9. Exercices

On commence par quelques exercices sur les axiomes et les monoïdes.

EXERCICE 2.1. (Quelques cas où l'existence des inverses est automatique)

(i) Un monoïde M est dit régulier *si pour tout $x, y, z \in M$, on a $xy = xz \Rightarrow y = z$. Montrer qu'un monoïde régulier fini est un groupe.*

(ii) Un anneau A est dit intègre *si pour tout $a, b \in A$ on a $ab = 0 \Rightarrow a = 0$ ou $b = 0$. Montrer qu'un anneau intègre fini est à division.*

(iii) Montrer que si G est un groupe fini, et si H est une partie de G, alors H est un sous-groupe si, et seulement si, H est non vide et stable par produits.

Si M est un monoïde et $m \in M$, on pose $\langle m \rangle = \{m^n \mid n \in \mathbb{N}\}$ (sous-monoïde engendré par m). On dit que M est *monogène* s'il existe $m \in M$ tel que $M = \langle m \rangle$.

EXERCICE 2.2. *Soient $n \geq 1$ un entier et $\mathrm{F}(n)$ le monoïde des fonctions de $\{0, 1, \ldots, n-1\}$ dans lui-même pour la composition $\circ$. Pour $0 \leq i < n$, on note $f_i \in \mathrm{F}(n)$ la fonction définie par $f_i(j) = j + 1$ pour $0 \leq j < n - 1$ et $f_i(n-1) = i$.*

(i) On pose $M_i = \langle f_i \rangle$. Montrer $|M_i| = n$.

(ii) (suite) Montrer $M_i \simeq M_j \iff i = j$.

(iii) Montrer qu'à isomorphisme près, il existe exactement n monoïdes monogènes de cardinal n.

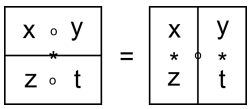
EXERCICE 2.3. (Monoïdes de cardinal ≤ 3)

(i) Montrer qu'à isomorphisme près, il existe exactement 2 monoïdes de cardinal 2, à savoir $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathbb{Z}/2\mathbb{Z}, \times)$.

(ii) Soit M un monoïde à 3 éléments. Montrer que soit M est monogène, soit on a $M \simeq (\mathbb{Z}/3\mathbb{Z}, \times)$, soit on a $x^2 = x$ pour tout $x \in M$.

(iii) En déduire qu'à isomorphisme près, il existe exactement 7 monoïdes de cardinal 3.

EXERCICE 2.4. (L'argument de Eckmann-Hilton) *Soit X un ensemble muni de deux lois unitaires $\circ$ et $\star$ avec $(x \circ y) \star (z \circ t) = (x \star z) \circ (y \star t)$ pour tout $x, y, z, t \in X$. Montrer $\circ = \star$, et que ces lois sont associatives et commutatives.*



EXERCICE 2.5. (*Sous-monoïdes de $(\mathbb{N}, +)$, partie I*)

(i) Soient $m, n \in \mathbb{N}$ premiers entre eux. Montrer que tout élément de $\mathbb{Z}$ s'écrit de manière unique sous la forme $am + bn$ avec $a, b \in \mathbb{Z}$ et $0 \leq b < m$.

(ii) (suite) En déduire que $\mathbb{N}m + \mathbb{N}n$ contient tous les entiers $> mn - m - n$, mais pas $mn - m - n$.

(iii) Soient $m_1, \ldots, m_n \in \mathbb{N}$ non nuls et premiers entre eux. Montrer qu'il existe un $r \in \mathbb{N}$ tel que $\mathbb{N}m_1 + \mathbb{N}m_2 + \cdots + \mathbb{N}m_n$ contient tous les entiers $\geq r$.

(iv) (suite) Pour $k \in \mathbb{N}$ on note f_k le nombre de n-uples $(a_1, \ldots, a_n) \in \mathbb{N}^n$ avec $k = a_1m_1 + a_2m_2 + \cdots + a_nm_n$. Montrer $f_k = \frac{k^{n-1}}{m_1 \cdots m_n} + \mathrm{O}(k^{n-2})$ pour $k \to \infty$ (Schur). On pourra examiner les pôles de la fraction rationnelle $\prod_{i=1}^{n} \frac{1}{1-z^{m_i}}$.

