Ag1 : Groupes, Anneaux, Corps

I Groupes

Pour parler d'espaces vectoriels, on a besoin de la structure de corps. On rencontre en algèbre linéaire beaucoup de groupes et d'anneaux. Il faut donc revoir les définitions de ces structures algébriques.

I.1 Structure de groupe

Définition : Un groupe est un ensemble G muni d'une loi interne $*$ ayant les propriétés suivantes :

(i) $*$ est associative : $a*(b*c) = (a*b)*c$ pour tous a, b, c dans G

(ii) $*$ admet un élément neutre (qui est unique) : il existe $e \in G$ tel que, pour tout $a \in G$

$$e * a = a * e = a$$

(iii) Tout élément a de G admet un inverse (parfois appelé symétrique), c'est-à-dire qu'il existe $b \in G$ tel que

$$a * b = b * a = e$$

Rappel : Une loi de composition interne est une application $*$ de G^2 dans G. L'image de (a, b) est notée $a * b$ (plutôt que $*(a, b)$, comme on le ferait classiquement pour une application).
L'associativité rend facultatif l'usage des parenthèses ; on peut noter $a * b * c$ sans ambiguité. Il est très compliqué de travailler avec des lois internes non

associatives, nous n'en rencontrerons d'ailleurs pas (exemple de loi non associative : le produit vectoriel, qui n'est plus au programme de mathématiques).
Le « symétrique » ou « inverse » est appelé « opposé » dans le cas où la loi est notée additivement $(+)$, « réciproque » dans le cas de la loi de composition $(\circ)$ sur un groupe de bijections. Il est donc, suivant les cas, noté a^{-1} ou $-a$. Le passage des notations « multiplicatives » aux notations « additives » est d'ailleurs un problème quand on passe des résultats généraux sur les groupes à leur transcription dans le cas d'une loi $+$.
Lorsque la loi est commutative, le groupe est dit commutatif ou abélien.
On ne doit pas oublier, lorsque la loi n'est pas commutative, de vérifier que le symétrique d'un élément a « marche » des deux côtés : la propriété $a * b = e$ n'implique pas en général $b * a = e$.
...mais pendant l'année, l'inversibilité dont on se préoccupera le plus souvent est celle des matrices et des endomorphismes. Or, bizarrement et heureusement, et bien que la multiplication des matrices ne soit pas du tout commutative, on a, dans $\mathscr{M}_n(\mathbf{K})$,

$$AB = I_n \Longleftrightarrow BA = I_n$$

et dans $\mathscr{L}(E)$*, si* E *est un espace vectoriel de dimension finie,*

$$u \circ v = Id_E \Longleftrightarrow v \circ u = Id_E$$

Proposition Soit A un ensemble muni d'une loi interne $*$. On suppose l'existence d'un élément neutre e (et donc son unicité...) ; si a et b sont des éléments de A inversibles pour $*$, alors $a * b$ l'est, et

$$(a * b)^{-1} =$$

I.2 Quelques groupes

On rencontre souvent la structure de groupe. Quelques exemples :

$(\mathbf{Z},+)$, $\big(\mathscr{M}_n(\mathbf{K}),+\big)$...plus généralement $(A,+)$ où $(A,+,*)$ est un anneau.

$(\mathbf{R},+)$, $(\mathbf{C},+)$, $(\mathbf{Q},+)$,...plus généralement $(\mathbf{K},+)$, où $(\mathbf{K},+,\times)$ est un corps.

$(\mathbf{R}_*,\times)$, $(\mathbf{C}_*,\times)$, $(\mathbf{Q}_*,\times)$, ...plus généralement $(\mathbf{K}_*,\times)$, où $(\mathbf{K},+,\times)$ est un corps.

$(\mathbf{R}_*^+,\times)$, $(\mathbf{Q}_*^+,\times)$.

$(\mathbf{U},\times)$ où $\mathbf{U}$ est l'ensemble des nombres complexes de module 1.

