

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

ROGER DESQ

Éléments inversibles dans un demi-groupe D

Séminaire Dubreil. Algèbre et théorie des nombres, tome 16, n° 1 (1962-1963), exp. n° 4, p. 1-16

http://www.numdam.org/item?id=SD_1962-1963__16_1_A4_0

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1962-1963, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

26 novembre 1962

ÉLÉMENTS INVERSIBLES DANS UN DEMI-GROUPE D

par Roger DESQ

[d'après E. S. LJAPIN (*)]

1. D demi-groupe quelconque.

DÉFINITION 1.1. - Un élément a d'un demi-groupe D est dit inversible à droite si $aD = D$; bilatèremment inversible (noté b -inversible) s'il est inversible à gauche et à droite.

THÉOREME 1.1. - Si l'ensemble G de tous les éléments b -inversibles n'est pas vide, c'est un groupe dont l'élément unité est unité pour tout le demi-groupe.

G est un sous-demi-groupe. Soient a et $b \in G$; il existe x, y avec $xb = a$, $by = a$.

$xD = xbd = ad = D$; x est inversible à droite, de même y est inversible à gauche.

Il existe i, c_1, c_2 avec $bi = b$; $c_1 a = i$; $bc_2 = i$; pour tout z , il existe z' avec $z = z' b$.

D'où : $zi = z' bi = z' b = z$, i est élément unité à droite de D .

$$z = zi = zbc_2 = zbic_2 = zbc_1 ac_2 = zbc_1 xbc_2 = (zbc_1) x$$

donc x est inversible à gauche et $x \in G$. De même $y \in G$, G vérifiant l'axiome des quotients est donc un groupe.

Soit e l'élément unité de G , $eD = D$, $De = D$, e est bien élément unité du demi-groupe D .

COROLLAIRE 1.1. - Pour que D ait des éléments b -inversibles, il faut et il suffit que D contienne un élément unité.

Soient $R = \{\text{éléments inversibles à droite et non inversibles à gauche}\}$.

$L = \{\text{éléments inversibles à gauche et non inversibles à droite}\}$.

$A = \{\text{éléments inversibles ni à droite, ni à gauche}\}$.

THÉOREME 1.2. - Pour un demi-groupe quelconque D nous avons la table de multiplication suivante

(*) [2], chapitre III, § 5 ; chapitre VI, § 1, 2 ; chapitre IX, § 4.

	G	R	L	Λ
G	G	R	L	Λ
R	R	R	D	$R + \Lambda$
L	L	Λ	L	Λ
Λ	Λ	Λ	$L + \Lambda$	Λ

(signifie que si G, L , par exemple, sont $\neq \emptyset$, on a $GL \subseteq L$).

Il y a seize cas à vérifier. Cette vérification est simplifiée si l'on remarque que :

$R + \Lambda = \{\text{éléments non inversibles à gauche}\}$, est un idéal à gauche.

$R + G = \{\text{éléments inversibles à droite}\}$, est un sous-demi-groupe.

Considérons par exemple $G\Lambda$.

$G\Lambda \subseteq R + \Lambda$ qui est un idéal à gauche.

Supposons qu'il existe $g \in G$, $a \in \Lambda$ avec $ga = r \in R$.

$gaD = rD = D$, $g \in G$, $\exists g' \in G$ avec $g'g = e$, $g'D = D$

$g'gaD = g'D \implies aD = D$ impossible.

Dans certaines cases du tableau précédent, il y a une somme de plusieurs éléments, montrons que le nombre de ces termes ne peut être diminué.

Soient Ω l'ensemble des entiers naturels $\mathcal{G}_\Omega$ l'ensemble des applications de Ω dans lui-même. Prenons, dans $\mathcal{G}_\Omega$,

e = application identique,

$$r_1 = \begin{pmatrix} 1, 2, 3, \dots, n, \dots \\ 1, 1, 2, \dots, n-1, \dots \end{pmatrix} \quad r_2 = \begin{pmatrix} 1, 2, 3, 4, \dots, n, \dots \\ 1, 1, 1, 2, \dots, n-2, \dots \end{pmatrix}$$

$$r_3 = \begin{pmatrix} 1, 2, 3, 4, \dots, n, \dots \\ 1, 2, 2, 3, \dots, n-1, \dots \end{pmatrix}$$

$$\ell_1 = \begin{pmatrix} 1, 2, 3, 4, \dots, n, \dots \\ 2, 3, 4, 5, \dots, n+1, \dots \end{pmatrix} \quad \ell_2 = \begin{pmatrix} 1, 2, 3, 4, \dots, n, \dots \\ 3, 4, 5, 6, \dots, n+2, \dots \end{pmatrix}$$

$$a_1 = \begin{pmatrix} 1, 2, 3, 4, \dots, n, \dots \\ 2, 2, 3, 4, \dots, n, \dots \end{pmatrix} \quad a_2 = \begin{pmatrix} 1, 2, 3, 4, \dots, n, \dots \\ 1, 1, 1, 1, \dots, 1, \dots \end{pmatrix}$$

les r_i étant surjectives divisent e à gauche, mais pas à droite, car ces applications ne sont pas injectives.

On voit de même que $r_i \in R$ ($i = 1, 2, 3$); $\ell_i \in L$ ($i = 1, 2$); $a_i \in \Lambda$ ($i = 1, 2$).

$$RL : r_1 \ell_1 = e \in G ,$$

$$r_2 \ell_1 = r_1 \in R ,$$

$$r_3 \ell_2 = \ell_1 \in L , \quad r_3 \ell_1 = a_1 \in \Lambda .$$

$$RA : r_1 a_1 = r_1 \in R ; \quad r_1 a_2 = a_2 \in \Lambda .$$

$$AL : a_1 \ell_1 = \ell_1 \in L ; \quad a_2 \ell_1 = a_2 \in \Lambda .$$

Cet exemple montre qu'en général la décomposition $D = G + R + L + \Lambda$ n'est pas une "sviaska" c'est-à-dire une bande (CLIFFORD).

Nous allons maintenant considérer les éléments inversibles particuliers que sont les éléments grossissants.

