Divers

Marc SAGE

Table des matières

1 sg matriciel et relation entre cosinus

est-ce que qqn saurait montrer que $1+2\cos\frac{2\pi}{n}$ ne peut pas etre de la forme $2\cos\left(2\pi\frac{p}{q}\right)$ avec p et q entiers, et $n\neq 6$?

Ma motivation pour ca est qu'un Type Fort (tm) m'a affirme que le groupe engendre par les matrices $S=\begin{pmatrix} a & 0 \\ 1 & 1 \end{pmatrix}$ et $T=\begin{pmatrix} 1 & -a \\ 0 & a \end{pmatrix}$ où $a=e^{\frac{2\pi i}{n}}$ avait pour $n\neq 6$ un element simple a decrire au moyen des generateurs qui etait d'ordre infini (rem : $S^n=1$, $T^n=1$, $(ST)^{3n}=1$). Le premier candidat est ST^{-1}. Si j'ecris que cet element est d'ordre fini (i.e. ses valeurs propres sont des racines de 1), j'obtiens sauf erreur l'egalite de $1+2\cos\frac{2\pi}{n}$ et de $2\cos\left(2\pi\frac{p}{q}\right)$

ivan, qui ne sait pas si ce qui precede est facile ou non

11 avri 2000 13h53

p.s. pour $n\leq 5$, le groupe engendre est d'ordre fini

2 groupes diédral et éléments d'ordre 2

if G is generated by order 2 elements s and t then G = <st> semidirect product <s> par l'action "prendre l'inverse"

Let G = <s,t> with |<s>| = |<t>| = 2, so that s = s^{-1} and
t = t^{-1}. Then G = <s,st> and s(st)s^{1} = ts = (st)^{-1}, so
<st> is normal in G, and [s,st] <> 1 unless |<st>| = 2 (or 1) ; in
any case <s> /\ <st> = 1, so G is the semidirect product
G = <st> x| <s> ~= C_|<st>| x| C_2 with dihedral action.

3 Sur les faux épi

$f:A\longrightarrow B$ est un népi si $\forall X,\ \mathrm{Hom}\,(X,A)\twoheadrightarrow\mathrm{Hom}\,(X,B)$, ie si

$$\begin{tikzcd} X \arrow[d, dotted, "\exists"'] \arrow[dr, "\forall"] & \\ A \arrow[r] & B \end{tikzcd}$$

Montrons (ou essayons...) que cela équivaut à morhisme surjectif.

Soit $f:A\longrightarrow B$ népi dans ensemble. On applique à $\mathrm{Id}_B : X\longrightarrow B$: il y a un $g:B\longrightarrow A$ tq $fg=\mathrm{Id}$, d'où g surjectif.

$$\begin{tikzcd} B \arrow[d, dotted, "\exists"', "g"] \arrow[dr, "\mathrm{Id}"] & \\ A \arrow[r] & B \end{tikzcd}$$

Soit $f:A\twoheadrightarrow B$ dans ensemble. Par AC, il y une section $s:B\longrightarrow A$, et on l'utilise pour compléter

$$\begin{tikzcd} X \arrow[dr, "g"] & \\ A & B \arrow[l, "s"] \end{tikzcd}$$

CONCLUSION : dans ENS, népi = surj.

Soit $f:G\longrightarrow H$ népi dans groupes. Montrons que f surj. On applique pareil à Id_H.

Soit $f:G\twoheadrightarrow H$ dans groupes. MOntrns que c'eest népi.

CONTRE EXEMPLE : si $\begin{tikzcd} Z/2Z \arrow[d, dotted, "\exists"', "\psi"] \arrow[dr, "\varphi"] & \\ Z \arrow[r, two heads, "f"] & Z/4Z \end{tikzcd}$, $0=\psi(2)=2\psi(1)$ d'où $\psi=0$ et $\varphi=0$.

4 Sur les vrais épi

pourquoi épi = surj ?

5 Nombres de sous-groupes d'un groupe ?

Des sous-$\mathbb{Q}$-espaces vectoriels, il y en a déjà pas mal, non ?

