le 22.02.18

Algèbre I :

Chapitre I

Relations d'équivalence ensembles quotients

Déf : Soit X un ensemble, soit $R \subset X \times X$, On suppose que R a les propriétés suivantes : (R relation d'équivalence)

1) $(x;x) \in R \quad \forall x \in X$ (Réflexivité) $x \sim x$
2) $(x;y) \in R \Rightarrow (y;x) \in R$ (Symétrie) $\forall x, y \in X$
3) $[(x;y) \in R$ et $(y;z) \in R] \Rightarrow (x;z) \in R$ (transitivité) $\forall x, y, z \in X$

Ex : $X = \mathbb{Z} = \{\dots -2; -1; 0; 1 \dots\}$

a) $n \sim m$ ssi $n = m$

b) Soit $d \in \mathbb{N}$ $\quad n \sim m \Leftrightarrow d$ divise $n - m$

Rappel : $d \mid n \Leftrightarrow \exists k \in \mathbb{N} \cdot d \cdot k = n$

Vérifions les 3 axiomes : 1) $n \sim d \Leftrightarrow d \mid n - n$ ok
On prend $k = 0$ et $d \cdot k = n - n$

2) Supposons $n \sim m \overset{?}{\Rightarrow} m \sim n$

$d \mid m - n \Rightarrow d \mid m - n$ (on change le signe de k)

3) Supposons $n \sim m$ et $m \sim 0 \overset{?}{\Rightarrow} n \sim 0$

$d \mid m - n$ et $d \mid 0 - m \quad d \mid m - n + 0 - m = d \mid 0 - n$ ok.

c) $X = \{$ droites du plan $\mathbb{R}^2\}$

$D \sim D' \Leftrightarrow$ les vecteurs directeurs de D et D' sont colinéaires.

Déf : Soit X un ensemble et $R \subset X \times X$ une relation d'équivalence
Soit $x \in X$. La classe d'équivalence de x est :

$$\bar{x} = \{ y \in X : y \sim x \} = [x]$$

⚠ $\bar{x}$ est un sous-ensemble de X

Proposition : Soit X un ensemble et $R \subset X \times X$ une rel. d'équivalence.
Alors X est partitionné par ses classes d'équivalences.

$$X = \bigsqcup_{x \in X} \bar{x}$$ (union disjointe ; mais mieux est réunion)

- $X = \bigcup_{x \in X} \bar{x}$ et [si $\bar{x} \cap \bar{y} \neq \emptyset$ alors $\bar{x} = \bar{y}$]

Preuve : $X \supset \bigcup_{x \in X} \bar{x}$ est évident car $\bar{x} \subset X \ \forall x \in X$

$X \subset \bigcup_{x \in X} \bar{x}$ en effet si $x \in X$ alors $x \in \bar{x}$

Suite: Prouvons que si $\overline{x} \cap \overline{y} \neq \emptyset \Rightarrow \overline{x} = \overline{y}$

soit $z \in \overline{x}$ et $z \in \overline{y}$, on a alors $z \sim x$ et $z \sim y \Rightarrow x \sim y$

donc $\overline{x} = \overline{y}$

Déf: Soit X un ensemble, et $R \subset X \times X$ une rel d'équivalence.
Un <u>système de représentants</u> de R est un sous-ensemble $T \subset X$ tel que : $\forall x \in X, \exists! t \in T : t \sim x$

On peut donc écrire $X = \bigsqcup_{t \in T} \overline{t}$

T s'appelle aussi transversale

Ex: a) $X = \{$ droites du plan $\}$

$D \parallel D' \Leftrightarrow D \sim D'$ $\quad T = \{$ droites contenant $o\}$

b) $X = \mathbb{Z}$, $d \in \mathbb{N}$ choisi

$n \sim n \Leftrightarrow d / m-n \Leftrightarrow \exists k \in \mathbb{Z}$ $d \cdot k = m - n$

$T = \{0; 1; 2; \dots; d-1\}$

T représente bien toutes les classes : soit $n \in \mathbb{Z}$
alors $n = d \cdot k + r$ où $0 \leq r \leq d-1$ (division euclidienne)
et donc $n \sim r$ car $d / n-r$
On vérifie que si r et r' sont dans T alors $r \sim r' \Rightarrow r = r'$

Proposition: Soit X un ensemble et $X = \bigsqcup_{t \in T} X_t$ (sous-ens de X)

une partition de X. Définissons : $x \sim y \Leftrightarrow \exists t \in T : x, y \in X_t$
C'est une relation d'équi dont les classes sont les X_t, $t \in T$

Preuve:

- $x \overset{?}{\sim} x \overset{?}{\Leftrightarrow} \exists t \in T : x \in X_t$ et $x \in X_t$ (Soit $x \in X$) ok
- $x \sim y \Rightarrow y \sim x$ mais $x \sim y \Leftrightarrow \exists t \in T : x \in X_t$ et $y \in X_t$
  $y \sim x \Leftrightarrow \exists t \in T : y \in X_t$ et $x \in X_t$ ok
- $x \sim y$ et $y \sim z \overset{?}{\Rightarrow} x \sim z$

$\Leftrightarrow \exists t, t' \in T$ $x, y \in X_t$ et $y, z \in X_{t'} \Rightarrow t = t'$ donc $x, y, z \in X_t = X_{t'}$ donc $x \sim z$.

Si $x \in X_t$ alors $\overline{x} = X_t$

Conclusion: "une relation d'équivalence sur X n'est rien d'autre qu'une partition de X."

Algèbre I :

Déf: Ensemble quotient associé à une relation d'équivalence

Soit X un ensemble, $R \subset X \times X$ une rel. d'équiv.
L'ensemble quotient définit par R est l'ensemble des classes d'équivalences de R.

$$X/_\sim = \{ \bar{x} : x \in X \}.$$

c'est un ensemble de sous-ensembles de X.

Déf: La projection canonique associée à la relation R sur X est l'application $\pi : X \longrightarrow X/_\sim$ ← l'ensemble quotient donne immédiatement la surjectivité
$x \longmapsto \bar{x}$

à tout éléments $x \in X$, l'application π associe le sous-ensemble $\bar{x} = \{ y \in X : y \sim x \}$ de X donc $\pi : X \to \mathcal{P}(X)$ où $\mathcal{P}(X)$ sont les parties de X (ici π n'est pas surjective)

On voit donc que $X/_\sim \subset \mathcal{P}(X)$.
L'image de π est l'ensemble des classes de R qui est $X/_\sim$ donc π est surjective.

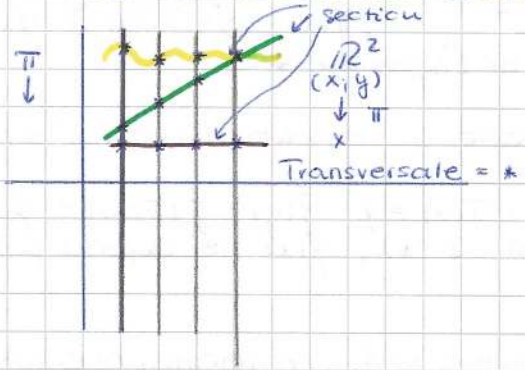
π (prend une lettre et associe le cartier)

Déf: Une section $\sigma : X/_\sim \to X$ de la proj. canonique $\pi : X \to X/_\sim$ est une application telle que $\pi \circ \sigma = id_{X/_\sim}$ ie: $\forall \bar{x} \in X/_\sim$

$$\pi \sigma(\bar{x}) = \bar{x}$$

Exo: Si σ est une section de π alors $\sigma(X/_\sim) \subset X$ est un système de représentants de la relation d'équ $\sim$.
De plus si $T \subset X$ est un système de représentants alors $X/_\sim \xrightarrow{\sigma} X$ (σ est l'unique élément de T tel que $\bar{t} = \bar{x}$)
$\bar{x} \longmapsto t$
définit une section de T.

"être sur la même droite verticale" = "$\sim$"

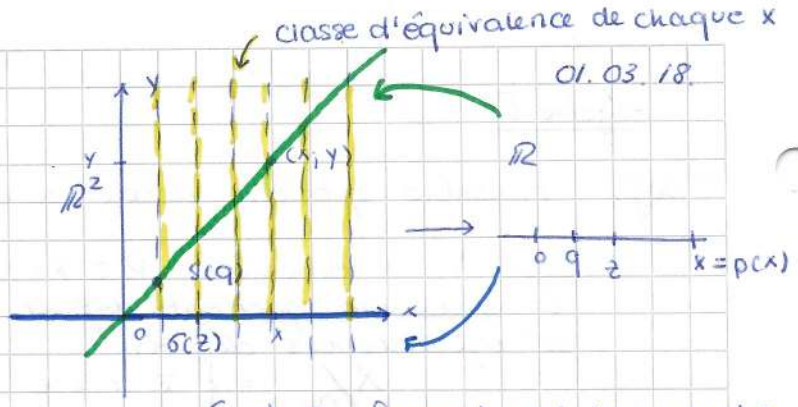


Algèbre 1 :

Ex: (section) soit $p : \mathbb{R}^2 \to \mathbb{R}$, $(x;y) \longmapsto x$

$\sigma : \mathbb{R} \to \mathbb{R}^2$, $x \longmapsto (x;0)$

$s : \mathbb{R} \to \mathbb{R}^2$, $x \longmapsto (x;x)$



σ et s forment par leur graphe un système de représentant

Rappel: une section $\sigma : X/_\sim \longrightarrow X$ de la projection canonique $\pi : X \longrightarrow X/_\sim$, $x \longmapsto \bar{x}$ est une application qui vérifie $\pi\sigma(\bar{x}) = \bar{x}$ $\forall \bar{x} \in X/_\sim$

Remarque: si σ est une section de π alors $\sigma(X/_\sim) = \operatorname{Im}\sigma \subset X$ est un système de représentants pour la relation d'équivalence.

Si $T \subset X$ est un système de représentants, alors on définit $\sigma : X/_\sim \longrightarrow X$, $\bar{x} \longmapsto t$ où t est l'unique élément de T tq $\bar{t} = \bar{x}$

Théorème: Soit $\pi : X \to Y$ une application surjective.
Soit $f : X \to Z$ une application. Alors il existe une application $\bar{f} : Y \to Z$ tq $\forall x \in X \quad \bar{f}\pi(x) = f(x)$ $\Longleftrightarrow$ $\forall x, x' \in X \ \ \pi(x) = \pi(x') \Rightarrow f(x) = f(x')$ (*)

Preuve:

- supposons que $\bar{f}$ existe
  Soit $x, x' \in X$: $\pi(x) = \pi(x')$
  donc $\bar{f}\pi(x) = \bar{f}\pi(x') \Rightarrow f(x) = f(x')$

- supposons $\forall x, x' \in X \ \ \pi(x) = \pi(x') \Rightarrow f(x) = f(x')$

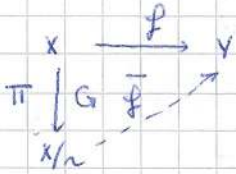
  soit $y \in Y$, comme π surjective on peut choisir $x \in X$ $\pi(x) = y$. On obtient ainsi une section de π
  $\sigma : Y \to X$, $y \mapsto x$ $\quad (\forall y \in Y \ \ \pi \circ \sigma(y) = y)$ $\quad \pi(\sigma\pi(x)) = \pi\sigma(\pi(x)) = \pi(x)$
  On pose $\bar{f} := f \circ \sigma$ $\quad \bar{f}\pi(x) = f\sigma\pi(x) \overset{\text{par l'hypothèse } *}{=} f(x)$ $\forall x \in X$.

Remarque: $\bar{f}$, l'application vérifiant la condition du thm est unique

Si $y \in Y$, soit $x \in X$: $\pi(x) = y$ $\quad \bar{f}(y) = \bar{f}(\pi(x)) = f(x)$ et d'après la condition 2 (*), $f(x)$ ne dépend pas du choix de x. $\pi(x) = y$

Corollaire: Soit X, un ensemble, et $R \subset X \times X$ une relation d'équivalence.
Soit $\pi : X \to X/_\sim$ la projection canonique (surjective)
Soit $f : X \to Y$ une application.
Alors $\exists !\ \bar{f} : X/_\sim \to X$ tq $\bar{f} \circ \pi = f \Leftrightarrow \left[x \sim x' \underset{\pi(x) = \pi(x')}{\Rightarrow} f(x) = f(y) \right]$

Preuve:



$\exists ?\ \bar{f} : X/\sim \to Y \quad \bar{f} \circ \pi = f$ (question)

$x \sim x' \Leftrightarrow \bar{x} = \bar{x'} \Leftrightarrow \bar{x} = \pi(x) = \bar{x'} = \pi(x')$

$\Leftrightarrow \pi(x) = \pi(x')$

"Chapitre 2" Groupes, sous-groupes, groupes-quotients, actions de groupe.

