Université Orsay-Paris-Saclay — Année 2021–2022

LDD/S6 MDD354 — Structures algébriques

Corrigé Des exercices IV.4

IV.4 . –Exercices

Exercice IV.4.1 On suppose que E est munie d'une relation d'équivalence $\sim$ et d'une loi

$$\cdot\ :\ E \times E \ \to\ E\ .$$

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

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

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

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

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

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 :

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

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 :

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

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 I.7.14 ,) 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.5.3 .)
Cependant ici, pour tout $\alpha\ \in\ E/\sim$, il existe $x\ \in\ E$ tel que $\alpha\ =\ \pi(x)$. Alors :

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

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 I.7.14 .

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

a. la surjectivité de π ! ! !

3) Donner des exemples déjà connus des constructions précédentes.

Solution

(cf. l'exercice IV.4.2 .)

Exercice IV.4.2 (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)***

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

iii) ***(Transitivité)***

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

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 $\overline{a}$ la classe de a modulo n .

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

Solution

C'est une propriété des relations d'équivalence qu'on a toujours $a \in \overline{a} = \pi_n(a)$ 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

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

Exercice IV.4.3 (Caractérisation des sous-groupes distingués) Compléter la preuve de la proposition IV.1.4 .

Solution

a $\Rightarrow$ *f* *Il s'agit d'à peine modifier l'argument déjà donné pour léquivalence entre b et f dans la preuve de la proposition IV.1.4 . 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 implique que $x * H * x^{-1} \subset H$.
Réciproquement, pour tout $y \in H$, $x^{-1} * y \in x^{-1} * H$. *D'après yyd de la proposition IV.1.4 ,* $x^{-1} * y \ \in \ H * x^{-1}$. *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 IV.4.4 (Image réciproque/directe) Faire la preuve de la proposition IV.1.10 .

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 :*

$$\begin{array}{llll} \forall x \in G,\ \forall y \in f^{-1}(L), & f(x * y * x^{-1}) & \overset{=}{f \text{ est un morphisme}} & f(x) * f(y) * f(x)^{-1} \\ & & \overset{\in}{L \text{ est distingué}} & L \\ \Rightarrow & x * y * x^{-1} & \in & f^{-1}(L)\ ; \end{array}$$

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* $H \ := \ \mathrm{GL}_2(\mathbb{R})$ *et*

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

Alors

$$\mathrm{Id}_{H|G} \ :\ G \ \to \ H$$

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

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

Exercice IV.4.5 (Sous-groupe d'un groupe fini) Faire la preuve de la proposition IV.3.3 et comparer avec la proposition II.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.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 IV.4.6 Faire la preuve du point i de la proposition IV.3.8 .

Exercice IV.4.7 (Un sous-groupe de GL_3) Soit $\mathbb{K}$ un corps commutatif. On considère l'ensemble U des matrices de $\mathrm{GL}_3(\mathbb{K})$ de la forme

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \textbf{ pour } (a, b, c) \in \mathbb{K} \times \mathbb{K} \times \mathbb{K}\ .$$

1) Montrer que U est un sous-groupe de $\mathrm{GL}_3(\mathbb{K})$.

Solution

Pour tout

$$\left(A := \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},\ B := \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \right) \in U \times U,$$

$$AB = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \in U\ .$$

Grâce à la formule ci-dessus on déduit également que B est l'inverse de A dans $\mathrm{GL}_3(\mathbb{K})$, si et seulement si :

$$\begin{array}{cc} & \left\{ \begin{array}{rcl} a+d & = & 0 \\ f+c & = & 0 \\ e+af+b & = & 0 \end{array} \right\} \\ \Leftrightarrow & \left\{ \begin{array}{lcr} d & = & -a \\ f & = & -c \\ e & = & ac-b \end{array} \right\} \\ \Leftrightarrow & B = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}\ . \end{array}$$

Ainsi $A^{-1} \in U$; ce qui combiné au fait que U est stable par la loi du groupe $\mathrm{GL}_3(\mathbb{K})$, assure que U est un sous-groupe de $\mathrm{GL}_3(\mathbb{K})$.

2) Le sous-groupe U est-il distingué dans $\mathrm{GL}_3(\mathbb{K})$?

Indication : *On pourra calculer $T * A * T^{-1}$, pour* $T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

Solution

On constate d'abord que $T^2 = \mathrm{Id}$ *i.e.* $T = T^{-1}$, *d'où :*

$$T * AT^{-1} = T * A = \begin{pmatrix} 1 & b & a \\ 0 & 1 & 0 \\ 0 & c & 1 \end{pmatrix} \notin U ;$$

si bien que U *n'est pas distingué dans* $\mathrm{GL}_3(\mathbb{K})$.

