Chapitre 1

Structures algébriques et relations binaires

1.1 Exposés préliminaires

Ce chapitre est un **récapitulatif** de notions introduites dans la foulée des définitions de première année (lois de composition, structures, polynômes), de ce fait les démonstrations les plus immédiates sont souvent omises.

1.1.1 Utilisations des structures algébriques

• Assurer des calculs valides
L'étude d'une structure algébrique sur un ensemble muni d'une opération, sert d'abord à assurer les **méthodes de calculs utilisables** pour chercher des éléments vérifiant des conditions (**équations)** imposées dans cet ensemble. Selon la variété des objets dont on dispose et les opérations définies sur ces objets, l'existence et le nombre de solutions d'une équation diffèrent.
Exemples : chercher (x, y) tel que $(E) : 51x + 44y = 1$ est un problème différent pour x et y entiers, qui suppose un travail sur les nombres premiers et les multiples dans $(\mathbb{Z}, +, \times)$ du cas où x et y sont réels, le point (x, y) parcourant alors une droite.
Résoudre l'équation $x^2 = 1$ (recherche des racines carrées de l'unité) dans $(\mathbb{R}, +, \times)$ ou $A^2 = I_2$ dans l'ensemble $(\mathcal{M}_2(\mathbb{R}), +, \times)$ des matrices carrées 2×2, demande qu'on réalise que la factorisation en $(x - 1)(x + 1) = 0$ ou en $(A - I_2)(A + I_2) = O_2$ est possible.
Dans le premier cas, l'anneau est intègre et on peut conclure que $x = 1$ ou $x = -1$. Dans le second, l'anneau n'est pas intègre, il y a d'autres solutions que $A = I_2$ et $A = -I_2$. Dont les matrices $S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$ où $\theta \in \mathbb{R}$ ou $T_c = \begin{pmatrix} 1 & c \\ 0 & -1 \end{pmatrix}$ avec $c \in \mathbb{R}$.
• Décomposer des objets compliqués
Des objets « volumineux » dans un ensemble muni d'une ou plusieurs opérations, peuvent se décomposer en des **combinaisons d'objets plus simples**.
Les entiers se décomposent en produits de nombres premiers, les polynômes en produits de polynômes irréductibles, les permutations en composées de cycles disjoints, $\mathbb{Z}/n\mathbb{Z}$ est monogène (engendré par un seul de ses éléments), les espaces vectoriels admettent des bases, etc. Dans ces questions de **composition-décomposition** nous pouvons faire un parallèle avec la chimie : le comportement des composés est fonction du comportement

de leur **générateurs**, comme celui d'une molécule est fonction des propriétés des atomes dont elle est constituée.
• **Reconnaître** une structure déjà rencontrée.
Il est utile d'avoir quelques **prototypes**, des structures de références qu'on a bien étudiées, et que la notion d'**isomorphisme** permet de réutiliser dans d'autres situations.
• Il y a de **nombreuses applications** directes et concrètes, mais méconnues, de l'algèbre.
Les groupes interviennent de façon centrale en géométrie, pour décrire les possibilités offertes par un engrenage ou une rotule en mécanique (exemple du groupe du cube ou de la pyramide), en chimie où les groupes de symétries d'une molécule expliquent une partie de ses propriétés, en cristallographie, les anneaux et corps interviennent dans l'étude des codes et du chiffrement des messages, etc...

1.1.2 Relations binaires, loi de composition

Relations binaires

Définition

Soit E un ensemble.
On appelle **relation binaire** $\mathcal{R}$ sur E tout sous-ensemble de $E \times E$.

On note usuellement $x \mathcal{R} y$ pour $(x, y) \in \mathcal{R}$.
La relation est dite :

- **réflexive** si et seulement si $\quad \forall x \in E,\ x \mathcal{R} x$,
- **symétrique** si et seulement si $\quad \forall (x, y) \in E^2,\ (x \mathcal{R} y) \Longrightarrow (y \mathcal{R} x)$,
- **antisymétrique** si et seulement si $\forall (x, y) \in E^2,\ (x \mathcal{R} y$ et $y \mathcal{R} x) \Longrightarrow (x = y)$,
- **transitive** si et seulement si $\quad \forall (x, y, z) \in E^3,\ (x \mathcal{R} y$ et $y \mathcal{R} z) \Longrightarrow (x \mathcal{R} z)$.

