

M-51 Pr: Pierre Dèbes

GROUPES ANNEAUX ET CORPS

Ensembles

1. Axiomatiques de N , relations d'équivalence, ensemble quotient, construction de Z .

Groupes, Anneaux et corps

- 1. groupes, sous-groupes, morphismes, noyau, image, groupe cyclique, ordre d'un élément, théorème de Lagrange, sous-groupe distingué, groupe quotient, groupe symétrique, groupe alterné, groupe opérant sur un ensemble, orbites, stabilisateurs, automorphismes intérieurs, classes de conjugaison, formule des classes, groupes diédraux et polygones réguliers.
- 2. Congruences, théorème chinois, groupe des éléments inversibles de Z/nZ , exemples de méthode de codage et de cryptage, morphismes d'anneaux, anneaux intègres, idéal, idéal premier, idéal principal, anneaux quotients, anneaux principaux, exemple des entiers de Gauss.
- 3. corps, sous-corps, corps premier, caractéristique d'un corps, corps des fractions d'un anneau intègre, construction de Q .

Polynômes et Nombres

1. Polynômes sur un corps K , polynômes irréductibles, idéaux de $K[X]$, algorithme d'Euclide, relations entre coefficients et racines ; corps des fractions rationnelles sur K .
2. construction de R (à partir des suites de Cauchy) et de C (à partir de $R[X]$), éléments algébriques, transcendants, dénombrabilité du corps des nombres algébriques sur Q .

M 51 - Groupes, Anneaux & Corps

(C1) Ensembles, équivalences, cardinal, dénombrabilité

1. Ensembles

$$E = \{1, 2, 3\}$$

- Un ensemble est un objet math. composé d'elts.
- On note E cet ensemble. Pour x élément de E .
- Ensemble composé d'aucun elt est l'ens vide : \emptyset .

1.2. Inclusion, intersection, réunion

(D1) Soit A, E ens, A est inclus dans E ou A est une partie ou m -ens de E si $\forall x \in A, x \in E$.
On note $A \subset E$.

L'ensemble des parties d'un ens E : $\mathcal{P}(E)$.

(D2) Soit E un ens, soit A, B 2 ss-ens de E , on définit la réunion $A \cup B$ par

$$A \cup B = \{x \in E, x \in A \text{ ou } x \in B\}$$

$$\rightarrow \text{l'intersection } A \cap B = \{x \in E, x \in A \text{ et } x \in B\}$$

$$\rightarrow \text{le produit cartésien } A \times B = \{(a, b) \in E \times E, a \in A, b \in B\}$$

$$\rightarrow \text{la différence ensembliste } A \setminus B = \{x \in E, x \in A \text{ et } x \notin B\}$$

2. Cardinal, dénombrabilité

2.1. Cardinal

(D3) 2 ens E, F st équipotents s'il \exists bijd de l'1 vers l'autre.
Si équipotents : ils ont m cardinal.

(D4) Un ens non vide E est fini s'il $\exists m \in \mathbb{N}^*$ tq E soit équipotent à l'ens $\{1, 2, \dots, m\}$.
On dit $\text{Card } E = m$.

Définition des entiers

On pose : $0 = \text{card}(\emptyset)$, $1 = \text{card}\{\emptyset\}$, $2 = \text{card}\{0, 1\}$
... $m+1 = \text{card}\{0, 1, \dots, m\}$

(R9) On mq (PR) si $\text{card}(E) = m$ et $F \subset E$ alors $\text{card}(F) \in \{0, 1, \dots, m\}$
D+, si $\text{card } F = m \Rightarrow \text{card } E = F$.

(P1) Soit E ens : ASSE :

$$(i) \exists \text{ inject} \mathbb{N} \xrightarrow{i} E$$

(ii) E équipotent à une partie de E distincte de E

$$(iii) \forall m \in \mathbb{N}, \text{card}(E) \neq m$$

(D5) E dit fini s'il n'est pas infini.

(Th) Cantor-Bernstein

soit E, F 2 ens, exis \exists appli injective $f: E \rightarrow F$
& appli injective $g: F \rightarrow E$ alors \exists ens E, F
st en biject^o, ils ont \hat{m} cardinal.

(Th) Cantor

soit E un ens nv & $\mathcal{P}(E)$ l'ens de y
parties \nexists sujet^o de E à $\mathcal{P}(E)$.

(P₁) L'ens $\mathcal{P}(E)$ des parties d'un ens E est en
biject^o q l'ens $\{0,1\}^E$ des appli de E
ds $\{0,1\}^b$.

2.2. Dénombrabilité

(D₁) Un ens infini E est dit dénombrable
s'il est en biject^o q l'ens \mathbb{N} .
(ie équivalent à \mathbb{N}).

(P₂) Tt ss-ens infini d'un ens dénombrable
est dénombrable.

(P7) $E \in \text{mV}$, R (nde) Les classes d'équivalences forment une partie de E , tte partie de E pt s'obtient manière unique et rel^e éqvlce.

3.2. Compatibilité

(D10) $E, F, f: E \rightarrow F, E$ muni \mathcal{R}_0 .

L'appli f est compatible de \mathcal{R}_0 si $\forall (x, y) \in E^2, x \mathcal{R}_0 y \Rightarrow f(x) = f(y)$.

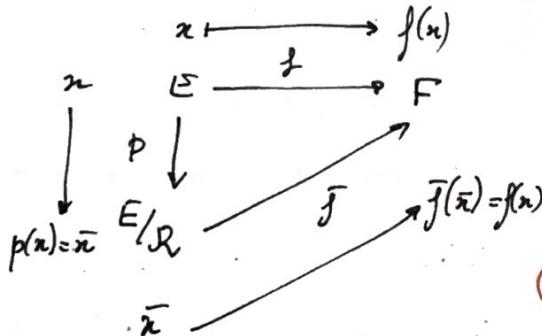
→ si f est compatible w \mathcal{R}_0 , on dit q' u passe au quotient.

(P8) $E, F, f: E \rightarrow F$, supp f compat w \mathcal{R}_0 def n E .

3! appli \bar{f} def n E/\mathcal{R}_0 tq $\forall x \in E$

$$f(x) = \bar{f}(\bar{x})$$

$$\text{Gm a: } \bar{f} \circ P = f$$



Décomposition canoniq:

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ P \downarrow & \uparrow i & \\ E/\mathcal{R}_f & \xrightarrow{\bar{f}} & \text{Im } f \end{array} \quad (i(x) = x \text{ inject canoniq}) \quad x \in \text{Im } f$$

2.6 Groupe Produit

(C2) Groupes

1. Premières définitions

1.1 Def

(D11) Une opérat (ou loi de composition interne) si ens G est

$$\begin{aligned} G \times G &\rightarrow G \\ (a, b) &\mapsto a.b \end{aligned}$$

(D12) Un groupe est ens mV muni opérat vérifiant:

- $\forall a, b, c \in G; a.(b.c) = (a.b).c$ associativité
- $\exists e \in G, \forall a \in G, e.a = a.e = a$, e : él^e neutre de G pt l'qui
- $\forall a \in G, \exists b \in G, a.b = b.a = e$, tt él^e de G admt symétrique, à noter

(D13) Lorsq opérat est commutative ie $\forall a, b \in G, ab = ba$. Le groupe est commutatif ou abélien.

1.2 sous-groupes

(D14) Une pie H d' a groupe G est sous-groupe si

- H est stable par l'opérat. de G : $\forall (a, b) \in H^2, ab \in H$
- $\forall a \in H, a^{-1} \in H$.

(P11) si G est gpe & $H \subset G, H \neq \emptyset$ alors H (g) de G si $\forall a \in H, \forall b \in H, ab^{-1} \in H$.

(P12) soit G (g), I ens mV , $(H_i)_{i \in I}$ famille (g) de G

$\Rightarrow \bigcap_{i \in I} H_i$ est (g) de G .

D15 $G \circledcirc$, sous-ens de G ,

$\langle S \rangle \stackrel{\text{def}}{=} \text{int sc}^G$ to \circledcirc de G contenant S .

(i) $\langle S \rangle$: \circledcirc de G

(ii) si $H \circledcirc$ de G q contit $S \Rightarrow \langle S \rangle \subset H$.

(i) et (ii) $\Leftrightarrow \langle S \rangle$ est + petit \circledcirc de G contit S .

D+, pr $S = \{a\}, a \in G$:

$$\langle S \rangle = \{a^k, k \in \mathbb{Z}\}$$

Généralmt: $\langle S \rangle = \{\text{prod finis élts de } S \text{ & leurs inverses}\}$

D16 On appelle ordre d'un élét a d'un groupe G , + petit entier $S^+ > 0$: n , s' $\exists a^n = e$.

(e : élét neutre). Si non a : ordre infini.

i.e.: $a^n = e$ et $a^k \neq e \quad \forall 0 < k < n$

$\Leftrightarrow a^n = e$ et $a^k \neq e \quad \forall \text{ divs}^R k \text{ de } n, 0 < k < n$.

