Séminaire Dubreil.
Algèbre et théorie
des nombres

Maurice Nivat

Congruences parfaites et quasi-parfaites

Séminaire Dubreil. Algèbre et théorie des nombres, tome 25, n° 1 (1971-1972), exp. n° 7, p. 1-9

<http://www.numdam.org/item?id=SD_1971-1972__25_1_A7_0>

Séminaire DUBREIL
(Algèbre)
25e année, 1971/72, n° 7, 9 p.

31 janvier 1972

CONGRUENCES PARFAITES ET QUASI-PARFAITES

par Maurice NIVAT

(rédigé avec la collaboration de Michèle BENOIS)

1. Introduction.

Nous définissons ci-dessous une classe de congruences sur un monoïde libre qui jouit de propriétés de décidabilité remarquables. Ces congruences ont été considérées pour la première fois, semble-t-il, par M. NIVAT à l'occasion de ses travaux sur les langages algébriques. Un langage algébrique qui joue un rôle fondamental dans toute la théorie est en effet le langage de Dyck que l'on définit comme classe d'équivalence du mot vide dans une congruence parfaite, congruence que les mathématiciens connaissent bien puisqu'il s'agit de celle qui permet de construire le groupe libre comme quotient d'un monoïde libre.

Nous ne donnons ci-dessous que les propriétés fondamentales, renvoyant à la bibliographie pour les applications.

2. Définitions : Systèmes parfaits et quasi-parfaits.

Soit Σ une partie finie de $X^* \times X^*$, où X^* est le monoïde libre engendré par l'alphabet fini X.

Nous notons 1 l'élément neutre de X^*, c'est-à-dire le mot vide et, pour tout $f \in X^*$, nous notons $|f|$ sa longueur, c'est-à-dire le nombre de lettres de X qui composent f.

Nous posons, pour tout $f, g \in X^*$,

1° $f \underset{\Sigma}{\longleftrightarrow} g \Leftrightarrow \exists\, \alpha, \beta \in X^*$, $(u, v) \in \Sigma \cup \Sigma^{-1}$ tels que $f = \alpha u \beta$ et $g = \alpha v \beta$.

Σ^{-1} désigne la partie de $X^* \times X^*$ formée des couples (u, v) tels que $(v,u) \in \Sigma$.

2° $f \underset{\Sigma}{\longrightarrow} g \Leftrightarrow f \underset{\Sigma}{\longleftrightarrow} g$ et $|f| > |g|$.

3° $f \underset{\Sigma}{\longmapsto} g \Leftrightarrow f \underset{\Sigma}{\longleftrightarrow} g$ et $|f| = |g|$.

Nous désignerons par $\overset{*}{\underset{\Sigma}{\longleftrightarrow}}$, $\overset{*}{\underset{\Sigma}{\longrightarrow}}$, $\overset{*}{\underset{\Sigma}{\longmapsto}}$, respectivement les fermetures transitives et reflexives de $\underset{\Sigma}{\longleftrightarrow}$, $\underset{\Sigma}{\longrightarrow}$, et $\underset{\Sigma}{\longmapsto}$. Par définition $\overset{*}{\underset{\Sigma}{\longleftrightarrow}}$ est la congruence engendrée sur X^* par Σ. Le plus souvent, quand aucune confusion n'est à craindre, nous omettrons l'indice Σ, et utiliserons les symboles $\longleftrightarrow$, $\longrightarrow$, $\longmapsto$ et leurs "étoiles".

Le mot $f \in X^*$ est dit irréductible pour Σ si, et seulement si, $\{g \mid f \underset{\Sigma}{\longrightarrow} g\}$ est vide.

Le système Σ de générateurs de la congruence $\overset{*}{\underset{\Sigma}{\leftrightarrow}}$ est dit quasi-parfait si, et seulement si, la condition suivante est satisfaite :

(C1) Pour tout couple de mots , h , h' , irréductibles pour Σ ,

$$h \overset{*}{\underset{\Sigma}{\leftrightarrow}} h' \Rightarrow h \overset{*}{\underset{\Sigma}{\mapsto}} h' .$$

Le système Σ est dit parfait si, et seulement si :

(C'1) Pour tout couple de mots, h , h' , irréductibles pour Σ ,

$$h \overset{*}{\underset{\Sigma}{\leftrightarrow}} h' \Rightarrow h = h' .$$

Il est immédiat que Σ est quasi-parfait s'il est parfait.

