Structures algébriques indispensables et arithmétique

Emmanuel Amiot

octobre 2018

1 Groupes

1.1 Rappels

On rappelle la définition générale d'un groupe :

DÉFINITION 1. *G est un groupe si et seulement si*

— *G est muni d'une loi de composition* **interne** *$*$, i.e. telle que*

$$\forall x, y \in G,\ x * y \in G$$

— *cette loi est* **associative** *:* $\forall x, y, z \in G,\ (x * y) * z = x * (y * z)$

— *Il y a un* **élément neutre** *e, tel que* $\forall x \in G,\ x * e = e * x = x$.

— *Tout élément de G possède un* **inverse***, i.e.*

$$\forall x \in G,\ \exists y \in G,\ x * y = y * x = e$$

Quand on a pour tout couple $(x, y) \in G^2, x * y = y * x$ *on dit que la loi est commutative et G est un groupe* **abélien** *(ou commutatif).*

Remarques :

1. la loi peut être notée de toutes sortes de façons : $+, \circ, \times, \ldots\ldots$ Ou même ne pas être notée du tout. Souvent on commet l'abus de parler de l'ensemble sans préciser la loi (ex : « le groupe $\mathbb{Z}\ldots$ »). Ce n'est pas bien. La seule convention est qu'une loi notée + est forcément commutative. Pour une loi + on parle d'opposé au lieu d'inverse.
2. On vérifie (faites-le !) que l'élément neutre est unique. S'il y a élément neutre à gauche et élément neutre à droite, alors ils sont identiques.
3. De même il ne peut pas y avoir deux inverses distincts. L'inverse à gauche = l'inverse à droite.
4. Dans un groupe on a le droit de **simplifier** : $a.x = a.y \iff x = y$.

EXERCICE 1. *Donner des exemples de lois internes non associatives.*

Donner des exemples de groupes non abéliens.

** Trouver un cas où il existe un inverse à droite mais pas à gauche.*

$(\mathbb{N}, +)$ *est-il un groupe ? pourquoi ?*

** recherche : se documenter sur la notion de monoïde, en présenter un ou des exemples intéressants.*

Exemples : $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, tout espace vectoriel E, sont des groupes pour la loi usuelle +.

$\mathbb{R}^*, \mathbb{R}_+^*, \mathbb{C}^*$ sont des groupes pour $\times$ ainsi que le cercle unité $\mathbb{U}$ ou les racines n^{es} de l'unité $\mathbb{U}_n$. Le groupe des matrices inversibles $\mathcal{G}\ell_n(\mathbb{K})$ est non commutatif.
Les éléments inversibles d'un anneau forment un groupe multiplicatif.
Les bijections (dites aussi permutations) S_X d'un ensemble X quelconque forment un groupe pour la loi de composition des applications $\circ$. Ceci comprend le cas très général des *transformations* qui *conservent* quelque chose (par exemple, les isométries de l'espace qui préservent un cube, les changements de variables qui préservent une équation différentielle, etc. . .).
NB : la loi $\circ$ est toujours associative.

EXERCICE 2. *Si X a n éléments, quel est le cardinal de S_X ? Ce groupe peut-il être commutatif?*

Un procédé pour construire des groupes plus grands :

DÉFINITION 2. *Le produit de deux groupes $(G, .)$ et $(G', \times)$ est l'ensemble $G \times G'$ muni de la* **loi produit** *:*

$$(g, g') \bullet (h, h') = (g.h, g' \times h')$$

Ceci se généralise bien sûr à un produit de n groupes. Exemple : l'ensemble des points du plan à coordonnées entières peut être considéré comme groupe produit $\mathbb{Z} \times \mathbb{Z}$.
Le groupe multiplicatif produit $\mathbb{R}_+^* \times \mathbb{U}$ traduit la **décomposition polaire d'un nombre complexe** (non nul), avec la loi

$$(r, e^{i\theta}) \times (r', e^{i\theta'}) = (rr', e^{i(\theta+\theta')})$$
$$re^{i\theta} \times r'e^{i\theta'} = rr'e^{i(\theta+\theta')}$$

1.2 Sous-groupes

Rien n'empêche une partie d'un groupe de profiter elle-aussi d'une structure de groupe. En particulier, l'associativité est une propriété héréditaire (si elle est vraie partout, elle est vraie aussi plus localement).

DÉFINITION 3. *Une partie $H \subset G$ est un sous-groupe ssi H avec la restriction de la loi de G est aussi un groupe. Pour cela il faut et il suffit que H soit non vide (!!!) et*

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

Démonstration. Vérifiez que H contient le neutre, est stable par . et par passage à l'inverse. ♦

Exemple : pourquoi les irrationnels de $\mathbb{R}$ ne forment-ils pas un sous-groupe ?
Exemple de sous-groupe : l'ensemble des racines cubiques de l'unité $\mathbb{U}_3$ est un sous-groupe de $\mathbb{U}_9$.

EXERCICE 3. *On considère le groupe F des isométries de $\mathbb{R}^3$ qui conservent un ballon de football, que les géomètres appellent icosidodécahèdre – le ballon, pas le sport (i.e. les isométries envoient une face pentagonale sur une face pentagonale, un hexagone sur un hexagone, un sommet sur un sommet, et le ballon dans la lucarne). Montrer* **sans aucun calcul** *que le sous-ensemble des rotations $R \subset F$ est un sous-groupe.*
*** Montrer qu'il a 120 éléments (avec un peu plus de calculs).*

PROPOSITION. *Toute intersection de sous-groupes de* G *est un sous-groupe de* G.

En revanche une réunion de sous-groupes n'a aucune raison d'en être un (la réunion de deux droites n'est pas un plan, mmmm ?)
On voit que l'ensemble des nombres pairs est un sous-groupe (additif) de $\mathbb{Z}$. Plus généralement,

THÉORÈME 1. *Les sous-groupes de* $(\mathbb{Z},+)$ *sont les* $(n\mathbb{Z},+)$ *(pour tous les* $n \in \mathbb{N}$*).*

Ce théorème est essentiel.

Démonstration. Soit G un tel sous-groupe. Mettant à part la solution $G=\{0\}$ il existe dans G au moins un élément non nul, et donc un élément $x>0$. La partie $G \cap [1,+\infty[$ est non vide, minorée et constituée d'entiers : elle possède un plus petit élément (cela peut se prouver par un algorithme : tant que $n \notin G, n = n+1\ldots$) qu'on appelle n.
Nous allons prouver que $G = n\mathbb{Z}$. Pour cela, si $x \in G$ on forme la division euclidienne de x par n :

$$x = n \times q + r \text{ où } 0 \leqslant r < n$$

Étant donné que $n \times q = n+n+\ldots n \in G$ (OK, si q est négatif on considère l'opposé, $-q \times n$) et que $x \in G$, il vient que $r = x - n\,q \in G$ par stabilité du sous-groupe G.
Or par construction, il n'y a pas d'élément de G qui soit >0 et strictement inférieur à n. La seule possibilité est donc $r=0$, i.e. x est multiple de n ou encore $x \in n\mathbb{Z}$.
On a montré que $G \subset n\mathbb{Z}$, mais si $n \in G$ alors on a aussi $n+n=2n, 2n+n=3n\ldots$ ainsi que leurs opposés et donc $n\mathbb{Z} \subset G$, d'où l'égalité.
Enfin et réciproquement, tout $n\mathbb{Z}$ est bien un sous-groupe de $(\mathbb{Z},+)$ (stabilité des multiples de n par soustraction). ♦

La stabilité par intersection de cette notion permet de donner la définition suivante, sur laquelle nous reviendrons surtout dans le cas d'un singleton :

DÉFINITION 4. *Le sous-groupe de* G *engendré par une partie* $A \subset G$ *est* **le plus petit sous-groupe contenant** A*, i.e. l'intersection des sous-groupes qui contiennent* A.

(À votre avis, cela a-t-il encore un sens si $A=\emptyset$? Les opinions diffèrent...)
On dira qu'une partie A est **génératrice** si elle engendre le groupe tout-entier.
Exemples :

- $G=(\mathbb{R},+)$. Le sous-groupe engendré par le singleton 1 est $(\mathbb{Z},+)$.
- G est l'ensemble des isométries affines de $\mathbb{R}^2$. L'ensemble A des rotations affines planes (i.e. avec des centres n'importe où dans le plan) n'est pas un groupe, mais il le devient si on y rajoute le(sous-groupe de)s translations : $\mathrm{gr}(A) = A \cup \mathcal{T}$.
- $G=S^1$, le cercle unité (groupe multiplicatif). Le groupe engendré par $A=\{e^{2i\pi/n}\}$ est le groupe $\mathbb{U}_n$ des racines $n^{\text{ièmes}}$ de l'unité. Notez qu'il a d'autres générateurs : par exemple, $e^{7i\pi/6}$ engendre aussi bien $\mathbb{U}_{12}$ que $e^{i\pi/6}$.
- $G=(\mathbb{R},+)$. Le groupe engendré par les inverses d'entiers $A=\{\frac{1}{n} \mid n \in \mathbb{N}^*\}$ est $\mathbb{Q}$.

