Groupes.

1. Une **loi de composition** sur un ensemble E est une application de $E \times E$ dans E.

La loi est **associative** si $(ab)c = a(bc)$ quel que soient $a, b, c \in E$.

La loi est **commutative** si $ab = ba$ quel que soient $a, b \in E$.

Si la loi est associative, on peut définir de façon unique, pour tout n, le produit ordonné de n éléments $a_1, ..., a_n$ de E tel que pour tout $k < n$ on a $a_1...a_n = (a_1...a_k)(a_{k+1}...a_n)$.

2. Un élément e de E est **neutre** si pour tout $a \in E$ on a $ae = ea = a$.

Lemme. Il existe au plus un élément neutre.

3. Si E admet un élément neutre e, on dit que a est **inversible** s'il existe un élément a', appelé **inverse** de a, tel que $aa' = a'a = e$.

Lemme. Si la loi est associative, il existe au plus un inverse de a, noté a^{-1}.

.

4. Un ensemble muni d'une loi de composition associative s'appelle **semi-groupe**. Un semi-groupe avec un élément neutre s'appelle **monoïde**. Un monoïde dans lequel tous les éléments sont inversibles s'appelle **groupe**.

Lemme. L'ensemble des éléments inversibles d'un monoïde est un groupe.

.

Exemple. Soit X un ensemble et E l'ensemble de toutes les applications de X dans X; la composition des applications fait de E un monoïde. Les applications inversibles (les bijections $X \to X$) constituent le **groupe des permutations** de X, noté $S(X)$.

Exemple. Soit V un espace vectoriel et E l'ensemble de toutes les endomorphismes de V; c'est un monoïde par rapport à la composition (en fait, c'est une *algèbre*). Les endomorphismes inversibles constituent le **groupe linéaire** de V, noté $GL(V)$.

Exemple: $(\mathrm{Z}/n\mathrm{Z}, \times)$ est un monoïde par rapport à la mutiplication (noter que $\mathrm{Z}/n\mathrm{Z}$ est un anneau). La classe de k est inversible modulo n si et seulement si k est premier avec n. Le groupe des classes inversibles - le groupe multiplicatif de $\mathrm{Z}/n\mathrm{Z}$ - sera noté $(\mathrm{Z}/n\mathrm{Z})^*$.

.

Le nombre d'éléments du groupe G s'appelle **l'ordre** de G et se note $|G|$.

.

5. Une partie H du groupe G est un **sous-groupe** de G si H est non-vide, stable pour la loi et si avec tout son élément H contient son inverse (donc si $a \in H$ et $b \in H$ alors $ab \in H$ et $a^{-1} \in H$).

.

Lemme. Les sous-groupes de $(\mathrm{Z}, +)$ sont de la forme $n\mathrm{Z}$.

Lemme. Une intersection de sous-groupes est un sous-groupe.

Soit G un groupe et A une partie non-vide de G. Le sous-groupe de G **engendré** par A, noté $< A >$, est l'intersection de tous les sous-groupes qui contiennent A; c'est le plus petit sous-groupe contenant A.

Lemme. $< A >$ consiste de tous les produits des éléments de A et de leurs inverses.

Si $< A >= G$, on dit que A **engendre** G .

Lemme. On a $< k, n >= d\mathrm{Z}$ où $d = pgcd(k, n)$ et $k\mathrm{Z} \cap n\mathrm{Z} = m\mathrm{Z}$ où $m = ppcm(k, n)$.

Corollaire. Le sous-groupe du groupe additif $(Z/nZ, +)$ engengré par k est dZ/nZ , où $d = \mathrm{pgcq}(k, n)$. L'ordre de ce sous-groupe est $n/\mathrm{pgcq}(k, n)$.

En particuleir, k engendre le groupe additif $(Z/nZ, +)$ si et seulement si k est premier avec n.

.

6. Morphismes. Soit G et G' deux groupes; une application $f : G \to G'$ est un **morphisme** de groupes si $f(ab) = f(a)f(b)$ quels que soit $a, b \in G$.

Lemme. $f : G \to G'$ est un **morphisme** de groupes, on a $f(e) = e'$ et $f(a^{-1}) = f(a)^{-1}$.