DÉFINITION 1.2. - Un élément g de D est dit grossissant à droite s'il existe un complexe $D' \subset D$, $D' \neq D$ tel que $D' g = D$.

THÉOREME 1.3. - Tout élément grossissant à droite est inversible à gauche, mais non inversible à droite.

$Dg \supseteq D' g = D \implies g$ inversible à gauche. Si g était de plus inversible à droite, g appartiendrait à G , il existerait g' avec $gg' = g'g = e$.

$D' = D' e = D' gg' = Dg' \supseteq Dgg' = De = D$; ce qui contredit la définition.

COROLLAIRE 1.2.

a. Aucun élément d'un demi-groupe ne peut être à la fois grossissant à gauche et grossissant à droite.

b. Un demi-groupe commutatif n'a pas d'éléments grossissants.

Soient $D^{(r)} = \{\text{éléments grossissants à droite}\};$

$D^{(\ell)} = \{\text{éléments grossissants à gauche}\};$

$D^{(n)} = D \setminus (D^{(r)} \cup D^{(\ell)})$.

THÉOREME 1.4. - $D^{(r)}$ et $D \setminus D^{(r)}$ sont des sous-demi-groupes de D . $D^{(r)}$ est un demi-groupe sans torsion.

Soient $g_1 \in D^{(r)}$; $g_2 \in G + L$, c'est-à-dire g_2 inversible à gauche; il existe $D' \subset D$, $D' g_1 = D$

$$D'(g_1 g_2) = D' g_1 g_2 = Dg_2 = D .$$

$D^{(r)}$ est un idéal à droite dans $G + L = \{\text{éléments inversibles à gauche}\}$.

Soient $a_1, a_2 \in D \setminus D^{(r)}$; s'il existait $D' \subset D$ avec $D' a_1 a_2 = D$ on aurait $D' a_1 \neq D$, car a_1 n'est pas grossissant à droite ; mais alors a_2 serait grossissant à droite.

Soit $g \in D^{(r)}$ avec $g^n = f$ élément idempotent.

$D = Dg = \dots = Dg^n = Df \Rightarrow f$ élément unité à droite.

Soit $D' \neq D$, $D' g = D$; $D' g^n = Dg^{n-1} = D$, mais $D' f = D'$, d'où $D' = D$.

COROLLAIRE 1.3. - Un demi-groupe périodique ne contient pas d'éléments grossissants.

THÉOREME 1.5. - $D = D^{(r)} + D^{(\ell)} + D^{(n)}$.

α . $D^{(r)}$ est un demi-groupe qui ne contient pas d'élément inversible à droite.

β . $D^{(\ell)}$ est un demi-groupe qui ne contient pas d'élément inversible à gauche.

γ . Si D a un élément unité, $D^{(n)}$ est non vide et c'est un demi-groupe qui ne contient pas d'éléments grossissants.

α . Soit x un élément de $D^{(r)}$ inversible à droite dans $D^{(r)}$. Il existe $z \in D^{(r)}$ avec $xz = x$.

$\exists D' \subset D$, $D' z = D$; $\forall a \in D$, $\exists b$ avec $bx = a$

$az = bxz = bx = a$; z est donc élément unité à droite de D , mais alors $D' = D$ (contradiction).

γ . $e \in D^{(n)} \Rightarrow D^{(n)} \neq \emptyset$.

Soit $x \in D^{(n)}$ tel qu'il existe $D' \subset D^{(n)}$ avec $D' x = D^{(n)}$.

$e \in D^{(n)} \Rightarrow \exists y$ avec $yx = e$; $(Dy) x = De = D$.

Comme $x \in D^{(n)}$, $Dy = D$.

$\exists z$ avec $zy = e$; $x = ex = zyx = ze = z$; $xy = e$.

$D' = D' e = D' xy = D^{(n)}$ $y \in D^{(n)}$ $xy = D^{(n)}$ $e \in D^{(n)}$.

2. D contient un élément unité.

Construction du demi-groupe bicyclique $\mathcal{B}$. - Soient $\mathcal{B} = \{[a, b]\}$, $a, b = 0, 1, 2, \dots, n, \dots$ et h la fonction définie par

$$h(x) = x \text{ si } x \geq 0 ; h(x) = 0 \text{ si } x < 0 .$$

Définissons dans $\mathcal{B}$ l'opération suivante :

$$[a_1, b_1][a_2, b_2] = [a_1 + h(a_2 - b_1) ; b_2 + h(b_1 - a_2)] .$$

$$\begin{aligned}
([a_1, b_1][a_2, b_2])[a_3, b_3] &= [a_1 + h(a_2 - b_1) ; b_2 + h(b_1 - a_2)][a_3, b_3] \\
&= [a_1 + h(a_2 - b_1) + h\{a_3 - b_2 - h(b_1 - a_2)\} ; b_3 + h\{b_2 + h(b_1 - a_2) - a_3\}] \\
[a_1, b_1]([a_2, b_2][a_3, b_3]) &= [a_1, b_1][a_2 + h(a_3 - b_2) ; b_3 + h(b_2 - a_3)] \\
&= [a_1 + h\{a_2 + h(a_3 - b_2) - b_1\} ; b_3 + h(b_2 - a_3) + h\{b_1 - a_2 - h(a_3 - b_2)\}] .
\end{aligned}$$

Il y a quatre cas à envisager

$$\begin{array}{cccc}
(1) & a_2 \geq b_1 & (2) & a_2 \geq b_1 \\
& a_3 \geq b_2 & & a_3 < b_2 \\
(3) & a_2 < b_1 & (4) & a_2 < b_1 \\
& a_3 \geq b_2 & & a_3 < b_2
\end{array}$$

On vérifie l'associativité en remarquant que $h(h(x)) = h(x)$ et
 $h(x + y) = h(x) + h(y)$ si x et $y \geq 0$,

Nous avons

$$\begin{aligned}
[a, b] &= [a, 0][0, b] = \\
[a, 0] &= [1, 0]^a \quad [0, b] = [0, 1]^b \\
[a, b][0, 0] &= [0, 0][a, b] \quad [0, 1][1, 0] = [0, 0] .
\end{aligned}$$

En posant $u = [1, 0]$; $v = [0, 1]$; $e = [0, 0]$.

