→ Voici les groupes.

Une nouveauté du XIXe siècle, les groupes se trouvent maintenant à tous les coins de rues mathématiques !

Principalement des rappels de Licence 2.

■ Définition.

Un **groupe** $(A, \circledast)$ est un ensemble A avec une loi $\circledast$, qui satisfait ces propriétés :

- la loi est interne : $\forall a, b \in A, a \circledast b \in A$
- il existe un neutre : $\exists e \in A, \forall a \in A, a \circledast e = e \circledast a = a$
- tout élément a un inverse : $\forall a \in A, \exists b \in A, a \circledast b = b \circledast a = e$
- la loi est associative : $\forall a, b, c \in A, (a \circledast b) \circledast c = a \circledast (b \circledast c)$.

Alors, ces 4 "axiomes" suffisent à déduire, par exemple, que le neutre est unique dans le groupe, et que chaque élément n'admet qu'un inverse. La loi peut être notée de plein de manières ; le plus souvent, c'est un "$+$", un "$\times$" ou sans symbole, comme on le fait avec la multiplication classiquement. Souvent, on oubliera même de préciser la loi quand on donnera un groupe, en parlant du groupe G plutôt que du groupe $(G, \circledast)$.

Un cas particulier de groupe est celui des groupes **abéliens**/**commutatifs**, où tous les éléments commutent : $\forall x, y \in G, x \circledast y = y \circledast x$.

■ Exemples.

Voici quelques exemples de groupes : $\{e\}$ avec un produit défini par $e \circledast e = e$, $\{-1, +1\}$ avec la multiplication, $(\mathbb{Z}, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{Q}^{*+}, \times)$, et ainsi de suite. Pour un groupe fini, on appelle **ordre** son cardinal.

■ Table de Cayley.

Pour un groupe fini, on peut former une **table de Cayley** (de multiplication) en choisissant un ordre des éléments, qu'on notera alors $g_1, \cdots, g_n$, et en formant un tableau contenant en position (i, j) le produit $g_i g_j$. Par exemple :

$\times$	1	-1
1	1	-1
-1	-1	1

$+_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

On définira $\mathbb{Z}/3$ plus tard. On dira que deux groupes G et H sont **isomorphes** si on peut passer de la table de Cayley de l'un, à celle de l'autre en renommant les éléments, et permutant les lignes/colonnes. Intuitivement, si ils "ont la même structure de groupe" ; on définira ça rigoureusement plus loin. Mais ça suffit à montrer qu'il n'y a, à isomorphisme près, qu'un groupe d'ordre 2 ou d'ordre 3. Remarque : un groupe abélien a une table de Cayley symétrique.

■ Équations.

Une équation de la forme $ax = b$ avec $a, b \in G$ fixés a exactement une solution, qui est $x = a^{-1}b$; similairement, $xa = b$ a exactement une solution, $x = ba^{-1}$. Ainsi, chaque élément du groupe apparaît exactement une fois par ligne et colonne de la table de Cayley du groupe.

■ Puissances et ordre.

On peut construire des **puissances** en appliquant de manière répétée la loi du groupe à un même élément. C'est-à-dire, on pose $x \circledast \cdots \circledast x$ avec n termes ($n \in \mathbb{N}^*$) la n-ième puissance de x ; et on note x^n ou nx selon la convention utilisée. On définit aussi $x^n = (x^{-1})^{-n}$ pour les n négatifs, et $x^0 = e$. On a alors que $x^{a+b} = x^a x^b$ et $x^{ab} = (x^a)^b$ pour tout $x \in G$ et tous $a, b \in \mathbb{Z}$.

Soit G groupe, et $x \in G$; si il existe, on appelle **ordre** de g (noté $\mathrm{ord}(g)$) le plus petit $n \in \mathbb{N}^*$ tel que $x^n = e$. Sinon, on dira que x est d'ordre infini.

■ Sous-groupe.

Si $(G, \circledast)$ est un groupe, un **sous-groupe** de G est un groupe formé d'un sous-ensemble $H \subseteq G$ et de la loi $\circledast$ restreinte à H. Une condition nécessaire et suffisante est que $e \in H$, $\forall x, y \in H, xy \in H$ et $\forall x \in H, x^{-1} \in H$. L'intersection de sous-groupes est aussi un sous-groupe.

■ Sous-groupe engendré.

D'ailleurs, le **sous-groupe engendré** par des éléments $x_1, \cdots, x_n \in G$ est défini comme le plus petit sous-groupe de G (pour l'inclusion) qui contienne $x_1, \cdots, x_n$. On peut le construire comme

$$\langle x_1, \cdots, x_n \rangle = \cap_{H \text{ sous-groupe de } G x_1, \cdots, x_n \in H} H$$

En particulier $\langle x \rangle = \{x^k : k \in \mathbb{Z}\}$.

■ Produits de groupe.

On peut définir le **produit** de deux groupes $(G, +)$ et $(H, \cdot)$ comme $(G \times H, *)$ avec la loi $*$ définie comme $(g_1, h_1) * (g_2, h_2) = (g_1 + g_2, h_1 \cdot h_2)$. Il contient, comme sous-groupes, $G \times \{e_H\}$ isomorphe à G et $\{e_G\} \times H$ isomorphe à H.

■ Conjugué.

Par la suite, on utilise souvent le conjugué de x par g, gxg^{-1} $(x, g \in G)$.

→ Cycliques et morphismes.

Un des types de groupes les plus connus, en tout cas il est facile à engendrer.

La motivation.

D – Un groupe est engendré par tous ces éléments, non ?
T - Oui, mais c'est plus intéressant de trouver le plus petit ensemble qui engendre ton groupe. On peut l'utiliser pour construire une présentation : une méthode d'expliciter un groupe par des générateurs et les relations qui les lient.
D - Et le cas le plus simple serait ...
T - Les groupes engendrés par un seul élément x, avec possiblement une condition $x^n = e$.

Groupe cyclique.

Un groupe **cyclique** est un groupe qu'on peut engendrer avec un de ses éléments : $G = \langle x \rangle$ pour au moins un des $x \in G$. Cet élément est appelé **générateur**. Par exemple $\mathbb{Z}$ est cyclique, car engendré par 1. On peut former le groupe des racines n-ièmes de l'unité : $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$, qui est engendré par $x = e^{\frac{2\pi i}{n}}$.

