end{aligned}$$

and $g = f_{-a}$, finishing the proof. □

The subgroup of $\mathrm{Aut}(A \times A)$ constructed in the proof of 1.6 is not in general normal; for example, $\mathrm{Fr}\,\kappa \times \mathrm{Fr}\,\kappa \cong \mathrm{Fr}\,\kappa$, and $\mathrm{Aut}\,\mathrm{Fr}\,\kappa$ is simple, for $\kappa \geq \omega$.

1.7. COROLLARY. *If A is atomless and* Aut A *is non-trivial, then* $|\mathrm{Aut}\, A| \geq \aleph_1$.

1.8. COROLLARY. *If A is infinite and* Aut A *is finite, then A is isomorphic to some product $B \times C$, where B is finite, and C is infinite, atomless, and rigid. Furthermore,* Aut A *is then isomorphism to some finite symmetric group – namely to the group of all permutations of the atoms of B.*

After these preliminaries, we now discuss automorphisms of products of rigid BAs. The following result describes automorphisms of a power of a rigid (complete) BA A in terms of elements of A.

1.9. THEOREM. *Let $|I| \cup |J| = \kappa$, let A be a rigid κ^+-complete BA, and let $f: {}^IA \to {}^JA$. Then the following conditions are equivalent:*

(i) *f is an isomorphism from ${}^IA$ onto ${}^JA$.*

(ii) *There is an a satisfying the conditions of* 1.4 *with respect to f.*

PROOF. (ii)$\Rightarrow$(i) is given by Theorem 1.4. Now assume (i). For any $i \in I$ and $j \in J$ let $a_{ij} = (f\xi_i 1)_j$. Now $\langle \xi_1 1 : i \in I \rangle$ is a partition of unity, so

(4) $\langle a_{ij} : i \in I \rangle$ is a partition of unity for each $j \in J$.

(5) For any $x \in A$, $i \in I$, and $j \in J$, $f\xi_i(x \cdot a_{ij}) = \xi_j(x \cdot a_{ij})$.

For, we have $\xi_j(x \cdot a_{ij}) = \xi_j(x \cdot (f\xi_i 1)_j) \leq f\xi_i 1$, so choose u so that $f\xi_i u = \xi_j(x \cdot a_{ij})$. Now $\langle (f\xi_i y)_y : y \leq u \rangle$ is an isomorphism of $A \upharpoonright u$ onto $A \upharpoonright (x \cdot a_{ij})$, so $u = x \cdot a_{ij}$. Hence (5) follows.

(6) $\langle a_{ij} : j \in J \rangle$ is a partition of unity for each $i \in I$.

In fact, if $j, k \in J$ and $j \neq k$, then

$$0 = \xi_j a_{ij} \cdot \xi_k a_{ik} = f\xi_i a_{ij} \cdot f\xi_i a_{ik} \quad \text{by (5)},$$

so $\xi_i a_{ij} \cdot \xi_i a_{ik} = 0$ and hence $a_{ij} \cdot a_{ik} = 0$. Furthermore,

$$\begin{aligned} f\xi_i 1 &= \sum_{j\in J} \xi_j (f\xi_i 1)_j = \sum_{j\in J} \xi_j a_{ij} \\ &= \sum_{j\in J} f\xi_i a_{ij} \quad \text{by (5)} \\ &= f\xi_i \sum_{j\in J} a_{ij}, \end{aligned}$$

and hence $1 = \Sigma_{j\in J} a_{ij}$. So (6) holds.

(7) For any $x \in A$, $i \in I$, and $j \in J$, $(f\xi_i x)_j = x \cdot a_{ij}$.

For,

$$\begin{aligned} (f\xi_i x)_j &= \Big(f \sum_{k\in J} \xi_i (x \cdot a_{ij})\Big)_j \\ &= \sum_{k\in J} (f\xi_i (x \cdot a_{ik}))_j \\ &= \sum_{k\in J} (\xi_k (x \cdot a_{ik}))_j \quad \text{by (5)} \\ &= x \cdot a_{ij}, \end{aligned}$$

as desired. Finally, if $x \in {}^I A$ and $j \in J$, then

$$\begin{aligned} (fx)_j &= \Big(f \sum_{i\in I} \xi_i x_i\Big)_j = \sum_{i\in I} (f\xi_i x_i)_j \\ &= \sum_{i\in I} x_i \cdot a_{ij} \quad \text{by (7)}, \end{aligned}$$

and the proof is complete. □

The case $I = J$ in Theorem 1.9 gives a characterization of $\mathrm{Aut}({}^I A)$. In particular, we obtain:

1.10. COROLLARY. *If A is an infinite rigid BA and $2 \le m < \omega$, then* $|\mathrm{Aut}({}^m A)| = |A|$.

A characterization of $\mathrm{Aut}({}^m A)$ different from that in 1.9 can be given, still for $2 \le m < \omega$: for A rigid, $\mathrm{Aut}({}^m A)$ is isomorphic to the subgroup of ${}^{\mathrm{Ult}\,A}\mathrm{Sym}(m)$ consisting of all continuous functions $f\colon \mathrm{Ult}\,A \to \mathrm{Sym}(m)$, where $\mathrm{Sym}(m)$ has the discrete topology: see McKENZIE and MONK [1975, Theorem 1.12].

Having given a kind of characterization of $\mathrm{Aut}({}^I A)$ for A rigid, the next natural problem is to describe when ${}^I A$ and ${}^I B$ are isomorphic for A and B rigid. To do this, we make a slight digression.

An important notion for any BA A is its *invariant subalgebra*: $\mathrm{Inv}\, A = \{a \in$

A: $fa = a$ for every $f \in \operatorname{Aut} A\}$. Note that $0, 1 \in \operatorname{Inv} A$ and if $0 < a < 1$, then $a \in \operatorname{Inv} A$ iff $A \restriction a$ and $A \restriction (-a)$ are totally different.

1.11. THEOREM. *Let A be rigid and let I be a non-empty set. Then* $\operatorname{Inv}({}^I A)$ *is the diagonal subalgebra of* ${}^I A$, *consisting of all constant functions in* ${}^I A$; *in particular,* $\operatorname{Inv}({}^I A) \cong A$.

PROOF. For each $a \in A$, let c_a be the member of ${}^I A$ such that $c_a i = a$ for all $i \in I$. Then

(8) $\qquad fc_a = c_a$ for all $a \in A$ and all $f \in \operatorname{Aut} A$.

(We cannot obtain this from 1.9, since we have no completeness assumptions.) In fact, suppose that $fc_a \neq c_a$. Choose $i \in I$ so that $(fc_a)i \neq a$. Then $(fc_a)i \not\leq a$ or $a \not\leq (fc_a)i$. Assume that $(fc_a)i \not\leq a$, and let $b = (fc_a)i \cdot -a$. Thus, $\xi_i b \leq fc_a$, so $f^{-1}(\xi_i b) \leq c_a$. Since $b \neq 0$, there is a $j \in I$ such that $(f^{-1}(\xi_i b))j \neq 0$. Now $(f^{-1}(\xi_i b))j \leq a$, $\xi_j(f^{-1}(\xi_i b))j \leq f^{-1}(\xi_i b)$ and hence $f\xi_j(f^{-1}(\xi_i b))j \leq \xi_i b \leq \xi_i(-a)$. Hence, a and $-a$ are not totally different, contradicting the rigidity of A. $a \not\leq (fc_a)i$ is treated similarly. So (8) holds.

Now suppose that $x \in {}^I A$ and x is not a constant mapping. Choose $i, j \in I$ so that $x_i \not\leq x_j$. Let $a = x_i \cdot -x_j$, so that $a \neq 0$. Then $\xi_i a \leq x$ and $\xi_j a \leq -x$, so x and $-x$ are not totally different. Hence $x \notin \operatorname{Inv}({}^I A)$. $\square$

1.12. THEOREM. *If A, B are rigid, $I \neq 0 \neq J$, and ${}^I A \cong {}^J B$, then $A \cong B$. Moreover, if I is finite and $|A| > 1$, then $|I| = |J|$.*

PROOF. By 1.11, $A \cong B$. Now assume that I is finite. We show that $|J| \leq |I|$ so that, by symmetry, $|I| = |J|$. Suppose that $|J| > |I|$. Then ${}^I A$ has a system $\langle x^k : k \leq |I| \rangle$ of non-zero, pairwise disjoint, pairwise isomorphic elements. For any fixed $m \leq |I|$ it is easy to convert such a system into a similar one $\langle \bar{x}^k : k \leq |I| \rangle$ with the same properties, where additionally $\bar{x}^m \leq \xi_i 1$ for some i. Thus, in $|I| + 1$ steps we obtain such a system with $\forall m \leq |I|\ \exists im \in I\ (\bar{x}^m \leq \xi_{im} 1)$. Since A is rigid, it follows that for each $j \in I$, $\xi_j 1$ does not contain two disjoint non-zero isomorphic elements. Hence, i is a one-to-one function, a contradiction. $\square$

Note that for any non-trivial finite BA A, if ${}^I A \cong {}^J A$ then $|I| = |J|$. For any infinite BA A, if $|I| \leq |J| \leq \operatorname{sat} A$ and ${}^I A \cong {}^J A$, then $|I| = |J|$. In fact, $\operatorname{sat}({}^I A) = |I|^+ \cup \operatorname{sat} A$ and $\operatorname{sat}({}^J A) = |J|^+$, so this is clear. (Recall that $\operatorname{sat} A = \min\{\kappa : |X| < \kappa$ for every disjoint system $X \subseteq A\}$.) In the remaining cases we can have ${}^I A \cong {}^J A$ with $|I| \neq |J|$:

1.13. THEOREM. *Suppose $\omega \leq \mu \leq \lambda$. Then there is a rigid complete BA A such that ${}^\mu A \cong {}^\lambda A$.*

PROOF. Let B be freely generated by $\langle x_{\alpha\beta}: \alpha<\mu, \beta<\lambda\rangle$, and set

$$I=\langle\{x_{\alpha\beta}\cdot x_{\alpha\gamma}: \alpha<\mu, \beta, \gamma<\lambda, \beta\neq\gamma\}\cup \{x_{\alpha\beta}\cdot x_{\gamma\beta}: \beta<\lambda, \alpha, \gamma<\mu, \alpha\neq\gamma\}\rangle^{\mathrm{id}}.$$

Set $C=B/I$ and $a_{\alpha\beta}=[x_{\alpha\beta}]$ for all $\alpha<\mu$, $\beta<\lambda$, where $[x_{\alpha\beta}]$ is the image of $x_{\alpha\beta}$ under the natural map $B\to C$. We claim now:

$$\forall\alpha<\mu\Big(\sum_{\beta<\lambda} a_{\alpha\beta}=1\Big) \quad\text{and}\quad \forall\beta<\lambda\Big(\sum_{\alpha<\mu} a_{\alpha\beta}=1\Big). \tag{9}$$

By symmetry it suffices to prove the first part of (9). Assume that $\alpha<\mu$, $c\in C$, and $c\cdot a_{\alpha\beta}=0$ for all $\beta<\lambda$. Say $c=[y]$. There is a finite $\Gamma\subseteq\mu\times\lambda$ such that $y\in\{x_{\gamma\delta}: (\gamma, \delta)\in\Gamma\}$. Pick $\beta<\lambda$ such that $(\gamma, \beta)\not\in\Gamma$ for all γ. Now $y\cdot x_{\alpha\beta}\in I$, so we can write

$$\begin{aligned} y\cdot x_{\alpha\beta} \leq\ & x_{\gamma1,\delta1}\cdot x_{\gamma1,\varepsilon1}+\cdots+x_{\gamma m,\delta m}\cdot x_{\gamma m,\varepsilon m} \\ &+x_{\xi1,\eta1}\cdot x_{\gamma1,\eta1}+\cdots+x_{\xi n,\eta n}\cdot x_{\gamma n,\eta n}, \end{aligned} \tag{10}$$

with obvious assumptions. There is an endomorphism f of B such that $fx_{\theta\psi}=x_{\theta\psi}$ for all $(\theta, \psi)\in\Gamma$, $fx_{\alpha\beta}=1$, and $fx_{\theta\psi}=0$ if $(\theta, \psi)\not\in\Gamma$ and $(\theta, \psi)\neq(\alpha, \beta)$. Note that if $(\xi i, \eta i)=(\alpha, \beta)$, then $fx_{\gamma i,\eta i}=0$, and if $(\gamma i, \eta i)=(\alpha, \beta)$, then $fx_{\xi i,\eta i}=0$ $(i=1, \ldots, n)$. It follows that if we apply f to (10) and then apply the natural homomorphism of B onto C we get an expression of the form:

$$[y]\leq[x_{\alpha,\rho1}]+\cdots+[x_{\alpha,\rho p}].$$

Since $[y]\cdot[x_{\alpha,\rho i}]=0$ for each $i=1, \ldots, p$, it follows that $[y]=0$, as desired.

