104

Groupes finis. Exemples et applications.

I Groupes finis

Définition 1 Un groupe est un couple $(G,\cdot)$ où G est un ensemble et $\cdot : G\times G \to G ; (g,h)\mapsto g\cdot h$, associative, admettant un élément neutre noté e et où chaque élément admet un inverse.

Définition 2 : Un sous groupe de $(G,\cdot)$ est la donnée de $H\subset G$, non vide, tel que $(H,\cdot)$ soit un groupe.

Exemple 3 : $(\mathbb{Z};+)$ est un groupe. C'est un sous groupe de $(\mathbb{R};+)$

Définition 4 : Un groupe est dit fini si l'ensemble sous-jacent l'est. On appelle ordre d'un groupe le cardinal de l'ensemble sous-jacent.

Exemple 5 : $(\mathbb{Z}/5\mathbb{Z},+)$ est un groupe fini d'ordre 5.

Définition 6 : Un groupe est dit cyclique si il est engendré par un unique élément et si le groupe est fini.

Exemple 7 : $(\mathbb{Z}/5\mathbb{Z},+)$ est engendré par 1 : il est cyclique.

II Ordre, indice et exposant d'un groupe fini

Théorème 8 : Théorème de Lagrange :
Soit G un groupe fini, H un sous groupe de G. L'ordre de H divise l'ordre de G.

Définition 9 : Soit G un groupe, $g\in G$. L'ordre de g est l'ordre de $\langle g\rangle$; le sous groupe engendré par g. En particulier, l'ordre de g divise G par thm 8.

Application 10 : Soit p et q premiers, impairs. On a $q\mid 2^p-1$. Alors $q\equiv 1[p]$.

Corollaire 11 : Un groupe d'ordre p premier est cyclique.

Exemple 12 : Pour p premier, les groupes $(\mathbb{Z}/p\mathbb{Z};+)$ sont cycliques.

Définition 13 : Soit G un groupe, $\mathrm{Int} : g\to \mathrm{Int}_g$ où $g\in G$ et où $\mathrm{Int}_g : G\to G,\ h\mapsto ghg^{-1}$. Int_g s'appelle un automorphisme intérieur de G.

Définition 14 : Soit G un groupe, H un sous-groupe de G. H est dit distingué dans G, noté $H\lhd G$, si $\forall g\in G$, $\mathrm{Int}_g(H)\subset H$; ie si H est stable par automorphisme intérieur.

Exemple 15 : Les $n\mathbb{Z}$ sont distingués dans $\mathbb{Z}$.

Remarque 16 : Tout sous groupe d'un groupe où la loi est commutative est distingué.

Définition 17 : Soit G un groupe, H un sous groupe distingué dans G. On note, pour $g\in G$, $gH=\{gh \mid h\in H\}$.
L'application $*: (g_1H * g_2H)\mapsto (g_1g_2)H$ définit une loi de groupe sur G/H l'ensemble quotient, définit par $G/H=\{gH\mid g\in G\}$.
L'application $\pi : G\to G/H,\ g\mapsto gH$ est un morphisme de groupe surjectif de noyau H.

Définition 18 : Soit G un groupe, $H\lhd G$. L'indice de H dans G ; noté $[G:H]$; est le cardinal de G/H.

Remarque 19 : En complément au théorème de Lagrange, on a en particulier $|G|=|H|\times[G:H]$.

Théorème 20 : Théorème de Poincaré
Soit G un groupe, H et K deux sous groupes. En étendant la notion d'indice de H dans G au cas où H n'est pas distingué comme le cardinal de l'ensemble $G/H=\{gH\mid g\in G\}$ qui, ici, n'est pas un groupe, on a
$$[G:H\cap K]=[G:H][H:H\cap K]\leqslant[G:H][G:K]$$

Théorème 21 : Formule des indices
Soit G un groupe, H un sous groupe de G et K un sous groupe de H. Alors $[G:K]=[G:H][H:K]$.
Si K est trivial on retrouve la formule $|G|=|H|[G:K]$

Définition 22 : L'exposant d'un groupe G de neutre e est le plus petit entier $n \in \mathbb{N}^*$ tel que $\forall g \in G$, $g^n = e$. Comme on travaille sur G fini, un tel n existe toujours, où g^n est le $n$ième itéré de g.