Les groupes cycliques sont abéliens.

Générateurs.

Un groupe fini G est cyclique si et seulement si il contient un élément x d'ordre $|G|$, qui est alors un générateur de G.

On a une caractérisation des générateurs : si x engendre G, alors : si x est d'ordre infini, x et x^{-1} sont les seuls générateurs ; sinon, si x est d'ordre n fini, un élément $y = x^k$ est générateur de G si et seulement si $\text{pgcd}(k, n) = 1$.

Sous-groupes.

Un sous-groupe d'un groupe cyclique est aussi cyclique. Pour un groupe cyclique fini d'ordre n, on a donc exactement un sous-groupe (cyclique) d'ordre d de G, pour tout $d|n$.

Classification.

De plus, deux groupes cycliques infinis sont isomorphes, et deux groupes cycliques finis de mêmes cardinaux sont isomorphes. Donc : tout groupe cyclique est ou bien isomorphe à $\mathbb{Z}$, ou isomorphe à un $\mathbb{Z}/n\mathbb{Z}$ pour un $n \in \mathbb{N}^*$.

Les ensembles $\mathbb{Z}/n\mathbb{Z}$.

Soit $n \in \mathbb{N}^*$. On peut poser une **relation d'équivalence** R sur $X = \mathbb{Z}$ par $x \sim y \Leftrightarrow n|(x-y)$, qu'on note souvent $x \equiv y (\text{mod })$ (congruence modulo n). Alors, on peut poser les **classes d'équivalence** $[x]_R = \{y \in X : y \sim\} \subseteq X$. On dit que x est un représentant de la classe $[x]_R$. Note : si $x \sim y$, alors $[x]_R = [y]_R$. Dans notre cas, on note $[k]_n$ la classe d'équivalence de k, et c'est $k + n\mathbb{Z}$. L'ensemble des classes d'équivalence, noté X/R est dans notre cas $\{[0]_n, \cdots, [n-1]_n\}$. Cet **ensemble quotient** est souvent noté $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/n$ ou $\mathbb{Z}_n$.

Les groupes $\mathbb{Z}/n\mathbb{Z}$.

On peut maintenant définir une loi de composition par $[x]_n + [y]_n := [x+y]_n$, qui ne dépend pas des représentants choisis. Muni de cette loi, $\mathbb{Z}/n\mathbb{Z}$ forme un groupe abélien de cardinal n. On peut explicitement réécrire les propriétés énoncées plus haut pour ce groupe. On note juste qu'on pourrait aussi définir une loi de composition sur $\mathbb{Z}/n\mathbb{Z}$ par $[x]_n \cdot [y]_n = [xy]_n$. Elle ne donne pas un groupe, mais on peut en former un en enlevant les éléments non-inversibles pour le produit ; on note $(\mathbb{Z}/n\mathbb{Z})^\times$ ce nouveau groupe abélien.

Morphisme de groupe.

Les morphismes de groupe ressemblent beaucoup aux applications linéaires que nous connaissons, puisque :

$f : (G, \times) \longrightarrow (H, *)$ est un **morphisme de groupe** si et seulement si $f(x \times y) = f(x) * f(y) \, \forall x, y \in G$

Intuitivement, un morphisme de groupe préserve les propriétés de groupes. En effet, un morphisme préserve le neutre ($f(e_G) = e_H$), l'inverse ($f\left(x^{-1}\right) = f(x)^{-1}$) et la loi interne ($f(x * y) = f(x) \times f(y)$) par définition.

Un **isomorphisme** est un morphisme bijectif ; et alors, on a l'équivalence entre l'existence d'un isomorphisme $f : G \longrightarrow H$ et $G \cong H$ (G et H sont isomorphes).

Propositions :

- f est injectif $\Longleftrightarrow \ker(f) = \{e_G\}$.
- $\ker(f) := \{x \in G \ : \ f(x) = e_H\}$ est un sous-groupe de G.
- $\text{Im}(f) := \{f(x) \in H : x \in G\}$ est un sous-groupe de H.

Hom$(\cdot, \cdot)$.

Si $(G, *)$ et $(H, +)$ sont deux groupes et H est abélien $\hom(G, H) = \{f : G \longrightarrow H : \text{morphisme de groupe}\}$ muni de la loi $(f, g) \mapsto (x \in G \mapsto f(x) + g(x))$ est un groupe abélien.

Par ailleurs, $\forall n \in \mathbb{N}$, $\hom\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \frac{\mathbb{Z}}{n\mathbb{Z}}\right)$ muni de la loi de composition est isomorphe à $\frac{\mathbb{Z}}{n\mathbb{Z}}$, puisque tout morphisme de ce groupe est entièrement déterminé par l'image de 1, qui peut donc être n'importe quel élément de $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

En revanche, si m et n sont premiers entre eux, $\hom\left(\frac{\mathbb{Z}}{m\mathbb{Z}}, \frac{\mathbb{Z}}{n\mathbb{Z}}\right) \cong \{(x \mapsto 0)\}$.

→ Morphismes, suite.

On peut diviser un groupe par un sous-groupe !
Enfin, seulement pour certains sous-groupes.

■ La motivation.

D – L'ordre d'un sous-groupe divise toujours l'ordre du groupe. Peut-on diviser un groupe par un sous-groupe ?
T - Comment fonctionne la preuve du théorème de Lagrange ?
D - On partitionne le groupe en classes à gauche. C'est ça les éléments du quotient ?
T - Oui, mais pour que ça fonctionne comme un groupe, il faut que les classes à gauche soient égales aux classes à droite. C'est cette condition qu'on appelle "être distingué".

■ Automorphismes.

Soit $(G, \cdot)$ un groupe. $S(G)$ est l'ensemble de ses bijections; c'est un groupe pour la composition. De plus, $\mathrm{Aut}(G)$, le groupe des **automorphismes** (isomorphismes de groupe $G \to G$) est un sous-groupe de $S(G)$.

Avec $k \in \frac{\mathbb{Z}}{n\mathbb{Z}}$, on note $f_k : \begin{array}{c} \frac{\mathbb{Z}}{n\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}} \\ x \mapsto k \cdot x \end{array}$

D'ailleurs, on a l'équivalence : f_k est un automorphisme $\iff k$ inversible dans $\frac{\mathbb{Z}}{n\mathbb{Z}} \iff k$ premier avec n $\iff k$ engendre $\frac{\mathbb{Z}}{n\mathbb{Z}}$

■ Classes suivant un sous-groupe.

