On the congruences of finitely generated free semigroups

By A. ÁDÁM in Budapest and G. POLLÁK in Szeged

To Professor L. Rédei on his 70th birthday

I. General preliminaries

In Sections 1 and 2 we introduce the basic terminology used in this paper for semigroups and groups, respectively. The content of Section 2 will be referred to only from Section 5 on (but not in Sections 3 and 4).

1. The set consisting of the elements $x_1, x_2, \ldots, x_k$ will be denoted by $(x_1, x_2, \ldots, x_k)$ (the context will always elucidate whether an ordered or an unordered set is meant).

Let X be a finite unordered set. We denote by $F(X)$ the free semigroup with identity element generated by X (non-commutative for $|X|>1$). The elements of X are called *generators*. The elements of $F(X)$ are called *words* too. If a subset G of $F(X)$ satisfies the implication

$$(p\in G \ \& \ x\in X) \Rightarrow px\in G$$

then we say that G is a *right ideal*. The *length* $|p|$ of the word $p=x_1 \ldots x_k$ is the number k of the generators whose product equals p. The words of length 1 are identified with the generators themselves. The identity element e of $F(X)$ is the only word of length 0 of $F(X)$; it is called the *empty word*, too.

Let an element $p=x_1 \ldots x_k$ of $F(X)$ be considered, let $i\,(\leqq k=|p|)$ be a natural number. Then the words $l_i(p)$ and $r_i(p)$ are defined by the formulae

$$l_i(p) = x_1 \ldots x_{k-i} \quad \text{and} \quad r_i(p) = x_{k-i+1} \ldots x_k.$$

Particularly, $l_k(p)=r_0(p)=e$. (We shall use the above notation chiefly in case $i=1$.) We obviously have

$$l_1(pq) = pl_1(q), \quad r_1(pq) = r_1(q)$$

if $|q|>0$.

The *right compatibility* of a binary relation ϱ on $F(X)$ is defined by

$$(\mathbf{C}_r) \qquad \varrho(p, q) \Rightarrow \varrho(pr, qr) \qquad (p, q, r \in F(X)).$$

Obviously, $(\mathbf{C}_r)$ is equivalent to

$$(\mathbf{C}'_r) \qquad \varrho(p, q) \Rightarrow \varrho(px, qx) \qquad (p, q \in F(X), x \in X).$$

A reflexive, symmetric and right compatible relation is called a *quasi-right-congruence*. A *right congruence* is then a transitive quasi-right-congruence.

For right congruences we introduce another technique of notation: the relation is denoted by $\mathscr{C}$ (instead of ϱ), furthermore, we write

$$p \equiv q \pmod{\mathscr{C}}$$

instead of $\varrho(p, q)$ and

$$p \not\equiv q \pmod{\mathscr{C}}$$

instead of $\bar{\varrho}(p, q)$.

2. Let X be a finite set (as in § 1). We denote by $G(X)$ the free group generated by X (non-commutative for $|X|>1$). Evidently, $F(X) \subseteq G(X)$. Define the subset $F^\circ(X)$ of $G(X)$ in the following manner: $\mu (\in G(X))$ belongs to $F^\circ(X)$ if and only if there exist two elements p, q of $F(X)$ such that $\mu = pq^{-1}$. If $\mu \in G(X)$ then, obviously, either both or none of μ, μ^{-1} are contained in $F^\circ(X)$.

Let $\mu, \nu \in F^\circ(X)$. We say that ν is a *right multiple* of μ (or μ is a *left divisor* of ν) if there exists $t \in F(X)$ such that $\nu = \mu t$ (notation: $\mu \underset{l}{|} \nu$). Dually, μ is a *right divisor* of ν (or ν is a *left multiple* of μ) if there exists $t \in F(X)$ such that $t\mu = \nu$ (notation: $\mu \underset{r}{|} \nu$). Further, we shall use the short notations $\mu \underset{l}{\|} \nu$ and $\mu \underset{r}{\|} \nu$ for $\mu \underset{l}{|} \nu$, $\mu \neq \nu$, and $\mu \underset{r}{|} \nu$, $\mu \neq \nu$, respectively.

In free commutative semigroups divisibility is a lattice order, in the non-commutative case $F^\circ(X)$, though ordered under right (resp. left) divisibility, is not directed under these orders. It holds e.g.

Lemma 0. *If* $p \underset{l}{|} a$, $q \underset{l}{|} a$ $(p, q, a \in F(X))$ *then either* $p \underset{l}{|} q$ *or* $q \underset{l}{|} p$.

Proof. p and q being beginning parts of the same word, one of them must be the shorter one.

We say that p and q are *comparable* $(p, q \in F(X))$, if $p \underset{l}{|} q$ or $q \underset{l}{|} p$.

We define the *least common right multiple* $[\mu, \nu]_r$ and the *greatest common right divisor* $(\mu, \nu)_r$ for $\mu, \nu \in F^\circ(X)$ as usual: $[\mu, \nu]_r$ is a common right multiple of μ and ν such that any common right multiple of them is a right multiple of $[\mu, \nu]_r$; and, similarly, $(\mu, \nu)_r$ is a common right divisor such that any common right divisor

is a right divisor of it. Lemma 0 implies that, for $p, q \in F(X)$, $[p, q]_r$ exists if and only if p and q are comparable. On the other hand, it is easy to see that

$$(p, q)_r = r_i(p) = r_i(q) \quad \text{where} \quad r_{i+1}(p) \neq r_{i+1}(q) \quad \text{for} \quad p, q \in F(X).$$

Such an i exists since $r_0(p) = r_0(q) = e$.

For $\mu \in F^\circ(X)$ we use the shorter notation

$$\mu^+ = [\mu, e]_r, \quad \mu^- = (\mu, e)_r^{-1}.$$

The fact that μ^+ and μ^- exist for every μ follows from

Lemma 1. *Let $p, q \in F(X)$, $\mu = pq^{-1}$. Then there exist uniquely determined elements p', q', t such that*

(i) $p = p't$,
(ii) $q = q't$,
(iii) $r_1(p') \neq r_1(q')$ *or* $p' = e$ *or* $q' = e$.

Moreover, the subsequent equalities hold:

$$p' = \mu^+, \quad q' = \mu^-, \quad pq^{-1} = \mu^+(\mu^-)^{-1}. \tag{2}$$

Proof. If $p = q$ then $t = p = q$, $p' = q' = e$ obviously suffice the conditions. Now let $p \neq q$. Put $t = (p, q)_r$. Then p' and q' are uniquely determined by (i) and (ii), and (iii) is fulfilled obviously. The uniqueness of t, p', q' follows now from the fact that the only right divisors of p (q) are the words $r_i(p), 1 \leqq i \leqq |p|$ ($r_i(q), 1 \leqq i \leqq |q|$).

Furthermore, $\mu = pq^{-1} = p'q'^{-1}$ and therefore it suffices to prove $p' = \mu^+$ ($q' = \mu^-$ follows then by a similar argument). But $p' = ep' = \mu q'$, i.e. $e \underset{l}{|} p'$, $\mu \underset{l}{|} p'$. On the other hand, if $e \underset{l}{|} s$ (i.e. $s \in F(X)$), $\mu \underset{l}{|} s$ then $s = \mu u = p'q'^{-1}u$. Now $p'q'^{-1}u \in F(X)$, $r_1(p') \neq r_1(q')$ imply $q'^{-1}u \in F(X)$. So we have $p' \underset{l}{|} s$, and the proof is complete.

It is a matter of routine to check the following properties:

$$\mu^- = (\mu^{-1})^+, \quad \mu^+ = (\mu^{-1})^-, \quad \mu^{-1} = \mu^-(\mu^+)^{-1}.$$

For arbitrary elements μ, ν of $F^\circ(X)$ we have:

Lemma 2. $[\mu, \nu]_r$ *exists if and only if μ^+ and ν^+ are comparable. In this case*

$$[\mu, \nu]_r = \begin{cases} \mu^+ & \text{if} \quad \nu^+ \underset{l}{\|} \mu^+, \\ \nu^+ & \text{if} \quad \mu^+ \underset{l}{\|} \nu^+, \\ \mu^+(\mu^-, \nu^-)_r^{-1} & \text{if} \quad \mu^+ = \nu^+. \end{cases}$$

Lemma 2′. *$(\mu, \nu)_r$ exists if and only if μ^- and ν^- are comparable. In this case*

$$(\mu, \nu)_r = \begin{cases} (\mu^-)^{-1} & \text{if } \nu^- \underset{l}{\|} \mu^-, \\ (\nu^-)^{-1} & \text{if } \mu^- \underset{l}{\|} \nu^-, \\ (\mu^+, \nu^+)_r(\mu^-)^{-1} & \text{if } \mu^- = \nu^-. \end{cases}$$

Proof of Lemma 2. Let $\mu \underset{l}{|} \lambda$, $\nu \underset{l}{|} \lambda$. Then $\nu^{-1}\lambda = \nu^-(\nu^+)^{-1}\lambda^+(\lambda^-)^{-1} \in F(X)$, $\mu^-(\mu^+)^{-1}\lambda^+(\lambda^-)^{-1} \in F(X)$. These imply $(\nu^+)^{-1}\lambda^+ \in F(X)$, $(\mu^+)^{-1}\lambda^+ \in F(X)$, i.e. $\mu^+ \underset{l}{|} \lambda^+$, $\nu^+ \underset{l}{|} \lambda^+$. Thus μ^+ and ν^+ have a common right multiple and so, as already remarked, they must be comparable. This proves the necessity of the condition.

