Licence — Algèbre. Feuille d'exercices N° 1

06-10/97

Le nombre d'astérisques donne une indication de la difficulté de l'exercice. Zéro astérique veut dire que la question posée est une conséquence directe ou presque directe des définitions. Un astérisque indique que la question est un peu plus difficile. Deux astérisques signifient que le problème est d'un niveau plus avancé, et ainsi de suite. Le symbole $\infty *$ indique un problème non résolu.

1. Pour chacun des couples d'un ensemble avec loi de composition interne suivants, décider s'il est un groupe, et, dans le cas où il en est un, trouver l'élément neutre, et, pour tout élément, son inverse.
   (a) $(\mathbb{N}, +)$.
   (b) $(\mathbb{R}, *)$, avec $x * y = x + y - 1$.
   (c) $(]-\pi/2, \pi/2[, *)$, avec $x * y = \arctan(\tan(x) + \tan(y))$.
   (d) $(\{f\colon \mathbb{R} \to \mathbb{R}\}, *)$, avec $f * g = f \circ g$.
   (e) $(\{A \in \mathrm{M}(100, \mathbb{Z}) \mid \det(A) \neq 0\}, \cdot)$, avec $\cdot$ la multiplication de matrices.
   (f) $(\{A \in \mathrm{M}(100, \mathbb{Z}) \mid \exists B \in \mathrm{M}(100, \mathbb{Z})\colon AB = BA = I\}, \cdot)$, avec $\cdot$ la multiplication de matrices.
   *(g) $(\{A \in \mathrm{M}(100, \mathbb{Z}) \mid \exists B \in \mathrm{M}(100, \mathbb{Z})\colon AB = I\}, \cdot)$, avec $\cdot$ la multiplication de matrices. En fait, vérifiez d'abord que $\cdot$ est bien une loi de composition interne !
   **(h) $(\{a \in \mathrm{End}(V) \mid \exists b \in \mathrm{End}(V)\colon ab = \mathrm{Id}_V\}, \circ)$, avec V un espace vectoriel sur un corps quelconque, éventuellement de dimension infinie.
2. Soient G un ensemble et $*$ une loi de composition interne associative sur G. Supposons que $(G, *)$ a un élément neutre e, et que pour tout x dans G il existe y et y' dans G tels que $yx = e = xy'$. Est-ce que $(G, *)$ est un groupe?

*3. Soient G un ensemble et $*$ une loi de composition interne associative sur G. Supposons que $(G, *)$ a un élément neutre e, et que pour tout x dans G il existe y dans G tels que $yx = e$. Est-ce que $(G, *)$ est un groupe?

4. (a) Soit X un ensemble de cardinal deux. Combien de lois de composition internes $*$ existe-t-il sur X tel que $(X, *)$ soit un groupe?
   *(b) Même que la question précédente, mais pour X de cardinal trois. Remarque: plus tard nous aurons les moyens de dire quelque chose de général pour X de cardinal fini n quelconque; la question est liée au nombre de groupes d'ordre n à isomorphisme près, et aux ordres de leurs groupes d'automorphismes.
   **(c) Est-ce que tout ensemble non vide peut être muni d'une structure de groupe?
5. Soit G un groupe. Montrer, en n'utilisant que la formule d'associativité dans la définition de groupe, que pour tous a, b, c, d et f dans G on a $(ab)(c(df)) = ((a(bc))d)f$.
6. (a) De combien de façons peut-on insérer trois paires de parenthèses dans le produit $x_1x_2x_3x_4x_5$ tel que le produit soit défini sans supposer la multiplication associative, et sans convention particulière comme en (I.1.3.5) du polycopié?
   *(b) (Problème de Catalan.) Pour $n \geq 3$, soit a_n le nombre de façons dont on peut insérer $n-2$ paires de parenthèses dans le produit $x_1x_2\cdots x_n$ tel que le produit soit défini sans hypothèse d'associativité, et sans convention. Posons $a_1 = a_2 = 1$. Montrer que pour $n \geq 2$ on a la formule de récurrence:
   $$a_n = \sum_{\substack{i+j=n \\ i \geq 1, j \geq 1}} a_i a_j,$$
   et en déduire que $a_n = \frac{1}{n}\binom{2n-2}{n-1}$. On pourra consulter le livre "Analyse combinatoire", par Louis Comtet, tome premier, page 66.

7. *(a) Donner un exemple d'un couple $(G,*)$ avec G un ensemble avec loi de composition interne $*$, satisfaisant aux conditions (ii) et (iii) de la définition de groupe, mais non à la condition (i).

   **(b) Même que (a), mais où en plus il existe, pour tout x et y dans G, des éléments uniques z et t de G tel que $zx = y = xt$. (Indication: on peut y arriver avec cinq éléments.) Est-ce qu'on peut même demander que $y = y'$ pour tout x?

8. (a) Soit G un groupe tel que pour tout x et y dans G on ait $(xy)^{-1} = x^{-1}y^{-1}$. Montrer que G est commutatif.

   (b) Soit G un groupe tel que pour tout x et y dans G on ait $(xy)^2 = x^2y^2$. Peut-on conclure que G est commutatif?

   *(c) Donner un exemple d'un groupe non commutatif G tel que pour tous x et y dans G on ait $(xy)^3 = x^3y^3$. Indication: considérer les a dans $\mathrm{M}(3, \mathbb{Z}/3\mathbb{Z})$ tel que $a_{i,i} = 1$ pour $1 \leq i \leq 3$ et $a_{i,j} = 0$ pour $1 \leq j < i \leq 3$. (Cela donne même un groupe non commutatif avec $x^3 = e$ pour tout x.)

   ***(d) Soit S un sous-ensemble de $\mathbb{Z}$, et G un groupe tel que pour tout n dans S et pour tous x et y dans G on ait $(xy)^n = x^ny^n$. Notons d le plus grand commun diviseur des entiers $n(n-1)/2$, où n parcourt S. Si $d = 1$, il est vrai que G est commutatif. Un cas pas trop difficile est: $S = \{3, 5\}$. Réciproquement, si tout G comme en haut est commutatif, alors $d = 1$.

*9. Soit K un corps fini, de cardinal q. (On sait que q est une puissance d'un nombre premier, mais cela ne joue aucun rôle dans cet exercice.) Soit $n \geq 0$ un entier. Montrer que $\mathrm{GL}(n, K)$ est d'ordre $\prod_{i=0}^{n-1}(q^n - q^i)$. Indication: un élément de $\mathrm{M}(n, K)$ est inversible si et seulement si ses colonnes forment une K-base de K^n.

10. Soit p un nombre premier, et notons $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Soit G un groupe commutatif, noté additivement, tel que pour tout x dans G on ait $px = 0$.

    (a) Montrer que l'application $\mathbb{F}_p \times G \to G$, $(\overline{a}, x) \mapsto ax$ est une loi de composition externe qui fait de G un $\mathbb{F}_p$-espace vectoriel.

    (b) Montrer que G est fini si et seulement si sa dimension en tant que $\mathbb{F}_p$-espace vectoriel est finie, et qu'on a alors la formule $|G| = p^{\dim(G)}$.

11. Soit G un groupe commutatif, noté additivement, tel que pour tout x dans G et tout entier n non nul il existe un unique y dans G avec $ny = x$. Montrer que G est le groupe additif sous-jacent à un $\mathbb{Q}$-espace vectoriel.

12. Soit G le sous-groupe $\{e^{2\pi i x} \mid x \in \mathbb{Q}\}$ de $\mathbb{C}^*$.

    (a) Montrer que tout élément de G est d'ordre fini.

    (b) Montrer que G est "divisible": pour tout x dans G et tout entier $n \neq 0$ il existe y dans G tel que $x = y^n$.

    (c) Est-ce que G est le groupe additif sous-jacent à un $\mathbb{Q}$-espace vectoriel?

*13. Soit G un groupe fini et x dans G d'ordre deux. Montrer que $|G|$ est pair. Indication: considérer l'application $l_x : y \mapsto xy$ de G vers G.

*14. Soit G un groupe fini d'ordre pair. Montrer qu'il existe x dans G avec $x \neq e$ et $x^2 = e$. Indication: considérer l'application $i : x \mapsto x^{-1}$ de G vers G.

15. Écrire les permutations suivantes comme produit de cycles disjoints.

    (a) $(3,1,4)(1,5,9,2,6)(5,3)$ dans $\mathfrak{S}_9$.

    (b) σ^{-1}, où $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{smallmatrix}\right)$ dans $\mathfrak{S}_5$.

    (c) σ^{-1}, où $\sigma = (5,6,2)(1,3)$ dans $\mathfrak{S}_6$.

16. Soit $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{smallmatrix}\right)$ dans $\mathfrak{S}_{12}$. Calculer σ^{2000}.

17. Soient $n \geq l \geq 0$, $\gamma = (i_1, \ldots, i_l)$ un l-cycle dans $\mathfrak{S}_n$, et σ dans $\mathfrak{S}_n$. Montrer que $\sigma\gamma\sigma^{-1}$ est le l-cycle $(\sigma(i_1), \ldots, \sigma(i_l))$.

18. Soient $n \geq 0$ et X un ensemble de cardinal n. Soit $f\colon \{1, 2, \ldots, n\} \to X$ une bijection. Montrer que $F\colon \mathfrak{S}_n \to \mathfrak{S}(X)$, $\sigma \mapsto f \circ \sigma \circ f^{-1}$ est un isomorphisme de groupes.

*19. Est-ce que $\mathfrak{S}(\mathbb{N})$ contient des éléments d'ordre infini ? Est-ce que le produit de deux éléments d'ordre fini est lui aussi d'ordre fini ? Indication: les réponses sont les mêmes si on remplace $\mathbb{N}$ par $\mathbb{Z}$, ou par $\mathbb{Q}$, ou par $\mathbb{Q}^2$, par exemple.

20. Déterminer les sept ensembles $X_n := \{\text{ordre}(\sigma) \mid \sigma \in \mathfrak{S}_n\}$, $1 \leq n \leq 7$.

*21. Montrer que $\sigma \in \mathfrak{S}_n$ entraîne que $\text{ordre}(\sigma) \leq e^{n/e}$.

22. (a) Trouver les σ dans $\mathfrak{S}_4$ tels que $\sigma^2 = (1,2)(3,4)$.
    *(b) Soit $n \geq 2$. Existe-t-il un σ dans $\mathfrak{S}_n$ tel que $\sigma^2 = (1,2)$? Même question pour $n \geq 6$ et $\sigma^2 = (1,2)(3,4,5,6)$.

23. (a) Soit $n \geq 1$ un entier. Déterminer la somme de tous les éléments du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
    (b) Soit $n \geq 1$ un entier. Notons $\mu_n(\mathbb{C})$ l'ensemble des solutions complexes de $x^n = 1$. Montrer que la multiplication des nombres complexes induit une structure de groupe sur $\mu_n(\mathbb{C})$. Déterminer le produit de tous les éléments de $\mu_n(\mathbb{C})$.

24. Déterminer, à isomorphisme près, tous les groupes d'ordre un, deux, trois et quatre, et donner leurs tables de groupe.

25. (a) Est-ce que $\mathbb{Z}/6\mathbb{Z}$ est isomorphe à $\mathfrak{S}_3$?
    (b) Est-ce que $\mathbb{Z}/6\mathbb{Z}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$?
    (c) Est-ce que $(\mathbb{R}, +)$ est isomorphe à $(\mathbb{R}_+^*, \cdot)$?
    (d) Est-ce que $(\mathbb{R}^*, \cdot)$ est isomorphe à $(\mathbb{C}^*, \cdot)$?
    (e) Est-ce que $(\mathbb{Q}^*, \cdot)$ est isomorphe à $(\mathbb{R}^*, \cdot)$?
    (f) Est-ce qu'il existe un morphisme de groupe f surjectif de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \cdot)$?

Licence — Algèbre. Feuille d'exercices N° 2

13-10/97

1. Soit G un groupe et $f\colon G \to G$ un morphisme tel que pour tout x dans G on a $f(f(x)) = x^{-1}$.
   (a) Est-que G est nécessairement commutatif?
   *(b) Donner un exemple de tels G et f, avec f différent de Id_G.
2. (2.2.5 du polycopié.) Soient V et W des $\mathbb{Q}$-espaces vectoriels, et $f\colon V \to W$ un morphisme de groupes de $(V,+)$ vers $(W,+)$. Montrer que f est en fait $\mathbb{Q}$-linéaire.
3. (2.2.7 du polycopié.) Montrer que les seuls endomorphismes de $(\mathbb{Z},+)$ sont les $n \mapsto an$, avec a dans $\mathbb{Z}$.
4. Soit G un groupe. Soit $\mathrm{Aut}(G)$ l'ensemble d'automorphismes de G.
   (a) Montrer que $(\mathrm{Aut}(G), \circ)$, où $\circ$ est la composition, est un groupe. Montrer que pour tout x dans G l'application $\mathrm{int}_x\colon G \to G\colon y \mapsto xyx^{-1}$ est un automorphisme de G.
   (b) Montrer que $\mathrm{int}\colon G \to \mathrm{Aut}(G)\colon x \mapsto \mathrm{int}_x$ est un morphisme. Son image s'appelle le groupe des automorphismes intérieurs de G et se note $\mathrm{Inn}(G)$.
   *(c) Montrer que $\mathrm{Inn}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$, c'est à dire, montrer que pour x dans G et σ dans $\mathrm{Aut}(G)$ on a $\sigma \mathrm{int}_x \sigma^{-1}$ dans $\mathrm{Inn}(G)$.
   (d) Monter que le noyau $\mathrm{Ker}(\mathrm{int})$ de $\mathrm{int}\colon G \to \mathrm{Aut}(G)$ est le centre $C(G)$ de G.

**5. Soit G un groupe tel que $\mathrm{Aut}(G)$ soit de cardinal un. Montrer que G est soit trivial, soit isomorphe à $(\mathbb{Z}/2\mathbb{Z},+)$.

6. Pour chacun des triples (G,H,f) suivants avec G et H des groupes et $f\colon G \to H$ une application, décider si f est un morphisme, et, dans le cas où il en est un, décider si f est injectif, si f est surjectif et si f est un isomorphisme.
   (a) $f\colon (\mathrm{M}(100,\mathbb{R}),+) \to (\mathrm{M}(100,\mathbb{R}),+)$, $a \mapsto a + {}^t a$.
   (b) $f\colon (\mathrm{M}(100,\mathbb{R}),+) \to (\mathrm{M}(100,\mathbb{R}),+)$, $a \mapsto ba$, avec b dans $\mathrm{M}(100,\mathbb{R})$ fixe.
   (c) $f\colon \mathrm{GL}(100,\mathbb{R}) \to \mathrm{GL}(100,\mathbb{R})$, $a \mapsto {}^t a$.
   (d) $f\colon \mathrm{GL}(100,\mathbb{R}) \to \mathrm{GL}(100,\mathbb{R})$, $a \mapsto {}^t a a$.
   (e) $f\colon \mathrm{GL}(100,\mathbb{R}) \to \mathbb{R}^*$, $a \mapsto \det(a)$.
   (f) $f\colon \mathrm{M}(100,\mathbb{R}) \to \mathrm{GL}(100,\mathbb{R})$, $a \mapsto \exp(a)$.
   (g) $f\colon (\mathbb{R},+) \to \mathrm{GL}(100,\mathbb{R})$, $t \mapsto \exp(ta)$, pour a dans $\mathrm{M}(100,\mathbb{R})$ fixe.
   (h) $f\colon (\mathbb{R},+) \to (\mathbb{R},+)$, $a \mapsto a + \arctan(1/(1+\sqrt{2})) - \pi/8$.
   (i) $f\colon \mathbb{C}^* \to \mathbb{R}^*$, $z \mapsto |z|$.
7. (a) Est-ce que le sous-ensemble $\{-1,0,1\}$ de $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$?
   (b) Soit $n \geq 2$. Est-ce que $\{g \in \mathrm{GL}(n,\mathbb{R}) \mid {}^t g = g\}$ est un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$?
   (c) Soit $n \geq 2$. Est-ce que $\{g \in \mathrm{GL}(n,\mathbb{R}) \mid {}^t g^{-1} = g\}$ est un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$?
   (d) Soit G un groupe. Est-ce que $\{x \in G \mid x^2 = e\}$ est un sous-groupe de G?
8. Soit H un sous-ensemble non vide d'un groupe G, stable par la loi de groupe. Est-ce que H est un sous-groupe? Et si on suppose que H est fini?
9. Soit G un groupe commutatif. Montrer que le sous-ensemble H de G des élements d'ordre fini est un sous-groupe.
10. Donner un exemple d'un groupe G et des sous-groupes H_1 et H_2, tels que $H_1 \cup H_2$ n'est pas un sous-groupe.

