Séminaire Dubreil.
Algèbre et théorie
des nombres

Gordon B. Preston

Les congruences dans les demi-groupes abéliens et libres

Séminaire Dubreil. Algèbre et théorie des nombres, tome 15, n° 2 (1961-1962), exp. n° 17, p. 1-6

<http://www.numdam.org/item?id=SD_1961-1962__15_2_A6_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
15e année, 1961/62, n° 17

2 avril 1962

LES CONGRUENCES DANS LES DEMI-GROUPES ABÉLIENS ET LIBRES

par Gordon B. PRESTON

Cet exposé a pour but de donner quelques résultats fondamentaux de L. RÉDEI. RÉDEI a écrit un livre sur les congruences dans les demi-groupes abéliens et libres avec un nombre fini de générateurs. Ce livre paraîtra bientôt. Je veux exposer quelques résultats de ce livre que L. RÉDEI a annoncés dans une conférence, faite à Oxford, en mai 1961.

Considérons un demi-groupe abélien et libre F avec n générateurs. On peut supposer que F est l'ensemble de toutes les séquences $(a_1 , a_2 , \dots , a_n)$ de n nombres entiers non-négatifs, avec une opération d'addition définie par

$$(a_1 , a_2 , \dots , a_n) + (b_1 , b_2 , \dots , b_n)$$

$$= (a_1 + b_1 , a_2 + b_2 , \dots , a_n + b_n) \quad .$$

La relation $\leq$ sur F définie par

$$(a_1 , a_2 , \dots , a_n) \leq (b_1 , b_2 , \dots , b_n)$$

si et seulement si $a_i \leq b_i$, pour $i = 1 , 2 , \dots , n$, est un ordre partiel sur F . De plus, avec cet ordre partiel, F devient un treillis.

Si $\alpha = (a_1 , a_2 , \dots , a_n)$ et $\beta = (b_1 , b_2 , \dots , b_n)$, on a :

$$\alpha \cup \beta = (a_1 \cup b_1 , a_2 \cup b_2 , \dots , a_n \cup b_n)$$

et

$$\alpha \cap \beta = (a_1 \cap b_1 , a_2 \cap b_2 , \dots , a_n \cap b_n) \quad ,$$

où $a_i \cup b_i$ signifie le maximum de a_i et b_i et où $a_i \cap b_i$ signifie le minimum de a_i et b_i .

Soit A un sous-ensemble de F . L'élément α de F est appelé <u>élément minimal de</u> A si $\beta < \alpha$ implique $\beta \notin A$.

Nous commençons par une proposition sur les idéaux de F. Un ensemble H de générateurs de l'idéal I est appelé une base pour I si aucun sous-ensemble propre de H n'engendre I.

LEMME 1. - Supposons que I soit un idéal de F. Alors, il existe une base unique pour I et cette base est finie. La base pour I consiste en tous les éléments minimaux de I.

Démonstration. - L'ensemble de tous les éléments minimaux de I est un ensemble fini pour un sous-ensemble quelconque I de F. Nous démontrerons ce résultat par induction sur le nombre n de générateurs de F. Evidemment le résultat est vrai pour $n = 1$. Supposons qu'on l'ait déjà démontré pour les demi-groupes abéliens et libres à $(n - 1)$ générateurs. Considérons l'ensemble des nombres entiers qui sont les j-ièmes composants des éléments de I, et notons par ℓ_j le plus petit de ces nombres. Notons par I_j l'ensemble de tous les éléments de I pour lesquels la j-ième composante est égale à ℓ_j. D'après l'hypothèse d'induction, l'ensemble M_j, de tous les éléments minimaux de I_j, est fini. Ecrivons

$$M = M_1 \cup M_2 \cup \ldots \cup M_n \quad .$$

Soit m_j le plus grand de tous les j-ièmes composants de l'ensemble (fini) M et posons $\mu = (m_1, m_2, \ldots, m_n)$. Alors, chaque élément de M est au plus égal à μ.

Notons par N_j l'ensemble de tous les éléments minimaux de I pour lesquels le j-ième composant p_j satisfait à la condition $\ell_j \leq p_j \leq m_j$. De l'hypothèse de l'induction résulte que chaque ensemble N_j est fini. Par conséquent

$$N = N_1 \cup N_2 \cup \ldots \cup N_n$$

est également fini. Supposons que $\gamma = (c_1, c_2, \ldots, c_n)$ soit un élément minimal quelconque de I. Alors on a $\gamma \in N$, ou $c_j > m_j$ pour $j = 1, 2, \ldots, n$. Le second cas est impossible, parce que, dans ce cas, on a $\mu < \gamma$ et par conséquent chaque élément de l'ensemble non vide M est plus petit que γ. Ainsi, N est un ensemble fini constitué par tous les éléments minimaux de I.

Il est facile de voir que N est la base unique de I.

COROLLAIRE. - Les idéaux de F satisfont à la condition de chaîne ascendante.