Conversely, if μ^+ and ν^+ are comparable then either $\mu^+ = \nu^+$, $(\mu^-, \nu^-)_r = t$, $\mu^- = mt$, $\nu^- = nt$ and $\mu^+(\mu^-, \nu^-)_r^{-1} = \mu m = \nu n$, or $\nu^+ \underset{l}{\|} \mu^+$ and $\mu \underset{l}{|} \mu^+$, $\nu \underset{l}{|} \nu^+ \underset{l}{\|} \mu^+$, or $\mu^+ \underset{l}{\|} \nu^+$ and $\nu \underset{l}{|} \nu^+$, $\mu \underset{l}{|} \mu^+ \underset{l}{\|} \nu^+$. On the other hand, if $\mu \underset{l}{|} \lambda$, $\nu \underset{l}{|} \lambda$ then, as above, $\mu^+ \underset{l}{|} \lambda^+$, $\nu^+ \underset{l}{|} \lambda^+$. This proves the lemma if $\mu^+ \neq \nu^+$. In the remaining case let $\lambda^+ = \mu^+ l$; then $\mu^{-1}\lambda = \mu^-(\mu^+)^{-1}\lambda^+(\lambda^-)^{-1} = mtl(\lambda^-)^{-1} \in F(X)$, $\nu^{-1}\lambda = ntl(\lambda^-)^{-1} \in F(X)$ and either $l \neq e$, $\lambda^- = e$ or $l = e$, $t = t'\lambda^-$ (since $r_1(m) \neq r_1(n)$). In both cases we have $\mu^+(\mu^-, \nu^-)_r \underset{l}{|} \lambda$ and this completes the proof of the lemma.

Lemma 2′ follows from the dual of Lemma 2 in virtue of the equality

$$(\mu, \nu)_r = [\mu^{-1}, \nu^{-1}]_r^{-1}. \tag{3}$$

Indeed, let $(\mu, \nu)_r = \gamma$, $\mu = m\gamma$, $\nu = n\gamma$. Then $\mu^{-1} = \gamma^{-1}m^{-1}$, $\nu^{-1} = \gamma^{-1}n^{-1}$ and thus $\gamma^{-1} = \mu^{-1}m = \nu^{-1}n$ is a common right multiple of μ^{-1} and ν^{-1}. On the other hand, if $\lambda = \mu^{-1}m' = \nu^{-1}n'$ $(m', n' \in F(X))$ then $\mu = m'\lambda^{-1}$, $\nu = n'\lambda^{-1}$ and so $\lambda^{-1} \underset{r}{|} \gamma$, i.e. $\gamma = c\lambda^{-1}$ $(c \in F(X))$ and $\lambda = \gamma^{-1}c$ is a right multiple of $\mu^{-1} = (\mu, \nu)_r^{-1}$.

II. Characterization of the right congruences inside $F(X)$

3. Let Ω be a set consisting of some unordered [1]) pairs of words. (Also pairs of type (p, p) are permitted.) We define the properties $(\mathbf{A}_1)$, $(\mathbf{A}_2)$ for Ω in the following manner:

$(\mathbf{A}_1)$ $(e, e) \in \Omega$.

$(\mathbf{A}_2)$ Whenever $(p, q) \in \Omega$, $t \in F(X)$ and $t \neq e$, then $(pt, qt) \notin \Omega$.

[1]) Equivalently, we may consider Ω consisting of ordered pairs provided that $(p, q) \in \Omega$ implies $(q, p) \in \Omega$.

Let us consider a quasi-right-congruence ϱ of $F(X)$. We say that the unordered pair (p, q) (where $p \in F(X)$, $q \in F(X)$, $|p| = j$, $|q| = k$) is a *critical pair* for ϱ if

$$\varrho(p, q) = \uparrow$$

and either of the subsequent three assertions holds:

(i) at least one of p, q is equal to e,

(ii) $r_1(p) \neq r_1(q)$,

(iii) $\varrho(l_1(p), l_1(q)) = \downarrow$.

Lemma 3. *For any pair* (r, s) $(r, s \in F(X))$, $\varrho(r, s)$ *is* $\uparrow$ *if and only if there exist three elements* p, q, t *of* $F(X)$ *such that* $r = pt$, $s = qt$ *and* (p, q) *is a critical pair for* ϱ.

Proof. The *sufficiency* follows from the property $(\mathbf{C}_r')$ of ϱ (applied successively). In order to verify *necessity*, let us consider the maximal i with $r_i(r) = r_i(s)$. If $\varrho(l_i(r), l_i(s)) = \uparrow$ then $l_i(r), l_i(s), r_i(r)$ satisfy the condition (as p, q, t respectively), because $(l_i(r), l_i(s))$ fulfils either (i) or (ii). If $\varrho(l_i(r), l_i(s)) = \downarrow$ then there exists a maximal h such that ($h < i$ and)

$$\varrho(l_h(r), l_h(s)) = \uparrow;$$

in this case $l_h(r), l_h(s), r_h(r) (= r_h(s))$ are convenient as p, q, t, resp., since $(l_h(r), l_h(s))$ fulfils (iii).

Lemma 4. *The set* Ω *of all the critical pairs for a quasi-right-congruence* ϱ *satisfies* $(\mathbf{A}_1)$, $(\mathbf{A}_2)$.

Proof. $\varrho(e, e) = \uparrow$ by reflexivity. This and (i) imply that $(\mathbf{A}_1)$ is fulfilled on Ω.

Suppose $(p, q) \in \Omega$ and $(e \neq) t \in F(X)$. $\varrho(p, q) = \uparrow$ implies $\varrho(pt, qt) = \uparrow$ by an iterated application of $(\mathbf{C}_r')$. We are going to show that the pair (pt, qt) does not fulfil any of (i), (ii), (iii). Since $t \neq e$, (i) cannot be satisfied. The same holds for (ii), because

$$r_1(pt) = r_1(t) = r_1(qt).$$

Assume that (iii) holds for (pt, qt); we want to get a contradiction. On one hand,

$$\downarrow = \varrho(l_1(pt), l_1(qt)) = \varrho(p \cdot l_1(t), q \cdot l_1(t));$$

on the other hand, $\varrho(p, q) = \uparrow$ implies

$$\varrho(p \cdot l_1(t), q \cdot l_1(t)) = \uparrow$$

by $(\mathbf{C}_r')$.

Lemma 5. *Suppose that the set* Ω *of unordered pairs of elements of* $F(X)$ *satisfies* $(\mathbf{A}_1)$ *and* $(\mathbf{A}_2)$. *Let a binary relation* ϱ *be defined by the following rule:*

$\varrho(r, s)=\uparrow$ (where $r, s\in F(X)$) if and only if there exist a pair (p, q) $(\in\Omega)$ and an element $t(\in F(X))$ such that $r=pt$ and $s=qt$. Then ϱ is a quasi-right-congruence of $F(X)$, moreover, the set of critical pairs of ϱ coincides with Ω.

Proof. (A_1) implies $\varrho(s, s)=\uparrow$, thus ϱ is reflexive. Since Ω consists of unordered pairs, ϱ is symmetrical. If $\varrho(r, s)=\uparrow$, $r=pt$, $s=qt$ and $(p, q)\in\Omega$ then $rx=(pt)x=$ $=p(tx)$, $sx=(qt)x=q(tx)$ for any $x(\in X)$, hence $\varrho(rx, sx)=\uparrow$, i.e. ϱ is right compatible.

It remains to verify the last statement of the lemma. Let (p, q) be a critical pair of ϱ. Since $\varrho(p, q)=\uparrow$, there exist three elements p', q', d of $F(X)$ such that $(p', q')\in\Omega$, $p=p'd$, $q=q'd$. If $d\neq e$, then neither (i) nor (ii) nor (iii) can be valid for (p, q); this contradiction shows that $d=e$, thus $(p, q)=(p', q')\in\Omega$. Conversely, let (p, q) be contained in Ω. We have $\varrho(p, q)=\uparrow$ (because of the possibility $d=e$). There exist a critical pair (p', q') and an element d' of $F(X)$ such that $p=p'd'$, $q=q'd'$. As we have already seen, $(p', q')\in\Omega$. If $d'\neq e$, then Ω does not fulfil (A_2), hence $d'=e$ and $(p, q)\,(=(p', q'))$ is a critical pair.

