Anneaux

Table des matières

À faire : regrouper dans un même paragraphe (le 3) voire dans un même fichier tous les exercices traitant de $\varphi : x \mapsto x^2$ ou de $B = \{a \in A \,/\, a^2 = e\}$.

1. DIVERS

1.1. Nilpotents

1. Montrer que dans un anneau :
   a. x nilpotent $\Rightarrow 1-x$ inversible.
      Réponse : si $x^n=0$ alors $(1-x)(1+x+\ldots+x^{n-1})=1$.
   b. xy nilpotent $\Rightarrow yx$ nilpotent. L'ordre est-il le même ?
      Réponse : si $(xy)^n=0$ alors $y(xy)^n x=0$ or ceci est égal à $(yx)^{n+1}$.
      L'ordre n'est pas forcément le même, exemple $x=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ et $y=\begin{pmatrix}0&0\\1&0\end{pmatrix}$, alors l'ordre de xy est 1 (car $xy=0$) tandis que l'ordre de yx est 2.
   c. x, y nilpotents et $xy=yx \Rightarrow (x+y)$ nilpotent.
      Réponse : par Newton, si $x^n=y^n=0$ alors $(x+y)^{2n}=0$ car dans le binôme il y a toujours un coefficient $\geqslant n$ puisque la somme des deux fait $2n$.
2. A-t-on des exemples où l'ordre de nilpotence de xy et celui de yx ne sont pas les mêmes (on démontre que l'un égale l'autre $+1$ ou mieux).

1.2. Éléments inversibles

1. si $1-ab$ inversible, montrer que $1-ba$ inversible aussi.
   Résolution 1
   Indication : factoriser $a-aba$ à gauche ou à droite.
   Réponse :
   Posons $K=(1-ab)^{-1}$, et remarquons que $a-aba=a(1-ba)=(1-ab)a$, on peut alors écrire que :

$$\begin{aligned} & Ka\times(1-ba)=a \\ \text{donc} \quad & bKa\times(1-ba)=ba \\ \text{d'autre part} \quad & 1\times(1-ba)=1-ba, \end{aligned}$$

   et en ajoutant les deux dernières lignes on a l'inverse de $1+ba$ qui apparaît.
   Résolution 2 (avoir vu auparavant l'exercice 1).
   Réponse :
   * Si ab nilpotent d'ordre p, alors :

$$(1+ab+(ab)^2+\ldots+(ab)^{p-1})(1-ab)=1 \ (1).$$

   Or d'après l'exercice 1, ba aussi est nilpotent, d'ordre $p+1$ donc :

$$(1+ba+(ba)^2+\ldots+(ba)^{p})(1-ba)=1 \ (2).$$

   (2) prouve que $1-ba$ est inversible, et si l'on multiplie (1) par b à gauche et par a à droite on obtient :

$$(1-ba)^{-1}=b(1-ab)^{-1}a+1$$

   * Cas général : il suffit de vérifier que $b(1-ab)^{-1}a+1$ convient.

1.3. Divers

1. $\mathcal{A}$ un anneau non trivial, soit $M=\{a\in A / a^2=a\}$, montrer que si M est fini, son cardinal est pair.
   Indication : considérer $x\mapsto 1-x$.
2. Trouver un anneau $\mathcal{A}'\subset\mathcal{A}$ tel que $\mathcal{A}'$ ne soit pas un sous-anneau de $\mathcal{A}$.
   $\mathcal{A}=\mathbb{Z}^2$ avec $+$ et $\times$ terme à terme, et $\mathcal{A}'=\mathbb{Z}\times\{0\}$ qui ne contient pas le neutre $(1,1)$.
   Ou bien $2\mathbb{Z}\subset\mathbb{Z}$ ou plus généralemnet tout idéal.

