Chapitre 1. Groupes, anneaux, corps, arithmétique

Fiche de cours

A. Arithmétique des entiers, numération

I. Arithmétique des entiers

1. Divisibilité dans $\mathbb{Z}$, division euclidienne dans $\mathbb{Z}$

▪ ***Définition.*** Soit $(a, b)\in\mathbb{Z}^2$. On dit que b est un diviseur de a (ou que a est un multiple de b, ou que b divise a), et l'on note : $b \mid a$, s'il existe un entier relatif q tel que : $a = bq$.

▪ Soit $a\in\mathbb{Z}$. On note $a\mathbb{Z}$, l'ensemble des multiples de a, c'est-à-dire l'ensemble $\{b\in\mathbb{Z} / \exists q\in\mathbb{Z}, b = aq\}$.

▪ ***Dvision euclidienne.*** Soient $a\in\mathbb{Z}$ et $b\in\mathbb{N}^*$. On a : $\exists!(q, r)\in\mathbb{Z}\times\mathbb{N}^* / a = bq + r$ tels que : $r\in[0, b-1]$. Les nombres q, r, a et b sont alors appelés respectivement le quotient, le reste, le dividende et le diviseur de la division euclidienne de a par b.

b divise alors a si, et seulement si : $r = 0$, c'est-à-dire si, et seulement si : $a = bq$.

2. PGCD et PPCM de deux entiers relatifs

Soit $(a, b, c)\in(\mathbb{Z}^*)^3$.

▪ ***PGCD.*** Soit H l'ensemble : $H = \{au + bv, (u, v)\in\mathbb{Z}^2\}$, noté également $a\mathbb{Z} + b\mathbb{Z}$, et soit n l'entier naturel tel que $n = \inf(H\cap\mathbb{N}^*)$. n est alors le plus grand commun diviseur (pgcd) de a et de b, et on note : $n = pcgd(a, b)$ ou $n = a\wedge b$.

▪ ***Propriétés.***

- $a\wedge 1 = 1$,
- $a\wedge a = a$,
- $a\wedge b = b\wedge a$,
- $(a\wedge b)\wedge c = a\wedge(b\wedge c)$,
- $(ab)\wedge(ac) = |a|\times(b\wedge c)$.

▪ ***PPCM.*** On peut écrire : $\exists!m\in\mathbb{N}^* / a\mathbb{Z}\cap b\mathbb{Z} = m\mathbb{Z}$. m est alors le plus petit commun multiple de a et de b, et on note : $m = ppcm(a, b) = a\vee b$.

▪ ***Propriétés.***

- $(a\vee 1) = a$,
- $(a\vee a) = a$,
- $(a\vee b) = (b\vee a)$,
- $(a\vee b)\vee c = a\vee(b\vee c)$,
- $(ab)\vee(ac) = |a|\times(b\vee c)$.

3. Algorithme d'Euclide

■ ***Théorème d'Euclide.*** Soit $(a, b, q, r) \in (\mathbb{Z}^*)^4 / a = bq + r$. On a : $a \wedge b = b \wedge r$.

■ ***Algorithme d'Euclide.*** Soient $(a, b) \in \mathbb{Z}^2$, q le quotient et r le reste de la division euclidienne de a par b. On appelle algorithme d'Euclide l'algorithme suivant, qui permet de déterminer le pgcd de a et de b :

- Si r = 0, alors : $a \wedge b = b$,
- Sinon, on répète les opérations suivantes :
  - on stocke la valeur de r dans une variable de stockage, notée s,
  - on affecte à r le reste de la division euclidienne de b par r,
  - on affecte à b l'ancienne valeur de r (stockée dans s),

jusqu'à ce que la condition (r = 0) soit réalisée. On a alors : $a \wedge b = s$, autrement dit le pgcd de a et de b est le dernier reste non nul des divisions euclidiennes successives de a par b, de b par r, etc.

Exemple : Si l'on cherche le pgcd des nombres 1463 et 1078, l'algorithme d'Euclide effectue les divisions euclidiennes successives suivantes :
- *$1463 = 1.1078 + 385$;*
- *$1078 = 2.385 + 308$;*
- *$385 = 1.308 + 77$;*
- *$308 = 4.77 + 0$.*

On trouve ainsi : $1463 \wedge 1078 = 77$.

4. Entiers premiers entre eux, théorèmes de Bézout et de Gauss

■ ***Définition.*** Soit $(a, b) \in (\mathbb{Z}^*)^2$. On dit que a et b sont premiers entre eux, ou étrangers, si : $a \wedge b = 1$.

■ ***Propriété.*** Soient $(a, b) \in (\mathbb{Z}^*)^2$ et d un diviseur commun à a et à b ($d \in \mathbb{N}^*$). En notant a' et b' les entiers relatifs tels que : $a = da'$ et : $b = db'$, on peut écrire : $(d = a \wedge b \Leftrightarrow a' \wedge b' = 1)$.

■ ***Théorème de Bézout.*** Soit $(a, b) \in (\mathbb{Z}^*)^2$. a et b sont premiers entre eux si, et seulement si : $\exists (u, v) \in \mathbb{Z}^2 / au + bv = 1$.

