Théorème de Lagrange :

I) Relation d'équivalence :

Définitions :

Soit E un ensemble muni d'une relation R.

On dit que R est ~~reff~~ reflexive ssi : $\forall x \in E$, xRx

Exemple : ① $E = \mathbb{R}$; $x R y \Leftrightarrow x \leq y$:

R est reflexive.

② $E = \mathbb{R}$; $x R y \Leftrightarrow x < y$

R n'est pas reflexive.

On dit que R est symétrique si :

$x R y$ alors $y R x$.

Exemple : ① $E = \mathbb{R}$; $x R y \Leftrightarrow x \leq y$

n'est pas symétrique : $1 \leq 2$ mais $2 \not\leq 1$

② $E = \{$ étudiant L_2 MEU $\}$.

$x R y \Leftrightarrow$ x est dans le même groupe de TD que y ;

Cette relation est symétrique.

• On dit que R est transitive si :

$$x R y \text{ et } y R z \Rightarrow x R z.$$

Exemple : ① $E = \mathbb{R}$; $x R y \Leftrightarrow x < y$

② $E = \mathbb{R}$; $x R y \Leftrightarrow xy > 0$

(transitive ?).

③ $E = \mathbb{Z}$; $a R b \Leftrightarrow \mathrm{pgcd}(a, b) = 1$

R transitive ?).

On dit que R est une relation d'equivalence si R est réflexive, symétrique et transitive.

Exemple : ① $E = \mathbb{Z}$; $a R b \Leftrightarrow a \equiv b [2]$.

② Soit $f : E \longrightarrow F$ une application

On definit sur E la relation :

$$x R y \Leftrightarrow f(x) = f(y).$$

R est une rélation d'equivalence.

③ etre dans le même groupe est une relation d'equivalence.

<u>Exo</u> : Soit E muni d'une relation R symétrique et transitive ; un étudiant fait le raisonnement suivant :

$$x R y \Rightarrow y R x, \quad (R \text{ symétrique})$$

On a donc : $x R y$ et $y R x \Rightarrow x R x$ car R est transitive, il conclut donc que R est reflexive.
Trouver l'erreur du raisonnement.

<u>Classe d'équivalence</u> :

(E muni d'une relation d'équivalence :
Soit $a \in E$, On definit la classe de a, $cl(a) = \{ b \in E, a R b \}$.

<u>proposition</u> : Soit R relation d'équivalence sur E

1) $a \in cl(a)$
2) : si $a, b \in E$; $a R b \Leftrightarrow$ ~~$\bar{a} = \bar{b}$~~ $cl(a) = cl(b)$
3) ; si $cl(a) \neq cl(b)$ i.e a et b ne sont pas en relation ; $cl(a) \cap cl(b) = \phi$.

<u>preuve</u> : 1) $a R a \Rightarrow a \in \bar{a}$

2) – si $a R b$; si $c \in cl(a)$;
$c R a$ et $a R b \Rightarrow c R b \Rightarrow c \in cl(b)$

$cl(\bar{a}) \subset cl(\bar{b})$; a, b jouent un rôle symétrique
donc $cl(\bar{b}) \subset cl(\bar{a})$ et par suite $cl(\bar{a}) = cl(\bar{b})$.

remplacer $\bar{a}$ par $cl(a)$

Réciproquement si $\bar{a} = \bar{b} \Rightarrow a \in \bar{a} = \bar{b} \Rightarrow aRb$

3) – Supposons que $\bar{a} \cap \bar{b} \neq \emptyset$, soit
$c \in \bar{a} \cap \bar{b} \Rightarrow cRa$ et $cRb \Rightarrow aRb$
et par suite $\bar{a} = \bar{b}$ ce qui est Absurde.

Remarque: On peut donc voir E comme la réunion des classes d'équivalences.