Soit G le groupe abélien et libre avec n générateurs lequel contient F. On peut considérer que G est l'ensemble de toutes les suites de n nombres entiers avec une addition définie par l'addition des composants.

On peut étendre l'ordre partiel sur F à un ordre partiel sur G avec $\alpha \geqslant \beta$ dans G si et seulement si $\alpha - \beta \geqslant 0$ dans F. Avec cet ordre, G devient un groupe réticulé. Nous définissons μ^+ et μ^- par

$$\mu^+ = \mu \cup 0 \quad ,$$

$$\mu^- = (-\mu) \cup 0 \qquad (\mu \in G) \quad .$$

Puis nous avons :

$$\mu = \mu^+ - \mu^- \quad ,$$

$$\mu \cup \nu = (\mu - \nu)^+ + \nu = (\nu - \mu)^+ + \mu$$

$$\mu \cap \nu = \mu - (\mu - \nu)^+ = \nu - (\nu - \mu)^+ \quad .$$

Maintenant, supposons que ρ est une congruence sur F, et définissons M_ρ par

$$M_\rho = \{(\alpha - \beta) : (\alpha , \beta) \in \rho\} \quad . \tag{1}$$

Il est facile de voir que M_ρ est un sous-groupe de G. Chaque élément μ de M_ρ détermine un idéal $f_\rho(\mu)$ de F défini par :

$$f_\rho(\mu) = \{\xi : (\xi + \mu^+ , \xi + \mu^-) \in \rho\} \quad . \tag{2}$$

LEMME 2. - Supposons que ρ soit une congruence sur F et que M_ρ et $f = f_\rho$ sont définis par (1) et (2). Alors, pour μ, ν quelconques de M_ρ, f a les propriétés :

C(i) $$f(o) = F \quad ;$$

C(ii) $$f(\mu) = f(-\mu) \quad ;$$

C(iii) $$(\mu^+ + f(\mu)) \cap (\nu^+ + f(\nu)) \subseteq (\mu \cup \nu) + f(\mu - \nu) \quad .$$

Démonstration. - Nous avons les propriétés C(i) et C(ii) parce que ρ est réflexive et symétrique.

Pour démontrer C(iii), considérons ξ dans l'ensemble $(\mu^+ + f(\mu)) \cap (\nu^+ + f(\nu))$. Par la définition même de $f(\mu)$, $\xi \in \mu^+ + f(\mu)$ si et seulement si $(\xi , \xi - \mu^+ + \mu^-) \in \rho$, c'est-à-dire, $(\xi , \xi - \mu) \in \rho$. De la même manière, $(\xi , \xi - \nu) \in \rho$. Posons

$$\eta = \xi - (\mu \cup \nu) \quad .$$

Il faut démontrer que $\eta \in f(\mu - \nu)$, c'est-à-dire que

$$(\eta + (\mu - \nu)^+ , \eta + (\mu - \nu)^-) \in \rho \quad .$$

Mais on calcule aisément :

$$\eta + (\mu - \nu)^+ = \xi - \nu \quad ,$$

et

$$\eta + (\mu - \nu)^- = \xi - \mu \quad ;$$

d'où le résultat, car $(\xi , \xi - \nu) \in \rho$ et $(\xi , \xi - \mu) \in \rho$ entraînent $(\xi - \nu , \xi - \mu) \in \rho$.

Nous considérons maintenant un sous-groupe quelconque M, de G, et une application f de M dans l'ensemble de tous les idéaux de F de sorte que f satisfait aux conditions C(i) à C(iii). Dans ce cas nous dirons que (f , M) est une paire de congruence de F.

Chaque paire de congruence $C = (f , M)$ détermine une relation $\rho = \rho(C)$ sur F définie ainsi :

$$(3) \qquad \rho = \rho(C) = \{(\alpha , \beta) : \alpha , \beta \in F , \alpha - \beta \in M \text{ et } \alpha \cap \beta \in f(\alpha - \beta)\} \quad .$$

LEMME 3. - Supposons que (f , M) soit une paire de congruence. Alors ρ, définie par (3), est une congruence sur F.

Démonstration. - Si $\alpha \in F$, alors $\alpha \cap \alpha = \alpha \in f(\alpha - \alpha) = f(o)$, parce que $f(o) = F$, en vertu de la condition C(i). Ainsi ρ est réflexive. De la condition C(ii) il résulte que $f(\alpha - \beta) = f(\beta - \alpha)$ quand $\alpha - \beta \in M$; par conséquent ρ est symétrique. Supposons que $(\alpha , \beta) \in \rho$ et que $\xi \in F$. Alors, on a

$$(\alpha + \xi) \cap (\beta + \xi) = (\alpha \cap \beta) + \xi \quad ;$$

car, $f(\alpha - \beta)$ étant un idéal de F, $(\alpha + \xi , \beta + \xi) \in \rho$. Ainsi ρ est une

relation régulière.

