Cours du Samedi 21 Juin.

Introduction : rappels sur les ensembles.

I) Groupes.

Définition. Un groupe est la donnée d'un ensemble G et d'une loi de composition interne notée $*$ définie de la manière suivante :

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (x, y) & \longmapsto & x * y \end{array}$$

et telle que $(G, *)$ vérifie les trois propriétés suivantes :
(1) (Elément neutre) Il existe e dans G tel que $\forall\, x \in G$, $e * x = x * e = x$.
(2) (Associativité) Pour tout x, y, $z \in G$, $(x * y) * z = x * (y * z) = x * y * z$.
(3) (Elément inverse) Pour tout x dans G, il existe x' dans G tel que : $x * x' = x' * x = e$. On pourra noter : $x' = x^{-1}$ à ne pas confondre avec la notation $\frac{1}{x}$.
Si de plus $\forall\, x$, $y \in G$, $x * y = y * x$, on dit que la loi $*$ est commutative et que $(G, *)$ est un groupe commutatif ou abélien.

Exemples : $(\mathbb{Z}, +)$ est un groupe abélien. En effet, la loi $+$ est bien une loi de composition interne de $\mathbb{Z} \times \mathbb{Z}$ dans $\mathbb{Z}$ (la somme de deux entiers relatifs est un entier relatif), $0 \in \mathbb{Z}$ est élément neutre pour la loi $+$, $+$ est associative et pour tout $x \in \mathbb{Z}$, il existe $y \in \mathbb{Z}$ tel que : $x + y = y + x = 0$: on prend $y = -x$. Enfin, la loi $+$ est commutative.

D'autres groupes seront cités par les élèves. Par contre, $(\mathbb{N}, +)$ n'est pas un groupe. En effet, $2 \in \mathbb{N}$ mais 2 n'a pas d'inverse dans $\mathbb{N}$ muni de $+$ car $-2 \notin \mathbb{N}$.

Propriétés. Soit $(G, *)$ un groupe.
1) L'élément neutre de G est unique.
2) L'inverse y d'un élément x de G est unique.
3) L'inverse de l'inverse de x est x.
4) Pour tous x,$y \in G$, $(x * y)^{-1} = y^{-1} * x^{-1}$.
5) Pour tous x, y, $z \in G$, si $x * y = x * z$ alors $y = z$.
6) Pour tout $x \in G$, pour tout $n \in \mathbb{Z}$, l'inverse de x^n est x^{-n}. On note : $(x^n)^{-1} = x^{-n}$.

Définition. Un groupe dit fini est un groupe qui a un nombre fini d'éléments. Son nombre d'éléments est appelé ordre ou cardinal et est noté : Card G ou $\#(G)$.

Définition. Soit $(G, *)$ un groupe. Soit $x \in G$.
On appelle ordre de x le plus petit entier naturel k tel que $x^k = e$ où e est l'élément neutre de G.

Exercice 1. Soit $(G, *)$ un groupe. Soit $x \in G$ d'ordre $n \geq 2$.
Montrer que $\forall\, 1 \leq m < n$, $x^m \neq e$.

Exercice 2. Soit $(G, *)$ un groupe. On suppose que tous les éléments de G sauf l'élément neutre sont d'ordre 2.
Montrer que G est commutatif.

II) Sous-groupes.

Définition. Soient $(G, *)$ un groupe et H un sous-ensemble non-vide de G. On dit que H est un sous-groupe de G lorsque les deux conditions suivantes sont vérifiées :
(1) H est stable pour la loi $*$ ($\forall\, x$, $y \in H$, $x * y \in H$).
(2) H est stable par passage à l'inverse ($\forall\, x \in H$, $x^{-1} \in H$).

Exemples.

$\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-groupes de $\mathbb{C}$ muni de l'addition mais pas $\mathbb{N}$.

