Université Paris Diderot – Paris 7 04/11/2017
U.F.R. de Mathématiques B. Keller et F. Lemma

L3 Math/Info : Algèbre et géométrie 1, U1MC35

Un corrigé de l'examen partiel

Avertissement : Les documents, calculettes et portables sont interdits.

1) **Question de cours.**

a) Définir la notion de groupe et celle d'action d'un groupe G sur un ensemble X.

Solution : Un groupe est un couple $(G, \star)$ formé d'un ensemble G et d'une application

$$\star : G \times G \to G\,,\ (g,h) \mapsto gh$$

tels que

1. $\star$ est associative, i.e. on a $(gh)k = g(hk)$ pour tous $g, h, k \in G$,
2. $\star$ admet un élément neutre e, i.e. $ge = g = eg$ pour tous $g \in G$,
3. tout élément $g \in G$ admet un inverse $g' \in G$, i.e. $gg' = e = g'g$.

Une action d'un groupe sur un ensemble X est la donnée d'une application

$$\cdot : G \times X \to X$$

telle que

1. on a $(gh) \cdot x = g \cdot (h \cdot x)$ pour tous $g, h \in G$ et $x \in X$ et
2. on a $e \cdot x = x$ pour tout $x \in X$.

b) Soient G un groupe fini non trivial et p le plus petit diviseur premier de l'ordre de G. Montrer qu'un sous-groupe d'indice p dans G est distingué.

Solution : Soit H un sous-groupe d'indice p dans G. On fait agir G par translation à gauche sur l'ensemble G/H des classes à gauche de G, i.e. on a

$$g.(xH) = (gx)H$$

pour tous $g, x \in G$. Comme cette action est transitive, le morphisme associé $f : G \to \mathfrak{S}_p$ est non constant. L'ordre de son image $f(G)$ divise $\mathrm{pgcd}(|G|, p!) = p$. Donc $|f(G)| = p$. D'après le premier théorème d'isomorphisme, on a un isomorphisme $G/\ker(f) \xrightarrow{\sim} f(G)$. Donc l'indice de $\ker(f)$ dans G est p. Or, par définition, on a $\ker(f) \subset H$. En outre, tous deux sont d'indice p. Donc $H = \ker(f)$ est bien distingué.

2) Soient $\alpha : G \to H$ et $\beta : G \to H$ deux morphismes de groupes. Est-il vrai ou faux que la partie $L = \{g \in G \mid \alpha(g) = \beta(g)\}$ de G est un sous-groupe ? Justifier.

Solution : C'est vrai. En effet, comme α et β sont des morphismes, on a $\alpha(e) = e = \beta(e)$ de façon que $e \in L$; pour $g, h \in L$, on a $\alpha(gh) = \alpha(g)\alpha(h) = \beta(g)\beta(h)$ de façon que $gh \in L$; pour $g \in L$, on a $\alpha(g^{-1}) = \alpha(g)^{-1} = \beta(g)^{-1} = \beta(g^{-1})$ de façon que $g^{-1} \in L$. Donc L est bien un sous-groupe.

3) Soient les permutations suivantes :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 4 & 3 & 7 & 9 & 5 & 10 & 6 & 8 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 5 & 7 & 6 & 2 & 9 & 10 & 1 & 8 \end{pmatrix}.$$

a) Déterminer la décomposition en cycles à supports disjoints de $\rho = \sigma\tau\sigma^{-1}$.
Solution : La décomposition en cycles à supports disjoints de τ est

$$\tau = (1\ 4\ 7\ 9)(2\ 3\ 5\ 6)(8\ 10).$$

La décomposition en cycles à supports disjoints du conjugué $\sigma\tau\sigma^{-1}$ s'obtient en remplaçant i par $\sigma(i)$ dans les cycles à supports disjoints de τ. Nous avons donc

$$\rho = \sigma\tau\sigma^{-1} = (2\ 3\ 5\ 6)(1\ 4\ 7\ 9)(10\ 8) = \tau.$$

b) Quel est l'ordre de ρ ? Quelle est sa signature ?
Solution : L'ordre de ρ est le ppcm des longueurs des cycles dans sa décomposition en produit de cycles à support disjoint. Donc cet ordre vaut $\text{ppcm}(4, 4, 2) = 4$. La signature d'un cycle de longueur l est $(-1)^{l-1}$. Donc la signature de ρ est $(-1)^3(-1)^3(-1)^1 = -1$.

4) Soit G un groupe. Le *commutateur* de deux éléments x et y de G est défini par

$$[x, y] = xyx^{-1}y^{-1}.$$

Le *sous-groupe dérivé de* G est par définition le sous-groupe $D(G)$ engendré par tous les commutateurs.

a) Montrer que $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ pour tout automorphisme φ de G et tous $x, y \in G$.
Solution : On a

$$\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = [\varphi(x), \varphi(y)].$$

b) Montrer que $D(G)$ est distingué dans G. *L'abélianisé de* G est le groupe quotient $G_{ab} = G/D(G)$.
Solution : Soient $g \in G$ et soit c_g l'automorphisme de G donné par la conjugaison avec g, i.e. $c_g(x) = gxg^{-1}$ pour tous $x \in G$. D'après le point a), l'automorphisme c_g envoie l'ensemble des commutateurs dans l'ensemble des commutateurs. Il envoie donc le sous-groupe $D(G)$ engendré par les commutateurs dans le sous-groupe $D(G)$. Ainsi, on a $gD(G)g^{-1} \subset D(G)$ pour tout $g \in G$. D'après un lemme du cours, il s'ensuit qu'on a $gD(G)g^{-1} = D(G)$ pour tout $g \in G$. Donc D(G) est bien distingué dans G.

