Université Rennes 1, Année 2012-2013
Master 1 Math., Algèbre générale de base

Feuille d'exercices 1 : (indications de) correction

Exercice 5.

(2) On peut se douter que la réponse est non. Arriver à un contre-exemple par le raisonnement demande de bien connaître la théorie des groupes. Pour voir l'exemple directement, allez directement à la fin de la réponse...

On applique une stratégie de base pour trouver des contre-exemples : on essaie de trouver le plus simple contre-exemple possible. Une idée qui va dans ce sens est de chercher un groupe G tel que $x^3 = 1$ pour tout $x \in G$ (ceci assure que $x \mapsto x^3$ est un morphisme de groupes) et qui ne soit pas abélien. Appliquant la « stratégie de base », on va chercher un contre-exemple parmi les groupes finis, de cardinal le plus petit possible. D'après le lemme de Cauchy, le groupe G doit être un 3-groupe, car si un nombre premier p divise l'ordre de G, alors il existe un élément x d'ordre p. Mais comme $x^3 = 1$, on trouve que $p = 3$.

Donc l'ordre de G est de la forme 3^n pour un certain n. Supposons que n est choisi minimal, c'est-à-dire qu'il existe un groupe d'ordre 3^n non abélien, mais tous les groupes d'ordre 3^{n-1} sont abéliens. Par une propriété classique des p-groupes, il existe dans G un sous-groupe distingué N d'ordre 3^{n-1}.

Posons $H = G/N$, c'est un groupe d'ordre 3 donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Comme G est d'exposant 3, n'importe quel antécédent d'un générateur de H est d'ordre 3 donc engendre un sous-groupe de G isomorphe à H. Ceci montre que la suite exacte

$$1 \to N \to G \to H \to 1$$

est scindée, ou dit autrement, que G est produit semi-direct de N par H. Ce produit semi-direct est décrit par un morphisme $H \to \mathrm{Aut}(N)$, et G est non abélien ssi ce morphisme est non trivial. Comme H n'a pas de sous-groupe non trivial, ce morphisme est non trivial ssi il est injectif.

Par ailleurs, d'après l'hypothèse faite sur G, le groupe N est d'exposant 3, et par choix de n il est abélien. Donc N est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^{n-1}$. Ainsi $\mathrm{Aut}(N) \simeq \mathrm{GL}_{n-1}(\mathbb{Z}/3\mathbb{Z})$. Il s'agit donc de trouver un sous-groupe d'ordre 3 dans $\mathrm{GL}_{n-1}(\mathbb{Z}/3\mathbb{Z})$. Le plus petit n pour lequel c'est possible est $n = 3$, et un exemple de tel sous-groupe est le sous-groupe des matrices unipotentes de la forme

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

avec a appartenant à $\mathbb{Z}/3\mathbb{Z}$.

Pour conclure, on pose $N = (\mathbb{Z}/3\mathbb{Z})^2$ et $H = \mathbb{Z}/3\mathbb{Z}$. On appelle $\theta : H \to \mathrm{Aut}(N) = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ le morphisme qui envoie a sur la matrice unipotente ci-dessus. Alors le produit semi-direct de N par H correspondant à θ est un groupe d'ordre 27, non abélien. On doit faire attention tout de même que, dans le raisonnement qui précède, rien ne montre que ce groupe est d'exposant 3. Il faut le vérifier, ce qui est un exercice facile de manipulation sur le produit semi-direct.

Une fois cette réponse trouvée, on peut regarder cet exemple droit dans les yeux et reconnaître un groupe connu qui s'est caché... On voit que la clef de l'exercice est donnée par les matrices unipotentes et qu'en fait le groupe qu'on a construit n'est autre que le groupe $U_3(\mathbb{F}_3)$ des matrices unipotentes triangulaires supérieures

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

à coefficients dans le corps à trois éléments $\mathbb{F}_3$. Notez que sur cette description, il est facile de voir que ce groupe est d'exposant 3.

Exercice 9.

(1) Ce sont les paires d'éléments x, y qui commutent entre eux. Si G est abélien, on a $D(G) = \{0\}$.

(2) L'inverse d'un commutateur $[x, y]$ est le commutateur $[y, x]$, donc le sous-groupe $D(G)$ est l'ensemble des produits finis de commutateurs. Soit $\varphi : G \to G$ un automorphisme de G. Soient x, y dans G. On a alors $\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = [\varphi(x), \varphi(y)]$. Ceci montre que φ envoie commutateurs sur commutateurs. Donc il envoie un produit fini de commutateurs sur un produit fini de commutateurs. Ainsi $\varphi(D(G)) \subset D(G)$, comme demandé.

En particulier $D(G)$ est stable sous les automorphismes intérieurs, i.e. distingué (on peut le voir directement en calculant le conjugué d'un commutateur). Notons $\pi : G \to D(G)$ le quotient et $\overline{x} = \pi(x)$. Pour montrer que $G/D(G)$ est abélien il suffit de montrer que les commutateurs dans $G/D(G)$ sont égaux à 1. Or l'expression d'un commutateur montre que $\overline{[x, y]} = [\overline{x}, \overline{y}]$. Ainsi le commutateur de $\overline{x}$ et $\overline{y}$ dans $G/D(G)$ est l'image dans $G/D(G)$ du commutateur de x et y, donc égal à 1 puisque π envoie les commutateurs sur 1.