Soient $(G, \cdot)$ un groupe et H un sous groupe de G. Si $x \in G$, $xH := \{x \cdot h,\ h \in H\}$ est appelé la **classe à gauche** de x modulo H. $Hx := \{h \cdot x,\ h \in H\}$ est la classe à droite. N.B.: on peut les voir comme des orbites (cf plus tard).

Ces classes forment une partition de G; i.e. $\forall x \in G$, x est dans une classe à gauche et si $y \in xH$, $xH = yH$ De plus, $|xH| = |H|$

■ Théorème de Lagrange.

Soient G un groupe fini et H un sous groupe de G. l'ordre de H divise l'ordre de G, et le quotient donne le nombre de classes à gauche modulo H : $|G : H| = |G|/|H|$. En conséquence, pour p premier, tout groupe d'ordre p est cyclique (donc isomorphe à $\frac{\mathbb{Z}}{p\mathbb{Z}}$).

■ Sous-groupe distingué.

H est dit **distingué** (ou **normal**) dans G si pour tout $\forall g \in G$, $gH = Hg$; ou de manière équivalente, si $\forall g \in G$, $gHg^{-1} = H$.

Voici des exemples importants de sous-groupes distingués de G, qui peuvent servir de méthode de preuve:

- $[G, G] = \langle a^{-1} \cdot b^{-1} \cdot a \cdot b \ : \ a, b \in G \rangle$ (groupe dérivé, engendré par les commutateurs)
- $Z(G) = \{g \in G : \forall x \in G,\ x \cdot g = g \cdot x\}$ (centre de G)
- $\ker(f)$ où $f : G \longrightarrow G'$ où G' est un groupe et f un morphisme de groupes.

(Pour montrer que $Z(G)$ est distingué en le regardant comme un ker, cf "automorphismes intérieurs")

■ Groupe quotient.

Soient $(G, \cdot)$ et H un sous-groupe distingué dans G. $G/H := \{gH =: [g] : g \in G\}$ est le **groupe quotient** de G par H, cependant que $[g]$ est la classe d'équivalence de g modulo H. $(G/H, *)$ est un groupe avec $* : ([x], [y]) \longrightarrow [x \cdot y] = x \cdot y \cdot H$

Les groupes quotients les plus célèbres sont les $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Généralement, quotienter un groupe sert à "nettoyer" un groupe. Typiquement, en prenant un groupe quelconque G et en quotientant par les commutateurs $[G, G]$, on obtient un groupe abélien "optimal" $G/[G, G]$, i.e. G si tous les éléments commutaient (C'est G "aux erreurs de commutation près). Un autre exemple se trouve ci-dessous.

■ Théorème d'homomorphisme.

$\forall f : G \longrightarrow G'$ morphisme de groupes, $\mathrm{Im}(f)$ et $G/\ker(f)$ sont isomorphes.

N.B. : on a "nettoyé" G en identifiant tous les éléments qui allaient donner 0 pour obtenir l'injectivité de notre nouveau morphisme.

Méthode : Pour montrer que A et B sont isomorphes, il peut être pratique de montrer que $A = G/\ker(f)$ et $B = \mathrm{Im}(f)$.

Attention : $\mathrm{Im}(f)$ isomorphe $G/\ker(f)$, mais a priori, $\mathrm{Im}(f) \times \ker(f)$ pas isomorphe à G. Exemple : $f : \frac{\mathbb{Z}}{4\mathbb{Z}} \in x \longrightarrow 2x$. $\mathrm{Im}(f) = \frac{\mathbb{Z}}{2\mathbb{Z}} = \ker(f)$, mais $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ pas cyclique donc pas isomorphe à $\frac{\mathbb{Z}}{4\mathbb{Z}}$

■ Automorphismes intérieurs.

Un peu de dualité (cf $Hom(\cdot, \cdot)$): soit g élément d'un groupe G. Alors $\mathrm{ad}_g : G \in x \longrightarrow g \cdot x \cdot g^{-1}$ est un automorphisme de G (d'inverse $\mathrm{ad}_{g^{-1}}$), appelé **automorphisme intérieur** de G.

On a l'intéressant résultat : $\mathrm{ad} : G \longrightarrow \mathrm{Aut}(G)$, $g \mapsto \mathrm{ad}_g$ est un morphisme de groupes, et $\ker(\mathrm{ad}) = Z(G)$.

Par exemple, pour $\mathfrak{S}_3$, tout automorphisme donne une permutation de l'ensemble des transpositions $\{(12), (13), (23)\}$, donc il n'y en a pas plus que 6 ; or $\ker(\mathrm{ad}) = Z(G) = \{id\}$ donc il y a exactement 6 automorphismes, tous intérieurs.

→ Groupe symétrique.

Tout groupe fini est sous-groupe d'un groupe symétrique, et pourtant, il suffit de deux générateurs pour construire $\mathfrak{S}_n$!

La motivation.

D – Pourquoi est-ce que tout groupe fini G est isomorphe à un sous-groupe d'un groupe symétrique ?
T - Pour tout $g \in G$, l'application $x \mapsto gx$ avec $x \in G$ est une permutation des éléments de G.
D - Donc si on voit G comme un sous-groupe de $S(G)$ (bijections de G dans G, un groupe) ...
T - ... G est isomorphe à un sous-groupe de $\mathfrak{S}_{|G|}$. C'est le théorème de Cayley.

Permutations.

Une **permutation** de $X_n = [[1, n]] := \{1, 2, \cdots, n\}$ est une bijection de X_n dans X_n ; le groupe des permutations est le **groupe symétrique**, noté $\mathfrak{S}_n$ (ou S_n, c'est plus facile à écrire). Ce groupe est d'ordre $n!$.

On peut noter une permutation σ comme

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$$

Transposition.

Une **transposition** est une permutation σ telle que

$$\begin{cases} \sigma(k) = m \\ \sigma(m) = k \\ \sigma(l) = l \text{ si } l \neq k, l \neq m \end{cases}$$

pour $m \neq k$ deux entiers entre 1 et n. On note $(k\,m)$ cette permutation. Elle n'échange que deux éléments de X_n. Note : les transpositions engendrent $\mathfrak{S}_n$.

