Чехословацкий математический журнал, т. 7 (82) 1957, Прага

10

# LES ANNEAUX NE CONTENANT QUE DES SOUS-ANNEAUX PROPRES CYCLIQUES

F. SZÁSZ, Debrecen (Hongrie).

(Reçu le 10 février 1956.)

L'auteur détermine tous les anneaux ayant la propriété suivante: Tous les sous-anneaux propres d'un tel anneau sont des anneaux cycliques. (Voir le théorème). Ici anneau cyclique signifie un anneau dont le groupe additif est cyclique.

L'auteur obtient comme corollaire de son théorème le résultat suivant: Un groupe abélien qui ne contient que des sousgroupes propres cycliques est ou cyclique lui-même, ou possède l'ordre $p^2$, ou est du type $p^\infty$.

Nous avons déterminé dans un travail antérieur [4] (voir la bibliographie à la fin de cet article) tous les anneaux $R$ qui ne possèdent pas d'autres sous-anneaux que les anneaux $nR$, $nR$ étant l'ensemble des éléments $nr$, $r \in R$, $n$ un nombre entier. Cette classe des anneaux est formée par l'ensemble des anneaux cycliques. Nous appelons *anneau cyclique* chaque anneau associatif $R$, dont le groupe additif $R^+$ est cyclique. Nous avons traité deux autres problèmes du même genre dans les travaux [5] et [6]. Le présent travail est consacré à un troisième problème.

Un anneau $R$ est appelé *l'anneau ayant la propriété* A, si tous ses sous-anneaux propres $S$ sont cycliques. Par exemple l'anneau des nombres entiers rationnels a la propriété A.

Nous allons démontrer le théorème suivant:

**Théorème.** *Les anneaux cycliques, l'anneau zéro construit au-dessus du groupe additif quasi-cyclique du type $p^\infty$, les corps finis de l'ordre $p$ et $p^q$ et les anneaux de l'ordre $p^2$ constituent l'ensemble de tous les anneaux ayant la propriété* A. *(Ici $p$, $q$ sont deux nombres premiers.)*

Remarque. Avant la démonstration élémentaire de ce théorème nous démontrerons d'abord quelque lemmes. (Quant aux notions les plus importantes de l'algèbre moderne je renvoie le lecteur par exemple aux livres [1], [2] et [3].)

La conséquence immédiate du théorème est le corollaire suivant:

*Un groupe abélien qui ne contient que des sousgroupes propres cycliques est ou cyclique lui-même, ou possède l'ordre $p^2$ ou est du type $p^\infty$.*

**Lemme 1.** *Un anneau $R$ dont le groupe additif $R^+$ est mixte ne possède pas la propriété* A.

Démonstration. Si $R^+$ était mixte, le sous-anneau $T$ des éléments d'ordre fini serait un sous-anneau cyclique, engendré par un élément $t \in T$, et il existerait un plus petit nombre naturel $n$ pour lequel $nT = \{0\}$. Par conséquent $nR$, étant un sous-anneau propre dans $R$, est cyclique et engendré par un élément $nr$, $n \in J$, $r \in R$ d'ordre infini. Les équations $t^2 = mt$, $tr = kt$ et $(nr)^2 = l(nr)$ sont évidemment vraies pour des nombres convenables, $m, k, l \in J$. Le sous-anneau $\{t, s\}$ engendré par un élément $t$ d'ordre fini et par un élément $s$ d'ordre infini, ne peut pas être cyclique. Il en suit $\{t, nr\} = \{t, 2nr\} = R$. On obtient de ces faits que $nr = at + b(2nr)$, $a, b \in J$, c'est-à-dire $at = (1 - 2b)\, nr$ ce qui est en vertu de $\mathfrak{O}(t) = n$, $\mathfrak{O}(r) = \infty$ $n \neq 0$, $b \in J$ impossible.

**Lemme 2.** *Un anneau $R$ sans diviseurs de zéro, ayant propriété $A$, est un corps premier $K_p$ ou un anneau cyclique ou bien un corps d'ordre $p^q$, $p$ et $q$ étant des nombres premiers.*

Démonstration. S'il existe un élément $0 \neq a \in R$ tel que $a \,.\, R \neq R$, le sous-anneau $aR$ doit être cyclique. En ce cas la correspondence $r \to ar$, $(r \in R)$ est un isomorphisme du groupe additif $R^+$ sur son sousgroupe $(aR)^+$, c'est-à-dire $R$ lui-même est cyclique.