Une congruence Θ sur X^* sera dite quasi-parfaite (resp. parfaite) si, et seulement si, il existe un système quasi-parfait (resp. parfait) Σ tel que $\Theta = \overset{*}{\underset{\Sigma}{\leftrightarrow}}$.

3. Chaînes.

Soit Σ un système de générateurs. Nous appelons chaîne allant de f en g , toute suite de mots $u_1 , \ldots , u_{k+1}$ de X^* satisfaisant :

1° $u_1 = f$,

2° $u_{k+1} = g$,

3° pour tout $i = 1 , \ldots , k$, $u_i \leftrightarrow u_{i+1}$.

Clairement, pour tout couple de mots, f , g , de X^* ,

$$f \overset{*}{\leftrightarrow} g \Leftrightarrow \text{il existe une chaîne allant de } f \text{ en } g .$$

Une chaîne $u_1 , \ldots , u_{k+1}$ est dite décomposable si, et seulement si, il existe deux indices $1 \leqslant i \leqslant j \leqslant k + 1$ tels que :

1° $u_1 \rightarrow u_2 \rightarrow \ldots \rightarrow u_i$,

2° $u_i \mapsto u_{i+1} \mapsto \ldots \mapsto u_j$,

3° $u_j \leftarrow u_{j+1} \leftarrow \ldots \leftarrow u_{k+1}$.

Par définition, la longueur de la chaîne $u_1 , \ldots , u_{k+1}$ est égale à k .

THÉORÈME 1. - Le système Σ est quasi-parfait si, et seulement si,

(C3) Pour toute chaîne u_1 , u_2 , u_3 de longueur 2 , il existe une chaîne décomposable allant de u_1 à u_3 .

Nous établissons d'abord un lemme.

LEMME 1. - Le système Σ est quasi-parfait si, et seulement si :

(C2) Pour toute chaîne $u_1 , \ldots , u_{k+1}$, il existe une chaîne décomposable allant de u_1 à u_{k+1} .

Démonstration. - De façon évidente, toute chaîne décomposable $u_1 , \dots , u_{k+1}$, allant d'un irréductible u_1 à un irréductible u_{k+1}, satisfait, pour tout $i = 1 , \dots , k$, $u_i \longmapsto u_{i+1}$. Nous avons ainsi (C2) $\Rightarrow$ (C1).

Réciproquement, soient $f , g \in X^*$ tels que $f \overset{*}{\longleftrightarrow} g$. Construisons, tant que cela est possible, la suite $f_1 = f , f_2 , \dots , f_{k+1}$ en prenant, pour tout $i = 1 , \dots , k$, $f_{i+1} \in \{h \mid f_i \longrightarrow h\}$. Cette construction s'arrête quand on arrive a un mot f_{k+1} tel que $\{h \mid f_{k+1} \longrightarrow h\} \neq \emptyset$; autrement dit, f_{k+1} est irréductible.

De la même façon, on construit la suite $g_1 = g , g_\ell , \dots , g_{\ell+1}$, telle que $g_1 \longrightarrow g_2 \longrightarrow \dots \longrightarrow g_{\ell+1}$, et $g_{\ell+1}$ est irréductible. Il est immédiat que f_{k+1} et $g_{\ell+1}$ sont congrus dans $\overset{*}{\longleftrightarrow}$. D'où, par (C1), $f_{k+1} \overset{*}{\longmapsto} g_{\ell+1}$ et, par suite, il existe une suite $h_1 = f_{k+1} , h_2 , \dots , h_{m+1} = g_{\ell+1}$ telle que, pour tout $i = 1 , \dots , m$, $h_i \longmapsto h_{i+1}$.