■ ***Corollaires.*** Soient $(a, b, c) \in (\mathbb{Z}^*)^3$ et $(n, p) \in (\mathbb{N}^*)^2$. On a :

- $(a \wedge (bc) = 1) \Leftrightarrow (a \wedge b = 1 \text{ et } a \wedge c = 1)$,
- $(a \wedge b = 1) \Leftrightarrow (a^n \wedge b^p = 1)$,
- $(ab) \wedge (ac) = |a| \wedge (b \wedge c)$.

■ ***Algorithme donnant les coefficients de Bézout.*** Soient $(a, b) \in (\mathbb{Z}^*)^2$, q_2 et r_2 le quotient et le reste de la division euclidienne de a par b. En notant $a = r_0$, $b = r_1$ et pour tout entier i supérieur ou égal à 2, r_i (resp. q_i) le reste (resp. le quotient) de la division euclidienne de r_{i-2} par r_{i-1}, on a : $\forall i \geq 2$, $r_{i-2} = r_{i-1}q_i + r_i$. En notant n le premier entier i tel que $r_i = 0$, on a, d'après l'algorithme d'Euclide : $a \wedge b = r_{n-1}$. L'algorithme suivant permet alors de déterminer les coefficients de Bezout relativement aux nombres a et b :

- On effectue l'algorithme d'Euclide en stockant dans des variables $r_2, \ldots, r_{n-1}$ (resp. $q_2, \ldots, q_{n-1}$) les restes (resp. les quotients) des divisions euclidiennes successives de r_{i-2} par r_{i-1} ($i \in [2, n-1]$).
- On introduit quatre variables entières c, d, u et v,
- Si n = 2 *(on a alors : $a \wedge b = b$ et : $a.0 + b.1 = a \wedge b$)*, on affecte à c, d, u et v les valeurs respectives a, b, 0 et 1,
- Sinon, on affecte à c, d, u et v les valeurs respectives r_{n-3}, r_{n-2}, 1 et $-q_{n-2}$ *(on a alors : $cu + dv = a \wedge b$)*,
- Si $n \geq 4$, pour tout entier i compris entre 4 et n, on effectue successivement les opérations suivantes :
  - on stocke la valeur de c dans une variable de stockage, notée s,

- on stocke la valeur de u dans une variable de stockage, notée t,
- on affecte à c la valeur d,
- on affecte à u la valeur r_{n-i},
- on affecte à v la valeur t,
- on affecte à d la valeur s + d(- q_{n-i+1}).

A l'issue de l'algorithme, c et d contiennent les valeurs a et b, et on a toujours : cu + dv = a ∧ b, d'où : au + bv = a ∧ b.

Exemple : Si l'on cherche les coefficients de Bezout des nombres 1463 et 1078, on effectue l'algorithme d'Euclide (cf. supra) et l'algorithme ci-dessus amène les résultats successifs suivants :

- *77 = 1.385 + (-1).308,*
- *77 = (-1).(1078 - 2.385) + 1.385 = (-1).1078 + 3.385,*
- *77 =3.(1463 - 1078) + (-1).1078 = 3.1463 + (-4).1078.*

*On trouve ainsi : 1463.**3** + 1078.**(-4)** = 1463 ∧ 1078 = 77.*

▪ ***Théorème de Gauss.*** Soient $(a, b, c) \in (\mathbb{Z}^*)^3$. On a : $\begin{cases} a \wedge b = 1 \\ a \mid bc \end{cases} \Rightarrow a \mid c$.

5. Nombres premiers

▪ Soit p un entier naturel supérieur ou égal à 2. p admet au moins 4 diviseurs : 1, -1, p et - p.

▪ ***Définition.*** Soit $p \in \mathbb{N}^*$. On dit que p est un nombre premier si $p \geq 2$ et si p admet exactement 4 diviseurs, et l'on note $\mathbb{P}$ l'ensemble des nombres premiers.

N. B. : 1 n'est pas un nombre premier.

▪ ***Propriété.*** Tout entier naturel supérieur ou égal à 2 admet au moins un diviseur premier.

▪ ***Corollaire.*** L'ensemble $\mathbb{P}$ des nombres premiers est infini.

▪ ***Indicatrice d'Euler.*** Soit $n \in \mathbb{N}^*$. On appelle indicatrice d'Euler, la fonction φ qui à tout entier n non nul associe le nombre d'entiers compris entre 1 et n premiers avec n.

▪ ***Décomposition en produit de facteurs premiers.*** Soit n un entier naturel supérieur ou égal à 2. Il existe un entier naturel $m \in \mathbb{N}^*$, une famille finie $(p_1, p_2, \ldots, p_m)$ de nombres premiers et deux à deux distincts, unique à l'ordre près, et une famille $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ d'entiers naturels non nuls, unique à l'ordre près, telles que : $n = \prod_{k=1}^{m} p_k^{\alpha_k}$. Cette écriture s'appelle décomposition de n en produits de facteurs premiers.

6. Nombres rationnels

▪ Soient $q \in \mathbb{Q}$ et $(a, b) \in \mathbb{N} \times \mathbb{Z}^* / q = \frac{a}{b}$. On peut écrire : $\exists!(a', b') \in \mathbb{Z} \times \mathbb{N}^* / q = \frac{a'}{b'}$ et : $a' \wedge b' = 1$. Cette écriture est appelée forme irréductible, ou forme simplifiée, de q.