*11. Soit G un groupe, H_1 et H_2 des sous-groupes. Montrer que $H_1 \cup H_2$ est un sous-groupe si et seulement si $H_1 \subset H_2$ ou $H_2 \subset H_1$.

12. Soit G un groupe. Un élément de G de la forme $xyx^{-1}y^{-1}$ est appelé un commutateur. Soit G' le sous-groupe de G engendré par tous les commutateurs: $G' = \langle\{xyx^{-1}y^{-1} \mid x, y \in G\}\rangle$.
    (a) Montrer que G' est un sous-groupe distingué de G.
    (b) Soit $f: G_1 \to G_2$ un morphisme avec G_2 commutatif. Montrer que $G'_1 \subset \mathrm{Ker}(f)$.
13. Soit $f: G_1 \to G_2$ un morphisme et x dans G_1 d'ordre fini. Montrer que ordre$(f(x))$ divise ordre(x).
14. Soit $G := \{\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \in \mathrm{M}(2, \mathbb{R}) \mid b \neq 0\}$.
    (a) Montrer que G est un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$.
    (b) Montrer que $H_1 := \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right) \mid b \neq 0\}$ est un sous-groupe non-distingué de G.
    (c) Montrer que $H_2 := \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbb{R}\}$ est un sous-groupe distingué de G.
    (d) Montrer que $f_1: G \to \mathbb{R}^*$: $\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \mapsto b$ est un morphisme et que $H_2 = \mathrm{Ker}(f_1)$.
    (e) Montrer que $f_2: G \to \mathbb{R}$: $\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \mapsto a$ n'est pas un morphisme.
    (f) Montrer que $g_1: \mathbb{R}^* \to H_1$: $b \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right)$ est un isomorphisme.
    (g) Montrer que $g_2: \mathbb{R} \to H_2$: $a \mapsto \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ est un isomorphisme.
15. Soit $f: G_1 \to G_2$ un morphisme de groupes.
    (a) Montrer que pour tout sous-groupe $H_1 \subset G_1$, l'image fH_1 de H_1 par f est un sous-groupe de G_2.
    (b) Montrer que pour tout sous-groupe $H_2 \subset G_2$, l'image réciproque $f^{-1}H_2$ de H_2 par f est un sous-groupe de G_1 contenant $\mathrm{Ker}(f)$.
    *(c) Soit maintenant f surjectif, $X_1 := \{H_1 \subset G_1 \mid H_1$ sous-groupe contenant $\mathrm{Ker}(f)\}$ et $X_2 = \{H_2 \subset G_2 \mid H_2$ sous-groupe$\}$. On a alors des applications $f_*: X_1 \to X_2$: $H_1 \mapsto fH_1$ et $f^*: X_2 \to X_1$: $H_2 \mapsto f^{-1}H_2$. Montrer que f_* et f^* sont des applications inverses.

*16. Soit $n \in \mathbb{Z}$. Déterminer tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

*17. Déterminer les centres des $\mathfrak{S}_n$, $n \geq 0$.

*18. Déterminer les centres des $\mathrm{GL}(n, K)$, pour tout $n \geq 0$ et tout corps K.

19. (Polycopié 11.7.2–11.7.4.) Soit $n \geq 0$.
    *(a) Montrer que $\mathfrak{S}_n$ est engendré par $\{(1, i) \mid 2 \leq i \leq n\}$.
    *(b) Montrer que $\mathfrak{S}_n$ est engendré par $\{(1, 2), (2, 3, \ldots, n)\}$.
    *(c) Montrer que $\mathfrak{S}_n$ est engendré par $\{(i, i+1) \mid 1 \leq i < n\}$.
    *(d) Montrer que $\mathfrak{S}_n$ est engendré par $\{(1, 2), (1, 2, \ldots, n)\}$.

**20. Pour quels n est-ce que $\{(1, 2, 3), (3, 4, \ldots, n)\}$ engendre $\mathfrak{S}_n$?

**21. Soit K un corps. Soit $n \geq 0$. Pour $1 \leq i, j \leq n$ notons $e(i, j)$ l'élément de $\mathrm{M}(n, K)$ tel que $e(i, j)_{k,l} = 1$ si $i = k$ et $j = l$ et $e(i, j)_{k,l} = 0$ sinon.
    (a) Montrer que $\mathrm{GL}(n, K)$ est engendré par la réunion de l'ensemble de ses éléments diagonaux avec l'ensemble $\{I + ae(i, j) \mid i \neq j,\ a \in K\}$. (Indication: penser aux opérations élémentaires sur lignes et colonnes.)
    (b) Est-ce encore vrai si au lieu de toutes les matrices diagonales on ne prend que celles avec $a_{i,i} = 1$ pour $i > 1$?
    (c) Est-ce que $\mathrm{GL}(n, K)$ est engendré par la réunion de l'ensemble de matrices diagonales avec $a_{i,i} = 0$ pour $i > 0$ avec l'ensemble $\{I + e(i, j) \mid i \neq j\}$.

22. (a) Soit $\sigma = (i_1, \ldots, i_k)$ un cycle de longueur k dans $\mathfrak{S}_n$. On considère l'opération de $\langle\sigma\rangle \subset \mathfrak{S}_n$ sur $\{1, 2, \ldots, n\}$. Déterminer les orbites pour cette opération.
    (b) Soit $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ une décomposition en cycles disjoints d'un élément σ de $\mathfrak{S}_n$. Donner la relation entre les longueurs l_i des σ_i et les cardinaux des orbites dans $\{1, 2, \ldots, n\}$ pour l'opération de $\langle\sigma\rangle$.

23. Soit G un groupe. On considère l'opération à gauche de G sur lui-même par conjugaison. L'orbite $\{aba^{-1} \mid a \in G\}$ de b s'appelle la classe de conjugaison de b. Le stabilisateur $G_b = \{a \in G \mid aba^{-1} = b\}$ s'appelle le centralisateur de b et se note $Z_G(b)$.
   (a) Déterminer les classes de conjugaison et les centralisateurs dans $\mathfrak{S}_3$.
   *(b) Soit $n \geq 1$. On appelle partition de n une suite finie $(x_1, x_2, \ldots, x_r)$ d'entiers telle que $n = x_1 + x_2 + \cdots + x_r$ et $x_1 \geq x_2 \geq \cdots \geq x_r > 0$. Donner une bijection entre l'ensemble des classes de conjugaison dans $\mathfrak{S}_n$ et l'ensemble des partitions de n.
   (c) Pour tout σ dans $\mathfrak{S}_4$, déterminer son centralisateur $Z_{\mathfrak{S}_4}(\sigma)$ et sa classe de conjugaison $\mathrm{conj}(\sigma)$. Vérifier dans chaque cas que $|\mathrm{conj}(\sigma)|\,|Z_{\mathfrak{S}_4}(\sigma)| = |\mathfrak{S}_4|$.
24. Soit G un groupe opérant à gauche sur un ensemble X. Soit $F := \{f \colon X \to \mathbb{R}\}$ l'ensemble des fonctions sur X à valeurs dans $\mathbb{R}$. Montrer que l'application $F \times G \to F$: $(f, a) \mapsto (x \mapsto f(ax))$ définit une opération à droite de G sur F. Le choix de $\mathbb{R}$ est-il essentiel? Est-ce qu'on aurait pu prendre un ensemble quelconque au lieu de $\mathbb{R}$?
25. Soient K un corps et $n \geq 1$ un entier. Montrer que l'application $\mathrm{GL}(n, K) \times K^n \to K^n$: $(a, x) \mapsto ax$ définit une opération à gauche. Quel est le nombre d'orbites?
26. Soient K un corps et $n \geq 1$ un entier. Nous allons étudier les relations d'équivalence induites par quelques opérations de $\mathrm{GL}(n, K)$ sur $\mathrm{M}(n, K)$.
   (a) Considérons l'opération de $\mathrm{GL}(n, K)$ sur $\mathrm{M}(n, K)$ par conjugaison. Montrer que pour x et y dans $\mathrm{M}(n, K)$ on a $x \sim y$ si et seulement si x et y sont des matrices semblables.
   *(b) Faisons opérer $\mathrm{GL}(n, K)$ sur $\mathrm{M}(n, K)$ par multiplication à gauche. Montrer que pour x et y dans $\mathrm{M}(n, K)$ on a $x \sim y$ si et seulement si $\mathrm{Ker}(x) = \mathrm{Ker}(y)$.
   *(c) Faisons opérer $\mathrm{GL}(n, K)$ sur $\mathrm{M}(n, K)$ à droite par multiplication à droite. Montrer que pour x et y dans $\mathrm{M}(n, K)$ on a $x \sim y$ si et seulement si $\mathrm{Im}(x) = \mathrm{Im}(y)$.

*27. Soient K un corps et $n \geq 1$, $m \geq 1$ des entiers. Considérons l'opération suivante de $\mathrm{GL}(n, K) \times \mathrm{GL}(m, K)$ sur $\mathrm{M}(n, m, K)$ donnée par: $(g, h) \cdot x = gxh^{-1}$. Soit $\sim$ la relation d'équivalence sur $\mathrm{M}(n, m, K)$ induite par cette opération. Montrer que pour x et y dans $\mathrm{M}(n, m, K)$ on a $x \sim y$ si et seulement si x et y ont même rang.

Licence — Algèbre. Feuille d'exercices N° 3

20-10/97

1. Soit $E(n)$ le nombre de relations d'équivalence sur l'ensemble $\{1, 2, \ldots, n\}$. Calculer $E(n)$ pour $n \leq 5$.
2. Pour chaque relation d'équivalence sur $\{1, 2, 3\}$, écrire explicitement l'ensemble quotient, et l'application quotient.
3. (5.4.4 du polycopié.) Soit G un groupe, opérant à gauche sur un ensemble X. Notons $f: G \to \mathfrak{S}(X)$ le morphisme correspondant à cette action.
   (a) Montrer que $\mathrm{Ker}(f)$ est l'intersection des stabilisateurs G_x, où x parcourt X.
   (b) On dit que l'action de G sur X est fidèle si f est injectif. Est-ce que toute action libre est fidèle?
   *(c) Est-ce que toute action fidèle est libre?

*4. Soit K un corps. Pour $n \geq 0$, notons $\mathbb{P}^n(K)$ l'ensemble des sous-K-espaces vectoriels de dimension un de K^{n+1}. Le groupe $\mathrm{GL}(n+1, K)$ opère sur $\mathbb{P}^n(K)$ par: $g * L := gL$. Quel est le noyau du morphisme $\mathrm{GL}(n+1, K) \to \mathfrak{S}(\mathbb{P}^n(K))$?

5. Soit G un groupe opérant à gauche sur un ensemble X. Soit $n \geq 1$. On dit que l'action de G sur X est n-transitive si pour tous $(x_1, x_2, \ldots, x_n)$ et $(y_1, y_2, \ldots, y_n)$ dans X^n avec les x_i tous distincts et les y_i tous distincts il existe g dans G tel que $g(x_i) = y_i$ pour tout i.
   (a) Montrer que l'action de $\mathfrak{S}_n$ sur $\{1, 2, \ldots, n\}$ est n-transitive.
   *(b) Soit K un corps. Montrer que l'action de $\mathrm{GL}(2, K)$ sur $\mathbb{P}^1(K)$ est 3-transitive, et que l'action de $\mathrm{GL}(3, K)$ sur $\mathbb{P}^2(K)$ est 2-transitive mais pas 3-transitive.
6. (6.7.4 du polycopié.) Soient G un groupe et H un sous-groupe. Montrer que l'application $i: G \to G$, $g \mapsto g^{-1}$ induit une bijection entre $H \backslash G$ et G/H.
7. (6.8.3 du polycopié.) Soient G un groupe, $H \subset G$ un sous-groupe, et $K \subset H$ un sous-groupe. Montrer que $(G : K) = (G : H)(H : K)$. Indication: voir le polycopié.

*8. Soit $f: G_1 \to G_2$ un morphisme de groupes. Supposons que G_1 est engendré par l'ensemble de ses éléments d'ordre 2 et que G_2 est fini et d'ordre impair. Montrer que f est trivial.

9. Soient G et H deux groupes, $x \in G$ d'ordre n et $y \in H$ d'ordre m. Montrer que l'ordre de l'élément (x, y) de $G \times H$ est le plus petit commun multiple de n et m.
10. Soit G un groupe. Soient a et b dans G.
    (a) Montrer que a, a^{-1}, bab^{-1} ont tous même ordre.
    (b) Montrer que ab et ba ont même ordre.
    (c) Soit n un entier. Exprimer l'ordre de a^n en termes de celui de a.
    (d) Supposons que $ab = ba$, que $\langle a \rangle \cap \langle b \rangle = \{e\}$, et que a et b sont d'ordre fini n et m, respectivement. Exprimer l'ordre de ab en termes de n et m.
    (e) Supposons que $ab = ba$, et que a et b sont d'ordre fini n et m, respectivement, avec n et m premiers entre eux. Exprimer l'ordre de ab en n et m.

*11. Soit G un groupe fini. Supposons qu'il existe x dans G, $x \neq e$, tel que

$$G = \{e\} \cup \{gxg^{-1} \mid g \in G\}.$$

Montrer que G est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

*12. Soient p, q et r trois nombres premiers (non nécessairement distincts) et G un groupe d'ordre pqr. Montrer que G peut être engendré par 3 éléments. Donner un exemple d'un tel G qui ne peut pas être engendré par deux éléments.

*13. Montrer que tout groupe d'ordre quatre est soit isomorphe à $\mathbb{Z}/4\mathbb{Z}$, soit à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

*14. Montrer que tout groupe d'ordre six est soit isomorphe à $\mathbb{Z}/6\mathbb{Z}$, soit à $\mathfrak{S}_3$.

*15. On dit qu'un groupe G est cyclique s'il existe un élément x dans G tel que $G = \langle x \rangle$. Montrer qu'un groupe fini d'ordre un nombre premier p est cyclique.

*16. Soient G un groupe fini et $H \subset G$ un sous-groupe. Supposons que $H \neq G$. Nous allons montrer que H ne coupe pas toutes les classes de conjugaison de G, ou autrement dit, qu'il existe une classe de conjugaison C de G telle que $H \cap C = \emptyset$.

(a) Montrer que H coupe toutes les classes de conjugaison de G si et seulement si

$$\bigcup_{a\in G} aHa^{-1} = G.$$

(b) Montrer que pour a et b dans G: $aH = bH$ entraîne $aHa^{-1} = bHb^{-1}$.

(c) Soit $n = |G|$ et $d = |H|$. Montrer que

$$\left|\bigcup_{a\in G} aHa^{-1}\right| \leq 1 + (n/d)(d-1)$$

(Indication: $|aHa^{-1}| = d$ et $e \in aHa^{-1}$.)

*17. Soit G un groupe opérant sur un ensemble X. Supposons que $|G| = 143 = 11.13$ et que $|X| = 108$. Montrer qu'il existe un x dans X tel que $G_x = G$.

*18. Un groupe de 35 éléments opère sur un ensemble de 19 éléments sans point fixe. Combien y a-t-il d'orbites pour cette opération?

*19. On se propose de déterminer tous les groupes finis qui ont exactement trois classes de conjugaison. Soit donc G un groupe fini, disons d'ordre n, et supposons que G a exactement trois classes de conjugaison.

(a) En considérant l'opération de G sur G par conjugaison, montrer qu'on a

$$(*) \qquad 1 = \frac{1}{n} + \frac{1}{a} + \frac{1}{b}$$

avec des entiers $a \geq b > 0$ tels que $a|n$ et $b|n$.

(b) Déterminer toutes les solutions de l'équation $(*)$ en entiers $n \geq a \geq b > 0$ tels que $a|n$ et $b|n$. (Indication: on a $b \leq 3$ car $n \geq a \geq b$.)

(c) Donner la liste complète des groupes finis, à isomorphisme près, qui ont exactement trois classes de conjugaison.

20. (7.2.1 du polycopié.) Soient k et n deux entiers tels que $0 \leq k \leq n$. Soit E l'ensemble des parties à k éléments de l'ensemble $\{1, 2, \ldots, n\}$. Le cardinal de E est noté $\binom{n}{k}$. Montrer, comme indiqué dans le polycopié, que $\binom{n}{k}$ est égal à $n!/k!(n-k)!$.

21. Soient n et r des entiers positifs. Soient $k_1, \ldots, k_r$ des entiers positifs tels que $n = k_1 + \cdots + k_r$. Généraliser l'exercice précédent au cas du nombre de partitions de l'ensemble $\{1, \ldots, n\}$ en parties $X_1, \ldots, X_r$, avec $|X_i| = k_i$.