$\mathcal{B}$ est engendré par u, v avec comme relations

$$vu = e ; eu = ue = u ; ev = ve = v$$

ce qui permet de poser $u^0 = v^0 = e$.

Les éléments de $\mathcal{B}$ s'écrivent $u^\alpha v^\beta$ avec $\alpha \geq 0, \beta \geq 0$. D'après l'identification que nous venons de faire, ceci est la forme canonique des mots de $\mathcal{B}$.

$$u^\alpha v^\beta u^{\alpha'} v^{\beta'} = \begin{cases} u^{\alpha+\alpha'-\beta} v^{\beta'} & \text{si } \alpha' \geq \beta \\ u^\alpha v^{\beta-\alpha'+\beta'} & \text{si } \alpha' < \beta \end{cases}$$

Remarque. - On aurait pu poser $\mathcal{B} = \{u, v\}$ avec $vu = e ; eu = ue = u ; ev = ve = v$. Les éléments de $\mathcal{B}$ étant des produits en u et v se mettent évidemment sous la forme $u^\alpha v^\beta$; mais on ne sait pas si cette forme est unique.

Dans $\mathcal{B}$ les éléments u^α ($\alpha > 0$) sont grossissants à droite, car
 $(\mathcal{B}v^\alpha) u^\alpha = \mathcal{B}v^\alpha u^\alpha = \mathcal{B}e = \mathcal{B}$.

$\mathcal{B}v^\alpha \neq \mathcal{B}$; en effet $\mathcal{B}v^\alpha$ ne contient que les éléments $u^\gamma v^{\alpha+\delta}$ $\delta \geq 0$.

Les éléments v^α ($\alpha > 0$) sont grossissants à gauche. Les autres éléments ne sont pas grossissants ; pour e évident ; pour $u^\alpha v^\beta$, $\alpha, \beta \neq 0$, car $u^\alpha v^\beta \mathcal{B} \neq v$ et $\mathcal{B}u^\alpha v^\beta \neq u$.

LEMME 2.1. - Pour tout élément x de $\mathcal{B}$, $x \neq u, v$, il existe un élément $x' \neq e$, qui n'est pas une puissance de x et qui permute avec x .

Si $x = u^\alpha v^\beta$ avec $\alpha > 0$, $\beta > 0$, $\alpha + \beta > 2$, on peut prendre $x' = uv$.

$$x'x = u^\alpha vu^\alpha v^\beta = u^\alpha v^\beta; \quad xx' = u^\alpha v^\beta uv = u^\alpha v^\beta.$$

$x^n = u^\alpha v^\beta \dots u^\alpha v^\beta = u^\gamma v^\delta$ avec $\gamma \geq \alpha$; $\delta \geq \beta \Rightarrow \gamma + \delta > 2$
donc $x^n \neq x'$, $\forall n$.

- Si $x = uv$ prendre $x' = u^2 v^2$, on a $xx' = x'x = x'$.

$$x^2 = uvuv = x \Rightarrow x^n = x \Rightarrow x' \neq x^n, \quad \forall n.$$

- Si $x = u^\alpha$, $\alpha > 1$ prendre $x' = u$; $x^n = u^{\alpha n} \neq u$.

- Si $x = v^\beta$, $\beta > 1$ prendre $x' = v$.

- Si $x = u$; $x' \neq u^n \Rightarrow x' = u^\alpha v^\beta$, $\beta > 0$

$$xx' = u^\alpha v^{\beta-1} \text{ avec } v^0 = e \text{ si } \beta = 1$$

$$x'x = u^{\alpha+1} v^\beta \quad xx' \neq x'x.$$

De même pour $x = v$, il n'existe pas de $x' \neq v^n$ permutant avec v .

THÉOREME 2.1. - $\mathcal{B}$ n'a pas d'automorphisme distinct de l'automorphisme identique.

Soit φ un automorphisme de $\mathcal{B}$. Si $x \neq u, v$, il existe $x' \neq x^n, e$, $xx' = x'x$. $\varphi(x)$ et $\varphi(x')$ possèdent la même propriété, ainsi que $\varphi^{-1}(x)$ et $\varphi^{-1}(x')$.

Donc $\varphi(u) = u$ ou v et, φ étant un automorphisme, on a soit

$$(1) \begin{cases} \varphi(u) = u \\ \varphi(v) = v \end{cases} \quad (2) \begin{cases} \varphi(u) = v \\ \varphi(v) = u \end{cases}$$

(1) $\Rightarrow \varphi =$ identité.

(2) $\varphi(u^2 v) = \varphi^2(u) \varphi(v) = v^2 u = v = \varphi(u)$, mais alors φ n'est pas un automorphisme.

COROLLAIRE 2.1. - Si $\mathcal{Q}$ est isomorphe à $\mathcal{B}$, il existe un seul isomorphisme entre $\mathcal{Q}$ et $\mathcal{B}$.

En effet soient $\varphi_1 : \mathcal{B} \rightarrow \mathcal{Q}$, $\varphi_2 : \mathcal{B} \rightarrow \mathcal{Q}$ deux isomorphismes. $\varphi_2^{-1} \circ \varphi_1$ est un automorphisme de $\mathcal{B} \Rightarrow \varphi_2 = \varphi_1$.

THÉOREME 2.2. - Soit D un demi-groupe ayant un élément unité $e_D = e$. Pour qu'un élément $x \in D$ soit grossissant à droite, il faut et il suffit qu'il existe

un isomorphisme φ de $\mathcal{B}$ dans D tel que $\varphi(e_{\mathcal{B}}) = e_D = e$, $\varphi(u) = x$.

1° Soit x un élément grossissant à droite de D ; il existe y avec $yx = e$.

Considérons $\mathcal{A} = \{x, y\}$, comme $yx = e$, tous les éléments de $\mathcal{A}$ se mettent sous la forme $x^\alpha y^\beta$, $x^0 = y^0 = e$, $\alpha \geq 0$, $\beta \geq 0$.