La suite $f_1 , f_2 , \dots , f_k , h_1 , \dots , h_{m+1} , g_\ell , g_{\ell-1} , \dots , g_1$ est bien une chaîne décomposable allant de f en g. Ainsi (C1) $\Rightarrow$ (C2), et le lemme est établi.

Remarque 1. - La démonstration du lemme 1 fournit un algorithme pour décider, étant donnés f et g dans X^*, si $f \overset{*}{\longleftrightarrow} g$ ou non. En effet, étant donnés les irréductibles f_{k+1} et $g_{\ell+1}$, on sait décider si $f_{k+1} \overset{*}{\longmapsto} g_{\ell+1}$ ou non, puisque, s'il existe une chaîne d'irréductibles $h_1 , \dots , h_{m+1}$ allant de f_{k+1} à $g_{\ell+1}$, il en existe une de longueur inférieure à

$$(\underset{\sim}{\text{card}}\ X)^{|f_{k+1}|} .$$

Démonstration du théorème 1. - Il suffit de montrer que (C3) $\Rightarrow$ (C1). On considère pour cela une chaîne $u_1 , \dots , u_{k+1}$, allant de $f = u_1$ en $g = u_{k+1}$, où f et g sont supposés irréductibles, et on suppose de plus $|f| \geqslant |g|$.

- Ou bien, pour tout $i = 2 , \dots , k + 1$, $|u_i| \leqslant |u_1|$,

- Ou bien il existe un $i \geqslant 2$, tel que $|u_i| > |u_1|$.

1er cas. - Ou bien pour tout $i = 1 , \dots , k$, $u_i \longmapsto u_{i+1}$, et il n'y a rien à démontrer ; ou bien il existe un indice h tel que, pour tout $i = 1 , \dots , h - 1$, $u_i \longmapsto u_{i+1}$ et $u_h \longrightarrow u_{h+1}$. Mais, par (C3), il existe une chaîne décomposable allant de u_{h-1} à u_{h+1}, ce qui implique qu'il existe v_{h-1} tel que $u_{h-1} \longrightarrow v_{h-1}$ (v_{h-1} est le deuxième élément de la chaîne décomposable en question). Répétant l'argument, on peut trouver v_{h-2} tel que $u_{h-2} \longrightarrow v_{h-2}$ en considérant une chaîne décomposable allant de u_{h-2} à v_{h-1}. On construit ainsi une suite de mots $v_1 , v_2 , \dots , v_{h-1}$ telle que, pour tout $i = 1 , \dots , h - 1$, $u_i \longrightarrow v_i$. Mais l'hypothèse d'irréductibilité de u_1 entraîne qu'il n'existe pas v_1 tel que $u_1 \longrightarrow v_1$. C'est donc que, dans la suite $u_1 , \dots , u_{k+1}$, il n'existe pas d'indice h tel que $u_h \longrightarrow u_{h+1}$, et l'on a bien $f \overset{*}{\longmapsto} g$.

2e cas. - Montrons qu'il existe une chaîne allant de f à g, de hauteur infé-

rieure strictement à la hauteur de $u_1, \ldots, u_{k+1}$. La hauteur de $u_1, \ldots, u_{k+1}$ est égale à $\max\{|u_i| \mid i = 1, \ldots, k+1\}$. Considérons alors h minimum tel que $|u_h|$ soit maximum : il existe certainement aussi ℓ tel que

$$u_h \vdash\!\dashv u_{h+1} \vdash\!\dashv \ldots \vdash\!\dashv u_\ell \ , \quad u_\ell \rightarrow u_{\ell+1} \ ,$$

et l'on a, par définition, $u_h \rightarrow u_{h-1}$.

Par (C3), il existe une chaîne décomposable allant de u_{h-1} à u_{h+1} dont nous désignerons l'avant-dernier élément par v_{h+1}. Certainement $u_{h+1} \rightarrow v_{h+1}$, et tout élément de la chaîne est de longueur strictement inférieure à $|u_{h+1}| = |u_h|$.