Déf: Un groupe est un ensemble muni d'une loi $G \times G \to G$, $(g;h) \mapsto gh$ telle que: $\forall x,y,z \in G$

1) $(xy)z = x(yz)$
2) $\exists\, e \in G : \forall x \quad xe = ex = x$
3) $\forall x \in G \ \exists x^{-1} \in G : xx^{-1} = x^{-1}x = e$

Ex:

1) $G = (\mathbb{R}; +) \quad (x;y) \mapsto x+y$
2) $G = (\mathbb{R}^*_+; \cdot) \quad (x;y) \mapsto x \cdot y$
3) $G = (\mathbb{C}^*; \cdot) \quad (z;w) \mapsto z \cdot w$
4) $G = (\{\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} \ a,x \in \mathbb{R}, a>0\}; \cdot) \quad (M;N) \mapsto M \cdot N$ (mult. matricielle)
est un groupe pour lequel $N \cdot M \neq M \cdot N$ en général
$\Rightarrow$ le groupe est non commutatif.

Déf: Soit G et H, deux groupes. Une application $h: G \to H$ telle que i) $h(e_G) = e_H$
ii) $h(x \cdot y) = h(x) \cdot_H h(y) \quad \forall x,y \in G$
alors l'application h est un homomorphisme

Ex:

1) $G = (\mathbb{R}; +) \quad H = (\mathbb{R}^*_+; \cdot) \quad h = \exp$
$\exp: \mathbb{R} \to \mathbb{R}^*_+, \ t \mapsto e^t \quad \exp(t+s) = \exp(t) \cdot \exp(s)$
2) $h: (\mathbb{R}; +) \to (\mathbb{C}^*; \cdot), \ t \mapsto e^{it}$
$h(t+s) = h(t) \cdot h(s)$
$\exp^i(t+s) = \exp^i(t) \cdot \exp^i(s)$
$e^{i(t+s)} = e^{it} \cdot e^{is}$
$h(t +_{\mathbb{R}} s) = h(t) \cdot_{\mathbb{C}^*} h(s)$
3) $G = (\mathbb{R}^*_+; \cdot) \quad H = (\mathbb{R}; +)$
$\log: \mathbb{R}^*_+ \to \mathbb{R}, \ t \mapsto \log t \quad \log(t \cdot s) = \log t + \log s$

Définition: Un isomorphisme entre 2 groupes G et H est un homomorphisme $h: G \to H$ qui est bijectif.

Ex: (Déf) ↳ Soit $h: G \to H$ un homomorphisme bijectif, alors $h^{-1}: H \to G$ est aussi un homomorphisme

Déf: Soit $h : G \to H$ un homomorphisme entre 2 groupes alors le noyau de h est :

$$\ker(h) = \{ g \in G \mid h(g) = e_H \}$$

et l'image de h est :

$$\mathrm{Im}(h) = \{ y \in H, \exists x \in G : h(x) = y \}$$

Exo: Ker et Im sont des sous-groupes de G, resp. H.
h injective $\Leftrightarrow \ker(h) = \{e_H\}$ h surjective $\Leftrightarrow \mathrm{Im}(h) = H$

Déf: Un automorphisme de groupe est un isomorphisme $h : G \to G$ du groupe dans lui-même.

Ex: Soit G un groupe et $g \in G$.

$$c(g) : G \to G, \quad x \mapsto gxg^{-1}$$

C'est un automorphisme de G: $\forall x, y \in G$

$c(g)(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = c(g)(x) \cdot c(g)(y)$

$c(g)(e) = geg^{-1} = gg^{-1} = e$

Donc $c(g)$ est un homomorphisme

$$c(g^{-1}) : G \to G, \quad x \mapsto g^{-1}xg \quad \text{"application inverse"}$$

si $c(g) \circ c(g^{-1})(x) = c(g)\, g^{-1}xg = gg^{-1}xgg^{-1} = x$ ok.

$\Rightarrow c(g)$ est bien un automorphisme.

Un exemple important de relation d'équivalence.

Déf: Soit G un groupe et H un sous groupe. L'espace quotient G/H est l'espace des classes d'équivalence pour la relation $x \sim_H y \Leftrightarrow xH = yH$ où $xH = \{ xh : h \in H \}$

Dém: Rel d'équi ? 1) $x \sim_H x$? , $xH = xH$ ok
2) $x \sim_H y \Rightarrow y \sim_H x$: $xH = yH \Leftrightarrow yH = xH$
3) $x \sim y$ et $y \sim z \Rightarrow x \sim z$ ok ∎

C'est bien une relation d'équi de la classe de $x \in G$ et $xH \subset G$

$$\pi : G \to G/H = G/\sim_H, \quad g \mapsto g \cdot H$$

Déf: un sous-groupe H d'un groupe G est un sous-ensemble d'un groupe G:

i) $e_G \in H$ ii) $x, y \in H \Rightarrow x \cdot y \in H$
iii) $x \in H \Rightarrow x^{-1} \in H$

Ex: $G = (\mathbb{C}^*, \cdot)$ $H = S^1 = \{ z \in \mathbb{C} : |z| = 1 \}$ est un sous-groupe

Algèbre I:

le 08.03.18

Rappel: Soit G, un groupe, soit $H < G$ un sous-groupe (Notation $<$)
On définit sur G, une relation d'équivalence $x \sim y \Leftrightarrow x^{-1}y \in H$

1. $x \sim_H x \Leftrightarrow e \in H$
2. $[x \sim_H y \Rightarrow y \sim_H x] \Leftrightarrow [x^{-1}y \in H \Rightarrow y^{-1}x \in H]$
3. $[x \sim_H y \wedge y \sim_H z] \Leftrightarrow [x^{-1}y \in H \text{ et } y^{-1}z \in H] \Rightarrow (x^{-1}yy^{-1}z) = x^{-1}z \in H \Leftrightarrow x \sim_H z$

Une classe d'équivalence est de la forme :
soit $g \in G$ $\bar{g} = \{x \in G : x \sim_H g\} = \{x \in G : x^{-1}g \in H\} = \{x \in G : x \in gH\}$
$= gH$

Notation: Si $E \subset G$ est un sous-ensemble. Soit $g \in G$ $gE = \{gx \in G : x \in E\}$

Déf: Un sous-groupe $H < G$ est dit normal si $\forall g \in G$ et $\forall h \in H$ $ghg^{-1} \in H$. En d'autres termes, H est préservé par $c(g)$ $\forall g$ (bijection) i.e: $c(g)\,H \subset H$

Ex: Si G est un groupe abélien (commutatif) dans ce cas, tout sous-groupe est normal

- Soit $H < G$.. Soit $g \in G$, $h \in H$ $ghg^{-1} = hg^{-1}g = h \in H$
- Soit $f : G \to Q$, un homomorphisme entre 2 groupes
  $\ker(f) = \{g \in G \mid f(g) = e\}$ est un sous-groupe normal
  En effet: $f(e) = e$ car f homomorphisme donc $e \in \ker(f)$
  $x, y \in \ker(f) \Rightarrow f(x) = f(y) = e$ alors $f(xy) = f(x)f(y) = e$ donc $xy \in \ker f$
  Soit $x \in \ker(f)$, $g \in G$, $gxg^{-1} \in \ker(f)$ car $f(gxg^{-1}) = f(g)f(x)f(g^{-1})$
  $= f(g)f(g^{-1}) = e$

Théorème: Soit G, un groupe et H un sous-groupe normal. Alors, il existe une unique structure de groupe sur l'ensemble quotient
$G/\sim = \bigcup_{g \in G} \{gH\}$ telle que $\pi : \begin{array}{ccc} G & \to & G/\sim \\ g & \mapsto & \bar{g} = gH \end{array}$
est un homomorphisme de groupe. On note l'ensemble quotient G/H (G modulo H)

Remarque: La classe $\bar{x} = xH$ peut être représentée sous la forme $x'H$ où $x' = xh$, $h \in H$, pour que la loi soit définie de manière cohérente, il faut vérifier que $x'y\,H = xy\,H$.
$x'yH = xhyH = xyy^{-1}hyH = xy(y^{-1}hy)H$.
Comme $H \lhd G$, que $h \in H$, $y^{-1} \in G$, alors $yhy^{-1} \in H$
donc $xy(y^{-1}hy)H = xyH$
On montre de même que la définition ne dépend pas du choix de y.
Associatif: $(xHyH)zH = xyHzH = (xyz)H = z(xy)H = xH\,yzH$
$eH = H$ est est l'élément neutre de G/H.
$HxH = eHxH = exH = xH$ et $xHx^{-1}H = xx^{-1}H = H$.

Preuve: On définit une loi de composition interne sur l'ensemble des classes d'équivalence, ainsi $G/H \times G/H \longrightarrow G/H$
$(xH; yH) \longmapsto xyH$

On doit prouver que $\pi : G \to G/H$ est un homomorphisme
$g \longmapsto gH$

$\pi(e_g) = e_g H = H$ est bien le neutre pour la loi sur G/H

$\pi(xy) = xyH = xHyH = \pi(x)\pi(y)$

vérifions que la loi définie est la seule qui fasse de π un homomorphisme.

Cela découle de la surjectivité de π.

Soit xH et $yH \in G/H$ $\quad xH \cdot yH = \pi(x) \cdot \pi(y) = \pi(xy) = xyH$

Proposition: Soit G un groupe et H un sous-groupe normal.
Alors il existe un groupe Q et un homomorphisme $f : G \to Q$ tel que $Ker(f) = H$.

Preuve On choisit $Q = G/H$ et $f = \pi$ $\quad \pi : G \to G/H$

$Ker(\pi) = \{ g \in G \mid \pi(g) = e_{G/H} \} = \{ g \in G \mid gH = H \} = H$

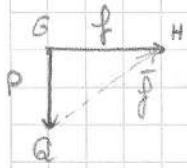
$gH = H$ est équivalent à $g \in H$

Preuve: $g \in H \Rightarrow gH = H$ si $gH = H \Rightarrow \exists h, h' \in H$
tel que $gh = h' \Rightarrow g = h'h^{-1} \in H$.

le 08.03.18

Algèbre I:

Théorème: *factorisation des applications (cas des groupes)*



Soit $f: G \to H$, un homomorphisme de groupe.
Soit $p: G \to Q$, un homomorphisme de groupe surjectif.
Alors il existe un unique homomorphisme $\bar{f}: Q \to H$
tel que : $\bar{f} \circ p = f \iff \ker p \subset \ker f$.

Cor: Soit N, un sous-groupe normal de G. Soit $\pi: G \to G/N$ la proj. canonique.
Soit $f: G \to H$ un homomorphisme (dans un groupe quelconque H)
Alors il existe un unique homomorphisme $\bar{f}: G/N \to H$ tq
$\bar{f} \cdot \pi = f \iff N \subset \ker(f)$.

Preuve: On pose $Q = G/N$; $p = \pi$ et on remarque $\ker p = \ker \pi = N$

Preuve: Théorème.

Supposons que $\bar{f}$ existe. $\ker p \subset \ker f$
Soit $g \in G$ $p(g) = e \to \bar{f}(p(g)) = \bar{f}(e) = e$
$= f(g) = e$

Supposons $\ker p \subset \ker f$. Supposons $p(x) = p(y)$ pour $x, y \in G$
Vérifions qu'alors $f(x) = f(y)$.
En effet, $p(x) = p(y) \Rightarrow p(x) \cdot p(y)^{-1} = e = p(x\bar{y}^{1}) \Rightarrow x\bar{y}^{1} \in \ker p \Rightarrow$
$f(x\bar{y}^{1}) = e = f(x) \cdot f(y)^{-1} \Rightarrow f(x) = f(y)$.