Lemmas 4, 5 combine to prove

Theorem 1. *To any quasi-right-congruence ϱ of $F(X)$ let us assign the set Ω of critical pairs of ϱ. This assignment is a one-to-one correspondence between all the quasi-right-congruences ϱ and all the sets Ω (of pairs of elements of $F(X)$) satisfying the properties (A_1), (A_2).*

4. The collection of right congruences of $F(X)$ is a proper subset of the collection of the quasi-right-congruences, since transitivity is required, too. Hence the collection of those sets Ω which correspond to right congruences (by virtue of Theorem 1) is likewise narrower than the set of all the Ω fulfilling (A_1) and (A_2).

The definition of the critical pair can be restated in case of a right congruence in the following manner: an unordered pair (p, q) of elements of $F(X)$ is a *critical pair* for the right congruence $\mathscr{C}$ if

$$p\equiv q \pmod{\mathscr{C}}$$

and one of the subsequent three assertions holds:

(i) at least one of p, q equals to e,

(ii) if $p\neq e$, $q\neq e$ then $r_1(p)\neq r_1(q)$,

(iii) if $p\neq e$, $q\neq e$ then $l_1(p)\not\equiv l_1(q) \pmod{\mathscr{C}}$.

Theorem 2. *Let Ω be a set of unordered pairs of elements of $F(X)$ and assume that Ω fulfils (A_1) and (A_2). The quasi-right-congruence ϱ corresponding to Ω (in sense of Lemma 4 and Theorem 1), is a right congruence if and only if the following additional requirements (A_3), (A_4) are satisfied by Ω:*

($\mathbf{A}_3$) *Whenever* $(p_1, q_1)\in\Omega$, $(p_2, q_2)\in\Omega$ *and there exists an element* $s(\neq e)$ *of* $F(X)$ *such that* $p_1=p_2s$, *then* $(q_1, q_2s)\in\Omega$.

($\mathbf{A}_4$) *Whenever* $(p, q_1)\in\Omega$ *and* $(p, q_2)\in\Omega$ *(where* p *is common) then there exist three elements* p', q', t *of* $F(X)$ *such that* $(p', q')\in\Omega$, $q_1=p't$ *and* $q_2=q't$ *(*$t=e$ *is permitted).*

Proof. *Necessity.* Let us consider the set Ω of critical pairs of a right congruence $\mathscr{C}$ of $F(X)$. In order to prove ($\mathbf{A}_3$), assume $(p_1, q_1)\in\Omega$, $(p_2, q_2)\in\Omega$, $p_1=p_2s$, $s\neq e$. Since $p_2\equiv q_2 \pmod{\mathscr{C}}$ implies $p_1=p_2s\equiv q_2s \pmod{\mathscr{C}}$ (by ($\mathbf{C}_r$)) and $p_1\equiv q_1 \pmod{\mathscr{C}}$ holds, we have $q_1\equiv q_2s \pmod{\mathscr{C}}$ by symmetry and transitivity.

Suppose that none of (i), (ii) and (iii) holds for (q_1, q_2s); we shall get a contradiction. We have $q_1\neq e$, $q_2s\neq e$,

$$r_1(q_1)=r_1(q_2s)=r_1(s) \tag{4}$$

and

$$l_1(q_1)\equiv l_1(q_2s)=q_2\cdot l_1(s) \pmod{\mathscr{C}} \tag{4'}$$

(since $s\neq e$). We are going to show that (p_1, q_1) cannot fulfil any of (i), (ii), (iii). $p_1(=p_2s)\neq e$, $q_1\neq e$ hold evidently. (4) implies $r_1(p_1)=r_1(p_2s)=r_1(s)=r_1(q_1)$. Since

$$q_2l_1(s)\equiv p_2l_1(s)=l_1(p_2s)=l_1(p_1) \pmod{\mathscr{C}}$$

holds, formula (4') implies

$$l_1(p_1)\equiv l_1(q_1) \pmod{\mathscr{C}}.$$

Thus (p_1, q_1) satisfies none of (i), (ii), (iii), hence (p_1, q_1) is not a critical pair. This contradicts the inclusion $(p_1, q_1)\in\Omega$.

Now we want to verify ($\mathbf{A}_4$). The congruences

$$p\equiv q_1 \pmod{\mathscr{C}}, \qquad p\equiv q_2 \pmod{\mathscr{C}}$$

imply

$$q_1\equiv q_2 \pmod{\mathscr{C}},$$

hence there exist three elements with the mentioned property (in consequence of Lemma 3).

Sufficiency. Let ϱ be a quasi-right-congruence, denote the set of critical pairs of ϱ by Ω. Suppose that Ω satisfies ($\mathbf{A}_3$) and ($\mathbf{A}_4$). We shall prove that ϱ is transitive.

Let r, s, v be three elements of $F(X)$ such that $\varrho(r, s)=\varrho(s, v)=\dagger$. Lemma 3 ensures the existence of six elements $p_1, q_1, t_1, p_2, q_2, t_2$ such that $(p_1, q_1)\in\Omega$, $(p_2, q_2)\in\Omega$, $r=p_1t_1$,

$$s=q_1t_1=p_2t_2 \tag{3}$$

and $v=q_2t_2$. We distinguish three cases.

Case 1: $|q_1| < |p_2|$. Then there exists a $w(\neq e)$ such that $p_2 = q_1 w$ and $t_1 = wt_2$. The condition $(\mathbf{A}_3)$ can be applied (with p_1, q_1, p_2, q_2, w as q_2, p_2, p_1, q_1, r, respectively); it assures $(q_2, p_1 w) \in \Omega$. Thus

$$\varrho(r, v) = \varrho(p_1 t_1, q_2 t_2) = \varrho(p_1 w t_2, q_2 t_2) = \dagger .$$

Case 2: $|q_1| = |p_2|$. Then $q_1 = p_2$ and $t_1 = t_2$. We can apply $(\mathbf{A}_4)$ (with p_1, p_2, q_2 as q_1, p, q_2, resp.); it follows that $p_1 = p't$, $q_2 = q't$, $(p', q') \in \Omega$. Hence

$$\varrho(r, v) = \varrho(p_1 t_1, q_2 t_1) = \varrho(p' t t_1, q' t t_1) = \dagger .$$

Case 3: $|q_1| > |p_2|$. The same inference can be applied as in Case 1 (the roles of q_1 and p_2 are interchanged).

III. Characterization of the right congruences of $F(X)$ by kernel functions

5. The function f (with one variable) is called a *right kernel function* if it satisfies the subsequent five requirements:

(I) The definition domain M of f is a (proper or non-proper) subset of $F^\circ(X)$.

(II) For every $\mu \in F^\circ(X)$, $f(\mu)$ is a non-empty right ideal of $F(X)$.

(III) The empty word e is contained in M and $f(e) = F(X)$.

(IV) $\mu \in M$ implies $\mu^{-1} \in M$ and $f(\mu^{-1}) = f(\mu)$.

(V) If $\mu, \nu \in M$ and $\mu^+ f(\mu) \cap \nu^+ f(\nu)$ is not empty then $\nu^{-1}\mu \in M$ and $\mu^+ f(\mu) \cap \nu^+ f(\nu) \subseteq [\mu, \nu]_r f(\nu^{-1}\mu)$.

In what follows we shall use the notation $\mu^+ f(\mu) \cap \nu^+ f(\nu) = L(\mu, \nu)$.

This concept is a generalization of that of the kernel function introduced by RÉDEI in [1].

For the moment it is not clear that (V) makes sense: the right side of the inclusion seems in general not to be defined. However, we are going to prove that the right side exists if the left one is nonempty.

This follows from Lemma 2 and

Lemma 6. *$L(\mu, \nu) \neq \emptyset$ implies that μ^+ and ν^+ are comparable.*

Proof. Indeed, for $a \in L(\mu, \nu)$ we have $a = \mu^+ t = \nu^+ u$ with $t \in f(\mu)$, $u \in f(\nu)$. Thus $\mu^+ \mid a$ and $\nu^+ \mid a$ hold and, by Lemma 0, this implies the comparability.

On the other hand, the requirement $\nu^{-1}\mu \in M$ in (V) is not so strong as one could think at first sight. Namely, we have

Lemma 7. *Let μ, ν be elements of $F^\circ(X)$. $\nu^{-1}\mu$ belongs to $F^\circ(X)$ if and only if μ^+ and ν^+ are comparable.*

Proof. Let $v^{-1}\mu = v^{-1}(v^+)^{-1}\mu^+(\mu^-)^{-1} \in F^\circ(X)$. Since $r_1(v^+) \neq r_1(v^-)$, $r_1(\mu^+) \neq r_1(\mu^-)$, we have either $(v^{-1}\mu)^+ = v^-$, $(v^{-1}\mu)^- = \mu^-(\mu^+)^{-1}v^+$ and $(\mu^+)^{-1}v^+ \in F(X)$ or $(v^{-1}\mu)^+ = v^-(v^+)^{-1}\mu^+$, $(v^{-1}\mu)^- = \mu^-$ and $(v^+)^{-1}\mu^+ \in F(X)$. In the first case we obtain $\mu^+ \underset{l}{|} v^+$, in the second one $v^+ \underset{l}{|} \mu^+$.

