LDD/S6 MDD354 Structures algébriques : Graphes, groupes, algèbre linéaire, topologie ...

Corrigé Des exercices II.9

II.9 . – Exercices

II.9.1 . – Magmas, groupes

Exercice II.9.1.1 Faire les détails de la preuve de la proposition II.7.14.

Solution

II.7.14.i Si ϵ et ϵ' sont neutres, alors

$$\epsilon = \epsilon * \epsilon' = \epsilon'.$$

II.7.14.ii Si y et z sont des symétriques de x pour $*$,

$$x * y = y * x = x * z = z * x = \epsilon.$$

Il s'ensuit que

$$y = y * \epsilon = y * (x * z) = (y * x) * z = \epsilon * z = z.$$

Exercice II.9.1.2 Étant donné un morphisme $f : M \rightarrow N$, (de magmas associatifs), montrer que :

- 1) si ϵ est l'élément neutre de M son image $f(\epsilon)$ n'est pas nécessairement l'élément neutre de N ;

Solution

C'est un contre exemple qui n'est pas particulièrement immédiat à construire parce que cette propriété est en fait souvent vraie. Nous ne connaissons pas nécessairement beaucoup d'exemples de magmas qui ne soient pas des groupes ; et dans le cas des groupes l'image de l'élément neutre est l'élément neutre.

Même quand un magma n'est pas un groupe l'ensemble $\mathbb{N}$ pour l'addition par exemple, il s'injecte naturellement dans un groupe $\mathbb{Z}$ et les morphismes de magma vont naturellement s'étendre en morphisme de groupes, envoyant neutre sur neutre ; et interdisant du même coup de construire un contre exemple.

Le fait de pouvoir se plonger dans un groupe correspond, pour un magma, ou à tout le moins pour un monoïde, à la propriété d'être intègre. Si l'on y déroge, on peut espérer construire un contre exemple.

Soit $M = \mathbb{R}$ muni de la multiplication (ou tout autre anneau bien sûr) et $N = \mathbb{R} \times \mathbb{R}$ muni de la multiplication $(x, y) * (z, t) = (x * z, y * t)$. Pour cette dernière loi l'élément neutre est $(1, 1)$.

Considérons enfin l'application

$$\phi : \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}, x \mapsto (x, 0).$$

On a bien entendu

$$\forall (x, y) \in \mathbb{R} \times \mathbb{R}, \phi(x * y) = (x * y, 0) = (x, 0) * (y, 0) = \phi(x) * \phi(y)$$

ce qui assure que ϕ est un morphisme de magma. Cependant

$$\phi(1) = (1, 0) \neq (1, 1).$$

- 2) si y est le symétrique de x dans M , $f(y)$ n'est pas nécessairement le symétrique de $f(x)$ dans N .

Solution

Cette propriété est fortement liée à la précédente. En reprenant les notations ci-dessus, pour $x \neq 0$, $\frac{1}{x}$ est le symétrique de x dans M . Or $\phi(x) = (x, 0)$ n'a tout simplement pas de symétrique dans N , ce ne peut donc, a fortiori être $\phi(\frac{1}{x})$.

Exercice II.9.1.3 Donner la preuve de la proposition II.7.21.

Solution

II.7.21.i Ceci revient à dire que $f *_{M^E} g$ est une application bien définie de E dans M

$$\forall (f, g) \in M^E \times M^E, ;$$

ce qui est clair.

II.7.21.ii Si on veut que $f \mapsto f(x)$ soit un morphisme, nécessairement

$$\forall (f, g) \in M^E \times M^E, (f *_{M^E} g)(x) = f(x) * g(x);$$

ce qui définit bien $*_{M^E}$ de manière unique.

II.7.21.iii

$$\begin{aligned} \forall (f, g, h) \in M^E \times M^E \times M^E, \forall x \in E, ((f *_{M^E} g) *_{M^E} h)(x) &= (f *_{M^E} g)(x) * h(x) \\ &= (f(x) * g(x)) * h(x) \\ &= f(x) * (g(x) * h(x)) \\ &= f(x) * (g *_{M^E} h)(x) \\ &= (f *_{M^E} (g *_{M^E} h))(x); \end{aligned}$$

associativité dans M

c'est-à-dire que $(f *_{M^E} g) *_{M^E} h = f *_{M^E} (g *_{M^E} h)$ i.e. $*_{M^E}$ est associative.

II.7.21.iv

$$\begin{aligned} \forall (f, g) \in M^E \times M^E, \forall x \in E, (f *_{M^E} g)(x) &= f(x) * g(x) \\ \text{commutativité de } M &= g(x) * f(x) \\ &= (g *_{M^E} f)(x). \end{aligned}$$

c'est-à-dire que $f *_{M^E} g = g *_{M^E} f$; i.e. $*_{M^E}$ est commutative.

II.7.21.v

$$\begin{aligned} \forall f \in M^E, \forall x \in E, (f *_{M^E} \epsilon_{M^E})(x) &= f(x) * \epsilon \\ &= f(x); \end{aligned}$$

i.e. $f *_{M^E} \epsilon_{M^E} = f$. On montrerait de même que $\epsilon_{M^E} *_{M^E} f = f$; si bien que ϵ_{M^E} est bien un élément neutre pour $*_{M^E}$.

Exercice II.9.1.4 1) Compléter la preuve de la proposition II.7.17.

2) a) Si ϵ est un élément neutre de M est-il encore un élément neutre d'un sous-magma N ?

Solution

Il se pourrait très bien que ϵ n'appartienne même pas N (cf. la question 1 de l'exercice II.9.1.2.)

b) Si N possède un élément neutre η celui-ci est-il nécessairement celui de M ?

Solution

Non ! (cf. la question 1 de l'exercice II.9.1.2.)

c) Si $x \in N$ possède une symétrique dans M celui-ci est-il aussi son symétrique dans N ?

Solution

On peut considérer $(\mathbb{N}, +)$ comme un sous-magma de $(\mathbb{Z}, +)$. Or dans $\mathbb{Z}$ tout élément a un opposé tandis que dans $\mathbb{N}$, seul 0 en a un.

d) Si $x \in N$ possède une symétrique dans N est-il aussi son symétrique dans M ?

Solution

Non ! (cf. la question 1 de l'exercice II.9.1.2.)

Solution

Remarque 2.5 Le fait qu'on ait fréquemment recours à l'exercice II.9.1.2 pour trouver ici des contre exemple vient de ce qu'être un sous-magma signifie que $\text{Id}_{M|_N} : N \rightarrow M$ est un morphisme. Il est certes injectif ce qui pourrait arranger certaines choses; mais de fait à l'exercice II.9.1.2 nous avons déjà construit des contre exemples avec un morphisme injectif ...

Exercice II.9.1.5 Soit $(M, *)$ un magma associatif, d'élément neutre ϵ et N un sous-magma tel que $\epsilon \in N$. Montrer que :

1) ϵ est l'élément neutre de N .

Solution

On ajoute ici l'hypothèse que $\epsilon \in N$ dont on va voir qu'elle n'est pas anodine : En effet pour tout $x \in N$, $x *_N \epsilon = x *_M \epsilon$ puisque N est un sous-magma. Donc $x *_N \epsilon = x$. De même

$$\epsilon *_N x = \epsilon *_M x = x.$$

2) si $x \in N$ a un inverse y dans N , c'est aussi son inverse dans M .

Solution

Puisque N est un sous-magma

$$y *_M x = y *_N x = \epsilon = x *_N y = x *_M y.$$

Exercice II.9.1.6 Faire la preuve de la proposition II.7.24.

Solution

II.7.24.i Si p est un morphisme

$$\begin{aligned} \forall ((x, y), (z, t)) \in (M \times N) \times (M \times N), \quad p((x, y) \dagger (z, t)) &= p(x, y) * p(z, t) \\ &= x * z; \end{aligned}$$

le même raisonnement pour q prouve que $\dagger$ est bien définie de manière unique.

— II.7.24.ii On a déjà vu dans ce contexte (cf. l'exercice I.5.1.5 et le point iii de la proposition I.1.13.15.) qu'il existe une unique application

$$h : P \rightarrow M \times N, \quad x \mapsto (f(x), g(x))$$

répondant à la question. Reste donc à voir que cette dernière est bien un morphisme or :

$$\begin{aligned} \forall (x, y) \in P, \quad h(x \dagger y) &= (f(x \dagger y), g(x \dagger y)) \\ &= (f(x) * f(y), g(x) \cdot g(y)) \\ &= (f(x), g(x)) \dagger (f(y), g(y)) \\ &= h(x) \dagger h(y). \end{aligned}$$

Exercice II.9.1.7 Soit X un ensemble. On munit l'ensemble A^X des applications de X dans A de la loi $(f, f') \mapsto ff'$ où $ff'(x) = f(x)f'(x)$ pour tout $x \in X$.

1) Montrer que la loi définie ci-dessus est la seule pour laquelle, pour tout $x \in XX$, $f \mapsto f(x)$ est un morphisme.

2) Montrer que cette loi sur A^X est associative et que A^X est un groupe pour cette loi si A est un groupe, un groupe abélien si A est un groupe abélien.

3) Si A est un groupe, et X un autre groupe, montrer que l'ensemble $\text{Hom}(X, A)$ des homomorphismes de groupes de X dans A est un sous-groupe de A^X , pourvu que A soit abélien.

Solution

$fg(ab) = f(ab)g(ab) = f(a)f(b)g(a)g(b) \stackrel{\text{abélien}}{=} f(a)g(a)f(b)g(b) = fg(a)fg(b)$. On a vraiment besoin que cela soit abélien.

Exercice II.9.1.8 (Affaiblissement des axiomes de groupe) Soit G un ensemble muni d'une loi associative notée $(G, *)$. On suppose qu'il existe un élément neutre à gauche e (c'est-à-dire que $e * x = x$ pour tout $x \in G$) et que tout élément admet un inverse à gauche (c'est-à-dire que pour tout $x \in G$, il existe $y \in G$ tel que $y * x = e$).

1) Montrer que l'inverse à gauche est aussi un inverse à droite i.e.

$$y * x = e \Rightarrow x * y = e.$$

Indication : On pourra considérer l'inverse à gauche z de y et calculer $e * (x * y) = (z * y) * (x * y)$.

Solution

Pour tout $x \in G$, il existe $y \in G$ tel que $y * x = e$ et $z \in g$ tel que $z * y = e$. Alors :

$$\begin{aligned}
 x * y &= e * (x * y) \\
 &= (z * y) * (x * y) \\
 &= ((z * y) * x) * y \\
 &= (z * (y * x)) * y \\
 &= (z * e) * y \\
 &= z * (e * y) \\
 &= z * y \\
 &= e.
 \end{aligned}$$

2) Montrer que e est aussi un *élément neutre* à droite i.e.

$$\forall x \in G, x * e = x.$$

Solution

Pour tout $x \in G, \exists y \in G$, tel que $y * x = e$; mais (cf. la question 1,) on a aussi $x * y = e$. Alors

$$x * e = x * (y * x) = (x * y) * x = e * x = x.$$

3) Montrer que $(G, *)$ est un groupe.