EXERCICE 4. *Montrer par récurrence sur* n *que* S_n *est engendré par les transpositions, i.e. les permutations* $\tau_{i,j}$ *qui échangent seulement deux éléments* $i \leftrightarrow j$.

1.3 Morphismes

Cette notion est très importante dans tous les domaines des mathématiques : il s'agit d'applications qui préservent la structure ambiante.

DÉFINITION 5. *Un morphisme de groupes est une application* $u : G \to G'$ *où* G, G' *sont des groupes (munis des lois * et* $\star$ *disons) telle que*

$$\forall x, y \in G \; u(x * y) = u(x) \star u(y)$$

EXERCICE 5. *Vérifier que l'image de l'élément neutre* e *de* G *est forcément l'élément neutre* e' *de* G' *et que l'image d'un inverse est l'inverse de l'image :* $u(x^{-1}) = u(x)^{-1}$.

Exemple :

- $x \mapsto 42x$ est un morphisme de $\mathbb{Z}$ dans lui-même.
- $z \mapsto |z|$ est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$.
- $\exp$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$. Et aussi de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$. Mais pas de $\mathcal{M}_n(\mathbb{R})$ dans $\mathcal{GL}_n(\mathbb{R})$.
- Det est un morphisme du groupe des matrices inversibles $\mathcal{GL}_n(\mathbb{K})$ dans $(\mathbb{K}^*, \times)$.
- La **signature** est un morphisme du groupe des permutations $(S_n, \circ)$ dans $(\{-1, 1\}, \times)$.

DÉFINITION 6. *Le noyau d'un morphisme* $u : G \mapsto G'$ *est* $\operatorname{Ker} u = \{x \in G \mid u(x) = e'\}$.
Son image est $\operatorname{Im} u = \{y \in G' \mid \exists x \in G, u(x) = y\}$.

PROPOSITION. *Image et noyau sont des sous-groupes (de* G', G *respectivement).*

Exemple : Vous souvenez-vous du groupe spécial orthogonal $SO(E)$ (ses éléments sont les rotations de l'espace euclidien E) ? Sachant que $O(E)$ est un groupe (les isométries sont les applications qui *conservent* la distance, donc elles forment un groupe), et que Det est un morphisme de $O(E)$ dans $\mathbb{R}^*$ (en fait dans $\{-1, 1\}$), $SO(E)$ qui est le noyau de ce morphisme est automatiquement un sous-groupe de $O(E)$. Il est élégant de montrer qu'un ensemble a telle ou telle structure en arguant de ce qu'il est l'image (ou le noyau) d'un autre espace de structure connue.

EXERCICE 6. *Noyau du morphisme susmentionné* $z \mapsto |z|$ *de* $(\mathbb{C}^*, \times)$ *dans* $\mathbb{R}_+^*, \times)$ *?*

PROPOSITION. *Un morphisme* u *est injectif ssi* $\operatorname{Ker} u = \{e\}$.

Ceci est immédiat à démontrer mais très important en pratique car l'injectivité se résume (pour un morphisme) à résoudre l'équation $u(x) = e'$ (et non $u(x) = u(x')$). Attention, cela doit se faire quand, **et seulement quand**, u est connu pour être un morphisme ! (on ne cherche pas le "noyau" de l'application $x \mapsto x + 3$!)

EXERCICE 7. ** Les noyaux ont une propriété additionnelle, prouvez-là : si* $H = \operatorname{Ker} u \subset G$ *alors pour tout élément* $g \in G$ *le* **sous-groupe conjugué** [1] $H' = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ *coïncide avec* H.

DÉFINITION 7. *Un* **isomorphisme** *est un morphisme qui est à la fois injectif et surjectif.*
Un automorphisme est un isomorphisme d'un groupe G *dans lui-même.*

Cela signifie que tout élément de G' possède un et un seul antécédent $x \in G \mid u(x) = x'$. Cela signifie surtout que la loi de G est le parfait miroir de celle de G' : toute relation $x.y = z$ dans G correspond à une unique relation $x' \times y' = z'$ dans G'. Connaître un groupe, c'est connaître tous ses groupes isomorphes.

PROPOSITION. *L'application réciproque d'un isomorphisme de* G *dans* G' *est un isomorphisme de* G' *dans* G.

Exemple : le logarithme et exp sont des isomorphismes réciproques. Ce qui permet de choisir le « sens » de la flèche qui nous va le mieux ! Plus généralement on a

EXERCICE 8. *La relation « être isomorphe à » est une relation d'équivalence dans l'ensemble de tous les groupes.*

EXERCICE 9. *Les groupes $n\mathbb{Z}$ (pour tout $n \in \mathbb{N}^*$) sont tous isomorphes.*

EXERCICE 10. *On note $e^{i\theta}$ l'élément générique de $\mathbb{U}$. Fabriquer un isomorphisme de $(\mathbb{U}, \times)$ dans $(SO_2(\mathbb{R}), \circ)$ (complexe unitaire $\mapsto$ rotation).*

EXERCICE 11. *Montrer que le groupe produit $G \times G'$ admet un sous-groupe isomorphe à G (resp. à G').*

EXERCICE 12. *Montrer que le groupe produit $\mathbb{R}_+^* \times \mathbb{U}$ est isomorphe à $\mathbb{C}^*$ (je ne précise pas les lois, exprès).*

EXERCICE 13. ** (thème d'étude) Les groupes additifs $\mathbb{Z}, \mathbb{Q}$, (plus dur...) $\mathbb{R}$ ne sont pas isomorphes.*

1.4 Le groupe $\mathbb{Z}/n\mathbb{Z}$

On reviendra sur cet ensemble en tant qu'anneau ultérieurement (pour les gouverner tous et dans les ténèbres les lier). Le but est de donner un sens à l'idée informelle "calculer avec la condition que chaque fois que l'on arrive à n, cela fait 0" – comme les aiguilles d'une montre qui renouvellent leur valeur tous les 12 ou 60.

1.4.1 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

DÉFINITION 8. $a \equiv b \pmod{n} \iff a$ *est congru à* b *modulo* $n \iff a - b \in n\mathbb{Z}$ *(c'est à dire que n divise $|a-b|$) ;*
La relation $\equiv \pmod{n}$ est une relation d'équivalence, ses classes constituent l'ensemble $\mathbb{Z}/n\mathbb{Z}$.

Remarquons qu'une telle classe est une progression arithmétique de raison n : si par exemple $n = 12, a = 3, \dot{a} = \{\ldots, -21, -9, 3, 15, 27, \ldots\}$. Un tel ensemble est invariant par translations de n (ou multiples !) Un exemple courant est celui des heures sur une montre. On a aussi les notes de la gamme (« Si bémol » désigne une classe d'équivalence modulo une octave, i.e. douze demi-tons).
Nous allons définir une loi de composition interne sur ces classes d'équivalence. Cela paraît terriblement abstrait mais en fait cela revient à faire des calculs « comme si n valait 0 », ou encore en calculant de manière circulaire.

1.4.2 Structure de groupe de $\mathbb{Z}/n\mathbb{Z}$

THÉORÈME 2. *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ a exactement n éléments. C'est un groupe additif avec la loi définie par*

$$\dot{a} + \dot{b} = \overbrace{a+b}^{\cdot}$$

On notera aussi bien $\dot{a} + \dot{b} = \dot{c}$ que $a + b \equiv c \pmod{n}$.
Ce qu'il n'est pas facile de comprendre est que cette définition a un sens ! Encore moins facile est de comprendre que la question se pose.
Concrètement : essayez d'ajouter $3 \pmod{10}$ à $5 \pmod{12}$, c'est à dire la séquence infinie $\cdots -17, -7, 3, 13, 23 \ldots 2013 \ldots$ à l'autre séquence $\ldots -19, -7, 5, 17, 29 \ldots 1205 \ldots$. Ça ne fait

rien de lisible ! Mais si le modulo est le même alors tout va bien (faites-le avec $n = 10$). Plus généralement :

Démonstration. D'abord $\dot{a} + \dot{b}$ ne dépend pas des **représentants choisis** de $\dot{a}, \dot{b}$: si on remplace a (resp. b) par $a + kn$, cela ne changera pas la classe de $a + b$.
Ensuite on vérifie que chaque classe possède un et un seul élément compris entre 0 et $n - 1$: c'est le reste de la division euclidienne par n. Ceci donne exactement n classes distinctes (disjointes, si on veut).
Enfin on vérifie que $(\mathbb{Z}/n\mathbb{Z}, +)$ est bien un groupe :

1. La loi $+$ est bien définie (interne) : $\dot{a} + \dot{b} = \dot{a + b}$ est bien un élément de $\mathbb{Z}/n\mathbb{Z}$.
2. Elle est associative : $(\dot{a} + \dot{b}) + \dot{c}$ et $\dot{a} + (\dot{b} + \dot{c})$ sont tous deux égaux à la classe de $a + b + c$.
3. La classe de 0 (qui n'est autre que l'ensemble des multiples de n, $\dot{0} = n\mathbb{Z}$ – très important) est élément neutre.
4. Tout élément possède un symétrique (opposé). ♦

REMARQUE 1. *Ce groupe est commutatif car* $\dot{a + b} = \dot{b + a}$.