Conversely, let μ^+ and v^+ be comparable. We distinguish two cases.

Case 1: $v^+ \underset{l}{|} \mu^+$. Then $\mu^+ = v^+ m$ $(m \in F(X))$ and

$$v^{-1}\mu = v^-(v^+)^{-1}\mu^+(\mu^-)^{-1} = v^- m(\mu^-)^{-1} \in F^\circ(X). \tag{5}$$

Case 2: $\mu^+ \underset{l}{|} v^+$. By Case 1 we have $\mu^{-1}v \in F^\circ(X)$ and, consequently, $v^{-1}\mu = (\mu^{-1}v)^{-1} \in F^\circ(X)$.

From (5) follows:

Lemma 8. *If* $v^+ \underset{l}{\|} \mu^+$, *then* $(v^{-1}\mu)^- = \mu^-$.

Obviously, (V) can be stated in the equivalent form

(V') If $\mu, v \in M$ then $L(\mu, v) = \mu^+ f(\mu) \cap v^+ f(v) \subseteq \begin{cases} [\mu, v]_r f(v^{-1}\mu) & \text{if } v^{-1}\mu \in M \\ \emptyset & \text{else.} \end{cases}$

As in the commutative case, the significance of right kernel functions is pointed out by the following analogue of Rédei's Fundamental Theorem:

Theorem 3. *Let $\mathscr{C}$ be a right congruence of $F(X)$ and let us define a function f as follows:*

(i) *The domain M of f consists of the elements μ of $F^\circ(X)$ for which there exists a pair (p, q) $(p, q \in F(X))$ such that $\mu = pq^{-1}$ and $p \equiv q \pmod{\mathscr{C}}$.*

(ii) *Whenever μ is an element of M, the set $f(\mu)$ consists of those elements $t\,(\in F(X))$ which satisfy $\mu^+ t \equiv \mu^- t \pmod{\mathscr{C}}$.*

Thus we have defined a one-to-one correspondence between all the right congruences and all the right kernel functions. The converse assignment can be expressed by the following rule: to any right kernel function f, we define a right congruence $\mathscr{C}_f$ such that

(iii) $p \equiv q \pmod{\mathscr{C}_f}$ *if and only if* $pq^{-1} \in M$ *and* $(p, q)_r \in f(pq^{-1})$.

Remark. As it will turn out from the proof, the properties defining the right kernel functions can be assigned to the properties of right congruences by a natural correspondence. Namely, (II) and right compatibility, (III) and reflexivity, (IV) and symmetry, (V) and transitivity correspond to each other (in pairs). In the proof, only the last mentioned correspondence requires much labour.

6. This section is devoted to prove Theorem 3. This amounts to prove the following statements:

(**A**) *Starting with an arbitrary right congruence* $\mathscr{C}$, *the function* f *satisfies the properties* (I)—(V).

(**B**) *If the right congruences* $\mathscr{C}_1, \mathscr{C}_2$ *are different, then the right kernel functions* f_1, f_2 *(assigned to* $\mathscr{C}_1, \mathscr{C}_2$, *respectively) are different, too.*

(**C**) *Starting with an arbitrary right kernel function* f, $\mathscr{C}_f$ *is a right congruence.*

(**D**) f *being a right kernel function, the function obtained from* $\mathscr{C}_f$ *by the rules* (i), (ii) *is equal to* f.

Proof of (A). The requirement (I) follows from (i).

Let $\mu \in M$. Then, by virtue of (i), there exist elements $p, q \in F(X)$ with $p \equiv q \pmod{\mathscr{C}}$, $pq^{-1} = \mu$. In consequence of Lemma 1, $p = \mu^+ t$, $q = \mu^- t$, i.e. there exists an element t for which $\mu^+ t \equiv \mu^- t \pmod{\mathscr{C}}$ and so $f(\mu) \neq \emptyset$. Furthermore, $t \in f(\mu)$ means (by (ii)) $\mu^+ t \equiv \mu^- t \pmod{\mathscr{C}}$ which implies $\mu^+ ts \equiv \mu^- ts \pmod{\mathscr{C}}$ i.e. $ts \in f(\mu)$ for every $s \in f(X)$. Hence $f(\mu)$ is a right ideal. This proves (II).

Since $e \equiv e \pmod{\mathscr{C}}$ holds trivially, (i) assures $e = ee^{-1} \in M$, i.e. the validity of (III).

As we have already remarked, if $\mu \in M$ then $\mu^+ t \equiv \mu^- t \pmod{\mathscr{C}}$ for some $t \in F(X)$. By symmetry of the relation $\mathscr{C}$, $\mu^- t \equiv \mu^+ t \pmod{\mathscr{C}}$ which means $\mu^-(\mu^+)^{-1} \in M$. Thus (IV) holds.

In order to prove (V), let $\mu, \nu \in M$ and suppose $a \in L(\mu, \nu)$. Then, by Lemma 6, μ^+ and ν^+ are comparable and hence, by Lemma 7, $\nu^{-1}\mu \in F(X)$. Let $a = \mu^+ t = \nu^+ u (t \in f(\mu), u \in f(\nu))$. Then

$$\mu^+ t \equiv \mu^- t \pmod{\mathscr{C}}, \qquad \nu^+ u \equiv \nu^- u \pmod{\mathscr{C}},$$

and so

$$\mu^- t \equiv \nu^- u \pmod{\mathscr{C}}. \tag{6}$$

Now there are three possibilities.

a) $\mu^+ \underset{l}{\|} \nu^+$. Then we have $\nu^+ = \mu^+ y$ $(y \in F(X))$, $a = \nu^+ u = \mu^+ yu$ and so $t = yu$. Combining this with (6) and (i), we obtain

$$\mu^- yu \equiv \nu^- u \pmod{\mathscr{C}}, \qquad \nu^-(\mu^- y)^{-1} = \nu^- y^{-1}(\mu^-)^{-1} \in M. \tag{7}$$

On the other hand,

$$\nu^{-1}\mu = \nu^-(\nu^+)^{-1}\mu^+(\mu^-)^{-1} = \nu^- y^{-1}(\mu^+)^{-1}\mu^+(\mu^-)^{-1} = \nu^- y^{-1}(\mu^-)^{-1}$$

and so $\nu^{-1}\mu \in M$. Further, since $\mu^+ \neq \nu^+$, $y \neq e$ and

$$r_1(\mu^- y) = r_1(y) = r_1(\mu^+ y) = r_1(\nu^+) \neq r_1(\nu^-),$$

that is to say, $(v^{-1}\mu)^+ = v^-$, $(v^{-1}\mu)^- = \mu^- y$ and $u \in f(v^{-1}\mu)$ (by (7) and (ii)). But now $[\mu, \nu]_r = v^+$ and we conclude $a = v^+ u \in [\mu, \nu]_r f(v^{-1}\mu)$ or $L(\mu, \nu) \subseteq [\mu, \nu]_r f(v^{-1}\mu)$.

b) $\mu^+ = v^+$. Let $(\mu^-, \nu^-)_r = d$, $\mu^- = md$, $\nu^- = nd$ $(m, n \in F(X))$. Instead of (7) we have now $t = u$ and

$$\mu^- u = mdu \equiv \nu^- u = ndu \pmod{\mathscr{C}}, \quad nm^{-1} \in M. \tag{8}$$

On the other hand,

$$\nu^{-1}\mu = \nu^-(\mu^-)^{-1} = nm^{-1},$$

so that again $\nu^{-1}\mu \in M$. Further, by (8), $(\nu^{-1}\mu)^+ = n$, $(\nu^{-1}\mu)^- = m$ and $du \in f(\nu^{-1}\mu)$. As $[\mu, \nu]_r = \nu^+ d^{-1}$ in our case, we can see that $a = \nu^+ u = \nu^+ d^{-1} du \in [\mu, \nu]_r f(\nu^{-1}\mu)$ which gives again $L(\mu, \nu) \subseteq [\mu, \nu]_r f(\nu^{-1}\mu)$.

c) $\nu^+ \parallel \mu^+$. This case is analogous to a).

Thus (V) is completely proved.