Solution

Grâce à la question 2 et à la question 1, les axiomes de la définition II.8.1.1 sont satisfaits.

Exercice II.9.1.9 (Unicité des éléments remarquables) Soit $(E, *)$ un ensemble muni d'une loi associative.

Solution

Il s'agit en définitive d'un magma (cf. cours définition II.7.1) associatif; et l'on pourra se borner ici à rappler les résultats de la proposition II.7.14 et de l'exercice II.9.1.1.

1) (**Élément neutre**)

Montrer que si $(E, *)$ possède un *élément neutre* ϵ celui-ci est unique.

Solution

(cf. le point i de la proposition II.7.14.)

2) (**Symétrique**)

Montrer que si $(E, *)$ possède un *élément neutre* ϵ , tout élément $x \in E$ possède au plus un symétrique.

Solution

(cf. le point ii de la proposition II.7.14.)

Exercice II.9.1.10 (Morphismes de groupes) Soit

$$f : (G, *, \epsilon_G) \rightarrow (H, \cdot, \epsilon_H)$$

un *morphisme de groupes* .

Solution

Cet exercice est évidemment à mettre en rapport avec exercice II.9.1.2 et l'on va constater que l'hypothèse que l'on a des groupes et non plus simplement des magmas donnent des propriétés supplémentaires :

1) (**Élément neutre**)

Montrer que $f(\epsilon_G) = \epsilon_H$.

Solution

On a $\epsilon_G * \epsilon_G = \epsilon_G$; ce qui entraîne, puisque f est un morphisme

$$f(\epsilon_G) \cdot f(\epsilon_G) = f(\epsilon_G * \epsilon_G) = f(\epsilon_G) .$$

Or H est un groupe si bien que $f(\epsilon_G)$ a un symétrique $\eta \in H$. L'égalité précédente entraîne alors :

$$\epsilon_H = \eta \cdot f(\epsilon_G) a = \eta \cdot f(\epsilon_G) \cdot f(\epsilon_G) \cdot f(\epsilon_G) = f(\epsilon_G) .$$

2) (Symétrique)

Montrer que pour tout $x \in G$, si y est son symétrique, $f(y)$ est le symétrique de $f(x)$.

Solution

Si $(x, y) \in G \times G$ sont symétriques l'un de l'autre

$$\begin{aligned} x * y = y * x &= \epsilon_G \\ \Rightarrow f(x * y) = f(y * x) &= f(\epsilon_G) \\ \Rightarrow f(x) \cdot f(y) = f(y) \cdot f(x) &= \epsilon_H ; \end{aligned}$$

en utilisant bien entendu question 1.

3) (Image)

Montrer que $\text{Im } f$ est un sous-groupe de $(H, \cdot)$.

Solution

Puisque G est un groupe il est non vide et par conséquent $\text{Im } f = f(G)$ est non vide.

De plus pour tout $(u, v) \in \text{Im } f \times \text{Im } f$, il existe $(x, y) \in G \times G$ tel que

$$u = f(x) \text{ et } v = f(y) .$$

Or (cf. 2.) $u^{-1} = f(x^{-1})$; si bien que $\cdot^{-1}v = f(x^{-1} * y)$ qui appartient à $\text{Im } f$, qui est donc bien un sous-groupe de H .

4) (Noyau)

Montrer que $\text{Ker } f$ est un sous-groupe de $(G, *)$.

Solution

Puisque (cf. 1.) $f(\epsilon_G) = \epsilon_H$, $\epsilon_G \in \text{Ker } f$; si bien que $\text{Ker } f \neq \emptyset$.

De plus :

$$\begin{aligned} \forall (x, y) \in \text{Ker } f \times \text{Ker } f, \quad f(x^{-1} * y) &= f(x^{-1}) \cdot f(y) \\ &= f(x)^{-1} \cdot f(y) \\ &= \epsilon_H^{-1} \cdot \epsilon_H \\ &= \epsilon_H \\ \Rightarrow x^{-1} * y &\in \text{Ker } f . \end{aligned}$$

ce qui prouve que $\text{Ker } f$ est un sous-groupe de G .

5) (Isomorphisme)

Montrer que si f est bijective et que g est son applications réciproque, alors g est un morphisme de groupe.

Solution

Ici il n'est pas utile d'avoir affaire à des groupes puisque le résultat est déjà vrai pour des magmas associatifs (cf. II.7.6.)

Exercice II.9.1.11 (Le groupe $(\mathcal{S}(E), \circ)$) Soit E un ensemble.

1) Vérifier que $\circ$ est une loi interne sur $\mathcal{S}(E)$.

Solution

La composée de deux bijections de E dans E est encore une bijection de E dans E .

2) Montrer qu'il existe un élément neutre pour la loi $\circ$ dans $\mathcal{S}(E)$ et le caractériser.

Solution

Il est immédiat de constater que

$$\forall f \in \mathcal{S}(E), \text{Id}_E \circ f = f \circ \text{Id}_E = f$$

c'est-à-dire que l'application $\text{Id}_E : E \rightarrow E$ caractérisée par

$$\forall x \in E, \text{Id}_E(x) = x$$

est un élément neutre pour $\circ$ dans $\mathcal{S}(E)$.

3) Montrer finalement que $(\mathcal{S}(E), \circ)$ est un groupe.

Solution

On a vu à la question 1 que la loi $\circ$ sur $\mathcal{S}(E)$ est une loi interne. Elle est évidemment associative. Elle possède un élément neutre Id_E (cf. la question 2.)

De plus pour toute bijection $f : E \rightarrow E$ il existe une bijection $g : E \rightarrow E$ telle que

$$\forall x \in E, g[f(x)] = f[g(x)] = x$$

c'est-à-dire que $f \circ g = g \circ f = \text{Id}_E$ (cf. l'exercice I.5.1.4.) donc que g est le symétrique de f pour $\circ$ qu'on notera usuellement f^{-1} .

Exercice II.9.1.12 (La bijection $\mathcal{S}(E) \cong \mathcal{S}(F)$) Soient E et F deux ensembles et $u : E \rightarrow F$ une bijection de E dans F dont on notera v la bijection réciproque i.e.

$$v : F \rightarrow E : v \circ u = \text{Id}_E, u \circ v = \text{Id}_F.$$

Montrer que l'application

$$\phi_u : (\mathcal{S}(E), \circ) \rightarrow (\mathcal{S}(F), \circ), f \mapsto u \circ f \circ v$$

est un isomorphisme de groupes.

Solution

i) (**Application**)

On constate d'abord que, pour tout $f \in \mathcal{S}(E)$, $\phi_u(f) = u \circ f \circ v$ est bien une application de F dans lui-même qui est de plus, une bijection comme composée de trois bijections. C'est donc bien un élément de $\mathcal{S}(F)$.

ii) (**Morphisme**)

De plus,

$$\begin{aligned} \forall (f, g) \in \mathcal{S}(E) \times \mathcal{S}(E), \quad \phi_u(f \circ g) &= u \circ f \circ g \circ v \\ &= u \circ f \circ v \circ u \circ g \circ v \\ &= \phi_u(f) \circ \phi_u(g); \end{aligned}$$

c'est-à-dire que ϕ_u est bien un morphisme de groupes.

iii) (**Isomorphisme**)

Notons

$$\phi_v : (\mathcal{S}(F), \circ) \rightarrow (\mathcal{S}(E), \circ), f \mapsto v \circ f \circ u$$

Alors :

$$\begin{aligned} \forall f \in \mathcal{S}(E), \quad \phi_v[\phi_u(f)] &= v \circ \phi_u(f) \circ u \\ &= v \circ u \circ f \circ v \circ u \\ &= f \\ \Rightarrow \quad \phi_v \circ \phi_u &= \text{Id}_{\mathcal{S}(E)}; \end{aligned}$$

et de plus :

$$\begin{aligned} \forall f \in \mathcal{S}(F), \quad \phi_u[\phi_v(f)] &= u \circ \phi_v(f) \circ v \\ &= u \circ v \circ f \circ u \circ v \\ &= f \\ \Rightarrow \quad \phi_u \circ \phi_v &= \text{Id}_{\mathcal{S}(F)}. \end{aligned}$$

Ceci prouve que ϕ_u est un isomorphisme, d'isomorphisme réciproque ϕ_v .

Exercice II.9.1.13 (Sous-groupes) 1) (Intersection de deux sous-groupes)

Pour deux sous-groupes H et K d'un groupe G , $H \cap K$ est un sous-groupe de G .

Solution

Puisque H et K sont des sous-groupes $\epsilon \in H$ et $\epsilon \in K$; si bien que $\epsilon \in H \cap K$ qui est donc non vide.
De plus $\forall (x, y) \in (H \cap K) \times (H \cap K)$,

$$x^{-1} * y \in H \text{ et } x^{-1} * y \in K$$

puisque H et K sont des sous-groupes. Par conséquent $x^{-1} * y \in H \cap K$ qui est donc un sous-groupe.

2) (Union de deux sous-groupes)

Étant donnés des sous-groupes H et K d'un groupe commutatif $(G, +)$, montrer que $H \cup K$ est un sous-groupe de $(G, +)$ si et seulement si $H \subset K$ ou $K \subset H$.

Indication : Montrer qu'il revient au même de démontrer que $[H \not\subset K \text{ et } H \cup K \text{ sous-groupe entraîne } K \subset H]$ puis prouver cette dernière assertion.

Solution

Étant donné un groupe commutatif $(G, +)$, H et K des sous-groupes, si $H \subset K$ (resp. $K \subset H$), $H \cup K = K$ (resp. H) qui est bien évidemment un sous-groupe.

Si $H \cup K$ est un sous-groupe de $(G, +)$ supposons que H n'est pas inclus dans K . Il existe alors $x \in H$ tel que $x \notin K$. Alors pour tout $y \in K$, x et y sont des éléments de $H \cup K$ et par conséquent $x + y \in H \cup K$ c'est-à-dire que $x + y \in K$ ou $x + y \in H$. Si $x + y \in K$, comme $y \in K$, $x + y - y \in K$ c'est-à-dire que $x \in K$ ce qui est contraire à l'hypothèse. Il s'ensuit que nécessairement $x + y \in H$. Comme $x \in H$, $x + y - x \in H$ c'est-à-dire que $y \in H$. Nous avons donc démontré que tout élément $y \in K$ est dans H c'est-à-dire que $K \subset H$.

3) (Famille filtrante)

Faire la preuve du point iv de la proposition II.8.3.7.

Solution

Notons $K := \bigcup_{n \in \mathbb{N}} H_n$. $\forall n \in \mathbb{N}$, H_n est un sous-groupe de G par hypothèse; et H_n est donc non vide; si bien que $K \neq \emptyset$.