22. (7.5.2 du polycopié.) Faites l'exercice 7.5.2 du polycopié.

*23. Soient K un corps fini, et q son cardinal.

(a) Soient $n \geq m \geq 0$ des entiers. Notons $G(n,m)$ l'ensemble des sous-K-espaces vectoriels de dimension m de K^n. Le groupe $\mathrm{GL}(n,K)$ opère sur $G(n,m)$ par $g * V := gV$. Montrer que cette action est transitive, et calculer $|G(n,m)|$. Remarquer que cette fonction de q est donnée par un polynôme à coefficients dans $\mathbb{Z}$. Noter aussi que $\mathbb{P}^n(K) = G(n+1, 1)$. Comment expliquez-vous sans calculer que $|G(n,n-m)| = |G(n,m)|$?

(b) Soient n, m et r des entiers positifs. Calculer le cardinal du sous-ensemble $R(n,m,r)$ de $\mathrm{M}(n,m,K)$ des matrices de rang r. Indication: faire opérer le groupe produit $\mathrm{GL}(n,K) \times \mathrm{GL}(m,K)$.

24. Soit $n \geq 0$. Notons X l'ensemble des formes $\mathbb{R}$-bilinéaires symétriques définies positives $b\colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$. Pour g dans $\mathrm{GL}(n,\mathbb{R})$, b dans X et x, y dans $\mathbb{R}^n$, posons $(b{*}g)(x,y) := b(gx,gy)$.

   *(a) Montrer que ceci définit une action à droite de $\mathrm{GL}(n,\mathbb{R})$ sur X. Notons b_0 le produit scalaire standard: $b_0(x,y) = {}^t xy$. Montrer que le stabilisateur de b_0 est le groupe $\mathrm{O}(n,\mathbb{R})$ des matrices orthogonales. Est-ce que l'action de $\mathrm{GL}(n,\mathbb{R})$ sur X est transitive?

   **(b) Identifions X à l'ensemble M des a dans $\mathrm{M}(n,\mathbb{R})$ qui sont symétriques et définies positives. Montrer que l'application quotient de $\mathrm{GL}(n,\mathbb{R})$ vers M envoie g vers ${}^t gg$. En considérant M comme sous-ensemble de $\mathrm{GL}(n,\mathbb{R})$, l'application de M vers M induite est donc $a \mapsto a^2$. Pour a dans M, notons $\sqrt{a}$ l'élément unique de M tel que $\sqrt{a}^2 = a$. Conclure que l'application $s\colon M \to \mathrm{GL}(n,\mathbb{R})$, $a \mapsto \sqrt{a}$, est une section de l'application quotient, et que tout g dans $\mathrm{GL}(n,\mathbb{R})$ s'écrit de façon unique comme au, avec a dans M et u dans $\mathrm{O}(n,\mathbb{R})$. Ceci s'appelle la décomposition polaire.

*25. Soit $n \geq 0$. Notons Y l'ensemble des formes $\mathbb{R}$-bilinéaires symétriques sur $\mathbb{R}^n$. Comme en haut, $\mathrm{GL}(n,\mathbb{R})$ opère à droite sur Y. Quel est le nombre d'orbites?

Licence — Algèbre. Feuille d'exercices N° 4

27-10/97

1. (6.8.1 du polycopié.) Soient G un groupe, et $H \subset G$ un sous-groupe d'indice deux. Montrer que H est distingué.
2. (8.6.1 du polycopié.) Faites l'exercice 8.6.1 du polycopié.
3. (8.8.6 du polycopié.) Soient G un groupe et C son centre. Montrer que tout sous-groupe de C est distingué dans G, et que G/C est isomorphe au groupe d'automorphismes intérieurs de G.
4. En appliquant directement les définitions, calculer une table de multiplication pour le groupe quotient $\mathbb{Z}/3\mathbb{Z}$. Même chose pour $\mathbb{R}^*/\mathbb{R}^*_{>0}$.
5. Soient G un groupe et $G' \subset G$ le sous-groupe engendré par les commutateurs: $G' = \langle\{xyx^{-1}y^{-1} \mid x, y \in G\}\rangle$. Montrer que G' est distingué. Montrer que G/G' est commutatif, et même caractéristique (cf. ex. 9).
6. Pour G un groupe, notons G_{tors} l'ensemble des éléments d'ordre fini de G; on dira que G est sans torsion si $G_{\text{tors}} = \{e\}$. Soit maintenant G un groupe commutatif. Nous avons déjà vu que G_{tors} est alors un sous-groupe de G. Montrer que G/G_{tors} est sans torsion, et que tout morphisme $f: G \to H$ avec H sans torsion se factorise de façon unique par $G \to G/G_{\text{tors}}$.

**7. Soient K un corps, et $n \geq 3$. Notons $G := \mathrm{GL}(n, K)$, et G' le sous-groupe de G engendré par les commutateurs de G. Nous allons montrer que $G' = \mathrm{SL}(n, K)$, le sous-groupe de matrices de déterminant un.
   (a) Montrer que $G' \subset \mathrm{SL}(n, K)$.
   (b) Pour $1 \leq i, j \leq n$ notons $e(i, j)$ l'élément de $\mathrm{M}(n, K)$ tel que $e(i, j)_{k,l} = 1$ si $i = k$ et $j = l$ et $e(i, j) = 0$ sinon. Soit a dans K. Montrer que $\mathrm{SL}(n, K)$ est engendré par l'ensemble des $\{I + ae(i, j) \mid 1 \leq i, j \leq n,\ i \neq j\ a \in K\}$. (Indication: penser aux opérations élémentaires sur les lignes et colonnes.)
   (c) Pour a dans K, calculer le commutateur de $I + ae(1, 2)$ et $I + e(2, 3)$.
   (d) Montrer que pour $1 \leq i, j \leq n$ avec $i \neq j$ et pour a dans K, $I + ae(i, j)$ est un conjugué de $I + ae(1, 2)$.
   (e) Montrer que $G' = \mathrm{SL}(n, K)$.
   (f) Montrer que tout morphisme $f: \mathrm{GL}(n, K) \to H$ avec H commutatif se factorise de façon unique par $\det: \mathrm{GL}(n, K) \to K^*$.

8. Soient G un groupe et $N \subset G$ un sous-groupe distingué. Montrer que $G/N = \{\overline{e}\}$ si et seulement si $N = G$. (Indication: utiliser les définitions.)
9. Un sous-groupe H d'un groupe G est dit caractéristique si pour tout automorphisme σ de G on a $\sigma(H) = H$. Soient G un groupe et $H_2 \subset H_1 \subset G$ des sous-groupes.
   (a) Supposons que H_1 est caractéristique dans G. Est-il distingué?
   *(b) Supposons que H_1 est distingué dans G. Est-il caractéristique?
   (c) Supposons que H_1 soit distingué dans G et que H_2 soit caractéristique dans H_1. Est-ce que H_2 est distingué dans G?
   (d) Supposons que H_2 soit distingué dans G. Est-il distingué dans H_1?
   **(e) Supposons que H_1 soit distingué dans G et que H_2 soit distingué dans H_1. Est-ce que H_2 est distingué dans G?
   **(f) Supposons que H_2 soit caractéristique dans H_1. Est-il caractéristique dans H_1?

*10. Soient G un groupe, x, y, z dans G et $N \subset G$ un sous-groupe distingué tels que $x^5 \in N$, $y^7 \in N$ et $y^{-1}zxz^{-1} \in N$. Montrer que $x \in N$ et que $y \in N$. (Indication: calculer dans G/N; quels peuvent être ordre($\overline{x}$), ordre($\overline{y}$) et que peut-on tirer de $y^{-1}zxz^{-1} \in N$?)

11. Soient G un groupe et $N \subset G$ un sous-groupe d'indice fini n.

   *(a) Supposons que N est distingué dans G. Montrer que pour tout x dans G on a $x^n \in N$.

   **(b) Donner un exemple où il existe x dans G avec x^n pas dans N.

*12. Soit H un sous-groupe d'indice fini de $\mathbb{C}^*$. Montrer que $H = \mathbb{C}^*$.

13. Soit G un groupe fini. Notons n l'ordre de G, et p le plus petit nombre premier qui divise n. Supposons que $H \subset G$ est un sous-groupe d'indice p. Nous allons montrer que H est distingué.

   (a) Comme en I.6.9 du polycopié, G opère sur G/H par translation à gauche, ce qui induit un morphisme $f\colon G \to \mathfrak{S}(G/H)$. Montrer que $\mathrm{Ker}(f) \subset H$.

   *(b) Montrer que $|f(G)| = p$ (Indication: quels sont les nombres premiers divisant $p!$?)

   *(c) Montrer que $H = \mathrm{Ker}(f)$.

*14. Soient G_1 et G_2 des groupes, $H_1 \subset G_1$ et $H_2 \subset G_2$ des sous-groupes distingués. Montrer que $H_1 \times H_2$ est un sous-groupe distingué de $G_1 \times G_2$, et que $(G_1 \times G_2)/(H_1 \times H_2)$ est isomorphe à $G_1/H_1 \times G_2/H_2$.

15. Soient G un groupe, H_1 et H_2 des sous-groupes distingués.

   *(a) Supposons que H_1 et H_2 sont isomorphes. Est-il vrai que G/H_1 est isomorphe à G/H_2?

   *(b) Supposons que G/H_1 et G/H_2 sont isomorphes. Est-il vrai que H_1 et H_2 sont isomorphes?

   **(c) Et si on suppose que G est fini?

*16. Soient G un groupe, H_1 et H_2 des sous-groupes distingués tels que $G = H_1H_2$ et $H_1 \cap H_2 = \{e\}$. Montrer que l'application $H_1 \times H_2 \to G$, $(h_1, h_2) \mapsto h_1h_2$, est un isomorphisme. (Indication: montrer d'abord que pour h_1 dans H_1 et h_2 dans H_2 on a $h_2h_1 = h_1h_2$, en considérant $h_1h_2h_1^{-1}h_2^{-1}$.)

17. Soit G un groupe. Soit $H \subset G$ un sous-groupe d'indice fini, et notons n cet indice. Montrer qu'il existe un sous-groupe distingué N dans G, contenu dans H et d'indice au plus $n!$ dans G. (Indication: considérer l'action de G sur G/H.)

18. (a) Soit C le cercle $\{z \in \mathbb{C} \mid |z| = 1\}$. Montrer que C est un sous-groupe de $\mathbb{C}^*$.

   (b) Montrer que $\mathbb{R}/\mathbb{Z}$ est isomorphe à C. (Indication: considérer le morphisme de groupes $f\colon \mathbb{R} \to \mathbb{C}^*\colon x \mapsto \exp(2\pi i x)$.)

19. *(a) Notons X l'ensemble $\{\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}$ des partitions de $\{1,2,3,4\}$ en deux ensembles à deux éléments chacun. Quel est le cardinal de X? Montrer que le morphisme $\mathfrak{S}_4 \to \mathfrak{S}(X)$ induit par l'action naturelle de $\mathfrak{S}_4$ sur X est surjectif.

   (b) Soient $G := \mathfrak{S}_4$ et $N := \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Montrer que $N \subset G$ est un sous-groupe distingué et que G/N est isomorphe à $\mathfrak{S}_3$.

20. Soit $G := \{\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \in \mathrm{M}(2,\mathbb{R}) \mid a \in \mathbb{R},\ b \neq 0\}$. Soit $N := \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{M}(2,\mathbb{R}) \mid a \in \mathbb{R}\}$.

   (a) Montrer que G est un sous-groupe de $\mathrm{GL}(2,\mathbb{R})$. Interpréter G comme stabilisateur pour une action convenable de $\mathrm{GL}(2,\mathbb{R})$.

   (b) Montrer que N est un sous-groupe distingué de G.

   (c) Montrer que G/N est isomorphe à $\mathbb{R}^*$.

21. (10.3.1 du polycopié.) Soit G un groupe fini. Notons n l'ordre de G. Alors G est cyclique si et seulement si G possède un élément d'ordre n.

*22. (10.3.3 du polycopié.) Soit G un groupe. Supposons que les seuls sous-groupes de G sont les sous-groupes triviaux: G et $\{e\}$. Montrer que soit $G = \{e\}$, soit G est cyclique d'ordre premier.

23. (10.3.4 du polycopié.) Pour $n \geq 1$ entier, posons $\Gamma_n = \{z \in \mathbb{C} \,|\, z^n = 1\}$.
   (a) Soit $n \geq 1$ entier. Montrer que Γ_n est un sous-groupe de $\mathbb{C}^*$, cyclique d'ordre n.
   *(b) Soit Γ un sous-groupe fini, d'ordre n disons, de $\mathbb{C}^*$. Montrer que $\Gamma = \Gamma_n$. (Indication: considérer les racines dans $\mathbb{C}$ du polynôme $X^n - 1$.)

*24. (10.3.5 du polycopié.) Soient G un groupe et C son centre. Supposons que G/C est monogène. Montrer que $G = C$. (Indication: prendre un élément γ de G tel que $\overline{\gamma}$ engendre G/C; montrer que γ est dans C.)

25. (10.3.6–7 du polycopié.) Soient p un nombre premier et G un groupe d'ordre p^2.
   *(a) Montrer que G est commutatif.
   *(b) Montrer que G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$, ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

*26. (10.3.8 du polycopié.) Pour quels entiers $m \geq 0$ est-ce que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est monogène?

*27. Combien de morphismes y a-t-il de $\mathbb{Z}/45\mathbb{Z}$ vers $\mathfrak{S}_3$? Et de $\mathfrak{S}_3$ vers $\mathbb{Z}/45\mathbb{Z}$?

28. (11.10.4 du polycopié.) Soient $n \geq 0$ et σ dans $\mathfrak{S}_n$.
   (a) Notons m le nombre d'orbites de σ. Montrer que $\varepsilon(\sigma) = (-1)^{n-m}$.
   (b) Notons s le nombre d'orbites de cardinal pair de σ. Montrer que $\varepsilon(\sigma) = (-1)^s$.

*29. Soit $n \geq 0$. Montrer que A_n est engendré par son sous-ensemble de cycles de longueur trois.

*30. Montrer que $\mathrm{A}_n \subset \mathfrak{S}_n$ est le sous-groupe engendré par les commutateurs de $\mathfrak{S}_n$. (Indication: calculer $(1,2)(1,3)(1,2)^{-1}(1,3)^{-1}$.) Conclure que si $f\colon \mathfrak{S}_n \to G$ est un morphisme avec G commutatif, alors $\mathrm{A}_n \subset \mathrm{Ker}(f)$.

*31. Soit $f\colon \mathfrak{S}_n \to \mathfrak{S}_m$ un morphisme. Montrer que $f\mathrm{A}_n \subset \mathrm{A}_m$. (Indication: utiliser l'exercice précédent.)

32. Soit $n \geq 0$.
   *(a) Trouver $m \geq 0$ et un morphisme injectif $f\colon \mathfrak{S}_n \to \mathrm{A}_m$.
   **(b) Quel est le plus petit $m \geq 0$ tel qu'il existe un morphisme injectif $f\colon \mathfrak{S}_n \to \mathrm{A}_m$?

33. Soit $n \geq 2$. Montrer que l'action de A_n sur $\{1, 2, \ldots, n\}$ est $n-2$-transitive, mais pas $n-1$-transitive.

34. (11.10.7 du polycopié.) En admettant le résultat que A_n est simple pour $n \geq 5$, montrer que pour $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont les deux sous-groupes triviaux, et A_n.

Licence — Algèbre. Feuille d'exercices N° 5

03-11/97

1. Soit $f: A \to B$ un morphisme d'anneaux. On dit que f est un isomorphisme s'il existe un morphisme d'anneaux $g: B \to A$ tel que $g \circ f = \mathrm{Id}_A$ et $f \circ g = \mathrm{Id}_B$.
   (a) Montrer que f est un isomorphisme si et seulement si f est bijectif.
   *(b) Donner un exemple d'anneaux A et B et de morphismes $f: A \to B$ et $g: B \to A$ où $g \circ f = \mathrm{Id}_A$ et $f \circ g \neq \mathrm{Id}_B$.
2. (1.3.8 du polycpoié.) Soit G un groupe commutatif, noté additivement. Pour f_1 et f_2 des applications de G vers G, notons $f_1 + f_2$ et $f_1 f_2$ les applications de G vers G telles que $(f_1 + f_2)(g) = f_1(g) + f_2(g)$, $(f_1 f_2)(g) = f_1(f_2(g))$ pour tout g dans G. Vérifier que, pour f_1 et f_2 dans $\mathrm{End}(G)$, $f_1 + f_2$ et $f_1 f_2$ sont des endomorphismes de G, et que $\mathrm{End}(G)$, muni de ces deux lois, est un anneau unitaire.
3. (1.5.3 du polycopié.) Soit A un anneau. Pour tout élément a de A, notons μ_a l'application $x \mapsto ab$ de A vers A.
   (a) Montrer que l'application $A \to \mathrm{End}(A, +)$, $a \mapsto \mu_a$, est un morphisme d'anneaux.
   (b) Montrer que si A est unitaire, ce morphisme est injectif.
   *(c) Donner des exemples où le morphisme $A \to \mathrm{End}(A, +)$ défini en haut est un isomorphisme, et où il n'en est pas.
   (d) Et si on avait voulu utiliser les multiplications à droite $x \mapsto xa$?

