MP*2 LLG
2025/2026

Feuille d'exercices : Algèbre générale

$\mathbb{Z}/n\mathbb{Z}$ et congruences

Exercice 1 *(Mines-Centrale-X-ULSR)** Soit p un nombre premier impair.

1. Dénombrer les carrés de $\mathbb{Z}/p\mathbb{Z}$.
2. Démontrer que t est un carré dans $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ si et seulement si $t^{\frac{p-1}{2}} \equiv 1 \quad [p]$.
3. En déduire que pour $p \geq 3$, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1[4]$.
4. On suppose $p \equiv -1$ [4]. Pour $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. Montrer que x est un carré si et seulement si $-x$ n'est pas un carré.
5. Soit p un nombre premier congru à -1 modulo 4. Pour tout $r \in (\mathbb{Z}/p\mathbb{Z})^*$, montrer que $\left\{(i,j) \in \left((\mathbb{Z}/p\mathbb{Z})^*\right)^2,\ i^2 - j^2 = r\right\}$ est de cardinal $p-3$·
6. On fixe $x \in \mathbb{F}_p^*$ et l'on pose $A = \left\{(\ell_1, \ell_2) \in L^2\ ;\ x = \ell_1 - \ell_2\right\}$. Calculer Card$A$.
7. Soit p premier impair quelconque. Dénombrer les $(x,y) \in (\mathbb{F}_p)^2$ tels que $x^2 + y^2 = 1$.
8. Soit $z \in \mathbb{F}_p \setminus \{0\}$. Dénombrer $\{\,(x,y) \in \mathbb{F}_p^2,\ x^2 + y^2 = z\}$.

Exercice 2 *(ENS)* Soit p un nombre premier impair. Soit $a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. On pose $m_a : x \in \mathbb{Z}/p\mathbb{Z} \mapsto ax$. Montrer que m_a est une permutation de $\mathbb{Z}/p\mathbb{Z}$, et qu'elle est de signature 1 si et seulement si a est un carré dans l'anneau $\mathbb{Z}/p\mathbb{Z}$.

Exercice 3 *(Lyon)* Soit $p \geq 5$ un nombre premier. Quand n n'est pas un multiple de p, on note n^* un entier tel que $nn^* \equiv 1[p^2]$. Montrer que : $\displaystyle\sum_{k=1}^{p-1} k^* \equiv 0\ [p^2]$.

Exercice 4 *(SR)*

1. Quels sont les inversibles de $\mathbb{Z}/n\mathbb{Z}$? De quelle structure cet ensemble est-il muni ? Quel est on cardinal ?
2. Soit $n \geq 2$ impair dont la décomposition en facteur premier est $n = \displaystyle\prod_{i=1}^{m} p_i^{\alpha_i}$. Montrer que la proportion d'éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ d'ordre pair est supérieure à $1 - \dfrac{1}{2^m}$. *On admet que, pour tout i, $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ est cyclique.*
3. Déterminer le nombre de solutions de $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$.
4. Caractériser les éléments $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ d'ordre $r = 2l$ pair tel que $g^l \neq -1$.

Exercice 5 *(X) **

1. Si $\alpha \in \mathbb{N}^*$, résoudre $x^2 = 1$ dans l'anneau $\mathbb{Z}/2^\alpha\mathbb{Z}$.
2. Pour quels $\alpha \in \mathbb{N}^*$ le groupe $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est-il cyclique ?

Exercice 6 *(Ulm)** Soit $n \geq 2$. Déterminer $(\mathbb{Z}/n\mathbb{Z})^*$. Pour quel n est-il cyclique ?

Exercice 7 *(X)**

1. Montrer qu'il existe une infinité de nombres premiers congrus à 2 modulo 3.
2. Si $(G,+)$ est un groupe abélien, une partie X de G est dite *sans somme* s'il n'existe pas de $(x,y) \in X^2$ tel que $x+y \in X$. Soit p un nombre premier de la forme $3k+2$ avec $k \in \mathbb{N}^*$. Montrer que $\mathbb{Z}/p\mathbb{Z}$ contient une partie sans somme de cardinal $k+1$.
3. Si A et B sont deux parties d'un corps fini $\mathbb{K}$, calculer $\displaystyle\sum_{x \in \mathbb{K}^*} |A \cap xB|$.
4. Soit A une partie finie de $\mathbb{Z}$. Montrer qu'il existe une partie B de A sans somme et de cardinal strictement supérieur à $\dfrac{|A|}{3}$.

