ON A THEOREM OF MALCEV[1]

GERARD LALLEMENT

ABSTRACT. For any pair of distinct elements a, b in a finitely generated abelian semigroup S, we indicate what are the homomorphisms ϕ of S onto a finite semigroup such that $\phi(a) \neq \phi(b)$. This improves a previous result of Malcev which states that the considered semigroups are residually finite.

A semigroup S is residually finite if for any pair of distinct elements a, $b \in S$, a and b can be separated by a congruence of finite index (i.e. there exists a congruence ρ on S such that S/ρ is finite and such that the classes of a and b are distinct). In 1958 A. I. Malcev proved the following theorem: *Any finitely generated abelian semigroup is residually finite* [6]. Malcev's elegant proof is based on two other results:

(1) Every finitely generated commutative algebra over a field of characteristic 0 is isomorphic to an algebra of $n \times n$ matrices over a field of characteristic 0 [5].

(2) Every finitely generated group or semigroup of $n \times n$ matrices over a field of characteristic 0 is residually finite [4].

The theorem of (1) is not easily extendable to noncommutative algebras. Furthermore in the proof of (2) Malcev used the Hilbert basis theorem which allows one to establish the result without an explicit construction of a congruence separating two elements. For possible extensions of Malcev's theorem to nonabelian semigroups, it is of interest to have an explicit description of congruences of finite index separating two given elements.

A solution to this problem is provided by our Theorem 3. For connections of residual finiteness with the problem of embedding a semigroup in a compact semigroup the reader is referred to [1].

1. Notation and conventions.
To avoid notation complications we assume that the semigroups discussed have an identity. If S has no

---

[1] The results contained in this paper have been presented at the Symposium on Semigroups and the Multiplicative Structure of Rings held at the University of Puerto Rico in Mayaguez, March 1970.

identity, then $S^1 = S \cup \{1\}$ is residually finite if and only if S is. Further in the case S has no identity, all the congruences defined on S^1 in this paper have restrictions to S which are easy to describe.

Recall that on an abelian semigroup S with identity, the Green congruence $\mathcal{H}$ is defined by $a \ \mathcal{H} \ b$ iff $aS = bS$. If H denotes an $\mathcal{H}$-class, define

$$G(H) = \{x \in S \mid Hx \cap H \neq \varnothing\};$$

$$Z(H) = S \backslash G(H);$$

$$\Delta(H) = \{x \in S \mid sS \nsubseteq xS \text{ for any } s \in H\};$$

$$\Sigma(H) = G(H) \cup \Delta(H);$$

$$U(H) = \{x \in S \mid sx = x \text{ for every } s \in H\}.$$

We also define a congruence σ_H by $x \ \sigma_H \ y$ iff either $x, y \in G(H)$ and $xs = ys$ for every $s \in H$ or $x, y \in Z(H)$.

The following facts are straightforward to prove and will be used in the next section without explicit mention: $G(H)$ is a subsemigroup of S containing $U(H)$; $Z(H)$ is a prime ideal of S containing $\Delta(H)$, and the latter is also an ideal of S; σ_H is the congruence defined by the Schützenberger representation of S relative to H [2, 3.5]; $\Sigma(H)$ is a subsemigroup of H and $\Sigma(H)/\sigma_H$ is a group with zero (or a group). If H is a regular $\mathcal{H}$-class [2, 2.3], then H is a maximal subgroup of S, $H \subseteq G(H)$ and $H^0 \cong \Sigma(H)/\sigma_H$; otherwise $H \subseteq Z(H) \backslash \Delta(H)$.

2. **Congruences of finite index separating elements.** Let $S = S^1$ be an abelian semigroup and H an $\mathcal{H}$-class of S. Define an equivalence ρ_H on S by $x \ \rho_H \ y$ if $x, y \in \Sigma(H)$ and $x \ \sigma_H \ y$ or $x, y \notin \Sigma(H)$ and $x = y$. Let $\bar{\rho}_H$ denote the smallest congruence on S containing ρ.

LEMMA 1. (1) *The restriction of $\bar{\rho}_H$ to $\Sigma(H)$ coincides with σ_H.*
(2) *The restriction of $\bar{\rho}_H$ to H is the equality.*
(3) *If H is a subgroup of S, then $\bar{\rho}_H = \sigma_H$.*

PROOF. We will construct $\bar{\rho}_H$ explicitly. The subset $Z(H) \backslash \Delta(H)$ can be divided in two parts Z_1 and Z_2 as follows:
$Z_1 = \{x \in Z(H) \backslash \Delta(H) \mid \text{ there exists } u \in U(H) \text{ such that } xu \in H\}$;
$Z_2 = $ complement of Z_1 in $Z(H) \backslash \Delta(H)$.
Then $Z_1 \cup \Delta(H)$ is an ideal of S. To prove it, let $x \in Z_1 \cup \Delta(H)$ and $y \in S$. If $xy \notin \Delta(H)$, then $x \in Z_1$ and there exists $u \in U(H)$ such that $xu \in H$. Since $xy \in Z(H) \backslash \Delta(H)$, we have $sS \subseteq xyS$ for any $s \in H$ and $sS \subseteq xyuS$. On the other hand $xyuS \subseteq xuS = sS$. It follows $xyu \in H$ and $xy \in Z_1$.