EXERCICE 2.6. (*Sous-monoïdes de $(\mathbb{N}, +)$, partie II*) *Un sous-monoïde M de $\mathbb{N}$ sera dit primitif si on a $M \neq \{0\}$ et si le pgcd de tous les éléments de M est 1.*

(i) Montrer qu'un sous-monoïde de $\mathbb{N}$ est primitif si, et seulement si, il contient tous les entiers $\geq r$ pour un certain $r \geq 0$.

(ii) Montrer que tout sous-monoïde de $\mathbb{N}$ est finiment engendré.

(iii) Montrer que deux sous-monoïdes primitifs de $\mathbb{N}$ isomorphes sont égaux.

(iv) En déduire qu'il existe une infinité de sous-monoïdes de $\mathbb{N}$ engendrés par 2 éléments, et deux à deux non isomorphes.

Soient M un monoïde et $x, y \in M$. On dit que y est un *inverse à droite* (resp. *inverse à gauche*) de x si on a $xy = 1$ (resp. $yx = 1$).

EXERCICE 2.7. (Neutres et inverses partiels) *Soient X un ensemble et M le monoïde des fonctions $X \to X$ pour la composition $\circ$.*

(i) Caractériser les éléments $f \in M$ ayant un inverse à droite (resp. à gauche).

(ii) Montrer que si X est infini alors M possède un élément ayant une infinité d'inverses à droite (resp. à gauche).

(iii) Montrer que dans tout monoïde, si un élément admet à la fois un inverse à droite et un inverse à gauche, alors ils sont égaux et uniques.

(iv) Caractériser les éléments $e \in M$ vérifiant $e^2 = e$. De plus, pour $e \in M$ avec $e^2 = e$, caractériser les $f \in M$ vérifiant $ef = f$ (resp. $fe = f$).

(v) Soit $e \in M$ vérifiant $e^2 = e$. Vérifier que $\circ$ induit une loi de composition associative sur eM, avec $e \in eM$ et $ex = x$ pour tout $x \in eM$. Montrer que e est un élément neutre de $(eM, \circ)$ si, et seulement si, on a $e = 1$ ou $|\mathrm{Im}\, e| = 1$.

Les exercices qui suivent portent sur les produits de parties et de groupes.

EXERCICE 2.8. *Soient G un groupe et H, K deux sous-groupes de G. On considère l'application $f : H \times K \to G$, $(h, k) \mapsto hk$. Donner une condition nécessaire et suffisante portant sur H et K pour que f soit respectivement :*

(i) un morphisme de groupes,

(ii) injective,

(iii) surjective,

(iv) un isomorphisme de groupes.

EXERCICE 2.9. *Soient G un groupe et H, K deux sous-groupes finis de G.*

(i) Montrer $|HK| = \frac{|H||K|}{|H \cap K|}$.

(ii) On suppose $|H|$ et $|K|$ premiers entre eux. Montrer $|HK| = |H|\,|K|$.

EXERCICE 2.10. *Soient G un groupe et H, K deux sous-groupes de G.*

(i) Montrer que HK est un sous-groupe de G, si et seulement si, $HK = KH$.

(ii) Donner un exemple où HK n'est pas un sous-groupe de G.

(iii) On suppose $H \lhd G$. Montrer que HK est un sous-groupe de G.

EXERCICE 2.11. *Soient G un groupe et H, K deux sous-groupes distingués avec $H \cap K = \{1\}$ et $G = HK$. Montrer que G est produit direct interne de H et K.*

EXERCICE 2.12. (Vrai ou faux) *Soient G un groupe et H, K deux sous-groupes de G avec $G = HK$. Une seule des affirmations suivantes est fausse : laquelle ?*

(i) On a $G = KH$.

(ii) Pour tout $a, b \in G$, on a $G = (aHa^{-1})(bKb^{-1})$.

(iii) Supposons $G = HL$ avec L un sous-groupe de G, ainsi que $H \cap K = H \cap L = \{1\}$, alors on a $K = L$.