Cycles.

On peut généraliser le concept : un k-**cycle** γ est une permutation qu'on peut décrire par

$$\begin{cases} \gamma(a_i) = a_{i+1} & \text{pour } 0 \leq i \leq k-2 \\ \gamma(a_{k-1}) = a_0 & \\ \gamma(s) = s & \text{si } s \neq a_i \text{ pour un } 0 \leq i \leq k-1 \end{cases}$$

pour $a_0, a_1, \cdots, a_{k-1} \in X_n$ distincts. On notera $(a_0\, a_1 \cdots a_{k-1})$ le cycle. L'ensemble $\{a_0, \cdots, a_{k-1}\}$ est appelé **support du cycle**. Une transposition est donc un 2-cycle, etc. $\mathfrak{S}_n$ est engendré par $\alpha = (1\,2)$ et $\beta = (1\,2 \cdots n)$.

Le conjugué d'un k-cycle est toujours un k-cycle ; donc deux cycles sont conjugués si et seulement si ils ont la même longueur.

Théorème de Cayley.

Soit G groupe fini ; alors il existe $n \in \mathbb{N}$ tel qu'il existe un sous-groupe H de $\mathfrak{S}_n$ isomorphe à G.

Produit de cycles disjoints.

Toute permutation peut s'écrire comme un **produit de cycles (à supports) disjoints** ; la décomposition est unique, à l'ordre des termes près. Soit donc $\sigma = c_1 \cdots c_s$ une permutation décomposée en produit de cycles disjoints, avec tous les cycles (même ceux de longueur 1). Notons λ_i la longueur du cycle c_i ; alors $\sum_{i=1}^{s} \lambda_i = n$. On réarrange les termes pour les avoir dans l'ordre $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s$. Alors $\lambda(\sigma) := [\lambda_1, \cdots, \lambda_n]$ est ce qu'on appelle une **partition** de n ; on appellera "**type de cycle**" la partition $\lambda(\sigma)$. Alors, deux permutations sont conjuguées si et seulement si elles ont le même type de cycle. Donc, le nombre de classes de conjugaisons de $\mathfrak{S}_n$ est le nombre de partitions de n.

Signature.

À chaque permutation σ, on peut associer +1 ou -1, par le biais de ce qu'on appelle la **signature** $\varepsilon(\sigma)$ de σ. Posons $\Delta_n(x_1, \cdots, x_n) = \prod_{1 \leq i < j \leq n}(x_i - x_j)$ un polynôme à n variables.

Si on définit l'action d'une permutation ρ sur un polynôme P à n variables par $(\rho P)(x_1, \cdots, x_n) := P(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$, il se trouve que $\rho\Delta_n$ donne toujours Δ ou $-\Delta$. Posons alors la signature comme le $\varepsilon(\rho)$ tel que $\rho\Delta_n = \varepsilon(\rho)\Delta_n$. (Si $\varepsilon(\rho) = +1$, alors ρ est dite paire ; impaire sinon.)

En plus, $\varepsilon : \mathfrak{S}_n \to (\{-1, +1\}, \times)$ est un morphisme de groupes. Une transposition est impaire, un k-cycle est pair si k impair, et vice-versa.

Déterminant.

Soit une matrice $A = (a_{i,j})_{i,j}$ une matrice de $\mathcal{M}_n(\mathbb{K})$; on peut poser le **déterminant** de A comme

$$\det(A) = \sum_{\rho \in \mathfrak{S}_n} \varepsilon(\rho) a_{1,\rho(1)} \cdot \cdots \cdot a_{n,\rho(n)}$$

Cette définition montre bien que le déterminant est multilinéaire (chaque terme est linéaire en chaque colonne). Comme les transpositions sont impaires, échanger deux colonnes d'une matrice multiplie le déterminant par -1. Puisque $\varepsilon(\rho) = \varepsilon(\rho^{-1})$, on a $\det(A) = \det(A^t)$. On peut retrouver plusieurs autres propriétés du déterminant à partir de là.

→ Groupe alterné et actions.

C'est de là que viennent les groupes rappelons-nous, ce sont des ensembles de transformations/bijections.

La motivation.

D – Le lemme de Burnside c'est sympa, mais est-ce que ça sert en dehors du dénombrement ?
T - Combien de colliers à p perles et a couleurs (p premier), à rotation près (on ne peut pas retourner le collier) ?
D - La formule donne $\frac{a^p+(p-1)a}{p}$, mais il faut utiliser que p premier sinon c'est faux.
T - Oui exactement. Parce que tu viens de montrer que p divise $a^p+(p-1)a$ vu qu'il y a un nombre entier de possibilités. Et donc, que p divise a^p-a. En réécrivant ça comme $a^p-a \equiv 0 (\text{mod } p)$, on obtient le petit théorème de Fermat.

Groupe alterné.

Dans $\mathfrak{S}_n$, on peut former le sous-groupe A_n ou $\mathfrak{A}_n$ des permutations paires ; c'est-à-dire, le noyau de l'application sgn : $\mathfrak{S}_n \to \{\pm 1\}$. On l'appelle **groupe alterné**, de cardinal $\frac{n!}{2}$, il est distingué dans $\mathfrak{S}_n$. Et, proposition : $\mathfrak{A}_n$ est engendré par les 3-cycles.

Groupe simple.

Un groupe est dit **simple** quand ces seuls sous-groupes distingués sont le sous-groupe trivial, et le groupe lui-même. Exemples : $\mathbb{Z}/p\mathbb{Z}$ est simple pour p premier. Mais pas $\mathfrak{S}_n$ (pour $n \geq 3$).

Simplicité de $\mathfrak{A}_n$.

Pour $n \geq 5$, il se trouve que $\mathfrak{A}_n$ est simple. En-dessous, $\mathfrak{A}_4$ possède un sous-groupe distingué propre : $K_4 = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$, $\frac{\mathfrak{S}_4}{K_4} \cong \mathfrak{S}_3$ et $\frac{\mathfrak{A}_4}{K_4} \cong \mathfrak{A}_3$. On utilise, pour montrer la simplicité de $\mathfrak{A}_n$ ($n \geq 5$), que : les 3-cycles sont conjugués dans $\mathfrak{A}_n$, et que $Z(\mathfrak{A}_n) = \{id\}$.

