Université M. Ismail – Faculté des Sciences – Département de Mathématiques

**Travaux Dirigés d'Algèbre 6 - S4 / Corrigé de la Série 2 – 2020-2021**

(Proposé par Pr. Rami)

**Exercice 1.** Puisque 5 est premier, les générateurs de $\mathbb{Z}/5\mathbb{Z}$ sont $\bar{1}$, $\bar{2}$, $\bar{3}$ et $\bar{4}$. Soit donc $f \in Aut(\mathbb{Z}/5\mathbb{Z})$. Puisque $f$ est bijective, on doit alors avoir :

$$Im(f) = \{mf(\bar{1}),\ m = 0, 1, 2, 3, 4\} = < f(\bar{1}) > = \mathbb{Z}/5\mathbb{Z}$$

($f$ est déterminée par $f(\bar{1})$). Donc $f(\bar{1}) = \bar{1},\ \bar{2},\ \bar{3},\ ou\ \bar{4}$. Ainsi, $Aut(\mathbb{Z}/5\mathbb{Z}) = \{f_1 = Id, f_2, f_3, f_4\}$ avec $f_k(\bar{1}) = \bar{k} = k\bar{1} = kId(\bar{1})$. En considère l'application :

$$\begin{array}{cccc} \varphi : & (Aut(\mathbb{Z}/5\mathbb{Z}), \circ) & \to & ((\mathbb{Z}/5\mathbb{Z})^*, \times) \\ & f_k & \mapsto & \bar{k} \end{array}$$

où $(\mathbb{Z}/5\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ désigne le groupe multiplicatif des inversibles de $\mathbb{Z}/5\mathbb{Z}$. On vérifie facilement que c'est un isomorphisme. Par suite $Aut(\mathbb{Z}/5\mathbb{Z}) \cong ((\mathbb{Z}/5\mathbb{Z})^*, \times) = (< \bar{2} >, \times)$ qui est cyclique d'ordre 4.

**Exercice 2.** Supposons que $G$ admet deux sous-groupes distincts $H$ et $K$ d'ordre $p$ (premier). On sait alors, d'après le cours que $card(HK) = \frac{|H||K|}{|H \cap K|}$. Mais $H \cap K$ étant un sous-groupe de $H$ (et de $K$), il est d'ordre 1 ou bien d'ordre $p$. Si $\mid H \cap K \mid = p$ alors $H \cap K = H = K$ (ils ont tous même ordre) ce qui est contraire à $H \neq K$ et par suite $\mid H \cap K \mid = 1$ et donc $card(HK) = p^2 > pq = \mid G \mid$. Ce qui est absurde (car $HK \subseteq G$). Par conséquent, $G$ admet au plus un sous-groupe d'ordre $p$.

Pour la déduction, remarquons que si $H$ est un sous-groupe de $G$ d'ordre $p$, alors, $\forall x \in G,\ x^{-1}Hx$ est aussi un sous-groupe de $G$ et il est aussi d'ordre $p$ (il y a une bijection entre les deux). Par suite, d'après ce qui précède, on aura $\forall x \in G,\ x^{-1}Hx = H$ et donc $H$ (s'il existe) sera distingué dans $G$.

**Exercice 3.**

1. Soit $G$ un groupe et $H$ un sous-groupe d'indice deux de $G$. On a alors $(G/H)_g = \{H, xH\}$ pour tout $x \notin H$ (car $\bar{e} = \bar{x} \Leftrightarrow x \in H$). De même $(G/H)_d = \{H, Hx\}$ pour tout $x \notin H$. Par suite, $\forall x \notin H$, on a $G = H \cup xH = H \cup Hx$ et $H \cap xH = H \cap Hx = \emptyset$ ce qui implique alors que $\forall x \notin H,\ xH = Hx$ ($z \in xH \Leftrightarrow z \notin H \Leftrightarrow z \in Hx$). D'autre part, on a par définition, $\forall h \in H$, on $hH = eH = He = Hh$. En conclusion, on a $\forall y \in G,\ yH = Hy$ et donc que $H$ est un sous-groupe distingué de $G$.
2. Rappelons que $Z(G) = \{x \in G : \forall g \in G,\ gx = xg\}$. On a alors, $\forall g \in G, \forall x \in Z(G),\ gx = xg$ par suite $\forall g \in G$, $gZ(G) = \{gx :\ x \in Z(G)\} = \{xg :\ x \in Z(G)\} = Z(G)g$ ; D'où $Z(G) \trianglelefteq G$. Si maintenant $H$ est un sous-groupe de $Z(G)$, il suffit de prendre $g \in H$ pour obtenir aussi que $H \trianglelefteq G$.

