EXERCICES

Il est parfaitement utopique d'espérer apprendre des Mathématiques, si élémentaires ou si supérieures soient-elles, sans résoudre des Exercices.

Les Exercices qu'on trouvera dans ce livre sont de trois sortes. Certains sont des illustrations pratiques ou même numériques des théories exposées dans le texte; le lecteur débutant ne pourra pas acquérir la technique du calcul sans résoudre une partie appréciable des Exercices de ce genre. D'autres apportent au texte des compléments théoriques élémentaires; en les étudiant, le lecteur s'habituera à manipuler le langage et les modes de raisonnements utilisés dans le texte; ceux de ces Exercices qui ne sont pas *très* faciles sont précédés d'un signe ¶. Enfin, la dernière catégorie est constituée par des Exercices qui apportent au texte des compléments importants et difficiles; ils sont destinés uniquement aux étudiants déjà avancés qui s'intéressent vraiment aux Mathématiques; ces Exercices sont précédés de deux ou même trois signes ¶.

Nous ne saurions trop insister enfin sur le fait que résoudre un Exercice ne consiste pas seulement à se convaincre, à l'aide d'un « brouillon » fait à la hâte, du fait qu'on en a à peu près compris la solution; si cette méthode est admissible pour les Exercices de calcul numérique, il faut par contre s'efforcer de *rédiger intégralement* les Exercices plus théoriques, où l'on doit construire de véritables démonstrations. De cette façon, et uniquement de cette façon, l'étudiant parviendra à acquérir un langage clair et correct, et à utiliser les termes techniques dans leur sens propre, ce qui, en Mathématiques, est le signe le plus certain de la compréhension d'un sujet.

1. Soient R et S deux relations. Montrer que, si R est fausse, la relation $(R \Longrightarrow S)$ est vraie. Peut-on déduire de là que S est vraie?

2. Soient R et S deux relations. Montrer que la relation

$$[R \text{ et } (\text{non } R)] \Longrightarrow S$$

est vraie.

3. Montrer à l'aide d'un exemple que la relation

$$(\forall x)\ (\exists y)R \Longrightarrow (\exists y)\ (\forall x)R$$

n'est généralement pas vraie.

4. Soient R et S deux relations équivalentes, et T une relation quelconque. Montrer que chacune des relations suivantes est vraie :

$$\begin{gathered}(\text{non } R) \Longleftrightarrow (\text{non } S)\\ (R \Longrightarrow T) \Longleftrightarrow (S \Longrightarrow T)\\ (T \Longrightarrow R) \Longleftrightarrow (T \Longrightarrow S)\\ (R \text{ et } T) \Longleftrightarrow (S \text{ et } T)\\ (R \text{ ou } T) \Longleftrightarrow (S \text{ ou } T).\end{gathered}$$

¶¶ 5. Démontrer les relations suivantes, où R, S et T désignent des relations quelconques :

$$\begin{gathered}R \Longrightarrow (S \Longrightarrow R)\\ (R \Longrightarrow S) \Longrightarrow [(S \Longrightarrow T) \Longrightarrow (R \Longrightarrow T)]\\ R \Longrightarrow [(\text{non } R) \Longrightarrow S]\\ (R \text{ ou } S) \Longleftrightarrow [(R \Longrightarrow S) \Longrightarrow S]\\ (R \Longleftrightarrow S) \Longleftrightarrow \{(R \text{ et } S) \text{ ou } [(\text{non } R) \text{ et } (\text{non } S)]\}\\ (R \Longleftrightarrow S) \Longleftrightarrow \text{non } [(\text{non } R) \Longleftrightarrow S]\\ \{R \Longrightarrow [S \text{ ou } (\text{non } T)]\} \Longleftrightarrow [(T \text{ et } R) \Longrightarrow S]\\ [R \Longrightarrow (S \text{ ou } T)] \Longleftrightarrow [S \text{ ou } (R \Longrightarrow T)\\ (R \Longrightarrow S) \Longrightarrow \{(R \Longrightarrow T) \Longrightarrow [R \Longrightarrow (S \text{ et } T)]\}\\ (R \Longrightarrow T) \Longrightarrow \{(S \Longrightarrow T) \Longrightarrow [(R \text{ ou } S) \Longrightarrow T]\}.\\ (R \Longrightarrow S) \Longrightarrow [(R \text{ et } T) \Longrightarrow (S \text{ et } T)]\\ (R \Longrightarrow S) \Longrightarrow [(R \text{ ou } T) \Longrightarrow (S \text{ ou } T)].\end{gathered}$$

6. Soient R et S deux relations et x une lettre ne figurant pas dans R. Montrer que les relations

$$(\forall x)\ (\text{R ou S}) \Longleftrightarrow (\text{R ou } (\forall x)\text{S})$$
$$(\exists x)\ (\text{R et S}) \Longleftrightarrow (\text{R et } (\exists x)\text{S})$$

sont vraies.

7. Soient R et S deux relations, x une lettre. Démontrer les relations

$$[(\forall x)(\text{R ou S})] \Longrightarrow [(\forall x)\text{R ou } (\exists x)\text{S}]$$
$$[(\exists x)\text{R et } (\exists x)\text{S}] \Longrightarrow [(\exists x)\ (\text{R et S})].$$

8. Les cannibales d'une tribu se préparent à manger un missionnaire. Désirant lui prouver une dernière fois leur respect de la dignité et de la liberté humaines, les cannibales proposent au missionnaire de décider lui-même de son sort en faisant une courte déclaration : si celle-ci est vraie, le missionnaire sera roti, et il sera bouilli dans le cas contraire. Que doit dire le missionnaire pour sauver sa vie ? (d'après Cervantès).

9. Le Colonel X traite le Professeur Y d'assassin. Deux semaines plus tard, le Colonel est l'objet d'une tentative d'assassinat inspirée par le Professeur. Le Colonel avait-il raison?

10. Énoncer des assertions équivalentes aux négations des assertions suivantes (*) :

a) Tout triangle rectangle possède un angle droit.

b) Dans toutes les prisons tous les détenus détestent tous les gardiens.

c) Pour tout entier x il existe un entier y tel que pour tout entier z la relation $z < y$ implique la relation $z < x + 1$.

11. Examiner les relations logiques existant entre les assertions suivantes :

A : Tous les hommes sont mortels.
B : Tous les hommes sont immortels.
C : Aucun homme n'est mortel.
D : Aucun homme n'est immortel.
E : Il existe des hommes immortels.
F : Il existe des hommes mortels.

12. Montrer, à l'aide de l'opération de Hilbert, que si R est une relation et x une lettre figurant dans R, la lettre x *ne figure plus* dans les relations $(\forall x)$R et $(\exists x)$R, en dépit des notations utilisées pour désigner ces deux relations.
Ce résultat fort simple montre que, dans la notation $(\forall x)$R, la lettre x ne figure que pour indiquer une opération à effectuer sur la relation R, opération ayant pour résultat, entre autres, d'éliminer x de la relation R. Un phénomène analogue se retrouve dans la notation traditionnelle

$$\int_0^1 f(x)dx,$$

où la lettre x ne joue évidemment aucun rôle et, en particulier, ne figure pas dans le résultat final.

(*) La façon la plus simple (et pour cause) d'écrire la négation d'une relation est de faire précéder celle-ci d'un signe « non ». Ce n'est évidemment pas ce qu'on demande au lecteur de faire dans cet *Exercice*...

Cet Exercice explique aussi pourquoi, dans la relation $(\forall x)$R, on peut si on le désire remplacer la lettre x par toute autre lettre ne figurant pas dans R; par exemple, les relations

$$(\forall x)\ (x \times y = x - z) \qquad \text{et} \qquad (\forall t)\ (t \times y = t - z)$$

sont non seulement équivalentes mais en fait identiques. Il n'en est par contre pas de même des relations

$$(\forall x)\ (x \times y = x - z) \qquad \text{et} \qquad (\forall y)\ (y \times y = y - z).]$$

¶ 13. Sur la planète Mars, on distingue en première approximation deux sortes d'opinions politiques : celles de droite et celles de gauche. D'autre part, les étudiants martiens se répartissent en deux associations : l'Union Planétaire des Étudiants Martiens (UPEM) et la Fédération Planétaire des Étudiants Martiens (FPEM). Sachant que les étudiants de gauche adhèrent à l'UPEM, démontrer que la FPEM est apolitique.

14. On considère quatre nombres entiers m, n, p, q sur lesquels on fait les hypothèses suivantes : *a*) les entiers m, p et q sont premiers entre eux; *b*) le reste de la division de m par pq est égal à 12; *c*) le reste de la division de $2n - 3$ par n est égal à 3; *d*) il n'existe aucun couple d'entiers x, y vérifiant la relation

$$x^4 - y^5 = p^2 - q^2 + m^6.$$

Démontrer que n est pair.

15. On considère les deux assertions suivantes :

a) : « En plein accord avec M. Robert Lacoste, ministre résidant en Algérie, nous confions la responsabilité de ramener la paix et la sécurité à Alger à la 10e division parachutiste. Cette unité gagnera en trois mois la bataille d'Alger sans tirer sur les immeubles avec des mitrailleuses lourdes, et sans qu'un seul avion français arrose de balles la Casbah. » (Extrait de la déclaration faite par le Général Salan à son procès).

b) : « The result was that the « battle of Algiers » became, for the paratroopers who fought it, and for France itself, a pyrrhic victory : it is estimated that out of the Kasbah's total population of 80 000 between 30 and 40 per cent of its active male population was, at one stage or another of the « battle », arrested for questioning and questioning came to involve the use of torture as a basic instrument, as a time-saving device to obtain quick results. » (Edward Behr, correspondant de *Time* à Alger, dans *The Algerian Problem*, W. W. Norton, New York, 1961).
Ces assertions sont-elles logiquement incompatibles? (On ne demande pas de décider si elles sont vraies ou fausses).

16. Utiliser la règle non (non A) $\Longleftrightarrow$ A pour simplifier la phrase suivante (extraite d'un compte rendu de match de football) :

« ... il ne se trouvera aucun sportif pour nier que le contraire n'eût été immérité... ».
Même question avec le texte suivant :

« Je vous envoie encore une note sur les examens. J'ai tenu à rappeler quelques principes fondamentaux. Je fais allusion à certaines « décisions » ou certains comportements qui sont encore, heureusement, peu nombreux. Mais, même s'ils restent peu nombreux et s'ils devaient être confirmés légalement, il ne manquera pas de gens pour dénier toute valeur à la qualité du travail que la très grande majorité des enseignants de la Faculté s'efforce de mener à bien. »

17. A la suite d'une représentation de *Pelléas et Mélisande*, un journaliste hésite entre les deux rédactions suivantes :

A) Jamais le rôle de Mélisande n'a été si bien chanté.

