

Feuille d'exercices : Algèbre générale

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

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

1. Dénombrer les carrés de $\mathbb{Z}/p\mathbb{Z}$.
2. Démontrer que t est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $t^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
3. En déduire que pour $p \geq 3$, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \pmod{4}$.
4. On suppose $p \equiv 1 \pmod{4}$. En calculant la classe de $(p-1)!$ modulo p de deux manières différentes, montrer que -1 est un carré modulo p .
5. Si -3 n'est pas un carré de $\mathbb{Z}/p\mathbb{Z}$, montrer que $(-3)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
6. Soit p un nombre premier congru à -1 modulo 4. Montrer que l'opposé d'un carré de $(\mathbb{Z}/p\mathbb{Z})^*$ n'est pas un carré. Et pour tout $r \in (\mathbb{Z}/p\mathbb{Z})^*$, montrer que $\{(i, j) \in ((\mathbb{Z}/p\mathbb{Z})^*)^2, i^2 - j^2 = r\}$ est de cardinal $p-3$.

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 $nn^* \equiv 1 \pmod{p^2}$. Montrer que : $\sum_{k=1}^{p-1} k^* \equiv 0 \pmod{p^2}$.

Exercice 4 (*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 5 (*U*)* Soit $n \geq 2$. Déterminer $(\mathbb{Z}/n\mathbb{Z})^*$.

Groupe symétrique

Exercice 6 (*Mines*) Soit $n \geq 2$ un entier, γ un n -cycle de \mathcal{S}_n . Écrire γ comme produit de transpositions.

Exercice 7 Soit $n \geq 3$. Déterminer l'ensemble des permutations de \mathcal{S}_n commutant avec tous les éléments de \mathcal{S}_n .

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

Exercice 9 (*PLSR*) Pour $\sigma \in \mathcal{S}_n$, on note $\epsilon(\sigma)$ sa signature et $\nu(\sigma)$ son nombre de points fixes. Calculer $\sum_{\sigma \in \mathcal{S}_n} \frac{\epsilon(\sigma)}{\nu(\sigma) + 1}$.

Exercice 10 (*ENS SR*)* Pour $n \in \mathbb{N}^*$, on note D_n le nombre de permutations de $\llbracket 1, n \rrbracket$ sans point fixe. Donner une relation entre D_{n+2} , D_{n+1} et D_n .

Exercice 11 (*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 $\sigma^2 = \text{Id}$. 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 12 (*Ulm*)* 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 13 (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 (ab) et $(12\dots n)$. À quelle condition a-t-on $G_{a,b} = \mathcal{S}_n$?

Exercice 14 (Ulm) Pour $n \in \mathbb{N}^*$, on note $g(n)$ le maximum des ordres des éléments de \mathcal{S}_n . Montrer que $\forall k \in \mathbb{N}^*$, $\frac{g(n)}{n^k} \xrightarrow{n \rightarrow +\infty} +\infty$. 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-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 17 (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 $\sum_{d|n} n_d(G)$, où $n = |G|$?
2. Que déduire de la question précédente si G est cyclique ?
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}^*, \cdot) . Montrer que G est cyclique.
5. Que dire dans la situation de la question précédente si $\mathbb{K} = \mathbb{C}$?

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

Quelques éléments de théorie des groupes

Exercice 19 (Mines)* Soit (G, \cdot) un groupe fini dont tous les éléments sont d'ordre ≤ 2 . Que peut-on dire de $|G|$?

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 $k \in \mathbb{N}^*$, $A_k = \left\{ \prod_{i=1}^k s_i, (s_1, \dots, s_k) \in S^k \right\}$ et $a_k = \text{card}(A_k)$.

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, \cdot) 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 $f : \begin{cases} H \times K & \rightarrow G \\ (h, k) & \mapsto hk \end{cases}$. Donner une condition nécessaire et suffisante pour que f soit un morphisme de groupes.
3. Soit $z = h_0 k_0 \in HK$, avec $(h_0, k_0) \in H \times K$. Montrer que les antécédents de z par f sont les $(h_0 t, t^{-1} k_0)$ avec $t \in H \cap K$.
4. En déduire que $\text{Card}(HK)\text{Card}(H \cap K) = \text{Card}(H)\text{Card}(K)$, 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 (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 $\forall g \in G, gD_G = D_Gg$.
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 23 (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 $f : N \rightarrow G$ et $g : G \rightarrow H$ 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 24 (X)

1. Soit (G, \cdot) un groupe abélien fini. Déterminer le produit des éléments de G .
2. On suppose que $G = S_3$. Quels sont les éléments de G que l'on peut écrire comme produits de tous les éléments de G dans un ordre quelconque, chaque élément apparaissant exactement une fois ?

Exercice 25 (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 $\frac{|G|}{2}$.

Exercice 26 (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 $\frac{|G|}{2}$.

