Formulaire sur les groupes

1 Ordre d'un élément, ordre d'un groupe

Définition (ORDRE D'UN ÉLÉMENT) : soit G groupe[1], $x \in G$. Alors :
Si $\exists n \in \mathbb{N}$ tq. $x^n = e_G$, on dit que l'ordre de x est fini. L'ordre de x est l'entier MINIMAL strictement positif tel que $x^n = e_G$. On notera : $|x| = n$
Si $\nexists n \in \mathbb{N}$ tq. $x^n = e_G$, on dit que l'ordre de x est infini

Définition (sous-groupe engendré) : soit G groupe, $x \in G$. L'ensemble $< x >:= \{x^k, k \in \mathbb{Z}\}$ est appelé sous-groupe de G engendré par x.

Proposition : $| < x > | = |x|$

2 Générateur, groupes monogènes, groupes cycliques

Définition (ÉLEMENT GÉNÉRATEUR) : Soit $x \in G$. On dit que x est générateur de G si $< x >= G$

rem. : si $G =< x >$, alors $|G| = | < x > |$

Définition : un groupe monogène est un groupe engendré par un élément, un groupe cyclique est un groupe monogène fini (il a donc un ordre).

Soit G monogène. On a donc : $\exists x \in G$, $G =< x >$ où $< x >:= \{x^k, k \in \mathbb{Z}\}$
Soit G cyclique d'ordre n. On a donc : $\exists x \in G$, $G =< x >= \{x^k, 1 \leqslant k \leqslant n\}$

Exemples :
(1) $(\mathbb{Z}, +)=< 1 >$ et $(n\mathbb{Z}, +)=< n >$ donc sont des groupes monogènes, de type finis (mais infinis donc non cycliques)
(2) $(\mathbb{Z}/n\mathbb{Z}, +)=< 1 >$ cyclique
(3) Tout groupe fini d'ordre premier est cyclique (4) si $\mathbb{K}$ corps abélien, G sous-groupe fini de $(\mathbb{K}, \text{“}\cdot\text{”})$, alors G cyclique

Définition (SYSTÈME DE GÉNÉRATEUR) : soit $(G, *)$ groupe[2], $A \subset G$. Alors
$< A >= \{x_1^{n_1} * ... * x_k^{n_k}, k \in \mathbb{N}, n_i \in \mathbb{Z}, x_i \in A\}$.
$< A >$ est l'intersection de tous les sous-groupes de G qui contiennent A.

On dit que A est un système de générateur si $< A >= G$. Si G possède un ensemble de générateur fini, on dit qu'il est de type fini.

rem : G fini $\Rightarrow G$ de type fini. La réciproque est fausse (ex : $\mathbb{Z}$)

3 Eléments inversibles de $(\mathbb{Z}/n\mathbb{Z})$

On notera les éléments inversibles[3] de $(\mathbb{Z}/n\mathbb{Z})$, “$\cdot$”) par : $(\mathbb{Z}/n\mathbb{Z})^\times$ $(\mathbb{Z}/2\mathbb{Z})^\times=\{1\} =< 1 >$ cyclique

$(\mathbb{Z}/3\mathbb{Z})^\times=\{1, 2\} =< 2 >$ cyclique
$(\mathbb{Z}/4\mathbb{Z})^\times=\{1, 3\} =< 3 >$ cyclique
$(\mathbb{Z}/5\mathbb{Z})^\times=\{1, 2, 3, 4\} =< 2 >$ cyclique
$(\mathbb{Z}/8\mathbb{Z})^\times=\{1, 3, 5, 7\}$ monogène, pas cyclique, car $\nexists x \in (\mathbb{Z}/8\mathbb{Z})$ tel que $< x >= (\mathbb{Z}/8\mathbb{Z})$

Remarque : si p premier, $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})^*$

4 Sous-groupe normal-distingué

M est un sous-groupe distingué (ou normal) de G si(si) :
$\forall g \in G, gMg^{-1} = M$
$\iff \forall g \in G, gM = Mg$
$\iff \forall g \in G, gMg^{-1} = M$
$\iff \forall g \in G, \forall m \in M, gmg^{-1} \in M$
$\iff G/M$ ***est un groupe pour la loi canonique, ie*** $\overline{g_1}.\overline{g_2} = \overline{g_1 g_2}$

