Lycée Louis-Le-Grand, Paris
MPSI 4 – Mathématiques
A. Troesch

Problème n° 14 : Structures algébriques

Correction du problème 1 – Théorème de Burnside

Partie I – Quelques résultats préliminaires

1. Soit G un groupe, et H un sous-groupe de G. Montrons que $N_G(H)$ est un sous-groupe de G. On a :
   - $N_G(H) \subset G$ par définition ;
   - $eH = H = He$, où e désigne le neutre de G, donc $e \in N_G(H)$
   - Si $x \in N_G(H)$ et $y \in N_G(H)$, alors

   $$yHy^{-1} = H \qquad \text{donc:} \qquad H = y^{-1}(yHy^{-1})y = y^{-1}Hy \qquad \text{donc:} \qquad xy^{-1}Hyx^{-1} = xHx^{-1} = H.$$

     On en déduit que $xy^{-1} \in N_G(H)$.

   D'après la caractérisation des sous-groupes, $\boxed{N_G(H) \text{ est un sous-groupe de } G}$.

   Par ailleurs :
   - pour tout $h \in H$, par stabilité H, $hH \subset H$
   - En particulier, étant donné $h \in H$, $h^{-1} \in H$, donc $h^{-1}H \subset H$, puis $hh^{-1}H \subset hH$, donc $H \subset hH$.

   D'après le principe de double inclusion, $hH = H$. De même, $Hh = H$. Ainsi, $h \in N_G(H)$. On a donc $\boxed{H \subset N_G(H)}$.
2. Soit G un groupe.
   (a) De même, étant donné $x \in G$:
   - $C_G(x) \subset G$ par définition
   - $ex = x = xe$ donc $e \in G$
   - Si y et z sont dans $C_G(E)$,

   $$x = zxz^{-1} \text{ donc: } z^{-1}xz = x \qquad \text{puis:} \qquad (yz^{-1})x(yz^{-1})^1 = yxy^{-1} = x.$$

     Ainsi, $yz^{-1} \in C_G(E)$.

   Par conséquent, $C_G(x)$ est un sous-groupe de G.

   (b) De façon évidente, $C_G(X) = \bigcup_{x \in X} C_G(x)$, donc $\boxed{C_G(X) \text{ est un sous-groupe de } G}$, comme intersection de sous-groupes de G.

   (c) Si $x \in C_G(H)$, alors pour tout $h \in H$, $xhx^{-1} = h \in H$, donc $x \in N_G(H)$. Ainsi, $\boxed{C_G(H) \subset N_G(H)}$.

Partie II – Produit semi-direct de deux sous-groupes de G

1. Soit $f : H \times K \to HK$ définie par $f(h,k) = hk$. La fonction f est toujours surjective, par définition de HK.
   - Supposons $H \cap K = \{e\}$. Montrons que f est injective. Soit (h,k) et (h',k') deux éléments de $H \times K$ tels que $f(h,k) = f(h',k')$, donc $hk = h'k'$. On a alors ${h'}^{-1}h = k'k^{-1}$. Cet élément est donc à la fois un élément de H et de K, donc, puisque $H \cap K = \{e\}$:

   $${h'}^{-1}h = e = k'k^{-1} \qquad \text{puis:} \qquad h = h' \text{ et } k = k'.$$

     On en déduit que f est injective, puis la bijectivité de f

- Supposons que $H \cap K \neq \{e\}$, Comme $H \cap K$ contient e, cela signifie qu'il existe un élément $x \in H \cap K$ différent de e. On a alors $(e,x) \in H \times K$ et $(x,e) \in H \times K$, et $f(e,x) = f(x,e)$. Comme $(e,x) \neq (x,e)$, f n'est pas injective, donc pas bijective.

On conclut donc : f est bijective si et seulement si $H \cap K = \{e\}$.

2. (a)
   - Supposons que HK est un sous-groupe de G.
     * Soit $x \in HK$. Puisque $x \in HK$, $x^{-1} \in HK$, donc il existe $h \in H$, $k \in K$ tels que $x^{-1} = hk$, puis $x = k^{-1}h^{-1} \in KH$. Donc $HK \subset KH$
     * Soit $x \in KH$, alors il existe $k \in K$, $h \in H$ tels que $x = kh$, donc $x^{-1} = h^{-1}k^{-1}$. Ainsi, $x^{-1} \in HK$, et HK étant un groupe, on en déduit que $x \in HK$. Ainsi, $KH \subset HK$.

