Corrigé de l'entraînement Groupes I

D. Harari

Agrégation

1. a) On a déjà $f(x+y) = f(x) + f(y)$ pour tous x, y de G par définition d'un morphisme de groupes, et de même $f(nx) = f(x)$ pour tout $n \in \mathbf{Z}$. Cette dernière égalité donne en passant au quotient $f(\bar{n}x) = \bar{n}f(x)$, où $\bar{n}$ est la classe de n dans $\mathbf{Z}/2\mathbf{Z}$, ce qui montre que f est bien un morphisme de $\mathbf{Z}/2\mathbf{Z}$-ev. Noter que de même, si A et B sont des groupes abéliens tels que $px = 0$ pour tout $x \in (A \cup B)$ (où p est un nombre premier), alors tout morphisme de groupes de A vers B est automatiquement un morphisme de $\mathbf{Z}/p\mathbf{Z}$-ev.

b) D'après a), le groupe S est aussi le groupe des automorphismes du $\mathbf{Z}/2\mathbf{Z}$-ev G, qui est de dimension 2. Il est donc isomorphe à $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$.

c) D'après b), le groupe S est de cardinal $(2^2-1)(2^2-2) = 6$. On voit facilement que $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$ n'est pas abélien, donc la seule possibilité est qu'il soit isomorphe à $\mathcal{S}_3$.

2. Soit $S = \{a_1, ..., a_r\}$ une partie finie de $\mathbf{Q}$. Écrivons chaque a_i sous forme $a_i = b_i/c_i$ avec $b_i \in \mathbf{Z}$ et $c_i \in \mathbf{N}^*$. Alors tout élément x du sous-groupe engendré par $(a_1, ..., a_r)$ est combinaison linéaire à coefficients entiers des a_i, d'où $x = y/z$ avec $z = c_1...c_r$ et $y \in \mathbf{Z}$. Choisissons un nombre premier p ne divisant aucun des c_i. Le rationnel $1/p$ ne peut pas s'écrire sous la forme ci-dessus (sinon on aurait $z = py$ et p diviserait $c_1...c_r$), donc il n'est pas dans le sous groupe engendré par S.

3. a) On note que H est abélien, donc $K \lhd H$ est automatique. Si $\tau = (a,b)(c,d)$ est une double transposition et $\sigma \in G$, on sait que $\sigma\tau\sigma^{-1} = (\sigma(a), \sigma(b))(\sigma(c), \sigma(d))$ est encore une double transposition (et bien sûr, tout conjugué de l'identité est l'identité), ce qui montre que $H \lhd G$. Par contre, si on choisit σ telle que $\sigma(a) = a$ et $\sigma(b) = c$, on voit que $\sigma\tau\sigma^{-1}$ n'est plus dans le sous-groupe K, celui-ci n'est donc pas distingué dans G.

b) Soit u un automorphisme de H. Comme K est caractéristique dans H, il est stable par u, d'où un morphisme obtenu par restriction de K dans K.

Comme u^{-1} laisse également stable le sous-groupe caractéristique K de H, la restriction (notée encore u) de u à K induit un automorphisme de K. Si maintenant H est caractéristique (resp. distingué) dans G, alors tout automorphisme (resp. tout automorphisme intérieur) v de G induit par restriction un automorphisme u de H (noter par contre que même si v est un automorphisme intérieur de G, u n'est pas forcément un automorphisme intérieur de H, cf. a). Comme K est caractéristique dans H, il est stable par u. Ainsi K est caractéristique (resp. distingué) dans G.

4. a) Soit x un élément d'ordre d de G. Soit H le sous-groupe de G engendré par x, il est de cardinal d et tout élément y de G satisfait l'équation $y^d = 1$ via le théorème de Lagrange. Comme K est un corps, cette équation a au plus d solutions, qui sont donc exactement les éléments de G. Parmi ceux-ci, ceux d'ordre exactement d sont au nombre de $\varphi(d)$, comme dans tout groupe cyclique de cardinal d. Finalement, on a montré que dès qu'il y a au moins un élément d'ordre d, il y a exactement $\varphi(d)$ éléments d'ordre d dans G.

b) Pour tout diviseur d du cardinal n de G, désignons par N_d le nombre d'éléments d'ordre d. On a, en triant les éléments par leur ordre :

$$\sum_{d|n} N_d = n.$$

Par ailleurs $N_d \leq \varphi(d)$ d'après a) ; d'après la formule $\sum_{d|n} \varphi(d) = n$, toutes les inégalités ci-dessus sont des égalités. En particulier $N_n = \varphi(n) > 0$, i.e. il y a au moins un élément d'ordre n, ce qui veut dire que G est cyclique.