B) Jamais si jeune cantatrice, aux si beaux cheveux, n'a si bien chanté Mélisande.

Lequel de ces compliments est le plus fort ? (Expliciter non A et non B.)

¶¶ **1.** La définition mathématique complète de l'ensemble vide, utilisant l'opération de Hilbert, est que $\emptyset$ désigne l'objet mathématique

$$\tau_x[(\forall x)\ (x \notin X)];$$

en déduire la définition de $\emptyset$ en langage formalisé (i.e. écrire $\emptyset$ sous la forme d'un assemblage ne comportant que des signes fondamentaux, à l'exclusion de toute abréviation).

¶¶ **2.** Construire une démonstration logiquement complète du Théorème 5 (cf. *Remarque* 6).

3. Écrire tous les éléments de l'ensemble

$$\mathfrak{P}(\mathfrak{P}(\mathfrak{P}(\mathfrak{P}(\emptyset)))).$$

4. Soient X et Y deux ensembles. Montrer que les relations $X \subset Y$ et $\mathfrak{P}(X) \subset \mathfrak{P}(Y)$ sont équivalentes.

¶ **5.** Montrer qu'il n'existe aucun ensemble X pour lequel la relation

$$\mathfrak{P}(X) \subset X$$

soit vraie.

6. Soient X l'ensemble des nombres x tels que $0 \leqslant x < 1/100\,000\,000$, et Y l'ensemble des nombres y tels que $0 < y \leqslant 100\,000\,000$; démontrer que $X \subset Y$.

1. Soient I l'ensemble des nombres réels θ tels que $0 \leqslant \theta \leqslant 2\pi$, et G l'ensemble des rotations autour d'un point donné O dans le plan. On considère l'application f de I dans G qui, à chaque nombre $\theta \in I$, associe la rotation d'angle θ autour du point O. L'application f est-elle surjective? injective? bijective? Que se passe-t-il lorsqu'on prend pour I l'ensemble des nombres réels θ tels que $0 < \theta \leqslant 2\pi$?

2. Soient X et Y des ensembles; pour qu'une partie G de $X \times Y$ soit le graphe d'une application de X dans Y, il faut et il suffit que l'application pr_1 de G dans X soit bijective.

3. Soient $f : X \to Y$ et $g : Y \to Z$ deux applications, et $h = g \circ f$ l'application composée. *a*) si h est injective, f est injective; si de plus f est surjective, alors g est injective. *b*) si h est surjective, g est surjective; si en outre g est injective, alors f est surjective.

4. On considère des ensembles X, Y, Z et des applications

$$f : X \to Y, \qquad g : Y \to Z, \qquad h : Z \to X;$$

on forme les applications composées

$$h \circ g \circ f, \qquad g \circ f \circ h, \qquad f \circ h \circ g$$

et on suppose soit que deux d'entre elles sont injectives et la troisième surjective, soit que deux d'entre elles sont surjectives et la troisième injective. Montrer qu'alors f, g et h sont bijectives.

5. Soient X, Y, Z trois ensembles, E l'ensemble de toutes les applications de $X \times Y$ dans Z, et F l'ensemble de toutes les applications de X dans l'ensemble

$$Z^Y$$

de toutes les applications de Y dans Z. Construire une bijection de E sur F.

6. On appelle **correspondance entre deux ensembles X et Y** tout triplet

$$f = (G, X, Y) \quad \text{avec} \quad G \subset X \times Y;$$

cette notion généralise donc celle d'application de X dans Y [une correspondance entre X et Y ou, comme on dit aussi, de X à Y, est aussi appelée fréquemment une « fonction multiforme non partout définie » pour des raisons qui apparaîtront plus bas; cette terminologie, utilisée jusqu'à une date très récente, présente l'inconvénient majeur de laisser supposer que la notion de correspondance est un cas particulier de celle de fonction, alors que c'est l'opposé qui est vrai.] L'ensemble G s'appelle le **graphe** de f. On dit que f est **définie** en un élément x de X si $x \in pr_1(G)$; il existe alors au moins un $y \in Y$ tel que $(x, y) \in G$, et on dit que x et y **se correspondent par** f (il peut naturellement arriver que f ne soit pas définie pour tous les $x \in X$, et que, si f est définie en x, il existe plusieurs $y \in Y$ qui correspondent à x par f; ce sont ces deux circonstances qui expliquent la terminologie « fonction multiforme non partout définie »).

a) Étudier (pour $X = Y = \mathbf{R}$, ensemble des nombres réels) les correspondances dont les graphes sont les ensembles définis par les équations suivantes :

$$xy = 1; \qquad axy + bx + cy + d = 0; \qquad x^2 + y^2 = 1; \qquad x = \sin y$$

(dans le second exemple, a, b, c, d sont des constantes réelles données). Dans chaque cas on déterminera les valeurs de x pour lesquelles la correspondance est définie, et les y qui correspondent à un tel x.

b) Soient Γ et Γ' deux cercles distincts dans un plan; on prend pour X et Y l'ensemble des points de Γ, et pour G l'ensemble des couples $(x, y) \in X \times X$ qui sont situés sur une même tangente à Γ'. Quels sont les points de Γ où f est définie? Combien de points correspondent-ils à un point où f est définie?

¶ **7.** Soit $f = (G, X, Y)$ une correspondance entre deux ensembles X et Y (cf. Exercice **6**); pour toute partie A de X, on note $f(A)$ l'ensemble des $y \in Y$ qui correspondent par f à au moins un $x \in A$, et pour toute partie B de Y on note

$$\bar{f}^1(B)$$

l'ensemble des $x \in X$ tels qu'il corresponde à x au moins un $y \in B$. Démontrer les relations

$$A \subset \bar{f}^1(f(A)), \qquad B \supset f(\bar{f}^1(B)).$$

¶ **8.** Soient $f = (G, X, Y)$ et $g = (H, Y, Z)$ deux correspondances; on appelle **composée** de g et f la correspondance

$$g \circ f = (K, X, Z) = h$$

définie comme suit : on a $(x, z) \in K$ si et seulement s'il existe un $y \in Y$ tel que l'on ait $(x, y) \in G$ et $(y, z) \in H$. Montrer que cette définition généralise celle de composée de deux applications; étendre le Théorème 2 du § 2 aux correspondances. Étant donnée une partie A de X, a-t-on nécessairement la relation $h(A) = g(f(A))$?

Si $f = (G, X, Y)$ est une correspondance, on appelle correspondance **réciproque** de f la correspondance

$$\bar{f}^1 = (G', Y, X)$$

où $G' \subset Y \times X$ est l'ensemble des couples (y, x) tels que $(x, y) \in G$. La correspondance composée $\bar{f}^1 \circ f$ est-elle l'application identique de X dans X? Montrer que, si f est une application de X dans Y, pour que la correspondance réciproque soit elle-même une application de Y dans X il faut et il suffit que f soit bijective; la correspondance $\bar{f}^1$ est alors identique à l'application réciproque de f.

les propriétés « topologiques » des polyèdres de dimension quelconque, et apparaît déjà chez Euler, qui a démontré le résultat suivant : étant donnée dans l'espace usuel une surface polyédrale, comportant a sommets, b arêtes et c faces, le nombre $a - b + c$ ne dépend pas de la façon dont on a décomposé cette surface en triangles. A partir d'une surface polyédrale décomposée en triangles, on construit un schéma simplicial comme suit : l'ensemble K est l'ensemble des sommets du polyèdre considéré P; toute partie à un élément de K est un simplexe de K; une partie $\{a, b\}$ à deux éléments de K est une arête si le segment de droite joignant le point a au point b est une arête de P; enfin une partie $\{a, b, c\}$ à trois éléments de K est une face si le triangle de sommets a, b, c est une face du polyèdre P. La généralisation à un nombre quelconque de dimensions est facile.]

a) Soient X un ensemble quelconque et $(U_i)_{i\in I}$ un recouvrement de X. On convient de dire qu'une partie S de l'ensemble d'indices I est un simplexe si elle est finie, non vide, et si l'intersection

$$\bigcap_{i\in S} U_i$$

est non vide. Montrer que le couple formé par l'ensemble I et les simplexes qu'on vient de définir est un schéma simplicial (appelé le nerf du recouvrement donné).

b) Soit K un schéma simplicial. On désigne par P(K) l'ensemble des fonctions f définie sur l'ensemble K, à valeurs réelles, et possédant les trois propriétés suivantes : l'ensemble des $x \in K$ tels que $f(x) \neq 0$ est un simplexe de K; on a $f(x) \geqslant 0$ pour tout $x \in K$; enfin, la somme

$$\sum_{x\in K} f(x)$$

des valeurs de f aux divers points de K (somme qui ne comporte qu'un nombre fini de termes non nuls) est égale à 1. Enfin, pour tout $x \in K$, on note U_x l'ensemble des $f \in P(K)$ telles que $f(x) \neq 0$. Montrer que la famille $(U_x)_{x\in K}$ est un recouvrement de l'ensemble P(K), et que le nerf de ce recouvrement est précisément le schéma simplicial donné K.
[Si le schéma simplicial K est fini et comporte n éléments $x_1, \ldots, x_n$, on peut représenter chaque $f \in P(K)$ par le point de $\mathbf{R}^n$ dont les coordonnées sont les n nombres $f(x_1), \ldots, f(x_n)$; on obtient alors une bijection de P(K) sur un polyèdre de l'espace $\mathbf{R}^n$, polyèdre dont la « forme» dépend précisément des relations combinatoires existant entre les divers simplexes du schéma simplicial donné. C'est l'opération fondamentale qui permet de transformer un problème en apparence purement « qualitatif », l'étude de la « forme » des polyèdres, en un problème purement algébrique, l'étude des schémas simpliciaux finis.

1. On appelle **partition** d'un ensemble X toute famille $(A_i)_{i\in I}$ d'ensembles non vides, deux à deux disjoints, ayant l'ensemble X pour réunion. Étant donnée une telle partition, on considère la relation

$$\text{il existe un } i \in I \text{ tel que } x \in A_i \text{ et } y \in A_i$$

entre éléments x, y de X. Montrer que celle-ci est une relation d'équivalence, dont on construira les classes et l'ensemble quotient. Montrer que toute relation d'équivalence sur X peut s'obtenir de la façon précédente.