1.4. Anneaux intègres

Définition 1. *$\mathcal{A}$ est dit intègre s'il est commutatif, unitaire, et intègre au sens que l'on entend.*

1. Soit $\mathcal{A}$ intègre. Montrer qu'on peut simplifier dans $\mathcal{A}$: si $a\,b = a\,c$ alors $b = c$. Tout élément $a \in \mathcal{A}$ est-il alors inversible ?
   $a(b-c) = 0 \Rightarrow b = c$ et non, par exemple $a = 2$ dans $\mathbb{Z}$.
2. Montrer que $\mathcal{A}$ intègre fini $\Leftrightarrow$ $\mathcal{A}$ corps (technique de « translation ») ;
   Soit $a \in \mathcal{A}$, alors $a\mathcal{A} = \mathcal{A}$ car $x \mapsto a\,x$ est injective. En particulier $\exists a' / a\,a' = e$.
3. Exemple d'anneaux non intègres : $M_n(\mathbb{R})$, $\mathbb{Z}/6\mathbb{Z}$, $(\mathcal{C}_0(\mathbb{R}), +, \times)$, $\mathbb{Z}^2$ avec le $+$ et le $\times$ terme à terme.

2. Idéaux & idéaux principaux, premiers, maximaux

2.1. Généralités

Définition 2. *Idéal de type fini = idéal $\mathcal{I}$ engendré par un nombre fini d'éléments :*

$$\mathcal{I} = (a_1) + \cdots + (a_n).$$

2.2. Idéaux

2.2.1. Divers

1. Donner un exemple de sous-groupe qui ne soit pas un idéal. Réponses :
   a. $\mathbb{Q}$ dans $(\mathbb{R}; +, \times)$;
   b. $\mathbb{Z}$ dans $(\mathbb{Q}; +, \times)$;
   c. $\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, a, b \in \mathbb{R} \right\}$ sous-groupe de $\mathcal{M}_n(\mathbb{R})$, mais idéal pas bilatère (à gauche seulement).
2. Un idéal est-il un sous-anneau ?
   Non car il n'a pas 1 ; mais c'est un sous-groupe stable par $\times$ donc un anneau inclus dans l'anneau..
3. Si $\mathcal{I}$ et $\mathcal{I}'$ sont deux idéaux, qu'en est-il de $\mathcal{I} \cap \mathcal{I}'$? $\mathcal{I} \cup \mathcal{I}'$?
   L'$\cup$ ne conserve pas les sous-groupes, par contre $\mathcal{I} \cap \mathcal{I}'$ est un idéal.
4. Démontrer que si un idéal contient 1 alors c'est l'anneau tout entier.
   Application : quels sont les idéaux d'un corps ?
   $\{0\}$ et le corps lui-même.
5. $\mathcal{A}$ et $\mathcal{A}'$ deux anneaux et $f : \mathcal{A} \to \mathcal{A}'$ un morphisme d'anneaux.
   a. Si f surjectif, montrer que les idéaux de $\mathcal{A}$ ont pour image des idéaux de $\mathcal{A}'$.
      il suffit d'appliquer les définitions.
   b. Si f non surjective, donner des exemples où l'image d'un idéal n'est pas un idéal.
      prendre l'injection canonique $f : \mathbb{Z} \to \mathbb{Q}$ définie par $f(x) = x$ et voir que $2\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$.
   c. Dans tous les cas, montrer que f^{-1} transforme les idéaux de $\mathcal{A}'$ en idéaux de $\mathcal{A}$.
6. Soit $\mathcal{I}$ idéal bilatère de $\mathcal{A}$, alors on peut munir $\mathcal{A}/\mathcal{I}$ d'une structure d'anneau.
   Soit $f : \mathcal{A} \to \mathcal{A}/\mathcal{I}$ la surjection canonique.

2.2.2. Exercices autour de $\mathcal{L}(E)$

Soit E un espace vectoriel de dimension finie (supérieure ou égale à 2) sur un corps K (commutatif ou non).

1. Montrer que $\mathcal{L}(E)$ n'a pas d'idéaux bilatères autres que $\emptyset$ ou lui-même.

Soit $\mathcal{I}$ idéal de $\mathcal{L}(E)$ et $u \neq 0$ dans $\mathcal{I}$.
Soient $a, b \neq 0$ dans E tels que $u(a) = b$.
Quitte à coposer par ce qu'il faut à gauche on peut supposer $u(a) = a$.
Soit $(a, e_2, ..., e_n)$ une base de E.
Quitte à composer par ce qu'il faut à gauche on peut construire $u' \in \mathcal{I}$ tel que $u'(a) = a$ et $u'(e_i) = 0$.
Quitte à composer par ce qu'il faut à gauche et à droite on peut construire des $u'_i \in \mathcal{I}$ tels que $u'_i(e_i) = e_i$ et $u'_i = 0$ dans le supplémentaire.
En ajoutant on a donc $U = u' + u'_2 + \cdots + u'_n \in \mathcal{I}$, or $U = \mathrm{Id}$ par construction.
Ainsi, $\mathcal{I} = \mathcal{L}(E)$.

