manque des exemples d'autres endroits du programme (matrices, polynômes ...)

104 Groupes finis : Exemples et applications

I) Introduction

1) Quelques définitions préliminaires

<u>Def 1</u> : i) Un groupe est dit <u>fini</u> s'il ne contient qu'un nbr fini d'elts.

ii) Soit G un grp. fini et g un élt de G, <u>l'ordre de g</u> est le plus petit entier $n \in \mathbb{N}^*$ tq $g^n = e$, noté $O(g)$

L'ordre de G est le cardinal de G, noté $|G|$

iii) On note $\langle g \rangle$ le sous-groupe de G engendré par g.

iv) S'il existe $g \in G$ tq $G = \langle g \rangle$, G est dit <u>cyclique</u>. $O(0)=1$

<u>Exemple 2</u> : • $G = \mathbb{Z}/3\mathbb{Z}$ est fini et cyclique. $G = \langle 1 \rangle = \langle 2 \rangle$ $(O(1)=3$ $O(2)=3)$

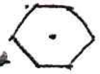
• le groupe de permutat° d'un ens. à n élts est fini.

<u>Exemple 3</u> : $\{e\}$ et $\mathbb{Z}/n\mathbb{Z}$ sont des groupes finis.

<u>Exemple 4</u> : $D_n = \langle r, s \mid r^n = e, s^2 = e, srs^{-1} = r^{-1} \rangle$

= ss-grp des isométries du plan laissant fixe un polygone régulier à n sommet centré en O.

$D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ et $|D_n| = 2n$
↳ groupe diédral



<u>Exemple 5</u> : Q : groupe quaternionique

$Q = \{1, -1, i, -i, j, -j, k, -k\}$ où $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$

Q est un groupe non abélien dont tous les sous-gr sont distingués.

Ex : $\{1\}$, $Z(G) = \{1, -1\}$, $\{1, -1, i, -i\}$: $|Q| = 8$

i est d'ordre 4 et $\langle i \rangle = \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$

Q n'est pas cyclique.

2) Théorème de Lagrange : Premiers résultats sur l'ordre d'un groupe

<u>Def 6</u> : Soit G un groupe et $H \lhd G$. On appelle <u>indice</u> $(G:H)$, l'ordre du groupe quotient G/H. $(G:H) = |G|/|H|$ (si G est fini)

<u>Exemple 7</u> : $(\mathbb{Z} : n\mathbb{Z}) = n$ $\quad (Q : \langle i \rangle) = 2$

<u>Application 8</u> : Soit G un grp fini et $H < G$ tq $(G:H) = 2$ alors $H \lhd G$

<u>Thm 9 (Lagrange)</u> : Soit G un grp fini et $H < G$, alors $|H| \mid |G|$

<u>Application 10</u> : L'ordre de tout élt de G divise l'ordre de G.

<u>Application 11</u> : Un groupe d'ordre premier est cyclique (et ses seul sous-grp sont $\{e\}$ et lui-même)

<u>Thm 12 (1er thm d'isomorphisme)</u> :

Soit $\varphi : G \to \Gamma$ un morp. de grp. Alors il existe un isomorp. $\tilde{\varphi} : G/\ker\varphi \to \operatorname{Im}\varphi$; si φ surj. alors $G/\ker\varphi \overset{\tilde{\varphi}}{\cong} \Gamma$

<u>Exemple 13</u> : $\det : GL(n,K) \to K^* \Rightarrow GL(n,K)/SL(n,K) \cong K^*$

<u>Thm 14</u> : (3ème thm d'isomorphisme)

Soit $K \subset H \subset G$ avec $H \lhd G$, $K \lhd G$. Alors $(G/K)/(H/K) \simeq G/H$

<u>Exemple 15</u> : $(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$

<u>Thm 16 (Cauchy)</u> : Soit G un groupe fini : $|G| = n$ et p premier tq $p \mid n$

Alors il existe un élt d'ordre p dans G.