D'après le thm dans le cas des ensembles, on sait qu'il existe une unique application $\bar{f}: Q \to H$ tq $\bar{f}p = f$

Reste à prouver que $\bar{f}$ est une homomorphisme.

$$\bar{f}(p(x)p(y)) = \bar{f}(p(xy)) = f(xy) = f(x)f(y) = \bar{f}(p(x))\,\bar{f}(p(y)).$$

Algèbre L :

le 15.03.18

Déf: Soit G_n, une suite de groupe et des homomorphismes $f_n : G_n \to G_{n+1}$
On dit que la suite $\dots \to G_n \xrightarrow{f_n} G_{n+1} \xrightarrow{f_{n+1}} G_{n+2} \to \dots$ est exacte si pour tout groupe G_n :

$$Im(f_{n-1}) = Ker(f_n)$$

Prop: Soit G, un groupe et N, un ss.grp normal de G. Alors la suite

$$\{1\} \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} G/N \to \{1\} \quad \text{est exacte.}$$

$i = e_N$: 1 est envoyé sur e_N

Preuve: exactitude en N : il faut prouver que l'image de $\{1\}$ dans N (qui est $e_N \in N$) est égale au noyau de i. On sait qu'un homomorphisme est injectif $\Leftrightarrow$ son noyau est réduit au sous-groupe trivial : $Ker(i) = \{e_N\}$

exactitude en G : $i(N) \overset{?}{=} Ker(\pi)$, ari, car $i(N) = N \subset G$ et $Ker(\pi) = N \subset G$

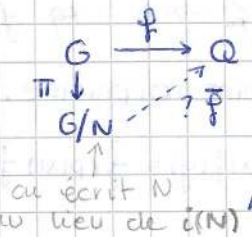
exactitude en G/N : $Im(\pi) = G/N$ (la projection canonique est surjective)
comme $G/N \to \{e\}$ est l'application qui à tout élément de G/N associe 1, son noyau est G/N tout entier.

Prop: Soit $\{1\} \to N \xrightarrow{i} G \xrightarrow{f} Q \to \{1\}$ une suite exacte de groupes. alors G/N est isomorphe à Q.

Rem: L'hypothèse implique que l'homo : $N \to G$ est injectif et que l'homo : $G \to Q$ est surjectif.

Rem: N est un ss-grpe normal de G, car $i(N) = N \lhd G$ et puis par hypothèse $i(N) = Ker(f)$ qui est un ss-grpe normal de G.

Preuve: (Prop)



On cherche à construire un homomorphisme $\bar{f} : G/N \to Q$, tq : $\bar{f} \circ \pi = f$

On sait que $\bar{f}$ existe $\Leftrightarrow$ (ssi) $Ker(\pi) \subset Ker(f)$
$Ker(\pi) = N$.

Par hypothèse (suite exacte) $i(N) = Ker(f) = N$
Donc $\bar{f}$ existe. Comme f est surjective, $\bar{f}$ l'est aussi.

Il reste à démontrer que $\bar{f}$ est injectif. C'est-à-dire, que le noyau de $\bar{f}$ est trivial.

Soit $gN \in G/N$, t.q $\bar{f}(gN) = e_Q \in Q$ (Il faut mq $g \in N$)

$e_Q = \bar{f}(\pi(g)) = f(g)$ donc $g \in Ker(f) = N$ donc $g \in N$.

donc $gN = N$ et c'est bien l'élément neutre de G/N, ce qui prouve l'injectivité de $\bar{f}$.

Actions de groupes

Si X est un ensemble, alors l'ensemble des bijections $Aut(X)$ de X dans lui-même est un groupe (pour la composition des appli°)

$$X \xrightarrow{f} X \xrightarrow{g} X \qquad g \circ f$$

$$Aut(X) \times Aut(X) \longrightarrow Aut(X) \qquad (f;g) \mapsto f \circ g$$

Id_X est l'élément neutre. $(f; f^{-1}) \to f^{-1} \circ f = Id_X$

Déf. Une action d'un groupe G sur un ensemble X est un homomorphisme de G dans $Aut(X)$.

Ex : $\alpha : G \to Aut(X)$ (homomorph.) $\quad g \mapsto \alpha(g)$ $\quad \left[\alpha(e_G) = Id_X \ ; \ \alpha(g \circ h) = \alpha(g) \circ \alpha(h) \ \ \forall g,h \in G\right]$

Notation : On peut décrire l'action de la manière suivante.

$$G \times X \longrightarrow X$$
$$(g;x) \longmapsto \alpha(g)(x) = g * x$$
$$(e_G; x) \longmapsto \left[e_G * x = \alpha(e_G)(x) = Id_X(x) = x\right] \ \forall x \in X$$

(équivalent)

$$\left[\forall g,h \in G \quad (gh; x) \mapsto gh * x = \alpha(gh)(x) = \alpha(g)\,\alpha(h)(x) = g * (h * x)\right]$$

Rem : $g^{-1}(g * x) = g^{-1}g * x = e_G * x = x \ \ \forall x \in X$

Prop : Soit $G \times X \to X$ $(g;x) \mapsto g * x$ une action de groupe G sur un ensemble X. La relation sur X définie par la condition

$x \sim y \iff x$ et y appartiennent à la même orbite
$\exists x_0 \in X : x \in \mathcal{O}(x_0)$ et $y \in \mathcal{O}(x_0)$

est une relation d'équivalence

Déf : Soit $G \times X \to X$ une action. Soit $x_0 \in X$, $\mathcal{O}(x_0) = \{g * x_0 : g \in G\} \subset X$ on appelle $\mathcal{O}(x_0)$ l'orbite de x_0 sous l'action de G.

Preuve : Prouvons tout d'abord que si 2 orbites se rencontrent alors elles sont égales. $\mathcal{O}(x_0) \cap \mathcal{O}(y_0) \neq \emptyset$ soit $z \in \mathcal{O}(x_0) \cap \mathcal{O}(y_0)$
$z = g x_0 = h y_0$ où $g \in G$, $h \in G$. si $w \in \mathcal{O}(y_0)$ $w = g_w y_0$ $g_w \in G$
$y_0 = h^{-1} g x_0$ $\qquad = g_w h^{-1} g x_0$

$\Rightarrow w \in \mathcal{O}(x_0)$
$\Rightarrow \mathcal{O}(y_0) \subset \mathcal{O}(x_0)$ de même $\mathcal{O}(x_0) \subset \mathcal{O}(y_0)$

Donc $x \sim y \iff \mathcal{O}(x) = \mathcal{O}(y)$
$G * x = G * y$
$x \sim y \iff G_x = G_y$

$x \overset{?}{\sim} x$: $G_x = G_x$ ok
$x \sim y$ et $y \sim x$: $G_x = G_y = G_x$.
$x \sim y$ et $y \sim z \overset{?}{\Rightarrow} x \sim z$: $G_x = G_y$ et $G_y = G_z \to G_x = G_z$ ok

Théorème : Lagrange

Soit G un groupe fini. Soit H un sous-groupe. Alors $|H|$ (cardinal de H) divise $|G|$ (cardinal de G)

Cor : Soit p un nombre premier. Soit $\mathbb{Z}/p\mathbb{Z} = G$. Le groupe $G = \mathbb{Z}/p\mathbb{Z}^*$

Remarque : $p\mathbb{Z} = \{k \cdot p \mid k \in \mathbb{Z}\}$ est bien un sous-groupe des entiers.

Il est normal, donc $\mathbb{Z}/p\mathbb{Z}$ est un groupe : $\{\bar{0}; \bar{1}; \dots; \overline{p-1}\} = \mathbb{Z}/p\mathbb{Z}$ ⌟

* il a que 2 sous-groupes $\{\bar{0}\} < \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} < \mathbb{Z}/p\mathbb{Z}$

Preuve : (du thm)

On sait que la relation définie par H décompose G en classe d'équivalence, en une partition. $G = \bigsqcup_{t \in T} tH$

Affirmation : chaque classe à le même nombre d'éléments :

$t, s \in T$

$$\ell_{st^{-1}} : tH \to sH$$
$$x \mapsto st^{-1}x$$
$$th \longmapsto st^{-1}Hh = sh = sH$$
$$\ell_{st^{-1}}^{-1} : sH \to sH$$
$$y \mapsto ts^{-1}y$$
$$sh \longmapsto ts^{-1}sh = th = tH$$

$$\ell_{ts^{-1}} \circ \ell_{st^{-1}}(x) = ts^{-1}st\,x = x = id(x).$$

Donc toutes les classes sont en bijection avec la classe de l'élément neutre qui est H.

$$|G| = \sum_{t \in T} |t \cdot H| = |T| \cdot |H|$$
$$\in \mathbb{N}$$

Algèbre I :

le 22.03.18

(Action de groupe)

rappel : G, groupe, X ensemble,

$Aut(X)$ le groupe des bijections de X dans X [e : $id(x) = x \ \forall x \in X$]

$\alpha : G \longrightarrow Aut(X)$ homomorphisme.

$G \times X \to X$
$(g ; x) \longmapsto g * x$ i) $e * x = x \ \forall x$ ii) $(gh) * x = g * (h * x)$

Ex : $X = \mathbb{R}^2$ le plan euclidien, $G = Isom(\mathbb{R}^2)$

$Isom(\mathbb{R}^2) \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$
$(g , v) \longmapsto g * v$ où par déf $g * v = g(v)$

si $g = id_{\mathbb{R}^2}$ $i_{\mathbb{R}^2}(v) = i_{\mathbb{R}^2}(*v = v$

$(gh) * v = (g \circ h)(v) = g(h(v)) = g * (h * v)$

Déf : Si $G \times X \longrightarrow X$ est une action. On fixe $x_0 \in X$.

Alors $G_{x_0} = \{ g : g * x_0 = x_0 \}$ est le stabilisateurs de x_0.

Prop : G_{x_0} est un sous-groupe de G.

Preuve : $e * x_0 = x_0 \ \forall x_0 \in X$ donc $e \in G_{x_0}$

$g, h \in G_{x_0}$, $(g \cdot h) x_0 = g * (h * x_0) = g * x_0 = x_0$

Soit $g \in G_{x_0}$ $g^{-1} * x_0 = ?$ $g * (g^{-1} * x_0) = (gg^{-1}) * x_0 = e * x_0 = x_0$.

donc $g^{-1} \in G_{x_0}$ [$g^{-1} g * x_0 = g^{-1}(x_0) = x_0$]

Ex : Dans l'exemple $X = \mathbb{R}^2$ le plan et $G = Isom(\mathbb{R}^2)$

Choisissons $x_0 = (0;0) \in \mathbb{R}^2$ $(Isom(\mathbb{R}^2))_{(0;0)} = \{$ des isométries de $\mathbb{R}^2$ qui ont $(0;0)$ comme pt. fixe $\}$

On vérifie que $Isom(\mathbb{R}^2)_{(0;0)}$ est constituée de toutes les rotations centrées en 0 et de toutes les réflexions orthogonales d'axe par $0 = (0;0)$

Rappel : Si $x_0 \in X$ est fixé, l'orbite de x_0 $\mathcal{O}(x_0) = \{ g * x_0 : g \in G \} = G * x_0 \subset X$ $(= G x_0)$

Ex : $X = \mathbb{R}^2$ et $G = Isom(\mathbb{R}^2)$, on restreint l'action au sous-groupe des rotations autour de $(0;0)$. Ce groupe se note $SO(2;\mathbb{R}) = \{$ rotation du $\mathbb{R}^2$ de centre $(0;0)\}$

Ex: (suite) On identifie $\mathbb{R}^2$ à $\mathbb{C}$ $(x;y) \longmapsto x+iy$ où $\|(x;y)\| = |x+iy|$

Toute rotation qui fixe l'origine s'écrit $z \longmapsto e^{i\theta} z$

$U(1;\mathbb{C}) = \{z \in \mathbb{C} \mid |z| = 1\} \cong SO(2;\mathbb{R})$ isomorphe.

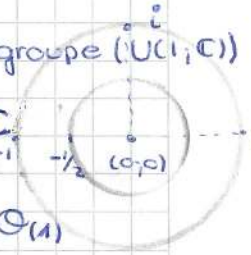
L'action de $U(1;\mathbb{C})$ sur $\mathbb{C}$ s'écrit $U(1;\mathbb{C}) \longrightarrow \mathbb{C}$
$(e^{i\theta}; z) \longmapsto e^{i\theta} * z$ où $*$ = '.'
la multiplication usuelle sur les complexes.

Décrivons l'orbite de $1 = x_0 \in \mathbb{C}$ sous l'action de notre groupe $(U(1;\mathbb{C}))$

$\mathcal{O}(1) = U(1;\mathbb{C}) * 1 = \{e^{i\theta} \cdot 1 : \theta \in \mathbb{R}\} = \{e^{i\theta} : \theta \in \mathbb{R}\} \subset \mathbb{C}$

$U(1;\mathbb{C}) * 1 = U(1;\mathbb{C}) * i$ $\quad U(1;\mathbb{C}) * \frac{1}{2} = U(1;\mathbb{C}) * \frac{1}{2} i$

$U(1;\mathbb{C}) * 0 = 0$ c-à-d juste un point.