Si l'on a $aR = R$ pour chaque élément $a \neq 0$, $a \in R$, l'anneau $R$ est un corps, comme il est bien connu. Parce que le groupe additif des nombres rationnels n'est pas cyclique, $R$ doit avoir la caractéristique $p$. Mais parmi les corps de caractéristique $p$ seulement le corps premier $K_p$ est un anneau cyclique. $R$ ne doit avoir alors d'autres sous-corps propres que le corps premier $K_p$. Il en suit d'abord que $R$ ne peut contenir d'éléments transcendants par rapport à $K_p$ et on en déduit ensuite aisément que $R$ est soit le corps premier $K_p$ lui-même, soit un surcorps fini commutatif d'ordre $p^q$, où $p$ et $q$ sont des nombres premiers.

**Lemme 3.** *Un anneau $R$ de caractéristique 0, dont le groupe additif est algébriquement fermé,*[1]) *ne peut pas avoir la propriété* A.

Démonstration. De la théorie des groupes abéliens algébriquement fermés on déduit que un tel groupe n'est pas cyclique. D'après le lemme 2 on peut trouver dans $R$ des éléments $a \neq 0$, $b \neq 0$ tels que $ab = 0$. On ne peut pas avoir simultanément $aR = R$, $bR = R$ à cause de $\{0\} = abR = aR = R$. On peut trouver alors dans $R$ des éléments $r$ tels que $rR \neq R$. Mais le groupe

[1]) A. G. Kuroš appelle un tel groupe „groupe complet", Irving Kaplansky, a divisible group". C'est un groupe abélien $G$, dans lequel chaque équation $nx = a$ possède des solutions pour chaque $a \in G$ et pour chaque nombre naturel $n$.

$(rR)^+$ est aussi algébriquement fermé: $n(rR) = r(nR) = rR$. Par conséquent dans le cas $rR \neq \{0\}$, $rR$ n'est pas cyclique. Il en suit $rR = \{0\}$. L'ensemble $Z$ de tous les éléments $r' \in R$, ayant la propriété $r'R = \{0\}$, n'est pas vide. On démontre assez facilement que $Z$ est un sous-anneau zéro de $R$ et que $Z^+$ est aussi algébriquement fermé. Par conséquent il faut que $R = Z$ et $R$ soit un anneau zéro. Mais dans un anneau zéro $R$ chaque sousgroupe de son groupe additif $R^+$ engendre un sous-anneau. Par conséquent $R^+$ qui est algébriquement fermé, c'est-à-dire une somme directe des groupes additifs des nombres rationnels, n'a pas la propriété A.

Démonstration du théorème. À cause du lemme 1 le groupe additif $R^+$ de $R$ n'est pas mixte. Si $R^+$ contient un élément $x \neq 0$ d'ordre infini, on tire du lemme 1 et du lemme 3 l'existence d'un nombre naturel $n$ tel que $nR \neq R$. En ce cas $nR$ doit être cyclique. Parce que $R^+$ est un groupe sans éléments d'ordre fini, la correspondence $r \to nr$ est un isomorphisme entre $R^+$ et son sousgroupe cyclique $(nR)^+$. Or le groupe $R^+$ doit être cyclique, lui-même.

Soit maintenant $R$ un anneau ayant la propriété A qui ne contient que des éléments d'ordre fini.

$R$ est donc, en raison de la théorie des anneaux, la somme directe de ses $p$-composants et le nombre de ces $p$-composants différents de zéro est à cause de la propriété A, nécessairement fini. Si la somme directe contient plusieurs $p$-composants différents, $R$ est un anneau cyclique. Dans le cas contraire il est un $p$-anneau $R = R_p$.

Dans l'anneau $R$ tous les éléments d'ordre $p$ constituent un sous-anneau $R^*$. Maintenant il faut distinguer deux cas.