NB: L'ordre n de a est aussi le cardinal du gpe $\langle a \rangle$.

$$\text{ordre de } a = |\langle a \rangle| = \text{Card}(\langle a \rangle)$$

(ordre élét = ordre \circledcirc engendré)

en Mdf

$$\begin{aligned} \mathbb{R}_+^* &\rightarrow \mathbb{R} \\ x &\mapsto \ln x \end{aligned}$$

$$\ln(x+y) = \ln(x) + \ln(y)$$

1.3. Morphismes

soit $(G, \cdot), (G', \star)$ 2 \circledcirc , appli $\varphi: G \rightarrow G'$ est

morphisme de groupes

$$\forall (a, b) \in G^2, \varphi(a \cdot b) = \varphi(a) \star \varphi(b).$$

Un morphisme bijectif est appelé isomorphisme.

P14 Soit $(G, \cdot), (G', \star)$ 2 \circledcirc & $\varphi: G \rightarrow G'$ [MDG] alors

- $\varphi(e) = e'$
- $\varphi(a^{-1}) = (\varphi(a))^{-1} \quad \forall a \in G$.

P15 Composé MDG \Rightarrow MDG.

$(G, \cdot); (G', \star); (G'', \Delta)$ 3 \circledcirc . $\psi: (G', \star) \rightarrow (G'', \Delta)$ [MDG]

Soit $\varphi: (G, \cdot) \rightarrow (G', \star)$ [MDG]

$\Rightarrow \psi \circ \varphi: (G, \cdot) \rightarrow (G'', \Delta)$ [MDG]

(de m si $[Isdg] \Rightarrow [Isdg]$) [MDG]

D18 $(G, \cdot); (G', \star)$ 2 \circledcirc , e' élém de G' ; $\varphi: (G, \cdot) \rightarrow (G', \star)$

$$\bullet \ker \varphi = \{x \in G, \varphi(x) = e'\}$$

$$\bullet \text{Im } \varphi = \{\varphi(x), x \in G\}$$

P16 $(G, \cdot), (G', \star)$ 2 \circledcirc , e, e' ; $\varphi: (G, \cdot) \rightarrow (G', \star)$ [MDG]

$\Rightarrow \ker \varphi \circledcirc G$ et $\text{Im } \varphi \circledcirc G'$

(P17)

- Morphisme Ψ injectif ssi $\ker \Psi = \{e\}$
- " " Ψ surjectif ssi $\text{Im } \Psi = G'$.

(P18)

soit $G \otimes$, un isomorphisme de G ds l.-m
est automorphisme. L'ens automorphismes de G :

$\text{Aut}(G)$. (est \otimes p composits applicatifs)

(P19)

$G \otimes, g \in G; \Psi_g: G \rightarrow G$

est un automorphisme $x \mapsto g x g^{-1}$
de G dit automorphisme intérieur.

2. Groupe quotient & groupe produit

2.1. Relais de congruences

(D19)

$G \otimes, H \otimes$ de G . On déf relais de congruence à droite & à gauche modulo H par:

- congruence à droite : $x \in G, y \in G, x \equiv_d y \pmod{H} \Leftrightarrow xy^{-1} \in H$
- congruence à gauche : $x \in G, y \in G, x \equiv_g y \pmod{H} \Leftrightarrow x^{-1}y \in H$

Notat:

$$xH = \{xh, h \in H\}$$

$$\text{D'où } \bar{x}^d = xH. \quad (\text{de m } \bar{x}^d = Hx = \{hx \mid h \in H\}).$$

2.6 Groupe Produit

(P21)

Tte classe à droite mod H est en bijecto w H . ($G \otimes, H \otimes$)

$$\begin{aligned} H &\xrightarrow{\delta} xH \\ h &\mapsto xh \end{aligned}$$

(P22)

Ens quotients $(G/H)_g$ & $(G/H)_d$ est en bijecto.
 $(G/H)_g = \{xH, x \in G\}$

(D23)

$$|(G/H)_g| = |(G/H)_d| = [G:H]$$

l'indice de H dans G
(nbr de classes).

2.2. TH de Lagrange

(T4)

$|H|$ divise $|G|$.

(Cor1)

$$[G:H] \cdot |H| = |G|$$

($G \otimes$ fini)

(Cor2) $x \in G, |x|$ divise $|G|$.

(Cor3) $G \otimes$ fini; on note $n = |G|, \forall x \in G, x^n = e_G$.

△ $6 \otimes$ diviseur du card du \otimes et potentiel ut de \otimes ms PAS tous. (@ A_4)

2.3. Sous-groupes distingués

But: Mettre \otimes x ($G/H)_g$ (resp $(G/H)_d$).

△ On n'a pas en général: $xH \cdot yH \in (G/H)_g$

Nota: $A, B \subset G, A \cdot B = \{a \cdot b \mid a \in A, b \in B\}$

si $A = \{x\}$, on note $\{x\} \cdot B = x \cdot B$.

NB: $Ax = B \Leftrightarrow A = Bx^{-1}$

(D22) Un H d'un G est dit distingué normal de G , noté $H \triangleleft G$

si $\forall g \in G, \forall h \in H, ghg^{-1} \in H$.

P23 $G \circledcirc H$, $H \triangleleft G$, Ainsi:

(i) \circledcirc H est distingué de G .

(ii) $\forall g \in G, ghg^{-1} \subset H$ (iii) $\forall g, ghg^{-1} = H$

(iv) $\forall g \in G, g^H \subset Hg$ (v) $\forall g, g^H = Hg$.

↳ les classes à gauche & à droite coïncident.

② TH, \circledcirc abélien : tt \circledcirc H est distingué.

③ $\ker \varphi$ distingué de G . ($\varphi: M6$)

P25 $[G:H] = 2 \Rightarrow H \triangleleft G$.

P26 $\text{Aut}(G) \triangleleft \text{Aut}(G)$

Q23 Le centre d'un \circledcirc G est l'ens. des élts de G

qui commutent avec tous, on le note $Z(G)$:

$$Z(G) = \{x \in G, xy = yx, \forall y \in G\}$$

Le centre de G est \circledcirc de G qui est commutatif & distingué de G .

Q24 Un groupe G est dit simple s'il n'admet pas d'autres sous-groupes distingués que \circledcirc trivial (étant nul & l'uni).

2.4. Groupe Quotient

P27 $G \circledcirc, H \triangleleft G$ distingué. On a $(G/H)_g = (G/H)d$

On note G/H un ensemble. La loi définie sur G/H par :

$\forall C, C' \in G/H$ alors $C.C' = \{c.c', c \in C, c' \in C'\}$

donne à G/H une structure de groupe.

P27' D+, la surject canoniq. $G \xrightarrow{s} G/H$ est un $M6$

Contexte : $G \circledcirc, H \triangleleft G, G/H$ groupe quotient $s: G \rightarrow G/H$

$$s(gg') = s(g).s(g')$$

$$g \mapsto s(g) = gH$$

P29 \circledcirc H de G est \triangleleft de G si et seulement si φ morphisme.

2.5. TH d'isomorphismes

Cor 4 (1^o TH I)

$\varphi: G \rightarrow G'$ $M6$, $H \triangleleft G$ tq $H \subset \ker \varphi$ alors

$\exists!$ $M6$ $\bar{\varphi}: G/H \rightarrow G'$ tq $\varphi = \bar{\varphi} \circ s$.

D+, $\text{Im } \bar{\varphi} = \text{Im } \varphi$; $\ker \bar{\varphi} = \ker \varphi / H$. (ep $H \triangleleft \ker \varphi$)

ep pour $H = \ker(\varphi)$:

$\bar{\varphi}|_{\text{Im } \varphi}: G/\ker \varphi \rightarrow \text{Im } \varphi$ est un isomorphisme.

$$G/\ker \varphi \cong \text{Im } \varphi$$

NB: $\ker \varphi / H \stackrel{\text{def}}{=} s(\ker \varphi)$

Tu 5 (2^o THI)

$G \trianglelefteq H, K \trianglelefteq G$, $K \triangleleft G$ alors l'ens HK ,
 $HK = \{hk, h \in H, k \in K\}$ est \trianglelefteq & on a:

$$HK/K \simeq H/H \cap K$$

$\forall K \triangleleft HK, H \cap K \triangleleft H$.

Tu 6 (3^o THI)

$G \trianglelefteq H, K \trianglelefteq G$ t/q $K \triangleleft H \cap G$ alors $H/K \triangleleft G/K$ &

$$G/H \simeq (G/K)/_{(HK)}$$

Tu 7 (TH de correspondance)

$G \trianglelefteq H, K \triangleleft G$, on note $p: G \rightarrow G/K$ sujet canoniq.
 Les applicat's :

- $\{H \trianglelefteq G \mid H \supset K\} \xrightarrow{\pi} \{\text{H}\trianglelefteq \text{de } G/K\}$
 $H \longmapsto H/K = p(H)$
- $\{\text{H}\trianglelefteq \text{ de } G/K\} \xrightarrow{\rho} \{H \trianglelefteq G \mid H \supset K\}$
 $\text{H} \longmapsto \rho^{-1}(\text{H})$

et réciproq's l'une de l'autre. Bijectivité.

$$\rho^{-1}(\text{H}) \supset \rho^{-1}(1_{G/K}) = \ker p = K.$$

2.6 Groupe Product

$H, K \trianglelefteq G$, $H \times K = \{(h, k) \mid h \in H, k \in K\}$
 $(h, k)(h', k') = (hh', kk')$

Prop 34 $G \trianglelefteq H, K \trianglelefteq G$ alors G isom au $H \times K$ \trianglelefteq
 $H \triangleleft G, K \triangleleft G, H \cap K = \{e_G\}, G = HK$.