3. Soit $H$ un sous-groupe d'ordre deux distingué dans $G$. On a alors $H = \{e, h\}$ d'où, $\forall x \in G\ xH = \{x, xh\} = Hx = \{x, hx\}$. Par suite, $\forall x \in G, xh = hx$ et donc $H \subseteq Z(G)$.
4. Soit $H$ un sous-groupe cyclique et distingué dans $G$ et soit $K$ un sous-groupe de $H$. Posons $H =< x >$ ; comme tout sous-groupe d'un groupe cyclique est cyclique, $\exists k \geq 1 :\ K =< x^k >$. Ainsi, $\forall g \in G$,

$$H \trianglelefteq G \Rightarrow gH = Hg \Rightarrow \exists x' \in H :\ gx = x'g \Rightarrow gx^k = (x')^k g \Rightarrow gK = Kg \Rightarrow K \trianglelefteq G.$$

**Exercice 4.** Soit $G$ un groupe commutatif d'ordre 10.

1. $\mid G \mid= 10 \Rightarrow \forall x \in G \backslash \{e\},\ o(x) = 2,\ 5\ ou 10$. Si $G$ est cyclique engendré par $x \in G$, alors $o(x^2) = 5$. Sinon, si tous les éléments de $G\backslash\{e\}$ sont d'ordre 2, alors $G$ serait commutatif, ce qui est contraire à l'hypothèse. D'où $\exists x \in G :\ o(x) = 5$.
2. D'après la question précédente, et comme 5 est premier, $H =< x >$ est un sous-groupe d'ordre 5 de $G$ et son indice est $[G : H] = 2$ par suite d'après l'exercice (3), $H \trianglelefteq G$. Enfin, puisque $H \trianglelefteq G$, $G/H$ est un groupe quotient et son ordre est $[G : H] = 2$ et donc $G/H = \{\bar{e}, \bar{x}\}$ de sorte que $\bar{x}^{-1} = \bar{x}$ ce qui entraîne que $\bar{x}$ est d'ordre 2.

**Exercice 5.** Soit $G$ un groupe tel que pour tout entier $n > 1$ fixé, on a : $\forall x, y \in G\ (xy)^n = x^n y^n$.

1. Montrons que $G^n = \{x^n :\ x \in G\}$ est un sous-groupe distingué de $G$.
   $G^n$ est un sous-groupe de $G$ car $G^n \subseteq G$, $e = e^n \in G^n$ et $\forall x^n,\ y^n \in G^n$, on $x^n y^n = (xy)^n \in G^n$ et $(x^n)^{-1} = (x^{-1})^n \in G^n$. D'autre part, $\forall g \in G$

$$\begin{aligned} gx^n g^{-1} &= gx(g^{-1}g)x(g^{-1}g)x \dots x(g^{-1}g)xg^{-1} \\ &= (gxg^{-1})(gxg^{-1}) \dots (gxg^{-1}) = (gxg^{-1})^n \in G^n. \end{aligned}$$

   Par conséquent, $G^n \trianglelefteq G$.
2. $(xy)^n = (xy)(xy) \dots (xy) = x(yx(yx) \dots (yx)y = x(yx)^{n-1}y$ et puisque $(xy)^n = x^n y^n$, on en déduit alors que $x(yx)^{n-1}y = x^n y^n$, ainsi, par multiplication par $x^{-1}$ à gauche et par $y^{-1}$ à droite, on obtient $(yx)^{n-1} = x^{n-1}y^{n-1}$.
3. Montrons que $G^{n-1} = \{x^{n-1} :\ x \in G\}$ est distingué dans $G$.
   On montre de la même manière, pour $G^n$, que $G^{n-1}$ est un sous-groupe de $G$ sachant que la différence entre les deux formules $(xy)^n = x^n y^n$ et $(yx)^{n-1} = x^{n-1}y^{n-1}$ ne change en rien le raisonnement dans les deux cas car $xy \in G$ et $yx \in G$. De même, $\forall g \in G$