On en verra bien d'autres, dont certains non commutatifs (ceux qui sont énumérés ci-dessus sont tous commutatifs). A part éventuellement pour $\mathbf{U}$, on ne vous demandera jamais de montrer que les groupes précédents sont bien des groupes. Attention néanmoins à ne pas inventer de faux groupes : $(\mathbf{N},+)$, $(\mathbf{Z}_*,\times)$, $(\mathbf{R},\times)$...par exemple, ne sont pas des groupes.

I.3 Groupe produit

Si $(G,*)$ et $(H,\square)$ sont deux groupes, si on définit

$$(g,h)\spadesuit(g',h') = (g*g', h\square h')$$

alors $(G\times H,\spadesuit)$ est un groupe, appelé produit de $(G,*)$ et $(H,\square)$.
Plus généralement, si on a défini des structures de groupes sur $G_1,\dots,G_p$, on définit une structure de groupe produit sur $G_1\times\cdots\times G_p$, de la même manière que pour $p=2$.

I.4 Sous-groupes

Définition : On dit que H est un sous-groupe de $(G,*)$ quand H est une partie de G stable par $*$ et telle que $(H,*)$ est un groupe.

On n'utilise à peu près jamais la définition, car on dispose des caractérisations équivalentes suivantes :

Caractérisation 1 : H est un sous-groupe de $(G,*)$ si et seulement si

$$H \subset G \quad , H \neq \emptyset \quad , \text{ et } \quad \left[(h,h') \in H^2\right] \Longrightarrow \left[h' * h^{-1} \in H\right]$$

Caractérisation 2 : H est un sous-groupe de $(G,*)$ si et seulement si H est une partie non vide de G telle que

$$H \subset G \quad , H \neq \emptyset \quad , \text{ et } \quad \left[(h,h') \in H^2\right] \Longrightarrow \left[(h * h', h^{-1}) \in H^2\right]$$

Exemple - Exercice : le centre Si $(G,*)$ est un groupe, on définit son centre comme l'ensemble des éléments de G qui commutent avec tous les éléments de G :

$$C = \{g \in G \,;\, \forall h \in G \quad g * h = h * g\}$$

Montrer que C est un sous-groupe de $(G,*)$.

Exercice On considère H_1 et H_2 deux sous-groupes d'un groupe $(G,*)$. Trouver une condition nécessaire et suffisante simple pour que $H_1 \cup H_2$ soit un sous-groupe de $(G,*)$.

Exercice *Classiquement posé à l'oral de divers concours*

Soit $(G,*)$ un groupe, dont H et K sont deux sous-groupes. On définit

$$H * K = \{h * k \,;\, (h,k) \in H \times K\}$$

Montrer que $H * K$ est un sous-groupe de $(G,*)$ si et seulement si $H * K = K * H$.

$\diamondsuit$ Il y a toujours au moins 2 sous-groupes du groupe $(G,\star)$: $\{e\}$ et G.
$\diamondsuit$ Pour montrer qu'un ensemble muni d'une loi est un groupe, on le fait très souvent apparaître (lorsque c'est possible) comme sous-groupe d'un groupe connu.
$\diamondsuit$ On utilise plus souvent la caractérisation 2 que la caractérisation 1.

I.5 Sous-groupe engendré

Proposition : Soit I un ensemble non vide; on suppose que, pour chaque $i \in I$, H_i est un sous-groupe de $(G,*)$. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de $(G,*)$.

On dit tout simplement : « une intersection de sous-groupes est un sous-groupe ».

Corollaire : Soit $(G,*)$ un groupe. Soit A une partie quelconque de G. Il y a un plus petit sous-groupe H de $(G,*)$ qui contient A. On l'appelle sous-groupe de $(G,*)$ engendré par A.

Caractérisation : H est le sous-groupe de $(G,*)$ engendré par A si et seulement si

(i) H est un sous-groupe de $(G,*)$.

(ii) $A \subset H$

(iii) Pour tout sous-groupe K de $(G,*)$, $A \subset K \implies H \subset K$.

Définition La partie A de $(G,*)$ est dite génératrice de G lorsque le sous-groupe de $(G,*)$ engendré par A est G.