2. Montrer que $\mathcal{L}(E)$ possède des idéaux à gauche et à droite non triviaux : pour tout sous-espace F de E, l'ensemble des endomorphismes de noyau contenant F est un idéal à gauche, tandis que l'ensemble des endomorphismes d'image contenue dans F est un idéal à droite.

2.3. Anneaux principaux

2.3.1. Rappel

DÉFINITION 3. *$\mathcal{A}$ principal lorsque :*

- *$\mathcal{A}$ intègre ;* • *$\mathcal{A}$ commutatif ;* • *tout idéal de $\mathcal{A}$ est principal.*

2.3.2. Exercices

1. Si $\mathcal{A}$ est intègre commutatif et euclidien (i.e. possède une division euclidienne), alors $\mathcal{A}$ est principal.
Preuve :
   - Soit I un idéal de $\mathcal{A}$, soit n_0 le min des $\{n = v(i), i \in I\}$, où v désigne le stathme de $\mathcal{A}$.
   Soient i_0 et i'_0 tels que $v(i_0) = v(i'_0) = n_0$ alors $i_0 = a\, i'_0 + r$ et $i'_0 = a'\, i_0 + r'$, mais du coup $v(r)$ et $v(r')$ seraient $< n_0$ d'où $r = r' = 0$. On trouve $i_0 = a\, i'_0$ et $i'_0 = a'\, i_0$.
   Soit $i \in I$ alors par division euclidienne de i par i_0 on a $i = \alpha\, i_0$. Ainsi, $I = (i_0)$.

à faire :
- transposer ceci vers le dossier L3 ;
- regarder ici http://www.les-mathematiques.net/phorum/read.php?3,1663206 ;
- peut-il exister un (pré)stathme dans un anneau non intègre ou non commutatif ?

2. Bezout est une traduction de « $\mathbb{Z}$ principal ».
Dans $\mathbb{Z}$, l'idéal $\mathcal{I} = \{a\, x + b\, y, a, b \in \mathbb{Z}\}$ est de la forme $d\mathbb{Z}$.
Du coup $d | a \wedge b$.
De plus soit μ un diviseur commun de a et b, alors μ divise un $a\, x_0 + b\, y_0 = d$.
Ainsi $d = a \wedge b$.

2.4. Idéaux premiers vs maximaux

Idéal premier, métaphore : « on ne peut pas y entrer en se combinant avec un autre, il faut y entrer soi, tout entier et tout seul »

DÉFINITION 4. *Distinguer :*

- *$a \in \mathcal{A}$ est un élément **irréductible** (dans $\mathcal{A}$) ssi $m\, n = a \Rightarrow [m = a$ ou $n = a]$;*
- *$\mathcal{I}$ est **premier** ssi $m\, n \in \mathcal{I} \Rightarrow [m \in \mathcal{I}$ ou $n \in \mathcal{I}]$.*

2.4.1. On peut avoir p irréductible mais (p) non premier

Voici un exemple :
$p = 1 + \mathrm{i}\sqrt{5} = (1, 1)$ dans $\mathcal{A} = \mathbb{Z}[\mathrm{i}\sqrt{5}]$. On pose $N(a, b) = a^2 + 5b^2$.

- p irréductible car si $m\, n = p$ alors $N(m) = 1$ (soit $m = 1$) ou $N(m) = 9$ (soit $n = 1$) ou $N(m = 3)$ (aucune solution) ;

- (p) non premier car $9 \in (p)$ (en effet, $9 = p \times (2 - \mathrm{i}\sqrt{5})$) mais $3 \notin (p)$ (sinon $3 = p\,z$ et $N(z) = 1$).