Il faut démontrer que ρ est aussi transitive. Considérons $(\alpha , \beta) \in \rho$ et $(\beta , \gamma) \in \rho$. Puis, $\alpha - \beta \in M$ et $\beta - \gamma \in M$, d'où $\alpha - \gamma \in M$. D'ailleurs $\alpha \cap \beta \in f(\alpha - \beta)$ et $\beta \cap \gamma \in f(\beta - \gamma)$, c'est-à-dire :

$$\beta - (\beta - \alpha)^+ \in f(\alpha - \beta) = f(\beta - \alpha) \quad ,$$

et

$$\beta - (\beta - \gamma)^+ \in f(\beta - \gamma) \quad .$$

D'où

$$\beta \in ((\beta - \alpha)^+ + f(\beta - \alpha)) \cap ((\beta - \gamma)^+ + f(\beta - \gamma)) \quad .$$

Ainsi, en utilisant la condition C(iii), on obtient :

$$\beta \in ((\beta - \alpha) \cup (\beta - \gamma)) + f(\alpha - \gamma) \quad .$$

Par suite,

$$\beta = \beta - \alpha + ((\beta - \gamma) - (\beta - \alpha))^+ + \eta \quad ,$$

où $\eta \in f(\alpha - \gamma)$. On en déduit :

$$\eta = \alpha - (\alpha - \gamma)^+ = \alpha \cap \gamma \quad .$$

Par conséquent, $\alpha \cap \gamma \in f(\alpha - \gamma)$ et $(\alpha , \gamma) \in \rho$. Ainsi ρ est transitive.

Nous avons démontré qu'une congruence quelconque ρ sur F détermine une paire de congruence (f_ρ , M_ρ) et que, réciproquement, chaque paire de congruence $\mathcal{C} = (f , M)$ détermine une congruence $\rho(\mathcal{C})$ sur F. Cette correspondance entre les congruences et les paires de congruence est, au fait, une relation biunivoque.

THÉORÈME. - L'application $\rho \to (f_\rho , M_\rho)$ définie par (1) et (2) est une application biunivoque de l'ensemble de toutes les congruences sur F sur l'ensemble de toutes les paires de congruence de F. L'application réciproque (de cette application) est $\mathcal{C} = (f , M) \to \rho(\mathcal{C})$, définie par (3).

Démonstration. - Écrivons $\mathcal{C} = (f_\rho , M_\rho)$. Nous démontrerons que $\rho(\mathcal{C}) = \rho$. Du fait que chacune des deux conditions $(\alpha , \beta) \in \rho$ et $(\alpha , \beta) \in \rho(\mathcal{C})$ entraîne que $\alpha - \beta \in M_\rho$, il suffit, pour la démonstration, de montrer que $(\alpha , \beta) \in \rho$ si et seulement si $\alpha \cap \beta \in f_\rho(\alpha - \beta)$, c'est-à-dire que $(\alpha , \beta) \in \rho$ si et seulement si

$$(\alpha \cap \beta + (\alpha - \beta)^+ \ , \ \alpha \cap \beta + (\alpha - \beta)^-) \in \rho \quad .$$

On voit immédiatement que cette propriété est vraie car :

$$\alpha \cap \beta + (\alpha - \beta)^+ = \alpha \quad \text{et} \quad \alpha \cap \beta + (\alpha - \beta)^- = \beta \quad .$$

Réciproquement, supposons que $\mathfrak{C} = (f \ , M)$ est une paire de congruence quelconque de F et posons $\rho = \rho(\mathfrak{C})$. Il faut démontrer que $f_\rho = f$ et que $M_\rho = M$. Evidemment $M_\rho \subseteq M$. Soit μ un élément de M . Puis, comme $f(\mu)$ est un idéal de F , on peut trouver un élément φ de F de sorte que

$$(\mu^+ + \varphi) \cap (\mu^- + \varphi) = (\mu^+ \cap \mu^-) + \varphi \in f(\mu) \quad .$$

Ainsi, il existe un élément φ de F pour lequel $(\mu^+ + \varphi \ , \ \mu^- + \varphi) \in \rho$, et, par conséquent,

$$\mu = (\mu^+ + \varphi) - (\mu^- + \varphi) \in M_\rho \quad .$$

Ainsi, $M \subseteq M_\rho$. D'où, $M = M_\rho$.

Pour un élément μ de M , $\xi \in f_\rho(\mu)$ si et seulement si $(\xi + \mu^+ \ , \ \xi + \mu^-) \in \rho$, c'est-à-dire, si et seulement si

$$(\xi + \mu^+) \cap (\xi + \mu^-) \in f(\xi + \mu^+ - \xi - \mu^-) = f(\mu) \quad ;$$

c'est-à-dire, si et seulement si

$$\xi = \xi + (\mu^+ \cap \mu^-) \in f(\mu) \quad .$$

Ainsi, $f = f_\rho$, et la démonstration du théorème est terminée.

Dans sa conférence à Oxford, L. RÉDEI a indiqué beaucoup d'autres résultats sur ce sujet. Il a dit que, dans son livre, il a obtenu une détermination complète de toutes les congruences sur F .