TD 11
Structures algébriques

1 Exercices corrigés en classe

Exercice 1. *Sous-groupes de* $\mathbb{R}$. Soit H un sous-groupe de $(\mathbb{R},+)$, $H \neq \{0\}$. Soit $a = \inf(H \cap \mathbb{R}_+^*)$.

1. Justifier l'existence de a.
2. Montrer que si $a = 0$, alors H est dense dans $\mathbb{R}$.
3. Montrer que si $a > 0$, alors $H = a\mathbb{Z} = \{ka, k \in \mathbb{Z}\}$.

Application Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$. Un réel T est appelé *période* de f si

$$\forall x \in \mathbb{R},\ f(x+T) = f(x).$$

4. Montrer que l'ensemble des périodes de f est un sous-groupe de $(\mathbb{R},+)$.
5. Soit f une fonction continue admettant 3 et $\sqrt{2}$ comme périodes. Montrer que f est constante.

Exercice 2. *Quelques questions indépendantes sur les morphismes de groupes*. Soit $(G,*)$ un groupe.

1. À quelle condition $x \mapsto x^{-1}$ est-il un morphisme de groupes ?
2. À quelle condition $x \mapsto x^2$ est-il un morphisme de groupes ?
3. Démontrer que pour tout a dans G, $x \mapsto a * x * a^{-1}$ est un automorphisme de G. *Les automorphismes de ce type sont appelés automorphismes intérieurs de* G. À quelle condition cet automorphisme est-il l'identité ?

Exercice 3. ●○○ Soient

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix},\ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix}$$

Décomposer σ en produits de cycles à supports disjoints, en produit de transpositions, la signature de σ, et calculer σ^{100}. Faire de même avec ρ.

Exercice 4. ●●○ Soit $n \geqslant 3$. Soient $a \neq b \in \{1, \dots n\}$ et soit $\sigma \in S_n$. Déterminer $\sigma \circ (a\ b) \circ \sigma^{-1}$. Généraliser en remplaçant $(a\ b)$ par un cycle quelconque, puis par une permutation quelconque.

Exercice 5. *Quelques sous-anneaux de* $\mathbb{C}$. ●○○

1. Montrer que l'ensemble des entiers de Gauss $\mathbb{Z}[i] = \{a + ib, (a,b) \in \mathbb{Z}^2\}$ est un sous-anneau de $(\mathbb{C},+,\times)$.
2. Montrer que l'ensemble $\mathbb{Z}[j] = \{a + jb, (a,b) \in \mathbb{Z}^2\}$ est un sous-anneau de $(\mathbb{C},+,\times)$.

Exercice 6. *Éléments nilpotents d'un anneau : utile pour les chapitres de matrices*. Soit $(A,+,\times)$ un anneau. Un élément x de A est dit **nilpotent** s'il existe n dans $\mathbb{N}$ tel que $x^n = 0_A$.

1. Si $A = \mathscr{M}_2(\mathbb{R})$, l'ensemble des matrices carrées de taille 2×2 à coefficients dans $\mathbb{R}$, donner un élément nilpotent de A.

On revient au cas général.

1. Démontrer qu'un élément nilpotent n'est pas inversible.
2. Démontrer que si x et y sont deux éléments nilpotents tels que $x \times y = y \times x$, alors $x \times y$ et $x + y$ sont nilpotents.
3. Démontrer que si x est un élément nilpotent, alors $1_A - x$ est inversible.

Exercice 7. ●●○ Soit a un élément de $\mathbb{Q}$ et α une racine de l'équation $x^2 = a$. Montrer que l'ensemble $\mathbb{Q}[\alpha] = \{q + \alpha r, (q,r) \in \mathbb{Q}^2\}$ muni des lois $+$ et $\times$ est un corps.

Stratégie pour les autres exercices. Ici, trois stratégies :

- vous avez trouvé le cours trop théorique, et vous voulez vous coller au programme officiel : il faut bien apprendre les définitions, refaire les exemples de cours, et faire les exercices 8, 10, 11, 22, 26.
- vous avez bien compris les définitions, les morphismes : faites les exercices 11, 12, 19, 23, 26, 27.
- vous trouvez ces notions vraiment simples : en plus des exercices précédents, les exercices 16, 21, 20 ! Les exercices 24 et 31 sont aussi de niveaux très solides !