Bonus.

L'idée de la théorie de Galois consiste à associer à chaque polynôme un groupe. Et on pourra résoudre $P(x) = 0$ par racines quand le groupe associé est résoluble. Un groupe est résoluble si on peut construire une "tour" de sous-groupes $1 \subset G_1 \subset \cdots \subset G_k = G$, avec chaque sous-groupe distingué ($G_m \lhd G_{m+1}$ pour tout m de 1 à $k-1$), et chaque quotient G_{m+1}/G_m abélien. Catastrophe, x^5-x-1 donne le groupe $\mathfrak{S}_5$ qui n'est pas résoluble, donc l'équation $x^5 - x - 1 = 0$ n'est pas résoluble par radicaux.

Action de groupes.

Soit G un groupe, X ensemble. Une **action** de G sur X est une application $\phi : G \times X \to X$ telle que $\forall x \in X, \phi(e,x) = x$, et telle que $\forall x \in X, g_1, g_2 \in G, \phi(g_1, \phi(g_2, x)) = \phi(g_1 \cdot g_2, x)$. On note souvent $g \cdot x$ pour $\phi(g,x)$; on dit aussi que G agit sur X. On peut voir une action comme un morphisme de G dans $\text{Bij}(X)$, le groupe des bijections de X dans X. On appelle aussi X un G-**ensemble** (ensemble muni d'une action de G).

Orbite et stabilisateur.

L'**orbite** de $x \in X$ est l'ensemble des valeurs possibles de $g \cdot x$; $O_x := Orb^G(x) := \{g \cdot x | g \in G\} \subseteq X$. Les orbites partitionnent X; en effet, on a équivalence entre "$y \in O_x$", "$O_x \cap O_y \neq$" et "$O_x = O_y$". On appelle $G\backslash X$ l'ensemble des orbites de X sous l'action de G.

Le **stabilisateur** G_x de $x \in X$ est l'ensemble des éléments qui fixent x ; $G_x := Stab^G(x) := \{g \in G | g \cdot x = x\} \subseteq G$. C'est même un sous-groupe de G. Et on a $G_{g \cdot x} = gG_xg^{-1}$.

Exemples.

Donnons quelques exemples d'actions. Les matrices de $\text{GL}_n(\mathbb{K})$ agissent sur les vecteurs $\mathbb{K}^n$ par $\phi(M,v) = Mv$. Par exemple, $O(2)$ agit sur $\mathbb{R}^2$; et l'orbite d'un point est le cercle centré à l'origine passant par ce point.

Si on prend $X = G$, on peut trouver des actions intéressantes. Par exemple, l'action par translation est définie comme $\phi(g,x) = gx$ et l'action par conjugaison comme $\phi(g,x) = gxg^{-1}$. Pour cette dernière action, les orbites sont appelées **classes de conjugaison**.

Lemme de Burnside.

Soit $g \in G$; on peut définir l'ensemble des points fixes X^g par $X^g = \{x \in X | g \cdot x = x\}$.

Soit G groupe fini qui agit sur X, on a alors que $|G| = |G_x| \cdot |O_x|$ pour tout $x \in X$. De là, on tire la **formule de Burnside** : pour G fini qui agit sur X fini, on a $|G\backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g|$. Intuitivement, chaque élément du groupe laisse un certain nombre de points fixes ; Burnside dit que la moyenne de ces nombres donne exactement le nombre d'orbites.

Formule des classes.

On a aussi cette formule pour $|G|$ fini : $|G| = |Z(G)| + \sum_{O \in G\backslash X, |O|>1} \frac{|G|}{|G_x|}$, appelée **formule des classes**. Elle nous donne que si $|G| = p^n$ avec p premier, alors $|Z(G)|$ est divisible par p, donc le centre est non-trivial. On en déduit que tout groupe d'ordre p^2 (p premier) est abélien. En général, les groupes d'ordre p^n sont intéressants ; on les appelle des p-**groupes**.

→ Groupe abélien de type fini.

Les groupes abéliens c'est déjà sympa ;
mais quand ils sont de type fini, on peut tous les classer.

■ La motivation.

D – Pourquoi est-ce que $\mathbb{Z}_{18}$ et $(\mathbb{Z}_3) \times (\mathbb{Z}_6)$ ne sont pas isomorphes ?
T - Parce que $\mathbb{Z}_{18}$ a des éléments d'ordre 18, mais les éléments de $(\mathbb{Z}_3) \times (\mathbb{Z}_6)$ sont d'ordre au plus 6.
D - D'accord, mais pourquoi alors $\mathbb{Z}_{18}$ et $(\mathbb{Z}_2) \times (\mathbb{Z}_9)$ sont-ils isomorphes ?
T - Parce que $([1]_2, [1]_9)$ est d'ordre 18 dans $(\mathbb{Z}_2) \times (\mathbb{Z}_9)$, donc le groupe est cyclique. C'est toute l'idée derrière le théorème des restes chinois en algèbre.

■ Groupe de type fini.

Un groupe est dit "**de type fini**" si on peut l'écrire comme le sous-groupe engendré par un nombre fini d'éléments : $G = \langle g_1, \cdots, g_n \rangle$. Par exemple, $\mathbb{Z}$, n'importe quel groupe fini, ou le produit de ou le quotient de deux groupes de type fini. Mais pas $\mathbb{Q}$ par exemple. En particulier, il est intéressant pour la suite de se rappeler que $\mathbb{Z}^k \times (\mathbb{Z}/a_1) \times \cdots \times (\mathbb{Z}/a_m)$. D'ailleurs, théorème : n'importe quel groupe abélien de type fini peut s'écrire sous cette forme. C'est pour montrer ce résultat qu'on introduit les notions suivantes.

■ Groupe abélien libre.

Un G abélien est dit "**libre de rang** n" si il existe un système de générateurs $(e_1, \cdots, e_n)$ avec pour tout $x \in G$, il existe une unique décomposition comme $x = x_1 e_1 + \cdots + x_n e_n$ avec des x_i entiers ; en d'autres termes, $\mathbb{Z}^n \ni (x_1, \cdots, x_n) \mapsto x_1 e_1 + \cdots + x_n e_n$ est un isomorphisme. On notera G.A.L. pour "Groupe Abélien Libre". Donc, typiquement, $\mathbb{Z}^n$ est abélien libre de rang n. C'est une version "entière" d'une base d'un espace vectoriel ; d'ailleurs, on appelle aussi $(e_1, \cdots, e_n)$ une **base** de G, et x_i les coefficients. Remarque : si $\mathbb{Z}^n \cong \mathbb{Z}^m$ alors $n = m$.

Note : si $f : G \to \mathbb{Z}$ avec G abélien est un morphisme non-trivial, alors $G \simeq \ker(f) \times \mathbb{Z}$.

Tout groupe abélien de type fini est le quotient d'un G.A.L. par un de ses sous-groupes. D'ailleurs, les sous-groupes H d'un G.A.L. G sont eux-mêmes des G.A.L., avec $\mathrm{rg}(H) \leq \mathrm{rg}(G)$. Par exemple, dans $\mathbb{Z}^2$, le sous-groupe des vecteurs (x, y) avec $x + y \equiv 0 \pmod 2$ est un groupe libre (de même rang ici), qu'on peut engendrer par $(1, 1)$ et $(2, 0)$ par exemple.

■ Bases adaptées.

Soit donc G un G.A.L. et $H \subseteq G$ sous-groupe. Si on a $\mathcal{E} = (e_1, \cdots, e_n)$ base de G et $\mathcal{F} = (f_1, \cdots, f_k)$ base de H, alors $\mathcal{E}$ et $\mathcal{F}$ sont **adaptées** (l'une à l'autre) si il existe des entiers a_i tels que $f_i = a_i e_i$. Dans ce cas-là, $G/H \cong (\mathbb{Z}/a_1) \times \cdots \times (\mathbb{Z}/a_k) \times \mathbb{Z}^{n-k}$. En fait, théorème : une base adaptée existe toujours.

■ Opérations élémentaires.

On a des opérations qui permettent de passer d'une base à une autre pour des G.A.L. ; on les appelle **transformations élémentaires**. Elles sont :

(1) : permutation de deux vecteurs : $e_i \mapsto e_j$, $e_j \mapsto e_i$

(2) : multiplication par -1 d'un des vecteurs : $e_i \mapsto -e_i$

(3) : ajouter un multiple d'un vecteur à un autre : $e_i \mapsto e_i + k e_j$

■ Matrice de rapport.

On peut alors définir la matrice $\mathcal{M}(\mathcal{E}, \mathcal{F})$, dite **matrice de rapport**, comme la matrice $n \times k$ des coefficients m_{ij} tels que $f_j = \sum_i m_{ij} e_i$; c'est une matrice de passage entre les deux bases.

Quand on considère la matrice $\mathcal{M}(\mathcal{E}, \mathcal{F})$, l'effet d'une transformation élémentaire est :

opération	de type 1	de type 2	de type 3
appliquée à $\mathcal{E}$	permutation des lignes i et j	multiplication de la i-ème ligne par -1	ajout de $-kL_i$ à L_j
appliquée à $\mathcal{F}$	permutation des colonnes i et j	multiplication de la i-ème colonne par -1	ajout de kC_i à C_j

Si on peut obtenir une base à partir d'une autre par ces transformations, les bases sont dites équivalentes. Si on peut passer d'une matrice à l'autre en appliquant ce genre de manipulations aux lignes et colonnes, les matrices sont dites équivalentes. (Le symbole est $\sim$ dans les deux cas.)

■ Quand $k = n$.

Si $k = n$, on a même que $|G/H| = a_1 \times \cdots \times a_n = |\det \mathcal{M}(\mathcal{E}, \mathcal{F})|$.

Si $G \cong (\mathbb{Z}/a_1) \times \cdots \times (\mathbb{Z}/a_n) \times \mathbb{Z}^r$, alors r est complètement déterminé par G. Il suffit pour ça de le diviser par son sous-groupe de torsion : $\mathrm{Tors}(G) = \{x \in G : x \text{ d'ordre fini}\}$; en effet, $G/\mathrm{Tors}(G)$ est un G.A.L.

Important : si $a_1, \cdots, a_k$ sont premiers entre eux, alors $(\mathbb{Z}/a_1 \cdots a_k) \cong (\mathbb{Z}/a_1) \times \cdots \times (\mathbb{Z}/a_k)$. C'est un théorème aussi connu sous le nom de "**théorème des restes chinois**" en algèbre. Donc, si on a un groupe de la forme $(\mathbb{Z}/a_1) \times \cdots \times (\mathbb{Z}/a_k)$, il est isomorphe à un groupe de la forme $(\mathbb{Z}/b_1) \times \cdots \times (\mathbb{Z}/b_l)$ avec $b_1 | b_2$, ... $b_{l-1} | b_l$. Les coefficients b_i sont alors uniques.

→ Géométrie affine.

C'est bien beau l'algèbre linéaire et tous les théorèmes, mais dès qu'on rajoute des translations ça passe en affine !

La motivation.

D – Il y a de nouveaux types d'isométries en géométrie affine ?
T - Oui ! Par exemple, une symétrie glissée ; c'est une symétrie suivie d'une translation.
D - Et pour les déplacements, c'est-à-dire les transformations rigides du physicien ?
T - Cette fois on a le vissage, une rotation suivie d'une translation selon l'axe de rotation. D'ailleurs, tout déplacement en 3d est un vissage (les translations et rotations en sont des cas particuliers); c'est ça l'idée derrière les torseurs.

Espace Vectoriel Euclidien.

Si on munit un espace vectoriel de dimension finie d'un produit scalaire, ça en fait un **espace vectoriel euclidien** (E.V.E.). Une application qui préserve le produit scalaire, à savoir telle que $\langle f(x), f(y)\rangle_F = \langle x, y\rangle_E$ avec $f : (E, \langle\cdot,\cdot\rangle_E) \to (F, \langle\cdot,\cdot\rangle_F)$ est dite **orthogonale** ; si E et F sont de même dimension (donc si f est bijective), alors f est une **isométrie**. Notons $O(E)$ l'ensemble des isométries de E dans E ; on l'appelle **groupe orthogonal**.

Symétrie.

Soit F un sous-espace vectoriel de E. Pour tout $x \in E$, il existe un unique $y \in F$ avec $(x-y) \perp y$ (c'est-à-dire, $\langle x-y, y\rangle = 0$). On appelle **projection orthogonale** sur F l'application p_F qui à x associe ce y ; et **symétrie orthogonale** par rapport à F l'application $s_F = 2p_F - \mathrm{id}$ qui à x associe $2y - x$. Si $\dim F = \dim E - 1$, s_F est qualifié de **réflexion**.

Théorème : les réflexions engendrent $O(E)$. Et si $A \in O(E)$, alors $E = \ker(A - \mathrm{Id}) \overset{\perp}{\oplus} \mathrm{im}(A - \mathrm{Id})$ (le $\overset{\perp}{\oplus}$ veut dire "en somme directe orthogonale").

Espace affine.

Un **espace affine** $\mathcal{E}$ de direction E (E espace vectoriel) est un ensemble $\mathcal{E}$ sur lequel agit le groupe E de manière transitive : pour tous $x, y \in \mathcal{E}$, il existe un unique $\vec{v} \in E$ tel que $x + \vec{v} = y$. On note alors $\overrightarrow{xy} := \vec{v}$, et parfois $\vec{\mathcal{E}}$ pour E. En se rappelant que E agit sur lui-même par translation, on voit qu'un espace vectoriel est un cas particulier d'espace affine, qu'on appelle **espace vectoriel affine**. Autre exemple : pour F s.e.v. de E, $\mathcal{F} := a + F$ (avec $a \in E$) est un espace affine de direction F.

Applications affines.

Pour $\varphi : \mathcal{E} \to \mathcal{F}$ application entre deux espaces affines, φ est dite **affine** si il existe $A : E \to F$ linéaire, tel que $\varphi(m + \vec{v}) = \varphi(m) + A(\vec{v})$. A est entièrement déterminé par φ, on la note $\vec{\varphi}$.

Pour E espace vectoriel affine, les translations sont des applications affines. Et plus généralement, pour $\varphi : E \to E$, on a : (φ affine) $\Leftrightarrow$ ($\exists A \in GL(E), B \in E \ : \varphi(x) = Ax + b$) Pour les translations, on a donc $\vec{\varphi} = Id_E$.

Isométrie affine.

Une application affine $\varphi : \mathcal{E} \to \mathcal{F}$ est un **isomorphisme** affine si il existe $\psi : \mathcal{F} \to \mathcal{E}$ affine avec $\varphi \circ \psi = Id_{\mathcal{E}}$ et $\psi \circ \varphi = Id_{\mathcal{F}}$. Théorème : chaque espace affine $\mathcal{E}$ est isomorphe à sa direction $\vec{\mathcal{E}}$.

Espace affine.

Un espace affine dont la direction est euclidienne est dit **euclidien**. $\varphi : \mathcal{E} \to \mathcal{F}$ affine entre deux espaces affines euclidiens est une **isométrie (affine)** si $\vec{\varphi}$ est une isométrie (vectorielle). Pour $\mathcal{E}$ espace affine euclidien, le groupe des isométries $\mathcal{E} \to \mathcal{E}$ est noté $\mathcal{O}(\mathcal{E})$. Ensuite, $\mathcal{O}(\mathcal{E}) \xrightarrow{\vartheta} O(E)$ donné par $\vartheta(\varphi) = \vec{\varphi}$ est un morphisme de groupes surjectif, de noyau $\ker\vartheta = \mathcal{T}(\mathcal{E})$ (les translations).

Soit $\mathcal{E}$ espace affine euclidien de direction E, et $\mathcal{F}$ s.-e. aff. de $\mathcal{E}$ de direction V. On a s_V symétrie par rapport à V, et donc on pose $\sigma_{\mathcal{F}}(x) = a + s_V(\overrightarrow{ax})$ avec un $a \in \mathcal{F}$ la symétrie (affine) par rapport à $\mathcal{F}$. Alors $\sigma_{\mathcal{F}}$ est une application affine de direction s_V (qui ne dépend pas du a choisi), et $\sigma_{\mathcal{F}|\mathcal{F}} = Id_{\mathcal{F}}$ et $\sigma_{\mathcal{F}}^2 = Id_{\mathcal{E}}$. Et là aussi, $\mathcal{O}(\mathcal{E})$ est engendré par les réflexions (affines).

Isométries affines.

Soit $\varphi(x) = Ax + b$ une isométrie affine d'un espace affine euclidien $\mathcal{E}$. Alors il existe une unique isométrie $\tilde{\varphi} : \mathcal{E} \to \mathcal{E}$ et $h \in E$ tel que $\varphi = \tilde{\varphi} \circ T_h = T_h \circ \tilde{\varphi}$ et que $\tilde{\varphi}$ ait un point fixe. On dit qu'une isométrie affine est **directe** (c'est un **déplacement**) si sa partie vectorielle est de déterminant 1, **indirecte** sinon (un **antidéplacement**). Classifions les isométries affines en dimension 2 et 3.

- $\dim E = 2$, isométrie directe. Translation ou rotation.
- $\dim E = 3$, isométrie directe. Translation, rotation autour d'un axe (dont le cas particulier, appelé retournement, d'une rotation de π radians) ; plus généralement, vissage (rotation suivie d'une translation selon l'axe de rotation).
- $\dim E = 2$, isométrie indirecte. Réflexion.
- $\dim E = 3$, isométrie indirecte. Symétrie (réflexions et symétrie centrale), réflexion suivie d'une rotation dans le plan de réflexion,ou symétrie glissée (réflexion suivie d'une translation par un vecteur dans la direction du plan de réflexion).

→ Théorie des corps.

Pour les systèmes dans $\mathbb{Z}/n\mathbb{Z}$, c'est pratique l'addition, la sous-traction et la multiplication, mais c'est encore mieux la division.

La motivation.

D – Tu connais ce truc avec le nombre 142 857 ?
T - Que quand tu le multiplies par 7, on obtient 999 999 ?
D - Non ! Quand tu le multiplies par 2, 3, 4, 5 ou 6, le résultat a les mêmes chiffres, dans un ordre différent (285714, 428571, 571428, 714285 et 857142).
T - Oui, ça marche aussi pour 17, 19, 23, 29 ... mais on ne sait pas si ça marche pour une infinité de nombres premiers. Ça vient de la structure des $\mathbb{Z}/p\mathbb{Z}$ correspondants. En fait ce sont des corps.

