ARKIV FÖR MATEMATIK Band 4 nr 41

Communiqué le 10 Janvier 1962

Remarques sur les groupes abéliens infinis admettant une base finie

Par TRYGVE NAGELL

1. Nous désignerons par A, B et C des éléments de groupes abéliens infinis, par a, b, c, d, f, g, u et v des nombres entiers rationnels et par i, j, m, q, r et s des nombres naturels. It faut d'abord préciser certaines notions, à propos des groupes abéliens infinis, que nous allons employer. Rappelons aussi de quelques faits simples au sujet de ces groupes.

Soit $\mathfrak{G}$ un groupe abélien infini. La composition des éléments dans $\mathfrak{G}$ sera désignée par le symbole d'addition $+$. Supposons qu'il existe dans $\mathfrak{G}$ un nombre fini d'éléments $A_1, A_2, \ldots, A_s$ tels qu'un élément quelconque C dans $\mathfrak{G}$ peut être généré de la manière suivante

$$C = c_1 A_1 + c_2 A_2 + \ldots + c_s A_s,$$

$c_1, c_2, \ldots, c_s$ étant des nombres entiers rationnels. Alors le système $A_1, A_2, \ldots, A_s$ sera appelé un *système générateur* de $\mathfrak{G}$, et nous désignerons le groupe par $\mathfrak{G}(A_1, A_2, \ldots, A_s)$. Ce système s'appelle une *base* du groupe quand le nombre s a sa valeur minimum. Alors il est bien connu que tout sous-groupe de $\mathfrak{G}$ admet aussi une base finie; voir p. ex. [1][1], p. 39–41. Nous allons, entre autres, donner une precision de ce résultat.

Pour simplifier nous considérons seulement les groupes abéliens *purs* (on dit aussi: *sans torsion*). Ainsi tous les éléments sont d'ordre infini, excepté l'élément-unité. Les éléments $A_1, A_2, \ldots, A_m$ du groupe pur G (distincts de l'élément-unité) sont dits *indépendants* entre eux quand la relation

$$a_1 A_1 + a_2 A_2 + \ldots + a_m A_m = 0$$

ne peut subsister que pour $a_1 = a_2 = \ldots = a_m = 0$; dans le cas contraire ceux-ci sont dits *dépendants* entre eux. Rappelons aussi les faits suivants: Pour que le système générateur $A_1, A_2, \ldots, A_r$ de $\mathfrak{G}$ constitue une base de $\mathfrak{G}$ il faut et il suffit que les éléments $A_1, A_2, \ldots, A_r$ soient indépendants. Le nombre d'éléments dans une base sera appelé le *rang* de $\mathfrak{G}$. Le rang est le nombre maximum d'éléments indépendants. Si r est le rang le système générateur $A_1, A_2, \ldots, A_r$ est une base. Pour les démonstrations nous renvoyons à [2], [3] ou [4].

[1] Les numéros figurant entre crochets renvoient à l'Index bibliographique placé à la fin de cette note.

2. Nous allons d'abord établir le résultat suivant:

Théorème 1. *Soit* **G** *un groupe abélien infini pur admettant la base finie* $A_1, A_2, \ldots, A_r$, *et soit* **U** *un sous-groupe de* **G**. *Pour certaines valeurs de* i $(1 \leqslant i \leqslant r)$ *il y a des éléments dans* **U** *de la forme*

$$C_i = a_1 A_1 + a_2 A_2 + \ldots + a_i A_i,$$

où $a_1, a_2, \ldots, a_i$ *sont des entiers rationnels et* $a_i \neq 0$. *Désignons par* b_{ii} *la plus petite valeur positive de* a_i *qui est possible quand les nombres* $a_1, a_2, \ldots, a_i$ *varient librement de façon que l'élément* C_i *appartienne à* **U**. *Soit, pour les valeurs de* i *en question,*

$$B_i = b_{i1} A_1 + b_{i2} A_2 + \ldots + b_{ii} A_i \tag{1}$$

un élément dans **U**, b_{i1}, b_{i2} *etc. étant des entiers rationnels. Alors les éléments* B_i *constituent un système générateur de* **U**. *Si* q *est le rang de* **U** *on a* $q \leqslant r$.

Démonstration. Si C est un élément quelconque de **U** on a

$$C = a_1 A_1 + a_2 A_2 + \ldots + a_r A_r.$$

Supposons que $a_r = a_{r-1} = \ldots = a_{m+1} = 0$ tandis que $a_m \neq 0$. Alors l'élément B_m du théorème 1 existe, et en vertu de la définition de b_{ii} il est évident que a_m est divisible par b_{mm}. En effet, en posant $a_m = c_m b_{mm} + d$, où $0 \leqslant d < b_{mm}$, on aura

$$C - c_m B_m = a_1' A_1 + a_2' A_2 + \ldots + a_{m-1}' A_{m-1} + d A_m.$$

Vu que $C - c_m B_m$ appartient à **U**, on a nécessairement $d = 0$. De la même manière on montre que a_{m-1}' (si $\neq 0$) est divisible par $b_{m-1,\,m-1}$. En continuant ce procédé on aura évidemment

$$C = \sum_i c_i B_i,$$

la somme étant étendue à toutes les valeurs i pour lesquelles B_i est défini. Le théorème 1 se trouve ainsi démontré. Nous allons y ajouter le résultat suivant:

Théorème 2. *Les éléments* B_i *dans le théorème* 1 *constituent une base de* **U**.

