

# 108: exemples de parties génératrices d'un groupe.

## Applications

Pierre Lissy

April 2, 2010

**Définition 1.** Soit  $G$  un groupe et  $A$  un sous-ensemble quelconque de  $G$ . On dit que la partie  $A$  génère  $G$  ssi tout élément de  $G$  s'écrit comme un produit d'éléments de  $A$ , ie  $\langle A \rangle = G$ .

Intérêt des parties génératrices: permet de réduire l'étude du groupe à celle de quelques éléments.

## 1 Générateurs de quelques groupes finis

### 1.1 Groupes cycliques

**Proposition 1.** Soit  $n \in \mathbb{N}$ . Dans  $\mathbb{Z}/n\mathbb{Z}$ ,  $o(C_n(m)) = \frac{n}{n \wedge m}$ . Donc  $(\mathbb{Z}/n\mathbb{Z}, +)$  est cyclique et ses générateurs sont les  $m$  tels que  $n \wedge m = 1$ . Inversément tout groupe cyclique de cardinal  $n$  est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$ .

**Définition 2.** On pose  $\varphi(n)$  le nombre d'entiers naturels  $k \leq n$  tels que  $k \wedge n = 1$ . C'est donc aussi le nombre de générateurs de  $(\mathbb{Z}/n\mathbb{Z}, +)$ .

**Exemple 1.** Si  $p$  est premier, tous les éléments à part 0 sont d'ordre  $p$ . Donc  $\varphi(p) = p - 1$ .

**Proposition 2.** [1] Soit  $d$  un diviseur naturel de  $n$ . Alors  $\mathbb{Z}/n\mathbb{Z}$  a exactement un seul sous-groupe d'ordre  $d$ , qui est  $\langle C_n(\frac{n}{d}) \rangle$ .

On peut calculer  $\varphi$  de manière récursive pas la formule suivante:

**Proposition 3.**  $n = \sum_{d|n} \varphi(d)$ .

Les groupes cycliques ont un avantage certain: l'ensemble des automorphismes est entièrement déterminé par la donnée de l'image de 1.

**Théorème 1.**  $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ .

**Lemme 1.** Si  $p$  est un nombre premier impair et  $\alpha \in \mathbb{N}^*$ , on a  $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z}$ .

**Lemme 2.**  $(\mathbb{Z}/2\mathbb{Z})^* \simeq 1$ . Pour  $\alpha \geq 2$ ,  $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-1}\mathbb{Z}$ .

On en déduit par le Corollaire 3 les automorphismes de  $\mathbb{Z}/n\mathbb{Z}$ .

**Corollaire 1.** [3]  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$  (ie.  $(\mathbb{Z}/n\mathbb{Z})^*$ ) est cyclique si et seulement si  $n = 2$ ,  $n = 4$ ,  $n = p^\alpha$  ou  $n = 2p^\alpha$  avec  $p$  premier impair et  $\alpha \in \mathbb{N}$ .

**Proposition 4.** On considère un corps  $k$  et le polynôme  $X^n - 1$ . Si  $n$  est premier à la caractéristique de  $k$ . On considère l'ensemble des racines de ce polynôme qui sont dans  $k$ . C'est l'ensemble des racines  $n$ -ièmes de l'unité. Il est cyclique isomorphe à un certain  $\mathbb{Z}/d\mathbb{Z}$  avec  $d|n$ .

On se palce maintenant dans le cas où  $K_n$  est le corps de décomposition de ce polynôme. On a alors un groupe cyclique isomorphe à  $\mathbb{Z}/n\mathbb{Z}$ .

**Définition 3.**  *$n$ -ième polynôme cyclotomique:  $\prod (X - \mu_i)$  où les  $\mu_i$  sont les racines primitives  $n$ -ièmes de l'unité, ie celles qui engendrent notre groupe des racines. Si l'on se donne une racine primitive  $n$ -ième, les autres s'obtiennent en prenant celle là à la puissance  $m$ ,  $m$  premier à  $n$ .*

**Remarque 1.** 1. de degré  $\varphi(n)$

2. unitaire

3. On se ramène toujours au cas de  $k_0$  le sous-corps premier de  $k$  en remarquant que  $\varphi_n$  pris comme polynôme de  $k$  est en fait tel que les racines appartiennent au corps de décomposition du polynôme pris comme polynôme sur  $k_0$ .