3. Groupes cycliq's

3.1. Définitions

D25 Groupe monog'

On appelle groupe monog' un \trianglelefteq engendré p un st él't :

$$G = \langle a \rangle = \{a^n, n \in \mathbb{Z}\} \quad \& \quad a^0 = e_G.$$

On appelle groupe cycliq un \trianglelefteq monog fini :

$$G = \langle a \rangle = \{a^k, k \in \mathbb{N}\} = \{e_G, a, a^2, a^3, \dots, a^{m-2}, a^{m-1}\} \quad \& \quad a^m = e_G$$

Rq si $G = \langle a \rangle$, \trianglelefteq cycliq engendré p a, m l'ordre de G.
 (q est aussi l'ordre de G).

L'applicat $\mathbb{Z} \rightarrow \langle a \rangle$ est un morphisme $a^{\frac{m+n}{m}} = a^{\frac{m}{m}} \cdot a^{\frac{n}{m}}$
 $m \mapsto a^m$ (sujetif p constat)

& de $\{h \in \mathbb{Z}, a^h = 1\} = m \mathbb{Z}$.

$$\bullet \mathbb{Z}/m\mathbb{Z} \simeq \langle a \rangle = G$$

• m est l'ordre de a si $a^m = 1$ & $\forall h \in \mathbb{Z}$

$$a^h = 1 \Leftrightarrow \frac{m}{h}$$

(Prop 36) pr $\bar{k} \in \mathbb{Z}/m\mathbb{Z}$,

$$\langle \bar{k} \rangle = \mathbb{Z}/m\mathbb{Z} \Leftrightarrow k \text{ est premier à } m.$$

3.3. Pptés

(Prop 37) Tout \mathfrak{G} cycliq d'ordre m est isomorphe au groupe quotient $\mathbb{Z}/m\mathbb{Z}$.

$$\mathfrak{G} \simeq \mathbb{Z}/m\mathbb{Z}, \text{ si } |\mathfrak{G}| = m.$$

(Prop 38) soit p nbr premier, G tq $|G| = p$ alors G est cycliq.

p premier, $|G| = p \Rightarrow G \mathfrak{G}$

(Prop 39) soit $G = \langle x \rangle \mathfrak{G}$, $|G| = n$ alors

1) si $H \mathfrak{G}$ de G , H est cycliq, on note $k > 0$:
+ ptt entier tq $\frac{kn}{k} \in H$ alors H est engendré par $\frac{kx}{k}$ & $|H| = \frac{m}{k}$

2) si d est un diviseur de $n \Rightarrow G$ possède uniq \mathfrak{G} d'ordre d q'te engendré par $\frac{n}{d}x$.

3.4. \mathfrak{G} & produits

(Prop 40) les \mathfrak{G} de $\mathbb{Z}/m\mathbb{Z}$ et les \mathfrak{G} $\frac{k\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{l\mathbb{Z}}{m\mathbb{Z}}$

$$\text{On a } \frac{k\mathbb{Z}}{m\mathbb{Z}} \simeq \frac{\mathbb{Z}}{(\frac{m}{k})\mathbb{Z}}$$

(Prop 41) $m, n \neq 0 \Rightarrow \mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

4. Action de groupe

4.1. Défs

Déf 1 soit X ens, $G \mathfrak{G}$. Une action (ou opérat) de G sur X est un homomorphisme de G ds le groupe $\text{Bij}(X)$ ds bijoles de X ds lui-même:

$$\pi: G \longrightarrow \text{Bij}(X)$$

$$g \longmapsto \pi(g): X \longrightarrow X$$

$$x \longmapsto \pi(g)(x) \stackrel{\text{not}}{=} g \cdot x$$

résultat de l'act de $g \in G$ sur x ds X .

Déf 2 soit $G \mathfrak{G}$ opérant sur ens X , $x \in X$:

- l'ens $\text{Stab}_G(x) = \{g \in G, g \cdot x = x\}$, noté aussi G_x , est \mathfrak{G} de G appelé stabilisateur de l'elt x .

- si A pie de X , on déf le stabilisateur de A ds G & le fixateur de A ds G par:

$$\text{Stab}_G(A) = \{g \in G, g \cdot A = A\}$$

$$\text{Fix}_G(A) = \{g \in G, \forall a \in A, g \cdot a = a\}$$

$$\pi(g)(A) = A$$

Déf 3 • Un elt x de X est un point fixe si $\forall g \in G, g \cdot x = x$.

• L'ens $O_x = \{\pi(g)(x), g \in G\} = \{g \cdot x, g \in G\}$ est appelé l'orbite de x ss l'act de G .

(Prop 42) soit $G \mathfrak{G}$ opérant sur $X \Rightarrow$ les orbites de X forment une partition de X

4.8 Formule des classes

(P₄₄) Soit G opérant sur l'ens X . Soit $x \in X$, on note $\mathcal{Q}_x = \text{Stab}(x)$ alors $\text{Stab}(x)$ est \oplus de G &

ens \mathcal{Q}_x & $\frac{G}{\text{Stab}(x)}$ st en biject. (ens quotient
pe relais de congruence à gauche
mod. $\text{Stab}(x)$)

(P₄₅) (Formule des classes)

si X fini, $\mathcal{Q}_{x_1}, \dots, \mathcal{Q}_{x_n}$: la liste finie des orbites de l'act alors :

$$\text{card}(X) = \sum_{i=1}^n \frac{|G|}{|\text{Stab}(x_i)|}$$

4.3. Action par conjugaison

(D₆) G , $X = G$, action par conjugaison de $G \times G$:

$$C: G \longrightarrow \text{Bij}(G)$$

$$\begin{aligned} g &\longmapsto c_g: G & \longrightarrow G \\ &x \longmapsto g x g^{-1} \end{aligned}$$

$\rightarrow \mathcal{Q}_x$ est la classe de conjugaison.

$$\rightarrow \mathcal{Q}_x = \{g x g^{-1}, g \in G\}.$$

Pour l'act par conjugaison: $|G| = |\mathcal{Z}(G)|$ somme de diviseurs de $|G|$ distincts de 1.

(P₄₇) si G est un p- \oplus (ie un \oplus d' \oplus l'ordre est une puissance non-triviale d'un nbr premier p) $\Rightarrow \mathcal{Z}(G) \neq \{1\}$.

(ie: $\exists g \in G, g \neq 1$ et $g \in \mathcal{Z}(G)$).

1.1. et 1.2.

5. Groupes symétriques

5.1. Définitions

$\mathcal{Y}_m = \text{Bij}(\{1, \dots, m\})$ permutations pr $m \geq 1$.

- (D₃₃)
 - o Une permutation $\sigma \in \mathcal{Y}_m$ se note $(\begin{smallmatrix} 1 & 2 & 3 & \dots & m \\ i_1 & i_2 & i_3 & \dots & i_m \end{smallmatrix})$ où $\sigma(k) = i_k \in E_m$, $k \in E_m$.
 - o On a cycle ou permutation circulaire de longueur k une permutation δ notée $(i_1 i_2 \dots i_k)$ où $1 \leq l \leq k-1$ $\delta(i_l) = i_{l+1}$, $\delta(i_k) = i_1$ & pour $s \notin \{i_1, i_2, \dots, i_k\}$, $\delta(s) = s$.
 - o L'ens $\{i_1, \dots, i_k\}$ est le support du cycle.
 - o Le support d'une permutation $\sigma \in \mathcal{Y}_m$ est l'ens $\{i \in E_m, \sigma(i) \neq i\}$.
 - o Un cycle de longueur 2 est transposition.
 - $\delta_{i,j} = (i,j)$ vérifie $\delta_{i,j}(i) = j$, $\delta_{i,j}(j) = i$ & pour $k \notin \{i,j\}$, $\delta_{i,j}(k) = k$.

(P₁₈)

$$|\mathcal{Y}_m| = m!$$

5.2. Décomposition en cycles

(Th₈) Tte permutation se décompose de manière unique (à l'ordre près) en produits de cycles à supports disjoints.

L1 Le support d'une permutation $\sigma \in \mathcal{Y}_m$ est stable ss l'act du $\langle \sigma \rangle$ de \mathcal{Y}_m engendré par σ .

L2 Soit $\gamma \in \mathcal{Y}_m$ est un k -cycle alors son support S contient exactement k élts & l'orbite de γ est de S ss l'act du $\langle \gamma \rangle <\gamma>$ et le support S est entia. $\langle \gamma \rangle \simeq \mathbb{Z}/k\mathbb{Z}$

P40 2 cycles à supports disjoints commutent.

R9 $\langle \gamma \rangle \xrightarrow{\text{Id}/\gamma} \text{Bij } \{1, \dots, m\}$
 $\langle \gamma \rangle \subset \mathcal{Y}_m$.