Démonstration. Il suffit de montrer que les éléments B_i sont indépendants entre eux. Supposons qu'on ait

$$\sum_i u_i B_i = 0, \tag{2}$$

et que $u_i = 0$ pour $i > m$ tandis que $u_m \neq 0$. En introduisant les valeurs de B_i données par (1) dans (2), nous obtenons une relation de la forme

$$\Sigma v_i A_i = 0,$$

où $v_i = 0$ pour $i > m$ tandis que $v_m = u_m b_{mm} \neq 0$. Or cela est impossible vu que les éléments $A_1, A_2, \ldots, A_m$ sont indépendants.

3. Si dans le théorème 1 le sous-groupe **U** a le même rang r que **G**, les éléments B_i ainsi que les nombres b_{ti} sont définis pour toutes les valeurs $i = 1, 2, \ldots, r$. Dans ce cas nous aurons le resultat suivant:

Théorème 3. *Supposons que le sous-groupe* **U** *dans le théorème* 1 *a le rang* r *et que les* r *éléments*

$$B_i = b_{i1} A_1 + b_{i2} A_2 + \ldots + b_{ii} A_i \tag{3}$$

constituent une base de **U**. *Alors on peut supposer qu'on a, pour* $1 \leqslant j \leqslant i-1$,

$$0 \leqslant b_{ij} < b_{jj}. \tag{4}$$

Il n'y a qu'une seule $B_1, B_2, \ldots, B_r$ *de* **U** *qui satisfait aux conditions* (4).

Démonstration. En divisant $b_{i,i-1}$ par $b_{i-1,i-1}$ on aura

$$b_{i,i-1} = f b_{i-1,i-1} + g,$$

où $0 \leqslant g < b_{i-1,i-1}$. Alors il est evident que, dans la base $B_1, B_2, \ldots, B_r$, l'élément B_i peut être remplacé par

$$B_i - f B_{i-1} = c_1 A_1 + c_2 A_2 + \ldots + c_{i-2} A_{i-2} + g A_{i-1} + a_{ii} A_i.$$

Ici on peut, d'une manière analogue, réduire le nombre c_{i-2} ($\text{si} \neq 0$) modulo $b_{i-2,i-2}$. En continuant ce procédé on voit que B_i peut être choisi tel que les inégalités (4) soient remplies.

Il reste à montrer qu'il n'y a aucune autre base $B_1', B_2', \ldots, B_r'$ de **U** qui satisfait aux conditions (4). En effet, supposons qu'on ait, pour $i = 1, 2, \ldots, r$,

$$B_i' = b_{i1}' A_1 + b_{i2}' A_2 + \ldots + b_{ii}' A_i,$$

où $0 \leqslant b_{ij}' < b_{jj}'$. Vu que les b_{ti} sont déterminés d'une manière unique on a, pour tous les i, $b_{ii}' = b_{ii}$. Alors la «différence»

$$B_i - B_i' = (b_{i1} - b_{i1}') A_1 + \ldots + (b_{i,i-1} - b_{i,i-1}') A_{i-1}$$

est un élément de **U**. Ici on a évidemment, en tenant compte des inégalités (4),

$$|b_{i,i-1} - b_{i,i-1}'| < b_{i-1,i-1}.$$

En vertu de la définition de $b_{i-1,i-1}$ il en résulte que $b_{i,i-1} = b_{i,i-1}'$. En continuant de cette manière on arrivera à la conclusion que $b_{ij} = b_{ij}'$ pour toutes les valeurs de i et j. Ainsi on a $B_{ij} = B_{ij}'$. Le théorème 3 se trouve donc démontré.

Les résultats que nous venons d'établir ont fait, depuis plus de trente ans, partie de mes cours sur la théorie des groupes. Ils sont, entre autres, très utiles pour les calculs numériques avec les nombres algébriques; voir p. ex. [5] et [6], p. 354.

INDEX BIBLIOGRAPHIQUE

1. HECKE, E., Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig 1923.
2. FUCHS, L., Abelian groups, Budapest 1958.
3. KUROSCH, A. G., Gruppentheorie, Berlin 1953.
4. KAPLANSKY, I., Infinite abelian groups, Ann Arbor 1954.
5. NAGELL, T., Die Bestimmung der Ringe mit gegebener Diskriminante in einem algebraischen Zahlkörper, Norsk Matematisk Forenings Skrifter, Ser. II, Nr. 9, Oslo 1933.
6. NAGELL, T., Sur quelques questions dans la théorie des corps biquadratiques, Arkiv f. matematik, Bd 4, Nr. 26. Stockholm 1961.

Tryckt den 13 juni 1962

Uppsala 1962. Almqvist & Wiksells Boktryckeri AB