Théorie des groupes

Corrigé feuille 4

Exercice 1 Par théorème de Bezout, il existe u, v tels que $|G|\,u + nv = 1$. $\forall g \in G,\ \ g^{|G|u+nv} = g$ et donc $g^{nv} = g$. En posant $\psi : g \mapsto g^v$, on a $\psi\phi = Id$. Donc ϕ est une permutation.

Exercice 2 On note $d = pgcd(n, m)$ et $H = \Gamma_n \cap \Gamma_m$.

1. On a immédiatement que $\Gamma_d \subset H$ et donc $Card(H) \geq d$
   H est un sous-groupe de Γ_n et Γ_m, donc $Card(H) \mid n$ et m. D'où $Card(H) \mid pgcd(n, m) = d$. On en déduit $Card(H) = d$ et donc $H = \Gamma_d$.
2. $pgcd(X^n - 1, X^m - 1) = \prod_{\lambda \in \Gamma_d}(X - \lambda)$ Dans $\mathbb{C}[X]$. Toute division euclidienne dans $\mathbb{R}[X]$ est aussi une division euclidienne dans $\mathbb{C}[X]$. Par unicité de la division euclidienne, on en déduit que le pgcd est le même.

Exercice 3 $\Rightarrow$: Soit H un sous-groupe de G. Alors par théorème de Lagrange, $|H| \mid |G|$, donc $|H| = 1$ ou p.

$\Leftarrow$: Soit $y \in G \setminus \{e\}$. $< y > \neq < e >$, donc $< y > = G$ et donc G est monogène.

Si G est infini, alors il est isomorphe à $\mathbb{Z}$ donc admet des sous-groupes propres non-triviaux. C'est absurde, G est donc fini et cyclique.

Si $|G|$ n'est pas premier, on a $|G| = k_1 k_2$ avec $k_1, k_2 \neq 1$. Alors $< y^{k_1} >$ est un sous-groupe d'ordre k_2, ce qui est absurde. Donc G est d'ordre premier.

Exercice 4 (Groupes abéliens d'ordre *pq*) Soit G un groupe d'ordre pq.

Supposons que G n'admet pas d'élément d'ordre pq.

Supposons que tous les éléments non-neutres sont d'ordre p. Soit g un tel élément. Alors le groupe quotient $G/ < g >$ est d'ordre q premier donc est cyclique. Soit $h \in G$ tel que $\overline{h}$ soit un générateur de $G/ < g >$. Alors $\overline{h}$ est d'ordre q. Or, h est d'ordre p donc $ordre(h) \mid p$, c'est à dire $q \mid p$. C'est absurde.

De la même façon, il est absurde que tous les éléments soient d'ordre q. Donc il existe un élément d'ordre p et un élément d'ordre q. Alors le produit de ces deux éléments est d'ordre pq. Absurde.

Donc G admet un élément d'ordre pq et est cyclique.

Exercice 5

Première possibilité : Dans $Isom(\mathbb{R}^2)$. Soit g la symétrie de $\mathbb{R}^2$ par rapport à l'axe des abscisses. On fixe $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Soit h la symétrie par rapport à l'axe faisant un angle $2\pi\alpha$ avec l'axe des abscisses. g et h sont des éléments d'ordre 2 dont le produit gh est la rotation de centre O et d'angle 2α qui est d'ordre infini.

Autre possibilité : Dans $\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}})$.

On note $g : (u_n) \mapsto (v_n)$ avec $v_n = u_{n+1}$ si n est pair et $v_n = u_{n-1}$ si n est impair.

On note $h : (u_n) \mapsto (v_n)$ avec $v_n = u_{n-1}$ si n est impair et $v_n = u_{n+1}$ si n est pair.

Ces deux éléments sont d'ordre 2. gh est l'application $(u_n) \mapsto (u_{n-2})$ qui est d'ordre infini.

Exercice 6 Soit $\varphi \in \mathrm{Aut}(\mathbb{Z}/6\mathbb{Z})$. 1 est un générateur de $\mathbb{Z}/6\mathbb{Z}$ donc φ est entièrement déterminé par $\varphi(1)$ et est en fait la multiplication par $\varphi(1)$. φ étant un automorphisme, il conserve l'ordre, donc $\varphi(1)$ est d'ordre 6. Les seuls éléments d'ordre 6 de $\mathbb{Z}/6\mathbb{Z}$ sont ceux qui sont premiers avec 6, c'est à dire 1 et $5 = -1$.