Exemple 23 : 5 est l'exposant de $(\mathbb{Z}/5\mathbb{Z};+)$
$\to \bar{1}^5 = \bar{1} + \dots + \bar{1} = \underbrace{\bar{0}}_{e} = \bar{2}^5 = \bar{3}^5 = \bar{4}^5$.

Corollaire 24 : Le théorème de Lagrange assure que l'exposant d'un groupe G divise son ordre.

Définition 25 : On définit l'indicatrice de Carmichael λ tel que $\lambda(n)$ est le plus petit entier non nul tel que $\forall a \in \mathbb{N}^*$, $a \wedge n = 1$, $a^{\lambda(n)} \equiv 1\,[n]$

Propriété 26 : $\lambda(n)$ est l'exposant du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$

III Groupes abéliens finis ; étude de $\mathbb{Z}/n\mathbb{Z}$

Définition 27 : Un groupe G est dit de type fini si G est engendré par une partie finie de lui-même.

Prop 28 : Un groupe fini est nécessairement de type fini

Propriété 29 : Soit G de type fini, abélien, engendré par $a_1, \dots, a_n$ d'ordres finis $s_1, \dots, s_n$. Alors G est fini d'ordre $S \mid s_1 \times \dots \times s_n$; et tel que $\operatorname{ppcm}(s_1, \dots, s_n) \mid S$.

Théorème 30 : Soit G abélien fini (et donc de type fini).
On a $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}$ où $n \in \mathbb{N}^*$ et où les $m_i \in \mathbb{N}^*$, tel que $\forall i \in [\![1;n-1]\!]$, $m_i \mid m_{i+1}$.

Remarque 31 : Si G est abélien de type fini, pas nécessairement fini, on peut généraliser ce résultat avec $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z} \times \mathbb{Z}^r$; $r \in \mathbb{N}$.

Proposition 32 : On a tout groupe d'ordre n cyclique si et seulement si $\varphi(n)$ est premier avec n.

Exemple 33 : Tout groupe d'ordre premier est cyclique. Cela implique que tout groupe d'ordre p premier est isomorphe à $(\mathbb{Z}/p\mathbb{Z})$.

Propriété 34 : Soit $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z};+)$ est un groupe cyclique possédant $\varphi(n) = \#\{k \wedge n = 1 \mid k \in [\![1;n-1]\!]\}$ générateurs. Si $n = p$ premiers, $(\mathbb{Z}/p\mathbb{Z};+)$ est engendré par tous ses éléments non nuls, et $(\mathbb{Z}/p\mathbb{Z};\times)^*$ est un groupe.

Propriété 35 : Dans $(\mathbb{Z}/n\mathbb{Z};\times)^*$, groupe abélien fini, $\exists\, k \in (\mathbb{Z}/n\mathbb{Z})^*$ d'ordre l'exposant, i.e. d'ordre $\lambda(n)$.
On a donc $(\mathbb{Z}/n\mathbb{Z};\times)^*$ cyclique $\iff \lambda(n) = \varphi(n)$

Application 36 : On a $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ où $n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ est sa décomposition en nombres premiers.

IV Actions de groupes finis

Soit G un groupe ; X un ensemble.

Définition 37 : $\varphi : G \to S(X)$ où $S(X) = \{$application de X dans $X\}$; vérifiant $\varphi(e) = id_X$ et
$\varphi(g_1)(\varphi(g_2)(x)) = \varphi(g_1 g_2)(x)$ $\forall x \in X$, $g_1, g_2 \in G$
est appelée une action de groupe. On dit que X agit sur X.

Exemple 38 : S_n le groupe symétrique d'ordre n agit sur $[\![1;n]\!]$ par l'action $\varphi : s \in S_n \mapsto [\![1;n]\!] \to [\![1;n]\!]$
$i \mapsto s(i)$.

Définition 39 : L'orbite de $x \in X$ par l'action de G est l'ensemble $O_x = \{y \in X ; \exists g \in G, \varphi(g)(x) = y\}$.
On notera abusivement $g.x$ plutôt que $\varphi(g)(x)$ si l'action est non ambigüe.

Propriété 40 : Les orbites forment une partition de X.