II. Numération

▪ ***Numération en base 10 (numération décimale).*** Soit n un entier naturel. En base 10, l'écriture de n est composée des chiffres de 0 à 9. Si $n = \sum_{i=0}^{p} \alpha_{p-i} 10^i$, alors n s'écrit : $\overline{\alpha_0 \alpha_1 \alpha_2 \ldots \alpha_p}^{10}$, ou, par convention, en omettant de surligner ces chiffres : $\alpha_0\alpha_1\alpha_2 \ldots \alpha_p$. Par exemple, on a : $123 = 1\times10^2 + 2\times10^1 + 3\times10^0$.

▪ ***Numération en base 2 (numération binaire).*** Soit n un entier naturel. Il existe une unique décomposition de la forme $n = \sum_{i=0}^{p} \alpha_{p-i} 2^i$ où $\forall i \in [0, p]$, $\alpha_i \in \{0, 1\}$. L'écriture de n en base 2 est alors : $\overline{\alpha_0 \alpha_1 \alpha_2 \dots \alpha_p}^{\,2}$. En base 2, l'écriture de n est composée uniquement des chiffres 0 et 1. Pour exprimer un nombre n connu sous sa forme décimale (base 10) en binaire (base 2), on effectue la division euclidienne de n par 2, puis du quotient ainsi obtenu par 2, et ainsi de suite jusqu'à obtenir un quotient nul. On note $r_1, r_2, \dots, r_p$ les restes successifs de ces divisions (on a alors $r_p = 1$). n s'écrit alors $\overline{r_p r_{p-1} r_{p-2} \dots r_1}^{\,2}$.

Exemple : si l'on veut écrire 1234 en base 2, on divise 1234 par 2 et l'on obtient un reste r_1 égal à 0, un quotient q_1 égal à 617 ; en divisant alors 617 par 2, on obtient un reste r_2 égal à 1 et un quotient q_2 égal à 308. En répétant cette opération à partir de q_2, on obtient alors : $r_3 = 0$, $r_4 = 0$, $r_5 = 1$, $r_6 = 0$, $r_7 = 1$, $r_8 = 1$, $r_9 = 0$, $r_{10} = 0$ et $r_{11} = 1$. On a donc : $1234 = \overline{10011010010}^{\,2}$.

▪ ***Algorithme d'exponentiation rapide.*** Soient $a \in \mathbb{R}$ et $n \in \mathbb{N}^*$ / $n = \overline{\alpha_0 \alpha_1 \alpha_2 \dots \alpha_p}^{\,2}$, où : $\forall i \in [0, p]$, $\alpha_i \in \{0, 1\}$. En notant S l'ensemble : $S = \{i \in I, \alpha_{p-i} = 1\}$. On a alors : $n = \sum_{i \in S} 2^i$ et : $a^n = \prod_{i \in S} a^{(2^i)}$. On appelle algorithme d'exponentiation rapide, l'algorithme suivant, qui permet de calculer rapidement a^n ($n \in \mathbb{N}^*$) en calculant les $a^{(2^i)}$, $i \in S$:

- On applique l'algorithme décrit auparavant pour déterminer la numérotation de n en base 2 ($n = \overline{\alpha_0 \alpha_1 \alpha_2 \dots \alpha_p}^{\,2}$),
- On introduit trois variables P, j et u à qui l'on affecte respectivement les valeurs 1, 0 et a,
- Pour chacun des entiers i compris entre 1 et p, si $\alpha_i \neq 0$, on effectue successivement les opérations suivantes :
  - on élève u au carré (i - j) fois de suite, et l'on stocke le résultat obtenu dans u (*u contient alors $a^{(2^i)}$ pour la dernière valeur i telle que $\alpha_i \neq 0$*),
  - on affecte à j la valeur i (*j contient alors la dernière valeur i telle que $\alpha_i \neq 0$*),
  - on affecte à P la valeur P × u (*P contient alors le produit des $a^{(2^k)}$ pour tout entier k inférieur ou égal à i tel que $\alpha_k \neq 0$*).

On a alors : $P = \prod_{k \in S} a^{(2^k)}$, autrement dit : $P = a^n$.

Exemple : si l'on veut calculer $(1,01)^{1234}$, comme $1234 = \overline{10011010010}^{\,2}$, l'algorithme d'exponentiation rapide utilise l'égalité : $(1,01)^{1234} = (1,01)^{2^{10}}.(1,01)^{2^7}.(1,01)^{2^6}.(1,01)^{2^4}.(1,01)^{2^1}$, donc il suffit de calculer :

- *$u_1 = (1,01)^{(2^1)}$ (une élévation au carré)*
- *$u_4 = (1,01)^{(2^4)} = ((u_1^2)^2)^2$ (trois élévations au carré),*
- *$u_6 = (1,01)^{(2^6)} = (u_4^2)^2$ (deux élévations au carré),*
- *$u_7 = (1,01)^{(2^7)} = u_6^2$ (une élévation au carré),*
- *$u_{10} = (1,01)^{(2^{10})} = ((u_7^2)^2)^2$ (trois élévations au carré),*
- *$P = (1,01)^{1234} = u_1 u_4 u_6 u_7 u_{10}$ (4 produits).*

Ainsi, 14 produits suffisent et on trouve finalement : P = 215 067,728290905.