¶ **2.** Soient R et S des relations d'équivalence sur des ensembles X et Y. Si (x', y') et (x'', y'') sont des éléments de $X \times Y$, on désigne par $T\{(x', y'), (x'', y'')\}$ la conjonction des relations $R\{x', x''\}$ et $S\{y', y''\}$; montrer que T est une relation d'équivalence sur $X \times Y$. Construire le graphe de T en fonction des graphes de R et S. Définir une bijection « canonique » du quotient de $X \times Y$ par T sur l'ensemble produit $(X/R) \times (Y/S)$.
Montrer, en utilisant ces résultats, que le Théorème 3 du § 4 est un cas particulier du Théorème 2.

3. Étant donnés, dans un plan rapporté à deux axes de coordonnées rectangulaires, deux points P′ et P″ de coordonnées (x', y') et (x'', y'') respectivement, on note $R\{P', P''\}$ la relation $x'y' = x''y''$. Montrer que c'est une relation d'équivalence dans le plan, et en construire les classes d'équivalence.
On désigne maintenant par $S\{P', P''\}$ la relation

$$(x'y' = x''y'') \qquad \text{et} \qquad (x'x'' \geqslant 0).$$

Est-ce encore une relation d'équivalence?

4. Soient A un ensemble et B une partie de A. On note $R\{X, Y\}$ la relation $X \cap B = Y \cap B$. Montrer que c'est une relation d'équivalence sur l'ensemble $\mathfrak{P}(A)$ et construire une bijection de l'ensemble $\mathfrak{P}(A)/R$ sur l'ensemble $\mathfrak{P}(B)$.

5. Construire les tables d'addition et de multiplication des entiers modulo 17.

6. Soit E l'espace usuel (considéré comme ensemble de points). On choisit un point O une fois pour toutes, et étant donnés des points P′, P″ on note $R\{P', P''\}$ la relation

les points O, P′ et P″ sont alignés.

Est-ce une relation d'équivalence sur E? On note E* l'ensemble des points $P \in E$ autres que O, de sorte que $E^* = E - \{O\}$; montrer que R est une relation d'équivalence sur E* et déterminer les classes d'équivalence correspondantes (l'ensemble quotient E*/R s'appelle **le plan projectif**).

7. Soit X l'ensemble de toutes les applications de **R** dans **R** (fonctions d'une variable réelle t, définies quel que soit t, et à valeurs réelles). Étant donnés deux éléments x, y de X, on désigne par $R\{x, y\}$ la relation

$$\text{il existe un nombre } c > 0 \text{ tel que l'on ait } \quad x(t) = y(t) \quad \text{pour} \quad |t| < c.$$

Montrer que R est une relation d'équivalence sur X.

8. Soit X l'ensemble de toutes les applications de **R** dans **R**; on choisit dans ce qui suit un entier $n \geqslant 0$. Étant données des fonctions $x, y \in X$, on désigne par $R\{x, y\}$ la relation

$$\lim_{t=0} \frac{x(t) - y(t)}{t^n} = 0$$

(qu'on écrit habituellement sous la forme

$$x(t) - y(t) = o(t^n) \qquad \text{pour} \qquad t \to 0).$$

Montrer que R est une relation d'équivalence sur X.

9. Soient X et Y deux ensembles, R et S des relations d'équivalence sur X et Y, et f une application de X dans Y. On considère le diagramme

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow p & & \downarrow q \\ X/R & & Y/S \end{array}$$

où p et q désignent les applications canoniques de X et Y sur leurs quotients. Montrer que les deux propriétés suivantes sont équivalentes : (i) il existe une application

$$\overline{f} : X/R \to Y/S$$

telle que

$$\overline{f} \circ p = q \circ f;$$

(ii) quels que soient $x', x'' \in X$, la relation

$$x' \equiv x'' \pmod{R} \qquad \text{implique} \qquad f(x') \equiv f(x'') \pmod{S}.$$

Montrer de plus que, si la condition (ii) est vérifiée, il existe une seule application $\overline{f}$ satisfaisant à (i).
Exemple : on prend $X = Y = \mathbf{Z}$, ensemble des entiers rationnels; on prend pour R la relation de congruence modulo r et pour S la relation de congruence modulo s (où r et s sont des entiers non nuls donnés); enfin on prend pour f l'application identique de X dans Y. Dans quel cas le résultat précédent s'applique-t-il?

10. Soit K un schéma simplicial (§ 3, *Exercice* 5); on suppose que toute partie à un élément de K soit un simplexe de K. Étant donnés deux éléments x et y de K, on désigne par $R\{x, y\}$ la relation suivante : il existe un entier $n \geqslant 0$ et des sommets

$$z_0 = x, \quad z_1, \ldots, z_n = y$$

de K tels que l'ensemble $\{z_i, z_{i+1}\}$ soit un simplexe de K pour tout i tel que $0 \leqslant i < n$. Montrer que R est une relation d'équivalence sur l'ensemble K. [Les classes modulo R s'appellent les **composantes connexes** du schéma simplicial K; on dit que K est **connexe s'il** possède une seule composante connexe.]

1. Soient X un ensemble et f une application de X dans l'ensemble $\mathfrak{P}(X)$ des parties de X. On note A l'ensemble des $x \in X$ vérifiant la relation $x \notin f(x)$. Montrer qu'il n'existe aucun $x \in X$ tel que $A = f(x)$. En déduire qu'il n'existe aucune application *surjective* de X dans $\mathfrak{P}(X)$, et que par suite on a

$$x < 2^x$$

pour tout nombre cardinal x (G. Cantor).

2. Soit $(f_n)_{n \in \mathbf{N}}$ une suite d'applications de l'ensemble **N** dans lui-même; on définit une application f de **N** dans **N** en posant

$$f(n) = f_n(n) + 1 \quad \text{pour tout } n \in \mathbf{N}.$$

Montrer qu'il n'existe aucun entier $p \in \mathbf{N}$ tel que $f = f_p$. En déduire que l'ensemble de toutes les applications de **N** dans **N** est non dénombrable (G. Cantor).

3. La réunion d'une infinité dénombrable d'ensembles dénombrables est un ensemble dénombrable (s'inspirer de la méthode utilisée dans l'*Exemple* 1 du n° 5).

4. Soit I l'ensemble des nombres réels compris entre 0 et 1; on représentera chaque $x \in I$ par un développement décimal illimité (pouvant se terminer par une infinité de chiffres 0). Soit $(x_n)_{n \in \mathbf{N}}$ une suite d'éléments de I; on forme un nombre $x \in I$ comme suit : la n^e décimale de x est égale à 1 si la n^e décimale de x_n est différente de 1, et est égale à 2 si la n^e décimale de x_n est égale à 1. Montrer qu'on a $x \neq x_n$ pour tout n. En conclure que l'ensemble I (et *à fortiori* l'ensemble **R** de tous les nombres réels) est non dénombrable (G. Cantor).
Préciser l'analogie entre ce raisonnement et celui de l'*Exercice* **2** ci-dessus.

5. Soient f une bijection d'un ensemble X sur une partie Y_1 d'un ensemble Y, et g une bijection de Y sur une partie X_1 de X; on se propose de montrer que X et Y sont équipotents (Bernstein). Pour cela, on définit des parties A_n de X et B_n de Y en posant

$$A_0 = X - X_1, \qquad B_1 = f(A_0), \qquad A_1 = g(B_1), \qquad B_2 = f(A_1), \qquad A_2 = g(B_2), \ldots$$

puis on définit une application h de X dans Y comme suit : étant donné un $x \in X$, on prend

$$h(x) = f(x) \quad \text{si} \quad x \in \bigcup_{n \in \mathbf{N}} A_n,$$

et dans le cas contraire (de sorte qu'alors $x \in X_1$) on prend

$$h(x) = g^{-1}(x).$$

Montrer que h est une bijection de X sur Y.

6. Soient E un ensemble fini à h éléments, et n un entier naturel. On considère les applications f de E dans **N** telles que la somme des h nombres $f(x)$, $x \in E$, soit au plus égale à n. Montrer que les applications f considérées sont en nombre égal à

$$\binom{n+h}{h}.$$

7. Montrer que, pour entier n, la somme des coefficients du binôme $\binom{n}{p}$ est égale à 2^n.

¶ **8.** Démontrer la relation

$$\binom{n}{0}\cdot\binom{n}{p} + \binom{n}{1}\cdot\binom{n-1}{p-1} + \binom{n}{2}\cdot\binom{n-2}{p-2} + \cdots + \binom{n}{p}\cdot\binom{n-p}{0} = 2^n \cdot \binom{n}{p}.$$

(On cherchera d'abord, dans un ensemble X à n éléments, combien il existe de parties à p éléments qui contiennent un ensemble à k éléments donné d'avance).

¶ **9.** Soient p et n des entiers tels que $1 \leqslant p \leqslant n$, et $S_{n,p}$ le nombre des applications surjectives de l'ensemble $\{1, 2, \ldots, n\}$ dans l'ensemble $\{1, 2, \ldots, p\}$. Montrer qu'on a

$$p^n = S_{n,p} + \binom{p}{1} S_{n,p-1} + \binom{p}{2} \cdot S_{n,p-2} + \cdots + \binom{p}{p-1}.$$

En déduire que

$$S_{n,p} = p^n - \binom{p}{1}\cdot(p-1)^n + \binom{p}{2}\cdot(p-2)^n - \cdots + (-1)^{p-1}\binom{p}{p-1}.$$

Simplifier ce résultat pour $p = 2, 3$.

¶¶¶ **10.** Soient E et F deux ensembles finis, et $x \mapsto A(x)$ une application de E dans l'ensemble des parties de F. Pour qu'il existe une *injection* f de E dans F vérifiant

$$f(x) \in A(x) \qquad \text{pour tout } x \in E,$$

il faut et il suffit qu'on ait

$$\text{Card}\left(\bigcup_{x \in H} A(x)\right) \geqslant \text{Card}\,(H)$$

pour toute partie H de E. (Ce résultat est généralement connu sous le nom de *lemme des mariages*).

11. En utilisant le fait que, dans tout ensemble (fini ou infini) d'entiers naturels, il existe un entier plus petit que tous les autres, démontrer les résultats classiques que voici :

a) Tout entier $n \geqslant 2$ possède au moins un diviseur premier (on rappelle qu'un **nombre premier** est un entier $p \geqslant 2$ n'admettant pas d'autres diviseurs positifs que 1 et p).