Par ailleurs pour tout $(x, y) \in K \times K$, il existe $(p, q) \in \mathbb{N} \times \mathbb{N}$ tel que $x \in H_p$ et $y \in H_q$.

Or il existe, par hypothèse, $r \in \mathbb{N}$ tel que $H_p \subset H_r$ et $H_q \subset H_r$; si bien que

$$x \in H_r \text{ et } y \in H_r.$$

Or H_r étant un sous-groupe de G , $x^{-1} * y \in H_r$; comme $H_r \subset K$, $x^{-1} * y \in K$; ce qui achève de prouver que K est un sous-groupe de G .

Exercice II.9.1.14 (Sous-groupe engendré) Soient G un groupe, S une partie de G et H une autre partie de G .

Montrer que les assertions suivantes sont équivalentes :

- L'ensemble H est l'intersection de tous les sous-groupes de G contenant S .
- L'ensemble H est un sous-groupe de G contenant S et tel que, pour tout sous-groupe K de G contenant S , $H \subset K$.
- H est constitué des éléments $s_1 s_2 \dots s_r$ avec $r \geq 1$ où un élément s_i est dans S ou a son inverse dans S .

Solution

$a \Rightarrow b$ L'intersection d'une famille (non nécessairement finie) de sous-groupes est encore un sous-groupe. Si chaque élément de la famille contient S , l'intersection contient encore S . Enfin si K est un sous-groupe contenant S , c'est précisément un élément de la famille et il contient donc l'intersection H .

$b \Rightarrow a$ Soit $\mathcal{H}$ l'ensemble de tous les sous-groupes de G contenant S . Alors par hypothèse $H \in \mathcal{H}$. Si $L = \bigcap_{K \in \mathcal{H}} K$, $L \subset H$. Mais, par hypothèse, $\forall K \in \mathcal{H}$, $H \subset K$, donc $H \subset L$, donc $H = L$.

$b \Leftrightarrow c$ Notons L l'ensemble des produits $s_1 \dots s_r$ avec

$$\forall 1 \leq i \leq r, s_i \in S \text{ ou } s_i^{-1} \in S.$$

Vérifions d'abord que L est un sous-groupe : Si $S = \emptyset$, $L = \{\epsilon\}$ où ϵ est l'élément neutre de G ; et L est donc bien un sous-groupe de G . Sinon $L \subset S$, de manière presque immédiate; ce qui entraîne $L \neq \emptyset$.

De plus, pour tout $s_1, \dots, s_r \in L$,

$$(s_1 \dots s_r)^{-1} = s_r^{-1} \dots s_1^{-1} \in L.$$

Enfin pour

$$(s_1 \dots s_r, s'_1 \dots s'_{r'} \in L \times L, s_1 \dots s_r \cdot s'_1 \dots s'_{r'} \in L;$$

ce qui achève de prouver que L est un sous-groupe de G contenant S .

Or l'équivalence $a \Leftrightarrow b$ assure qu'un tel sous-groupe est unique et que c'est donc bien H défini en b .

Exercice II.9.1.15 (Caractérisation des sous-groupes distingués) Compléter la démonstration de la proposition II.8.10.3.

Solution

$a \Rightarrow f$ Il s'agit d'à peine modifier l'argument déjà donné pour l'équivalence entre b et f dans la preuve de la proposition II.8.10.3. En effet

$$\forall (x, y) \in G \times H, y \sim_{H,d} e \text{ et } x^{-1} \sim_{H,d} x^{-1};$$

ce qui entraîne, en vertu du point a $y * x^{-1} \sim_{H,d} e * x^{-1}$; c'est-à-dire

$$x * y * x^{-1} = x^{-1^{-1}} * y * x^{-1} \in H.$$

$f \Rightarrow a$ Étant donné un quadruplet (x, z, y, t) d'éléments de G , si $x \sim_{H,d} z, z^{-1}x \in H$; ce qui entraîne, en vertu de l'assertion f

$$y^{-1} * z^{-1} * x * y = y^{-1} * z^{-1} * x * y^{-1^{-1}} \in H.$$

Si de plus $y \sim_{H,d} t, t^{-1} * y \in H$. Puisque H est un groupe il s'ensuit que

$$t^{-1} * z^{-1} * x * y = t^{-1} * y * y^{-1} * z^{-1} * x * y \in H;$$

c'est-à-dire que

$$x * y \sim_{H,d} z * t.$$

$e \Rightarrow f$ est immédiat.

$f \Rightarrow d$ Soit $x \in G$. Pour tout $y \in x * H$, il existe $z \in H$, tel que $y = x * z$ i.e. $y * x^{-1} = x * z * x^{-1}$. Or, d'après $f, x * z * x^{-1} \in H$. Il existe donc $w \in H$ tel que

$$y * x^{-1} = x * z * x^{-1} = w,$$

d'où $y = w * x$ c'est-à-dire que $y \in H * x$. On vient donc de montrer que f implique que $x * H \subset H * x$.

L'inclusion réciproque s'obtient par le même argument, en appliquant cette fois f à l'élément x^{-1} .

$d \Rightarrow e$ Soit $g \in G$. Pour tout $y \in x * H * x^{-1}$, il existe $z \in H$ tel que $y = x * z * x^{-1}$. Or $x * z \in x * H$. D'après $d, x * z \in H * x$. Il existe donc $w \in H$ tel que $x * z = w * x$; c'est-à-dire que

$$y = x * z * x^{-1} = w * x * x^{-1} = w \in H.$$

On vient donc de démontrer que d implique que $x * H * x^{-1} \subset H$.

Réciproquement, $\forall y \in H, x^{-1} * y \in x^{-1} * H$. D'après yyd de la proposition II.8.10.3, $x^{-1} * y \in H * x^{-1}$.

Il existe donc $z \in H$ tel que $x^{-1} * y = z * x^{-1}$ c'est-à-dire

$$y = x * z * x^{-1} \in x * H * x^{-1}.$$

On vient donc de montrer que $H \subset x * H * x^{-1}$; ce qui termine la preuve.

Exercice II.9.1.16 (Image réciproque/directe) Faire la preuve de la proposition II.8.10.8.

Solution

i) (Image réciproque)

Soit donc $L \subset H$ un sous-groupe distingué de H . On sait déjà que $f^{-1}(L)$ est un sous-groupe de G . De plus :

$$\begin{aligned} \forall x \in G, \forall y \in f^{-1}(L), \quad f(x * y * x^{-1}) & \stackrel{=}{=} f(x) * f(y) * f(x)^{-1} \\ & \stackrel{\substack{L \text{ est distingué} \\ \in}}{\in} L \\ \Rightarrow \quad x * y * x^{-1} & \in f^{-1}(L); \end{aligned}$$

c'est-à-dire que $f^{-1}(L)$ est distingué.

ii) **(Image directe)**

Considérons un sous-groupe stricte $G \subset H$; c'est-à-dire que $G \neq H$. Supposons de plus que G n'est pas distingué dans H . On peut par exemple prendre $H := \text{GL}_2(\mathbb{R})$ et

$$G := \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, (a, b) \in \mathbb{R}^2, ab \neq 0 \right\}.$$

Alors

$$\text{Id}_{H|G} : G \rightarrow H$$

est un morphisme de groupes et $f(G) = G$ qui n'est pas distingué dans H ; alors que G est distingué dans lui-même.

iii) **(Le cas surjectif)**

Considérons un morphisme $f : G \rightarrow H$ surjectif et $K \subset G$ un sous-groupe distingué . Alors :

$$\begin{aligned} \forall y \in f(K), \forall x \in H, \exists v \in K, y = f(v) & \wedge \exists u \in G, x = f(u) \\ \Rightarrow x * y * x^{-1} &= f(u) * f(v) * f(u)^{-1} \\ &= f(v * u * v^{-1}) \\ &\in f(K). \end{aligned}$$

Exercice II.9.1.17 (Sous-groupe d'un groupe fini) Faire la démonstration de la proposition II.8.12.3 et comparer avec la proposition II.8.3.5.

Solution

Dans le cas d'un groupe fini on n'est pas obligé de vérifier que $x^{-1} \in H$; contrairement à ce qui est exigé dans la situation de la proposition II.8.3.5. En effet, $x * x \in H$ entraîne, par récurrence, que

$$\forall n \in \mathbb{N}, x^n \in H.$$

Or G étant fini

$$\exists n \in \mathbb{N}, x^n = e;$$

si bien que $x^{-1} = x^{n-1}$ qui appartient donc à H .

Exercice II.9.1.18 Faire la preuve du point i de la proposition II.8.12.8.

Exercice II.9.1.19 (Groupe des automorphismes) Complétez la construction de l'exemple II.8.3.6.

Solution

Étant donné un groupe G ,

- on constate d'abord que $\text{Aut}(G) \neq \emptyset$, puisqu'on a remarqué (cf. l'exemple II.8.2.8,) que $\text{Id}_G \in \text{Aut}(G)$.
- De plus pour tout $\phi \in \text{Aut}(G)$, puisque $\phi \in \mathcal{S}(G)$, il exist $\psi \in \mathcal{S}(G)$ tel que

$$\phi \circ \psi = \psi \circ \phi = \text{Id}_G.$$

Il résulte alors lemme II.7.5 que ψ est également un morphisme et donc un automorphisme i.e. $\psi \in \text{Aut}(G)$.

- Enfin $\forall (\phi, \psi) \in \text{Aut}(G) \times \text{Aut}(G)$, $\phi \circ \psi \in \mathcal{S}(G)$, puisqu'on sait déjà que $\mathcal{S}(G)$ est un groupe. De plus $\phi \circ \psi$ est un morphisme d'après le point ii du lemme II.8.2.3.

Il résulte alors des vérifications ci-dessus et de la proposition II.8.3.5 que $(\text{Aut}(G), \circ)$ est un sous-groupe de $(\mathcal{S}(G), \circ)$.

Exercice II.9.1.20 On suppose que E est munie d'une relation d'équivalence $\sim$ et d'une loi

$$\cdot : E \times E \rightarrow E.$$

On suppose que $\cdot$ et $\sim$ sont compatibles c'est-à-dire que

$$\forall (x, y, z, t) \in E \times E \times E, (x \sim y \wedge z \sim t \Rightarrow x \cdot z \sim y \cdot t).$$

On note $\pi : E \rightarrow E / \sim$ la surjection canonique .

1) Montrer qu'il existe une unique loi $\dagger : E / \sim \times E / \sim \rightarrow E / \sim$ tel que π soit un morphisme c'est-à-dire que

$$\forall (x, y) \in E \times E, (\pi(x \cdot y) = \pi(x) \dagger \pi(y)).$$

On parle alors de *structure quotient*.