$$\begin{aligned} gx^{n-1}g^{-1} &= gx(g^{-1}g)x(g^{-1}g)x \dots x(g^{-1}g)xg^{-1} \\ &= (gxg^{-1})(gxg^{-1}) \dots (gxg^{-1}) = (gxg^{-1})^{n-1} \in G^{n-1}. \end{aligned}$$

   Par conséquent, $G^{n-1} \trianglelefteq G$.

**Exercice 6.** Soit $G$ un groupe et $A$ une partie non vide de $G$. On pose

$N_A = \{(g_1a_1g_1^{-1})(g_2a_2g_2^{-1})\dots(g_na_ng_n^{-1}) :\ n \in \mathbb{N}^*\ et\ \forall 1 \leq i \leq n;\ g_i \in G\ et\ a_i \in A \cup A^{-1}\}.$

1. Montrons que $A \subseteq N_A \trianglelefteq G$.
On a $A \subseteq N_A$ vient du fait que l'on peut prendre $n = 1$, $a_1 = a \in A$, $g_1 = e$ ; et donc $a = g_1a_1g_1^{-1} \in N_A$.
Montrons ensuite que $N_A$ est un sous-groupe de $G$. On a clairement $\emptyset \neq N_A \subseteq G$.
Soit maintenant
$$x = (g_1a_1g_1^{-1})(g_2a_2g_2^{-1})\dots(g_na_ng_n^{-1}) \in N_A$$
et
$$x' = (g'_1a'_1(g'_1)^{-1})(g'_2a'_2(g'_2)^{-1})\dots(g'_ma"_m(g'_n)^{-1}) \in N_A$$
alors
$$xy = g"_1a"_1(g"_1)^{-1})(g"_2a"_2(g"_2)^{-1})\dots(g"_{n+m}a"_n(g"_{n+m})^{-1}) \in N_A$$
(avec $g"_i = g_i, 1 \leq i \leq n$, $a"_i = a_i, 1 \leq i \leq n$ et $g"_{n+i} = g'_i$, $a"_{n+i} = a'_i, 1 \leq i \leq m$).
Ensuite on a
$$x^{-1} = (g_n^{-1}a_n^{-1}g_n)\dots(g_1^{-1}a_1^{-1}g_1) = (h_1b_1(h_1)^{-1})\dots(h_nb_n(h_n)^{-1}))$$
avec $h_i = (g_{n-i+1})^{-1} \in G,\ b_i = (a_{n-i+1})^{-1} \in A \cup A^{-1},\ 1 \leq i \leq n$. Par conséquent, $N_A$ est un sous-groupe de $G$.
Soit maintenant $g \in G$ et $x = (g_1a_1g_1^{-1})(g_2a_2g_2^{-1})\dots(g_na_ng_n^{-1}) \in N_A$. On peut écrire
$$gxg^{-1} = ((gg_1)a_1(gg_1)^{-1})((gg_1)a_1(gg_1)^{-1})\dots((gg_1)a_1(gg_1)^{-1})$$
sachant qu'on a inséré $e = g^1g$ entre deux termes consécutifs de $x$. On a donc $gxg^{-1} \in N_A$ et par suite $N_A \trianglelefteq G$.

2. Montrons enfin que $N_A$ est le plus petit sous-groupe distingué de $G$ contenant $A$.
On a déjà vu que $A \subseteq N_A$. Soit donc $K \trianglelefteq G$ tel que $A \subseteq K$. On a alors :
$K$ sous-groupe, entraîne que $A \cup A^{-1} \subseteq K$, puis, puisque $K \trianglelefteq G$, alors pour tout $x = (g_1a_1g_1^{-1})(g_2a_2g_2^{-1})\dots(g_na_ng_n^{-1}) \in N_A$, ses facteurs $g_ia_ig_i^{-1} \in K;\ 1 \leq i \leq n$ et par suite $x \in K$. D'où $K \subseteq N_A$.