Bon, je vais sûrement dire plein de conneries comme à chaque fois que je poste sur ce forum, mais je crois que cet argument fin et subtil se généralise à tous les groupes commutatifs indénombrables.

Donc on prend G un groupe commutatif. On note G_{tor} sa porte de torsion et on a la suite exacte :

0 -> G_{tor} -> G -> G/G_{tor} -> 0

Comme G est infini, un de deux groupes G_{tor} ou G/G_{tor} a même cardinal que G, et donc il suffit de traiter les deux cas suivants :

1) G est de torsion

2) G est sans torsion

Commençons par le premier. Dans ce cas, je note G_n la partie de n-torsion. La réunion de tous les G_n est G et donc au moins l'un des G_n a le même cardinal que G (puisque G est supposé indénombrable).

Je prends un tel n et je prends p un diviseur premier de n. Si G_p n'a pas le même cardinal que G, l'image de la multiplication par p dans G_n s'identifie au quotient G_n/G_p et donc on construit ainsi un sous-groupe de G_n tué par n/p de même cardinal que G. Sinon, G_p est un sous-groupe de G de même cardinal que G tué par p.

Ainsi, on arrive à construire un sous-groupe de G de même cardinal que G tué par un nombre premier p. C'est alors un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel et on utilise le même argument fin et subtil que dans le cas de $\mathbb{R}$ pour conclure.

Si maintenant G est sans torsion, je regarde G' $= G \otimes_{\mathbb{Z}} \mathbb{Q}$. G s'injecte alors dans G', disons via φ qui à g associe $g \otimes 1$. Et donc $G\prime$ est un $\mathbb{Q}$-espace vectoriel de dimension le cardinal de G. Si $_{A\prime}$ est un sous espace vectoriel de $G\prime$, on pose $A := \varphi^{-1}(A')$ et on vérifie que l'on peut retrouver $A\prime$ à partir de A simplement en faisant $A \otimes_{\mathbb{Z}} \mathbb{Q}$.

Ainsi l'ensemble des sous-espaces vectoriels de $G\prime$ s'injecte dans l'ensemble des sous-groupes de G. Le cardinal du premier ensemble est le même que celui de $\mathfrak{P}(G)$, et donc il en est de même de l'ensemble des sous-groupes de G.

Bon, en conclusion l'ensemble des sous-groupes de G quand G est commutatif est toujours celui de $\mathfrak{P}(G)$. Sauf erreur :-) .

6 Groupe dual

Pour un groupe abelien infini tu n'as clairement plus equipotence entre les deux ($\mathrm{Hom}(\mathbb{Z}, \mathbb{C}^*) = \mathbb{C}^*$ qui n'est pas vraiment pareil que $\mathbb{Z}$), mais comme il t'a deja ete repondu cela ne gene pas le fait que, pour tout element non nul x d'un groupe abelien A il existe un morphisme de A dans $\mathbb{C}^*$ tel que x n'est pas dans le noyau.

La preuve est trivale si A est finiment engendre : alors A est la somme directe d'une partie libre $\mathbb{Z}^n$ et d'une partie de torsion finie ; pour un element de torsion tu travailles sur la partie de torsion qui est finie (le resultat y est d'ailleurs aussi relativement trivial), pour un element pas de torsion tu ne travailles que sur la partie libre et le probleme de trouver n nombres complexes non nuls tels qu'un produit donne de ces nombres (correspondnt a la decomposition de x dans la base canonique de $\mathbb{Z}^n$) soit different de 1, ce qui est clairement trivial.

Denis Auroux, 3 fév 02, 3h51

Groumpf !

La reponse est oui, j'ai eu la flemme de poster la demo en detail la derniere fois, je vais donc le faire maintenant.

Si χ est un caractere, $\chi\left(aba^{-1}b^{-1}\right) = \chi(a)\,\chi(b)\,\chi(a)^{-1}\,\chi(b)^{-1} = 1$ donc $D(G)$ est inclus dans tous les noyaux des caracteres.