Exercice 27 (ENS) Soient (G, \cdot) 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 28 (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 29 (X) Soit G un groupe fini. Pour $x \in G$, on note \bar{x} la classe de conjugaison de x :

$\bar{x} = \{gxg^{-1} ; g \in G\}$; on dit que x est ambivalent si $x^{-1} \in \bar{x}$.

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 $\frac{1}{|G|} \sum_{x \in G} \rho(x)^2$ est le nombre de classes de conjugaison ambivalentes de G .

Exemples de groupes

Exercice 30 (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 31 (*Mines*) * Soient p un nombre premier et $q = (p^2 - 1)(p^2 - p)$.

1. Calculer le cardinal de $GL_2(\mathbb{Z}/p\mathbb{Z})$.
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 32 (*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 33 (*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 34 (*X*)

1. Montrer que $SL_2(\mathbb{Z})$ est un sous-groupe de $GL_2(\mathbb{R})$.
2. Soit P l'ensemble des $z \in \mathbb{C}$ tels que $\text{Im}(z) > 0$. Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans $SL_2(\mathbb{Z})$ et si z est dans P , montrer que $M.z = \frac{az + b}{cz + d}$ est dans P .
3. Montrer que, si M et M' sont dans $SL_2(\mathbb{Z})$ 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 $SL_2(\mathbb{Z})$ 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 $|\text{Re}(z')| \leq \frac{1}{2}$.

Exercice 35 (*X*) *

On considère G le groupe des symétries d'un pentagone régulier, c'est-à-dire les isométries vectorielles de \mathbb{C} conservant \mathbb{U}_5 .

1. Décrire G . En donner un système de générateurs.
On note $\{r, s\}$ un système de générateurs de G , avec $r^5 = 1$ et $s^2 = 1$.
Montrer que $G = \{r^k, 0 \leq k \leq 4\} \sqcup \{sr^k, 0 \leq k \leq 4\}$.
2. On souhaite maintenant montrer que tout groupe à 10 éléments est isomorphe, soit à $\mathbb{Z}/10\mathbb{Z}$, soit au groupe des symétries du pentagone. On considère (G, \cdot) un groupe à 10 éléments, non cyclique. Montrer que G possède un élément d'ordre 5, noté ρ , et un élément d'ordre 2, noté σ .
Montrer que $G = \{\rho^k, 0 \leq k \leq 4\} \sqcup \{\sigma\rho^k, 0 \leq k \leq 4\}$. Montrer que $\sigma\rho\sigma^{-1} \in \{\rho, \rho^{-1}\}$. En distinguant les cas, conclure.

Exercice 36 (*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 37 (*ENS Lyon*) * Déterminer à isomorphisme près tous les groupes de cardinal 8.

Exercice 38 (*X*) Soit G un groupe d'ordre $2n$ avec n impair.

1. Montrer que G contient un élément d'ordre 2.

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

Anneaux

Exercice 39 Montrer que dans \mathbb{Z} toute suite croissante d'idéaux est stationnaire.

Exercice 40 (*Mines*) Soit $(A, +, \times)$ un anneau. On dit qu'un élément x est *nilpotent* s'il existe $k \in \mathbb{N}^*$ tel que $x^k = 0_A$.

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

Exercice 41 (*Centrale*) Soient $\alpha > \beta$ les deux racines de $P = X^2 - X - 1$. On pose $A = \{x + \alpha y, (x, y) \in \mathbb{Z}^2\}$ et $\sigma : x + \alpha y \mapsto x + \beta y$.

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

Exercice 42 (*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 43 (*X*)

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

Exercice 44 (*Lyon*) On note $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2}, (a, b) \in \mathbb{Z}^2\}$.

- Montrer que $\mathbb{Z}[i\sqrt{2}]$ est un sous-anneau de \mathbb{Q} .
- Montrer que l'anneau $A := \mathbb{Z}[i\sqrt{2}]$ est euclidien, c'est-à-dire qu'il existe une fonction $N : \mathbb{Z}[i\sqrt{2}] \rightarrow \mathbb{N}$ 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 $N(r) < N(b)$.
- Énoncer et démontrer un théorème d'existence et d'unicité d'une décomposition en facteurs irréductibles dans $\mathbb{Z}[i\sqrt{2}]$.

Exercice 45 (*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 $(a, b) \in \mathbb{Z}^2$.

- Montrer qu'il existe $\omega \in \mathbb{Z}[\sqrt{d}]$ tel que $\{x \in \mathbb{Z}[d] : N(x) = 1\} = \{\varepsilon\omega^k \mid \varepsilon \in \{-1, 1\}, k \in \mathbb{Z}\}$.
- 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 46 (*X*)

- Montrer qu'il existe une infinité de nombres premiers congrus à 2 modulo 3.
- 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 $k + 1$.
- Si A et B sont deux parties d'un corps fini \mathbb{K} , calculer $\sum_{x \in \mathbb{K}^*} |A \cap xB|$.
- 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 $\frac{|A|}{3}$.

Exercice 47 (*X*)

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