Groupe symétrique

Exercice 8 *(SR)* On donne un entier $n \geqslant 2$ et, dans le groupe $\mathcal{S}_n$, on considère l'application qui à σ associe $\sigma c \sigma^{-1}$, où c désigne le cycle $(1, 2, \ldots, n)$. Déterminer l'image de cette application.

Exercice 9 *(ENS SR)** Pour $n \in \mathbb{N}^*$, on note D_n le nombre de permutations de $[\![1,n]\!]$ sans point fixe. Donner une relation entre D_{n+2}, D_{n+1} et D_n. Trouver une expression pour D_n.

Exercice 10 *(ENS-X)** Soit n un entier supérieur ou égal à 2. Le but de l'exercice est de déterminer les automorphismes de $\mathcal{S}_n$ pour $n \neq 6$.

1. Pour toute permutation $\sigma \in \mathcal{S}_n$, on note $Z(\sigma)$ l'ensemble des permutations qui commutent avec σ. Montrer que $Z(\sigma)$ est un sous-groupe de $\mathcal{S}_n$.
2. Soit $\sigma \in \mathcal{S}_n$ telle que $\sigma^2 =$ Id. Dénombrer $Z(\sigma)$.
3. Soit φ un automorphisme sur $\mathcal{S}_n$. Montrer que pour tout $\sigma \in \mathcal{S}_n$, $Z(\varphi(\sigma)) = \varphi(Z(\sigma))$.
4. Soit τ une transposition. Montrer que $\varphi(\tau)$ s'écrit comme un produit de transpositions à supports disjoints.
5. On suppose que pour toute transposition τ, $\varphi(\tau)$ est aussi une transposition. Montrer qu'il existe $\rho \in \mathcal{S}_n$ tel que, pour tout $\sigma \in \mathcal{S}_n$, $\varphi(\sigma) = \rho \circ \sigma \circ \rho^{-1}$.
6. Montrer que, si $n \neq 6$, un automorphisme du groupe $(\mathcal{S}_n, \circ)$ envoie une transposition quelconque sur une transposition. Conclure.

Exercice 11 *(Paris)** Soit G un groupe fini et soit $s \in G$. On pose, pour tout $g \in G$, $\mu_s(g) = sg$. Expliquer que μ_s est une permutation de G et déterminer sa signature (après avoir expliqué qu'elle ne dépendait pas de la numérotation des éléments de G).

Exercice 12 *(ENS)**

1. Donner le nombre minimal de permutations nécessaires pour engendrer le groupe $\mathcal{S}_n$.
2. Donner le nombre minimal de transpositions nécessaires pour engendrer le groupe $\mathcal{S}_n$.
3. On suppose que pour toute transposition τ de $\mathcal{S}_n$ et tout n-cycle c de $\mathcal{S}_n$, les permutations τ et c engendrent $\mathcal{S}_n$. Montrer que n est premier.
4. Réciproquement, montrer que si n est premier alors pour toute transposition τ de $\mathcal{S}_n$ et tout n-cycle c de $\mathcal{S}_n$, les permutations τ et c engendrent $\mathcal{S}_n$.
5. Soient $n \geq 2$ un entier, a et b deux éléments distincts de $\{1, \dots, n\}$, $G_{a,b}$ le sous-groupe de $\mathcal{S}_n$ engendré par $(a\,b)$ et $(1\,2 \dots n)$. À quelle condition a-t-on $G_{a,b} = \mathcal{S}_n$?

Exercice 13 *(SR)*

1. Soient $\sigma \in S_n$ et $c_1 \circ \cdots \circ c_r$ sa décomposition en produit de cycles à supports disjoints. Calculer l'ordre de σ dans le groupe S_n.
2. On note $g(n)$ l'ordre maximal d'une permutation de S_n.
   Montrer que g est croissante et $n \leq g(n) \leq n!$
3. Trouver n minimal tel que $g(n) > n$.
4. On note $(p_k)_{k \in \mathbb{N}^*}$ la suite strictement croissante des nombres premiers. Montrer que : $n \geq \sum_{i=1}^{r} p_i^{\alpha_i} \implies g(n) \geq \prod_{i=1}^{r} p_i^{\alpha_i}$.
5. On suppose que $g(n) = \prod_{i=1}^{r} p_i^{\alpha_i}$. Montrer que : $n \geq \sum_{i=1}^{r} p_i^{\alpha_i}$.
6. Montrer que $\forall \varepsilon > 0$, $\exists C > 0$, $\forall n \in \mathbb{N}^*$, $g(n) \leq Ce^{\varepsilon n}$.