Solution

i) (**Unicité**)

Pour tout $(\alpha, \beta) \in E/\sim \times E/\sim$, il existe $(x, y) \in E \times E$ tel que

$$\alpha = \pi(x) \text{ et } \beta = \pi(y).$$

Alors nécessairement, dès l'instant où l'on exige que π soit un morphisme

$$\alpha \dagger \beta = \pi(x) \dagger \pi(y) = \pi(x \cdot y);$$

ce qui assure que $\dagger$ est au plus définie d'une manière.

ii) (**Existence**)

Reste à voir si la formule ci-dessus définit bien $\dagger$; en d'autres termes s'il n'y a pas d'ambiguïté sur la définition. En effet, si $(z, t) \in E \times E$ vérifie

$$\alpha = \pi(z) \text{ et } \beta = \pi(t),$$

on a, également nécessairement

$$\alpha \dagger \beta = \pi(z \cdot t).$$

Il faut alors remarquer que :

$$\begin{array}{l} \Leftrightarrow x \sim z \\ \sim \text{ et } \cdot \text{ sont compatibles} \\ \Rightarrow \end{array} \quad \begin{array}{l} \pi(x) = \alpha = \pi(z) \quad \wedge \quad \pi(y) = \beta = \pi(t) \\ \wedge \quad y \sim t \\ x \cdot y \sim z \cdot t \\ \pi(x \cdot y) = \pi(z \cdot t); \end{array}$$

ce qui assure que $\dagger$ est bien définie.

2) Montrer que si $\cdot$ est associative, (resp. possède un *élément neutre*) (resp. est commutative) il en est de même de $\dagger$. Montrer que si $x \in E$ possède un symétrique y pour $\cdot$ alors $\pi(y)$ est le symétrique de $\pi(x)$ pour $\dagger$.

Solution

i) (**Associativité**)

Supposons que $\cdot$ est associative. Alors :

$$\begin{array}{l} \forall (\alpha, \beta, \gamma) \in E/\sim \times E/\sim \times E/\sim, \quad \exists (x, y, z) \in E \times E \times E, \quad \alpha = \pi(x), \beta = \pi(y), \gamma = \pi(z) \\ \alpha \dagger (\beta \dagger \gamma) = \pi(x) \dagger [\pi(y) \dagger \pi(z)] \\ = \pi(x) \dagger \pi(y \cdot z) \\ = \pi[x \cdot (y \cdot z)] \\ = \pi[(x \cdot y) \cdot z] \\ = \pi(x \cdot y) \dagger \pi(z) \\ = [\pi(x) \dagger \pi(y)] \dagger \pi(z) \\ = (\alpha \dagger \beta) \dagger \gamma; \end{array}$$

ce qui prouve que $\dagger$ est associative.

ii) (**Commutativité**)

C'est un calcul à peu près identique à celui fait ci-dessus.

iii) (**Élément neutre**)

On pourrait légitimement penser que si $e \in E$ est un *élément neutre* pour $\cdot$, $\pi(e)$ est un *élément neutre* pour $\dagger$. On a cependant vu (cf. la question 1 de l'exercice II.9.1.2.) qu'en toute généralité l'image du neutre n'est pas nécessairement le neutre; même si c'est le cas dans le contexte des groupes (cf. la question 1 de l'exercice II.9.1.10.)

Cependant ici, pour tout $\alpha \in E/\sim$, il existe $x \in E$ tel que $\alpha = \pi(x)$. Alors :

$$\begin{array}{l} \alpha \dagger \pi(e) = \pi(x) \dagger \pi(e) \\ = \pi(x \cdot e) \\ = \pi(x) \\ = \alpha \\ = \pi(e \cdot x) \\ = \pi(e) \dagger \pi(x) \\ = \pi(e) \dagger \alpha; \end{array}$$

ce qui prouve que $\pi(e)$ est bien un élément neutre . On pourrait laisser le lecteur réfléchir encore un peu à ce qu'on a ajouté ici^a par rapport à la question 1 de l'exercice II.9.1.2 .

iv) **(Symétrie)**
découle du point ci-dessus.

a. la surjectivité de π !!!

3) Donner des exemples déjà connus des constructions précédentes.

Exercice II.9.1.21 (Congruence modulo n) 1) Montrer que tout entier relatif divise 0 tandis que 0 ne divise que lui-même.

Solution

En effet pour tout $a \in \mathbb{Z}$, $0a = 0$; en revanche

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}, ab = 0 \Rightarrow a = 0 \text{ ou } b = 0 .$$

Pour tout entier naturel n on définit la **relation de congruence modulo n sur $\mathbb{Z}$ par a congrue à b modulo n si n divise $b - a$ et l'on écrit**

$$a \equiv b [n] .$$

2) Montrer que la relation de congruence modulo n est une relation d'équivalence .

Solution

i) **(Réflexivité)**

Puisque $n|0$, pour tout $a \in \mathbb{N}$, $n|a - a$ donc

$$a \equiv a [n] .$$

ii) **(Symétrie)**

$$\begin{aligned} \forall (a, b) \in \mathbb{Z} \times \mathbb{Z}, \quad a &\equiv b [n] \\ \Rightarrow \quad n &| b - a \\ \Rightarrow \quad n &| a - b \\ \Rightarrow \quad b &\equiv a [n] . \end{aligned}$$

iii) **(Transitivité)**

$$\begin{aligned} \forall (a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, \quad a &\equiv b [n] \quad \wedge \quad b \equiv c [n] \\ \Rightarrow \quad n &| b - a \quad \wedge \quad n | c - b \\ \Rightarrow \quad n &| b - a + c - b \\ \Rightarrow \quad n &| c - a \\ \Rightarrow \quad a &\equiv c [n] . \end{aligned}$$

On notera $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des **classes d'équivalence** pour la relation de congruence modulo n , qu'on abrègera en **Classes de congruence modulo n** .

Pour tout $a \in \mathbb{Z}$, on notera $\pi_n(a)$ ou $\bar{a}$ la classe de a modulo n .

3) a) Montrer que $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ est une application surjective. On l'appelle usuellement *surjection canonique*.

Solution

C'est une propriété des relations d'équivalence qu'on a toujours $a \in \bar{a} = \pi_n(a)$ si bien que π_n est surjective.

b) Est-elle injective ?

Solution

Pour $n = 0$,

$$a \equiv b [n] \Leftrightarrow a = b$$

et dans ce cas et dans ce cas seulement, π_n est injective.

Dans le cas général

$$\forall a \in \mathbb{Z}, a \neq a + n \text{ et } a \equiv a + n [n] \Rightarrow \pi_n(a) = \pi_n(a + n).$$

4) Donner le cardinal de $\mathbb{Z}/n\mathbb{Z}$.

Solution

On sait que

$$\forall n \in \mathbb{N}^*, \#(\mathbb{Z}/n\mathbb{Z}) = n$$

et

$$\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}.$$

5) Un entier naturel n étant fixé, montrer que, pour tout quadruplet (a, b, c, d) d'entiers relatifs,

$$a \equiv c [n] \text{ et } b \equiv d [n] \Rightarrow a + b \equiv c + d [n];$$

c'est-à-dire que la relation de congruence et la loi d'addition $+$ sont compatibles

Solution

$$\begin{aligned} \forall (a, b, c, d) \in \mathbb{Z}^4, \quad & a \equiv c [n] \quad \wedge \quad b \equiv d [n] \\ \Rightarrow & n | c - a \quad \wedge \quad n | d - b \\ \Rightarrow & n \quad | \quad (c + d) - (a + b) = c - a + d - b. \end{aligned}$$

II.9.2 . – Action de groupe

II.9.2.1. – Quelques résultats du cours à démontrer

Exercice II.9.2.1.1 Quelques résultats du cours à propos des actions de groupe (cf. II.8.5)

1) Faire la démonstration du lemme II.8.6.5

Solution

II.8.6.5.a $\Rightarrow$ II.8.6.5.b Notons $O_G(x)$ l'unique orbite. Pour tout $y \in E, y \in O_G(y)$. Or par hypothèse, $O_G(x) = O_G(y)$ donc $y \in O_G(x)$; si bien que $E \subset O_G(x)$. Comme tautologiquement $O_G(x) \subset E$,

$$\forall y \in E, E = O_G(x) = O_G(y).$$

II.8.6.5.b $\Rightarrow$ II.8.6.5.c On sait qu'il existe $x \in E$ tel que $O_G(x) = E$. (On a en fait même montré que pour tout $x \in E E = O_G(x)$.) Pour tout $(y, z) \in E \times E$,

$$y \in O_G(x) \text{ et } z \in O_G(x);$$

i.e.

$$\exists (a, b) \in G \times G, y = a \cdot x \text{ et } z = b \cdot x$$

d'où il résulte $y = (a * b^{-1}) \cdot z$.

II.8.6.5.c $\Rightarrow$ II.8.6.5.a Est immédiat.

2) Faire la démonstration de la proposition II.8.7.1.

Solution

Bien entendu si ϵ désigne l'élément neutre de G , pour tout $x \in E$, et par définition d'une action $\epsilon \cdot x = x$; si bien que $\epsilon \in \text{Stab}_G(x)$. Ainsi $\text{Stab}_G(x) \neq \emptyset$.

Par ailleurs,

$$\begin{aligned} \forall (a, b) \in \text{Stab}_G(x) \times \text{Stab}_G(x), \quad & a \cdot x = x \quad \wedge \quad b \cdot x = x \\ \Rightarrow & a \cdot x = x \quad \wedge \quad x = b^{-1} \cdot x \\ \Rightarrow & a \cdot (b^{-1} \cdot x) = x \\ \Rightarrow & (a * b^{-1}) \cdot x = x \\ \Rightarrow & a * b^{-1} \in \text{Stab}_G(x); \end{aligned}$$

ce qui achève de prouver que $\text{Stab}_G(x)$ est un sous-groupe de G .

3) Faire la démonstration du point i de la proposition II.8.7.3.

Solution

On pourrait simplement dire que $a \sim b \Leftrightarrow p(a) = p(b)$ est une relation d'équivalence pour laquelle $p^{-1}(\{p(a)\})$ est la classe d'équivalence de a . Alors, les classes formant une partition de G on obtient le résultat. Il est presque aussi immédiat de le montrer directement. En effet puisque p est surjective,

$$\forall y \in O(x), p^{-1}(\{y\}) \neq \emptyset.$$

Par ailleurs

$$\forall a \in G, a \in p^{-1}(\{p(a)\})$$

ce qui entraîne

$$G = \bigcup_{y \in O(x)} p^{-1}(\{y\}).$$

Enfin :

$$\begin{aligned} \forall (y, z) \in O(x) \times O(x), & p^{-1}(\{y\}) \cap p^{-1}(\{z\}) \neq \emptyset \\ \Rightarrow \exists a \in G, & a \in p^{-1}(\{y\}) \wedge a \in p^{-1}(\{z\}) \\ \Rightarrow & p(a) = y \wedge p(a) = z \\ \Rightarrow & y = z \\ \Rightarrow & p^{-1}(\{y\}) = p^{-1}(\{z\}); \end{aligned}$$

ce qui achève de prouver que $\{p^{-1}(\{y\}), y \in O(x)\}$ est une partition de G .