<u>Prop 17</u> : Soit G un groupe fini agissant sur un ensemble X, alors

$|G.x| = (G : G_x)$ i.e $|G| = |G_x| \cdot |G.x|$ pour tout $x \in X$

<u>Prop 18</u> : (Formule des classes) Soit G un grp fini et $G \circlearrowright X$ (X ens), soit $\bigcup_{i=1}^{n} X_i$ la partition de X en orbites sous l'action de G, on a :

$$|X| = \sum_{i=1}^{n} |X_i| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|} \quad \text{où } x_i \in X_i, \; n \in \mathbb{N}^*$$

<u>Application 19</u> : (Thm de Wedderburn)

Tout corps gauche fini est commutatif.

dev 1

II) p-groupes et p-Sylows

1) p-groupes

<u>def 20</u> : Soit p premier. Un <u>p-groupe</u> est un grp dont tt élt est une puissance de p.

<u>Prop 21</u> : G est un p-groupe $\Leftrightarrow$ $|G|$ est une puissance de p

<u>Exemple 22</u> : $\mathbb{Z}/p^k\mathbb{Z}$, Q (groupe quaternionique), $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

<u>Prop 23</u> : Tout groupe d'ordre p^2 est abélien

<u>Exemple 24</u> : $\mathbb{Z}/4\mathbb{Z}$ abélien ; $\mathbb{Z}/8\mathbb{Z}$ abelien mais Q non abélien

2) p-Sylow

<u>Def 25</u> : Soit G un grp d'ordre $p^\alpha m$ où p premier et $p \nmid m$. On appelle <u>p-Sylow</u> de G un sous-grp de G de cardinal p^α.

<u>Thm 26</u> (Sylow) Soit G un grp tq $|G| = p^\alpha m$ avec $p \nmid m$

0) G contient un p-Sylow.

1) Si $H < G$ est un p-groupe, $\exists$ un p-Sylow S avec $H \subset S$

2) les p-Sylows sont tous conjugués

3) $n_p \equiv 1 \, [p]$ et $n_p \mid m$ où n_p est le nbr de p-Sylow de G.

Cor 27: Soit S un p-Sylow de G, on a :

$$S \triangleleft G \iff S \text{ est l'unique } p\text{-Sylow de } G \iff n_p = 1$$

Exemple 28: Dans $\mathbb{Z}/6\mathbb{Z}$, il y a un unique 3-Sylow car ($6 = 2 \times 3$) $n_3 | 2$ et $n_3 \equiv 1 [3]$

Exemple 29: $\mathbb{Z}/7\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2$ ne contient pas d'élt d'ordre 9 mais il contient un sous-groupe d'ordre 9.

Application 30: Il n'y a pas de grp simple à 30 éléments

Application 31: Classification des groupes d'ordre 12, 60.

Application 32 (Groupe d'ordre pq) dev 2

Soit $|G| = pq$ avec p, q premiers et $p < q$

- Si $p \nmid q-1$, $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$
- Si $p | q-1$ $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ ou $\mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$

où α est un morph° non trivial $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$

Proposition 33: Soient G un grp fini et p variant parmi les diviseurs premiers de $|G|$. On a équivalence entre :

(i) Tous les p-Sylows de G sont distingués.
(ii) Le groupe G est produit direct de ses p-Sylows.

III) Cas abéliens

Prop 34 G cyclique $\Rightarrow$ G abélien

Exemple 35: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est abélien mais n'est pas cyclique

Prop 36: G cyclique fini $\iff G \cong \mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N}^*)$

Prop 37: G cyclique d'ordre $n \iff \forall d | n, \exists ! H < G, |H| = d$

Corollaire 38: G d'ordre premier $p \iff G$ cyclique et $G \cong \mathbb{Z}/p\mathbb{Z}$

Corollaire 39: soit $G = \mathbb{Z}/n\mathbb{Z}$. Pour tout diviseur d de n, il existe $g \in G$ d'ordre d dans G.

Exemple 40: $\mathbb{Z}/6\mathbb{Z}$: $o(1) = 6$; $o(0) = 1$; $o(2) = 3$; $o(3) = 2$

Application 41 si p et q sont deux nbr premiers divisant n, il existe un élément d'ordre pq dans $\mathbb{Z}/n\mathbb{Z}$.