Exercice 14 *(Ulm)* Pour $n \in \mathbb{N}^*$, on note $g(n)$ le maximum des ordres des éléments de $\mathcal{S}_n$. Montrer que $\forall k \in \mathbb{N}^*$, $\dfrac{g(n)}{n^k} \underset{n \to +\infty}{\to} +\infty$. *Question subsidiaire : Pour quels n l'entier $g(n)$ est-il impair ?*

Groupes cycliques et monogènes

Exercice 15 *(Mines)* Soit G un groupe cyclique de cardinal n. Quel est le nombre de sous-groupes de G ?

Exercice 16 *(X)* Soient G un groupe fini de neutre e et, pour d diviseur de G, $n_d(G)$ le nombre d'éléments d'ordre d de $|G|$.

1. Que vaut $\sum_{d \mid n} n_d(G)$, où $n = |G|$?
2. Calculer les $n_d(G)$ lorsque G est cyclique. Que déduire de la question précédente dans ce cas ?
3. Montrer que G est cyclique si et seulement si, pour tout diviseur d de $|G|$, l'ensemble $\{x \in G \ ; \ x^d = e\}$ est de cardinal majoré par d.
4. On suppose qu'il existe un corps $\mathbb{K}$ tel que G soit un sous-groupe de $(\mathbb{K}^*, .)$. Montrer que G est cyclique.

5. Que dire dans la situation de la question précédente si $\mathbb{K} = \mathbb{C}$?

Exercice 17 *(X-ENS)** Soit K un corps. Montrer que si G est un sous-groupe fini de K^*, alors G est cyclique. En particulier, si K est un corps fini, K^* est un groupe cyclique.

Exercice 18 *(Ulm)* Les sous-groupes stricts de $(\mathbb{Q}, +)$ sont-ils monogènes ?

Quelques éléments de théorie des groupes

Exercice 19 *(Mines-X-ENS)** Soit $(G, \cdot)$ un groupe fini dont tous les éléments sont d'ordre ≤ 2. Montrer que G est abélien. Que peut-on dire de $|G|$? Montrer que G est isomorphe à un $(\mathbb{Z}/2\mathbb{Z})^n$.

Exercice 20 *(Centrale)*

On note S une partie non vide d'un groupe multiplicatif fini G de cardinal n, contenant l'élément neutre e de G. Pour $k \in \mathbb{N}^*$, $A_k = \left\{ \prod_{i=1}^{k} s_i,\ (s_1, \ldots, s_k) \in S^k \right\}$ et $a_k = card(A_k)$.

1. Montrer que $(a_n)_{n\in\mathbb{N}^*}$ est une suite croissante.
2. Montrer que pour tout $k \geq n$, $a_{k+1} = a_k$.
3. Montrer que A_n est un sous-groupe de G.

Exercice 21 *(Mines)* Soit $(G, .)$ un groupe de neutre noté e. Soient H et K deux sous-groupes de G. On note $HK = \{hk,\ (h,k) \in H \times K\}$.

1. Montrer que HK est un sous-groupe de G si et seulement si $KH \subset HK$.
2. On définit $f : \begin{cases} H \times K & \to G \\ (h,k) & \mapsto hk \end{cases}$. Donner une condition nécessaire et suffisante pour que f soit un morphisme de groupes.
3. Soit $z = h_0k_0 \in HK$, avec $(h_0, k_0) \in H \times K$. Montrer que les antécédents de z par f sont les $(h_0t, t^{-1}k_0)$ avec $t \in H \cap K$.
4. En déduire que $\mathrm{Card}(HK)\mathrm{Card}(H\cap K) = \mathrm{Card}(H)\mathrm{Card}(K)$, et que f est injective si et seulement si $H \cap K = \{e\}$.
5. On dit que H est distingué lorsque : $\forall x \in G,\ xHx^{-1} \subset H$. On suppose H et K distingués.
   (a) Montrer que HK est un sous-groupe distingué de G.
   (b) Montrer que si $H \cap K = \{e\}$ et $HK = G$ alors G est isomorphe à $H \times K$.

Exercice 22 *(Mines)* Soient G un groupe fini et $\Omega = G^2$ que l'on munit de la probabilité uniforme.
On pose : $C = \{(x, y) \in G^2\ ;\ xy = yx\}$ et $p = \mathbf{P}(C)$.

1. Montrer que $p > 0$. Que dire si $p = 1$?
   Dans la suite, on suppose que G n'est pas commutatif.
2. Calculer p lorsque $G = \mathcal{S}_3$ puis lorsque $G = \mathcal{S}_4$.
3. On définit la relation $\sim$ sur G^2 par : $x \sim y \iff \exists g \in G, x = gyg^{-1}$. Montrer que $\sim$ est une relation d'équivalence.
4. On note s le nombre de classes d'équivalence. Montrer que : $p = \dfrac{s}{\mathrm{Card}G}$.
5. (ENS) Montrer que si G est non abélien $p \leqslant \dfrac{5}{8}$.