Inversement je note $A = G/D(G)$. C'est un groupe abelien (par la propriete universelle de $D(G)$). Soit y un element de G qui n'est pas dans $D(G)$, et x la classe residuelle de y dans A, donc x non nul dans A. Je note B le sous-groupe de A engendre par x. J'affirme qu'il existe un caractere c sur B non trivial. En effet, si x est d'ordre fini n, on l'envoie sur une racine primitive n-ieme de l'unite (et s'il est d'ordre infini, on l'envoie sur n'importe quoi, par exemple -1). Soit alors C un sous-groupe de A maximal parmi ceux auxquels χ s'etend. J'affirme que $C = A$. Sinon il existe z non dans C, et on prolonge χ au sous-groupe engendre par C et z en prolongeant a $\langle z\rangle$ le caractere induit par χ sur $\langle z\rangle \cap C$.

Ainsi on a construit un caractere $A \longrightarrow \mathbb{C}^*$ non trivial en x, et la composee $G \longrightarrow A \longrightarrow \mathbb{C}^*$ est un caractere de G non trivial en y.

Prince Hughes, 3 fév 02, 12h41

7 Sg d'indice 2 dans $SL_2(\mathbb{Z})$

Un théorème célèbre (je n'ai pas de références) affirme que si $n > 2$, tout sous-groupe fini de $G = SL_2(\mathbb{Z})$ contient un sous-groupe de congruences, i.e. le noyau d'un morphisme vers un $SL_n\left(\mathbb{Z}/M\mathbb{Z}\right)$ pour un certain entier M.

Comme $SL_n(\mathbb{Z})$ est engendré par ses transvections (exo pas dur, par récurrence sur n, en raisonnant sur le plus petit coefficient en valeur absolu de la matrice, puis faire des divisions euclidiennes), la projection canonique de ce dernier vers $SL_n\left(\mathbb{Z}/M\mathbb{Z}\right)$ est surjective, conclusion :

Les sous-groupes d'indices 2 de G sont ceux des $SL_n\left(\mathbb{Z}/M\mathbb{Z}\right)$

Comme tu l'as dit, se donner un sous groupe d'indice 2 d'un groupe A c'est se donner un morphisme dans $\mathbb{Z}/2\mathbb{Z}$. Comme on a que $SL_n\left(\mathbb{Z}/M\mathbb{Z}\right)$ est produit direct des $SL_n\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ ou p^r est la p-composante de M, $p \mid M$ premier (c'est vrai par Bezout en tant qu'algèbre pour $M_n\left(\mathbb{Z}/M\mathbb{Z}\right)$, puis pour GL_n on prends les inversibles, puis on remarque que la décomposition est compatible avec le déterminant et on obtient le cas de SL_n), se donner un morphisme de $SL_n\left(\mathbb{Z}/M\mathbb{Z}\right)$ vers $\mathbb{Z}/2\mathbb{Z}$, c'est se donner des morphismes pour chaque $p \mid M$, de $SL_n\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ vers $\mathbb{Z}/2\mathbb{Z}$. On se ramène donc au cas M primaire. On fixe donc un premier p, je vais utiliser un résultat classique (que j'ai appris dans Modular Fonction III, article de Swinnerton Dyer, mais il semble du a Serre)

Soit G un sous-groupe de $SL_2\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ dont la projection dans $SL_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ est surjective, alors si p est différent de 2 ou 3, $G = SL_2\left(\mathbb{Z}/p^r\mathbb{Z}\right)$. De plus si $p = 2$ (resp 3), il suffit que la projection dans $SL_2\left(\mathbb{Z}/8\mathbb{Z}\right)$ (resp $SL_2\left(\mathbb{Z}/9\mathbb{Z}\right)$) soit surjective, pour que l'on ait la meme conclusion.

Rmq : Cela marche tout aussi bien pour un sous-groupe de lie fermé de $SL_2(\mathbb{Z}_p)$. C'est simplement un problème de relèvement.

Pour la preuve je pourrai la poster si tu veux, c'est totalement élémentaire et court.