Réciproquement, Id et $-Id$ sont bien deux automorphismes distincts de $\mathbb{Z}/6\mathbb{Z}$.

D'où $\mathrm{Aut}(\mathbb{Z}/6\mathbb{Z}) = \{Id, -Id\}$.

Exercice 7 On note $\{x_i,\ \ i \in [\![1, s]\!]\}$ une famille de représentants des classes à droites de G mod K.

1. Soient $x, y \in H$. On note $\hat{x}$ et $\hat{y}$ leurs classes à gauches respectives modulo $H \cap K$.
   Si $\hat{x} \neq \hat{y}$, alors $x^{-1}y \notin H \cap K$. Comme on sait que $x^{-1}y \in H$, on a forcément $x^{-1}y \notin K$, c'est à dire que les classes à gauche de x et y modulo K sont différentes.
   Il y a donc moins de classes d'équivalence à gauche dans H modulo $H \cap K$ que dans G mod K, ce qui est le résultat recherché.

2. Si $G = HK$, $G = \cup_{h\in H} hK$. On peut alors choisir dans H une famille de représentants des classes à gauche de $GmodK$. Notons $\{h_1, \dots, h_l\}$ avec $l = [G : K]$.

$$G = \bigsqcup_{i=1}^{l} h_i K.$$

$$G \cap H = \bigsqcup_{i=1}^{l} (h_i K \cap H) = \bigsqcup_{i=1}^{l} h_i (K \cap H).$$

Et donc $[G : K] = [H : H \cap K]$.

Vérifions que $(h_i K \cap H) = h_i(K \cap H)$:

– Soit $x \in h_i K \cap H$. Alors $x = h_i k = h$ avec $h \in H$ et $k \in K$. Donc $k = h h_i^{-1} \in H \cap K$. On a bien $x \in h_i(K \cap H)$.

– Soit $x \in h_i(K \cap H)$. Alors $x = h_i g$ avec $g \in H \cap K$. On a donc $x \in H$ et $x \in h_i K$.

3.

$$[G : H]\,[G : K] = [H : H \cap K]\,[K : H \cap K]\,.$$

$$[G : H]\,[G : K] = \frac{[G : H \cap K]}{[G : H]}\,\frac{[G : H \cap K]}{[G : K]}.$$

$$[G : H]^2\,[G : K]^2 = [G : H \cap K]^2\,.$$

Comme les indices sont tous positifs, on a le résultat.

Exercice 8 (Sous-groupes de type fini)

1. Soit $(i, j) \in [\![1, 2n]\!] \times [\![1, m]\!]$. Les classes à droites forment une partition de G, donc il existe un unique $k \in [\![1, m]\!]$ tel que $g_j x_i \in H g_k$.
   Donc il existe un unique $h_{i,j} \in H$ tel que $g_j x_i = h_{i,j} g_k$.
2. $\{h_{i,j},\ (i, j) \in [\![1, 2n]\!] \times [\![1, m]\!]\} \subset H$ donc $< h_{i,j}\ (i, j) \in [\![1, 2n]\!] \times [\![1, m]\!] > \subset H$.
   Soit $a \in H$. Comme $\{x_1, \dots, x_{2n}\}$ engendre G :

$$a = x_{i_1} \dots x_{i_l}.$$

$$a = e_G x_{i_1} \dots x_{i_l}.$$

$$a = h_{i_1,j_1} g_{k_1} x_{i_2} \dots x_{i_l}.$$

$$a = h_{i_1,j_1} h_{i_2,j_2} g_{k_2} x_{i_3} \dots x_{i_l}.$$

$$\vdots$$

$$a = h_{i_1,j_1} \dots h_{i_l,j_l} g.$$

   Où g est un des g_j. $a \in H$ et $h_{i_1,j_1} \dots h_{i_l,j_l} \in H$, donc $g \in H$. Donc $g = e$, sinon, $Hg \cap H = \emptyset$ et $g \notin H$.

Exercice 9 (Groupe diédral infini)

On se place dans $\mathbb{R}$ espace affine euclidien, et on note $\mathcal{I}(\mathbb{R})$ l'ensemble des isométries de $\mathbb{R}$.
On note $G = \{\varphi \in \mathcal{I}(\mathbb{R});\ \ \varphi(\mathbb{Z}) = \mathbb{Z}\}$.