Exemples :
(1) si G est abélien, tous les sous groupes de G sont normaux
(2) $\{e_G\}$ et G sont normaux
(3) soit $\phi : G \to H$ homomorphisme de groupes. Alors $Ker\phi$ est un sous-groupe normal de G
(4) tout sous groupe d'ordre 2 est normal
(5) $[G, G] := \langle g.h.g.h^{-1}, g, h \in G\rangle$ est un sous groupe normal (commutateur de G)

L'intérêt des sous-groupes distingués est donc qu'il existe une structure de groupe sur G/H telle que : $\pi : \begin{array}{ccc} G & \to & G/H \\ x & \mapsto & [x] \end{array}$ soit un homomorphisme de groupe
(puis théorême de factorisation)

[1] Source : Dixmier, Pajitnov, Terracher. Tapée par Gwendal. Mise à jour le 16/02/2006

[2] si loi+, $< A >= \{n_1 x_1 + ... + n_k x^k\}$

[3] On s'intéresse évidemment aux éléments inversibles pour la loi “ $\cdot$ ” (car groupe pour la loi +, donc tous les éléments sont inversibles). Elément neutre : $\overline{1}$

5 Groupes symétriques

5.1 Décomposition d'une permutation en cycles

Soit $\tau \in S_n$ une permutation. Alors il existe une décomposition de τ en cycles disjoints :
(1) $\tau = \sigma_1 \circ ... \circ \sigma_k$
(2) $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i, \forall i, j = 1...k$
(3) $|\tau| = ppcm(|\sigma_1|, ..., |\sigma_k|)$

5.2 Signature d'une permutation

Soit $\tau \in S_n$ une permutation. On définit la signature de τ par $\xi(\tau) = (-1)^{nbe\ d'inversions}$

-Prop : τ une TRANSPOSITION. Alors $\xi(\tau) = -1$
-Prop : σ un CYCLE de longueur k. Alors $\xi(\sigma) = (-1)^{k-1}$
-Prop : $\xi(\sigma_1 \circ \sigma_2)=\xi(\sigma_1)\xi(\sigma_2)$
-Prop : $\xi(\sigma) = (-1)^{n-(nombre\ d'orbite\ de\ \sigma)}$

5.3 Décomposition d'un cycle en transpositions

Théorême : tout cycle $\sigma \in S_n$ peut se décomposer en produit de transpositions :
$(x_1, ..., x_p) = (x_1, x_2)(x_2, x_3)...(x_{p_1}, x_p)$

rem : cycle de longueur $p \longrightarrow$ décomposition en $p - 1$ transpositions

Exemple : $\sigma=$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 10 \\ 3 & 4 & 2 & 1 & 8 & 7 & 9 & 11 & 12 & 10 & 5 & 6 \end{pmatrix}$$

Décomposition en cycles disjoints : $\sigma =$ (1 3 2 4)(5 8 11)(6 7 9 12)
Décomposition en transpositions : $\sigma =$ (1 3)(3 2)(2 4)(4 5)(5 8)(8 11)(6 7)(7 9)(9 12)
Ordre : $|\sigma| = ppcm(4, 3, 4) = 12$
$\sigma^{11} = \sigma^{-1} =$ (1 4 2 3)(5 11 8)(6 12 9 7)

6 Actions de groupes

Action de groupe : soit $(G, \circ)$ un groupe, E un ensemble. Une application $* : G \times E \to E$ vérifiant les conditions ci-dessous est appelé action de G sur E

1. $(g_1 \circ g_2) * x=g_1 * (g_2 * x), \forall x \in E, g_i \in G$
2. $e_G * x = x, \forall x \in E$

Exemples d'actions :
(1) S_3 sur $(\mathbb{Z}/2\mathbb{Z})^3$:
$\sigma * (x_1, x_2, x_3)=(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)})$
(2) S_n sur $\{1, ..., n\}$: $\sigma * (i)=\sigma(i)$
(3) S_n sur $(\mathbb{R}^n$: $\sigma * (x_1, ..., x_n)=(x_{\sigma(1)}, ..., x_{\sigma(n)})$
(4) G sur G par conjugaison : $g_1 * g_2 = g_1 \circ g_2 \circ g_1^{-1}$