Exercice II.9.2.1.2 Faire la démonstration du point ii de la proposition II.8.9.5.

Solution

On sait que pour (cf. cours lemme II.8.9.1.) $g \in G$, l'application $G \rightarrow G, x \mapsto g * x * g^{-1}$ est un automorphisme de G . L'image d'un sous-groupe est donc encore un sous-groupe. Ceci entraîne que l'application

$$g \times G \rightarrow G, (g, H) \mapsto g * H * g^{-1}$$

est bien définie.

Il est immédiat que $\epsilon \cdot H = \epsilon * H * \epsilon^{-1} = H$. En outre :

$$\begin{aligned} \forall (g, h) \in G \times G, (gh) * H * (gh)^{-1} &= \{(gh) * k * (gh)^{-1}, k \in H\} \\ &= \{g * h * k * h^{-1} * g^{-1}, k \in H\} \\ &= \{g * k * g^{-1}, k \in h * H * h^{-1}\} \\ &= g \cdot (h * H * h^{-1}) \\ &= g \cdot (h \cdot H); \end{aligned}$$

ce qui achève de prouver qu'on a bien défini une action.

Exercice II.9.2.2 (Stabilisateur) Soit $(G, *)$ un groupe et E un ensemble muni d'une action de G notée $g \cdot x$ pour tout $(g, x) \in G \times E$.

Montrer que pour tout $(x, g) \in E \times G, \text{Stab}_G(g \cdot x) = g * \text{Stab}_G(x) * g^{-1}$.

Solution

(Voir aussi la proposition II.8.7.5 du cours.)

Pour tout $(x, g, h) \in E \times G \times G, h \in \text{Stab}(G)g \cdot x$ si et seulement si $h \cdot (g \cdot x) = g \cdot x$ si et seulement si

$$g^{-1} \cdot (h \cdot (g \cdot x)) = x \Leftrightarrow (g^{-1} * h * g) \cdot x = x \Leftrightarrow g^{-1} * h * g \in \text{Stab}_G(x)$$

c'est-à-dire qu'il existe $k \in \text{Stab}_G(x)$ tel que $g^{-1} * h * g = k$ i.e. $h = g * k * g^{-1}$ c'est-à-dire finalement que

$$h \in g * \text{Stab}_G(x) * g^{-1}.$$

Exercice II.9.2.3 (Équation aux classes)

Soit $(G, *)$ un groupe dont on note e l'élément neutre .

Pour tout $(x, y) \in G \times G$, on dit que y est conjugué à x s'il existe $g \in G$ tel que $y = g^{-1} * x * g$. On notera $x \sim y$.

1) Montrer que la relation « est conjugué à » est une relation d'équivalence dite relation de conjugaison ce qui permettra de dire dorénavant x et y sont conjugués. On appellera classe de conjugaison d'un élément $x \in G$ et on notera $\bar{x}$ sa classe pour la relation de conjugaison.

Solution

i) (Réflexivité)

$$\forall x \in G, x = e^{-1} * x * e \Rightarrow x \sim x$$

si bien que $\sim$ est réflexive.

ii) (Symétrie)

$\forall (x, y) \in G \times G, x \sim y \Rightarrow \exists g \in G, y = g^{-1} * x * g \Rightarrow yx = g * y * g^{-1} = (g^{-1})^{-1} * y * g^{-1} \Rightarrow y \sim x$,
c'est-à-dire que $\sim$ est symétrique.

iii) (Transitivité)

$$\begin{array}{llll} \forall (x, y, z) \in G \times G \times G, & x \sim y & \text{et} & y \sim z \\ \Rightarrow & & \exists (g, h) \in G \times G, & \\ & y = g^{-1} * x * g & \text{et} & z = h^{-1} * y * h \\ \Rightarrow & z = h^{-1} * g^{-1} * x * g * h & = & (g * h)^{-1} * x * (g * h) \\ \Rightarrow & & x & \sim & z. \end{array}$$

c'est-à-dire que $\sim$ est transitive.

2) On appelle *centre du groupe* G qu'on note $\mathcal{Z}(G)$ le sous-ensemble

$$\mathcal{Z}(G) := \{g \in G; \forall h \in G, g * h = h * g\} \subset G.$$

a) Montrer que $\mathcal{Z}(G)$ est un *sous-groupe distingué* de G .

Solution

i) ($\mathcal{Z}(G)$ est non vide)

Tout d'abord

$$e \in \mathcal{Z}(G) \Rightarrow \mathcal{Z}(G) \neq \emptyset.$$

ii) (Inverse)

Par ailleurs,

$$\forall z \in \mathcal{Z}(G), \forall x \in G, z^{-1} * z = (x^{-1} * z)^{-1} = (z * x^{-1})^{-1} = x * z^{-1} \Rightarrow z^{-1} \in \mathcal{Z}(G).$$

iii) (Produit)

Enfin

$$\forall (z, w) \in \mathcal{Z}(G) \times \mathcal{Z}(G), \forall x \in G, z * w * x = z * x * w = x * z * w \Rightarrow z * w \in \mathcal{Z}(G).$$

Ce qui précède entraîne que $\mathcal{Z}(G)$ est un sous-groupe de G .

iv) (Distingué)

$\forall z \in \mathcal{Z}(G), \forall x \in G, x^{-1} * z * x = z \in \mathcal{Z}(G)$ ce qui entraîne que $\mathcal{Z}(G)$ est distingué.

b) À quelle condition nécessaire et suffisante sur $\mathcal{Z}(G)$ G est-il abélien ?

Solution

Il est clair que G est abélien si et seulement si $\mathcal{Z}(G) = G$.

c) Caractériser les éléments de $\mathcal{Z}(G)$ à l'aide de leur classe de conjugaison.

Solution

$$\forall z \in \mathcal{Z}(G), \forall y \in G, z \sim y \Rightarrow \exists g \in G, y = g^{-1} * z * g = z * g^{-1} * g = z.$$

C'est-à-dire que si $z \in \mathcal{Z}(G)$ sa classe de conjugaison est un singleton.

Réciproquement si la classe de conjugaison de $z \in G$ est un singleton c'est $\{z\}$. Or pour tout $g \in G$, $g^{-1} * z * g$ est conjugué à z par définition. Il s'ensuit que

$$\forall g \in G, g^{-1} * z * g = z \Rightarrow z * g = g * z \Rightarrow z \in \mathcal{Z}(G).$$

L'ensemble $\mathcal{Z}(G)$ est donc formé des éléments de G dont la classe de conjugaison est un singleton.

d) Montrer que si $G/\mathcal{Z}(G)$ est monogène alors G est abélien.

Indication : On pourra penser à écrire (en le justifiant bien entendu !) un élément $x \in G$ sous la forme

$$x = z * g^n, z \in \mathcal{Z}(G), \bar{g} \text{ générateur de } G/\mathcal{Z}(G), n \in \mathbb{N}.$$

Solution

Pour tout $x \in G$, notons $\tilde{x}$ sa classe dans $G/\mathcal{Z}(G)$. Puisque $G/\mathcal{Z}(G)$ est monogène il existe $\gamma := \tilde{g} \in G/\mathcal{Z}(G)$ tel que pour tout $\alpha \in G/\mathcal{Z}(G)$ il existe $k \in \mathbb{Z}$ tel que $\alpha = \gamma^k$. Ainsi

$$\begin{aligned} \forall x \in G, \exists k \in \mathbb{Z}, \quad \tilde{x} &= \gamma^k \\ &= \tilde{g}^k \\ \Rightarrow \quad \exists z \in \mathcal{Z}(G), & \\ \Rightarrow \quad g^*(g^k)^{-1} &= z \\ \Rightarrow \quad x &= z * g^k. \end{aligned}$$

Il s'ensuit que

$$\begin{aligned} \forall (x, y) \in G \times G, \\ \exists (z, w) \in \mathcal{Z}(G) \times \mathcal{Z}(G), \\ \exists (k, \ell) \in \mathbb{Z} \times \mathbb{Z}, \quad x = z * g^k, \quad y = w * g^\ell \\ \Rightarrow \quad x * y &= z * g^k * w * g^\ell \\ &= z * w * g^{k+\ell} \\ &= w * z * g^{\ell+k} \\ &= w * z * g^\ell * g^k \\ &= w * g^\ell * z * g^k \\ &= y * x, \end{aligned}$$

c'est-à-dire que G est abélien.

3) Pour tout $x \in G$, on appelle *stabilisateur de x* et on note $\text{Stab}_G(x)$ l'ensemble

$$\text{Stab}_G(x) := \{g \in G; x = g^{-1} * x * g\} \subset G.$$

a) Montrer que, pour tout $x \in G$, $\text{Stab}_G(x)$ est un sous-groupe de G .

Solution

Il est clair que

$$e \in \text{Stab}_G(x) \Rightarrow \text{Stab}_G(x) \neq \emptyset.$$

Par ailleurs les vérifications que

$$\forall (y, z) \in \text{Stab}_G(x) \times \text{Stab}_G(x), y^{-1} \in \text{Stab}_G(x) \text{ et } y * z \in \text{Stab}_G(x)$$

sont exactement les mêmes que celles faites à le point a de la question 2.

b) Quelle sous-groupe remarquable de G est contenu dans $\text{Stab}_G(x)$ pour tout $x \in G$, Que vaut

$$\bigcap_{x \in G} \text{Stab}_G(x) ?$$

Solution

il est clair que

$$\forall x \in G, \mathcal{Z}(G) \subset \text{Stab}_G(x);$$

Il est presque aussi immédiat de vérifier que

$$\bigcap_{x \in G} \text{Stab}_G(x) = \mathcal{Z}(G).$$

Pour tout $x \in G$, tout $(y, z) \in G \times G$, on note $z \sim_x y$ si $y * z^{-1} \in \text{Stab}_G(x)$.

c) Rappeler pourquoi $\sim_x$ est une relation d'équivalence.

Solution

(cf. cours proposition II.8.10.2, point i.)

d) Montrer que, pour tout $x \in G$, on a une bijection

$$G / \sim_x \cong \bar{x}.$$

Solution

Considérons l'application

$$\phi : G \rightarrow \bar{x}, g \mapsto g^{-1} * x * g.$$

Par construction même, ϕ est surjective. Par ailleurs,

$$\begin{aligned} \forall (y, z) \in G \times G, & \quad \phi(y) = \phi(z) \\ \Leftrightarrow & \quad y^{-1} * x * y = z^{-1} * x * z \\ \Leftrightarrow & \quad z * y^{-1} * x * y * z^{-1} = x \\ \Leftrightarrow & \quad y * z^{-1} \in \text{Stab}_G(x) \\ \Leftrightarrow & \quad y \sim_x z. \end{aligned}$$

On en déduit qu'il existe une unique application

$$\bar{\phi} : G / \sim_x \rightarrow \bar{x}$$

injective définie par

$$\bar{\phi}(\eta) = \phi(y) \quad \forall \eta \in G / \sim_x, \forall y \in \eta.$$

ceci entraîne encore que $\bar{\phi}$ est surjective donc bijective.

e) En déduire que si G est fini

$$\forall x \in G, \#(G) = \#(\bar{x}) \cdot \#(\text{Stab}_G(x)).$$

Solution

(cf. II.8.7.4.)