Thm 42 (Chinois) : Soit $p \wedge q = 1$, Alors $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Exemple 43: $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$

Prop 44: Soit $s \in \mathbb{Z}$; on a :

$s \wedge n = 1 \iff \bar{s}$ générateur du grp $(\mathbb{Z}/n\mathbb{Z}, +) \iff \bar{s} \in (\mathbb{Z}/n\mathbb{Z})^*$

Prop 45: $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ (abélien).

Thm 46: (Structure des groupes finis)

Soit G un grp fini abélien. Alors $\exists ! (d_1, \dots, d_k)$ liste d'entiers > 1 tq $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z}$ et $d_i | d_{i+1}$ pour tout $i \in [\![1, k-1]\!]$

Exemple 47: $\mathbb{Z}/8\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

IV) Groupe symétrique

Def 48: Le groupe des bijections de $\{1, \dots, n\}$ dans $\{1, \dots, n\}$ pour la loi de composit° des applicat° est appelé groupe de permutation ou groupe symétrique, on le note $\mathfrak{S}_n$.

Prop 49: $|\mathfrak{S}_n| = n!$

Thm 50 (Cayley) : Tout ss-grp fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Def 51: Soient $n \in \mathbb{N}$, $\sigma \in \mathfrak{S}_n$.

i) les elts i de $\{1, \dots, n\}$ qui vérifient $\sigma(i) = i$ sont appelés points fixes de σ

ii) L'ens. $\{1, \dots, n\}$ privé des points fixes de σ est appelé support de σ et est noté $\mathrm{Supp}(\sigma)$

Prop 52: Si $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\rho) = \emptyset$, alors $\mathrm{supp}(\sigma\rho) = \mathrm{supp}(\sigma) \cup \mathrm{supp}(\rho)$ et $\sigma\rho = \rho\sigma$

Def 53: Soient $1 \le l \in \mathbb{N}$ et $i_1, \dots, i_l$ des elts distincts de $\{1, \dots, n\}$. La permutat° $\gamma \in \mathfrak{S}_n$ définie par

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ et } k < l \\ i_1 & \text{si } j = i_l \end{cases}$$

est noté $(i_1, i_2, \dots, i_l)$ et est appelé cycle de longueur l

Def 54: Un cycle de longueur 2 est appelée une transposition

Exemple 55: $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$ est un cycle, 3 est pt fixe et $\gamma = (1, 4, 2, 5) = (4, 2, 5, 1)$

Thm 56: Tout $\sigma \in \mathfrak{S}_n$ s'écrit comme $\sigma = \gamma_1 \dots \gamma_m$ où $(\gamma_i)_i$ sont des cycles de longueur ≥ 2 dont les supports sont 2 à 2 disjoints.

Exemple 57: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix} = (1\,3\,4\,5)(2\,6\,8)$

Def 58: Soit $n \in \mathbb{N}^*$, On appelle type d'une permutation $\sigma \in \mathfrak{S}_n$ et on note $[l_1, \dots, l_m]$ la liste des cardinaux l_i des orbites dans $\{1, \dots, n\}$ de l'action de $\langle\sigma\rangle$ sur $\{1, \dots, n\}$ rangé par ordre croissant. On le note $\mathrm{type}(\sigma)$

Exemple 59 : type(γ) = $[1,4]$, type(σ) = $[1,3,4]$

Prop 60 : Une permutation $\sigma \in \mathfrak{S}_n$ de type $[l_1, l_2, \dots, l_m]$ a pour ordre ppcm$(l_1, \dots, l_m)$

Prop 61 : Deux permutations σ et ρ sont conjuguées dans $\mathfrak{S}_n$ (ie $\exists g \in \mathfrak{S}_n$ tq $\sigma = g \rho g^{-1}$) ssi elles sont de même type.