Prop: Soit $G \times X \longrightarrow X$ une action d'un groupe G sur un ensemble X. Alors

i) si x_0 et y_0 sont 2 points de X : $\mathcal{O}(x_0) = \mathcal{O}(y_0)$ alors G_{x_0} et G_{y_0} sont conjuguées

ii) Soit $x_0 \in X$. L'application $G \longrightarrow X$, $g \longmapsto g * x_0$ induit une bijection $G/G_{x_0} \cong \mathcal{O}(x_0)$

Preuve: i) comme x_0 et y_0 sont dans la même orbite $\exists\, g_{x_0y_0} \in G$ tq

$g_{x_0y_0} * x_0 = y_0$ $\qquad$ Stabilisateur $G_{y_0} \longrightarrow$ Stabilisateur G_{x_0} est bien définie
$g \longmapsto g_{x_0y_0}^{-1} g\, g_{x_0y_0}$

En effet, $(g^{-1}_{x_0y_0} g\, g_{x_0y_0}) * (x_0) = (g^{-1}_{x_0y_0} g) * y_0 = g^{-1}_{x_0y_0} * y_0 = x_0$

Ci est bien définit et c'est bien une bijection car son inverse est $G_{x_0} \longrightarrow G_{y_0}$ $g \longmapsto g_{x_0y_0}\, g\, g_{x_0y_0}^{-1}$

ii) Soit $x_0 \in X$, $f: G \longrightarrow X$, $g \longmapsto y * x_0$, $\pi: G \longrightarrow G/G_{x_0}$, $g \longmapsto g G_0$ la projection canonique (On a vu que G_0 est un ss-groupe) (attention en général G_{x_0} n'est pas normal)

$$\begin{array}{ccc} G & \xrightarrow{f} & X \\ {\scriptstyle\pi}\downarrow & \nearrow ? & \\ G/G_{x_0} & & \end{array} \qquad \exists\, \bar{f}: G/G_{x_0} \longrightarrow X \text{ tq } \bar{f} \circ \pi = f.$$

car si $\pi(g) = \pi(h)$ pour $g, h \in G$ alors $f(g) = f(h)$!
(Critère pour l'existence de $\bar{f}$

$\pi(g) = \pi(h) \iff gG_{x_0} = hG_{x_0}$ donc $h = k \cdot g$ pour un certain $k \in G_{x_0}$

$f(k) = h * x_0 = (gk) * x_0 = g(k * x_0) = g * x_0 = f(g) \Rightarrow \bar{f}\ G/G_{x_0} \xrightarrow{=\mathrm{Im}(f)} \mathcal{O}(x_0)$

existe et est surjective. Donc en fait, on a un diagramme

$$\begin{array}{ccc} G & \xrightarrow{f} & \mathrm{Im}(f) = \mathcal{O}(x_0) \\ {\scriptstyle\pi}\downarrow & \nearrow {\scriptstyle\bar{f}} & \\ G/G_{x_0} & & \end{array}$$

Algèbre I : le 22.03.18

Preuve : (suite) comme f est surjective sur $\mathcal{O}(x_0)$ $\bar{f}$ l'est aussi

De plus $\bar{f} : G/G_{x_0} \to \mathcal{O}(x_0)$ est injective.

Soit gG_{x_0} et hG_{x_0} des éléments de G/G_{x_0} tels que $\bar{f}(gG_{x_0}) = \bar{f}(hG_{x_0})$ ssi $hG_{x_0} = gG_{x_0}$.

$f(g1) = \bar{f}(gG_{x_0}) = \bar{f}(hG_{x_0}) = f(h1) = h * x_0$

$\Rightarrow g * x_0 = h * x_0$ on applique g^{-1}

$g^{-1}g * x_0 = g^{-1}h * x_0$

$x_0 = g^{-1}h * x_0$

donc $g^{-1}h \in G_{x_0}$, donc $\exists k \in G_{x_0}$ tq : $g^{-1}h = k$ $h = gk$

$\Rightarrow hG_0 = gkG_0 = gG_0$

Algèbre I : le 29.03.18

Déf : Soit G, un groupe. Soit $E \subset G$ un sous-ensemble.

On note $\langle E \rangle$, le plus petit sous-groupe de G qui contient E.

On appelle $\langle E \rangle$ le sous-groupe engendré par E.

Prop : $\langle E \rangle$ est bien définit, c'est-à-dire que $\langle E \rangle$ existe et est unique

Preuve : On considère l'intersection de tous les sous-groupes de G qui contiennent E : $\bigcap_{E \subset H < G} H$

Remarquons que $E \subset G$ et que G est un sous-groupe de G.

Une intersection de sous-groupes de G est toujours un sous-groupe de G. (évident)

Ainsi, $\bigcap_{E \subset H < G} H$ est un sous-groupe qui contient E.

C'est le plus petit possible :

Soit J un sous-groupe de G qui contient E.

Ainsi J est un des sous-groupes qui apparaît dans la définition

$\bigcap_{E \subset H < G} H \leq J$

Ainsi, $\langle E \rangle = \bigcap_{E \subset H < G} H$

Cas particulier: E est un singleton $E=\{s\}$ $s\in G$

Déf: Un sous-groupe H d'un groupe G est dit cyclique (ou homogène) s'il est engendré par un élément.

Retour p 16 : déf: On dit que E est un système de générateurs de $\langle E\rangle$.

Remarque: Dans le cas où $\langle E\rangle = G$, on dit que G est engendré par E.

Théorème: Soit H un sous-groupe de $(\mathbb{Z},+)$. Alors H est cyclique, plus précisément, $\exists n\in\mathbb{Z}$ tq $H=\{k\cdot n \text{ où } k\in\mathbb{Z}\}$

Preuve: $0\in H$. Si $H=\{0\}$, $H=\{k\cdot 0 / k\in\mathbb{Z}\}$

Si $\{0\}\subsetneq H$, soit $h\in H$, $h\neq 0$ (Si $h<0$, $(-h)>0$ et $(-h)\in H$)

Donc $\{k\in H : h>0\}\neq\emptyset$
$\subset \mathbb{N}$ qui est bien ordonné donc on peut trouver un + petit élément.

Notons n ce plus petit élément. [$n>0$, $n\in H$ et si $k\in H$ et $k>0$ alors $n\leq k$]

Aff: $H=\{k\cdot n : k\in\mathbb{Z}\}$.

Preuve: Tout d'abord $\{kn : k\in\mathbb{Z}\}\subset H$, en effet: $n\in H$

donc $n+n\in H$, $n+n+n\in H$, ..., $k\cdot n\in H$ (où $k\in\mathbb{N}$)

et ($-n\in H$, $-n-n\in H$ et $-kn\in H$) $k<0$

$H\subset\{k\cdot n : k\in\mathbb{Z}\}$

Soit $h\in H$, $h=kn+r$ $0\leq r<n$ où $k\in\mathbb{Z}$ (Div euclid)

$h-kn=r\in H$ Donc $r=0$
$\in H$ $\in H$
(Sinon r contredirait la minimalité de n)

Donc $h=k\cdot n$, ce qui prouve $H\subset\{kn : k\in\mathbb{Z}\}$

Thm: Classification des groupes cycliques

Les groupes cycliques sont les suivants:

$\mathbb{Z}/n\mathbb{Z}$ $n = 1, \dots$ et $\mathbb{Z}$ $(n = 0)$

Tout groupe engendré par un élément est isomorphe à un groupe de la liste et deux groupes de la liste ne sont pas isomorphes.

Preuve: Soit G, un groupe cyclique. Par définition, il existe donc $s \in G$ tel que le plus petit sous-groupe de G contenant s est égal à G.

$\{s^n : n \in \mathbb{Z}\} \subset G$, on considère l'ensemble des puissances positives et négatives de s. $(s^2 = s \cdot s \subset G)$

C'est un sous-groupe qui contient s. et c'est le plus petit ($s^n \cdot s^m = s^{n+m}$, $s^0 = e$, $s^{-n} \cdot s^n = s^0 = e$, $s^1 = s$) → preuve du ss-grpe sous-groupe de G contenant s.

Donc $\{s^n : n \in \mathbb{Z}\} = G$ ✱

Soit $f : \begin{matrix} \mathbb{Z} & \longrightarrow & G \\ m & \longmapsto & s^m \end{matrix}$ est une application surjective

f est un homomorphisme de groupes:

- $0 \longmapsto e$? $\quad 0 \longmapsto s^0 = e$
- $f(n+m) = s^{n+m} = s^n \cdot s^m = f(n) \cdot f(m)$

$\ker(f)$ est un sous-groupe de $\mathbb{Z}$.

Donc: $\ker(f) = \{k \cdot n \text{ où } k \in \mathbb{Z}\}$ pour un certain $n \in \mathbb{N} \cup \{0\}$

$$\{0\} \longrightarrow \ker f \xrightarrow{i} \mathbb{Z} \xrightarrow{f} G \longrightarrow \{1\}$$

On obtient une suite exacte, donc $\mathbb{Z}/\ker f \simeq G$

Conclusion:

Si $n > 1$ $\quad G = \mathbb{Z}/n\mathbb{Z}$ $\quad (\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$

si $n = 1$ $\quad G = \mathbb{Z}/\mathbb{Z} = \{0\}$

si $n = 0$ $\quad G = \mathbb{Z}/\{0\} = \mathbb{Z}$

Déf: Soit G, un groupe et $g \in \mathbb{Z}$

L'<u>ordre de g</u> est le cardinal du sous-groupe de G engendré par g. $E = \{g\}$, $C(E) = C(g)$ notation

C'est un groupe cyclique, donc $C(g) = \begin{cases} \mathbb{Z} & \text{ordre infini} \\ \mathbb{Z}/n\mathbb{Z} & n = 1, \dots \text{ ordre } n \end{cases}$

$O(g) = |C(g)|$

Prop: L'ordre de g est le + petit entier n tq $g^n = e$

Preuve: Exo

Prop: Soit G un groupe fini. Soit $g \in G$. $O(g) \mid |G|$

L'ordre de g divise le cardinal de G.

Preuve:

$O(g) = |\langle g \rangle|$ $\quad$ $|\langle g \rangle| \mid |G|$ $\Rightarrow$ $O(g) \mid |G|$

L'ordre de g est par déf le cardinal du ss-grpe engendré par g, qui lui divise le cardinal de G (Lagrange)

Anneaux, arithmétique:

Déf: Un **anneau** A est :

(les lois ne sont pas toujours les usuelles)

- un groupe abélien (commutatif) $(A, +)$ (loi du groupe Δ)
  0 est le neutre et $-a$ désigne l'inverse
  ↕ copie "+"
- avec une loi de multiplication : $A \times A \longrightarrow A$ $\quad (a,b) \mapsto a \cdot b$ (loi du groupe)
  - associative : $(ab)c = a(bc)$ $\quad \forall a,b,c \in A$
  - élément neutre : $1_A \cdot a = a \cdot 1_A = a$ $\quad \forall a \in A$
  - distributivité : $a(b+c) = ab + ac$ $\quad \forall a,b,c \in A$
    $(b+c)a = ba + ca$

On dit que A est un anneau commutatif si $ab = ba$ $\forall a,b \in A$

---

le 12.04.18

Remarque: Dans un anneau, on ne demande pas d'inverse pour la multiplication

Ex:

a) $\{0\}$ est l'anneau trivial

b) $\mathbb{Z}$ (pas d'inverse pour "."), $\mathbb{Q}$ et $\mathbb{R}$ (commutatif ss $\mathbb{Z}$) 3

c) $M_n(\mathbb{R})$ munit de l'addition composante par composante et de la multiplication matricielle.

d) $C(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \text{ continue}\}$ munit de l'addition et de la multiplication point par point. (L'anneau n'a pas d'inverse multiplicatif pour tous les f par zéro)

e) Soit A, un anneau commutatif. Alors $A[X]$, l'ensemble des polynômes à coeff dans A et à variable x, est un anneau commutatif

Algèbre I :

Ex : e) (suite)

Un tel polynôme est une somme $\sum_{i\geq 0} a_i x^i$, avec un nbr fini de $a_i \neq 0$

Soient $P(x) = \sum_{i\geq 0} a_i x^i$, $deg(P) = max\{i \mid a_i \neq 0\} = m$ et

$Q(x) = \sum_{j\geq 0} b_j x^j$, $deg(Q) = n$

Les opérations sont :

$(P+Q)(x) = \sum_{k\geq 0} (a_k + b_k) x^k = (a_0 + b_0) + (a_1 + b_1)x + \dots$ ⊕

$(PQ)(x) = \sum_{i+j=k\geq 0} a_i b_j x^k = a_0 b_0 + (a_1 b_0 + a_0 b_1)x^1 + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \dots$ ⊖

Elles sont bien définies car $deg(P+Q) \leq max\{deg P; deg Q\}$

et $deg(PQ) \leq deg(P) + deg(Q)$

(Essayer de trouver un exemple où l'inégalité est nécessaire)

Depuis, $0_{A[X]} = 0 + 0X + 0X^2 + \dots$

$(-P)(X) = (-a_0) + (-a_1)X + \dots$ $\quad 1_{A[X]} = 1 + 0X + 0X^2 \dots$

Les autres propriétés découlent des propriétés de l'anneau

Comme pour les groupes, on a une notion de morphismes qui préservent la structure.

