

Sous-groupes du cercle unité (fgn analyse 1 page 29)

Pierre Lissy

April 29, 2010

Lemme 1. *Les sous-groupes de $\mathbb{R}$ sont soit de la forme $a\mathbb{Z}$ soit denses.*

Proof. Considérons $a = \inf \{x \in G \cap \mathbb{R}^{+*}\}$. De deux choses l'une

1. $a > 0$. Alors $a \in G$. En effet, si $a \notin G$, alors comme $2a > a$, par définition de la borne inférieure, il existe un $x \in G$ tel que $a < x < 2a$. De plus, il existe $a < y < x$ avec $y \in A$ encore une fois par définition de la borne inférieure. Dans ce cas, on a $x - y \in G \cap \mathbb{R}^{+*}$ et $x - y < 2a - y < 2a - a < a$, ce qui n'est pas possible compte tenu de la définition de a . Ainsi, on a $a \in G$. Donc on a déjà $a\mathbb{Z} \subset G$. Supposons qu'il existe un élément $x \in G$ avec $x \notin a\mathbb{Z}$. Alors comme $a > 0$ il existe un certain entier n tel que $na < x < (n+1)a$. Mais $x \in G$ et $na \in G$ donc $x - na \in G$, de plus, on a $0 < x - na < a$, ce qui n'est pas possible par hypothèse. On a donc bien $G = a\mathbb{Z}$.
2. $a=0$. Montrons alors que G est dense. Il suffit par exemple de montrer qu'il rencontre tout intervalle ouvert de la forme (a, b) . mais $(b-a) > 0$ donc il existe $g \in G$ tel que $0 < g < b-a$. Mais on sait que $g\mathbb{Z} \subset G$, et comme il existe nécessairement un k tel que $kg \in (a, b)$ (sinon on aurait $g > b-a$), on a bien l'intersection non vide que l'on souhaitait.

□

Lemme 2. *Le sous-groupe $a\mathbb{Z} + b\mathbb{Z}$ est dense ssi a/b irrationnel.*

Proof. Supposons $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$. Alors notamment, $a = cu$ et $b = cv$ avec u et v entiers donc $a/b = u/v$ est rationnel. Inversément, supposons $a/b = u/v$ avec u et v entiers premiers entre eux. Alors $a\mathbb{Z} + b\mathbb{Z} = b(u/v\mathbb{Z} + \mathbb{Z}) = bv(u\mathbb{Z} + v\mathbb{Z}) = bv\mathbb{Z}$ car u et v sont premiers entre eux (théorème de Bézout). Donc on a bien $A\mathbb{Z} + b\mathbb{Z}$ de la forme $c\mathbb{Z}$. □

On peut maintenant conclure. Soit G un sous-groupe de U . On considère l'ensemble suivant: $G' = \{t \in \mathbb{R} | e^{it} \in G\}$. C'est un sous-groupe additif de $\mathbb{R}$ car il contient trivialement 0 et que si t et t' sont tels que e^{it} et $e^{it'} \in G$ alors $e^{i(t+t')} = e^{it}e^{it'} \in G$. De plus, l'application $t \in G' \mapsto e^{it}$ in G' est surjective, car on sait que tout élément de G s'écrit sous la forme $e^{i\theta}$, et alors par définition $\theta \in G'$. On disjuncte alors les cas.

1. G' est dense dans $\mathbb{R}$. Alors par continuité de l'application $t \mapsto e^{it}$ on a que $e^{iG'}$ est dense dans $e^{i\mathbb{R}} = U$, mais la remarque précédente a montré que $e^{iG'} = G$ donc G est dense dans U .
2. G' est de la forme $a\mathbb{Z}$, avec $a \geq 0$. Si $a = 0$ on obtient le groupe trivial. Sinon choisissons $a > 0$ et disjunctons encore les cas.
 - (a) $a/(2\pi)$ n'est pas rationnel. On remarque alors que $e^{iG'} = e^{a\mathbb{Z} + 2i\pi\mathbb{Z}}$ et par la remarque faite précédemment, $a\mathbb{Z} + 2i\pi\mathbb{Z}$ est dense dans $\mathbb{R}$, donc son image par le morphisme continu précédent est dense dans U , ie G est dense dans U .
 - (b) $a/(2\pi)$ est rationnel. On a $a = 2\pi p/q$ avec p et q premiers entre eux. On remarque alors que si $n \in \mathbb{Z}$, en effectuant la division euclidienne de n par q , on a $n = qb + r$ avec $r < q$ et $e^{ian} = e^{2i\pi p/q(qb+r)} = e^{2\pi pr}$. Ainsi, on a une surjection de $e^{iG'} = G$ dans l'ensemble des entiers compris entre 0 et $q-1$, qui est fini. Ceci implique que G est fini, de cardinal inférieur à q . De plus, il n'est pas difficile de voir que $G = U_q$. En effet, comme p et q sont premiers entre eux, on a existence de u et v tels que $pu + qv = 1$, ie $pu/q + v = 1/q$. Donc $e^{iua} = e^{2i\pi/q} \in G$, or le groupe engendré par cet élément est de cardinal q . Donc G est de cardinal q est égal à U_q .