MT10/P11 - Corrigé de l'examen médian

Exercice 1 (groupes, sous-groupes, groupe dérivé) (10 points)
Soient deux groupes, $(G, *, e)$ et $(G', *', e')$, et un morphisme $f : G \to G'$.

1. Soit H un sous-groupe de G. $f(H) \overset{\text{déf}}{=} \{f(h) \ : \ h \in H\} \subset G'$ et n'est pas vide car H n'est pas vide. Si $x_1 = f(h_1)$ et $x_2 = f(h_2)$, où $h_1, h_2 \in H$, sont deux éléments de $f(H)$, alors
$$x_1 *' x_2^{-1} = f(h_1) *' f(h_2)^{-1} = f(h_1 * h_2^{-1}),$$
puisque f est un morphisme ; comme H est un sous-groupe, on a $h_1 * h_2^{-1} \in H$, et donc $x_1 *' x_2^{-1} \in f(H)$. Ceci prouve que $f(H)$ est un sous-groupe de G'.
2. Soit H' un sous-groupe de G'.
   (a) $f^{-1}(H') \overset{\text{déf}}{=} \{x \in G \ : \ f(x) \in H'\} \subset G$ n'est pas vide car $e \in f^{-1}(H')$ puisque $f(e) = e'$. Soient $x_1, x_2 \in f^{-1}(H')$, c'est-à-dire tels que $f(x_1) \in H'$ et $f(x_2) \in H'$. Comme f est un morphisme, on a donc
   $$f(x_1 * x_2^{-1}) = f(x_1) *' f(x_2)^{-1} \quad \in H',$$
   puisque H' est un sous-groupe de G'. Ceci prouve que $f^{-1}(H')$ est un sous-groupe de G.
   (b) On suppose de plus que H' est distingué dans G'. Pour montrer que $f^{-1}(H')$ est distingué dans G, considérons $h \in f^{-1}(H')$ et $x \in G$, et montrons que $x * h * x^{-1} \in f^{-1}(H')$. Pour cela, calculons
   $$f(x * h * x^{-1}) = f(x) *' f(h) *' f(x)^{-1} \quad \in H',$$
   car $f(h) \in H'$ et H' est distingué dans G'.
3. **(commutateurs et groupe dérivé en général)**
   (a) Si G est commutatif, on a
   $$(\forall x, y \in G) \qquad [x, y] = x * y * (y * x)^{-1} = (x * y) * (x * y)^{-1} = e$$
   Donc $D(G) = \{e\}$.
   (b) $[x, y]^{-1} = \left(x * y * (y * x)^{-1}\right)^{-1} = (y * x) * (x * y)^{-1} = [y, x]$.
   (c) $f([x, y]) = f\left(x * y * (y * x)^{-1}\right) = f(x) *' f(y) *' \left(f(y) *' f(x)\right)^{-1} = [f(x), f(y)]$.
   (d) Par calcul direct, ou en utilisant la question précédente dans le cas où le morphisme f est l'automorphisme intérieur $i_g : x \mapsto g * x * g^{-1}$, il vient $g * [x, y] * g^{-1} = [g * x * g^{-1}, g * y * g^{-1}]$.
   (e) Pour montrer que $D(G)$ est un sous-groupe distingué de G, il suffit de montrer que $i_g(D(G)) \subset D(G)$, pour tout $g \in G$. D'après la question précédente, on sait que $i_g([x, y]) \in D(G)$. Donc le groupe engendré par les $i_g([x, y])$, qui est $i_g(D(G))$, est inclus dans (le groupe) $D(G)$. Ainsi, $D(G)$ est un sous-groupe distingué de G.
   (f) Par la question (c), on a $f([x, y]) \in D(G')$. En particulier, le groupe $D(G')$ contient le groupe engendré par les $f([x, y])$, qui est justement $f(D(G))$.
   (g) On suppose de plus que f est surjectif. Pour montrer que $f(D(G)) = D(G')$, il reste à montrer que $D(G') \subset f(D(G))$. Mais si f est surjective, tout commutateur de G' s'écrit $[x', y'] = [f(x), f(y)] = f([x, y])$, donc $f(D(G))$ contient tous les commutateurs de G'. Comme $f(D(G))$ est un sous-groupe, il doit aussi contenir $D(G')$ qui est par définition le plus petit sous-groupe contenant les commutateurs.

4. **(commutateurs et groupe dérivé dans $\mathfrak{S}_3$)**
On adoptera la notation des cycles pour désigner les éléments de $\mathfrak{S}_3$, le groupe des bijections de $\{1;2;3\}$ dans lui-même, de sorte que :

$$\mathfrak{S}_3 = \{\mathrm{Id}; (1\ 2); (1\ 3); (2\ 3); (1\ 2\ 3); (1\ 3\ 2)\}$$

(a) Comme $(1\ 2) \circ (1\ 2) = \mathrm{Id}$, on a $< (1\ 2) >= \{\mathrm{Id}; (1\ 2)\}$.

(b) On a $(1\ 2\ 3) \circ (1\ 2\ 3) = (1\ 3\ 2)$, puis $(1\ 2\ 3) \circ (1\ 3\ 2) = \mathrm{Id}$. On a donc

$$< (1\ 2\ 3) >= \{\mathrm{Id}; (1\ 2\ 3); (1\ 3\ 2)\}.$$

(c) On a $(1\ 2) \circ (1\ 2\ 3) = (2\ 3)$, et $(2\ 3) \circ (1\ 2\ 3) = (1\ 3)$, par conséquent $< (1\ 2), (1\ 2\ 3) >= \mathfrak{S}_3$.