Supposons $x^{\alpha_1} y^{\beta_1} = x^{\alpha_2} y^{\beta_2}$ avec $\alpha_1 \geq \alpha_2$.

$$y^{\alpha_2} x^{\alpha_1} y^{\beta_1} = y^{\alpha_2} x^{\alpha_2} y^{\beta_2} \Rightarrow x^{\alpha_1 - \alpha_2} y^{\beta_1} = y^{\beta_2}.$$

Si $\alpha_1 = \alpha_2$, $y^{\beta_1} = y^{\beta_2}$; si $\beta_1 \neq \beta_2$ soit $\gamma = \sup(\beta_1, \beta_2)$

$$y^{\beta_1} x^\gamma = y^{\beta_2} x^\gamma \Rightarrow x^d = e, \quad d = |\beta_1 - \beta_2| ;$$

x étant sans torsion, on a $d = 0$.

Si $\alpha_1 > \alpha_2$, $x^d \supseteq x x^{\alpha_1 - \alpha_2 - 1} y^{\beta_1} D = y^{\beta_2} D \supseteq y^{\beta_2} x^{\beta_2} D = D$. x serait inversible à droite ce qui contredit le théorème 1.3. On obtient donc un isomorphisme φ de $\mathcal{B}$ sur $\mathcal{A} \subseteq D$ en posant $\varphi(u^\alpha v^\beta) = x^\alpha y^\beta$, on a

$$\varphi(e_{\mathcal{B}}) = e, \quad \varphi(u) = x.$$

2° Soit φ un isomorphisme de $\mathcal{B}$ dans D tel que $\varphi(e_{\mathcal{B}}) = e$;

$$\varphi(u) \varphi(v) = \varphi(uv) \neq \varphi(e_{\mathcal{B}}) = e.$$

$$\varphi(v) \varphi(u) = \varphi(vu) = e.$$

Ceci montre que $\varphi(v)$ n'est pas inversible à gauche, car si on avait $a \varphi(v) = e$, on aurait $a \varphi(v) \varphi(u) = \varphi(u) \Rightarrow ae = \varphi(u)$, mais $\varphi(u)$ ne répond pas à la question.

$$[D \varphi(v)] \varphi(u) = De = D ; \quad D \varphi(v) \neq 0, \text{ car } e \notin D \varphi(v).$$

$\varphi(u)$ est bien un élément grossissant à droite.

COROLLAIRE 2.2. - Dans un demi-groupe ayant un élément unité chaque élément grossissant est régulier.

On a

$$x = \varphi(u), \quad \varphi(u) \varphi(v) \varphi(u) = \varphi(uvu) = \varphi(u).$$

COROLLAIRE 2.3. - Si un demi-groupe, avec élément unité, a des éléments grossissants d'un côté, il en a aussi de l'autre.

Exemple montrant qu'il n'en est pas ainsi lorsque D n'a pas d'élément unité :

Soit A un demi-groupe avec zéro, ayant au moins deux éléments et tel que le produit de deux éléments soit toujours 0.

Soient B un demi-groupe quelconque et $D = A \cup B$; avec comme produit dans A et dans B le produit initial, et si $x \in A$, $y \in B$, $xy = 0$; $yx = x$.

Soient $z_1 = (x_1 x_2) x_3$, $z_2 = x_1(x_2 x_3)$.

Si x_1 ou $x_2 \in A$, $z_1 = z_2 = 0$.

Si $x_1, x_2 \in B$, $x_3 \in A$, alors $z_1 = x_3$; $z_2 = x_3$.

Si $x_1, x_2, x_3 \in B$, $z_1 = z_2$, car B est un demi-groupe.

Soient $x \in A$, $y \in B$, $D' \subset D$ avec $D' = A' \cup B'$, $A' \subseteq A$; $B' \subseteq B$.

$$xD' = xA' \cup xB' = 0 \cup 0 = 0 , \quad D'x = A'x \cup B'x \subseteq 0 \cup x .$$

$$yD' = yA' \cup yB' \subseteq A' \cup yB' , \quad D'y = A'y \cup B'y \subseteq 0 \cup B'y .$$

Ce calcul montre que D ne peut avoir d'élément grossissant à droite, mais si B contient un élément g grossissant à gauche, alors g est grossissant à gauche dans D . Prendre $D' = A \cup B'$ ou $B' \subset B$, $gB' = B$.

THÉOREME 2.3 (Réciproque du théorème 1.3). - Dans un demi-groupe avec élément unité les éléments grossissants à droite et seulement eux sont inversibles à gauche et non inversibles à droite.

Soit l tel que $Dl = D$, $lD \neq D$.

Soit r tel que $rl = e$, e élément unité de D .

$$r(lD) = eD = D \implies r \text{ grossissant à gauche.}$$

Considérons $\alpha = \{r, l\}$, $rl = e$, les éléments de α sont de la forme $l^\alpha r^\beta$ ($l^0 = r^0 = e$) .

$$\text{Soit } l^{\alpha_1} r^{\beta_1} = l^{\alpha_2} r^{\beta_2} .$$

Si $\alpha_1 = \alpha_2$, $r^{\beta_1} = r^{\beta_2}$ comme r est grossissant, $\beta_1 = \beta_2$.

$$\text{Soit } \alpha_1 > \alpha_2 , \quad l^{\alpha_1 - \alpha_2} r^{\beta_1} = r^{\beta_2} .$$

$$rD = D ; \quad lD \supseteq l^{\alpha_1 - \alpha_2} rD = r^{\beta_2} D = D \text{ ce qui contredit } lD \neq D .$$

Donc $\alpha = \{r, l\}$ est isomorphe au demi-groupe bicyclique $\mathcal{B}$, le théorème 2.2 $\implies l$ grossissant à droite.

Avec les notations des théorèmes 1.2 ; 1.5 , nous avons :

$$R = D^{(l)} \quad L = D^{(r)} \quad D^{(n)} = G + A .$$

3. Inversibilité potentielle.

DÉFINITION 3.1. - Un élément $a \in D$ est dit potentiellement inversible à gauche, s'il existe un sur-demi-groupe D' de D dans lequel a est inversible à gauche.