     Des deux inclusions, on déduit : $HK = KH$.
   - Réciproquement, supposons que $HK = KH$.
     * On a $HK \subset G$ et $e = e \times e \in HK$.
     * Soit $x \in HK$, alors il existe $h \in H$, $k \in K$ tel que $x = hk$, donc $x^{-1} = k^{-1}h^{-1} \in KH = HK$.
     * Soit $(x,y) \in (HK)^2$. Alors il existe $(h_1,h_2) \in H^2$, $(k_1,k_2) \in K^2$ tels que
     $$x = h_1k_1 \qquad \text{et} \qquad y = h_2k_2.$$
     On a alors $xy = h_1k_1h_2k_2$. Comme $k_1h_2 \in KH = HK$, il existe $h_3 \in H$ et $k_3 \in K$ tels que $k_1h_2 = h_3k_3$, d'où
     $$xy = (h_1h_3)(k_3k_2) \in HK.$$

     Ainsi, HK est un sous-groupe de G.

   On conclut que $\boxed{HK \text{ est un sous-groupe de } G \text{ si et seulement si } HK = KH}$.

   (b) Dans ce cas :
   - $H \cup K \subset HK$ de façon évidente (si $h \in H$, $h = h \times e$, et de même pour K).
   - Si L est un groupe tel que $H \cup K \subset L$, par stabilité, pour tout $h \in H$ et tout $k \in K$, $(h,k) \in L^2$, donc $hk \in L^2$. On en déduit que $HK \subset L$.

   Ainsi, $\boxed{HK \text{ est le plus petit sous-groupe de } G \text{ contenant } H \cup K.}$

3. On suppose dans cette question que G est produit semi-direct de K par H.

   (a)
   - Au vu des hypothèses $H \cap K = \{e\}$ et $HK = G$, la fonction $f : (h,k) \to hk$ est une bijection de $H \times K$ sur G. Soit $g \in G$. Il existe donc $h \in H$ et $k \in K$ uniques tels que $g = xy$. La condition $\alpha(xy) = x$ pour tout $x \in H$ et tout $y \in K$ impose alors $\alpha(g) = x$. Cela assure l'$\boxed{\text{unicité de } \alpha}$
   - Le raisonnement précédent donne aussi l'$\boxed{\text{existence}}$. Plus formellement, on obtient la description suivante : $\alpha = p_H \circ f^{-1}$, où p_H désigne la projection $(h,k) \mapsto h$ de $H \times K$ sur H.
   - Par ailleurs, étant donné g_1 et g_2 deux éléments de G, il existe h_1, h_2, k_1, k_2 tels que $g_1 = h_1k_1$ et $g_2 = h_2k_2$. On a alors $\alpha(g_1) = h_1$ et $\alpha(g_2) = h_2$. Par ailleurs, K étant distingué, $h_2K = Kh_2$, donc il existe k_3 dans K tel que $k_1h_2 = h_2k_3$. Ainsi :
   $$\alpha(g_1g_2) = \alpha(h_1k_1h_2k_2) = \alpha((h_1h_2)(k_3k_2)) = h_1h_2 = \alpha(g_1)\alpha(g_2).$$

   Ainsi, $\boxed{\alpha \text{ est un morphisme de groupes.}}$

   (b)
   - Pour tout $h \in H$, $\alpha(h) = \alpha(h \times e) = h$. Ainsi, $\alpha_{|H} = \mathrm{id}_H$, donc $\boxed{\alpha(H) = H}$.
   - Soit $h \in H \cap \mathrm{Ker}(\alpha)$. On a alors
   $$e = \alpha(h) = \alpha(h \times e) = h.$$

   Ainsi, $H \cap \mathrm{Ker}(\alpha) \subset \{e\}$, et e étant dans tout sous-groupe, $\boxed{H \cap \mathrm{Ker}(\alpha) = \{e\}}$.

4. Soit G un groupe, H un sous-groupe de G, et α un morphisme de G dans H tel que $\alpha(H) = H$ et $H \cap \mathrm{Ker}(\alpha) = \{e\}$. On pose $K = \mathrm{Ker}(\alpha)$.
   - On a évidemment $HK \subset G$
   - Soit $g \in G$, et $h' = \alpha(g) \in H$. Puisque $\alpha(H) = H$ il existe h tel que $\alpha(h) = h'$. Posons alors $k = h^{-1}g$. On a :
   $$\alpha(k) = \alpha(h^{-1}g) = \alpha(h)^{-1}\alpha(g) = h'^{-1}h' = e,$$

   donc $k \in \mathrm{Ker}(\alpha)$. On a donc $g \in HK$, donc $G \subset HK$.