2.4.2. On peut avoir $\mathcal{I}$ premier mais non maximal

Voici des exemples :

- $\mathcal{A} = \mathbb{Z} \times \mathbb{Z}$ et $\mathcal{I} = p\mathbb{Z} \times p\mathbb{Z}$ (on a $\mathcal{I} \subset \mathbb{Z} \times p\mathbb{Z}$);
- $\mathcal{A} = \mathbb{R}[X]$ et $\mathcal{I} = (X^2)$ (on a $\mathcal{I} \subset (X)$) ;
- $\mathcal{A} = \mathbb{R}[X]$ et $\mathcal{I} = (X)$ (on a $\mathcal{I} \subset (X) + (2)$) ;

3. Anneaux classiques

3.1. Exemples pour comprendre la notion d'isomorphisme

3.1.1. Anneaux isomorphes de natures diverses

$(\mathbb{F}_2)^{\mathbb{N}} \sim \mathcal{A} = (\mathcal{P}(E), \Delta, \cap)$, anneaux de Boole, vus sur un ensemble de suites puis sur un ensemble d'ensembles.

3.1.2. Même ensemble muni de structures différentes

La structure n'est pas définie par l'ensemble mais pas les lois qu'on met dessus.
Exemple :

- l'anneau des suites réelles à support fini avec $\times$ terme à terme n'a pas la même structure que $\mathbb{R}[X]$ alors qu'il porte sur des éléments qui sont en fait les mêmes ;
- $(\mathbb{Z}/p\mathbb{Z}, +)$ est un groupe tandis que $(\mathbb{F}_p, +, \times)$ est un corps :

3.2. Exercices divers

1. $\mathcal{B}(\mathcal{P}(E), \cup, \cap)$ et $\mathcal{B}'(\mathcal{P}(E), \cap, \cup)$ sont-ils des anneaux ?
   Non, car il n'y a pas d'inverse pour $\cup$ ni pour $\cap$!
2. $(\mathcal{C}_0(\mathbb{R}), +, \times)$
3. Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps **ssi** n premier.
4. comparer $(\mathbb{Z}/2\mathbb{Z})^2$ avec les deux lois :
   - terme à terme (idempotent) ;
   - identification (a, b) et $a + b\,i$;

   regarder les idéaux.

4. Anneaux $(\mathcal{A}[X], \times, +)$

4.1. $K[X]$ est principal

Théorème 5. *$\mathcal{A}[X]$ principal $\Leftrightarrow$ $\mathcal{A}$ est un corps.*

Démonstration.
$\Rightarrow$ soit $a \in \mathcal{A}$. Prenons $(P) = (a) + (X)$:
C'est l'idéal des polynômes de $\mathcal{A}[X]$ dont le coefficient constant est multiple de a.
On a $a = PQ$ et $X = PR$ et $P = a\,U + X\,V$.
Déjà, P et Q sont donc constants, écrivons $P = p$ et $Q = q$ alors $a = p\,q$.
Posons $u = U(0)$, on a alors $p = a\,u$ et $a = p\,q$ donc $a = a\,u\,q$.
On en déduit (car $\mathcal{A}$ intègre) que $u\,q = 1$ donc u et q sont inversibles.
De $X = p\,R$ on déduit que $R = r\,X$ donc $X = p\,r\,X$ donc p aussi est inversible.

Conclusion : a est inversible.

$\Leftarrow$ soit $\mathcal{I}$ un idéal de $\mathcal{A}$.
Soit $N \subset \mathbb{N}$ l'ensemble des degrés des polynômes non nuls de $\mathcal{I}$. Soit $n = \min(N)$.
Soient $P, Q \in \mathcal{I}$ unitaires alors $P - Q \in \mathcal{I}$ est de degré $< n$ donc $P = Q$.
Conclusion : $\mathcal{I} = (P)$. □

4.2. Polynômes égaux

Le principe suivant est vrai si $\mathcal{A}$ est infini et intègre :

Si $\forall a \in \mathcal{A}, P(a) = Q(a)$ alors $P = Q$.
Autre formulation :
Deux polynômes P, Q distincts (quant à leurs coefficients) ne peuvent prendre partout les mêmes valeurs ($\forall a \in \mathcal{A}, P(a) = Q(a)$)

Contre exemples :

- dans $\mathcal{A}$ non intègre : pour $P(X) = X^2 + X$ dans l'anneau de Boole $\mathcal{A} = (\mathcal{P}(\mathbb{N}), \Delta, \cap)$, on a :
$$\forall a \in \mathcal{A}, P(a) = 0\,;$$
- dans $\mathcal{A}$ corps fini : pour $P(X) = X^2 + X$ dans $\mathbb{F}_2$ on a aussi : $\forall a \in \mathcal{A}, P(a) = 0$;
- dans $\mathcal{A}$ non intègre et fini : $P(X) = X^4 - X^2$ et $Q(X) = 6X(X+1)$ dans $\mathbb{Z}/12\mathbb{Z}$ ne prennent que des valeurs nulles. Preuve du premier, voir fichier « arithmétique ».