4) Soit p un nombre premier et $r \in \mathbb{N}^*$. on suppose désormais que $\#(G) = p^r$.

a) Montrer que si $r = 1$, i.e. $\#(G) = p$ G est cyclique et par conséquent abélien.

Solution

Puisque p est premier $p \geq 2$ si bien que $G \neq \{e\}$ c'est-à-dire qu'il existe $x \in G, x \neq e$. Soit $H := \{x^k, k \in \mathbb{Z}\}$. H est un sous-groupe de G dont le cardinal divise donc celui de G . On a donc $\#(H) = 1$ ou $\#(H) = p$. Or

$$x \in H, e \in H, x \neq e \Rightarrow \#(H) \geq 2 \Rightarrow \#(H) = p \Rightarrow H = G;$$

si bien que G est monogène et fini donc cyclique.

On suppose maintenant que $r \in \mathbb{N}^*$ est quelconque.

b) Quelles valeurs peut prendre $\#(\bar{x})$ pour $x \in G$?

Solution

On a vu à le point e de la question 3 que $\#(\overline{x})|\#(G)$ il s'ensuit que

$$\forall x \in G, \exists k \in \mathbb{N}, 0 \leq k \leq r, \#(\overline{x}) = p^k.$$

Notons $\mathcal{C}$ l'ensemble des classes de conjugaison de G ,

$$\mathcal{C}_0 := \{c \in \mathcal{C}; \#(c) = 1\} \text{ et } \mathcal{C}_\infty := \mathcal{C} \setminus \mathcal{C}_0.$$

c) Montrer que

$$\#(\mathcal{Z}(G)) = \#(G) - \sum_{c \in \mathcal{C}_\infty} \#(c)$$

et en déduire que $p|\#(\mathcal{Z}(G))$.

Solution

on a :

$$\begin{aligned} G &= \bigcup_{c \in \mathcal{C}} c \\ &= \left(\bigcup_{c \in \mathcal{C}_0} c \right) \cup \left(\bigcup_{c \in \mathcal{C}_\infty} c \right) \\ &= \left(\bigcup_{x \in \mathcal{Z}(G)} \{x\} \right) \cup \left(\bigcup_{c \in \mathcal{C}_\infty} c \right) \\ &= \mathcal{Z}(G) \cup \left(\bigcup_{c \in \mathcal{C}_\infty} c \right). \end{aligned}$$

Cette union étant disjointe il en découle que

$$\begin{aligned} \#(G) &= \#(\mathcal{Z}(G)) + \sum_{c \in \mathcal{C}_\infty} \#(c) \\ \Leftrightarrow \#(\mathcal{Z}(G)) &= \#(G) - \sum_{c \in \mathcal{C}_\infty} \#(c) \\ \Rightarrow p &| \#(\mathcal{Z}(G)). \end{aligned}$$

En effet, d'après le point b ,

$$\forall c \in \mathcal{C}_\infty, p|\#(c).$$

d) En déduire qu'il existe $k \in \mathbb{N} 1 \leq k \leq r$ tel que $\#(\mathcal{Z}(G)) = p^k$.

Solution

Puisque $\mathcal{Z}(G)$ est un sous-groupe de G (cf. le point a de la question 2 .) $\#(\mathcal{Z}(G))|\#(G)$. Il s'ensuit qu'il existe $0 \leq k \leq r$ tel que $\#(\mathcal{Z}(G)) = p^k$.

Mais d'après le point c , $p|\#(\mathcal{Z}(G))$ ce qui entraîne $k \geq 1$.

e) Déduire de ce qui précède que, si $\#(G) = p^2$, G est abélien.

Solution

Il découle du point précédent que

$$\#(\mathcal{Z}(G)) = p \text{ ou } \#(\mathcal{Z}(G)) = p^2 \Rightarrow \#(G/\mathcal{Z}(G)) = p \text{ ou } \#(G/\mathcal{Z}(G)) = 1.$$

Dans le premier cas $G/\mathcal{Z}(G)$ est monogène en vertu du point a et dans le deuxième cas il est évidemment monogène aussi.

Il découle alors du point d de la question 2 que G est abélien.

II.9.3 . – Morphismes**Exercice II.9.3.1 (Morphismes) 1) (Identité)**

Faire la démonstration du point i du lemme II.1.3.

2) (Composé)

Faire la démonstration du point ii du lemme II.1.3.

Exercice II.9.3.2 (Inverse) Faire la démonstration du lemme II.3.3.

Solution

i) (II.3.3.i)

C'est exactement le point ii de la proposition II.7.14.

ii) (II.3.3.ii)

C'est une conséquence immédiate du point i qui assure l'unicité et qui assure l'existence.

Exercice II.9.3.3 (Isomorphismes) Compléter la démonstration de la proposition II.3.5.

Solution

On doit donc montrer que entraîne .

$$\begin{array}{ccc}
 \mathcal{E}(G) & \xrightarrow{\mathcal{E}(\phi)} & \mathcal{E}(H) \\
 \text{Si } \varepsilon(G) \downarrow & & \varepsilon(H) \downarrow \\
 \mathcal{V}(G) \times \mathcal{V}(G) & \xrightarrow{\mathcal{V}(\phi) \times \mathcal{V}(\phi)} & \mathcal{V}(H) \times \mathcal{V}(H) \\
 \mathcal{E}(H) & \xrightarrow{\mathcal{E}(\psi)} & \mathcal{E}(G) \\
 \varepsilon(H) \downarrow & & \varepsilon(G) \downarrow \\
 \mathcal{V}(H) \times \mathcal{V}(H) & \xrightarrow{\mathcal{V}(\psi) \times \mathcal{V}(\psi)} & \mathcal{V}(G) \times \mathcal{V}(G)
 \end{array}$$

est un isomorphisme de graphes au sens , il existe un morphisme de graphes tel que $\psi \circ \phi = \text{Id}_G$ et $\phi \circ \psi = \text{Id}_H$. Ceci entraîne, en particulier que :

$$\begin{aligned}
 \text{Id}_{\mathcal{V}(G)} &= \mathcal{V}(\psi \circ \phi) = \mathcal{V}(\psi) \circ \mathcal{V}(\phi) , \\
 \text{Id}_{\mathcal{V}(H)} &= \mathcal{V}(\phi \circ \psi) = \mathcal{V}(\phi) \circ \mathcal{V}(\psi) , \\
 \text{Id}_{\mathcal{E}(G)} &= \mathcal{E}(\psi \circ \phi) = \mathcal{E}(\psi) \circ \mathcal{E}(\phi) , \\
 \text{Id}_{\mathcal{E}(H)} &= \mathcal{E}(\phi \circ \psi) = \mathcal{E}(\phi) \circ \mathcal{E}(\psi) .
 \end{aligned}$$

Ceci entraîne que $\mathcal{V}(\phi)$ et $\mathcal{E}(\phi)$ sont bijectives .

Exercice II.9.3.4 (Groupe des automorphismes) Soit G un graphe (resp. un graphe à involution ,) (resp. un graphe non-orienté .)

1) Montrer que $\text{Aut}_{\text{Gph}}(G)$ (resp. $\text{Aut}_{\text{GphInv}}(G)$,) (resp. $\text{Aut}_{\text{GphN-o}}(G)$,) est un groupe pour la loi de composition $\circ$.

Solution

Loi interne On sait (cf. le point ii du lemme II.1.3 (resp. ,) (resp. ,)) que le composé de deux morphismes est un morphisme (pour la structure correspondante.) Ainsi la loi de composition $\circ$ est-elle interne sur $\text{End}_{\text{Gph}}(G)$, (resp. $\text{End}_{\text{GphInv}}(G)$,) (resp. $\text{End}_{\text{GphN-o}}(G)$,)

Associative La loi $\circ$ de composition des applications est associative.

Élément neutre L'identité Id_G est un élément neutre (cf. le point iii du lemme II.1.3 (resp. ,) (resp. ,))

Inverse Enfin un automorphisme est en particulier un isomorphisme et possède donc un inverse (cf. (resp. ,) (resp. ,)) lequel est encore un automorphisme .

2) Montrer que l'application $\text{Aut}_{\text{Gph}}(G)$ (resp. $\text{Aut}_{\text{GphInv}}(G)$,) $(\text{Aut}_{\text{GphN-o}}(G),)$ $\phi \mapsto \mathcal{V}(\phi)$ = $\mathcal{S}(\mathcal{V}(G))$

est un morphisme de groupes .

Solution

On rappelle que l'ensemble $\mathcal{S}(\mathcal{V}(G))$ des bijections de $\mathcal{V}(G)$ sur lui-même est un groupe pour la loi de composition $\circ$ d'élément neutre $\text{Id}_{\mathcal{V}(G)}$.

Pour tout $(\phi, \psi) \in \text{Aut}_{\text{Gph}}(G) \times \text{Aut}_{\text{Gph}}(G)$ (resp. $\text{Aut}_{\text{GphInv}}(G) \times \text{Aut}_{\text{GphInv}}(G)$,) $\mathcal{V}(\psi \circ \phi) = \mathcal{V}(\psi) \circ \mathcal{V}(\phi)$; ce qui assure le résultat. (resp. $\text{Aut}_{\text{GphN-o}}(G) \times \text{Aut}_{\text{GphN-o}}(G)$,)

3) Étant donné un *graphe* (resp. un *graphe à involution* ,) (resp. un *graphe non-orienté* ,) H et $\phi : G \cong H$ un *isomorphisme de graphes* (resp. un *isomorphisme de graphes à involution* ,) (resp. un *isomorphisme de graphes non-orientés* ,) construire un *isomorphisme de groupes*

$$\begin{aligned} & \text{Aut}_{\mathbf{Gph}}(G) \cong \text{Aut}_{\mathbf{Gph}}(H), \\ \text{(resp. } & \text{Aut}_{\mathbf{Gph}^{\text{Inv}}}(G) \cong \text{Aut}_{\mathbf{Gph}^{\text{Inv}}}(H), \text{)} \\ \text{(resp. } & \text{Aut}_{\mathbf{Gph}^{\text{N-o}}}(G) \cong \text{Aut}_{\mathbf{Gph}^{\text{N-o}}}(H) \text{).} \end{aligned}$$

Solution

Pour tout $\alpha \in \text{Aut}(G)$ le composé $\phi \circ \alpha \circ \phi^{-1}$ est (cf. le point ii du lemme II.1.3, (resp. ,)= (resp. ,)) est un *morphisme* , donc un *endomorphisme* de H ; c'est aussi un *isomorphisme* donc un *automorphisme* . On définit ainsi une *application*

$$\begin{aligned} a_\phi : \text{Aut}(G) & \longrightarrow \text{Aut}(H) \\ \alpha & \longmapsto \phi \circ \alpha \circ \phi^{-1}. \end{aligned}$$

Or :

$$\begin{aligned} \forall (\alpha, \beta) \in \text{Aut}(G) \times \text{Aut}(G), \quad a_\phi(\alpha \circ \beta) & = \phi \circ \alpha \circ \beta \circ \phi^{-1} \\ & = \phi \circ \alpha \circ \phi^{-1} \circ \phi \circ \beta \circ \phi^{-1} \\ & = a_\phi(\alpha) \circ a_\phi(\beta); \end{aligned}$$

ce qui assure que a_ϕ est un *morphisme de groupes* .

