Anneaux et corps

- **Anneau:** Ensemble A muni de 2 lois x et + tel que

1) A+ est un groupe commutatif (élément neutre noté 0 ou 0_A)
2) la loi x est associative et possède un élément neutre (noté 1 ou 1_A)
3) la loi x est distributive par rapport à la loi + soit x(y+z)=xy+xz et (x+y)z = xz+yz.

Si de plus la loi x est commutative on dit que l'anneau est commutatif.

- La loi x est également distributive par rapport à la soustraction x(y-z)=xy-xz et (x-y)z = xz-yz.

On a aussi 0a=a0=0 , a(–b)= –ab , (–a)b = –ab, (–1)a = –a. Par convention $a^0 = 1$.

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de + et x sont des anneaux.
- Si F(X,A) ensemble des applications d'un ensemble X dans un anneau A muni de + (f+g)(x)=f(x)+g(x) et de x (fg)(x)=f(x)g(x) est un anneau (commutatif si A l'est aussi).
- $\mathbb{M}_n(A)$ ensemble des matrices carrées d'ordre n à coefficients dans un anneau A est un anneau.
- L'ensemble A[X] des polynômes en X à coefficients dans un anneau A est un anneau.
- **Produit direct d'anneaux** si A1,….,An sont des anneaux le produit cartésien A1XA2X…..XAn muni de l'addition et de la multiplication canoniques sur les ensembles produits est un anneau.

- **Sous anneaux :** On dit qu'un sous ensemble B d'un anneau A est un sous anneau si

1) B est stable par x et + (tout composé se trouve dans B) **2)** B a une structure d'anneau (1∈B)

- $\mathbb{Z}$ sous anneau de $\mathbb{R}$ lui-même sous anneau de $\mathbb{C}$
- L'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ est un sous anneau de F($\mathbb{R}$,$\mathbb{R}$).
- {a + ib | a,b ∈$\mathbb{Z}$ } est un sous anneau de $\mathbb{C}$ appelé anneau de Gauss.

- **Idéaux :** On dit qu'un sous ensemble B d'un anneau <u>commutatif</u> A est un idéal si

1) B est un sous groupe de (A,+) **2)** Tout x ∈B et y ∈A le produit xy ∈B

- Les idéaux de $\mathbb{Z}$ sont les n$\mathbb{Z}$.
- Soient deux ensembles tels que Y⊂ X, le sous ensemble de F(X,$\mathbb{R}$) formé par les applications qui s'annulent sur Y est un idéal de F(X,$\mathbb{R}$).
- soit a ∈A {ax |x ∈A } est **l'idéal principal** engendré par a. On le note **aA** ou **(a)** (n$\mathbb{Z}$ si A=$\mathbb{Z}$)
- $\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$, ni de $\mathbb{R}$, ni de $\mathbb{C}$
- Les idéaux d'un anneau produit commutatif AXB sont le IXJ avec I idéal de A et J idéal de B.

- **Anneau quotient d'un anneau commutatif**. Un idéal I est un sous groupe de (A,+).

On peut définir sur A une relation d'équivalence x $\mathcal{R}$ y ⇔ x – y ∈I ce qui définit un ensemble quotient A/I dans lequel la loi de composition interne est héritée de + par $\bar{x} + \bar{y} = \overline{x+y}$.
Dans A/I on peut aussi définir le produit de 2 classes par $\bar{x}\,\bar{y} = \overline{xy}$ et on vérifie que le résultat est indépendant du choix des représentants des 2 classes.
Des lors, A/I a une structure d'anneau, on l'appelle anneau quotient A/I

- $\mathbb{Z}$/n$\mathbb{Z}$ est un anneau quotient dont les lois sont définies par $\bar{x} + \bar{y} = \overline{x+y}$ et $\bar{x}\,\bar{y} = \overline{xy}$

- **Groupe des éléments inversibles:** a est inversible si ∃ b tels que ab=ba=1. b est noté a^{-1}.

On note A^* l'ensemble des éléments inversibles. (A^* , x) est un groupe. $\mathbb{Z}^*$ ={-1;+1}

- Si A et B sont des anneaux, on a $(AXB)^* = A^*XB^*$ et si A et B finis $card((AXB)^*)=card(A^*)\,card(B^*)$.
- Si A commutatif et I idéal de A , on a I=A ⇔ il existe un élément inversible dans I

● **Corps** l'anneau A est un corps si et seulement si 1 ≠ 0 et toute élément ≠ 0 est inversible: **$A^{*}= A- \{0\}$**

● $\mathbb{Q}$, $\mathbb{R}$,$\mathbb{C}$ sont des corps ● Tout idéal du corps A est égal à A ou à {0}.

● **Sous corps:** On appelle sous corps de K tout anneau L de K qui est un corps.
K est le **surcorps** de L.

● **Anneau intègre** A est intègre si A est commutatif, non réduit à 0 (1≠0) et pour tous a,b de A on a:
$a\neq 0 \; et \; b\neq 0 \Rightarrow ab\neq 0$.