De la même façon, il existe une chaîne décomposable allant de v_{h+1} à u_{h+2}, telle que, si v_{h+2} désigne l'avant-dernier élément, $u_{h+2} \rightarrow v_{h+2}$, et tout élément de la chaîne est de longueur strictement inférieure à $|u_{h+2}| = |u_h|$. Poursuivant cette construction, on construit v_{h+1}, v_{h+2}, ..., v_ℓ tels qu'il existe une chaîne allant de u_{h-1} à v_ℓ dont tous les éléments sont de longueur inférieure à $|u_h|$ et $u_\ell \rightarrow v_\ell$.

Il ne reste plus qu'à remplacer la chaîne de longueur 2 $v_\ell \leftarrow u_\ell \rightarrow u_{\ell+1}$ par une chaîne décomposable allant de v_ℓ à $u_{\ell+1}$ pour obtenir une chaîne allant de f en g et de hauteur strictement inférieure à celle de $u_1, \ldots, u_{k+1}$.

Le théorème 1 a un important corollaire.

COROLLAIRE 1. - Il existe un algorithme pour décider, étant donné un système Σ, s'il est quasi-parfait ou non.

Démonstration. - Soit S l'ensemble des chaînes de la forme (u, abc, v) où (u, ab) et (bc, v) appartiennent à $\Sigma \cup \Sigma^{-1}$ et $b \neq 1$. L'ensemble S est manifestement fini puisque Σ l'est, et pour chaque chaîne (u, abc, v) de S, on peut décider s'il existe une chaîne décomposable allant de u en v (par la remarque 1). Notre corollaire découle ainsi du lemme suivant.

LEMME 2. - Σ est quasi-parfait si, et seulement si,

(C4) Pour toute chaîne de S, soit (u, abc, v), il existe une chaîne décomposable allant de u en v.

Démonstration. - Toute chaîne de longueur 2 non décomposable (h_1, h_2, h_3) est telle que

$$h_2 = \alpha_1 a_1 \beta_1 = \alpha_3 a_3 \beta_3$$

$$h_1 = \alpha_1 b_1 \beta_1 \ , \qquad h_3 = \alpha_3 b_3 \beta_3 \ ,$$

où (a_1, b_1) et (a_3, b_3) éléments de $\Sigma \cup \Sigma^{-1}$ satisfont

$$\text{soit} \quad |a_1| = |b_1| \ , \quad |a_3| > |b_3| \ ,$$

$$\text{soit} \quad |a_1| > |b_1| \ , \quad |a_3| \geq |b_3| \ .$$

Or, si $|\alpha_1| \geqslant |\alpha_3\, a_3|$, nous pouvons écrire

$$h_2 = \alpha_3\, a_3\, \alpha_2\, a_1\, \beta_3$$

et il est clair que, si $h'_2 = \alpha_3\, b_3\, \alpha_2\, b_1\, \beta_1$, la chaîne (h_1 , h'_2 , h_3) est une chaîne décomposable allant de h_1 en h_3 . En effet, $h_1 = \alpha_3\, b_3\, \alpha_2\, a_1\, \beta_1$ et $h_3 = \alpha_3\, a_3\, \alpha_2\, b_1\, \beta_1$. Le même phénomène se passe si $|\alpha_3| \geqslant |\alpha_1\, a_1|$.

Autrement dit, quand a_1 et a_3 ne se chevauchent pas, la condition (C3) est trivialement vérifiée.

Si au contraire a_1 et a_3 se chevauchent, il est clair qu'il existe α , β tels que $h_1 = \alpha u \beta$, $h_2 = \alpha f \beta$ et $h_3 = \alpha v \beta$ pour quelque chaîne $(u , f , v) \in S$, et l'existence d'une chaîne décomposable $u_1 , \ldots , u_{k+1}$ allant de u en v entraîne l'existence d'une chaîne décomposable $\alpha u_1 \beta , \ldots , \alpha u_{k+1} \beta$ allant de h_1 en h_3 . Ainsi $(C4) \Rightarrow (C3)$, et le lemme 2 est établi, ainsi que le corollaire.

COROLLAIRE 2. - Il existe un algorithme pour décider, étant donné un système Σ , s'il est parfait ou non.