Déf : Soient A et B des anneaux. Un homomorphisme de groupes $\varphi : (A;+) \longrightarrow (B;+)$ est appellé un homomorphisme d'anneaux si $\varphi(1_A) = 1_B$ et $\forall x, y \in A$, $\varphi(xy) = \varphi(x)\varphi(y)$

Ex :

- $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
- $\varphi : A \longrightarrow B$, $\varphi(x) = 0$ $\forall x \in A$, n'est pas un homom. d'anneau sauf si $B = \{0\}$

  Ainsi, il peut arriver qu'il n'existe aucun homom d'anneau entre 2 anneaux. ($\mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}$)

Comme avec les groupes, on a une notion de sous-ensemble qui partage la même structure que l'anneau.

Déf : Soit A un anneau.

- Un sous-anneau B de A est un sous-groupe de $(A;+)$ contenant 1_A tq $\forall x, y \in B$, $xy \in B$.

Déf: (suite)

- Un idéal (bilatère) I de A est un sous-groupe de $(A;+)$ tq $\forall a \in A, \forall x \in I$, $ax \in I$ et $xa \in I$

Ex: Idéaux

- A est un idéal et $\{0\}$ aussi
- $n\mathbb{Z} \subset \mathbb{Z}$ est un idéal
- $\{f: \mathbb{R} \to \mathbb{R} \mid f(1)=0\}$ est un idéal de $C(\mathbb{R})$

Remarque:

- Tout idéal est en particulier un sous-groupe normal de $(A;+)$ car $(A;+)$ est abélien
- Si $1_A \in I$, alors $I = A$ ($\forall a \in A \; 1_A a = a \Rightarrow a \in I$)

La notion d'idéal est celle qui va nous intéresser. En effet, c'est l'analogue des sous-groupes normaux.

Thm: Soit A un anneau et I un idéal de A. Alors $\exists!$ structure d'anneau sur A/I tq $\overline{\pi}: A \to A/I$ est un homom d'anneau.

Remarque:

- Comme I est normal, A/I est bien un groupe et $\overline{\pi}$ est bien un homom de groupe. De plus A/I est abélien, car A l'est aussi.
- On va vouloir définir une multiplication sur A/I. Celle-ci devra satisfaire $(ab+I) = \overline{\pi}(ab) = \overline{\pi}(a)\overline{\pi}(b) = (a+I)(b+I)$ équivalent additif de $gN \cdot \{n \in \mathbb{N} / ng \in \dots\}$

Preuve: On définit
$$\begin{array}{ccc} A/I \times A/I & \longrightarrow & A/I \\ [(a+I);(b+I)] & \longmapsto & (ab+I) \end{array}$$

On doit vérifier que cette application est bien définie et qu'elle respecte les axiomes.

- Bien définie: Rappel: Pour $a \in A$, les $b \in A$ tq $b+I = a+I$ sont exactement les éléments $a+j$, $j \in I$

Donc, on veut mq $\forall j \in I$, $\forall a,b \in A$: $((a+j)+I)(b+I) = (a+I)(b+j+I) = (ab+I)$

Soient $a,b \in A$, $j \in I$. On a $((a+j)+I)(b+I) = (a+j)b + I = ab + jb + I$

$= ab + (\underbrace{jb}_{\in I} + I) = ab + I$. De même pour $(a+I)((b+j)+I)$.

$\downarrow$

I idéal

le 12.04.18

Algèbre I :

Preuve : Suite

- Neutre : $1_{A/I} = 1 + I$ car $(1+I)(a+I) = 1a + I = a + I \quad \forall a \in A$

L'associativité et la distributivité découlent des props de A.

Ex de preuve car chiant et faak (Sdenn)

Ex : $(a+I)[(b+I)+(c+I)] = (a+I)(b+c+I) = (a(b+c)+I)$

$= (ab+ac+I) = (ab+I)+(ac+I) = (a+I)(b+I)+(a+I)(c+I)$

Finalement, on vérifie que :

- π est un homomorphisme d'anneau (π homom groupe ⇒ 2 trucs à vérifier)

Par construction, $\pi(ab) = \pi(a)\,\pi(b) \quad \forall a,b \in A$, de plus

$\pi(1_A) = 1 + I = 1_{A/I}$

Cette structure est unique à cause de la remarque 2. ▨

Exemple : $(\mathbb{Z}/n\mathbb{Z}\,;+;\cdot)$ anneau.

le 19.04.18

Déf : Soit m,n deux entiers positifs, le PGCD (plus grand commun diviseur) de m et n, noté $PGCD(m;n)$, est l'unique entier d positif tq

i) d/m et d/n

ii) si d'/m et d'/m, alors $d' \leq d$ (nous verrons que $d' | d$)

Thm de Bézout : Soient $m,n \in \mathbb{Z}$, Alors

a) le + petit idéal de $\mathbb{Z}$ contenant m et n est constitué des multiples entiers de $PGCD(|m|,|n|)$

b) $\exists k,l \in \mathbb{Z}$ tq $PGCD(|m|,|n|) = km + ln$

c) $\forall d \in \mathbb{Z}$ si $d|m$ et $d|n$ alors $d | PGCD(|m|,|n|)$

Preuve : Posons $I := \{ km + ln \mid k,l \in \mathbb{Z} \}$, Alors I contient $m\,(k=1,l=0)$ et $n\,(k=0,l=1)$, et est un idéal de $\mathbb{Z}$. De plus tout idéal de $\mathbb{Z}$ contenant m et n contient I, c'est donc le plus petit idéal de $\mathbb{Z}$ contenant m et n. Comme I est un sous-groupe de $(\mathbb{Z};+)$ il est donc cyclique. Soit donc $d \in \mathbb{Z}$ un générateur de I.

le 19.04.18

Preuve: (Suite)

Alors $I = \langle d \rangle = d\mathbb{Z} = \{kd \mid k \in \mathbb{Z}\}$, sans perdre la généralité on prend $d \geq 0$.

Affirmation: $d = PGCD(|m|; |n|)$

Preuve: Comme $d \cdot k = m$ pour un $k \in \mathbb{Z}$, on a $|m| = \pm kd$ de même pour n. Donc $d \mid |m|$ et $d \mid |n|$.

Soit d' entier positif tq $d' \mid |m|$ et $d' \mid |n|$. Alors $m, n \in \langle d' \rangle$

Or par la minimalité de I, on a que $\langle d \rangle = I \subset \langle d' \rangle$

Ceci implique que $d = kd'$ pour un certain $k \in \mathbb{Z}$, ie $d' \mid d$

Ceci prouve l'affirmation et le pt c) du thm de Bézout ∎

Comme $\{kd \mid k \in \mathbb{Z}\} = I = \{km + ln \mid k, l \in \mathbb{Z}\}$ les points a) et b) sont aussi satisfaits par l'affirmation ∎

Déf: Deux entiers m, n sont premiers entre eux si $PGCD(|m|, |n|) = 1$

Ex: i) 13 et 10 sont premiers entre eux
ii) 12 et 35 " "
iii) 8 et 12 ne le sont pas, car $PGCD(8, 12) = 4$.

Déf: Un entier positif $p \neq 1$ est premier si ses seuls diviseurs positifs sont 1 et p.

Lemme de Gauss: Soit p un nombre premier et soient a, b des entiers positifs, Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Preuve: Supposons que $p \mid ab$ et que $p \nmid a$ (p ne divise pas a)

Mq alors $p \mid b$, ce qui prouvera le Lemme.

Comme p premier et $p \nmid a$ alors $PGCD(a, p) = 1$. Par le thm de Bézout (b) $\exists k, l \in \mathbb{Z}$ tq $1 = kp + la$ Donc $b = bkp + bla$. Comme par hyp $p \mid ab$ on a que p divise le membre de droite $(bkp + lab) \Rightarrow p \mid b$ ∎

le 19.04.18

Algèbre I :

Rem : Soit p un nombre premier, soyent $m, n \in \mathbb{Z}$, soyent $k, L \in \mathbb{N} \cup \{\infty\}$.

Alors si $p^k m = p^L n$ et $p \nmid m$ et $p \nmid n$ $\Rightarrow k = L$ et $m = n$

Preuve : si $k \geq L$, alors $p^{k-L} m = n \Rightarrow k = L \Rightarrow m = n$ $\blacksquare$
$p \nmid n$

Déf : Soit p un nombre premier. On définit $v_p : \mathbb{N} \longrightarrow \mathbb{N} \cup \{\infty\}$, $n \longmapsto v_p(n) =$ le plus grand entier k tq $p^k \mid n$

pour $n \in \mathbb{N}$, $v_p(n)$ est appellée la valuation p-adique de n

Dans ce cas, on a $n = p^{v_p(n)} \cdot k$ avec $k \in \mathbb{Z}$ et $p \nmid k$

Prop : Soit p un nombre premier. Pour $m, n \in \mathbb{N}$, on a $v_p(m \cdot n) = v_p(m) + v_p(n)$.

Preuve : Écrivons $m = p^{v_p(m)} \cdot k$, $p \nmid k$ et $n = p^{v_p(n)} \cdot L$, $p \nmid L$

$\Rightarrow m \cdot n = p^{v_p(m) + v_p(n)} k \cdot L$ et on a que $p \nmid k \cdot L$ par lemme de Gauss

Par la remarque précédente (p. 24), on a que $v_p(m \cdot n) = v_p(m) + v_p(n)$ $\blacksquare$

Théorème fondamental de l'arithmétique :

Soit $n \in \mathbb{N}$, alors $\exists !$ écriture $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ où $\mathcal{P}$ est l'ensemble des nbr premiers

Preuve : • Unicité : Découle de la remarque

• Existence : Récurrence sur n

Pour $n = 1$, on prend $v_p(1) = 0$ $\forall p \in \mathcal{P}$ et on a le résultat.

Supposons que le résultat est vrai jusqu'à $n-1$, mq il reste vrai pour n

- Si les seuls diviseurs de n sont 1 et n, alors n est premier donc le résultat est vrai.
- Sinon, $\exists d$ diviseur de n tq $d \neq 1$ et $n \neq d$. Donc $\exists k \in \mathbb{Z}$ tq $n = dk$ avec $d < n$ et $k < n$.
  Par l'hyp de récurrence on a $d = \prod_p p^{v_p(d)}$ et $k = \prod_p p^{v_p(k)}$
  $\Rightarrow n = \prod_p p^{v_p(d) + v_p(k)} = \prod_p p^{v_p(dk)} = \prod_p p^{v_p(n)}$ $\blacksquare$

Thm : Euclide

Il existe une infinité de nombre premier.

Preuve : Par l'absurde, supposons qu'il existe un nbr fini de nbr premier.

Notons $\mathcal{P} = \{p_1, \dots, p_n\}$. Posons $N = 1 + p_1 \dots p_n$. Soit $p \in \mathcal{P}$ tq $v_p(N) > 0$

Alors $p \mid N \Leftrightarrow p \mid 1 + p_1 \dots p_n \Rightarrow p \mid 1$ Contradictoire. $\blacksquare$

$\exists j \in \{1, \dots, n\}$ tq $p = p_j$

Notation: Soient m, n des entiers positifs. Le plus petit commun multiple (PPCM) de m et n est noté $PPCM(m,n)$

Prop: Soyent m, n des entiers positifs. Alors :

1) $PPCM(m,n) = \prod_{p \in \mathbb{P}} p^{\max\{v_p(m); v_p(n)\}}$

2) $PGCD(m,n) = \prod_{p \in \mathbb{P}} p^{\min\{v_p(m); v_p(n)\}}$

3) $PGCD(m,n) \cdot PPCM(m,n) = m \cdot n$

Preuve : 1) $\prod_{p \in \mathbb{P}} p^{\max\{v_p(m); v_p(n)\}}$ est bien un multiple de m et n, et c'est le + petit possible.

2) $\prod_{p \in \mathbb{P}} p^{\min\{v_p(m); v_p(n)\}}$ est bien un diviseur de m et n, et c'est le + grand possible.

3) Découle du fait que $\forall a,b \in \mathbb{N} \cup \{0\}$, $\max\{a,b\} + \min\{a,b\} = a+b$.

---

le 26.04.18

Déf: Soit A un anneau avec élément neutre pour la multiplication (unitaire) ($\exists 1 \in A, \forall a \in A \quad 1 \cdot a = a \cdot 1 = a$) On appelle unité tout $a \in A$ pour lequel il existe $v \in A$: $av = va = 1$.

Prop: $A^* = \{a \in A \mid \exists v \in A : av = va = 1\}$ est un groupe pour la multiplication.