Remarques.
1) Les conditions de la définition peuvent être réunies en une seule : H est un sous-groupe de G si et seulement si H est non-vide et $\forall\, x, y \in H$, $x * y^{-1} \in H$.
2) Pour montrer que H est non-vide, il est en général très facile de vérifier qu'il contient l'élément neutre de G. Si H ne contient pas l'élément neutre de G, H ne peut pas être un sous-groupe de G.
3) Tout sous-groupe d'un groupe abélien est abélien.
4) Tout groupe G admet au moins deux sous-groupes dits triviaux : G et $\{e\}$ (e étant l'élément neutre de G).

Théorème de Lagrange. Soit H un sous-groupe d'un groupe fini G. Alors H est fini et l'ordre (le cardinal) de H divise celui de G.

Démonstration.
Notons : $\#(G) = n$. Il est clair que H est fini, notons : $\#(H) = m$. Pour tout $x \in G$, notons : $xH = \{xh, h \in H\}$ (ce sous-ensemble est appelé la classe de x à gauche modulo H).

D'une part, pour tout $x \in G$, l'ensemble xH est formé de m éléments. En effet, si l'on note $H = \{h_1, h_2, ..., h_m\}$, $h_i \neq h_j\ \forall\, i \neq j$, alors xH est l'ensemble des éléments de la forme xh_i pour $1 \leq i \leq m$ et $xh_i \neq xh_j$ lorsque $i \neq j$ (car $xh_i = xh_j$ implique $h_i = h_j$ donc $i = j$).

D'autre part, l'ensemble des classes xH distinctes obtenues lorsque x décrit G est une partition de G. En effet, tout $x \in G$ s'écrit $x = xe$ avec $e \in H$ donc $x \in xH$. Ceci prouve que G est inclus dans la réunion des classes xH et donc que G est cette réunion car l'autre inclusion est triviale.
Il reste à vérifier que deux classes distinctes xH et yH sont disjointes.
Pour cela, supposons qu'il existe $z \in xH \cap yH$ i.e : il existe h', $h'' \in H$ tels que : $z = xh' = yh''$. Tout élément xh de xH s'écrit alors : $xh = (yh''h'^{-1})h = y(h''h'^{-1}h)$ avec $h''h'^{-1}h \in H$ et donc $xh \in yH$. On conclut alors que $xH \subseteq yH$. L'inclusion réciproque s'obtient de même et l'on déduit que $xH = yH$. On a ainsi prouvé que deux classes non disjointes sont égales d'où on a le résultat voulu par contraposée.
On a finalement : $n = mq$ où q désigne le nombre de classes xH distinctes obtenues lorsque x décrit G. Ainsi, m divise n.

Définition et propriété. Soient G un groupe et x un élément de G. On appelle sous-groupe monogène engendré par x dans G le sous-groupe engendré par le singleton $\{x\}$. On le note $< x >$. C'est le plus petit sous-groupe de G contenant x et l'on a : $< x >= \{x^m, m \in \mathbb{Z}\}$.

Preuve. Le sous-groupe $< x >$ contient x donc (par stabilité pour la loi de G), il contient aussi $x.x = x^2$, $x^2.x = x^3$ et par récurrence x^m pour tout entier $m \geq 1$. Il contient aussi nécessairement le symétrique x^{-1} de x donc aussi $x^{-1}.x^{-1} = x^{-2}$ et par récurrence x^{-m} pour tout entier $m \geq 1$. Enfin, il contient le neutre $e = x.x^{-1}$ que l'on note par convention : x^0. Ceci montre que $< x > \supseteq \{x^m, m \in \mathbb{Z}\}$. Il est clair réciproquement que $\{x^m, m \in \mathbb{Z}\}$ est un sous-groupe de G contenant x.

Propriété. Soit G un groupe. Soit x un élément de G. Si x est d'ordre fini $n \geq 1$ dans G, alors le sous-groupe $< x >$ est fini d'ordre n et l'on a : $< x >= \{e, x, x^2, x^3, ..., x^{n-1}\}$.