I.6 Morphismes

Définition : On appelle morphisme du groupe $(G,*)$ dans le groupe $(H,.)$ toute application ϕ de G dans H telle que

$$\forall (g,g') \in G^2 \qquad \phi(g*g') = \phi(g).\phi(g')$$

Premiers exemples, morphismes célèbres :

1. un morphisme du groupe $(\mathbf{R},+)$ dans le groupe $(\mathbf{R}_*^+,\times)$:
2. un morphisme du groupe $(\mathbf{R}_*^+,\times)$ dans le groupe $(\mathbf{R},+)$:
3. Un morphisme du groupe $(\mathbf{GL}_n(\mathbf{K}),\times)$ dans le groupe $(\mathbf{K}_*,\times)$ (rappel : $\mathbf{GL}_n(\mathbf{K})$ est le groupe des matrices inversibles à coefficients dans $\mathbf{K}$) :
4. Un morphisme du groupe $(\mathbf{R},+)$ dans le groupe $(\mathbf{U},\times)$:

Proposition (image de l'élément neutre) : Si ϕ est un morphisme de $(G,*)$ dans $(H,.)$, alors, avec des notations évidentes,

$$\phi(e_G) = e_H$$

Proposition (image de l'inverse) : Si ϕ est un morphisme de $(G,*)$ dans $(H,.)$, alors, avec des notations évidentes,

$$\forall a \in G \qquad \phi(a^{-1}) = \big(\phi(a)\big)^{-1}$$

Proposition (image d'un sous-groupe) : L'image par un morphisme d'un sous-groupe de $(G,*)$ est un sous-groupe de $(H,.)$.

Proposition (image réciproque d'un sous-groupe) : L'image réciproque par un morphisme d'un sous-groupe de $(H,.)$ est un sous-groupe de $(G,*)$.

$\diamondsuit$ Ces deux propositions donnent deux méthodes utiles (car rapides et élégantes) pour démontrer qu'un ensemble est un sous-groupe. Par exemple, l'ensemble des matrices de $\mathscr{M}_n(\mathbf{K})$ dont le déterminant vaut ± 1 est un groupe multiplicatif.

I.7 Noyau, image d'un morphisme

Définition : Soit ϕ un morphisme de $(G,*)$ dans $(H,.)$. L'ensemble

$$\ker\phi = \{g \in G \ / \ \phi(g) = e_H\}$$

est un sous-groupe de $(G,*)$ (c'est $\phi^{-1}(\{e_H\})$, appelé noyau de ϕ.

Proposition (caractérisation de l'injectivité d'un morphisme) : Un morphisme est injectif si et seulement si son noyau est réduit à $\{e_G\}$

Remarque de rédaction : on vérifie facilement (cela a déjà été dit) que si ϕ est un morphisme de groupes, $\phi(e_G) = e_H$. Le noyau $\ker\phi$ contient donc toujours e_G.
Pour démontrer que ϕ est injectif (après avoir vérifié que ϕ était bien un morphisme) on cherche donc à montrer : $\phi(x) = e_H \Rightarrow x = e_G$.
L'implication réciproque, toujours vraie, n'a pas à être montrée.

Définition : De même, $\mathrm{Im}\,\phi = \{\phi(g)\ ,\ g \in G\}$ est un sous-groupe de $(H,.)$, appelé image de ϕ (c'est $\phi(G)$). Le morphisme est surjectif si et seulement si son image est H.

$\diamondsuit$ Pour montrer qu'un morphisme est surjectif, pas de méthode extraordinaire : on prend $y \in H$ quelconque, on cherche à montrer l'existence de x dans G tel que $\phi(x) = y$.