Proof of **(B)**. We prove the assertion indirectly. Suppose that the right kernel functions f_1, f_2 are identical to each other, let this single function be denoted by f, its domain by M. Whenever

$$p \equiv q \pmod{\mathscr{C}_1}$$

then $pq^{-1} \in M$ and

$$(p, q)_r \in f(pq^{-1})$$

(by (i) and (ii), cf. Lemma 1), hence $p \equiv q \pmod{\mathscr{C}_2}$. Since the roles of $\mathscr{C}_1, \mathscr{C}_2$ can be interchanged, $\mathscr{C}_1$ and $\mathscr{C}_2$ coincide.

Proof of **(C)**. Assume that f satisfies (I)—(V); we want to verify that $\mathscr{C}_f$ is reflexive, symmetrical, transitive, and right compatible.

If $p = q$ then $pq^{-1} = e$ and $(p, q)_r = p$. Since the inclusion $p \in f(e)$ is guaranteed by (III), $p \equiv p \pmod{\mathscr{C}_f}$ holds for each $p (\in F(X))$.

The subsequent four assertions are equivalent:

$$p \equiv q \pmod{\mathscr{C}_f},$$

$$pq^{-1} \in M \quad \& \quad (p, q)_r \in f(pq^{-1}),$$

$$qp^{-1} \in M \quad \& \quad (q, p)_r \in f(qp^{-1}),$$

$$q \equiv p \pmod{\mathscr{C}_f}$$

(the equivalence of the first two statements follows from (iii); the same holds for the third and fourth ones; the equivalence of the second and third assertions is implied by (IV) (cf. Lemma 1)), thus $\mathscr{C}_f$ is a symmetrical relation.

In order to prove the transitivity [2]) suppose that

$$p \equiv q \pmod{\mathscr{C}_f} \quad \text{and} \quad p \equiv s \pmod{\mathscr{C}_f}.$$

(iii) imply $\mu = pq^{-1} \in M$, $\nu = ps^{-1} \in M$,

$$t = (p, q)_r \in f(\mu) \quad \text{and} \quad u = (p, s)_r \in f(\nu).$$

Thus, we have $p = \mu^+ t = \nu^+ u \in \mu^+ f(\mu) \cap \nu^+ f(\nu)$ and so $\nu^{-1}\mu \in M$ and $p \in [\mu, \nu]_r f(\nu^{-1}\mu)$ by (V). Suppose $\nu^+ = \mu^+ y$ $(y \in F(X))$ (this can be done without loosing generality). Then $p = \mu^+ yu$ and $t = yu$. It follows

$$p = \mu^+ yu \equiv \mu^- yu = q \pmod{\mathscr{C}_f},$$

$$p = \mu^+ yu = \nu^+ u \equiv \nu^- u = s \pmod{\mathscr{C}_f}.$$

We distinguish two cases.

a) $y \neq e$. Then $[\mu, \nu]_r = \nu^+$ and $u \in f(\nu^{-1}\mu)$ because of $p = \nu^+ u \in [\mu, \nu]_r f(\nu^{-1}\mu)$. On the other hand, $(\nu^{-1}\mu)^+ = (\nu^- y^{-1}(\mu^-)^{-1})^+ = \nu^-$, $(\nu^{-1}\mu)^- = \mu^- y$ and using (iii) we obtain

$$s = \nu^- u \equiv \mu^- yu = q \pmod{\mathscr{C}_f}.$$

b) $y = e$. Then $[\mu, \nu]_r = \nu^+ d^{-1}$, where $d = (\mu^-, \nu^-)_r$ and $p = \nu^+ u \in [\mu, \nu]_r f(\nu^{-1}\mu)$ implies $du \in f(\nu^{-1}\mu)$. It is easy to see, on the other hand, that $(\nu^{-1}\mu)^+ = \nu^- d^{-1}$, $(\nu^{-1}\mu)^- = \mu^- d^{-1}$ and (iii) provides again

$$s = \nu^- u = \nu^- d^{-1} \cdot du \equiv \mu^- d^{-1} \cdot du = q \pmod{\mathscr{C}_f}.$$

This completes the proof of transitivity.

In order to verify $(\mathbf{C}_r)$, suppose $p \equiv q \pmod{\mathscr{C}_f}$. Then $\mu = pq^{-1} \in M$ and $t = (p, q)_r \in f(\mu)$ by (iii). Let z be an arbitrary element of $F(X)$. Then $pz(qz)^{-1} = pq^{-1} \in M$. Moreover, in virtue of (II),

$$(pz, qz)_r = (p, q)_r z \in f(\mu) = f(pz \cdot z^{-1}q^{-1}) = f(pz(qz)^{-1}).$$

Hence $pz \equiv qz \pmod{\mathscr{C}_f}$.

Proof of **(D)**. Let us start with a right kernel function f. Let us denote the function, assigned to $\mathscr{C}_f$ by virtue of (i), (ii), by f'; let the domains of f, f' be denoted by M, M', respectively.

First we shall show $M = M'$. Suppose $\mu \in M'$. There exist two elements p, q of $F(X)$ such that $\mu = pq^{-1}$ and $p \equiv q \pmod{\mathscr{C}_f}$;

[2]) Strictly speaking, we do not prove the original transitivity property but a version of it which is equivalent to transitivity by virtue of symmetry.

hence $\mu = pq^{-1} \in M$ by (iii). Conversely, let $\mu \in M$ and $t \in f(\mu)$. Then

$$\mu^+ t \equiv \mu^- t \pmod{\mathscr{C}_f}$$

(by (iii)), hence (i) implies

$$\mu = \mu^+ t(\mu^- t)^{-1} \in M'.$$

Our last aim is to prove $f(\mu) = f'(\mu)$ for an arbitrary element μ of $M(=M')$. For each $t(\in F(X))$, $t \in f(\mu)$ is equivalent to

$$\mu^+ t \equiv \mu^- t \pmod{\mathscr{C}_f}$$

(by (iii)) and this congruence is equivalent to $t \in f'(\mu)$ (by (ii)).

7. Now we want to generalize some results of RÉDEI concerning kernel functions. For this aim we need some further notions an notations.

Following RÉDEI, we say that the sets $A_1, \ldots, A_k$ form a *set star* if their meet equals the meet of any $k-1$ of them:

$$\bigcap_{i=1}^{k} A_i = \bigcap_{i \neq j} A_i \qquad (j = 1, \ldots, k). \tag{9}$$

The fact that $A_1, \ldots, A_k$ form a set star will be briefly described thus: $(A_1, \ldots, A_k)^*$. Obviously, (9) is equivalent to

$$\bigcap_{\substack{i=1 \\ i \neq j}}^{k} A_i \subseteq A_j \qquad (j = 1, \ldots, k).$$

It is clear as well that for subsets of a left cancellative semigroup S

$$(A_1, \ldots, A_k)^* \Rightarrow (\sigma A_1, \ldots, \sigma A_k)^*$$

holds for any $\sigma \in S$.

Let A, B be subsets of $F(X)$. Denote by $\mathscr{R}(A)$ the maximal right ideal contained in A (it exists if A contains a right ideal at all), and put

$$A \overset{2}{+} B = (A \cup B) \setminus (A \cap B).$$

Now we can prove

Theorem 4. *Having axioms* (I)—(IV) *accepted, axiom* (V′) *is equivalent to either of the following conditions:*

a) *the binary relation defined on* $F(X)$ *by* $(p, q), \in f(pq^{-1})$ *is transitive*;

b$^+$) *if* $\mu, \nu \in M$ *then either* $\mu^+ f(\mu) \cap \nu^+ f(\nu) = \emptyset$ *or* $\nu^{-1}\mu \in M$ *and*

$$(\mu^+ f(\mu), \nu^+ f(\nu), [\mu, \nu], f(\nu^{-1}\mu))^*;$$

o

b$^-$) *if* $\mu, \nu \in M$ *then either* $\mu^- f(\mu) \cap \nu^- f(\nu) = \emptyset$ *or* $\mu\nu^{-1} \in M$ *and*

$$(\mu^- f(\mu),\ \nu^- f(\nu),\ (\mu, \nu)_r^{-1} f(\mu\nu^{-1}))^*;$$

c$^+$) *if* $\mu, \nu \in M$ *then either* $A \cap B = \emptyset$ *or* $\nu^{-1}\mu \in M$ *and*

$$A \cap B \subseteq f(\nu^{-1}\mu) \subseteq \mathscr{R}(F(X) \setminus (A \overset{2}{+} B)),$$

where

$$A = [\mu, \nu]_r^{-1} \mu^+ f(\mu), \quad B = [\mu, \nu]_r^{-1} \nu^+ f(\nu);$$

c$^-$) *if* $\mu, \nu \in M$ *then either* $C \cap D = \emptyset$ *or* $\mu\nu^{-1} \in M$ *and*

$$C \cap D \subseteq f(\mu\nu^{-1}) \subseteq \mathscr{R}(F(X) \setminus (C \overset{2}{+} D)),$$

where

$$C = (\mu, \nu)_r \mu^- f(\mu), \ D = (\mu, \nu)_r \nu^- f(\nu).$$

Proof. (V′) $\Leftrightarrow$ a) has been already stated (end of Section 5) and, as a matter of fact, we proved it in Section 6.

b$^+$)$\Rightarrow$(V) and c$^+$)$\Rightarrow$(V) hold obviously.