Pour conclure, soit donc G un sous-groupe d'indice 2 de $SL_n\left(\mathbb{Z}/p^r\mathbb{Z}\right)$, sa projection modulo p, dans $SL_n\left(\mathbb{Z}/p\mathbb{Z}\right)$, est surjective, hors comme ce dernier n'a pas de sous-groupe d'indice 2 quelque soit p quand $n > 2$ (car son abélianisé est trivial), on en déduit que G se surjecte sur $SL_n\left(\mathbb{Z}/p\mathbb{Z}\right)$. Soit f le morphisme vers $\mathbb{Z}/2\mathbb{Z}$, de noyau G. $SL_n\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ étant engendré par ses transvections (car $SL_n(\mathbb{Z})$ l'est), il est donc engendré par des $SL_2\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ par blocs (et aussi par des $SL_3\left(\mathbb{Z}/p^r\mathbb{Z}\right)$). Soit f restreint à un $SL_2\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ donné, son noyau est soit $SL_2\left(\mathbb{Z}/p^n\mathbb{Z}\right)$, soit un de ses sous-groupes d'indice 2. Si $p > 3$, son image mod p est tout $SL_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ (toujours car l'abélianisé est trivial), et donc c'est encore tout (par le lemme de Serre). Donc si $p > 3$, f est trivial, et G n'existe pas. Il reste les cas, $p = 2$ et 3. Discutons les selon l'assertion suivante :

1- Soit $SL_3\left(\mathbb{Z}/8\mathbb{Z}\right)$ ou $SL_3\left(\mathbb{Z}/9\mathbb{Z}\right)$ a un sous-groupe d'indice 2, auquel cas ton problème est clos : Je te laisse ce cas, je n'ai pas le courage de les traiter.

2- Soit ils n'en ont pas, alors tout $SL_2\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ par bloc s'inclut dans un $SL_3\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ par bloc, le noyau de H de f restreint a ce SL_3 se surjecte alors sur $SL_3\left(\mathbb{Z}/8\mathbb{Z}\right)$ (resp $SL_3\left(\mathbb{Z}/9\mathbb{Z}\right)$), et donc restreint au SL_2 aussi, par conséquent, d'àprès les cas $p = 2, 3$ du lemme de Serre, on en déduit que H contient le $SL_2\left(\mathbb{Z}/p^n\mathbb{Z}\right)$ en question. QED.

En bref, j'ai ramené ton problème à savoir si $SL_3\left(\mathbb{Z}/8\mathbb{Z}\right)$ ou $SL_3\left(\mathbb{Z}/9\mathbb{Z}\right)$ a un sous-groupe d'indice 2 ou non.

Tiens, une petite astuce apporte une simplification substantielle :

si N est premier à p, $SL_n\left(\mathbb{Z}/p^r\mathbb{Z}\right)$ n'a pas de quotient d'ordre N : Il est engendré par ses tyransvections, et toute transvection est une puissance Nième (elle engendre $\left(\mathbb{Z}/p^r\mathbb{Z}\right)^*$, N y est inversible.).

Conslusion on obtient de suite que si p n'est pas 2, $SL_n\left(\mathbb{Z}/_{p^r\mathbb{Z}}\right)$ n'a pas de sous-groupe d'indice 2. Cela exclu d'ailleurs le cas $SL_3\left(\mathbb{Z}/_{9\mathbb{Z}}\right)$. En vu de ce que tu veux, il reste :

Est-ce que les carrés de $SL_3\left(\mathbb{Z}/_{8\mathbb{Z}}\right)$ l'engendrent ? Sais pas.

La preuve que j'ai donnée hier marche encore en remplacant "morphisme dans $\mathbb{Z}/_{2\mathbb{Z}}$" par morphisme dans un $\mathbb{Z}/_{l\mathbb{Z}}$, l premier. On conclut du lemme de Serre (il est utile car l'astuce précédente ne conclut pas les sousgroupes d'indice p de $SL_2\left(\mathbb{Z}/_{p^r\mathbb{Z}}\right)$, mais peut-etre la encore on peut le faire de maniere directe) que :

$SL_n(\mathbb{Z})$, $n > 3$, n'a pas de quotient d'ordre l si $l > 3$. C'est encore vrai pour $n = 2$, on en connait l'abélianisé, c'est un sous-groupe libre a deux générateurs d'indice 12 dans $SL_2(\mathbb{Z})$.