Prop 62 : Pour $\omega \in \mathfrak{S}_n$, et tout cycle $(i_1, \dots, i_l) \in \mathfrak{S}_n$, on a
$\omega (i_1, \dots, i_l) \omega^{-1} = (\omega(i_1), \dots, \omega(i_l))$

Cor 63 : Dans $\mathfrak{S}_n$, tous les cycles d'ordre p sont conjugués

Application 64 (Thm de Brauer) (dev 3)

Soit K un corps de car. 0. Pour $\sigma \in \mathfrak{S}_n$, notons $P_\sigma \in GL(n,K)$ la matrice associée à σ dans la base canon. de K^n ($P_\sigma = (\delta_{i,\sigma(j)})$). Alors σ et τ sont conjuguées ssi P_σ et P_τ sont conjuguées dans $GL_n(K)$

Prop 65 : Le groupe $\mathfrak{S}_n$ est engendré par les transpositions.

Def 66 : Soient $1 \leq n \in \mathbb{N}$ et $\sigma \in \mathfrak{S}_n$. On appelle signature de $\sigma \in \mathfrak{S}_n$ et on note $\varepsilon(\sigma)$, le nombre $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$

Prop 67 : L'applicat° $\varepsilon : \mathfrak{S}_n \to (\mathbb{Q}^*, \times)$ est un morph. de grp dont l'image est incluse dans $\{-1, 1\}$

Prop 68 :
- Si σ est une transposit°, $\varepsilon(\sigma) = -1$
- Si σ est de type $[l_1, \dots, l_m]$, $\varepsilon(\sigma) = (-1)^{l_1 + \dots + l_m - m}$

Def 69 : Soit $n \in \mathbb{N}$, une permutat° $\sigma \in \mathfrak{S}_n$ est dite paire si $\varepsilon(\sigma) = 1$
impaire si $\varepsilon(\sigma) = -1$

Def 70 : Le noyau du morphisme $\varepsilon : \mathfrak{S}_n \to \{-1,1\}$ est appelé groupe alterné et est noté $\mathfrak{A}_n$.

Prop 71 : Pour $n \geq 2$, le groupe $\mathfrak{A}_n$ est le seul ss-groupe d'indice 2 de $\mathfrak{S}_n$

Prop 72 : Le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles pour $n \geq 3$

Thm 73 : Le groupe $\mathfrak{A}_n$ est simple pour $n \geq 5$

Corollaire 74 : $D(\mathfrak{A}_n) = \mathfrak{A}_n$ pour $n \geq 5$ et $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geq 2$

Corollaire 75 : Pour $n \geq 5$, les ss-grp distingués de $\mathfrak{S}_n$ sont $\{1\}$, $\mathfrak{A}_n$, $\mathfrak{S}_n$

Corollaire 76 : Soit H un ss-grp d'indice n de $\mathfrak{S}_n$ alors $H \cong \mathfrak{S}_{n-1}$

Thm 77 : Pour $n \neq 6$: Aut $\mathfrak{S}_n$ = Int $\mathfrak{S}_n$

Prop 78 : Pour $n \neq 6$, on a équivalence entre :
a) Aut $\mathfrak{S}_n$ = Int $\mathfrak{S}_n$ (pour $n \geq 3$ Aut $\mathfrak{S}_n \cong \mathfrak{S}_n$)
b) les ss-grp d'indice n de $\mathfrak{S}_n$ sont tous conjugués

Rem 79 : Aut $\mathfrak{S}_6 \neq$ Int $\mathfrak{S}_6$

V) Groupes linéaires

1) Groupes linéaires sur $\mathbb{F}_q$

(Dans la suite $n \in \mathbb{N}^*$, k un corps fini)

Prop 80 : Card$(GL(n, \mathbb{F}_q)) = \prod_{i=0}^{n-1} (q^n - q^i)$

Thm 81 :
- $D(GL(n,k)) = SL(n,k)$ sauf dans le cas : $(n = 2, k = \mathbb{F}_2)$
- $D(SL(n,k)) = SL(n,k)$ sauf dans les 2 cas : $n=2$ et $k = \mathbb{F}_2$; $n = 2$ et $k = \mathbb{F}_3$