**Exercice 7.** Soit $G$ un groupe, $H$ un sous-groupe de $Z(G)$ tel que $G/H$ est cyclique. Montrons alors que $G$ est abélien. Notons au début que d'après l'exercice 3), $H \trianglelefteq G$ donc $G/H$ est bien un groupe quotient.

Soient donc $x, y \in G$ deux éléments quelconques. Comme $H \subseteq Z(G)$, on a : si $x \in H$ ou $y \in H$, alors $xy = yx$. Supposons donc que $x \notin H$ et $y \notin H$. Il en résulte que $\bar{x} \neq \bar{e} = H$ et $\bar{y} \neq \bar{e} = H$ dans $G/H$. Maintenant $G/H$ cyclique, entraine qu'il existe $a \in G$ tel que

$G/H = <\bar{a}>$ et donc $\bar{x} = (\bar{a})^k$ et $\bar{y} = (\bar{a})^l$ $(k, l \geq 1)$ et donc $\exists h, h' \in H$ tels que $x = a^k h$ et $y = a^l h'$. On obtient alors :

$$xy = a^k h a^l h' = h a^k a^l h' = h a^l a^k h' = h' a^l h a^k = yx.$$

Ainsi, on a $\forall x, y \in G,\ xy = yx$ et par conséquent $G$ est commutatif.

**Exercice 8.** Soit $H^*,\ H,\ K^*\ et\ K$ quatre sous-groupes d'un groupe $G$. On suppose que $H^* \trianglelefteq H$ et $K^* \trianglelefteq K$.

1. Montrons que $F = (H \cap K^*)(K \cap H^*) \trianglelefteq H \cap K$.
   Premièrement, puisque $H \cap K^*$, $K \cap H^*$ et $H \cap K$ sont des sous-groupes de $G$ et que $H \cap K^* \subseteq H \cap K$ et $K \cap H^* \subseteq K \cap H = H \cap K$, alors $H \cap K^*$ et $K \cap H^*$ sont des sous-groupes de $H \cap K$. Pour montrer que $F \trianglelefteq H \cap K$, il suffit de montrer que $(H \cap K^*) \trianglelefteq H \cap K$ et $(K \cap H^*) \trianglelefteq H \cap K$.
   Soit donc $g \in H \cap K$ et $x \in H \cap K^*$, on a alors $gx \in gK^*$ et $g \in K$ entraîne qu'il existe $x' \in K^*$ tel que $gx = x'g$. Or, $g \in H$ et $x \in H$ implique que $x' = gxg^{-1} \in H$ et par suite, $x' \in H \cap K^*$. D'où $\forall g \in H \cap K,\ g(H \cap K^*) = (H \cap K^*)g$ et donc $H \cap K^* \trianglelefteq H \cap K$. On montre de même que $K \cap H^* \trianglelefteq H \cap K$ et on conclut ainsi que $F \trianglelefteq H \cap K$.
2. Soit $f : H^*(H \cap K) \to (H \cap K)/F$ définie par $f(h^*x) = xF$.
   (a) Notons au début que $f$ est bien définie et est un homomorphisme de groupes. Ensuite, $h^*x \in Ker(f) \Leftrightarrow xF = F \Leftrightarrow x \in F \Leftrightarrow \exists ab \in F :\ h^*x = h^*ab$. Or, $F$ étant un groupe, en écrivant $F = (K \cap H^*)(H \cap K^*)$, on a alors $ab = b'a'$ avec $a' \in K \cap H^*$ et $b' \in H \cap K^*$ et par suite, $h^*x = (h^*a')b' \in H^*(H \cap K^*)$ car $h^*a' \in H^*$. D'où, $Ker(f) \subseteq H^*(H \cap K^*)$. Inversement, $\forall h^*x \in H^*(H \cap K^*)$, on a $f(h^*x) = xF = F$ car $x = xe \in F$ et donc $Ker(f) = H^*(H \cap K^*)$.
   (b) Il suffit de noter que $f$ est surjective et utiliser le premier théorème d'isomorphisme qui donne l'isomorphisme :
   $$H^*(H \cap K)/H^*(H \cap K^*) \cong (H \cap K)/F.$$
   (c) En remarquant la symétrie imposée dans la définition de $F$, on voit qu'il suffit de prendre $g : K^*(K \cap H^*) \to (H \cap K)/F$ définie par $g(k^*x) = xF$ et d'en déduire (de la même manière) que :
   $$K^*(H \cap K)/K^*(H^* \cap K) \cong (H \cap K)/F.$$
   Il en résulte l'isomorphisme :
   $$H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K).$$