- Par hypothèse, $H \cap K = \{e\}$.
- Soit $k \in K$ et $g \in G$. On a

$$\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g)^{-1} = \alpha(g)e\alpha(g)^{-1} = \alpha(g)\alpha(g)^{-1} = \mathrm{e}.$$

  Ainsi, $gkg^{-1} \in K$. Par conséquent, K est un sous-groupe distingué de G.

On en déduit que $\boxed{G \text{ est produit semi-direct de } \mathrm{Ker}(\alpha) \text{ par } H}$.

Partie III – Théorème de Burnside

1. Soit $(x, y) \in H^2$. Comme $H \subset N_G(H) = C_G(H)$, x est dans le centralisateur de y, donc x et y commutent. Ainsi, $\boxed{H \text{ est abélien}}$.
2. Soit $(x, y) \in G \times H$, et $z = xyx^{-1}$. On suppose que $z \in H$.
   (a)
   - Puisque $z \in H$, on a $H \subset N_G(H) = C_G(H) \subset C_G(z)$. Ainsi, H est un sous-groupe de $C_G(z)$. D'après le théorème de Lagrange, l'ordre de H divise l'ordre de $C_G(z)$, qui divise l'ordre de G. On en déduit que la valuation p-adique de $C_G(z)$ est égale à r, et par conséquent, $\boxed{H \text{ est un } p\text{-sous-groupe de Sylow de } C_G(z)}$.
   - Par régularité de x et x^{-1}, l'application définie sur H par $h \mapsto xhx^{-1}$ est injective, donc sa corestriction à son image xHx^{-1} est bijective. Par conséquent, H et xHx^{-1} ont même cardinal p^r.
   - xHx^{-1} est un sous-ensemble non vide de G, et pour tout $(a, b) \in (xHx^{-1})^2$, il existe h et k dans H tels que

$$a = xhx^{-1} \qquad \text{et} \qquad b = xkx^{-1} \qquad \text{donc:} \qquad ab^{-1} = xhk^{-1}x^{-1} \in xHx^{-1}.$$

     D'après la caractériation des sous-groupes, xHx^{-1} est un sous-groupe de G
   - Soit $a \in xHx^{-1}$. Montrons que $a \in C(z)$. Il existe $h \in H$ tel que $a = xhx^{-1}$. On a alors

$$aza^{-1} = xhx^{-1}xyx^{-1}xh^{-1}x^{-1} = xhyh^{-1}x^{-1}.$$

     Or, h, h^{-1} et y sont dans H qui est abélien, donc $hyh^{-1} = hh^{-1}y = y$. Ainsi

$$aza^{-1} = aya^{-1} = z.$$

     On en déduit que xHx^{-1} est un sous-groupe de $C(z)$.
   - Pour les mêmes raisons que plus haut, $\boxed{xHx^{-1} \text{ est donc un } p\text{-sous-groupe de Sylow de } C(z)}$.

   (b) Les p-sous-groupes de Sylow étant deux à deux conjugués, il existe $x' \in C_G(z)$ tel que $H = x'(xHx^{-1})x'^{-1}$. Il en découle que $x'x \in N_G(H) = C_G(H)$. Comme $x' \in C_G(H)$, on obtient $x \in C_G(H)$, donc $x \in G_C(y)$. La définition de z amène alors $\boxed{z = y}$.
3. Soit $y \in G$, et $(x_1, \ldots, x_m)$ un système de représentants des classes à gauche modulo H dans G.
   (a) Soit $i \in [\![1, m]\!]$. Les ensembles $x_1H, \ldots, x_mH$ formant une partition de G, l'élément yx_i est dans l'un et un seul d'entre eux. Ainsi, il exite un unique indice $\sigma(i) \in [\![1, m]\!]$ tel que $yx_i \in x_{\sigma(i)}H$. Il existe alors $h \in H$ tel que

$$yx_1 = x_{\sigma(i)}h$$

   Mais alors h est tout déterminé par la nécessité d'avoir $h = yx_1x_{\sigma(i)}^{-1}$.