Thm 82 : Soit G un grp, $|G| = n$, G est isomorphe à un ss-grp de $GL(n,k)$

Thm 83 : $GL_n(\mathbb{F}_q)$ admet un q-Sylow : le grp des matrices triang. sup. avec une diagonale de 1

Prop 84 : $Z(GL_n(\mathbb{F}_p)) = \{\lambda Id, \lambda \in \mathbb{F}_p\} = \{$homothéties$\}$
$Z(SL_n(\mathbb{F}_p)) = \{\lambda Id, \lambda \in \mathbb{F}_p$ tq $\lambda^n = 1\} = \{$homothéties de det 1$\}$

Def 85 : Le groupe projectif linéaire $PGL_n(\mathbb{F}_p) = GL(\mathbb{F}_p) / Z(GL_n(\mathbb{F}_p))$
spécial projectif linéaire $PSL_n(\mathbb{F}_p) = SL(\mathbb{F}_p) / Z(SL(\mathbb{F}_p))$

Prop 86 : $Aut(\mathbb{F}_p^n) \cong GL_n(\mathbb{F}_p)$

Thm 87 : $PSL(n,k)$ est simple sauf si $\begin{cases} n = 2, k = \mathbb{F}_2 \\ n = 2, k = \mathbb{F}_3 \end{cases}$

Exemple 88 :
i) $GL(2, \mathbb{F}_2) = SL(2, \mathbb{F}_2) = PSL(2, \mathbb{F}_2) \cong \mathfrak{S}_3$
ii) $PGL(2, \mathbb{F}_3) \simeq \mathfrak{S}_4$; $PSL(2, \mathbb{F}_3) \cong \mathfrak{A}_4$
iii) $PGL(2, \mathbb{F}_4) = PSL(2, \mathbb{F}_4) \simeq \mathfrak{A}_5$
iv) $PGL(2, \mathbb{F}_5) \simeq \mathfrak{S}_5$; $PSL(2, \mathbb{F}_5) \simeq \mathfrak{A}_5$

2) Sous groupes finis de $SO_2(\mathbb{R})$ et $SO_3(\mathbb{R})$

Prop 89 :
- les ss-groupes finis de $SO_2(\mathbb{R})$ sont des ss-grp cyclique finis
- les ss-grp finis de $O_2(\mathbb{R})$ qui ne sont pas dans $SO_2(\mathbb{R})$ sont des groupes $\cong D_n$, $n \in \mathbb{N}$

Prop 90 : Si G est un ss-groupe non trivial de $SO_3(\mathbb{R})$ alors G est isomorphe à l'un des grp : $\mathbb{Z}/n\mathbb{Z}$, D_n, $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$ ($2 \leq n \in \mathbb{N}$)

Application 91 : Classification des polyèdres réguliers

Questions :

* $\mathfrak{S}_4$ simple ?
* Sous-groupe distingués ?
* $\mathfrak{S}_4 / \text{Klein} \cong ?$ $\underline{D_3}$ ou $\mathbb{Z}/6\mathbb{Z}$. (ordre des éléments)

or $D_3 \simeq S_3$.

* Trouver $\underset{3 \text{ élts}}{X}$ telle que $\mathfrak{S}_4 \xrightarrow{f} \text{Aut}(X) = \mathfrak{S}_3$
  / H noyau de f.

utiliser les p-sylow.

$$\mathfrak{S}_4 \times X \longrightarrow X$$
$$(\sigma, S_i) \longmapsto \sigma S_i \sigma^{-1}.$$

* donner un 2-sylow de $\mathfrak{S}_4$. D_4.