On Z_2 we define δ by: $v \ \delta \ w$ iff there exists $x, y \in G(H)$, $z \in Z_2$, such

that $x \, \sigma_H \, y$ and $v = zx$, $w = zy$. Denote by δ^t the transitive closure of δ.

Define the relation θ on S by: $x \, \theta \, y$ iff (a) x and $y \in G(H)$ and $x \, \sigma_H \, y$ or (b) x and $y \in Z_1$ and there exists u, $v \in U(H)$ such that $ux = vy$ or (c) x and $y \in Z_2$ and $x \, \delta^t \, y$ or (d) x, $y \in \Delta(H)$.

One checks easily that θ is an equivalence. To show that θ is a congruence, assume $x \, \theta \, y$ and let $z \in S$. In case one of x, y, z is in $\Delta(H)$ obviously $xz \, \theta \, yz$. Thus we consider only the other cases:

(i) $x, y \in G(H)$. If $z \in G(H)$, clearly xz, $yz \in G(H)$ and $xz \, \sigma_H \, yz$. If $z \in Z_1$, there exists $u \in U(H)$ such that $zu \in H$. It follows xz, $yz \in Z_1$ and $xzu = yzu$, i.e. $xz \, \theta \, yz$. If $z \in Z_2$, then xz, $yz \in Z_2$. To see this, assume for example $xz \in Z_1$; then for some $u \in U(H)$, $xzu \in H$; but by the definition of $\mathcal{K}$ and σ_H, $x \in G(H)$ implies the existence of $x' \in G(H)$ such that $xx' \in U(H)$; then $xx'zu \in H$ and $xx'u \in U(H)$ which contradicts $z \in Z_2$. It is not possible that xz and $yz \in \Delta(H)$, for $z \notin \Delta(H)$ implies $sS \subseteq zS$ for any $s \in H$; thus $sS = sxS \subseteq xzS$ and $xz \notin \Delta(H)$. The only possibility is xz, $yz \in Z_2$. By the definition of δ, we then have $xz \, \theta \, yz$.

(ii) x, $y \in Z_1$. There exists u, $v \in U(H)$ such that xu, $yv \in H$. If $z \in G(H)$ then xzu, $yzv \in H$ and xz, $yz \in Z_1$. Since $xu' = yv'$ for some u', $v' \in U(H)$, clearly $xzu' = yzv'$ and $xz \, \theta \, yz$. Now if $z \in Z(H)$, either $xz \in Z_1$ or $xy \in \Delta(H)$. If for example $xz \in Z_1$, then $xzu'' \in H$ for some $u'' \in U(H)$. It follows $xzu'u'' = yzv'u'' \in H$ and $yz \in Z_1$. Consequently $xz \, \theta \, yz$.

(iii) x, $z \in Z_2$. To show that $xz \, \theta \, yz$ for every $z \in S$, it is sufficient to show that $x \, \delta \, y$ implies $xz \, \theta \, yz$ for every $z \in S$. Assuming $x \, \delta \, y$, there exists $\alpha, \beta \in G(H)$ and $t \in Z_2$ such that $x = \alpha t$, $y = \beta t$, $\alpha \, \sigma_H \, \beta$. If $z \in G(H)$, then αz, $\beta z \in G(H)$ and $\alpha z \, \sigma_H \, \beta z$. Thus $xz = \alpha zt$ and $yz = \beta zt$ imply $xz \, \delta \, yz$ (it is clear that xz, $yz \in Z_2$). In case $z \in Z_1$, then xz and $yz \in Z_1 \cup \Delta(H)$. If $xz \in Z_1$ for example, there exists $u \in U(H)$ such that $xzu \in H$. But $xzu = xzuv$ where v is an element of $U(H)$ such that $zv \in H$. Now, $xzvu = \alpha tzvu = \alpha zvtu = \beta zvtu = yzvu \in H$; which shows that $yz \in Z_1$ and establishes $xz \, \theta \, yz$. Finally, when $z \in Z_2$, either $tz \in \Delta(H)$ and then xz, $yz \in \Delta(H)$, or $tz \in Z_2$ and again $xz \, \theta \, yz$ or $tz \in Z_1$. In this last case $tzu \in H$ for some $u \in U(H)$; it follows $xzu = \alpha tzu = \beta tzu = yzu \in H$, which shows that xz, $yz \in Z_1$ and satisfy $xz \, \theta \, yz$.