*4. Combien d'anneaux commutatifs unitaires y a-t-il, à isomorphisme près, de cardinal n, pour $0 \leq n \leq 6$?

*5. Soit A un anneau unitaire, tel que $(A, +)$ soit isomorphe à $(\mathbb{Z}, +)$. Montrer que A est isomorphe à $\mathbb{Z}$.

6. Soient A un anneau et $n \geq 0$ un entier. Comme toujours, notons $\mathrm{M}(n, A)$ l'ensemble des matrices de type (n, n) à coefficients dans A. Montrer que l'addition et multiplication usuelles ($(a + b)_{i,j} = a_{i,j} + b_{i,j}$ et $(ab)_{i,j} = \sum_k a_{i,k} b_{k,j}$) font de $\mathrm{M}(n, A)$ un anneau, unitaire si A l'est.
7. Soient A un anneau, a et b dans A, et $n \geq 0$ entier.
   (a) (1.8.4 du polycopié.) Supposons que a et b commutent, c'est à dire, que $ab = ba$. Montrer que
   $$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$
   *(b) Est-ce que l'hypothèse $ab = ba$ est nécessaire?
   (c) Plus généralement, soient $r \geq 0$ entier et $a_1, \ldots, a_r$ dans A des éléments qui commutent deux à deux. Montrer que
   $$(a_1 + \cdots + a_r)^n = \sum_{\substack{k_1 + \cdots + k_r = n \\ k_1, \ldots, k_r \geq 0}} \frac{n!}{k_1! \cdots k_r!} a_1^{k_1} \cdots a_r^{k_r}.$$
8. (a) Soient A un anneau, I un ensemble, et, pour tout i dans I, A_i un sous-anneau de A. Montrer que l'intersection des A_i est un sous-anneau de A. (Quelle est la convention pour $I = \emptyset$?)
   (b) Soient A un anneau unitaire et S un sous-ensemble de A. On définit alors le sous-anneau unitaire $\langle S \rangle$ de A engendré par S comme étant l'intersection de tous les sous-anneaux unitaires de A contenant S. Montrer que $\langle S \rangle$ est le plus petit sous-anneau unitaire de A contenant S, et que $\langle S \rangle$ est l'ensemble des éléments de A de la forme $\sum_{i=1}^{n} \varepsilon_i s_1^{m_1} \cdots s_{r_i}^{m_{r_i}}$, avec $n \geq 0$, $\varepsilon_i = \pm 1$, s_j dans S, $r_i \geq 0$ et $m_i \geq 0$ des entiers.

9. Soit X un ensemble de cardinal trois. Donner un isomorphisme d'anneaux entre $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ et $\mathbb{R}^X$.
10. Soit X un ensemble. Considérons l'anneau $\mathbb{F}_2^X$ (voir 1.3.5 du polycopié). Montrer qu'il est isomorphe à $(\mathcal{P}(X), \Delta, \cap)$, où $\mathcal{P}(X)$ est l'ensemble des parties de X et Δ la différence symétrique.
11. Notons $f\colon \mathbb{R}[X] \to \mathrm{M}(2, \mathbb{R})$ l'application $P \mapsto \left(\begin{smallmatrix} P(0) & P'(0) \\ 0 & P(0) \end{smallmatrix}\right)$. Est-ce que f est un morphisme d'anneaux?
12. (a) Soit A un anneau unitaire, contenant un corps K comme sous-anneau unitaire. Montrer que l'addition de A et la multiplication $K \times A \to A$ font de A un K-espace vectoriel.

    *(b) Est-ce que le résultat de la partie précédente reste vrai si l'on supprime le mot "unitaire"?
13. Soit X un ensemble. Le support d'un élément f de $\mathbb{R}^X$ est défini comme étant l'ensemble des x dans X avec $f(x) \neq 0$. Notons $\mathbb{R}^{(X)}$ le sous-ensemble de $\mathbb{R}^X$ qui consiste des f dont le support est fini. Montrer que $\mathbb{R}^{(X)}$ est un sous-anneau de $\mathbb{R}^X$. Est-il unitaire?
14. Soit G un groupe. Considérons l'ensemble $\mathbb{R}^{(G)}$, muni de son addition naturelle, et muni de la multiplication dite "convolution": $(f_1 * f_2)(g) := \sum_{g_1 g_2 = g} f_1(g_1) f_2(g_2)$. Montrer qu'en effet la fonction $f_1 * f_2$ sur G est bien définie (c'est à dire, que la somme dans la définition est finie), et dans $\mathbb{R}^{(G)}$. Montrer ensuite que $\mathbb{R}^{(G)}$, muni de ces deux lois, est un anneau. Il s'appelle l'algèbre réelle du groupe G. Est-ce qu'on peut remplacer $\mathbb{R}$ par n'importe quel anneau?
15. Est-ce que $\{-1, 0, 1\}$ est un sous-anneau de $\mathbb{Z}$?

**16. Soit A un sous-anneau unitaire de $\mathbb{Q}$. Montrer qu'il existe un sous-ensemble P_1 de l'ensemble P des nombres premiers, tel que A soit l'ensemble des a/b avec a et b premiers entre eux et b de la forme $p_1^{m_1} \cdots p_n^{m_n}$, avec les p_i dans P_1.

**17. Soient K un corps, n et m des entiers tels que $1 \leq m < n$. Montrer qu'il n'y a pas de morphisme d'anneaux unitaires de $\mathrm{M}(n, K)$ vers $\mathrm{M}(m, K)$.

À partir d'ici, les anneaux sont supposés commutatifs et unitaires.

*18. (2.2.4 du polycopié.) Montrer que les diviseurs de zéro dans $\mathcal{C}(\mathbb{R}, \mathbb{R})$ sont les $f\colon \mathbb{R} \to \mathbb{R}$ tel que $f^{-1}(0)$ est d'intérieur non vide.

19. (2.2.6 du polycopié.) Soient A un anneau, a et b dans A. Montrer que ab est non diviseur de zéro si et seulement si a et b sont non diviseurs de zéro.
20. (2.4.7 du polycopié) Existe-t-il des anneaux A et B tels que $A \times B$ soit intègre?

*21. (2.4.8 du polycopié.) Soit $U \subset \mathbb{C}$ ouvert, et soit A l'anneau des fonctions $f\colon U \to \mathbb{C}$ holomorphes. Montrer que A est intègre si et seulement si U est connexe et non vide.

22. (3.2.1 du polycopié.) Vérifier que les trois conditions de la définition 3.1 du polycopié sont équivalentes.
23. (3.2.5 du polycopié.) Soit A un anneau fini. Montrer que tout non diviseur de zéro est inversible. Et si on ne suppose pas que A soit fini?
24. (3.2.6 du polycopié.) Soient A un anneau, a et b dans A. Montrer que ab est inversible si et seulement si a et b le sont.
25. (3.2.7 du polycopié.) Soit A un anneau. Un élément x de A est dit nilpotent s'il existe un entier $n > 0$ tel que $x^n = 0$. Soit x dans A. Montrer que si x est nilpotent, alors $1 - x$ est inversible. (Indication: voir 1.8.6 du polycopié.)
26. (3.2.8 du polycopié.) Soit $f\colon A \to B$ un morphisme d'anneaux. Montrer que $f(A^\times) \subset B^\times$. Soit a un non diviseur de zéro dans A. Est-ce que $f(a)$ est non diviseur de zéro dans B?

27. (3.3.2 du polycopié.) Pour tout entier n avec $0 \leq n \leq 10$, faire la liste des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, et de leurs inverses.
28. (3.5.3 du polycopié.) Soit A un anneau. Montrer que les conditions suivantes sont équivalentes:
    1. A est un corps,
    2. $A^\times = A - \{0\}$,
    3. $A - \{0\}$ est un groupe pour la multiplication.
29. (3.5.7 du polycopié.) Existe-t-il des anneaux A et B tels que $A \times B$ soit un corps?

*30. Soit n dans $\mathbb{Z}$. Montrer que l'application $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}, +) \to \mathbb{Z}/n\mathbb{Z}$, $f \mapsto f(1 \bmod n)$ induit un isomorphisme entre $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}, +)$ et le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

31. Notons $\mathbb{Q}(i)$ le sous-anneau de $\mathbb{C}$ engendré par $\mathbb{Q} \cup \{i\}$. Montrer que $\mathbb{Q}(i)$ est l'ensemble des $a + bi$ avec a et b dans $\mathbb{Q}$. Montrer que $\mathbb{Q}(i)$ est un corps.
32. Notons $\mathbb{Z}[i]$ le sous-anneau de $\mathbb{C}$ engendré par i. Montrer que $\mathbb{Z}[i]$ est l'ensemble des $a + bi$ avec a et b dans $\mathbb{Z}$. Faire la liste des éléments de $\mathbb{Z}[i]^\times$.
33. Soit A le sous-anneau de $\mathbb{C}$ engendré par $2i$ (rappel: tous les anneaux et sous-anneaux sont supposés unitaires). Montrer que A est l'ensemble des $a + 2bi$ avec a et b des entiers. Faire la liste des éléments de $A^\times$.
34. Soient A un anneau, I et J des idéaux de A. Montrer que $I \cap J$ et $I + J$ sont des idéaux de A. On définit IJ comme étant l'idéal engendré par l'ensemble des ij, avec i dans I et j dans J. Montrer que IJ est l'ensemble des éléments de la forme $i_1 j_1 + \cdots + i_n j_n$, avec $n \geq 0$ entier, i_k dans I et j_k dans J. Montrer que $IJ \subset I \cap J$. Donner un exemple où $IJ \neq I \cap J$. Montrer que si I et J sont engendrés par S et T, respectivement, alors IJ est engendré par les st avec s dans S et t dans T.
35. Soit $f\colon A \to B$ un morphisme d'anneaux. Soit I un idéal de A, et soit J un idéal de B. Est-ce que $f^{-1}J$ est un idéal de A? Est-ce que $f(I)$ est un idéal de B?

*36. (4.1.5 et 4.1.6 du polycopié.) Soit x_0 dans $\mathbb{R}$. Posons $A := \mathcal{C}(\mathbb{R}, \mathbb{R})$ et $I := \{f \in A \mid f(x_0) = 0\}$. Montrer que I est un idéal de A. Montrer que I n'est pas principal. Que se passe-t-il si on remplace A par $\mathbb{R}[X]$, ou par $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$, ou par $\mathbb{R}^\mathbb{R}$?

37. Pour A un anneau, notons $\mathrm{nil}(A)$ le sous-ensemble de A des éléments nilpotents. Un anneau est dit réduit si $\mathrm{nil}(A) = \{0\}$.

    *(a) Soit A un anneau. Montrer que $\mathrm{nil}(A)$ est un idéal.

    (b) Soit A un anneau. Montrer que $A/\mathrm{nil}(A)$ est réduit, et que tout morphisme de A vers un anneau réduit se factorise de façon unique par le morphisme quotient $A \to A/\mathrm{nil}(A)$.

*38. Un idéal I d'un anneau A est dit maximal, si, premièrement, I n'est pas égal à A, et, deuxièmement, I et A sont les seuls idéaux de A contenant I. Soient A un anneau et I un idéal dans A. Montrer que I est maximal si et seulement si A/I est un corps.

39. Un idéal I d'un anneau A est dit premier si A/I est intègre. Soient A un anneau et I un idéal de A. Montrer que I est premier si et seulement si $I \neq A$ et $ab \in I$ implique $a \in I$ ou $b \in I$.
40. (**Théorème Chinois.**) Soient A un anneau, I et J deux idéaux de A.

    (a) Notons $f\colon A \to A/I$ et $g\colon A \to A/J$ les morphismes quotients. Notons $h\colon A \to A/I \times A/J$ l'application $a \mapsto (f(a), g(a))$. Montrer que h est un morphisme, et que $\mathrm{Ker}(h) = I \cap J$.

    *(b) Supposons que I et J sont étrangers, ce qui veut dire que $I + J = A$. Montrer qu'alors h est surjectif. Montrer que $I \cap J = IJ$.

(c) Supposons que $I + J = A$. Notons $q\colon A \to A/IJ$. Montrer qu'il existe un unique morphisme d'anneaux $\overline{h}\colon A/IJ \to A/I \times A/J$ tel que, pour tout a dans A, on ait $\overline{h}(q(a)) = h(a)$, et que ce morphisme est un isomorphisme.

(d) Soient m et n deux entiers premiers entre eux. Montrer qu'il existe un unique isomorphisme d'anneaux $f\colon \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tel que $f(a \bmod nm) = f(a \bmod m, a \bmod n)$ pour tout a dans $\mathbb{Z}$.

*41. (**Superthéorème Chinois**) Généraliser l'exercice précédent au cas d'un anneau A et des idéaux $I_1, \ldots, I_n$ tel que $I_i + I_j = A$ pour tous $i \neq j$. Plus précisement, montrer que $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$ et que les applications naturelles induisent un isomorphisme:

$$f\colon A/I_1 \cdots I_n \longrightarrow A/I_1 \times \cdots \times A/I_n.$$

Indication: récurrence sur n; appliquer le résultat pour $n = 2$ à $I_1 \cdots I_{n-1}$ et I_n.

**42. Soit $n \geq 2$ un entier. Combien d'entiers a y a-t-il tel que $0 \leq a < 10^n$, et dont le carré, écrit en base 10, se termine par $n - 1$ fois zéro suivi d'un 1? Indication: appliquer le théorème Chinois.

43. (5.9 du polycopié.) Soit K le corps $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Soit $L := K[X]/(X^2 + X + 1)$. Montrer que L est un corps à quatre éléments, et écrire des tables d'addition et de multiplication.

Licence — Algèbre. Feuille d'exercices N° 6

10-11/97

1. (6.4.2 du polycopié.) Soit A un anneau. Montrer que l'image de l'unique morphisme $\varphi_A : \mathbb{Z} \to A$ est le plus petit sous-anneau de A.
2. (6.4.5 du polycopié.) Soient A un anneau et n un entier > 0. Montrer les équivalences :

$$\begin{aligned} \operatorname{car}(A) = 0 &\iff 1_A \text{ est d'ordre infini dans } (A,+) \\ &\iff \varphi_A \text{ est injectif} \\ &\iff \operatorname{Im} \varphi_A \text{ est isomorphe à } \mathbb{Z} \\ &\iff A \text{ contient un sous-anneau isomorphe à } \mathbb{Z}. \end{aligned}$$

$$\begin{aligned} \operatorname{car}(A) = n &\iff 1_A \text{ est d'ordre } n \text{ dans } (A,+) \\ &\iff \operatorname{Im} \varphi_A \text{ est isomorphe à } \mathbb{Z}/n\mathbb{Z} \\ &\iff A \text{ contient un sous-anneau isomorphe à } \mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

3. (6.4.6 du polycopié.) Trouver la caractéristique de chacun des anneaux suivants : l'anneau nul ; $\mathbb{Z}/n\mathbb{Z}$; $\mathbb{Q}$; $(\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$; le produit de deux anneaux donnés ; $^*\prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$; $^*A^I$ où I est un ensemble et A un anneau ; $\mathcal{C}([0,1],\mathbb{R})$).
4. Soient K et L deux corps de caractéristiques différentes. Montrer qu'il n'existe aucun morphisme de K dans L.

   A-t-on une assertion analogue pour deux anneaux quelconques ? pour deux anneaux intègres ? De façon générale, si $f : A \to B$ est un morphisme (resp. un morphisme injectif) d'anneaux, quelle(s) relation(s) peut-on trouver entre les caractéristiques de A et de B ?
5. (7.2.2 du polycopié.) Soit p un nombre premier. Si A et B sont deux anneaux de caractéristique p, montrer que tout morphisme d'anneaux de A dans B est $\mathbb{F}_p$-linéaire.