$\diamondsuit$ Encore deux méthodes utiles pour démontrer qu'un ensemble est un sous-groupe : le faire apparaître comme image ou noyau d'un morphisme de groupes. Elles ne sont pas d'égale importance : on s'occupe plus souvent de noyaux que d'images.
Par exemple,

$$SL_n(\mathbf{K}) = \{M \in M_n(\mathbf{K}) \ ; \ \det(M) = 1\}$$

est un groupe multiplicatif.
Exercice : Montrer que

$$\mathbf{U}_n = \{z \in \mathbf{C} \ ; \ z^n = 1\}$$

est, pour tout entier naturel non nul n, un groupe multiplicatif.
Exercice : Soit $(G, *)$ un groupe. On note $\mathfrak{S}$ l'ensemble des bijections de G dans G (les éléments de $\mathfrak{S}$ sont aussi appelés permutations de G). On admet que $(\mathfrak{s}, \circ)$ est un groupe. Pour tout g, on définit

$$\begin{array}{rccc} \phi_g : & G & \longrightarrow & G \\ & h & \longmapsto & g * h * g^{-1} \end{array}$$

1. Montrer que l'application $g \to \phi_g$ est un morphisme de $(G, *)$ dans $(\mathfrak{S}, \circ)$.
2. Caractériser les éléments du noyau du morphisme précédent. Retrouver le résultat d'un exercice sur les sous-groupes.

I.8 Isomorphismes

Un **isomorphisme** est un morphisme bijectif. Alors sa réciproque est aussi un morphisme.
Lorsqu'il existe un isomorphisme de $(G, *)$ dans $(H, .)$, les deux groupes sont dits **isomorphes**. Etudier G ou étudier H, c'est alors étudier la même structure.
Par exemple, $(\mathbf{R}, +)$ et $(\mathbf{R}_*^+, \times)$ sont isomorphes.
Exercice Si $(G, *)$ est un groupe, si $g \in G$, montrer que

$$\phi_g \ : \ h \longmapsto g * h * g^{-1}$$

est un isomorphisme de $(G, *)$ sur lui-même (i.e. un « automorphisme » de $(G, *)$).
Une remarque de méthode : On pense trop souvent que montrer qu'une application est bijective, c'est montrer qu'elle est injective et surjective. Bien évidemment, ce n'est pas une mauvaise idée. Mais il est très fréquent que pour

montrer qu'une application $f : X \to Y$ est bijective la méthode la plus rapide soit d'exhiber une application $g : Y \to X$ telle que $f \circ g = \mathrm{Id}_X$ et $g \circ f = \mathrm{Id}_Y$.

I.9 Puissances d'un élément d'un groupe

a Définition

Soit $(G, *)$ un groupe, dont on note e l'élément neutre. Soit a un élément de G; on définit, pour tout entier naturel n, a^n par récurrence :

$$a^0 = e_G \quad \text{, et} \quad \forall n \in \mathbf{N} \quad a^{n+1} = a * a^n$$

puis, si z est un entier négatif :

$$a^z = (a^{-z})^{-1}$$

Autrement dit, si n est un naturel non nul,

$$a^n = \underbrace{a * a * \cdots * a}_{n \text{ facteurs}}$$

et

$$a^{-n} = (\underbrace{a * a * \cdots * a}_{n \text{ facteurs}})^{-1} = \underbrace{a^{-1} * a^{-1} * \cdots * a^{-1}}_{n \text{ facteurs}}$$

Dans le cas où la loi est notée $+$, on écrit na au lieu de a^n : si n est un naturel non nul,

$$na = \underbrace{a + a + \cdots + a}_{n \text{ facteurs}}$$

et

$$-na = -(\underbrace{a + a + \cdots + a}_{n \text{ facteurs}}) = \underbrace{-a + (-a) + \cdots + (-a)}_{n \text{ facteurs}}$$

et, bien sûr, on se permet de noter $a - b$ pour $a + (-b)$.