Exercice 23 *(X)* Soit G un groupe. Pour $(a, b) \in G^2$, on note $[a, b] = aba^{-1}b^{-1}$. On note D_G le sous-groupe de G engendré par les éléments de la forme $[a, b]$.

1. Montrer que $\forall (g, h) \in G \times D_G,\ ghg^{-1} \in D_G$.
2. Montrer que $\forall g \in G,\ g\, D_G = D_G\, g$.
3. On pose $\mathcal{Q}_G = \{xD_G \mid x \in G\}$.
   (a) Montrer que $\mathcal{Q}_G$ est une partition de G.
   (b) Montrer que la fonction $(xD_G, yD_G) \in (\mathcal{Q}_G)^2 \mapsto (xy)D_G \in \mathcal{Q}_G$ est convenablement définie et munit $\mathcal{Q}_G$ d'une structure de groupe, puis montrer que $x \in G \mapsto xD_G$ est un morphisme de G dans $\mathcal{Q}_G$.
   (c) Montrer que $\mathcal{Q}_G$ est abélien.
4. On munit $\mathbb{C}$ de sa structure canonique de plan euclidien. On suppose ici que G est le groupe des isométries vectorielles de $\mathbb{C}$ qui stabilisent $\mathbb{U}_3$. Décrire les groupes G, D_G et $\mathcal{Q}_G$.

Exercice 24 *(X)* Soit G un groupe. On note de $D(G)$ le groupe engendré par les $xyx^{-1}y^{-1}$, $x, y \in G$. On note D^n la n-ième itérée de l'opération D, et l'on dit que G est résoluble lorsqu'il existe $n \in \mathbb{N}^*$ tel que $D^n(G) = \{e\}$ où e est le neutre de G.

1. On suppose qu'il existe deux groupes H et N, deux morphismes $f : N \to G$ et $g : G \to H$ respectivement injectifs et surjectifs tels que $\ker s = \text{Im} i$. Montrer que G est résoluble si et seulement si H et N le sont.
2. Montrer que le groupe des permutations S_5 n'est pas résoluble.

Exercice 25 *(Centrale)* Soit G un groupe abélien fini de cardinal 99. Montrer que G admet un sous-groupe de cardinal 9.

Exercice 26 *(X)* Soit G un groupe fini. On suppose que G est engendré par $\{x, y\}$ où x et y sont deux éléments d'ordre 2 de G. Montrer que G contient un sous-groupe de cardinal $\dfrac{|G|}{2}$.

Exercice 27 *(X)** Soit $(G, \cdot)$ un groupe fini. Pour $g \in G$, soit τ_g l'application de G dans G définie par $\forall x \in G, \tau_g(x) = gx$.

1. Soit $g \in G$. Montrer que $\tau_g \in \mathcal{S}(G)$ et calculer la signature de τ_g.
2. On suppose que $|G| = 2^m k$ avec $m \in \mathbb{N}^*$ et k entier impair, et que G contient un élément d'ordre 2^m. Montrer que G contient un sous-groupe de cardinal $\dfrac{|G|}{2}$.

Exercice 28 *(X)** Soit G un groupe d'ordre $2n$ avec n impair.

1. Montrer que G contient un élément d'ordre 2.
2. Montrer que G contient un sous-groupe de cardinal n. *Ind.* Considérer l'application Ψ qui à $g \in G$ associe l'application $h \mapsto gh$.
3. Dans le groupe symétrique S_4, on considère $a = (123)$ et $b = (12)(34)$. Calculer aba^{-1} et bab^{-1}.
4. Le groupe alterné $\mathcal{A}_4$ contient-il un sous-groupe d'ordre $|\mathcal{A}_4|/2$?

Exercice 29 *(X)*

1. Trouver deux groupes G_1 et G_2 non isomorphes de cardinal $2023 = 7.17^2$.
2. Soit p premier. Montrer qu'un groupe de cardinal p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.
3. Soient G, H deux groupes finis et $\psi : G \to H$ un morphisme surjectif.
   Montrer que $|G| = |H| \times |\ker \psi|$.
4. On suppose que G est un groupe de cardinal 2023, que $H = \mathbb{Z}/7\mathbb{Z}$ et que $\varphi : G \to H$ est un morphisme surjectif. Montrer que G est isomorphe à $\mathbb{Z}/7\mathbb{Z} \times \ker \varphi$.
5. Montrer que tout groupe de cardinal 2023 est isomorphe à G_1 ou G_2.

