Anneaux

Revoir le vocabulaire : intégrité, diviseur à gauche, à droite
; régulier à gauche, à droite
; inversible — —
; nilpotents.

I Idéaux d'un anneau unitaire

Not : $(A,+,\cdot)$ anneau unitaire

Déf : On dit qu'une partie I de A est un idéal à gauche de A lorsque : I est un sous groupe de A pour $+$

$$\forall \lambda \in A \ \forall a \in I : \lambda a \in I$$: stabilité avec $\lambda \in A$

Ex : $\{0\}$, A.

Ex : Si $a \in A$ $\{\mu a \mid \mu \in A\} = \langle a \rangle$ est un idéal à gauche appelé idéal à gauche engendré par a

Propriétés : 1) Si I est un idéal de A, $I = A \Leftrightarrow 1_A \in I$
$\Rightarrow$ clair $\Leftarrow$ aussi

Conséquence : $\underbrace{I \cap U(A)}_{\neq \emptyset} \Rightarrow I = A$ ~~...~~

2) Une intersection d'idéaux (à gauche) est un idéal

3) Si I et J sont deux idéaux : $I + J$ aussi

Ex Soit A un a.c.u Vérifier que
A corps $\Leftrightarrow$ les seuls idéaux de A sont $\{0\}$ et A
2) Idéaux de $\mathbb{R} \times \mathbb{R}$

① ...
② idéaux de $\mathbb{R}\times\mathbb{R}$: $\{0\}$, ou $\mathbb{R}\times\mathbb{R}$, $\mathbb{R}\times\{0\}$, $\mathbb{R}\times\mathbb{R}$

Obs : Soit I un idéal de $\mathbb{R}\times\mathbb{R}$
i) Si I . — — — — évident

Idéal engendré : A est un acc
Th-déf : Si X est une partie de A, $\bigcap I = \mathcal{J}(X)$ est un idéal de A, appelé idéal engendré par X $\begin{cases} I \text{ idéal de } A \\ X \subset I \end{cases}$

Ex $I(\emptyset = \{0\})$, $I(\{1\}) = A$

Idéal principal $I(\{a\}) = \langle a \rangle = \{\lambda a \mid \lambda \in A\}$
Description : $I(X) = \{x \in A \mid \exists p \in \mathbb{N}\ \exists (x_1, \dots x_p) \in X^p\ \exists (\lambda_1 \dots \lambda_p) \in A^p\ x = \sum_{i=1}^{p} \lambda_i x_i\}$

en effet $\mathcal{J}$ est un idéal, $X \subset \mathcal{J}$ et tout idéal de A contenant X contient $\mathcal{J}$.
RM : $\mathcal{J}(X) = A \iff \exists (x_1, \dots, x_p) \in X^p\ \exists (\lambda_1, \dots, \lambda_p)\ \sum_{1}^{p} \lambda_i x_i = 1$

Idéal et morphisme :
Prop : Soit $f : A \to B$ un morphisme d'anneaux $(f(1_A) = 1_B)$

1) $\operatorname{Ker} f$ est un idéal de A, 2) si $\mathcal{J}$ est un idéal de B, $f^{-1}(\mathcal{J})$ est un idéal de A

⚠ Image directe : $\mathbb{Z} \to \mathbb{Q}$

Exercices : un idéal I de A est dit premier lorsque $\forall x, y \in A^2\ xy \in I \Rightarrow x \in I$ ou $y \in I$
ex : $\{0\}$ est premier $\iff A$ est intègre.
① trouver les idéaux premiers de $\mathbb{Z}$

Soit I un idéal de $\mathbb{Z}$ (de la forme $n\mathbb{Z}$) $\neq \{0\}$

$n=1$ OK ; $n\geq 2$: n premier OK
n non premier notons $n=pq$: $\sigma p \in pq\mathbb{Z}$
$q \notin n\mathbb{Z}$
$p \notin n\mathbb{Z}$

Voc : Un idéal de A, I, est dit maximal lorsque $I \neq A$, $\forall J$ idéal de A, $I \subset J \Rightarrow I = J$ ou $J = A$