Y a-t-il un contre exemple avec $\mathcal{A}$ de caractéristique nulle ?

4.3. Principe de factorisation

On a la propriété :
$$[P(\mu) = 0 \Rightarrow P \text{ se factorise par} (X - \mu)] \tag{1}$$
Elle se démontre :

- par une considération d'idéal principal : $\mathcal{I} = \{P / P(\mu) = 0\} = (X - \mu)$;
- à l'aide de la division euclidienne en divisant $P(X)$ par $(X - \mu)$;
- ou en factorisant directement $P(X)$ par $(X - \mu)$ à l'aide de l'identité :
$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + a\,b^{n-2} + b^{n-1}).$$

4.3.1. Applications

1. $K[X]$ est (intègre) et principal donc tout polynôme de racine a se factorise par $(X - a)$ donc tout polynôme de degré n a au plus n racines ;

4.3.2. Si $\mathcal{A}$ n'est pas un corps, alors, dans $\mathcal{A}[X]$...

1. ...il n'y a pas de division euclidienne.
   En donner un exemple.
   Dans $\mathbb{Z}[X]$, essayer de diviser X par $2X$...
2. ...il n'y a pas de stathme (montrer par un exemple que le degré ne veut plus rien dire).
   ...on peut avoir deux polynômes égaux par leurs valeurs sans l'être par leurs coefficients.
   Dans $\mathbb{Z}/4\mathbb{Z}$ (voir plus bas) on a identité de polynômes : $2X = 2X^2$.
3. ...$\mathcal{A}[X]$ n'est pas principal.
   Donner un exemple d'idéal non principal de $\mathcal{A}[X]$.
   $(2) + (X)$, soit l'idéal des polynômes dont le terme constant est pair.
4. ...le principe de factorisation ne sert plus à rien.
   En effet, si a, b annulent P alors $P(X) = (X - a)Q(X)$ mais il n'y a aucune raison que $Q(b) = 0$ si par exemple $\mathcal{A}$ n'est pas intègre.

Donner un exemple
Soit $P(X)=2X$ dans $\mathbb{Z}/4\mathbb{Z}[X]$: on a $P(0)=P(2)=0$.
On trouve par identification : $P(X)=2X=-2X(X-2)=2X^2$...

4.4. Si K est fini, alors, dans $K[X]$...

1. ...on peut avoir $P^{(n)}(x)=0$ pour toute valeur de n, sans pour autant que $P=0$.
   Exemple $P(X)=X^p$ dans $\mathbb{F}_p$ et $x=0$.

5. Anneaux $(\mathbb{Z}[a],\times,+)$

5.1. $\mathbb{Z}[i]$

$\mathbb{Z}[i]$ euclidien (norme $|.|^2$) donc principal ;

5.2. $\mathbb{Z}[\sqrt{a}]$

5.2.1. Divers

1. $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[\sqrt{3}]$ ne sont pas isomorphes en tant qu'anneaux (mais en tant que groupes, si) ;
   En effet, si $\varphi:\mathbb{Z}[\sqrt{2}]\to\mathbb{Z}[\sqrt{3}]$ était un isomorphisme, on aurait $\varphi(\sqrt{2}^2)=\varphi(\sqrt{2})^2$ donc $\varphi(2)=$
2. $\mathbb{Z}[\sqrt{a}]$ n'a pas d'autre automorphisme que l'identité et la conjugaison ;

5.2.2. Une norme sur $\mathbb{Z}[\sqrt{2}]$

1. Dans $\mathbb{Z}[\sqrt{2}]$, on pose $N(a+b\sqrt{2})=a^2-2b^2$:
   a. montrer que $N(x\,y)=N(x)\,N(y)$;
   b. montrer que x inversible ssi $N(x)=\pm1$;
   c. montrer que les inversibles sont les $\pm(1+\sqrt{2})^n, n\in\mathbb{Z}$.