2 Groupes

Exercice 8. *Lois de groupe sur* $\mathbb{R}$. ◐○○

1. Montrer que $\mathbb{R}$ muni de la loi $*$ définie par

$$\forall (x,y) \in \mathbb{R}^2,\ x * y = \sqrt[3]{x^3+y^3},$$

est un groupe abélien.

2. $\mathbb{R}$ muni de la loi $\star$ définie par

$$\forall (x,y) \in \mathbb{R}^2,\ x \star y = \sqrt{x^2+y^2}$$

est-il un groupe ?

Exercice 9. *Groupe des similitudes*. ●○○
Montrer que l'ensemble des similitudes directes non dégénérées est un groupe pour la loi de composition.

Exercice 10. ◐○○
Montrer que l'ensemble $\{z \in \mathbb{C}^*,\ \exists n \in \mathbb{N}^*, z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Exercice 11. *Sous-groupes classiques d'un groupe*. ●◐○
Cet exercice doit vous paraître redondant : la deuxième question est incluse dans la première, la troisième dans un exercice déjà fait. Dès que vous vous en rendez compte, passez à autre chose.
Soit $(G,\cdot)$ un groupe.

1. Soit A une partie de G. On note $C(A) = \{x \in G,\ \forall a \in A, x \cdot a = a \cdot x\}$ (centralisateur de A). Montrer que $C(A)$ est un sous-groupe de G.

2. On appelle centre de G l'ensemble $Z(G) = \{x \in G,\ \forall y \in G, x \cdot y = y \cdot x\}$. Montrer que $Z(G)$ est un sous-groupe de G, et même qu'il est distingué dans G, c'est-à-dire que

$$\forall x \in Z(G), \forall y \in G, y \cdot x \cdot y^{-1} \in Z(G).$$

3. On suppose G abélien. On dit qu'un élément x de G est **de torsion** s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$. Démontrer que l'ensemble des éléments de torsion de G est un sous-groupe de G.

Exercice 12. ●●○ Soit $(G,*)$ un groupe. On note, si A et B sont deux sous-groupes de G, $AB = \{a * b,\ a \in A,\ b \in B\}$. Démontrer que AB est un sous-groupe de G si, et seulement si $AB = BA$.

Exercice 13. *Groupe dont tous les éléments sont d'ordre 2.* ●●○ Soit $(G, *)$ un groupe fini tel que pour tout x dans G, $x^2 = e$ (où e désigne le neutre de G).

1. Démontrer que G est abélien.
2. Soit H un sous-groupe strict de G et $x \notin H$. On note $xH = \{x * h,\ h \in H\}$. Démontrer que $H \cup xH$ est un sous-groupe de G. Si H contient p éléments, combien $H \cup xH$ contient-il d'éléments ?
3. ●●● En déduire que le cardinal de G est une puissance de 2.

Exercice 14. ●●◐ Soit E un ensemble de cardinal n.

1. (a) Combien peut-on définir de lois de composition internes sur E ?
   (b) Combien sont commutatives ?
   (c) Combien possèdent un élément neutre ?
2. (a) Combien peut-on définir de relations binaires sur E ?
   (b) Combien sont réflexives ?
   (c) Combien sont symétriques ?

Exercice 15. *Relation de conjugaison.* ●◐○ Soit G un groupe. On définit la relation $\sim$ sur G par

$$\forall (x, y) \in G,\ (x \sim y) \Leftrightarrow (\exists g \in G, x = gyg^{-1}).$$

Montrer que $\sim$ est une relation d'équivalence sur G.
Lorsque G est abélien, quelles sont les classes de conjugaison ?

Exercice 16. ●●●

1. Déterminer tous les sous-groupes finis de $(\mathbb{C}^*, \times)$.

Soit A une partie de $\mathbb{C}$. On dit que A est compacte si de toute suite d'éléments à valeurs dans A, on peut extraire une sous-suite de A qui converge **DANS** A.