Exo : $\{0\}$ maximal $\Leftrightarrow$ A est un corps

Exo idéaux maximaux de $\mathbb{Z}$: $p\mathbb{Z}$, p premier

Exo : Un idéal maximal I est premier

Soit $x,y \in A$ tq $xy \in I$

On suppose $x \notin I$ Mq $y \in I$

Alors $I \subsetneq I + \langle x \rangle$ donc par maximalité $I + \langle x \rangle = A$

ie $\exists \lambda \in A$ $\exists a \in I$ tq $a + \lambda x = 1 \Rightarrow \underbrace{ay}_{\in I} + \underbrace{\lambda xy}_{\in I} = \underbrace{y}_{\in I}$

Ex pers : Soit $\mathbb{K}$ un CC. On suppose que l'on possède un sous anneau A de $\mathbb{K}$ tq $\forall x \in \mathbb{K} \setminus \{0\}$ $x \in A$ ou $x^{-1} \in A$
Soit $I = \{a \in A \mid a = 0$ ou $a^{-1} \notin A\}$. Mq I est l'unique idéal maximal de A.

II Divisibilité :

Ici, A est un acu INTÈGRE

Déf Soit $(a,b) \in A^2$. On dit que a/b lorsque $\exists c \in A : b = ac$

Ex Tout $a \in A$ divise 0

$a | 1 \iff a \in U(A)$

Props : 1) Si a/b et $a \neq 0$ l'él $c \in A$ tq $ac = b$ est unique.

2) Si a/b et b/c alors a/c

Voc : On dit que a et b sont associé si $\exists u \in U(A)$ tq $b = au$
$(U(A), \cdot)$ est un groupe, c'est une relation d'équivalence avec $\bar{0} = \{0\}$, $\bar{1} = U(A)$

Prop. Soit $(a,b) \in A^2$; a et b sont associés ssi a/b et b/a, il vient

D/ Si $a = 0$ ou $b = 0$ OK. Si $ab \neq 0$ (intégrité de A)
il vient $b = ac$ / $a = bc'$ donc $a = a(cc')$ et $a \neq 0 \Rightarrow cc' = 1$

Déf : Soit $(a,b) \in A \setminus \{0,0\}$. On dit que $d \in A$ est un pgcd de (a,b) lorsque $\forall c \in A$, $c | a$ et $c | b \iff c | d$

Prop Si d et d' sont deux pgcd de (a,b), alors d et d' sont associés
En effet par déf $d' | d$ et $d | d'$.

III Anneaux principaux

A) Généralités

Déf : On dit que l'acu A est principal lorsque A est intègre et que tout idéal de A est principal

Ex 1) $\mathbb{Z}$

2) $\mathbb{K}[X]$ En effet, soit I un idéal de $\mathbb{K}[X]$, $I \neq \{0\}$

Soit $P \in I$ de degré minimal, il vient $\langle P \rangle \subset I$
et si $B \in I$, on a $B = PQ + R$ où $\deg R < \deg P$

avec de plus avec de plus $B - PQ = R \in I$

$R = 0$, $B \in \langle P \rangle$, $\langle P \rangle = I$

Δ $\mathbb{Z}[X]$ n'est pas principal. Soit $I = \langle 2 \rangle + \langle X \rangle$

Par l'abs $I = \langle P \rangle$, où $P \in \mathbb{Z}[X]$

alors $2 \in \langle P \rangle$ $2 = PQ$ donc P = cste $P = 1$ $I = \mathbb{Z}[X]$

Ceci est impossible car si $B \in I$, $B(0)$ est pair
$P = 2$ alors $2 | X$, abs.

B) Arithmétique des anneaux principaux

Dans tout ce qui suit, A est un anneau principal.

Prop : Soit $(a, b) \in A^2$, Alors $a | b \Leftrightarrow \langle b \rangle \subset \langle a \rangle$ } inversement l'ordre

D/ Si $b = ac$ alors $b \in \langle a \rangle$ donc $\langle b \rangle \subset \langle a \rangle$

Si ~~$\langle b \rangle \subset \langle a \rangle$~~ $b = ac$ il vient $b \in \langle a \rangle$ donc $\langle b \rangle \subset \langle a \rangle$
Si $\langle b \rangle \subset \langle a \rangle$ il vient $b \in \langle a \rangle$, d'où $c \in A$, $b = ac$

Th Soit $(a, b) \in A^2 \setminus (0, 0)$. Alors (a, b) possède un pgcd.