EXERCICE 2.13. (Propriété universelle[12] des produits) *Soit $\{G_i\}_{i\in I}$ une famille de groupes. On pose $P = \prod_{i\in I} G_i$ (groupe produit), et pour $j \in I$, on note $\pi_j : P \to G_j, (g_i)_i \mapsto g_j$ la projection canonique. Vérifier $\pi_j \in \mathrm{Hom}(P, G_j)$ et montrer que pour tout groupe G, l'application $\mathrm{Hom}(G, P) \to \prod_{i\in I} \mathrm{Hom}(G, G_i)$, $f \mapsto (\pi_i \circ f)_i$, est bijective.*

L'exercice qui suit est un contre-exemple à la philosophie (pas si mauvaise) qui consiste à penser que tout énoncé trés général en théorie des groupes est soit faux, soit trivialement vrai, soit extrêmement difficile !

EXERCICE 2.14. *Soient G, H et K des groupes finis. On se propose de montrer que* si on a $G \times H \simeq G \times K$, alors on a $H \simeq K$. *Pour deux groupes X, Y, on notera $\mathrm{Inj}(X, Y) \subset \mathrm{Hom}(X, Y)$ le sous-ensemble des morphismes injectifs.*

(i) Montrer que pour tout groupe fini S, on a $|\mathrm{Hom}(S, H)| = |\mathrm{Hom}(S, K)|$.

(ii) En déduire que pour tout groupe fini S, on a $|\mathrm{Inj}(S, H)| = |\mathrm{Inj}(S, K)|$.

(iii) Conclure.

(iv) Donner un exemple de groupe infini G vérifiant $G \times \mathbb{Z}/2\mathbb{Z} \simeq G \simeq G \times G$.

EXERCICE 2.15. (Anneau de Boole) *Si X est un ensemble, on considère la loi Δ sur $\mathrm{P}(X)$ définie par $A \,\Delta B = (A \cup B) \smallsetminus (A \cap B)$* (différence symétrique). *Montrer que $(\mathrm{P}(X), \Delta, \cap)$ est un anneau, naturellement isomorphe à l'anneau produit $(\mathbb{Z}/2\mathbb{Z})^X$.*

On donne maintenant deux premiers exercices sur le groupe des isométries d'un espace euclidien E. On rappelle que si H est un hyperplan affine de E, et si D désigne la droite vectorielle de E orthogonale à la direction de H, la *reflexion affine* d'hyperplan H est l'isométrie τ_H de E donnée par la formule $\tau_H(h + d) = h - d$ pour tout $d \in D$ et tout $h \in H$.

12. Étant donné un groupe connu H, c'est souvent une bonne idée que d'essayer de comprendre les $\mathrm{Hom}(H, G)$ ou $\mathrm{Hom}(G, H)$ (*propriété universelle du groupe H*).

EXERCICE 2.16. (Théorème de Cartan-Dieudonné) *Soient E un espace euclidien de dimension $n \geq 1$ et $f \in \mathrm{Iso}(E)$.*

(i) Montrer que l'ensemble $\mathrm{Fix}\, f$ des points fixes de f est soit vide, soit un sous-espace affine de E.

Si $\mathrm{Fix}\, f = \emptyset$ on pose $p = -1$. Sinon, on pose $p = \dim \mathrm{Fix}\, f$.

(ii) Montrer que f est produit d'au plus $n - p$ réflexions affines (Théorème de Cartan-Dieudonné).

(iii) En déduire que f est affine : on a $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ pour tout $x, y \in E$ et $\lambda, \mu \in \mathbb{R}$ avec $\lambda + \mu = 1$.

EXERCICE 2.17. *Soit $E = \mathbb{R}$ muni de la distance (euclidienne !) usuelle. On s'intéresse au groupe $\mathrm{Iso}(1) = \mathrm{Iso}(E)$.*

(i) Décrire les réflexions affines de E.

(ii) Montrer que tout élément non trivial de $\mathrm{Iso}(1)$ est soit une translation, soit une réflexion affine.

(iii) Montrer que l'on a $\mathrm{Iso}(1) = HK$ avec H, K des sous-groupes vérifiant $H \simeq \mathbb{R}$ et $K \simeq \mathbb{Z}/2\mathbb{Z}$. A-t-on $\mathrm{Iso}(1) \simeq \mathbb{R} \times \mathbb{Z}/2\mathbb{Z}$?