Petit Rappel: Soit E un ensemble; une partition de E est la donné de parties de E; U_i qui vérifie: (1) $E = \bigcup_i U_i$ ← partie de E

réunion   indice

(2) $U_i \cap U_j = \emptyset$ si $i \neq j$

Exemple: $E = \{$étudiants L_2 EU$\}$.
U_i = groupe i ;

La proposition précédent dit tout simplement qu'une relation d'équivalence R sur E donne une partition de E (par les classes d'équivalence).

Exemple:

Exemples 1 : ① $E = \mathbb{Z}$; $a R b \iff a \equiv b \, [2]$.

On a deux classes d'équivalences ; la classe des nombres pairs, et la classe des nombres impairs.

plus généralement : $a R b \iff a \equiv b \, [n]$;

On a n classes d'équivalences :

$\bar{0} = \{$ multiples de $n \}$.

$\bar{1} = \{ kn + 1 \, ; \, k \in \mathbb{Z} \}$

$\overline{n-1} = \{ kn + n - 1 , \, k \in \mathbb{Z} \}$.

~~les élements , 0, 1, ..., n-1 s'appelent~~

Chaque élément d'une classe d'équivalence s'appelle un représentant de sa classe ; On choisit souvent un représentant "simple", par exemple

0 représente les nombres pairs

1 — — — — impairs.

On a vu donc ~~don~~ qu'une relation d'équivalence nous donne une partition de E. On a une réciproque :

Proposition : Soit E un ensemble, U_i une partition de E

· On définit sur E la relation R ;

$x R y \Leftrightarrow \exists i$ tel que $x \in U_i$ et $y \in U_i$

proposition : R est une relation d'équivalence.

preuve : $E = \bigcup_i U_i$;

· Soit $x \in E$, $\exists i$, tel que : $x \in U_i$ donc $x R x$.

symétrie : si $x R y \Leftrightarrow \exists i$; $x \in U_i$ et $y \in U_i \Rightarrow y R x$

· transitivité : $x R y \Leftrightarrow \exists i$ tel que $x \in U_i$ et $y \in U_i$

$y R z \Leftrightarrow \, .. \, j \, -$ $y \in U_j$ et $z \in U_j$

$U_i \cap U_j = \phi$ si $i \neq j \Rightarrow i = j$ et $x R z$.

Application : G groupe, $|G| = 2n$, $\exists x \in G$ d'ordre 2.

Notion d'ensemble quotient ;

(E, R) une relation d'équivalence :

On rappelle $\mathcal{P}(E)$ est l'ensemble des parties de E

Exemple : si $E = \{1, 2\}$,

$\mathcal{P}(E) = \{ \phi, \{1\}, \{2\}, \{1, 2\} \}$.

On définit E/R = ensemble quotient de E par R.

Comme le sous-ensemble de $\mathcal{P}(E)$ formé des classes d'équivalences et on a une projection canonique

$$p : E \longrightarrow E/R$$
$$x \longrightarrow \bar{x} = cl(x).$$

(vu comme un élément

Exemples ① $E = \mathbb{R}^*$, $x R y \Leftrightarrow xy > 0$

$$cl(1) = \{x \in \mathbb{R}^*, x > 0\}.$$

$$cl(-1) = \{x \in \mathbb{R}^*, x < 0\}.$$

$E/_{\mathbb{R}}$ contient deux éléments $\bar{1}$ et $\overline{-1}$

Tout élément de $cl(1)$ est un représentant de cette classe

② $E = \mathbb{Z}$; $x R y \Leftrightarrow x \equiv y\ [2]$.

$cl(0) = \{$ pairs $\}$.

$cl(1) = \{$ impairs $\}$.

$E/_R$ contient deux éléments, les pairs et les impaires

$\Rightarrow$ $E/R = \{\bar{0}, \bar{1}\}$;

plus généralement : $x R y \Leftrightarrow x \equiv y [n]$.

$E/_R = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. ($n$ élément).

③ $E = \mathbb{Z} \times \mathbb{N}^*$; $(x,y) R (x',y') \Leftrightarrow xy' - x'y = 0$

(R est une relation d'équivalence).

$cl(x,y) = \{(x',y')$ tel que $\frac{x}{y} = \frac{x'}{y'}\}$.