Concrètement il est très facile de faire une telle addition : on retire le point, on ajoute, et on reprend la classe modulo n, en choisissant un autre représentant si on le juge bon.
Ex : modulo 12, on a $\dot{7} + \dot{8} + \dot{9} + \dot{10} = \dot{34} = \dot{10}$.

PROPOSITION. *L'application $\pi_n : a \mapsto \dot{a}$ est un morphisme surjectif du groupe $(\mathbb{Z}, +)$ dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Ceci permettrait de retrouver le théorème précédent (car l'image d'un groupe par un morphisme est un groupe) en trente secondes, mais on cherche à limiter le nombre de démissions de la MP en début d'année...

REMARQUE 2. *Ce morphisme est surjectif, son noyau est $n\mathbb{Z}$. On l' appelle projection canonique.*

EXERCICE 14. *Chercher les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$, de $\mathbb{Z}/7\mathbb{Z}$.*

EXERCICE 15. *Chercher les morphismes de groupes entre $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$ (il y en a deux dans chaque sens). * Même question avec $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.*

EXERCICE 16. *Montrer que l'application $\dot{x} \mapsto e^{2ix\pi/n}$ est bien définie de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{U}$ (attention ! que se passe-t-il si on remplace x par un x' distinct, mais congru à x ?...), et qu'elle définit un isomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{U}_n, \times)$. Cela fournit une visualisation géométrique des groupes cycliques.*

Observons que toute classe modulo n peut s'écrire $\dot{1} + \dot{1} + \ldots \dot{1}$ avec le nombre adéquat de termes dans l'addition. Cela signifie que le singleton $\{\dot{1}\}$ engendre tout le groupe $\mathbb{Z}/n\mathbb{Z}$. Cela mérite des approfondissements.

1.5 Ordre d'un élément

DÉFINITION 9. *Un groupe est monogène $\iff$ il est engendré par un élément.*

Notons multiplicativement la loi du groupe G, et e son élément neutre. Le sous-groupe engendré par $a \in G$ contient forcément tous les $a^n, n \in \mathbb{Z}$. Précisons que a^{-n} est l'inverse

de a^n. Réciproquement, comme $a^{n+p} = a^n.a^p$ on a immédiatement que $\{a^n \mid n \in \mathbb{Z}\}$ est un sous-groupe (de G).

PROPOSITION. $\mathrm{gr}(a) = \{a^n \mid n \in \mathbb{Z}\}$. *C'est l'image du morphisme canonique* $\pi : n \mapsto a^n$ *de* $\mathbb{Z}$ *dans* G.

DÉFINITION 10. *Si le groupe* $\mathrm{gr}(a)$ *est fini, alors l'ordre de* a *est le cardinal de* $\mathrm{gr}(a)$. *On parle alors d'un groupe* **cyclique**.

Cette définition n'est pas pratique. Améliorons-là en considérant, au lieu de l'image, le noyau de π :

PROPOSITION. a *est d'ordre fini ssi* π *est non injective. Alors son noyau est* $\mathrm{Ker}\,\pi = n\mathbb{Z}$ *où* n *est l'ordre de* a.

n *est donc le plus petit élément de* $\{p \in \mathbb{N}^* \mid a^p = e\}$.

Démonstration. Le nœud de cette proposition est le lemme donnant les sous-groupes de $(\mathbb{Z}, +)$ comme étant de la forme $n\mathbb{Z}$ (les cas particuliers $n = 0, 1$ sont possibles) (notons que **tout sous-groupe de** $\mathbb{Z}$ **est monogène**).
On a deux cas : si π est injective, son image est infinie (en fait, isomorphe à $\mathbb{Z}$). Sinon, le noyau n'étant pas réduit à $\{0\}$, il est de la forme $n\mathbb{Z}$ où n est bien ce qui est annoncé. ♦

REMARQUE 3. *Pour* $0 \leqslant i < j < n$ *on a* $a^i \neq a^j$ *(très utile) [car sinon on aurait* $a^{j-i} = e$*] : autrement dit, la restriction de* π *à* $\{0, 1, 2, \ldots, n-1\}$ *est une bijection d'image* $\mathrm{gr}(A)$. *Encore autrement dit, l'ordre de* a *est le plus grand entier* r *tel que* $e, a, \ldots a^{r-1}$ *soient deux à deux distincts, c'est le nombre de puissances distinctes de* a*, etc. . ..*

COROLLAIRE 1. *Tout groupe cyclique est isomorphe à un des* $\mathbb{Z}/n\mathbb{Z}$. *Un groupe monogène infini est isomorphe à* $\mathbb{Z}$.

EXERCICE 17. *On considère une permutation* $\sigma \in S_n$.
À l'aide de la décomposition en produits de cycles, montrer que l'ordre de σ *est le ppcm des longueurs des cycles de* σ.
On considère le groupe des isométries conservant un rectangle (non carré).
Énumérer ses quatre éléments, vérifier que ce n'est pas un groupe cyclique.

Plus généralement, un groupe à n éléments est cyclique si et seulement si il possède un élément d'ordre n (au moins). Il est alors abélien. La considération du noyau de π donne le critère suivant :

PROPOSITION. *Soit* r *l'ordre de l'élément* a *du groupe* G. *On a*

$$a^n = e \quad \Longleftrightarrow \quad r \mid n \quad \Longleftrightarrow \quad n \in r\mathbb{Z} \quad (n \text{ doit être un multiple de } r)$$

Exemple : L'ordre multiplicatif de 2 modulo 11 est 10, en effet

$$2^{10} = 1024 = 93 \times 11 + 1 \equiv 1 \mod 11$$

et aucune des puissances inférieures n'est congrue à 1.
L'ordre multiplicatif de 3 est égal à 5, car $3^5 = 243 = 22 \times 11 + 1 \equiv 1 \mod 11$ et c'est la première puissance congrue à 1. Alternativement, on peut dire que le seul $r > 1$ qui divise 5 est 5, et utiliser la proposition précédente.

Enfin l'ordre de 4 est aussi égal à 5.

EXERCICE 18. *Classer les éléments de $\mathbb{Z}/20\mathbb{Z}$ selon leur ordre.*

EXERCICE 19. *Généraliser l'exemple ci-dessus : si a est d'ordre n, montrer que l'ordre de a^2 est soit n, soit $n/2$ selon la parité de n.*

EXERCICE 20. *Donner une matrice à coefficients entiers d'ordre 6 (* voire 12).*

THÉORÈME DE LAGRANGE. *Soit G un groupe fini, de cardinal $|G| = n$. Alors pour tout élément g de G, l'ordre de g divise le cardinal du groupe : $ord(g) \mid n$.*
Avec la caractérisation de l'ordre, ceci équivaut à $g^{|G|} = e$.

Ce résultat est le b-a-ba de l'étude des groupes finis — dont la classification a nécessité plus de 100,000 pages de publications sur près de 50 ans...

Démonstration. Seul le cas d'un groupe abélien est exigible dans notre programme *(dans la forme la plus générale on prouve que le cardinal d'un sous-groupe divise celui du groupe).*
Soit $g \in G$ et numérotons les éléments de $G = \{g_1, g_2 \dots g_n\}$; alors l'ensemble $\{g.g_1, g.g_2 \dots g.g_n\}$ n'est autre que G car ses éléments ont été simplement permutés. En effet, l'application $h \mapsto g.h$ est clairement bijective. Autrement dit, $\exists \sigma \in S_n$ telle que

$$g.g_1 = g_{\sigma(1)} \quad g.g_2 = g_{\sigma(2)} \quad g.g_n = g_{\sigma(n)}$$

Donc par associativité et commutativité, on a

$$g_1.g_2 \dots .g_n = g_{\sigma(1)} \dots g_{\sigma(n)} = (g.g_1).(g.g_2) \dots (g.g_n) = g^n.\big(g_1.g_2 \dots .g_n\big)$$

et par simplification (légale dans un groupe) il reste bien $g^n = e$ ce qui signifie (par caractérisation de l'ordre) que l'ordre de g divise n. ♦

Quels sont les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$, c'est à dire ses éléments d'ordre maximal ? cf. infra à ce sujet. Remarquons pour l'instant que tout élément de $\mathbb{Z}/12\mathbb{Z}$ n'est pas d'ordre 12, et qu'il y a quatre générateurs.