Définition

Une relation binaire $\mathcal{R}$ réflexive, symétrique et transitive sur E est dite **relation d'équivalence** sur E.

Si $\mathcal{R}$ est une relation d'équivalence sur E, pour $x \in E$, on appelle **classe d'équivalence** de x modulo $\mathcal{R}$ le sous-ensemble de E : $\quad \overline{x} = \{y \in E,\ x \mathcal{R} y\}$.
Puisque $\mathcal{R}$ est réflexive : $\forall x \in E,\ (x \mathcal{R} x)$ donc $(x \in \overline{x})$, ainsi $\overline{x}$ n'est jamais vide.
Puisque $\mathcal{R}$ est symétrique : $\forall (x, y) \in E^2,\ (x \mathcal{R} y) \Longleftrightarrow (y \mathcal{R} x)$ donc $(y \in \overline{x}) \Longleftrightarrow (x \in \overline{y})$.
Puisque $\mathcal{R}$ est transitive : $\forall (x, y, z) \in E^3,\ (x \mathcal{R} y$ et $z \in \overline{y}) \Longrightarrow (z \in \overline{x})$
donc $(y \in \overline{x}) \Longrightarrow (\overline{y} \subset \overline{x})$. Mais par symétrie, on a aussi l'inclusion réciproque.
Ainsi $(x \mathcal{R} y) \Leftrightarrow (\overline{x} = \overline{y})$, deux classes d'équivalence sont confondues ou disjointes.
On appelle **représentant** d'une classe $\overline{x}$, tout élément y de $\overline{x}$ (en effet alors $\overline{x} = \overline{y}$).

Théorème

Les classes d'équivalence selon $\mathcal{R}$ constitue une partition de E.
L'ensemble des classes d'équivalence modulo $\mathcal{R}$ dans E est appellé **ensemble quotient** de E par $\mathcal{R}$.

L'ensemble quotient est un sous-ensemble de $\mathcal{P}(E)$ constitué de parties non vides, deux à deux disjointes et dont la réunion est égale à E.

La congruence modulo n : pour $n \in \mathbb{N}$, dans $E = \mathbb{Z}$,
on définit $\big(x \mathcal{R} y\big) \Longleftrightarrow \big(y - x$ est un multiple de $n\big) \Longleftrightarrow \big(y - x \in n\mathbb{Z}\big)$.

C'est une relation d'équivalence. Pour $n = 0$ la classe de x ne contient que x : $\overline{x} = \{x\}$.

Pour $n = 1$, tous les éléments sont dans la même classe, $\overline{1} = \mathbb{Z}$.
Pour $n \geqslant 2$, l'ensemble quotient est usuellement noté $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, il a n élements dont on peut en faire la liste : $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\right\}$. Voir la suite page 34.

Définition

Une relation binaire $\mathcal{R}$ réflexive, antisymétrique et transitive sur E est dite **relation d'ordre** sur E. Le couple $(E, \mathcal{R})$ est un ensemble **ordonné**.

On appelle relation d'ordre **strict** associée à la relation d'ordre $\mathcal{R}$ la relation binaire :
$\forall (x, y) \in E^2$, $\big(x \prec y\big) \iff \big(x \,\mathcal{R}\, y \text{ et } x \neq y\big)$ qui n'est plus une relation d'ordre.
La relation d'ordre $\mathcal{R}$ est dite **totale**, et $(E, \mathcal{R})$ est dit totalement ordonné, si et seulement si deux éléments de E sont toujours comparables : $\forall\, (x, y) \in E^2$, $x \,\mathcal{R}\, y$ ou $y \,\mathcal{R}\, x$.

Définitions

Si $(E, \mathcal{R})$ est un ensemble ordonné, si A est une partie non vide de E et si $a \in E$:
- a est un **majorant** de A si et seulement si $\forall x \in A$, $x \,\mathcal{R}\, a$,
- a est un **plus grand élément** de A, si et seulement si $a \in A$ et a majore A,
- a **borne supérieure** de A, noté $a = \sup(A)$,
  si et seulement si a est plus petit élément de l'ensemble des majorants de A.