1. Remarque : $\tau^n \circ \sigma = x \mapsto n - x$.
   Soit $H = \{\tau^n, \tau^n \circ \sigma;\quad n \in \mathbb{Z}\}$. On a facilement que $H \subset G$.
   Soit $\varphi \in G$. On note $a = \varphi(0)$. φ est une isométrie donc conserve les distances. On en déduit que $\varphi(1) = a + 1$ ou $a - 1$. Ensuite, on connait toutes les autres images. Soit $n \neq 0, 1$. Alors $\varphi(n)$ est à distance n de a, donc est $a + n$ ou $a - n$. Comme la distance entre $\varphi(1)$ et $\varphi(n)$ doit être $n - 1$, il n'y a qu'une seule possibilité pour $\varphi(n)$.
   Si $\varphi(1) = a + 1$, alors $\varphi = x \mapsto x + n = \tau^n$. Si $\varphi(1) = a - 1$, alors $\varphi = x \mapsto n - x = \tau^n \circ \sigma$.
   Donc $G \subset H$. Et $G = H$

2. Remarque : $\sigma \circ \tau^n = \tau^{-n} \circ \sigma$.

   Pour tout $n \in \mathbb{N}$, l'inverse de τ^n est tau^{-n} et $\tau^n \circ \sigma$ est son propre inverse.

   Les deux stabilités par produit un peu compliquées :

   $\tau^n \circ \sigma \circ \tau^m \circ \sigma = \tau^{n-m}$.

   $\tau^n \circ \sigma \circ \tau^m = \tau^{n-m} \circ \sigma$.

   Comme G non-vide, c'est bien un sous-groupe de $\mathcal{I}(\mathbb{R})$

3. Ce groupe, que l'on note $K =< r, s >$ a un générateur d'ordre 2 et un d'ordre infini. Ils vérifient : $sr = r^{-1}s$.

   Pour tout $n \in \mathbb{N}$, $r^n s$ est la symétrie par rapport à l'axe faisant un angle $4\pi\alpha^n$ avec l'axe des abscisses. Comme α est irrationnel, tous ces axes sont deux à deux distincts et donc les $r^n s$ sont tous deux à deux distincts. De même, tous les r^n sont deux à distincts. Donc $\{r^n, r^n s, \ \ n \in \mathbb{Z}\} \subset < r, s >$.

   En montrant une stabilité par inverse et produit, on montre que $\{r^n, r^n s, \ \ n \in \mathbb{Z}\}$ est un sous-groupe de $\mathcal{I}(\mathbb{C})$. D'où $K = \{r^n, r^n s, \ \ n \in \mathbb{Z}\}$.

   On note $\varphi : \begin{array}{ccc} D_\infty & \to & K \\ \tau^k\sigma^l & \mapsto & r^k s^l \end{array}$ (avec $k \in \mathbb{Z}$ et $l \in \{0, 1\}$). On a bien sur que φ est surjective et que $\ker \varphi = \{e\}$. φ est un morphisme car les règles de calcul sont les mêmes. (A détailler).

   On a donc exhibé un isomorphisme.

Exercice 10 On cherche $f : \mathbb{R} \to \mathbb{C}^*$ continue telle que $f(x + y) = f(x)f(y)$ pour tout x, y dans $\mathbb{R}$.
f morphisme implique que $f(0) = 1$.

1. **Etude de** $|f|$. On note $g = |f| : \mathbb{R} \to \mathbb{R}_+^*$. g est un morphisme de groupes ($|f(x + y)| = |f(x)|\,|f(y)|$) continu.

   Soit $\frac{p}{q} \in \mathbb{Q}$. ($p$ et q entiers premiers entre eux)

   $$g(1) = g\left(\frac{1}{q} + \cdots + \frac{1}{q}\right) = g\left(\frac{1}{q}\right) \times \cdots \times g\left(\frac{1}{q}\right) = g\left(\frac{1}{q}\right)^q$$

   $g(1)$ n'a qu'une seule racine q-ième dans $\mathbb{R}_+^*$, on peut donc dire sans ambiguïté que $g(\frac{1}{q}) = g(1)^{1/q}$. Ensuite, la propriété de morphisme nous donne que $g(\frac{p}{q}) = g(1)^{\frac{p}{q}}$.

   g et $x \mapsto exp(xln(g(1)))$ coïncident donc sur $\mathbb{Q}$, qui est dense dans $\mathbb{R}$. Ces deux fonctions étant continues, elles coïncident également sur $\mathbb{R}$ tout entier.