Les exercices suivant traitent de la notion d'ordre d'un élément.

EXERCICE 2.18. *(i) Donner un exemple de groupe infini dont tous les éléments sont d'ordre fini.*

(ii) Donner un exemple de groupe possédant deux éléments a, b avec $a^2 = 1$, $b^2 = 1$ et ab d'ordre infini.

EXERCICE 2.19. (Cauchy abélien) *On suppose que le groupe abélien fini G est engendré par des éléments $x_1, \ldots, x_n$, avec x_i d'ordre d_i.*

(i) Montrer que $|G|$ divise $d_1 \ldots d_n$.

(ii) En déduire que si p premier divise $|G|$, alors G admet un élément d'ordre p.

EXERCICE 2.20. *Soient a et b des entiers avec $a, b \geq 3$. On pose $\zeta_n = e^{2i\pi/n}$ pour $n \geq 1$ et l'on considère les éléments A, B et U_t de $\mathrm{SL}_2(\mathbb{C})$ définis par*

$$A = \begin{pmatrix} \zeta_a & 0 \\ 0 & \zeta_a^{-1} \end{pmatrix} \quad B = \begin{pmatrix} 0 & -1 \\ 1 & \zeta_b + \zeta_b^{-1} \end{pmatrix} \quad \text{et} \quad U_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \quad \text{avec } t \in \mathbb{C}.$$

(i) Montrer que A est d'ordre a, et que B est d'ordre[13] *b, dans le groupe $\mathrm{SL}_2(\mathbb{C})$.*

(ii) On pose $B_t = U_t\, B\, U_t^{-1}$. Calculer la trace de AB_t.

(iii) On suppose $c \geq 3$ entier, ou $c = \infty$. Montrer que pour t bien choisi, le produit $A\, B_t$ est d'ordre c.

(iv) En travaillant[14] *dans $\mathbb{Z}/p\mathbb{Z}$ pour $p \equiv 1 \bmod abc$ (avec p premier), à la place du corps $\mathbb{C}$, montrer que pour tous entiers $a, b, c \geq 3$, il existe un groupe fini possédant un élément d'ordre a, un autre d'ordre b, de produit d'ordre c.*

13. Observer que si $g \in \mathrm{SL}_2(\mathbb{C})$ est de trace $x + x^{-1}$ avec $x \in \mathbb{C}^\times$, le polynôme caractéristique de g est $(X - x)(X - x^{-1})$.

14. Voir l'Exercice 2.41.

(v) Montrer que si l'on a g et h dans $\mathrm{GL}_2(\mathbb{C})$, avec g d'ordre 2, h d'ordre impair, et gh d'ordre fini, alors gh est d'ordre pair.

(vi) En se plaçant dans GL_3 ou dans le groupe quotient $\mathrm{SL}_2/\{\pm 1\}$, généraliser le (iv) à tout $a, b, c \geq 2$.

EXERCICE 2.21. (Propriétés universelles des groupes monogènes) *Soient G un groupe monogène engendré par l'élément $g \in G$ et H un groupe arbitraire. On considère l'application $\mathrm{ev}_g : \mathrm{Hom}(G, H) \to H,\ f \mapsto f(g)$ (« évaluation en g ») .*

(i) Montrer que ev_g est injective et que son image vaut H si G est infini, et $\{x \in G,\ x^N = 1\}$ si G est d'ordre $N \geq 1$.

(ii) On suppose H abélien. Montrer que ev_g est un morphisme de groupes.

Les exercices suivants portent sur les notions d'indice et de sous-groupe distingué.

EXERCICE 2.22. *Montrer que tout sous-groupe d'indice fini d'un groupe G contient un sous-groupe à la fois distingué et d'indice fini dans G.*

EXERCICE 2.23. *Soient H un sous-groupe distingué d'indice fini n de G, et $g \in G$. Montrer $g^n \in H$.*

EXERCICE 2.24. *Soient G un groupe engendré par $g_1, \ldots, g_n$, ainsi que H un sous-groupe d'indice 2. Montrer que H est engendré par les $g_i g_j$ avec $1 \leq i, j \leq n$.*

EXERCICE 2.25. *Soient G un groupe et A, B deux sous-groupes de G.*

(i) On suppose $A \subset B$. Montrer $[G : A] = [G : B]\,[B : A]$, au sens où si deux de ces trois quantités sont finies, la troisième l'est aussi, et cette égalité est vérifiée.