1. Trouver tous les groupes à 1, 2 ou 3 éléments.

2. On munit un ensemble à quatre éléments (notés e, a, b, c dans ce qui suit) de la loi de composition commutative donnée par la table de multiplication suivante :

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Montrer que l'on obtient ainsi un groupe commutatif. Trouver tous ses automorphismes. (Ce groupe est connu sous le nom de **Vierergruppe** de Klein). Interpréter géométriquement ce groupe (considérer, dans l'espace, les symétries par rapport aux arêtes d'un trièdre trirectangle).

3. Montrer que le groupe $\mathfrak{S}_4$ des permutations de l'ensemble $\{1, 2, 3, 4\}$ possède un sous groupe invariant isomorphe au Vierergruppe de Klein.

4. On munit l'ensemble $\mathbf{R}$ des nombres réels de la loi de composition

$$(x, y) \to \sqrt[3]{x^3 + y^3};$$

montrer qu'on obtient ainsi un groupe, isomorphe au groupe additif $\mathbf{R}$.

5. Soient $G_1, \ldots, G_n$ des groupes, et $H_1, \ldots, H_n$ des sous-groupes de $G_1, \ldots, G_n$; montrer que $H_1 \times \cdots \times H_n$ est un sous-groupe du groupe produit $G_1 \times \cdots \times G_n$.

6. Soit G un groupe noté multiplicativement. Pour tout $a \in G$, on définit une application s_a de G dans G en posant

$$s_a(x) = ax \quad \text{pour tout } x \in G$$

(**translation à gauche** d'amplitude a dans G; le lecteur comprendra l'origine de cette terminologie en examinant le cas où G est le groupe additif des vecteurs d'origine donnée O de l'espace usuel). Montrer que l'application $a \to s_a$ est un isomorphisme du groupe G sur un groupe de permutations de l'ensemble G.

7. Soient G un groupe cyclique à m éléments et x un générateur de G. Pour que x^k soit un générateur de G, il faut et il suffit que les entiers m et k soient premiers entre eux (utiliser le théorème de Bezout). Dans le cas général, quel est l'ordre du sous-groupe de G engendré par x^k ?

8. Soient m et n des entiers rationnels. Pour qu'il existe un entier r tel que l'on ait

$$r \equiv 0 \pmod{m} \qquad \text{et} \qquad r \equiv 1 \pmod{n},$$

il faut et il suffit que m et n soient premiers entre eux.

q Déduire de là le résultat suivant. Soient G un groupe commutatif, x et y des éléments de G d'ordres m et n premiers entre eux; alors $z = xy$ est d'ordre mn, et le sous-groupe engendré par z contient x et y. (On appelle **ordre** d'un élément x d'un groupe l'ordre, i.e. le nombre d'éléments, du sous-groupe engendré par x; cet ordre est fini si et seulement s'il existe un entier $n \neq 0$ tel que

$$x^n = e;$$

dans ce cas, l'ordre de x est le *plus petit* $n \geqslant 1$ vérifiant cette relation, comme le lecteur le démontrera).

q **9.** Soient G et H des groupes cycliques à m et n éléments. Pour que $G \times H$ soit cyclique il faut et il suffit que m et n soient premiers entre eux. Si x et y sont des générateurs de G et H, le couple (x, y) est alors un générateur de $G \times H$.

q **10.** Tout groupe fini d'ordre premier est cyclique, et admet pour générateur chacun de ses éléments autre que l'élément neutre (utiliser le Théorème 4 du § 7, ou l'*Exercice* 7).

11. Soit A une partie d'un groupe G. On appelle **centralisateur** de A dans G l'ensemble Z(A) des $x \in G$ tels que $xa = ax$ pour tout $a \in A$. Montrer que Z(A) est un sous-groupe de G. Montrer que Z(G) (qu'on appelle le **centre** de G) est un sous-groupe commutatif et invariant de G.

12. Deux éléments x et y d'un groupe G sont dits **conjugués** s'il existe un $s \in G$ tel que

$$y = sxs^{-1}.$$

Montrer que

$$x \text{ et } y \text{ sont conjugués}$$

est une relation d'équivalence sur l'ensemble G. On prend pour G le groupe des rotations autour d'un point donné O dans l'espace, et on choisit une droite D passant par O; montrer que tout élément de G est conjugué d'une rotation autour de D.

13. Étant donnée une partie A d'un groupe G, on note sAs^{-1} (pour $s \in G$ donné) l'ensemble des éléments de G de la forme sxs^{-1}, avec $x \in A$. Montrer que si A est un sous-groupe il en est de même de sAs^{-1} (on dit alors que c'est un sous-groupe **conjugué** de A dans G). On appelle **normalisateur** d'un sous-groupe A de G l'ensemble N(A) des $s \in G$ tels que $sAs^{-1} = A$. Montrer que le centralisateur de A (*Exercice* **11**) est un sous-groupe invariant du normalisateur de A.

14. Soit G un groupe opérant sur un ensemble X.

a) Montrer que la relation

$$\text{il existe un } s \in G \text{ tel que } y = sx$$

est une relation d'équivalence sur l'ensemble X (la classe pour cette relation d'un $x \in X$ s'appelle l'**orbite** de x par G). Montrer que, pour tout $x \in X$, l'ensemble des $s \in G$ tels que $sx = x$ est un sous-groupe H_x de G (appelé **stabilisateur** de x dans G), et que les stabilisateurs des divers points d'une même orbite sont deux à deux conjugués dans G au sens de l'*Exercice* **13**.

b) On considère, pour un $x \in X$ donné, l'application f de G dans X donnée par

$$f(s) = sx;$$

montrer qu'elle est composée de l'application canonique de G sur G/H_x et d'une application de G/H_x dans X; montrer que celle-ci induit une bijection de G/H_x sur l'orbite M de x par G, et que $\text{Card}(G) = \text{Card}(M) \cdot \text{Card}(H_x)$ si G est fini.

c) Décrire les orbites et les stabilisateurs lorsqu'on prend pour X l'espace usuel et pour G le groupe des rotations autour d'un point donné O dans X.

d) On suppose que G est fini, d'ordre une puissance d'un nombre premier p, et que X est fini, le nombre d'éléments de X n'étant pas multiple de p. Montrer qu'alors G admet au moins un **point fixe** dans X (i.e. qu'il existe un $x \in X$ tel que $sx = x$ pour tout $s \in G$).

e) Soit G un **p-groupe** i.e. un groupe fini dont l'ordre est une puissance d'un nombre premier p. En faisant opérer G sur lui-même par les automorphismes intérieurs (cf. *Exemple* **19**), montrer que le centre de G (*Exercice* **11**) n'est pas réduit à l'élément neutre.

15. Soient G un groupe et H un sous-groupe de G; on fait opérer G sur G/H (*Exemple* **20**). Montrer que les éléments de G/H dont le stabilisateur contient H sont les images, par l'application canonique de G dans G/H, des éléments du sous-groupe N(H), normalisateur de H dans G, défini dans l'*Exercice* **13** ci-dessus.

16. Soit H un sous-groupe *invariant* d'un groupe G. Montrer qu'il existe sur l'ensemble G/H une et une seule loi de composition faisant de G/H un groupe et telle que l'application canonique de G dans G/H soit un homomorphisme de groupes (utiliser le Théorème 3 du § 4); le groupe ainsi obtenu s'appelle le **groupe quotient** de G par H. Que se passe-t-il lorsqu'on prend pour G le groupe additif **Z** des entiers rationnels et pour H un sous-groupe de G?

Soit p l'application canonique de G sur G/H; montrer que, pour tout sous-groupe A de G/H, il existe un et un seul sous-groupe K de G contenant H tel que $A = p(K)$, et que l'on a du reste $K = p^{-1}(A)$.

On appelle **sous-groupe dérivé** de G le sous-groupe, noté G' ou D(G), engendré par les éléments de la forme $xyx^{-1}y^{-1}$. Montrer que D(G) est un sous-groupe invariant de G, et que, si H est un sous-groupe invariant de G, pour que le groupe quotient G/H soit commutatif il faut et il suffit que $H \supset D(G)$.

qq 17. Étant donnés des sous-groupes A et B d'un groupe G, on note (A, B) le sous-groupe de G engendré par les éléments $xyx^{-1}y^{-1}$ où $x \in A$ et $y \in B$. On pose

$$D(G) = (G, G), \qquad D^2(G) = D(D(G)), \qquad D^3(G) = D(D^2(G)), \text{ etc...}$$

Montrer que les conditions suivantes sont équivalentes :

a) Il existe un entier r tel que $D^{r+1}(G) = \{e\}$;

b) On peut construire des sous-groupes

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = G$$

de G tels que, pour chaque indice i vérifiant $0 \leqslant i \leqslant s-1$, le sous-groupe H_i soit invariant dans H_{i+1} et le groupe quotient H_{i+1}/H_i soit commutatif (la notion de groupe quotient est définie dans l'*Exercice* précédent);

c) On peut construire des sous-groupes invariants

$$\{e\} = K_0 \subset K \subset \cdots \subset K_s = G$$

de G tels que tous les groupes quotients K_{j+1}/K_j soient commutatifs.

Un groupe G vérifiant ces conditions est dit **résoluble.** Montrer que tout sous-groupe d'un groupe résoluble est résoluble. Soient G un groupe et H un sous-groupe invariant de G; si les groupes H et G/H sont résolubles, il en est de même de G.

q 18. Soit G un p-groupe (*Exercice* 14). Montrer que tout sous-groupe et tout groupe quotient de G est un p-groupe. En utilisant l'*Exercice* 14, *e*), montrer que G contient des sous-groupes invariants

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = G$$

tels que les quotients H_i/H_{i-1} soient isomorphes au groupe additif $\mathbf{Z}/p\mathbf{Z}$ (i.e. soient cycliques d'ordre p) pour $1 \leqslant i \leqslant r$. En particulier, un p-groupe est résoluble.