Références :

- Félix ULMER, Théorie des groupes
- Daniel PERRIN, Cours d'Algèbre
- Aviva SZPIRGLAS, L3 Algèbre

Développement n° 1 : $\boxed{\text{Théorème de Wedderburn}}$

Lemme : $\forall q \in \mathbb{N}$ tel que $q \geq 2$

Soient $n, d \in \mathbb{N}^*$ tels que $q^d - 1 \mid q^n - 1$

Alors d divise n

Démonstration (lemme)

Supposons $q^d - 1 \mid q^n - 1$ avec $n, d \in \mathbb{N}^*$ et $q \geq 2$
($q \in \mathbb{N}^* \setminus \{1\}$)

alors $q^d - 1 \geq 1 > 0$

d'où $\dfrac{q^n - 1}{q^d - 1} \in \mathbb{N}$

Effectuons la division euclidienne de n par d :

$n = kd + r$ avec $k, r \in \mathbb{N}$ et $0 \leq r < d$

$$\frac{q^n - 1}{q^d - 1} = \frac{q^{kd+r} - q^r}{q^d - 1} + \frac{q^r - 1}{q^d - 1}$$

$$= q^r \frac{q^{kd} - 1}{q^d - 1} + \frac{q^r - 1}{q^d - 1}$$

$$= \underbrace{q^r \sum_{i=0}^{k-1} (q^d)^i}_{\in \mathbb{N}} + \frac{q^r - 1}{q^d - 1}$$

D'où $\dfrac{q^r - 1}{q^d - 1} \in \mathbb{N}$, Or $r < d$

d'où $q^r - 1 < q^d - 1$

Ainsi $q^r - 1 = 0$ et donc $r = 0$

Ainsi $d \mid n$ ■

Théorème (Wedderburn) :

Tout corps gauche fini est commutatif.

Démonstration :

Soit k un corps gauche fini

Notons Z le centre de k ; $Z = \{ a \in k \mid \forall x \in k, ax = xa \}$

Z est un sous-corps de k de cardinal $q \geq 2$

(il contient 0 et 1)

D'où $|k| = q^n$ où $n \in \mathbb{N}^*$ (car k est un Z-EV)

Supposons par l'absurde que k soit non-commutatif, alors $n > 1$ (sinon $k = Z$)

D'où k^* opère sur lui-même par conjugaison :

$$\begin{cases} k^* \times k^* \longrightarrow k^* \\ g \ , \ x \ \longmapsto gxg^{-1} \end{cases}$$

Pour $x \in k^*$, on note $w(x)$ l'orbite de x par l'action de conjugaison et $k_x = \{ y \in k \mid yx = xy \}$

k_x est un sous-corps de k

On a $|k_x| = q^d$ (car Z est un sous-corps de k_x)
$(d \in \mathbb{N}^*)$

Or k_x^* est un sous-groupe de k^*, d'où par le théorème de Lagrange $q^d - 1 \mid q^n - 1$

Et donc, par le lemme $d \mid n$

Le cardinal de l'orbite de x est alors

$$|w(x)| = \frac{|k^*|}{|k_x^*|} = \frac{q^n - 1}{q^d - 1}$$

Or, on a dans $\mathbb{Z}$, par définition du polynôme cyclotomique :

$$q^n - 1 = \prod_{m|n} \Phi_m(q) \quad \text{et} \quad q^d - 1 = \prod_{m|d} \Phi_m(q)$$

$$\frac{q^n - 1}{q^d - 1} = \prod_{\substack{m|n \\ m\nmid d}} \Phi_m(q)$$

Si $d \neq n$, alors $\Phi_n(q) \mid \dfrac{q^n - 1}{q^d - 1}$

On a les équivalences suivantes :

$$\begin{aligned} k_x = k &\iff \forall h \in k,\ x = hxh^{-1} \\ &\iff \omega(x) = \{x\} \\ &\iff \forall h \in k,\ xh = hx \\ &\iff x \in Z \end{aligned}$$

Notons $(x_i)_{i=1,\dots,t}$ un système de représentant des différentes orbites de k^* non réduite à un point.