**Exercice 9.** Un groupe $G$ est dit résoluble s'il possède une suite de sous-groupes

$$(1) \quad G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \{e\}.$$

telle que $\forall 0 \leq i \leq n-1,\ G_{i+1} \trianglelefteq G_i$ et $G_i/G_{i+1}$ est abélien.

1. Soit $G$ un groupe abélien. En posant $G_0 = G$ et $G_1 = \{e\}$, on déduit que $G$ est résoluble. En particulier, tout groupe cyclique est abélien, il est donc résoluble.
2. Soit $f : G \to G'$ un homomorphisme de groupes tel que $G$ soit résoluble muni de la suite (1). Il est clair que chaque $f(G_i)$ est un un sous-groupe de $f(G)$ et que $f(G_{i+1}) \subseteq f(G_i)$.

   Montrons que $f(G_{i+1}) \trianglelefteq f(G_i)$. Soit $y = f(x) \in f(G_i)$ et $z = f(x') \in f(G_{i+1})$, c. à. d. $yz \in yf(G_{i+1})$. On a $yz = f(x)f(x') = f(xx')$. Or, $xx' \in xG_{i+1} = G_{i+1}x \Rightarrow \exists x" \in G_{i+1},\ xx' = x"x$ et donc $yz = f(x"x) = f(x")f(x) \in f(G_{i+1})y$. On en déduit que $yf(G_{i+1}) \subseteq f(G_{i+1})y,\ \forall y \in f(G_i)$ et donc $f(G_{i+1}) \trianglelefteq f(G_i)$.

   Considérons maintenant $q \circ f_{|G_i} : G_i \to f(G_i) \to f(G_i)/f(G_{i+1})$ définie par : $q \circ f_{|G_i}(x) = \overline{f(x)}$. C'est la composée de deux homomorphismes surjectifs de groupes et on a clairement $f(G_{i+1}) \subseteq Ker(q \circ f_{|G_i})$. Par suite, d'après le premier théorème d'isomorphisme $q \circ f_{|G_i}$ se factorise en $q \circ f_{|G_i} = \bar{f} \circ p$ avec $p : G_i \to G_i/G_{i+1}$ et $\bar{f} : G_i/G_{i+1} \to f(G_i)/f(G_{i+1})$. On a donc $\forall x \in G_i,\ \overline{f(x)} = \bar{f}(\bar{x})$.

   D'autre part, soit $\bar{y}, \bar{y'} \in f(G_i)/f(G_{i+1})$. On a $\bar{y}\bar{y'} = \overline{yy'}$ et si $y = f(x)$ et $y' = f(x')$ alors $\bar{y}\bar{y'} = \bar{f}(\overline{xx'}) = \bar{f}(\bar{x}\bar{x'}) = \bar{f}(\bar{x'}\bar{x})$ car $G_i/G_{i+1}$ est abélien. Par suite $\bar{y}\bar{y'} = \bar{y'}\bar{y}$ ce qui entraîne que $f(G_i)/f(G_{i+1})$ est aussi abélien. En conclusion, $f(G)$ est résoluble lorsqu'il est muni de la suite

   $$f(G) = G'_0 \supseteq G'_1 = f(G_1) \supseteq G'_2 = f(G_2) \supseteq \ldots \supseteq G'_n = \{e\}.$$