Remarque : Ainsi, si x est un réel, $3x$ peut être vu comme le produit des deux nombres réels 3 et x, mais aussi comme une addition de trois termes égaux à x.

b Image d'une puissance par un morphisme

Si ϕ est un morphisme de $(G, *)$ dans $(H, .)$, alors

$$\forall a \in G \quad \forall n \in \mathbf{Z} \qquad \phi(a^n) = \big(\phi(a)\big)^n$$

c Sous-groupe engendré par un élément

Soit a un élément du groupe $(G, *)$. L'application

$$\phi_a \,:\, z \longmapsto a^z$$

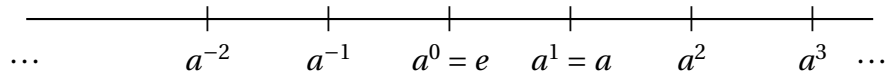
est un morphisme du groupe $(\mathbf{Z}, +)$ dans le groupe $(G, *)$. On a

$$\mathrm{Im}(\phi_a) = \{a^z \,;\, z \in \mathbf{Z}\}$$

On sait que $\mathrm{Im}(\phi_a)$ est un sous-groupe de $(G, *)$. C'est le plus petit sous-groupe contenant a : si un sous-groupe H de $(G, *)$ contient a, il contient $\mathrm{Im}(\phi_a)$.
(démonstration facile : si H contient a, comme il est stable par * il contient a^n pour tout $n \in \mathbf{N}$ par récurrence, puis comme il est stable par passage à l'inverse il contient a^{-n} pour tout $n \in \mathbf{N}$).
On dit que $\mathrm{Im}(\phi_a)$ est le sous-groupe de $(G, *)$ engendré par a. Autrement dit, le sous-groupe de $(G, *)$ engendré par a est l'ensemble des puissances (entières) de a.

Proposition Deux situations bien différentes peuvent se présenter :

1. **Premier cas** Si ϕ_a est injectif, le sous-groupe engendré par a est isomorphe à $\mathbf{Z}$:

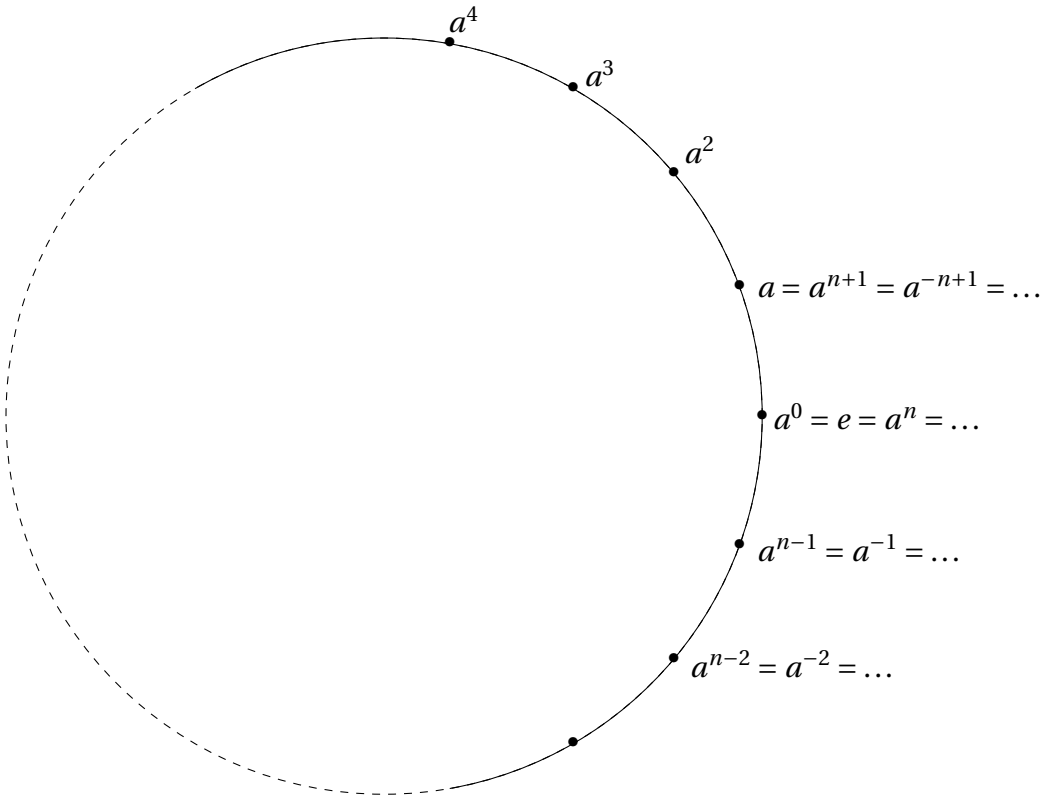


   Les a^k, $k \in \mathbf{Z}$, sont deux à deux distincts.