Alors, par la formule des classes, on a :

$$|k^*| = |Z^*| + \sum_{i=1}^{t} |\omega(x_i)|$$

d'où $q^n - 1 = q - 1 + \displaystyle\sum_{i=1}^{t} \frac{q^n - 1}{q^{d_i} - 1}$ où $q^{d_i} = |k_{x_i}|$
$(d_i | n)$ et $(d_i \neq n)$

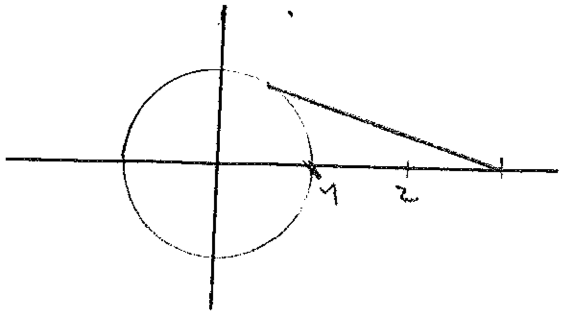
D'où $\Phi_n(q) \mid q - 1$ (car il divise les deux autres termes de l'égalité)

En particulier $|\Phi_n(q)| \leq q - 1$

On a $\Phi_n(q) = (q - \xi_1) \dots (q - \xi_\ell)$ où $\xi_1, \dots, \xi_\ell \in \mathbb{C}$ sont les racines primitives $n^{\text{ième}}$ de 1 et vérifient donc $|\xi_i| = 1$ et $\xi_i \neq 1$
(puisque $n \neq 1$)

Mais alors, $\forall j \in [1, \cdots, \ell]$,

$$|q - \xi_j| > q - 1$$



et donc $|\Phi_n(q)| > (q-1)^\ell \geq q-1$

Et on aboutit à une contradiction. ■

<u>Références :</u>

- Daniel PERRIN, Cours d'Algèbre. Ellipses
- Xavier GOURDON, Algèbre. Ellipses

<u>Leçons concernées :</u>

- 101 : Groupe opérant sur un ensemble
- 102 : Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
- 104 : Groupes finis : Exemples et Applications.
- 123 : Corps finis : Application.

Développement n° 2 : $\boxed{\text{Groupes d'ordre } pq}$

Lemme : Soit H et N des groupes et $\alpha, \beta : H \to \mathrm{Aut}(N)$ deux morphismes tels que $\alpha = \beta \circ \Phi$ pour $\Phi \in \mathrm{Aut}(H)$
Alors $N \rtimes_\alpha H \cong N \rtimes_\beta H$

Démonstration :

Soient $f :$
$$\begin{aligned} N \rtimes_\alpha H &\longrightarrow N \rtimes_\beta H \\ (n, h) &\longmapsto (n, \Phi(h)) \end{aligned}$$

et $g :$
$$\begin{aligned} N \rtimes_\beta H &\longrightarrow N \rtimes_\alpha H \\ (n, h) &\longmapsto (n, \Phi^{-1}(h)) \end{aligned}$$

On vérifie aisément que f et g sont des morphismes puis qu'ils sont inverses l'un de l'autre.

Lemme : 1) Tout sous-groupe d'un groupe cyclique est cyclique

2) Soit $(d, n) \in (\mathbb{N}^*)^2$, où $d \mid n$, Alors il existe un unique sous-groupe d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$

Démonstration :

1) Soit G un groupe cyclique engendré par x, H un sous-groupe de G non réduit à $\{e\}$. Soit $d = \inf\{k \in \mathbb{N}^*, x^k \in H \setminus \{e\}\}$. Soit $x^k \in H$ et $(q, r) \in \mathbb{N}^2$ tels que $k = dq + r$ avec $0 \leq r < d$ (division euclidienne de k par d). On a $x^k = (x^d)^q x^r$. Donc $x^r \in H$, ie $r = 0$
Ainsi x^d engendre H qui est bien cyclique.

2) Soit $H = \{x \in \mathbb{Z}/n\mathbb{Z},\ dx = 0\}$. H est un sous-grp qui contient tout sous-groupe d'ordre d. En particulier $\{\bar{0}, \bar{k}, \dots, \overline{(d-1)k}\}$ où $k = n/d$. Donc $|H| \geq d$.