D/ Soit $I = \langle a \rangle + \langle b \rangle = \{\lambda a + \mu b \mid (\lambda, \mu) \in A^2\}$ ($I \neq \{0\}$)
A étant principal, il existe $d \in A \setminus \{0\}$ tq $\langle a \rangle + \langle b \rangle = \langle d \rangle$
* $\langle a \rangle \subset \langle d \rangle$ et $\langle b \rangle \subset \langle d \rangle \Rightarrow d | a$ et $d | b$
(si $c | d$ alors $c | a$ et $c | b$)

** Si $c | a$ et $c | b$ il vient $\langle a \rangle \subset \langle c \rangle$ et $\langle b \rangle \subset \langle c \rangle$, donc
$\langle a \rangle + \langle b \rangle \subset \langle c \rangle$, soit $\langle d \rangle \subset \langle c \rangle$ i.e. $c | d$

pgcd $(a,b) = \{$ associé de $d\}$ | choix de $\mathbb{Z}$: positif
choix de $\mathbb{K}[X]$: normalisé

RMI | $d \in \langle a \rangle + \langle b \rangle$ et donc $\exists (u,v) \in A^2, d = au + bv$.

Pommelet : on se fait à pgcd avec des idéaux dans les anneaux ce qui peut les servir

Th - déf : Soit $(a,b) \in A^2 \setminus \{(0,0)\}$ [Tout pgcd de (a,b) est inversible

$\Leftrightarrow \exists (u,v) \in A^2, au + bv = 1$ on dit alors que a et b sont premiers entre eux, et on note $a \wedge b = 1$

$\Rightarrow$ déjà vu $\Leftarrow$ $1 \in \langle a \rangle + \langle b \rangle \Rightarrow \langle a \rangle + \langle b \rangle = A = \langle 1 \rangle$
$\Rightarrow 1$ est un pgcd de a et b

Formulation équivalente : tout diviseur commun à a et b est inversible.

Prop. 1) Si $\lambda \in A \setminus \{0\}$ et si d est un pgcd de $(a,b) \neq (0,0)$
λd est un pgcd de $(\lambda a, \lambda b)$

D/ $\langle \lambda a \rangle + \langle \lambda b \rangle = \lambda (\langle a \rangle + \langle b \rangle) = \lambda \langle d \rangle = \langle \lambda d \rangle$

2) Soit $(a,b) \in A^2 \setminus \{(0,0)\}$ d un pgcd de a et de b, $a = da'$ et $b = db'$ alors $a' \wedge b' = 1$

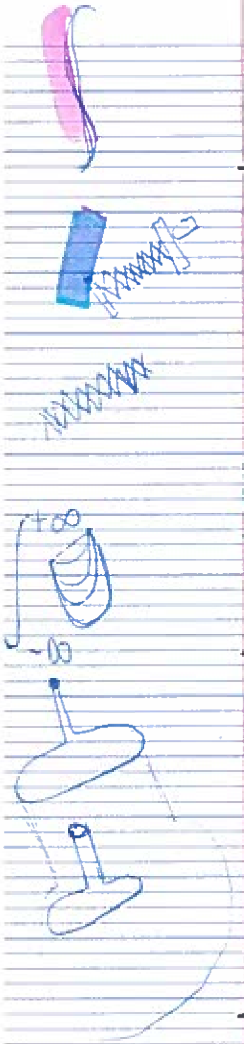
D/ $au + bv = d \Rightarrow d(a'u + b'v) = d \Rightarrow a'u + b'v = 1$
$d \neq 0$
A intègre

3) $\left.\begin{array}{l} a \wedge b = 1 \\ a \wedge c = 1 \end{array}\right\} \Rightarrow a \wedge bc = 1$

On part de $\left.\begin{array}{l} au + bv = 1 \\ au' + cv' = 1 \end{array}\right\}$ produit $a(auu' + ucv' + u'bv) + bc(vv') = 1$

① GAUSS Soit $a,b,c \in A\setminus\{0\}$, si $a | bc$ et $a \wedge b = 1$ alors $a|c$

D/ On part de $au+bv=1$ d'où $\underbrace{auc+\overbrace{bvc}^{a\,v(bc)}}_{a \text{ divise}}=c$