*6. (7.2.3 du polycopié.) Soit p un nombre premier. Si A est un anneau de caractéristique p, montrer que A est fini si et seulement si A est de dimension finie comme $\mathbb{F}_p$-espace vectoriel, et qu'alors le cardinal de A est une puissance de p.

7. (7.4.3 du polycopié.) Soit K un corps fini. Montrer que l'endomorphisme de Frobenius F_K de K est un automorphisme de K. Quelle est sa restriction au plus petit sous-corps de K ?

*8. (8.4.2 du polycopié.) Soit R un anneau. On suppose que pour tout anneau A il existe un unique morphisme d'anneaux de R dans A. Montrer qu'il existe un unique isomorphisme d'anneaux de R sur $\mathbb{Z}$.

9. Soit A un anneau. Montrer que A est intègre si et seulement si il est isomorphe à un sous-anneau d'un corps.
10. Soit A un corps. Quel est le corps des fractions de A ?
11. Quel est le corps des fractions de $\mathbb{Z}/6\mathbb{Z}$?
12. Soient A un anneau intègre, K son corps des fractions, B un sous-anneau de K contenant A. Quel est le corps des fractions de B ?

*13. Soit $f : A \to B$ un morphisme injectif d'anneaux intègres, et soient $i : A \to K$ et $j : B \to L$ les morphismes canoniques de A et B dans leurs corps des fractions respectifs. Montrer qu'il existe un unique morphisme $g : K \to L$ tel que $g \circ i = j \circ f$. L'hypothèse d'injectivité de f est-elle nécessaire ?

*14. Soient A un anneau intègre, K son corps des fractions. Considérons un système homogène de m équations linéaires

$$(S) \qquad \sum_{j=1}^{n} a_{i,j} x_j = 0, \quad i = 1 \dots, m$$

en n inconnues $x_1, \ldots, x_n$, à coefficients $a_{i,j} \in A$. Montrer que (S) a une solution non nulle $(x_1, \ldots, x_n)$ dans A^n si et seulement si il a une solution non nulle dans K^n.
Plus précisément, soit V le sous-K-espace vectoriel de K^n formé des solutions de (S). Montrer que V est engendré (comme K-espace vectoriel) par $V \cap A^n$. Pourquoi cette propriété implique-t-elle la précédente ?

*15. Soient A un anneau intègre, K son corps des fractions, et $n \in \mathbb{N}$. Montrer que $\mathrm{M}(n, A)$ (cf. feuille 5, exercice 6) est un sous-anneau (non commutatif en général !) de $\mathrm{M}(n, K)$.
On note $\mathrm{GL}(n, A)$ l'ensemble des matrices $M \in \mathrm{M}(n, A)$ qui sont inversibles dans $\mathrm{M}(n, A)$, i.e. telles qu'il existe $N \in \mathrm{M}(n, A)$ vérifiant $MN = NM = I_n$.
Entre les propriétés suivantes, trouver toutes les implications qui sont vraies pour tout $M \in \mathrm{M}(n, A)$ (par exemple, (i)$\Rightarrow$(iii) est toujours vraie mais pas (v)$\Rightarrow$(vi)) :

(i) $M \in \mathrm{GL}(n, A)$;
(ii) $M \in \mathrm{GL}(n, K)$;
(iii) il existe $N \in \mathrm{M}(n, A)$ telle que $MN = I_n$;
(iv) il existe $N \in \mathrm{M}(n, A)$ telle que $NM = I_n$;
(v) $\det(M) \in A$;
(vi) $\det(M) \in A^*$;
(vii) $\det(M) \in A^\times$.

*16. On garde les notations de l'exercice précédent, et l'on pose

$$\mathrm{SL}(n, A) = \{M \in \mathrm{M}(n, A) \mid \det(M) = 1\}.$$

$\mathrm{SL}(n, A)$ est-il un sous-groupe distingué de $\mathrm{GL}(n, A)$? de $\mathrm{SL}(n, K)$?
Quel est l'indice de $\mathrm{SL}(n, \mathbb{Z})$ dans $\mathrm{GL}(n, \mathbb{Z})$?

Licence — Algèbre. Feuille d'exercices N° 7

17-11/97

1. Donner une démonstration de la Proposition 1.4 du polycopié, c'est à dire, montrer, en partant de la Définition 1.2, que, pour A un anneau, $(A[X], +, \times)$ est un anneau commutatif unitaire, que l'application $A \to A[X]$, $a \mapsto (a, 0, 0, \ldots)$ est un morphisme d'anneaux injectif, et que, si l'on pose $X := (0, 1, 0, 0, \ldots)$, alors pour toute suite finie $(a_0, a_1, \ldots, a_n)$ d'éléments de A on a, dans $A[X]$, l'identité:
$$\sum_{i=0}^{n} a_i X^i = (a_0, a_1, \ldots, a_n, 0, 0, \ldots).$$
2. Soit A un anneau. Notons $A[[X]]$ l'ensemble des suites $(a_0, a_1, \ldots)$ d'éléments de A, indexées par $\mathbb{N}$. Pour $a = (a_0, a_1, \ldots)$ et $b = (b_0, b_1, \ldots)$ dans $A[[X]]$, définissons $a + b$ et ab dans $A[[X]]$ par:
$$(a+b)_n = a_n + b_n, \qquad (ab)_n = \sum_{\substack{i+j=n \\ i,j \geq 0}} a_i b_j.$$
Montrer que $A[[X]]$, avec ces deux lois de composition, est un anneau commutatif unitaire, qui contient $A[X]$ comme sous-anneau. Cet anneau s'appelle l'anneau des séries formelles à coefficients dans A, en l'indéterminée X. Bien sûr, on a envie d'écrire un élément $(a_0, a_1, a_2, \ldots)$ comme une somme infinie $\sum_i a_i X^i$, mais cela n'a pas de sens pour l'instant.
3. Soit A un anneau. Notons $A[X, X^{-1}]$ l'ensemble des suites $a = (\ldots, a_{-1}, a_0, a_1, \ldots)$ d'éléments de A, indexées par $\mathbb{Z}$, presque tous nuls. Pour a et b dans $A[X, X^{-1}]$, définissons des suites $a + b$ et ab par:
$$(a+b)_n = a_n + b_n, \qquad (ab)_n = \sum_{i+j=n} a_i b_j.$$
Montrer que pour a et b dans $A[X, X^{-1}]$, $a + b$ et ab sont dans $A[X, X^{-1}]$. Montrer que $A[X, X^{-1}]$, avec ces deux lois de composition, est un anneau commutatif unitaire, qui contient $A[X]$ comme sous-anneau. Cet anneau s'appelle l'anneau des polynômes de Laurent à coefficients dans A, en l'indéterminée X.
4. Soit A un anneau. Notons $A((X))$ l'ensemble des suites $a = (\ldots, a_{-1}, a_0, a_1, \ldots)$ d'éléments de A, indexées par $\mathbb{Z}$, telles qu'il existe n dans $\mathbb{Z}$ avec $a_i = 0$ pour $i \leq n$ (noter que n dépend de a). Pour a et b dans $A((X))$, définissons des suites $a + b$ et ab par:
$$(a+b)_n = a_n + b_n, \qquad (ab)_n = \sum_{i+j=n} a_i b_j.$$
Montrer que pour a et b dans $A((X))$, $a + b$ et ab sont dans $A((X))$. Montrer que $A((X))$, avec ces deux lois de composition, est un anneau commutatif unitaire, qui contient $A[X, X^{-1}]$ et $A[[X]]$ comme sous-anneaux. Cet anneau s'appelle l'anneau des séries de Laurent à coefficients dans A, en l'indéterminée X. Montrer que si l'on avait considéré les suites a telles qu'il existe n avec $a_i = 0$ pour $i \geq n$, on aurait trouvé un anneau commutatif unitaire isomorphe à $A((X))$, mais qu'on pourrait noter $A((X^{-1}))$.

*5. Soit A un anneau. Est-ce que les formules $(a+b)_n = a_n + b_n$ et $(ab)_n = \sum_{i+j=n} a_j b_j$ font de l'ensemble des séries d'éléments de A, indexées par $\mathbb{Z}$, un anneau?

6. Soit A un anneau. Notons $A[X,Y]$ l'ensemble des doubles suites d'éléments de A, indexées par $\mathbb{N} \times \mathbb{N}$, presque tous nuls. Autrement dit, $A[X,Y]$ est le sous-ensemble des a dans $A^{\mathbb{N}\times\mathbb{N}}$ tels que $a(i,j) = 0$ sauf pour un nombre fini de couples (i,j). Pour a et b dans $A[X,Y]$ on définit des suites $a+b$ et ab par:

$$(a+b)_{n,m} = a_{n,m} + b_{n,m}, \qquad (ab)_{n,m} = \sum_{\substack{i+j=n \\ k+l=m}} a_{i,k} b_{j,k}.$$

Montrer que ces formules font de $A[X,Y]$ un anneau commutatif unitaire. Montrer que si l'on note X la suite telle que $X_{1,0} = 1$ et $X_{i,j} = 0$ si $(i,j) \neq (1,0)$, et Y la suite telle que $Y_{0,1} = 1$ et $Y_{i,j} = 0$ si $(i,j) \neq (0,1)$, alors on a pour tout a dans $A[X,Y]$ l'identité:

$$a = \sum_{i,j} a_{i,j} X^i Y^j.$$

7. Démontrer le Lemme 1.7 du polycopié.

*8. Soit A un anneau. Montrer que $A[X]$ est intègre si et seulement si A l'est. De même pour $A[[X]]$, $A[X,X^{-1}]$ et $A((X))$.

*9. Soit A un anneau. Montrer que $A[X]$ n'est pas un corps. De même pour $A[[X]]$ et $A[X,X^{-1}]$. (Ce dernier est un peu plus difficile.)

**10. Soit A un anneau. Montrer que $A((X))$ est un corps si et seulement si A en est un. Montrer que, pour A un corps, $A((X))$ est le corps de fractions de $A[[X]]$.

*11. (1.8.3 du polycopié.) Soient A un anneau et P dans $A[X]$. Supposons que le terme constant de P est dans $A^\times$, et que tous les autres coefficients de P sont nilpotents. Montrer que P est dans $A[X]^\times$.

12. Soit K un corps.

   *(a) Montrer que le morphisme $f\colon K[X] \to K^K$ de (1.9) du polycopié est injectif si et seulement si K est infini.

   *(b) Montrer que f est surjectif si et seulement si K est fini.

13. Soit K un corps fini, de cardinal q et de caractéristique p.

   *(a) Montrer que q est une puissance de p.

   *(b) Montrer que pour tout a dans K, on a $a^q = a$. Indication: $K^\times$ est de cardinal $q-1$.

   *(c) Soit $f\colon K[X] \to K^K$ le morphisme de (1.9) du polycopié. Montrer que $\mathrm{Ker}(f)$ est l'idéal engendré par $X^q - X$.

14. Soit A l'anneau $\mathbb{Z}/4\mathbb{Z}$. Est-ce que le morphisme $f\colon A[X] \to A^A$ de (1.9) du polycopié est surjectif?

15. (1.9.1 du polycopié.) Soient A un anneau et a dans A. Notons $\varepsilon_a\colon A[X] \to A$ l'application $P \mapsto P(a)$ qui évalue en a. Montrer que ε_a est un morphisme d'anneaux. Montrer que ε_a est surjectif. Montrer que $\mathrm{Ker}(\varepsilon_a)$ est l'idéal $(X-a)$ engendré par $X-a$, et que ε_a induit un isomorphisme de $A[X]/(X-a)$ vers A.

Licence — Algèbre. Feuille d'exercices N° 8

24-11/97

*1. Soient A un anneau, P dans $A[X]$ unitaire. Montrer que pour tout F dans $A[X]$ il existe Q et R dans $A[X]$ uniques, tels que $F = PQ+R$ et $\deg(R) < \deg(P)$. Indication: pour l'existence, faire récurrence sur $\deg(F)$; pour l'unicité: si Q' et R' ont les mêmes propriétés, considérer les degrés des deux cotés de l'identité $P(Q-Q') = R'-R$.

*2. Donner un exemple d'un anneau A et de F et P dans $A[X]$ avec P non nul, tel qu'il n'existe pas de Q et R dan $A[X]$ avec $F = PQ + R$ et $\deg(R) < \deg(P)$.

3. Faites la division euclidienne, dans $\mathbb{F}_2[X]$, de $X^{64} + X$ par $X^{16} + X$.

4. Soient A un anneau, a dans A et F dans $A[X]$.
   (a) Montrer que le reste de la division euclidienne de F par $X - a$ est $F(a)$.
   (b) Montrer que $F(a) = 0$ si et seulement si F appartient à l'idéal principal $(X - a)$ de $A[X]$.

5. Montrer que dans un anneau intègre A, a et b engendrent le même idéal si et seulement si il existe un u dans $A^\times$ tel que $b = ua$.

*6. Soit k un corps. Montrer que $k[X]$ est un anneau principal, c'est à dire, que tout idéal de $k[X]$ est principal. Indication: adapter la preuve que $\mathbb{Z}$ est principal en remplaçant la division euclidienne dans $\mathbb{Z}$ par celle dans $k[X]$. Vous pouvez aussi vous inspirer de la preuve de la Proposition 3.3 du chapitre III du polycopié. Montrer que chaque idéal non nul de $k[X]$ est engendré par un unique élément unitaire de $k[X]$.

*7. (3.4.3 du polycopié.) Soient k un corps, $k \to K$ une extension, et V un K-espace vectoriel. Montrer que V est de façon naturelle un k-espace vectoriel. Supposons que K soit de dimension finie en tant que k-espace vectoriel, et que V soit de dimension finie en tant que K-espace vectoriel.
   (a) Montrer que $\dim_k(V) = [K : k] \dim_K(V)$. Indication: si $(\lambda_1, \ldots, \lambda_d)$ est une k-base de K, et $(v_1, \ldots, v_n)$ une K-base de V, alors la famille $(\lambda_i v_j)_{1\leq i\leq d,\, 1\leq j\leq n}$ est une k-base de V.
   (b) Montrer que si L est une extension de degré fini de K, alors on a l'identité $[L : k] = [L : K][K : k]$.

8. (3.5.1 du polycopié.) Soient k un corps, A et B des k-algèbres. Notons $\phi\colon k \to A$ et $\psi\colon k \to B$ les morphismes structuraux de A et B. Montrer qu'une application $f\colon A \to B$ est un morphisme de k-algèbres si et seulement si $f \circ \phi = \psi$.

9. (Propriété "pro-universelle" de $k[[X]]$.) Soit k un corps. Montrer que pour toute k algèbre A et tout élément nilpotent a de A il existe un unique morphisme de k-algèbres $\varepsilon_a\colon k[[X]] \to A$ tel que $\varepsilon_a(X) = a$.

10. (Propriété universelle de $k[X, X^{-1}]$.) Soit k un corps. Montrer que pour toute k-algèbre A et tout élément a de $A^\times$ il existe un unique morphisme de k-algèbres $\varepsilon_a\colon k[X, X^{-1}] \to A$ tel que $\varepsilon_a(X) = a$. Montrer que cette construction induit une bijection entre $\mathrm{Hom}_{k-\mathrm{alg}}(k[X, X^{-1}], A)$ et $A^\times$.

11. (le groupe $\mathrm{Aut}_{k-\mathrm{alg}}(k[X])$.) Soit k un corps.
   *(a) Soit Q dans $k[X]$. Considérons le morphisme $\varepsilon_Q\colon k[X] \to k[X]$, $P \mapsto P(Q)$. Montrer que ε_Q est injectif si et seulement si Q est non nul. Montrer que ε_Q est surjectif si et seulement si $\deg(Q) = 1$.
   **(b) Montrer que l'application $f\colon \mathrm{Aut}_{k-\mathrm{alg}}(k[X]) \to \{a + bX \mid a \in k,\, b \in k^*\}$, $g \mapsto g(X)$, est bijective, et écrire explicitement la loi de groupe induite par cette bijection sur l'ensemble $\{a + bX \mid a \in k,\, b \in k^*\}$.

**(c) Montrer que $\mathrm{Aut}_{k-\mathrm{alg}}(k[X])$ est isomorphe au groupe des transformations affines du k-espace vectoriel k, c'est à dire, au sous-groupe de $\mathfrak{S}(k)$ engendré par les $\mu_b\colon x \mapsto bx$ (b dans k^*) et les translations $t_a\colon x \mapsto x + a$ (a dans k).