$\overline{(x,y)}$ représente donc un élément de $\mathbb{Q}$.

$(2,4), (12,24) \dots$ sont tous des représentant de la $\overline{(1,2)}$

$\frac{1}{2} = \frac{2}{4} = \frac{12}{24} \dots$

Classes modulo un sous groupe :

Soit G un groupe, H un sous groupe.

Soit $a \in G$; On pose $aH = \{ax, x \in H\}$

$Ha = \{xa, x \in H\}$.

On definit sur G, deux relation, R_g et R_d.

$x R_g y \iff y \in xH$, R_g = gauche,

$x R_d y \iff y \in Hx$. R_d = droite

$x R_g y \iff y \in xH \iff y = xh, h \in H$

$\iff x^{-1}y = x^{-1}xh = h$, $h \in H$

$\iff x^{-1}y \in H$.

$x R_d y \iff yx^{-1} \in H$.

__proposition__ : R_g et R_d sont deux relations d'équivalences

__Remarque__ : si G est abélien, $R_g = R_d$

__preuve__ : • $x R_g x \iff x^{-1}x \in H \iff 1 \in H$; (H est un sous groupe)

• $x R_g y \iff x^{-1}y \in H \iff (x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} = y^{-1}x \in H$

$\iff y R_g x$.

• $x R_g y$ et $y R_g z \iff x^{-1}y \in H$ et $y^{-1}z \in H$

$\Rightarrow x^{-1}y \cdot y^{-1}z \in H \Rightarrow x^{-1}z \in H \Rightarrow x R z$

(1)

La classe de x à gauche $cl_g(x) = xH$

— — — droite $cl_d(x) = Hx$.

$x = 1$; $cl_g(1) = cl_d(1) = H$.

on peut donc former G/R_g et G/R_d.

Proposition : (a) $\begin{array}{l} H \longrightarrow Hx \\ h \longrightarrow hx \end{array}$ et $\begin{array}{l} H \longrightarrow xH \\ h \longmapsto xh \end{array}$

Sont bijectives.

(b) $i : \begin{array}{l} G \longrightarrow G \\ x \longrightarrow x^{-1} \end{array}$ est une bijection qui

envoie xH sur Hx^{-1} c.a.d. $i(xH) = Hx^{-1}$

(c) $\varphi : G/R_g \longrightarrow G/R_d$

$\bar{x}_g = xH \longrightarrow \overline{x^{-1}}_d = Hx^{-1}$

est bijective.

Preuve : (a) c'est évident.

(b) $i(xh) = (xh)^{-1} = h^{-1}x^{-1}$; de la même

on obtient donc : $i(xH) \subset Hx^{-1}$

manière on obtient $Hx^{-1} \subset i(xH)$.

(c). b) $\Rightarrow \varphi$ est bien définie

(2)

si $\varphi(\bar{x}_g) = \varphi(\bar{y}_g) \Rightarrow \bar{x^{-1}}_d = \bar{y^{-1}}_d$ ou encore

$$Hx^{-1} = Hy^{-1} \Rightarrow Hx^{-1}y = H \Rightarrow x^{-1}y \in H.$$

$$\Rightarrow y \in xH \Rightarrow x R_g y \Leftrightarrow \bar{x}_g = \bar{y}_g.$$

φ surjective : soit $\bar{y}_d \in G/_{R_d}$;

~~$\varphi(\bar{y^{-1}}$~~

$$\varphi(\bar{y^{-1}}_g) = \bar{y}_d.$$

Supposons que G est fini : la proposition précédente nous permet de dire que :

ⓐ Toute les classes d'équivalence à gauche ou à ~~de~~ droite ont le même nombre d'éléments. à savoir $|H|$.

ⓑ) il y a autant de classes à gauche ~~ou~~ et à droite, et ~~si $|xH| = |Hy|$~~ ;

Ceci nous amène à la définition suivante :

Déf : Soit G un groupe fini ;
l'indice de de H dans G, noté $[G : H]$ est
le nombre de classes d'équivalence $=$ cardinal de $G/_{R_g}$
$=$ cardinal de $G/_{R_d}$.