L3 Le support d'une permutation $\sigma \in \mathcal{Y}_m$ est stable ss l'action du $\langle \sigma \rangle$ de \mathcal{Y}_m engendré par σ .

P50 Le conjugué d'un k -cycle est un k -cycle & 2 cycles de mè longueur sont conjugués.

$$\tau(i_1 \dots i_k) \tau^{-1} = (\tau(i_1) \dots \tau(i_k))$$

$\mu \circ \tau \in \mathcal{Y}_m$, $(i_1 \dots i_k)$ k -cycle de \mathcal{Y}_m

Tus Tte permutation $\sigma \in \mathcal{Y}_m$ s'écrit de façon unique (à l'ordre près) en produit $\sigma = c_1 \circ c_2 \circ \dots \circ c_n$ de cycles à supports disjoints.

L3 Pour $\sigma \in \mathcal{Y}_m$, Ω une orbite de σ , $\Omega = \{\sigma^t(i), t \in \mathbb{Z}\}$
& $\frac{\Omega}{\Omega}$ est un cycle de longueur $\text{card}(\Omega)$.

Cor6 Le \mathfrak{S}_n symétrique \mathcal{Y}_m est engendré par transposés.

G67 Deux permutations σ & σ' de \mathcal{Y}_m sont conjuguéesssi
 $\forall k \in \mathbb{N}, 2 \leq k \leq m$, apparaissent mè k -cycles de la décomposition canonique en produit de cycles à supports disjoints.

P51 L'ordre d'une permutation $\sigma \in \mathcal{Y}_m$ est égal au ppcm des longueurs des cycles à supports disjoints entrant dans la décomposition de σ .

5.5
Signature

$$\text{D34} \quad \varepsilon(\sigma) = \prod_{1 \leq i < j \leq m} \sigma(j) - \sigma(i), \quad \sigma \in \mathcal{Y}_m$$

$$\prod_{1 \leq i < j \leq m} (j-i)$$

P52 L'appli $\varepsilon: \mathcal{Y}_m \rightarrow \{-1, 1\}$ est MDG.

$$(\varepsilon(\sigma \circ \gamma) = \varepsilon(\sigma) \cdot \varepsilon(\gamma))$$

$$\varepsilon(\gamma) = (-1)^{\frac{k-1}{2}}$$

transposés -1
long k cycle.

⑤ $\ker \varepsilon = \{\sigma \in \mathbb{Y}_n, \varepsilon(\sigma) = 1\}$ est \textcircled{g} distingué
de \mathbb{Y}_n d'indice 2 dans \mathbb{C}_n : \textcircled{g} alterné.

GRUPE QUOTIENT
Relat de congruença
TR de Leyom,
distinç
quotient
TR isomorfo
TR correspõe

$G @ H$ de G . On déf. relatif de congruence à droite & à gauche modulo H par :

- $\triangleright x \in G, y \in G, x \equiv d y \pmod{H} \Leftrightarrow xy^{-1} \in H$
- $\triangleright x \in G, y \in G, x \equiv g y \pmod{H} \Leftrightarrow x^{-1}y \in H$

$xH = \{xh, h \in H\} = \bar{x}$

$|H| \text{ divide } |G|$
 $[G : H], |H| =$
 $\forall x \in G, |x| \text{ divide }$
 $\Theta @ \lim_{n \rightarrow \infty} n =$
 $\forall x \in G, x^n = e_G$

	$G \otimes H$ est :	$Z(G) \otimes G$ est commutatif
1B1	(i) $H \triangleleft G$	$G \otimes H$ distg. $(G/H)_g = (G/H)_d$
	(ii) $\forall g \in G, ghg^{-1} \in H$	en le note G/H . La loi d'op. sur G/H est
1G1	(iii) $\forall g, ghg^{-1} = H$	si $C, C' \in G/H$ alors $C \cdot C' = \{c \cdot c'\}_{ccc}$
1G1	(iv) $\forall g, gh \in Hg$	donne à G/H s'ac de \otimes .
	(v) $\forall g, gh = Hg$	

$\text{ef pr } H = \ker(\varphi)$	$G \oplus H, K \oplus G \triangleleft G \text{ tq } \textcircled{3}$
$\overline{\varphi} / \text{Im } \varphi: G/\ker \varphi \rightarrow \text{Im } \varphi$	$K \subset H \subset G \Rightarrow H/K \triangleleft G/K \text{ &}$
est un isomorphisme.	$G/H \cong (G/K)/_{(HK)}$
$G/\ker \varphi \cong \text{Im } \varphi$	$\textcircled{4}, K \triangleleft G, p: G \rightarrow G/K \text{ surjective}$

$$G \circledcirc H, K \triangleleft G \text{ tq } \textcircled{3} \\ K \subset C_G \Rightarrow H/K \triangleleft G/K \& \\ G/H \simeq (G/K)/_{(HK)} \\ \textcircled{4} \text{ } K \triangleleft G, p: G \rightarrow G/K \text{ surjective} \\ \exists g \in G \text{ s.t. } \forall x \in K \text{ } g^{-1}xg \in K$$

ENSEMBLES
C, A, U
Cardinal
Dénombrabilité
Des entiers
Relais d'équiv
Comptabilité
~~Thé~~ Cantor
Demp canon

<p>A, E ens, ACE ou A est ss-ens de E si $\forall n \in A, \exists e \in E$, note ACE. (n-ens ou pie Ens partie : $\mathcal{P}(E)$)</p>	<p>soit E ens, $ASIE$:</p> <ol style="list-style-type: none"> \exists injectif $f: A \rightarrow E$ E équip. à pie E distincte $\forall m \in A$, $\text{card}(f(m)) = 1$ <p>E est fini s'il n'est pas</p>
<p>$A \cup B = \{x \in E, x \in A \text{ ou } x \in B\}$</p>	<p>TH Cantor - E</p>

- L'ensemble des parties d'un ensemble E
- Ens infini E
en biject ap.
(équivalent)
- Bernstein
- Existe un appli injet.

	$\exists x \in E$, $x = y$, $y \in F$	($\exists x \in E$) $x = y$ et $y \in F$
et en $\exists y \in F$	$\exists x \in E$ $x = y$, $y \in F$	$\exists x \in E$ tel que $x = y$ et $y \in F$
applis	$\exists x \in E$ $x = y$, $y \in F$	$\exists x \in E$ tel que $x = y$ et $y \in F$
à IV.	$\exists x \in E$ $x = y$, $y \in F$	$\exists x \in E$ tel que $x = y$ et $y \in F$
à IV).	$\exists x \in E$ $x = y$, $y \in F$	$\exists x \in E$ tel que $x = y$ et $y \in F$

- si E muni de R_0 rde, classes d'équiv. form. partition de E , tte
 R partie de E pt s'obt. manière uniq \in rde.
 S- T $E, F, f: E \rightarrow F$ muni R_0 . L'appel f est compatible ap R_0 si
 $\forall (x, y) \in E^2, x \sim_R y \Rightarrow f(x) = f(y)$.
 (si f est compatible ap R_0 , on dit qu' f passe au quotient)
 $E, F, f: E \rightarrow F$, supp f compat ap R_0 def n E , $\exists!$ appli J def
 sur E/R_0 tq $\forall x \in E$ $f(x) = \bar{f}(\pi)$. On a $\bar{f} \circ P = f$.

GROUPES
 Définitions
 (G), (G)
 (G) engendré
 Morphisme
 MDG
 automorph.
 Ker, Im, q

<p>On appelle opérateur :</p> <ul style="list-style-type: none"> $G \times G \rightarrow G$ $(a, b) \mapsto a \cdot b$ <p>Un groupe est un ensemble munis d'un opérateur :</p> <ul style="list-style-type: none"> $\forall a, b, c \in G : a(b.c) = (a.b).c$ Assoc. $\exists e \in G, \forall a \in G, ea = a \cdot e = a$ Neutralité $\forall a \in G, \exists b \in G, a \cdot b = b^{-1} \cdot a = e$ Symétrie <p>Qd opérateur est commutative ie</p> <p>$\forall a, b \in G, ab = ba$. $\textcircled{1}$ abélien</p> <p>Une loi de composition interne $\textcircled{2}$ G est $\textcircled{3}$ si :</p> <ul style="list-style-type: none"> G est stable par opérateur de G : $\forall (a, b) \in G, a \cdot b \in G$ 	<p>$\forall a \in H, \forall b \in G$</p> <p>soit $g \textcircled{4}$, l'env</p> <p>$\Rightarrow \bigcap_{i \in I} H_i$ est</p> <p>$\textcircled{5}$ de G conn</p> <p>(i) $\subset S$:</p> <p>(ii) si $H \textcircled{6}$ de</p> <p>(iii) et (ii) $\Leftrightarrow < S$</p> <p>Pr $S = \{a\}$,</p> <p>$< S = \{a\}$</p>
---	--

$\text{H}, ab^{-1} \in H$
 $\forall i, (H_i)_{i \in \mathbb{N}}$ famille de
 (2) de G .
 $\langle S \rangle \neq \text{interv} \text{ tenant } S$.
 (3) de G
 $\exists G \ni \text{cont } S \Rightarrow \langle S \rangle \subset C$
 $\exists > + \text{petit } (2) \text{ de } G \text{ cont }$
 $a \in G : \text{Généralisation}$
 $\exists \in \mathbb{N} : \text{Généralisation}$