B. Structures algébriques usuelles

I. Groupes, sous-groupes

1. Loi de composition interne

Soit E un ensemble non vide.

▪ ***Définition.*** On appelle loi de composition interne sur E toute application définie sur E^2 et à valeurs dans E.

■ ***Notation.*** Soit $*$ une loi de composition interne sur E. On note : $x * y = *(x, y)$.

■ ***Associatitivité.*** Soit $*$ une loi de composition interne sur E. On dit que $*$ est associative si :

$\forall (x, y, z) \in E^3, (x * y) * z = x * (y * z)$.

■ ***Commutativité.*** Soit $*$ une loi de composition interne sur E. On dit que $*$ est commutative si :

$\forall (x, y) \in E^2, x * y = y * x$.

■ ***Élément neutre.*** Soient $*$ une loi de composition interne sur E et e un élément de E. On dit que e est élément neutre de E pour la loi $*$ si : $\forall x \in E, x * e = e * x = x$. Si E possède un élément neutre pour la loi $*$, alors cet élément est unique.

■ ***Inverse.*** Soient $*$ une loi de composition interne sur E admettant un élément neutre noté e, et x un élément de E. On dit que x est inversible pour la loi $*$ s'il existe un élément x' de E tel que : $x * x' = x' * x = e$. L'élément x' est alors appelé l'inverse, ou le symétrique, de x pour la loi $*$.

■ ***Distributivité.*** Soient $*_1$ et $*_2$ deux lois de composition internes sur E. On dit que $*_2$ est distributive par rapport à $*_1$ si : $\forall (x, y, z) \in E^3, (x *_1 y) *_2 z = x *_1 (y *_2 z) = (x *_2 z) *_1 (y *_2 z)$.

2. Groupe, sous-groupe

■ ***Groupe.*** Soit G un ensemble muni d'une loi de composition interne $*$. On dit que l'ensemble G muni de la loi $*$, noté $(G, *)$, est un groupe si :

– la loi $*$ est associative,
– G admet un élément neutre pour la loi $*$,
– tout élément de G est inversible pour la loi $*$.

Remarque : un groupe $(G, *)$ est souvent noté G.

■ $(\mathbb{Z}, +)$ est un groupe. On appelle groupe additif des nombres entiers, le groupe $(\mathbb{Z}, +)$.

■ ***Sous-groupe.*** Soient $(G, *)$ un groupe et H une partie de G. On dit que H est un sous-groupe de $(G, *)$ si :

– H contient l'élément neutre de G pour la loi $*$,

– H est stable par la loi $*$ (autrement dit : $\forall (x, y) \in H^2, (x * y) \in H$),

– pour tout élément a de H, le symétrique de a pour la loi $*$ appartient à H.

Caractérisation d'un sous-groupe : H est un sous-groupe de $(G, *)$ si, et seulement si :

– H est non vide,
– $\forall (x, y) \in H^2, (x * y^{-1}) \in H$ *(où y^{-1} désigne le symétrique de y pour la loi $*$).*

■ Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles $n\mathbb{Z}$, où $n \in \mathbb{N}$.

3. Groupe commutatif

■ ***Définition.*** Soit $(G, *)$ un groupe. On dit que $(G, *)$ est un groupe commutatif si la loi $*$ est commutative.

Remarque : la loi d'un groupe commutatif est souvent notée $+$.

■ ***Notation Σ.*** Soient $(G, +)$ un groupe commutatif, n et m deux entiers naturels tels que $n \leq m$ et $(a_n, ..., a_m)$ un $(m - n + 1)$ - uplet d'éléments de G. On note : $a_n + ... + a_m = \sum_{i=n}^{m} a_i$.

4. Morphisme de groupes

■ ***Définitions.*** Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes et f une application de G_1 dans G_2.

• On dit que f est un morphisme de groupes (ou homomorphisme) de $(G_1, *_1)$ dans $(G_2, *_2)$ si :

$\forall (x, y) \in G_1^2$, $f(x *_1 y) = f(x) *_2 f(y)$.

• On dit que f est un isomorphisme de groupes de $(G_1, *_1)$ sur $(G_2, *_2)$ si f est un morphisme de groupes bijectif de $(G_1, *_1)$ sur $(G_2, *_2)$.

• On dit que f est un automorphisme de groupes de $(G_1, *_1)$ si f est un morphisme de groupes bijectif de $(G_1, *_1)$ sur lui-même.

▪ ***Groupes isomorphes.*** Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On dit que $(G_1, *_1)$ et $(G_2, *_2)$ sont isomorphes s'il existe un isomorphisme de groupes de $(G_1, *_1)$ dans $(G_2, *_2)$.

▪ ***Image.*** Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes et f un morphisme de groupes de G_1 dans G_2. On appelle image de f, et l'on note Im f, l'ensemble $f(G_1)$.

Propriété : Im f est un sous-groupe de $(G_2, *_2)$.

▪ ***Noyau.*** Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes, e_2 l'élément neutre de G_2 et f un morphisme de groupes de G_1 dans G_2. On appelle noyau de f, l'ensemble $f^{-1}(\{e_2\})$, c'est-à-dire l'ensemble $\{x \in G_1, f(x) = e_2\}$.

Remarque : La notation f^{-1} est une convention et ne signifie pas que f est bijective (cf. chapitre "Préliminaires").