On définit, de la même manière $a_{\phi^{-1}} : \text{Aut}(H) \rightarrow \text{Aut}(G)$, $\beta \mapsto \phi^{-1} \circ \beta \circ \phi$; qui est, de même un *morphisme de groupes* . On vérifie immédiatement que

$$a_{\phi^{-1}} \circ a_\phi = \text{Id}_{\text{Aut}(G)} \text{ et } a_\phi \circ a_{\phi^{-1}} = \text{Id}_{\text{Aut}(H)} ;$$

ce qui prouve que a_ϕ et $a_{\phi^{-1}}$ sont des *isomorphismes inverses l'un de l'autre*.

II.9.4 . –Sous-graphes

Exercice II.9.4.1 (Sous-graphes) Faire la démonstration de la proposition II.2.1.

Solution

Reste donc à montrer que le point b de la proposition II.2.1 entraîne le point a.

Si la restriction de l'identité à

$(\mathcal{V}(H), \mathcal{E}(H))$ est un *morphisme de graphes* , elle vérifie en particulier

l'axiome MorGph_3 de la définition II.1.1 ou sa formulation équivalente . Ainsi pour tout $e \in \mathcal{E}(H)$, si $\varepsilon(H)(e) = (u, v) \in \mathcal{V}(H) \times \mathcal{V}(H)$, $\varepsilon(G)(\text{Id}_{\mathcal{E}(G)}|_{\mathcal{E}(H)}(e)) = (\text{Id}_{\mathcal{V}(G)}|_{\mathcal{V}(H)} \times \text{Id}_{\mathcal{V}(G)}|_{\mathcal{V}(H)})(u, v) = (u, v)$; c'est-à-dire $\varepsilon(H)(e) = \varepsilon(G)(e)$; ce qui correspond bien au point a de la proposition II.2.1.

Exercice II.9.4.2 (Sous-graphe) Faire la démonstration de la proposition II.2.3.

Solution

II.2.3.a $\Rightarrow$ II.2.3.b Il suffit d'utiliser la caractérisation II.2.1.a.

II.2.3.b $\Rightarrow$ II.2.3.a Dans ce cas, $(W, F, \varepsilon(G)|_F)$ est bien un *graphe* ; et toujours d'après le point a de la proposition II.2.1 c'est bien un *sous-graphe* de G .

L'unicité de H résulte de ce que si un tel *sous-graphe* existe, nécessairement, toujours d'après le point a de la proposition II.2.1, $\varepsilon(H) = \varepsilon(G)|_F$; et le *sous-graphe* H est donc $(W, F, \varepsilon(G)|_F)$.

II.9.5 . –

Graphes finis simples non-orientés

Exercice II.9.5.1 (Chemins et cycles dans un graphe) Soit $G := (\mathcal{V}(G), \mathcal{E}(G), \varepsilon(G))$ un *graphe fini* (non vide.) On note $\delta(G) := \min_{u \in \mathcal{V}(G)} (d_G(u))$.

1) Montrer que G contient un *chemin* de longueur $\delta(G)$ i.e. un *sous-graphe isomorphe* à $\mathbf{P}_{\delta(G)}$.

Solution

On va en fait montrer un résultat plus fort ; à savoir que pour tout sommet $u \in \mathcal{V}(G)$, il existe un chemin dont u est un sommet ; en d'autres termes un chemin contenant u ou « passant par u . »

Soit $u \in \mathcal{V}(G)$ et $\mathbf{P}$ l'ensemble des chemins P tels que $u \in \mathcal{V}(P)$. L'ensemble $\mathbf{P}$ est non vide puisque il contient au moins le chemin de longueur 0 constitué du seul sommet u (isomorphe au graphe isolé $\mathbf{I}_1$.) La longueur des éléments de $\mathbf{P}$ est majorée par $\#(\mathcal{V}(G))$. Il existe donc $P_{\max} \in \mathbf{P}$ de longueur maximale .

Notons $\mathcal{V}(P_{\max}) := \{u_0, \dots, u_n\}$ et $\mathcal{E}(P_{\max}) := \{u_i, u_{i+1}\}_{0 \leq i \leq n-1}$.

Si u_n a un voisin $v \notin \mathcal{V}(P_{\max})$, en posant $u_{n+1} := v$ et $\mathcal{V}(Q) := \{u_0, \dots, u_{n+1}\}$, $Q \in \mathbf{P}$ est un chemin de longueur $n + 1$; ce qui contredit le fait que $P_{\max}$ est de longueur maximale dans $\mathbf{P}$.

Les voisins de u_n appartiennent donc tous à $\mathcal{V}(P_{\max})$; ce qui entraîne que $\#(\mathcal{V}(P_{\max})) \geq \delta(G) + 1$; ce qui entraîne finalement que la longueur de $P_{\max}$ est supérieure ou égale à $\delta(G)$.

2) Si $\delta(G) \geq 2$, montrer que G contient un cycle de longueur $> \delta(G)$ i.e. un sous-graphe isomorphe à $\mathbf{C}_\ell$, $\ell > \delta(G)$.

Solution

Soit $P_{\max}$ un chemin de longueur maximale construit comme à la question 1 ; et notons $\mathcal{V}(P_{\max}) := \{u_0, \dots, u_n\}$. Tous les voisins de u_0 appartiennent à $\mathcal{V}(P_{\max})$; sans quoi, comme nous l'avons observé à la question 1, $P_{\max}$ ne serait pas de longueur maximale . Puisque $\delta(G) \geq 2$, $I := \{i \in [1; n] ; u_i \in N_G(u_0)\} \neq \emptyset$. Posons donc $j := \max(I)$. Comme $j \geq \delta(G)$, le C le cycle tel que $\mathcal{V}(C) := \{u_0, \dots, u_j\}$ a au moins $\delta(G) + 1$ sommets et est donc de longueur strictement supérieure à $\delta(G)$.

Exercice II.9.5.2 (Exemples de groupes d'automorphismes) Soit $n \in \mathbb{N}$.

1) Déterminer le groupe $\text{Aut}_{\text{Gph}^{\text{N-0}}}(\mathbf{I}_n)$ du graphe isolé à n sommets s.

Solution

On a montré, que l'application $\sigma : \text{Aut}(\mathbf{I}_n) \rightarrow \mathcal{S}([1; n])$, $\phi \mapsto \mathcal{V}(\phi)$ est un morphisme de groupes . Or $\mathcal{E}(\mathbf{I}_n) = \emptyset$, si bien qu'un automorphisme $\phi \in \text{Aut}(\mathbf{I}_n)$ est nécessairement de la forme $(\mathcal{V}(\phi), \emptyset \rightarrow \emptyset)$; ce qui prouve que σ est une application bijective et donc un isomorphisme .

Le groupe des bijections de l'ensemble $[1; n]$ est usuellement appelé groupe symétrique et noté $\mathcal{S}_n$; si bien que σ donne un isomorphisme de groupes

$$\text{Aut}(\mathbf{I}_n) \cong \mathcal{S}_n .$$

2) Déterminer le groupe $\text{Aut}_{\text{Gph}^{\text{N-0}}}(\mathbf{K}_n)$ du graphe complet à n sommets .

Solution

On dispose du même morphisme de groupes qu'à la question 1, (toujours donné par σ), $\sigma : \text{Aut}(\mathbf{K}_n) \rightarrow \mathcal{S}_n$, $\phi \mapsto \mathcal{V}(\phi)$.

Pour tout $s \in \mathcal{S}_n$ il existe

$\phi \in \text{Aut}(\mathbf{K}_n)$ tel que $\sigma(\phi) = s$, si et seulement si il existe une bijection $t : \mathcal{E}(\mathbf{K}_n) \rightarrow \mathcal{E}(\mathbf{K}_n)$ tel que (s, t) soit un morphisme de graphes .

Unicité de t Pour $s \in \mathcal{S}_n$ s'il existe $t \in \mathcal{S}(\mathcal{E}(\mathbf{K}_n))$ tel que $(s, t) \in \text{Aut}(\mathbf{K}_n)$, nécessairement

pour tout $e \in \mathcal{E}(\mathbf{K}_n)$ tel que $\varepsilon(\mathbf{K}_n)(e) = \{u, v\} \in \mathcal{P}_2(\mathbf{K}_n)$, $\varepsilon(\mathbf{K}_n)(t(e)) = \{s(u), s(v)\}$. Or, puisque $s \in \mathcal{S}_n$, $s(u) \neq s(v)$; et par conséquent $\varepsilon(\mathbf{K}_n)^{-1}(\{\{u, v\}\})$ est un singleton ; si bien que $t(e)$ est uniquement déterminé.

Existence de t Reste à vérifier que la construction ci-dessus définit bien un morphisme de graphes non-orientés ; ce qui est, pour ainsi dire, immédiat.

On vient donc de montrer, comme à la question 1, que σ est une application bijective et donc un isomorphisme de groupes . On a donc

$$\text{Aut}(\mathbf{K}_n) \cong \mathcal{S}_n .$$

Exercice II.9.5.3 (Automorphismes) 1) Déterminer le groupe des automorphismes du graphe fini simple non-orienté $\mathbf{P}_n$ pour $n \geq 2$.