12. Soit k un corps. Soient A une k-algèbre, et a dans A. Notons $\varepsilon_a\colon k[X] \to A$ le morphisme $P \mapsto P(a)$.
    (a) Montrer que ε_a est injectif si et seulement si la famille $(a^n)_{n\geq 0}$ est linéairement indépendante dans le k-espace vectoriel A.
    *(b) Supposons que ε_a n'est pas injectif. Notons alors f_a l'unique générateur unitaire de $\mathrm{Ker}(\varepsilon_a)$; f_a s'appelle le polynôme minimal de a sur k. Soit d le degré de f_a. Montrer que ε_a induit un isomorphisme de $k[X]/(f_a)$ vers $\mathrm{Im}(\varepsilon_a)$, et que par conséquent $\dim_k(\mathrm{Im}(\varepsilon_a)) = d$, et que $(1, a, \ldots, a^{d-1})$ est une k-base de $\mathrm{Im}(\varepsilon_a)$.
    *(c) Soit V un k-espace de dimension finie n. Soit a dans $\mathrm{End}_k(V)$. Montrer que $\varepsilon_a\colon k[X] \to \mathrm{End}_k(V)$ n'est pas injectif, et que $0 \leq \deg(f_a) \leq n$. Est-ce que $\deg(f_a)$ peut prendre toute valeur entre 1 et n?

13. (4.3.2 du polycopié.) Soit k un corps. Posons $A := k[X]/(X^2)$, la k-algèbre des "nombres duaux". Notons ω dans A la classe de X. Montrer que l'application $(a, b) \mapsto a + b\omega$ est un isomorphisme de groupes du groupe produit $k^* \times k$ vers $A^\times$. Montrer que $\mathrm{nil}(A)$ est l'idéal engendré par ω.

*14. Soit k un corps. Pour $P = a_0 + \cdots + a_nX^n$ dans $k[X]$ on définit la dérivée P' de P par $P' := \sum_{i=1}^n ia_iX^{i-1}$. On va voir que cette dérivée a une interprétation comme en calcul infinitésimal. Soit $A = \{a + b\omega \mid a, b \in k\}$ la k-algèbre des nombres duaux. Considérons le morphisme de k-algèbres $\varepsilon\colon k[X] \to A[X]$, $P \mapsto P(X + \omega)$. Montrer que $P(X + \omega) = P(X) + \omega P'(X)$.

*15. (4.3.4 du polycopié.) Faites l'exercice IV.4.3.4 du polycopié.

Licence — Algèbre. Feuille d'exercices N° 9

01-12/97

1. Donner les listes des diviseurs de 1, -1 et 12 dans l'anneau $\mathbb{Z}$.
2. Soit $n \geq 0$ un entier. Montrer que n est premier si et seulement si $\mathrm{Div}(n)$ (l'ensemble des diviseurs de n) est de cardinal quatre.
3. Soit p dans $\mathbb{Z}$ un nombre premier (c'est à dire, $p > 1$ et $\mathrm{Div}(p)$ est $\{1, -1, p, -p\}$).
   *(a) Montrer que $\mathbb{Z}/p\mathbb{Z}$ est intègre. Indication : utiliser que $\mathbb{Z}$ est principal.
   (b) Soient a et b dans $\mathbb{Z}$. Montrer que si p divise ab, alors p divise a ou b.
   *(c) Soit n dans $\mathbb{N}$. Soit a un diviseur de p^n. Montrer que a est de la forme $\pm p^m$, avec $0 \leq m \leq n$, sans utiliser le fait que la décomposition en nombres premiers dans $\mathbb{N}^*$ existe et est unique. Infication : récurrence sur n.
4. Soit A un anneau intègre. Soient a, b et c dans A tel que ac divise bc. Supposons que c est non nul. Montrer que a divise b.
5. Soit n dans $\mathbb{Z}$. Montrer que la classe de n modulo 3 est égale à la classe modulo 3 de la somme des chiffres dans l'écriture de n en base 10. Faire la chose analogue pour les classes de n modulo 9 et 11. Indication : calculer 10^i modulo 3, 9 et 11.
6. (1.2.5 et 1.3.2 du polycopié.) Soit U un ouvert de $\mathbb{C}$, connexe et non vide (en fait, est-ce que connexe implique non vide ?), et soit A l'anneau des fonctions $f\colon U \to \mathbb{C}$ holomorphes (cf. II.2.4.8). Pour f dans A et z dans U, notons $\mathrm{ord}_z(f)$ l'ordre de f en z (qui est $+\infty$ si f est nulle). Pour f et g dans A, montrer que f divise g si et seulement si pour tout z dans U on a $\mathrm{ord}_z(f) \leq \mathrm{ord}_z(g)$. Montrer que f et g dans A sont associés si et seulement si pour tout z dans U on a $\mathrm{ord}_z(f) = \mathrm{ord}_z(g)$.
7. Montrer les assertions dans 2.3.1 et 2.3.3 du polycopié.
8. Soient k un corps et A la sous-k-algèbre de $k[X]$ engendrée par X^2 et X^3.
   (a) Soit F dans $k[X]$. Montrer que F est dans A si et seulement si le coefficient de X dans F est nul.
   **(b) Montrer que A est intègre et que le couple X^5 et X^6 n'a ni de PGCD, ni de PPCM.

*9. Soit A un anneau intègre. Soient a et b dans A. Notons D l'ensemble des divisieurs communs de a et b. Notons M l'ensemble des multiples communs de a et b qui divisent ab. Montrer que l'application $f\colon D \to A$, $d \mapsto ab/d$, induit une bijection de D vers M. Montrer que pour d_1 et d_2 dans D on a $d_1|d_2$ si et seulement si $f(d_2)|f(d_1)$. Conclure que si a et b ont un PPCM, alors ils ont un PGCD. Est-ce que la réciproque est vraie ? (Indication : essayer les éléments X^2 et X^3 dans l'anneau A de l'exercice précédent.)

*10. A partir des définitions de PGCD et PPCM, montrer que, dans $\mathbb{Z}$, toute famille d'éléments admet un PGCD et un PPCM. Indication : utiliser que tout idéal de $\mathbb{Z}$ est principal.

11. Calculer le PPCM et le PGCD dans $\mathbb{Z}$ de 1001 et 1991.
12. (2.3.7 du polycopié.) Soit A un anneau intègre. Soient n dans $\mathbb{N}$ et $a_1, \ldots, a_n$ dans A. Montrer que 0 est un PPCM des a_i si et seulement si l'un des a_i est nul. Montrer que dans $\mathbb{Z}$, 0 est le PPCM de la famille des entiers non nuls.
13. (2.3.8 du polycopié.) Soient A un anneau intègre, a, a' et b dans A. Supposons que $a \equiv a' \pmod{b}$. Montrer que tout PGCD de a et b est aussi un PGCD de a' et b.

*14. L'algorithme d'Euclide, pour calculer le PGCD de deux entiers a et b, consiste à remplacer le plus grand des deux (en valeur absolue) par le reste modulo l'autre, si cet autre est non nul. Soient a et b dans $\mathbb{Z}$, pas tous les deux nuls. Montrer que le nombre de divisions euclidiennes à faire, dans l'algorithme d'Euclide pour calculer le PGCD de a et b, est borné par :

$$\frac{2}{\log 2} \log(\max(|a|, |b|)).$$

Indication : montrer que pour $a \geq b \geq 1$ dans $\mathbb{Z}$, le reste c de la division euclidienne de a par b satisfait $0 \leq c < |a|/2$.

15. Soit k un corps. Soient F et G dans $k[X]$, non nuls. Montrer que le nombre de divisions euclidiennes à faire, dans l'algorithme d'Euclide pour calculer le PGCD de F et G, est borné par :

$$1 + \min(\deg(F), \deg(G)).$$

*16. Soit k un corps. Soient a et b dans $\mathbb{N}$. Soit d le PGCD positif de a et b. Montrer que $X^d - 1$ est un PGCD de $X^a - 1$ et $X^b - 1$ dans $k[X]$. Indication : utiliser l'algorithme d'Euclide.

*17. (2.7.1 du polycopié.) Faites l'exercice 2.7.1.

18. Montrer les assertions dans 2.9.2 du polycopié.

*19. (2.8.4 et 2.9.6 du polycopié.) Soit A l'anneau des fonctions holomorphes sur un ouvert connexe U de $\mathbb{C}$. Montrer que f et g dans A sont premiers entre eux si et seulement si f et g n'ont pas de zéro commun. Montrer que f dans A est irréductible si et seulement si f a un unique zéro qui de plus est simple. Autrement dit, les irréductibles de A sont les associés des $w \mapsto w - z$, z dans U.

20. (3.2.1 du polycopié.) Soient A un anneau euclidien et $\phi: A \to \mathbb{N}$ une fonction euclidienne, c'est à dire, une fonction comme dans la définition d'anneau euclidien. Montrer que pour tout $a \neq 0$ dans A on a $\phi(a) > \phi(0)$.

*21. (3.2.5 du polycopié.) Considérons le sous-anneau $\mathbb{Z}[i]$ de $\mathbb{C}$ formé des $x + yi$ avec x et y dans $\mathbb{Z}$. Montrer que $\mathbb{Z}[i]$ est euclidien, en montrant que $\phi: \mathbb{Z}[i] \to \mathbb{N}$, $z \mapsto |z|^2$ est une fonction euclidienne. Indication : pour a et b dans $\mathbb{Z}[i]$ avec b non nul, considérer le nombre complexe a/b, et l'élément le plus proche de $\mathbb{Z}[i]$.

*22. Notons j le nombre complexe $\exp(2\pi i/3)$. Notons $\mathbb{Z}[j]$ le sous-anneau de $\mathbb{C}$ engendré par j. Montrer que les éléments de $\mathbb{Z}[j]$ s;écrivent de façon unique sous la forme $x + yj$ avec x et y dans $\mathbb{Z}$. Montrer que $\mathbb{Z}[j]$ de $\mathbb{C}$ est euclidien. Indication : faites comme pour $\mathbb{Z}[i]$.

23. Donner la liste des éléments de $\mathbb{Z}[i]^\times$. Donner les listes des diviseurs de 1, 2, 3, 4 et 5 dans $\mathbb{Z}[i]$.

24. Montrer que pour a dans $\mathbb{Z}[i]$ la classe de $|a|^2$ modulo quatre est zéro, un ou deux. Soit p un nombre premier qui est trois modulo quatre. Montrer que p est irréductible dans $\mathbb{Z}[i]$. Nous verrons plus loin que ce sont les seuls nombres premiers qui sont irréductibles dans $\mathbb{Z}[i]$. Par conséquent, nous verrons que tout nombre premier de la forme $4n+1$ est la somme de deux carrés. De même, montrer que tout nombre premier congru à deux modulo trois est irréductible dans $\mathbb{Z}[j]$.

*25. Soient k un corps, F, G et H dans $k[X]$, tels que H est un PGCD de F et G. Soit K une extension de k. Montrer que H est un PGCD de F et G dans $K[X]$.

26. Soit D le disque unité fermé dans $\mathbb{C}$: $D = \{z \in \mathbb{C} \,|\, |z| \leq 1\}$. Notons A l'anneau des fonctions $f: D \to \mathbb{C}$ holomorphes (f est dite holomorphe s'il existe U un ouvert de $\mathbb{C}$ contenant D, et $g: U \to \mathbb{C}$ holomorphe, tels que f soit la restriction de g à D).

    (a) Montrer que $A^\times$ consiste des f avec $f(z) \neq 0$ pour tout z dans D.

    *(b) Soit f dans A non nul. Montrer que les $\mathrm{ord}_z(f)$, pour z dans D, sont presque tous nuls. Montrer que f est le produit d'un élément de $A^\times$ par le polynôme $\prod_{z \in D}(X - z)^{\mathrm{ord}_z(f)}$.

*(c) Montrer que A est euclidien.

**(d) L'anneau des fonctions holomorphes sur le disque unité ouvert est-il principal?

27. Soit $\mathbb{Z}[\sqrt{2}]$ le sous-anneau de $\mathbb{R}$ engendré par $\sqrt{2}$.

*(a) Montrer que tout élément de $\mathbb{Z}[\sqrt{2}]$ s'écrit de façon unique sous la forme $x+y\sqrt{2}$, avec x et y dans $\mathbb{Z}$.

*(b) Soient x et y dans $\mathbb{Z}$. Montrer que $x+y\sqrt{2}$ est dans $\mathbb{Z}[\sqrt{2}]^\times$ si et seulement si $x^2-2y^2=\pm 1$.

**(c) Montrer que $\mathbb{Z}[\sqrt{2}]^\times$ est engendré par $\{-1, \sqrt{2}-1\}$.

*28. Montrer, de façon analogue que pour $\mathbb{Z}[i]$, que la fonction $\phi\colon \mathbb{Z}[\sqrt{2}] \to \mathbb{N}$, $x+y\sqrt{2} \mapsto |x^2-2y^2|$, est euclidienne.

**29. Soit A un anneau euclidien. Soit $\phi\colon A \to \mathbb{N}$ une fonction euclidienne. Montrer que la fonction $f\colon A \to \mathbb{N}$, $a \mapsto \min\{\phi(ax) \,|\, 0 \neq x \in A\}$, est euclidienne, et a la propriété supplémentaire que $f(ab) \geq f(a)$ pour tous a et b avec b non nul.

*30. (4.6.1 du polycopié.) Soit A un anneau principal. Soient $n \geq 0$ dans $\mathbb{Z}$ et a, $b_1, \ldots, b_n$ dans A. Montrer que a est premier avec le produit $b_1 \cdots b_n$ si et seulement si, pour tout i, a est premier à b_i. En déduire que si a et b dans A sont premiers entre eux, il en est de même de a^n et b^m, pour n et m entiers > 0. Pouvez-vous déduire cette propriété directement de la définition du PGCD?

31. (4.9.1 du polycopié.) Généraliser II.3.3 au cas de A anneau principal: pour A un anneau principal et a dans A non nul, montrer que les inversibles de $A/(a)$ sont les classes des éléments de A premiers avec a.

*32. Paramétrer l'ensemble des solutions dans $\mathbb{Z}$ du système d'équations:

$$\left\{\begin{array}{rcrl} x & \equiv & 1 & (2) \\ x & \equiv & -1 & (3) \\ x & \equiv & 2 & (5) \\ x & \equiv & 5 & (7). \end{array}\right.$$

*33. Paramétrer les ensembles des solutions dans $\mathbb{Z}$ des systèmes d'équations:

$$\left\{\begin{array}{rcrl} x & \equiv & 1 & (10) \\ x & \equiv & 6 & (25), \end{array}\right. \qquad \left\{\begin{array}{rcrl} x & \equiv & 1 & (10) \\ x & \equiv & 17 & (25). \end{array}\right.$$

*34. Paramétrer l'ensemble des solutions dans $\mathbb{F}_2[X]$ du système d'équations:

$$\left\{\begin{array}{rcll} F & \equiv & 1 & (X^2+X) \\ F & \equiv & x & (X^2+X+1). \end{array}\right.$$

35. Soit A un anneau intègre. Notons Irr l'ensemble des éléments irréductibles de A. Montrer que l'application $A^\times \times \mathrm{Irr} \to \mathrm{Irr}$, $(u,a) \mapsto ua$, est une action de $A^\times$ sur Irr. Montrer que cette action est libre. Notons $p\colon \mathrm{Irr} \to \mathrm{Irr}/A^\times$ l'application quotient. Donner une bijection entre les SRI de A et l'ensemble des applications $s\colon \mathrm{Irr}/A^\times \to \mathrm{Irr}$ telles que $p \circ s = \mathrm{Id}$.

36. (5.1.6 du polycopié.) Existe-t-il un anneau intègre A qui a un SRI et pas plus? Existe-t-il un anneau intègre A tel que l'ensemble des irréductibles de A soit un SRI? Et si on veut en plus que A ne soit pas un corps?

37. (5.3 du polycopié.) Faites ce qui est demandé dans le 5.3 du polycopié.

38. Prenons dans $\mathbb{F}_3[X]$ le SRI des polynômes irréductibles unitaires. Quelle est la décomposition en irréductibles de X^3-X^6?

*39. Soit n un entier qui n'est pas un carré dans $\mathbb{Z}$. Montrer que n n'est pas un carré dans $\mathbb{Q}$.