Notons aussi la notion **d'élément maximal**, noté $a = \max(A)$,
- a est un élément maximal de A si et seulement si
  $a \in A$ et $\forall x \in A$, $(a \,\mathcal{R}\, x) \Longrightarrow (x = a)$.

On a, par adaptations directes, les définitions de minorant, de plus petit élément, de borne inférieure et d'élément minimal.
Un plus grand élément est nécessairement unique, mais il peut y avoir plusieurs éléments maximaux. Si la relation d'ordre est totale, la notion d'élément maximal coïncide avec celle de plus grand élément, mais elles différent pour une relation d'ordre partielle (c'est à dire non totale), comme dans l'exemple suivant.

Dans $\mathbb{N}^*$, la divisibilité est une relation d'ordre.
Etude des majorants de $A = \{2, 3, 4, 5, 6, 7, 8, 9\}$ et $B = \{2, 4, 8, 16, 32\}$.

Notons que la divisibilité est une relation d'ordre partielle : deux éléments ne sont pas nécessairement comparables. Si $A = \{2, 3, 4, 5, 6, 7, 8, 9\}$ alors A n'a pas de plus grand élément, par exemple 2 n'est pas plus petit que 9 car il ne le divise pas. Mais 5, 6, 7, 8 et 9 sont des éléments maximaux. Par exemple si $x \in A$ et que 5 divise x alors $x = 5$.
Un majorant de A doit être un multiple de tous ses éléments donc de $5 \times 7 \times 8 \times 9 = 2520$ qui est ainsi $\sup(A)$ dans $\mathbb{N}^*$ (le plus petit des majorants). Les majorants de A sont les multiples de 2520.

Par contre $B = \{2, 4, 8, 16, 32\}$ a un plus grand élément qui est aussi $\sup(B)$: c'est 32. Les majorants de B sont alors les multiples de 32.

Lois de composition

Définition

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

On note usuellement $x * y$ l'image du couple (x, y) par cette application.

Une loi $*$ de composition interne sur E est dite :
- **commutative** si et seulement si $\forall\,(x,y)\in E^2$, $x*y=y*x$,
- **associative** si et seulement si $\forall\,(x,y,z)\in E^3$, $(x*y)*z=x*(y*z)$,
- $e\in E$ est **élément neutre** pour $*$ si et seulement si $\forall x\in E$, $x*e=e*x=x$.

Définitions

Un couple $(E,*)$ où $*$ est une loi de composition interne associative et possédant un élément neutre e, est un **monoïde**.
Dans un monoïde, si pour $x\in E$, il existe $y\in E$, tel que $x*y=y*x=e$ alors x est dit symétrisable et y est le **symétrique** de x pour $*$.

Si x et y sont symétrisables alors $x*y$ est symétrisable et $\boxed{(x*y)^{-1}=y^{-1}*x^{-1}}$

Si x est symétrisable, alors il est régulier ou **simplifiable**, c'est à dire que :
$(x*a=x*b)\Longrightarrow(a=b)$ et $(a*x=b*x)\Longrightarrow(a=b)$ en composant par x^{-1}.

Distributivité

Si E est muni de deux lois de composition internes, notées $*$ et $\bullet$, on dit que $\bullet$ est **distributive** par rapport à $*$, si et seulement si $\forall\,(x,y,z)\in E^3$, $(x*y)\bullet z=(x\bullet z)*(y\bullet z)$ et $z\bullet(x*y)=(z\bullet x)*(z\bullet y)$.

Finissons par la définition :

loi de composition externe

Pour E et F deux ensembles, on appelle **loi de composition externe** de F sur E toute application de $F\times E$ dans E.

1.1.3 Les entiers naturels et la récurrence

Plus petit, plus grand élément dans $\mathbb{N}$

L'ensemble des entiers naturels, noté $\mathbb{N}$, contient 0, tout élément n admet un successeur $s(n)$ (noté $n+1$) qui lui est distinct, et tout élément différent de 0 admet un prédecesseur $p(n)$ (noté $n-1$) tel que $\forall n\in\mathbb{N}$, $p(s(n))=n$ et $\forall n\in\mathbb{N}\setminus\{0\}$, $s(p(n))=n$.
$\mathbb{N}$ est alors muni d'une relation d'ordre et d'opérations : addition et multiplication.