EXERCICE 21. *On considère un automorphisme de groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$. Montrer qu'il est parfaitement défini par l'image de $\mathbf{1} = \dot{1}$ et que cette image doit être, comme $\mathbf{1}$, un élément générateur du groupe.*

2 Anneaux

Que ce soit dans $\mathbb{R}$, $\mathbb{Z}$; ou (moins couramment) $\mathbb{Z}/n\mathbb{Z}$, on peut non seulement ajouter mais aussi multiplier. Et les deux opérations se "mélangent" bien, au sens où l'on sait développer une expression comme $(a + b) \times c$ ou même $(a + b)^n$, etc. La structure idoine est celle d'anneau.

2.1 Définitions, propriétés élémentaires et exemples

DÉFINITION 11.

— *Un anneau est un groupe commutatif pour l'addition, avec une multiplication qui est une loi interne, associative, distributive par rapport à l'addition et munie d'un élément neutre.*

— *Une partie d'un anneau est un sous-anneau ssi c'est un sous-groupe additif, où la multiplication est interne et possède un élément neutre. Concrètement, on doit vérifier la stabilité par soustraction, par multiplication, et la présence de 1*

— *Un anneau est* **intègre** *si on a le droit de simplifier :*

$$\forall a \neq 0, ax = ay \Rightarrow x = y$$

Cela équivaut à dire qu'il n'y a pas de diviseurs de zéro *:* $ab = 0 \Rightarrow a$ *ou* $b = 0$.

— *Enfin un* **morphisme d'anneaux** *est une application* f *entre deux anneaux qui vérifie pour tous* x, y *dans l'anneau de départ* $f(x+y) = f(x) + f(y), f(x \times y) = f(x) \times f(y)$ *et* $f(1) = 1$ *; c'est un isomorphisme s'il est de plus bijectif.*

Exemples : $\mathbb{R}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}$ mais pas $\mathbb{R}_+$ ou $\mathbb{N}$. L'ensemble des nombres décimaux est un anneau. $\mathcal{M}_n(\mathbb{K})$ est un anneau non commutatif, et non intègre. On étudiera plus en détail $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{K}[X]$.
L'image d'un anneau par un morphisme d'anneaux est un sous-anneau, mais pas son noyau (cf. infra la section sur les idéaux).

REMARQUE 4.

• *La formule du binôme* $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ *est vraie dans tout anneau* **commutatif**.

• *Un anneau contient toujours au moins deux éléments,* 0_A *et* 1_A *qu'on note juste 0 et 1 sauf ambiguïté.*

DÉFINITION 12. *On définit une structure* **d'anneau produit** *sur le produit d'anneaux* $A \times B$ *par*

$$(a,b) + (a',b') = (a+a', b+b') \qquad (a,b) \times (a',b') = (a \times a', b \times b')$$

avec les éléments neutres $(0_A, 0_B)$ *et* $(1_A, 1_B)$.

La structure suivante est celle de corps :

DÉFINITION 13. *Un corps est un anneau commutatif dans lequel tout élément non nul admet un inverse (pour* $\times$*).*

PROPOSITION. $k' \subset k$ *est un sous-corps de* k *ssi pour tous* $(x,y) \in k' \times k'^*$ *les éléments* $x - y$ *et* xy^{-1} *restent dans* k'.

Remarque : $(K, +)$ et $(K \backslash \{0\} = K^*, \times)$ sont deux groupes abéliens. Tout corps est un anneau intègre, la réciproque est fausse.
Exemples : $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ sont des corps. $\mathbb{Z}/12\mathbb{Z}$ n'est pas un corps. $\mathbb{Z}$ non plus, bien qu'intègre.

EXERCICE 22. *Montrer que l'ensemble des fractions rationnelles* $\mathbb{R}(X)$ *est un corps.*

EXERCICE 23. *Soit* k *un corps et* $P \in k[X]$ *un polynôme de degré* n. *Montrer que* P *possède au maximum* n *racines (on rappelle que* $P(\alpha) = 0 \iff \exists Q \in \mathbb{K}[X], P(X) = (X - \alpha)Q(X)$*). Trouver les racines de* $X^2 - 1$ *dans* $\mathbb{Z}/12\mathbb{Z}$*, comparer.*

2.2 L'anneau cyclique

Il y a un anneau particulièrement fondamental, « Ash nazg durbatulûk, ash nazg gimbatul, Ash nazg thrakatulûk » :

FIGURE 1 – Sur l'anneau de Sauron

2.2.1 $\mathbb{Z}/n\mathbb{Z}$ comme anneau

On vérifie que les congruences sont compatibles avec la multiplication comme on l'a fait pour l'addition, et il vient

THÉORÈME 4. *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni des lois + et $\times$ est un anneau commutatif. Ses éléments neutres sont $\dot{0}$ et $\dot{1}$. L'application π_n est un morphisme d'anneaux, surjectif.*

EXERCICE 24. *On considère l'algorithme suivant :*

```
sdc(n::entier)
 Tant que n a plus de 1 chiffre
 Remplacer n par la somme de ses chiffres
Retourne n
```

Montrer que ça marche (l'algorithme se termine) et que $\mathrm{sdc}(n)$ est constitué d'un seul chiffre (un entier entre 1 et 9) qui est congru à n modulo 9. En déduire que $\mathrm{sdc}(a \times b) = \mathrm{sdc}(a) \times \mathrm{sdc}(b)$ (preuve par 9).

EXERCICE 25. *On considère un nombre composé $n = pq$. Montrer que l'application*

$$\Psi : \pi_n(x) \mapsto (\pi_p(x), \pi_q(x))$$

est bien définie de $\mathbb{Z}/n\mathbb{Z}$ dans l'anneau produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, et que c'est un morphisme d'anneaux. (exemple : $n = 24 = 6 \times 4$, le morphisme envoie la classe de 7 mod 24 sur le couple $(\dot{7}, \bar{7}) = (\dot{1}, \bar{3}) \in \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$)
Quel est son noyau ? À quelle condition est-ce un isomorphisme ?

2.2.2 Éléments particuliers de $\mathbb{Z}/n\mathbb{Z}$

Comme on le voit dans le cas $n = 12$, il se passe des choses étranges dans $\mathbb{Z}/n\mathbb{Z}$: par exemple $\dot{6} \times \dot{4} = \dot{0}$, sans parler de $\dot{5} \times \dot{5} = \dot{1}$! Précisons les différents cas possibles :

THÉORÈME 5. *Les éléments de $\mathbb{Z}/n\mathbb{Z}$ se répartissent en deux classes :*

— *Les diviseurs de zéro ; ce sont les $\dot{a} \in \mathbb{Z}/n\mathbb{Z}$ tels qu'il existe $\dot{b} \neq \dot{0}$ avec $\dot{a} \times \dot{b} = \dot{0}$.*

— *Les éléments inversibles pour $\times$.*

On a la caractérisation :

$$\dot{a} \text{ est inversible} \iff \dot{a} \text{ n'est pas un diviseur de zéro} \iff a \text{ est premier avec } n.$$

Ces éléments inversibles sont précisément les générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Notez que ce théorème est faux dans $\mathbb{Z}$: 5 n'est certes pas un diviseur de 0, mais n'est pas inversible... dans $\mathbb{Z}$. En revanche il est vrai dans tout anneau qu'un diviseur de 0 n'est jamais inversible.

Ce théorème utilise les notions d'arithmétique étudiées en Sup ("premier avec", pgcd). On considère $d = \text{pgcd}(a, n)$, en notant que cela ne dépend pas du représentant de a choisi.

Démonstration. Si $d > 1$ alors $1 < n/d < n$ et $a \times \dfrac{n}{d} = \dfrac{a}{d} \times n$ donc en posant $b = n/d$ on a $\dot{a} \times \dot{b} = \dot{0}$ et $\dot{a}$ est diviseur de 0.

Si au contraire $d = 1$, par la propriété de BEZOUT (que l'on reverra bientôt) il existe des entiers u, v tels que $au + nv = 1$. En passant modulo n, on trouve que $\dot{u}$ est l'inverse de $\dot{a}$.

Enfin si $\dot{a}$ est inversible, c'est qu'il existe $\dot{b}$ tel que $\dot{a}\dot{b} = \dot{1}$; mais alors, le groupe engendré par $\dot{a}$ contient le groupe engendré par $\underbrace{\dot{a} + \dot{a} + \ldots \dot{a}}_{b \text{ fois}} = \dot{1}$ i.e. c'est le groupe entier.