Il faudrait calculer l'abélianisé de $SL_3(\mathbb{Z}_2)$ et celui de $SL_3(\mathbb{Z}_3)$. Il est fort à parier que les groupes dérivers y soient ouverts d'indice fini. Il faudrait s'assurer de savoir si oui ou non ils sont triviaux.

D'ailleurs, que dire de : Si M dans $M_n(\mathbb{Z})$ est un commutateur dans $M_n(\mathbb{Z}_p)$ pour tout p, est-ce un commutateur dans $M_n(\mathbb{Z})$?

Gaga, 21 avril 2004, 3h03, 12h35

8 Un groupe de type fini n'a qu'un nombre fini de sous-groupe d'indice fini donné

Identifions un sous-groupe H d'indice n à $\{1, ..., n\}$. On a ainsi une action de G sur $\{1, ..., n\}$ définie par multiplication, d'où un morphisme de G dans S_n, et pour lequel H est le stabilisateur de 1. Or il n'y a qu'un nombre fini de tel morphismes, vu que G est de type fini :-)

9 Tout groupe de type fini linéaire (sg d'un $GL_k(R)$, R anneau commutatif) est résiduellment fini ; (Th de Malcev).

Soit G un sg de type fini de $GL_k(R)$ où R anneau commatutif.

Je rappelle que G ets dit résiduellement fini si pour tout élément $x \in G$ différent de 1 il existe un morphisme $G->H$, H fini, et tq x ne soit pas dans le noyau.

Je viens de trouver une preuve partielle sur le web et je ne peux pas m'empêcher de la réécrire (en complétant) tellement elle me surprend par sa simplicité (à moins que j'aie raconté des bétises avec les idéaux max).

Soit G un tel groupe : en prenant un nb fini de générateurs, quitte à se estreindre à l'anneau engendré par les coefficients de tous ces générateurs, OPS R de type fini (comme anneau i.e. comme $\mathbb{Z}$-algèbre).

Soit $x = A := 1 + B \in G \setminus \{\mathrm{Id}\}$.

Lemme : il existe $\mathfrak{m}$ idéal maximal tq B n'est pas dans l'intersection des $\mathfrak{m}^n$.

preuve :

[Lemme : si, pour $\mathfrak{m}$ idéal max, B est dans $\bigcap \mathfrak{m}^n$, alors il existe u dans $R \setminus \mathfrak{m}$ tq $uB = 0$.

En effet par Nakayama, l'image de $\bigcap \mathfrak{m}^n$ est réduite à zéro dans le localisé par rapport à $\mathfrak{m}$ (parce que ce dernier est local noetherien). Donc pour tout b dans $\bigcap \mathfrak{m}^n$, il existe u pas dans $\mathfrak{m}$ tq $xu = 0$. En faisant ça pour tous les $b_{i,j}$, on obtient des $u_{i,j}$: le produit u des $u_{i,j}$ n'est pas dans $\mathfrak{m}$ car $\mathfrak{m}$ est premier. Donc $uB = 0$.]

Preuve du premier lemme. S'il est faux, soit I l'idéal des u annulant B. I n'est contenu dans aucun idéal max, donc est R. Donc $B = 0$, contradiction.

Donc l'image de A dans un $GL_k(A/\mathfrak{m}^n)$ est différente de 1. Il suffit de voir que $A/\mathfrak{m}^n$ est un anneau fini.

$A/\mathfrak{m}$ est un corps de type fini, donc est fini. Il reste à montrer $A/\mathfrak{m}^n$ fini.

C'est facile de montrer que, si I est un idéal de type fini et d'indice fini d'un anneau A, alors A/I^n est fini pour tout n.

En effet il suffit de le faire pour $n = 2$ et réitérer (car les I^n sont aussi de type fini).

Donc montrons A/I fini implique A/I^2 fini.

Soit $u_1, ..., u_r$ des générateurs de I. On a une surjection $A^r \twoheadrightarrow I : (a_1, ..., a_r) \longmapsto \sum a_i u_i$ qu'on compose en donnant une surjection : $A^r \twoheadrightarrow I/I^2$ qui se factorise : $(A/I)^r \twoheadrightarrow I/I^2$.

Donc I/I^2 est fini, donc A/I^2 aussi.