(d) On a $[(1\ 2), (1\ 3)] = (1\ 2) \circ (1\ 3) \circ ((1\ 3) \circ (1\ 2))^{-1} = (1\ 2) \circ (1\ 3) \circ (1\ 2) \circ (1\ 3)$. Par ailleurs $(1\ 2) \circ (1\ 3) = (1\ 3\ 2)$, et finalement :

$$[(1\ 2), (1\ 3)] = (1\ 3\ 2) \circ (1\ 3\ 2) = (1\ 2\ 3).$$

(e) $[(1\ 2), (1\ 2\ 3)] = (1\ 2) \circ (1\ 2\ 3) \circ ((1\ 2\ 3) \circ (1\ 2))^{-1} = (1\ 2) \circ (1\ 2\ 3) \circ (1\ 2) \circ (1\ 3\ 2)$. $(1\ 2) \circ (1\ 2\ 3) = (2\ 3)$, et $(1\ 2) \circ (1\ 3\ 2) = (1\ 3)$, et finalement :

$$[(1\ 2), (1\ 2\ 3)] = (2\ 3) \circ (1\ 3) = (1\ 2\ 3).$$

(f) On peut calculer les autres commutateurs et voir qu'aucun commutateur ne donne une permutation. Mais on peut aussi le voir en remarquant qu'un commutateur est une composée d'un nombre pair de permutations (on a vu que les cycles de longueur 3 sont des composées de 2 permutations). Il s'ensuit que

$$D(\mathfrak{S}_3) = \{\mathrm{Id}; (1\ 2\ 3); (1\ 3\ 2)\}.$$

Exercice 2 (Le groupe des quaternions) (5 points)

1. Avec les relations de l'énoncé, il vient (par exemple) $i * i * j = i * k = -j = (-1) * j$. Donc en utilisant j^{-1}, on trouve $i * i = -1$.
2. De la même façon, on obtient $j * j = -1$ et $k * k = -1$. D'où finalement la table de $*$,

x \ x'	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

$x * x'$

dont on admirera la belle structure en carrés 2*2 ...

3. Les symétriques se lisent dans la table : dans la ligne du i, on repère le 1, dont la colonne est celle de $-i$, qui est donc i^{-1}. On peut aussi le voir en multipliant $i * i = -1$ par -1. De même pour j et k. Ainsi $x^{-1} = -x$, pour $x = i, j, k$.
4. Pour obtenir les sous-groupes de $\mathbb{H}_8$, on commence par déterminer les sous-groupes engendrés par -1, i, j et k. On trouve facilement :

$$\begin{aligned} < -1 > &= \{1; -1\} \\ < i > &= \{1; i; -1; -i\} \\ < j > &= \{1; j; -1; -j\} \\ < k > &= \{1; k; -1; -k\} \end{aligned}$$

   $\mathbb{H}_8$ n'a pas d'autre sous-groupe non trivial, puisque $< i, j >=< i, k >=< j, k >= \mathbb{H}_8$.
5. $< -1 >$ est évidemment distingué puisque ses éléments commutent avec tous les éléments de $\mathbb{H}_8$.
   Pour les autres sous-groupes, on peut remarquer que $x * y = -(y * x)$ pour tout couple (x, y) d'éléments de $\mathbb{H}_8$ qui ne commutent pas. Par suite, pour deux éléments x et y qui ne commutent pas, on trouve

$$x * y * x^{-1} = -(x * y * x) = x * x * y = -y$$

   Ceci implique que les sous-groupes de $\mathbb{H}_8$ sont distingués.
   scolie : cette situation est exceptionnelle [1], par exemple, dans $\mathfrak{S}_3$, le sous-groupe $< (1,\ 2) >$ n'est pas distingué. Sur cet exemple, on voit aussi que ce n'est pas parce qu'un sous-groupe est commutatif qu'il est distingué ...

Exercice 3 (arithmétique variée) (5 points)

1. Comme $\text{pgcd}(2, 27) = 1$, 2 est inversible dans l'anneau $\mathbb{Z}/27\mathbb{Z}$. On obtient son inverse en cherchant une relation de Bézout entre 2 et 27. Ici l'algorithme d'Euclide aboutit en un coup : $27 = 2 * 13 + 1$. Et donc, en calculant modulo 27, il vient $2 * (-13) = 1$, soit $2^{-1} = -13 = 14$.
2. Calculons modulo 11. On a $12 = 1$, et donc aussi $12^{2011} = 1$. En parculier, 12^{2011} n'est pas multiple de 11.
3. Il suffit de remarquer que $3^{2n} = 9^n$, et de calculer modulo 7 :

$$3^{2n} - 2^n = 9^n - 2^n = 2^n - 2^n = 0$$

   ce qui prouve que $3^{2n} - 2^n$ est divisible par 7, pour tout $n \in \mathbb{N}$.
4. **Une faille bien connue de RSA** :
   Raoul ignore les clefs privées d_A et d_B, mais connait N et les clefs publiques e_A et e_B. Si ces dernières sont premières entre elles comme le dit l'énoncé, Raoul pense immédiatement à l'algorithme d'Euclide étendu qui lui permet de calculer une relation de Bézout, soit des entiers $a, b \in \mathbb{Z}$ tels que

$$ae_A + be_B = 1.$$

   S'il réussit à intercepter les messages (cryptés) m_A et m_B, il pourra calculer

$$m_A^a m_B^b = (m^{e_A})^a (m^{e_B})^b = m^{ae_A + be_B} = m \quad [N]$$

1. En fait, je ne connais pas d'autre groupe non commutatif dont tous les sous-groupes sont distingués ; alors si vous avez d'autres exemples, je suis preneur ...