Propriété : Ker f est un sous-groupe de $(G_1, *_1)$.

5. Groupe $\mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N}^*)$

▪ ***Sous-groupes de*** $\mathbb{Z}$. Les sous-groupes du groupe $(\mathbb{Z}, +)$ sont les sous-ensembles $n\mathbb{Z}$, où $n \in \mathbb{N}$.

▪ ***Relation de congruence modulo n*** $(n \in \mathbb{N}^*)$. Soient $n \in \mathbb{N}^*$ et $\mathcal{R}_n$ la relation définie sur $\mathbb{Z}$ par : $x \mathcal{R}_n y \Leftrightarrow (x - y) \in n\mathbb{Z}$. La relation $\mathcal{R}_n$ est une relation d'équivalence appelée relation de congruence modulo n. Pour tout couple d'entiers relatifs (x, y), on note $x \equiv y \bmod n$, ou $x \equiv y\ [n]$, la propriété : $x \mathcal{R}_n y$. On dit alors que x est congru à y modulo n.

Propriété : soit $(x, x', y, y') \in \mathbb{Z}^4$ tel que : $x \equiv x'\ [n]$ et : $y \equiv y'\ [n]$. On a : $x + y \equiv x' + y'\ [n]$.

▪ ***Groupe-quotient*** $\mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N}^*)$. Soit $n \in \mathbb{N}^*$.

• Pour tout $k \in \mathbb{Z}$, on note $\overline{k}$ l'ensemble des entiers relatifs équivalents à k pour la relation de congruence modulo n, i.e. l'ensemble des entiers congrus à k modulo n.

• On appelle ensemble-quotient de $\mathbb{Z}$ par $n\mathbb{Z}$, et l'on note $\mathbb{Z}/n\mathbb{Z}$, l'ensemble : $\left\{\overline{k}, k \in [0, n-1]\right\}$.

• On définit alors sur $\mathbb{Z}/n\mathbb{Z}$ la loi de composition interne + définie par : $\overline{x} + \overline{y} = \overline{x + y}$. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe communtatif, d'élément neutre $\overline{0}$.

Remarque : $\mathbb{Z}/n\mathbb{Z}$ est une partition de $\mathbb{Z}$ en n classes d'équivalence pour la relation de congruence modulo n.

▪ Soit $n \in \mathbb{N}^*$. On définit sur $\mathbb{Z}/n\mathbb{Z}$ la loi de composition interne + définie par : $\overline{x} + \overline{y} = \overline{x + y}$. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif, d'élément neutre $\overline{0}$.

▪ ***Morphisme canonique de*** $\mathbb{Z}$ ***sur*** $\mathbb{Z}/n\mathbb{Z}$. Soit $n \in \mathbb{N}^*$. L'application définie sur $\mathbb{Z}$ par : $x \mapsto \overline{x}$ est un morphisme de groupes de $(\mathbb{Z}, +)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$, appelé morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

6. Génération d'un groupe

▪ ***Partie, génératrice, élément générateur d'un groupe.*** Soient $(G, *)$ un groupe et $A \subset G$.

• On appelle sous-groupe de $(G, *)$ engendré par A, et l'on note gr(A), l'intersection de tous les sous-groupes de $(G, *)$ contenant A.

• On dit que A est une partie génératrice de $(G, *)$ si : $gr(A) = G$.

• Si $A = \{a\}$ où $a \in G$, on appelle sous-groupe de $(G, *)$ engendré par a, et l'on note gr(a), le sous-groupe engendré par $\{a\}$.

• Si $A = \{a\}$ où $a \in G$, on dit que a est un générateur de G si la partie $\{a\}$ est génératrice de $(G, *)$.

▪ Soient (G, $*$) un groupe et $a \in G$. L'application φ_a définie sur $\mathbb{Z}$ par : $k \mapsto a * a * ... * a$ (k fois) est un morphisme de groupes de $(\mathbb{Z}, +)$ dans (G, $*$).

*Remarque : si la loi du groupe G est notée + (resp ×), (a * a *... * a) est souvent noté ka (resp. a^k).*

Propriétés :

• Im φ_a est le sous-groupe de (G, $*$) engendré par a.

• Ker φ_a est soit réduit à {0} (on dit alors que a est d'ordre infini), soit de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}^*$ (on dit alors que g est d'ordre n).

• Si Ker φ_a est réduit à {0}, alors (Im φ_a, $*$) est isomorphe à $(\mathbb{Z}, +)$.

• Si Ker φ_a est de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}^*$, alors (Im φ_a, $*$) est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

▪ ***Ordre d'un groupe fini.***

• Soit (G, $*$) un groupe. On dit que (G, $*$) est un groupe fini si G est un ensemble fini.

• Soit (G, $*$) un groupe fini. On appelle ordre du groupe (G, $*$), le cardinal de l'ensemble G.

▪ ***Groupe cyclique.*** Soit (G, $*$) un groupe. On dit que (G, $*$) est un groupe cyclique s'il est fini et qu'il admet un générateur.

▪ Soient $n \in \mathbb{N}^*$, (G, $\cdot$) un groupe cyclique d'ordre n, a un générateur de (G, $\cdot$), s le morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ et pour tout $k \in \mathbb{Z}$, m l'unique antécédent par s de $\overline{k}$ appartenant à $[0, n-1]$. L'application définie sur $\mathbb{Z}/n\mathbb{Z}$ par : $\overline{k} \mapsto a^m$ est un isomorphisme de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sur (G, $\cdot$).

