Anneaux et Corps

Définition (anneau) : $(A, +, \times)$ est un anneau ssi :
Soit $(A, +)$ un groupe abelien muni d'une 2ème loi de composition interne notée $\times$; $(x, y) \longrightarrow xy$.
qui a les propriétés suivante :

1) La multiplication est associative $(xy)z = x(yz)$
2) . . . — distributive par rapport à l'addition

$$x(y+z) = xy + \cancel{x}z \text{ et } (y+z)x = yx + zx.$$

3) ~~la mu~~ il existe un élément neutre 1 pour la loi $\times$.

$$x1 = 1x = x ;$$

si de plus la multiplication est commutative
alors i.e $xy = yx$, A est commutatif

Remarques : si A est un anneau :

$$x0 = 0x = 0 , \forall x \in A$$

preuve :

$$x = (1+0)x = 1x + 0x = x + 0x$$

ou encore

donc : $-x + x = -x + x + 0x$

$$0 = 0x.$$

on montre de même que $x0 = 0$
en écrivant : $x + (-1)x = 1 \cdot x + (-1)x = (1 + (-1))x = 0x = 0$
on obtient $(-1)x = -x$

Exemples : $A = M_n(\mathbb{R})$ est un anneau (non commutatif)

Dans la suite du cours ; tous les anneaux seront supposés commutatifs et $1 \neq 0$

Notion de sous-anneau : Soit A un anneau ;
$B \subset A$ est ~~un sous anneau~~ on dit sous-anneau de A ssi : B est un sous groupe additif de A tel que : $1 \in B$; $\forall x \in B, \forall y \in B$, $xy \in B$

Remarque : un sous-anneau de A est lui même un anneau.

Exemples : 1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux

2) $\mathbb{R}[X]$ est un anneau

3) $\mathbb{Z}[X]$ — — anneau.

4) L'anneau des entiers de Gauss

$\mathbb{Z}[i] = \{ a + bi, a \in \mathbb{Z}, b \in \mathbb{Z} \}$

$\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.

– Multiples, diviseurs ; éléments inversibles.

Définition : A un anneau ; a, b éléments de A.
On dit que a divise b ou que b est un multiple de a

Si : $b = a q$; $q \in A$; on note $a | b$

Un élément $a \in A$ est inversible s'il possède un inverse pour la multiplication i.e.
$\exists\, b \in A$ tel que $ab = 1$; $b = a^{-1}$ (notation).

Remarques : 1) 0 n'est pas inversible ;

2) si $B \subset A$ un sous anneau ;
$a \in B$ peut être inversible dans A sans l'être dans B. par exemple 2 est inversible dans $\mathbb{Q}$ mais ne l'est pas dans $\mathbb{Z}$.

Proposition : Soit A un anneau ; $A^\circ = \{ ~~en~~ a \in A,\ a$ inversible $\}$ est un groupe multiplicatif.

Preuve : Soit $a \in A^\circ$, $b \in A^\circ$, $(ab)^{-1} = b^{-1} a^{-1}$ ~~E~~, donc $ab \in A^\circ$; $1 \in A^\circ$; $a \in A^\circ$, a^{-1} est inversible donc $a^{-1} \in A$.

Exemple : 1) $A = \mathbb{Z}$, $\mathbb{Z}^* = \{-1, 1\}$ est bien un groupe.
2) $A = M_n(\mathbb{R})$; $A^\circ = GL_n(\mathbb{R})$ est un groupe.

Proposition : Soient A, B deux anneaux ; $A \times B$ est un anneau ; et $(A \times B)^\circ = A^\circ \times B^*$

$(A\times B, +, \times)$;

$(a,b)+(c,d)=(a+c, b+d)$

$(a,b)\times(c,d)=(ac, bd)$

On vérifie facilement que $A\times B$ est un anneau.

Soit $(a,b)\in A\times B$; $(a,b)\in(A\times B)^*$ ssi

$\exists (x,y)\in A\times B$ tel que $(a,b)(x,y)=(ax,by)=(1,1)$

$\Leftrightarrow$ $\exists (x,y)$ tq : $ax=1$ et $bx=1$

$\Leftrightarrow$ $a\in A^*$ et $b\in B^*$

<u>Définition</u> : Soit A un anneau ; on dit que A est intègre ssi : $xy=0 \Leftrightarrow x=0$ ou $y=0$

<u>Définition</u> : Soit K un anneau, on dit que K est un corps ssi $K^*=K-\{0\}$.