Voilà : arguments utilisés : noetherianité des anneaux (propriétés A noeth$=>A[X], A_{\mathfrak{m}}$ noetheriens), Nakayama.

10 $\left\langle a, b \;;\; a^3 = b^3 = (ab)^3 \right\rangle$ est infini

On le réalise comme groupe de matrices avec

$$a = \begin{pmatrix} 1 & \\ & j \end{pmatrix} \text{ et } b = \begin{pmatrix} 1 & 1 \\ & j \end{pmatrix}.$$

11 Groupes ayant même nombre de sous-groupes d'indice k pour tout k

Contre exemple : pour p premier différent de 2, $\left(\mathbb{Z}/p\mathbb{Z}\right)^3$ et le groupe des matrices 3x3 unipotentes triangulaires supérieures sur $\mathbb{Z}/p\mathbb{Z}$.

Les deux sont de cardinal p^3, tous leurs éléments différents de l'identité sont d'ordre p, mais l'un est abélien et pas l'autre.

12 Groupes non abéliens minimuax simpels

Soit G un groupe non-abélien minimal, ie tout sous-groupe strict de G est abélien. Alors j'affirme que G n'est pas simple.

Pour le voir, et par l'absurde : si A et B sont des sous-groupes stricts maximaux de G, $A \cap B$ est normal dans $AB = G$, donc $A \cap B$ est trivial.

Soit H un sous-groupe maximal, H est son normalisateur, et donc la formule aux classes me donne que l'union des gHg^{-1} est de cardinal $n - \frac{n}{m} + 1$ (où $m = [G : H]$, on a $\frac{n}{m}$ conjugués distincts de H, dont les intersections sont deux à deux triviales).

Je peux donc prendre x un élément qui n'est pas dans l'union de ces conjugués, $H\prime$ un groupe maximal qui contient x ($H\prime$ existe car G n'est pas cyclique), alors le même raisonnement me fournit $2n + 1 - \frac{n}{m} - \frac{n}{m'} > n$ éléments distincts de G, absurde.

13 Semi-groupe et carré latin

Les mathématiciens qui se sont intéressés à la notion de groupe ont découvert que le tableau définissant la loi d'un groupe vérifie un lemme, dit de réarrangement :

chaque élément du groupe apparait une fois et une seule dans chaque ligne et chaque colonne de la table.

Mais ils ont aussi découvert que tout tableau vérifiant cette propriété ne définit pas obligatoirement la loi d'un groupe. La loi obtenue est cependant « quasiment » celle d'un groupe, d'où le nom de quasigroupe donné aux structures correspondantes.

Le lemme de réarrangement peut s'exprimer de manière plus formelle :

- dire qu'un élément apparait une fois et une seule sur chaque ligne revient à affirmer que pour tous x et z, l'équation $xy = z$ a une et une seule solution en y ;

- de même, dire qu'un élément apparait une fois et une seule sur chaque colonne revient à affirmer que pour tous y et z, l'équation $xy = z$ a une et une seule solution en x.

14 Triduaux

Soit G un groupe abélien. Pour tout groupe X, on note X' le groupe des morphismes de groupes de X dans G. On dispose d'une application naturelle de X dans X'' qui à x associe l'application $f \mapsto f(x)$. Montrer qu'elle n'est pas nécessairement injective.

On suppose maintenant que X est de la forme $Y\prime$. Montrer qu'alors l'application X -> X'' est injective, et même qu'elle admet une rétraction, c'est-à-dire qu'il existe une application X'' -> X telle que la composée X -> X'' -> X soit l'identité de X.

15 Résiduellement fini

Soit G de type fini, N un sous-groupe fini distingue de G tel que G/N soit residuellement fini. A-t-on G residuellement fini ?

Rappel : un groupe est dit residuellement fini si l'intersection de ses sous-groupes distingues d'indice fini est reduite a $\{1\}$.

Remarques :

-il suffit de montrer le resultat pour N dans le centre de G.

-ce serait deja bien d'obtenir une demo pour le cas particulier ou d'un groupe de type fini dont le groupe derive est fini ($N = G\prime$).

16 groupes dénombrables

y a-t-il a isomorphisme pres un nombre denombrable de groupes de type fini ?

cf. Lyndon & Schupp, Combinatorial group theory, Springer.