Preuve: Soit $a,b \in A^*$, vérifions que $a \cdot b \in A^*$ soit $v \in A$ tq $av = va = 1$ et soit $v \in A$ tq $vb = bv = 1$

$abvv = a \cdot bv \cdot v = a \cdot 1 \cdot v = av = 1$. de même $vv \cdot a \cdot b = 1$

$1 \in A^*$ $1 \cdot 1 = 1$ est l'élément neutre. ($1 \cdot a = a$)

Si $a \in A^*$, il existe $v \in A$: $a \cdot v = v \cdot a = 1$ v est aussi une unité donc $v \in A^*$.

Déf: Un corps est un anneau unitaire A tq $A^* = A \setminus \{0\}$ ($0 \neq 1$)

Déf: Un anneau est intègre si $ab = 0 \Rightarrow a = 0$ ou $b = 0$ $\forall a,b \in A$

Prop: Un corps est intègre

Preuve: Soient $a,b \in A$ tq $a \neq 0$ $b \neq 0$. Par hypothèse $A \setminus \{0\} = A^*$
Soit $v \in A$ tq $va = av = 1$ et soit $v \in A$ tq $bv = vb = 1$
$vabv = 1 \cdot 1 = 1$ donc $ab \neq 0$ (On a prouvé la contraposée)

$(P \Rightarrow Q) \iff (\neg Q \Rightarrow \neg P)$

Prop: Soit A un anneau unitaire. Supposons que A est fini.
$|A| < \infty$. Alors A est intègre $\Leftrightarrow$ A est un corps.

Preuve: On a vu qu'en général si A est un corps alors A est intègre.
Supposons A intègre et montrons que A est un corps.
Soit $a \in A$, $a \neq 0$, Cherchons un inverse.
Soit $M_a : (A,+) \longrightarrow (A,+)$, $x \longmapsto x \cdot a$ M_a est un homom de groupe pour $(A,+)$
$\ker(M_a) = \{x \in (A,+) \mid M_a(x) = 0\} = \{0\}$ ($a \neq 0$ et A intègre) $\Rightarrow M_a$ injective.
Comme $|A| < \infty$ M_a est une bijection.
Donc $1 \in \mathrm{Im}(M_a)$ $\exists x \in A$ tq $x \cdot a = 1 = a \cdot x$ (ûn raisonnement avec aM)
Donc a possède bien un inverse. ∎

Prop. Soit $m \in \mathbb{N}$, $A = \mathbb{Z}/m\mathbb{Z}$ sont équivalents
1) A est intègre 2) A est un corps 3) m est premier

Ex:
- $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre ($[2]\cdot[3] = [0]$ mais $[2] \neq [0] \neq [3]$ ($2 \cdot 3 = 0$ mais $2 \neq 0 \neq 3$) ↑ ce sont des classes
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}$ (↑ intègres, ↑ pas intègre)

Preuve: A intègre $\Rightarrow$ A corps (déjà vu $< \infty$)
m premier $\Leftrightarrow$ $A^* = A \setminus \{0\}$
Soit $0 < a < m$ $[a] \in \mathbb{Z}/m\mathbb{Z}$ si $m = p$ est premier alors
$(p,a) = 1$ $\Rightarrow$ p et a sont premier entre eux: $\exists k, l \in \mathbb{Z}$
$kp + la = 1$ (Bezout)
Donc $al \equiv 1 \bmod p$ où $p = m$
Donc $[a]\cdot[1] = [1]$ $[a]$ est bien inversible
$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/m\mathbb{Z}$, $l \longmapsto [l]$ Réciproquement : si $m = ab$, $a,b \in \mathbb{N}$
$a \neq 1$ et $b \neq 1$ $\mathbb{Z}/m\mathbb{Z}$ $[a][b] = [ab] = [m] = 0 \in \mathbb{Z}/m\mathbb{Z}$
($[a] \neq 0$, $[b] \neq 0$)

Prop: Soit $[a] \in \mathbb{Z}/m\mathbb{Z}$. Alors $[a] \in (\mathbb{Z}/m\mathbb{Z})^* \iff (a,m) = 1$

Preuve:

- Si $(a,m) = 1 \xrightarrow{\text{Bézout}} \exists k, l \in \mathbb{Z}$ tq $ka + lm = 1$ $\pi(ka+lm) = \pi(1)$

  (π: homom d'anneau) $\pi(k)\pi(a) + \pi(l)\pi(m) = \pi(1)$

  $[k][a] = [1] \Rightarrow [a]$ est inversible.

- Réciproquement si $[a] \in (\mathbb{Z}/m\mathbb{Z})^* \Rightarrow \exists k \in \mathbb{Z}/m\mathbb{Z}$ tq $[k][a] = [1]$

  $\exists s \in \mathbb{Z}$ tq $ka = 1 + sm \Rightarrow 1 = ka + \tilde{s}m \Rightarrow (a,m) = 1$

Rappel: Si $a, b \in \mathbb{Z}$ PGCD$(a,b) = d$ où $d > 0$ est générateur de $I = \{ka + lb : k, l \in \mathbb{Z}\}$ le plus petit idéal / ss-groupe contenant a et b. $I = \langle d \rangle$ (Super Important)

Déf: L'indicateur d'Euler $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$

C'est-à-dire que $\varphi(m)$ compte le nombre d'entier dans la liste $1, 2, 3, \ldots, m$ qui sont premiers à m.

Ex: $\varphi(p) = p - 1$ si p premier

on retrouve $p - 1 = \varphi(p)$ ainsi : si p premier $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ est un corps

et donc $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1 \Rightarrow \mathbb{Z}/p\mathbb{Z} \setminus \{0\} = (\mathbb{Z}/p\mathbb{Z})^*$

Prop: Soient A et B deux anneaux unitaires.
Alors $A \times B$ est un anneau unitaire et $(A \times B)^* = A^* \times B^*$

Preuve: $(a,b) + (a',b') = (a+a', b+b')$ $(a,b) \cdot (a',b') = (aa', bb')$.

$(a,b) \cdot (1_A, 1_B) = (a,b)$ donc $1_{A\times B} = (1_A, 1_B)$ pas ici.

$(a,b) \in (A \times B)^* \iff \exists (u,v) \in A \times B : (a,b)(u,v) = (1_A, 1_B) = 1_{A\times B}$

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

Théorème chinois: Si m et n sont premiers entre eux, alors

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & (\underset{\tilde{\pi}_m(x)}{x}, \underset{\tilde{\pi}_n(x)}{x}) \end{array}$$

est un isomorphisme d'anneaux.

le 26.04.18

Algèbre I :

Preuve : $\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ est bien un homom d'anneaux

$x \longmapsto x$

$\mathbb{Z} \xrightarrow{\pi_m} \mathbb{Z}/m\mathbb{Z}$ $\quad \ker(\pi_{mn}) = mn\mathbb{Z} \subseteq m\mathbb{Z} = \ker(\pi_m)$

$\pi_{mn} \downarrow \quad \nearrow ? \ \tilde{\pi}_m$

$\mathbb{Z}/mn\mathbb{Z}$ $\quad$ donc $\tilde{\pi}_m$ existe et est un homom. d'anneaux.

Surjection : c'est surjectif car l'image contient un système de générateur $(1,0)$ et $(0,1)$ qui engendrent $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$1 = km + ln \ (\exists k, l \in \mathbb{Z} \ (m,n) = 1)$

$|\mathbb{Z}/mn\mathbb{Z}| = mn = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|$

Prop : si $(m,n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

Preuve : (Thm chinois) $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

donc $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*$

$\cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$

Algèbre I : le 03.05.18

Rappel : si $m \in \mathbb{N}$, $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$

Prop : si $(m;n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Thm : (Euler) $\forall m \in \mathbb{N}$, $\varphi(m) = m \cdot \prod_{p/m} (1 - \frac{1}{p})$ où le produit porte sur les facteurs premiers de m.

Preuve : On applique le thm fondamental de l'arithmétique :

$m = \prod_{p \in \mathcal{P}} p^{v_p(m)}$ tout entier m s'écrit de manière unique comme produit de puissance de ses facteurs premiers.

Donc $\varphi(m) = \varphi\left(\prod_{p \in \mathcal{P}} p^{v_p(m)}\right) = \prod_{p \in \mathcal{P}} \varphi\left(p^{v_p(m)}\right)$

Exemple : $\varphi(p) = p - 1 = |(\mathbb{Z}/p\mathbb{Z})^*|$ $\quad \varphi(p^2) = p^2 - p = p^2(1 - \frac{1}{p})$

Ne sont pas premiers $(0, p, 2p, \dots p(p-1), p^2)$

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

Ne sont pas premier $(0, p, 2p, \dots (p^{k-1} - 1)p, p^k)$ avec p^k

les multiples de p sont les entiers qui ne sont pas premier à p^k

Exactement.

le 03.05.18

Preuve: (suite)

On a donc $\varphi(m) = \prod_{p \in \mathcal{P}} \varphi(p^{v_p(m)}) = \prod_{p \in \mathcal{P}} (p^{v_p(m)} - p^{v_p(m)-1})$

$= \prod_{p \in \mathcal{P}} p^{v_p(m)} (1 - \frac{1}{p}) = m \cdot \prod_{p \mid m} (1 - 1/p)$ ▨

Ex: $m = 18 = 3 \cdot 3 \cdot 2 = 3^2 \cdot 2$ $\quad p = 5 \quad v_5(18) = 0$

$v_3(18) \quad v_2(18)$ $\quad p = 7 \quad v_7(18) = 0$

$m = 18 = 3 \quad \cdot 2$

(pour la décomposition en facteur premier, on ne prend que les p qui divisent m)

Prop: (Euler) (RSA) Soient $m, x \in \mathbb{N}$ tq $(m, x) = 1$. Alors $x^{\varphi(m)} \equiv 1 \bmod m$

Preuve: On voit x comme un élément de $(\mathbb{Z}/m\mathbb{Z})^* \ni [x]$ classe modulo m de x. $G = (\mathbb{Z}/m\mathbb{Z})^*$ est un groupe pour la multiplication. On a $[x]^{|G|} = e \in G$ élément neutre

(Pourquoi? car si G est un grp fini et si $x \in G$, alors $x^{|G|} = e$

En effet : soit $\theta(x) :=$ l'ordre de $x = |\langle x \rangle| =$ + petit k tq $x^k = e$. On sait $|\langle x \rangle|$ divise $|G|$, on sait donc $x^{|G|} = e = x^{\theta(x) \cdot d}$ où $d \cdot \theta(x) = |G|$ et donc $(x^{\theta(x)})^d = e^d = e$)

On sait que $|G| = |(\mathbb{Z}/m\mathbb{Z})^*| = \varphi(m)$

et donc $[x]^{\varphi(m)} = [x]^{|G|}$ ce qui se traduit $x^{\varphi(m)} \equiv 1 \ [m]$ ▨

Corps, sous-corps, extensions :

Rappel: **Déf:** un corps est un anneau unitaire dans lequel tout élément à un inverse multiplicatif (sauf 0)

Rem: Il existe des corps non-commutatif (ou corps gauche)

Thm: Tous les corps finis sont commutatifs. ($\mathbb{Z}/p\mathbb{Z}$)

Prop: Soit A un anneau commutatif unitaire. Soit $I < A$ un idéal. Alors A/I est un corps $\Leftrightarrow$ I est maximal.

Illustration: $A = \mathbb{Z}$ et $I = m\mathbb{Z}$ les multiples d'un entier m

On sait que $\mathbb{Z}/m\mathbb{Z}$ est un corps $\Leftrightarrow$ m est premier

Donc $m\mathbb{Z}$ est maximal $\Leftrightarrow$ m est premier.

le 03.05.18

Algèbre I :

Déf : On dit que I un idéal de A est maximal $\Leftrightarrow$ soit J un idéal de A tq $I \subset J \subset A$ alors soit $J = I$, soit $J = A$

Preuve : (Prop) • Supposons I est maximal (on sait que A/I est un anneau avec unité $1_{A/I} = 1_A + I \in A/I$.)

Il faut donc mq si $[a] \in A/I$ tq $[a] \neq 0 \in A/I$ alors $\exists [b] \in A/I$ tq $[a][b] = 1_{A/I}$.

On sait que $[a] \neq 0 \in A/I$ donc $a \notin I$, soit J le + petit idéal de A qui contient I et a. $J = \{xI + ya \mid x, y \in A\}$

$= \{xb + ya : x, y \in A \text{ et } b \in I\}$

Comme $a \in J \supset I$ et $a \notin I$ par maximalité de I, on a $J = A$

En particulier $1_A \in J$, donc $\exists x, y \in A$ et $b \in I$ tq $1_A = xa + yb$

Cette égalité vue dans le quotient A/I. On applique $\pi : A \to A/I$, $a \mapsto [a]$

ai en particulier $\pi(1_A) = 1_A + I = [1]$

Donc $1_{A/I} = \pi(1_A) = \pi(x)\pi(a) + \pi(b)\pi(y) = [x][a] + [y] \cdot 0_{A/I} = [x][a]$

$0_{A/I} = I \in A/I$

• Supposons A/I est un corps et mq I est maximal.