Exemple : en conservant les mêmes notations, l'application définie sur $\mathbb{Z}/n\mathbb{Z}$ par : $\overline{k} \mapsto e^{i\frac{2m\pi}{n}}$ est un isomorphisme de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sur $(\mathbb{U}_n, \times)$, où l'on rappelle que $\mathbb{U}_n$ désigne l'ensemble des racines n-èmes (complexes) de l'unité.

▪ ***Générateurs de*** $(\mathbb{Z}/n\mathbb{Z}, +)$. Soit $n \geq 2$.

• $\overline{1}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

• Pour tout $k \in \mathbb{Z}$, $\overline{k}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si, et seulement si, k est premier avec n.

7. Produit de deux groupes

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On définit sur $G_1 \times G_2$ la loi de composition interne $*$ par : $\forall (x_1, y_1) G_1^2, \forall (x_2, y_2) G_2^2, (x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$. $(G_1 \times G_2, *)$ est un groupe.

II. Anneaux, sous-anneaux

1. Anneau, sous-anneau

▪ ***Définition.*** Soient A un ensemble non vide, + et × deux lois de compositions internes sur A. On dit que A, muni des deux lois + et ×, que l'on note (A, +, ×), est un anneau (ou anneau unitaire) si :

– (A, +) est un groupe commutatif,

– la loi × est associative, et distributive par rapport à la loi +,

– A admet un élément neutre pour la loi ×.

▪ ***Anneau commutatif.*** Soit (A, +, ×) un anneau. On dit que (A, +, ×) est un anneau commutatif si la loi × est commutative.

Remarque : on rappelle que dans un anneau (A, +, ×), la loi + est quant à elle toujours commutative.

▪ $(\mathbb{Z}, +, \times)$ est un anneau (commutatif). On appelle anneau des nombres entiers, l'anneau $(\mathbb{Z}, +, \times)$.

▪ ***Notation*** Σ. Soient (A, +, ×) un anneau, n et m deux entiers naturels tels que $n \leq m$ et $(a_n, ..., a_m)$ un $(m-n+1)$ - uplet d'éléments de A. On note : $a_n + ... + a_m = \sum_{i=n}^{m} a_i$.

▪ ***Distributivité.*** Soit $(n, m, p, q)\in\mathbb{N}^4$ tel que $n \leq m$ et $p \leq q$. On a : $\sum_{i=n}^{m}\left(a_i \times \sum_{j=p}^{q} b_j\right) = \sum_{i=n}^{m}\left(\sum_{j=p}^{q} a_i \times b_j\right)$.

▪ ***Sous-anneau.*** Soient $(A, +, \times)$ un anneau et B une partie de A. On dit que B est un sous-anneau de $(A, +, \times)$ si :

– B est un sous-groupe de $(A, +)$,
– B est stable pour la loi $\times$,
– B contient l'élément neutre de A pour la loi $\times$.

Caractérisation d'un sous-anneau : B est un sous-anneau de $(A, +, \times)$ si, et seulement si :

– B contient l'élément neutre de A pour la loi $\times$,
– $\forall(x, y)\in B^2$, $(x \times y)\in B$,
– $\forall(x, y)\in B^2$, $(x + (-y))\in B$ *($(-y)$ désignant l'inverse de y pour la loi $+$).*

2. Morphisme d'anneaux

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux, d'éléments neutres respectifs 1_A et 1_B pour les lois $\times_A$ et $\times_B$.

▪ ***Définition.*** Soit φ une application de A dans B. On dit que φ est un morphisme d'anneaux de $(A, +_A, \times_A)$ dans $(B, +_B, \times_B)$ si :

– φ est un morphisme de groupes de $(A, +_A)$ dans $(B, +_B)$, i.e. si : $\forall(x, y)\in A^2$, $\varphi(x +_A y) = \varphi(x) +_B \varphi(y)$,
– $\forall(x, y)\in A^2$, $\varphi(x \times_A y) = \varphi(x) \times_B \varphi(y)$,
– $\forall(x, y)\in A^2$, $\varphi(1_A) = 1_B$.

Remarque : φ étant un morphisme de groupes de $(A, +_A)$ dans $(B, +_B)$, le noyau et l'image de φ ont déjà été définis.

▪ ***Isomorphisme d'anneaux.*** Soit φ un morphisme d'anneaux de $(A, +_A, \times_A)$ dans $(B, +_B, \times_B)$. On dit que φ est un isomorphisme d'anneaux de $(A, +_A, \times_A)$ sur $(B, +_B, \times_B)$ si φ est bijectif.

3. Idéal d'un anneau commutatif

Soit $(A, +, \times)$ un anneau commutatif.

▪ ***Définition.*** Soit I une partie non vide de A. On dit que I est un idéal de A si :

– I est stable pour la loi $+$,
– $\forall(a, i)\in A \times I$, $(a \times i)\in I$ (ou $(i \times a)\in I$, l'anneau étant supposé commutatif).

▪ ***Idéal engendré par un élément.*** Soit $x\in A$. L'ensemble $\{x \times y, y\in A\}$, noté xA (ou Ax, l'anneau étant supposé commutatif), est un idéal de A appelé idéal de A engendré par x.