Exercice 30 *(ENS)* Soient $(G, .)$ un groupe, $\text{Aut}(G)$ l'ensemble de ses automorphismes.

1. Montrer que $(\text{Aut}(G), \circ)$ est un groupe.
2. Quels sont les groupes finis tels que $\text{Aut}(G)$ soit réduit à un élément ?

Exercice 31 *(Cachan, Rennes)* Soient p un nombre premier, m un entier non divisible par p et k un entier non nul. Soit G un groupe de cardinal $p^k m$. Il s'agit de montrer que G a un sous-groupe de cardinal p^k.

1. Traiter le cas $m = 1$, puis le cas G cyclique.
2. On définit $M = \{A \subset G,\ \text{Card}(A) = p^k\}$. Montrer que p ne divise pas le cardinal de M.
3. Soit la relation d'équivalence $\sim$ sur M : $A_1 \sim A_2 \Leftrightarrow \exists g \in G, A_1 = gA_2$. Montrer qu'il existe une classe d'équivalence de cardinal non divisible par p. On prend A un représentant de cette classe.
4. Soit $H = \{g \in G,\ gA = A\}$. Montrer que H est un sous-groupe de G de cardinal p^k.

Exercice 32 *(X)* Soit G un groupe fini. Pour $x \in G$, on note $\overline{x}$ la classe de conjugaison de x :
$\overline{x} = \{gxg^{-1}\ ;\ g \in G\}$; on dit que x est ambivalent si $x^{-1} \in \overline{x}$.

1. Montrer que si une classe de conjugaison contient un élément ambivalent, alors tous ses éléments le sont.
2. Pour $x \in G$, soit $\rho(x)$ le nombre de $g \in G$ tels que $g^2 = x$. Montrer que $\dfrac{1}{|G|} \displaystyle\sum_{x \in G} \rho(x)^2$ est le nombre de classes de conjugaison ambivalentes de G.

Exercice 33 *(PLSR-Paris)* Soit G un groupe. Si X et Y sont des parties non vides de G, on pose $X^{-1} = \{x^{-1},\ x \in X\}$ et $XY = \{xy,\ (x, y) \in X \times Y\}$. Dans la suite, X désigne une partie finie non vide de G.

1. On suppose que $|XX| < 2\,|X|$. Montrer que $XX^{-1} = X^{-1}X$.
2. On suppose que $|XX^{-1}| < \dfrac{3}{2}\,|X|$. Montrer que $X^{-1}X$ est un sous-groupe de G.

3. On suppose que $|XX| < \frac{3}{2}|X|$. Montrer que $X^{-1}X$ est un sous-groupe de G.

Exercice 34 *(Paris)* Soient G un groupe et $A \subset G$ fini. Montrer l'équivalence entre

(i) $|AA| = |A|$

(ii) Il existe H sous-groupe fini de G et $x \in G$ tels que $A = xH$ et $x^{-1}Hx = H$.

Exercice 35 *(Centrale-X)** Soit $(G, .)$ un groupe abélien fini de cardinal n. On note $\widehat{G}$ l'ensemble des morphismes de groupes de $(G, .)$ dans $(\mathbb{C}^*, \times)$.

1. Montrer que l'ensemble $\widehat{G}$ est un groupe pour la multiplication ordinaire des fonctions. Donner $\widehat{G}$ pour $(\mathbb{Z}/n\mathbb{Z}, +)$.
2. Montrer que, si $\chi \in \widehat{G}$ n'est pas le morphisme trivial, $\sum_{g \in G} \chi(g) = 0$.
3. Si χ et χ' sont deux éléments distincts de $\widehat{G}$, montrer que $\sum_{g \in G} \overline{\chi(g)}\chi'(g) = 0$.
4. Montrer que $\widehat{G}$ est une partie libre de $\mathbb{C}^G$ (on procédera par récurrence). Et en déduire que $|\widehat{G}| \leq n$.
5. Si $x \in G$, soit δ_x l'élément de $\widehat{\widehat{G}}$ défini par $\forall \chi \in \widehat{G},\ \delta_x(\chi) = \chi(x)$. Montrer que $x \mapsto \delta_x$ est un isomorphisme de G sur $\widehat{\widehat{G}}$.
6. Quel est le cardinal de $\widehat{G}$?

Exemples de groupes

Exercice 36 *(ENS)** Soit p un nombre premier. On dit que G est un p-groupe si l'ordre de tout élément de G est une puissance de p.