2. **Etude de** $arg(f)$. On note $h = arg(f) : \mathbb{R} \mapsto \mathbb{R}/2\pi\mathbb{Z}$. C'est bien un morphisme ($arg(f(x + y)) = arg(f(x)f(y)) = arg(f(x)) + arg(f(y))$) continu.

   $\ker h$ est un sous-groupe de $\mathbb{R}$, donc est de la forme $a\mathbb{Z}$ avec a un réel ou bien est dense dans $\mathbb{R}$.

   Si $\ker h$ est dense dans $\mathbb{R}$, alors h et la fonction nulle coïncident sur un ensemble dense dans $\mathbb{R}$ et h est donc nulle sur $\mathbb{R}$ tout entier.

   On suppose dans la suite que $\ker h$ est non-dense. Soit alors $a \in \mathbb{R}$ tel que $\ker h = a\mathbb{Z}$.

   Si $a = 0$, h est alors un isomorphisme. Il existe donc x tel que $h(x) = \pi$. Par propriété de morphisme, $h(3x) = 3h(x) = 3\pi = \pi$. Cela contredit que h est une bijection. Donc $a \neq 0$.

   h est injective sur $[0, a[$. Sinon, il existerait x et y dans $[0, a[$ tels que $h(x) = h(y)$ et on aurait $h(x - y) = 0$ et $x - y \in \ker h = a\mathbb{Z}$ alors que $|x - y| < |a|$ (Absurde).

   h est donc une injection continue de $[0, a[$ dans $[0, 2\pi[$. h est donc strictement croissante ou strictement décroissante (pour ne pas contredire le théorème des valeurs intermédiaires). Supposons dans la suite qu'elle est strictement croissante.

   Montrons par récurrence que pour tout n entier, $h(a.2^{-n}) = \pi.2^{-(n-1)}$.
   - Initialisation $n = 1$: $h(a/2) = (1/2)h(a)[\pi]$, donc $h(a/2) = 0$ ou π. Comme on sait déjà que $h(0) = 0$ et que h est injective, on a forcément $h(a/2) = \pi$.
   - Hérédité Supposons que pour un n fixé, $h(a.2^{-n}) = \pi.2^{-(n-1)}$. Alors $h(a.2^{-(n+1)}) = (1/2)h(a.2^{-n})[\pi]$, donc $h(a.2^{-(n+1)}) = \pi.2^{-n}$ ou $\pi.(1 + 2^{-n})$. Comme on sait que h est strictement croissante, on doit avoir $h(a.2^{-(n+1)}) < h(a.2^{-n})$, d'où $h(a.2^{-(n+1)}) = \pi.2^{-n}$. D'où le résultat par récurrence.

Ensuite, la propriété de morphisme nous permet de calculer que :

$$\forall n \in \mathbb{N}, \quad \forall k \in [\![0, 2^{n-1}]\!], \quad h\left(\frac{ka}{2^n}\right) = \frac{k\pi}{2^{n+1}}$$

Cela signifie que h et $x \mapsto \frac{2\pi x}{a}$ coïncident sur $\left\{\frac{ka}{2^n}, \quad n \in \mathbb{N}, k \in [\![0, 2^{n-1}]\!]\right\}$ qui un ensemble dense dans $[0, a[$. Elles sont continues donc sont égales sur tout $\mathbb{R}$.

Conclusion : $arg(f)$ est une multiplication par un réel (éventuellement nul).

3. **Bilan**. En rassemblant ce que l'on sait sur son module et son argument, on obtient que :

$$f : x \mapsto |f(x)|\, e^{i.arg(f(x))} = e^{\lambda x}.e^{i\theta x} = e^{(\lambda + i\theta)x}$$

où λ et θ sont des réels. f est donc de la forme $x \mapsto e^{\alpha x}$ avec $\alpha \in \mathbb{C}$.

Il est facile de voir que réciproquement, pour tout α complexe, $x \mapsto e^{\alpha x}$ est un morphisme continu de $\mathbb{R}$ dans $\mathbb{C}^*$.

Remarquons que selon les valeurs prises par α, on peut obtenir la fonction constante égale à 1 ($\alpha = 0$), une exponentielle réelle ($\alpha \in \mathbb{R}$), un enroulement de $\mathbb{R}$ autour du cercle ($\alpha \in i\mathbb{R}$) ou une exponentielle complexe paramétrant une spirale (autres cas).