Let us prove (V)$\Rightarrow$b$^+$). We have to show only

$$[\mu, \nu]_r f(\nu^{-1}\mu) \cap \nu^+ f(\nu) \subseteq \mu^+ f(\mu) \tag{10}$$

since we get herefrom the second inclusion by interchanging μ and ν (note that $f(\mu^{-1}\nu) = f(\nu^{-1}\mu)$ by (IV)), and the third one coincides with (V). Now apply (V) to $\nu^{-1}\mu$ instead of μ and ν^{-1} instead of ν; then we have

$$(\nu^{-1}\mu)^+ f(\nu^{-1}\mu) \cap \nu^- f(\nu^{-1}) \subseteq [\nu^{-1}\mu, \nu^{-1}]_r f(\mu),$$

and, multiplying by ν,

$$\nu(\nu^{-1}\mu)^+ f(\nu^{-1}\mu) \cap \nu^+ f(\nu^{-1}) \subseteq \nu[\nu^{-1}\mu, \nu^{-1}]_r f(\mu).$$

Thus (10) will be proved if we can ascertain that $\nu(\nu^{-1}\mu)^+ = [\nu, \mu]_r$ and $\nu[\nu^{-1}\mu, \nu^{-1}]_r = \mu^+$.

If $\mu^+ = \nu^+ t$, $t \neq e$, then $\nu^{-1}\mu = \nu^- t (\mu^-)^{-1}$ and

$$\nu(\nu^{-1}\mu)^+ = \nu^+ (\nu^-)^{-1} \nu^- t = \nu^+ t = \mu^+ = [\nu, \mu]_r,$$
$$\nu[\nu^{-1}\mu, \nu^{-1}]_r = \nu\nu^- t = \nu^+ t = \mu^+.$$

If $\nu^+ = \mu^+ t$, $t \neq e$, then $\nu^{-1}\mu = \nu^- t^{-1} (\mu^-)^{-1}$ and $\nu(\nu^{-1}\mu)^+ = \nu^+ = [\nu, \mu]_r$,
$\nu[\nu^{-1}\mu, \nu^{-1}]_r = \nu[\nu^- t^{-1} (\mu^-)^{-1}, \nu^- t^{-1} (\mu^+)^{-1}]_r = \nu\nu^- t^{-1} = \nu^+ t^{-1} = \mu^+$.

If $\mu^+ = \nu^+$, $(\mu^-, \nu^-)_r = t$, $\nu^- = \nu' t$, $\mu^- = \mu' t$, then $\nu^{-1}\mu = \nu' \mu'^{-1}$ and

$$\nu(\nu^{-1}\mu)^+ = \nu\nu' = \nu^+ t^{-1} = [\mu, \nu]_r,$$
$$\nu[\nu^{-1}\mu, \nu^{-1}]_r = \nu[\nu' \mu'^{-1}, \nu' t (\nu^+)^{-1}]_r = \nu\nu' t = \nu^+ = \mu^+$$

and hereby (10) is true in all three cases.

In order to see $b^+) \Leftrightarrow b^-)$ it suffices to replace μ and ν by μ^{-1} and ν^{-1} in $b^+)$ and $b^-)$. Then, in view of (3), they turn into each other.

A similar argument shows the equivalence of $c^+)$ and $c^-)$.

To complete the proof it remains to show $b^+) \Rightarrow c^+)$. The first inclusion of $c^+)$ follows obviously from $b^+)$ (it is a simple transscription of (V)). As for the second one, note that it can be transscribed as

$$f(\nu^{-1}\mu) \cap (A \overset{2}{+} B) = \emptyset. \tag{11}$$

Indeed, (11) means that $f(\nu^{-1}\mu) \subseteq F^\circ(X) \setminus (A \overset{2}{+} B)$. But $f(\nu^{-1}\mu)$ being contained in $F(X)$ and, moreover, being a right ideal of it, the obtained inclusion gives already $f(\nu^{-1}\mu) \subseteq \mathscr{R}(F(X) \setminus (A \overset{2}{+} B))$. On the other hand, (10) shows that

$$[\mu, \nu]_r f(\nu^{-1}\mu) \cap \nu^+ f(\nu) \subseteq \mu^+ f(\mu) \cap \nu^+ f(\nu)$$

or, multiplying by $[\mu, \nu]_r^{-1}$,

$$f(\nu^{-1}\mu) \cap B \subseteq A \cap B.$$

Similarly,

$$f(\nu^{-1}\mu) \cap A \subseteq A \cap B.$$

The two latter formulas together give (11).

Thus, we have proved Theorem 4. The graph of the equivalency proof was

$$\text{(V)} \quad \begin{array}{l} \nearrow b^+ \leftrightarrow b^- \\ \downarrow \\ \searrow c^+ \leftrightarrow c^- \end{array}$$

We remark that c^+ and c^- are concerned with subsets of $F^\circ(X)$ and not necessarily of $F(X)$.

As an analogue to Theorem 5 of RÉDEI [1], we prove

Theorem 5. *For elements $\mu_1, \ldots, \mu_k$ $(k \geqq 2)$ of the domain M of a right kernel function f, satisfying*

$$\mu_1 \ldots \mu_k = e, \quad \coprod_{s=0}^{l-1} \mu_{i+s} \in F^\circ(X) \qquad (i, l = 1, \ldots, k;\ i+s \bmod k), \tag{12}$$

we have

$$(\mu_1^+ f(\mu_1), \mu_1 \mu_2^+ f(\mu_2), \ldots, \mu_1 \ldots \mu_{k-1} \mu_k^+ f(\mu_k))^*. \tag{13}$$

Following RÉDEI, we call (13) the *star property of right kernel functions.*

Proof. First one can see that condition (12), if satisfied for $\mu_1, \ldots, \mu_k$, holds for $\mu_2, \ldots, \mu_k, \mu_1$, too. Further, the sets $\mu_2^+ f(\mu_2), \ldots, \mu_2 \ldots \mu_{k-1} \mu_k^+ f(\mu_k), \mu_2 \ldots \mu_k \mu_1^+ f(\mu_1)$ can be obtained from those comprised in (13) by a left multiplication by μ_1^{-1}. This

is obvious for the first $k-1$ of them; for the last set it follows from the fact that $\mu_2 \dots \mu_k \mu_1 = e$ and hence

$$\mu_2 \dots \mu_k \mu_1^+ = \mu_1^- = \mu_1^{-1} \mu_1^+.$$

Thus a cyclic permutation of $\mu_1, \dots, \mu_k$ carries (13) over into an equivalent statement and therefore it suffices to prove

$$\bigcap_{i=1}^{k-1} \mu_1 \dots \mu_{i-1} \mu_i^+ f(\mu_i) \subseteq \mu_1 \dots \mu_{k-1} \mu_k^+ f(\mu_k). \tag{14}$$

In order to do this, we remark that

$$\mu^+ f(\mu) \cap \mu \nu^+ f(\nu) \subseteq (\mu\nu)^+ f(\mu\nu) \quad \text{for} \quad \mu, \nu \in M, \ \mu^- \text{ and } \nu^+ \text{ comparable.} \tag{15}$$

This is a consequence of (V) applied to μ^{-1}, ν and of the identity

$$(\mu\nu)^+ = \mu[\mu^{-1}, \nu]_r$$

already used in the proof of the foregoing theorem. (15) makes it possible to prove by induction

$$\mu_1^+ f(\mu_1) \cap \mu_1 \mu_2^+ f(\mu_2) \cap \dots \cap \mu_1 \dots \mu_{j-1} \mu_j^+ f(\mu_j) \subseteq (\mu_1 \dots \mu_j)^+ f(\mu_1 \dots \mu_j). \tag{16}$$

Indeed, for $j=2$ (16) coincides with (15) applied to the case $\mu = \mu_1$, $\nu = \mu_2$. Now if (16) holds for some j $(1 < j < k)$ then, using (15) for $\mu = \mu_1 \dots \mu_j$, $\nu = \mu_{j+1}$, we have

$$\mu_1^+ f(\mu_1) \cap \mu_1 \mu_2^+ f(\mu_2) \cap \dots \cap \mu_1 \dots \mu_j \mu_{j+1}^+ f(\mu_{j+1}) \subseteq$$
$$\subseteq (\mu_1 \dots \mu_j)^+ f(\mu_1 \dots \mu_j) \cap \mu_1 \dots \mu_j \mu_{j+1}^+ f(\mu_{j+1}) \subseteq (\mu_1 \dots \mu_{j+1})^+ f(\mu_1 \dots \mu_{j+1}).$$

Put $j = k-1$ in (16). Then the left hand sides of (14) and (16) are equal. But $\mu_1 \dots \mu_{k-1} = \mu_k^{-1}$, $(\mu_1 \dots \mu_{k-1})^+ = \mu_k^- = \mu_1 \dots \mu_{k-1} \mu_k^+$ and so the right hand sides of both inclusions coincide, too. This proves (14) and thereby Theorem 5.