(ii) Soit AB/B le sous-ensemble de G/B constitué des parties de la forme aB avec $a \in A$. Montrer que AB/B est en bijection naturelle avec $A/(A \cap B)$.

(iii) Montrer que si A et B sont d'indice fini dans G, il en va de même de $A \cap B$.

(iv) On suppose A et B d'indices finis et premiers entre eux. Montrer $G = AB$.

EXERCICE 2.26. (Centre et automorphismes intérieurs) *Soit G un groupe. On pose $\mathrm{Z}(G) = \{g \in G \mid gh = hg,\ \forall h \in G\}$ (le « centre » de G).*

(i) Montrer que $\mathrm{Int} : G \to \mathrm{Aut}(G), g \mapsto \mathrm{int}_g$, est un morphisme de groupes de noyau $\mathrm{Z}(G)$.

(ii) En déduire que l'image $\mathrm{Int}(G)$ est un sous-groupe de $\mathrm{Aut}(G)$ (sous-groupe des automorphismes intérieurs), que $\mathrm{Z}(G)$ est un sous-groupe distingué de G, puis $G/\mathrm{Z}(G) \simeq \mathrm{Int}(G)$.

(iii) Montrer que $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$.

EXERCICE 2.27. *(i) Montrer que si G est un groupe tel que $G/\mathrm{Z}(G)$ est monogène, alors G est abélien.*

(ii) Examiner le cas $G = \mathrm{H}_8$.

EXERCICE 2.28. *Soit G un groupe tel que* $\mathrm{Aut}(G) = \{1\}$. *Montrer* $|G| \leq 2$.

EXERCICE 2.29. *Soient G un groupe et H une partie*[15] *de G. On pose*

$$\mathrm{N}_G(H) = \{g \in G \mid gHg^{-1} = H\} \quad \text{et} \quad \mathrm{C}_G(H) = \{g \in G \mid gh = hg,\ \forall h \in H\}$$

(respectivement, le normalisateur *de H dans G et le* centralisateur *de H dans G).*

(i) Montrer que $\mathrm{C}_G(H)$ *et* $\mathrm{N}_G(H)$ *sont des sous-groupes de G.*

(ii) Montrer que $\mathrm{N}_G(H)$ *est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.*

(iii) Montrer aussi que $\mathrm{C}_G(H)$ *est un sous-groupe distingué de* $\mathrm{N}_G(H)$, *et que* $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ *est isomorphe à un sous-groupe de* $\mathrm{Aut}(H)$.

(iv) (Exemple) On suppose $G = \mathrm{GL}_2(k)$ *avec k un corps et* $H = \{\left[\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right],\ x \in k\}$. *Déterminer* $\mathrm{C}_G(H)$ *et* $\mathrm{N}_G(H)$.

EXERCICE 2.30. *On se place dans le groupe* $\mathrm{GL}_2(\mathbb{Q})$ *et on considère l'élément* $g = \left[\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ *et le sous-groupe* $H = \{\left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right],\ n \in \mathbb{Z}\}$ *(justifier).*

(i) Vérifier $gHg^{-1} \subsetneq H$.

(ii) Vérifier que $H' := \cup_{n \geq 0}\, g^{-n}Hg^n$ *est le plus petit sous-groupe de* $\mathrm{GL}_2(\mathbb{Q})$ *contenant H tel que* $gH'g^{-1} = H'$, *puis le déterminer.*

EXERCICE 2.31. *Soient* $(G_i)_{i \in I}$ *une famille de groupes et, pour tout* $i \in I$, H_i *un sous-groupe distingué de* G_i.

(i) Monter que le sous-groupe $H = \prod_{i \in I} H_i$ *est distingué dans* $G = \prod_{i \in I} G_i$.

(ii) Montrer que le groupe G/H *est naturellement isomorphe à* $\prod_{i \in I} G_i/H_i$.

