Théorie des groupes

Correction feuille 2

Exercice 1

1. Morphisme : $f(a+b) = a+b+a^t+b^t = f(a)+f(b)$. $\ker f = \{a = -^t a\} = A_n$. $\mathrm{Im}(f) = S_n(f)$.
2. Non-morphisme : $PourA = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix}$, on obtient $f(AB) \neq f(A)f(B)$.
3. Morphisme : $det(ab) = det(a)det(b)$. $\ker(f) = \mathrm{SL}_n(\mathbb{R})$. $\mathrm{Im}(f) = \mathbb{R}^*$. Donc f surjectif.
4. Morphisme : $|zz'| = |z|\,|z'|$. $\ker(f) = \mathbb{U}$. $\mathrm{Im}(f) = \mathbb{R}_+^*$.

Exercice 2 $\phi : G_1 \to G_2$ morphisme de groupe.
Soit $g \in G_1$ d'ordre n. Alors $g^n = e_1$.

$$\phi(g)^n = \phi(g^n) = \phi(e_1) = e_2.$$

Donc l'ordre de $\phi(g)$ divise n.

Exercice 3 On note H ce groupe. Montrons que $H = \mathbb{Q}_+^*$. On a bien sur $H \subset \mathbb{Q}_+^*$ car les premiers sont rationnels.

Soit $x \in \mathbb{Q}_+^*$. Alors $x = \frac{p}{q}$ avec $p, q \in \mathbb{N}$. Soient $p = \prod_1^s p_i^{\alpha_i}$ et $q = \prod_1^t q_i^{\beta_i}$ les décompositions respectives en facteurs premiers de p et q. Pour tout i de 1 à s, $p_i \in H$ donc $p_i^{\alpha_i} \in H$. Et donc $p \in H$. De même, pour tout i de 1 à t, $q_i \in H$ donc $q_i^{\beta_i} \in H$. Et donc $q \in H$ et $\frac{1}{q} \in H$.

D'où $x \in H$. Cela montre que $\mathbb{Q}_+^* \subset H$. D'où $H = \mathbb{Q}_+^*$.

Exercice 4 Soit g d'ordre 2 dans G_1. L'ordre de $\varphi(g)$ divise l'ordre G_2 par le théorème de Lagrange. Donc est impair. Or par l'exercice 2, l'ordre de $\varphi(g)$ divise 2. Donc $\varphi(g) = e$. Tous les générateurs de G_1 sont d'image triviale donc φ est constante égale à e_{G_2}.

Exercice 5 (a) Si l'ordre de g est fini égal à n : $(g^{-1})^n g^n = e$. Comme $g^n = e$, $(g^{-1})^n = e$. Donc $ord(g^{-1})$ divise $ord(g)$. En appliquant cela à g^{-1}, on obtient que $ord(g^{-1})$ divise $ord(g)$. D'où l'égalité. $g \mapsto hgh^{-1}$ est un automorphisme, donc préserve l'ordre par exercice 2.
Si l'ordre de g est infini, alors l'ordre de g^{-1} ne peut être fini (cela contredirait le point précédent). Donc $ord(g^{-1}) = \infty$. Même raisonnement pour hgh^{-1}, qui est forcément d'ordre infini.

(b) On applique que g et hgh^{-1} ont le même ordre à $g' = gh$, ce qui donne directement le résultat.

(c) On pose m l'ordre de g. Alors :

$$m = min\{k \in \mathbb{N},\ (g^n)^k = e\}.$$

$$m = min\{k \in \mathbb{N},\ m \mid kn\}.$$

$$m = \frac{1}{n} min\{k \in \mathbb{N},\ m \mid k \text{ et } n \mid k\}.$$

$$m = \frac{\mathrm{ppcm}(n, m)}{n}.$$

(d) On note a l'ordre de gh. on effectue les divisions euclidiennes de a par n et m.

$$a = pn + r, \quad 0 \leq r < n.$$

$$a = qm + s, \quad 0 \leq s < m.$$

Alors $e = (gh)^a = g^r h^s$. Si $r \neq 0$ et $s \neq 0$, alors $g^r = h^{-s}$, ce qui contredit que $< g > \cap < h >= \emptyset$. Donc $r = 0$ ou $s = 0$. Si $r = 0$ alors $h^s = e$ et donc $s = 0$ (car $s < m =$ordre(h). De même si $s = 0$ alors $r = 0$.
On a donc que $n \mid a$ et $m \mid a$. Donc $\mathrm{pgcd}(n, m) \mid a$. Réciproquement, $(gh)^{\mathrm{pgcd}(n,m)} = e$, d'où $a = \mathrm{pgcd}(n, m)$.