Démonstration. - Σ est parfait $\Longleftrightarrow \Sigma$ est quasi-parfait, et il n'existe pas de couple $(f , g) \in \Sigma$, f et g irréductibles et de même longueur.

En effet, s'il existe $(f , g) \in \Sigma$, $|f| = |g|$, f et g irréductibles, Σ n'est pas quasi-parfait. Si réciproquement, Σ est quasi-parfait sans être parfait, il existe au moins deux irréductibles congrus h et h' , tels que $h \overset{*}{\longmapsto} h'$: ce qui impose l'existence de $(f , g) \in \Sigma$, $|f| = |g|$, où f est facteur de h , donc irréductible. Σ étant quasi-parfait, g est alors aussi irréductible.

COROLLAIRE 3. - Il existe un algorithme pour décider, étant donnés deux systèmes Σ et Σ' , si les deux congruences qu'ils engendrent sont identiques (Nous disons alors que Σ et Σ' sont équivalents).

Démonstration. - Le corollaire résulte de la remarque 1. En effet, la congruence $\overset{*}{\underset{\Sigma}{\longleftrightarrow}}$ est plus fine que la congruence $\overset{*}{\underset{\Sigma'}{\longleftrightarrow}}$ (c'est-à-dire, pour tout f , g

$$f \overset{*}{\underset{\Sigma}{\longleftrightarrow}} g \Rightarrow f \overset{*}{\underset{\Sigma'}{\longleftrightarrow}} g\ ),$$

si, et seulement si, pour tout $(a , b) \in \Sigma$, on a $a \overset{*}{\underset{\Sigma'}{\longleftrightarrow}} b$, et il existe un algorithme pour en décider puisque Σ est fini.

On décide de la même façon si $\overset{*}{\underset{\Sigma'}{\longleftrightarrow}}$ est plus fine que $\overset{*}{\underset{\Sigma}{\longleftrightarrow}}$. En fait, nous avons une propriété plus forte qui fait l'objet du paragraphe suivant : il est possible, étant donné un système Σ , de construire un système Σ' équivalent, revêtant une forme canonique telle que deux systèmes sous forme canonique sont équivalents si, et seulement si, ils sont égaux.

4. Systèmes précanoniques.

Définitions. - Le mot $f \in X^*$ est dit primitif dans Σ si, et seulement si,

pour tout α , β , u , v ,

$$f = \alpha u \beta \quad \text{et} \quad u \longrightarrow v \Rightarrow \alpha = \beta = 1 \ .$$

Nous dirons que la chaîne u_1 , ... , u_{k+1} de Σ , allant de f en g , utilise le couple (u , v) de Σ si, et seulement si, il existe $i \in \{1 , \dots , k\}$, $\alpha , \beta \in X^*$, tels que $u_i = \alpha u \beta$, $u_{i+1} = \alpha v \beta$ ou $u_i = \alpha v \beta$, $u_{i+1} = \alpha u \beta$.

Nous appelons couple homogène de longueur n de Σ , tout couple $(f , g) \in \Sigma$ tel que $|f| = |g| = n$. Le couple homogène (f , g) de Σ est dit essentiel si, et seulement si, toute chaine décomposable, allant de f en g dans Σ , utilise un couple homogène de longueur $|f| = |g|$: on remarque immédiatement que cette condition implique que f et g soient irréductibles. Si u_1 , ... , u_{k+1} est une chaîne décomposable de Σ , allant de f en g , pour un couple essentiel (f , g) , il existe $i \in \{1 , \dots , k\}$ tel que (u_i , u_{i+1}) où (u_{i+1} , u_i) est un couple de Σ .

Nous dirons enfin que le système quasi-parfait Σ est précanonique si, et seulement si,

1° Les couples homogènes de Σ sont tous essentiels.

2° Les couples inhomogènes (f , g) , où $|f| \neq |g|$, ont comme composante de plus grande longueur un mot primitif.

LEMME 3. - Si Σ est un système quasi-parfait, il existe un système précanonique Σ' contenu dans Σ et équivalent à Σ . Il existe un algorithme pour calculer un tel système Σ' , Σ étant donné.

