Théorie des groupes

Corrigé Feuille 6

Exercice 1 1. Soit $\phi : \begin{array}{ccc} \mathbb{R} & /to & \mathbb{U} \\ \theta & \mapsto & e^{2i\pi\theta} \end{array}$. ϕ est un morphisme surjectif avec : $\ker\phi = \mathbb{Z}$. Par le premier théorème d'isomorphisme, on a : $\mathbb{R}/\mathbb{Z} \cong \mathbb{U}$.

2. Soit $\psi : \begin{array}{ccc} \mathbb{C}* & /to & \mathbb{R}_+* \\ z & \mapsto & |z| \end{array}$. ψ est un morphisme surjectif avec : $\ker\psi = \mathbb{U}$. Par le premier théorème d'isomorphisme, on a : $\mathbb{C}*/\mathbb{U} \cong \mathbb{R}_+*$.

Exercice 2 On note $\pi : G \to G/N$ l'injection canonique dans le quotient. Alors $\pi(H)$ est un sous-groupe de G/N et donc $ord(\pi(H))$ divise n par théorème de Lagrange.

On note $\pi' = \pi\,|_H^{\pi(H)}$. C'est évidement un morphisme surjectif auquel on peut appliquer le premier théorème d'isomorphisme. $\pi(H) \cong H/\ker(\pi')$. On en déduit que $ord(\pi(H)) \mid ord(H) = s$. L'ordre de $\pi(H)$ divise donc s et n qui sont premiers entre eux, donc $ord(\pi(H)) = 1$, ce qui signifie que $H \subset N$.

Exercice 3 1.

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & c+c'+ab \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} = Id_3$$

Γ est non-vide, stable par produit et inversion donc est un sous-groupe de $GL_3(K)$.

2. $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ commute avec toute matrice $\begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix}$ si et seulement si pour tout a' et b' dans K, on a $ab' = a'b$. Cela équivaut à $a = b = 0$. D'où $Z(G) = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid c \in K \right\}$.

3. Soit $\varphi : \begin{array}{ccc} \Gamma/Z(\Gamma) & \to & k \times K \\ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} & \mapsto & (a,b) \end{array}$. C'est un morphisme par formule de la question 1.

Premier théorème d'isomorphisme avec $\ker\phi = Z(\Gamma) : \Gamma/Z(\Gamma) \cong K \times K$.

Exercice 4 Soit $x \in F$ et $\alpha \in Aut(F)$.
$h\alpha(x)h^{-1} = /alpha(/alpha^{-1}(h)x\alpha^{-1}(h)^{-1})$.
Comme x est dans F, $\{/alpha^{-1}(h)x\alpha^{-1}(h)^{-1}\}$ est fini. Donc $\alpha(x) \in F$.
On en déduit que $\alpha(F) \subset F$. En appliquant cela à α^{-1}, on a aussi que $F \subset \alpha(F)$.

Exercice 5 (Classification des groupes d'ordre $2p$, p premier)

1. On note $H = \{e, a, \dots, a^{n-1}, b, ab, \dots a^{n-1}b\}$.
   $abab = e$ donc $aba = b$. On a aussi que $a^{n-1} = a$ et $b = b^{-1}$.
   Soit x un élément de G : Alors il s'écrit sous la forme $b^{\alpha}a^{i_1}ba^{i_2}ba^{i_3}\dots a^{i_{k-1}}ba^{i_k}b^{\epsilon}$ avec $\alpha, \epsilon \in \{0, 1\}$ et pour tout j de 1 à k, $i_j \in \mathbb{N}$.
   Comme $ba = a^{n-1}b$, on peut supposer que $\alpha = 0$. D'où :

$$\begin{aligned} x &= a^{i_1}ba^{i_2}ba^{i_3}b\dots a^{i_{k-1}}ba^{i_k}b^{\epsilon} \\ &= a^{i_1}a^{i_2(n-1)}ba^{i_3}b\dots a^{i_{k-1}}ba^{i_k}b^{\epsilon} \\ &= a^{i_1}a^{i_2(n-1)}a^{i_3(n+1)}b\dots a^{i_{k-1}}ba^{i_k}b^{\epsilon} \\ &\vdots \\ &= a^{i_1+i_2(n+1)+i_3(n+1)+\dots i_k(n+1)}b^{\epsilon} \end{aligned}$$

   Donc $x \in H$. Et $G \subset H$.
   Reste à montrer que les $2n$ éléments sont tous deux à deux distincts. les a^i sont bien sur deux à deux distincts. De même pour les a^ib.
   Si $a^i = a^jb$. Si $i = j$, alors $b = e$. Absurde. Donc $b = a^{i-j}$ est une puissance de a. Notons $k = i - j$. Alors $a^{2k} = b^2 = e$. Or, $a^{2k+2} = abab = e$. Donc $a^2 = e$. Donc $b = e$ ou $b = a$ (et alors $ab = e$). Absurde. Tous les éléments sont bien distincts, et on a donc $G = \{e, a, \dots, a^{n-1}, b, ab, \dots a^{n-1}b\}$.