Soit $k \in \mathbb{N}^*$. On dit qu'un groupe G est k-divisible si $\forall x \in G, \exists y \in G, x = y^k$, et qu'il est divisible s'il est k-divisible pour tout k.

1. Montrer qu'un p-groupe p-divisible non trivial est infini.
2. Montrer que $\bigcup_{n \geq 1} \mathbb{U}_{p^n}$ est un p-groupe p-divisible abélien infini. On l'appellera dans la suite $\mathbb{Z}/p^\infty\mathbb{Z}$.
3. Montrer que $\mathbb{Z}/p^\infty\mathbb{Z}$ est divisible.
4. Montrer que tout sous-groupe H propre de $\mathbb{Z}/p^\infty\mathbb{Z}$ est cyclique.
5. Soit G un p-groupe p-divisible. Montrer que G contient une copie de $\mathbb{Z}/p^\infty\mathbb{Z}$.

Exercice 37 *(Mines)* * Soient p un nombre premier et $q = (p^2 - 1)(p^2 - p)$.

1. Calculer le cardinal de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.
2. Montrer que, pour tout $A \in \mathcal{M}_2(\mathbb{Z}/p\mathbb{Z})$, $A^{q+2} = A^2$.
3. Soit $n \in \mathbb{N}^*$. Calculer le cardinal de $GL_n(\mathbb{Z}/p\mathbb{Z})$, ainsi que celui de $SL_n(\mathbb{Z}/p\mathbb{Z})$.

Exercice 38 *(Mines)** Soit $SL_2(\mathbb{Z})$ l'ensemble des matrices de $\mathfrak{M}_2(\mathbb{Z})$ de déterminant 1. Montrer que $SL_2(\mathbb{Z})$ est un sous-groupe de $GL_2(\mathbb{R})$. Montrer que les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ engendrent ce groupe.

Exercice 39 *(Ulm)* On considère $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ a \equiv d \equiv 1 - c \equiv 1[3] \right\}$. Montrer que G est le sous-groupe engendré par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$.

Exercice 40 *(X)*

1. Montrer que $\mathrm{SL}_2(\mathbb{Z})$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.
2. Soit P l'ensemble des $z \in \mathbb{C}$ tels que $\mathrm{Im}(z) > 0$. Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans $\mathrm{SL}_2(\mathbb{Z})$ et si z est dans P, montrer que $M.z = \dfrac{az + b}{cz + d}$ est dans P.
3. Montrer que, si M et M' sont dans $\mathrm{SL}_2(\mathbb{Z})$ et z dans P, $M'.(M.z) = M'M.z$.
4. Soient $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, G le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ engendré par S et T. Montrer que, si $z \in P$, il existe $M \in G$ tel que, si $z' = M.z$, on ait $|z'| \geq 1$ et $|\mathrm{Re}(z')| \leq \dfrac{1}{2}$.

Exercice 41 *(PLSR)*

1. Soient $n \geq 3$ et $\mathcal{Q}$ un polygone régulier à n côtés. Montrer que l'ensemble des isométries affines du plan préservant $\mathcal{Q}$ est un groupe à $2n$ éléments.
2. On note maintenant $n = q$, nombre premier impair, et D_{2q} le groupe précédent. Montrer que tout groupe de cardinal $2q$ est isomorphe à $\mathbb{Z}/2q\mathbb{Z}$ ou à D_{2q}.

Exercice 42 *(X)** Soit G un groupe d'ordre 8 non cyclique.

1. Montrer qu'il admet un élément d'ordre 2 et que tous les éléments sont d'ordre 1, 2 ou 4.
2. On suppose que tous les éléments sont d'ordre au plus 2. Que dire de G ?
   On suppose désormais qu'il existe un élément a d'ordre 4, on note H le sous groupe engendré par a.
3. On suppose qu'il existe un élément de $G \setminus H$ d'ordre 2. Montrer que, pour tout $x \in G$, $xHx^{-1} = H$. Que dire de G ?
4. On suppose désormais qu'il n'existe pas d'élément d'ordre 2 hors de H. Que dire de G ?

Exercice 43 *(ENS Lyon)** Déterminer à isomorphisme près tous les groupes de cardinal 8.

Exercice 44 *(Lyon)*

1. Donner des exemples de groupes d'ordre 12 commutatifs ainsi qu'un exemple non commutatif.
2. Montrer que tout groupe d'ordre 12 admet un élément d'ordre 2.
3. Trouver à isomorphisme près les groupes commutatifs d'ordre 12.
4. Montrer que tout groupe d'ordre 12 admet un élément d'ordre 3.
5. Trouver tous les groupes d'ordre 12 à isomorphisme près.