<u>proposition</u> : un corps est un anneau intègre.

<u>preuve</u> : Soit K un corps, $x,y\in K$ tel que : $xy=0$; si $x\neq 0$; x est inversible

donc : $x^{-1}xy=x^{-1}0 \Leftrightarrow y=0$

Réciproquement ($x=0$, $\forall x\in K$).

Exemples : ① $\mathbb{Z}$ est un anneau intègre, $\mathbb{Z}$ n'est pas un corps :

② $A = \mathbb{R}[X]$; $A^* = \{$ polynômes constants non nul$\}$.

③ $A = \mathbb{Z}[i]$; on va chercher ~~A*~~ à déterminer A^*.

Soit $z \in A$; $z = a + bi$.

$|z|^2 = a^2 + b^2$ est un entier positif.

~~Considérons~~ Soit $z \in A^*$, $\exists z' \in A^*$, tel que

$z z' = 1$; ou encore

$|z z'| = |z||z'| = 1$, on en déduit

que $|z|^2 = |z'|^2 = 1$ ce qui donne :

$z \in \{1, -1, i, -i\}$, on vérifie

que ces élément sont tous inversible.

④ Montrons que dans $\mathbb{Z}[i]$: $2+3i \mid 5+i$

$$\frac{5+i}{2+3i} = \frac{13 - 13i}{13} = 1 - i$$

autrement dit : $(5+i) = (2+3i)(1-i)$ dans

$5+i$ est un multiple de $2+3i$ et de $1-i$ dans $\mathbb{Z}[i]$

<u>Morphisme</u> : on dit qu'une application $f : A \longrightarrow B$ est un morphisme d'anneau

ssi : $\forall (x,y) \in A^2$;

$$f(x+y) = f(x+y).$$

$$f(xy) = f(x) f(y)$$

$$f(1_A) = 1_B .$$

<u>Exemple</u> :
$$\mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]$$
$$z \longrightarrow \bar{z}$$
est un morphisme d'anneau.

<u>proposition</u> : Soit $f : A \longrightarrow B$ un morphisme d'anneau ; Soit $x \in A^*$; $f(x) \in B^*$ et

$$(f(x))^{-1} = f(x^{-1}).$$

la restriction de $f|_{A^*} : A^* \longrightarrow B^*$ est un morphisme de groupe.

<u>preuve</u> : Soit $x \in A^*$, $f(xx^{-1}) = f(1_A) = 1_B$
$$= f(x) f(x^{-1}) = 1_B$$

<u>Définition</u> Soit A un anneau ; un idéal de A est un sous-groupe I additif de A et qui a la propriété suivante : $\forall a \in I$, $\forall x \in A$, $xa \in I$

Exemple : ① $\{0\}$ est un ideal de A

② A - - - de A.

③ Soit $a \in A$; $aA = \{ax, x \in A\}$ est un ideal de A ; c'est l'ideal engendré par a. {les multiples de a est un ideal de A ; comme $n\mathbb{Z}$ est un ideal de $\mathbb{Z}$.

definition : Soit A un anneau, I un ideal de A ; On dit que I est un ideal principal si $I = aA = (a)$.

proposition : Soit $f : A \to B$ un morphisme d'anneau de noyau de f est un ideal de A, l'image de f est un sous-anneau de B

preuve : Ker f est un sous-groupe additif de A (déjà vu !)

Soit $a \in \operatorname{Ker} f$, $\forall x \in A$; $f(ax) = f(a) f(x) = 0 \cdot f(x) = 0$

donc $ax \in \operatorname{Ker} f$.

Im f est un sous groupe additif de B qui contient en plus $1_B = f(1_A)$.

$u = f(x)$, $v = f(y)$ élements de Im f ;

$uv = f(xy) \in \operatorname{Im} f$.

Exercice : Soit A ~~un corps~~ ; un anneau ;

~~$a \in$~~ I un idéal de A ;

Supposons que $a \in I$ est inversible alors :

$I = A$;

preuve : $a \in I$, $aa^{-1} = 1 \in I$ (I un idéal).

$\forall\, b \in A$; $b = b \times 1 \in I \Rightarrow A \subset I$ et

par suite $A = I$.

Comme conséquence ~~on~~ On a :

(I) (1) Soit A un anneau ; A est un corps ssi

les idéaux de A sont $\{0\}$ et A.

(2) Soit K un corps, B un anneau.