Réponse : (i) il suffit d'écrire $N(x)=x\cdot\bar{x}$ où $\overline{a+b\sqrt{2}}=a-b\sqrt{2}$ et (ii) il suffit de regarder les inversibles dans $(\mathbb{Z},\times,+)$ et (iii) déjà il est clair que les $\pm(1+\sqrt{2})^n, n\in\mathbb{Z}$ ont une norme égale à ±1.

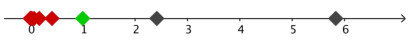

Figure 1. Visualisation des $(1+\sqrt{2})^n$
en rouge, $n=-1,-2,-3$...
en vert $n=0$
en noir $n=1,2,...$

Il s'agit de montrer qu'il n'y a pas d'autres inversibles dans $]1;1+\sqrt{2}[$.
Supposons qu'il y en a un, appelons-le $x=a+b\sqrt{2}$.
On a donc $(a+b\sqrt{2})(a-b\sqrt{2})=\pm1$.
Vu que $a+b\sqrt{2}\in]1;1+\sqrt{2}[$, par passage à l'inverse on a :

$$a-b\sqrt{2}\in\begin{cases}]\sqrt{2}-1;1[& \text{si } +1\\ ]-1;1-\sqrt{2}[& \text{si } -1.\end{cases}$$

En prenant la moyenne de ces deux nombres on a donc :

$$a\in\begin{cases}\left]\frac{\sqrt{2}}{2};1+\frac{\sqrt{2}}{2}\right[& \text{si } +1\\ ]0;1[& \text{si } -1.\end{cases}$$

donc $a=1$, $b=0$ et c'est $+1$ et $x=1$ et la démonstration est finie.

6. ANNEAU DES SUITES RÉELLES

6.1. Dans $(\mathbb{R}^{\mathbb{N}}, +, \times)$ (addition et multiplication terme à terme)

1. L'ensemble $F = \{u \in \mathbb{R}^{\mathbb{N}} / \exists n \in \mathbb{N} / \forall p \geqslant n, u_p = 0\}$, autrement dit l'ensemble des suites à support fini, est-il un idéal ? principal ? de $\mathbb{R}^{\mathbb{N}}$

Remarque 6. On pourrait voire F comme $\mathbb{R}[X]$ plongé dans $\mathbb{R}^{\mathbb{N}}$ mais pas avec la même loi multiplicative.

Réponse : idéal oui, évident, principal non car si $(u_0, u_1, ..., u_{n_0}, 0, ...)$ engendrait F, alors F ne contiendrait pas $(u_0, u_1, ..., u_{n_0}, u_{n_0+1}, 0, ...)$.

7. ANNEAUX DE BOOLE

7.1. Forme multiplicative : $\forall a \in \mathcal{A}, a^2 = a$

Soit $(\mathcal{A}, \times, +)$ un anneau (pas forcément commutatif *a priori*) tel que $\forall a \in \mathcal{A}, a^2 = a$.

Montrer que :

1. $\forall a, b \in \mathcal{A}, a\,b + b\,a = 0$.
2. $\forall a \in \mathcal{A}, a + a = 0$.
3. A commutatif.
4. La relation $x \preccurlyeq y \Leftrightarrow y\,x = x$ définit un ordre.
5. $\forall a, b \in \mathcal{A}, a\,b(a+b) = 0$
6. A est non-intègre sauf cas trivial $\mathcal{A} = \mathbb{Z}/2\mathbb{Z}$.