Démonstration. - Supposons que (f , g) soit un couple homogène de Σ et que (f , g) ne soit pas essentiel. Montrons que le système $\Sigma' = \Sigma \setminus \{(f , g)\}$ est quasi-parfait et équivalent à Σ .

L'équivalence est immédiate car, si (f , g) n'est pas essentiel, il existe une chaîne décomposable de Σ allant de f en g , et n'utilisant pas de couple homogène de longueur $n = |f| = |g|$. En particulier, cette chaîne n'utilise pas le couple (f , g) , et c'est donc aussi une chaîne de Σ' . Il s'ensuit que $f \overset{*}{\underset{\Sigma'}{\longleftrightarrow}} g$ et immédiatement l'équivalence de Σ et Σ' .

Remarquons maintenant que les deux ensembles $\mathrm{Irr}(\Sigma)$ et $\mathrm{Irr}(\Sigma')$ de mots irréductibles dans Σ et Σ' sont identiques. En effet, si h $\mathrm{Irr}(\Sigma)$ était réductible dans Σ' , il existerait un mot h' plus court que h tel que $h \overset{*}{\underset{\Sigma}{\longleftrightarrow}} h'$, et ceci implique h réductible dans Σ , qui est quasi-parfait.

Inversement, " $h \in \mathrm{Irr}(\Sigma')$ et h réductible dans Σ " implique qu'il existe un couple (u , v) de $\Sigma \cup \Sigma^{-1}$, $|u| > |v|$ et $\alpha , \beta \in X^*$ tels que $h = \alpha u \beta$. Le couple (u , v) appartenant aussi à $\Sigma' \cup \Sigma'^{-1}$, h est réductible dans Σ' .

Il reste à montrer que, pour tout couple d'irréductibles, $(h , h') \in \mathrm{Irr}(\Sigma')$,

$$h \overset{*}{\underset{\Sigma'}{\longleftrightarrow}} h' \Rightarrow h \overset{*}{\underset{\Sigma'}{\longmapsto}} h' \ .$$

Clairement,

$$h \overset{*}{\underset{\Sigma'}{\longleftrightarrow}} h' \Rightarrow h \overset{*}{\underset{\Sigma}{\longleftrightarrow}} h' \Rightarrow h \overset{*}{\underset{\Sigma}{\longmapsto}} h'$$

il existe donc une chaîne décomposable allant de h en h' dans Σ, n'utilisant que des couples homogènes. Si cette chaîne n'utilise pas (f , g), c'est aussi une chaîne de Σ', et donc $h \overset{*}{\underset{\Sigma}{\longmapsto}} h'$. Si elle utilise (f , g), on substitue à chaque maillon utilisant (f , g), une chaîne n'utilisant que des couples homogènes de longueur inférieure à $|f| = |g|$, chaîne qui existe puisque (f , g) n'est pas essentiel. La chaîne ainsi obtenue est une chaîne de Σ' et $h \overset{*}{\underset{\Sigma'}{\longmapsto}} h'$. Le système Σ' est quasi-parfait.

Supposons maintenant que $\Sigma \cup \Sigma^{-1}$ contienne un couple (f , g), où $|f| > |g|$ et f n'est pas primitif. Nous considérons comme ci-dessus

$$\Sigma' = \Sigma \setminus \{(f , g) , (g , f)\} .$$

Le mot f n'étant pas primitif, il existe α, β, u, v tels que $f = \alpha u \beta$, $\alpha\beta \neq 1$ et $u \underset{\Sigma}{\longrightarrow} v$. Σ étant quasi-parfait, il existe une chaîne décomposable de Σ allant de $\alpha v \beta$ en g, chaîne qui n'utilise pas le couple (f , g) puisque tous ses éléments sont de longueur strictement inférieure à $|f|$. C'est donc aussi une chaîne de Σ' et, puisque (u , v) $\Sigma' \cup \Sigma'^{-1}$, on en déduit $f \overset{*}{\underset{\Sigma'}{\longleftrightarrow}} g$. L'équivalence de Σ et Σ' en découle immédiatement.