(3) Si G/H est abélien, ses commutateurs sont égaux à 1. Alors tout commutateur $[x, y] \in G$ s'envoie par le morphisme de quotient $f : G \to G/H$ sur un commutateur, donc sur 1. Donc $[x, y] \in \ker(f) = H$. Ceci montre que $D(G) \subset H$.

(4) De même que dans (3), si M est abélien alors un commutateur dans G s'envoie par f sur un commutateur dans M i.e. sur le neutre. Ainsi $D(G) \subset \ker(f)$ et la propriété universelle du quotient implique que f se factorise de manière unique par un morphisme $G/D(G) \to M$.

(5) Si $n \leq 2$ les réponses sont faciles car $\mathfrak{S}_n$ et $\mathfrak{A}_n$ sont abéliens. On va supposer ici que $n \geq 3$. Pour la preuve du fait que les 3-cycles engendrent $\mathfrak{A}_n$, je renvoie à un cours de théorie des groupes : par exemple, votre cours de L3, ou le livre *Cours d'Algèbre* de D. Perrin (Ellipses) ou *Éléments de théorie des groupes* de J. Calais (PUF).

Comme le morphisme signature $\epsilon : \mathfrak{S}_n \to \mathbb{Z}/2\mathbb{Z}$ est à valeurs dans un groupe abélien, on voit qu'il envoie tout commutateur sur le neutre. Ceci montre que $[x, y] \in \mathfrak{A}_n$. Il s'ensuit que $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$. Montrons que réciproquement $\mathfrak{A}_n \subset D(\mathfrak{S}_n)$. Soient i, j, k trois chiffres distincts. On a $(i, j)(j, k) = (i, j, k)$ donc

$$(i, j)(j, k)(i, j)^{-1}(j, k)^{-1} = (i, j)(j, k)(i, j)(j, k) = (i, j, k)(i, j, k) = (k, j, i).$$

Ceci montre que tout 3-cycle (k, j, i) est le commutateur d'un élément de $\mathfrak{S}_n$, à savoir $[(i, j), (j, k)]$. En conséquence le sous-groupe engendré par les 3-cycles, c'est-à-dire $\mathfrak{A}_n$, est inclus dans le sous-groupe engendré par les commutateurs, c'est-à-dire $D(\mathfrak{S}_n)$.

Si $n \geq 5$, on montre que $D(\mathfrak{A}_n) \subset \mathfrak{A}_n$. La subtilité est qu'il faut exprimer un 3-cycle comme un commutateur *d'un élément de* $\mathfrak{A}_n$ alors que ci-dessus on l'a exprimé comme commutateur de transpositions, qui ne sont pas dans $\mathfrak{A}_n$. Pour cela, on utilise l'indication de l'énoncé selon laquelle les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$. En particulier, (i,j,k) et son carré, qui est encore un 3-cycle : $(i,j,k)^2 = (k,j,i)$ sont conjugués dans $\mathfrak{A}_n$. Ceci signifie qu'il existe $\sigma \in \mathfrak{A}_n$ tel que $(i,j,k)^2 = \sigma(i,j,k)\sigma^{-1}$. En multipliant à droite par $(i,j,k)^{-1}$ on trouve

$$(i,j,k) = \sigma(i,j,k)\sigma^{-1}(i,j,k)^{-1} = [\sigma,(i,j,k)].$$

C'est un commutateur de $\mathfrak{A}_n$ et on a fini.

Exercice 11.

On note avant de commencer que l'ensemble HN, qui est par définition l'ensemble des produits $hn \in G$ avec $h \in H$ et $n \in N$, est un sous-groupe *lorsque N (ou H) est distingué.* Ceci résulte du simple fait que $hnh'n' = hh'[(h')^{-1}nh'n']$ qui est bien un produit d'un élément de H par un élément de N, puisque $(h')^{-1}nh' \in N$.

(1) (i) $\Rightarrow$ (ii). Soit $\nu : H \to G/N$ la restriction de π au sous-groupe H. Le noyau de ν est $H \cap N$ dont trivial par hypothèse, donc ν est injectif. Il est aussi surjectif, car si $g \in G$ il existe $h \in H$, $n \in N$ tel que $g = hn$ et alors $\pi(g) = \pi(hn) = \pi(h)$ (puisque $N = \ker(\pi)$) $= \nu(h)$ par définition de ν. On a montré que tout élément de G/N, qui est une classe $\overline{g} = \pi(g)$, est dans l'image de ν. En résumé ν est un isomorphisme, et la composée

$$G/N \xrightarrow{\nu^{-1}} H \subset G$$

est visiblement une section de π.

(ii) $\Rightarrow$ (i). Si s est une section, on vérifie que son image H vérifie les conditions de (i).

(2) On a montré que $H \simeq G/N$ dans la preuve de (i) $\Rightarrow$ (ii). Montrons que G est en bijection avec $N \times H$. Comme la condition (i) est satisfaite, tout élément $g \in G$ s'écrit hn. Cette écriture est unique, car $h_1n_1 = h_2n_2$ entraîne $(h_2)^{-1}h_1 = n_2(n_1)^{-1}$ or le membre de gauche appartient à H, le membre de droite appartient à N, et $H \cap N = 1$. Il s'ensuit que $(h_2)^{-1}h_1 = n_2(n_1)^{-1} = 1$ puis $h_1 = h_2$ et $n_1 = n_2$. Alors l'application $G \to N \times H$ qui envoie g sur (n,h) tel que $g = hn$ est une bijection. Attention ! ce n'est pas un morphisme de groupes en général...

(3) *à suivre...*