

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^{re} 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 $\forall (x, y) \in E^2, x \mathcal{R}_0 y \Rightarrow f(x) = f(y)$.

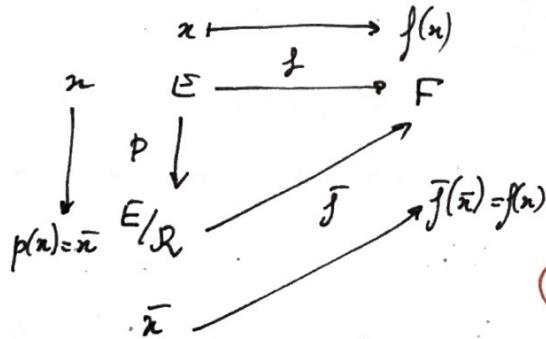
→ si f est compatible à \mathcal{R}_0 , on dit qu'il passe au quotient.

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

3! appli \bar{f} def sur 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:

$$E \xrightarrow{f} F$$

$$P \downarrow \quad \uparrow i$$

$$E/\mathcal{R}_f \xrightarrow{\bar{f}} \text{Im } f$$

$$(i(x) = x \text{ injct canoniq})$$

$$x \in \text{Im } f$$

(3)

2.6 Groupe Produit

(C2) Groupes

1. Premières définitions

1.1 Def

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

$$G \times G \rightarrow G$$

$$(a, b) \mapsto a.b$$

(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 : élmt neutre de G pt l'opérat
- $\forall a \in G, \exists b \in G, a.b = b.a = e$, tt élmt de G admt symétric, \bar{a} note

(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'un groupe G est sous-groupe si

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

(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 $n^+ > 0$: n , s' $a^n = e$.

(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)

ex 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 composit applicat.)

(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 relai de congrue à droite & à gauche modulo H par:

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

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

D'où $\bar{x}^d = xH$. (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 . ($G \otimes, H \otimes$)

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

(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

(TH) $|H|$ divise $|G|$.

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

(Cor1) $x \in G, |x|$ divise $|G|$.

(Cor2) $G \otimes$ fini; on note $n = |G|, \forall x \in G, x^n = e_G$.

△ $6 \otimes$ diviseur du ord du \otimes et potentiel de \otimes ms PAS tous. (@^{s4}A₄)

2.3. Sous-groupes distingués

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

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

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

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

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

(D24) 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 $s: G \xrightarrow{s} G/H$

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

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

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)

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

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

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

Tu 6 (3^o THI)

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

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

Tu 7 (TH de correspondance)

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

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

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

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

2.6 Groupe Product

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

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

3. Groupes cycliq's

3.1. Définitions

D25 Groupe monog'

On appelle groupe monog' un \triangleleft 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 \triangleleft 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 $G = \langle a \rangle$, \triangleleft 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 $\{h \in \mathbb{Z}, a^h = 1\} = m \mathbb{Z}$.

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

• 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 $k > 0$:
+ ptz entier tq $\frac{kn}{k} \in H$ alors H est engendré par $\frac{kn}{k}$ & $|H| = \frac{m}{k}$

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 $\mathfrak{G} \frac{k\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\ell\mathbb{Z}}{m\mathbb{Z}}$.

$$\text{On a } \frac{k\mathbb{Z}}{m\mathbb{Z}} \simeq \frac{1}{(\frac{m}{k})}\mathbb{Z}$$

(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-m.

$$\begin{aligned} \pi: G &\longrightarrow \text{Bij}(X) \\ g &\longmapsto \pi(g): X \longrightarrow X \quad \text{bijective} \\ x &\longmapsto \pi(g)(x) = g \cdot x \quad \text{résultat de l'act de } g \in G \text{ sur } x \text{ ds } X. \end{aligned}$$

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:

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

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

- 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 43) 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)

$$\Rightarrow |\mathcal{Z}(G)| \neq 13$$

(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 m̄ 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.

D1 P_n $\sigma \in \mathcal{Y}_m$, Ω une orbite de σ , $\Omega = \{\sigma^t(i), t \in \mathbb{Z}\}$
& $\sigma|_{\Omega}$ est un cycle de longueur $\text{card}(\Omega)$.

Cn6 Le \mathfrak{S}_m symétrique \mathcal{Y}_m est engendré par transposés.

G17 Deux permutations σ & σ' de \mathcal{Y}_m sont conjuguéesssi
 $\forall k \in \mathbb{N}, 2 \leq k \leq m$, apparaissent m̄ m̄ k -cycles de la décomposition canonique en produit de cycles à supports disjoints.

P151 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
 $\text{long } k \text{ cycle.}$

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.