Nous avons comme ci-dessus $\mathrm{Irr}(\Sigma) = \mathrm{Irr}(\Sigma')$ (trivialement), et, si h, h' sont deux irréductibles de Σ' tels que $h \overset{*}{\underset{\Sigma'}{\longleftrightarrow}} h'$, nous avons aussi $h \overset{*}{\underset{\Sigma}{\longleftrightarrow}} h'$, donc $h \overset{*}{\underset{\Sigma}{\longmapsto}} h'$ et $h \overset{*}{\underset{\Sigma'}{\longmapsto}} h'$, puisque Σ et Σ' contiennent les mêmes couples homogènes.

Finalement, en supprimant dans Σ soit un couple homogène inessentiel, soit un couple inhomogène dont la plus longue composante n'est pas primitive, on obtient un système Σ' quasi-parfait et équivalent à Σ. Il est clair que l'on peut recommencer l'opération sur Σ', et ainsi de suite jusqu'à trouver une partie de Σ qui ne contient plus de tels couples. C'est le système précanonique équivalent à Σ cherché.

Q. E. D.

5. Systèmes canoniques.

Définition. - Le système quasi-parfait Σ est dit canonique si, et seulement si,

1° $(f , g) \in \Sigma \Rightarrow (g , f)$ Σ,

2° $(f , g) \in \Sigma$, $g \overset{*}{\underset{\Sigma}{\longleftrightarrow}} h$, $|f| > |g|$ et $|f| > |h| \Rightarrow (f , h) \in \Sigma$.

3° $(f , g) \in \Sigma$, $g \overset{*}{\underset{\Sigma}{\longmapsto}} h$, $|f| = |g| = |h|$ et (f , h) essentiel $\Rightarrow (f,h) \in \Sigma$.

4° Tout couple homogène de Σ est essentiel.

5° Pour tout couple inhomogène (f , g) de Σ, $|f| > |g| \Rightarrow f$ primitif.

THÉORÈME 2. - Au vu du lemme 1, on peut supposer Σ précanonique.

Pour obtenir Σ' canonique et équivalent à Σ on rajoute des couples formés en vertu des règles 1°, 2°, 3°,

- si $(f , g) \in \Sigma$, $g \overset{*}{\underset{\Sigma}{\leftrightarrow}} h$, $|f| > |g|$ et $|f| > |h|$, le couple (f , h) rajouté satisfait bien la condition 5° ;

- si $(f , g) \in \Sigma$, $g \overset{*}{\underset{\Sigma}{\vdash\!\dashv}} h$, $|f| = |g| = |h|$, il peut se faire que le couple (f , h) soit inessentiel s'il existe une chaîne de Σ allant de f à h et n'utilisant que des couples homogènes de longueur strictement inférieure à $|f| = |g|$. Mais on peut décider si c'est le cas avant de rajouter (f , h) à Σ . Procédant ainsi, en rajoutant les couples un à un, on obtiendra un système canonique au bout d'un temps fini puisque le nombre de couples que l'on peut rajouter est fini, chacun d'entre eux ayant comme composante de plus grande longueur la composante d'un couple de Σ .

THÉORÈME 3. - Deux systèmes canoniques sont équivalents si, et seulement si, ils sont identiques.

Démonstration. - Supposons Σ équivalent à Σ' . Soit $(f , g) \in \Sigma$, $|f| > |g|$. Il existe une chaîne décomposable allant de f en g dans Σ' soit $u_1 = f$, $u_2 , \dots , u_{k+1} = g$. Supposons que (f , u_2) n'appartienne pas à Σ' . Il existe alors α , β , u , v tels que $f = \alpha u \beta$, $\alpha\beta \neq 1$, $(u , v) \in \Sigma'$ et $|u| > |v|$. Mais $(u , v) \in \Sigma' \Rightarrow u \overset{*}{\underset{\Sigma}{\leftrightarrow}} v$, et l'existence d'une chaîne décomposable $v_1 = u$, $v_2 , \dots , v_{\ell+1} = v$, allant de u en v dans Σ , montre que u est réductible dans Σ , ce qui contredit le fait que f soit primitif puisque u est un facteur propre de f .