Trois exemples d'actions de S_3 sur S_3 :
(1) action triviale : $\sigma \circ \tau = \tau$
(2) action par translation : $\sigma * \tau = \sigma \circ \tau$
(3) action conjugaison (automorphisme. intérieur) : $\sigma * \tau = \sigma \circ \tau \circ \sigma^{-1}$

7 Divers

– Orbite de x : O_x=$\{g * x, g \in G\}$

– Stabilisateur de x : St_x=$\{g \in G, g * x = x\}$ (sous-groupe de G)

– Centre de G : $Z(G)$=$\{g \in G, \forall h \in G, hg = gh\}$ (c'est un sous-groupe distingué-normal)

– $G = S_n$. Support de $\sigma \in S_n(E)$: $supp(\sigma) = \{x \in E, \sigma(x) \neq x\}$

Remarque : si $y \in O_x$, alors $O_y = O_x$

8 Formule des classes

Soit $* : G \times X \longrightarrow X$

8.1 Action transitive

Si l'action est transitive :
Cardinal de l'orbite=$\dfrac{cardinal\ du\ groupe}{cardinal\ du\ stabilisateur}$

$$|X| = \frac{|G|}{|St_x|} \text{ où } x \in X$$

8.2 Action non transitive

Si l'action est non transitive :
Cardinal de X=somme des cardinaux des orbites=$\sum_{x \in X} \dfrac{|G|}{|St_x|}$, où St_x : stabilisateur de x

8.2.1 cas particulier : Action par conjugaison

Si G fini, $|G| = |Z(G)| + \sum_{i=1}^{n} \dfrac{|G|}{|St_{x_i}|}$
où $x_i \in O_i$ avec $O_1, ..., O_n$ les orbites tq. $card(O_i) > 1$
$Z(G)$ est le centre de x dans G pour l'action de conjugaison : $Z(G) = \{g \in G, gx = xg\}$=$\{g \in G, gxg^{-1} = x\}$

Plus simplement : $|G| = \sum_{x \in\ systeme\ de\ representant(1)} |O_x|$
$= |Z(G)|+ \sum_{x \in\ systeme\ de\ representant(2)} |O_x|$

où $x \in$ *systeme de representant* sous entend qu'il ne faut pas compter deux fois les mêmes orbites

Exemple : $S_3 = \{Id, \tau_1, \tau_2, \tau_3, \sigma, \sigma^2\}$
$Z(G) = O_{Id} = \{Id\}$
$O_{\tau_1} = \{\tau_1, \tau_2, \tau_3\} = O_{\tau_2} = O_{\tau_3}$
$O_\sigma = \{\sigma, \sigma^2\} = O_{\sigma^2}$
Donc $S_3 = \sum_{x\in\{Id,\tau,sigma\}} = |Z(G)| + \sum_{x\in\{\tau,sigma\}} =$
$|O_{Id}| + |O_{\tau_1}| + |O_\sigma| = 1+3+2=6$

9 Théorême de factorisation

9.1 Décomposition canonique d'une application

Soit $f : E \longrightarrow F$ une application, $\mathcal{R}$ la relation d'équivalence $f(x) = f(y)$, s l'application canonique $s : \begin{array}{ccc} E & \to & E/\mathcal{R} \\ x & \mapsto & [x] \end{array}$. L'application s est surjective, l'application i est injective, et on a :

On écrit souvent cela sous forme de théorême :
Théorême : Il existe une unique application h de $EE/\mathcal{R}$ dans $f(E)$ telle que $f = i \circ h \circ s$. Cette application est bijective.
Si u est un élément de $E/\mathcal{R}$, son image par h s'obtient en choisissant un représentant quelconque de u et en prenant son image par f.

9.2 Décomposition canonique d'un homomorphisme de groupes

Soit G_1, G_2 deux groupes, f un homomorphisme de G_1 dans G_2. Nous supposerons G_1 abélien (commutatif). Alors $Ker(f)$ est distingué-normal, et on a :

Si de plus, f est surjective, on a :

Rappel : f surjective *ie* $Im(f) = f(G_1)$

9.3 Décomposition canonique d'un homomorphisme d'anneaux

Soit A_1, A_2 deux anneaux, f un homomorphisme de A_1 dans A_2. Nous supposerons A_1 abélien (commutatif). Alors $Ker(f)$ est distingué-normal, et $Ker(f)$ est un idéal de A_1, et on a :

Si de plus, f est surjective, on a :