2. Les parties suivantes de $\mathbb{C}$ sont-elles compactes : $\mathbb{R}$, $\{z \in \mathbb{C},\ |z| \leqslant 1\}$, $\{z \in \mathbb{C},\ |z| < 1\}$, $\{a + ib,\ (a, b) \in \mathbb{Q}^2\}$?
3. ●●● Déterminer tous les sous-groupes compacts de $(\mathbb{C}^*, \times)$.

3 Morphismes, parties génératrices

Exercice 17. *Morphismes sur $\mathbb{Z}$, sur $\mathbb{Q}$.* ●●○

1. Déterminer tous les morphismes de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$. Préciser, à chaque fois, le noyau et l'image de ce morphisme.
2. Quels sont les automorphismes de groupe de $(\mathbb{Z}, +)$?
3. Trouver tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Exercice 18. ●●○ On munit $\mathbb{Z}^2$ de la loi $+$ (addition coordonnée par coordonnée). On considère un morphisme φ de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}^2, +)$.

1. Démontrer que pour tout k dans $\mathbb{Z}$, $\varphi(k) = k\varphi(1)$.
2. Démontrer que φ ne peut pas être un isomorphisme.

Exercice 19. ●●◐ Un **isomorphisme** de groupes est un morphisme de groupes bijectif. Deux groupes sont dits isomorphes s'il existe un isomorphisme de l'un vers l'autre.
Démontrer que $(\mathbb{Q}, +)$ et $(\mathbb{Q}^*, \times)$ ne sont pas isomorphes.

Exercice 20. *Nombre de morphismes d'un groupe.* ●●● Soit $(G, \cdot)$ un groupe fini à n éléments.

1. Soit H une partie génératrice de G à p éléments. Montrer qu'il y a au plus n^p morphismes de G.
2. Démontrer que G admet une partie génératrice qui possède moins de $\lceil \log_2(n) \rceil$ éléments, où $\lceil \cdot \rceil$ désigne la partie entière supérieure.
3. En déduire que G possède au plus $n^{\lceil \log_2(n) \rceil}$ morphismes.

Exercice 21. ●●● Soit G un groupe abélien de cardinal supérieur ou égal à 2. Un élément μ de G est dit *mou* si pour toute partie H génératrice de G, $H \setminus \{\mu\}$ est génératrice de G. On note M l'ensemble des éléments mous de G.

1. Démontrer que M est un sous-groupe de G. On l'appelle sous-groupe de Frattini de G.
2. Dans cette question, $G = (\mathbb{Z}, +)$. Montrer que l'ensemble des éléments mous de G est $\{0\}$.
3. Dans cette question, $G = (\mathbb{Q}, +)$. On va montrer que tout rationnel est mou. Soit $r = \dfrac{p}{q}$ dans $\mathbb{Q}$ et H une partie génératrice de $\mathbb{Q}$, $K = H \setminus \{r\}$.
   (a) Si $r \notin H$, conclure immédiatement que K est génératrice.

   On suppose alors que $r \in H$.
   (b) Démontrer que $H \setminus \{r\}$ n'est pas vide.
   (c) Posons K le sous-groupe engendré par $H \setminus \{r\}$. Soit $A = qK = \{qx, x \in K\}$
      i. Démontrer qu'il existe $d \in \mathbb{N}^*$ tel que $A \cap \mathbb{Z} = d\mathbb{Z}$.
      ii. Démontrer qu'il existe $k \in \mathbb{N}$, $u \in \mathbb{Z}$, $(n_1, \dots, n_k) \in \mathbb{Z}^k$, $(r_1, \dots, r_k) \in (H \setminus \{r\})^k$ tels que
      $$\frac{1}{qd} = ur + n_1 r_1 + \cdots + n_k r_k,$$
      puis démontrer que
      $$1 - qdur \in d\mathbb{Z}.$$
      iii. Démontrer que $d = 1$ et conclure.

4 Groupe symétrique

Exercice 22. ●◐○ Soit E un ensemble contenant au moins trois éléments. Montrer que S_E n'est pas commutatif.