Nous avons donc $(f , u_2) \in \Sigma'$, mais aussi (f , g) en vertu de la condition 2.

Soit maintenant $(f , g) \in \Sigma$, (f , g) homogène de longueur n . Le couple (f , g) étant essentiel, f et g sont irréductibles dans Σ , et donc aussi dans Σ' (évidemment). D'où l'existence d'une chaîne décomposable $u_1 = f$, $u_2 , \dots , u_{k+1} = g$, allant de f en g dans Σ' , et n'utilisant que des couples homogènes de Σ' . Si cette chaîne n'utilise que des couples homogènes de longueur strictement inférieure à n , soient $\{(h_i , k_i) \mid i \in I\}$, il existe aussi dans Σ une chaîne décomposable allant de f en g et n'utilisant que des couples homogènes de longueur strictement inférieure à n . En effet,

$$(h_i , k_i) \in \Sigma' \Rightarrow h_i \overset{*}{\underset{\Sigma}{\vdash\!\dashv}} k_i ,$$

et toute chaîne allant de h_i à k_i dans Σ ne peut contenir que des mots de longueur strictement inférieure à n . Ceci contredit le fait que (f , g) est essentiel dans Σ .

Nous savons ainsi qu'il existe un $i \in \{1 , \dots , k\}$ tel que $(u_i , u_{i+1}) \in \Sigma'$. Prenons le plus petit. Si (u_i , g) n'était pas essentiel dans Σ' , on montrerait,

par l'argument ci-dessus, que (f , g) ne serait pas essentiel dans Σ contrairement à l'hypothèse, et de même si (f , g) n'était pas dans Σ' .

Nous avons ainsi montré que $\Sigma \subset \Sigma'$. En inversant les rôles parfaitement symétriques de Σ et Σ' , on montre $\Sigma' \subset \Sigma$, et donc $\Sigma = \Sigma'$.

Q. E. D.

6. Conclusion.

Les systèmes parfaits et quasi-parfaits générateurs de congruence posent certainement plus de problèmes que nous n'en avons résolus. Trouver des conditions assurant l'algébricité des classes, et étudier les propriétés des ensembles algébriques ainsi obtenus, ce qui était le but initial, fait l'objet des travaux d'Yves COCHET. Etudier la décidabilité de quelques problèmes classiques sur les monoïdes quotient d'un monoïde libre, quand la congruence en question est parfaite ou quasi-parfaite, fait l'objet des travaux de Michèle BENOIS. Le rôle des congruences parfaites dans un certain nombre de questions de théorie des langages et d'algorithmique a été mis en lumière par Philippe BUTZBACH : il s'agit de l'équivalence des grammaires simples et de celle des schémas récursifs libres. De nombreuses questions demeurent ouvertes. Signalons le problème suivant :

Existe-t-il un algorithme pour décider de l'égalité de deux classes de congruences parfaites ou quasi-parfaites ?

Nous conjecturons une réponse positive.

BIBLIOGRAPHIE

[1] BENOIS (Michèle). - Systèmes finis, Grenoble 1972 (multigraphié).

[2] BUTZBACH (P.). - Une famille de congruences de Thue pour lesquelles le problème de l'équivalence est décidable. Application à l'équivalence des grammaires séparées, "Automata, languages and programming", Proceedings of a symposium [1972. Rocquencourt], p. 3-12. - Amsterdam, North Holland publishing Company, 1973.

[3] COCHET (Y.). - Thèse 3e cycle, Math., Rennes 1971.

[4] COCHET (Y.) et NIVAT (M.). - Une généralisation des ensembles de Dyck, Israel J. of Math., t. 9, 1971, p. 389-395.

[5] NIVAT (M.). - On some families of languages related to the Dyck set, "Second annual symposium on theory of Computing" [1970. Northampton], p. 221. - New York, Association for Computing Machinery, 1970.

Maurice NIVAT
9 rue Portalis
75008 PARIS