From the definition of θ one sees easily that $\rho \subseteq \theta$. If γ is a congruence containing ρ, let us show that $\theta \subseteq \gamma$. If $x \, \theta \, y$ and we are in the cases (a) or (d) above, clearly $x \, \gamma \, y$. In the case (b), $ux = vy$ implies $ux \, \rho \, vy$ and thus $ux \, \gamma \, vx$. But we have $1 \, \rho \, u \, \rho \, v$ and also $1 \, \gamma \, u \, \gamma \, v$. It follows $x \, \gamma \, ux \, \gamma \, vy \, \gamma \, y$. In the case (c) with $x \, \delta \, y$, then $x = \alpha t$, $y = \beta t$ with $\alpha, \beta \in G(H)$ satisfying $\alpha \, \sigma_H \, \beta$. Since $\alpha \, \rho \, \beta$, it follows $\alpha \, \gamma \, \beta$ and thus $x \, \gamma \, y$. Consequently $\theta = \bar{\rho}_H$. The assertion (1) in the statement of

the lemma is obvious (see (a) and (d) in the definition of θ). If H is a subgroup of S, then $H \subset G(H)$ and $Z(H) = \Delta(H)$ which proves (3). Furthermore in this case, the restriction of θ to H, which coincides with σ_H, is the equality. If H is not a subgroup of S, then $H \subseteq Z_1$ and by part (b) of the definition of θ, θ restricted to H is the equality. This completes the proof of (2).

COROLLARY. *Let S be an abelian semigroup with identity and H an $\mathcal{H}$-class of S. Denote by ϕ_H the canonical homomorphism $\phi_H : S \to S/\bar{\rho}_H$. Then $\phi_H(S)$ has a nonzero ideal M contained in every nonzero ideal of S. M is isomorphic to the principal factor of H (i.e. $H/\Delta(H)$). The group of units of $\phi_H(S)$ is the Schützenberger group of $M \backslash 0$.*

PROOF. The corollary is a transcription in $S/\bar{\rho}_H$ of properties of $\bar{\rho}_H$. One may observe that if H is a subgroup of S with identity e, then ϕ_H can be defined by $\phi_H(x) = xe$ if $xe \in H$ and $\phi_H(x) = 0$ if $xe \notin H$.

Our next step consists in defining the convenient congruences on finitely generated semigroups with the same properties as $\phi_H(S)$.

LEMMA 2. *Let S be a finitely generated abelian semigroup with identity and zero. Assume that S has an ideal $M \neq 0$ contained in every nonzero ideal of S, and that the group G of units of S is the Schützenberger group of $M \backslash 0$. Let N be a subgroup of G of finite index. Then, the congruence on S defined by $a \rho_N b$ iff $aN = bN$ is of finite index. Furthermore, given $s, t \in M$, $s \neq t$, there exists a subgroup N of G of finite index such that $sN \neq tN$.*

PROOF. If $H = M \backslash 0$ is a group then $H = G$ and $S = G^0$. The last part of the lemma expresses the residual finiteness of a finitely generated abelian group. Consider now the case $M^2 = 0$. We have $G(H) = G$, $\Delta(H) = 0$, $Z(H) = M \cup Z_2$ and $Z_1 = H$ (Z_1 and Z_2 are defined in the proof of Lemma 1). Since N is of finite index, ρ_N has a finite number of classes in G. Since G acts transitively on H, ρ_N has also a finite number of classes in M. Thus it remains to show that Z_2 contains only a finite number of ρ_N-classes. Considering the quotient semigroup S/ρ_N it is equivalent to prove that if a semigroup S satisfies all the hypotheses of the lemma and also has a finite group of units, then S is finite. Thus let $x_1, x_2, \cdots, x_r$ be the generators of S contained in $Z(H)$ and let $g_1, g_2, \cdots, g_k$ be the elements of G. Then, the elements $x_i g_j$ with $1 \leq j \leq k$, form a set of generators of $Z(H)$. Let $\{y_1, \cdots, y_n\}$ be a minimal set of generators of $Z(H)$. Then $\{y_1, y_2, \cdots, y_n\} \subseteq Z_2$ since for every element $z \in Z_2$ there exists $z' \in Z_2$ such that $zz' \in H$. To prove that $Z(H)$ (and thus S) is finite, we shall show that for every y_i ($1 \leq i \leq n$) there exists an integer δ_i such that $y_i^{\delta_i} = 0$. Let s be a