c) Montrer que G_{ab} est abélien.
Solution : Soient $x, y \in G$ et soit $\pi : G \to G_{ab}$ la surjection canonique. Par définition de $D(G)$, le commutateur $[x, y]$ appartient à $D(G)$ et donc au noyau de π. On a donc

$$\pi(x)\pi(y)\pi(x)^{-1}\pi(y)^{-1} = \pi([x, y]) = e.$$

En multipliant à droite par $\pi(y)\pi(x)$, on trouve

$$\pi(x)\pi(y) = \pi(y)\pi(x)$$

ce qu'il fallait montrer.

d) Montrer que pour tout morphisme de groupes $f : G \to H$ vers un groupe abélien H, il existe un unique morphisms $\overline{f} : G_{ab} \to H$ tel que $f = \overline{f} \circ \pi$, où π désigne la surjection canonique $G \to G_{ab}$.

Solution : Comme H est abélien, tout commutateur d'éléments de H est égal à e. Donc pour $x, y \in G$, on a

$$f([x, y]) = f(xyx^{-1}y^{-1}) = [f(x), f(y)] = e.$$

Les commutateurs appartiennent donc au noyau de f et, par conséquent, le sous-groupe D(G) qu'ils engendrent est contenu dans $\ker(f)$. Par la propriété universelle du groupe quotient $G_{ab} = G/D(G)$, il existe un unique morphism $\overline{f} : G_{ab} \to H$ tel que $f = \overline{f} \circ \pi$.

e) Déterminer $D(G)$ et G_{ab} lorsque G est le groupe D_3.

Solution : Par définition, le groupe D_3 est le groupe des isométries linéaires laissant stable un triangle équilatère centré en l'origine. Il est constitué de l'identité, des trois symétries par rapport aux bissectrices du triangle τ_1, τ_2, τ_3 et des rotations ρ et ρ^2, où la mesure de l'angle de ρ vaut $2\pi/3$. Le déterminant

$$\det : D_4 \to \{1, -1\}$$

est un homomorphisme vers un groupe abélien. Tous les commutateurs sont donc contenus dans son noyau, qui n'est autre que le sous-groupe de rotations $R = \{e, \rho, \rho^2\}$. On a donc $D(D_3) \subset R$. De l'autre côté, on a

$$[\tau_1, \rho] = \tau_1\rho\tau_1^{-1}\rho^{-1} = \rho^{-1}\rho^{-1} = \rho^{-2} = \rho.$$

Donc $R \subset D(D_3)$ et finalement $D(D_3) = R$. Par le premier théorème d'isomorphisme, le déterminant induit un isomorphisme

$$(D_3)_{ab} = D_3/D(D_3) \xrightarrow{\sim} \{1, -1\}.$$

f) Supposons à partir de maintenant que G est le groupe des matrices inversibles triangulaires supérieures 2×2 à coefficients réels. Soit U la partie de G formée des matrices dont les coefficents diagonaux valent 1. Montrer que U est un sous-groupe de G.

Solution : La matrice identité appartient bien à U. Soient

$$u = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \quad \text{et} \quad v = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}$$

deux éléments de U. Alors leur produit

$$uv = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix}$$

appartient clairement à U et il en est de même de l'inverse

$$u^{-1} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}.$$

Donc U est bien un sous-groupe.

g) Montrer que tout commutateur d'éléments de G appartient à U.
Solution : Soient des éléments de G

$$x = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \quad \text{et} \quad y = \begin{bmatrix} d & e \\ 0 & f \end{bmatrix}.$$

On a

$$\begin{aligned} [x,y] = xyx^{-1}y^{-1} &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \frac{1}{ac} \begin{bmatrix} c & -b \\ 0 & a \end{bmatrix} \frac{1}{df} \begin{bmatrix} f & -e \\ 0 & d \end{bmatrix} \\ &= \frac{1}{acdf} \begin{bmatrix} acdf & g \\ 0 & acdf \end{bmatrix} \end{aligned}$$

pour un nombre réel g ce qui montre bien que $[x,y] \in U$.

h) Montrer que réciproquement, tous les éléments de U sont des commutateurs d'éléments de G. *Indication : on pourra considérer le commutateur de deux éléments de la forme*

$$g = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad et \quad h = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

où a est un scalaire non nul et b un scalaire quelconque. Déduire que $D(G) = U$.
Solution : On a

$$\begin{aligned} [g,h] &= \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & b(1-a^2) \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Si on pose $a = 2$, on a $b(1-a^2) = -3b$ et on voit que $[g,h]$ parcourt bien le groupe U lorsque $a \in \mathbf{R}^*$ et $b \in \mathbf{R}$. Donc $U \subset D(G)$. Avec l'inclusion réciproque démontrée au point précédent, on obtient $U = D(G)$.

i) Montrer que G_{ab} est isomorphe au groupe produit $\mathbf{R}^* \times \mathbf{R}^*$.
Solution : Soit

$$\varphi : G \to \mathbf{R}^* \times \mathbf{R}^*, \ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mapsto (a,c).$$

Alors φ est clairement un morphisme de groupes surjectif de noyau U. Par le premier théorème d'isomorphisme, φ induit un isomorphisme $G/U \xrightarrow{\sim} \mathbf{R}^* \times \mathbf{R}^*$. Comme $U = D(G)$, on obtient un isomorphisme $G_{ab} \xrightarrow{\sim} \mathbf{R}^* \times \mathbf{R}^*$.