4. Divisibilité dans un anneau intègre

▪ Soit $(A, +, \times)$ un anneau. On dit que $(A, +, \times)$ est l'anneau nul si $0_A = 1_A$. On a alors : $A = \{0_A\}$.

▪ ***Anneau intègre.*** Soit $(A, +, \times)$ un anneau. On dit que $(A, +, \times)$ est un anneau intègre s'il est non nul, commutatif, et si : $\forall(a, b)\in A^2$, $a \times b = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$.

▪ Soient $(A, +, \times)$ un anneau intègre et $(x, y)\in A^2$. On dit que x divise y, et l'on note $x \mid y$, s'il existe $z\in A$ tel que : $x \times z = y$.

▪ Soient $(A, +, \times)$ un anneau intègre et $(x, y)\in A^2$. x divise y si, et seulement si, $yA \subset xA$.

5. Idéaux de $\mathbb{Z}$ et compléments d'arithmétique

▪ $(\mathbb{Z}, +, \times)$ est un anneau commutatif.

▪ Les idéaux de $(\mathbb{Z}, +, \times)$ sont les sous-groupes de $(\mathbb{Z}, +)$, i.e. les ensembles $n\mathbb{Z}$, où $n\in\mathbb{N}$.

▪ ***Caractérisation du PPCM de deux entiers.*** Soit $(a, b)\in(\mathbb{Z}^*)^2$. $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$. Le ppcm de a et de b

est l'unique entier $p \in \mathbb{N}^*$ vérifiant : $a\mathbb{Z} \cap b\mathbb{Z} = p\mathbb{Z}$.

▪ ***Caractérisation du PGCD de deux entiers.*** Soit $(a, b) \in (\mathbb{Z}^*)^2$. L'intersection de tous les idéaux de $(\mathbb{Z}, +, \times)$ contenant $a\mathbb{Z} \cup b\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$ (appelé idéal engendré par $a\mathbb{Z} \cup b\mathbb{Z}$), égal à $\text{pgcd}(a, b)\mathbb{Z}$.

▪ ***Théorème de Bézout.*** Soit $(a, b) \in (\mathbb{Z}^*)^2$. a et b sont premiers entre eux si, et seulement si, l'idéal de $(\mathbb{Z}, +, \times)$ engendré par $a\mathbb{Z} \cup b\mathbb{Z}$ est égal à $\mathbb{Z}$.

▪ ***Théorème de Gauss.*** Soient $(a, b) \in (\mathbb{Z}^*)^2$. On a : $\begin{cases} a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \\ (bc)\mathbb{Z} \subset a\mathbb{Z} \end{cases} \Rightarrow c\mathbb{Z} \subset a\mathbb{Z}$.

6. Anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$.

▪ Soit $(x, x', y, y') \in \mathbb{Z}^4$. On a : $x \equiv y\ [n]$ et $x' \equiv y'\ [n] \Rightarrow (x + x') \equiv (y + y')\ [n]$.

▪ On définit sur $\mathbb{Z}/n\mathbb{Z}$ la loi de composition interne $\times$ définie par : $\overline{x} \times \overline{y} = \overline{xy}$. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

▪ ***Morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.*** L'application définie sur $\mathbb{Z}$ par : $x \mapsto \overline{x}$ est un morphisme d'anneaux de $(\mathbb{Z}, +, \times)$ sur $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, appelé morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

▪ ***Eléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.*** Soit $x \in \mathbb{Z}$. $\overline{x}$ est inversible (pour la loi $\times$) dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ si, et seulement si, $\overline{x}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, i.e. si, et seulement si, x est premier avec n.

Remarque : le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est égal à $\varphi(n)$, où φ est la fonction indicatrice d'Euler.

▪ Soient $(A, +, \times)$ un anneau, s le morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$, et φ un morphisme d'anneaux de $(\mathbb{Z}, +, \times)$ dans $(A, +, \times)$ tel que : $\text{Ker}\ \varphi = n\mathbb{Z}$. Il existe alors un morphisme d'anneaux g de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ dans $(A, +, \times)$ tel que : $\varphi = g \circ s$.

III. Corps, sous-corps

1. Corps, sous-corps

▪ ***Définition.*** Soient K un ensemble non vide, + et $\times$ deux lois de compositions internes sur K. On dit que K, muni des deux lois + et $\times$, que l'on note $(K, +, \times)$, est un corps si :

– $(K, +, \times)$ est un anneau non réduit à $\{0_K\}$, où 0_K est l'élément neutre de K pour la loi +, *(on dit alors que $(K, +, \times)$ est un anneau non nul)*,
– la loi $\times$ est commutative *(on dit alors que $(K, +, \times)$ est un anneau commutatif)*,
– tout élément de $K \setminus \{0_K\}$ admet un symétrique pour la loi $\times$.

▪ $(\mathbb{Q}, +, \times)$ est un corps. On appelle corps des nombres rationnels, le corps $(\mathbb{Q}, +, \times)$.

▪ ***Sous-corps.*** Soient $(K, +, \times)$ un corps. On dit que L est un sous-corps de $(K, +, \times)$ si :

– L est un sous-anneau de $(K, +, \times)$,
– $(L, +, \times)$ est un corps.