19. Soit G un groupe cyclique d'ordre fini n.

a) Montrer que pour tout diviseur d de n, les $x \in G$ tels $x^d = e$ sont en nombre d.

b) Soit d un diviseur de n. Pour qu'un $x \in G$ puisse s'écrire sous la forme y^d pour un $y \in G$ convenablement choisi, il faut et il suffit que

$$x^{n/d} = e.$$

qq 20. Soit G un groupe commutatif fini d'ordre n. On suppose que, pour tout diviseur d de n, les $x \in G$ tels que

$$x^d = e$$

soient en nombre d *au plus*; on se propose d'en déduire que G est *cyclique* (résultat indispensable pour l'étude des corps finis : voir § 33, *Exercice* 2). Dans ce qui suit, on désigne par

$$n = p_1^{r_1} \ldots p_h^{r_h}$$

la décomposition de n en facteurs premiers.

a) Prouver que, pour tout i tel que $1 \leqslant i \leqslant h$, il existe un $a_i \in G$ vérifiant

$$a_i^{p_i^{r_i}} = e, \qquad a_i^{p_i^{r_i-1}} \neq e$$

et que a_i est d'ordre

$$q_i = p_i^{r_i}$$

exactement.

b) Montrer, en utilisant le fait que les q_i sont deux à deux premiers entre eux, que l'élément $a_1 \dots a_h$ est d'ordre $q_1 \dots q_h = n$, et en conclure que G est cyclique comme annoncé.

c) Montrer qu'on parviendrait à la même conclusion en faisant l'hypothèse moins forte que voici : pour $1 \leqslant i \leqslant h$, les $x \in G$ tels que

$$x^{p_i} = e$$

sont en nombre p_i au plus.

21. Soit f un homomorphisme d'un groupe fini G dans un groupe H. Montrer que

$$\mathrm{Card}(G) = \mathrm{Card}(\mathrm{Ker}(f)) . \mathrm{Card}(\mathrm{Im}(f)).$$

22. Soient G un groupe commutatif fini et n un entier tel que (*)

$$x^n = e \qquad \text{pour tout } x \in G.$$

a) On suppose $n = rs$ avec r et s premiers entre eux; soit M (resp. N) l'ensemble des $x \in G$ tels que

$$x^r = e \text{ (resp. } x^s = e).$$

Montrer que M et N sont des sous-groupes de G. En écrivant l'identité de Bezout pour r et s, montrer que l'application

$$f : M \times N \to G$$

donnée par $f(x, y) = xy$ est un isomorphisme de groupes.

b) Soit

$$n = p_1^{r_1} \dots p_h^{r_h} = q_1 \dots q_h \qquad \text{où} \qquad q_i = p_i^{r_i}$$

la décomposition de n en facteurs premiers; pour tout i tel que $1 \leqslant i \leqslant h$, soit M_i le sous-groupe des $x \in G$ tels que

$$x^{q_i} = e.$$

Montrer que G est isomorphe au produit direct des groupes $M_1, \dots, M_h$.

c) Soient M un groupe commutatif fini, p un nombre premier et r un entier naturel; on suppose que

$$x^{p^r} = e$$

pour tout $x \in M$; montrer que Card (M) est une puissance de p (observer que, si $M \neq \{e\}$, on peut trouver dans M un sous-groupe M' d'ordre p; l'introduction du groupe quotient M/M', cf. *Exercice* 16, permet alors de raisonner par récurrence sur le nombre d'éléments de M).

d) Démontrer le théorème suivant : *soit* G *un groupe commutatif fini d'ordre*

$$n = p_1^{r_1} \dots p_h^{r_h};$$

alors G *est isomorphe au produit direct de* h *groupes d'ordres* $p_1^{r_1}, \dots, p_h^{r_h}$ (ce résultat, que Gauss avait déjà plus ou moins démontré en 1801, sera complété dans les *Exercices* du § 31 : un groupe commutatif dont l'ordre est une puissance de p est isomorphe à un produit direct de groupes *cycliques* dont les ordres sont des puissances de p. Il en résultera que tout groupe commutatif fini est isomorphe à un produit direct de groupes cycliques. L'étude complète des groupes commutatifs à un nombre fini de générateurs a été faite par Kronecker en 1870; un tel groupe est produit direct d'un groupe commutatif fini et d'un groupe $\mathbf{Z}^n$).

(*) L'énoncé de cet *Exercice* est rédigé en notation multiplicative, mais le lecteur aura intérêt, pour des généralisations ultérieures, à le traduire en notation additive.

¶ **23.** On reprend la question *a*) de l'*Exercice* précédent. Soit A (resp. B) le sous-groupe de G formé des x tels que l'on ait

$$x = y^s \text{ (resp. } x = y^r)$$

pour au moins un $y \in G$. Montrer que A = M et B = N (on prouvera qu'on a les relations

$$\mathrm{Card}(G) = \mathrm{Card}(M) . \mathrm{Card}(N) = \mathrm{Card}(A) . \mathrm{Card}(N) = \mathrm{Card}(B) . \mathrm{Card}(M)$$

et on observera que $A \subset M$, $B \subset N$).

On suppose que $n = \mathrm{Card}(G)$. Montrer que $\mathrm{Card}(M) = r$, $\mathrm{Card}(N) = s$.

24. Soit $s \in \mathfrak{S}_n$ une permutation de l'ensemble $X = \{1, 2, \dots, n\}$ et soit G le sous-groupe de $\mathfrak{S}_n$ formé par les puissances de s.

a) Montrer qu'on peut trouver des parties non vides $I_1, \dots, I_r$ de X vérifiant les conditions suivantes : on a $g(I_k) = I_k$ pour $1 \leqslant k \leqslant r$ et tout $g \in G$; les ensembles I_k sont deux à deux disjoints et leur réunion est X tout entier; pour que $p, q \in X$ appartiennent à un même I_k, il faut et il suffit qu'il existe un $g \in G$ tel que $q = g(p)$. Relation avec l'*Exercice* 14, *a*) ?

b) Montrer que les conditions précédentes caractérisent les ensembles I_k (à ceci près qu'on peut naturellement modifier l'ordre dans lequel on les écrit).

c) Montrer que, pour chaque k, on peut écrire les éléments de I_k sous forme d'une suite $i_0, \dots, i_p$ de telle sorte que l'on ait

$$s(i_0) = i_1, \quad s(i_1) = i_2, \quad \dots, \quad s(i_{p-1}) = i_p, \quad s(i_p) = i_0$$

(*décomposition d'une permutation en cycles*; on appelle cycle pour s toute suite d'entiers $i_0, \dots, i_p$ écrits dans l'ordre naturel, deux à deux distincts, et vérifiant les relations précédentes).

d) Trouver les cycles des permutations suivantes :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 3 & 6 & 5 & 7 & 4 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 9 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix}.$$

(NB. — On utilise ici la notation standard pour représenter une permutation s; celle-ci consiste à écrire sur la seconde ligne les images par s des éléments de la première).

e) Étant donnée une permutation $s \in \mathfrak{S}_n$, soient $n_1, \dots, n_r$ les nombres de termes des divers cycles de s. Montrer que l'ordre de s (i.e. le plus petit entier $q \geqslant 1$ tel que $s^q = e$, ou l'ordre du groupe cyclique engendré par s) est le ppcm des entiers $n_1, \dots, n_r$.

f) On considère la permutation

$$s : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix};$$

calculer l'ordre du sous-groupe de $\mathfrak{S}_{10}$ engendré par s. Calculer la permutation

25. Dans cet Exercice, on utilise la terminologie suivante. Étant donnée une suite

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow \cdots G_n \xrightarrow{f_n} G_{n+1}$$

formée de groupes additifs G_i et d'homomorphismes $f_i : G_i \to G_{i+1}$, on dit que cette suite est **exacte** si, pour chaque entier i tel que $1 \leqslant i < n$, l'image de l'homomorphisme f_i est égale au noyau de l'homomorphisme suivant f_{i+1}. D'autre part, on dit qu'un diagramme, par exemple

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{k} & E \\ \downarrow p & & \downarrow q & & \downarrow r & & \downarrow s & & \downarrow t \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{k'} & E' \end{array} \qquad (1)$$

formé d'ensembles et d'applications de ces ensembles les uns dans les autres, est **commutatif** si, quels que soient les «sommets» X et Y du diagramme, toutes les applications de X dans Y qu'on obtient en composant, de toutes les façons possibles, les applications figurant dans le diagramme donné, sont égales. Dans le cas du diagramme (1), la commutativité se traduirait par la relation $f' \circ p = q \circ f$ et de nombreuses autres relations analogues que le lecteur écrira.

On considère un diagramme *commutatif* (1) dans lequel A, B, ... sont des groupes additifs, et les applications des homomorphismes de groupes. On suppose que les deux lignes horizontales du diagramme sont des suites *exactes* — de sorte qu'on a

$$\mathrm{Im}(f) = \mathrm{Ker}(g), \qquad \mathrm{Im}(f') = \mathrm{Ker}(g'),$$

etc... Établir les résultats suivants (connus sous le nom de **lemme des cinq**) :

a) Si p est surjectif, et si q et s sont injectifs, alors r est injectif.

b) Si q et s sont surjectifs, et si t est injectif, alors r est surjectif.

c) Si p est surjectif, si q et s sont bijectifs, et si t est injectif, alors r est bijectif.

1. Soit K un anneau (qu'on *ne* suppose *pas* commutatif).

a) Montrer que, si deux éléments x et y de K commutent (i.e. si $xy = yx$), on a

$$x^n - y^n = (x - y)\,(x^{n-1} + x^{n-2}y + \cdots + x\,y^{n-2} + y^{n-1})$$

pour tout entier $n \geqslant 1$.

b) On dit qu'un élément x de K est **nilpotent** s'il existe un entier $n \geqslant 1$ tel que

$$x^n = 0.$$

Montrer qu'alors $1 - x$ est inversible.

c) Si deux éléments nilpotents x et y de K commutent, alors $x + y$ est nilpotent (utiliser la formule du binôme pour un exposant assez élevé), ainsi que xy.

d) Soit a un élément de K; on considère l'application u de K dans K donnée par

$$u(x) = ax - xa \quad \text{pour tout } x \in \mathrm{K}.$$

Montrer que, si $a^2 = 0$, on a $u^2(x) = 0$ pour tout $x \in \mathrm{K}$, et que si $a^3 = 0$ on a $u^5(x) = 0$ pour tout $x \in \mathrm{K}$. Montrer d'une manière générale que, si a est nilpotent, il existe un entier q tel que

$$u^q(x) = 0 \quad \text{pour tout } x \in \mathrm{K}.$$

Montrer que l'on a

$$u^p(x) = \sum_{k=0}^{p} (-1)^k \binom{p}{k} a^{p-k} x a^k.$$

e) On dit qu'un élément u de K est **unipotent** si $1 - u$ est nilpotent. Montrer que si $u, v \in \mathrm{K}$ sont unipotents et commutent, alors uv est aussi unipotent. Montrer que tout élément unipotent de K est inversible, et a pour inverse un élément unipotent.