RÉDEI's First Reciprocity Theorem reads in the non-commutative case as follows:

Theorem 6. *Let* $\mathfrak{m}, \mathfrak{n}$ *be right ideals of* $F(X), \mu, \nu \in F^\circ(X)$ *and*

$$\hat{\xi} = \begin{cases} \mathfrak{m} & \text{if} \quad \xi = \mu, \mu^{-1}, \\ \mathfrak{n} & \text{if} \quad \xi = \nu, \nu^{-1}, \end{cases} \tag{16}$$

$$\hat{\xi} = F(X) \quad \text{for} \quad \xi = e.$$

The existence of a right kernel function f *satisfying* $f(\mu) = \mathfrak{m}, f(\nu) = \mathfrak{n}$ *is equivalent to the condition*

$$(\mu_1^+ \hat{\mu}_1, \mu_1 \mu_2^+ \hat{\mu}_2, \dots, \mu_1 \dots \mu_{k-1} \mu_k^+ \hat{\mu}_k)^* \quad (k \geqq 3) \tag{17}$$

for any system $\mu_1, \ldots, \mu_k$ *which satisfies*

$$\mu_i = \mu, \mu^{-1}, \nu, \nu^{-1}; \quad \mu_1 \ldots \mu_k = e; \quad \prod_{s=0}^{l-1} \mu_{i+s} \in F(X) \tag{18}$$

$$(i, l = 1, \ldots, k; \ i+s \bmod k).$$

If the function f mentioned in the theorem exists, we shall say that the pairs $(\mu, \mathfrak{m})$ and $(\nu, \mathfrak{n})$ are *compatible*.

Proof. If $(\mu, \mathfrak{m})$ and $(\nu, \mathfrak{n})$ are compatible then (17) follows from Theorem 5.

Now let (17) be fulfilled for any system satisfying (18). Let us define a right kernel function f as follows. For the domain of f we take $M \subseteq H = F^{\circ}(X) \cap \langle \mu, \nu \rangle$, where $\langle \mu, \nu \rangle$ denotes the subgroup of $G(X)$ generated by μ and ν, and M consists of those elements α of H for which there exist $\mu_1, \ldots \mu_t$ $(\mu_i = \mu, \mu^{-1}, \nu, \nu^{-1}; i = 1, \ldots, t)$ such that

$$\alpha = \mu_1 \ldots \mu_t, \tag{19}$$

$$D = D(\mu_1, \ldots, \mu_t) = \bigcap_{i=1}^{t} (\alpha^+)^{-1} \mu_1 \ldots \mu_{i-1} \mu_i^+ \hat{\mu}_i \neq \emptyset. \tag{20}$$

Further, put $f(e) = F(X)$, $f(\alpha) = \bigcup_{\mu_1 \ldots \mu_t = \alpha} D(\mu_1, \ldots, \mu_t)$ for $\alpha \neq e$, where $(\mu_1, \ldots, \mu_t)$ ranges over all systems satisfying (19). We are going to show that f is a right kernel function.

Axioms (I) and (III) hold trivially.

In order to see (II), we have only to show that $f(\alpha) \subseteq F(X)$. But

$$D \subseteq (\alpha^+)^{-1} \mu_1^+ \hat{\mu}_1 \cap (\alpha^+)^{-1} \mu_1 \ldots \mu_{t-1} \mu_t^+ \hat{\mu}_t \subseteq (\alpha^+)^{-1} \mu_1^+ F(X) \cap (\alpha^+)^{-1} \alpha \mu_t^- F(X) =$$

$$= (\alpha^+)^{-1} \mu_1^+ F(X) \cap (\alpha^-)^{-1} \mu_t^- F(X) \subseteq (\alpha^+)^{-1} F(X) \cap (\alpha^-)^{-1} F(X) \subseteq F(X)$$

which proves also $f(\alpha) \subseteq F(X)$.

Since

$$\left((\alpha^+)^{-1} \mu_1 \ldots \mu_{i-1} \mu_i^+\right)\left((\mu_i^-)^{-1} \mu_{i+1} \ldots \mu_t \alpha^-\right) = (\alpha^+)^{-1} \alpha \alpha^- = e,$$

we have

$$(\alpha^+)^{-1} \mu_1 \ldots \mu_{i-1} \mu_i^+ = (\alpha^-)^{-1} \mu_t^{-1} \ldots \mu_{i+1}^{-1} \mu_i^-.$$

Hence (in view of (16))

$$D(\mu_t^{-1}, \ldots, \mu_1^{-1}) = \bigcap_{i=t}^{1} (\alpha^-)^{-1} \mu_t^{-1} \ldots \mu_{i+1}^{-1} \mu_i^- (\mu_i^{-1})^{\wedge} = D(\mu_1, \ldots, \mu_t)$$

and thus $f(\alpha^{-1}) = f(\alpha)$.

Finally, let

$$\beta = \beta_1 \ldots \beta_n \in M, \quad \alpha^+ f(\alpha) \cap \beta^+ f(\beta) \neq \emptyset \quad (\beta_i = \mu, \mu^{-1}, \nu, \nu^{-1}; \ i = 1, \ldots, n).$$

Then $\alpha^{-1}\beta \in H$ by Lemma 7 and

$$D(\mu_t^{-1}, \dots, \mu_1^{-1}, \beta_1, \dots, \beta_n) =$$

$$= \left(\left(\bigcap_{i=t}^{1} ((\alpha^{-1}\beta)^+)^{-1}\mu_t^{-1} \dots \mu_{i+1}^{-1}\mu_i^+(\mu_i^{-1})\hat{}\right) \cap \right.$$

$$\left. \cap \left(\bigcap_{j=1}^{n} ((\alpha^{-1}\beta)^+)^{-1}\mu_t^{-1} \dots \mu_1^{-1}\beta_1 \dots \beta_{j-1}\beta_j^+\hat{\beta}_j\right)\right) =$$

$$= [\alpha, \beta]_r^{-1}\left(\alpha \bigcap_{i=t}^{1} \mu_t^{-1} \dots \mu_{i+1}^{-1}\mu_i^+(\mu_i^{-1})\hat{}\right) \cap [\alpha, \beta]_r^{-1}\left(\bigcap_{j=1}^{n} \beta_1 \dots \beta_{j-1}\beta_j^+\hat{\beta}_j\right) =$$

$$= [\alpha, \beta]_r^{-1}(\alpha^+ D(\mu_t^{-1}, \dots, \mu_1^{-1}) \cap \beta^+ D(\beta_1, \dots, \beta_n)).$$

Now, since $\alpha^+ f(\alpha) \cap \beta^+ f(\beta)$ is a union of sets analogous to that in the last parenthesis, at least one of these sets must be nonempty and therefore $\alpha^{-1}\beta \in M$. Further,

$$\alpha^+ f(\alpha) \cap \beta^+ f(\beta) = \alpha^+ f(\alpha^{-1}) \cap \beta^+ f(\beta) = \left(\alpha^+ \bigcup_{\mu_t^{-1}\dots\mu_1^{-1}=\alpha^{-1}} D(\mu_t^{-}, \dots, \mu_1^{-1})\right) \cap$$

$$\cap \left(\beta^+ \bigcup_{\beta_1\dots\beta_n=\beta} D(\beta_1, \dots, \beta_n)\right) = \bigcup_{\substack{\mu_t^{-1}\dots\mu_1^{-1}=\alpha^{-1}, \\ \beta_1\dots\beta_n=\beta}} (\alpha^+ D(\mu_t^{-1}, \dots, \mu_1^{-1}) \cap \beta^+ D(\beta_1, \dots, \beta_n)) =$$

$$= \bigcup_{\substack{\mu_t^{-1}\dots\mu_1^{-1}=\alpha^{-1}, \\ \beta_1\dots\beta_n=\beta}} [\alpha, \beta]_r D(\mu_t^{-1}, \dots, \mu_1^{-1}, \beta_1, \dots, \beta_n) \subseteq [\alpha, \beta]_r f(\alpha^{-1}\beta).$$

Thus (V) is proved, too.

We have shown till now that f is a right kernel function. It remains to check whether $f(\mu) = \mathfrak{m}$, $f(\nu) = \mathfrak{n}$ are true. Now, on one hand, it is easy to see that $\mathfrak{m} \subseteq f(\mu)$ since $D(\mu_1) = \mathfrak{m}$ for $\mu_1 = \mu$. On the other hand, put $\alpha = \mu$ in (19) and (20). Adjoin one more element $\mu_{t+1} = \mu^{-1}$ to the system $\mu_1, \dots, \mu_t$. Then, for the system $\mu_1, \dots, \mu_{t+1}$ and the right kernel function f, the conditions of Theorem 5 are fulfilled so that (13) holds with $k = t+1$. In particular,

$$\bigcap_{i=1}^{t} \mu_1 \dots \mu_{i-1}\mu_i^+\hat{\mu}_i \subseteq \mu_1 \dots \mu_t\mu_{t+1}^+\hat{\mu}_{t+1} = \mu^+\mathfrak{m},$$

or

$$\bigcap_{i=1}^{t} (\mu^+)^{-1}\mu_1 \dots \mu_{i-1}\mu_i^+\hat{\mu}_i = D(\mu_1, \dots, \mu_t) \subseteq \mathfrak{m},$$

and hence $f(\mu) \subseteq \mathfrak{m}$.

The equality $f(\nu) = \mathfrak{n}$ can be treated analogously. Thus, Theorem 6 is proved.

RÉDEI's other results can hardly be carried over to our case since they are mostly based on the fact that the ideals of the free commutative semigroups of

finite rank are finitely generated. However, it might be of some interest to have some information about right kernel functions pertaining to two-sided congruences, and this question gives rise to investigations having no correspondent in the commutative case.

IV. Two-sided congruences

8. It is easy to find the analogues of the concepts and results in Chapter II for the two-sided case. Indeed, the only thing we have to do is to replace $(\mathbf{A}_2)$ and $(\mathbf{A}_3)$ by the conditions

$(\mathbf{A}_2^*)$ $(p, q)\in\Omega$ and $(spt, sqt)\in\Omega$ imply $s=t=e$;

$(\mathbf{A}_3^*)$ Whenever $(p_1, q_1)\in\Omega$, $(p_2, q_2)\in\Omega$ and $s_1p_1t_1=s_2p_2t_2$ then there exist elements q_1', q_2', u, v such that $q_1=uq_1'v$, $q_2=uq_2'v$ and $(q_1', q_2')\in\Omega$.

It would even suffice to require $(\mathbf{A}_3^*)$ for both cases $s_2=t_1=e$ and $s_2=t_2=e$. The proofs are essentially the same as in Chapter II.

As for kernel functions, we have

Theorem 7. *The right congruence $\mathscr{C}_f$ defined by the right kernel function f is a two-sided one if and only if*

(VI) *for any $\mu\in M$, $p\in F(X)$ holds: $f(p\mu p^{-1})\in M$ and $(p\mu^+, p\mu^-)_r f(\mu)\subseteq f(p\mu p^{-1})$.*

A right kernel function f satisfying (VI) will be called an *R-function.*

Proof. Let $\mathscr{C}_f$ be a two-sided congruence, $\mu\in M$, $p\in F(X)$, $t\in f(\mu)$. Then $\mu^+t\equiv\mu^-t \pmod{\mathscr{C}_f}$ and, consequently, $p\mu^+t\equiv p\mu^-t \pmod{\mathscr{C}_f}$. Suppose $(p\mu^+, p\mu^-)_r=d$, $p\mu^+=ad$, $p\mu^-=bd$. Then, obviously, $a=(p\mu p^{-1})^+$, $b=(p\mu p^{-1})^-$ and $adt\equiv bdt \pmod{\mathscr{C}_f}$. This means that $dt\in f(p\mu p^{-1})$ and this proves (VI).

Conversely, let (VI) hold and let $q\equiv s \pmod{\mathscr{C}_f}$. Take an arbitrary $p\in F(X)$ and denote $qs^{-1}=\mu$. Then $q=\mu^+t$, $s=\mu^-t$, $t\in f(\mu)$ and by (VI)

$$(p\mu^+, p\mu^-)_r t\in f(p\mu p^{-1}). \tag{21}$$

But

$$(p\mu^+, p\mu^-)_r t=(p\mu^+t, p\mu^-t)_r=(pq, ps)_r. \tag{22}$$

Using the notation $(pq, ps)_r=d$, $pq=ad$, $ps=bd$ one can see that $a=(pqs^{-1}p^{-1})^+=(p\mu p^{-1})^+$, $b=(p\mu p^{-1})^-$ and, in view of (21) and (22), $ad\in(p\mu p^{-1})^+f(p\mu p^{-1})$, $bd\in(p\mu p^{-1})^-f(p\mu p^{-1})$, so that

$$pq=ad\equiv bd=ps \pmod{\mathscr{C}_f}.$$

Thus, $\mathscr{C}_f$ is a left congruence too, and the proof is complete.

It is worth while to point out some special cases of Theorem 7.

Corollary 1. *Let f be an R-function. If $\mu\notin M\setminus(F(X)\cup F(X)^{-1})$ then $f(\mu)\subseteq f(p\mu p^{-1})$ for every $p\in F(X)$.*

Indeed, if $\mu \notin F(X) \cup F(X)^{-1}$ then $(p\mu^+, p\mu^-)_r = (\mu^+, \mu^-)_r = e$.

Corollary 2. *Let f be an R-function. Then $pf(qp) \subseteq f(pq)$ for any $p, q \in F(X)$. Especially, $pf(p) \subseteq f(p)$ for $p \in M \cap F(X)$.*

Put $\mu = qp$ in (VI).

The concepts dual to right kernel functions and R-functions will be called left kernel functions and L-functions. Obviously, all results obtained in our paper can be dualized. In consequence of Theorem 3 and its dual, there is a one-to-one correspondence between R- and L-functions such that the corresponding pairs pertain to the same congruence. If the R-function f and the L-function g define the same congruence, we shall say they are conjugate and we use the notation $g = \bar{f}, f = \bar{g}$. Further, denote the domain of a function h by M_h.

Theorem 8. *The conjugate $\bar{f}$ of the R-function f is determined by the equalities*

$$M_{\bar{f}} = \{(\mu^- s)^{-1} \mu (\mu^- s) \mid \mu \in M_f, s \in f(\mu)\}, \tag{23}$$

$$\bar{f}(\bar{\mu}) = \{t \mid (t\bar{\mu}_-)\bar{\mu}(t\bar{\mu}_-)^{-1} \in M_f, (t\bar{\mu}_+, t\bar{\mu}_-)_r \in f((t\bar{\mu}_-)\bar{\mu}(t\bar{\mu}_-)^{-1})\} \quad \text{for} \quad \bar{\mu} \in M_{\bar{f}}, \tag{24}$$

where $\bar{\mu}_+ = [\bar{\mu}, e]_l$, $\bar{\mu}_- = (\bar{\mu}, e)_l^{-1}$.

Indeed, if $\mathscr{C}$ is the congruence defined by f (and $\bar{f}$) then $\mu \in M_f$, $s \in f(\mu)$ implies

$$\mu^+ s \equiv \mu^- s \pmod{\mathscr{C}}$$

or, by the dual of Theorem 3,

$$(\mu^- s)^{-1} \mu^+ s = (\mu^- s)^{-1} \mu (\mu^- s) \in M_{\bar{f}}.$$

Conversely, if $\bar{\mu} \in M_{\bar{f}}$, $t \in \bar{f}(\bar{\mu})$ then

$$t\bar{\mu}_+ \equiv t\bar{\mu}_- \pmod{\mathscr{C}}.$$

Put $\mu = (t\bar{\mu}_+)(t\bar{\mu}_-)^{-1} = (t\bar{\mu}_-)\bar{\mu}(t\bar{\mu}_-)^{-1}$, $s = (t\bar{\mu}_+, t\bar{\mu}_-)_r$. We have $\mu \in M_f$, $s \in f(\mu)$ and $t\bar{\mu}_+ = \mu^+ s$, $t\bar{\mu}_- = \mu^- s$. Hence

$$\bar{\mu} = (t\bar{\mu}_-)^{-1}(t\bar{\mu}_+) = (\mu^- s)^{-1} \mu^+ s = (\mu^- s)^{-1} \mu (\mu^- s).$$

Finally, if $\bar{\mu} \in M_{\bar{f}}$ and $\mu = (t\bar{\mu}_-)\bar{\mu}(t\bar{\mu}_-)^{-1} \in M_f$, $s = (t\bar{\mu}_+, t\bar{\mu}_-)_r \in f((t\bar{\mu})\bar{\mu}(t\bar{\mu})^{-1})$ for some t then

$$t\bar{\mu}_+ = \mu^+ s \equiv \mu^- s = t\bar{\mu}_- \pmod{\mathscr{C}},$$

so that $t \in \bar{f}(\bar{\mu})$. This completes the proof of Theorem 8.

Reference

[1] L. RÉDEI, *Theorie der endlich erzeugbaren kommutativen Halbgruppen* (Leipzig—Budapest, 1963).

(Received March 20, 1970)