.

La composée de deux morphismes est un morphisme. Si un morphisme f est bijectif, son inverse f^{-1} est un morphisme; dans ce cas f est un **isomorphisme**. L'isomorphisme est une relation d'équivalence entre les groupes. Si les groupes sont isomorphes, leurs propriétés algébriques sont identiques.

Exemple. Soit $a \in G$; alors $f : Z \to G$ défini par $f(k) = a^k$ est un morphisme.

Remarque: on définit de même façon les morphismes des monoïdes, d'anneaux, etc.

Exemple. L'application $f : Z \to Z/nZ$ qui associe à l'entier k sa classe modulo n est un morphisme d'anneaux (l'addition et la multiplication dans Z/nZ sont définies de façon à ce que f soit un morphisme).

L'ensemble de tous les morphismes $f : G \to G$ est un monoïde; les morphismes bijectifs forment le groupe des automorphismes de G.

Exemple. Soit $a \in G$ et $f_a(b) = aba^{-1}$, alors $f_a : G \to G$ est un automorphisme de G. L'application qui fait correspondre à $a \in G$ l'automorphisme f_a est un morphisme de G dans le groupe des automorphismes de G.

Soit $f : G \to G'$ un morphisme de groupes. On définit le **noyau** de f par $\mathrm{Ker}(f) = \{x \in G : f(x) = e'\}$. $\mathrm{Ker}(f)$ est un sous-groupe de G. L'image $\mathrm{Im}(f)$ est un sous-groupe de G'.

.

7. Lemme. a) Si H est un sous-groupe de G, $f(H)$ est sous-groupe de G'. Si H' est un sous-groupe de G', $f^{-1}(H')$ est sous-groupe de G.

b) f est injectif si et seulement si $\mathrm{Ker}(f) = \{e\}$.

c) $|G| = |Ker(f)||Im(f)|$.

.

8. Un groupe est dit **monogène** s'il est engengré par un seul élément; un groupe monogène fini est dit **cyclique**.

Exemples: $(\mathrm{Z}, +)$; $(\mathrm{Z}/n\mathrm{Z}, +)$.

Remarque: autrement dit, un groupe est monogène si il est l'image homomorphe de Z.

Soit $a \in G$; **l'ordre** de a est le plus petit entier $k > 0$ tel que $a^k = e$; si un tel k n'existe pas, on dit que l'ordre de a est infini.

En particulier, un groupe fini est cyclique si et seulement si il contient un éélément dont l'ordre est égal à l'ordre du groupe.

Structure des groupes cycliques.

9. Proposition. a) L'image homomorphe d'un groupe cyclique est cyclique.

b) Tout sous-groupe d'un groupe cyclique est cyclique.

c) Deux groupes cycliques de même ordre sont isomorphes. Un groupe cyclique d'ordre n est isomorphe à $(\mathrm{Z}/n\mathrm{Z}, +)$. Un groupe monogène infini est isomorphe à $(\mathrm{Z}, +)$

d) Soit G un groupe cyclique d'ordre n et H un sous-groupe de G. Alors l'ordre de H divise n et pour tout diviseur d de n il existe un seul sous-groupe H_d d'ordre d: on a $H_d = \{x \in G : x^d = e\}$.

.

10. L'indicatrice d'Euler $\varphi(n)$ est le nombre d'entiers entre 1 et n qui sont permiers avec n. Noter que $\varphi(n)$ est égale au nombre de générateurs du groupe additif $(\mathrm{Z}/n\mathrm{Z}, +)$ et à l'ordre du groupe multiplicatif $(\mathrm{Z}/n\mathrm{Z})^*$.

Si p est premier, $\varphi(p) = p - 1$.

Lemme. Soit G un groupe cyclique d'ordre n et d un diviseur de n. Le nombre d'éléments de G d'ordre d est égal à $\varphi(d)$.

Corollaire: formule d'Euler. $\sum_{d|n} \varphi(d) = n$.

.

Groupe des permutations.

.

1. On dit que le groupe G **agit** (ou *opère*) sur un ensemble E si on a un morphisme ϕ de G dans le groupe des permutations de E: pour tout $g \in G$, $\phi(g) \in S(E)$ et $\phi(gh) = \phi(g)\pi(h)$.