**Théorème 2.** *Les polynômes cyclotomiques sont irréductibles*

**Corollaire 2.** *On connaît la décomposition en irréductibles de  $X^n - 1 = \prod_{d|n} \varphi_d(X)$ .*

**Application 1** (Wedderburn). *Tout corps fini est commutatif*

## 1.2 Groupes symétriques et alternés

**Théorème 3.** *Les transpositions engendrent  $S_n$ . De plus, toute permutation s'écrit comme produit d'au plus  $n - 1$  transpositions.*

**Application 2.** *Pour trouver la signature d'une permutation, on a juste à regarder le nombre de transpositions dans une de ses décompositions en produit de transpositions.*

**Application 3.** *On se sert de cette propriété pour montrer que tout automorphisme de  $S_n$  avec  $n$  non égal à 6 est intérieur: on montre que tout automorphisme qui envoie une transposition sur une transposition est intérieur (on utilise énormément les générateurs ici) et on conclut pour des raisons de cardinal dans le cas  $n$  non égal à 6.*

**Théorème 4.** *Les transpositions de la forme  $(1\ 2), \dots, (1\ n)$  engendrent  $S_n$ , tout comme celles de la forme  $(1\ 2), \dots, (n-1\ n)$ . Les transpositions de la forme  $(1\ 2), \dots, ((n-1)\ n)$  engendrent  $S_n$*

**Application 4.** [5][page 145] *Une forme  $p$ -linéaire sur un  $ev$  est alternée dès que  $x_k = x_k + 1 \Rightarrow f(x_1, \dots, x_p) = 0$ .*

**Théorème 5.** *Les cycles engendrent  $S_n$ . Plus précisément, toute permutation s'écrit de manière unique (à l'ordre près) comme produit de cycles à support disjoints commutant deux à deux.*

**Corollaire 3.** *Toute permutation de  $S_n$  est d'ordre au plus  $n$ .*

**Théorème 6.**  *$(1\ 2)$  et  $(1\ 2 \dots n)$  suffisent à engendrer  $S_n$ .*

**Théorème 7.** *Pour  $n \leq 5$ , les 3-cycles engendrent  $A_n$ .*

On voit ici l'importance des générateurs dans les questions de simplicité: on prend un sous-groupe distingué, et on essaie de montrer qu'il contient un ensemble de générateurs. Pour peu que cet ensemble de générateurs soit conjugué, il suffit juste d'en avoir un et le tour est joué!

**Application 5.** *Les  $A_n$  sont simples pour  $n = 3$  et  $n \geq 5$ .  $A_4$  contient un unique sous-groupe strict distingué non trivial isomorphe au groupe de Klein.*

**Corollaire 4.** *Le centre de  $S_n$  est trivial,  $D(S_n) = D(A_n) = A_n$ .*

**Proposition 5.** *Classes de conjugaisons = permutations du même type.*

## 1.3 Groupes diédraux

**Définition 4.** Le groupe diédral  $D_n$  est le groupe des isométries laissant invariantes le polygone régulier à  $n$  côtés.

**Proposition 6.** Le groupe diédral est composé de  $n$  rotations et de  $n$  symétries orthogonales, il est de cardinal  $2n$ . L'ensemble des rotations forment un sous-groupe distingué de  $D_n$ .

**Proposition 7.** Soit  $r$  la rotation d'angle  $2\pi/n$  et  $s$  une réflexion quelconque  $s$ . Alors  $r$  et  $s$  engendrent  $D_n$ .

**Application 6.** Les rotations sont d'ordre  $n$ , les réflexions d'ordre 2. Les conjugués d'une rotation sont elle-même et son opposé. Les réflexions sont toutes conjuguées dans le cas impair, dans le cas pair il y a deux classes de conjugaison: celles qui passent par les sommets et celles qui passent par les milieux des sommets. Le centralisateur d'une rotation est l'ensemble des rotations, celui d'une réflexion dans le cas impair est la réflexion et l'identité, dans le cas pair c'est le groupe engendré par la réflexion et  $-Id$ .

On peut grâce aux générateurs étudier le groupe des automorphismes de certains groupes diédraux.

**Application 7.** [3][page 51] Le groupe des automorphismes de  $D_4$  est lui-même

Enfin, un théorème qui caractérise les diédraux et est assez important en pratique.