Définition de corps.

Un **corps** est essentiellement un ensemble où on peut ajouter, soustraire, multiplier et diviser (sauf par 0). Formellement, c'est une structure $(\mathbb{K}, +, \times)$ tel que :

- $(\mathbb{K}, +)$ est un groupe additif, notons 0 le neutre ;
- $(\mathbb{K}\backslash\{0\}, \times)$ est un groupe commutatif ; on note 1 le neutre, et $\mathbb{K}^*$ pour $\mathbb{K}\backslash\{0\}$;
- et la distributivité : $a\times(b+c) = a\times b + a\times c$ (pour tous $a, b, c \in \mathbb{K}$).

Les exemples typiques sont $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Pour p premier, on peut munir $\mathbb{Z}/p\mathbb{Z}$ de l'addition et de la multiplication pour former un corps noté $\mathbb{F}_p$. Si n est composé, $\mathbb{Z}/n\mathbb{Z}$ ne peut pas donner un corps.

Polynômes sur un corps.

$\mathbb{K}[X]$ est l'ensemble des polynômes à coefficients dans $\mathbb{K}$; c'est-à-dire l'ensemble des expressions de la forme $a_0 + a_1X + \cdots + a_nX^n$ avec des $a_i \in \mathbb{K}$. Le **degré** est alors le plus grand entier tel que $a_n \neq 0$. Comme d'usage, on peut définir somme et produit de polynômes de $\mathbb{K}[X]$:

$$\left(\sum_{i=0}^{m} a_iX^i\right) + \left(\sum_{j=0}^{n} b_jX^j\right) = \sum_{k=0}^{\max(m,n)} (a_k + b_k)X^k$$

$$\left(\sum_{i=0}^{m} a_iX^i\right) \times \left(\sum_{j=0}^{n} b_jX^j\right) = \sum_{k=0}^{m+n}\left(\sum_{i+j=k} a_ib_j\right)X^k$$

On a alors deux propriétés importantes sur le degré : $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$ et $\deg(PQ) = \deg(P) + \deg(Q)$.

Division euclidienne.

Grâce à ces propriétés, on peut définir une division euclidienne de polynômes : pour A, B dans $\mathbb{K}[X]$, il existe une unique paire (Q, R) (quotient, reste) de polynômes de $\mathbb{K}[X]$ avec $A = BQ + R$, et $\deg(R) < \deg(B)$. On notera $B|A$ ("B divise A") si le reste est nul. Grâce à cette division, on a l'équivalence entre $P(\alpha) = 0$ et $(X-\alpha)|P$. Et donc, théorème conséquent : un polynôme de degré n a au plus n racines (comptées sans multiplicités).

Structure de $\mathbb{K}^*$.

Pour un corps fini $\mathbb{K}$, on a le théorème suivant : $(\mathbb{K}^*, \times)$ est cyclique. L'idée de la preuve est que tout élément x de $\mathbb{K}^*$ satisfait la condition $X^q = 1$, avec q l'ordre de $\mathbb{K}^*$. Si $\mathbb{K}^*$ n'est pas cyclique, on peut trouver $d|q$ tel que $X^d = 1$ pour tout x, mais alors $X^d - 1$ a q racines, contradiction. On appelle **primitif** un élément de $\mathbb{K}^*$ qui engendre $\mathbb{K}^*$ par rapport à la multiplication. Par exemple, 2 est primitif dans $\mathbb{F}_5$ ($[2]_5^0 = [1]_5, [2]_5^1 = [2]_5, [2]_5^2 = [4]_5, [2]_5^3 = [3]_5$ donc 2 engendre $\{[1]_5, [2]_5, [3]_5, [4]_5\}$), mais pas dans $\mathbb{F}_7$ (on ne peut pas obtenir 5 par exemple). Une conjecture d'Artin demande si tout entier a (qui n'est ni un carré, ni -1) est primitif dans une infinité de $\mathbb{F}_p$ (p premier). À ce jour, cette conjecture n'est vérifiée/réfutée pour aucun a.

Nombre unipériodique.

Soit un nombre rationnel α/β ; on peut l'écrire comme une partie entière, et une partie fractionnaire qui est éventuellement périodique ; on définit $\mathcal{P}(\alpha/\beta)$ comme la période, c'est-à-dire le morceau répété (le plus petit possible). Bien sûr, il y a une ambiguité ; dans 0.13713713713..., on pourrait dire que le morceau [137] est la période, tout aussi bien que [371] ou [713]. Donc $\mathcal{P}(\alpha/\beta)$ est défini à une permutation cyclique près. Par exemple, $\mathcal{P}(1/3) = [1]$; $\mathcal{P}(1/7) = [142857]$; $\mathcal{P}(1/11) = [09]$, etc. Notons que $\mathcal{P}(2/7) = [285714] = [142857] = \mathcal{P}(1/7)$. Les N tels que $\mathcal{P}(1/N) = \mathcal{P}(2/N) = \cdots = \mathcal{P}(\frac{N-1}{N})$ sont dits **unipériodiques**. On s'intéresse maintenant aux $1/p$ avec p premier ; on met les cas $p = 2$ et $p = 5$ à part. Alors, théorème : p est unipériodique si et seulement si 10 est primitif modulo p. C'est le cas pour $p = 7$ ($[10]_7 = [3]_7$ engendre $(\mathbb{Z}/7\mathbb{Z})^*$), et 17, 19, etc.

Bonus (hors cours).

Si $\mathbb{Z}/n\mathbb{Z}$ ne donne pas un corps pour n composé, il existe quand même des corps $\mathbb{F}_q$ si et seulement si q est de la forme p^n, avec p premier et n entier (e.g. il existe un $\mathbb{F}_8$, un $\mathbb{F}_9$, mais pas de $\mathbb{F}_{10}$). On appelle caractéristique d'un corps, le plus petit entier n tel que $1+1+\cdots+1$ (n fois) $= 0$; si ce n'est le cas pour aucun entier, on dit que le corps est de caractéristique 0. Donc $\mathbb{F}_p$ est de caractéristique p (p premier), et $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristiques 0.