Tout morphisme d'anneau de $K \longrightarrow B$

est injectif.

preuve : (1) ; si A un corps ; tout idéal est soit

$\{0\}$, ~~soit~~ A. (~~si $a \in I$, et a inv~~

Réciproquement : Soit $a \in A$; $a \neq 0$; aA est un

idéal de A non réduit à $\{0\}$, donc : $aA = A$

par suite $1 \in aA$; ~~et donc $aA =$~~, il existe

donc $a' \in A$ tel $1 = aa'$ i.e. $a \in A^*$

(2) $\operatorname{Ker} f$ est un idéal de K, différent de K (car $f(1_A) = 1_B$)

$\operatorname{Ker} f = \{0\}$ et f est donc injectif.

L'anneau $\mathbb{Z}/n\mathbb{Z}$.

$n \geq 2$; $\mathbb{Z}/n\mathbb{Z}$ est muni de deux lois :

$+$, $\bar{a} + \bar{b} = \overline{a+b}$

$\times$ $\bar{a} \cdot \bar{b} = \overline{ab}$

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif

<u>proposition</u> : $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$ ($\bar{k}$ inversible)

ssi : $(k, n) = 1$

<u>preuve</u> : $(k, n) = 1 \iff \exists\, u, v \in \mathbb{Z}^2$ tq :

$ku + nv = 1$ (th de Bezout)

$\iff \exists\, u \in \mathbb{Z}$; $ku \equiv 1\ [n]$

$\iff \exists\, u \in \mathbb{Z}$; $\bar{k}\,\bar{u} = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$

$\iff \bar{k}$ inversible $\left((\bar{k})^{-1} = \bar{u}\right)$.

<u>Exemple</u> : $\mathbb{Z}/20\mathbb{Z}$; les inversibles sont :

$\bar{1}, \bar{3}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}$

$(\mathbb{Z}/20\mathbb{Z})^* = \{\pm\bar{1}, \pm\bar{3}, \pm\bar{7}, \pm\bar{9}\}$.

$\bar{9}^{-1}$? on cherche une relation de Bezout :

$9 \times 9 - 4 \times 20 = 1$, d'où $\bar{9}^{-1} = \bar{9}$

<u>Remarque</u> : $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^* \iff \bar{a}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ (additif)

<u>proposition</u>.. Soit p, q deux entiers premiers entre eux, les deux ~~anneaux~~ groupes $(\mathbb{Z}/pq\mathbb{Z})^*$ et $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ sont isomorphes

[on reviendra plus tard].

<u>Fonction d'Euler</u>.

Soit $n \geq 2$ un entier. On note $\varphi(n)$ le nombre d'entiers k ; $1 \leq k \leq n$ tel que $(k, n) = 1$. φ s'appelle la fonction d'euler.

<u>proposition</u> :

(a) Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est d'ordre $\varphi(n)$
[contient exactement $\varphi(n)$ éléments)

(b) Pour tout entier a premier à n ;
$a^{\varphi(n)} = 1\ [n]$.

(c) Soit G un groupe cyclique d'ordre n.
G possède $\varphi(n)$ generateurs.

<u>preuve</u> : (a) proposition precedente.
(b). $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe fini d'ordre $\varphi(n)$;

pour tout $a \in \mathbb{Z}$, $(a,n)=1$;

$\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ et $\bar{a}^{\varphi(n)} = 1$ ou encore

$a^{\varphi(n)} \equiv 1\ [n]$.

c) $G = \langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$.

ordre $a^k = \dfrac{n}{pgcd(k,n)}$; a^k est générateur si

ordre (a^k) = ordre $G = n \iff pgcd(k,n)=1$.

le nombre de (a^k) générateur est $\varphi(n)$!

<u>Exemple</u> : $|(\mathbb{Z}/20\mathbb{Z})^*| = 8$; $\varphi(20) = 8$.

$\varphi(9) = 6$; $\varphi(5) = 4$, $\varphi(10) = 4$.

Calcule de $\varphi(n)$; On a la proposition suivante.