Réciproquement, si ce groupe est le groupe entier alors il contient $\dot{1}$ d'où l'existence de $b \in \mathbb{N}$ tel que $\underbrace{\dot{a} + \dot{a} + \ldots \dot{a}}_{b \text{ fois}} = \dot{1}$ i.e. $\dot{b}\dot{a} = \dot{1}$. ♦

Exemple : en musique occidentale, on obtient les douze tonalités par « cycles de quintes » ; concrètement cela signifie qu'on passe d'une tonalité à une autre en ajoutant 7 demi-tons, modulo 12. Effectivement $\dot{7}$ engendre $\mathbb{Z}/12\mathbb{Z} = \{\dot{0}, \dot{7}, \dot{2}, \dot{9}, \ldots \dot{1}, \ldots\}$.

PROPOSITION. *L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ forme un groupe multiplicatif, noté $(\mathbb{Z}/n\mathbb{Z})^*$.*

C'est en fait **vrai dans tout anneau** : par exemple dans $\mathbb{Z}$, on a le groupe des inversibles qui a deux éléments, ± 1 ; dans un corps, tout élément non nul est inversible, par définition. Dans $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid (a, b) \in \mathbb{Z}^2\}$, il y a une infinité d'éléments inversibles (par exemple $17 - 12\sqrt{2}$).

PROPOSITION. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n = p$ est premier.*

On a ainsi une famille infinie de corps, finis et de cardinal premier.

Il existe des corps finis plus complexes, mais leur cardinal est toujours une puissance d'un nombre premier.

EXERCICE 26. *Montrer que $\mathbb{Z}/p^\alpha\mathbb{Z}$ n'est PAS un corps pour $\alpha > 1$.*

EXERCICE 27. *Montrer que l'ensemble des matrices 2×2 à coefficients dans $\mathbb{Z}/3\mathbb{Z}$ de la forme $\begin{pmatrix} \dot{a} & -\dot{b} \\ \dot{b} & \dot{a} \end{pmatrix} = \dot{a}I + \dot{b}J$ est un corps à 9 éléments.*

Version soft : quel est l'inverse de $\begin{pmatrix} \dot{2} & -\dot{1} \\ \dot{1} & \dot{2} \end{pmatrix}$?

EXERCICE 28. *Montrer que pour* p *premier,* $a^{p-1} = \dot{1}$ *pour tout* a *non nul de* $\mathbb{Z}/p\mathbb{Z}$ *(petit théorème de Fermat).*

Notons que la recherche de l'inverse d'un nombre modulo n se fait par l'algorithme d'EUCLIDE pour la recherche des coefficients de BEZOUT. C'est important en cryptographie : une méthode de codage consiste à multiplier le message m (écrit comme un grand nombre, par exemple grâce au codage ASCII ou UNICODE), par un nombre donné k (la clef de chiffrage) et à réduire le résultat modulo un (grand) n fixé. On décrypte alors le message en multipliant le message chiffré $\dot{k}\dot{m}$ par l'inverse de k modulo n. L'inconvénient de cette méthode est que si n, k sont découverts, il est assez facile de trouver $\dot{k}^{-1}$.

2.2.3 Le théorème chinois

THÉORÈME CHINOIS. *Si* p, q *sont premiers entre eux alors* $\mathbb{Z}/(pq)\mathbb{Z}$ *est isomorphe à l'anneau produit* $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Ceci se généralise aisément à un plus grand nombre de facteurs **premiers entre eux deux à deux**.

Démonstration. Pour tout entier $x \in \mathbb{Z}$ notons différemment les classes modulo p, q et $n = pq$: respectivement $\dot{x}, \bar{x}, \widetilde{x}$.
On définit un morphisme d'anneau par $\Psi(\widetilde{x}) = (\dot{x}, \bar{x})$: cette application est bien définie car si on change x en $x + kn$ – restant dans la même classe modulo n – on ne modifie pas les images $\dot{x}, \bar{x}$. Ψ va donc de $\mathbb{Z}/(pq)\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et il est immédiat que c'est un morphisme d'anneaux : par exemple

$$\Psi(\widetilde{x}.\widetilde{y}) = \Psi(\widetilde{x.y}) = (x\dot{.}y, x\bar{.}y) = (\dot{x}.\dot{y}, \bar{x}.\bar{y}) = (\dot{x}, \bar{x}) \times (\dot{y}, \bar{y}) = \Psi(x) \times \Psi(y)$$

De plus $\widetilde{x} \in \operatorname{Ker}\Psi \iff \dot{x} = \dot{0}$ et $\bar{x} = \bar{0}$, ce qui signifie que l'entier x (tout entier x dans la classe $\widetilde{x}$) est multiple de p et multiple de q, et donc de $n = pq$ puisque ces deux entiers sont premiers entre eux. Or cela signifie que $\widetilde{x} = \widetilde{0}$, autrement dit Ψ est injective.
Comme les ensembles de départ et d'arrivée ont même cardinal n, c'est une bijection, et donc un isomorphisme. ♦

REMARQUE 5. *Cette démonstration est fort abstraite. Mais les astronomes chinois voulaient surtout calculer la surjectivité de* Ψ*, i.e. résoudre des systèmes de congruence de la forme* $\begin{cases} x \equiv a \pmod p \\ x \equiv b \pmod q \end{cases} \iff \Psi(\widetilde{x}) = (\dot{a}, \bar{b})$ *afin de savoir quand tel ou tel astre se trouverait à tel ou tel endroit du ciel. Concrètement on résout ce problème à l'aide de la relation de Bezout : si* $up + vq = 1$ *alors* $x = up$ *(resp.* $y = vq$*) vérifie le système* $\begin{cases} x \equiv 0 \pmod p \\ x \equiv 1 \pmod q \end{cases}$ *(resp.* $\begin{cases} y \equiv 1 \pmod p \\ y \equiv 0 \pmod q \end{cases}$ *et la solution de la double congruence est* $bup + avq$.

Ce théorème est crucial, ramenant la structure de l'anneau cyclique à des cas plus simples – un peu comme la décomposition en facteurs premiers, dont il se fait l'écho. Il permet entre autres choses de calculer les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.
En effet, on déduit du théorème chinois que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à l'anneau produit $\mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/q^\beta\mathbb{Z} \times \dots$ où $n = p^\alpha q^\beta \dots$.
En conséquence les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ proviennent (dans l'anneau produit) des éléments inversibles de chacun des $\mathbb{Z}/p^\alpha\mathbb{Z}$, qui sont les éléments premiers avec p. Il en

résulte :

$$\mathrm{Card}(\mathbb{Z}/n\mathbb{Z})^* = \mathrm{Card}(\mathbb{Z}/p^\alpha\mathbb{Z})^* \times \mathrm{Card}(\mathbb{Z}/q^\beta\mathbb{Z})^* \times \dots$$

Exemple : $\mathbb{Z}/12\mathbb{Z}$ est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ par l'application $x \mapsto (\dot{x}, \bar{x})$. La bijection réciproque est (le vérifier) $(\dot{x}, \bar{x}) \mapsto 4\dot{x} - 3\bar{x}$. Les éléments inversibles proviennent ainsi des couples $(\dot{x}, \bar{x})$ avec $\dot{x} = \dot{1}, \dot{2}$ et $\bar{x} = \bar{1}, \bar{3}$. On trouve les classes modulo 12 de $1, 5, 7, 11$.

EXERCICE 29. *Montrer que* $a \wedge 561 = 1$ *entraîne que* $a^{560} \equiv 1 \mod 561$ *(décomposer 561 et utiliser le petit théorème de Fermat).*

EXERCICE 30. ** Montrer que les différences d'éléments de* $(\mathbb{Z}/n\mathbb{Z})^*$*, i.e. les* $b - a$ *où* a, b *sont inversibles modulo* n*, forment le groupe* $\mathbb{Z}/n\mathbb{Z}$ *tout entier si* n *est impair et le sous-groupe* $2\mathbb{Z}/n\mathbb{Z}$ *engendré par la classe de 2 sinon. Le faire pour* $n = p^\alpha$ *et conclure avec le thm chinois ci-dessus.*

Sur ce coup, les chinois furent... les premiers.
Cf. `https://www.smbc-comics.com/comic/jonathan-dowling`.

2.2.4 Calcul de la Φ d'Euler

DÉFINITION 14. $\Phi(n)$ *est le cardinal de* $(\mathbb{Z}/n\mathbb{Z})^*$*, i.e. le nombre d'éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$*, i.e. le nombre d'entiers naturels inférieurs à* n *et premiers avec* n*.*

Par exemple, $\Phi(p) = p - 1$ pour p premier.

LEMME 1. *Pour* d *divisant* n*, un entier a une chance sur* d *(pour la distribution uniforme) d'être divisible par* d*.*

Démonstration. On fait le rapport à n du nombre des multiples de d dans $[0, n-1]$, à savoir $\{0, d, 2d, \dots n - d\}$, ce qui donne bien $1/d$. En d'autres termes, les éléments de $[0, n-1]$ premiers avec d sont dans la proportion $\dfrac{d-1}{d}$. ♦

Comme être premier avec p est équivalent à être premier avec une puissance de p pour p premier, on en déduit que $\Phi(p^k) = p^k(1 - \dfrac{1}{p})$ pour p premier.