.

2. Theorème (Cayley). Tout groupe est isomorphe à un sous-groupe du groupe des permutations. Plus précisement, G est isomorphe à un sous-groupe de $S(G)$.

[Il suffit de considérer l'action de G sur G par les "translations": $\phi(g)(h) = gh$.]

.

On utilisera l'abréviation: $\phi(g)(x) = g \cdot x$.

Soit $E = [1, n]$; par définition, le groupe S_n agit sur E.

3. La permutation circulaire de k entiers $i_1, ..., i_k$, notée $(i_1, ..., i_k)$, envoie i_j en i_{j+1}, envoie i_k en i_1 et laisse fixes les autres éléments. Une telle permutation s'appelle **cycle** de longuer k ; l'ensemble $\{i_1, ..., i_k\}$ est son **support**.

Les cycles de supports disjoints commutent entre eux.

Une **transposition** est un cycle de longueur 2.

4. Lemme. Toute permutation se décompose en produit des transpositions.

.

Changement de numérotation. Soit σ une permutation des objets numérotés par les entiers de 1 à n. On change les numéros; au lieu de i le nouveau numéro sera $\rho(i)$, où ρ est une bijection de $[1, n]$ sur $[1, n]$. Alors par rapport à la nouvelle numérotation σ s'écrira comme $\sigma' = \rho\sigma\rho^{-1}$, le résultat de la conjugaison de σ par ρ.

Les permutations conjugées ont les mêmes propriétés algébriques.

.

5. Soit E un ensemble sur lequel agit le groupe G. Une partie F de E est **invariante** ou **stable** par G si pour tout $g \in G$ et tout $x \in F$ on a $g \cdot x \in F$.

Soit $x \in E$; la G-**orbite** de x est l'ensemble $O_x = \{g \cdot x, g \in G\}$. Toute orbite est invariante.

6. Lemme. Les 3 propriétés suivantes sont équivalentes:

i) $x \in O_y$

ii) $y \in O_x$

iii) $O_x = O_y$.

Corollaire. E est la réunion des orbites deux à deux disjointes.

Soit $\sigma \in S_n$. Le sous-groupe $< \sigma >$ agit sur $[1, n]$ et l'ensemble $[1, n]$ se décompose en orbites sous l'action (des puissances) de σ. Sur chaque orbite la permutation σ agit comme un cycle dont la longueur est le cardinal de l'orbite: on peut écrire $O = \{i_1, ..., i_l\}$ et $\sigma(i_k) = i_{k+1}$, $\sigma(i_l) = i_1$. On définit le cycle correspondant $c_O = (i_1, ..., i_l)$ et on a $\sigma = \prod_{orbites} c_O$.

(les orbites singletons - les points fixes de σ - ne comptent pas parce que pour elles $c_O = id$).

.

7. Proposition. Toute permutation se décompose en produit des cycles de support disjoints. Cette décomposition est unique à l'ordre de facteurs près.

8. Corollaire. a) Soit $l_1, ..., l_k$ les longueurs des cycles dans la décomposition de σ. Alors l'ordre de σ est égal à ppcm$(l_1, ..., l_k)$.

b) Deux permutations sont conjuguées si et seulement si elles ont les mêmes listes des longueurs des cycles dans leurs décomposition en produit des cycles disjoints.

.

9. Signature. Lemme. Soit $\pi \in S_n$. Les expressions suivantes donnent le même résultat:

1. $\text{sign}(\pi) = (-1)^r$, si π se décompose en produit de r transpositions.

2. $\text{sign}(\pi) = (-1)^{n+o(\pi)}$, où $o(\pi)$ est le nombre des orbites de π (le nombre de cycles plus le nombre de points fixes de π).

3. $\text{sign}(\pi) = (-1)^{I(\pi)}$, où $I(\pi)$ est le nombre d'inversions pour π - le nombre de paires (i, j) tels que $i < j$ mais $\pi(i) > \pi(j)$.

4. $\text{sign}(\pi) = \prod_{i<j}(\pi(i) - \pi(j))/(i - j)$.