On donne maintenant quelques exercices sur les groupes usuels. On s'intéresse d'abord aux sous-groupes additifs de $\mathbb{Q}$. On notera P l'ensemble des nombres premiers, et suivant Steinitz, on appellera *super rationel* toute collection $s = (s_p)_{p \in \mathrm{P}}$, avec $s_p \in \mathbb{Z} \coprod \{+\infty\}$ pour tout $p \in \mathrm{P}$, et $s_p \geq 0$ pour tout p assez grand. On notera S l'ensemble des super rationels. On rappelle aussi, pour $p \in \mathrm{P}$, la *valuation* p-adique[16] $\mathrm{v}_p : \mathbb{Q} \to \mathbb{Z} \coprod \{+\infty\}$.

EXERCICE 2.32. (Sous groupes de $\mathbb{Q}$) *Pour tout super rationnel s, on note* $H_s \subset \mathbb{Q}$ *l'ensemble des* $x \in \mathbb{Q}$ *vérifiant* $\mathrm{v}_p(x) \geq -s_p$ *pour tout* $p \in \mathrm{P}$.

(i) Soit $s \in S$. *Vérifier que* H_s *est un sous-groupe de* $\mathbb{Q}$.

(ii) Montrer que le sous-groupe des rationels décimaux est de la forme H_s.

(iii) Soient $\lambda \in \mathbb{Q}$ *et* $s, t \in S$. *Montrer que les sous-groupes* $\mathbb{Z}\lambda$, $H_s + H_t$ *et* $H_s \cap H_t$ *sont tous de la forme* H_r *pour un certain* $r \in S$ *à déterminer.*

(iv) Montrer que tout sous-groupe de $\mathbb{Q}$ *est de la forme* H_s *pour un unique* $s \in S$.

(v) En déduire une description des sous-groupes de $\mathbb{Q}/\mathbb{Z}$.

(vii) Soient $s, t \in S$. *À quelle condition les groupes* H_s *et* H_t *sont-ils isomorphes ?*

15. En pratique, H sera souvent un sous-groupe de G.

16. Par définition, on a $\mathrm{v}_p(0) = +\infty$, et pour tout $x \in \mathbb{Q}$ non nul, $\mathrm{v}_p(x)$ est l'unique entier $m \in \mathbb{Z}$ tel que x s'écrive sous la forme $p^m a/b$ avec a et b entiers premiers à p.

EXERCICE 2.33. *(i)* (Kronecker) *Montrer que si* $\alpha \in \mathbb{R} \smallsetminus \mathbb{Q}$, *alors* $\mathbb{Z} + \mathbb{Z}\alpha$ *est dense dans* $\mathbb{R}$.

(ii) Montrer que la suite $(\cos n)_{n\geq 1}$ *est dense dans* $[-1, 1]$.

EXERCICE 2.34. *(i) Montrer que tout morphisme continu* $\mathbb{R} \to \mathbb{C}$ *est de la forme* $x \mapsto \alpha x$ *avec* $\alpha \in \mathbb{C}$. *Est-ce encore vrai sans l'hypothèse de continuité ?*

(ii) Montrer[17] *que tout morphisme continu* $\mathbb{R} \to \mathbb{C}^\times$ *est de la forme* $x \mapsto e^{\alpha x}$ *avec* $\alpha \in \mathbb{C}$.

(iii) En déduire que tout morphisme continu $\mathrm{S}^1 \to \mathbb{C}^\times$ *est de la forme* $z \mapsto z^n$ *avec* $n \in \mathbb{Z}$.

(iv) Plus généralement, montrer que tout morphisme continu $\mathbb{R} \to \mathrm{GL}_n(\mathbb{C})$ *est de la forme* $x \mapsto e^{Ax}$ *avec* $A \in \mathrm{M}_n(\mathbb{C})$.

On termine par quelques applications des groupes à la théorie des nombres.

EXERCICE 2.35. *Soit* $n \geq 1$ *un entier premier à* 10. *Montrer que la période du nombre rationnel* $1/n$ *coïncide avec l'ordre de* 10 *dans* $(\mathbb{Z}/n\mathbb{Z})^\times$.