Soit J un idéal de A tq $I \subset J \subset A$, on doit mq $J = A$

Soit $a \in J \setminus I$. Donc $[a] \neq 0_{A/I} = I$. Par hypothèse $\exists b \in A$, $[a][b] = 1_{A/I}$. Donc $(a + I)(b + I) = 1_A + I$

donc $1_A \in J$ / En effet : $1_A = \underbrace{ab}_{\in J} + \underbrace{aI + Ib + I^2 - I}_{\in I \subset J}$

Donc $b \in J$ ce qui amène à $1_A \in J$)

Donc $A = J$ car si $1_A \in J$ alors $\forall a \in A$ $1_A \cdot a \in J$

et $a \cdot 1_A \in J$ donc $\forall a \in A$ $a \in J$.

On a bien mq I est maximal ▨

Programme: pour écrire ii2

- On va définir l'anneau des suites de Cauchy de rationels

Déf: Soit $A = \{ (x_n)_{n\in\mathbb{N}} : x_n \in \mathbb{Q}$ qui est de Cauchy $\}$

$\forall n \in \mathbb{N}, \exists N \in \mathbb{N}, \forall p,q \in \mathbb{N} \quad |x_{N+q} - x_{N+p}| < \frac{1}{n}$

C'est un anneau. (à démontrer)

Déf: $I = \{ (x_n)_{n\in\mathbb{N}} \in A : \lim_{n\to\infty} x_n = 0 \}$

- On choisit un idéal maximal (à démontrer)

---

le 17.05.18

Rappel: On note (x_n) une suite d'éléments de $\mathbb{Q}$, on suppose

(x_n) de Cauchy $\forall \varepsilon > 0 \ \varepsilon \in \mathbb{Q} \ \exists N \in \mathbb{N}$ si $n,m > N \ |x_n - x_m| < \varepsilon$

Rem: On utilise uniquement les rationels.

Preuve: $A := \{ (x_n)_{n\in\mathbb{N}} : x_n \in \mathbb{Q}$ qui est de Cauchy $\}$

C'est un anneau :

(x_n) et (y_n) de Cauchy $\longrightarrow$ $(x_n + y_n)$ de Cauchy

// $\longrightarrow$ $(x_n \cdot y_n)$ de Cauchy

$\underline{0} = (0,0\ldots0) \qquad \underline{1} = (1,1\ldots1)$

Prop: $I = \{ (x_n)_{n\in\mathbb{N}} \in A : \lim_{n\to\infty} x_n = 0 \}$ est un idéal maximal

Preuve: Si (x_n) et $(y_n) \in I \Rightarrow \lim_{n\to\infty} (x_n + y_n) = 0 = \lim x_n + \lim y_n$

Soit $(x_n) \in I$ et $(a_n) \in A$

alors $(a_n)\cdot(x_n) = (a_n \cdot x_n) \quad \lim_{n\to\infty} a_n \cdot x_n = 0$ (Vrais car a_n bornée)

$I < A$ est maximal:

Soit $J > I \subset A$ où J est idéal de A. Soit $(y_n) \in J \setminus I$

[(y_n) ne tend pas vers 0] Donc $\exists \delta > 0 \ \forall N \in \mathbb{N} \ \forall n > N \ |y_n| > \delta$

Soit $M > \max\{|y_1| \ldots |y_N|\}$, Soit $z_n = y_n + (\underbrace{M,\ldots,M}_{N}, 0, \ldots 0)$

$(z = (z_n) \in A)$

Soit $z^{-1} := (z_1^{-1}, \ldots, z_n^{-1}\ldots)$ forme une de Cauchy.

le 17.05.18

Algèbre I :

Preuve : (suite)

$z^{-1} := (z_1^{-1}; \dots; z_n^{-1}; \dots)$ forme une suite de Cauchy. Ceci car les (y_n) forment une suite de Cauchy et $|y_n| > \delta$ si $n > N$ ($\sin n > N$ $z_n = y_n$)

$z \cdot z^{-1} = (z_1, z_2, \dots z_n, \dots) \cdot (z_1^{-1}; z_2^{-1}; \dots; z_n^{-1}; \dots) = (1; \dots; 1)$

$z = y + (\underbrace{\pi, \pi, \dots; \pi}_{N}; 0; \dots 0) \quad y \in J \Rightarrow z \in J \quad z^{-1} \in A$

$\in I \subset J$

et donc $z \cdot z' \in J \Rightarrow (1, \dots 1) \in J \Rightarrow J = A \quad ((1, \dots 1) = 1_A)$

On a Donc I est un idéal maximal de A.

Conséquence : le quotient A/I est un corps commutatif.

On définit $\mathbb{R} := A/I$.

- Comment penser à $x \in \mathbb{R}$. $x = (x_1, \dots, x_n, \dots) + I$ ← les suites de Cauchy qui tendent vers 0.

où $(x_1 \dots x_n \dots) \in A$ est une suite de Cauchy de $\mathbb{Q}$.

Déf : $x \in \mathbb{R} = A/I$ est positif si : ou bien $x = 0 \in A/I$ ou bien $\exists \delta > 0$ et $N \in \mathbb{N}$: $\forall n \geq N \quad x_n > \delta$ $\quad \mathbb{R}^+ = \{x \in \mathbb{R}, x \geq 0\}$ et $\mathbb{R}^+_* = \{x \in \mathbb{R}, x > 0\}$

Ex :
- $[(-1; -1/2; -1/3; \dots; -1/n \dots)] = 0 = I$
- $[(-10; 1; -100; 1; 1 - 1/n; \dots)] > 0$

Déf : $x, y \in \mathbb{R}$, on dit que x est + grand ou = à $y \Leftrightarrow x - y \geq 0$

Proposition : la relation $x \geq y$ sur $\mathbb{R}$ est une relation d'ordre totale

ie : $\forall x, y, z \in \mathbb{R}$ i) 1) $x \leq y$ et $y \leq z \Rightarrow x \leq z$ (transitif)

2) $x \leq x$ (Réflexif) 3) $x \leq y$ et $y \leq x \Rightarrow x = y$ (ordre)

4) soit $x \leq y$ soit $y \leq x$ (ordre total)

ii) $\mathbb{R} = (-\mathbb{R}^*_+) \sqcup \{0\} \sqcup \mathbb{R}^*_+$

iii) Compatibilité de $\geq$ avec les lois :

1) $x \geq y$ et $z \geq t \Rightarrow x + z \geq y + t$

2) $x \geq 0$ et $y \geq 0 \Rightarrow x \cdot y \geq 0$

Déf: Soit $x, y \in \mathbb{R}$ alors $\max\{x;y\} = \begin{cases} y & \text{si } x \leq y \\ x & \text{si } y \leq x \end{cases}$

Déf: Soit $x \in \mathbb{R}$, alors on définit sa norme $|x| := \max\{x; -x\}$

Prop: $\mathbb{R} \longrightarrow \mathbb{R}_+$, $x \longmapsto |x|$ vérifie : i) $|x| \geq 0$ ii) $|xy| = |x||y|$

iii) $|x| = 0 \iff x = 0$ iv) $|x+y| \leq |x| + |y|$

Prop: 1) A anneau commutatif unitaire, Alors A est un corps $\iff$ les seuls idéaux de A sont $\{0\}$ et A.

2) Soit $h: A \to B$ un homomorphisme entre 2 corps, alors h est injectif.

Preuve: 1) Soit A, un corps et J un idéal de A tq $J \neq \{0\}$

Soit $x \in J$, $x \neq 0$, alors $x^{-1} \in A$ et $1 = x^{-1} x \Rightarrow J = A$

Si les seuls idéaux de A sont $\{0\}$ et A. Soit $x \in A$, $x \neq 0$

Soit J = le + petit idéal de A qui contient x.

$J = \{xa \mid a \in A\}$ comme $x \neq 0 \in J \Rightarrow J = A$

par hyp. $ax = 1$ pour un certain $a \in A$. $\Rightarrow$ A est un corps.

2) $\ker h < A$ est un idéal de A comme $h(1_A) = 1_B \neq 0_B$

alors $\ker h \neq A$ comme A est un corps alors $\ker h = \{0\}$

$\Rightarrow$ h est surjectif.

Prop: $\mathbb{Q} \xrightarrow{h} \mathbb{R}$, $q \longmapsto [(q,q,\dots)]$ est un homomorphisme de corps

1) $h(|q|) = |h(q)| \quad \forall q \in \mathbb{Q}$

2) $\mathbb{Q}$ est dense dans $\mathbb{R}$ (ie: $h(\mathbb{Q}) \subset \mathbb{R}$ est un ss-ensemble dense de $\mathbb{R}$

$\forall x \in \mathbb{R}\ \forall \varepsilon > 0\ \varepsilon \in \mathbb{Q}\ \exists q \in \mathbb{Q} \xhookrightarrow{h} \mathbb{R}$

$|q - x| < \varepsilon$)

Algèbre I :

Preuve : C'est bien un homomorphisme. C'est donc une application injective.

(on pense à h comme à une inclusion et on confond q et $h(q)$.

1) $h(|q|) = \begin{cases} h(q) & \text{si } q \geq 0 \\ h(-q) & \text{si } q < 0 \end{cases}$ $(\forall q \in \mathbb{Q}) = \begin{cases} [(q\ldots\ q)] & \text{si } q \geq 0 \\ [(-q\ldots\ -q)]] & \text{si } q < 0 \end{cases}$

$|h(q)| = |[(q,\ldots\ q)]| = \begin{cases} [(q\ldots\ q)] & \text{si } q \geq 0 \\ -[(q\ldots\ q)] & \text{si } q < 0 \end{cases} = \begin{cases} [(q\ldots)] & \text{si } q \geq 0 \\ [(-q\ldots 1] & \text{sinon} \end{cases}$

2) Soit $x \in \mathbb{R}$, $\varepsilon > 0$ $\varepsilon \in \mathbb{Q}$, $x = [(x_1, x_2, \ldots\ .)]$ $x_1 \ldots \in \mathbb{Q}$

de Cauchy. Soit N : $n, m \geq N : |x_n - x_m| < \varepsilon/2$

$q = [(x_N; x_N; \ldots\ .)] \in \mathbb{Q} = h(\mathbb{Q}) \subset \mathbb{R}$

Affirmation : $\varepsilon \leq q - x \leq \varepsilon$ relations entre nbr réels.

Preuve : On a d'une part $x + \varepsilon - q \geq 0$

En effet, si $m > N$ $x_m + \varepsilon - q_m = x_n + \varepsilon - x_N \geq \varepsilon/2$

de $\hat{m}$ pour $\varepsilon \leq q - x$.

⌟

Fin de la construction de $\mathbb{R}$: le 24.05.18

Lemme : Soit $x \in \mathbb{R}$, soit (x_n) une suite de Cauchy de rationel tq $[(x_n)] = x$. $x_n := h(x_n) \in \mathbb{R}$ $\left(h(x_n) = [(x_1, x_2 \ldots)]\right)$

la suite $x_1, x_2, \ldots, x_n, \ldots$ de réel converge vers x.

Preuve : Soit $\varepsilon > 0$, $\varepsilon \in \mathbb{Q}$ donné, Soit $N \in \mathbb{N}$, $n m \geq N$ $|x_n - x_m| < \varepsilon/2$

ici x_n et x_m sont des éléments de $\mathbb{Q}$

(N existe car on a supposé $(x_n)_{n \in \mathbb{N}}$ de Cauchy)

Donc si $n, m \geq N$ on a : $\varepsilon + x_n - x_m > \varepsilon/2$
$\varepsilon + x_m - x_n > \varepsilon/2$

Donc $\varepsilon + x_n - x > 0$ vus comme nobres réels
$\varepsilon + x - x_n > 0$ (déf de positivité)

Toute suite de Cauchy converge

le 24.05.18

Thm : $\mathbb{R}$ est un corps commutatif totalement ordonné, complet

(Qui contient $\mathbb{Q}$ comme corps (sous-) dense)

Preuve : Tout a été prouvé, sauf la complétude. ← Dernière Étape de la construction de $\mathbb{R}$

Soit $x_1, x_2, \dots, x_n, \dots$ une suite de Cauchy de nombres réels. Comme $\mathbb{Q} \subset \mathbb{R}$ est dense, on peut choisir $\forall n \in \mathbb{N}$,

$q_n \in \mathbb{Q} \subset \mathbb{R}$: $|q_n - x_n| < \frac{1}{n}$

Affirmation : la suite $q_1, \dots, q_n, \dots$ est de Cauchy

Preuve : Soit $\varepsilon > 0$, $\varepsilon \in \mathbb{Q}$, soit $N \in \mathbb{N}$: $n, m \geq N$ alors $|x_n - x_m| \leq \varepsilon/2$

(N existe car $x_1, \dots, x_N, \dots$ est de Cauchy) $N \geq 4/\varepsilon$

$|q_m - q_n| = |q_m - x_m + x_m - x_n + x_n - q_n| \leq |q_m - x_m| + |x_m - x_n|$

$+ |x_n - q_n| \leq \frac{1}{m} + \varepsilon/2 + 1/n \leq \frac{2}{N} + \frac{\varepsilon}{2} \leq \varepsilon.$ ∎

$x = [(q_1, \dots, q_n \dots)] \in \mathbb{R}$

Prouvons $\lim_{n \to \infty} x_n = x$.