$\Rightarrow \exists a^n = e$. Sinon a: d'ordre ∞ .

i.e.: $a^n = e$ et $a^k \neq e \quad \forall 0 < k < n$

$\Leftrightarrow a^n = e$ et $a^k \neq e \quad \forall$ divis k de n , $0 < k < n$

Ordre n de a est ainsi le cardinal du $\{a\}$ $\langle a \rangle$.

ordre de a = $|\langle a \rangle| = \text{Card}(\langle a \rangle)$

soit (G, \cdot) , (G', \star) , $\& \oplus$, appli $\Phi: G \rightarrow G'$ est MDG si
 $\forall (a, b) \in G^2$, $\Phi(a \cdot b) = \Phi(a) \star \Phi(b)$

Un morphisme bijectif est isomorphisme.

soit (G, \cdot) , (G', \star) , $\Phi: G \rightarrow G'$ MDG alors

- $\Phi(e) = e'$

$\text{Compte MDG} \Rightarrow \text{MDG}$	$G \oplus, g \in G,$ $\varphi_g: B \rightarrow G$ est un automorphisme $x \mapsto g x g^{-1}$
$(G, \cdot), (G, \star) \text{ 2 } \oplus, \varphi: (G, \cdot) \rightarrow (G, \star)$	$\ker \varphi = \{x \in G, \varphi(x), e' \}$
$\ker \varphi = \{x \in G, \varphi(x), e' \}$	$\text{Im } \varphi = \{\varphi(x), x \in G\}$
$\ker \varphi \oplus G \& \text{Im } \varphi \oplus G'$	$\text{de } G \text{ dit automorphisme intérieur.}$
$\varphi \text{ injectif sur } \ker \varphi = \{e\}$	
$\varphi \text{ surjectif sur } \text{Im } \varphi = G'$	
$G \oplus, \text{isomorphisme de } G \text{ de } \mathbb{C} - M$ est automorphisme.	$H \times K = \{(h, k), h \in H, k \in K\}$ $(h, k)(h', k') = (hh', kk')$

Groupes symétriques

$$S_n = \{ \text{bij}(\{1, \dots, n\}) \text{ permutations de } n \}$$

Une permutation $\sigma \in S_n$ se note $(i_1 \ i_2 \ \dots \ i_m)$ où $\sigma(i_k) = i_{k+1} \in E_m$, $k \in E_m$.

• Cycle ou permutation circul de long k de une permutation σ notée $(i_1 \ i_2 \ \dots \ i_k)$ où $\forall 1 \leq l \leq k-1 : \sigma(i_l) = i_{l+1}$, $\sigma(i_k) = i_1$ $\forall s \notin (i_1 \ i_2 \ \dots \ i_k)$, $\sigma(s) = s$.

• Ens $\{i_1, \dots, i_k\}$ est support du cycle.

• Support permutation $\sigma \in S_n$ est l'ens $\{i \in E_m, \sigma(i) \neq i\}$.

• Un cycle de long r est transposé. $\exists i, j \in E_m$ tels que $\sigma(i) = j$; $\sigma(j) = i$

$|S_n| = n!$ Le conjugué d'un k-cycle est un k-cycle et 2 cycles de m-long k sont conjugués.

Tte permutation se décompose de manière unique (à l'ordre près) en produit de cycles à supports disjoints.

Le support d'une permutation $\sigma \in S_m$ est stable ss l'orbite (O) de S_m engendré par σ .

Soit $\sigma \in S_m$ soit un k-cycle alors son support S contient exactement k élts & l'orbite de S est de S est l'orbite du $\langle \sigma \rangle$ est le support de S initial. $\langle \sigma \rangle \cong \mathbb{Z}/k\mathbb{Z}$

2 cycles à supports disjoints commutent.

$$\langle \sigma \rangle \xrightarrow{\text{Id/0}} \text{bij}(\{1, \dots, n\})$$

$$\langle \sigma \rangle \subset S_m$$

$$\sigma(i_1 \ \dots \ i_k) \sigma^{-1} = (\sigma(i_1) \ \dots \ \sigma(i_k))$$

$$\forall \sigma \in S_m, (i_1 \ \dots \ i_k) \text{-cycle}$$

Tte permutation $\sigma \in S_m$ s'écrit de façon unique (ulp) c'est à dire $\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_m$ de cycles à supports disjoints.

$$\sigma \in S_m, O \text{ une orbite de } \sigma,$$

$$O = \{ \sigma^k(i), i \in \mathbb{Z}/k\mathbb{Z} \}$$

$$\sigma|_O \text{ est cycle de long } |O|$$

• Symétrique S_m est engendré par transpositions.

$\sigma, \sigma' \in S_m$ st conjugués si $\forall k \in \mathbb{N}$, $\exists k \leq n$, apparaît m nbs k-cycles dans le décomp. canonique en T de cycles à supp. disj.

Ordre permutation $\sigma \in S_m = \text{ppcm}(\ell^R \text{ axes})$ étant de la décomp de σ .

$$E(\sigma) = \left(\prod_{1 \leq i < j \leq m} \sigma(j) - \sigma(i) \right) / \left(\prod_{1 \leq i < j \leq m} j - i \right), \sigma \in S_m$$

$$E: S_m \rightarrow \mathbb{Z}/13 \quad \text{MDG} \quad (E(\sigma \circ \delta) = E(\sigma) \cdot E(\delta))$$

$$E(\sigma) = (-1)^{k-1} \text{ long } \sigma \text{ cycle, un transposition : } -1.$$

ker $E = \{ \sigma \in S_m, E(\sigma) = 13 \}$ est le dist. de S_m d'indice 2 de S_m : appellé alterné.

Groupes cycliques

On appelle $\mathbb{Z}/m\mathbb{Z}$: \mathbb{Z} engendré par 1 él. $G = \langle a \rangle = \{a^n, n \in \mathbb{Z}\} \Leftrightarrow a^0 = e_G$.

On appelle $\mathbb{Z}/m\mathbb{Z}$: \mathbb{Z} monog fini :

$$G = \langle a \rangle = \{a^k, k \in \mathbb{N}\} = \{e_G, a^1, \dots, a^{m-1}, a^m = e_G\}$$

soit $G = \langle a \rangle$, \mathbb{Z} cyclique engendré par a , $m = |G|$, $\mathbb{Z} \rightarrow \langle a \rangle$ est MDG: $a^{m+m} = a^m \cdot a^m$, $m \mapsto a^m$ (injectif & constant)

$$\Rightarrow H = \{n \in \mathbb{Z}, a^n = 1\} = m\mathbb{Z}$$

$$\mathbb{Z}/m\mathbb{Z} \cong \langle a \rangle = G$$

n ordre de a si $a^n = 1$ et $\forall k \in \mathbb{Z}$ $a^{nk} = 1 \Leftrightarrow n \mid k$.

$$\text{si } k \in \mathbb{Z}/m\mathbb{Z},$$

$$\langle k \rangle = \mathbb{Z}/m\mathbb{Z} \Leftrightarrow k \text{ premier à } m$$

$$\langle g \rangle \cong \mathbb{Z}/m\mathbb{Z}, \text{ si } |g| = m$$

$$p \text{ premier, } |G| = p \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$$

$$\text{soit } G = \langle x \rangle, \text{ si } |G| = m \text{ alors}$$

$$1) \text{ Hg } G, H \text{ est cyclique, } k \geq 0:$$

$$+ \text{ ptt entier tq } k \in H \text{ alors } H \text{ est engendré par } k \text{ & }$$

$$|H| = \frac{m}{k}$$

$$2) \text{ si } d \text{ diviseur de } m \rightarrow G$$

$$\text{partie unique } \mathbb{Z}/d\mathbb{Z} \text{ d'ordre } d$$

$$\text{qui est engendré par } \frac{m}{d} \text{.}$$

$$\text{sg de } \mathbb{Z}/m\mathbb{Z} \text{ et } \mathbb{Z}/k\mathbb{Z} \text{ & } \mathbb{Z}/l\mathbb{Z}$$

$$\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}/(m/l)\mathbb{Z}$$

$$m, n \text{ premiers} \Rightarrow \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$\text{soit } X \text{ ens, } G \text{ opérant sur } X \text{ (ou agissant)}$$

$$\text{de } G \text{ sur } X \text{ est homomorphisme de } G \text{ da le}$$

$$3) \text{ Bij}(X) \text{ de bijod de } X \text{ da le-ri:}$$

$$\pi: G \rightarrow \text{Bij}(X)$$

$$g \mapsto \pi(g): X \rightarrow X$$

$$x \mapsto \pi(g)(x) = g \cdot x$$

$$\text{Stab}_G(x) = \{g \in G, g \cdot x = x\} = G_x$$

$$\text{Stab}_G(A) = \{g \in G, g \cdot A = A\}$$

$$\text{Fix}_G(A) = \{g \in G, \forall a \in A, g \cdot a = a\}$$

$$\Omega_x = \{ \pi(g)(x), g \in G \} = \{g \cdot x, g \in G\}$$

$G \text{ opérant sur } X \Rightarrow$ orbites de l'act de X formant une partition de X

$G \text{ opérant sur } X, x \in X \Rightarrow \text{stab}_G(x) \text{ de } G \text{ &}$

$\Omega_x \text{ & } G/\text{stab}_G(x) \text{ st bijod}$

si X fini, $\Omega_1, \dots, \Omega_n$:

$$|X| = \sum_{i=1}^n \frac{|G|}{|\text{stab}_G(x_i)|}$$

$G \text{ opérant sur } X \text{ da le-ri:}$

$$C: G \rightarrow \text{Bij}(G)$$

$$g \mapsto c_g: G \rightarrow G$$

$$x \mapsto g \cdot x^{-1}$$

$\Rightarrow \Omega_x = \{c_g(x), g \in G\}$

$$\Omega_x = \{g \cdot x^{-1}, g \in G\}$$

D) $\ker \varepsilon = \{\sigma \in S_n, \varepsilon(\sigma) = 1\}$ est le distingué de S_n d'indice 2 dans S_n : appelé alterné.