2. **Deuxième cas** Si ϕ_a n'est pas injectif, le sous-groupe engendré par a est fini : il existe $n \geq 1$ unique tel que

$$\mathrm{Im}(\phi_a) = \{a^k \,;\, 0 \leq k \leq n-1\} = \{e, a, a^2, \ldots, a^{n-1}\}$$

   n est le plus petit entier naturel non nul tel que $a^n = e$. Le sous-groupe engendré par a est de cardinal n. On dit que a est d'ordre n.



Ici, l'égalité entre puissances de a se traduit facilement par des congruences :

$$a^k = a^\ell \iff$$

On dit dans ce deuxième cas que a est d'ordre fini.

Démonstration On s'intéresse au noyau de $\mathrm{Ker}(\phi_a)$ qui est, lui, un sous-groupe de $(\mathbf{Z}, +)$. On utilise alors le

Lemme : Si H est un sous-groupe de $(\mathbf{Z}, +)$, il existe un unique $n \in \mathbf{N}$ tel que $H = n\mathbf{Z}$.

[**démonstration** dans le chapitre d'arithmétique. Ou ici :

si $H = \{0\}$, on a évidemment un unique n convenable : $n = 0$.

Sinon, $H \cap \mathbf{N}_*$ a un plus petit élément. En effet, si s est un élément non nul de H, s ou $-s$ est dans $H \cap \mathbf{N}_*$. Donc $H \cap \mathbf{N}_* \neq \emptyset$. Et une partie non vide de $\mathbf{N}$ a un plus petit élément.

On appelle n le plus petit élément de $H \cap \mathbf{N}_*$. Comme H est un groupe, on a $n\mathbf{Z} \subset H$ (démonstration « facile » vue plus haut).

On montre l'inclusion réciproque à l'aide de la division euclidienne : soit $m \in H$. Il existe un (unique) couple (q,r) d'entiers tels que

$$m = nq + r \qquad , 0 \leq r < n$$

Comme H est un groupe pour + qui contient $n\mathbf{Z}$,

$$r = \underbrace{m}_{\in H} - \underbrace{nq}_{\in H} \in H$$

Et r ne peut pas être dans $H \cap \mathbf{N}_*$ (car $r < n$), donc nécessairement $r = 0$. Donc $m \in n\mathbf{Z}$. Et on a bien montré $H = n\mathbf{Z}$. L'unicité de n ne pose pas de problème, car si $n_1\mathbf{Z} = n_2\mathbf{Z}$ n_1 et n_2 se divisent mutuellement, ils sont donc égaux ou opposés, si on les impose positifs ils sont nécessairement égaux.]

Utilisons ce lemme : il existe donc un unique entier naturel n tel que

$$\mathrm{Ker}(\phi_a) = n\mathbf{Z}$$

Si $n = 0$, ϕ_a est injective, on est dans le premier cas.

Si $n > 1$, on a

$$a^k = e \iff k \in n\mathbf{Z} \iff n|k$$

Et donc

$$a^k = a^\ell \iff a^{k-\ell} = e \iff n|k-\ell$$

On en déduit sans mal qu'on est dans le deuxième cas.

Proposition Si G est fini, tous les éléments de G sont d'ordre fini. Et l'ordre de chaque élément divise l'ordre du groupe.