EXERCICE 2.36. *(i) Soient* G *un groupe fini et* S, T *des parties de* G *vérifiant* $|S| + |T| > |G|$. *Montrer* $G = ST$.

(ii) (Application) *Soient* p *premier et* $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$. *Montrer que tout élément de* $\mathbb{Z}/p\mathbb{Z}$ *est de la forme* $ax^2 + by^2$ *avec* $x, y \in \mathbb{Z}/p\mathbb{Z}$.

(iii) Montrer que (i) ne vaut pas en général si l'on suppose $|S| + |T| = |G|$.

EXERCICE 2.37. *Soient* p *un nombre premier impair et* $a \in \mathbb{Z}$ *premier à* p. *On rappelle que l'on pose* $(\frac{a}{p}) = 1$ *si* a *est un carré modulo* p, *et* $(\frac{a}{p}) = -1$ *sinon (symbole de Legendre).*

(i) En utilisant l'involution $x \mapsto a/x$, *montrer* $(p-1)! \equiv -(\frac{a}{p})\, a^{(p-1)/2} \bmod p$.

(ii) En déduire $(p-1)! \equiv -1 \bmod p$ *(théorème de Wilson), ainsi que* $(\frac{a}{p}) \equiv a^{(p-1)/2} \bmod p$ *(congruence d'Euler).*

(iii) Retrouver $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ *pour tout* $a, b \in \mathbb{Z}$.

EXERCICE 2.38. (Symboles de Legendre de $-1, 2$ et 3) *Soit* p *premier impair.*

(i) Montrer que pour $p \equiv 1 \bmod 4$, *et* $x = \frac{p-1}{2}!$, *on a* $x^2 \equiv -1 \bmod p$.

(ii) En s'inspirant de l'égalité $2\, e^{2i\pi/3} = -1 + i\sqrt{3}$ *dans* $\mathbb{C}$, *montrer que* -3 *est un carré dans* $\mathbb{Z}/p\mathbb{Z}$ *si, et seulement si, on a* $p \equiv 1 \bmod 3$ *ou* $p = 3$.

(iii) En déduire une condition nécessaire et suffisante sur p *pour que* 3 *soit un carré dans* $\mathbb{Z}/p\mathbb{Z}$.

(iv) En s'inspirant de l'égalité $\sqrt{2} = e^{2i\pi/8} + e^{-2i\pi/8}$ *dans* $\mathbb{C}$, *montrer que si* $p \equiv 1 \bmod 8$ *alors* 2 *est un carré dans* $\mathbb{Z}/p\mathbb{Z}$ *(Euler).*

17. On pourra soit utiliser le *théorème de relèvement* : toute application continue $f : \mathbb{R} \to \mathbb{C}^\times$ est de la forme e^g avec $g : \mathbb{R} \to \mathbb{C}$ continue, soit montrer qu'un morphisme continu $f : \mathbb{R} \to \mathbb{C}^\times$ est automatiquement dérivable en observant, pour tout $x, \epsilon \in \mathbb{R}$, l'égalité $\int_x^{x+\epsilon} f(t)dt = f(x) \int_0^\epsilon f(t)dt$.

(v) (suite) En admettant l'existence d'un corps à p^2 éléments contenant $\mathbb{Z}/p\mathbb{Z}$, montrer que 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $p \equiv \pm 1 \bmod 8$.

On rappelle qu'un nombre premier est dit *de Fermat* s'il est de la forme $2^m + 1$ avec $m \geq 1$ (en fait, m est nécessairement une puissance de 2). Les seuls premiers de Fermat connus actuellement sont $3, 5, 17, 257$ et 65537...

EXERCICE 2.39. *Soit p un nombre premier de Fermat.*

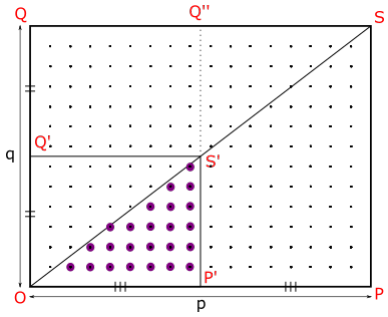
(i) Soit $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. Montrer que x engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ si, et seulement si, x n'est pas un carré.