(P₅₃) Le (g) alterné $c_m \in S_m$ & $|c_m| = \frac{|S_m|}{2} = \frac{m!}{2}$.

(P₅₄) Pour $m \geq 3$, c_m engendre les 3-cycles.

(L₃) Pour $m \geq 2$, les transpositions τ_i , $1 \leq i \leq m-1$ engendent S_m .

(L₄) Le produit de 2 transpositions dont les supports ont un élément commun est un 3-cycle. $(ik)(ij) = (ijk)$

(T₁₃) Cycles

Pour $m \geq 5$, le (g) alterné c_m est simple.

(ie c_m n'admet pas de (g) distingué propre (distinct de id_m & lui-même)).

C₂: Anneaux

(D₃₉) Un anneau $(A, +, \cdot)$ est un (m) muni de 2 opérations, une addition & multiplication vérifiant pp's :

1) $(A, +)$ (g) abélien (un élément neutre 0_A en 0).

2) multiplication associative ($\forall a, b, c \in A : (a.b).c = a.(b.c)$)

3) multiplication distributive sur l'addition $a(b+c) = ab + ac$

$$\text{et } (a+b)c = ac + bc$$

(D₄₀) Un (g) A est dit unitaire, si \exists élément neutre pour la multiplication: 1_A .

(Dans la suite tous les (g) sont considérés unitaires) (14)

D₄₁) Un (g) A est dit commutatif lorsqu'il est commutatif. $(\mathbb{Z}, +, \cdot)$; $(\mathbb{Q}, +, \cdot)$, $(\mathbb{K}, +, \cdot)$ mais pas $(\mathbb{M}, +, \cdot)$.

L₅) Ds (g) A, 0_A est absorbant pr \otimes , ie $\forall a \in A, 0_A \cdot a = a \cdot 0_A = 0_A$.

(P₅₈) FFN si $a, b \in A$ & n entier $> 0 \Rightarrow$

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \quad \text{où } \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

D₄₂) Un (g) A est intégré si {commutatif}

$ab = 0 \Leftrightarrow a = 0 \text{ ou } b = 0 \quad \forall (a, b) \in A^2$

Si l'(g) A n'est pas (i), $a, b \neq 0$ vérifient $ab = 0$ et diviseurs de zéro. $\mathbb{Z}/6\mathbb{Z}$ (m), $\bar{2} \neq \bar{0}, \bar{3} \neq \bar{0} \text{ et } \bar{2} \cdot \bar{3} = \bar{0} : \bar{2}, \bar{3} \text{ et diviseurs de zéro.}$

Z: pas d'inverse.

D₄₃) Un élément de A est dit inversible s'il $\exists b \in A$ tq $ab = 1$ & $ba = 1$. (b inverse de a , $b = a^{-1}$).

Notons $A^\times = U(A)$: ces éléments inv : unités de A. (A^\times, \cdot) : (g) abélien.

→ un (g) A do tel que tt élément non-nul est inv est CORPS.
 $\Rightarrow A^\times \neq A^*$.

(P₅₉) Tt corps commutatif est (g) intégré.

D₄₄) Si A est (g) de A (g) on 1) $(B, +)$ 2) $(A, +)$

2) B stable pr multiplication

3) $1_A \in B$

$$\Rightarrow (B, +, \cdot) \text{ est (g).}$$

D₄₅) A (g), B (g) $\Rightarrow A \times B$ (g) produit.

η: $(A \times B, +, \cdot)$, oppo $g_A \neq g_B$.

II / Idéaux

P46 si I est un idéal de A alors I est un idéal de A si

$$\begin{cases} (I, +) \text{ est } (A, +) \\ ax \in I \end{cases}$$

, $\forall a \in A, \forall x \in I$.

TH1 si I idéal de A, les 2 opérations de A, addition & multiplication passent à l'ons quotient :

$$A/I = \{a+I, a \in A\}$$

ens classe d'équivalence modulo I.

$\rightarrow (A/I, +, \cdot)$ est un corps, appelé quotient de A par I.

P60 si A est un idéal de A :

$$I = A \Leftrightarrow \exists u \in A^*, u \in I \Leftrightarrow 1_A \in I.$$

D47 si I, J sont des idéaux de A :

$$I + J = \{x + y, x \in I, y \in J\}$$

$$IJ = \left\{ \sum_{\text{finie}} x_k y_k, x_k \in I, y_k \in J \right\}.$$

P61 si I, J sont des idéaux de A $\Rightarrow I + J$ & IJ sont des idéaux de A.

P48 si $S_{\text{inv}} \subset A$, l'idéal engendré par S est

$$\left\{ \sum_{\text{finie}} a_k s_k, a_k \in A, s_k \in S \right\}.$$

idéal engendré par l'elt $x \in A$:

$$(x) = \{ax, a \in A\} \text{ noté } A_x.$$

Ce type d'idéal est un idéal principal.

Un idéal dont tous les éléments sont propres est idéal principal.

D49 Un idéal est dit premier si $\forall a, b \in A$,

$$ab \in I \Rightarrow a \in I \text{ ou } b \in I.$$

P62 $\Rightarrow I$ est premier si A/I est intègre.

D50 Un idéal M d'un idéal A est dit normal si $M \neq A$ & si pour tout idéal I de A, $M \subset I$ et $I \neq A \Rightarrow I = M$.

P64 Un idéal M est maximal si A/M est corps.

P65 Maximal \Rightarrow premier (car corps \Rightarrow idéal intègre)

P66 Toute idéal d'un idéal A est contenue dans un idéal max.

III / Morphisme d'un & TH passage au quotient

D51 $\phi: A \rightarrow B$ est un MDA si

- 1) $\phi(x+y) = \phi(x) + \phi(y)$ $\forall (x, y) \in A^2$
- 2) $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$
- 3) $\phi(1_A) = 1_B$.

P67

1. H MDA $\phi: A \rightarrow B$, $\ker \phi = \{x \in A, \phi(x) = 0_B\}$ est un idéal de A.
2. L'image, $\text{Im } \phi = \phi(A)$, d'un mda A est un idéal de B.
3. si J est un idéal de B $\Rightarrow \phi^{-1}(J) = \{x \in A, \phi(x) \in J\}$ est un idéal de A.
4. si I est un idéal de A, $\phi(I)$ n'est pas nécessairement un idéal de B mais si ϕ est surjective alors $\phi(I)$ est un idéal de B.

⑩₁₂ (Th d'isomorphisme)

soit $\phi: A \rightarrow B$ mda, soit $I \triangleleft A$ tq $I \subset \ker \phi$

$\Rightarrow \phi$ "parse au quotient module I " ie: $\exists!$ MDA $\bar{\phi}$ tq

$\bar{\phi}: A/I \rightarrow B$ tq $\bar{\phi} \circ s = \phi$, ie le diag ci-dessous commute,

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow & \dashrightarrow & \downarrow \bar{\phi} \\ A/I & \xrightarrow{s} & B \end{array} \quad \text{où } s: A \rightarrow A/I \text{ est la} \\ \text{suject canoniq.}$$

\mathfrak{d}^+ , $\text{Im } \bar{\phi} = \text{Im } \phi$. $\ker \bar{\phi} = s(\ker \phi) = \ker \phi / I$.

et pr $I = \ker \phi \Rightarrow A/\ker \phi \simeq \text{Im } \phi$.

Correspondance entre idéaux d'un et quotient de et
A \triangleleft , K \triangleleft de A. A/K \triangleleft quotient.

Notat: $\mathcal{I}d(A/K) = \{ \text{idéaux de } A/K \}$

$\mathcal{I}d_K(A) = \{ \text{idéaux de } A \text{ contenant } K \}$

$s: A \rightarrow A/K$ (suject)

On a applicato : $f: \mathcal{I}d_K(A) \longrightarrow \mathcal{I}d(A/K)$

$$j \longmapsto s(j)$$

$g: \mathcal{I}d(A/K) \longrightarrow \mathcal{I}d_K(A)$

$$j \longmapsto s^{-1}(j)$$

et $s^{-1}(j) = s^{-1}(0_{A/K}) = \ker(s) = K$.