**Théorème 8.** On considère un sous-groupe tel qu'il est engendré par deux éléments  $a$  et  $b$  tels que  $a$  est d'ordre  $n$ ,  $b$  est d'ordre 2 et  $(ab)^2 = e$ . Alors le groupe est isomorphe à  $D_n$ .

**Application 8.** On s'en sert dans la démo pour les sous-groupes finis de  $SO_3$

## 2 Générateurs en algèbre linéaire

### 2.1 Générateurs de $SL(E)$ et de $GL(E)$ .

**Définition 5.** On considère un hyperplan de  $E$  d'équation  $f(x) = 0$ , et un élément  $u$  inversible égal à  $Id$  sur  $H$ . Transvection d'hyperplan  $H$ : une des définitions équivalentes

1.  $\det(u) = 1$
2.  $u$  n'est pas diago
3.  $\text{Im}(u - Id) \subset H$
4. Le morphisme quotient  $E/H$  sur lui-même est l'identité
5. Il existe  $a$  dans  $H$  tel que  $u(x) = x + f(x)a$ .
6. Dans une base convenable on a deux un dans la dernière colonne tout en bas et  $Id$  autre part.

**Définition 6.** On considère un hyperplan de  $E$  d'équation  $f(x) = 0$ , et un élément  $u$  inversible égal à  $Id$  sur  $H$ . Dilatation d'hyperplan  $H$ : une des définitions équivalentes.

1.  $\det(u)$  non égal à 1
2.  $u$  a une valeur propre différente de 1 et est diago
3.  $\text{Im}(u - Id) \not\subset H$
4. Dans une base on a un  $\lambda$  en bas.

**Lemme 3.** Si l'on se donne deux éléments  $x$  et  $y$ , il existe une transvection  $u$  ou un produit de deux transvections  $v$  tel que  $u(x) = y$  ou  $uv(x) = y$ .

**Théorème 9.** *Les transvections engendrent  $SL(E)$ . Elles sont conjuguées dans  $GL(E)$  et dans  $SL(E)$  pour  $\dim(E) \geq 3$ . On a même seulement besoin de  $n$  éléments, sauf si c'est une homothétie et il en faut  $n + 1$ .*

Encore une fois, on en déduit assez facilement un résultat de simplicité

**Théorème 10.**  *$PSL(n, k)$  est simple pour un corps  $k$  quelconque et  $n \geq 3$*

**Corollaire 5.**  *$D(GL(n, k)) = D(SL(n, k)) = SL(n, k)$  pour  $n \geq 3$ .*

**Remarque 2.** *Encore vrai pour  $n = 2$  et  $k \neq F_2, F_3$ , mais plus difficile. De plus, on rappelle que dans le cas  $n$  impair,  $PSL$  est égal à  $SL$ . Dans le cas d'un corps algébriquement clos,  $PSL$  est égal à  $PGL$ .*

**Corollaire 6.** *Les transvections et les dilatations engendrent  $GL(E)$*

**Application 9.** *[7][page 178-]  $Sl_n$  est cpa dans le cas réel ou complexe.*

**Application 10.** *Les matrices diagonalisables inversibles réelles engendrent  $GL_n(\mathbb{R})$*

**Application 11.** *Les matrices inversibles de trace nulle engendrent  $GL_n(\mathbb{R})$ .*

## 2.2 Générateurs de $O(E)$ et $SO(E)$

**Proposition 8.** *Le groupe  $O(E)$  est engendré par les réflexions. Plus précisément, tout élément de  $O(E)$  est produit d'au plus  $n$  réflexions. En fait, on a même besoin de seulement  $n - \dim \{\text{pts fixes de } g\}$  éléments.*

**Proposition 9.** *Pour  $n \geq 3$ ,  $SO$  est engendré par les renversements. Au plus  $n$  renversements nécessaires.*

Encore une fois, les générateurs donnent des résultats de simplicité et sur les automorphismes.

**Application 12.** *tous les automorphismes de  $SO_3$  sont intérieurs.*

**Application 13.**  *$SO_3(\mathbb{R})$  est simple.*

**Application 14.**  *$PSO_n$  est simple pour  $n$  non égal à 4. Dans le cas impair, cela revient juste à dire que  $SO_n$  est simple.*

## 2.3

## References

- [1] Perrin
- [2] Combes
- [3] Ortiz
- [4] Querré
- [5] Gourdon algèbre
- [6] Itard nombres premiers
- [7] fgn algèbre 2