(ii) En déduire que 3 engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ pour $p \neq 3$.

EXERCICE 2.40. (Une démonstration géométrique de la loi de réciprocité quadratique, d'après Eisenstein [18]) *Soit p un nombre premier impair et soit $q \geq 1$ un entier impair premier à p. On se propose de montrer, suivant Eisenstein, la relation*

$$\left(\frac{q}{p}\right) = (-1)^e,$$

où e est le nombre de points de coordonnées entières du triangle OP'S' ci-dessous :



(i) En déduire que pour p et q premiers impair on a $(\frac{q}{p}) = (\frac{p}{q})(-1)^{\frac{(p-1)(q-1)}{2}}$ (« loi de réciprocité quadratique »).

On suppose d'abord simplement l'entier $q \geq 1$ premier à p. On pose $X = \{2, 4, \ldots, p-1\}$ et on note $R \subset \{1, \ldots, p-1\}$ l'ensemble des restes de la division par p des qx, pour $x \in X$.

(ii) Vérifier que l'application $\{1, \ldots, p-1\} \to X$, définie par

$$r \mapsto \begin{cases} r & \text{si } r \text{ est pair,} \\ p - r & \text{sinon,} \end{cases}$$

induit une bijection de R sur X.

(iii) En déduire $(\frac{q}{p}) = (-1)^{\sum r}$, la somme portant sur les $r \in R$. (On pourra considérer le produit des éléments de X modulo p)

(iv) Vérifier que si $x \in X$, et si r est le reste de la division de qx par p, on a $r \equiv [qx/p] \bmod 2$.

18. *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste*, Crelle's Journal 28, 246–249 (1844).

(v) En déduire $(\frac{q}{p}) = (-1)^f$ *où* f *désigne le nombre des points à l'intérieur du triangle* OPS *dont les coordonnées sont entières, et d'abscisse paire.*

(vi) On suppose q *impair. Soit* A *(resp.* B*) le nombre des points à coordonnées entières et d'abscisse paire à l'intérieur du trapèze* $P'PSS'$ *(resp. du triangle* $S'SQ''$*). Montrer* $A \equiv B \bmod 2$.

(vii) En déduire la relation d'Eisenstein.

(viii) Montrer aussi $(\frac{2}{p}) = (-1)^f$ *où* f *désigne le nombre d'entiers pairs compris entre* $p/2$ *et* p*, puis* $f \equiv \frac{p^2-1}{8} \bmod 2$ *(« loi complémentaire »).*

L'exercice complémentaire suivant a été utilisé au (iv) de l'Exercice 2.20.

EXERCICE 2.41. (Théorème de Dirichlet faible) *Soit* $n \geq 1$ *un entier. On se propose de montrer qu'il existe une infinité de nombres premiers* $p \equiv 1 \bmod n$*. On considère le* n*-ème polynôme cyclotomique* $\Phi_n = \prod_{1 \leq k < n, (k,n)=1} (X - e^{2ik\pi/n})$*. C'est un polynôme unitaire de degré* $\varphi(n)$ *dans* $\mathbb{C}[X]$.

(i) Montrer $X^n - 1 = \prod_{d|n} \Phi_d$*, et en déduire*[19] $\Phi_n \in \mathbb{Z}[X]$.

(ii) Montrer que si k *est un corps dans lequel* $n.1 \neq 0$*, le polynôme* $X^n - 1$ *n'a pas de racine double dans* k.

(iii) (suite) En déduire qu'un élément $x \in k^\times$ *et d'ordre* n *si, et seulement si, on a* $\Phi_n(x) = 0$.

(iv) Montrer que pour tout polynôme $P \in \mathbb{Z}[X]$ *non constant, l'ensemble des nombres premiers divisant l'un des entiers* $P(n)$ *avec* $n \in \mathbb{Z}$*, est infini.*

(v) Conclure.

19. On rappelle que si on a $P, Q \in \mathbb{Z}[X]$ avec Q unitaire, on dispose d'une *division euclidienne* $P = AQ + B$ avec $A, B \in \mathbb{Z}[X]$ et $\deg B < \deg Q$.