Exercice 23. ●●◐

1. Démontrer que le centre (défini comme en 11) de $\mathcal{S}_n$ est trivial (i.e. égal à $\{\mathrm{Id}\}$) pour $n \geqslant 3$). *On pourra utiliser l'exercice 4*
2. Démontrer que le centre de $\mathcal{A}_n$ est trivial pour $n \geqslant 4$.

Exercice 24. ●●● Vous venez d'obteir ce jeu de taquin dans votre paquet de céréales. Où est l'arnaque ?

4	1	3
5	2	7
8	6	

Exercice 25. ●●● Soit E un ensemble de cardinal n. On appelle dérangement de E toute permutation de E sans point fixe. On note d_p le nombre de dérangements d'un ensemble à p éléments.

1. Montrer que $n! = \sum_{k=0}^{n} \binom{n}{k} d_k$.
2. Démontrer la formule d'inversion de Pascal : soit f une fonction définie sur $\mathbb{N}$, soit g définie pour tout n par $g(n) = \sum_{k=0}^{n} \binom{n}{k} f(k)$. Montrer que pour tout entier naturel n, $f(n) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} g(k)$.
3. En déduire une formule pour d_n.
4. Quelle est la limite de la proportion $\frac{d_n}{n!}$ des dérangements de E parmi les permutations de E quand n tend vers $+\infty$?

5 Anneaux et corps

Exercice 26. *Anneau des dyadiques*. ●●○ On définit le sous-ensemble A de $\mathbb{Q}$ par

$$A = \left\{ \frac{p}{2^n}, p \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

1. Montrer que A est un sous-anneau de $\mathbb{Q}$. Est-il intègre ? Tout élément de A est-il inversible pour $\times$?
2. Déterminer $U(A)$.

Exercice 27. *Anneaux de Boole*. ●●○ On appelle anneau de Boole tout anneau $(A, +, \times)$ tel que $\forall a \in A, a^2 = a$.

1. Montrer que $\forall a \in A, a + a = 0_A$.
2. En déduire que A est commutatif pour la loi $\times$.
3. Montrer que si A est fini, son cardinal est nécessairement différent de 3.
4. Montrer que si $\text{Card}(A) > 2$, alors A n'est pas intègre.
5. On définit une relation binaire sur A par $x \preceq y$ si, et seulement si $yx = x$. Montrer que $\preceq$ est une relation d'ordre sur A.

Exercice 28.
1. ●●○ Déterminer tous les morphismes de corps de $\mathbb{Q}$ dans $\mathbb{Q}$ (indication : il n'y en a pas beaucoup... !)
2. ●●○ Soit f un morphisme de corps de $\mathbb{R}$ dans $\mathbb{R}$. Démontrer que f est égale à l'identité sur les rationnels, puis que $f(\mathbb{R}_+) \subset \mathbb{R}_+$, puis que f est croissante, et enfin que $f = \text{Id}_{\mathbb{R}}$.

Exercice 29. ●●○ Soit ϕ une racine de l'équation

$$x^2 - x - 1 = 0.$$

Montrer que $\mathbb{Q}[\phi] = \{q + \phi r, (q, r) \in \mathbb{Q}^2\}$ est un corps.

Exercice 30. *Anneau* $\mathbb{Z}(\sqrt{2})$. ●◐○ - ●●●
On définit $\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b, (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau commutatif et intègre.

2. Soit $x = a + \sqrt{2}b$ un élément de $\mathbb{Z}[\sqrt{2}]$.
   (a) Montrer que le couple (a, b) est unique.
   (b) On pose alors $N(x) = a^2 - 2b^2$. Montrer que pour tous x, y de $\mathbb{Z}[\sqrt{2}]$,

$$N(xy) = N(x)N(y).$$

3. On veut déterminer $U(\mathbb{Z}[\sqrt{2}])$.
   (a) Montrer que $x \in U(\mathbb{Z}[\sqrt{2}])$ si, et seulement si $N(x) = 1$ ou $N(x) = -1$.
   (b) Montrer que pour tout entier n de $\mathbb{Z}$, $(1 + \sqrt{2})^n$ appartient à $U(\mathbb{Z}[\sqrt{2}])$.