   D'où $\boxed{\text{l'existence et l'unicité de } \sigma(i) \in [\![1, m]\!] \text{ et } h_i \in H \text{ tels que } yx_i = x_{\sigma(i)}h_i.}$

   (b)
   - L'application σ est bien définie de $[\![1, n]\!]$ dans $[\![1, n]\!]$.
   - Soit (i, j) dans $[\![1, m]\!]^2$ tels que $\sigma(i) = \sigma(j)$. On a alors

$$yx_ih_i^{-1} = x_{\sigma(i)} = x_{\sigma(j)} = yx_jh_j^{-1}.$$

     Par régularité des éléments d'un groupe, $x_ih_i^{-1} = x_jh_j^{-1}$, donc $x_iH \cap x_jH \neq \varnothing$, d'où $x_iH = x_jH$, ces ensembles formant une partition. Comme les x_i sont des représentants de classes deux à deux distinctes, on peut en conclure que $i = j$, donc que σ est injective.
   - Pour des raisons de cardinalité, σ est alors bijective. Donc $\boxed{\sigma \in \mathfrak{S}_m}$.

(c) T définit une application de G dans H. De plus, étant donné g et g' dans G, en définissant les h_i (pour g_i) et les h'_i (pour g'_i), et σ et σ' les éléments de $\mathfrak{S}_m$ associés, on a, pour tout $i \in [\![1, m]\!]$:

$$gg' = x_{\sigma\circ\sigma'(i)} h_{\sigma'(i)} x_{\sigma'(i)}^{-1} x_{\sigma'(i)} h'_i x_i^{-1} = x_{\sigma\circ\sigma'(i)} h_{\sigma'(i)} h'_i x_i.$$

Ainsi, la permutation associée à gg' est $\sigma \circ \sigma'$, et la famille (h''_i) est définie par :

$$\forall i \in [\![1, m]\!], \quad h''_i = h_{\sigma'(i)} h'_i.$$

Puisque H est abélien et que σ' est une permutation, on en déduit que

$$T(gg') = \prod_{i=1}^{m} h_{\sigma'(i)} h'_i = \prod_{i=1}^{m} h_i \prod_{i=1}^{m} h'_i = T(g)T(g').$$

Ainsi, $\boxed{T \text{ est un morphisme de groupes de } G \text{ dans } H.}$

(d) • Soit $y \in G$, et σ la permutation de $[\![1, m]\!]$ associée. On définit sur $[\![1, m]\!]$ la relation suivante :

$$i \sim j \iff \exists k \in \mathbb{N}, i = \sigma^k(j),$$

Il s'agit d'une relation d'équivalence :

∗ Soit $i \in [\![1, m]\!]$, $i = \sigma^0(i)$, donc $i \sim i$, d'où la reflexivité.

∗ Soit i, j tels que $i \sim j$. Alors il existe k tel que $j = \sigma^k(i)$. Comme $\mathfrak{S}_m$ est un groupe fini, l'élément σ est aussi d'ordre fini (son ordre divise l'ordre de $\mathfrak{S}_m$), il existe donc $\ell \in \mathbb{N}$ tel que $(\sigma^\ell) = \mathrm{id}$. Soit q et r le quotient et le reste de la division euclidienne de k par ℓ. Il vient alors :

$$\sigma^{\ell-r}(j) = \sigma^{\ell-r+k}(i) = \sigma^{(q+1)\ell}(i) = \mathrm{id}^{q+1}(i) = i,$$

et $\ell - r \in \mathbb{N}$. Ainsi, $j \sim i$. D'où la symétrie.

∗ Soit $i_1 \sim i_2$ et $i_2 \sim i_3$. Il existe $(k, \ell) \in \mathbb{N}^2$ tels que $i_2 = \sigma^k(i_1)$ et $i_3 = \sigma^\ell(i_2)$, donc $i_3 = \sigma^{k+\ell}(i_1)$. Ainsi, $i_1 \sim i_3$, d'où la transitivité.

Ainsi, il s'agit bien d'une relation d'équivalence.

• On considère alors $\{X_1, \dots, X_t\}$ la partition de $[\![1, m]\!]$ formée des classes d'équivalence. Soit $j \in [\![1, t]\!]$ et $i \in X_j$. Puisque σ est d'ordre fini, il existe $k > 0$ tel que $\sigma^k(i) = i$. Soit k_0 la plus petite de ces valeurs. Alors $\sigma^0(i), \sigma^1(i), \dots, \sigma^{k_0-1}(i)$ sont des éléments deux à deux distincts de X_j (si $\sigma^q(i) = \sigma^r(i)$, avec $q < r$, en appliquant la fonction bijective σ^{-q}, on contredit la minimalité de k_0). De plus, la suite $(\sigma^k(i))_{n\in\mathbb{N}}$ est alors périodique de période minimale k, les k valeurs prises sur une période étant deux à deux distinctes. Or, par définition de la relation d'ordre et de ses classes, les valeurs prises par cette suite sont exactement les éléments de X_j, donc $k = |X_j|$. Ainsi, la restriction de σ à X_j est une permutation cyclique : après avoir donné un ordre cyclique aux éléments de X_j, chaque application de la permutation σ fait tourner les éléments. En particulier, $X_j = \{\sigma^k(i),\ i \in [\![0, k_0 - 1]\!]\}$.