Now it is known that C can be completely embedded in a rigid complete BA A. By (9) and Theorem 1.4 our theorem follows. □

The above results give a fairly complete picture of possibilities for ${}^{I}A$, A rigid. Now we discuss how the powers ${}^{I}A$, ${}^{J}B$ can be combined.

1.14. LEMMA. *Let A be a complete BA with at least one non-trivial rigid element. (An element a is **rigid** provided that $A\restriction a$ is rigid.) Then there is a non-empty collection C of rigid, pairwise disjoint and isomorphic, non-zero elements of A such that $\Sigma\, C$ and $-\Sigma\, C$ are totally different.*

PROOF. Let y be a non-zero rigid element of A. By Zorn's lemma let D be a maximal family of pairwise disjoint elements of A each isomorphic to y, and with $y\in D$. For each $d\in D$ let f_d be an isomorphism of $A\restriction y$ onto $A\restriction d$. Let E be a maximal collection of pairwise disjoint elements $(d, e)\in(A\restriction y)\times(A\restriction -\Sigma\, D)$ such that $A\restriction d\cong A\restriction e$. For each $(d, e)\in E$ let g_{de} be an isomorphism of $A\restriction d$ onto $A\restriction e$. Let $z=\Sigma_{(d,e)\in E}\, d$, and set $x=y\cdot -z$. Then $x\neq 0$ since D is maximal, and x is rigid since $x \le y$. Let $C = \{f_u x: u \in D\}$. Thus, C is a collection of pairwise disjoint elements of A each isomorphic to x; also, $x \in C$ since $x = f_y x$ and $y \in D$. To complete the proof it suffices to derive a contradiction from the assumptions $0 \ne v \le \Sigma\, C$, $w \le -\Sigma\, C$, h an isomorphism from $A \restriction v$ onto $A \restriction w$. Choose $u \in D$ such that $v \cdot f_u x \ne 0$. Now there are three cases.

Case 1. $\exists t \in D[h(v \cdot f_u x) \cdot t \ne 0]$. Thus, $s \overset{\text{def}}{=} h(v \cdot f_u x) \cdot f_t z \ne 0$, since $f_t y = t$ and $f_t(y \cdot -z) = f_t x \le \Sigma\, C$ while $h(v \cdot f_u x) \le -\Sigma\, C$. Then $f_t^{-1}s$ and $f_u^{-1}h^{-1}s$ are isomorphic disjoint non-zero subelements of y, a contradiction; $f_t^{-1}s \le z$ and $f_u^{-1}h^{-1}s \le x$, so $f_t^{-1}s \cdot f_u^{-1}h^{-1}s = 0$.

Case 2. $\forall t \in D[h(v \cdot f_u x) \cdot t = 0]$ but $\exists (d, e) \in E[h(v \cdot f_u x) \cdot e \ne 0]$. This time $g_{de}^{-1}(h(v \cdot f_u x) \cdot e)$ and $f_u^{-1}h^{-1}(h(v \cdot f_u x) \cdot e)$ are isomorphic disjoint non-zero elements of y, a contradiction.

Case 3. $h(v \cdot f_u x) \le -\Sigma\, D \cdot -\Sigma_{(d,e)\in E}\, e$. Then $(f_u^{-1}(v \cdot f_u x), h(v \cdot f_u x)) \in (A \restriction y) \times (A \restriction -\Sigma\, D)$, $A \restriction f_u^{-1}(v \cdot f_u x) \cong A \restriction h(v \cdot f_u x)$, and $(f_u^{-1}(v \cdot f_u x), h(v \cdot f_u x)) \cdot (d, e) = 0$ for all $(d, e) \in E$, contradicting the maximality of E. $\square$

1.15. Theorem. *Let A be a complete BA in which the rigid elements are dense. Then there exists a system $\langle B_\alpha: \alpha < B \rangle$ of non-trivial pairwise totally different rigid BAs and a strictly increasing sequence $\langle \kappa\alpha: \alpha < \beta \rangle$ of non-zero cardinals such that $A \cong \Pi_{\alpha<\beta}\, {}^{\kappa\alpha}B_\alpha$.*

Proof. By an easy transfinite construction using Lemma 1.14 we can write $A \cong \Pi_{\alpha<\beta}\, {}^{\kappa\alpha}B_\alpha$, as in the theorem, except that $\langle \kappa\alpha: \alpha < \beta \rangle$ is just a sequence of non-zero cardinals. But we can assume that $\alpha < \gamma < \beta$ implies $\kappa\alpha \le \kappa\gamma$. Now for any $\alpha < \beta$ we have

$$\prod \{{}^{\kappa\gamma}B_\gamma: \kappa\alpha = \kappa\gamma\} = {}^{\kappa\alpha}\prod \{B_\gamma: \kappa\alpha = \kappa\gamma\}\,,$$

and by Theorem 1.2, $\Pi\, \{B_\gamma: \kappa\alpha = \kappa\gamma\}$ is rigid. The theorem follows. $\square$

The representation in Theorem 1.15 is not unique, by Theorem 1.13. It is possible to refine this representation so as to obtain uniqueness; see McKenzie and Monk [1975, Theorem 1.21].

1.2. Products of homogeneous BAs

Products of homogeneous algebras, and their automorphisms, can be analyzed much as for products of rigid algebras.

1.16. Theorem. *If A is a complete homogeneous BA and A has a disjoint family of size $|I|$, then ${}^I A \cong A$.*

1.17. Theorem. *If A and B are non-trivial homogeneous BAs, A has no disjoint family of size $|I|$, and ${}^I A \cong {}^J B$, then $|I| = |J|$ and $A \cong B$.*

PROOF. Let f be the isomorphism from ${}^{I}A$ onto ${}^{J}B$. A and B have isomorphic non-zero elements, so $A \cong B$. Suppose $|I| \neq |J|$; wlog say $|I| > |J|$. For each $j \in J$ let $K_j = \{i \in I: f(\xi_i 1)_j \neq 0\}$. Since A has no disjoint family of size $|I|$, each set K_j has power $<|I|$. Thus, for every $j \in J$, A has a disjoint family of size $|K_j| < |I|$, and $|I| = \Sigma_{j \in J} |K_j|$. Thus, $|I|$ is singular, so by the Erdös–Tarski theorem A has a disjoint family of size $|I|$, a contradiction. □

1.18. THEOREM. *Let A be a complete BA in which the homogeneous elements are dense. Then there is a non-decreasing sequence $\langle \kappa_\alpha : \alpha < \beta \rangle$ of non-zero cardinals and a system $\langle B_\alpha : \alpha < \beta \rangle$ of pairwise totally different, non-trivial, homogeneous BAs such that for every $\alpha < \beta$ with $\kappa_\alpha > 1$, B_α has no disjoint family of size κ_α, and $A \cong \Pi_{\alpha<\beta} {}^{\kappa_\alpha}B_\alpha$. The representation is unique: if $A \cong \Pi_{\alpha<\gamma} {}^{\lambda_\alpha}C_\alpha$ with similar conditions, then $\beta = \gamma$, $\kappa_\alpha = \lambda_\alpha$ for each $\alpha < \beta$, and for each $\alpha < \beta$ there is a permutation π of $\{\delta : \kappa_\delta = \kappa_\alpha\}$ such that $B_\delta \cong C_{\pi\delta}$ for each such δ.*

PROOF. Given any homogeneous element a of A, there is a maximal disjoint family C such that $a \in C$ and all elements of C are isomorphic. Thus, $\Sigma\, C$ and $-\Sigma\, C$ are totally different. Repeating this construction transfinitely, we easily arrive at the indicated representation.

Now suppose that another representation is given, as indicated; say f is an isomorphism from $\Pi_{\alpha<\beta} {}^{\kappa_\alpha}B_\alpha$ onto $\Pi_{\alpha<\beta} {}^{\lambda_\alpha}C_\alpha$. By Theorem 1.17 it suffices now to take any $\alpha < \beta$ and find $\delta < \gamma$ such that ${}^{\kappa_\alpha}B_\alpha \cong {}^{\lambda_\delta}C_\delta$. Since the C_δ's are pairwise totally different, we know that there is a unique $\delta < \gamma$ such that $(f\xi_\alpha 1)_\delta \neq 0$. Thus, ${}^{\kappa_\alpha}B_\alpha$ is isomorphic to an element of ${}^{\lambda_\delta}C_\delta$. Hence, $B_\alpha \cong C_\delta$ and $\kappa_\alpha \leq \lambda_\delta$. By symmetry, there is an $\varepsilon < \beta$ such that $C_\delta \cong B_\varepsilon$ and $\lambda_\delta \leq k_\varepsilon$. So $\alpha = \varepsilon$ and $\kappa_\alpha = \lambda_\delta$, as desired. □

This representation theorem has the following consequence for automorphisms: Aut A is isomorphic to $\Pi_{\alpha<\beta}$ Aut$({}^{\kappa_\alpha}B_\alpha)$. Thus, for a complete BA in which the homogeneous elements are dense, the automorphism problem reduces to considering automorphisms of complete BAs ${}^{I}A$, A homogeneous. Not much is known about these automorphisms. If A is homogeneous and complete, then Aut A is simple. See ŠTĚPÁNEK [Ch. 16 in this Handbook] and RUBIN [Ch. 15 in this Handbook] for more on automorphism of homogeneous BAs.

1.3. Products of BAs with no rigid or homogeneous factors

Not much is known about BAs of the kind mentioned. Complete BAs with no rigid or homogeneous factors were shown to exist in ŠTĚPÁNEK and BALCAR [1977]. See also KOPPELBERG [1978] and ŠTĚPÁNEK [1982]. An easy example of an incomplete BA with no rigid or homogeneous factor was given in BRENNER [1983]. See also ŠTĚPÁNEK [Ch. 16 in this Handbook].

To close this section we mention some open problems.

PROBLEM 1. If the isomorphism in the proof of Lemma 1.1 is onto, are the BAs pairwise totally different?

PROBLEM 2. Does the decomposition in Theorem 1.3 extend to incomplete BAs in some form?

PROBLEM 3. What can one say about $|\mathrm{Aut}({}^I A)|$ for A homogeneous?

2. Galois theory of simple extensions

Given BAs $A \subseteq B$, we let $\mathrm{Aut}_A B = \{f \in \mathrm{Aut}\, B: f \restriction A \text{ is the identity}\}$. Connections between $\mathrm{Aut}_A B$ and Boolean algebraic properties of the extension relation between A and B may loosely be called *Galois theory* for Boolean algebras. In this section and the next one we deal with this theory. As will be seen, the results are easy and may be considered as part of the folklore of this subject (especially by ring theorists). In this section we take the case in which B is a simple extension of A: $B = A(u) \stackrel{\text{def}}{=} \langle A \cup \{u\} \rangle$. In both the sections our treatment is quite elementary. Some of the results and formulations may seem more natural when expressed in terms of the sheaf theory described in Part I of this Handbook.

If $A \subseteq B$ and $u \in B$, we define two ideals I_0^u and I_1^u of A:

$$I_0^u = \{a \in A: a \cdot u = 0\},$$

$$I_1^u = \{a \in A: a \cdot -u = 0\}.$$

Ideals I and J in a BA A are *disjoint* if $I \cap J = \{0\}$.

2.1. THEOREM. (i) *Let $A(u)$ be a simple extension of A. Then I_0^u and I_1^u are disjoint ideals of A. Furthermore, $u \in A$ iff $I_0^u + I_1^u = A$.*

(ii) *Conversely, let J_0 and J_1 be disjoint ideals of A. Then there is a simple extension $A(u)$ of A such that $I_0^u = J_0$ and $I_1^u = J_1$. If $A(v)$ is any other simple extension of A with $I_0^v = J_0$, $I_1^v = J_1$, then there is an isomorphism of $A(u)$ onto $A(v)$ which is the identity on A.*

PROOF. The first part of (i) is clear. If $u \in A$, let $x \in A$ be arbitrary. Then $x = x \cdot -u + x \cdot u \in I_0^u + I_1^u$. So $I_0^u + I_1^u = A$. Conversely, suppose that $I_0^u + I_1^u = A$. Say $1 = x + y$ with $x \in I_0^u$, $y \in I_1^u$. Then $x \cdot y = 0$ since I_0^u and I_1^u are disjoint. Thus, $y = -x$. Now $x \cdot u = 0$ and $-x \cdot -u = 0$, so $x = -u$ and $u \in A$.