COROLLAIRE 2. *On a* $\Phi(n) = n \prod_{p|n} (1 - \dfrac{1}{p}) = \prod_i p_i^{m_i}(1 - \dfrac{1}{p_i})$ *si* $n = \prod_i p_i^{m_i}$.

Démonstration. Ceci résulte du théorème chinois, puisqu'on en déduit $\Phi(p.q) = \Phi(p)\Phi(q)$ pour p, q premiers entre eux, et *a fortiori*

$$\Phi(\mathbb{Z}/n\mathbb{Z}) = \Phi(\mathbb{Z}/p^\alpha\mathbb{Z}) \times \Phi(\mathbb{Z}/q^\beta\mathbb{Z}) \times \dots = \prod_i p_i^{m_i}(1 - \frac{1}{p_i}).$$

Mais on peut aussi garder un vocabulaire probabiliste. En effet, les propriétés d'être divisible par p ou par q sont deux variables aléatoires indépendantes (pour p, q premiers entre eux !) i.e. la probabilité de la conjonction des deux est le produit des probabilités : la probabilité d'être multiple de p est $1/p$, de même pour q, et la probabilité d'être multiple de p et q est celle d'être multiple de $p \times q$ (aussi un diviseur de n donc le Lemme s'applique), c'est donc $1/(pq)$.
On en déduit que la probabilité d'être premier avec n est le produit des probabilités d'être premier avec chacun de ses diviseurs premiers, soit $\prod_i (1 - \dfrac{1}{p_i})$, ce qui donne la formule annoncée. ♦

Exemple : Cas particuliers :

$$\Phi(n = 2^a 3^b) = \frac{1}{2}\frac{2}{3}n = \frac{n}{3} \qquad \Phi(pq) = (p-1)(q-1) \qquad \Phi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

On remarque sur le premier cas qu'il y a des droites sur le graphe de Φ :

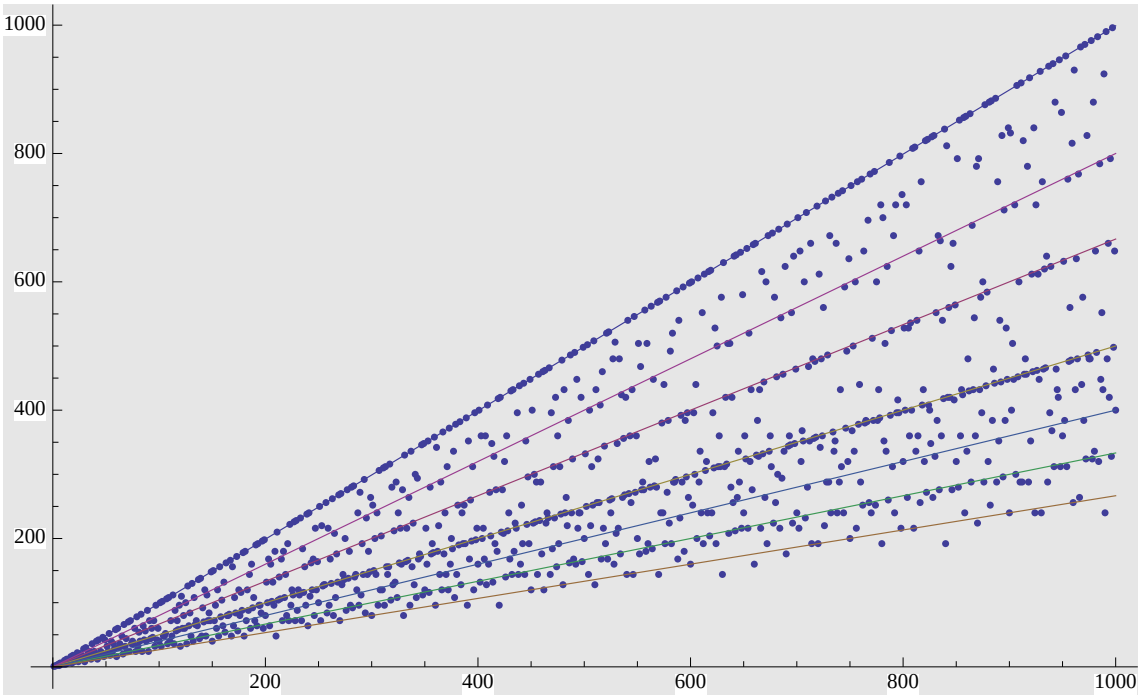

FIGURE 2 – Graphe de la fonction d'Euler

EXERCICE 31.

— *(TD info) : fabriquer votre propre algorithme pour calculer* $\Phi(n)$.
— *Trouver d'autres pentes possibles pour de telles droites.*
— *Montrer que* $\Phi(n)$ *n'est jamais impair (sauf* $\Phi(2)$*).*
— ** (recherche) Encadrer la fonction d'Euler (la difficulté est d'intuiter une minoration). Si nécessaire on pourra utiliser le résultat de l'exercice 30.*
— ** Montrer qu'il existe des nombres pairs (*$\in 2\mathbb{N}^*$*) qui ne sont pas de la forme* $\Phi(n)$.

2.2.5 La méthode RSA

Où l'arithmétique permet de gagner des milliards ! (Rivest, Shamir et Adleman n'en ont pas tant profité)

Dans le cas de $\mathbb{Z}/(pq\mathbb{Z})$ où p, q sont deux nombres premiers distincts, on a $\Phi(n) = \Phi(pq) = (p-1)(q-1)$. Posons $A = \mathbb{Z}/n\mathbb{Z}$, A^* le groupe de ses éléments inversibles. On considère un message m (de taille inférieure à n), et une clef de **chiffrage** k qui est en général publique, ainsi que n (par exemple ces deux nombres figurent dans la puce d'une carte bleue). En revanche p, q sont gardés secrets.

Le message codé est $m^k \pmod n$. On n'a pas besoin de k multiplications pour faire ce calcul mais environ $\log_2(k)$ seulement (exponentiation rapide : par exemple $m^{16} = (((m^2)^2)^2)^2$).

LEMME (THÉORÈME D'EULER ; GÉNÉRALISATION DU P.T.F.).
Pour tout $m \in A^*$, $m^{(p-1)(q-1)} = m^{\Phi(n)} = 1$.

Démonstration. L'ordre d'un élément divise le cardinal du groupe... c'est le Thm de Lagange. ♦

COROLLAIRE 3. *Pour tout* $m \in A$, $m^{1+(p-1)(q-1)} = m$.

En d'autres termes, dans $\mathbb{Z}/n\mathbb{Z}$ les suites géométriques sont toutes périodiques ![2]

EXERCICE 32. *Dernier chiffre de* $1997^{1998^{1999}}$ *? Somme des chiffres de la somme des chiffres de la somme des chiffres de* 4444^{4444} *?*

Ceci généralise le petit théorème de Fermat et résulte du théorème de Lagrange. Pour le corollaire, il suffit de rajouter le cas des multiples de p (ou de q), pour lesquels on calcule que $p^{q-1} \equiv 1 \pmod{q}$ et $p \equiv 0 \pmod{p}$ d'où $p^{1+(p-1)(q-1)} \equiv p \pmod{n}$.
Cela va permettre d'inverser la manip, c'est à dire de décrypter.
Plus généralement, pour tout message $m \in A$ et tout nombre $z \equiv 1 \pmod{(p-1)(q-1)}$ on a aussi bien $m^z \equiv m \pmod{n}$.
Soit alors d l'inverse de k **modulo** $(p-1)(q-1)$ qu'on obtient par Bezout apliqué à (p,q). Donc $kd \equiv 1 \pmod{(p-1)(q-1)}$, et le **déchiffrage** de m^k s'obtient simplement en élevant le message chiffré m^k à la puissance d : $\boxed{(m^k)^d = m \pmod{n}}$.