2. Corps $\mathbb{Z}/p\mathbb{Z}$

Soit $p \in \mathbb{N}^*$. $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps si, et seulement si, p est premier.

3. Caractéristique d'un corps

Soit $(K, +, \times)$ un corps.

▪ ***Définition.*** On appelle caractéristique de $(K, +, \times)$, le nombre égal à 0 si le sous-groupe additif de K engendré par 1_K est infini, et au cardinal de ce sous-groupe si celui-ci est fini.

▪ Si la caractéristique de $(K, +, \times)$ est non nulle, c'est le plus petit entier n tel que $\sum_{k=1}^{n} 1_K = 0_K$.

Remarque : La quasi-totalité des corps étudiés en MP/MP* sont de caractéristique nulle (tout corps de caractéristique nulle étant infini). S'agissant des corps finis, leur caractéristique est soit 0, soit un nombre premier. Par exemple, le corps $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ est de caractéristique 5.

IV. Groupe symétrique

1. Définitions

▪ ***Groupe symétrique.*** Soit $n \in \mathbb{N}^*$. On appelle groupe symétrique (ou groupe symétrique des permutations) d'indice n, et on note $\mathcal{S}_n$, l'ensemble des permutations de $[1, n]$, c'est-à-dire l'ensemble des bijections de $[1, n]$ sur $[1, n]$.

▪ On munit $\mathcal{S}_n$ de la loi $\circ$ définie par : $\forall (\sigma, \sigma') \in \mathcal{S}_n^2$, $\forall x \in [1, n]$, $\sigma \circ \sigma'(x) = \sigma(\sigma'(x))$. On a alors : $(\mathcal{S}_n, \circ)$ est un groupe.

▪ ***Notation.*** Soient n un entier supérieur ou égal à 2 et $\sigma \in \mathcal{S}_n$. On note : $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

▪ ***Cycle.*** Soient n un entier supérieur ou égal à 2, $\sigma \in \mathcal{S}_n$ et $p \in [2, n]$. On dit que σ est un cycle de longueur p s'il existe une p-liste $(x_k)_{1 \le k \le p}$ $(p \in \mathbb{N}^*)$ d'éléments distincts de $[1, n]$ telle que pour tout entier k appartenant à $[1, p-1]$, $\sigma(x_k) = x_{k+1}$, telle que $\sigma(x_p) = x_1$ et telle que pour tout élément x de $[1, n] \setminus \{x_1, x_2, \dots, x_p\}$, $\sigma(x) = x$.

On note alors : $\sigma = (x_1, x_2, \dots, x_p)$.

▪ ***Transposition.*** Soient n un entier supérieur ou égal à 2 et $\sigma \in \mathcal{S}_n$. On dit que σ est une transposition si σ est un cycle de longueur 2.

2. Décomposition d'une permutation en produit de transpositions

▪ On appelle produit de permutations, la composée de deux permutations.

▪ Soit n un entier supérieur ou égal à 2. Tout élément de $\mathcal{S}_n$ peut se décomposer en un produit de transpositions.

3. Signature

Soient n un entier supérieur ou égal à 2 et $\sigma \in \mathcal{S}_n$.

▪ ***Inversion.*** Soient i et j deux éléments distincts de $[1, n]$. On dit que la paire $\{i, j\}$ est une inversion de σ si : $(\sigma(i) - \sigma(j)).(i - j) < 0$. On note $\mathrm{Inv}(\sigma)$ le nombre d'inversions de σ.

▪ ***Signature d'une permutation.*** On appelle signature de σ, et l'on note $\varepsilon(\sigma)$, le nombre égal à $(-1)^{\mathrm{Inv}(\sigma)}$. Si $\varepsilon(\sigma) = 1$, on dit que σ est une permutation paire, et si $\varepsilon(\sigma) = -1$, on dit que σ est une permutation impaire.

▪ ***Signature d'une transposition.*** Si σ est une transposition, alors sa signature vaut - 1.

▪ $(\{-1, 1\}, \times)$ est un groupe.

▪ L'application f définie sur $\mathcal{S}_n$ par : $\sigma \mapsto \varepsilon(\sigma)$ est un morphisme (surjectif) de groupes de $(\mathcal{S}_n, \circ)$ dans le groupe multiplicatif $(\{-1, 1\}, \times)$.

▪ ***Sous-groupe alterné*** $\mathcal{A}_n$. On appelle sous-groupe alterné d'indice n, et l'on note $\mathcal{A}_n$, l'ensemble des éléments de $\mathcal{S}_n$ dont la signature est égale à 1.

VI. Programme officiel

Hors programme :

- Si σ est un cycle de longueur p, alors σ^k est un cycle si, et seulement si, p et k sont premiers entre eux.
- Deux cycles de supports disjoints commutent.
- Card $(\mathfrak{A}_n) = \frac{1}{2}\, n!$
- Notion générale de groupe-quotient, d'anneau-quotient.
- Anneau principal.
- Anneau unifère.
- Anneau non unitaire.
- Anneau monogène.
- Idéal à gauche, à droite, idéal bilatère d'un anneau non commutatif.

A la limite du programme :

- Support d'un cycle.
- Morphisme de corps.

NB : Les espaces vectoriels et les algèbres (autres structures algébriques classiques) sont traités à part dans le chapitre "Espaces vectoriels".