Cette notion a été introduite par LJAPIN. L'étude qui suit résulte des travaux de ŠUMOV (1958).

Soit $\mathcal{K}$ un système de générateurs de D , si $\forall k \in \mathcal{K}$, il existe dans D un élément z_k tel que $z_k a = k$, a est inversible à gauche dans D . En effet si $s = k_1 \dots k_n$, on a

$$(k_1 k_2 \dots k_{n-1} z_{k_n}).a = s.$$

L'écriture $x \in D^*$ signifie que $x \in D$ ou que x est le mot vide.

LEMME 3.1. - Soit a un élément de D potentiellement inversible à gauche ; si pour un n et pour $x, y \in D^*$, on a $a^n x = a^n y$, alors $sx = sy$, $\forall s \in D$.

En effet soit D' un sur-demi-groupe dans lequel a est inversible à gauche. Dans D' il existe $b_1, \dots, b_n$, avec

$$b_1 a = s ; b_2 a = b_1 ; \dots ; b_n a = b_{n-1}.$$

$$b_n a^n x = b_{n-1} a^{n-1} x = \dots = b_1 a x = s x$$

$$\implies s x = s y.$$

$$b_n a^n y = b_{n-1} a^{n-1} y = \dots = b_1 a y = s y$$

LEMME 3.2. - Si dans D , $a^2 x = a^2 y$ implique $sx = sy$, $\forall s \in D$; pour $x, y \in D^*$, $a^n x = a^n y$ implique $sx = sy$, $\forall s \in D$, $\forall n$.

En effet si x et y , tels que $ax = ay$, $a^2 x = a^2 y \implies sx = sy$.

$$\begin{aligned} a^n x = a^n y, \quad n > 2 &\implies a^2 (a^{n-2} x) = a^2 (a^{n-2} y) \implies a(a^{n-2} x) = a(a^{n-2} y) \\ &\implies a^{n-1} x = a^{n-1} y \end{aligned}$$

d'où par induction

$$a^2 x = a^2 y \text{ et } sx = sy.$$

THÉOREME 3.1. - Dans le cas où a est de type fini, la condition du lemme 3.1 est nécessaire et suffisante pour que a soit inversible à gauche dans D .

Soit (h, d) le type de a , on a $a^{h+d} = a^h$, $a^h a^d = a^h$. La condition du lemme 3.1 $\implies sa^d = s$, $\forall s \in D$.

$(sa^{d-1}).a = s$, a est bien inversible à gauche dans D . On peut remarquer

que dans ce cas le sous-demi-groupe engendré par a est un groupe. En effet, il existe $x_1, \dots, x_h$, avec $x_1 a = a$, $x_2 a = x_1 \dots x_h a = x_{h-1} \Rightarrow x_h a^h = a$.

$$a^{h+d} = a^h \Rightarrow x_h a^{h+d} = x_h a^h \Rightarrow a^{1+d} = a.$$

Construction fondamentale. - Soit a un élément de D vérifiant la condition du lemme 3.1.

Soit $K = \{(x, n)\}$, $x \in D$, n entier ≥ 0 .

$\mathcal{B} = \{\text{mots sur } K, W \in \mathcal{B}, W = (x_1, n_1) \dots (x_s, n_s)\}$ dans lesquels n_i, n_{i+1} ne peuvent être nuls en même temps.

$W.W' = W''$ si $W' = (x'_1, n'_1) \dots (x'_s, n'_s)$, $W'' =$ produit des mots $W.W'$ si $n_s \neq 0$ ou si $n'_1 \neq 0$.

Si $n_s = 0$, $n'_1 = 0$, alors dans W'' le terme $(x_s, 0)(x'_1, 0)$ est remplacé par $(x_s x'_1, 0)$. $\mathcal{B}$ est un demi-groupe.

Définissons dans $\mathcal{B}$ les relations suivantes.

$$\left\{ \begin{array}{l} W \sim W' (\eta_1) \text{ si } W, W' \in \mathcal{B} . \\ W = (x_1, k)(x_2, 0) ; ax_2 = a^{k+1} r ; W' = (x_1 r, 0), x_1, x_2 \in D, r \in D^* . \\ W \sim W' (\eta_2) \text{ si } W, W' \in \mathcal{B} . \\ W = (x_1, k)(x_2, 0), ax_2 = a^\ell r, W' = (x_1, k - \ell + 1)(r, 0) \\ \text{pour } k \geq \ell > 1 ; r \in D^* \text{ si } r \text{ mot vide, } (r, 0) \text{ mot vide} . \\ W \sim W' (\eta_3) \text{ si on a soit} \\ W \sim W' (\eta_1) ; W' \sim W (\eta_1) ; W \sim W' (\eta_2) ; W' \sim W (\eta_2) ; W = W' . \end{array} \right.$$

Remarquons que si $W \sim W' (\eta_i)$, alors $\forall x \in D, W(x, 0) \sim W'(x, 0) (\eta_i)$ pour $i = (1, 2, 3)$.

Définition dans $\mathcal{B}$ d'un opérateur σ . - Soit $W = (x_1, k_1) \dots (x_m, k_m) \in \mathcal{B}$ et soit, s'il existe (x_t, k_t) l'élément le plus à droite de ce mot tel que $t < m$, $k_{t+1} = 0$ et qu'il existe $r \in D^*$ avec $ax_{t+1} = a^{k_{t+1}} r$. $\sigma(W)$ se réduit de W en remplaçant $(x_t, k_t)(x_{t+1}, 0)$ par $(x_t r, 0)$ [si $k_{t-1} = 0$, $(x_{t-1}, 0)(x_t r, 0) = (x_{t-1} x_t r, 0)$]. S'il n'existe pas dans W d'élément (x_t, k_t) , on pose $\sigma(W) = W$. σ est bien défini, car si $ax_{t+1} = a^{k_{t+1}} r = a^{k_{t+1}} r'$ d'après l'hypothèse que vérifie a , $xr = xr'$, $\forall x \in D$, donc $x_t r = x_t r'$.