Exemple : ~~n~~ Soit n un entier ~~n~~ ≥ 1.

$G = \mathbb{Z}, +$; $n\mathbb{Z}$ est un sous-groupe de $G = \mathbb{Z}$.

$\mathbb{Z}$ est commutatif ; donc les classes à gauche et à droite sont les mêmes.

$$x R y \Leftrightarrow y + (-x) \in n\mathbb{Z} \Leftrightarrow x \equiv y \, [n].$$

On retrouve donc la relation congruence ~~comme une~~ ~~une relation donné par le quotient~~

$cl(0) = n\mathbb{Z}$; $cl(1) = 1 + n\mathbb{Z}$ ... , $cl(n-1) = n-1+n\mathbb{Z}$

et $\mathbb{Z}/R = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$.

Th. de Lagrange : Soit G un groupe fini, H un sous groupe de G.

$$\boxed{[G : H] = \frac{\text{Cardinal}(G)}{\text{Cardinal}(H)}}$$

En particulier : $\text{Card}(H)$ divise $\text{Card}(G)$.

On appelle ordre d'un groupe = ~~car~~ nombre d'éléments de ce groupe..

Il faut donc Retenir : l'ordre d'un sous groupe H de G divise l'ordre G (G fini) preuve : on va utiliser juste les classes à gauches :

les classes à gauches xH forment une partition de G (relation d'equivalence). :

$$G = \bigcup_{i \in [1,n]} x_i H$$

Ici : n = nombre de classe d'equivalence $= [G : H]$

$|x_i H| = H$; donc $|G| = n|H| = [G : H] . |H|$.

Corollaire 1 : Soit G un groupe fini ; soit $a \in G$, l'ordre de a divise $|G|$.

preuve : $\langle a \rangle$ est un sous groupe de G d'ordre $|\langle a \rangle|$ = ordre de a ; d'après le th de Lagrange.

ordre a divise $|G|$.

~~Corrol~~ Corollaire 2 : si G est un groupe à n élement pour tout $a \in G$, $a^n = 1$

preuve : Soit q = ordre de a ; $q | n$, $a^q = 1$

$\Rightarrow a^n = 1$ ($n = kq$, $a^n = a^{kq} = (a^q)^k = 1^k = 1$)

Exemples :

(1) $G = \{1, -1, i, -i\}$ sous groupe de $\mathbb{C}^*$

$|G| = 4$; $\forall a \in G$; $a^4 = 1$

l'ordre de a divise 4 pour tout $a \in G$.

si $a = -1$; l'ordre de $a = 2 \mid 4$.

$H = \{1, -1\}$ est un sous groupe de G ;

$|H| \mid |G|$ $\quad 2 \mid 4$.

G ne possède pas un sous groupe d'ordre 3

(2) S_3 ; $|S_3| = 6$;

$\forall \sigma \in S_3$; $\sigma^6 = I_d$;

les diviseurs positifs de 6 sont 1, 2, 3, 6.

si $\sigma \in S_3$; ordre $\sigma \in \{1, 2, 3, 6\}$.

par exemple $\tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ d'ordre 2.

$\tau_{123} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ est d'ordre 3.

groupe $\mathbb{Z}/n\mathbb{Z}$:

On va munir $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ d'une structure de groupe.

$\bar{a} + \bar{b} = \overline{a+b}$; cette loi est bien définie car si $\overline{a'} = \bar{a}$ et $\overline{b'} = \bar{b}$, $b' \neq b$, et $a' \neq a$ (des représentants différentes).

$\overline{a+b} = \overline{a'} + \overline{b'}$.

On vérifie facilement grâce aux propriétés de la congruence que $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien.

Retour sur le groupe cyclique :

Rappel : un groupe est dit monogène s'il est engendré par un seul élément ;

$G = \langle a \rangle$, a s'appelle générateur.

si de plus G est fini, i.e a est d'ordre fini

G s'appelle groupe cyclique.

proposition : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ est cyclique.

preuve : $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$

Remarque : un groupe cyclique peut avoir plusieurs générateurs.