For (ii), define $F: A \to (A/J_0) \times (A/J_1)$ by $fa = (a/J_0, a/J_1)$ for all $a \in A$. Clearly, f is an isomorphism into. Since $(A/J_0) \times (A/J_1)$ is generated by $\mathrm{Rng}\, f \cup \{(1/J_0, 0/J_1)\}$, the existence of the desired $A(u)$ is clear. The uniqueness part follows from the Sikorski extension criterion. □

The automorphism groups $\mathrm{Aut}_A A(u)$ are characterized in the following theorem. In this theorem and several others below, Σ and Π refer to operations in the completion of A.

2.2. THEOREM. *Let $A(u)$ be a simple extension of A. Let $F = \{a \in A: a \cdot \Sigma (I_0^u + I_1^u) = 0\}$. Then $\langle F, \Delta \rangle$ is an abelian 2-group, and it is isomorphic to* $\mathrm{Aut}_A A(u)$

PROOF. For each $a \in F$ define $f_a\colon A(u) \to A(u)$ by setting $f_a x = x$ for all $x \in A$ and $f_a u = a \triangle u$; f_a extends to an endomorphism of $A(u)$ by Sikorski's extension criterion. In fact, if $x \in A$ and $x \cdot u = 0$, then $x \in I_0^u$, so $x \cdot a = 0$, hence $x \cdot (a \triangle u) = 0$; if $x \in A$ and $x \cdot -u = 0$, then $x \in I_1^u$, so $x \cdot a = 0$, hence $x \cdot -(a \triangle u) = x \cdot (a \cdot u + -a \cdot -u) = 0$. Now $f_a \circ f_a =$ identity, so f_a is an automorphism. Thus, $f\colon F \to \mathrm{Aut}_A A(u)$. It is easily checked that F is closed under Δ, hence $\langle F, \Delta \rangle$ is an abelian 2-group, and f is an isomorphism from F into $\mathrm{Aut}_A A(u)$. Now let $g \in \mathrm{Aut}_A A(u)$ be arbitrary. Write $gu = b \cdot u + c \cdot -u$ with b, $c \in A$. Now $b \cdot c \le gu$, so $b \cdot c = g^{-1}(b \cdot c) \le u$. Similarly, $-b \cdot -c \cdot gu = 0$ implies that $-b \cdot -c \cdot u = 0$. So $gu = (b + -c) \cdot u + (c \cdot -b) \cdot -u$. Let $a = c \cdot -b$. We claim that $a \in F$. To show this first let $x \in I_0^u$. Thus, $x \cdot u = 0$, so $x \cdot gu = 0$, hence $x \cdot c \cdot -b \cdot -u = 0$; but $x \cdot u = 0$ then yields $0 = x \cdot c \cdot -b = x \cdot a$. Second, let $x \in I_1^u$. Now $g(-u) = -gu = c \cdot -b \cdot u + (b + -c) \cdot -u$, so the same proof yields $x \cdot a = 0$ again. Thus, $x \in F$. Clearly, $f_a = g$. $\square$

By Theorems 2.1 and 2.2 the relative automorphism groups $\mathrm{Aut}_A A(u)$ can be of any size κ for which there a BA of size κ, namely 2^m for any $m \in \omega$, and any infinite κ.

Given a simple extension $A(u)$ of A, we denote by $F = F^{Au}$ the ideal F defined in Theorem 2.2, and by $f = f^{Au}$ the isomorphism defined there.

If $G \subseteq \mathrm{Aut}\, B$, we set $\mathrm{Fix}\, G = \{b \in B\colon gb = b \text{ for all } g \in G\}$.

2.3. THEOREM. *Let G be a subset of $\mathrm{Aut}_A A(u)$ and set $F' = \{a \in F^{Au}\colon f_a^{Au} \in G\}$. Then $\mathrm{Fix}\, G = \{c \cdot u + d \cdot -u\colon c, d \in A \text{ and } (c \triangle d) \cdot \Sigma F' = 0\}$.*

PROOF. To prove $\subseteq$, let $a \in F'$, $c, d \in A$, and $c \cdot u + d \cdot -u \in \mathrm{Fix}\, G$; we show that $(c \triangle d) \cdot a = 0$. We have

$$
\begin{aligned}
c \cdot u + d \cdot -u &= f_a(c \cdot u + d \cdot -u) \\
&= c \cdot -a \cdot u + c \cdot a \cdot -u + d \cdot a \cdot u + d \cdot -a \cdot -u\,.
\end{aligned}
$$

Hence, $c \cdot u = c \cdot -a \cdot u + d \cdot a \cdot u$, so $[(c \cdot a) \triangle (d \cdot a)] \cdot u = 0$. Similarly, $[(c \cdot a) \triangle (d \cdot a)] \cdot -u = 0$, so $(c \triangle d) \cdot a = 0$.

The inclusion $\supseteq$ is treated similarly. $\square$

Now we can characterize "closed" groups:

2.4. THEOREM. *Let $A(u)$ be a simple extension of A, let G be a subset of $\mathrm{Aut}_A A(u)$, and set $F' = \{a \in F^{Au}\colon f_a \in G\}$. Then the following conditions are equivalent:*

(i) $G = \mathrm{Aut}_{\mathrm{Fix}\, G} A(u)$.

(ii) $F' = \{a \in F^{Au}\colon a \le \Sigma F'\}$.

PROOF. (i)$\Rightarrow$(ii). Assume (i) and take any $a \in F^{Au}$ with $a \le \Sigma F'$; we show that $a \in F'$. To this end it suffices to take any $x \in \mathrm{Fix}\, G$ and show that $f_a x = x$. By Theorem 2.3, say $x = c \cdot u + d \cdot -u$ with $(c \triangle d) \cdot \Sigma F' = 0$. So $(c \triangle d) \cdot a = 0$, hence $x \in \mathrm{Fix}\{f_a\}$ by 2.3.

(ii)$\Rightarrow$(i). Assume (ii), and let $g \in \mathrm{Aut}_{\mathrm{Fix}\, G}\, A(u)$; we want to show that $g \in G$. Say $g = f_a$ with $a \in F^{Au}$; we need to show that $a \in F'$. Suppose $a \not\in F'$; then by (ii) $a \cdot -\Sigma\, F' \neq 0$; say $b \in A^+$ and $b \leq a \cdot -\Sigma\, F'$. By 2.3 we have $b \cdot u \in \mathrm{Fix}\, G$, so

$$b \cdot u = f_a(b \cdot u) = b \cdot -a \cdot u + b \cdot a \cdot -u\,.$$

So $b \cdot -u = 0$. Similarly, $b \cdot -u \in \mathrm{Fix}\, G$, hence $b \cdot u = 0$, so $b = 0$, a contradiction. □

Using 2.4 it is easy to construct examples of closed groups, and examples of non-closed groups. Also we can show:

2.5. THEOREM. *Let $A(u)$ be a simple extension of A. Then the following conditions are equivalent*:

(i) *For every subgroup G of $\mathrm{Aut}_A\, A(u)$ we have $G = \mathrm{Aut}_{\mathrm{Fix}\, G}\, A(u)$.*

(ii) $|\mathrm{Aut}_A\, A(u)| \leq 2$.

PROOF. Trivially (ii)$\Rightarrow$(i). Now suppose that $|\mathrm{Aut}_A\, A(u)| > 2$. By Theorem 2.2 choose $0 < b < a$ in F^{Au}. Let $G = \{Id, f_a\}$. By Theorem 2.3 it is clear that $f_b \in \mathrm{Aut}_{\mathrm{Fix}\, G}\, A(u)$. Hence $G \neq \mathrm{Aut}_{\mathrm{Fix}\, G}\, A(u)$. □

Now we consider the other aspect of Galois theory, namely closed algebras.

2.6. THEOREM. *For any simple extension $A(u)$ of A the following conditions are equivalent*:

(i) $A = \mathrm{Fix}\, \mathrm{Aut}_A\, A(u)$.

(ii) $I_0^u + I_1^u = \{x \in A\colon x \leq \Sigma\, (I_0^u + I_1^u)\}$.

PROOF. (i)$\Rightarrow$(ii). Assume (i), and let $x \in A$ with $x \leq \Sigma\, (I_0^u + I_1^u)$; we are supposed to show that $x \in I_0^u + I_1^u$. Now $x \cdot \Sigma\, F^{Au} = 0$, so by Theorem 2.3, $x \cdot -u \in \mathrm{Fix}\, \mathrm{Aut}_A\, A(u) = A$. Hence, also $x \cdot u \in A$, and $x = x \cdot -u + x \cdot u \in I_0^u + I_1^u$.

(ii)$\Rightarrow$(i). Assume (ii), and let $x \in \mathrm{Fix}\, \mathrm{Aut}_A\, A(u)$; we show that $x \in A$. By Theorem 2.3 write $x = c \cdot u + d \cdot -u$ with $c, d \in A$ and $(c \,\triangle\, d) \cdot \Sigma\, F = 0$. Now $\Sigma\, F = -\Sigma\, (I_0^u + I_1^u)$, so by (ii) choose $a \in I_0^u$ and $b \in I_1^u$ with $c \,\triangle\, d = a + b$. Then

$$\begin{aligned} x &= c \cdot -d \cdot u + d \cdot -c \cdot -u + c \cdot d \\ &= c \cdot -d \cdot b \cdot u + d \cdot -c \cdot a \cdot -u + c \cdot d \\ &= c \cdot -d \cdot b + d \cdot -c \cdot a + c \cdot d \in A\,. \quad \square \end{aligned}$$

Some special cases of simple extensions are of interest. There are two extreme cases: in the first, $|\mathrm{Aut}_A\, A(u)| = 1$, or equivalently, by Theorem 2.2, $I_0^u + I_1^u$ is dense in A. We then call $A(u)$ a *rigid* simple extension. The second extreme case occurs when u is independent over A, i.e. $a \cdot u \neq 0 \neq a \cdot -u$ for all $a \in A^+$. This is equivalent to saying that $I_0^u = I_1^u = \{0\}$. In this case we have $F^{Au} = A$ and $\mathrm{Fix}\, \mathrm{Aut}_A\, A(u) = A$.

It is of interest to see the connection of the observations in this section with the known Galois theory of commutative rings. We give some indications along these lines; see CHASE, HARRISON and ROSENBERG [1965], DEMEYER and INGRAHAM [1971], MAGID [1974], and VILLAMAYOR and ZELINSKY [1969] for the general theory and further references.

Suppose that $A \subseteq B$. We form the amalgamated free product $B \oplus_A B$. There is a homomorphism μ from $B \oplus_A B$ into B such that $\mu(b \oplus c) = b \cdot c$ for all $b, c \in B$. (For clarity we write $b \oplus c$ for $b \cdot c$, where b comes from the first factor B, and c from the second.) We say that B is a *separable extension* of A provided that there is a $u \in B \oplus_A B$ such that $\mu u = 1$ and $(\ker u) \cdot u = \{0\}$.

2.7. THEOREM. *If $A \subseteq B$, then B is a separable extension of A iff B is a finite extension of A.*

PROOF. $\Rightarrow$. Let $u \in B \oplus_A B$ be such that $\mu u = 1$ and $(\ker \mu) \cdot u = \{0\}$. Write $u = \Sigma_{i=1}^m b_i \oplus c_i$ with $c_i \cdot c_j = 0$ for $i \neq j$, each $c_i \neq 0$. Since $1 = \mu u = \Sigma_{i=1}^m b_i \cdot c_i$, it follows that $c_i \leq b_i$ for all i, and $\Sigma_{i=1}^m c_i = 1$. We may assume that $c_i = b_i$ for all i. Now we claim that $B = \langle A \cup \{c_1, \ldots, c_m\} \rangle$. Let $d \in B$. Then, since $(\ker \mu) \cdot u = \{0\}$, for any i, $(d \oplus (-d)) \cdot (c_i \oplus c_i) = 0$, so there is an $s_i \in A$ such that $d \cdot c_i \leq s_i$ and $-d \cdot s_i \cdot c_i = 0$. Hence $d \cdot c_i = s_i \cdot c_i$. Therefore

$$d = d \cdot \sum_{i=1}^m c_i = \sum_{i=1}^m s_i \cdot c_i ,$$

hence $d \in \langle A \cup \{c_1, \ldots, c_m\} \rangle$.

$\Leftarrow$. Let $B = \langle A \cup \{u_1, \ldots, u_m\} \rangle$. We may assume that $u_i \cdot u_j = 0$ for $i \neq j$, and $u_1 + \cdots + u_m = 1$. Set $v = \Sigma_{i=1}^m u_i \oplus u_i$. Thus, $\mu v = 1$. Now it is easily verified that $\ker \mu$ is generated by $\{d \oplus (-d) \colon d \in B\}$. So to check that $\ker \mu \cdot v = \{0\}$ it suffices to take any $d \in B$ and $1 \leq i \leq m$ and show that $(d \oplus (-d)) \cdot (u_i \oplus u_i) = 0$. Write $d = \Sigma_{i=1}^m s_i \cdot u_i$ with each $s_i \in A$. Then $d \cdot u_i = s_i \cdot u_i \leq s_i$ and $-d \cdot u_i = -s_i \cdot u_i \leq -s_i$, hence $[d \oplus -d] \cdot (u_i \oplus u_i) = 0$. □

Let B be any BA. Automorphisms f and g of B are *strongly distinct* if for every non-zero $b \in B$ there is an $s \in B$ such that $fs \cdot b \neq gs \cdot b$.

2.8. LEMMA. *If I_0^u or I_1^u is non-trivial, then no members of* $\mathrm{Aut}_A\, A(u)$ *are strongly distinct.*

PROOF. Say $0 \neq a \in I_0^u$. Let g and h be distinct members of $\mathrm{Aut}_A\, A(u)$. By 2.2, write $g = f_d$, $h = f_e$, with $d, e \in F^{Au}$. Then for any $s \in A(u)$ write $s = s_0 \cdot u + s_1 \cdot -u$. Then

$$\begin{aligned} f_d s \cdot a &= [s_0 \cdot (d \triangle u) + s_1 \cdot -(d \triangle u)] \cdot a \\ &= s_1 \cdot a , \end{aligned}$$

since $a \cdot u = 0$ and $a \cdot d = 0$. Similarly, $f_e s = s_1 \cdot a$. This shows that f_d and f_e are not strongly distinct. □

2.9. Lemma. *Assume that u is independent over A [hence $I_0^u = I_1^u = \{0\}$ and $F^{Au} = A$]. Let $d, e \in A$. Then the following conditions are equivalent*:

(i) *f_d and f_e are strongly distinct.*

(ii) *$d = -e$.*

Proof. (i)$\Rightarrow$(ii). Suppose that $d \neq -e$. Then there are two possibilities.

Case 1. $d + e \neq 1$. Say $0 \neq a \in A$ and $a \cdot d = 0 = a \cdot e$. Thus, $a \cdot u \neq 0$. Then for any $s \in A(u)$, say with $s = s_0 \cdot u + s_1 \cdot -u$, with $s_0, s_1 \in A$,

$$\begin{aligned} f_d s \cdot a \cdot u &= [s_0 \cdot (d \triangle u) + s_1 \cdot -(d \triangle u)] \cdot a \cdot u \\ &= s_0 \cdot a \cdot u \,, \end{aligned}$$

and similarly $f_e s \cdot a \cdot u = s_0 \cdot a \cdot u$, so f_d and f_e are not strongly distinct.

Case 2. $d \cdot e \neq 0$. Then $d \cdot e \cdot u \neq 0$ and for any $s \in A(u)$ as above, $f_d s \cdot d \cdot e \cdot u = s_1 \cdot d \cdot e \cdot u = f_e s \cdot d \cdot e \cdot u$, again showing that f_d and f_e are not strongly distinct.

(ii)$\Rightarrow$(i). Given $0 \neq b \in A(u)$, say wlog b has the form $c \cdot u$ with $c \in A$. Then $f_d(-u) \cdot c \cdot u = -(d \triangle u) \cdot c \cdot u = c \cdot d \cdot u$ and $f_{-d}(-u) \cdot c \cdot u = c \cdot -d \cdot u \neq c \cdot d \cdot u$. Hence, f_d and f_{-d} are strongly distinct. $\square$

Let $A \leq B$. We say that B is *Galois over A* if B is a separable extension of A and there is a finite subgroup G of strongly distinct members of $\mathrm{Aut}_A B$ such that $\mathrm{Fix}\, G = A$.

2.10. Theorem. *For $A(u)$ a simple extension of A the following conditions are equivalent*:

(i) *$A(u)$ is Galois over A*;

(ii) *$u \in A$ or u is independent over A.*

Proof. (i)$\Rightarrow$(ii): by Lemma 2.8. (ii)$\Rightarrow$(i): assume that u is independent over A. By Lemma 2.9, f_0 and f_1 are strongly distinct, so it suffices to show that $\mathrm{Fix}\{f_0, f_1\} = A$. Suppose that $b \in \mathrm{Fix}\{f_0, f_1\}$; say $b = b_0 \cdot u + b_1 \cdot -u$, with b_0, $b_1 \in A$. Then $b = f_1 b = b_0 \cdot (1 \triangle u) + b_1 \cdot -(1 \triangle u) = b_0 \cdot -u + b_1 \cdot u$, so $b_0 \cdot u = b_1 \cdot u$, hence $b_0 \triangle b_1 \in I_0^u = \{0\}$, hence $b_0 = b_1$. Thus $b \in A$. $\square$

Given $A \leq B$, we call B *weakly Galois over A* if there is a finite partition of unity $\langle a_i : i < m \rangle$ in A such that for each $i < m$, $B \restriction a_i$ is Galois over $A \restriction a_i$.

2.11. Theorem. *$A(u)$ is weakly Galois over A iff I_0^u and I_1^u are principal.*

Proof. $\Rightarrow$. Let $\langle a_i : i < n \rangle$ be a partition of unity in A such that $A(u) \restriction a_i$ is Galois over $A \restriction a_i$ for all $i < n$. Note that $A(u) \restriction a_i = (A \restriction a_i)(u \cdot a_i)$ for each $i < n$. Say by Theorem 2.10 that $u \cdot a_i \in A \restriction a_i$ for all $i < m$, while $u \cdot a_i$ is independent over $A \restriction a_i$ for $m \leq i < n$. Let $x = \Sigma_{i<m} -u \cdot a_i$, $y = \Sigma_{i<m} u \cdot a_i$. Thus, $x \in I_0^u$ and $y \in I_1^u$. Suppose that z is any member of I_0^u. Thus, $z \leq -u$. Suppose $z \cdot a_i \neq 0$ with $m \leq i < n$. Then $z \cdot a_i \cdot u \neq 0$, a contradiction. Hence, $z \leq x$. This shows that $I_0^u = \langle \{x\} \rangle^{\mathrm{id}}$. Similarly, $I_1^u = \langle \{y\} \rangle^{\mathrm{id}}$.

$\Leftarrow$. Say $I_0^u = \langle\{x\}\rangle^{\mathrm{id}}$ and $I_1^u = \langle\{y\}\rangle^{\mathrm{id}}$. Let $z = -x \cdot -y$. Then $\langle x+y, z\rangle$ is a partition of unity in A. Now $A(u) \upharpoonright (x+y) = A \upharpoonright (x+y)$. For, suppose that $b \in A(u) \upharpoonright (x+y)$. Thus, $b \leq x+y$ and, say, $b = c \cdot u + d \cdot -u$ with $c, d \in A$. Then $b \cdot x = d \cdot x \in A$ and similarly $b \cdot y \in A$, so $b \in A$. Also, $A(u) \upharpoonright z$ is Galois over $A \upharpoonright z$, in fact $u \cdot z$ is independent over $A \upharpoonright z$. For, suppose that $0 \neq b \in A \upharpoonright z$. If $b \cdot u \cdot z = 0$, then $b \cdot u = 0$, hence $b \in I_0^u$ and $b \leq x$ so $b = 0$, a contradiction. Similarly, $b \cdot -a \cdot z = 0$ is impossible. $\square$

3. Galois theory of finite extensions

It is more complicated to analyze the relative automorphism groups for arbitrary finite extensions. This was carried out by KOPPELBERG [1982] using sheaf theory. We present these results here in a non-sheaf setting. We begin with a generalization of Theorem 2.1. If $B = \langle A \cup F\rangle$ for some finite set F, where $A \leq B$, then we write $B = A(F)$. We call F *reduced* if it is a partition of unity, and for all distinct $u, v \in F$ we have $u \notin \langle A \cup (F\backslash\{u, v\})\rangle$. Any finite extension $A(F)$ can be written in the form $A(G)$, G reduced: just let G be a partition of unity such that $A(F) = A(G)$ of smallest cardinality – clearly possible. Note that if F is reduced, then $0 \notin F$. We call $\langle b_i : i < m\rangle$ reduced if $\{b_i : i < m\}$ is and the b_i's are distinct. If $\langle b_i : i < m\rangle$ is a finite system of elements, we set $A(b_0, \ldots, b_{m-1}) = A(\{b_0, \ldots, b_{m-1}\})$. A finite system $\langle I_i : i < m\rangle$ of ideals is an *extender* if the following conditions hold:

(1) $\qquad I_0 \cap \cdots \cap I_{m-1} = \{0\}$.

(2) $\qquad$ For all $i, j < m$ and all $a \in A$, if $a \in I_i$, then $-a \notin I_j$.

Given a finite partition of unity $u = \langle u_i : i < m\rangle$ in B, and $A \leq B$, we define an associated sequence of ideals $\langle J_i^u : i < m\rangle$ by

$$J_i^u = \{a \in A : a \cdot u_i = 0\}.$$

The following extension of Theorem 2.1 holds.

3.1. THEOREM. (i) *Let $\langle u_i : i < m\rangle$ be reduced in $A(u_0, \ldots, u_{m-1})$. Then $\langle J_i^u : i < m\rangle$ is an extender.*

(ii) *Conversely, let $\langle K_i : i < m\rangle$ be an extender. Then there is an extension B of A and a reduced system $\langle u_i : i < m\rangle$ in B such that $B = A(u_0, \ldots, u_{m-1})$ and $J_i^u = K_i$ for all $i < m$. If $C = A(v_0, \ldots, v_{m-1})$ with $\langle v_i : i < m\rangle$ a partition of unity and $J_i^v = K_i$ for all $i < m$, then there is an isomorphism g of B onto C such that $ga = a$ for all $A \in A$ and $gu_i = v_i$ for all $i < m$.*

PROOF. For (i), clearly $J_0^u \cap \cdots \cap J_{m-1}^u = \{0\}$. Now suppose that $i, j < m$, $a \in J_i^u$, and $-a \in J_j^u$. Then $a \cdot u_i = 0 = -a \cdot u_j$, so $i \neq j$ since $u_i \neq 0$. Then $u_i = (-\Sigma_{k\neq i,j}\, u_k) \cdot -a$, so $u_i \in \langle A \cup \{u_k : k \neq i, j\}\rangle$, a contradiction.

For (ii), let $B=\Pi_{i<m} A/K_i$, and define $g: A\rightarrow B$ by setting $(ga)_i = a/K_i$ for each $i<m$. Clearly, g is an isomorphism into. For each $i<m$ let $u_i\in B$ be defined by $u_i i=1$, $u_i j=0$ if $j\neq i$. Then $\langle u_i: i<m\rangle$ is a partition of unity, and $B=(g[A])(u_0,\ldots,u_{m-1})$. Also, clearly $J_i^u = g[K_i]$ for all $i<m$. To show that $\langle u_i: i<m\rangle$ is reduced, suppose that $i, j<m$, $i\neq j$, and $u_i\in\langle g[A]\cup\{u_k: k\neq i, j\}\rangle$. It is easily seen that

$$(*)\qquad \langle g[A]\cup\{u_k: k\neq i, j\}\rangle = \{b\in B: \text{for some } a\in A,\ b_i = a/K_i \text{ and } b_j = a/K_j\}\,.$$

Hence there is an $a\in A$ with $u_i i = a/K_i$ and $u_i j = a/K_j$. Thus, $a\in K_j$ and $-a\in K_i$, a contradiction. The final assertion of (ii) is clear by the Sikorski extension criterion. □

It is worth noting that not every finite extension is a simple extension. For, suppose that u is independent over A and $v\notin A(u)$. Then we claim that $A(u, v)$ is not a simple extension of A. For, suppose that $A(u,v)=A(w)$. Write $u = a\cdot w + b\cdot -w$, where $a, b\in A$. Then $a\cdot b\cdot -u=0$, so $a\cdot b=0$. Similarly, $-a\cdot -b=0$, so $b=-a$. Thus, $u=a\cdot w + -a\cdot -w$. Hence, $-u=-a\cdot w + a\cdot -w$, so $w = a\cdot u + -a\cdot -u\in A(u)$. Therefore $v\in A(u)$, a contradiction.

Now we shall give a (rather complicated) description of the members of $\mathrm{Aut}_A B$, where $B=A(u_0,\ldots,u_{m-1})$, with $\langle u_i: i<m\rangle$ reduced. For each $p\in \mathrm{Ult}\, A$, let $B_p = B/\langle p\rangle^{\mathrm{fi}}$, and let pr_p be the natural homomorphism from B onto B_p. Thus B_p is a finite BA, and its atoms are the non-zero elements in $\{pr_p u_0,\ldots, pr_p u_{m-1}\}$. Now if $g\in \mathrm{Aut}_A B$, then g induces an automorphism of B_p, hence a permutation of the atoms of B_p, hence a permutation of $\{0,\ldots, m-1\}$. Our description hinges on a characterization of these permutations. We denote by S_m the symmetric group of all permutations of $\{0,\ldots,m-1\}$.

Temporarily fix $p\in\mathrm{Ult}\,A$. If $i, j<m$, we write *$i\sim j$ at p* provided that there is a $c\in p$ such that for all $q\in \mathrm{Ult}\,A$ with $c\in q$ we have $-u_i\in\langle q\rangle^{\mathrm{fi}}$ iff $-u_j\in\langle q\rangle^{\mathrm{fi}}$. Clearly, this is an equivalence relation on m. It is easily checked that $i\sim j$ at p iff there is a $c\in p$ such that for all $a\in A\restriction c$, $a\in J_i^u$ iff $a\in J_j^u$. Next, if $\rho\in S_m$ we say that ρ is *compatible with p* if $i\sim \rho i$ at p for all $i<m$. Finally, if $g\in \mathrm{Aut}_A B$ and $\rho\in S_m$, we say that *g is induced by ρ at p* if for all $i<m$ we have $pr_p g u_i = pr_p u_{\rho i}$. (Note that g is uniquely determined "on B_p" by this last condition.) If one of these three relations holds – $i\sim j$ at p, ρ is compatible with p, g is induced by ρ at p – then there is a $c\in p$ such that the given relation holds for any q with $c\in q$ in place of p.

3.2. LEMMA. *Let $p\in \mathrm{Ult}\,A$ and $\rho\in S_m$. Then ρ is compatible with p iff there is a $g\in\mathrm{Aut}_A B$ which is induced by ρ at p.*

PROOF. First suppose that ρ is compatible with p. By a remark before this lemma, choose $c\in p$ such that for all $a\in A\restriction c$ and all $i<m$, $a\in J_i^u$ iff $a\in J_{\rho i}^u$. Sikorski's extension criterion yields an isomorphism g of B into B such that $g\restriction A$ is the identity and $gu_i = -c\cdot u_i + c\cdot u_{\rho i}$ for all $i<m$. Clearly, g maps onto B, and so

$g \in \mathrm{Aut}_A B$. To show that g is induced by ρ at p, take any $i < m$. Clearly, $-(gu_i \triangle u_{\rho i}) \in \langle p \rangle^{\mathrm{fi}}$, so $pr_p gu_i = pr_p u_{\rho i}$, as desired.

Now suppose that $g \in \mathrm{Aut}_A B$ is induced by ρ at p. Let $i < m$. Choose $c \in p$ such that $c \leq (-gu_i + u_{\rho i}) \cdot (gu_i + -u_{\rho i})$. Then for any $a \in A \restriction c$, $a \in J_i^u$ iff $a \cdot u_i = 0$ iff $a \in J_{\rho i}^u$. Hence, ρ is compatible with p. $\square$

Now we are ready for the theorem characterizing members of $\mathrm{Aut}_A B$. If T is a finite partition of unity in A, then a function $h\colon T \to S_m$ is *compatible with* T if for all $t \in T$ and all $p \in \mathrm{Ult}\, A$ with $t \in p$ we have that h_t is compatible with p.

3.3. THEOREM. (i) *Let T be a finite partition of unity in A, and suppose that $h\colon T \to S_m$ is compatible with T. Then there is a $g = g_h \in \mathrm{Aut}_A B$ such that, for all $i < m$,*

$$gu_i = \sum_{t \in T} t \cdot u_{h_t i} \,.$$

Moreover, g is induced by h_t at p whenever $t \in p$.

(ii) *For T a finite partition of unity in A, let $G_T = \{g_h\colon h\colon T \to S_m$ is compatible with $T\}$. Then G_T is a finite subgroup of* $\mathrm{Aut}_A B$.

(iii) *If H is a finite subset of* $\mathrm{Aut}_A B$, *then there is a finite partition T of unity in A such that $H \subseteq G_T$.*

PROOF. (i) For the existence of g it suffices to show that if $i < m$ and $t \in T$, then there is an isomorphism k of $B \restriction (t \cdot u_i)$ onto $B \restriction (t \cdot u_{h_t i})$ such that $k(a \cdot t \cdot u_i) = a \cdot t \cdot u_{h_t i}$ for all $a \in A$. To do this, it is enough to check that $a \cdot t \cdot u_i = 0$ iff $a \cdot t \cdot u_{h_t i} = 0$. Suppose that $a \cdot t \cdot u_i \neq 0$. Say $a \cdot t \cdot u_i \in q \in \mathrm{Ult}\, B$. Let $p = A \cap q$; so $p \in \mathrm{Ult}\, A$. Now $t \in p$, so h_t is compatible with p. Choose $c \in p$ so that for all $x \in A \restriction c$, $x \in J_i^u$ iff $x \in J_{h_t i}^u$. Now $a \cdot t \cdot u_i \cdot c \in q$, so $a \cdot t \cdot u_i \cdot c \neq 0$, hence $a \cdot t \cdot c \not\in J_i^u$. Therefore $a \cdot t \cdot c \not\in J_{h_t i}^u$, so $a \cdot t \cdot u_{h_t i} \neq 0$. The converse is similar. For the final statement of (i) assume that $t \in p$. Then for any $i < m$, $t \cdot gu_i = t \cdot u_{h_t i} \leq u_{h_t i}$ and $t \cdot u_{h_t i} \leq gu_i$, so $t \leq (-gu_i + u_{h_t i}) \cdot (-u_{h_t i} + gu_i)$, consequently $pr_p gu_i = pr_p u_{h_t i}$.

(ii) Obviously G_T is finite. The identity element of $\mathrm{Aut}_A B$ is g_h, where h_t is the identity for each $t \in T$. If h, $k\colon T \to S_m$ are compatible with T, then so is l, where $l_t = h_t \circ k_t$ for each $t \in T$, and $g_l = g_h \circ g_k$. If h is compatible with T, then so is k, where $k_t = h_t^{-1}$ for each $t \in T$, and $g_h^{-1} = g_k$. Thus, (ii) holds.

(iii) Temporarily fix $k \in H$; we construct a finite partition of unity T_k in A. For each $\rho \in S_m$ let

$$v_\rho^k = \{p \in \mathrm{Ult}\, A\colon \rho \text{ induces } k \text{ at } p\} \,.$$

Then v_ρ^k is an open subset of $\mathrm{Ult}\, A$ by the comment before Lemma 3.2. Furthermore,

$$(\dagger) \qquad \mathrm{Ult}\, A = \bigcup_{\rho \in S_m} v_\rho^k \,.$$

In fact, let $p \in \mathrm{Ult}\, A$. Define $\rho \in S_m$ as follows; let $i < m$. If $-u_i \in \langle p \rangle^{\mathrm{fi}}$, set $\rho i = i$; otherwise $ku_i / \langle p \rangle^{\mathrm{fi}}$ is an atom $u_j / \langle p \rangle^{\mathrm{fi}}$ of B_p, and we set $\rho i = j$. Clearly, ρ induces k at p, and so $p \in v_\rho^k$. That is, (†) holds.

By (†) and the compactness of Ult A, there is a partition of unity $\langle c_\rho^k : \rho \in S_m \rangle$ in A, $c_\rho^k = 0$ allowed, such that $sc_\rho^k \subseteq v_\rho^k$ for all $\rho \in S_m$. Clearly, if $c_\rho^k \in p \in \mathrm{Ult}\, A$, then ρ is compatible with p – this is the content of Lemma 3.2. We let T_k be the set of non-zero elements of $\{c_\rho^k : \rho \in S_m\}$. Then let T be the common refinement of all the partitions T_k for $k \in H$. To prove that $H \subseteq G_T$, let $k \in H$ be arbitrary. We define $h: T \to S_m$. Given $t \in T$, choose $h_t \in S_m$ so that $t \le c_{h_t}^k$. Now h is compatible with T, since if $t \in T$ and $p \in \mathrm{Ult}\, A$ with $t \in p$, then $c_{h_t}^k \in p$ and so h_t is compatible with p. We claim that $g_h = k$. To show this, take any $i < m$ and $t \in T$; we show that $g_h(t \cdot u_i) = k(t \cdot u_i)$. Now $g_h(t \cdot u_i) = t \cdot u_{h_t i}$ and $k(t \cdot u_i) = t \cdot ku_i$. Suppose that these are not the same. Say $t \cdot (u_{h_t i} \Delta ku_i) \in q \in \mathrm{Ult}\, B$ and set $p = A \cap q$. Thus $t \in p$, so $c_{h_t}^k \in p$. By construction, then, h_t induces k at p. Hence, $-(ku_i \Delta u_{h_t i}) \in \langle p \rangle^{\mathrm{fi}} \subseteq q$, a contradiction. This finishes the proof of Theorem 3.3. □

Recall that a group G is *locally finite* if every finitely generated subgroup of G is finite.

3.4. COROLLARY. $\mathrm{Aut}_A\, B$ *is locally finite.*

Now we discuss in the general finite extension case the general notions of ring theory mentioned in the previous section – Galois and weakly Galois BAs. First we have a simple lemma generalizing Lemma 2.8.

3.5. LEMMA. *If $a \le u_i$ for some $i < m$ and some $a \in A^+$, then no members of* $\mathrm{Aut}_A\, B$ *are strongly distinct.*

PROOF. By Theorem 3.3, we may assume that our two arbitrary members of $\mathrm{Aut}_A\, B$ have the form g_h, g_k, where $h, k: T \to S_m$ are compatible with T, T some finite partition of unity in A. Choose $t \in T$ so that $a \cdot t \ne 0$. We show that $g_h s \cdot a \cdot t = g_k s \cdot a \cdot t$ for any $s \in B$, so that g_h and g_k are not strongly distinct. Say $s = e_0 \cdot u_0 + \cdots + e_{m-1} \cdot u_{m-1}$, with $e_0, \ldots, e_{m-1} \in A$. Then, since $a \le u_i$,

$$g_h s \cdot a \cdot t = g_h(s \cdot a \cdot t) = g_h(s_i \cdot a \cdot t \cdot u_i) = g_h(s_i \cdot a \cdot t) = s_i \cdot a \cdot t\,.$$

Similarly, $g_k s \cdot a \cdot t = s_i \cdot a \cdot t$. □

For the next theorem, we say that C is a *relatively complete* subalgebra of D if $C \le D$ and for every $d \in D$ there is a smallest $c \in C$ such that $d \le c$; see, for example, HALMOS [1955].

3.6. THEOREM. *Let A and B be as above. Then the following conditions are equivalent*:

(i) *For every $i < m$, J_i^u is principal.*
(ii) *A is relatively complete in B.*

(iii) *There is a* $g \in \mathrm{Aut}_A B$ *such that* $gb \neq b$ *for all* $b \in B \backslash A$.
(iv) *There is a finite subgroup* G *of* $\mathrm{Aut}_A B$ *such that* $\mathrm{Fix}\, G = A$.

PROOF. (i)$\Rightarrow$(ii). Say $J_i^u = \langle a_i \rangle^{\mathrm{id}}$ for each $i < m$. Let $b \in B$; say $b = c_0 \cdot u_0 + \cdots + c_{m-1} \cdot u_{m-1}$ with $c_0, \ldots, c_{m-1} \in A$. Set $d = c_0 \cdot -a_0 + \cdots + c_{m-1} \cdot -a_{m-1}$. Thus, $b \leq d \in A$. Suppose $b \leq e \in A$. Then for any $i < m$, $c_i \cdot u_i = b \cdot u_i \leq e \cdot u_i$, so $c_i \cdot -e \cdot u_i = 0$, hence $c_i \cdot -e \leq a_i$, or $c_i \cdot -a_i \leq e$. Thus, $d \leq e$, as desired.

(ii)$\Rightarrow$(iii). Define $p \equiv q$ iff $p, q \in \mathrm{Ult}\, A$ and for all $i < m$, $-u_i \in \langle p \rangle^{\mathrm{fi}}$ iff $-u_i \in \langle q \rangle^{\mathrm{fi}}$. This is an equivalence relation on Ult A. Each equivalence class is open: let $p \in \mathrm{Ult}\, A$. For each $i < m$ let a_i be the smallest element of $A \geq u_i$ and let c_i be a_i or $-a_i$ depending on which is in p. Then $s(c_0 \cdot \cdots \cdot c_{m-1})$ is contained in the equivalence class of p. In fact, let $c_0 \cdot \cdots \cdot c_{m-1} \in q \in \mathrm{Ult}\, A$ and let $i < m$. If $-u_i \in \langle p \rangle^{\mathrm{fi}}$, then $b \leq -u_i$ for some $b \in p$. Thus, $u_i \leq -b$, so $a_i \leq -b$ and so $c_i = -a_i$. Hence, $-a_i \in q$ and so $-u_i \in \langle q \rangle^{\mathrm{fi}}$. The converse is similar. Thus, indeed, each equivalence class is open. Hence, there is a finite partition of unity T such that for each $t \in T$, st is contained in an equivalence class.

Let $t \in T$. Let $p \in \mathrm{Ult}\, A$ with $t \in p$. There is a permutation h_t of $\{0, \ldots, m-1\}$ such that $h_t i = i$ whenever $pr_p u_i = 0$, while $pr_p u_i \mapsto pr_p u_{h_t i}$ is a cyclic permutation of the atoms of B_p for $pr_p u_i \neq 0$. The equivalence property assures us that this definition does not need to depend on p. Clearly, h is compatible with T.

Now let $b \in B \backslash A$. Let $p \in \mathrm{Ult}\, A$ such that $b, -b \notin \langle p \rangle^{\mathrm{fi}}$. Say $t \in T$ with $t \in p$. By Theorem 3.3(i), g_h is induced by h_t at p. Since h_t is cyclic and $pr_p b$ is the sum of some, but not all, atoms of B_p, g_h moves b.

(iii)$\Rightarrow$(iv). This is clear by Theorem 3.3(ii), (iii).

(iv)$\Rightarrow$(i). Let $i < m$, and suppose that J_i^u is not principal. Then

$$(*) \qquad \{a \in A: -a \cdot u_i = 0\} \cup \{a \in A: \forall x \in (A \upharpoonright -a)^+ (x \cdot u_i \neq 0)\}$$

has the finite intersection property. In fact, otherwise we obtain:

$$a_1 \cdot \cdots \cdot a_n \cdot c_1 \cdot \cdots \cdot c_p = 0\,,$$

with $a_1, \ldots, a_n, c_1, \ldots, c_p \in A$, $-a_k \cdot u_i = 0$ for $k = 1, \ldots, n$, and $\forall x \in (A \upharpoonright -c_k)^+ (x \cdot u_i \neq 0)$ for $k = 1, \ldots, p$. So $c_1 \cdot \cdots \cdot c_p \leq -a_1 + \cdots + -a_n$, and hence $c_1 \cdot \cdots \cdot c_p \cdot u_i = 0$. Choose $d \in J_i^u$ with $c_1 \cdot \cdots \cdot c_p < d$. Then $d \cdot -(c_1 \cdot \cdots \cdot c_p) \neq 0$; say $d \cdot -c_k \neq 0$. But $d \cdot u_i = 0$, contradicting the choice of the c_k's. So $(*)$ holds.

Let $p \in \mathrm{Ult}\, A$ contain the set $(*)$. Now by Theorem 3.3(iii), we may assume that the subgroup G described in (iv) has the form G_T for some finite partition of unity T in A. Say $t \in T \cap p$. Let α be the equivalence class of i under the relation $\sim$ at p. By the remark before Lemma 3.2, choose $a \in p$ such that for every $q \in \mathrm{Ult}\, A$, if $a \in q$, then for any $j, k \in \alpha$ we have $j \sim k$ at q. Now we claim

$$(\dagger) \qquad \text{there is a } j \notin \alpha \text{ such that } -u_j \notin \langle p \rangle^{\mathrm{fi}}\,.$$

For, otherwise, for each $j \notin \alpha$ there is a $c_j \in p$ such that $c_j \leq -u_j$. By the definition of p (see $(*)$), there is then an element $x \in (A \upharpoonright \prod_{j \notin \alpha} c_j \cdot a)^+$ such that

$x \cdot u_i = 0$. If $x \in q \in \mathrm{Ult}\, A$, then $pr_q u_k = 0$ for all $k < m$, a contradiction. So (†) holds.

Let $b = a \cdot t \cdot \Sigma_{k \in \alpha} u_k$. Then $0 < pr_p b < 1$, using (†), so $b \notin A$. We claim that $gb = b$ for each $g \in G_T$ (contradicting (iv)). Say $g = g_h$, where $h: T \to S_m$ is compatible with T. Thus, h_t is compatible with p, and so h_t maps α into α. By Theorem 3.3(i) we have $g(a \cdot t \cdot u_k) = a \cdot t \cdot u_{h_t k}$ for each $k \in \alpha$, so $gb = b$. This finishes the proof of Theorem 3.6. □

We call $\langle u_i : i < m \rangle$ *independent over* A if for all $i < m$ and all $a \in A$ we have $a \cdot u_i \neq 0 \neq a \cdot -u_i$.

3.7. LEMMA. *If $\langle u_i : i < m \rangle$ is independent over A and A is a relatively complete subalgebra of B, then B is Galois over A.*

PROOF. Let σ be a cyclic permutation of $\{0, \ldots, m-1\}$. Then using the proof of Theorem 3.6(ii)⇒(iii), we choose $h: T \to S_m$ compatible with T such that $h_t = \sigma$ for all $t \in T$, and $\mathrm{Fix}\{g_h\} = A$. It suffices to show that the powers of g_h are strongly distinct. Suppose that k and l are such that $\sigma^k \neq \sigma^l$. Assume that v and w are associated with σ^k and σ^l, respectively, and let $0 \neq b \in B$. Say $b = e_0 \cdot u_0 + \cdots + e_{m-1} \cdot u_{m-1}$ with $e_0, \ldots, e_{m-1} \in A$. Say $e_i \cdot u_i \neq 0$, and choose $t \in T$ with $t \cdot e_i \cdot u_i \neq 0$. Let $\sigma^k j = i$. Then $v(t \cdot u_j) \cdot b = t \cdot e_i \cdot u_i$, while $w(t \cdot u_j) \cdot b = t \cdot e_s \cdot u_s$ for some $s \neq i$, so $v(t \cdot u_j) \cdot b \neq w(t \cdot u_j) \cdot b$, so v and w are strongly distinct. □

The converse of Lemma 3.7 does not hold. To see this, let A be a complete atomless BA, and suppose that $0 < a < 1$ in A. Using Theorem 3.1 it is easy to find an extension $B = A(u_0, u_1, u_2, u_3)$ of A such that $I_0^u = I_1^u = \langle a \rangle^{\mathrm{id}}$ and $I_2^u = I_3^u = \{0\}$, with $\langle u_i : i < 4 \rangle$ reduced. Then A is a relatively complete subalgebra of B, $\langle u_i : i < 4 \rangle$ is not independent over A, but B is Galois over A. The last statement is seen by the argument of the proof of Lemma 3.7, letting σ be the permutation $(0,1)(2,3)$.

We do not have a characterization of the Galois extensions, but there is one for the weakly Galois extensions:

3.8. THEOREM. *B is weakly Galois over A iff A is relatively complete in B.*

PROOF. ⇒. Say $\langle a_i : i < n \rangle$ is a finite partition of unity in A such that $B \restriction a_i$ is Galois over $A \restriction a_i$ for each $i < n$. By Theorem 3.6, $A \restriction a_i$ is relatively complete in $B \restriction a_i$ for all $i < n$. Hence, A is relatively complete in B.

⇐. For each $i < m$ choose $a_i \in A$ maximum such that $a_i \leq -u_i$. Then for each $E \subseteq m$ set

$$c_E = \prod_{i \in E} a_i \cdot \prod_{i \in m \setminus E} -a_i\,.$$

Let $X = \{c_E : E \subseteq m\} \setminus \{0\}$. Thus, X is a finite partition of unity. For $E \subseteq m$ and $c_E \neq 0$, $B \restriction c_E$ is generated by $A \restriction c_E \cup \{u_i \cdot c_E : i \in m \setminus E\}$. If $x \in A \restriction c_E$, $i \in m \setminus E$, and $x \cdot u_i \cdot c_E = 0$, then $x \leq -u_i$, so $x \leq a_i$ and hence $x = 0$. Thus, for each such E there is a subset F of $\{u_i \cdot c_E : i \in m \setminus E\}$ which is reduced, and independent over A – so $B \restriction c_E$ is Galois over $A \restriction c_E$. This finishes the proof. □

4. The size of automorphism groups

In this section we present the known results (mainly from McKENZIE and MONK [1975]) concerning the relationships between $|A|$ and $|\mathrm{Aut}\, A|$, more precisely, those provable in ZFC. As we shall see, under GCH all the a priori possible relations between these two cardinals are true.

The results depend on the following basic theorem. (It is also found in MONK [Ch. 13 in this Handbook] in a stronger form, with a more complicated proof.)

4.1. THEOREM. *There is an atomic BA A of power 2^ω with $|\mathrm{Aut}\, A| = \omega$.*

PROOF. Let $\langle f_\xi : \xi < 2^\omega \rangle$ enumerate all of the permutations of ω which move infinitely many integers. Now we shall define two sequences: a sequence $\langle A_\xi : \xi \leq 2^\omega \rangle$ of subalgebras of $\mathscr{P}\omega$, and a sequence $\langle B_\xi : \xi \leq 2^\omega \rangle$ of subsets of $\mathscr{P}\omega$, so that for all $\xi \leq 2^\omega$ we have $|A_\xi|, |B_\xi| \leq |\xi| + \omega$ and $A_\xi \cap B_\xi = 0$. To start with, we let A_0 be the BA of finite and cofinite subsets of ω, and $B_0 = 0$. For λ a limit ordinal $\leq 2^\omega$ we set $A_\lambda = \bigcup_{\xi<\lambda} A_\xi$, $B_\lambda = \bigcup_{\xi<\lambda} B_\xi$. The step from $\xi < 2^\omega$ to $\xi + 1$ is the essential thing.

Choose I infinite, $I \subseteq \omega$, so that $I \cap f_\xi[I] = 0$. The following claim is the heart of the proof:

(1) there is an infinite $J \in \mathscr{P}I \backslash A_\xi$ such that $\langle A_\xi \cup \{J\} \rangle \cap (B_\xi \cup \{f_\xi[J]\}) = 0$.

Suppose that (1) fails. Thus,

(2) for every infinite $J \in \mathscr{P}I \backslash A_\xi$ there exist $C, D \in A_\xi$ such that $(C \cap J) \cup (D \backslash J) \in B_\xi \cup \{f_\xi[J]\}$.

Let K_0 be a family of pairwise almost disjoint infinite subsets of I with $|K_0| = 2^\omega$. Then by (2) and the condition $|A_\xi| \leq |\xi| + \omega$ there exist $C, D \in A_\xi$ such that the set

$$K_1 = \{J \in K_0 \backslash A_\xi : (C \cap J) \cup (D \backslash J) \in B_\xi \cup \{f_\xi[J]\}\}$$

has power $> |A_\xi| \cup |B_\xi|$. Now

(3) there exist at most two $J \in K_1$ such that $(C \cap J) \cup (D \backslash J) = f_\xi[J]$.

For suppose: there are at least three such, J_0, J_1, J_2. Now $f_\xi[J_i] \cap J_i = 0$, so $D \backslash J_i = f_\xi[J_i]$ for $i < 3$. Hence,

$$\begin{aligned} f_\xi[J_0 \cap J_1] \cup f_\xi[J_0 \cap J_2] &= (f_\xi[J_0] \cap f_\xi[J_1]) \cup (f_\xi[J_0] \cap f_\xi[J_2]) \\ &= [D \backslash (J_0 \cup J_1)] \cup [D \backslash (J_0 \cup J_2)] \\ &= (D \backslash J_0) \cap [\omega \backslash (J_1 \cap J_2)] ; \end{aligned}$$

but the first set is finite and the last cofinite, a contradiction. So (3) holds.

Let K_2 be K_1 without the J's of (3). Since $|K_2| > |B_\xi| + \omega$, there is an $E \in B_\xi$ such that the set

$$K_3 = \{J \in K_2 : (C \cap J) \cup (D \backslash J) = E\}$$

has at least two elements J, H. Then

$$E = [(C \cap J \cap H) \cup D] \backslash [(D \cap H \cap J) \backslash E] \in A_\xi \,,$$

a contradiction. Hence (1) holds.

Choose J as in (1). Let $A_{\xi+1} = \langle A_\xi \cup \{J\} \rangle$, $B_{\xi+1} = B_\xi \cup \{f_\xi[J]\}$. This finishes the construction. Let $A = A_\alpha$, where $\alpha = 2^\omega$. Clearly, $|A| = 2^\omega$. A is a subalgebra of $\mathcal{P}\omega$ containing all singletons. As such, each automorphism of A is induced by a permutation of ω. Each finite permutation of ω induces an automorphism of A. These are the only automorphisms of A. For suppose that g is an automorphism of A induced by the non-finite permutation f of ω. Say $f = f_\xi$ with $\xi < \omega$. Then with J as in the construction we have $J \in A$ but $gJ = f_\xi[J] \notin A$, a contradiction. □

From Theorem 4.1 we can obtain at once the main facts about the size of automorphism groups:

4.2. THEOREM. (i) *If $m \in \omega$, $m \neq 0$, and $\kappa > \omega$, then there is a BA A with $|A| = \kappa$ and* $|\mathrm{Aut}\ A| = m!$. *For any infinite BA B with $|\mathrm{Aut}\ B| < \omega$ we have $|\mathrm{Aut}\ B| = m!$ for some positive integer m.*

(ii) *If $2^\omega \leq \kappa$, then there is a BA A such that $|\mathrm{Aut}\ A| = \omega$ and $|A| = \kappa$.*

(iii) *If $\omega < \kappa \leq \lambda$, then there is a BA A with $|A| = \lambda$ and $|\mathrm{Aut}\ A| = \kappa$.*

(iv) *If $\omega \leq \kappa$, then there is a BA A with $|A| = \kappa$ and $|\mathrm{Aut}\ A| = 2^\kappa$.*

PROOF. We already proved (i) in Corollary 1.8. For (ii), let A be the BA given in Theorem 4.1: $|A| = 2^\omega$, $|\mathrm{Aut}\ A| = \omega$, A atomic, and let B be an atomless rigid BA of power κ. Then $A \times B$ is as desired, by Theorem 1.2. For (iii), let A be a rigid BA of power κ and B a rigid BA of power λ such that A and B are totally different. Then $A \times A \times B$ is the desired algebra, by Theorems 1.2 and 1.6. Finally, for (iv) take A to be the free BA on κ generators. □

Theorem 4.2 does not say anything about denumerable BAs. We now show that in this case the automorphism groups are always of size 2^ω. Actually, the proof also gives one of the consistency results concerning possible improvements of Theorem 4.2.

4.3. THEOREM. *If the κ-Martin's axiom holds, and A is a BA with infinitely many atoms with $|A| = \kappa$, then the symmetric group on ω can be isomorphically embedded in* Aut A.

PROOF. We shall apply Theorem 2.2 of MARTIN and SOLOVAY [1970]. To this end let a be a one-to-one mapping of ω into the set of atoms of A. Clearly, there is an ultrafilter F on A such that $x \in F$ whenever $\{i \in \omega: a_i \leq -x\}$ is finite. Set $B = \{J \subseteq \omega: \text{for some } x \in F, J = \{i \in \omega: a_i \leq x\}\}$ and $C = \{J \subseteq \omega: \text{for some } x \in F, J = \{i \in \omega: a_i \cdot x = 0\}\}$. If $J \in B$ and $\mathcal{K}$ is a finite subset of C, say $J = \{i \in \omega: a_i \leq x_J\}$ with $x_J \in F$, and $K = \{i \in \omega: a_i \cdot x_K = 0\}$ with $x_K \in F$, for each $K \in \mathcal{K}$. Then $x_J \cdot \Pi_{k\in\mathcal{K}} x_K \in F$, and $a_i \leq x_J \cdot \Pi_{k\in\mathcal{K}} x_K$ implies that $i \in J \setminus \bigcup \mathcal{K}$. It follows that $J \setminus \bigcup \mathcal{K}$ is infinite, since otherwise $-(x_J \cdot \Pi_{K\in\mathcal{K}} x_K) \in F$. So Theorem 2.2 of MARTIN and SOLOVAY [1970] applies, and we infer:

(1) there is a $D \subseteq \omega$ such that $J \cap D$ is finite for each $J \in C$ and infinite if $J \in B$.

Let $E = \{a_i: i \in D\}$. Then by (1),

(2) for all $x \in A \setminus F$ the set $\{e \in E: e \leq x\}$ is finite; and E is infinite.

By (2), we can write each $x \in A \setminus F$ in the form $t_x + \Sigma M_x$, where no member of E is $\leq t_x$, and M_x is a finite subset of E. For any permutation f of E and any $x \in A \setminus F$ we set

$$f^+ x = t_x + \sum_{e \in M_x} fe ;$$

if $x \in F$ we set $f^+ x = -f^+(-x)$. It is routine to check that f^+ is an automorphism of A and f is an isomorphism of the symmetric group on E into Aut A. □

4.4. COROLLARY. *If* $|A| = \omega$, *then* $|\text{Aut } A| = 2^\omega$.

4.5. COROLLARY. *If Martin's axiom holds and* $|\text{Aut } A| = \omega$, *then* $|A| \geq 2^\omega$.

PROOF. By Corollary 1.7, A has infinitely many atoms. Hence, the corollary follows from 4.3. □

These are all the results provable in ZFC that we know concerning the size of automorphism groups of arbitrary BAs. Under GCH, the results are complete. Thus, let κ and λ be cardinals, with λ infinite. Then the following conditions are equivalent under GCH:

(A) There is a BA A such that $|\text{Aut } A| = \kappa$ and $|A| = \lambda$.

(B) One of the following holds:

(1) $\kappa = m!$ for some positive integer m, and $\lambda > \omega$;

(2) $\lambda = \omega$ and $\kappa = \omega_1$;

(3) $\lambda > \omega$ and $\omega \leq \kappa \leq \lambda^+$.

There are consistency results with not(GCH) also. Thus, from Theorem 4.17 in MONK [Ch. 13 in this Handbook] it follows that it is consistent that if $\omega < \kappa \leq 2^\omega$, then there is a BA A with $|\text{Aut } A| = \omega$ and $|A| = \kappa$, where 2^ω can be large. For further results along these lines see VAN DOUWEN [1980] and ROITMAN [1981].

Now we consider the size of automorphism groups of special kinds of BAs, namely complete BAs, atomic BAs, interval algebras, and superatomic BAs.

For complete BAs, the main new fact is as follows (KOPPELBERG [1981]):

4.6. THEOREM. *If A is a complete BA and $|\mathrm{Aut}\, A|$ is infinite, then* $|\mathrm{Aut}\, A|^{\omega} = |\mathrm{Aut}\, A|$.

PROOF. By Theorem 1.3 we can write $A \cong B_0 \times B_1 \times C \times D$, where B_0 is atomic, B_1 is an atomless product of homogeneous algebras, C is a product of rigid BAs, and D has no rigid or homogeneous direct factors. Note that if E is homogeneous, then

$$\begin{aligned} |{}^{\omega}\mathrm{Aut}\, E| &\le |\mathrm{Aut}^{\omega}\, E| && (1.1) \\ &= |\mathrm{Aut}\, E| && (1.16) \\ &\le |{}^{\omega}\mathrm{Aut}\, E|\,. \end{aligned}$$

Hence, by 1.2 and 1.18, $|\mathrm{Aut}\, B_1|^{\omega} = |\mathrm{Aut}\, B_1|$.

Hence, it suffices to show that $|\mathrm{Aut}(C \times D)|^{\omega} = |\mathrm{Aut}(C \times D)|$. Now $C \times D$ has no homogeneous direct factors. Hence, from ŠTĚPÁNEK [Ch. 16, 3.13, in this Handbook] we know that $\mathrm{inv}(C \times D)$ is atomless (see the definition before 1.11). Let X be a partition of unity in $\mathrm{inv}(C \times D)$ satisfying the following conditions:

(1) for all $x \in X$ and all $a, b \in ((C \times D) \restriction x)^{+}$, $|\mathrm{Aut}((C \times D) \restriction a)| = |\mathrm{Aut}((C \times D) \restriction b)|$.

(2) if $x \in X$, then there are infinitely many $y \in X$ such that $|\mathrm{Aut}((C \times D) \restriction x)| = |\mathrm{Aut}((C \times D) \restriction y)|$.

(We need $\mathrm{inv}(C \times D)$ atomless to get (2).) Since x and y are totally different for distinct $x, y \in X$, we get

$$|\mathrm{Aut}(C \times D)| = \prod_{x \in X} |\mathrm{Aut}((C \times D) \restriction x)| = \kappa^{\omega}$$

for some κ, as desired. □

Theorem 4.6 shows that the following theorem cannot be improved in ZFC.

4.7. THEOREM. (i) *If $m \in \omega$, $m \neq 0$, $\kappa \ge \omega$, and $\kappa^{\omega} = \kappa$, then there is a complete BA A with $|A| = \kappa$ and $|\mathrm{Aut}\, A| = m!$.*

(ii) *If $\omega < \kappa \le \lambda$, $\kappa^{\omega} = \kappa$, $\lambda^{\omega} = \lambda$, then there is a complete BA A with $|A| = \lambda$ and $|\mathrm{Aut}\, A| = k$.*

(iii) *If $\omega \le \kappa = \kappa^{\omega}$, then there is a complete BA A with $|A| = \kappa$ and $|\mathrm{Aut}\, A| = 2^{\kappa}$.*

Turning to atomic BAs, note first that if A is atomic, then any finite permutation of the atoms of A extends to an automorphism of A. Hence, in this case we have the restrictions $|\mathrm{At}\, A| \le |\mathrm{Aut}\, A| \le 2^{|A|}$. Our main result for atomic BAs is the following generalization of Theorem 4.1 and its proof. We use this notation – if κ and λ are infinite cardinals, then

$$\mathrm{Sym}\,\kappa = \{f: f \text{ is a permutation of } \kappa\}\,;$$

$$\mathrm{Supp}\,f = \{\alpha < \kappa: f\alpha \neq \alpha\} \text{ for } f \in \mathrm{Sym}\,\kappa:$$

$$\mathrm{Sym}_{<\lambda}\,\kappa = \{f \in \mathrm{Sym}\,\kappa: |\mathrm{Supp}\,f| < \lambda\}\,.$$

4.8. THEOREM. *Let $\omega \leq \lambda \leq \kappa$. Then there is a BA $A \subseteq \mathscr{P}\kappa$ with $|A| = 2^\kappa$ such that $[\kappa]^{<\lambda} \subseteq A$ and* Aut A *is naturally isomorphic to* $\mathrm{Sym}_{<\lambda}\,\kappa$.

PROOF. Let $\langle f_\xi: \xi < 2^\kappa \rangle$ enumerate $\mathrm{Sym}\,\kappa \backslash \mathrm{Sym}_{<\lambda}\,\kappa$. We call two subsets X, $Y \subseteq \kappa$ *equivalent modulo* $[\kappa]^{<\lambda}$ if $X \triangle Y \in [\kappa]^{<\lambda}$. Let $\langle X_\alpha: \alpha < 2^\kappa \rangle$ be a system of subsets of κ which are independent modulo $[\kappa]^{<\kappa}$, that is, so that $\langle X_\alpha/[\kappa]^{<\kappa}: \alpha < 2^\kappa \rangle$ is a system of independent elements of $\mathscr{P}\kappa/[\kappa]^{<\kappa}$.

Now we construct by transfinite recursion two sequences $\langle Y_\alpha: \alpha < 2^\kappa \rangle$ and $\langle B_\alpha: \alpha < 2^\kappa \rangle$; each Y_α will be a subset of κ, and each B_α a subset of 2^κ such that $|B_\alpha| \leq \omega + |\alpha|$. The only essential part of the construction is to do this so that the following condition holds:

(1) for each $\beta < 2^\kappa$, $\langle Y_\alpha: \alpha \leq \beta \rangle \cup \langle X_\alpha: \beta < \alpha < 2^\kappa, \alpha \not\in B_\beta \rangle$ is independent modulo $[\kappa]^{<\kappa}$, and for all $\xi \leq \beta$, $f_\xi[Y_\xi] \not\in \langle \{Y_\alpha: \alpha \leq \beta\} \cup [\kappa]^{<\lambda} \rangle$.

Let γ be $<2^\kappa$ so that Y_β and B_β have been defined for all $\beta < \gamma$ so that (1) holds. The rest of the proof is to construct Y_γ and B_γ. To begin with, let $B^\gamma = \bigcup_{\alpha<\gamma} B_\alpha \cup (\gamma + 1)$. Then clearly

(2) $\langle Y_\alpha: \alpha < \gamma \rangle \cup \langle X_\alpha: \alpha \in 2^\kappa \backslash B^\gamma \rangle$ is independent modulo $[\kappa]^{<\kappa}$; $|B^\gamma| \leq \omega + |\gamma|$; and for all $\xi < \gamma$, $f_\xi[Y_\xi] \not\in \langle \{Y_\alpha: \alpha < \gamma\} \cup [\kappa]^{<\lambda} \rangle$.

Now let δ_0 and δ_1 be the two least elements of $2^\kappa \backslash B^\gamma$. We claim

(3) there exist disjoint non-empty $Z_0, Z_1 \subseteq \kappa$, $Z \subseteq \kappa$, and $\bar{X} \in \langle \{X_{\delta_0}, X_{\delta_1}\} \rangle \backslash \{\kappa\}$ such that $Z = Z_0 \cup Z_1 \subseteq \bar{X}$, $|Z_0| = \lambda$, and $f_\gamma[Z_0] = Z_1$.

In fact, since $f_\gamma \not\in \mathrm{Sym}_{<\lambda}\,\kappa$, there are disjoint $C, D \subseteq \kappa$ with $|C| = \lambda$ and $f_\gamma[C] = D$. There is an atom T_0 of $\langle \{X_{\delta_0}, X_{\delta_1}\} \rangle$ such that $|T_0 \cap C| = \lambda$, and there is an atom T_1 of $\langle \{X_{\delta_0}, X_{\delta_1}\} \rangle$ such that $|T_1 \cap f_\gamma[T_0 \cap C]| = \lambda$. Let $Z_0 = f_\gamma^{-1}[T_1 \cap f_\gamma[T_0 \cap C]]$, $Z_1 = T_1 \cap f_\gamma[T_0 \cap C]$, $\bar{X} = T_0 \cup T_1$, and note that $\langle \{X_{\delta_0}, X_{\delta_1}\} \rangle$ has four atoms; (3) follows.

Now for each $\delta \in 2^\kappa \backslash (B^\gamma \cup \{\delta_0, \delta_1\})$ and each $S \subseteq Z_0$ we set

$$Y^{\delta S} = (X_\delta \backslash Z) \cup S\,;$$

$$B^{\delta S} = B^\gamma \cup \{\delta, \delta_0, \delta_1\}\,.$$

Note that $Y^{\delta S} \cap (\kappa \backslash \bar{X}) = X_\delta \cap (\kappa \backslash \bar{X})$. Let $C = (\mathscr{P}\kappa/[\kappa]^{<\kappa}) \restriction ((\kappa \backslash \bar{X})/[\kappa]^{<\kappa})$. For each $W \subseteq \mathscr{P}\kappa$ let $hW = (W \backslash [\kappa]^{<\kappa}) \cdot ((\kappa \backslash \bar{X})/[\kappa]^{<\kappa})$. Then h is a homomorphism from $\mathscr{P}\kappa$ onto C, and it takes the elements Y_α, $\alpha<\gamma$, $Y^{\delta S}$, X_β, $\beta\in 2^\kappa\backslash B^{\delta S}$ to independent elements. Hence,

(4) for all $\delta\in 2^\kappa\backslash(B^\gamma\cup\{\delta_0,\delta_1\})$ and all $S\subseteq Z_0$, $\langle Y_\alpha:\alpha<\gamma\rangle \cup\{(\gamma, Y^{\delta S})\}\cup\langle X_\alpha:\alpha\in 2^\kappa\backslash B^{\delta S}\rangle$ is independent.

[Eventually we will let $Y_\delta = Y^{\delta S}$, $B_\gamma = B^{\delta S}$ for some such δ and S.] Now we need

(5) let $\xi<\gamma$ and $A, B\in\langle Y_\alpha:\alpha<\gamma\rangle$. Then there is at most one $\delta\in 2^\kappa\backslash (B^\gamma\cup\{\delta_0,\delta_1\})$ such that for some $S\subseteq Z_0$ we have $f_\xi[Y_\xi]$ equivalent to $(A\cap Y^{\delta S})\cup(B\backslash Y^{\delta S})$ modulo $[\kappa]^{<\lambda}$.

For, suppose not; say $\delta^i\in 2^\kappa\backslash(B^\gamma\cup\{\delta_0,\delta_1\})$, $S^i\subseteq Z_0$, $\delta^0\neq\delta^1$, and

(6) $$f_\xi[Y_\xi]\equiv(A\cap Y^{\delta^i S^i})\cup(B\backslash Y^{\delta^i S^i}),\quad i=1,2.$$

Then

$$\begin{aligned}(\kappa\backslash\bar{X})\cap(A\triangle B)\cap(X_{\delta^1}\triangle X_{\delta^2}) &\subseteq(\kappa\backslash Z)\cap(A\triangle B)\cap(X_{\delta^1}\triangle X_{\delta^2})\\ &\subseteq[(A\cap Y^{\delta^1 S^1})\cup(B\backslash Y^{\delta^1 S^1})]\triangle[(A\cap Y^{\delta^2 S^2})\cup(B\backslash Y^{\delta^2 S^2})],\end{aligned}$$

from which it follows by (2) that $A\triangle B=0$ and so $A=B$, so (6) yields $f_\xi[Y_\xi]$ equivalent to A modulo $[\kappa]^{<\lambda}$, contradicting (2). Thus (5) holds.

There are at most $\omega+|\gamma|$ triples (ξ, A, B) as in (5); so let δ be the least member of $2^\kappa\backslash(B^\gamma\cup\{\delta_0,\delta_1\})$ such that there are not ξ, A, B, S as described in (5). Thus

(7) for all $\xi<\gamma$ and all $S\subseteq Z_0$ we have $f_\xi[Y_\xi]\not\in\langle\{Y_\alpha:\alpha<\gamma\} \cup\{Y^{\delta S}\}\cup[\kappa]^{<\lambda}\rangle$.

Now we claim that for $S=0$ or $S=Z_0$ we have $f_\gamma[Y^{\delta S}]\not\in\langle\{Y_\alpha:\alpha<\gamma\}\cup\{Y^{\delta S}\}\cup[\kappa]^{<\lambda}\rangle$. (This will finish the construction.) Suppose that this is not true. Then there are $A_i, B_i\in\langle\{Y_\alpha:\alpha<\gamma\}\rangle$, $i=1,2$, such that

(8) $$\begin{aligned}f_\gamma[Y^{\delta 0}]&\equiv(A_1\cap Y^{\delta 0}\cup(B_1\backslash Y^{\delta 0})\operatorname{mod}[\kappa]^{<\lambda},\\ f_\gamma[Y^{\delta Z_0}]&\equiv(A_2\cap Y^{\delta Z_0})\cup(B_2\backslash Y^{\delta Z_0})\operatorname{mod}[\kappa]^{<\lambda}.\end{aligned}$$

Note that $f_\gamma[y^{\delta 0}]\backslash\bar{X}=f_\gamma[Y^{\delta Z_0}]\backslash\bar{X}$, $Y^{\delta 0}\backslash\bar{X}=Y^{\delta Z_0}\backslash\bar{X}=X_\delta\backslash\bar{X}$, and (consequently) $(\kappa\backslash Y^{\delta 0})\backslash\bar{X}=(\kappa\backslash Y^{\delta Z_0})\backslash\bar{X}=(\kappa\backslash X_\delta)\backslash\bar{X}$. Hence, intersecting both sides of the congruences (8) with $\kappa/\bar{X}$ we get

$$\begin{aligned}(A_1\cap X_\delta\backslash\bar{X})\cup(B_1\cap(\kappa\backslash X_\delta)\backslash\bar{X})&\equiv(A_2\cap X_\delta\backslash\bar{X})\\ &\cup(B_2\cap(\kappa\backslash X_\delta)\backslash\bar{X})\operatorname{mod}[\kappa]^{<\lambda}.\end{aligned}$$

Since $\langle Y_\alpha: \alpha < \gamma \rangle \cup \langle X_\delta, \overline{X}_{\delta_0}, X_{\delta_1} \rangle$ are independent modulo $[\kappa]^{<\kappa}$, this equivalence is actually an equality, and implies that $A_1 = A_2$ and $B_1 = B_2$.

Intersecting the congruences (8) with Z_1 we get

$$0 \equiv B_1 \cap Z_1 \bmod [\kappa]^{<\lambda} ,$$

$$Z_1 \equiv B_1 \cap Z_1 \bmod [\kappa]^{<\lambda} ,$$

so $|Z_1| < \lambda$, a contradiction.

So we choose $S = 0$ or $S = Z_0$ so that $f_\gamma[Y^{\delta S}] \notin \langle \{Y_\alpha: \alpha < \gamma\} \cup \{Y^{\delta s}\} \cup [\kappa]^{<\lambda} \rangle$. Let $Y_\gamma = Y^{\delta S}$, $B_\gamma = B^{\delta S}$. Then (1) holds for γ.

This finishes the construction. Let $A = \langle \{Y_\alpha: \alpha < Z_\kappa\} \cup [\kappa]^{<\lambda} \rangle$. The desired conclusions are clear from (1). □

Concerning the size of automorphism groups of atomic BAs, we also recall a corollary of Theorem 4.8 of MONK [Ch. 13 in this Handbook] there is an atomic BA A with $|A| = |\mathrm{Aut}\, A| = |\mathrm{At}\, A| = 2^\omega$.

Assume GCH for the following remarks. For any atomic BA we have $|\mathrm{At}\, A| \leqq |\mathrm{Aut}\, A| \leqq |A|^+$ and $|A| \leqq |\mathrm{At}\, A|^+$. By Theorem 4.8, for any infinite κ there is a BA A such that $|\mathrm{At}\, A| = |\mathrm{Aut}\, A| = \kappa$ and $|A| = \kappa^+$. If B is the finite–cofinite algebra on κ, then $|\mathrm{At}\, B| = |B| = \kappa$ and $|\mathrm{Aut}\, B| = \kappa^+$. And $|\mathscr{P}\kappa| = \kappa^+ = |\mathrm{Aut}\, \mathscr{P}\kappa|$, while $|\mathrm{At}\, \mathscr{P}\kappa| = \kappa$. The essential missing possibility here is an atomic algebra A such that $|\mathrm{At}\, A| = |\mathrm{Aut}\, A| = |A| = \kappa$. By the remark of the preceding paragraph, there is such an algebra for $\kappa = \omega_1$. Of course, there is none for $\kappa = \omega$. We do not know whether there are such for $\kappa > \omega_1$.

Turning to automorphism groups of interval algebras, first recall that for each $\kappa > \omega_1$ there is a rigid, cardinality-homogeneous interval algebra of power κ. Hence, parts (i) and (iii) of Theorem 4.2 hold for interval algebras. Part (iv) also holds, by taking the interval algebra on an ordered set S of power κ which has 2^κ order-automorphisms (for the existence of such an ordered set see, for example, MONK [1976, p. 451]). We do not know whether part (ii) holds; in particular, we do not know whether there is an interval algebra of power 2^ω with automorphism group of power ω.

We know even less about the size of automorphism groups of superatomic BAs. Perhaps it is even true that always $|\mathrm{Aut}\, A| = 2^{|\mathrm{At}\, A|}$ for A superatomic.

References

BRENNER, G.

[1983] A simple construction for rigid and weakly homogeneous Boolean algebras answering a question of Rubin, *Proc. Amer. Math. Soc.*, **87**, 601–606.

CHASE, S., D. HARRISON and A. ROSENBERG

[1965] Galois theory and Galois cohomology of commutative rings, *Memoirs Amer. Math. Soc.*, **52**, 15–33.

DEMEYER, F. and E. INGRAHAM

[1971] Separable algebras over commutative rings, *Lect. Notes in Math.*, **181** (Springer-Verlag), 157 pp.

VAN DOUWEN, E.K.
[1980] A consistent very small Boolean algebra with countable automorphism group, *Alg. Univ.*, **11**, 389–392.
HALMOS, P.
[1955] Algebraic logic, I. Monadic Boolean algebras, *Comp. Math.*, **12**, 217–249.
KOPPELBERG, S.
[1978] A complete Boolean algebra without homogeneous or rigid factors, *Math. Ann.*, **232**, 109–114.
[1981] A lattice structure on the isomorphism types of complete Boolean algebras. Set theory and model theory. *Lect. Notes in Math.*, **872** (Springer-Verlag) 98–126.
[1982] On Boolean algebras with distinguished subalgebras, *Enseign. Math.*, **28**, 233–252.
MAGID, A.
[1974] *The Separable Galois Theory of Commutative Kings* (Marcel Dekker, Inc., New York) xvii + 134 pp.
MARTIN, D. and R.M. SOLOVAY
[1970] Internal Cohen extensions, *Ann. Math. Logic*, **2**, 143–178.
MCKENZIE, R. and J.D. MONK
[1975] On automorphism groups of Boolean algebras. Infinite and Finite Sets, *Colloq. Math. Soc. J. Bolyai*, 951–988.
MONK, J.D.
[1976] *Mathematical Logic* (Springer-Verlag) x + 531 pp.
ROITMAN, J.
[1981] The number of automorphisms of an atomic Boolean algebra, *Pac. J. Math.*, **94**, 231–242.
ŠTĚPÁNEK, P.
[1982] Boolean algebras with no rigid or homogeneous factors, *Trans. Amer. Math. Soc.*, **270**, 131–147.
ŠTĚPÁNEK, P. and B. BALCAR
[1977] Embedding theorems for Boolean algebras and consistency results on ordinal definable sets, *J. Symb. Logic*, **42**, 64–76.
VILLAMAYOR, O. and D. ZELINSKI
[1969] Galois theory with infinitely many idempotents, *Nagoya Math. J.*, **35**, 83–98.

J. Donald Monk
University of Colorado

Keywords: Boolean algebra, automorphism, group, totally different, rigid, homogeneous, Galois theory, simple extension.

MOS subject classification: primary 06E05; secondary 03G05, 13B05, 20B27.