⑩ a) f & g st & bijcts réciproq l'une de l'autre.

b) D+, pr $j \in \mathcal{I}d_K(A)$: $A/J \simeq A/K / s(j)$ ie $A/J \simeq A/K / J/K$

Rq signifia: Tl idéal J de A/K s'écriv de façon uniq
 $J = s(j) = j/K$ & j \triangleleft de A contenant K.

§4. Corps des fractions d'un \triangleleft ①.

① = $\text{Frac}(\mathbb{Z})$, soit A \triangleleft , S = A*, $A \times S = \{(a, s), a \in A, s \in S\}$
A x S def p Rde $(a, s) R (a', s') \Leftrightarrow (s'a - s'a') = 0$

• On note $\frac{a}{s}$: la cde du couple (a, s)

② Ens $((A \times S)/R, +, \cdot)$ est corps noté $F_1(A)$.

4: $A \rightarrow F_1(A)$ est mda injectif. Le corps $F_1(A)$ est le plus petit corps contenant A.

§5. Anneau Principal

③ Un \triangleleft commutif est principal si $\left\{ \begin{array}{l} \text{intègre} \\ \forall I \triangleleft \text{ de } A, \exists x \in A, I = (x) \end{array} \right.$

④ soit A \triangleleft , $a \in A$ divise $b \in A$, noté a/b si

$$a/x \exists c, b=ac \text{ si } bA \subset aA = (b)$$

Un élé x d'un \triangleleft A est dit irréductible si il

$\left\{ \begin{array}{l} \text{n'est pas inv} \\ x = ab \Rightarrow a \text{ ou } b \text{ est inv} \end{array} \right.$

i.e x ne pt pas s'écrire x pdt de 2 élé a & b de A sans que

1) l'un des 2 soit inv.

- (P69) Soit A @ principal, $x \neq 0$ de A : ASSE:
- elt x est irréductible
 - idéal (x) est premier
 - idéal (x) est maximal.
- (P70) A @ intègre, $a, b \in A$, $a|b$ si $\exists c \in A$, $b = ac$
- (a) \supset (b)
 - (b) $b \in (a)$
- $\bullet a|b$ et $b|a \Leftrightarrow (a) = (b) \Leftrightarrow b = ac$ & c inversible de A .
 $\hookrightarrow a, b$ st dits associés.

§ 5.2. Décomposition en produit d'elts irréductibles

Ds @ pl, Il élt s'écrir de manière uniq à produit d'elts irréductibles. Caractérisat amix factuels dt @ppx st ces part.

(D55) Soit la Rule def'n @ A q $x R y \Leftrightarrow \exists u \in A^\times, x = uy$.
 On dit x & y st associés. D'où $(x) = (y)$.

Un système de représentants d'elts irréductibles de I' @

A est ens elts irréductibles $(x_i)_{i \in I}$ \leftarrow ens indics pas idéal tq

\forall elt inéd. $a \in A$, $\exists i \in I$ tq $a R x_i$

$\forall i \neq j \Rightarrow x_i$ & x_j ne st pas \Leftrightarrow , \nexists elt inv u tq $x_i = ux_j$.

(D10) Soit A @ppl, $\{x_i, i \in I\}$ un SDRDEI de a . Tt elt $x \neq 0, x \in A$

$x = u \prod_{i \in I} x_i^{m_i}$, $u \in A^\times$, $m_i \in \mathbb{N}$, $m_i \neq 0$ pnt les fam' d'indics $i \in I$.

Cette décomp est uniq: $u \prod_{i \in I} x_i^{m_i} = v \prod_{i \in I} x_i^{m_i} \Leftrightarrow u = v$ et $m_i = m_i$

(u, v elts inv, $(m_i)_{i \in I}, (m_i)_{i \in I}$ familles d'entiers nuls sauf un mbt fini).

$$R9: \text{pgcd}(ca, cb) = c \cdot \text{pgcd}(a, b) \text{ car } \min(\gamma + \alpha_i, \gamma + \beta_i) = \min(\alpha_i, \beta_i)$$

- (P70) A @ intègre, $a, b \in A$, $a|b$ si $\exists c \in A$, $b = ac$
- (a) \supset (b)
 - (b) $b \in (a)$
- $\bullet a|b$ et $b|a \Leftrightarrow (a) = (b) \Leftrightarrow b = ac$ & c inversible de A .
 $\hookrightarrow a, b$ st dits associés.
- (§ 5.3. Euclide, Gauss, Dézout)
- (P56) $\text{pgcd}(a, b) = d \in A \rightarrow$ vérifie $\begin{cases} d|a \text{ et } d|b \\ \forall c \in A, c|a \text{ et } c|b \Rightarrow c|d \end{cases}$
- $\text{ppcm}(a, b) = m \in A \rightarrow$ vérifie $\begin{cases} a|m \text{ et } b|m \\ \forall c \in A, a|c \text{ et } b|c \Rightarrow m|c \end{cases}$
- (P9) $a, b \in A$,
- $\bullet m = \text{ppcm}(a, b) \Leftrightarrow (m) = (a) \cap (b)$
 - $\bullet d = \text{pgcd}(a, b) \Leftrightarrow (d) = (a) + (b)$
- $\rightarrow \forall a \in A$ (pt) $\Rightarrow \text{pgcd}(a, b) \& \text{ppcm}(a, b) \exists$ tjs. $(a, b) \neq 1$ st @ppx
- $\rightarrow a = u \prod_{i \in I} x_i^{\alpha_i}, b = v \prod_{i \in I} x_i^{\beta_i}; \forall i \quad a|x_i \Leftrightarrow \forall i \in I, \alpha_i \leq \beta_i$.

(P70) A @ pl, $\{x_i, i \in I\}$ sdrei de A , $a, b \in A$,
 u, v elts inv, $a = u \prod_{i \in I} x_i^{\alpha_i}, b = v \prod_{i \in I} x_i^{\beta_i}, \alpha_i, \beta_i \neq 0$
 $\Rightarrow \text{ppcm}(a, b) = \prod_{i \in I} x_i^{\max(\alpha_i, \beta_i)}, \text{pgcd}(a, b) = \prod_{i \in I} x_i^{\min(\alpha_i, \beta_i)}$

$\bullet a, b \in A$, @pl A st pre si $\text{pgcd}(a, b) = 1_A$.
 \hookrightarrow les seuls div communs de a & b st les inv.

(D) (Euclide)

Soit x élt inéd. @ A $x|ab \Rightarrow x|a$ ou $x|b$.

$$\Leftrightarrow ab \in (x) \Rightarrow a \in (x) \text{ ou } b \in (x)$$

① (Gauss) A ap, $a \in A$, si $x|_{ab}$ et $a/b = 1_A \Rightarrow x|_b$. §8. @ $\mathbb{Z}/m\mathbb{Z}$

⑨ (Bézout) A pl, $a, b \in A$

$$\Rightarrow (a) + (b) = \text{pgcd}(a, b) = (d)$$

\rightarrow si a, b pcc, $(a) + (b) = A \leftarrow$ idéal engendré par 1.
i.e. $\exists u, v \in A, ua + vb = 1$

§6. Anneaux euclidiens

@ anneaux $\mathbb{Z}, \mathbb{Z}[x]$; contre @ : $\mathbb{Z}[x]$

④ x tjs ppx.

⑤ A est euclidien s'il est intègre & munie DE,

i.e. $\exists \nu: A \setminus \{0\} \rightarrow \mathbb{N}$ (stathme euclidien) tq

$\forall (a, b), b \neq 0, \in A, \exists q, r \in A, a = bq + r$
& ($\nu(r) < \nu(b)$ ou $b = 0$).

⑥ TH @ euclidien est pl.

§7. @ entiers de Gauss

entiers de Gauss : $\mathbb{Z}[i] = \{a+ib, (a, b) \in \mathbb{Z}^2\}$

⑦ $\mathbb{Z}[i]$ est ss-@ de $(\mathbb{C}, +, \cdot)$.

⑧ L'ens élts inv de $\mathbb{Z}[i]$, $(\mathbb{Z}[i])^\times = \{1, -1, i, -i\}$

⑨ $\mathbb{Z}[i]$ est @ euclidien, log' m munie de la norme N def p

$$N: \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}$$

$$a+ib \mapsto a^2 + b^2$$

⑩ @ \mathbb{Z} est euclidien dc pl.

⑪ Les idéaux de @ \mathbb{Z} st ens $m\mathbb{Z} = \{mk, k \in \mathbb{Z}\}$ pr $m \in \mathbb{N}$.

⑫ Nrs premiers st élts irréduct. de \mathbb{Z} .

\rightarrow les seuls inv de \mathbb{Z} st 1 & -1.

8.2. Congruences

⑬ soit $m \in \mathbb{N}^*$, entiers x & y de \mathbb{Z} st congrus modulo m , si $\frac{m}{n-y}$.
 $n \equiv y \pmod{m} \Leftrightarrow \frac{m}{n-y} \Leftrightarrow \exists k \in \mathbb{Z}, x = y + km$.

⑭ La relati de congruence modulo un entier non nul

8.3. Elts inversibles

soit $m \in \mathbb{N}^*$, ens $\mathbb{Z}/m\mathbb{Z}$ @ q m'est pas intègre en général. $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$.