Démonstration Soit $g_0 \in G$. Si g_0 n'était pas d'ordre fini, G contiendrait $\mathrm{Im}(\phi_{g_0})$, mais cette image est isomorphe à $\mathbf{Z}$ donc infinie, contradiction. Maintenant, il s'agit de montrer que l'ordre de g_0 divise $|G|$. La preuve générale sera vue plus tard. Le cas où $(G,*)$ est commutatif est intéressant, utile à comprendre. On dit que

$$\psi \ : \ h \mapsto g_0 * h$$

est une bijection de G sur lui-même. On écrit alors

$$\prod_{h\in G} h = \prod_{h\in G} \psi(h)$$

et le résultat s'en déduit après un petit peu d'écriture et de réflexion.

Remarque Quand un groupe est fini, tous les éléments du groupe sont donc d'ordre fini. Dans un groupe infini, il y a au moins un élément d'ordre fini : l'élément neutre. Ce peut être le seul (exemple : $(\mathbf{Z},+)$, $(\mathbf{R},+)$, $(\mathbf{R}_*^+,\times)\ldots$) ou non…

Exercice Caractériser dans $(\mathbf{U},\times)$ les éléments $e^{i\theta}$ qui sont d'ordre fini.

Exercice Démontrer que la matrice

$$\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

est d'ordre fini dans $GL_2(\mathbf{R})$ (peut se faire à peu près sans calcul).

Exercice Voici la liste des éléments de $\mathfrak{S}_3$. Indiquer pour chaque élément son ordre.

$$\{\mathrm{Id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

Exercice Dans $\mathfrak{S}_{10}$, déterminer l'ordre de $(1\ 4\ 3\ 7\ 8)(2\ 5\ 7)$.

Exercice Soit g un élément d'ordre fini n dans un groupe $(G,*)$. Soit d un diviseur de n. Déterminer un élément d'ordre d dans $(G,*)$.

Exercice Soit $(G,*)$ commutatif. On suppose que g_1 et g_2 sont deux éléments de $(G,*)$ d'ordres respectifs n_1 et n_2. On suppose $n_1 \wedge n_2 = 1$. Montrer que $g_1 * g_2$ est d'ordre fini, et calculer cet ordre.

II Anneaux, corps

II.1 Structures

a Anneau

Définition Un anneau $(A,+,\times)$ est un ensemble muni de deux lois internes $+$ et $\times$ vérifiant :

- $(A,+)$ est un groupe commutatif,
- $\times$ est une loi associative
- Il y a dans A un élément neutre pour $\times$, souvent noté 1_A (à ne pas oublier),
- $\times$ est distributive sur $+$:

$$a\times(b+c)=a\times b+a\times c,$$
$$(a+b)\times c=a\times c+b\times c.$$

La loi de groupe commutatif est à peu près toujours notée $+$, la deuxième loi n'est pas toujours notée $\times$: il arrive assez souvent par exemple que ce soit une loi de composition d'applications $(\circ)$ comme dans l'anneau $(\mathscr{L}(E),+,\circ)$.
Lorsque $\times$ est commutative, on parle d'anneau commutatif (mais pas d'anneau abélien).

b Anneaux célèbres

$(\mathbf{Z},+,\times)$, $(\mathbf{K}[X],+,\times)$, $(\mathscr{M}_n(\mathbf{K}),+,\times)$, $(\mathscr{L}(E),+,\circ)$, $(\mathbf{Z}/m\mathbf{Z},+,\times)$ (pour ce dernier, voir chapitre d'arithmétique).

c Eléments inversibles

Proposition : Soit $(A,+,\times)$ un anneau, commutatif ou non. L'ensemble A^* des éléments de A inversibles (pour $\times$, bien sûr), muni de $\times$, est un groupe.