● Tout anneau A fini intègre est un corps.
En effet f:x → ax avec a ≠0 est injective car ax=ay avec x ≠y impliquerait a(x-y)=0 (non intégrité). Par ailleurs card({ax}) = card(A) donc f surjective. Pour tout a ≠ 0 il existe donc x tel que ax = 1 et a est inversible.

● Si n ≥2 et non premier $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

● Si A et B sont intègres, le produit A X B ne l'est pas puisque (0,1)(1,0)=(0,0)

● F($\mathbb{R}$,$\mathbb{R}$) n'est pas intègre: (f(x)=0 sur $\mathbb{R}^-$, f(x)≠0 sur$\mathbb{R}^{*+}$).(f(x)≠0 sur $\mathbb{R}^-$, f(x)=0 sur$\mathbb{R}^{*+}$) = 0

● **Homomorphisme d'anneaux**: f de A dans B vérifiant
1) f(a+b)=f(a)+f(b) **2)** f(xy)=f(x)f(y) **3)** $f(1_A)=f(1_B)$

● Pour n≥ 1 la surjection canonique de $\mathbb{Z}$ dans n$\mathbb{Z}$: x → $\overline{x}$ est un homomorphisme

● Soit f homomorphisme de A dans B et A',B' des sous anneaux de ces ensembles.
1) f(A') est un sous anneau de B **2)** f^{-1}(B') est un sous anneau de A

● Si de plus A et B sont commutatifs et J idéal de B alors f^{-1}(J) est un idéal de A
Par contre, si I est un idéal de A , en général f(I) n'est pas un idéal.

● Le noyau de f est ker(f)= $\{x\in A \mid f(x)=0_B\}$. f(A) est un sous anneau appelé image de f (im(f))

● **Isomorphisme d'anneaux** : c'est un homomorphisme bijectif (On dit que A et B sont isomorphes)

● Si A est commutatif et f un homomorphisme dans B alors ker(f) est un idéal de A et f(A) est isomorphe à A/ker(f). (l'isomorphisme associe $\overline{x}$ et f(x))

● A ne possède pas de sous anneau ≠ A ⇔ A isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec n ≥ 0.

● **Formule de Newton** dans un anneau A on a $(a+b)^n = \sum_0^n C_n^k a^k b^{n-k}$

Exercices

▣ Si dans un anneau A on a pour tout a,b : $(ab)^2=a^2b^2$ montrer que A est commutatif.

▣ Un idéal P d'un A commutatif et dit **premier** si **1)** P ≠A **2)** ∀x,y ∈A on a xy∈P ⇒ x∈P ou y∈P
Quels sont les idéaux premiers de $\mathbb{Z}$?

▣ Montrer que le groupe des inversibles de Z[i] est {-1,1,-i, i} isomorphe à ($\mathbb{Z}/2\mathbb{Z}$)X($\mathbb{Z}/2\mathbb{Z}$), +

▣ Soient x,y∈A | 1 – xy soit inversible. Montrer que 1 – yx est aussi inversible.

▣ Soit l'ensemble X et f∈ F(X,A). Montrer f inversible ⇔ f(X) ⊂ A^{*}

▣ I idéal de A commutatif montrer A/I intègre ⇔ I idéal **premier**

▣ Montrer que A intègre avec un nombre fini d'idéaux est un corps.
(Pour montrer que x non nul est inversible on peut considérer la suite des idéaux principaux (x^n) pour n≥1.)

▣ A et B commutatif et f homomorphisme surjectif de A→B.
Démontrer que si I idéal de A alors f(I) idéal de B.

▣ Soit k un corps, A anneau non nul, f homomorphisme K → A . Montrer que f est injectif.

Résumé

<table>
<tr><th></th><th>loi ╫</th><th>loi ★</th><th>Propriétés</th></tr>
<tr><td>groupe
$\mathbb{Z}$, +
$\mathbb{R}^{+\star}$, x</td><td>associative
élément neutre e
symétrique</td><td></td><td>nx et x^n sont définis selon la notation adoptée
sous groupe H
relation d'équivalence x^{-1}╫ y∈H
classes d'équivalence $\bar{x}$ =x ╫H ∈ G/H</td></tr>
<tr><td rowspan="2">anneau
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$</td><td>associative
élément neutre 0
symétrique</td><td>associative
élément neutre 1</td><td rowspan="2">sous anneaux Dans anneau commutatif, idéal
idéal = sous groupe de A,+
et x∈I et y ∈A xy∈I
aA idéal principal engendré par A
relation d'équivalence x – y ∈I, anneau quotient
les éléments inversibles de ★ forment un groupe
formule de newton valable dans un anneau</td></tr>
<tr><td colspan="2">★ distributive par rapport à ╫</td></tr>
<tr><td rowspan="2">corps
$\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$</td><td>associative
élément neutre 0
symétrique</td><td>associative
élément neutre 1
symétrique si ≠ 0</td><td rowspan="2">Anneau intègre commutatif non réduit à 0 et si x et y non nul, xy n'est pas nul.
Tout anneau intègre fini est un corps</td></tr>
<tr><td colspan="2">★ distributive par rapport à ╫
0 ≠ 1</td></tr>
</table>