La **signature** de π est définie par une de ces formules.

10. Lemme. $\text{sign}(\pi\sigma) = \text{sign}(\pi)\ \text{sign}(\sigma)$. Aurement dit, *sign* est un morphisme de S_n dans le groupe multiplicatif $\{1, -1\}$.

.

Quelques résultats supplémentaires.

.

1. Propriétés de l'ordre d'un élément.

Lemme. a) L'ordre de a est égal à l'ordre du sous-groupe engendré par a.

b) Si $a^n = e$, alors ord(a) divise n.

c) Un groupe fini G est engendré par a si et seulement si ord$(a) = |G|$.

d) Si ord$(a) = n$, alors ord$(a^k) = n/pgcd(k, n) = ppcm(k, n)/k$.

e) Si $G =< a >$, alors a^k est un générateur de G si et seulement si k est premier avec n.

f) $\text{ord}(ab) = \text{ord}(ba)$.

g) Soit $\text{ord}(a) = k$, $\text{ord}(b) = n$ et $ab = ba$. Alors $\text{ord}(ab)$ est fini et divise $ppcm(k, n)$.

h) Si G est commutatif, l'ensemble d'éléments d'ordre fini est un sous-groupe de G.

i) Soit $\text{ord}(a) = k$, $\text{ord}(b) = n$ et $ab = ba$. Alors $\text{ord}(ab) = kn$ si et seulement si k est premier avec n.

2. Produit des groupes. Etant donné deux groupes G_1 et G_2 on définit dans l'ensemble $G_1 \times G_2$ la loi du **groupe-produit** ou **produit direct** "composante par composante": $(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2)$. Cette définition s'étend à un nombre quelconque de groupes. (On définit de même façon le produit de monoïdes et des anneaux.)

Lemme. Le produit de deux groupes cycliques est cyclique si et seulement si leurs ordres sont premiers entre eux.

.

3. Théorème chinois. Soit k et n premiers entre eux. Alors l'anneau $\mathrm{Z}/kn\mathrm{Z}$ est isomorphe à l'anneau produit $\mathrm{Z}/k\mathrm{Z} \times \mathrm{Z}/n\mathrm{Z}$.

[Il suffit d'associer à la classe $a \pmod{kn}$ le couple ($a \pmod{k}$, $a \pmod{n}$).]

.

Corollaire. Soit k et n premiers entre eux. Alors le groupe multiplicatif $(\mathrm{Z}/kn\mathrm{Z})^*$ est isomorphe au produit $(\mathrm{Z}/k\mathrm{Z})^* \times (\mathrm{Z}/n\mathrm{Z})^*$.

Corollaire. Multiplicativité de l'indicatrice d'Euler. Soit k et n premiers entre eux. Alors $\varphi(kn) = \varphi(k)\varphi(n)$.

Si $n = p_1^{a_1}...p_l^{a_l}$ la décomposition de n en facteurs premiers,

$\varphi(n) = (p^{a_1} - p^{a_1-1})...(p^{a_l} - p^{a_l-1})$.

.

4. Théorème de Lagrange. Dans un groupe fini l'ordre de tout sous-groupe divise l'ordre du groupe.

Corollaire. a) Dans un groupe fini l'ordre de tout élément divise l'ordre du groupe.

b) Tout groupe d'ordre premier est cyclique.

Appliqué au groupe $(\mathrm{Z}/n\mathrm{Z})^*$, le corollaire a) donne

5. Théorème d'Euler. Si k est premier avec n, on a $k^{\varphi(n)} = 1 \pmod{n}$.

Corollaire: petit théorème de Fermat. Si p est premier qui ne divise pas k, alors $k^{p-1} = 1 \pmod{p}$.

6. Théorème de Cauchy. Soit G un groupe fini net p un diviseur premier de l'ordre de G. Alors G possède un élément d'ordre p.

Corollaire. Un groupe fini commutatif dont l'ordre n'est pas divisible par un carré est cyclique.

7. Théorème. Tout groupe commutatif fini est isomorphe au produit direct des groupes cycliques.

8. Théorème. Tout groupe commutatif engendré par un nombre fini d'éléments est isomorphe au produit direct des groupes monogènes.