Dans le chapitre "some embedding theorems", il est prouve que tout groupe denombrable G se plonge dans un groupe $G\prime$ qui est engendre par deux elements, et tel que pour tout n, G possede un element d'ordre n si et seulement si $G\prime$ possede un element d'ordre n. [La construction utilise les extensions HNN.]

Soit, pour toute partie S de l'ensemble des nombres premiers, C_S le groupe somme $\bigoplus_{p\in S} \mathbb{Z}/p\mathbb{Z}$. Soit G_S le groupe obtenu a partir de C_S par le procede ci-dessus. Alors les G_S sont engendrés par deux elements, donc dénombrables, et sont deux a deux non isomorphes, parce que pour tout p premier, il existe un element d'ordre p dans G_S si et seulement si il y en a dans C_S, çàd ssi p appartient a S.

17 Lemme de Dietzmann

Soit $G = \langle x_1, ..., x_n \rangle$ avec les x_i d'ordre fini et ayant un nombre fini de conjugues dans G ; alors G est fini.

C'est pas joli, peut-etre faux, mais essayons :

Il me semble que tout x de G s'ecrit (pas de maniere unique, mais c'est inutile) $x_{1,1}^{a_{1,1}} x_{1,2}^{a_{1,2}} ... x_{n,m_n}^{a_{n,nm}}$ dans cet ordre, ou les $x_{i,j}$ sont les conjugues (en nb. fini) des generateurs (en nb. fini) $x_i = x_{i,1}$ pour $i = 1...n$.

Pour ca, on part d'une ecriture de x comme produit d'x_i, soit un mot de longeur donnee l ; on commence par "rassembler" tous les $x_{1,j}$, tous les $x_{2,j}$, ... tous les $x_{n,j}$ par blocs en utilisant essentiellement que $axb = x\left(x^{-1}ax\right)b$.

Puis on travaille sur chaque bloc pour rassembler les conjugues identiques, et (c'est pas completement evident mais je crois que ca marche*****) on arrive a la forme cherchee. Notons que pendant tout le procede la longueur l n'a pas bouge.

***** on peut toujours dire que, en "regroupant" systematiquement les $x_{i,1}$, les $x_{i,2}$, etc... on reduit le nombre total de "blocs" $x_{i,j}^{a_{i,j}}$, donc par recurrence sur le nombre de blocs on trouve un produit du genre annonce avec un ordre quelconque entre les conjugues d'un meme x_i... mais apres tout il n'y a qu'un nombre fini de tels ordres.

18 Groupes duaux

Je m'intéresse aux groupes G vérifiant :

1. G est le seul sous-groupe infini de G
2. Tout partie finie de G engendre un sous-groupe fini de G (G est "localement fini")

Est-ce que ça caratérise les groupes "quasi-cycliques" $\mathbb{Z}[\frac{1}{p}] \diagup \mathbb{Z}$ (p premier) ?

Il y a un analogue "dual" plus facile : soit G un groupe vérifiant :
(1') $\{1\}$ est le seul sous-groupe d'indice infini de G.
Alors G est isomorphe à $\mathbb{Z}$.
Esquisse de preuve :
Clairement, un tel groupe n'a pas de sous-groupe fini non trivial, donc est sans torsion. Donc il possède un élément d'ordre infini, ce qui prouve qu'il possède un sous-groupe d'indice fini isomorphe à $\mathbb{Z}$.

Or, on montre qu'un groupe sans torsion, possédant un sous groupe cylique infini d'indice fini doit lui-même être cyclique. Je poste la preuve sur demande ; en attendant, c'est un exo sympa.

.....
Pour insister encore sur les rôles duaux de $\mathbb{Z}$ et $Z\left[\frac{1}{p}\right]$:

a) Si G est un groupe non trivial, alors il existe une injection d'un $\mathbb{Z}\left[\frac{1}{p}\right]$ ou de $\mathbb{Z}$ dans G.

a') Si G est un groupe abélien non trivial, alors il existe une surjection de G vers un $\mathbb{Z}\diagup p\mathbb{Z}$ ou vers un $\mathbb{Z}\left[\frac{1}{p}\right]\diagup\mathbb{Z}$ (p premier).