5. a) Soit u l'application de l'ensemble des classes à gauche G/A dans l'ensemble des classes à gauche $(G/H)/B$ qui envoie aA sur $\bar{a}B$, où $\bar{a}$ est la classe de a dans le groupe quotient G/H. Cette application est bien définie car si $aA = a'A$, alors $a^{-1}a' \in A$ d'où $p(a^{-1}a') \in B$, ce qui signifie que $(\bar{a})^{-1}\bar{a'} \in B$, ou encore $\bar{a}B = \bar{a'}B$. Cette application est clairement surjective. Enfin, on a $\bar{a}B = \bar{a'}B$ si et seulement si $a^{-1}a' \in A$ (même calcul que ci-dessus), c'est-à-dire ssi $aA = a'A$, ce qui montre que u est bijective. Ceci donne le résultat par définition de l'indice (noter qu'on n'a pas besoin de supposer G fini, il suffit que B soit supposé d'indice fini dans G/H).

b) Si G est cyclique, on sait qu'il a un (unique) sous-groupe de cardinal $p^{\alpha-1}$ puisque $p^{\alpha-1}$ divise p^α, donc le résultat est vrai. Supposons G non cyclique et procédons par récurrence sur α. Le cas $\alpha = 1$ est clair. Supposons le résultat vrai jusqu'à $\alpha - 1$ et montrons-le pour α. Comme G n'est pas cyclique, il possède un élément a autre que le neutre d'ordre $< p^\alpha$, ce qui

veut dire que le sous-groupe H engendré par a est de cardinal strictement compris entre 1 et p^α. En particulier le quotient G/H est de cardinal p^β avec $1 \leq \beta < \alpha$. L'hypothèse de récurrence appliquée à G/H dit que G/H possède un sous-groupe d'indice p, et a) nous permet d'en déduire qu'il en va de même pour G.

c) On sait que le centre Z de G est distingué, non trivial, et de cardinal strictement plus petit que celui de G vu que G n'est pas abélien. En raisonnant par récurrence sur $\alpha \geq 1$, on peut donc supposer que G/Z admet un sous-groupe d'indice p, et on conclut encore avec a).

d) Cela résulte de c) par récurrence descendante sur i avec $0 \leq i \leq \alpha$.

e) Oui : cela résulte immédiatement du premier théorème de Sylow et de d).

6. a) On a déjà vu que $V_4 \lhd G$ (exercice 3. a) par exemple). Ainsi G/V_4 est un groupe. Comme il est de cardinal 3, il est abélien (cyclique même), et les propriétés du sous-groupe dérivé indiquent alors que $D(G) \subset V_4$.

b) On a $D(G) \neq \{1\}$ car G n'est pas abélien. Par ailleurs, un sous groupe de cardinal 2 de G est composé de l'identité et d'une double transposition, et on a déjà vu (exercice 3. a) qu'un tel sous-groupe n'était pas stable par conjugaison.

c) D'après a), $D(G)$ est un sous-groupe de V_4, donc il est de cardinal 1, 2, ou 4. Les deux premiers cas sont exclus par la question b) (puisque $D(G)$ est distingué dans G), donc finalement le cardinal de $D(G)$ est 4, soit $D(G) = V_4$.

d) L'ensemble S des classes à gauche selon H est composé de H et du complémentaire de H (puisque S est de cardinal 2), tout comme celui des classes à droite (pour la même raison). Ainsi, pour tout $a \in A$, on a $aH = Ha$ (cet ensemble étant H ou son complémentaire, suivant que a est dans H ou pas), soit $aHa^{-1} = H$. Ainsi, $H \lhd A$.

e) D'après d), un tel sous-groupe H serait distingué dans $\mathcal{A}_4$. De plus, le quotient G/H serait de cardinal 2, donc abélien, ce qui impliquerait $D(G) \subset H$. Or, ceci n'est pas possible d'après le théorème de Lagrange vu que $D(G)$ est de cardinal 4.