Réponses :

1. $(a+b)^2 = a + b \Rightarrow a\,b + b\,a = 0$
2. On écrit $(a+a)^2$ ou bien on prend $b=1$ ou $b=a$ dans le précédent.
3. $\left\{ \begin{array}{l} a\,b + a\,b = 0 \\ a\,b + b\,a = 0 \end{array} \right. \Rightarrow a\,b = b\,a$.
4. Propriétés d'un ordre :
   a. $a \preccurlyeq b$ puisque $a^2 = a$;
   b. si $a \preccurlyeq b$ et $b \preccurlyeq a$ alors $b\,a = a$ et $a\,b = b$ d'où $a = b$;
   c. si $a \preccurlyeq b$ et $b \preccurlyeq c$, alors cela signifie que : $b\,a = a (1)$ et $c\,b = b (2)$; alors $1 \Rightarrow c\,b\,a = c\,a$ et on remplace $c\,b$ par b d'où $b\,a = c\,a$ d'où $a = c\,a$ d'où $a \preccurlyeq c$.
5. $a\,b\,(a+b) = a\,b\,a + a\,b\,b = b\,a\,a + a\,b = b\,a + a\,b = 0$.
6. Pour tout $a \in \mathcal{A}$ on a $a^2 - a = 0 \Leftrightarrow a(a-1) = 0$ donc $\mathcal{A}$ intègre $\Rightarrow$ tout $a \in \mathcal{A}$ est égal à 0 ou 1 donc $\mathcal{A} = (\mathbb{Z}/2\mathbb{Z}, +, \times)$. Si $\mathcal{A}$ possède davantage que 2 éléments, $\mathcal{A}$ n'est pas intègre.
   peut-être que ce truc prouve que $\mathcal{A}$ est un 2^n ev ?

est-ce que tout anneau vérifiant $a^2 = a$ est un $\mathcal{A} = (\mathcal{P}(E), \Delta, \cap)$? déjà il faudrait qu'il soit de cardinal 2^n et si on dit que tout tel anneau est un idéal d'un $\mathcal{A} = (\mathcal{P}(E), \Delta, \cap)$ alors on est obligé d'admettre aussi qu'un tel idéal est un (F) où $F \subset E$ et donc d'ordre 2^p aussi.

7.2. Forme ensembliste : $\mathcal{A} = (\mathcal{P}(E), \Delta, \cap)$

E un ensemble de cardinal n, et $\mathcal{A}$ l'anneau $\mathcal{A} = (\mathcal{P}(E), \Delta, \cap)$ où $U \Delta V = (U \cup V) \backslash (U \cap V)$.
Le Δ est la loi additive, et le $\cap$ la loi multiplicative.
Pour montrer que $(\mathcal{A}, \Delta)$ est un groupe, voir fichier « groupes ».

1. Montrer que $\mathcal{A}$ est un anneau non intègre et identifier son 0 et son 1.
2. Montrer que $\forall a \in \mathcal{A}, 2a = 0$ et vérifier toutes les autres propriétés du **6.1**.

3. Montrer que $\mathcal{A}(\mathcal{P}(E),\Delta,\cap)$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$ où $n=|E|$ avec les lois terme à terme.

On a la correspondance $+\leftrightarrow\Delta$ et $\times\leftrightarrow\cap$. L'opération $\cup$ correspond à

7.3. Forme applicative

E un ensemble de cardinal n, et $\mathcal{A}$ l'anneau des applications $a: E\to\mathbb{F}_2$ muni du $+$ et du $\times$ de $\mathbb{F}_2$.
On a coïncidence avec le paragraphe précédent.

7.4. Forme « suites »

$\mathcal{A}=(\mathbb{F}_2)^{\mathbb{N}}$, anneau des suites à valeurs dans $\mathbb{Z}/2\mathbb{Z}$ avec $+$ et $\times$ terme à terme;

7.5. Remarques diverses

On a un exemple d'anneau, fini ou infini suivant $|E|$, mais n'ayant qu'un seul élément inversible (le 1 ou le E ou le $a: x\in E\mapsto 1$).

7.6. Idéaux

à mettre en forme...

Si I est un idéal de $\mathcal{A}$, alors :

1. I stable par Δ et $\cap$ donc par $\cup$.
2. Soit $X\in I$, alors tout $Y\subset X$ est aussi dans I puisque $Y=Y\cap X$.
3. Si E est fini :
   a. si $B=\bigcup_{u\in I} u$ alors $I=\mathcal{P}(B)$.
   b. Réciproquement, les $\mathcal{P}(B)$ avec $B\subset E$ sont idéaux.