Exemples. $\mathbb{Z}/6\mathbb{Z}$ est engendré par $\bar{1}$

mais aussi par 5 ;

$$\langle \bar{5} \rangle = \langle 0, \bar{5}, \overline{10} ; \overline{15}, \overline{20}, \overline{25} \rangle$$
$$= \langle \bar{0}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1} \rangle$$

Une première application du th de Lagrange.

Proposition : Soit G un groupe à p éléments p un nombre premier, alors G est cyclique

preuve : Soit $a \in G$, $a \neq 1$;

On a d'après Lagrange : $|\langle a \rangle| \mid p$

donc $\langle a \rangle = 1$ ou p, comme $a \neq 1$

on a $\langle a \rangle = p$ ou encore $\langle a \rangle = G$.

On a en fait montré plus : G est cyclique et tout élément $a \in G$, $a \neq 1$ est générateur de G.

i.e G est engendré par tous ses éléments $\neq 1$.

On considère un groupe G à n éléments ;

On suppose que $G = \langle a \rangle$ (G cyclique).

. Les élements de G s'écrivent a^k ; $k = 0, \dots, n-1$

On voudrait calculer l'ordre de chaque élement a^k en fonction de k et de n.

On a le résultat suivant (très utile).

<u>proposition</u> : $G = \langle a \rangle$, a d'ordre n.

$$\text{ordre}(a^k) = \frac{n}{\text{pgcd}(n,k)}.$$

<u>preuve</u> : Soit $d = \text{pgcd}(n,k)$.

$n = k'd$; ; $(k', k'') = 1$.
$k = k''d$.

$$(a^k)^{\frac{n}{d}} = a^{\cancel{k}} \cdot a^{k''\cancel{d} \times \frac{n}{\cancel{d}}} = a^{nk''} = (a^n)^{k''} = 1$$

Soit $\ell = \text{ordre}(a^k)$; $\ell \mid \frac{n}{d}$.

$1 = (a^k)^\ell = a^{k\ell} \Rightarrow k\ell$ est un multiple de n ou encore

i.e. $n \mid k\ell = k''d.\ell \mid n = k'd$, comme $(k'', k') = 1$, par

$k' \mid k''\cancel{d}\ \cancel{\ell}\ \cancel{k'}$; le lemme de Gauss : On a : $\cancel{d} \mid \cancel{k'}$; $k' \mid \ell$

~~donc~~ $\cancel{\ell\ \ell}\ \cancel{n = k'd}$ et enfin $\boxed{\ell = \frac{n}{d}}$

$\frac{n}{d} \mid \ell$

(9)

4

Corollaire : Soit C_n un groupe cyclique à n élément, $C_n = \langle a \rangle$; les générateurs de C_n sont a^k ; avec $(k, n) = 1$

Exemples : $G = \mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle$; les generateurs de G sont $\bar{k}.\bar{1} = \bar{k}$ avec $(k, 12) = 1$; on trouve.

$\bar{k} = 1$, $\bar{k} = 5$, $\bar{k} = 7$, $\bar{k} = 11$

Calculons les ordres des autres éléments :
les ordres possibles sont les diviseurs de 12.
donc 1, 2, 3, 4, 6, 12.

1 ⟹ élément neutre

12 — les generateurs

les éléments d'ordre 2, ~~k.1~~

$$\text{ordre } \bar{k} = \text{ordre}(\bar{k}.1) = \frac{n}{(k,n)} = 2$$

$\text{ordre}(\bar{k}) = 2 = \frac{12}{(k,n)}$, i.e. $\text{pgcd}(k, n) = 6$.

c.a.d $k = 6$, un seul élément.

l'ordre 3 : k tel que $\text{pgcd}(k, 12) = 4$

c.a.d $\bar{4}$ et $\bar{8}$.

ordre 4 : $\bar{3}$, $\bar{9}$

ordre 6 : $\bar{2}$, $\bar{10}$