C) Elément irréductible:

Déf Un élément p de $A\setminus\{0\}$ est dit irréductible lorsque p n'est pas inversible ~~lorsque~~ et que $\forall a \in A$, $a|p \Rightarrow a$ inversible ou bien a et p associés

Th Soit $(a,p) \in (A\setminus\{0\})^2$ avec p irréductible

① $p|a$ ou bien $a\wedge b=1$

② Soit $b\in A$, $p|ab \Rightarrow p|a$ ou $p|b$

D/ Soit d un pgcd de (a,p)

Alors $d|a$ et $d|p$, si d est inversible, $a\wedge p=1$

Si d n'est pas inversible, comme p est irréductible, d et p sont associés donc p $d=pu$ avec u inversible
$p=du^{-1}$ et $p|a$

② GAUSS si $p\nmid a$ on a $p\wedge a=1$ or $p|ab$ et gauss donc $p|b$

Conséquence: si $p_1,\dots,p_r,q_1,\dots,q_s$ sont des irréductibles 2 à 2 non associés, alors $p_r\wedge q_j=1$ et $\left.\begin{array}{l} p_1\wedge q_1\dots q_s=1 \\ p_r\wedge q_1\dots q_s=1\end{array}\right\}$ $p_1\dots p_r\wedge q_1\dots q_s=1$

Th Soit $a \in A \setminus \{0\}$
① Il existe $u \in U(A)$, $r \in \mathbb{N}$, $p_1 \dots p_r$ irréductibles tq $a = u p_1 \dots p_r$
② Si de plus $a = v q_1 \dots q_s$, q_i irréd, alors $r = s$ et $\exists \sigma \in S(⟦1, r⟧)$
$\forall i \in ⟦1, r⟧$ $p_{\sigma(i)}$ associée à q_i

D/ Existence $A = \mathbb{Z}$ par récurrence sur $|a|$. Si a n'est pas irréductible le plus petit diviseur $p > 1$ de a l'est, on applique q rec (H) à $\frac{|a|}{p}$

Unicité : rec sur $r + s$, $r = s = 1$ $up = uq$: $p/q \Rightarrow q$ et p associés

Si $u p_1 \dots p_r = v q_1 \dots q_s$ avec $r, s \geq 1$

Si $\forall j$, p_1 non associé à q_j $p_1 \wedge q_j = 1$ donc $p_1 \wedge q_1 \dots q_s = 1$ abs

Par ex : p_1 associé à q_1 on simplifie $u p_2 \dots p_r = u' q_2 \dots q_s$ etc

Complément hors général :

Def Un anneau c. n A est dit noetherien si toute suite croissante (I_n) d'idéaux est stationnaire

Prop Si A est principal, il est noetherien

D/ Soit (I_n) une suite croissante d'idéaux de A. $I = \bigcup_{n \in \mathbb{N}} I_n$ est alors un idéal de A. Si $(a, b) \in I^2$ il existe $m \in \mathbb{N}$ tq $a \in I_m$, $n \in \mathbb{N}$, $b \in I_n$. On $I_m \subset I_{m+n}$
$I_n \subset I_{m+n}$
et alors $a + b \in I_{m+n} \subset I$

A étant principal $\exists a \in A$, $I = \langle a \rangle$ Or $\exists N \in \mathbb{N}$, $a \in I_N$ alors $I = \langle a \rangle \subset I_N \subset I$ $I = I_N$ et par suite

$\forall n \geq N \; I = J_n$

Existence Par l'abs a non produit d'irréductibles (a non inv)

$\Rightarrow a = a_1 b_1$ a_1 non réd (inv)
b_1 non réd

Si a_2 et b_2 sont P.I, ~~[illegible]~~ aussi, non. produit d'irréd a

Par exemple a_1 non PI b_1 aussi abs

$a_1 = a_2 b_2$

l'un de $a_2 b_2$ est non produit d'irréductibles (sinon ..)