Définition 41 : Le sous groupe $G_x = \{g \in G, g.x = x\}$ est appelé stabilisateur de x. Si x et y sont dans la même orbite tel que $g.x = y$, on a $G_y = g G_x g^{-1}$.

Remarque 42 : $G/G_x \to O_x$ est une bijection.
$g \mapsto g.x$

Cela assure que $|G| = |G_x| \times |O_x|$

Définition 43 : On note $Fix_g = \{x \in X ; g.x = x\}$.

Théorème 44 : Théorème de Cayley

Soit G un groupe fini. G est isomorphe à un sous groupe de $S_{|G|}$; où S_n est le groupe symétrique d'ordre n.

Propriété 45 : S_n le groupe des permutations de $[\![1;n]\!]$ est engendré par l'ensemble des cycles (par décomposition en cycle de support disjoint), par l'ensemble des transpositions de la forme $(1;k)$, et par $(1;2)$ et $(1;2;\dots;n)$

Définition 46 : Un sous groupe G du groupe des isométries de $\mathbb{R}^n$ est dit paveur si il existe un pavé P compact, convexe, d'intérieur non vide tel que

i) $g(P)$ recouvrent $\mathbb{R}^n$ quand g décrit G

ii) $\forall g;h \in G,\ g \neq h,\ \overset{\circ}{g(P)} \cap \overset{\circ}{h(P)} = \emptyset$.

Propriété 47 : S^4 peut être vu comme un groupe de pavage.

Dev 1

Définition 48 : On note $\varepsilon : S_n \to \{\pm 1\}$

$$\sigma \mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

le morphisme de groupe appelé signature.

Remarque 49 : En pratique, $\varepsilon(\sigma) = 1$ si le nombre de transposition pour écrire σ est paire, $\varepsilon(\sigma) = -1$ sinon.

Définition 50 : $\mathcal{A}_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$ est un groupe, sous groupe de S_n, appelé groupe alterné. $\mathcal{A}_n = \mathrm{Ker}(\varepsilon)$.

Remarque 51 : $\mathcal{A}_n$ est d'indice 2 dans S_n et contient $\frac{n!}{2}$ élément.

Propriété 52 : Pour $n \geq 5$; $\mathcal{A}_n$ est un groupe simple ;

ie qui ne possède pas de sous-groupe distingué autre que le groupe trivial et lui-même

Dev 2

Théorème 53 : Théorème de Cauchy

Soit G un groupe d'ordre n. Soit p premier, $p \mid n$.
$\exists H$ sous groupe de G d'ordre p.

Définition 54 : On appelle p-groupe, pour p premier, un groupe dont tous les éléments ont pour ordre une puissance de p.

Proposition 55 : Un groupe fini est un p groupe ssi son ordre est une puissance de p.

Définition 56 : On appelle p-Sylow de G un p-sous-groupe de G maximal pour l'inclusion. On note $Syl_p(G)$ l'ensemble des p-Sylow

Proposition 57 : Soit G groupe fini ; N un p-sous groupe de G.
$N \lhd G \Rightarrow N \subset \bigcap_{P \in Syl_p(G)} P$.

Théorème 58 : Théorèmes de Sylow

Soit G un groupe fini d'ordre $p^e m$, p premier, $e \in \mathbb{N}^*$, et m tel que $\mathrm{pgcd}(m,p) = 1$.

i) Les p-Sylow de G sont ses sous groupes d'ordre p^e

ii) Les p-Sylow sont tous conjugués. Si P est un p-Sylow de G, alors $\# Syl_p(G) = [G : N_G(P)]$ où $N_G(P)$ est le normalisateur de P ; $N_G(P) = \{g \in G, gPg^{-1} = P\}$

iii) Soit $n_p = \# Syl_p(G)$; $n_p \mid m$ et $n_p \equiv 1 [p]$.

Application 59 Il n'existe qu'un groupe d'ordre 15 : $\mathbb{Z}/15\mathbb{Z}$.

Théorème 60 : Formule de Burnside

Soit X un ensemble fini et G un groupe fini agissant sur X.
On a $|Orb_X(G)| = \frac{1}{|G|} \sum_{g \in G} |Fix_g|$; où $Orb_X(G)$ est l'ensemble des orbites de X par l'action de G.

Application 61 :

Il y a 57 possibilités de colorier un cube avec 3 couleurs différentes

Dev 3