Notations.

η étant une relation binaire dans D , nous écrirons $x \sim y(\eta')$, $x, y \in D$ s'il existe $u_1, u_2 \in D^*$, $x_1, y_1 \in D$ tels que $x = u_1 x_1 u_2$; $y = u_1 y_1 u_2$; $x_1 \sim y_1(\eta)$.

η'' = fermeture transitive de η' . η'' est la relation d'équivalence régulière engendrée par η si η est une relation réflexive, symétrique.

On a $W \sim \sigma(W)$ (η_1') et $\forall x \in D$, $\sigma[(x, 0)] = (x, 0)$ ou $W = \sigma(W)$.

Propriétés de η_3 , η_3' , η_3'' .

LEMME 3.3. - Si $W \sim W'$ (η_3') alors $\sigma(W) \sim \sigma(W')$ (η_3').

Soient $W = T_1 \cdot U \cdot T_2$, $W' = T_1 \cdot U' \cdot T_2$, $U \sim U'$ (η_3).

Prendre $U \sim U'$ (η_1), $i = 1, 2$, car le cas $U = U'$ est trivial et le cas $U' \sim U$ (η_1) est symétrique du précédent.

D'après la remarque qui suit la définition de η_3 on peut supposer que T_2 commence par (x, p) avec $p \neq 0$.

- Si $\sigma(T_2) \neq T_2$, $\sigma(W) = T_1 \cdot U \cdot \sigma(T_2)$; $\sigma(W') = T_1 \cdot U' \cdot \sigma(T_2)$ d'où $\sigma(W) \sim \sigma(W')$ (η_3')

- Si $\sigma(T_2) = T_2$. Supposons $U \sim U'$ (η_1) alors $\sigma(U) = U'$ ce qui donne

$$\sigma(W) = T_1 \cdot \sigma(U) \cdot T_2 \implies \sigma(W) = W'$$

$$\text{or } \begin{cases} W' \sim \sigma(W') & (\eta_1') \\ \text{ou } W' = \sigma(W') \end{cases} \implies \sigma(W) \sim \sigma(W') & (\eta_3')$$

Si $U \sim U'$ (η_2) alors

$$U = (x_1, k) \cdot (x_2, 0); ax_2 = a^\ell r; U' = (x_1, k - \ell + 1)(r, 0) \quad k \geq \ell > 1.$$

S'il existe s tel que $ax_2 = a^{k+1} s$, on a $\sigma(W) = T_1 \cdot (x_1 s, 0) \cdot T_2$

$$a^\ell r = a^{k+1} s \implies ar = a^{k-\ell+2} s$$

d'après la propriété de a .

$$\sigma(W') = T_1 \cdot (x_1 s, 0) \cdot T_2 = \sigma(W).$$

S'il n'existe pas de s vérifiant $ax_2 = a^{k+1} s$, il n'existe pas non plus de s tel que $ar = a^{k-\ell+2} s$, par suite

$$\sigma(U) = U; \quad \sigma(U') = U'$$

$$\sigma(W) = \sigma(T_1) \cdot U \cdot T_2; \quad \sigma(W') = \sigma(T_1) \cdot U' \cdot T_2$$

d'où

$$\sigma(W) \sim \sigma(W') & (\eta_2').$$

LEMME 3.4. - Si $(x, 0) \sim (y, 0) \ (\eta_3'')$, on a $x = y$.

En effet

$$(x, 0) \sim (y, 0) \ (\eta_3'') \implies \exists V_1, V_2, \dots, V_p \in \mathcal{B}$$

tels que

$$(x, 0) = V_1 ; V_1 \sim V_2 \ (\eta_3') ; \dots ; V_i \sim V_{i+1} \ (\eta_3') ; \dots ; V_p = (y, 0) .$$

Récurrence sur p . Si $p = 1$ trivial,

$$\sigma[(x, 0)] = (x, 0) = \sigma(V_1) ; \sigma(V_p) = \sigma[(y, 0)] = (y, 0) .$$

Le lemme 3.3 entraîne $\sigma(V_i) \sim \sigma(V_{i+1}) \ (\eta_3')$.

$V_2 \sim (x, 0) \ (\eta_3')$, la seule possibilité est $V_2 \sim (x, 0) \ (\eta_1')$ avec $V_2 = (x_1, 0)(x_2, k)(x_3, 0)$; $ax_3 = a^{k+1}r$; $x = x_1 x_2 r$; mais alors

$$\sigma(V_2) = (x_1 x_2 r, 0) = (x, 0) .$$

On obtient donc une suite $\sigma(V_1) ; \sigma(V_2) ; \dots ; \sigma(V_p)$ plus courte que la précédente. Par suite $x = y$.

THÉOREME 3.2. - Pour qu'un élément a d'un demi-groupe D soit potentiellement inversible à gauche, il faut et il suffit que $\forall x, y \in D^*$, tels que $a^2 x = a^2 y$, on ait $sx = sy$, $\forall s \in D$.

La condition nécessaire résulte du lemme 3.1.

Condition suffisante : Considérons $\mathcal{B}$ comme un sur-demi-groupe de D en identifiant $(x, 0)$ avec x ; et $\overline{\mathcal{B}} = \mathcal{B}/\eta_3''$. Dans $\overline{\mathcal{B}}$ l'élément $\overline{a}$ (classe de $a \bmod \eta_3''$) est inversible à gauche. En effet pour $\forall (x, k)$, on a $k \geq 1$,

$$(x, k+1)(a, 0) \sim (x, k) \ (\eta_2) \quad \text{prendre } l=2 ; r \text{ mot vide.}$$

$$(x, 1)(a, 0) \sim (x, 0) \ (\eta_1) \quad \text{prendre } r \text{ vide.}$$

Dans $\overline{\mathcal{B}}$ on a

$$\overline{(x, k+1) \cdot a} = \overline{(x, k)} ,$$

Soit φ l'homomorphisme naturel de $\mathcal{B}$ sur $\overline{\mathcal{B}}$.

La restriction de φ à D est un isomorphisme d'après le lemme 3.4.