Preuve. Soit x^m avec $m \in \mathbb{Z}$, un élément quelconque de $< x >$. Par division euclidienne de m par n, il existe des entiers uniques q et r tels que : $m = nq + r$ avec $0 \leq r \leq n - 1$. On a : $x^m = x^{nq+r} = (x^n)^q.x^r = e^q.x^r = x^r$ ce qui prouve que $< x >$ est inclus dans l'ensemble $E = \{x^r, 0 \leq r \leq n - 1\}$. La réciproque étant claire, on a : $< x >= E$. Il reste à vérifier que E est formé des n éléments distincts : e, x, x^2, x^3 , ... , x^{n-1}. Pour cela, supposons que $x^i = x^j$ avec $0 \leq i, j \leq n - 1$, alors $x^{i-j} = e$ avec $-n < i - j < n$, ce qui, par minimalité de l'ordre n de x, implique $i - j = 0$ donc $i = j$. On a donc bien $E = \{e, x, x^2, ..., x^{n-1}\}$.

Propriété. Soit G un groupe fini de cardinal n. Soit x un élément de G d'ordre m.
Alors m divise n.

Preuve. On a vu que, comme x est d'ordre m, le sous-groupe $< x >$ de G s'écrit : $< x >= \{e, x, x^2, ..., x^{m-1}\}$. Ce sous-groupe de G a m éléments donc par le théorème de Lagrange, on en déduit que m divise n.

Exercice 3. Soit G un groupe.
Que dire des sous-groupes de G si G est de cardinal 1 ? De cardinal 2 ? De cardinal 3 ? De cardinal premier p ?

Exercice 4. Soit G un groupe (muni d'une loi de composition interne $*$) de cardinal 4. On note e l'élément neutre de G.
1) Montrer que G peut s'écrire sous la forme : $\{e, x, y, z\}$ (où x, y et z sont 3 éléments de G deux à deux distincts et tous distincts de e).
2) Montrer que x, y et z sont chacun d'ordres 2 ou 4.
3) Dans cette question uniquement, on suppose que x, y et z sont chacun d'ordre 2.
Déterminer tous les sous-groupes de G dans ce cas.
On suppose maintenant que y est l'inverse de x.
4) Montrer que x et y sont d'ordres 4 et que z est d'ordre 2.
5) Montrer que $x^2 = x * x = z$ et que $x^3 = x * x * x = y$.
6) Déterminer tous les sous-groupes de G dans ce cas.

III) Morphismes de groupes.

Définition. Soient G un groupe muni d'une loi de composition interne . et G' un groupe muni d'une loi de composition interne $*$. On appelle morphisme de groupes ou homomorphisme de groupes de G dans G' toute application $f : G \longrightarrow G'$ telle que : $\forall\, x, y \in G$, $f(x.y) = f(x) * f(y)$.

Exemple. L'application $\exp : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ qui à tout nombre réel associe son exponentielle est un morphisme de groupes de $\mathbb{R}$ muni de l'addition dans $\mathbb{R}_+^*$ muni de la multiplication car : $\forall\, x, y \in \mathbb{R}$, $\exp(x+y) = \exp(x).\exp(y)$.

Propriétés. Soient G un groupe muni d'une loi de composition interne . et G' un groupe muni d'une loi de composition interne $*$ et $f : G \longrightarrow G'$ un morphisme de groupes. On a :
(1) $f(e) = e'$, où e désigne l'élément neutre de G et e' celui de G'.
(2) $\forall\, x \in G$, $f(x^{-1}) = f(x)^{-1}$.
(3) $\forall\, x \in G$, $\forall\, n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.
(4) Pour tout sous-groupe H de G, l'image directe $f(H) = \{f(x), x \in H\}$ est un sous-groupe de G'.
(5) Pour tout sous-groupe H' de G', l'image réciproque $f^{-1}(H') = \{x \in G, f(x) \in H'\}$ est un sous-groupe de G.
(6) La composée de deux morphismes de groupes est un morphisme de groupes.

Exercice 5. Démontrer les 6 propriétés précédentes.