[Pour des exemples d'éléments unipotents et nilpotents d'un anneau, voir l'*Exercice* 10 des §§ 12, 13 et 14 et l'*Exercice* 19 du § 19. En Analyse, la théorie des *développements limités* fournit aussi des exemples d'éléments nilpotents : considérer l'anneau des fonctions $f(t)$ d'une variable réelle t, définie au voisinage de $t = 0$, et, un entier $n \geqslant 1$ étant choisi, passer au quotient — cf. *Exercice* 7, *c*) ci-dessous — par l'idéal des fonctions qui sont $o(t^n)$ quand t tend vers 0; l'anneau quotient a évidemment des éléments nilpotents non nuls — par exemple l'image dans ce quotient de la fonction t].

qq **2.** Soit K un anneau; on suppose que le corps **Q** des nombres rationnels est un sous-anneau de K (ce qui permet de multiplier tout $x \in \mathrm{K}$ par tout nombre rationnel, et en particulier de diviser tout $x \in \mathrm{K}$ par tout entier rationnel non nul).

a) Soit x un élément nilpotent de K (*Exercice* 1); on définit (*)

$$\exp(x) = 1 + \frac{x}{1} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots$$

Montrer, à l'aide de la formule du binôme, que si $x, y \in K$ sont nilpotents et commutent on a

$$\exp(x + y) = \exp(x).\exp(y).$$

b) Soit u un élément unipotent de K (*Exercice* 1); on définit

$$\log(u) = -\frac{1-u}{1} - \frac{(1-u)^2}{2} - \cdots - \frac{(1-u)^n}{n} - \cdots;$$

montrer que si $u, v \in K$ sont unipotents et commutent on a

$$\log(uv) = \log(u) + \log(v).$$

c) Soit x un élément nilpotent de K. Montrer que $\exp(x)$ est unipotent et que

$$\log(\exp(x)) = x.$$

d) Soit u un élément unipotent de K. Montrer que $\log(u)$ est nilpotent et que

$$\exp(\log(u)) = u.$$

e) Pour tout élément nilpotent x de K, on définit

$$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots + (-1)^n \frac{x^{2n}}{(2n)!} + \cdots$$
$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} + \cdots$$

Démontrer que si $x, y \in K$ sont nilpotents et commutent on a

$$\cos(x+y) = \cos(x).\cos(y) - \sin(x).\sin(y)$$
$$\sin(x+y) = \sin(x).\cos(y) + \sin(y).\cos(x).$$

Montrer que

$$\cos^2(x) + \sin^2(x) = 1$$

pour tout élément nilpotent de K; on pose bien entendu $\cos^2(x) = \cos(x).\cos(x)$ et $\sin^2(x) = \sin(x).\sin(x)$.

(*) Ces définitions ont évidemment leur origine dans les développements en série entière des fonctions

$$e^t,\ \log(1+t),\ \cos t \text{ et } \sin t$$

étudiées en Analyse. Il n'y a ici aucun problème de convergence puisque les « séries » sont en réalité des sommes finies. L'*Exercice* consiste à transposer sur un plan purement algébrique la relation existant entre, par exemple, la propriété bien connue

$$e^{x+y} = e^x e^y$$

de la fonction exponentielle usuelle, et la nature du développement en série entière de celle-ci. Il arrive souvent que l'on puisse ainsi trouver des analogues purement algébriques de phénomènes faisant intervenir des considérations d'Analyse, i.e. des passages à la limite.

3. Soit K un anneau; quels que soient $x, y \in K$, on pose

$$[x, y] = xy - yx.$$

Démontrer l'**identité de Jacobi**

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.$$

4. Dans un anneau K, on considère des éléments x, y, h vérifiant les relations

$$[h, x] = 2x, \qquad [h, y] = -2y, \qquad [x, y] = h.$$

a) Établir les formules

$$[h, x^n] = 2n.x^n, \qquad [h, y^n] = -2n.y^n$$

b) Montrer que l'élément

$$4xy + h^2 - 2h$$

de K commute à x, y et h.

c) Montrer que le plus petit sous-anneau de K contenant x, y et h est l'ensemble des éléments qui peuvent s'écrire sous la forme d'une somme d'un nombre fini de termes de la forme

$$a.x^i y^j h^k$$

où i, j, k sont des entiers naturels et a un entier rationnel.

5. Soit p un nombre premier. On désigne par $\mathbf{Z}_p$ l'ensemble des $x \in \mathbf{Q}$ qu'on peut écrire sous la forme d'une fraction dont le dénominateur n'est pas divisible par p.

a) Montrer que $\mathbf{Z}_p$ est un sous-anneau de $\mathbf{Q}$.

b) Pour tout $x \in \mathbf{Q}$ on a soit $x \in \mathbf{Z}_p$ soit $x^{-1} \in \mathbf{Z}_p$.

c) Les seuls sous-anneaux de $\mathbf{Q}$ contenant $\mathbf{Z}_p$ sont $\mathbf{Z}_p$ et $\mathbf{Q}$.

d) Pour tout idéal I de l'anneau $\mathbf{Z}_p$ il existe un entier $n \geqslant 0$ et un seul tel que I soit engendré par p^n (i.e. formé des $p^n u$, $u \in \mathbf{Z}_p$).

e) Pour tout $x \in \mathbf{Q}$ non nul il existe un $n \in \mathbf{Z}$ et un seul tel que

$$x = p^n.u$$

où u est un élément inversible de l'anneau $\mathbf{Z}_p$.

f) Pour tout $x \in \mathbf{Q}$ non nul on pose $v_p(x) = n$ où n est l'entier de la question précédente; en outre on définit (*)

$$v_p(0) = +\infty.$$

(*) On désigne par le symbole $+\infty$ un objet soumis aux règles de calcul que voici, et à celles-ci uniquement (autrement dit, les opérations non définies ci-dessous *n'ont aucun sens*) :

$$n + (+\infty) = +\infty \quad \text{pour tout} \quad n \in \mathbf{Z}; \qquad (+\infty) + (+\infty) = +\infty;$$

enfin on convient que

$$+\infty > n \quad \text{pour tout} \quad n \in \mathbf{Z}; \qquad +\infty \geqslant +\infty.$$

Il s'ensuit par exemple que $\operatorname{Max}(2, +\infty) = +\infty$. Bien entendu on pourrait se passer, pour définir v_p, du symbole $+\infty$: il suffit de ne pas attribuer de sens à $v_p(0)$, et d'énoncer alors les relations à démontrer de telle sorte qu'on n'ait jamais à écrire $v_p(0)$. Cette méthode compliquerait beaucoup la situation.

Montrer que l'on a

$$v_p(xy) = v_p(x) + v_p(y)$$
$$v_p(x + y) \geqslant \text{Min } [v_p(x), v_p(y)]$$

quels que soient $x, y \in \mathbf{Q}$; et que $\mathbf{Z}_p$ est l'ensemble des $x \in \mathbf{Q}$ tels que $v_p(x) \geqslant 0$.

g) Montrer que l'intersection des sous-anneaux $\mathbf{Z}_p$ de $\mathbf{Q}$ associés à tous les nombres premiers p est l'anneau $\mathbf{Z}$ des entiers rationnels.

6. Soient K un corps commutatif et A un sous-anneau de K. On dit que A est un **anneau de valuation** de K si $A \neq K$ et si l'on a

$$x \in A \quad \text{ou} \quad x^{-1} \in A \quad \text{pour tout } x \in K \text{ non nul.}$$

Montrer qu'alors les éléments non inversibles de l'anneau A forment un idéal $\mathfrak{m}$ de A, et que tout idéal de A, distinct de A tout entier, est contenu dans $\mathfrak{m}$ [de sorte que $\mathfrak{m}$ est l'unique idéal maximal de A, dans la terminologie de l'*Exercice* 7, *d*) ci-dessous].

On appelle **valuation discrète** de K toute fonction v définie sur K, dont les valeurs sont des entiers rationnels ou le symbole $+\infty$, et possédant les propriétés suivantes :

$$v(0) = +\infty; \qquad v(x) \in \mathbf{Z} \quad \text{si} \quad x \neq 0;$$
$$v(xy) = v(x) + v(y) \quad \text{quels que soient} \quad x, y \in K;$$
$$v(x + y) \geqslant \text{Min } [v(x), v(y)] \quad \text{quels que soient} \quad x, y \in K.$$

On suppose v non triviale (i.e. que $v(K)$ ne se réduit pas à 0 et $+\infty$). Montrer que l'ensemble A des $x \in K$ tels que $v(x) \geqslant 0$ est un anneau de valuation de K, et que l'idéal maximal $\mathfrak{m}$ de A est l'ensemble des $x \in K$ tels que $v(x) > 0$. On choisit un élément $\pi \in \mathfrak{m}$ tel que $v(\pi)$ soit minimum; montrer que $\mathfrak{m} = A\pi$ et que tout idéal de A est de la forme $A\pi^n$, pour un entier $n \geqslant 0$.

Montrer que les seuls anneaux de valuation du corps $\mathbf{Q}$ sont les anneaux $\mathbf{Z}_p$ de l'*Exercice* précédent. Trouver toutes les valuations discrètes de $\mathbf{Q}$.