On vient de décrire la décomposition en cycles disjoints de la permutation σ : la permutation σ peut être vue comme un ensemble de cycles disjoints : à chaque fois qu'on applique une nouvelle fois σ, on fait tourner d'un cran chaque cycle. Les cycles n'ont pas tous la même taille, donc on n'en fait pas le tour à la même vitesse. Cette situation est à comparer aux roues de tailles différentes d'un tracteur ou d'une locomotive à vapeur : une permutation est un ensemble de roues de tailles différentes, qu'on fait tourner simultanément.

Soit $J \subset [\![1, n]\!]$ un système de représentant de chaque classe X_i. On note $X(j)$ la classe représentée par $j \in J$. Étant donné $j \in J$, on a alors, le produit étant justifiant par le fait que les éléments dont on fait le produit sont dans H qui est abélien) :

$$\begin{aligned}\prod_{i\in X(j)} h_i = \prod_{i\in X(j)} x_{\sigma(i)}^{-1} y x_i = \prod_{k=0}^{n_j-1} x_{\sigma^{k+1}(j)}^{-1} y x_{\sigma^k(j)} \\ = x_{\sigma^{n_j}(j)}^{-1} y x_{\sigma^{n_j-1}(j)} x_{\sigma^{n_j-1}(j)}^{-1} y x_{\sigma^{n_j-2}(j)} \dots x_{\sigma^2(j)}^{-1} y x_{\sigma(j)} x_{\sigma(j)}^{-1} y x_j\end{aligned}$$

et après simplifications :

$$\prod_{i\in X(j)} h_i = x_{\sigma^{n_j}(j)}^{-1} y^{n_j} x_j = x_j y^{n_j} x_j^{-1}.$$

En particulier, comme $\prod_{i\in X(j)} h_i \in H$, on a pour tout $j \in J$, $\boxed{x_j^{-1} y^{n_j} x_j \in H}$

- Du fait que H est abélien, on obtient, en faisant le produit des expressions trouvées sur chacune des parts de la partition $X(j), j \in J$:

$$\prod_{i=1}^{m} h_i = \prod_{j\in J} x_j^{-1} y^{n_j} x_j \qquad \text{soit:} \qquad \boxed{T(y) = \prod_{j\in J} x_j^{-1} y^{n_j} x_j}$$

- Comme les n_j sont les cardinaux de parts d'une partition de $[\![1, m]\!]$, on a $\boxed{\sum_{j\in J} n_j = m}$.

(e) Soit $y \in H$. D'après la question 2 (appliquée avec $x = x_j^{-1}$), puisque $x_j^{-1} y^{n_j} x_j \in H$ ainsi que y^{n_j}, il vient, pour tout $j \in J$:

$$x_j^{-1} y^{n_j} x_j = y^{n_j}.$$

Ainsi, $T(y) = \prod_{j\in J} y^{n_j} = y^{\sum_{j\in J} n_j}$, donc $\boxed{T(y) = y^m}$.

(f) La fonction $y \mapsto y^m$ est bijective de H dans H, car m est premier avec p^α. En effet, on a alors, d'après le théorème de Bézout, l'existence de deux entiers u et v tels que $um + vp^\alpha = 1$. La fonction $y \mapsto y^u$ de H dans H est alors une réciproque de $y \mapsto y^m$, puisque

$$(y^u)^m = (y^m)^u = y^{mu} = y^{1-vp^\alpha} = y \times (y^{-v})^{p^\alpha} = y,$$

d'après le théorème de Lagrange, H étant d'ordre p^α. Ainsi $\boxed{T(H) = H}$.
Par ailleurs soit $h \in \mathrm{Ker}(T) \cap H$, on a :

$$e = T(h) = h^m,$$

donc l'ordre de h divise m. Comme l'ordre de h divise p^α (théorème de Lagrange), l'ordre de h divise $p^\alpha \wedge m = 1$. Ainsi $h = e$. On en déduit que $\mathrm{Ker}(T) \cap H \subset \{e\}$, puis $\mathrm{Ker}(T) \cap H = \{e\}$.
D'après la question II-4, $\boxed{G \text{ est donc un produit semi-direct de } \mathrm{Ker}(T) \text{ par } H.}$