Propriétés

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

Raisonnement par récurrence

Théorème de la récurrence

Soit $P(n)$ une proposition logique (vraie ou fausse) dépendant de l'entier n.
Initialisation : si $P(0)$ est vraie,
et **hérédité** : si , pour tout n de $\mathbb{N}$, $P(n)\Longrightarrow P(n+1)$
$\Big\}$ alors $P(n)$ est vraie pour tout n de $\mathbb{N}$.

Démonstration
Par l'absurde, en supposant $A=\{n\in\mathbb{N},\ P(n)\text{ fausse}\}$ non vide. Alors A admet un plus petit élément m et puisque $P(0)$ est vraie (initialisation), alors $m\geqslant 1$.

Ainsi $m-1 \in \mathbb{N}$ et $m-1 \notin A$. Donc $P(m-1)$ est vraie, ce qui entraine que $P(m)$ est vraie avec l'hérédité, d'où une contradiction. Ainsi $A = \emptyset$.
Remarques : il est clair que la propriété $P(n)$ peut être formulée par : $P(n) = Q(n_0+n)$ où $n_0 \in \mathbb{Z}$, où Q peut être vraie ou fausse. Alors l'initialisation se fait en n_0 pour Q.
De même $P(n)$ peut être la conjonction des propriétés ($Q(0)$ et $\ldots$ et $Q(n)$).

Pour $n \in \mathbb{N}^*$, on note $S_2(n)$ la somme $\displaystyle\sum_{k=1}^{n} k^2$.
Montrer que $\forall n \in \mathbb{N}^*$, la propriété $\mathcal{P}(n) : S_2(n) = \dfrac{n(n+1)(2n+1)}{6}$ est vraie.

Initialisation : $\mathcal{P}(1)$ est vraie car $S_2(1) = 1 = \dfrac{1\times 2\times 3}{6}$
Hérédité : si la propriété $\mathcal{P}(n)$ est vérifiée pour $n \in \mathbb{N}^*$ quelconque et fixé, on a :
$S_2(n+1) = S_2(n) + (n+1)^2 = \dfrac{n(n+1)(2n+1)}{6} + (n+1)^2$,
alors $S_2(n+1) = (n+1)\left[\dfrac{2n^2+7n+6}{6}\right] = \dfrac{(n+1)(n+2)\,(2(n+1)+1)}{6}$,
ce qui assure que $\mathcal{P}(n+1)$ est vraie.
Par le **théorème de récurrence**, la propriété est assurée pour tout $n \in \mathbb{N}^*$.

Attention à l'initialisation ! On confond souvent « Récurrence » et « Hérédité ».
Contrexemple : Etude de la propriété $\mathcal{P}(n) : 2^n \leqslant n!$

On peut assurer que $\forall n \geqslant 1 : \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$:
car si $2^n \leqslant n!$ et $1 \leqslant n$, alors $2 \leqslant (n+1)$ donc $2^{n+1} \leqslant (n+1)!$
L'hérédité est assurée pour $n \geqslant 1$.
Mais $\mathcal{P}(1)$, $\mathcal{P}(2)$ et $\mathcal{P}(3)$ sont fausses ! L'initialisation ne peut se faire que pour $n = 4$, où $2^4 = 16 \leqslant 4! = 24$ et la propriété $\mathcal{P}(n)$ est assurée par récurrence pour $n \geqslant 4$.

Attention à ne pas confondre : relation de récurrence et démonstration par récurrence.
Soit pour $n \in \mathbb{N}$, la fonction définie sur $[-1,1]$ par $T_n : x \mapsto \cos(n \operatorname{Arccos}(x))$.
Montrer que pour $n \in \mathbb{N}$, $T_{n+2}(x) = 2x\,T_{n+1}(x) - T_n(x)$,
et que $\forall n \in \mathbb{N}$, T_n est une fonction polynômiale de degré n, de la parité de n,
et de coefficient dominant 2^{n-1}. (Polynômes de Tchebychev).