⑮ Les élts $(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{k}, \text{pgcd}(k, m) = 1\}$

" " gérant du $(\mathbb{Z}/m\mathbb{Z}, +)$. $\begin{cases} (i) \bar{k} \wedge m = 1 \\ (ii) (\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{k}, \bar{k} \wedge m = 1\} \\ (iii) \bar{k} \text{ engende } \mathbb{Z}/m\mathbb{Z} \end{cases}$

⑯ $m \in \mathbb{N}^*$, $\mathbb{Z}/m\mathbb{Z}$ est corps si m premier.

⑰ m premier si $m \wedge k = 1 \forall k = 1, 2, \dots, p-1$

$$\text{ssi } (\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \dots, \bar{p-1}\} = (\mathbb{Z}/m\mathbb{Z}) \setminus \{\bar{0}\}.$$

⑤ (Gauss) A ap, $a \in A$, si $x|_{ab}$ et $a/b = 1_A \Rightarrow x|_b$. §8. a $\mathbb{Z}/m\mathbb{Z}$

⑥ (Bézout) A pl, $a, b \in A$

$$\Rightarrow (a) + (b) = \text{pgcd}(a, b) = (d)$$

\rightarrow si a, b pcc, $(a) + (b) = A \leftarrow$ idéal engendré par 1.
i.e. $\exists u, v \in A, ua + bv = 1$

§6. Anneaux euclidiens : $\mathbb{Z}[i]$ (anneau des entiers de Gauss)

@ anneaux ppx, \mathbb{Z} , $\mathbb{R}[x]$; contre @ : $\mathbb{Z}[x]$

⑦ tjs ppx.

⑧ A est euclidien s'il est intègre & munie DE,
i.e. $\exists \nu: A \setminus \{0\} \rightarrow \mathbb{N}$ (stature euclidien) tq
 $\forall (a, b), b \neq 0, \in A, \exists q, r \in A, a = bq + r$
& $(\nu(r) < \nu(b)$ ou $\nu = 0$).

⑨ Tt @ euclidien est pl.

§7. ① entiers de Gauss

entiers de Gauss : $\mathbb{Z}[i] = \{a+ib, (a, b) \in \mathbb{Z}^2\}$

⑩ $\mathbb{Z}[i]$ est ss-@ de $(\mathbb{C}, +, \cdot)$.

⑪ L'ons élts inv de $\mathbb{Z}[i]$, $(\mathbb{Z}[i])^\times = \{1, -1, i, -i\}$

⑫ $\mathbb{Z}[i]$ est @ euclidien, log' m munit de la norme N dff p

$$N: \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}$$

$$a+ib \longmapsto a^2 + b^2$$

⑬ \mathbb{Z} est euclidien dc pl.

⑭ Les idéaux de \mathbb{Z} st ens $m\mathbb{Z} = \{mk, k \in \mathbb{Z}\}$ pr $m \in \mathbb{N}$.

⑮ Nrs premiers st tels irréduct. de \mathbb{Z} .

\rightarrow les seuls inv de \mathbb{Z} st 1 & -1.

8.2. Congruences

⑯ soit $m \in \mathbb{N}^*$, entiers x & y de \mathbb{Z} st congrus modulo m , si $\frac{m}{x-y}$.
 $n \equiv y \pmod{m} \Leftrightarrow \frac{m}{x-y} \Leftrightarrow \exists k \in \mathbb{Z}, x = y + km$.

⑰ La relati de congruence modulo un entier non nul

8.3. Elts inversibles

soit $m \in \mathbb{N}^*$, ens $\mathbb{Z}/m\mathbb{Z}$ @ q m'est pas intègre en général. $\begin{cases} (\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\} \\ = \{-1, 3\} \end{cases}$

⑱ Les élts $(\mathbb{Z}/m\mathbb{Z})^\times = \{k, \text{pgcd}(k, m) = 1\}$
généralis du ⑨ $(\mathbb{Z}/m\mathbb{Z}, +)$. $\begin{cases} (i) k \wedge m = 1 \\ (ii) (\mathbb{Z}/m\mathbb{Z})^\times = \{k, k \wedge m = 1\} \\ (iii) k \text{ engendre } \mathbb{Z}/m\mathbb{Z} \end{cases}$

⑲ $m \in \mathbb{N}^*$, $\mathbb{Z}/m\mathbb{Z}$ est corps si m premia.

⑳ m premia si $m \wedge k = 1 \quad \forall k = 1, 2, \dots, p-1$

$$\text{si } (\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \dots, \bar{p-1}\} = (\mathbb{Z}/m\mathbb{Z}) \setminus \{\bar{0}\}.$$

(D6) $\phi(n) = \text{card}((\mathbb{Z}/n\mathbb{Z})^\times)$: l'indicatrice d'Euler
 $= \text{nbr de } k \in \{1, \dots, n\} \text{ tq } k \wedge n = 1.$

• $\phi(p) = p-1$

(P22) soit $n \in \mathbb{N}^*$ $\Rightarrow n = \sum_{d|n} \phi(d)$

(Th) (Chinois)

si m, n st 2 entiers > 0 , preuve

$$\Rightarrow \mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}. \quad (*)$$

$$\xrightarrow{\text{Rq}} (*) \Rightarrow (\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times \\ = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

$$\Rightarrow \phi(mn) = \phi(m) \times \phi(n) \quad \text{si } \text{pgcd}(m, n) = 1.$$

Rq : si p premier, $x \in \mathbb{N}$,

$$\phi(p^x) = p^x - p^{x-1}.$$

Chapitre : Polynômes

$$K[X] \stackrel{\text{def}}{=} \left\{ \sum_{m=0}^N a_m X^m, \quad a_0, \dots, a_N \in K, \quad N \in \mathbb{N} \right\}$$

• K est \oplus commutatif. $a_N X^N \leftarrow \deg \text{ polygone } \neq 0$
 $\leftarrow \text{coeff dominant.}$

$$\begin{aligned} \deg(P+Q) &\leq \sup(\deg P, \deg Q) \\ \deg(PQ) &= \deg(P) + \deg(Q) \end{aligned}$$

(P26) K corps \Rightarrow 1) \oplus $K[X]$ intègre
 2) 2'ens $(K[X])^\times = K^\times$.

(P28) (FF Taylor)

$$K_m[X] = \{P \in K[X], \deg P \leq m\}, \quad P \in K_m[X], \quad a \in K:$$

$$P(x) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (x-a)^k$$

§2. Division Euclidienne

(P29) soit K \oplus intègre, soit $P \in K[X]$, supp $P \neq 0$ & coeff dominant de P est invertible do K & $\deg P \geq 1$. Pq $F \in K[X]$, $\exists! Q, R \in K[X]$ tq $F = PQ + R$ & $\deg(R) < \deg(P)$.

(C) si K est un corps, $K[X]$ est \oplus euclidien dc principal

\hookrightarrow vérifie pptéo (L) Gauss, Euclid, Bézout, décomp TI des irréductibles

§ 3. Racines d'un polynôme

④ Racine d'un polynôme $P \in K[x]$, $a \in K$
est racine de P du K si $P(a) = 0$ ou zéro de P .

$$\textcircled{P_{90}} \quad P(x) = (x-a)Q + R, \quad R = P(a)$$

⑥₈ (Multiplicité) $P \in K[x]$, $a \in K$ racine, multiplicité de la racine a , l'exposant + grde puiss de $(x-a)$ q divise P .

⑨₁ $P \in K[x]$, K corps, supp a_1, \dots, a_m racines distinctes de P de multiplicité sup m_1, \dots, m_m alors P est divisible par $(x-a_1)^{m_1} (x-a_2)^{m_2} \dots (x-a_m)^{m_m}$

Ca-Tu si $P \in K[x]$ est un polynôme non-nul alors nbr racines distinctes de P du K est $\leq \deg P$.

$\textcircled{P_{92,93}}$ si a racine de multiplicité k du P
devient racine de multiplicité $k-1$ pr P' .

§ 4. Polynômes irréductibles

$K[x]$ est \oplus \textcircled{P} , $(K[x])^\pi = K^\pi = K^*$ \{0\}

⑤ $P \in K[x]$ dit irréductible si $\forall F, G \in K[x]$,
 $P = FG$ équivaut à $F \in K[x]^\pi$ ou $G \in K[x]^\pi$,
 $\Leftrightarrow \deg F$ ou $\deg G = 0$

① $\@ \deg P=1 \Rightarrow P$ irréductible. $\rightarrow P=(x-a)Q$

\triangleright si $P(a)=0$, $a \in K$, $\deg P \geq 2 \Rightarrow P$ est réductible.

\rightarrow Irréductibles de $K[x]$: n'pe dépd de K .

⑨₅ ($K=\mathbb{C}$), les irréductibles de $\mathbb{C}[x]$ st les polynômes de $\deg 1$.

⑨₆ Les irréductibles de $\mathbb{R}[x]$ st de 2 types:

- les polynômes de $\deg 1$.
- les polynômes de $\deg 2$ sans racine du \mathbb{R} (x^2+1).

Th d'Alembert-Gauss

Tf $P \in \mathbb{C}[x]$ de $\deg n \geq 1$ admet racine ds \mathbb{C} .