   Ainsi, si E est fini, $\mathcal{A}$ est principal.
4. Si E est infini :
   a. $I=\{\text{parties finies de } E\}$ est un idéal qui n'est pas de la forme $\mathcal{P}(B)$ et n'est pas principal car si $I=\langle F\rangle$ avec $F\subsetneq E$, alors soit $f\notin F$, on a $\{f\}\in I$ mais $\{f\}\notin\langle F\rangle$.

   Ainsi, si E est infini, $\mathcal{A}$ n'est pas principal.

$\mathcal{A}(\mathcal{P}(\mathbb{Z}),\Delta,\cap)$ principal (prendre l'union de tous les éléments d'un idéal...) ;
on peut travailler d'abord sur l'exemple $\mathcal{I}=<2\mathbb{Z},3\mathbb{Z}>$;
Soit $\mathcal{I}$ un idéal de $\mathcal{A}$, alors $\mathcal{I}$ est stable par Δ et $\cap$ donc par $\cup$.

oit $\mathcal{A}=(\mathcal{P}(E),\Delta,\cap)$:

1. prouver que les idéaux de $\mathcal{A}$ sont stables par union ;
2. si un idéal contient E c'est l'anneau tout entier ;
3. prouver que les $(\mathcal{P}(F),\Delta,\cap)$, avec $\mathcal{F}$ sous-ensemble de E, sont des idéaux de $\mathcal{A}$;

8. Anneaux-quotient

8.1. Structure d'anneau de $\mathcal{A}/\mathcal{I}$, généralités

Si $\mathcal{I}$ idéal de $\mathcal{A}$, on peut définir $\mathcal{A}/\mathcal{I}$ par :

$$\dot{x}=\dot{y}\Leftrightarrow x-y\in\mathcal{I}.$$

Le fait que $\mathcal{I}$ soit un idéal permet $\dot{x}=\dot{y}\Rightarrow\dot{a}\dot{x}=\dot{a}\dot{y}$ d'où la structure d'anneau sur $\mathcal{A}/\mathcal{I}$.

On a la surjection canonique $p: \left\{ \begin{array}{l} \mathcal{A} \to \mathcal{A}/\mathcal{I} \\ a \mapsto \dot{a} \end{array} \right.$.

1. Montrer qu'il y a bijection entre les idéaux de $\mathcal{A}/\mathcal{I}$ et les idéaux de $\mathcal{A}$ contenant $\mathcal{I}$.
   Utiliser p^{-1}.
2. Montrer que $\mathcal{A}/\mathcal{I}$ intègre $\Leftrightarrow$ $\mathcal{I}$ premier.

$$\begin{aligned} \mathcal{A}/\mathcal{I} \text{ intègre} &\Leftrightarrow \forall \dot{a}, \dot{b} \in \mathcal{A}/\mathcal{I}, \dot{a}\dot{b} = \dot{0} \Rightarrow \dot{a} = \dot{0} \text{ ou } \dot{b} = \dot{0} \\ &\Leftrightarrow \forall a, b \in \mathcal{A}, ab \in \mathcal{I} \Rightarrow a \in \mathcal{I} \text{ ou } b \in \mathcal{I} \\ &\Leftrightarrow \mathcal{I} \text{ premier.} \end{aligned}$$

3. Montrer que $\mathcal{A}/\mathcal{I}$ corps $\Leftrightarrow$ $\mathcal{I}$ maximal.
   $\Rightarrow$ si $\mathcal{A}/\mathcal{I}$ est un corps, alors soit $\mathcal{J} \supset \mathcal{I}$ un autre idéal, soit $j \in \mathcal{J} \setminus \mathcal{I}$, soit $k \in \mathcal{A}$ tel que $\dot{j}\dot{k} = \dot{1}$, on a alors un $i \in \mathcal{I}$ tel que $jk - i = 1$ or $jk - i \in \mathcal{J}$. On a montré que $\mathcal{J} = \mathcal{A}$.
   $\Leftarrow$ si $\mathcal{I}$ maximal, alors soit $a \in \mathcal{A} \setminus \mathcal{I}$, on a $(a) + \mathcal{I} = \mathcal{A}$ donc $\exists b \in \mathcal{A}, i \in \mathcal{I} / ab + i = 1$ ce qui veut dire $\dot{a}\dot{b} = \dot{1}$. On a montré que tout $\dot{a} \neq \dot{0}$ est inversible dans $\mathcal{A}/\mathcal{I}$.