• La première relation est une relation de récurrence entre les T_n mais elle se montre **directement**, et non par récurrence. Avec les formules de trigonométrie :
$\forall n \in \mathbb{N}$, $n \geqslant 2, \forall y \in \mathbb{R}$, $\cos(ny) + \cos((n+2)y) = 2\cos((n+1)y)\cos(y)$.
Appliqué à $y = \operatorname{Arccos}(x)$ pour $x \in [-1,1]$, donc avec $x = \cos(y)$,
on obtient $\forall n \in \mathbb{N}$, $n \geqslant 2, \forall x \in [-1,1]$, $T_n(x) + T_{n+2}(x) = 2x\,T_{n+1}(x)$
• Montrons les autres propriétés par récurrence. Appelons $\mathcal{Q}(n)$ la proposition : T_n est une fonction polynômiale sur $[-1,1]$ de degré n, de la parité de n, et de coefficient dominant 2^{n-1}. Et $\mathcal{P}(n)$ la conjonction : ($\mathcal{Q}(n)$ et $\mathcal{Q}(n+1)$).
Initialisation : on a $T_0(x) = 1$ et $T_1(x) = x$. $\mathcal{Q}(0)$ et $\mathcal{Q}(1)$ sont vraies.
Donc $\mathcal{P}(0)$ est vraie.
Hérédité : supposons la propriété $\mathcal{P}(n)$ vraie pour $n \in \mathbb{N}$, quelconque fixé.
$\mathcal{Q}(n)$ et $\mathcal{Q}(n+1)$ sont donc vraies, et alors $T_{n+2}(x) = 2x\,T_{n+1}(x) - T_n(x)$ assure que $\mathcal{Q}(n+2)$ est vraie et donc $\mathcal{P}(n+1)$ vraie.
Par le **théorème de récurrence**, les propriétés $\mathcal{P}(n)$ et donc $\mathcal{Q}(n)$ sont assurées pour tout $n \in \mathbb{N}^*$.

1.1.4 Ecriture d'un entier dans une base de numération b

Théorème

Soit $b \in \mathbb{N}$, avec $b \geqslant 2$. Pour tout $N \in \mathbb{N}$,
il existe un unique entier naturel n et une seule suite finie $(a_0, a_1, \ldots, a_n)$ de $n+1$ termes, éléments de $\mathbb{N} \cap [0, b-1]$ tels que $N = \sum_{k=0}^{k=n} a_k b^k$ et $a_n \neq 0$.

Démonstration

• *Existence* : par récurrence sur N.

∘ Initialisation : l'existence est assurée pour $N \in [0, b-1]$ avec $n = 0$ et $a_0 = N = a_0\, b^0$.

∘ Hérédité : pour $N \geqslant b$, supposons l'existence assurée pour les entiers jusqu'à $N-1$.
Par division euclidienne de N par b, on assure l'existence de (q, r) tels que $N = b\,q + r$ et $r \in [0, b-1]$. Par l'hypothèse de récurrence appliquée à $q \leqslant N-1$, on a une relation du type $q = \sum_{k=0}^{k=p} c_k b^k$ avec $p \in \mathbb{N}$ et $c_p \neq 0$. Ainsi $N = \sum_{k=0}^{k=p} c_k b^{k+1} + r$.

On pose $n = p+1$, $a_0 = r$, et $\forall k,\ 1 \leqslant k \leqslant n$, $a_k = c_{k-1}$ alors $N = \sum_{k=0}^{k=n} a_k b^k$ et $a_n \neq 0$.

D'où l'existence assurée pour N.

• *Unicité* : si l'on avait deux développements différents : $N = \sum_{k=0}^{k=n_1} a_k b^k = \sum_{k=0}^{k=n_2} d_k b^k$,

alors $\sum_{k=0}^{\max(n_1,n_2)} (a_k - d_k)\, b^k = 0$ et $D = \{k \in \mathbb{N} \cap [0, \max(n_1 n_2)], a_k \neq d_k\}$ est non vide.

Si $p = \sup(D)$ alors $|(a_p - d_p)\, b^p| = \left| \sum_{k=0}^{k=p-1} (a_k - d_k)\, b^k \right|$ car ces entiers sont opposés.