$\overline{\mathcal{B}}$ étant engendré par les $\overline{(x, k)}$, $\overline{a}$ est inversible à gauche dans $\overline{\mathcal{B}}$.

COROLLAIRE 3.1. - Dans un semi-groupe D tous les éléments sont potentiellement inversibles à droite.

Soit $a \in D$, $a^2 x = a^2 y \implies x = y$ si x et $y \in D \implies sx = sy$.

$$a^2 x = a^2 \implies ax = a .$$

Mais si dans D , $ax = a$, a simplifiable, alors x est élément unité de D . Donc $sx = s$, $\forall s \in D$.

Un élément potentiellement b -inversible (c'est-à-dire tel qu'il existe $D' \supseteq D$ avec $aD' = D' a = D'$) est évidemment potentiellement inversible à gauche et à droite. La réciproque est fausse. On peut construire un exemple où D est un semi-groupe et où D contient un élément non potentiellement b -inversible. En particulier ce semi-groupe n'est pas immergeable dans un groupe.

Soit le demi-groupe libre $\mathbb{W}_K$ construit avec comme système de générateurs $K = \{x_1, x_2, x_3, x_4, x_5, x_6\}$.

Soient

$$K_1 = \{x_1, x_2, x_3, x_4\}, \quad K_2 = \{x_1, x_2, x_5, x_6\}$$

$$\mathcal{B} = \{x_1 x_5, x_1 x_6, x_2 x_5, x_3 x_1, x_3 x_2, x_4 x_1\}.$$

Remarquons que $x_i x_j \in \mathcal{B} \Rightarrow x_i \in K_1; x_j \in K_2$.

Soient

$$\delta : K_1 \rightarrow K_1$$

$$\delta(x_1) = x_3; \quad \delta(x_2) = x_4; \quad \delta(x_3) = x_1; \quad \delta(x_4) = x_2$$

$$\tau : K_2 \rightarrow K_2$$

$$\tau(x_1) = x_5; \quad \tau(x_2) = x_6; \quad \tau(x_5) = x_1; \quad \tau(x_6) = x_2.$$

Remarquons que

$$\delta^2(x_i) = x_i; \quad \tau^2(x_j) = x_j.$$

Définissons dans $\mathbb{W}_K$ la relation η suivante $U, V \in \mathbb{W}_K$, $U \sim V$ (η) si $U = V$ ou $U = x_i x_j \in \mathcal{B}$ et $V = \delta(x_i) \cdot \tau(x_j)$.

(η) est réflexive et symétrique.

Propriétés de (η).

α . Si $x_i x_k \in \mathcal{B}$; $x_j x_k \in \mathcal{B}$; alors on ne peut avoir $x_j = \delta(x_i)$.

β . Si $x_{i_1} x_{i_2} \dots x_{i_s} \sim x_{j_1} x_{j_2} \dots x_{j_s}$ (η''); si $x_{i_1} \notin K_1$, alors $x_{i_1} = x_{j_1}$.

γ . Si $x_{i_1} \in K_1$ alors $x_{j_1} = x_{i_1}$ ou $x_{j_1} = \delta(x_{i_1})$.

δ . Si $x_k x_{i_1} \dots x_{i_s} \sim x_k x_{j_1} \dots x_{j_s}$ (η'), alors

$$x_{i_1} \dots x_{i_s} \sim x_{j_1} \dots x_{j_s} \quad (\eta').$$

e. Si $x_k x_{i_1} \dots x_{i_s} \sim x_k x_{j_1} \dots x_{j_s} \quad (\eta'')$, alors

$$x_{i_1} \dots x_{i_s} \sim x_{j_1} \dots x_{j_s} \quad (\eta'').$$

En effet soient

$$U_1 \sim U_2 \quad (\eta') \dots U_\alpha \sim U_{\alpha+1} \quad (\eta') \dots U_m \sim U_{m+1} \quad (\eta')$$

où

$$U_1 = x_k x_{i_1} \dots x_{i_s}; \quad U_\alpha = x_{\alpha_0} x_{\alpha_1} \dots x_{\alpha_s}; \quad U_{m+1} = x_k x_{j_1} \dots x_{j_s};$$

$$2 \leq \alpha \leq m.$$

Remarque : deux mots liés par (η') ont la même longueur, ce qui justifie l'écriture des U_α .

Raisonnons par récurrence sur le nombre $m + 1$ de termes de la suite U_α . Si $x_k x_{i_1} \notin \mathcal{B}$ ou $x_k x_{j_1} \notin \mathcal{B}$, le 2^e ou le m -ième terme commence par x_k , l'hypothèse de récurrence donne le résultat car pour $m = 1$ nous sommes dans le cas (δ) .

Soit $m > 1$. S'il existe α avec $x_{\alpha_0} = x_k$ en appliquant l'hypothèse de récurrence à $U_1, U_2, \dots, U_\alpha; U_\alpha, U_{\alpha+1}, \dots, U_m$, on obtient

$$x_{i_1} \dots x_{i_s} \sim x_{\alpha_1} \dots x_{\alpha_s} \quad (\eta'')$$

$$x_{\alpha_1} \dots x_{\alpha_s} \sim x_{j_1} \dots x_{j_s} \quad (\eta'')$$

d'où le résultat.

Si pour α , $x_{\alpha_0} \neq x_k$, comme $x_k x_{i_1}$ ou $x_k x_{j_1} \in \mathcal{B}$, on a $x_k \in \mathcal{K}_1$, donc d'après (γ) $x_{\alpha_0} = \delta(x_k)$.

$$x_{20} = \delta(x_k) \implies x_{21} = \tau(x_{i_1})$$

et

$$x_{22} = x_{i_2}; \dots x_{2s} = x_{i_s}.$$

De même

$$x_{m_0} = \delta(x_k); \quad x_{m_1} = \tau(x_{j_1}); \quad x_{m_2} = x_{j_2} \dots x_{m_s} = x_{j_s},$$

$U_2 \sim U_m \quad (\eta'')$. Donc l'hypothèse de récurrence donne

$$x_{21} x_{22} \dots x_{2s} \sim x_{m_1} \dots x_{m_s} \quad (\eta'').$$

(β) et $(\gamma) \Rightarrow x_{2s} = x_{m_1}$ ou $x_{2_1} = \delta(x_{m_1})$, mais $x_{20} x_{21} \in \mathcal{B}$;
 $x_{m_0} x_{m_1} \in \mathcal{B} \Rightarrow 2^e$ cas impossible.