2. $e.x = x$ pour tout x.
   $a^i.a^j = a^{i+j \mod n}$
   $a^i.a^jb = a^{i+j \mod n}b$
   $a^ib.a^j = a^{i-j \mod n}b$
   $a^ib.a^jb = a^{i-j \mod n}$
   C'est bien la même table que D_n. Donc $\psi : \begin{array}{ccc} G & \to & D_n \\ a & \mapsto & r \\ b & \mapsto & s \end{array}$ est bien un isomorphisme.

3. Soit G un groupe d'ordre $2p$.
   (a) Si G contient un élément d'ordre $2p$, G est cyclique.
   (b) Si tous les éléments sont d'ordre 2, alors G abélien. Donc pour un x dans G, on a $< x > \lhd G$ qui est un groupe de cardinal p, dans lequel tous les éléments sont d'ordre 2. Donc $2 \mid p$. Comme p est premier, $p = 2$. il n'y qu'un seul groupe d'ordre 4, $\mathbb{Z}/2\mathbb{Z}$, qui est isomorphe à D_2.
   (c) Si l'on est pas dans les cas précédents, il existe x d'ordre p dans G. En notant $\pi : g \to G/ < x >$ la projection canonique, on considère un y dans G tel que $\pi(y) \neq e$ (existe car π surjective). Alors, l'ordre de $\pi(y)$ (qui est 2) divise l'ordre de y. Donc $o(y)) = 2$ ou $2p$. Si c'est $2p$, G est cyclique, ce qui est absurde. Donc y est d'ordre 2.
   $\ker \pi$ est un sous-groupe d'ordre 2 de G. Donc il existe y d'ordre 2 dans G.
   $< x >$ est distingué dans G donc $\varphi : z \mapsto yzy$ est un automorphisme de $< x >$. Or $< x >$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On voit alors φ comme ϕ automorphisme de $\mathbb{Z}/p\mathbb{Z}$. Tout automorphisme de $\mathbb{Z}/p\mathbb{Z}$ vérifie $\phi(1)^2 = \phi(\phi(1))$. De plus $\varphi \circ \varphi = Id$, donc $\phi\phi(1) = 1$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, 1 admet exactement deux racines : -1 et 1. Donc $\Phi = \pm Id$. Donc $\varphi = Id$ ou $\varphi : z \mapsto z^{-1}$.
   Si $\phi = Id$: Alors $yxy = x$, donc x et y commutent et xy est un élément d'ordre $2p$. Absurde.
   Donc $\phi = -Id$ et $yxy = x^{-1}$, c'est à dire $(xy)^2 = e$. Donc xy est d'ordre 2.
   $< x, y >$ est un groupe de cardinal au moins $p + 1$, car il contient $< x >$ et y. Comme son cardinal doit diviser $2p$, c'est $2p$. D'où $< x, y >= G$.
   D'après la propriété démontrée au début, $G \cong D_n$.
   (d) Soit G est cyclique d'ordre $2p$ et isomorphe à $\mathbb{Z}/2p\mathbb{Z}$, soit G est isomorphe à D_p.

Exercice 6 (Une première action de groupe) 1. φ_x a pour inverse $\varphi_{x^{-1}}$.

2. Trivial
3. $\ker \Phi$ est le groupe que l'on recherche.
   C'est bien un sous-groupe distingué de G
   Par premier théorème d'isomorphisme, $|G/\ker \Phi| = |Im\Phi| \leq n!$. Donc $\ker \Phi$ est d'indice plus petit que $n!$.
   Si $x \in \ker \Phi$, $\varphi_x = Id$ et donc $H = xH$. Donc il existe h et h' dans H tels que $h = xh'$, soit $x = hh'^{-1}$ et $x \in H$.
   D'où $\ker \Phi \subset H$.