Anneaux

Exercice 45 Montrer que dans $\mathbb{Z}$ toute suite croissante d'idéaux est stationnaire.

Exercice 46 *(Mines)* Soit $(A, +, \times)$ un anneau. On dit qu'un élément x est *nilpotent* s'il existe $k \in \mathbb{N}^*$ tel que $x^k = 0_A$.

1. Soit x un élément nilpotent de A. Montrer que $(1 - x)$ est inversible et déterminer son inverse.
2. Montrer que si A est commutatif alors l'ensemble de éléments nilpotents de A, noté $Nil(A)$ forme un idéal de A.
3. Qu'en est-il si A n'est pas commutatif ?
4. Trouver tous les $n > 0$ tels que $\mathbb{Z}/n\mathbb{Z}$ admette un élément nilpotent non nul.

Exercice 47 *(Mines)* Soit A un anneau commutatif intègre. Montrer que toute partie finie non vide $\mathcal{P}$ de $A \setminus \{0\}$ stable par multiplication est un sous-groupe du groupe multiplicatif $A^\times$ des éléments inversibles de A.

Exercice 48 *(SR)* On dit que A est un anneau euclidien si A est un anneau intègre (donc commutatif) et qu'il existe $t : A \setminus \{0\} \to \mathbb{N}$ vérifiant :
— pour tout $(a, b) \in A \times (A \setminus \{0\})$, il existe $(q, r) \in A^2$ tel que $a = bq + r$ avec $r = 0$ ou $t(r) < t(b)$,
— $\forall (a, b) \in (A \setminus \{0\})^2, t(ab) \geq t(a)$.

1. Les anneaux $\mathbb{Z}$ et $\mathbb{R}[X]$ sont-ils euclidiens ? Montrer qu'un corps est un anneau euclidien.
2. Soient A un anneau euclidien et I un idéal de A. Montrer qu'il existe $x \in A$ tel que $I = xA$. Y a-t-il unicité de x ?
3. Dans cette question, on se donne A un anneau euclidien tel que $t(1) = 1$. Soit $x \in A$. Montrer que x est inversible si et seulement si $t(x) = 1$.

Exercice 49 *(Centrale)* Soient $\alpha > \beta$ les deux racines de $P = X^2 - X - 1$. On pose $A = \left\{x + \alpha\, y,\ (x, y) \in \mathbb{Z}^2\right\}$ et $\sigma : x + \alpha\, y \mapsto x + \beta\, y$.

1. Montrer que A est un anneau et que σ est un automorphisme de A. Expliciter σ^{-1}.
2. On note U l'ensemble des inversibles de A et $N : z \in A \mapsto z\,\sigma(z)$.
   (a) Montrer : $\forall z \in A\,,\ z \in U \iff \left|N(z)\right| = 1$.
   (b) Soit $V = U \cap]1, +\infty[$. Montrer que si $x + \alpha\, y \in V$, alors $x \geq 0$ et $y \geq 1$.
   (c) En déduire que $V = \left\{\alpha^n,\ n \in \mathbb{N}^*\right\}$.

Exercice 50 *(X)*

1. Montrer que, si un nombre réel s'écrit $a + b\sqrt{2}$ avec $(a, b) \in \mathbb{Z}^2$, cette écriture est unique.
2. Montrer que l'ensemble $\mathbb{Z}[\sqrt{2}]$ des nombres réels de la forme précédente est un sous-anneau de $\mathbb{R}$.
3. Déterminer les automorphismes de l'anneau $\mathbb{Z}[\sqrt{2}]$.

4. Si $(x,y) \in \mathbb{Z}^2$ et $z = x + \sqrt{2}y$, on pose $N(z) = x^2 - 2y^2$. Montrer que z est un inversible de $\mathbb{Z}[\sqrt{2}]$ si et seulement si $N(z) = \pm 1$.
5. Montrer que les inversibles de $\mathbb{Z}[\sqrt{2}]$ sont les $\pm(1+\sqrt{2})^k$ avec $k \in \mathbb{Z}$.

Exercice 51 *(Lyon)* On note $\mathbb{Z}[i\sqrt{2}] = \left\{a + ib\sqrt{2},\ (a,b) \in \mathbb{Z}^2\right\}$.