Exercice 6 Notons g un élément générateur de G. On a $G =< g >$. Si G est infini, alors $\varphi : \begin{array}{ccc} G & \to & \mathbb{Z} \\ g^n & \mapsto & n \end{array}$ est un isomorphisme. Soit H un sous-groupe de G. Alors $\varphi(H) = K$ est un sous-groupe de $\mathbb{Z}$, donc est de la forme $k\mathbb{Z}$ avec k un entier naturel. Donc $H = \varphi^{-1}(K) =< g^k >$ est bien monogène.

Si G est fini d'ordre n, alors $\varphi : \begin{array}{ccc} G & \to & \mathbb{Z}/n\mathbb{Z} \\ g^k & \mapsto & k \end{array}$ est un isomorphisme. Soit H un sous-groupe de G. Alors $\varphi(H) = K$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, donc est de la forme $k\mathbb{Z}/n\mathbb{Z}$ avec k un entier naturel. Donc $H = \varphi^{-1}(K) =< g^k >$ est bien monogène.

Si m divise n, alors $< g^{\frac{n}{m}} >$ est un sous-groupe d'ordre m de G.

Exercice 7 Soit $\phi \in \mathrm{Aut}(\mathbb{Z})$. On pose $A = \phi(1)$. On a alors que pour tout x dans $\mathbb{Z}$, $\phi(x) = x.A$. 1 n'a un antécédent que dans les cas $A = 1$ et $A = -1$. Réciproquement, Id et $-Id$ sont bien des automorphismes de $\mathbb{Z}$.

D'où $\mathrm{Aut}(\mathbb{Z}) = \{Id, -Id\}$.

Exercice 8 Soit G un groupe tel que $\mathrm{Aut}(G) = \{e\}$. On veut montrer que G est d'ordre au plus deux.

1. Soit $h \in G$. On sait que $h \mapsto hgh^{-1}$ est au automorphisme. C'est donc l'identité. C'est à dire que pour tout $g \in G$, $hgh^{-1} = g$. Et donc $hg = gh$.
2. $g \mapsto g^{-1}$ est toujours bijective. Comme G est abélien, $(gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1}$ pour tout h et g. $g \mapsto g^{-1}$ est donc un automorphisme.
3. Comme le seul automorphisme de G est l'identité, on en déduit que $g \mapsto g^{-1}$ est l'identité, c'est à dire que chaque élément est son propre inverse, ce qui revient à dire que tous les éléments sont d'ordre 1 ou 2. On peut donc munir G d'une loi de composition externe par $\mathbb{Z}/2\mathbb{Z}$: $(\lambda \in \mathbb{Z}/2\mathbb{Z}, g \in G) \mapsto \lambda.g$. La seule condition délicate à vérifier est que $(\lambda + \mu)x = \lambda x + \mu x$ pour tout $x \in G$ et tous $\lambda, \mu \in \mathbb{Z}/2\mathbb{Z}$. C'est le fait que tous les éléments soit d'ordre 1 ou 2 qui nous l'assure.
4. Soit $\phi \in GL(V)$. Alors ϕ est en particulier inversible et est un morphisme de groupe donc est un automorphisme. Si V était de dimension 2 ou plus, il existerait au moins un changement de base formant un automorphisme non-trivial, ce qui contredirait notre hypothèse. Donc $dim_{\mathbb{Z}/2\mathbb{Z}}(V) =$ 0 ou 1. Et donc G est de cardinal 1 ou 2.

Exercice 9 Il faut choisir le bon ensemble de générateurs sur lequel raisonner.

Propositon : S_n est engendré par $\{(1i), \quad 2 \leq i \leq n\}$.