Mais $|a_k - d_k| \leqslant b-1$, et $\left| \sum_{k=0}^{k=p-1} (a_k - d_k)\, b^k \right| \leqslant (b-1) \sum_{k=0}^{k=p-1} b^k = (b-1)\, \dfrac{1-b^p}{1-b} = b^p - 1$.

Donc l'un est supérieur à b^p et l'autre lui est strictement inférieur : **absurde**.

Définition

Les entiers de $[0, b-1]$ sont les **chiffres** en base b. Pour $N \in \mathbb{N}$, les $(a_k)_{0 \leqslant k \leqslant n}$ sont les chiffres de **l'écriture en base** b de N, qu'on note $N = \overline{a_n \cdots a_1 a_0}$.

1.1.5 Des entiers aux complexes

$\mathbb{N}$, ensemble des entiers naturels, repose sur la possibilité de faire une liste « sans fin » d'objets distincts. Les mathématiciens ont construit de nouveaux ensembles de nombres pour rendre possibles des opérations algébriques, essentiellement pour assurer l'existence d'inverses : passage de $\mathbb{N}$ à $\mathbb{Z}$, puis de $\mathbb{Z}$ à $\mathbb{Q}$. On aboutit ainsi au corps des rationnels.

Des raisons topologiques (assurer l'existence de limites de suites) ont présidé à la construction de $\mathbb{R}$, sur-corps de $\mathbb{Q}$. La recherche des racines des polynômes a mené à la construction de $\mathbb{C}$, chaque complexe étant une association de deux réels. D'autres constructions d'objets composites (entiers de Gauss, quaternions, octaves de Cayley, polynômes, matrices, etc.) ouvrent de nouvelles possibilités à partir des nombres déjà connus. L'étude de la structure algébrique rend compte des **modes de calculs possibles** sur ces objets.

1.2 Définitions des structures fondamentales

1.2.1 Groupes, anneaux, corps

Groupe

Soit G un ensemble non vide, et $*$ une loi de composition interne définie sur G.

Définition de groupe

$(G,*)$ est un **groupe** si et seulement si :

$$\begin{cases} (i) & \text{la loi } * \text{ est associative } : \forall\,(a,b,c)\in G^3,\ (a*b)*c = a*(b*c)\,, \\ (ii) & \text{il existe un élément neutre pour } * \text{ dans } G : \\ & \qquad \exists\, e\in G,\ \forall a\in G\ ,\ e*a = a*e = a, \\ (iii) & \text{tout élément de } G \text{ admet un élément symétrique pour } * \\ & \qquad \forall a\in G,\ \exists\, a'\in G,\ a*a' = a'*a = e. \end{cases}$$

Sous-groupe

Définition d'un sous-groupe

Soit $(G,*)$ un groupe. $(H,*)$ où H est une partie non vide de G est un **sous-groupe** de $(G,*)$ si H est stable pour la loi $*$ et a une structure de groupe pour la loi induite.

Ce qui revient à dire que H contient le neutre de G, car le neutre de H est nécessairement celui de G, que H est stable par produit par $*$ et passage à l'inverse.

Théorème de caractérisation

Soit $(G,*)$ un groupe, H une partie non vide de G.

$$\Big((H,*) \text{ sous-groupe de } (G,*)\Big) \Longleftrightarrow \Big(H\neq\emptyset \text{ et } \forall\,(x,y)\in H^2\ ,\ x*y^{-1}\in H\Big).$$

Démonstration, en notant (1) *et* (2) *nos propositions*
Il est clair que (1) $\Longrightarrow$ (2), car H contient le neutre, est stable par produit par $*$, et passage à l'inverse.
Si (2) est vraie, alors pour un x de H, $x*x^{-1} = e\in H$, puis que $e*x^{-1} = x^{-1}\in H$, et finalement que pour $(x,y)\in H^2$, $x*(y^{-1})^{-1} = x*y\in H$. On a bien un sous-groupe.

Intersection de sous-groupes

Soit $(G,*)$ un groupe, et $(H_i,*)_{i\in I}$ une famille de sous-groupes de G, alors
$H = \bigcap_{i\in I} H_i$ est un sous-groupe de $(G,*)$.