Exercice IV.4.8 (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 $\overline{x}$ 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)***

$$\forall (x, y) \in G \times G,\ x \sim y \Rightarrow \exists g \in G,\ y = g^{-1} * x * g \Rightarrow y\, x = g * y * g^{-1} = (g^{-1})^{-1} * y * g^{-1} \Rightarrow y \sim x,$$

c'est-à-dire que $\sim$ *est symétrique.*

iii) ***(Transitivité)***

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

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*

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

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

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

Il s'ensuit que

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

c'est-à-dire que G est abélien.

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

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

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

Solution

Il est clair que

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

Par ailleurs les vérifications que

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

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 $\mathrm{Stab}_G(x)$ pour tout $x \in G$, Que vaut

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

Solution

il est clair que

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

Il est presqu'aussi immédiat de vérifier que

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

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

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

Solution

(cf. cours proposition IV.1.3, point i .)

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

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

Solution

Considérons l'application

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

Par construction même, ϕ est surjective. Par ailleurs,

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

On en déduit qu'il existe une unique application

$$\overline{\phi} : G/\sim_x \to \overline{x}$$

injective définie par

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

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

e) En déduire que si G est fini

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

Solution

(cf. III.4.4 .)

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 $\#(\overline{x})$ 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 :

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

Cette union étant disjointe il en découle que

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

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.

Exercice IV.4.9 (Action d'un sous-groupe distingué) Soit H un sous-groupe distingué d'un groupe G qui agit transitivement sur un ensemble X.

Montrer que les orbites de l'action (induite de l'action de G) de H sur X ont toutes même cardinal.

Solution

Pour tout $x \in X$ notons $O(x)$ son orbite sous l'action de H.

*i) (**Première méthode**)*
On a alors

$$\#(H) = \#\big(O(x)\big) \cdot \#\big(\mathrm{Stab}_H(x)\big) \,.$$

Or

$$\begin{aligned} \mathrm{Stab}_H(x) &= \{h \in H \,;\, h \cdot x = x\} \\ &= \{g \in G \,;\, g \in H \,,\, g \cdot x = x\} \\ &= \mathrm{Stab}_G(x) \cap H \,. \end{aligned}$$

Or pour tout

$$\forall (x,y) \in X \times X,\ \exists g \in G,\ y = g \cdot x$$

puisque l'action de G est transitive. Il s'ensuit que

$$\mathrm{Stab}_G(y) = g * \mathrm{Stab}_G(x) * g^{-1} \,.$$

Il s'ensuit que :

$$\begin{aligned} \mathrm{Stab}_H(y) &= \mathrm{Stab}_G(y) \cap H \\ &= \big(g * \mathrm{Stab}_G(x) * g^{-1}\big) \cap H \\ &= \big\{g * k * g^{-1} \,,\, k \in \mathrm{Stab}_G(x)\big\} \cap H \\ &= \big\{g * k * g^{-1} \,,\, k \in \mathrm{Stab}_G(x) \,,\, g * k * g^{-1} \in H\big\} \\ &= \big\{g * k * g^{-1} \,,\, k \in \mathrm{Stab}_G(x) \,,\, k \in H\big\} \text{ puisque } h \text{ est distingué} \\ &= \big\{g * k * g^{-1} \,,\, k \in \mathrm{Stab}_G(x) \cap H\big\} \\ &= g * (\mathrm{Stab}_G(x) \cap H) * g^{-1} \\ &= g * \mathrm{Stab}_H(x) * g^{-1} \,. \end{aligned}$$

Il en résulte que

$$\forall (x,y) \in X \times X,\ \#\big(\mathrm{Stab}_H(x)\big) = \#\big(\mathrm{Stab}_H(y)\big) \,;$$

ce qui entraîne que

$$\#\big(O(x)\big) = \#\big(O(y)\big) \,.$$

*ii) (**Deuxième méthode**)*

Puisque l'action de G est transitive, pour tout $(x, y) \in X \times X$, il existe $g \in G$ tel que $y = g \cdot x$. Pour tout $z \in O(x)$ il existe $h \in H$ tel que $z = h \cdot x$. Alors

$$g \cdot z = (gh) \cdot x = (g * h * g^{-1}) \cdot y \in H .$$

On définit ainsi une application

$$O(x) \to O(y) , \; z \mapsto g \cdot z$$

dont l'application

$$O(y) \to O(x) , \; z \mapsto g^{-1} \cdot z$$

est la bijection réciproque.

On a donc définit, et ce indépendamment de toute hypothèse de finitude sur G ou X, des bijections entre chaque couple d'orbite sous l'action de H. Si donc ces dernières sont finies, elles ont même cardinal.

Solution

Soit x, y deux éléments de X. Alors par transitivité il existe $g \in G$ tel que $g \cdot x = y$.