$a_2 = a_3 b_3$ ....

d'où $a_4, a_5, \ldots$

$I_n = \langle a_n \rangle$; $a_{n+1} | a_n$ donc $I_{n+1} \subset J_n$

si $I_{n+1} = J_n$ il vient $a_n | a_{n+1}$

a_n et a_{n+1} associés or $a_n = a_{n+1} b_{n+1}$

$\Rightarrow b_{n+1}$ inversible Abs

ainsi $\forall n \in \mathbb{N} \; I_n \subsetneq I_{n+1}$ A n'est pas noethérien.

160

D) Ecriture d'un élément

On choisit, dans chaque classe d'éléments irréductibles associés un représentant on note $\mathcal{P}$ l'ens des représentations

Ex. $\mathbb{Z}$ $\mathcal{P} = \{2, 3, 5, 7, 11, \dots\}$

$\mathbb{K}[X]$, $\mathbb{K}_{cc}$, $\mathcal{P} = \{P$ irréductibles $|$ Prunitaire$\}$

Ecriture Soit $a \in \mathbb{K}^*$ il existe une famille $\alpha_p \in \mathbb{N}^{(\mathcal{P})}$ presque nulle ie $\{p \in \mathcal{P} \mid \alpha_p > 0\}$ est fini et $u \in U(A)$

tq $a = u \underbrace{\prod_{\alpha_p \neq 0} p^{\alpha_p}}_{=1 \text{ si } \emptyset} = u \sum_{p \in \mathcal{P}} p^{\alpha_p}$

(Aussi $a = U p_1^{\alpha_1} \dots p_r^{\alpha_r}$ $\alpha_i \geq 1$, p_i $2 \grave{a} 2 \neq$)

Prop : 1) $a = u \prod_{p \in \mathcal{P}} p^{\alpha_p}$, $b = v \prod_{p \in \mathcal{P}} p^{\beta_p}$ alors

$$a \mid b \Leftrightarrow \forall p \in \mathcal{P}, \alpha_p \leq \beta_p$$

D/ ($\Leftarrow$) clair ($\Rightarrow$) fixons $p_0 \in \mathcal{P}$. Alors $p_0^{(\alpha p_0)} \mid a$ et $a \mid b$

donc $p_0^{\alpha_{p_0}} \mid \prod_{p \in \mathcal{P}} p^{\beta_p}$ supposons que $\alpha_{p_0} > \beta_{p_0}$ il vient

$p^{\alpha p_0 - \beta p_0} \mid \prod_{\substack{p \in \mathcal{P} \\ p \neq p_0}} p^{\beta_p}$ Or $p_0 \wedge p = 1$, si $p \neq p_0$

$p_0^{\alpha_0 - \beta_0} \wedge p^{\beta_p} = 1$

et donc $p^{\alpha p_0 - \beta p_0} \wedge \prod_{\substack{p \in \mathcal{P} \\ p \neq 0}} p^{\beta_p} = 1$ Absurde

2) Avec les m notations : $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\alpha_p, \beta_p)}$

$a \vee b = \prod_{p \in \mathcal{P}} \max(\alpha_p, \beta_p)$

③ nbre de diviseurs dans $\mathbb{N}^*$ $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ p_i premiers 2 à 2

$$d(n) = \prod_{i=1}^{n} (1+\alpha_i)$$

<u>Exos</u>. ① Soit $a \in \mathbb{N}^*$, $a \geq 2$, $m \in \mathbb{N}^*$, $m \geq 2$

Mq Si $a^m - 1$ est premier, m aussi ~~et~~ $a = 2$

si $2^m + 1$ est premier, $m = 2^k$ $k \in \mathbb{N}$

D/ 1) $a \geq 3$ $a-1 \mid a^m - 1$ abs / $m = kl$ $k \geq 2$ $l \geq 2$
$a^m - 1 = (a^k)^l - 1 = (a^k - 1)(\dots)$
abs

Si m possède un facteur impair k, $m = kl$

$$2^m + 1 = (2^l)^k + 1 = (2^l + 1)(\dots)$$ m n'a pas de facteurs pairs.

donc $m = 2^k \dots$

② Mq il existe une infinité de nbres premiers congrus à -1 mod 4

S/ ABS soit $p_1 \dots p_N$ les nbres premiers de la forme $4k - 1$
et $m = p_1 \dots p_N$

On regarde $4m^2 - 1 \equiv -1 [4]$ possède au moins un facteur premier $4m^2 - 1 \wedge p_i = 1$, il est diff de p_i ABS