<u>proposition</u> : Soit p un nombre premier ;

a) $\varphi(p) = p-1$.

b) $\varphi(p^r) = p^r - p^{r-1}$

c) si $(n,m)=1$, $\varphi(nm) = \varphi(n)\varphi(m)$

<u>preuve</u> : ⓐ Soit p un nombre premier, tout entier $1 \leq k \leq p-1$ est premier à p ; d'où $\varphi(p) = p-1$

(5) : Soit $r \geq 2$; des entiers premiers à p^r sont ceux qui ne sont pas multiples de p.
On va compter les multiples de p compris entre 1 et p^r : ce sont donc les kp ; avec $1 \leq k \leq p^{r-1}$, il y a donc p^{r-1} multiples de p compris entre 1 et p^r. On en déduit donc que

$$\varphi(p^r) = p^r - p^{r-1}$$

(c) $(\mathbb{Z}/nm\mathbb{Z})^*$ et $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ sont isomorphes

Ces deux ensembles ont même cardinal.

$\text{Card}(\mathbb{Z}/nm\mathbb{Z})^* = \varphi(nm)$.

$\text{Card}(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$

$\text{Card}(\mathbb{Z}/m\mathbb{Z})^* = \varphi(m)$.

On en déduit que $\varphi(nm) = \varphi(n)\varphi(m)$

Exemples : $\varphi(63)$: On écrit $63 = 3^2 \times 7$ (décomposition en facteurs premiers) ;

$$\varphi(63) = \varphi(3^2) \times \varphi(7) = (3^2 - 3) \times (7-1) = 6 \times 6 = 36$$

$$\varphi(20) = \varphi(2^2 \times 5) = \varphi(2^2) \times \varphi(5) = (2^2 - 2) \times (5-1) = 2 \times 4 = 8.$$

On vu que $\mathbb{Z}/n\mathbb{Z}$ est un anneau, est-il intègre ? un corps :

Commençons par le cas $n = p$ nombre premier.

On a : $|\mathbb{Z}/n\mathbb{Z}| = n$; $|(\mathbb{Z}/n\mathbb{Z})^{*}| = \varphi(n) = n-1$ (n premier)

autrement dit : $(\mathbb{Z}/n\mathbb{Z})^{*} = \mathbb{Z}/n\mathbb{Z} - \{0\}$, on conclut que $(\mathbb{Z}/n\mathbb{Z})$ est un corps (p premier). On le note

$\mathbb{F}_p$

Exemple $\mathbb{F}_2 = \{\dot{0}, \dot{1}\}$; $\mathbb{F}_3 = \{\bar{0}, \pm\bar{1}\}$; $\mathbb{F}_5 = \{\bar{0}, \pm 1, \pm 2\}$

Regardons ce qui se passe si n n'est pas premier : par exemple $n = pq$; : $\bar{p}$ et $\bar{q}$ sont différents de $\bar{0}$; mais $\bar{p}\bar{q} = \bar{0}$; $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre

On vient de montrer la proposition suivante :

<u>proposition</u> : $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ est intègre $\Leftrightarrow$ n est premier.

<u>Remarque</u> : dans $\mathbb{F}_p$; on a.

a) $pa = 0$ pour tout $a \in \mathbb{F}_p$

b) si $a \neq 0$; $a^{p-1} = 1$ (~~th~~ Euler).

b) $\Rightarrow$ Soit n un entier nat ; p un nombre premier ; $(n,p) = 1$

$n^{p-1} \equiv 1\ [p]$ (13)

ou plus généralement :

Soit n un entier, p un nombre premier.

$n^p \equiv n \, [p]$. (petit th de Fermat).

Application :

① Soit p un nombre premier.

$u_n = 3^{n+p} - 3^{n+1} \equiv 0 \, [p]$ pour tout n :

On a :

$3^p \equiv 3 \, [p]$;

$u_n = 3^n \cdot 3^p - 3^n \cdot 3 \equiv 3^n \cdot 3 - 3^n \cdot 3 \equiv 0 \, [p]$

② 26 divise $n^{13} - n$, pour tout entier n.

$p = 2$; $n^2 \equiv n \, [2]$; $n^{13} - n \equiv n^{4 \times 3} \cdot n - n \, [2]$

$n^4 \equiv n^2 \equiv n \, [2]$

$\equiv n^3 \cdot n - n \equiv [2]$

$\equiv n^4 - n \equiv [2]$

$\equiv 0 \, [2]$

$p = 13$; $n^{13} \equiv n \, [13]$.

donc $2 \mid n^{13} - n$ et $13 \mid n^{13} - n$.

$(2, 13) = 1 \Rightarrow 26 \mid n^{13} - n$.

(3) $5^{1000} \equiv 5^{6 \times 166 + 4} \equiv 1 \times 5^4 \equiv 2 \, [7]$