Tous les sous-groupes contiennent le neutre e, donc H est non vide, et vérifie la caractérisation précédente.

Anneau

Soit A un ensemble non vide, $+$ et $*$ deux lois de composition internes définies sur A.

Définition : anneau

$(A,+,*)$ est un **anneau** (tous les anneaux seront unitaires) si et seulement si :

$$\begin{cases} (i) & (A,+) \text{ est un groupe commutatif, avec } 0_A \text{ comme élément neutre,} \\ (ii) & \text{la loi } * \text{ est associative,} \\ (iii) & \text{la loi } * \text{ est distributive par rapport à } +\,, \\ (iv) & \text{la loi } * \text{ possède un élément unité dans } A, \text{ noté } 1_A \textbf{ et } 1_A\neq 0_A. \end{cases}$$

Si de plus $*$ est commutative, on dit que $(A,+,*)$ est un anneau **commutatif**.

En particulier $\Big(0,+,\times\Big)$ n'est pas un anneau, car $1_A = 0_A$.
Un élément x d'un anneau est **inversible**, s'il existe un inverse, noté x^{-1}, pour la loi $*$.

Théorème
L'ensemble des inversibles d'un anneau, noté $Inv(A)$ forme un groupe pour la loi $*$.

Démonstration : Ce sous-ensemble $Inv(A)$ est non vide, car il contient le neutre 1_A.
$Inv(A)$ est stable par produit car si x et y sont inversibles, alors $x * y$ est inversible, d'inverse $y^{-1} * x^{-1}$.
Et $Inv(A)$ est stable par passage à l'inverse car l'inverse x^{-1} d'un x inversible est naturellement inversible puisque $x^{-1} * x = x * x^{-1} = 1_A$, on a donc $(x^{-1})^{-1} = x$.

Sous-anneau

Soit $(A,+,*)$ un anneau et B une partie non vide de A.

Définition : sous-anneau
$(B,+,*)$ est un **sous-anneau** de $(A,+,*)$ si et seulement si :
$$\begin{cases} \forall (x,y) \in B^2\,,\ (x-y) \in B, \\ \forall (x,y) \in B^2\,,\ (x*y) \in B, \\ 1_A \in B. \end{cases}$$

Ce ne sont pas les parties les plus remarquables d'un anneau, les **idéaux** sont plus féconds.
Remarque : $(\{0\},+,\times)$ n'est pas un sous-anneau de l'anneau $(\mathbb{R},+,\times)$, du fait du $3^{ème}$ axiome non vérifié. Par contre $\{0\}$ sera un idéal de l'anneau $(\mathbb{R},+,\times)$.

Idéal d'un anneau commutatif

Définition : idéal
Soit $(A,+,*)$ un anneau commutatif, I une partie non vide de A. I est un **idéal** de A si et seulement si : $\begin{cases} (I\,,+) \text{ est un sous-groupe de } (A\,,+), \\ \forall (a,x) \in A \times I\ ,\ \ (a*x) \in I. \end{cases}$

Il s'agit donc d'un sous-groupe additif de A, **absorbant** par l'opération $*$.
En particulier : $\{0\}$ et A sont des idéaux de A.

Théorème de caractérisation
Si I est une partie non vide de A, et $(A,+,*)$ un anneau commutatif :
$$(I \text{ est un idéal de } A) \Longleftrightarrow \begin{cases} \forall\,(x,y) \in I^{\,2}\ ,\ \ (x+y) \in I, \\ \forall\,(a,x) \in A \times I\ ,\ \ (a*x) \in I. \end{cases}$$

On note que si I est un idéal de A : $(I = A) \Longleftrightarrow (1_A \in I)$.

Opérations sur les idéaux

Théorèmes sur les idéaux
Si p entier, avec $p \geqslant 2$ et $I_1, I_2, \cdots, I_p$ sont p idéaux d'un anneau $(A,+,\times)$,
alors $I = \bigcap_{k=1}^{p} I_k$ et $S = I_1 + I_2 + \cdots + I_p$ sont encore des idéaux de l'anneau.

S est l'ensemble des sommes d'éléments pris respectivement dans chacun des I_k.
Il est clair que I et S sont des sous-groupes additifs, absorbants par produit.