Exercice 7
1. Non-vide (contient e)
   Neutre : e
   Inverse : Pour $x_1 \dots x_n \in L(X)$, $x_n^{-1} \dots x_1^n$ est aussi dans $L(X)$ et est son inverse.
   Associativité : moche. Soient $x, y, z \in L(X)$. On note w le plus grand préfixe de y tel que w^{-1} soit un suffixe de x (C'est la partie qui va se simplifier). On note $x = x'w^{-1}$
   De même, on note t le plus grand suffixe de y tel que t^{-1} soit un préfixe de z. On note $z = t^{-1}z'$.
   Deux cas :
   – Si $|y| \geq |w| + |t|$. Alors $y = wy't$ et
     $(x \star y) \star z =$ réduction$(x'w^{-1}wy't) \star z = (x'y't) \star z =$ réduction$(x'y'tt^{-1}z') = x'y'z'$.
     $x \star (y \star z) = x\star$ réduction$(wy'tt^{-1}z') = x \star (wy'z') =$ réduction$(x'w^{-1}wy'z') = x'y'z'$.
   – Sinon, cela signifie que w et t se chevauche dans y. On écrit alors $y = w'y't'$ tel que $w = w'y'$ et $t = y't'$. Alors $y = wt' = w't$ et
     $(x \star y) \star z =$ réduction$(x'w^{-1}wt') \star z = (x't') \star z =$ réduction$(x't't'^{-1}y'^{-1}z') = x'y'^{-1}z'$.
     $x \star (y \star z) = x\star$ réduction$(w'tt^{-1}z') = x \star (w'z') =$ réduction$(x'y'^{-1}w'^{-1}w'z') = x'y'^{-1}z'$.
   La loi de composition est donc bien associative et $L(X)$ est bien un groupe.
2. $L(\{a\}) \cong \mathbb{Z}$. (Car c'est un groupe monogène infini)
3. On pose ρ qui à tout élément $x_i \in X$ associe le mot x_i dans $L(X)$. Cette application est injective puisque deux éléments de X donne lieu à deux mots différents. Enfin, tous les éléments de $L(X)$ étant des mots en les éléments de X et X^{-1}, $L(X) =< Im(\rho) >$.
4. Commençons par étendre f à $X \cup X^{-1}$ en posant pour $x \in X$ $f(x^{-1}) = f(x)^{-1}$.
   Pour un mot $a = x_1 \dots x_n$ dans $L(X)$, on définit $\overline{f}(a)$ par : $\overline{f}(x_1 \dots x_n) = f(x_1) \dots f(x_n)$, et $f(e) = e$.
   Soient a et b deux éléments de $L(X)$. On note $w = w_1 \dots w_l$ (avec les $w_i \in X \cup X^{-1}$) le plus grand suffixe de a tel que w^{-1} soit un préfixe de b. Alors, $a = vw$, $b = w^{-1}z$ et $ab = vz$. Et on écrit $v = v_1 \dots v_k$, $z = z_1 \dots z_m$ avec les $v_i, z_i \in X \cup X^{-1}$ et $v_k \neq z_1^{-1}$.
   $\overline{f}(a)\overline{f}(b) = \overline{f}(v_1 \dots v_k w_1 \dots w_l)\overline{f}(w_l^{-1} \dots w_1^{-1} z_1 \dots z_m)$
   $\overline{f}(a)\overline{f}(b) = f(v_1) \dots f(v_k)f(w_1) \dots f(w_l)f(w_l^{-1}) \dots f(w_1^{-1})f(z_1) \dots f(z_m)$
   $\overline{f}(a)\overline{f}(b) = f(v_1) \dots f(v_k)f(z_1) \dots f(z_m)$ car $f(w_i^{-1}) = f(w_i)^{-1}$.
   $\overline{f}(a)\overline{f}(b) = \overline{f}(vz) = \overline{f}(ab)$.
   Donc $\overline{f}$ est bien un morphisme.
5. Soit G un groupe de type fini, et X une partie génératrice (finie) de G. On note f l'inclusion de X dans G.
   Par la question précédente, f se prolonge en un morphisme $\overline{f}$ de $L(X)$ dans G
   Remarquons que $\overline{(f)}$ est alors surjective. En effet, tout élément de G est un mot en les éléments de $X \cup X^{-1}$ donc est l'image du mot correspondant par $\overline{f}$.
   Le premier théorème d'isomorphisme appliqué à $\overline{f}$ nous dit alors que $L(X)/\ker \overline{f} \cong$.