Correction :

(1) On écrit : $f(e.e) = f(e) * f(e)$ donc $f(e) = f(e) * f(e)$ ainsi, $f(e)^{-1} * f(e) = f(e)^{-1} * f(e) * f(e)$ d'où : $e' = e' * f(e)$ donc $e' = f(e)$.
(2) On a : $f(x.x^{-1}) = f(x) * f(x^{-1}) = f(e) = e'$ donc $f(x^{-1}) = f(x)^{-1}$.
(3) Soient $x \in G$ et $n \in \mathbb{N}$. Commençons par démontrer la propriété dans le cas : $n \in \mathbb{N}$.
On procède par récurrence sur n. Pour $n = 0$ on a bien : $f(x^0) = f(e) = e' = f(x)^0$.
Supposons que $f(x^n) = f(x)^n$ pour un certain rang $n \in \mathbb{N}$, on a : $f(x^{n+1}) = f(x^n.x) = f(x^n) * f(x) = f(x)^n * f(x)$ car $f(x^n) = f(x)^n$ par hypothèse de récurrence. Donc $f(x^{n+1}) = f(x)^{n+1}$.
Ainsi, $\forall\, x \in G$, $\forall\, n \in \mathbb{N}$, $f(x^n) = f(x)^n$.
Soit maintenant $n \in \mathbb{Z}^-$, alors $-n \in \mathbb{N}$ et on a : $\forall\, x \in G$, $f(x^{-n}) = f(x)^{-n}$. Or, $x^n = (x^{-n})^{-1}$ donc par la propriété (2), on a : $f(x^n) = f((x^{-n})^{-1}) = f(x^{-n})^{-1} = (f(x)^{-n})^{-1} = f(x)^n$.
(4) H est un sous-groupe de G donc e (l'élément neutre de G) est dans H et $f(e) = e'$ (e' étant le neutre de G') donc $e' \in f(H)$ et $f(H)$ est non vide.
Soient y, $z \in f(H)$. Montrons que $y * z^{-1} \in f(H)$.

y, $z \in f(H)$ donc il existe x et $x' \in H$ tels que $y = f(x)$ et $z = f(x')$. On a : $y * z^{-1} = f(x) * f(x')^{-1} = f(x) * f(x'^{-1}) = f(x.x'^{-1})$ et $x.x'^{-1} \in H$ (car x, $x' \in H$ et H est un sous-groupe de G) donc $y * z^{-1} \in f(H)$.
Ainsi, $f(H)$ est un sous-groupe de G'.
(5) H' est un sous-groupe de G' donc $e' \in H'$ et on a : $f(e) = e'$ et $e' \in H'$ donc $e \in f^{-1}(H')$ donc $f^{-1}(H')$ est non vide.
Soient x, $y \in f^{-1}(H')$. Montrons que $x.y^{-1} \in f^{-1}(H')$. On a : $f(x.y^{-1}) = f(x) * f(y^{-1}) = f(x) * f(y)^{-1}$.
Comme x, $y \in f^{-1}(H')$, $f(x)$ et $f(y) \in H'$ et comme H' est un sous-groupe de G', $f(x) * f(y)^{-1} \in H'$ donc $f(x.y^{-1}) \in H'$ ainsi, $x.y^{-1} \in f^{-1}(H')$.
D'où $f^{-1}(H')$ est un sous-groupe de G.
(6) Soient G, G' et G'' trois groupes munis respectivement des lois : ., $*$ et $\times$ et $f : G \longrightarrow G'$ et $g : G' \longrightarrow G''$ deux morphismes deux groupes.
Montrons que $g \circ f : G \longrightarrow G''$ est un morphisme de groupes.
Soient x, $y \in G$. On a : $(g \circ f)(x.y) = g(f(x.y)) = g(f(x) * f(y)) = g(f(x)) \times g(f(y)) = (g \circ f)(x) \times (g \circ f)(y)$.
Donc $g \circ f : G \longrightarrow G''$ est un morphisme de groupes.

Définitions-propriétés. Soient G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes.

(1) L'ensemble $f(G) = \{f(x), x \in G\}$ est un sous-groupe de G' appelé image de f et noté $\mathrm{Im}\, f$.
(2) L'ensemble $f^{-1}(\{e'\}) = \{x \in G, f(x) = e'\}$ est un sous-groupe de G, appelé noyau de f et noté $\mathrm{Ker}\, f$.