Licence — Algèbre. Feuille d'exercices N° 10

08-12/97

1. (6.3 du polycopié.) Soit A un anneau principal. Un élément a de A est dit sans facteur carré si $v_p(a) \leq 1$ pour tout p irréductible dans A.
   (a) Soit a dans A. Montrer que a est sans facteur carré si et seulement si les seuls carrés dans A qui divisent a sont des inversibles.
   (b) Soit a dans A. Montrer que les trois conditions suivantes sont équivalentes :
      1. a est sans facteur carré ;
      2. l'anneau $A/(a)$ est isomorphe à un produit de corps ;
      3. l'anneau $A/(a)$ est réduit, c'est à dire, zéro est le seul nilpotent.
2. (6.4 du polycopié.) Soit A un anneau intègre dans lequel tout x non nul admet une décomposition en irréductibles unique, comme dans le théorème III 5.2. (Un tel anneau s'appelle un anneau factoriel.) Démontrer pour A les résultats du paragraphe 4, jusqu'a 4.8 inclus, sauf le fait que le PGCD de deux éléments a et b soit dans l'idéal $Aa + Ab$ engendré par a et b. En fait, on peut montrer que $\mathbb{Z}[X]$ est factoriel, ce qui montre que la factorialité n'implique pas cette propriété qu'ont les PGCD dans les anneaux principaux.
3. Donner un exemple de trois entiers a, b et c tels que $a\mathbb{Z}+b\mathbb{Z}+c\mathbb{Z} = \mathbb{Z}$, mais $a\mathbb{Z}+b\mathbb{Z} \neq \mathbb{Z}$, $a\mathbb{Z}+c\mathbb{Z} \neq \mathbb{Z}$ et $b\mathbb{Z}+c\mathbb{Z} \neq \mathbb{Z}$. Est-ce qu'il existe, pour tout $n \geq 3$ un sous-ensemble S de $\mathbb{Z}$ de cardinal n, tel que l'idéal engendré par S soit $\mathbb{Z}$, et que pour tout sous-ensemble $T \subset S$ différent de S, l'idéal engendré par T n'est pas égal à $\mathbb{Z}$?
4. Soit A un anneau principal, et soit K son corps de fractions. Montrer que tout élément x de K s'écrit sous la forme :
   $$x = a_0 + \sum_{i=1}^{n} \frac{a_i}{p_i^{e_i}},$$
   avec $n \geq 0$, les $e_i > 0$, les a_i dans A et les p_i des irréductibles dans A non associées entre eux deux à deux. Montrer que si en plus A est euclidien, et si $\phi\colon A \to \mathbb{N}$ est une fonction euclidienne, alors on peut écrire x sous la forme :
   $$x = a_0 + \sum_{i=1}^{n} \frac{a_i}{p_i^{e_i}},$$
   avec $n \geq 0$, les a_i dans A, les p_i des irréductibles dans A non associées entre eux deux à deux, tels que $\phi(a_i) < \phi(p_i^{e_i})$ pour tout $i \geq 1$.
5. Soit k un corps. Soit d un entier plus grand ou égal à un. Soit f dans $k[X]$ de degré d. Montrer que tout élément g de $k[X]$ s'écrit de façon unique sous la forme :
   $$g = \sum_{i=0}^{n} a_i f^i,$$
   avec $n \geq 0$ et les a_i dans $k[X]$ de degré $< d$.
6. Soit k un corps. Montrer que tout élément f de $k(X)$ s'écrit de façon unique sous la forme :
   $$f = a_0 + \sum_{i=1}^{n} \sum_{j=1}^{e_i} \frac{a_{i,j}}{p_i^j},$$
   avec $n \geq 0$, les p_i des irréductibles unitaires non associés entre eux deux à deux dans $k[X]$, et les $a_{i,j}$ dans $k[X]$ tels que $\deg(a_{i,j}) < \deg(p_i)$.

7. (Algorithme d'Euclide étendu.) Soit A un anneau euclidien, $\phi\colon A \to \mathbb{N}$ une fonction euclidienne. Soient a et b dans A. L'algoritme d'Euclide nous donne un PGCD d de a et b, ainsi que des éléments u et v de A tels que $d = ua + vb$. Décrivons cet algorithme en donnant un exemple : $A = \mathbb{Z}$, $\phi(n) = |n|$, $a = 19$ et $b = 15$. Une division de 19 par 15 s'écrit : $19 = 1{\cdot}15 + 4$, une division de 15 par 4 s'écrit : $15 = 4{\cdot}4 - 1$. Pour trouver des u et v tels que $-1 = u{\cdot}15 + v{\cdot}19$, on procède comme suit :

$$\begin{array}{rcrcr} 0{\cdot}15 & + & 1{\cdot}19 & = & 19 \\ 1{\cdot}15 & + & 0{\cdot}19 & = & 15 \\ -1{\cdot}15 & + & 1{\cdot}19 & = & 4 \\ 5{\cdot}15 & - & 4{\cdot}19 & = & -1 \end{array}$$

Evidemment, les deux premières lignes sont des identités tautologiques. La troisième ligne est obtenue des deux premières en prenant la première moins la deuxième, ce qui correspond à la division de 19 par 15. La quatrième ligne est la deuxième moins 4 fois la troisième, ce qui correspond à la division de 15 par 4.

   (a) Soit a votre numéro de téléphone personnel, b votre numéro de sécurité sociale. Calculer un PGCD d de a et b, ainsi que des nombres u et v tels que $d = ua + vb$.

   (b) Notons $a := X^5 + 1$ et $b := X^2 + X + 1$ dans $\mathbb{F}_2[X]$. Calculer le PGCD d de a et b, ainsi que des u et v dans $\mathbb{F}_2[X]$ tels que $d = ua + vb$.

8. (2.8.3 du polycopié.) Soit k un corps. Montrer que l'ensemble des polynômes irréductibles de $k[X]$ est infini, en s'inspirant de la démonstration d'Euclide pour l'ensemble des nombres premiers.

9. (2.8.4 du polycopié.) Il résulte de la remarque 2.8.2 que l'exercice 2.8.3 est trivial si k est infini : l'argument d'Euclide, bien que correct, est inutile dans ce cas. Si k est fini, déduire de 2.8.3 qu'il existe dans $k[X]$ des irréductibles de degré arbitrairement grand. (Plus loin, on montra que si k est fini, il existe des irréductibles dans $k[X]$ de degré $d \geq 1$ quelconque.)

10. (5.4.3 du polycopié.) Soit k un corps. Montrer que pour tous a dans k, F et G dans $k[X]$, on a $\mathrm{mult}_\alpha(FG) = \mathrm{mult}_\alpha(F) + \mathrm{mult}_\alpha(G)$ et $\mathrm{mult}_\alpha(F+G) \geq \inf(\mathrm{mult}_\alpha(F), \mathrm{mult}_\alpha(G))$.

11. (5.4.4 du polycopié.) Soit k un corps. Pour m dans $\mathbb{N}$, α dans k et F dans $k[X]$, montrer que $\mathrm{mult}_\alpha(F) = m$ si et seulement si il existe G dans $k[X]$ avec $F = (X - \alpha)^m G$ et $G(\alpha) \neq 0$.

12. Trouver les racines dans $\mathbb{Q}$ de $6X^3 - 29X^2 - 7X + 10$.

*13. Soient a et b dans $\mathbb{Z}$, avec b non nul. Montrer qu'il existe q et r dans $\mathbb{Z}$ tels que $a = qb + r$ et $|r| \leq |b|/2$. Montrer que la fonction $\phi\colon \mathbb{Z} \to \mathbb{N}$ donnée par $\phi(0) = 0$ et $\phi(n) = 1 + \mathrm{entier}(\log_2(n))$ pour n non nul est une fonction euclidienne. (Ici $\log_2(n)$ signifie le logarithme de n en base 2.)

Licence — Algèbre. Feuille d'exercices N° 11

15-12/97

*1. (D'après Martin Gardner.) Cinq marins se retrouvent naufragés sur une île où n'habite qu'un singe. Avant que la nuit tombe, ils rassemblent toutes les noix de coco, pour les jours à venir. Pendant la nuit, un des marins se réveille. N'ayant pas confiance en ces camarades, il repartit les noix de coco en cinq parts égales, donne la noix de coco restant au singe, cache sa part, refait un tas des quatre parts qui restent et se rendort. Un à un, la même chose arrive aux quatre autres. Question : combien de noix de coco y avait-il, étant donné que ce nombre est au plus cinq mille ?

2. Un triplet (a, b, c) dans $\mathbb{N}^3$ est appelé un triplet pythagoricien si $a^2 + b^2 = c^2$ et $abc \neq 0$. Un triplet pythagoricien (a, b, c) est dit primitif si $\mathrm{PGCD}(a, b, c) = 1$. Nous allons classifier les triplets pythagoriciens primitifs, à l'aide de la décomposition unique dans $\mathbb{Z}$.

   (a) Soit (a, b, c) un triplet pythagoricien. Montrer que les conditions suivantes sont équivalentes :

      1. $\mathrm{PGCD}(a, b, c) = 1$,
      2. $\mathrm{PGCD}(a, b) = 1$,
      3. $\mathrm{PGCD}(a, c) = 1$,
      4. $\mathrm{PGCD}(b, c) = 1$.

   *(b) Soit (a, b, c) un triplet pythagoricien primitif. En considérant les carrés dans $\mathbb{Z}/4\mathbb{Z}$, montrer que, quitte à échanger a et b, on a $a \equiv 1\ (2)$, $b \equiv 0\ (2)$ et $c \equiv 1\ (2)$. Montrer qu'alors $a^2 = (c - b)(c + b)$, et que $\mathrm{PGCD}(c - b, c + b) = 1$. (Indication : l'idéal de $\mathbb{Z}$ engendré par $c - b$ et $c + b$ contient $2c$ et $2b$.) En déduire qu'il existe des entiers u et v avec $0 < u < v$, impairs, premier entre eux, tel que $c - b = u^2$ et $c + b = v^2$.

   (c) Conclure que tout triplet pythagoricien primitif (a, b, c) avec b pair s'écrit sous la forme $(uv, (v^2 - u^2)/2, (v^2 + u^2)/2)$, avec $0 < u < v$ dans $\mathbb{N}$ premier entre eux et impairs.

   (d) Montrer que pour u et v dans $\mathbb{N}$ premier entre eux, impairs et tel que $u < v$, $(uv, (v^2 - u^2)/2, (v^2 + u^2)/2)$ est un triplet pythagoricien primitif. Conclure que les triplets pythagoriciens primitifs avec b pair sont les triplets $(uv, (v^2 - u^2)/2, (v^2 + u^2)/2)$, avec $u < v$ premier entre eux et uv impair.

   *(e) Soit (a, b, c) un triplet pythagoricien primitif avec b pair. En écrivant $(b/2)^2 = ((c - a)/2)((c + a)/2)$, montrer qu'il existe des entiers u et v, premier entre eux, tel que $0 < u < v$, $(c - a)/2 = u^2$ et $(c + a)/2 = v^2$. Conclure que les triplets pythagoriciens primitifs avec b pair sont les triplets $(v^2 - u^2, 2uv, v^2 + u^2)$, avec $0 < u < v$ premier entre eux et uv pair.

*3. A un triplet pythagoricien primitif (a, b, c) on fait correspondre le point $(a/c, b/c)$ du cercle C dans $\mathbb{R}^2$ de rayon un et de centre 0. Un élément de C est dit rationnel si ses deux coordonnées sont rationnelles. En considérant les droites passant par $(-1, 0)$, montrer que tout autre point rationnel de C est de la forme $(2t/(1+t^2), (1-t^2)/(1+t^2))$, avec t dans $\mathbb{Q}$. En déduire les classifications des triplets pythagoriciens primitifs de la question précédente.

4. (5.9.1 du polycopié.) Faites ce qui est demandé à la fin de la remarque IV.5.9.1 du polycopié.

5. (5.9.2 du polycopié.) Faites ce qui est demandé dans IV.5.9.2 du polycopié.

6. Soit A un anneau, I et J des idéaux dans A, $p: A \to B$ et $q: A \to C$ des morphismes d'anneaux surjectifs avec $I = \mathrm{Ker}(p)$ et $J = \mathrm{Ker}(q)$. Montrer que $p(I + J)$ est l'idéal

$p(J)$ de B. En appliquant Proposition II.5.6 à p, montrer que p induit un isomorphisme d'anneaux $\overline{p}: A/(I+J) \to B/p(J)$. En utilisant la même chose pour q, montrer que p et q induisent un isomorphisme

$$\overline{p} \circ \overline{q}^{-1}: C/q(I) \to B/p(J).$$

7. Soit p un nombre premier, différent de deux. Montrer, en utilisant le théorème de Wilson, que
$$\left(\left(\frac{p-1}{2}\right)!\right)^2 = (-1)^{(p+1)/2}$$
dans $\mathbb{F}_p$. Conclure que si p est congru à 1 modulo 4, alors X^2+1 admet une racine dans $\mathbb{F}_p$. Montrer également la réciproque : si X^2+1 admet une racine dans $\mathbb{F}_p$, alors p est congru à 1 modulo 4.
8. (a) Soit $f: \mathbb{Z}[X] \to \mathbb{Z}[i]$ le morphisme d'anneaux tel que $f(X) = i$. Montrer que $\mathrm{Ker}(f)$ est l'idéal engendré par X^2+1. Conclure qu'il existe un isomorphisme d'anneaux $g: \mathbb{Z}[X]/(X^2+1) \to \mathbb{Z}[i]$, unique, tel que g envoie la classe de X vers i.
   *(b) Soit n dans $\mathbb{Z}$. Montrer que f induit un isomorphisme de $(\mathbb{Z}/n\mathbb{Z})[X]/(X^2+1)$ vers $\mathbb{Z}[i]/(n)$. Indication : montrer d'abord que le morphisme $\mathbb{Z}[X] \to (\mathbb{Z}/n\mathbb{Z})[X]$ qui envoit X vers X a noyau l'idéal engendré par n ; ensuite, utiliser un des exercices précedents.
   *(c) Soit p un nombre premier congru à 1 modulo 4. Montrer que $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{F}_p \times \mathbb{F}_p$. Conclure que p est réductible dans $\mathbb{Z}[i]$, et qu'il existe a et b dans $\mathbb{Z}$ avec $p = a^2 + b^2$. Combien de tels couples (a, b) y a-t-il?

*9. Soit p un nombre premier. Montrer que X^2+X+1 admet une racine dans $\mathbb{F}_p$ si et seulement si p n'est pas congru à -1 modulo 3. Montrer que si p n'est pas congru à -1 modulo 3, alors il existe a et b dans $\mathbb{Z}$ tel que $p = a^2 + ab + b^2$.

*10. Soit p un nombre premier. Soit n dans $\mathbb{N}$. Montrer que $\mathbb{F}_p^*$ possède un élément d'ordre n si et seulement si n divise $p-1$.

*11. Soit p un nombre premier. Soit ϕ un isomorphisme de groupes de $\mathbb{F}_p^*$ vers $\mathbb{Z}/(p-1)\mathbb{Z}$. Calculer $\phi(-1)$.

*12. Soit $p \neq 2$ un nombre premier. Montrer que dans $\mathbb{F}_p^*$ il y a exactement $(p-1)/2$ carrés et $(p-1)/2$ non carrés. Montrer que $a \neq 0$ dans $\mathbb{F}_p$ est un carré si et seulement si $a^{(p-1)/2} = 1$.

13. Montrer que X^2-1 a un nombre infini de racines dans $\mathrm{M}(2,\mathbb{R})$. Autrement dit, dans la notation de IV.4.5, l'ensemble $\mathrm{sol}(X^2-1, \mathrm{M}(2,\mathbb{R}))$ est infini.

*14. Donner une autre démonstration du fait que $\mathbb{C}$ est algébriquement clos, basée sur le fait que tout minimum local d'une fonction $z \mapsto |f(z)|$ avec f analytique est nul. Plus précisement, soit f dans $\mathbb{C}[X]$ non constant. Montrer que la fonction $g: \mathbb{C} \to \mathbb{R}$, $g(z) = |f(z)|$, atteint une valeur minimale, et que cette valeur minimale est nulle.

*15. Soit $f := X^3 + 3X - 2$ dans $\mathbb{Q}[X]$. Montrer que $\mathbb{Q}[X]/(f)$ est un corps. Est-il isomorphe à un sous-corps de $\mathbb{R}$? Est-il isomorphe à un sous-corps de $\mathbb{C}$ non contenu dans $\mathbb{R}$? Combien f a-t-il de racines dans $\mathbb{Q}[X]/(f)$? Notons u la classe de X dans $\mathbb{Q}[X]/(f)$. Montrer que $(1, u, u^2)$ est une $\mathbb{Q}$-base de $\mathbb{Q}[X]/(f)$. Exprimer $(2u^2+u-3)(3u^2-4u+1)$ et $(u^2-u+4)^{-1}$ dans cette base.

16. Montrer que $\mathbb{F}_2[X]/(X^3+X+1)$ est un corps. Trouver un générateur du groupe multiplicatif. Même chose pour $\mathbb{F}_2[X]/(X^4+X+1)$.