Dans le premier cas, où $R^* \neq R$, $(R^*)^+$ est un groupe cyclique d'ordre $p$ et l'équation $p^k x = r$, $r \in R^*$, $r \neq 0$, est ou n'est pas résoluble dans $R$ simultanément pour tous les éléments $r \in R^*$, $r \neq 0$. Supposons d'abord que cette équation est résoluble pour tous les nombres naturels $k = 1, 2, 3, \ldots$ On tire de la théorie des groupes abéliens primaires que $R^+ \cong C(p^\infty)$. Donc $R^+$ est algébriquement fermé et si l'on a $aR \neq \{0\}$, le sous-anneau $aR$ doit être aussi algébriquement fermé. Par conséquent on a $aR = R$ ou $aR = \{0\}$ pour chaque $a \in R$. Mais le premier cas est impossible, parce que $(aR)^+$ ne contient que des éléments d'ordre $p^n$ au plus, $p^n$ étant l'ordre de l'élément $a$. On a alors $aR = \{0\}$ pour tous les $a \in R$, d'où $R^2 = \{0\}$. $R$ est donc l'anneau zéro construit sur le groupe quasi-cyclique $C(p^\infty)$ comme son groupe additif.

Supposons ensuite que l'équation $p^k x = r$, $r \in R^*$, $r \neq 0$ soit résoluble dans $R$, mais l'équation $p^{k+1} y = r$ ne le soit pas. Choisissons l'élément $c$ dans $R$ de la manière qu'on ait $p^k c = r$. Donc, il n'existe pas dans $R$ un élément $r$ tel que $pr = c$, c'est-à-dire $c$ non $\in pR$. Nous allons démontrer que le groupe cyclique $C'$ engendré par $c$ coïncide avec $R^+$. Supposons $C' \neq R^+$. Dans ce cas il existe un élément $s \in R$, $s$ non $\in C'$ tel que $ps = mc \in C'$ avec un $m \in J$ convenable.

Si l'on avait $(m, p) = 1$, la congruence $mx \equiv 1 \pmod{p^{k+1}}$ aurait une solution $x$ dans $J$ et on en tirerait $c = xps$ ce qui n'est pas compatible avec $c$ non $\epsilon pR$. Par conséquent on a $m = pm_1$ et on peut écrire $ps = pm_1c$, $p(s - m_1c) = 0$. L'élément $s_1 = s - m_1c$ non $\epsilon C$, c'est-à-dire $s_1 \neq 0$. $s_1$ est donc d'ordre $p$, $s_1 \epsilon R^*$. Nous pouvons alors poser $s_1 = lr$ avec un $l \epsilon J$. On en déduit $s_1 = s - m_1c = lp^kc$, c'est-à-dire $s = m_1c + lp^kc$ ce qui est contraire à la supposition $s$ non $\epsilon C$. Nous avons alors démontré $C = R^+$.

Dans le second cas nous avons $R^* = R$. $R$ est alors un $p$-anneau élémentaire. $R$ ayant la propriété A, chaque sous-anneau propre $R'$ de $R$ qui n'est pas zéro doit avoir l'ordre $p$: $\mathfrak{O}(R') = p$. À cause du lemme 2 on conclut que $R$ possède des diviseurs de zéro. Soit alors $a \neq 0$, $b \neq 0$, $ab = 0$ dans $R$. Supposons d'abord $\{a\} = R$, $\{b\} = R$. On a donc $R^2 = \{0\}$. Il en suit $\mathfrak{O}(R) = p$. Supposons ensuite $\{a\} \neq R$, $\{b\} = R$. Dans ce cas $R$ est commutatif et $\{a\}$ est un idéal dans $R$ à cause de $\{a\}R = \{0\}$. $R$ n'ayant que sous-anneaux propres d'ordre $p$, on a $\mathfrak{O}\{a\} = p$ et l'anneau facteur $R/\{a\}$ ne possède pas d'ideaux propres et de sous-anneaux propres, sauf le sous-anneau et l'idéal zéro. Si l'on désigne par $B$ la classe de $R/\{a\}$ qui contient l'élément $b$, $R/\{a\}$ est engendré par $B$. Si $R/\{a\}$ n'a pas de diviseurs de zéro, $R/\{a\}$ doit être le corps premier de caractéristique $p$. Dans le cas contraire il faut que $B^2 = 0$ et $R/\{a\}$ est un anneau zéro. Par conséquent on a dans tous les deux cas $\mathfrak{O}(R/\{a\}) = p$ et $\mathfrak{O}(R) = p^2$.