On a : $|x - x_n| \leq |x - q_n| + |q_n - x_n| \leq |x - q_n| + 1/n$ $\leq 1/n$

d'après le lemme $\lim_{n \to \infty} q_n = x$ donc $\lim_{n \to \infty} |x - q_n| = 0$

Donc $\lim_{n \to \infty} |x - x_n| \leq \lim_{n \to \infty} 1/n = 0$ ∎

Le corps des nombres complexes comme extension du corps des nombres réels

Thm : Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$, l'anneau des polynômes à coefficients dans $\mathbb{K}$. Alors $\mathbb{K}[X]$ est euclidien.

C'est-à-dire, si $P, Q \in \mathbb{K}[X]$ et $Q \neq 0$ alors il existe un unique $D \in \mathbb{K}[X]$, un unique $R \in \mathbb{K}[X]$ tel que :

i) $P = D \cdot Q + R$

ii) $R = 0$ ou $\deg R < \deg Q$

C'est l'analogue de la division euclidienne dans $\mathbb{Z}$.

Preuve : Soit $\langle Q \rangle$ l'idéal de $\mathbb{K}[X]$ engendré par Q, soit $\pi : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]/\langle Q \rangle$ la projection canonique.

Soit $G_n < \mathbb{K}[X]$ l'espace vectoriel sur $\mathbb{K}$ des polynômes de $\mathbb{K}[X]$ de degré $\leq n$. $\mathbb{K}[X] = \bigcup_{n \in \mathbb{N}} G_n$

On applique π : $\mathbb{K}[X]/\langle Q \rangle = \bigcup_{n \in \mathbb{N}} \pi(G_n)$

Soit $d+1$ le degré de Q (On peut supposer $\deg Q \geq 1$, car si $\deg Q = 0$ ie $Q = q \in \mathbb{K}$ $q \neq 0$ $P = \underbrace{q}_{Q} \cdot \underbrace{q^{-1} P}_{D} + \underbrace{0}_{R}$)

Affirmation : $\bigcup_{n \in \mathbb{N}} \pi(G_n) = \pi(G_d)$

Preuve : Il suffit de prouver que si $n \geq d$ $\pi(G_{n+1}) = \pi(G_n)$

Faisons une récurence sur n avec le pas initial $n = d$

- si $n = d$ $\pi(G_{d+1}) = \pi(G_d)$ il suffit de prouver

$$\pi(X^{d+1}) \in \pi(G_d)$$

(Remarque : π est un homom d'anneau et une app lin d'un ev sur $\mathbb{K}$, $\langle Q \rangle$ est un idéal, mais aussi un ss. e.v et donc $\mathbb{K}[X]/Q$ est aussi un ss ev)

$\pi(X^{d+1}) \in \pi(G_d)$ car $Q(X) = q_{d+1} X^{d+1} + \dots + q_1 X + q_0$

$\Rightarrow q_{d+1}^{-1} Q(X) = X^{d+1} + R(X)$ où $R(X) \in G_d$ donc

$X^{d+1} = -R(X) + q_{d+1}^{-1} Q(X)$ donc $\pi(X^{d+1}) = \pi(-R(X)) \in \pi(G_d)$

($\pi(Q(X)) = 0$)

Preuve de Aff dans Preuve de thm.

- si $n \geq d$: Supposons $\Pi(G_{n+1}) = \Pi(G_n)$

Montrons alors $\Pi(G_{n+2}) = \Pi(G_{n+1})$

On a $\Pi(G_{n+2}) = \Pi(X \cdot G_{n+1} + G_{n+1}) = \Pi(X)\Pi(G_{n+1}) + \Pi(G_{n+1})$

$= \Pi(X)\Pi(G_n) + \Pi(G_n) = \Pi(XG_n + G_n) = \Pi(G_{n+1})$

Ce qui démontre l'affirmation ∎

Preuve thm : (Suite)

Soit $P(x) \in K[x]$, on a donc $\Pi(P(x)) = \Pi(R(x))$ pour un certain $R(x) \in G_d$ $\deg R(x) < \deg Q(x) = d+1$

$\Pi(R(x)) = \Pi(P(x))$ signifie $\exists D(x) \in K[x]$:

$$P(x) = Q(x)D(x) + R(x)$$

- Unicité de D et de R :

si $DQ + R = D'Q + R'$ alors $(D-D')Q = R' - R$

comme $R - R' = 0$ on a $\deg(R-R') < \deg Q$

$\Rightarrow D - D' = 0 \quad \Rightarrow R' - R = 0.$

---

le 31.05.18

Rappel : Dans $K[x]$, la division euclidienne des polynômes est possible : Si $P, Q \in K[x]$ et $Q(x) \neq 0$

i) $P(x) = D(x) \cdot Q(x) + R(x)$ $\quad \exists D, R \in K[x]$

ii) $\deg(R(x)) < \deg(Q(x))$ ou $R(x) = 0 \in K[x]$

Corollaire : Tout idéal I de $K[x]$ s'écrit sous la forme $I = \langle Q \rangle$

$= \{D(x)Q(x) : D(x) \in K[x]\}$ pour un certain $Q \in K[x]$

Preuve : (même démonstration que pour $\mathbb{Z}$)

Soit I un idéal de $K[x]$. Si $I = \{0\}$ il n'y a rien à démontrer.

Supposons $I \neq \{0\}$. Soit $Q(x) \in I$ de degré minimal et $Q(x) \neq 0$

Montrons que $I = \langle Q \rangle$: $\langle Q \rangle \subset I$ et $I \subset \langle Q \rangle$

Soit $p \subset I$, on effectue P/Q, donc $P = D \cdot Q + R$.

Preuve : (Suite)

$\underbrace{P(x)}_{\in I} = \underbrace{D(x)Q(x)}_{\in I} + R(x)$ donc $R \in I$

Il y a deux possibilités pour $R(x)$:

Soit $\deg R < \deg Q$, ce qui est exclu car Q minimal dans I

Soit $R = 0$, ce qui est la seule option

Ce qui implique $P(x) = D(x)Q(x) \in I$

$\Rightarrow I \subset \langle Q \rangle$ ∎

Déf : un PGCD de $P(x), Q(x) \in K[x]$ est un générateur de l'idéal de $K[x]$ engendré par $P(x)$ et $Q(x)$.

Thm : Bézout

Soit $P, Q \in K[x]$, $\exists U, V \in K[x]$:

$$U(x)P(x) + V(x)Q(x) = PGCD(P,Q)$$

Preuve : $PGCD(P,Q) \subset \langle PGCD(P,Q) \rangle = \{ U(x)P(x) + V(x)Q(x) : U, V \in K[x] \}$

Prop : Le PGCD est le PGCD ! (ie : soit D un PGCD de P et Q alors i) $D \mid P$ et $D \mid Q$ ii) si $D' \mid P$ et $D' \mid Q$ alors $D' \mid D$)

Preuve :

Par définition, si $\langle D \rangle \ni P$ et $\langle D \rangle \ni Q$ donc $D \mid P$ et $D \mid Q$.

Si $D' \mid P$ et $D' \mid Q \Rightarrow D' \mid U \cdot P + V \cdot Q \quad \forall U, V \in K[x] \overset{*}{\Rightarrow} D' \mid D$

* comme $D = U \cdot P + V \cdot Q$ pour certain U et V. ∎

Déf : Un polynôme $P \in K[x]$ est dit irréductible si

$P(x) = A(x) \cdot B(x)$ où $B, A \in K[x]$ alors ou bien $\deg A = \deg P$

ou bien $\deg B = \deg P$

Prop : Lemme de Gauss

Si $P \in K[x]$ est irréductible et si $P(x) \mid A(x) \cdot B(x)$ $A, B \in K[x]$

alors soit $P \mid A$, soit $P \mid B$ (comme un nbr premier)

Preuve : Supposons que $P \nmid A$, il faut donc mq $P \mid B$.

Comme $P \nmid A$, $PGCD(P,A) = 1$

D'après Bézout, $\exists u,v \in K[X]$ tq $U \cdot P + V \cdot A = 1$

On multiplie par B : $UPB + VAB = B$ comme $P \mid UPB$ et $P \mid VAB$

$P \mid UPB + VAB \Rightarrow P \mid B$ ▨

Prop: Soit $I \subset K[X]$ un idéal, les conditions suivantes sont équivalentes

1) I est maximal
2) I est premier
3) $I = (P)$ avec $P \in K[X]$ irréductible

Déf: Un idéal I dans un anneau commutatif unitaire est premier si $\forall a,b \in A$, $ab \in I \Rightarrow$ soit $a \in I$ soit $b \in I$.

Preuve: I est maximal $\Leftrightarrow$ $K[X]/I$ est un corps

Un corps est intègre (si $\forall a,b \in A$ $ab = 0 \Rightarrow a = 0$ ou $b = 0$)

$K[X]/I$ intègre $\Leftrightarrow$ I est premier

- I premier $\Rightarrow$ $I = (P)$ où P irréductible

  On sait $I = (P)$ avec $P \in K[X]$. Supposons $P = AB$

  avec $A,B \in K[X]$, comme I premier $AB = P \in I$

  $\Rightarrow$ Soit $A \in I$, soit $B \in I$ donc $P \mid A$ ou $P \mid B$

  $\Rightarrow \deg P \overset{\deg}{\leq} A$ ou $\deg P \leq \deg B$

  comme $P = AB$ on a $\deg A \leq P$ et $\deg B \leq \deg P$

  donc soit $\deg P = \deg A$ soit $\deg P = \deg B$ ⌟

- (P) avec P irréductible est maximal.

  Soit $Q \in K[X]$ tq $Q \notin (P)$, mq idéal engendré par P et Q $= K[X]$.

  comme $P \nmid Q$ et P irréductible alors $PGCD(P,Q) = 1$.

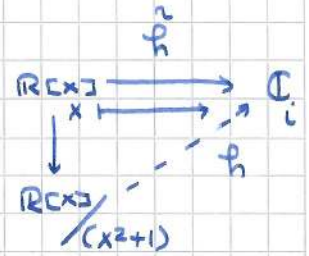
  $J = \langle P,Q \rangle = \{UP + VQ ; u,v \in K[X]\} = \langle 1 \rangle = K[X]$

le 31.05.18

Algèbre I:

Thm: Il existe un isomorphisme de corps

$$\begin{array}{ccc} \mathbb{R}[X]/(X^2+1) & \xrightarrow{\varphi} & \mathbb{C} \\ [X] & \longmapsto & \varphi([X]) = i \end{array}$$

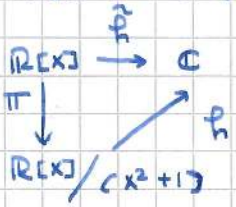


Preuve:

x^2+1 est irréductible dans $\mathbb{R}[X]$

(x^2+1) est alors maximal et $\mathbb{R}[X]/(x^2+1)$ est un corps

$$\begin{array}{ccc} \mathbb{R}[X] & \xrightarrow{\tilde{\varphi}} & \mathbb{C} \\ P(X) & \longmapsto & P(i) \end{array}$$ est un homomorphisme d'anneau surjectif



φ existe si $\ker(\pi) \subset \ker(\tilde{\varphi})$

$\ker(\pi) = \{D(X)(X^2+1),\ D \in K[X]\}$

$\tilde{\varphi}(D(X)(X^2+1)) = D(i)(i^2+1) = D(i)\cdot 0 = 0$

Donc c'est bon, donc φ existe et est un homom d'anneau unitaire surjectif. ($\tilde{\varphi}$ unitaire et surjectif)

Comme φ homom de corps, φ injectif $\Rightarrow$ φ isomorphisme.