Preuves. Pour (1), G est un sous-groupe de G donc par la propriété précédente, $f(G) = \mathrm{Im}\, f$ est un sous-groupe de G'. Pour (2), $\{e'\}$ est un sous-groupe de G' donc par la propriété précédente, $f^{-1}(\{e'\}) = \mathrm{Ker}\, f$ est un sous-groupe de G.

Propriété. Soient G (muni de .) et G' (muni de $*$) deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes.

(1) f est surjective si et seulement si $\mathrm{Im}\, f = G'$.
(2) f est injective si et seulement si $\mathrm{Ker}\, f = \{e\}$.

Preuve. Le point (1) est immédiat par la définition même de la surjectivité.
Pour (2), supposons d'abord f injective. Soit $x \in \mathrm{Ker}\, f$ alors $f(x) = e' = f(e)$ donc par injectivité de f, $x = e$.
Ainsi, $\mathrm{Ker}\, f = \{e\}$.
Réciproquement, supposons que $\mathrm{Ker}\, f = \{e\}$. Soient $x, y \in G$ tels que $f(x) = f(y)$, on a donc $f(x) * f(y)^{-1} = e'$ ainsi, $f(x.y^{-1}) = e'$ donc $x.y^{-1} \in \mathrm{Ker}\, f$ donc $x.y^{-1} = e$ donc $x = (y^{-1})^{-1} = y$. Ainsi, f est injective.

Définitions. Soit G un groupe.
Un morphisme de groupes bijectif est un isomorphisme de groupes.
Un morphisme de groupes bijectif de G dans lui-même est appelé : automorphisme de groupes.

Propriété. Si f est un isomorphisme de groupes de G (muni de .) dans G' (muni de $*$), alors la bijection réciproque f^{-1} est un isomorphisme de groupes de G' dans G.

Preuve. Posons : $x = f^{-1}(x')$ et $y = f^{-1}(y')$. Puisque f est un morphisme de groupes, on a : $\forall\, x, y \in G$, $f(x.y) = f(x) * f(y)$ donc $f(x.y) = x' * y'$ ainsi, $x.y = f^{-1}(x' * y')$ d'où $\forall\, x', y' \in G'$, $f^{-1}(x' * y') = f^{-1}(x').f^{-1}(y')$.
Donc f^{-1} est un morphisme de groupes de G' dans G.

Définition. Soient G et G' deux groupes. On dit que G et G' sont isomorphes s'il existe un isomorphisme de groupes de G dans G'. On note : $G \simeq G'$.

Exercice 6. Soient G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes.
Soit $x \in G$ d'ordre $n \geq 1$. Montrer que $f(x)$ est d'ordre au plus n.

Exercice 7. Soit $(G, \times)$ un groupe. On note e son élément neutre.
Pour $a \in G$, on note τ_a l'application de G dans G définie par : $\tau_a(x) = axa^{-1}$.
1) Que vaut τ_e ?

2) Montrer que τ_a est un morphisme de groupes de G dans lui-même.
3) Vérifier que $\forall\ a, b \in G$, $\tau_a \circ \tau_b = \tau_{ab}$.
4) Montrer que l'application τ_a est bijective et déterminer sa bijection réciproque.
5) En déduire que $\mathcal{T} = \{\tau_a, a \in G\}$ muni de la composition : $\circ$ est un groupe.

Exercice 8. Soient $(G, *)$ un groupe et $a \in G$.
On définit une loi de composition interne $\top$ sur G par $x \top y = x * a * y$.
1) Montrer que $(G, \top)$ est un groupe.
2) Soient H un sous-groupe de $(G, *)$ et $K = a^{-1} * H = \{a^{-1} * x, x \in H\}$.
Montrer que K est un sous-groupe de $(G, \top)$.
3) Montrer que $f : x \longmapsto x * a^{-1}$ est un isomorphisme de $(G, *)$ dans $(G, \top)$.