fixed element of H. From the fact that $sy_i = 0$ for every $i = 1, \cdots, n$, we deduce that s cannot have two expressions $y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_n^{\alpha_n}$ and $y_1^{\beta_1} y_2^{\beta_2} \cdots y_n^{\beta_n}$ with $\alpha_i \leq \beta_i$ for $i = 1, 2, \cdots, n$ and $\alpha_{i_0} \neq \beta_{i_0}$ for at least one i_0. Thus [**3**, Proposition 4.1] the number of possible expressions of s as a product of $y_1, y_2, \cdots, y_n$ is finite. Let $s = y_1^{\gamma_1} y_2^{\gamma_2} \cdots y_i^{\gamma_i} \cdots y_n^{\gamma_n}$ be an expression of s with a maximal γ_i. Then $y_i^{\gamma_i+1} = 0$ or $y_i^{\gamma_i+2} = 0$. To see this, assume $y_i^{\gamma_i+1} \neq 0$; then $y_i^{\gamma_i+1} \notin Z_2$, otherwise we could find $z \in Z_2$ such that $y_i^{\gamma_i+1} z = s$ contradicting the maximality of γ_i. Similarly $y_i^{\gamma_i+1} \neq s$. Thus $y_i^{\gamma_i+1} = t$ for some $t \in H$, $t \neq s$; it follows $y_i^{\gamma_i+2} = 0$ and for every y_i, there exists δ_i such that $y_i^{\delta_i} = 0$. Therefore $Z(H)$ is finite and the first part of the lemma is proved. Now consider two elements $s, t \in M$, $s \neq t$. If $s, t \in H$, there exists exactly one $g \in G$ such that $sg = t$. But G being finitely generated is residually finite and there exists a subgroup N of G of finite index with $g \notin N$. The corresponding congruence ρ_N is of finite index. If $sN = tN$ then $t = sn = sg$ for some $n \in N$; it follows $s = sng^{-1}$ and $ng^{-1} = 1$ implies $g \in N$, a contradiction. Thus $sN \neq tN$. If $s \in H$, $t = 0$, one may take $N = G$, and this completes the proof of the lemma.

With S and N as in Lemma 2 we denote by ψ_N the canonical homomorphism $\psi_N : S \to S / \rho_N$. The following theorem summarizes all the results obtained previously.

THEOREM 3. *Let S be a finitely generated abelian semigroup and a, $b \in S$, $a \neq b$.*

(a) *If a and b are not $\mathfrak{IC}$ equivalent, let H denote the $\mathfrak{IC}$-class of the element a or b generating the larger ideal, or one of the two $\mathfrak{IC}$-classes if the ideals are not comparable. If G denotes the Schützenberger group of H, the homomorphism $\psi_G \circ \phi_H$ maps S onto a finite semigroup and a, b have distinct images.*

(b) *If a and b are $\mathfrak{IC}$ equivalent, let H denote their common $\mathfrak{IC}$-class, and G the Schützenberger group of H. Let N be a subgroup of G of finite index which does not contain the unique element $g \in G$ such that $ag = b$. Then $\psi_N \circ \phi_H$ maps S onto a finite semigroup and a, b have distinct images.*

In particular, this gives a direct proof of the theorem of Malcev mentioned in the introduction.

REFERENCES

1. L. W. Anderson and R. P. Hunter, *On residual properties of certain semigroups*, Contributions to Extension Theory of Topological Structures (Proc. Sympos., Berlin, 1967), Deutsch. Verlag Wiss., Berlin, 1969, pp. 15–19. MR **39** #7017.

2. A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*. Vol. 1, Math. Surveys, no. 7, Amer. Math. Soc., Providence, R. I., 1961. MR **24** #A2627.

3. S. Eilenberg and M. P. Schützenberger, *Rational sets in commutative monoids*, J. Algebra **13** (1969), 173–191. MR **40** #254.

4. A. I. Mal'cev, *On the faithful representation of infinite groups by matrices*, Mat. Sb. **8 (50)** (1940), 405–422; English transl., Amer. Math. Soc. Transl. (2) **45** (1965), 1–18. MR **2**, 216.

5. ———, *On the representations of infinite algebras*, Mat. Sb. **13 (55)**, (1943), 263–286. (Russian) MR **6**, 116.

6. ———, *On homomorphisms onto finite groups*, Ivanov. Gos. Ped. Inst. Uč. Zap. **18** (1958), 49–60. (Russian)

PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PENNSYLVANIA 16802