7. Soit I un idéal bilatère d'un anneau K; on note

$$x \equiv y \pmod{I}$$

la relation $x - y \in I$ (**congruence** modulo I).

a) Montrer que c'est une relation d'équivalence sur l'ensemble K. Que se passe-t-il si $K = \mathbf{Z}$ et $I = p\mathbf{Z}$?

b) Montrer que les relations

$$x' \equiv y' \pmod{I} \qquad \text{et} \qquad x'' \equiv y'' \pmod{I}$$

impliquent les relations

$$x' + x'' \equiv y' + y'' \pmod{I} \qquad \text{et} \qquad x'x'' \equiv y'y'' \pmod{I}.$$

c) On note K/I l'ensemble quotient de K par la relation d'équivalence considérée, et θ l'application canonique de K sur K/I; montrer qu'il existe sur l'ensemble K/I une et une seule structure d'anneau telle que l'application θ soit un homomorphisme (imiter la construction donnée pour les anneaux $\mathbf{Z}/p\mathbf{Z}$). On dit que K/I est l'**anneau quotient** de K par l'idéal bilatère I.

d) On suppose K commutatif. On dit qu'un idéal I de K est **maximal** si $I \neq K$ et si les seuls idéaux de K contenant I sont I et K. Montrer que, pour que I soit maximal, il faut et il suffit que l'anneau quotient K/I soit un *corps* (on notera qu'un corps ne possède aucun idéal autre que lui-même et $\{0\}$, et réciproquement). Quels sont les idéaux maximaux de l'anneau $\mathbf{Z}$?

e) Un idéal I d'un anneau commutatif K est dit **premier** si $I \neq K$ et si, pour $x, y \in K$, la relation

$$xy \in I \qquad \text{implique} \qquad x \in I \quad \text{ou} \quad y \in I.$$

Montrer que cette condition signifie que l'anneau quotient K/I est *intègre*. Quels sont les idéaux premiers de l'anneau $\mathbf{Z}$?

f) Montrer que tout idéal maximal est premier. [NB — La réciproque n'est vraie que pour des catégories d'anneaux très particulières.]

g) Soient K un corps commutatif et A un sous-anneau de K; on suppose que tout $x \in K$ puisse se mettre sous la forme u/v avec $u, v \in A$ et $v \neq 0$ (ceci signifie que K est le corps des fractions de A, cf. § 29). Soit (*) $\mathfrak{p}$ un idéal premier de A; on note $A_{\mathfrak{p}}$ (**anneau local de** $\mathfrak{p}$) l'ensemble des éléments de K qui peuvent se mettre sous la forme

$$u/v \qquad \text{avec} \qquad u, v \in A \quad \text{et} \quad v \notin \mathfrak{p}.$$

Montrer que $A_{\mathfrak{p}}$ est un sous-anneau de K possédant un seul idéal maximal, et que si l'on associe à chaque idéal $I \neq A_{\mathfrak{p}}$ de l'anneau $A_{\mathfrak{p}}$ son intersection $I \cap A$ avec A, on définit une *bijection* de l'ensemble des idéaux $I \neq A_{\mathfrak{p}}$ de $A_{\mathfrak{p}}$ sur l'ensemble des idéaux de A contenus dans $\mathfrak{p}$.

8. Soient A et B deux anneaux. Montrer qu'on obtient un anneau (**composé direct** de A et B) en munissant l'ensemble $A \times B$ des lois de compositions données par les formules

$$(x', y') + (x'', y'') = (x' + x'', y' + y''), \qquad (x', y') \cdot (x'', y'') = (x'x'', y'y'').$$

Le composé direct $A \times B$ peut-il être un anneau d'intégrité?

9. Soient m et n des entiers rationnels premiers entre eux.

a) Montrer que, quels que soient $a, b \in \mathbf{Z}$, il existe $x \in \mathbf{Z}$ tel que

$$x \equiv a \pmod{m} \qquad \text{et} \qquad x \equiv b \pmod{n}$$

et que la classe de x modulo mn est entièrement déterminée par la classe de a modulo m et celle de b modulo n. Exemple : trouver toutes les solutions du système de congruences

$$x \equiv 4 \pmod{7}, \qquad x \equiv 9 \pmod{11}.$$

b) On considère les anneaux $A = \mathbf{Z}/m\mathbf{Z}$, $B = \mathbf{Z}/n\mathbf{Z}$ et $C = \mathbf{Z}/mn\mathbf{Z}$. A l'aide de la question précédente, construire un isomorphisme du composé direct $A \times B$ (*Exercice* 8) sur l'anneau C. (On pourra utiliser le Théorème 3 du § 4).

c) Soient $q_1, \ldots, q_h$ des entiers deux à deux premiers entre eux. Montrer par récurrence sur h que, quels que soient $a_1, \ldots, a_h \in \mathbf{Z}$, il existe un $x \in \mathbf{Z}$ qui vérifie les h relations

$$x \equiv a_i \pmod{q_i} \quad (1 \leqslant i \leqslant h).$$

(Ce résultat est connu sous le nom de **théorème chinois**, attendu que les Chinois en utilisaient des cas particuliers pour choisir les dates d'événements liés aux périodes de certains phénomènes astronomiques ou autres.)

(*) La tradition pour désigner des idéaux est d'utiliser des lettres gothiques; on ne s'y est pas conformé dans le texte du § 8 pour éviter de troubler les débutants.

d) Soit

$$n = p_1^{r_1} \dots p_h^{r_h}$$

la décomposition d'un entier n en facteurs premiers. Montrer que l'anneau $\mathbf{Z}/n\mathbf{Z}$ est isomorphe au composé direct des h anneaux $\mathbf{Z}/q_i\mathbf{Z}$, où l'on pose

$$q_i = p_i^{r_i} \quad (1 \leqslant i \leqslant h).$$

e) Soient $q_1, \dots, q_h$ des entiers rationnels quelconques; pour qu'on puisse résoudre le système de congruences

$$x \equiv a_i \pmod{q_i} \quad 1 \leqslant i \leqslant h,$$

il faut et il suffit qu'on ait

$$a_i \equiv a_j \pmod{d_{ij}} \qquad \text{pour} \qquad 1 \leqslant i < j \leqslant h,$$

où d_{ij} désigne le pgcd de q_i et q_j.

10. Soient I et J des idéaux d'un anneau commutatif K. On note $I + J$ (**somme** des idéaux I et J) l'ensemble des éléments de K qui peuvent se mettre sous la forme $x + y$ avec $x \in I$ et $y \in J$, et IJ (**produit** des deux idéaux I et J) l'ensemble des $z \in K$ possédant la propriété suivante : il existe un entier $n \geqslant 1$, des éléments $x_1, \dots, x_n$ de I, et des éléments $y_1, \dots, y_n$ de J, tels que $z = x_1 y_1 + \dots + x_n y_n$.

a) Montrer que $I + J$ est le plus petit idéal de K contenant I et J. Montrer que IJ est aussi un idéal de K, contenu dans $I \cap J$. Établir les relations

$$I + J = J + I, \qquad I + (I' + I'') = (I + I') + I'',$$
$$IJ = JI, \qquad I(I'I'') = (II')I'', \qquad I(J' + J'') = IJ' + IJ''$$

où I, I', etc... désignent des idéaux de K. Interprétation de $I + J$ et de IJ lorsque I et J sont principaux?

b) On dit que deux idéaux I et J de K sont **étrangers** lorsque $I + J = K$. Quelle est la signification de cette propriété lorsque $K = \mathbf{Z}$? Montrer que, si I et J sont étrangers, on a $I \cap J = IJ$.

c) Pour que deux idéaux I et J de K soient étrangers, il faut et il suffit que, quels que soient $a, b \in K$, il existe $x \in K$ tel que l'on ait

$$x \equiv a \pmod{I} \qquad \text{et} \qquad x \equiv b \pmod{J}.$$

En déduire que l'anneau quotient K/IJ (*Exercice* 7) est isomorphe au composé direct (*Exercice* 8) des anneaux K/I et K/J.

d) Soient $I, J_1, \dots, J_r$ des idéaux de K; on suppose I et J_k étrangers pour $1 \leqslant k \leqslant r$. Montrer que I est étranger au produit $J_1 \dots J_r$.

e) Soient $J_1, \dots, J_r$ des idéaux deux à deux étrangers. Montrer que

$$J_1 \dots J_r = J_1 \cap \dots \cap J_r.$$

f) Soient $J_1, \dots, J_r$ des idéaux deux à deux étrangers. Montrer que, quels que soient $a_1, \dots, a_r \in K$ on peut trouver un $x \in K$ tel que l'on ait

$$x \equiv a_k \pmod{J_k} \quad \text{pour } 1 \leqslant k \leqslant r.$$

g) Deux idéaux maximaux (*Exercice* 7, (*d*)) de K sont étrangers dès qu'ils sont distincts.

¶ **11.** Soient $I_1, \dots, I_r$ des idéaux d'un anneau commutatif K. Si un idéal **premier** (*Exercice* 7, (*e*)) de K contient le produit $I_1 \dots I_r$ il contient l'un au moins des idéaux $I_1, \dots, I_r$.
Soit I un idéal non premier de K. Montrer qu'il existe des idéaux J' et J'' de K possédant les propriétés suivantes : J' et J'' contiennent I et sont distincts de I, et I contient l'idéal produit J'J''.

12. Étant donné un idéal I d'un anneau commutatif K, on appelle **radical** de I l'ensemble des $x \in K$ tels que l'on ait

$$x^n \in I$$

pour un entier $n \geqslant 1$ au moins. Dans cet *Exercice*, on désigne le radical d'un idéal I par la notation

$$\sqrt{I}$$

(laquelle est aussi mauvaise que possible comme le montreront les formules qui vont suivre...).

a) Montrer que le radical d'un idéal I est encore un idéal. Que se passe-t-il si $I = \{0\}$? Quel est le radical d'un idéal premier (*Exercice* 7, (*e*)) de K?

b) Démontrer les formules suivantes, où I et J désignent deux idéaux quelconques de l'anneau K :

$$\sqrt{I.J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$
$$\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$$
$$\sqrt{\sqrt{I}} = \sqrt{I}.$$

c) Déterminer complètement le radical d'un idéal de l'anneau **Z** des entiers rationnels.

13. On dit qu'un idéal I d'un anneau commutatif K est **primaire** si $I \neq K$ et si, quels que soient les éléments x, y de K tels que l'on ait

$$xy \in I, \qquad x \notin I,$$

il existe un entier $n \geqslant 1$ tel que

$$y^n \in I.$$

Montrer que le radical d'un idéal primaire est un idéal premier.

¶ Pour que I (supposé distinct de K) soit primaire, il faut et il suffit que, dans l'anneau quotient K/I, tout diviseur de zéro soit nilpotent.
Quels sont les idéaux primaires de l'anneau **Z**?

14. Soit $\mathfrak{m}$ un idéal maximal d'un anneau commutatif K. Montrer que les puissances

$$\mathfrak{m}^n = \mathfrak{m} \dots \mathfrak{m} \ (n \text{ facteurs})$$

de $\mathfrak{m}$ sont des idéaux primaires, ayant $\mathfrak{m}$ pour radical.

15. Soient $\mathfrak{m}$ un idéal maximal d'un anneau commutatif K, et $\mathfrak{a}$ un idéal de K contenu dans $\mathfrak{m}$. On suppose que chaque élément de $\mathfrak{m}$ possède une puissance dans $\mathfrak{a}$. Montrer que $\mathfrak{a}$ est primaire et que son radical est $\mathfrak{m}$.