Preuve : Soit $(a_1 a_2 \dots a_k)$ un cycle de S_n. Alors :

$$(a_1 a_2 \dots a_k) = (a_n a_{n-1})(a_n a_{n-2}) \dots (a_n a_1).$$

$$(a_1 a_2 \dots a_k) = [(1a_n)(1a_{n-1})(1a_n)]\,[(1a_n)(1a_{n-2})(1a_n)] \dots [(1a_n)(1a_1)(1a_n)]\,.$$

Donc les cycles sont engendrés par les transpositions de la forme $(1i)$. Comme tout élément de S_n peut-être décomposé en produit du cycles, on obtient que S_n tout entier est engendré par $\{(1i), \quad 2 \leq i \leq n\}$.
□

$\varphi((12))$ est d'ordre 1 ou 2. Et donc $\varphi((12)) = \pm 1$. Soit $j \in [\![3, n]\!]$. $(1j) = (2j)(12)(2j)$. Alors $\varphi((1j)) = \varphi((2j))\varphi((12))\varphi((2j))$. On est dans $\mathbb{C}^*$ donc les éléments commutent, et $\varphi((2j))$ est d'ordre 1 ou 2. On a donc $\varphi((1j)) = \varphi((12))$. Tous les $(1j)$ ont donc la même image : 1 ou -1, et l'image de tout élément de S_n est alors entièrement déterminée.

On en déduit qu'il y a au plus 2 morphismes de S_n dans $\mathbb{C}^*$. On connait le morphisme trivial et la signature, qui sont distincts, ce sont donc les 2 morphismes en question.

$\mathrm{Hom}(S_n, C^*) = \{e, \varepsilon\}$.

Exercice 10 φ est non-constante, donc il existe $a \in G$ tel que $\varphi(a) \neq 1$.

$x \mapsto ax$ est bijective, donc on peut réécrire notre somme :

$$\begin{aligned}\sum_{x \in G} \varphi(x) &= \sum_{x \in G} \varphi(ax) \\ &= \sum_{x \in G} \varphi(a)\varphi(x) \\ &= \varphi(a) \sum_{x \in G} \varphi(x)\end{aligned}$$

Comme $\varphi(a) \neq 1$, on a bien que $\sum\limits_{x \in G} \varphi(x) = 0$

Exercice 11 (Groupe quasi-cyclique de Prüfer)

— G_p est stable par inverse car si $z \in G_p$, z^1 est une racine de l'unité de même ordre que z.
Soit y et z dans G_p avec k et k' leurs ordres. Alors $(yz)^(max(k, k')) = 1$. Donc G_p est stable par produit et c'est bien un sous-groupe de $\mathbb{C}^*$.

— On va "découper" G_p en tranches successives :
Soit $U_k = \{z, \quad z^{p^k} = 1\}$ pour tout $k \in \mathbb{N}$. Alors $U_k \subset U_{k+1}$ pour tout k et $G_p = \cup_{n \in \mathbb{N}} U_k$. il est facile de vérifier que U_k est un sous-groupe de G_p.
Soit H un sous-groupe propre de G_p. On pose $k = max\{l \mid U_l \subset H\}$. Ce max existe car H est propre.
Pour tout $l > k$. Soit $x \in U_l \setminus U_k$. Alors x est une racine primitive p^m-ième de l'unité avec $m > k$ (sinon on aurait $x \in U_k$). Donc $U_m / subset < x >$. Or $U_m \not\subset H$ par minimalité de k. Donc $x \notin H$ et $H \subset U_k$.
Au final : $H = U_k$, qui est bien cyclique (engendré par $exp(\frac{2i\pi}{p^k})$) et non-maximal car strictement inclus dans U_{k+1}.

— Supposons que G_p puisse être engendré par une famille finie d'éléments. Notons $g_1, \ldots, g_k$ ces éléments et pour tout $i \leq k$, on note n_i un entier tel que $g_i^{n_i} = 1$. Alors en posant $N = max\{n_i \mid i \in [\![1, 1k]\!]\}$, on a que $g_i^{p^N} = 1$. D'où $< g_1, g_2, \ldots, g_k > \subset U_N$ et $G_p \subset U_N$, ce qui est absurde.
G_p ne peut pas être engendré par une famille finie d'éléments.