On peut par exemple appliquer ce résultat à $\mathbf{Z}$:
et à $\mathscr{M}_n(\mathbf{K})$:

d Corps

Un corps est un anneau commutatif $\mathbf{K}$ ($\times$ est commutative) non réduit à $\{0_\mathbf{K}\}$, tel que $\mathbf{K}^* = \mathbf{K}\backslash\{\mathbf{0_K}\}$.
Dans le cadre du programme, un corps est donc nécessairement commutatif. Parler de « corps commutatif » est donc redondant.

e Corps célèbres

$(\mathbf{Q},+,\times)$, $(\mathbf{R},+,\times)$, $(\mathbf{C},+,\times)$,, $(\mathbf{K}(X),+,\times)$, $(\mathbf{Z}/p\mathbf{Z},+,\times)$ (p premier) (voir chapitre d'Arithmétique)…

f Anneau intègre

Un anneau intègre est un anneau commutatif non réduit à $\{0_A\}$ et « sans diviseurs de 0_A » :

$$\Big(a\times b = 0_A\Big) \Longleftrightarrow \Big(a = 0_A \text{ ou } b = 0_A\Big)$$

L'intégrité d'un anneau permet de construire son « corps des fractions » : $\mathbf{K}(X)$ à partir de $\mathbf{K}[X]$, $\mathbf{Q}$ à partir de $\mathbf{Z}$…

II.2 Sous-structures

Définition Un **sous-anneau** de l'anneau $(A,+,\times)$ est une partie B de A qui est un sous-groupe de $(A,+)$, stable par $\times$ **et contenant** 1_A.

Proposition Une partie B de A est un sous-anneau de $(A,+,\times)$ si et seulement si

(i) $1_A \in B$

(ii) $\forall (a,b)\in B^2 \quad a-b\in B$

(iii) $\forall (a,b)\in B^2 \quad a\times b\in B$

$\diamondsuit$ *Ne pas oublier* **(i)** *: le singleton* $\{0_A\}$ *n'est pas considéré comme un sous-anneau.*
Ne pas non plus remplacer **(ii)** *par*

$$\forall (a,b)\in B^2 \quad a+b\in B$$

(on montrerait pas exemple que $\mathbf{N}$ *est un sous-anneau de* $(\mathbf{Z},+,\times)$*, ce qui est faux).*

Définition Un **sous-corps** de $\mathbf{K}$ est une partie B de $\mathbf{K}$ qui est un sous-anneau de $\mathbf{K}$ et qui contient l'inverse de chacun de ses éléments non nuls : on ajoute donc aux conditions de sous-anneau la condition

$$\forall x \in \mathbf{K} \setminus \{0_{\mathbf{K}}\} \qquad 1/x \in \mathbf{K}$$

II.3 Calcul dans un anneau

Dans un anneau A, avec des notations évidentes :
$a \times 0_A = 0_A \times a = 0_A$.

$(-1_A) \times a = a \times (-1_A) = -a$.

$(-a) \times b = a \times (-b) = -(a \times b)$.

$$a \times \sum_{i=1}^{p} b_i = \sum_{i=1}^{p} (a \times b_i).$$

$$\left(\sum_{i=1}^{p} b_i \right) \times a = \sum_{i=1}^{p} (b_i \times a)$$

et, si a et b commutent ($a \times b = b \times a$) :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} (a^k \times b^{n-k})$$

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2} \times b + \cdots + b^{n-1}) = (a-b) \times \sum_{k=0}^{n-1} (a^k \times b^{n-1-k})$$

La première est la formule du binôme (de Newton), la seconde n'a pas de dénomination spécifique mais sert beaucoup, le plus souvent sous la forme

$$(1_A - a) \left(\sum_{k=0}^{n} a^k \right) = 1_A - a^{n+1}$$

Table des matières

I Groupes **1**

I.1 Structure de groupe 1
I.2 Quelques groupes 3
I.3 Groupe produit 3
I.4 Sous-groupes 3
I.5 Sous-groupe engendré 5
I.6 Morphismes 5
I.7 Noyau, image d'un morphisme 6
I.8 Isomorphismes 7
I.9 Puissances d'un élément d'un groupe 8
a Définition 8
b Image d'une puissance par un morphisme 8
c Sous-groupe engendré par un élément 9

II Anneaux, corps **13**

II.1 Structures 13
a Anneau 13
b Anneaux célèbres 13
c Eléments inversibles 13
d Corps 14
e Corps célèbres 14
f Anneau intègre 14
II.2 Sous-structures 14
II.3 Calcul dans un anneau 15