1. Montrer que $\mathbb{Z}[i\sqrt{2}]$ est un sous-anneau de $\mathbb{Q}$.
2. Montrer que l'anneau $A := \mathbb{Z}[i\sqrt{2}]$ est euclidien, c'est-à-dire qu'il existe une fonction $N : \mathbb{Z}[i\sqrt{2}] \to \mathbb{N}$ telle que, pour tout $(a,b) \in A \times (A \setminus \{0\})$, il existe un couple $(q,r) \in A^2$ tel que $a = bq + r$ et $N(r) < N(b)$.
3. Énoncer et démontrer un théorème d'existence et d'unicité d'une décomposition en facteurs irréductibles dans $\mathbb{Z}[i\sqrt{2}]$.

Exercice 52 *(Lyon)* Soit $d \in \mathbb{N}^*$ sans facteur carré. On note $\mathbb{Z}[d] = \{a + b\sqrt{d} \mid (a,b) \in \mathbb{Z}^2\}$ et on pose $N(a+b\sqrt{d}) = a^2 - db^2$ pour tout $(a,b) \in \mathbb{Z}^2$.

1. Montrer qu'il existe $\omega \in \mathbb{Z}[\sqrt{d}]$ tel que $\{x \in \mathbb{Z}[d] : N(x) = 1\} = \{\varepsilon\omega^k \mid \varepsilon \in \{-1,1\}, k \in \mathbb{Z}\}$.
2. Montrer que $\omega \neq \pm 1$. On commencera par montrer qu'il existe un réel $C > 0$ tel que $\{x \in \mathbb{Z}[d] :\ |N(x)| \leq C\}$ soit infini.

Exercice 53 *(X)*

1. Montrer que $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ est un anneau et déterminer ses inversibles.
2. On admet que l'idéal engendré par 2 est un idéal maximal, montrer que cet anneau est principal.

Exercice 54 (X) Soit (p_n) une suite de nombre premiers distincts. On définit par récurrence :

$$(Z_n) = \begin{cases} Z_0 = \mathbb{Q} \\ Z_{n+1} = Z_n + \sqrt{p_n} Z_n \end{cases}$$

1. Montrer que les Z_n sont des corps.
2. Montrer que les $\sqrt{p_n}$ sont linéairement indépendants sur $\mathbb{Q}$.
3. Soit (x_n) une suite de nombres sans facteurs premiers, deux à deux distincts. Montrer qu'ils sont linéairement indépendants.

Exercice 55 *(X)* Soit $d \in \mathbb{Z} \setminus \{0\}$. On considère l'équation $(*) : x^2 - dy^2 = 1$ d'inconnue $(x,y) \in \mathbb{Z}^2$.

1. Traiter les cas $d < 0$ et $d = k^2$ avec $k \in \mathbb{N}$.
2. Dans la suite, on suppose $d > 0$ et $\sqrt{d} \notin \mathbb{N}$. Soit $(x_0, y_0) \in \mathbb{N}^2 \setminus \{(\pm 1, 0)\}$ solution de $(*)$. On pose $z = x_0 + \sqrt{d}\, y_0$. Montrer que, pour tout $n \in \mathbb{N}^*$, il existe un unique $(x_n, y_n) \in \mathbb{N}^2$ tel que $z^{n+1} = x_n + \sqrt{d}\, y_n$.
3. En déduire que, si l'ensemble des solutions de $(*)$ est non trivial, i.e. n'est pas réduit à $\{(\pm 1, 0)\}$, il en existe une infinité.
4. Soit $x \in \mathbb{R}$. Montrer que, pour tout $n \in \mathbb{N}$, il existe $(p,q) \in \mathbb{Z}^2$ tel que $|p - qx| < \dfrac{1}{n}$.
5. Montrer qu'il existe une infinité de couples $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $|p - qx| < \dfrac{1}{q}$.
6. Montrer qu'il existe $K \in \mathbb{R}$ pour lequel il existe une infinité de couples d'entiers (p,q) tels que $|p^2 - dq^2| < K$.
7. Conclure que $(*)$ possède des solutions non triviales.

Exercice 56 *(X)**

1. Montrer que l'équation $a^2 - 2b^2 = 1$ admet une infinité de solutions $(a,b) \in \mathbb{N}^2$. Déterminer l'ensemble des solutions.
2. Que dire de l'ensemble des solutions de $a^2 - 2b^2 = -1$?

Exercice 57 *(Paris)* Soit A un anneau tel que tout élément de $a \in A$ est nilpotent ou idempotent, c'est-à-dire tel que $a^2 = a$.

1. Montrer que tout élément de A est idempotent.
2. Montrer que A est commutatif.
3. On suppose que A est fini. Montrer qu'il existe $n \in \mathbb{N}^*$ tel que A soit isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.