Solution

- Si on note $\mathbf{P}_2 = (\{a, b\}, \{\{a, b\}\})$, les seules bijections de $\{a, b\}$ sont l'identité et la transposition (ab) qui sont des automorphismes de $\mathbf{P}_2$. Le groupe des automorphismes de $\mathbf{P}_2$ est donc $S_2 \cong \mathbb{Z}/2\mathbb{Z}$.
- Si on note $\mathbf{P}_3 = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\})$, un automorphisme envoyant un sommet sur un sommet de même degré, si σ est un tel automorphisme, $\sigma(a) = a$ ou $\sigma(a) = c$ et nécessairement $\sigma(b) = b$. Il en résulte que les deux seuls automorphismes de $\mathbf{P}_3$ sont l'identité et la transposition (ac) . Le groupe des automorphismes est ici encore $\mathbb{Z}/2\mathbb{Z}$.
- Notons $\mathbf{P}_n := (x_1, \dots, x_n)$. Les mêmes considérations sur les degrés entraînent que pour tout automorphisme σ de $\mathbf{P}_n$ $\sigma(x_1) = x_1$ ou $\sigma(x_1) = x_n$. Alors $\{\sigma(x_1), \sigma(x_2)\}$ est une arête de $\mathbf{P}_n$, ce qui entraîne (puisque le seul voisin de x_1 , (resp. x_n) est x_2 (resp. x_{n-1})) que $\sigma(x_2) = x_2$ (resp. $\sigma(x_2) = x_{n-1}$). Par récurrence, il en résulte que pour tout $1 \leq i \leq n$, $\sigma(x_i) = x_i$ (resp. $\sigma(x_i) = x_{n+1-i}$). Les deux seuls automorphismes de $\mathbf{P}_n$ sont donc l'identité et la symétrie $x_i \mapsto x_{n+1-i}$; si bien que le groupe des automorphismes de $\mathbf{P}_n$ est encore isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

2) (Automorphismes de $\mathbf{C}_4$)

On note $\Gamma := \text{Aut}_{\text{Graph}}(\mathbf{C}_4)$ le groupe des automorphismes du cycle $\mathbf{C}_4$.

a) Montrer que l'application $\mathcal{V}$ qui à tout $\alpha = (\mathcal{V}(\alpha), \mathcal{E}(\alpha)) \in \Gamma$ associe $\mathcal{V}(\alpha)$ est un morphisme de groupes (cf. la définition II.8.2.1.) de Γ dans le groupe symétrique $\mathcal{S}_4$.

Solution

L'ensemble des sommets $\mathcal{V}(\mathbf{C}_4)$ de $\mathbf{C}_4$ est (cf. I.4.12.) est $\mathbb{Z}/4\mathbb{Z}$; si bien que pour tout $\alpha \in \Gamma$, $\mathcal{V}(\alpha)$ est bien une bijection de $\mathbb{Z}/4\mathbb{Z}$; $\mathcal{S}(\mathbb{Z}/4\mathbb{Z})$ étant lui-même isomorphe à $\mathcal{S}_4$.

Comme $\forall (\alpha, \beta) \in \Gamma \times \Gamma$, $\mathcal{V}(\alpha \circ \beta) = \mathcal{V}(\alpha) \circ \mathcal{V}(\beta)$, l'application est bien un morphisme de groupes.

b) Le morphisme $\mathcal{V}$ est-il surjectif ?

Solution

Soit

$$\begin{aligned} \tau : \mathbb{Z}/4\mathbb{Z} &\longrightarrow \mathbb{Z}/4\mathbb{Z} \\ 0 &\mapsto 0 \\ 1 &\mapsto 2 \\ 2 &\mapsto 1 \\ 3 &\mapsto 3. \end{aligned}$$

S'il existe $\alpha \in \Gamma$ tel que $\mathcal{V}(\alpha) = \tau$, il existe $\mathcal{E}(\alpha) : \mathcal{E}(\mathbf{C}_4) \rightarrow \mathcal{E}(\mathbf{C}_4)$ tel que

$$\forall e \in \mathcal{E}(\mathbf{C}_4), \mathcal{P}_{1,2}(\tau)(\varepsilon(\mathbf{C}_4)(e)) = \varepsilon(\mathbf{C}_4)(\mathcal{E}(\alpha)(e)).$$

En particulier $\mathcal{E}(\alpha)(\{0, 1\}) \in \varepsilon(\mathbf{C}_4)^{-1}(\{\{\tau(0), \tau(1)\}\}) = \varepsilon(\mathbf{C}_4)^{-1}(\{\{0, 2\}\}) = \emptyset$; ce qui contredit l'existence de $\mathcal{E}(\alpha)$ si bien que $\mathcal{V}$ n'est pas surjective.

c) Est-il injectif ?

Solution

Puisque $\mathcal{V}$ est un morphisme de groupes, il suffit de considérer son noyau (cf. le point i de la définition II.8.3.9.)

Soit $\alpha \in \text{Ker } \mathcal{V}$. Pour tout $e \in \mathcal{E}(\mathbf{C}_4)$, il existe $(v, w) \in \mathcal{V}(\mathbf{C}_4) \times \mathcal{V}(\mathbf{C}_4)$ tel que $\varepsilon(e) = \{v, w\}$. Il s'ensuit que $\varepsilon(\alpha(e)) = \{\alpha(v), \alpha(w)\}$. Or $\mathcal{V}(\alpha) = \text{Id}_{\mathcal{V}(\mathbf{C}_4)}$, par hypothèse; si bien que

$$\varepsilon(\alpha(e)) = \{v, w\} = \varepsilon(e).$$

Il s'ensuit donc que $\varepsilon(\alpha(e)) \in \varepsilon^{-1}(\{\{v, w\}\})$. Or, puisque $\mathbf{C}_4$ est un graphe simple (cf. la définition I.4.1.) $\#\varepsilon^{-1}(\{\{v, w\}\}) \leq 1$. Comme $e \in \varepsilon^{-1}(\{\{v, w\}\})$,

$$\varepsilon^{-1}(\{\{v, w\}\}) = \{e\}.$$

Il en résulte que $\alpha(e) = e$; c'est-à-dire que $\mathcal{E}(\alpha) = \text{Id}_{\mathcal{E}(\mathbf{C}_4)}$; si bien que $\alpha = \text{Id}_G$; d'où l'on déduit finalement que

$$\text{Ker } \mathcal{V} = \{\text{Id}_G\}.$$

Il résulte alors que $\mathcal{V}$ est injectif.

À noter que la seule propriété de $\mathbf{C}_4$ qu'on a utilisée est qu'il est simple; et le résultat vaudrait donc pour n'importe quel graphe simple non-orienté (cf. la proposition II.6.4.1.)

d) Déterminer Γ .

Solution

$$\text{Soit } \rho := \left(\begin{array}{l} \mathcal{V}(\rho) : \quad \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \\ \quad \quad \quad i \longmapsto i+1 \\ \mathcal{E}(\rho) : \quad \mathcal{E}(\mathbf{C}_4) \longrightarrow \mathcal{E}(\mathbf{C}_4) \\ \quad \quad \quad \{i, i+1\} \longmapsto \{i+1, i+2\} \end{array} \right) \text{ est un élément de } \Gamma.$$

Pour tout $\tau \in \Gamma$, il existe $k \in \mathbb{Z}$ (et même $k \in \mathbb{N}$ et même $k \in [0; 3]$) tel que

$$\mathcal{V}(\tau)(0) = \mathcal{V}(\rho)^k(0) = \mathcal{V}(\rho^k)(0). \quad 1$$

Reste donc à déterminer les éléments $\xi \in \Gamma$ tels que $\mathcal{V}(\xi)(0) = 0$. Un tel ξ vérifie nécessairement $0 \in \mathcal{E}(\xi)(\{0, 1\})$; ce qui entraîne

$$\mathcal{E}(\xi)(\{0, 1\}) = \{0, 1\} \text{ ou } \{0, 3\}.$$

Ceci entraîne $\mathcal{V}(\xi)(1) = 1$ ou $\mathcal{V}(\xi)(1) = 3$.

Soit $\mathcal{V}(\xi)(1) = 1$. Le même raisonnement que ci-dessus à propos des arêtes d'extrémités 1, entraîne que $\mathcal{V}(\xi)(2) = 2$ ou $\mathcal{V}(\xi)(2) = 0$. Or $\mathcal{V}(\xi)$ étant injective, nécessairement $\mathcal{V}(\xi)(2) = 2$; et pour la même raison d'injectivité, $\mathcal{V}(\xi)(3) = 3$; c'est-à-dire que $\mathcal{V}(\xi) = \text{Id}_{\mathcal{V}(\mathbf{C}_4)}$; ce qui entraîne, en utilisant le point c, par exemple, $\xi = \text{Id}_{\mathbf{C}_4}$.

Soit $\mathcal{V}(\xi)(1) = 3$. Comme on a toujours $\mathcal{V}(\xi)(3) \in \{0, 3\} \cup \{0, 1\}$, par injectivité de $\mathcal{V}(\xi)$, $\mathcal{V}(\xi)(3) = 1$. Toujours en vertu de l'injectivité de $\mathcal{V}(\xi)$, $\mathcal{V}(\xi)(2) = 2$.

arête s Soit σ défini par :

$$\begin{array}{l} \mathcal{V}(\sigma) : \quad \mathcal{V}(\mathbf{C}_4) = \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathcal{V}(\mathbf{C}_4) = \mathbb{Z}/4\mathbb{Z} \\ \quad \quad \quad 0 \longmapsto 0 \\ \quad \quad \quad 1 \longmapsto 3 \\ \quad \quad \quad 2 \longmapsto 2 \\ \quad \quad \quad 3 \longmapsto 1, \end{array} \quad 2$$

$$\begin{array}{l} \mathcal{E}(\sigma) : \quad \mathcal{E}(\mathbf{C}_4) \longrightarrow \mathcal{E}(\mathbf{C}_4) \\ \quad \quad \quad \{0, 1\} \longmapsto \{0, 3\} \\ \quad \quad \quad \{1, 2\} \longmapsto \{2, 3\} \\ \quad \quad \quad \{2, 3\} \longmapsto \{1, 2\} \\ \quad \quad \quad \{3, 0\} \longmapsto \{0, 1\}. \end{array}$$

On vérifie que $\sigma \in \Gamma$; ce qui est à peu près immédiat et que c'est le seul vérifiant 2 et, par conséquent

$$\text{le seul vérifiant } \mathcal{V}(\sigma)(0) = 0 \text{ et } \mathcal{V}(\sigma)(1) = 3.$$

Remarquons finalement que $\sigma \circ \sigma = \text{Id}_{\mathbf{C}_4}$.

Pour tout $\tau \in \Gamma$, il existe $k \in [0; 3]$ tel que $\mathcal{V}(\tau)(0) = \mathcal{V}(\rho^k)(0)$; si bien que $\mathcal{V}(\rho^{-k} \circ \tau)(0) = 0$. Il en résulte que $\rho^{-k} \circ \tau = \text{Id}_{\mathbf{C}_4}$ ou $\rho^{-k} \circ \tau = \sigma$; si bien que

$$\tau = \rho^k \circ \text{Id}_{\mathbf{C}_4} \text{ ou } \tau = \rho^k \circ \sigma;$$

et finalement

$$\gamma = \{ \rho^k \circ \sigma^\ell \}_{ \substack{ k \in [0; 3] \\ \ell \in [0; 1] } }.$$