D'autre part H est cyclique d'après 1) et tout générateur a un ordre divisant d (def. de H), donc $|H| \leq d$. Ainsi $|H| = d$ et tout sous-groupe d'ordre d est égal à H.

<u>Théorème</u> : Soit G un groupe d'ordre pq avec p et q premiers, $p < q$

- Si $p \nmid q-1$, alors $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$
- Si $p \mid q-1$, alors :

  ou bien $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$

  ou bien $G \cong (\mathbb{Z}/q\mathbb{Z}) \rtimes_\alpha (\mathbb{Z}/p\mathbb{Z})$

  où α est une action non triviale de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$

<u>Démonstration</u> :

D'après le théorème de Sylow, il existe dans G un sous-groupe Q d'ordre q et un sous-groupe H d'ordre p.

Notons n_q le nombre de q-Sylows de G.

Alors d'après le théorème de Sylow : $n_q \mid p$ et $n_q \equiv 1\ [q]$

Donc $n_q = 1$. Ainsi Q est distingué dans G.

D'après Lagrange $|Q \cap H|$ divise $|Q| = q$

divise $|H| = p$

donc $|Q \cap H| = 1$. Ainsi $Q \cap H = \{e\}$

Puisque $Q \triangleleft G$, QH est un sous groupe de G

Or QH contient Q et contient H

Donc $|QH| \geqslant q + p - 1$

Ainsi $|QH| = pq$ et $G = QH$

Donc $G = Q \rtimes H$

Or $Q \cong \mathbb{Z}/q\mathbb{Z}$ et $H \cong \mathbb{Z}/p\mathbb{Z}$

D'où $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$

De plus $n_p \mid q$ (n_p est le nombre de p-Sylows de G)

et $n_p \equiv 1 \; [p]$

Donc $n_p = 1$ ou $n_p = q$

- Si $p \nmid q-1$ alors $q \not\equiv 1 \; [p]$

donc par ce qui précède $n_p = 1$

Ainsi $H \lhd G$ (et comme $Q \lhd G$)

On a $G \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

- Si $p \mid q-1$ combien de classe d'iso $\neq$?

$\alpha : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$

Or $\mathbb{Z}/p\mathbb{Z}$ est simple

Donc soit $\ker(\alpha) = \mathbb{Z}/p\mathbb{Z}$ et α est le morphisme trivial,

donc $G \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

soit $\ker(\alpha) = \{0\}$, d'où α est injectif et $\alpha(\mathbb{Z}/p\mathbb{Z})$

est un sous-groupe d'ordre p de $\mathbb{Z}/(q-1)\mathbb{Z}$

Or $\mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous-groupe d'ordre p

Donc, pour tous les α possibles, $\alpha(\mathbb{Z}/p\mathbb{Z})$ sera le même et unique sous-groupe de $\mathbb{Z}/(q-1)\mathbb{Z}$ d'ordre p.

De plus α est déterminé de manière unique par l'image de 1 et détermine entièrement le produit semi-direct.

Soit α_1, α_2 deux possibilités pour α

Supposons $\alpha_1(1) = a$ et $\alpha_2(1) = b$ avec $a, b \neq 0$

Alors $\alpha_1 = \alpha_2 \circ \Phi$ où $\Phi \in Aut(\mathbb{Z}/p\mathbb{Z})$ (tq $\Phi(1) = \alpha_2^{-1}(a)$)

d'où d'après le lemme $\mathbb{Z}/q\mathbb{Z} \rtimes_{\alpha_1} \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\alpha_2} \mathbb{Z}/p\mathbb{Z}$ ■

<u>Références :</u>

- PERRIN, Cours d'Algèbre
- SZPRIGLAS, L3 Algèbre
- FRANCINOU, GIANELLA, Exercices de Maths pour l'Agreg Algèbre 1.

<u>Leçons concernées :</u>

- 103 : Exemples de sous-groupes distingués et de groupes quotient. Applications.
- 104 : Groupes finis. Exemples et Applications.
- 120 : Anneau $\mathbb{Z}/n\mathbb{Z}$. Applications
- 121 : Nombres premiers. Applications.