Supposons enfin que pour tous les diviseurs de zéro $a \neq 0$, $b \neq 0$, $ab = 0$ on ait $\{a\} \neq R$, $\{b\} \neq R$. Ici il faut examiner de nouveau deux cas. Si l'on a pour tous les diviseurs de zéro $a \neq 0$, $b \neq 0$, $ab = 0$, $\{a\} \cap \{b\} \neq \{0\}$, il faut que $\{a\} = \{b\}$, parce que $\mathfrak{O}(\{a\}) = \mathfrak{O}(\{b\}) = p$. On en tire $a^2 = 0$. Dans ce cas $Ra = R$ est impossible, parce que, autrement $R = (Ra)a = \{0\}$. $Ra = \{0\}$ signifie que $R$ est un anneau zéro d'ordre $p$. Il nous reste le cas $0 \neq Ra \neq R$. $Ra$ est alors cyclique et on voit aisément qu'on peut écrire $Ra = \{ra\}$ avec un $r \epsilon R$ convenable. Mais $ra$ et $a$ étant deux diviseurs de zéro $raa = 0$, on a $Ra = \{a\}$. On peut répéter les même considérations pour $aR$ et on voit que $\{a\}$ est un idéal bilatéral dans $R$. Nous en concluons comme tout-à-l'heure que $R/\{a\}$ possède l'ordre $p$ et que $R$ lui-même est d'ordre $p^2$.

Dans le second cas deux diviseurs de zéro $a \neq 0$, $b \neq 0$ existent dans $R$ tels, que $ab = 0$, $\{a\} \cap \{b\} = \{0\}$. $\{a\}$, $\{b\}$ ayant l'ordre $p$, on a $a^2 = ma$, $b^2 = nb$ avec $m$, $n \epsilon J$ convenables et on peut écrire $R = \{a\} + \{b\} + \{ba\}$ avec $(ba)^2 = 0$. La somme n'est pas nécessairement directe. L'anneau $R_1 = \{a, ba\}$ a l'ordre $p$ ou $R_1 = R$. Si $\mathfrak{O}(R_1) = p$, on a $R_1 = \{a\}$, $ba \epsilon \{a\}$, c'est-à-dire $R = \{a\} + \{b\}$ et $\mathfrak{O}(R) = p^2$. Si $R_1 = R$, on peut écrire $b = n_1a + n_2ba$ avec $n_1, n_2 \epsilon J$ convenables. De $\{a\} \cap \{b\} = \{0\}$ il suit $(p, n_2) = 1$. La congruence $n_2x \equiv 1 \mod p$ étant résoluble, on a $ba \epsilon \{a\} + \{b\}$, donc $R = \{a\} + \{b\}$ et $\mathfrak{O}(R) = p^2$.

Pour résummer: Un anneau arbitraire, ayant le propriété A, appartient aux catégories des anneaux énumérées dans le théorème. Inversement il est clair que chacun de ceux anneaux possède la propriété A.

## BIBLIOGRAPHIE


[1] *А. Г. Курош:* Теория групп, Москва, 1953.

[2] *G. Pickert:* Einführung in die höhere Algebra, Göttingen, 1951.

[3] *L. Rédei:* Algebra I, Budapest, 1954.

[4] *F. Szász:* On rings every subring of which is a multiple of the ring, Publ. Math. Debrecen, *4* (1956), 237–238.

[5] *F. Szász:* On groups every cyclic subgroup of which is a power of the group, Acta. Math. Acad. Sci. Hungar *6* (1955), 475–477.

[6] *F. Szász:* On groups every non-trivial power of which is cyclic, A Magyar Tudományos Akadémia Matematikai és Fizikai Osztályának Közleményei. V. *4* (1955), 491 à 492.

[7] *T. Szele:* On direct decomposition of abelian groups, Journal of the London Math. Soc., Vol. *28* (1953), 247–250.


## Резюме

### О КОЛЬЦАХ, СОДЕРЖАЩИХ ТОЛЬКО ЦИКЛИЧЕСКИЕ СОБСТВЕННЫЕ ПОДКОЛЬЦА


Ф. САС (F. Szász), Дебрецен, Венгрия.



(Поступило в редакцию 10/II 1956 г.)



В настоящей заметке доказана следующая

**Теорема.** *Произвольное кольцо $R$ обладает свойством* A (*т. е. любое собственное подкольцо $S$ кольца $R$ циклично*), *тогда и только тогда, если $R$ циклично, или $R$ является нуль-кольцом, построенным на аддитивной группе $C(p^\infty)$, или кольцом порядка $p^2$, или конечным полем порядка $p^q$* ($p$ *и* $q$ *простые числа*).

Как следствие этой теоремы автор получает следующий результат:

*Абелева группа, содержащая только циклические собственные подгруппы является или сама циклической группой или группой порядка $p^2$ или группой типа $p^\infty$.*