16. Pour qu'un élément d'un anneau commutatif K soit inversible, il faut et il suffit qu'il n'appartienne à aucun autre idéal de K que K lui-même.

On admet le **théorème de Krull** que voici : étant donné un anneau commutatif (*) K, tout idéal de K, distinct de K, est contenu dans au moins un idéal maximal de K [on rappelle, *Exercice* 7, *d*), qu'un idéal I de K est dit maximal si $I \neq K$ et si les seuls idéaux de K contenant I sont I et K].
Montrer que, pour qu'un élément de K soit inversible, il faut et il suffit qu'il n'appartienne à aucun idéal maximal de K.

17. Soit I l'intersection de tous les idéaux maximaux d'un anneau commutatif K. Montrer qu'un élément a de K appartient à I si et seulement si $1 + ax$ est inversible pour tout $x \in K$ (utiliser l'*Exercice* précédent).
[Ce résultat (Jacobson) s'étend aux anneaux non commutatifs : dans un tel anneau, l'intersection des idéaux à gauche maximaux est identique à l'intersection des idéaux à droite maximaux; et les éléments a de cette intersection sont caractérisés par le fait que $1 + xay$ est inversible quels que soient $x, y \in K$. Les démonstrations de ces résultats sont parfaitement élémentaires.]

18. On désigne par $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$ pour p premier. On munit l'ensemble $\mathbf{F}_{11} \times \mathbf{F}_{11}$ des deux lois de composition données par les formules suivantes :

$$(u, v) + (x, y) = (u + x, v + y)$$
$$(u, v) \cdot (x, y) = (ux + 7vy, uy + vx)$$

(où 7 désigne naturellement la classe modulo 11 de l'entier naturel 7). Montrer qu'on obtient de cette façon un corps commutatif à 121 éléments.

19. Montrer que, si p est un nombre premier, le coefficient du binôme $\binom{n}{p}$ est multiple de p pour $1 \leqslant n \leqslant p - 1$. En déduire que, si p est un nombre premier impair, on a

$$(1 + p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$$

pour tout entier $k \geqslant 0$ (raisonner par récurrence).

(*) Le théorème de Krull s'étend en fait à tout anneau K, commutatif ou non, de la façon suivante. Dans un tel anneau, un idéal à gauche (resp. à droite, bilatère) I est dit **maximal** si $I \neq K$ et si les seuls idéaux à gauche (resp. à droite, bilatère) de K contenant I sont I et K. Ceci dit, tout idéal à gauche (resp. à droite, bilatère) de K, autre que K lui-même, est contenu dans au moins un idéal à gauche (resp. à droite, bilatère) maximal de K.
Lorsque $K = \mathbf{Z}$, le théorème de Krull signifie que tout entier $n \geqslant 2$ possède au moins un diviseur premier. Le théorème de Krull peut donc être considéré comme une extension de ce résultat à *tous les anneaux sans exception*; à ce titre, et en dépit de la simplicité de son énoncé, c'est l'un des résultats les plus utiles de toute l'Algèbre, et on l'a même utilisé (Gelfand) depuis une vingtaine d'années pour démontrer des théorèmes difficiles d'Analyse, en l'appliquant à des anneaux dont les éléments sont des fonctions d'une ou plusieurs variables réelles vérifiant certaines conditions.
La démonstration générale du théorème de Krull est facile pourvu qu'on connaisse suffisamment la théorie des Ensembles et des nombres transfinis (c'est même l'un des points précis où l'on voit la « grande » théorie des nombres transfinis servir à démontrer des résultats « concrets » très peu évidents). On verra au § 18 une démonstration élémentaire du théorème de Krull pour les anneaux *noethériens* (mais ceux qu'on étudie en Analyse le sont rarement). L'idée de la démonstration générale est que, si l'anneau K ne contenait aucun idéal maximal, on pourrait construire dans K une chaîne croissante infinie, et même « transfinie », d'idéaux (autrement dit, attacher à chaque cardinal α un idéal I_α de telle sorte que, pour $\alpha < \beta$, l'idéal I_α soit *strictement* contenu dans I_β — la construction est évidemment facile pour les α finis, et toute la difficulté est de prolonger la récurrence au delà des entiers naturels), ce qui serait en contradiction avec le fait qu'il n'existe pas d'injection de l'ensemble (sic) de tous les cardinaux dans un ensemble donné (en espèce, l'ensemble des idéaux de K), pour la raison que les cardinaux ne forment pas un ensemble...

20. On pose $r = \sqrt[3]{2}$. Montrer que l'ensemble des nombres de la forme

$$a + br + cr^2,$$

où a, b, c sont des nombres *rationnels* arbitraires, est un sous-corps du corps **R** des nombres réels.
(Cet *Exercice* sera aussi, pour le lecteur débutant, une occasion de *démontrer* que 2 n'est pas le cube d'un nombre rationnel).

§ 9

1 *a*) Montrer que tout nombre complexe $d \neq 0$ possède exactement deux racines carrées dans le corps **C** (on cherchera leur module et leur argument en fonction de ceux de d).

b) En déduire que toute équation du second degré

$$az^2 + bz + c = 0$$

à coefficients a, b, c complexes, possède au moins une racine dans **C**, et en possède deux si

$$b^2 - 4ac \neq 0.$$

c) Résoudre dans **C** les équations

$$z^2 + (5 - 2i)z + 5 - 5i = 0$$
$$z^2 + (1 - 2i)z - 2i = 0$$
$$z^4 - 30z^2 + 289 = 0$$

2. Trouver les parties réelle et imaginaire des nombres complexes suivants :

$$\frac{(1+2i)^2 - (1-i)^3}{(3+2i)^3 - (2+i)^2}; \qquad \frac{(1+i)^9}{(1-i)^7}; \qquad \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)^3; \qquad \sqrt[4]{2 - i\sqrt{12}};$$
$$(az^2 + bz)(bz^2 + az) \quad \text{où} \quad z = -\frac{1}{2} + \frac{i\sqrt{3}}{2}.$$

3. Calculer le module et l'argument des nombres complexes suivants :

$$-1 + i; \qquad -1 - i\sqrt{3}; \qquad 2 + \sqrt{3} + i; \qquad \left(\frac{1 + i\sqrt{3}}{1 - i}\right)^{20};$$
$$(1 + \cos\theta + i.\sin\theta)^n.$$

4. Trouver toutes les solutions complexes des équations suivantes (on utilisera la formule de Moivre) :

$$z^3 + 1 = 0; \qquad z^5 = 1; \qquad z^6 + 27 = 0; \qquad z^8 = \frac{1+i}{\sqrt{3} - i}.$$

5. *a*) Calculer

$$\cos 5t, \qquad \cos 8t, \qquad \sin 6t, \qquad \sin 9t, \qquad \operatorname{tg} 6t$$

en fonction des lignes trigonométriques de l'angle t.

b) Calculer

$$\sin^3 t, \qquad \sin^4 t, \qquad \cos^5 t, \qquad \cos^6 t$$

à l'aide des lignes trigonométriques des multiples entiers de l'angle t.

6. Soient u et v deux nombres complexes. Montrer qu'on a la relation

$$|u + v|^2 + |u - v|^2 = 2(|u|^2 + |v|^2);$$

interprétation géométrique?

7. Démontrer les relations suivantes :

$$2^{2n}\cos^{2n}t = 2\cos 2nt + 2\binom{2n}{1}\cos(2n-2)t + \cdots + 2\binom{2n}{n-1}\cos 2t + \binom{2n}{n},$$
$$2^{2n}\cos^{2n+1}t = \cos(2n+1)t + \binom{2n+1}{1}\cos(2n-1)t + \cdots + \binom{2n+1}{n}\cos t,$$
$$2^{2n}\sin^{2n}t = 2\sum_{k=0}^{k=n-1}(-1)^{n+k}\binom{k}{2n}\cos 2(n-k)t + \binom{n}{2n},$$
$$2^{2n}\sin^{2n+1}t = \sum_{k=0}^{k=n}(-1)^{n+k}\binom{k}{2n+1}\sin(2n-2k+1)t,$$
$$\binom{1}{n} - \frac{1}{3}\binom{3}{n} + \frac{1}{9}\binom{5}{n} - \frac{1}{27}\binom{7}{n} + \cdots = \frac{2^n}{3^{\frac{n-1}{2}}}\sin\frac{n\pi}{6},$$
$$\cos\frac{\pi}{11} + \cos\frac{3\pi}{11} + \cos\frac{5\pi}{11} + \cos\frac{7\pi}{11} + \cos\frac{9\pi}{11} = \frac{1}{2}.$$

8. Soit **U** l'ensemble des nombres complexes z tels que $|z| = 1$; montrer que c'est un sous-groupe du groupe multiplicatif **C*** des nombres complexes non nuls. Construire un isomorphisme entre les groupes $\mathbf{U} \times \mathbf{R}_+^*$ et **C***. Montrer que **U** est isomorphe au groupe des rotations autour d'un point dans le plan.

9. On appelle **demi-plan de Poincaré** l'ensemble P des nombres complexes z tels que

$$\operatorname{Im}(z) > 0,$$

et **disque unité** l'ensemble D des nombres complexes z tels que

$$|z| < 1.$$

Montrer que

$$z \mapsto \frac{z - i}{z + i}$$

est une application bijective de P sur D (on désignera par A et B les points d'affixes i et $-i$,

par M le point d'affixe z, et on interprétera le module et l'argument de $z - i/z + i$ à l'aide des éléments du triangle MAB).

10. On désigne par a, b, c, d des nombres réels tels que $ad - bc = 1$.

a) Montrer que, pour tout nombre complexe z non réel, on a

$$\mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \frac{\mathrm{Im}\,(z)}{|cz+d|^2}.$$

b) Soit P le demi-plan de Poincaré (*Exercice* 9). Montrer qu'il existe une permutation s de P telle que

$$s(z) = \frac{az+b}{cz+d}$$

pour tout $z \in P$, et que les permutations de P obtenues de cette façon (en faisant varier a, b, c, d) forment un groupe de transformations de l'ensemble P.

c) Montrer que l'application s de P dans P définie dans la question *b*) peut se décomposer en un produit de transformations appartenant à l'un des trois types suivants :

$$z \mapsto z + u \quad (u \text{ réel}); \qquad z \mapsto vz \quad (v \text{ réel strictement positif}); \qquad z \mapsto -1/z.$$

Interpréter géométriquement ces applications.

d) