AUTOMORPHISM GROUPS OF UNARY ALGEBRAS ON GROUPS

G. H. WENZEL

To my father, Wilhelm A. Wenzel, on his sixtieth birthday

This paper presents a systematic study of the automorphism groups of those unary (universal) algebras $\mathfrak{A} = \langle G; F\rangle$ whose carrier set G is the carrier set of some group $\mathfrak{G} = \langle G; \cdot\rangle$ and whose automorphism set $\mathrm{Aut}(\mathfrak{A})$ contains the right translations of the latter group. These algebras appear, apart from the known classical contexts, repeatedly in characterization theorems of endomorphism semigroups (End) and automorphism groups (Aut) of algebras due to Grätzer (**3**; **4**; **5**), Makkai (**7**), Armbrust and Schmidt (**1**), Birkhoff (**2**), and others.

Our main result (Theorem 1) constitutes an essential strengthening of a theorem of Birkhoff and represents the automorphism group $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle$ of a unary algebra $\mathfrak{A} = \langle G; F\rangle$ (where F is contained in the set $L(\mathfrak{G})$ of left translations of the group $\mathfrak{G} = \langle G; \cdot\rangle$) as wreath product of two groups that are easily determined from F and G. In the remainder of § 1 we deduce in the form of corollaries some well-known results due to Birkhoff, Grätzer, and others that follow quite easily from our general result. In § 2 we mention a few observations concerning arbitrary universal algebras on groups.

We assume familiarity with the diverse algebraic concepts and keep essentially to the denotations and terminology as introduced in (**4**). Universal algebras (shortly: algebras) are denoted by capital German letters ($\mathfrak{A}$, $\mathfrak{C}$, $\mathfrak{G}, \ldots$) or pairs of capital italic letters ($\langle A; F\rangle$, $\langle C; F\rangle$, $\langle G; F\rangle, \ldots$), where the first letters denote non-empty sets on which the sets of fundamental operations, denoted by the second letter, operate. All mappings, except the polynomials, are applied at the right side of the arguments; polynomials (i.e., all mappings that result from a finite number of applications of the fundamental operations to the projections) are applied at the left side. $\bigvee$, $\bigwedge$ are set-theoretical union and intersection, $\dot{\bigvee}$ denotes the disjoint set-theoretical union, $\cup$ and $\cap$ stand for lattice-theoretical union and intersection. $\mathfrak{C}(\mathfrak{A}) = \langle C(\mathfrak{A}); \cup, \cap\rangle$ is the (algebraic) congruence lattice of the algebra $\mathfrak{A}$; $\omega \in C(\mathfrak{A})$ ($i \in C(\mathfrak{A})$) are the smallest (biggest) elements in that lattice.

1. Unary operations. If a group $\mathfrak{G} = \langle G; \cdot\rangle$ is given, then we have the set $R(\mathfrak{G})$ of right translations r_a, $a \in G$. The question about the sets F of unary

Received April 1, 1968.

operations that assure that $\mathfrak{A} = \langle G; F\rangle$ satisfies $R(\mathfrak{G}) \subseteq \mathrm{Aut}(\mathfrak{A})$ is easily answered and stated in the next remark.

Remark. $R(\mathfrak{G}) \subseteq \mathrm{Aut}(\mathfrak{A})$ holds true if and only if $F \subseteq L(\mathfrak{G}) = \{l_a; a \in G\}$.

The question that we are interested in is the structure of the automorphism group of the universal algebra $\mathfrak{A} = \langle G; F\rangle$ if, conversely, $F \subseteq L(\mathfrak{G})$.

THEOREM 1. *Let $\mathfrak{A} = \langle G; F\rangle$ be a unary algebra, where $\mathfrak{G} = \langle G; \cdot\rangle$ is a group and $F \subseteq L(\mathfrak{G})$. If $\langle [F]; \cdot\rangle$ is the subgroup of $\mathfrak{G}$ generated by all elements b such that $l_b \in F$ ($[F] = \{1\}$ if $F = \phi$), then $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle$ is isomorphic to the wreath product $\langle [F] \wr S_\alpha; \cdot\rangle$* (see **2**, p. 81) *resulting from a fixed decomposition into left cosets of G, say*

$$G = [F]x_0 \vee^{\cdot} [F]x_1 \vee^{\cdot} \ldots \vee^{\cdot} [F]x_\gamma \vee^{\cdot} \ldots, \qquad \gamma < \alpha,\ x_0 = 1,$$

where $\langle S_\alpha; \cdot\rangle$ is the symmetric group on the ordinals $\{\gamma; \gamma < \alpha\}$ and $[F]$ acts as permutation group via right translations on itself.

Proof. Let $G = [F]x_0 \vee^{\cdot} [F]x_1 \vee^{\cdot} \ldots \vee^{\cdot} [F]x_\gamma \vee^{\cdot} \ldots, \gamma < \alpha$, and $\phi \in \mathrm{Aut}(\mathfrak{A})$. If $1\phi = c$, then $b\phi = l_b(1)\phi = l_b(1\phi) = b\cdot c$ and $c = 1\phi = (b\cdot b^{-1})\phi = l_b(b^{-1})\phi = l_b(b^{-1}\phi) = b\cdot(b^{-1}\phi)$, i.e. $b^{-1}\phi = b^{-1}c$ holds for all b with $l_b \in F$. Induction on the length of the words shows that $d\phi = dc$ holds for all $d \in [F]$, for if $d = b_1^{\nu_1}\cdot b_2^{\nu_2}\cdot \ldots \cdot b_n^{\nu_n}$ ($\nu_i \in \{-1, +1\}$) with $l_{b_i} \in F$ and $\nu_1 = +1$, then it is clear. If $\nu_1 = -1$, then we conclude:

$$b_1(b_1^{-1}\cdot b_2^{\nu_2}\cdot \ldots \cdot b_n^{\nu_n})\phi = (b_1\cdot b_1^{-1}\cdot b_2^{\nu_2}\cdot \ldots \cdot b_n^{\nu_n})\phi = b_2^{\nu_2}\cdot \ldots \cdot b_n^{\nu_n}\cdot c,$$

i.e.

$$d\phi = b_1^{-1}b_2^{\nu_2}\cdot \ldots \cdot b_n^{\nu_n}\cdot c = dc.$$

Thus, 1ϕ determines ϕ on $[F]$ to be $r_{1\phi}$. Similarly, $x_i\phi$ ($i \geqq 1$) determines ϕ on $[F]x_i$ to be $r_{x_i\phi}$. We conclude that $(fx_i)\phi = f(x_i\phi)$ for all $f \in [F]$ and

$$G = [F]\cdot(1\phi) \vee^{\cdot} [F]\cdot(x_1\phi) \vee^{\cdot} \ldots \vee^{\cdot} [F]\cdot(x_\gamma\phi) \vee^{\cdot} \ldots, \qquad \gamma < \alpha.$$

Thus, ϕ induces in a natural fashion a permutation σ_ϕ of $\{\gamma; \gamma < \alpha\}$, namely $\gamma\sigma_\phi = \delta$ if $x_\gamma\phi \in [F]x_\delta$. ϕ also induces a mapping τ_ϕ: $\{\gamma; \gamma < \alpha\} \to [F]$ as follows:

If $x_\gamma\phi = f_{\delta_\gamma}{}^\phi x_{\delta_\gamma} =$ (by definition of σ_ϕ) $f_{\gamma\sigma_\phi}{}^\phi x_{\gamma\sigma_\phi}, f_{\delta_\gamma} = f_{\gamma\sigma_\phi} \in [F], 0 \leqq \gamma < \alpha$, then $\gamma\tau_\phi = f_{\gamma\sigma_\phi}{}^\phi$. Thus, if we use the Cartesian denotation, we have:

$$\tau_\phi = (f_{0\sigma_\phi}{}^\phi, f_{1\sigma_\phi}{}^\phi, \ldots, f_{\gamma\sigma_\phi}{}^\phi, \ldots), \qquad \gamma < \alpha.$$

LEMMA 1. *If $H = \{(\tau_\phi, \sigma_\phi); \phi \in \mathrm{Aut}(\mathfrak{A})\}$, then $H = [F]^\alpha \times S_\alpha$.*

To prove the lemma, let $(\tau, \sigma) \in [F]^\alpha \times S_\alpha$ and define $\phi: G \to G$ by $(fx_\gamma)\phi = f\cdot(\gamma\tau)\cdot x_{\gamma\sigma}$ ($g = fx_\gamma \in G$). It is easy to see that $\phi \in \mathrm{Aut}(\mathfrak{A})$; moreover, $\gamma\sigma_\phi = \gamma\sigma$ and $\gamma\tau_\phi = \gamma\tau$, i.e. $(\tau, \sigma) = (\tau_\phi, \sigma_\phi) \in H$. This proves the lemma.

We now define multiplication on H in the intuitive manner, namely:

$$(\tau_\phi, \sigma_\phi) \cdot (\tau_\psi, \sigma_\psi) = (\tau_\phi * \tau_\psi, \sigma_\phi \cdot \sigma_\psi),$$

where

$$\tau_\phi * \tau_\psi = (f_{0\sigma_\phi}{}^{\phi} \cdot f_{0\sigma_{\phi\cdot\psi}}{}^{\psi}, \ldots, f_{\gamma\sigma_\phi}{}^{\phi} \cdot f_{\gamma\sigma_{\phi\cdot\psi}}{}^{\psi}, \ldots), \qquad \gamma < \alpha,$$

if $\tau_\phi = (f_{0\sigma_\phi}{}^{\phi}, f_{1\sigma_\phi}{}^{\phi}, \ldots, f_{\gamma\sigma_\phi}{}^{\phi}, \ldots)$, $\gamma < \alpha$, and $\tau_\psi = (f_{0\sigma_\psi}{}^{\psi}, f_{1\sigma_\psi}{}^{\psi}, \ldots, f_{\gamma\sigma_\psi}{}^{\psi}, \ldots)$, $\gamma < \alpha$. If we define multiplication this way, then θ: $\langle \mathrm{Aut}(\mathfrak{A}), \cdot \rangle \rightarrow \langle H; \cdot \rangle$, mapping ϕ onto (τ_ϕ, σ_ϕ), becomes an isomorphism, hence $\langle H; \cdot \rangle$ is a group isomorphic to $\mathrm{Aut}(\mathfrak{A})$. To see this we calculate:

(1) θ is clearly one-to-one and onto (Lemma 1).

(2) If $\phi, \psi \in \mathrm{Aut}(\mathfrak{A})$, then: $(\phi \cdot \psi)\theta = (\tau_{\phi.\psi}, \sigma_{\phi.\psi})$, where $\gamma\sigma_{\phi.\psi} = \delta$ if $x_\gamma\phi \cdot \psi \in [F]x_\delta$; $\phi\theta = (\tau_\phi, \sigma_\phi)$, where $\gamma\sigma_\phi = \delta$ if $x_\gamma\phi \in [F]x_\delta$; $\psi\theta = (\tau_\psi, \sigma_\psi)$, where $\gamma\sigma_\psi = \delta$ if $x_\gamma\psi \in [F]x_\delta$. Now, if $x_\gamma\phi \in [F]x_\delta$, then $(x_\gamma\phi)\psi \in ([F]x_\delta)\psi = [F](x_\delta\psi) = [F]x_\epsilon$ if $x_\gamma\phi \in [F]x_\delta$, $x_\delta\psi \in [F]x_\epsilon$. Hence, $\gamma\sigma_{\phi.\psi} = \epsilon$. On the other hand, $\gamma\sigma_\phi = \delta$, $\delta\sigma_\psi = \epsilon$, i.e. $\gamma\sigma_\phi \cdot \sigma_\psi = \epsilon$. Thus, $\sigma_{\phi.\psi} = \sigma_\phi \cdot \sigma_\psi$.

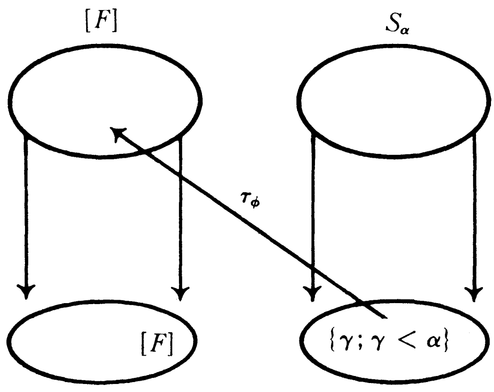
(3) If we use the denotation introduced above, then $x_\gamma\phi = f_{\gamma\sigma_\phi}{}^{\phi} x_{\gamma\sigma_\phi}$, $x_\gamma\psi = f_{\gamma\sigma_\psi}{}^{\psi} x_{\gamma\sigma_\psi}$. This implies that $x_\gamma\phi \cdot \psi = (f_{\gamma\sigma_\phi}{}^{\phi} x_{\gamma\sigma_\phi})\psi = f_{\gamma\sigma_\phi}{}^{\phi}(x_{\gamma\sigma_\phi}\psi) = f_{\gamma\sigma_\phi}{}^{\phi} \cdot f_{\gamma\sigma_\phi\sigma_\psi}{}^{\psi} x_{\gamma\sigma_\phi.\sigma_\psi} = f_{\gamma\sigma_\phi}{}^{\phi} \cdot f_{\gamma\sigma_{\phi\cdot\psi}}{}^{\psi} \cdot x_{\gamma\sigma_{\phi\cdot\psi}}$ while, on the other hand, $x_\gamma\phi \cdot \psi = f_{\gamma\sigma_{\phi\cdot\psi}}{}^{\phi\cdot\psi} x_{\gamma\sigma_{\phi\cdot\psi}}$. Hence, $f_{\gamma\sigma_\phi}{}^{\phi} \cdot f_{\gamma\sigma_{\phi\cdot\psi}}{}^{\psi} = f_{\gamma\sigma_{\phi\cdot\psi}}{}^{\phi\cdot\psi}$, i.e.

$$\begin{aligned}
\tau_{\phi.\psi} &= (f_{0\sigma_{\phi\cdot\psi}}{}^{\phi\cdot\psi}, \ldots, f_{\gamma\sigma_{\phi\cdot\psi}}{}^{\phi\cdot\psi}, \ldots) \quad (\gamma < \alpha) \\
&= (f_{0\sigma_\phi}{}^{\phi} \cdot f_{0\sigma_{\phi\cdot\psi}}{}^{\psi}, \ldots, f_{\gamma\sigma_\phi}{}^{\phi} \cdot f_{\gamma\sigma_{\phi\cdot\psi}}{}^{\psi}, \ldots) \quad (\gamma < \alpha) \\
&= \tau_\phi * \tau_\psi.
\end{aligned}$$

(4) If we combine (2) and (3), we see that $(\phi \cdot \psi)\theta = (\tau_{\phi.\psi}, \sigma_{\phi.\psi}) = (\tau_\phi * \tau_\psi, \sigma_\phi \cdot \sigma_\psi) = (\tau_\phi, \sigma_\phi) \cdot (\tau_\psi, \sigma_\psi) = (\phi\theta) \cdot (\psi\theta)$.

Thus, θ is indeed an isomorphism.

We now turn to the wreath product $\langle [F] \wr S_\alpha; \cdot \rangle$ which arises (see diagram) as indicated in the theorem (see (**6**)). Using the foregoing lemma we note that $[F] \wr S_\alpha$ consists of all permutations $\theta_{\tau_\phi, \sigma_\psi}$ on the set $[F] \times \{\gamma; \gamma < \alpha\}$



https://doi.org/10.4153/CJM-1969-127-2 Published online by Cambridge University Press

defined by $(g, \gamma)\theta_{\tau_\phi,\sigma_\phi} = (g(\gamma\tau_\phi), \gamma\sigma_\phi)$. We now define $\Phi: \langle [F] \wr S_\alpha; \cdot \rangle \to \langle H; \cdot \rangle$ by $\theta_{\tau_\phi,\sigma_\phi}\Phi = (\tau_\phi, \sigma_\phi) = ((f_{0\sigma_\phi}{}^\phi, \ldots, f_{\gamma\sigma_\phi}{}^\phi, \ldots)(\gamma < \alpha), \sigma_\phi)$. This mapping Φ is clearly one-to-one and onto; moreover,

$$\begin{aligned}(g, \gamma)\theta_{\tau_\phi,\sigma_\phi}\cdot\theta_{\tau_\psi,\sigma_\psi} &= (g(\gamma\tau_\phi), \gamma\sigma_\phi)\theta_{\tau_\psi,\sigma_\psi} = ([g(\gamma\tau_\phi)][(\gamma\sigma_\phi)\tau_\psi], \gamma\sigma_\phi\cdot\sigma_\psi)\\ &= ([g\cdot f_{\gamma\sigma_\phi}{}^\phi]\cdot[f_{\gamma\sigma_\phi\cdot\sigma_\psi}{}^\psi], \gamma\sigma_\phi\cdot\sigma_\psi) = (g\cdot f_{\gamma\sigma_{\phi\cdot\psi}}{}^{\phi\cdot\psi}, \gamma\sigma_{\phi\cdot\psi})\\ &= (g(\gamma\tau_{\phi\cdot\psi}), \gamma\sigma_{\phi\cdot\psi}) = (g, \gamma)\theta_{\tau_{\phi\cdot\psi},\sigma_{\phi\cdot\psi}}\end{aligned}$$

which shows that

$$\theta_{\tau_\phi,\sigma_\phi}\cdot\theta_{\tau_\psi,\sigma_\psi} = \theta_{\tau_{\phi\cdot\psi},\sigma_{\phi\cdot\psi}}.$$

Hence, $(\theta_{\tau_\phi,\sigma_\phi}\cdot\theta_{\tau_\psi,\sigma_\psi})\Phi = \theta_{\tau_{\phi\cdot\psi},\sigma_{\phi\cdot\psi}}\Phi = (\tau_{\phi\cdot\psi}, \sigma_{\phi\cdot\psi}) =$ (as proved before) $(\tau_\phi * \tau_\psi, \sigma_\phi\cdot\sigma_\psi) = (\tau_\phi, \sigma_\phi)\cdot(\tau_\psi, \sigma_\psi) = (\theta_{\tau_\phi,\sigma_\phi}\Phi)\cdot(\theta_{\tau_\psi,\sigma_\psi}\Phi)$. Thus, Φ is an isomorphism; hence $\theta\cdot\Phi^{-1}: \langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle \to \langle [F] \wr S_\alpha; \cdot \rangle$ is an isomorphism.

We apply this theorem to obtain the following result.

THEOREM 2. *The hypotheses are as in Theorem* 1.

(1) *The sequence*

$$\langle 1;\cdot\rangle \to \langle [F]^\alpha;\cdot\rangle \xrightarrow{\delta_1} \langle \mathrm{Aut}(\mathfrak{A});\cdot\rangle \xrightarrow{\delta_2} \langle S_\alpha;\cdot\rangle \to \langle 1;\cdot\rangle$$

is an exact sequence of groups for some δ_1, δ_2.

(2) *The normal subgroup* $\langle [F]^\alpha; \cdot \rangle$ *of* $\langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle$ *(which is, of course, considered as subgroup via the natural embedding) is isomorphic to* $\langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle$ *if* $\alpha = 1$. *In case of finite groups* $\mathfrak{G}$ *or* $\langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle$ *we have* $\langle [F]^\alpha; \cdot \rangle \cong \langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle$ *if and only if* $\alpha = 1$.

Proof. As is well known from the theory of wreath products, $\langle [F] \wr S_\alpha; \cdot \rangle$ has the normal subgroup $\langle [F]^*; \cdot \rangle$, where $[F]^* = \{\theta_{\sigma_\phi,\tau_\phi}; \tau_\phi = \mathrm{id}\}$; moreover, $\langle [F]^*; \cdot \rangle \cong \langle [F]^\alpha; \cdot \rangle$ and $\langle [F] \wr S_\alpha/[F]^*; \cdot \rangle \cong \langle S_\alpha; \cdot \rangle$. These remarks prove (1).

(2) If $\alpha = 1$, then $\langle [F] \wr S_\alpha; \cdot \rangle = \langle [F]^*; \cdot \rangle \cong \langle [F]^\alpha; \cdot \rangle$, i.e., by Theorem 1, $\langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle \cong \langle [F]^\alpha; \cdot \rangle$. If, on the other hand, $\alpha \neq 1$ and $\mathrm{Aut}(\mathfrak{A})$ is finite, then $\langle [F]^*; \cdot \rangle$ is a proper subgroup of $\langle [F] \wr S_\alpha; \cdot \rangle$, and hence $\langle [F]^\alpha; \cdot \rangle \ncong \langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle$.

COROLLARY 1 (Birkhoff). $\mathfrak{A} = \langle G; L(\mathfrak{G}) \rangle$ *satisfies* $\mathrm{Aut}(\mathfrak{A}) \cong \mathfrak{G}$ *for every group* $\mathfrak{G}$.

Proof. $F = L(\mathfrak{G})$ implies $\alpha = 1$; hence $\mathfrak{G} = \langle [F]; \cdot \rangle \cong \langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle$.

Of course, to obtain Birkhoff's result, we do not really need all left translations. The same proof shows the next slightly stronger statement.

COROLLARY 2. (1) $\mathfrak{A} = \langle G; F \rangle$, $F \subseteq L(\mathfrak{G})$, *satisfies* $\langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle \cong \mathfrak{G}$ *for all* F *with* $[F] = G$ *(i.e.* $\alpha = 1$*).*

(2) *If* $\mathrm{Aut}(\mathfrak{A})$ *is finite, then* $\mathfrak{A} = \langle G; F \rangle$, $F \subseteq L(\mathfrak{G})$, *satisfies* $\langle \mathrm{Aut}(\mathfrak{A}); \cdot \rangle \cong \mathfrak{G}$ *if and only if* $[F] = G$ *(i.e.* $\alpha = 1$*) or* $|G| = 2$.

Neither Theorem 2(2) nor Corollary 2(2) can be sharpened to infinite groups as the following example shows.

Example. Let $\langle \mathfrak{Z}; +\rangle$ be the additive group of integers, $\langle S_{\omega_0}; +\rangle$ the permutation group on $\{\gamma; \gamma < \omega_0\}$ (with $+ = \circ$). Then $\mathfrak{A} = \langle \mathfrak{Z} \times S_{\omega_0}; l_{(2,1)}\rangle$, i.e. $F = \{l_{(2,1)}\}$, satisfies $[F] = 2\mathfrak{Z} \times \{1\}$ and $\alpha = \omega_0$. Thus, $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle \cong \langle [F] \wr S_\alpha; \cdot\rangle \cong \langle 2\mathfrak{Z} \wr S_{\omega_0}; \cdot\rangle \cong \langle \mathfrak{Z} \wr S_{\omega_0}; \cdot\rangle = \mathfrak{G}$ while $\alpha \neq 1$, i.e. $[F] \neq G$.

COROLLARY 3. *The group* $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle$ *is simple if and only if* $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle$ *is isomorphic to* $\mathfrak{G}$ *and* $\mathfrak{G}$ *is simple* ($\mathfrak{A} = \langle G; F\rangle$, $F \subseteq L(\mathfrak{G})$).

Proof. The converse being obvious, let $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle$ be a simple group. Then we claim that $\alpha = 1$ or $\langle G; \cdot\rangle$ is the 2-element group. Assume that we proved this; then Corollary 2 shows that $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle \cong \mathfrak{G}$ if $\alpha = 1$; if $\alpha \neq 1$, then $\mathfrak{G}$ is a 2-element group and, of course, the two right translations constitute $\mathrm{Aut}(\mathfrak{A})$, thus again $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle \cong \mathfrak{G}$.

LEMMA 2. *If* $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle$ *is a simple group, then* $\alpha = 1$ *or* $|G| = 2$.

Proof. Since $\langle [F]^\alpha; \cdot\rangle$ is a normal subgroup of $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle$ (see Theorem 2), we conclude that $[F]^\alpha = \{1\}$ or $\mathrm{Aut}(\mathfrak{A})$. If $[F]^\alpha = \mathrm{Aut}(\mathfrak{A})$ $(= [F]^\alpha \wr S_\alpha)$, then $\alpha = 1$. If $[F]^\alpha = \{1\}$, then $[F] = 1$, i.e. $F = \emptyset$ or $F = \{l_1\}$; in other words, $\mathfrak{A}$ is a trivial algebra and $\mathrm{Aut}(\mathfrak{A}) = S_G$ (the full permutation group on G). Since S_G is simple if and only if $|G| \leqq 2$, we obtain $|G| = 1$, i.e. $\alpha = 1$, or $|G| = 2$, i.e. $\langle G; \cdot\rangle$ is the 2-element group. This proves the lemma and Corollary 3.

It can, of course, happen that $\mathrm{Aut}(\mathfrak{A})$ is simple while $\mathfrak{A}$ is not simple. To see this, just take a simple group $\mathfrak{G}$ with non-simple subgroup lattice and consider $\langle G; L(\mathfrak{G})\rangle = \mathfrak{A}$. Since every subgroup and its right cosets determine a congruence relation on $\mathfrak{A}$, the proof is complete.

COROLLARY 4. $\mathrm{Aut}(\mathfrak{A})$ *is finite of prime order if and only if* $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle \cong \mathfrak{G}$ *and* $\mathfrak{G}$ *is finite of prime order.*

The corollary is clear since prime order groups are simple.

COROLLARY 5. *Simple unary algebras* $\mathfrak{A} = \langle A; F\rangle$ *permit a multiplication on* A *such that* $\mathfrak{G} = \langle A; \cdot\rangle$ *becomes a group,* $F \subseteq L(\mathfrak{G})$, *and* $\mathfrak{G} \cong \langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle$.†

Proof. Since $\mathfrak{A} = \langle A; F\rangle$ is simple and unary, it is quite trivial that

(1) $\mathfrak{A}$ has a simple subalgebra lattice, i.e. $[a] = A$ for all $a \in A$, and that

(2) $A = \{a\phi; \phi \in \mathrm{Aut}(\mathfrak{A})\}$ since $\{G_a; G_a = \{a\phi; \phi \in \mathrm{Aut}(\mathfrak{A})\}\}$ are evidently the blocks of a congruence on $\mathfrak{A}$. Thus, $a\phi \neq a\psi$ is equivalent to $\phi \neq \psi$ and $(a\phi)\cdot(a\psi) = a\phi\psi$ makes $\langle A; \cdot\rangle = \mathfrak{G}$ a group isomorphic to $\langle \mathrm{Aut}(\mathfrak{A}); \cdot\rangle$ on which $\mathrm{Aut}(\mathfrak{A})$ acts in a form of right-translations. Hence, $F \subseteq L(\mathfrak{G})$. Thus, $\mathfrak{A}$ is of our type, and our results are applicable.

COROLLARY 6 (Grätzer (**3**)). *Simple unary algebras* $\mathfrak{A}$ *are finite of prime order; so are their automorphism groups.*

Proof. Corollary 5 and the simplicity of the subgroup lattice of $\langle A; \cdot\rangle$ settle the matter.

†$\mathfrak{A}$ is "simple" if $|C(\mathfrak{A})| = 2$ and $|\mathrm{Aut}(\mathfrak{A})| \neq 1$.

https://doi.org/10.4153/CJM-1969-127-2 Published online by Cambridge University Press

2. Binary operations. The question about the binary operations F that cause an algebra $\mathfrak{A} = \langle G; F\rangle$ with $R(\mathfrak{G}) \subseteq \text{Aut}(\mathfrak{A})$ finds its answer in the following result.

THEOREM 3. *If* $\mathfrak{A} = \langle G; F\rangle$ *is a binary algebra* ($\mathfrak{G} = \langle G; \cdot\rangle$ *is a group*), *then* $R(\mathfrak{G}) \subseteq \text{Aut}(\mathfrak{A})$ *holds if and only if* $F \subseteq \{\psi_\sigma; \sigma \in G^G\}$ *when* $\psi_\sigma(1, g) = g\sigma$ *and, in general,* $\psi_\sigma(x, y) = ((y\cdot x^{-1})\sigma)\cdot x$.

Proof. To prove the necessity let $\psi \in F$. Then $\psi(x, y)\cdot a = (\psi(x, y))r_a = \psi(xr_a, yr_a) = \psi(xa, ya)$ for all $x, y, a \in G$. Define $\sigma \in G^G$ by $\psi(1, g) = g\sigma$, then $\psi(x, y) = \psi(1\cdot x, (y\cdot x^{-1}))\cdot x = \psi(1, y\cdot x^{-1})\cdot x = (y\cdot x^{-1})\sigma\cdot x$, i.e. $\psi = \psi_\sigma$. To establish sufficiency we check that $(\psi_\sigma(x, y))\cdot r_a = (((yx^{-1})\sigma)\cdot x)r_a = ((y\cdot x^{-1})\sigma)x\cdot a$ while

$$\psi_\sigma(xr_a, yr_a) = \psi_\sigma(xa, ya) = (((ya)(a^{-1}x^{-1}))\sigma)\cdot xa((yx^{-1})\sigma)x\cdot a.$$

Hence, $\psi_\sigma(x, y)r_a = \psi_\sigma(xr_a, yr_a)$ which proves the theorem.

This theorem yields immediately a result part of which was also observed by Grätzer (**3**).

COROLLARY 7. *Given a group* $\mathfrak{G}$, *there exists always a simple algebra* $\mathfrak{A}$ *such that* $\text{End}(\mathfrak{A}) = \text{Aut}(\mathfrak{A}) \cong \mathfrak{G}$.

Proof. We define $\mathfrak{A} = \langle G; L(\mathfrak{G}) \vee \{\psi_\sigma; \sigma \in G^G\}\rangle$. $\text{End}(\mathfrak{A}) = \text{Aut}(\mathfrak{A}) \cong \mathfrak{G}$ follows immediately from the preceding results. If θ is a congruence relation on $\mathfrak{A}$ with $a \equiv b\ (\theta)$ and $a \neq b$, then $a^{-1}\cdot a \equiv a^{-1}b\ (\theta)$, i.e. $1 \equiv d\ (\theta)$ for some $d \neq 1$. If $c \in G$ is arbitrary, we apply ψ_{σ_c}, where $\sigma_c \in G^G$ maps 1 to 1 and $g \neq 1$ to c. Then $1 \equiv d\ (\theta)$ and $1 \equiv 1\ (\theta)$ imply that $\psi_{\sigma_c}(1, 1) \equiv \psi_{\sigma_c}(1, d)\ (\theta)$ or $1\sigma_c \equiv d\sigma_c\ (\theta)$, i.e. $1 \equiv c\ (\theta)$. Hence $x \equiv y\ (\theta)$ for all $(x, y) \in A \times A$, and $\mathfrak{A}$ is simple.

Remark. In the same fashion one can prove that $R(\mathfrak{G}) \subseteq \text{Aut}(\mathfrak{A})$, where $\mathfrak{A} = \langle G; F\rangle$ is any universal algebra built upon the group $\langle G; \cdot\rangle = \mathfrak{G}$ if and only if every *n-ary* $(n \geqq 0)$ operation is of the form $\psi_\sigma(x_1, \ldots, x_n) = ((x_2x_1^{-1}, x_3x_1^{-1}, \ldots, x_nx_1^{-1})\sigma)x_1$ with $\sigma \in G^{G^{n-1}}$ (where $G^{G^{-1}} = \emptyset$, unless $|G| = 1$ in which case we set $G^{G^{-1}} = \{1\}$ and ψ_1 is the identity operation on G).

COROLLARY 8. *In order to preserve* $R(\mathfrak{G}) \subseteq \text{Aut}(\mathfrak{A})$ *in the universal algebra* $\mathfrak{A} = \langle G; F\rangle$ *we can introduce at the most* $|G^{G^{n-1}}|$ *different n-ary operations in* F *and the upper bound is obtainable.*

REFERENCES

1. M. Armbrust and J. Schmidt, *Zum Cayleyschen Darstellungssatz*, Math. Ann. *154* (1964), 70–72.

2. G. Birkhoff, *Lattice theory*, rev. ed., Amer. Math. Soc. Colloq. Publ., Vol. 25 (Amer. Math. Soc., Providence, R.I., 1948).

3. G. Grätzer, *On the endomorphism semigroup of simple algebras*, Math. Ann. *170* (1967), 334–338.
4. ——— *Universal algebra*, The University Series in Higher Mathematics (Van Nostrand, Princeton, N.J., 1968).
5. ——— *Some results on universal algebras*, Mimeographed notes, 1962.
6. M. Hall, *The theory of groups* (Macmillan, New York, 1959).
7. M. Makkai, *Solution of a problem of G. Grätzer concerning endomorphism semigroups*, Acta Math. Acad. Sci. Hungar. *15* (1964), 297–307.

Queen's University,
Kingston, Ontario

https://doi.org/10.4153/CJM-1969-127-2 Published online by Cambridge University Press