17. (IV.8.1.1 du polycopié.) Décomposer dans $\mathbb{C}[X]$ le polynôme $P := X^4+1$. Décomposer P dans $\mathbb{R}[X]$, et en déduire que P est irréductible dans $\mathbb{Q}[X]$. (Indication : considérer la décomposition dans $\mathbb{Q}[X]$, et remarquer que tout facteur irréductible est un produit de facteurs irréductibles de P dans $\mathbb{R}[X]$.)

18. Faites la démonstration de la Proposition IV.8.4. Autrement dit : pour k un corps et P dans $k[X]$ de degré deux ou trois, montrer que P est réductible si et seulement si il admet une racine dans k.
19. (IV.8.5.2 du polycopié.) Généraliser la Proposition IV.8.5 aux polynômes à coefficients dans un anneau principal.
20. Montrer que dans $\mathbb{Q}[X]$ il existe des polynômes irréductibles de degré ≥ 1 quelconque.
*21. (IV.8.6.2 du polycopié.) Soient $a > 0$ dans $\mathbb{Q}$ et $n > 1$ un entier impair. Montrer que $X^n + a$ est réductible si et seulement si il existe un diviseur $d > 1$ de n tel que a soit une puissance d-ième dans $\mathbb{Q}$. Pour n pair la question est plus compliquée : montrer que $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$, tandis que $X^4 + 4$ est réductible dans $\mathbb{Q}[X]$.
**22. Soit p un nombre premier. Montrer que les seuls sous-espaces stables dans $\mathbb{Q}^{p-1}$ pour l'endomorphisme donnée par la matrice :

$$\begin{pmatrix} 0 & & & & -1 \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -1 \\ & & & 1 & -1 \end{pmatrix}$$

sont $\{0\}$ et $\mathbb{Q}^{p-1}$.
23. (IV.8.7.3 du polycopié.) Par un changement de variable convenable, retrouver à l'aide du critère d'Eisenstein l'irréductibilité de X^4+1 dans $\mathbb{Q}[X]$. Généraliser aux polynômes $X^{2^n} + 1$, n dans $\mathbb{N}$.
*24. (IV.8.8 du polycopié.) Faites les exercices dans IV.8.8 du polycopié.
25. (IV.9.2.1 du polycopié.) Pourquoi n'a-t-on pas défini la dérivation de polynômes comme on le fait pour les fonctions réelles ?
26. (IV.9.2.2 du polycopié.) Donner un exemple d'un corps k et d'un polynôme non constant P dans $k[X]$ tel que le degré de $D(P)$ est plus petit que $\deg(P) - 1$.
27. (IV.9.4.1 du polycopié.) Donner un exemple d'un corps k, d'un polynôme P dans $k[X]$ et d'une racine α de P dans k tel que $\mathrm{mult}_\alpha(P') > \mathrm{mult}_\alpha(P) - 1$.
*28. (IV.9.4.3 du polycopié.) Faites ce qui est demandé dans IV.9.4.3 du polycopié.
*29. Est-ce que $X^{100}+X^{50}+X+1$ a une racine multiple dans une extension algébriquement close de $\mathbb{F}_2$?
**30. Est-ce que $X^{100} + X^{50} + X + 1$ a une racine multiple dans $\mathbb{C}$?
31. (IV.9.6.2 du polycopié.) Donner explicitement pour chaque n dans $\mathbb{N}$ un isomorphisme entre $\mu_n(\mathbb{C})$ et $\mathbb{Z}/n\mathbb{Z}$.

Licence — Algèbre. Feuille d'exercices N° 12

05-01/98

1. Soient A un anneau et $n \geq 0$ un entier. Montrer que tout P dans $A[X_1, \ldots, X_n]$ sécrit de façon unique sous la forme $P = \sum_i P_i$, avec P_i combinaison linéaire de monômes de degré (total) i. Montrer que pour P et Q dans $A[X_1, \ldots, X_n]$ on a $(PQ)_n = \sum_{i+j=n} P_i Q_j$.
2. (IV.10.4 du polycopié.) Soit A un anneau intègre. Soit $n \geq 0$. Montrer que l'anneau $A[X_1, \ldots, X_n]$ de polynômes en n variables à coefficients dans A est intègre, par récurrence sur n. Montrer que $\deg(PQ) = \deg(P) + \deg(Q)$ pour tous P et Q dans $A[X_1, \ldots, X_n]$. Montrer que $A[X_1, \ldots, X_n]^\times = A^\times$.
3. Soient A un anneau, n, i et j des entiers ≥ 0 tels que $n = i+j$. Donner un isomorphisme d'anneaux entre $A[X_1, \ldots, X_n]/(X_1, \ldots, X_i)$ et $A[X_1, \ldots, X_j]$.

*4. (IV.10.6.2 du polycopié.) Soient k un corps, $n \geq 0$ un entier et $S_1, \ldots, S_n$ des parties infinies de k. Soit S le sous-ensemble $S_1 \times \cdots \times S_n$ de k^n. Soit P dans $k[X_1, \ldots, X_n]$ tel que $P(s) = 0$ pour tout s dans S. Montrer que P est nul.

5. (IV.10.6.3 du polycopié.) Soient k un corps, $n \geq 0$ un entier. Soit P dans $k[X_1, \ldots, X_n]$ non nul.
   *(a) Supposons que k est de caractéristique nulle. Montrer qu'il existe des entiers $a_1, \ldots, a_n$ tels que $P(a_1, \ldots, a_n) \neq 0$.
   **(b) Supposons que k est un sous-corps de $\mathbb{C}$. Montrer que le sous-ensemble $\{x \in k^n \mid P(x) \neq 0\}$ est un ouvert dense de k^n, pour la topologie induite par la topologie usuelle de $\mathbb{C}^n$.
6. Soit k un corps fini, de cardinal q. Soit $n \geq 0$ un entier. Notons A la k-algèbre de fonctions sur k^n à valeurs dans k. Notons $f\colon k[X_1, \ldots, X_n]$ le morphisme de k-algèbres $P \mapsto \tilde{P}$ de IV.10.6.1.
   *(a) Montrer que f est surjectif.
   *(b) Montrer que $\mathrm{Ker}(f)$ est engendré par les $X_i^q - X_i$.
7. Donner un élément de $\mathbb{Q}[X, Y]$ tel que $f(0,0) = 1$ et $f(1,0) = f(-1,0) = f(0,1) = f(0,-1) = 0$. Quel est le degré minimal d'un tel élément ?
8. Soit k un corps infini. Soit P dans $k[X, Y]$.
   *(a) Supposons que pour tout x dans k on ait $P(x, 0) = 0$. Montrer que Y divise P.
   *(b) Supposons que pour tout x dans k on ait $P(x, x) = 0$. Montrer que $X - Y$ divise P.
9. (IV.11.2.1 du polycopié.) Montrer que ${}^n\Sigma_d = 0$ si $d > n$. Montrer que ${}^0\Sigma_0 = 1$.
10. (IV.11.2.3 du polycopié.) Montrer les relations de récurrence de IV.11.2.3 du polycopié.
11. (Identités de Newton.) Pour n et d des entiers ≥ 0 posons ${}^n\Pi_d := X_1^d + \cdots + X_n^d$ dans $\mathbb{Z}[X_1, \ldots, X_n]$.
    *(a) Soient n dans $\mathbb{N}$. Montrer que :
    $$\begin{aligned} {}^n\Pi_0 &= n, \\ {}^n\Pi_1 &= {}^n\Sigma_1, \\ {}^n\Pi_2 &= {}^n\Sigma_1^2 - 2\,{}^n\Sigma_2, \\ {}^n\Pi_3 &= {}^n\Sigma_1^3 - 3\,{}^n\Sigma_1\,{}^n\Sigma_2 + 3\,{}^n\Sigma_3, \end{aligned}$$
    **(b) Soient n et d dans $\mathbb{N}$. Montrer que :
    $${}^n\Pi_d - {}^n\Sigma_1\,{}^n\Pi_{d-1} + {}^n\Sigma_2\,{}^n\Pi_{d-2} - \cdots + (-1)^{d-1}\,{}^n\Sigma_{d-1}\,{}^n\Pi_1 + (-1)^d d\,{}^n\Sigma_d = 0.$$

Indication : pour $d \geq n$, utiliser les identités IV.11.3.2 du polycopié, multipliées par X_j^{d-n} ; pour $d < n$, utiliser que l'expression est symétrique, que

$$^{n}\Sigma_d(X_1, \ldots, X_d, 0, \ldots, 0) = {}^{d}\Sigma_d$$

et que, si $d > 0$, on a l'identité $^{n}\Pi_d(X_1, \ldots, X_d, 0, \ldots, 0) = {}^{d}\Pi_d$.

*(c) Soit n dans $\mathbb{N}$. Montrer que :

$$\begin{aligned} {}^{n}\Sigma_1 &= {}^{n}\Pi_1, \\ 2\,{}^{n}\Sigma_2 &= {}^{n}\Pi_1^2 - {}^{n}\Pi_2, \\ 6\,{}^{n}\Sigma_3 &= {}^{n}\Pi_1^3 - 3\,{}^{n}\Pi_1\,{}^{n}\Pi_2 + 2\,{}^{n}\Pi_3. \end{aligned}$$

Montrer que pour tout d dans $\mathbb{N}$, $d!\,{}^{n}\Pi_d$ est un polynôme à coefficients dans $\mathbb{Z}$ en les ${}^{n}\Sigma_i$.

12. (IV.12.3.1 du polycpoié.) Soit k un corps. Expliciter l'application ${}^{n}\boldsymbol{\Sigma}$ pour chaque $n \leq 3$.

*13. (IV.12.4 du polycopié.) Faites l'exercice IV.12.4 du polycopié.

14. (IV.12.7.1 du polycopié.)
   (a) Est-ce que l'application ${}^{2}\boldsymbol{\Sigma}$ de $\mathbb{Q}^2$ vers $\mathbb{Q}^2$ est bijective ?
   (b) Soit k un corps tel que pour tout n dans $\mathbb{N}$ l'application ${}^{n}\boldsymbol{\Sigma}$ de k^n vers k^n soit bijective. Est-ce que k est algébriquement clos ?
   **(c) Soit k un corps tel que l'application ${}^{2}\boldsymbol{\Sigma}$ de k^2 vers k^2 soit bijective. Est-ce que k peut être fini ? Est-ce que k est algébriquement clos ?

15. (IV.12.8.3 du polycopié.) Soit $f\colon \mathbb{C}^2 \to \mathbb{R}$ donnée par $f(x,y) = |x-y|$. Montrer que f est symétrique, et trouver une formule simple pour l'unique $\widehat{f}\colon \mathbb{C}^2 \to \mathbb{R}$ tel que $f = \widehat{f} \circ \boldsymbol{\Sigma}$.

*16. (IV.12.9 du polycopié.) Faites l'exercice IV.12.9 du polycopié.

*17. (IV.12.10.1 du polycopié.) Soient A un anneau, n dans $\mathbb{N}$ et P dans $A[X_1, \ldots, X_n]$. Montrer que si P est symétrique, alors $\widetilde{P}$ l'est aussi. Montrer la réciproque pour A un corps infini.

18. Soit $n \geq 2$ un entier. Considérons l'action naturelle de $\mathfrak{S}_n$ sur $\mathbb{Z}[X_1, \ldots, X_n]$.
   (a) Quel est le cardinal de l'orbite du monôme X_1 ? Et de $X_1^2X_2$? Et de X_1X_2 ?
   (b) Existe-t-il un monôme dont l'orbite est de cardinal $n!$?
   *(c) Quels sont les cardinaux possibles pour les orbites de monômes ?
   **(d) Soit H un sous-groupe de $\mathfrak{S}_n$. Existe-t-il un élément P de $\mathbb{Z}[X_1, \ldots, X_n]$ tel que H soit le stabilisateur de P ?

19. Soit n dans $\mathbb{N}$. Considérons l'action naturelle de $\mathfrak{S}_n$ sur $\mathbb{Z}[X_1, \ldots, X_n]$. Soit P dans $\mathbb{Z}[X_1, \ldots, X_n]$. Montrer que $\sum_\sigma \sigma(P)$, où la somme est prise sur $\mathfrak{S}_n$, est symétrique. Est-ce que tout polynôme symétrique est de cette forme ?

20. (IV.12.11.8 du polycopié.) Calculer $X^2Y^2 + Y^2Z^2 + Z^2X^2$ en fonction de $X+Y+Z$, $XY+YZ+ZX$ et XYZ, le tout dans $\mathbb{Z}[X,Y,Z]$. Est-ce qu'on peut se passer d'un des trois polynômes symétriques élémentaires ?

21. Calculer $X^2Y + X^2Z + XY^2 + XZ^2 + Y^2Z + YZ^2$ en fonction des trois polynômes symétriques élémentaires.

22. (IV.12.12.9 du polycopié.) Soit F dans $\mathbb{R}[X]$ unitaire de degré trois. Peut-on déduire du discriminant de F le nombre de racines réelles de F, comptées avec multiplicités ? Et le nombre de racines réelles distinctes de F ?

*23. Montrer que toutes les racines dans $\mathbb{C}$ du polynôme $X^{10} + 2X^9 - 6X^7 + 10X^4 - 3X + 12$ sont simples. Indication : le discriminant de ce polynôme est un entier.

*24. Montrer que toutes les racines dans $\mathbb{C}$ de $X^{100} + 6X^{61} - 3X^{49} + 678X^{17} - 1234567$ sont simples.

25. (Examen janvier 1996.) Pour a, b et c dans $\mathbb{C}$ on considère le polynôme $P = X^3 + aX^2 + bX + c$. On désigne par α, β et γ les racines de P dans $\mathbb{C}$ (comptées avec multiplicités). Calculer, en fonction de a, b et c, le polynôme unitaire Q dans $\mathbb{C}[X]$ de degré trois ayant pour racines $\alpha^2\beta^2$, $\beta^2\gamma^2$ et $\gamma^2\alpha^2$.

26. (Examen janvier 1996.) Soit k un corps. Notons p la caractéristique de k. Soit $n \geq 2$. Notons P le polynôme $X^n - X + 1$ à coefficients dans k. Soit K une clôture algébrique de k.
    (a) Dans chacun des cas suivants, décider si P a au moins une racine multiple dans K, et déterminer le cas échéant une telle racine :
        (i) p divise n ;
        (ii) $p = 0$;
        (iii) $p = 23$ et $n = 3$.
    (b) Calculer la somme des puissances d-ièmes des racines de P dans K :
        (i) pour $d = n$;
        (ii) pour $d = n + 1$;

27. (Examen janvier 1996.) Soient F et G dans $\mathbb{Q}[X]$ deux polynômes non nuls. On suppose que les $\mathbb{Q}$-algèbres $A := \mathbb{Q}[X]/(F)$ et $B := \mathbb{Q}[X]/(G)$ sont isomorphes. Les assertions suivantes sont-elles vraies ou fausses (on justifiera les réponses) :
    (a) si F est irréductible, alors G est irréductible ;
    (b) F et G ont une racine commune dans $\mathbb{C}$.

28. (Examen de septembre 1996.) Soit P dans $\mathbb{Q}[X]$ le polynôme $3X^{571} + 289X^{102} + 51$.
    (a) Montrer que P est irréductible.
    (b) Soit K le corps $\mathbb{Q}[X]/(P)$. Est-ce que K est isomorphe à un sous-corps de $\mathbb{R}$? (On justifiera la réponse.)

29. (Examen de septembre 1996.) Soient L un corps, K un sous-corps de L. On suppose que L est de dimension deux en tant que K-espace vectoriel.
    (a) Soit α dans L et non dans K. Montrer que α est racine d'un polynôme irréductible de degré deux à coefficients dans K. (Indication : considérer les puissances de α.)
    (b) Soit P dans $K[X]$ irréductible de degré deux, ayant une racine dans L. Montrer que les corps L et $K[X]/(P)$ sont isomorphes.
    (c) (i) Déduire des questions précédentes qu'il existe P dans $K[X]$ de degré deux tel que L soit isomorphe à $K[X]/(P)$.
        (ii) On suppose de plus que la caractéristique de K est différente de deux. Montrer que le polynôme P de (a) peut être choisi de la forme $X^2 - m$, pour m dans K convenable.
    (d) (Indépendante des précédentes.) On prend $K := \mathbb{F}_2$, $L := K[X]/(X^2 + X + 1)$. Montrer que L est bien un corps mais qu'il n'existe aucun élément m de K tel que L soit isomorphe à $K[X]/(X^2 - m)$.