On peut à nouveau appliquer l'hypothèse qui donne

$$x_{22} \dots x_{2s} \sim x_{m_2} \dots x_{m_s} \quad (\eta'')$$

c'est-à-dire

$$x_{i_2} \dots x_{i_s} \sim x_{j_2} \dots x_{j_s} \quad (\eta'').$$

Mais $x_{i_1} = \tau(x_{21})$, $x_{j_1} = \tau(x_{m_1})$, $x_{21} = x_{m_1}$ d'où

$$x_{i_1} x_{i_2} \dots x_{i_s} \sim x_{j_1} x_{j_2} \dots x_{j_s} \quad (\eta'').$$

ζ. Si

$$x_{i_1} x_{i_2} \dots x_{i_s} x_k \sim x_{j_1} x_{j_2} \dots x_{j_s} x_k \quad (\eta''),$$

alors

$$x_{i_1} x_{i_2} \dots x_{i_s} \sim x_{j_1} x_{j_2} \dots x_{j_s} \quad (\eta'').$$

Démonstration analogue à celle de (ε) .

ξ. $x_2 x_6 \not\sim x_4 x_2 \quad (\eta'')$.

Résulte de ce que $x_2 x_6$ n'est lié qu'à lui-même par η .

Considérons maintenant le demi-groupe quotient $\mathbb{W}_K^\eta = \mathbb{W}_K / \eta''$. Ses éléments sont les classes notées $\bar{W}$, si $W \in \mathbb{W}_K$.

Des propriétés (ε) et (ζ) de η'' , on déduit

$$\begin{aligned} \bar{x}_k \bar{U} &= \bar{x}_k \bar{V} \Rightarrow \bar{U} = \bar{V} \\ \bar{U} \bar{x}_k &= \bar{V} \bar{x}_k \Rightarrow \bar{U} = \bar{V} \end{aligned}$$

$\mathbb{W}_K^\eta$ est donc un semi-groupe.

LEMME 3.5. - Si dans un demi-groupe D des éléments $y_1, \dots, y_6$ vérifient $y_1 y_5 = y_3 y_1$, $y_2 y_5 = y_4 y_1$, $y_1 y_6 = y_3 y_2$ et s'il existe un sur-demi-groupe D' dans lequel y_1 soit bilatèrément inversible, on a $y_2 y_6 = y_4 y_2$.

Dans D' il existe u et v tels que $y_1 u = y_2$; $vy_1 = y_2$

$$y_2 y_6 = vy_1 y_6 = vy_3 y_2 = vy_3 y_1 u = vy_1 y_5 u = y_2 y_5 u$$

$$= y_4 y_1 u = y_4 y_2.$$

Dans le semi-groupe $\mathbb{W}_K^\eta$ les éléments $\bar{x}_1, \dots, \bar{x}_6$ vérifient les hypothèses du lemme 3.5, mais on n'a pas $\bar{x}_2 \bar{x}_6 = \bar{x}_4 \bar{x}_2$, donc $\bar{x}_1$ n'est pas un élément

potentiellement b-inversible.

Remarque. - Le 23 avril 1956, J. RIGUET avait fait dans ce séminaire un exposé [3] ayant pour titre : "Travaux soviétiques récents sur la théorie des demi-groupes". Il s'agissait d'un mémoire de E. S. LJAPIN [1]. Le théorème principal de la première partie de ce travail était énoncé : "Pour qu'un élément d'un demi-groupe soit potentiellement inversible, il faut et il suffit qu'il soit simplifiable". L'exemple ci-dessus contredit évidemment ce théorème. En reprenant l'exposé de RIGUET, on peut constater qu'en plus de certaines imprécisions dans la définition de l'application σ , c'est le lemme 2 qui est faux. Soient $u = t_1 t_2$; $v = t_1 x \bar{x} t_2$. On n'a pas $\sigma(v) = u$ ou $\sigma(u) \rightarrow \sigma(v)$.

En effet prenons comme demi-groupe E le demi-groupe $\mathcal{W}_K^\eta = \{y_1, y_2, y_3, y_4, y_5, y_6\}$ avec

$$y_1 y_5 = y_3 y_1 ; \quad y_2 y_5 = y_4 y_1 ; \quad y_1 y_6 = y_3 y_2 ; \quad y_2 y_6 \neq y_4 y_2 .$$

Faisons jouer à y_1 le rôle de x dans l'exposé de RIGUET.

Soit

$$u = (y_2 \bar{x} y_3) \cdot y_2 , \quad v = y_2 \bar{x} y_3 x \bar{x} y_2 .$$

Mais

$$\begin{aligned} u &= y_2 \bar{x} x y_6 & \sigma(u) &= y_2 y_6 \\ v &= y_2 \bar{x} x y_5 \bar{x} y_2 & \sigma(v) &= y_2 y_5 \bar{x} y_2 = y_4 x \bar{x} y_2 . \end{aligned}$$

D'où

$$\sigma(v) \neq u ; \quad \sigma(u) \not\rightarrow (v) .$$

Donc, du théorème énoncé au début de cette remarque, seule reste valable la condition nécessaire.

BIBLIOGRAPHIE

- [1] LJAPIN (E. S.). - Inversibilité potentielle des éléments d'un demi-groupe [en russe], Mat. Sbornik, N. S., t. 38, 1956, p. 373-388.
- [2] LJAPIN (E. S.). - Polugrupp' [Demi-groupes]. - Moskva, 1960.
- [3] RIGUET (Jacques). - Travaux soviétiques récents sur la théorie des demi-groupes, Séminaire Dubreil-Pisot : Algèbre et Théorie des nombres, t. 9, 1955/56, n° 21, 13 p.