Exemple : $n = 13 \times 11 = 143, k = 17, m = 51, m^k = 116$.
On trouve l'inverse de k modulo $(p-1)(q-1) = 120$ facilement à la main, ou façon Bezout. Ici on trouve $113 \times 17 - 16 \times 120 = 1$: donc $d = 113$. Effectivement $116^{113} \equiv 51 = m \pmod{143}$

REMARQUE 6. *La confidentialité du procédé repose sur deux espoirs :*
- *— Que le calcul de* $d = k^{-1} \pmod{(p-1)(q-1)}$ *soit difficile.*
- *— Qu'il soit nécessaire ! (par exemple on pourrait retomber sur* m *pour une puissance relativement petite du message chiffré* m^k *– c'est effctivement une des méthodes utilisées par les hackers... et dans l'exemple on a déjà* $(m^k)^3 = m$ *!)*

Typiquement, p, q *sont des nombres premiers d'une centaine de chiffres. Pour savoir modulo quoi inverser, il faut connaître* $\Phi(n)$ *ce qui est équivalent à connaître* p *et* q *: en effet* $n - \Phi(n) = p + q - 1$ *et connaissant somme et produit il est facile de retrouver les deux facteurs. Ce problème est donc équivalent à celui de factoriser* n*, ce que l'on ne sait pas faire* ***en principe*** *pour un nombre de 250-300 chiffres décimaux (le record est de 768 bits).*

EXERCICE (THÈME DE RECHERCHE). *L'ordre d'un élément inversible de* $\mathbb{Z}/n\mathbb{Z}$ *est donc un diviseur de* $\Phi(n)$*. Mais existe-t-il toujours un élément d'ordre* égal à $\Phi(n)$ *? En d'autres termes, le groupe multiplicatif* $(\mathbb{Z}/n\mathbb{Z})^*$ *est-il cyclique ? Sinon, à quelle condition sur les facteurs premiers de* n *(en particulier le facteur 2) l'est-il ?*

2.2.6 La formule sommatoire

À titre d'exemple, donnons une jolie formule magique (hors-programme) :

PROPOSITION. $\sum_{d|n} \Phi(d) = n$

2. Parfois à partir d'un certain rang seulement, si on ne commence pas pas 1.

Démonstration. Utilisons la philosophie du théorème chinois.

— La formule est triviale quand $n = p$ est premier : $1 + (p-1) = p$.

— Ce n'est guère plus difficile quand $n = p^\alpha$: il vient

$$\sum_{k=0}^{\alpha} \Phi(p^k) = 1 + (p-1) + p(p-1) + p^2(p-1) + \dots p^{\alpha-1}(p-1) = p^\alpha$$

— Pour le cas général, je me restreins à deux facteurs premiers pour simplifier les notations : posons $n = p^\alpha q^\beta$. Tout diviseur de n s'écrit donc $d = p^a q^b, a \leqslant \alpha, b \leqslant \beta$. De plus, $\Phi(d) = \Phi(p^a)\Phi(q^b)$. Donc

$$\sum_{d|n} \Phi(d) = \sum_{a\leqslant\alpha, b\leqslant\beta} \Phi(p^a)\Phi(q^b) = \sum_{a\leqslant\alpha} \Phi(p^a) \sum_{b\leqslant\beta} \Phi(q^b) = p^\alpha q^\beta = n$$

♦

2.3 Idéaux d'un anneau commutatif

Notez bien que jusqu'à la fin du chapitre, tous les anneaux considérés sont commutatifs.

2.3.1 Définitions

Pour commencer : on remarque que $n\mathbb{Z}$ n'est pas seulement un sous-groupe de $\mathbb{Z}$, c'est « presque » un sous-anneau... c'est (en tout cas) le noyau d'un morphisme d'anneaux, le cas des groupes montre que c'est là une structure importante :

DÉFINITION 15. *Un idéal I est un sous-groupe additif, stable par multiplication par tout élément de l'anneau A :*

— $\forall x, y \in I \quad x - y \in I$

— $\forall a \in A \quad \forall x \in I \quad a.x \in I$

Attention ! la deuxième propriété n'est pas une stabilité INTERNE mais EXTERNE. Cela rappelle la loi externe des espaces vectoriels.

EXEMPLE FONDAMENTAL :

DÉFINITION 16. *Un idéal* **principal** *est une partie de la forme $aA = \{ax \mid x \in A\}$.*

C'est l'ensemble des multiples de a, autrement dit l'idéal engendré par a (le plus petit qui contienne a).

Tout idéal de $\mathbb{Z}$ étant un de ses sous-groupes, est de la forme $n\mathbb{Z}$, donc est principal. On dit que l'anneau est principal quand tous ses idéaux le sont. Cette notion n'est pas au programme mais on en a besoin pour la suite [en fait on ne verra guère d'exemples d'anneaux non principaux !].

PROPOSITION. *Le noyau d'un morphisme d'anneaux est un idéal.*

$n\mathbb{Z}$ est le type même d'un tel idéal (noyau de la projection canonique π_n modulo n).

EXERCICE 34.

— *aA et bA sont un seul et même idéal si, et seulement si, $a = b.u$ avec u inversible.*

— *Un idéal est l'anneau entier ssi il contient un élément inversible (1).*

PROPOSITION. *a divise b (ie $\exists c \mid b = ac$) ssi l'idéal aA contient l'idéal bA : $a \mid b \iff bA \subset aA$.*

Cette dernière propriété explique pourquoi DEDEKIND a introduit cette notion (sous une forme plus compliquée) : elle généralise la notion de divisibilité. [3]

EXERCICE 35. *On note π_n la surjection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. Montrer que l'image inverse (= l'ensemble des antécédents) d'un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. En déduire que tout idéal de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est principal. Quels sont les idéaux de $\mathbb{Z}/20\mathbb{Z}$?*

EXERCICE 36. *On considère l'anneau $\mathcal{D}_n$ des matrices diagonales de taille n. Montrer que tout idéal est principal, engendré par une matrice ayant des 0 et des 1 sur la diagonale. Combien cet anneau a-t-il d'idéaux ?*

EXERCICE 37. *On considère l'ensemble $\mathbb{Z}^2$ des couples d'entiers relatifs. On le munit de l'addition canonique*

$$(a, b) + (x, y) = (a + x, b + y)$$

et d'une multiplication qui l'est moins :

$$(a, b) * (x, y) = (ax + by, ay + bx).$$

Montrer que $(\mathbb{Z}^2, +, *)$ est un anneau commutatif.
Dans cet anneau, tout idéal n' est pas forcément principal.

2.3.2 Propriétés des idéaux d'un anneau commutatif

On vérifie immédiatement la proposition suivante : **PROPOSITION.** *La somme et l'intersection de deux*

On peut considérer les deux idéaux $6\mathbb{Z}$ et $10\mathbb{Z}$: on voir apparaître les pgcd, ppcm de 10 et 6 puisque on trouve $6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$ et $6\mathbb{Z} \cap 10\mathbb{Z} = 30\mathbb{Z}$. Généralisons :

DÉFINITION 17. *Quand $aA \cap bA = cA$ on pose $c = \text{ppcm}(a, b) = a \vee b$.*
Quand $aA + bA = dA$ on pose $d = \text{pgcd}(a, b) = a \wedge b$.

REMARQUE 7. *Forcément un tel c (resp. d) existe toujours, quand l'anneau est principal. Alors c est effectivement multiple de a et de b, et tout multiple commun de a, b est multiple de c. De même pour d : $a \in dA$ et b aussi donc d doit diviser a et b, et comme $d \in aA + bB$, d estr multiple de tout divieseur commun à a et b, c'est donc le plus grand d'entre eux.*
En revanche dans $\mathbb{R}[X, Y]$ par exemple, la somme des idéaux engendrés par X et par Y est l'idéal des polynômes P tels que $P(0, 0) = 0$, qui n'est pas principal : dans cet anneau on n'a pas de pgcd.
D'après un exercice ci-dessus, c ou d sont définis au produit par un élément inversible près ($-cA = cA$!).
Deux nombres n'ayant aucun diviseur commun sont dits premiers entre eux. *On en déduit dans $\mathbb{Z}$, et* plus généralement dans tout anneau principal *:*

3. Dedekind étudiait des sous-anneaux de $\mathbb{C}$, engendrés par $e^{2i\pi/n}$ afin d'étudier l'équation $x^n + y^n + z^n = 0$. Cela l'a amené à constater qu'on n'avait pas toujours de factorisation unique dans ces anneaux – contrairement à ce qu'a dû croire Fermat quand il a rédigé sa fameuse note dans sa marge trop petite...

THÉORÈME 7.