4. ●●● Montrer que réciproquement, les inversibles de $\mathbb{Z}[\sqrt{2}]$ sont de la forme $\pm(1 + \sqrt{2})^n$, $n \in \mathbb{Z}$.

Exercice 31. ●●◐ Soit E un ensemble. Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.

Indications

1. Exercice dur (notamment pour un premier exo de TD). Un conseil : utilisez la définition epsilonesque de la borne inf.
   1. Évident.
   2. À ε fixé, trouver h dans H tel que $0 < h < \varepsilon$ et, pour x dans $\mathbb{R}$, faire des « sauts » de taille h pour atteindre x !
   3. Une inclusion est évidente, l'autre beaucoup moins : pour l'autre, supposer que l'on a h dans H qui ne soit pas dans $a\mathbb{Z}$. Prendre $\varepsilon =$ à la distance de h à $a\mathbb{Z}$ et voir ce que l'on peut en dire !
2. Indication : les deux premières conditions sont les mêmes. Attention à la manipulation des quantificateurs notamment !
3. Appliquer la méthode du cours !
4. PRENDRE UN EXEMPLE ! Prendre par exemple $n = 5$, $(a\ b) = (1\ 2)$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$.
5. Revenir aux définitions.
6. **1.** Penser à une matrice triangulaire.
   2. Supposer que c'est le cas.
   3. Utiliser les règles de calcul dans un anneau, et prendre une puissance suffisamment grande.
   4. Remarquer que $1_A = 1_A - 0_A = 1_A - x^n$ si n est tel que $x^n = 0$.
7. La difficulté est de montrer que l'inverse d'un élément de $\mathbb{Q}[\alpha]$ est dans $\mathbb{Q}[\alpha]$: utiliser pour cela la quantité conjuguée.
8. **1.** Revenir aux définitions, et utiliser que $(\sqrt[3]{x})^3 = x$.

2. Utiliser un contre-exemple (pas d'inverse par exemple, ou pas de neutre).

9. Les similitudes dégénérées sont les $z \mapsto az + b$ pour lesquelles $a = 0$.

10. Attention, remarquer que si l'on prend deux éléments dans cet ensemble, les n correspondants ne seront pas les mêmes !

11. Revenir aux définitions.

12 **ATTENTION !** $AB = BA$ **ne signifie pas** que les éléments de A et ceux de B commutent.Raisonner par double implication. Pour l'implication directe, **partir de** a **dans** A **et** b **dans** B **et montrer que** $ab \in BA$**.** Pour l'implication réciproque, essayer de dérouler la définition d'un sous-groupe, et, à un moment, lorsque vous trouvez $a * b$, écrivez-le comme $a' * b'$.

13 **1.** Remarquer que pour tout x, $x = x^{-1}$. Écrire donc que $x * y = (x * y)^{-1}$.

2. Faire la preuve en trois étapes. Pour le produit de deux éléments, distinguer 3 cas : les deux sont dans H, les deux sont dans aH et l'un est dans H/l'autre dans aH.

3. Raisonner de proche en proche : on prend x et on prend $H = \{e, x\}$ qui est un sous-groupe. Si $H = G$, c'est bon. Sinon, appliquer la question précédente.

14 Penser qu'une loi se définit par sa table d'opérations !

15. Ne pas oublier les trois définitions d'une relation d'équivalence.

16. **1.** Montrer que ce sont les $\mathbb{U}_n$. Déjà montrer, à l'aide du module, qu'ils sont dans $\mathbb{U}$, puis utiliser que si un sous-groupe est fini alors tout élément, à une certaine puissance, donne 1.

2. Les réponses sont oui, non, non. Penser en particulier que « dense » implique « non compact » .

3. Montrer que ce sont les mêmes que les groupes finis. On pourra en particulier s'intéresser au morphisme $\varphi : \left|\begin{array}{l}\mathbb{R} \to \mathbb{U} \\ \theta \mapsto \mathrm{e}^{i\theta}\end{array}\right.$ et dire que si G est un sous-groupe compact de $\mathbb{U}$, alors $\varphi^{-1}(G)$ est un sous-groupe de $\mathbb{R}$ et qu'il est donc discret ou dense. Démontrer que s'il est discret, de la forme $a\mathbb{Z}$, alors si $a \notin 2\pi\mathbb{Q}$, alors G est dense (dur !)