(b) $\mathbb{Z}$ est le seul $\mathbb{Z}$-module projectif indécomposable
(b') $\mathbb{Q}$ et les $\mathbb{Z}\left[\frac{1}{p}\right]\diagup\mathbb{Z}$ sont les seuls $\mathbb{Z}$-modules injectifs indécomposables

Enfin, dans le même esprit, un truc amusant :
Si G est un groupe abélien infini, alors il existe une injection vers G d'un des groupes infinis de la liste (*) ci-dessous ; et il existe aussi une surjection de G vers un des groupes infinis de cette même liste :
(*) Les groupes en question sont :
- $\mathbb{Z}$
- $\mathbb{Z}\left[\frac{1}{p}\right]\diagup\mathbb{Z}$, p premier
- $(\mathbb{Z}\diagup p\mathbb{Z})^N$, p premier
- $\bigoplus_{p\in I}(\mathbb{Z}\diagup p\mathbb{Z})$, I ensemble infini de nombres premiers

Enfin, une généralisation, et je me tais après ça, promis :
*si G est un groupe abélien localement compact non trivial, alors G se surjecte continûment vers un $Z/p\mathbb{Z}$, $(\mathbb{Z}\diagup p\mathbb{Z})^N$ (discret), ou vers le cercle $\mathbb{S}_1$.
*si de plus G n'est pas compact, alors G se surjecte continûment vers un des groupes discrets de la liste (*) plus haut, ou vers $\mathbb{R}$.

Yves, 13 avril 04, 22h05 (avancées)

19 Groupes bizarres

Soit p un nombre premier assez grand ($> 10^{60}$ pour une borne connue). Il existe un groupe G, vérifiant :

1. Tout sous-groupe propre de G, non trivial, est isomorphe à Z/pZ
2. G est non abélien.

Exercice (facile)
- tout élément non trivial de G est d'ordre p
- G est engendré par deux éléments
- G est simple

– G est infini

Ce groupe a été construit par Ol'Shanskii. Il en a construit aussi un analgue avec vérifiant 1') et 2), avec 1') : Tout sous-groupe propre de G, non trivial, est isomorphe à Z.

Yves a.b.maths, 13 mars 04, 16h18

Les solutions :

- Le sous-groupe engendré par x est abélien, donc est un sous-groupe propre par 1), donc est isomorphe à Z/pZ, donc x est d'ordre p.
- Soient x,y qui ne commutent pas (existent par 2). Le sous-groupe engendré par x et y est donc non abélien, donc non cyclique, donc non propre, i.e. c'est G.
- D'abord, notons que le centre est trivial : sinon, soit x un élément central et y non central. Par a), x et y engendrent un sous-groupe isomorphe à (Z/pZ)2, contradiction avec 1.

  Maintenant soit N un sous-groupe distingué non trivial. Soit H le commutant de N. Alors H contient N, mais, par 1, H=N ou H=G. Ce dernier est exclu car N serait central sinon. L'action de G sur H par conjugaison a donc pour noyau H, i.e. G/H s'injecte dans Aut(H). Or, Aut(H) est d'ordre p-1, et les éléments de G/H sont tous d'ordre p, contradiction.
- Si G était fini, ce serait alors un p-groupe, donc aurait un centre non trivial.

Pour ceux qui auraient trouvé abusif d'appeler cet exercice "facile", je voulais dire ça surtout en comparaison de la difficulté requise pour construire de tel groupes.

Ces groupes ont le don de donner des contre-exemples à pas mal de question "naïves" sur les groupes de type fini genre :

Soit G un groupe de type fini.

*Si tout élément de G est d'ordre fini, est-ce que G est fini ?

*S'il existe n tel que x^n=1 pour tout x dans G, est-ce que G est fini ?

(problème de Burnside, résolu positivement pour n=2,3,4,6, négativement
pour n grand (n>10000 disons), mais ouvert pour n=5,7,8,9,...)

*Si tout sous-groupe de G est de type fini ("G noetherien"), est-ce que G est dans la plus petite classe de groupes contenant Z, les groupes finis, et stable par extensions ?