BEZOUT *: Les entiers* a *et* b *sont premiers entre eux ssi il existe* u, v *tels que*

$$au + bv = 1$$

GAUSS *: Soient* $a, b, c \in \mathbb{Z}$ *; si* a *divise* bc *en étant premier avec* c*, alors* a *divise* b*.*

Démonstration. BEZOUT : on se ramène à considérer $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.
GAUSS : $a \mid bc \iff bc\mathbb{Z} \subset a\mathbb{Z}$ et $a \wedge c = 1 \iff a\mathbb{Z} + c\mathbb{Z} = \mathbb{Z}$; en combinant il vient

$$b\mathbb{Z} = bc\mathbb{Z} + ab\mathbb{Z} \subset a\mathbb{Z}$$

càd $a \mid b$. ♦

EXERCICE 38. *Montrer de façon similaire (avec les idéaux de* $\mathbb{Z}$*) les propriétés suivantes :*

- *Si* a *est premier avec* b *et avec* c*, alors il est premier avec* bc *(*EUCLIDE*).*
- *Si* a *et* b *sont premiers entre eux et divisent tous deux* c*, alors* ab *divise* c*.*

Ces propriétés restent vraies dans tout anneau principal !
Déduire du théorème de GAUSS *que pour* p *premier,* p *divise tous les* $\binom{p}{k}, k = 1 \dots p-1$*. On en tire la belle relation* $(a+b)^p = a^p + b^p$ *valable dans* $\mathbb{Z}/p\mathbb{Z}$ *qui par récurrence redonne le PTF :* $(1+1)^p = 1^p + 1^p = 2$ *! Et de proche en proche* $a^p = a \dots$
Montrer aussi par le théorème de GAUSS *que si le carré d'un rationnel est un entier, alors ce rationnel est un entier.*

2.4 Le cas de $k[X]$

Curieusement, tout se passe comme dans $\mathbb{Z}$. C'est qu'on a la même propriété d'existence d'une division euclidienne, comme on l'a vu en Sup :

2.4.1 Division euclidienne dans $k[X]$

THÉORÈME 8. *Soient* A, B *deux polynômes,* B *non nul. Alors il existe un et un seul couple* (Q, R) *tel que*

$$A = B.Q + R \qquad d^\circ(R) < d^\circ B$$

Dem par récurrence sur le degré : c'est effectuer la division en partant du terme de plus haut degré !

2.4.2 Idéaux de $k[X]$

COROLLAIRE 4. $k[X]$ *est principal, i.e. les idéaux de* $k[X]$ *sont engendrés par un seul élément : ils sont de la forme* $I = (P) = P.k[X]$*. Avec la condition « P unitaire », P est uniquement déterminé : c'est* **le** *polynôme unitaire dont le degré est minimal dans* I*.*

Démonstration. Ceci se démontre exactement comme dans le cas de $\mathbb{Z}$: supposant l'idéal non réduit à $\{0\}$, soit P un polynôme (unitaire si on veut quitte à multiplier par un scalaire) de degré minimal dans $I \setminus \{0\}$. Pour un polynôme quelconque $M \in I$ on fait la division euclidienne $M = P \times Q + R$ où $d^\circ R < d^\circ P$; alors $P \times Q$ appartient à I par définition d'un idéal, M aussi par hypothèse et donc $R = M - P \times Q \in I$. Vue la condition sur le degré, c'est que $R = 0$, i.e. M est multiple de P. ♦

POLYNOME MINIMAL. *Fondamental : si on a un morphisme de* $k[X]$ *dans un anneau quelconque* A *(par exemple* $P \mapsto P(a)$ *où* a *est un élément d'une* $k-$*algèbre, comme on le verra avec des endomorphismes), le noyau de ce morphisme est un idéal, donc est l'ensemble des multiples d'un unique polynôme unitaire. Par exemple, pour* $k = \mathbb{Q}$ *et le morphisme* $P \mapsto P(\sqrt{2}) \in \mathbb{R}$*, on a le noyau qui est l'ensemble des multiples de* X^2-2*. Pour* $a = \sqrt[3]{7}$*, le polynôme minimal est* $X^3 - 7$*.*
Pour une matrice nilpotente, le polynôme minimal est de la forme X^n *(où* n *est* l'indice de nilpotence*).*

EXERCICE 39. *Montrer que le polynôme minimal de* $\sqrt{2} + \sqrt{3}$ *dans* $\mathbb{Q}[X]$*, i.e. le plus petit polynôme rationnel (en terme de degré) qui annule ce réel, est* $X^4 - 10X^2 + 1$*.*

2.4.3 Propriétés arithmétiques de $k[X]$

(dans ce paragraphe le corps k est un sous-corps de $\mathbb{C}$, généralement $\mathbb{R}$ mais parfois $\mathbb{Q}$).
Vu l'existence d'une division euclidienne, comme dans $\mathbb{Z}$, les théorèmes de GAUSS, BEZOUT, EUCLIDE, ... s'appliquent. PGCD et PPCM existent et sont uniques (à un élément inversible, càd une unité, càd une constante non nulle, près).

EXERCICE INFO : ALGORITHME D'EUCLIDE AVEC POLYNÔMES.
Faire une procédure qui calcule le pgcd D *de deux polynômes donnés* $A, B \in \mathbb{R}[X]$*.*
Plus compliqué, la procédure rend aussi deux polynômes de Bezout U, V *tels que* $AU + BV = D$*.*

DÉFINITION 18. $P \in k[X]$ *est* **irréductible** $\iff$ *dans toute décomposition* $P = A.B$*, l'un des facteurs* A *ou* B *est un polynôme constant.*

Ainsi tout polynôme de degré 1 est irréductible (on ne peut avoir A, B de degré $1/2$!!). Dans $\mathbb{R}[X]$, tout polynôme de degré 3 est réductible, puisqu'il admet une racine et donc un facteur de degré 1.

EXERCICE 41. *Montrer qu'un polynôme de degré 2 ou 3 est irréductible dans* $k[X]$ *si et seulement si il n'y a pas de racine, mais que c'est faux pour le degré 4.*

EXERCICE 42. *Montrer que ltout polynôme minimal (cf. supra) est irréductible dans* $k[X]$*.*

PROPOSITION. *D'après le théorème de* D'ALEMBERT-GAUSS*, les facteurs irréductibles sont :*
- *dans* $\mathbb{C}[X]$*, les polynômes de degré 1.*
- *dans* $\mathbb{R}[X]$*, les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.*

EXERCICE 43. *Montrer que le polynôme* $1 + X^4$ *est irréductible dans* $\mathbb{Q}[X]$ *(commencer par le réduire dans* $R[X]$*).*

L'intérêt de ces facteurs est qu'ils permettent d'écrire les polynômes comme produit et non comme somme. On peut donc choisir la représentation la plus avantageuse (par exemple, pour étudier des variations il est bon de factoriser la dérivée...) :

THÉORÈME 9. *Tout polynôme admet une factorisation unique en produit de facteurs irréductibles (à l'ordre près, et en prenant les facteurs unitaires).*

Par exemple dans $\mathbb{R}[X]$, le polynôme $2X^4+2$ se factorise en $2 \times (X^2+X\sqrt{2}+1) \times (X^2-X\sqrt{2}+1)$.

Exemple non trivial : dans $\mathbb{Q}[X]$, le polynôme $X^{15}-1$ se décompose en

$$(X-1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^8-X^7+X^5-X^4+X^3-X+1)$$

car ces facteurs sont irréductibles dans $\mathbb{Q}[X]$ (bon courage pour le démontrer, on peut passer par la décomposition dans $\mathbb{R}[X]$).

Démonstration. L'existence est assez facile : si P est irréductible, on factorise au pire le coefficient du terme du plus haut degré et c'est fini. Sinon, c'est que P se factorise en facteurs de degré strictement plus petit, et une récurrence sur le degré permet de conclure.
* L'unicité est plus délicate – surtout que c'est « unique à l'ordre près » et à des constantes près ! Montrons un Lemme qui exprime essentiellement ce que l'on veut :

LEMME 2. *Soit $P = \lambda \prod A_i = \lambda \prod B_j$ deux décompositions de P en produit de facteurs irréductibles unitaires (λ est le coefficient dominant). Alors tout A_i est un des B_j.*

En effet, si pour tout $j, B_j \neq A_i$ alors $A_i \wedge B_j = 1$ (vus qu'ils sont irréductibles, leurs pgcd sont soit 1 soit eux-mêmes) et alors A_i serait premier avec le produit des B_j, soit P, ce qui est absurde. ♦

Notez que ce théorème est le pendant du théorème de décomposition des entiers en produit de facteurs premiers (qui peut d'ailleurs se redémontrer de façon similaire)

EXERCICE 44. *Montrer que si $X-a_0, X-a_1, X-a_2, \dots X-a_n$ sont des facteurs de P, avec les a_i tous distincts, alors P est multiple de $\prod_{i=0}^{n}(X-a_i)$. En déduire que l'application $P \mapsto \big(P(a_0), P(a_1), P(a_2), \dots P(a_n)\big)$ est un isomorphisme de $\mathbb{K}_n[X]$ dans $\mathbb{K}^{n+1}$, et en particulier qu'il existe un et un seul polynôme de degré n au plus prenant des valeurs données en $n+1$ points donnés (interpolation de Lagrange).*

EXERCICE 45. *On considère l'ensemble des polynômes de $\mathbb{R}[X]$ qui s'écrivent P^2+Q^2 (où $P, Q \in \mathbb{R}[X]$). Montrer que cet ensemble est stable par multiplication interne.*
** En déduire (réfléchir) que tout polynôme qui ne prend que des valeurs positives sur $\mathbb{R}$ est somme de deux carrés.*