17. **1.** S'intéresser à l'image de 1 et penser que $\mathbb{Z}$ est engendré par 1 ! !

2. Cf. question précédente : si on veut atteindre tout $\mathbb{Z}$, que faut-il sur l'image de 1 ?

3. Si on note $a = f(1)$, que vaut, pour $n \in \mathbb{N}$, $f(1/n)$?

19. S'il existe un morphisme φ, 2 admet un antécédent x par φ. Que vaur alors $\varphi(x/2)$?

20. **1.** Penser au fait que si on connaît un morphisme sur une partie génératrice, alors on le connaît partout.

2. Partir d'un élément de G non neutre, x_1, et considérer $\langle x_1 \rangle$ qui a au moins deux éléments. Prendre ensuite $x_2 \notin \langle x_1 \rangle$... et poursuivre !

3. Combiner les deux questions précédentes.

21. **1.** Montrer que si x et y sont mous, alors $x \cdot y^{-1}$ est mou : pour ce faire, penser que si x est mou, alors pour toute partie génératrice H de G, il existe $a_1, \ldots, a_p$ dans H différents de x tels que $x = a_1 \cdot \cdots \cdot a_p$.

2. Procéder par double inclusion, et remarquer que si x est mou et n'appartient pas à un sous-groupe maximal H, alors $\langle H \rangle \neq \langle H \cup \{x\} \rangle$.

3. Dans le premier cas, c'est $\{0\}$. Dans le second, montrer qu'il s'agit de $\mathbb{Q}$.

22. Trouver deux transpositions ne commutant pas.

23. **1.** Fait en cours.
    2. Utiliser que si σ et τ commutent, $\sigma \circ \tau \circ \sigma^{-1} = \tau$.
    3. Utiliser des double-transpositions !

24. Modéliser le problème en disant qu'une grille correspond à une permutation. Se demander quel est l'effet d'un mouvement de taquin sur la permutation.

26. **1.** La vérification se fait à l'aide du cours. Il est intègre mais tout élément n'est pas inversible.
    2. Démontrer que ce sont les puissances de 2 (positives ou négatives).

27. **1.** Calculer $(a+a)^2$ de deux manières différentes.
    2. Calculer $(a+b)^2$.
    3. Supposer que l'anneau à 3 éléments : 0_A, 1_A et x, et se demander ce que vaut $1_A + c$.
    4. Démontrer que si $x \in A$, x et $x - 1_A$ sont des diviseurs de zéro.
    5. Vérifier les 3 axiomes d'une relation d'ordre.

28 **1.** C'est une des preuves du chapitre 1 que de montrer que si $f(x+y) = f(x) + f(y)$, alors si $r \in \mathbb{Q}$, $f(r) = rf(1)$. Mais que vaut $f(1)$?
    2. Commencer comme précédemment. Ensuite, prendre $x \geqslant 0$, et remarquer que $x = a^2$ avec $a \in \mathbb{R}$... Cela devrait montrer que $f(\mathbb{R}_+) \subset \mathbb{R}_+$. En déduire la croissance (par propriété de morphisme) et encadrer $x \in \mathbb{R}$ par deux suites adjacentes de rationnels.

29. Soient ϕ et θ les deux racines de l'équation. Pour la stabilité par produit, utiliser l'équation. Par quotient, utiliser la « quantité conjuguée » : penser que $(q+\phi r)(q+\theta r)$ a une expression assez simple.

30. **1.** Simple vérification.
    2.
    3.
    4. Supposons que l'on ait un élément inversible de la forme $a + \sqrt{2}b$ avec a, b positifs (c'est possible, quitte à multiplier par -1 et/ou par le conjugué), et tel que $\min(a, b)$ soit minimal, mais tel que $(a, b) \neq (1, 1)$.

31. Vérifier les axiomes d'un anneau (pas d'un sous-anneau), et ne pas hésiter à utiliser les fonctions indicatrices.