   En particulier, si $G$ est résoluble, alors tout groupe $G/H$ quotient est image directe de l'homomorphisme $p : G \to G/H$ et donc il est aussi résoluble.
3. Soit $f : G \to G'$ un homomorphisme injectif de groupes. Montrons que si $G'$ est résoluble, alors $G$ est résoluble. On suppose donc que $G'$ est muni de la suite

   $$G' = G'_0 \supseteq G'_1 \supseteq G'_2 = f(G_2) \supseteq \ldots \supseteq G'_n = \{e'\}$$

   telle que $\forall 0 \leq i \leq n-1,\ G'_{i+1} \trianglelefteq G'_i$ et $G'_i/G'_{i+1}$ est abélien. On considère alors la suite (sachant que (toujours) $G = f^{-1}(G')$ et que, puisque $f$ est injective, $\{e\} = f^{-1}(\{e'\})$) :

   $$G = G_0 \supseteq G_1 = f^{-1}(G'_1) \supseteq G_2 = f^{-1}(G'_2) \supseteq \ldots \supseteq G_n = \{e\}.$$

   On sait que $f^{-1}(G'_{i+1})$ est un sous-groupe de $f^{-1}(G'_i)$ (car $G'_{i+1}$ est un sous-groupe de $G'_i$), pour montrer qu'il en est distingué, si $x \in f^{-1}(G'_i) \Leftrightarrow f(x) \in G'_i$, alors $xf^{-1}(G'_{i+1}) = x\{x' \in G :\ f(x') \in G'_{i+1}\} = \{xx' : f(x) \in G'_i,\ f(x') \in G'_{i+1}\}$. Par suite, comme $G'_{i+1} \trianglelefteq G'_i,\ f(x)f(x') \in f(x)G'_{i+1} = G'_{i+1}f(x) \Rightarrow \exists y \in G'_{i+1} : f(x)f(x') = yf(x)$. Mais $f(x)f(x') = yf(x) \Rightarrow y = f(x)f(x')f(x^{-1}) = f(xx'x^{-1}) \Rightarrow xx'x^{-1} \in f^{-1}(G'_{i+1}) \Rightarrow xx' \in f^{-1}(G'_{i+1})x$. D'où $xf^{-1}(G'_{i+1}) \subseteq f^{-1}(G'_{i+1})x,\ \forall x \in f^{-1}(G'_i)$. Ce qui montre en fait que $f^{-1}(G'_{i+1}) \trianglelefteq f^{-1}(G'_i)$.

   Il reste à montrer que $f^{-1}(G'_i)/f^{-1}(G'_{i+1})$ est abélien. Soient donc $x, x' \in f^{-1}(G'_i)$ ce qui équivaut à $f(x), f(x') \in G'_i$.

Comme $G'_i/G'_{i+1}$ est abélien, on a, (modulo $G'_{i+1}$),

$$\overline{f(x)f(x')} = \overline{f(x')f(x)} \Rightarrow \overline{f(xx')} = \overline{f(x'x)}$$

et par suite

$$f(xx')(f(x'x))^{-1} = f(xx'x^{-1}x'^{-1}) \in G'_{i+1} \Rightarrow xx'x^{-1}x'^{-1} \in G_{i+1} \Rightarrow \bar{x}\bar{x'} = \bar{x'}\bar{x}$$

et par conséquent $f^{-1}(G'_i)/f^{-1}(G'_{i+1})$ est abélien.
En conclusion, $f^{-1}(G')$ est aussi résoluble et c'est le cas en particulier de tout sous-groupe $H$ d'un groupe résoluble $G$ car alors $H = \iota^{-1}(H)$ où $\iota : H \hookrightarrow G$ désigne l'inclusion de $H$ dans $G$.

4. Montrons que le groupe symétrique $\mathcal{S}_3$ est résoluble. Pour cela, notons que $\mid \mathcal{S}_3 \mid = 3 \times 2$. Ainsi, d'après l'exercice 2, $\mathcal{S}_3$ admet au plus un sous-groupe d'ordre 3. Dans le cas, il existe effectivement et c'est $\mathcal{A}_3$ et on sait que $\mathcal{A}_3 \trianglelefteq \mathcal{S}_3$ (car $\mathcal{A}_3 = Ker(\varepsilon)$), en plus $\mathcal{S}_3/\mathcal{A}_3$ est d'ordre 2 donc il est cyclique et par suite abélien. Il suffit donc de considérer la suite
$$G_0 = \mathcal{S}_3 \supseteq \mathcal{A}_3 \supseteq \{e\}$$
pour conclure.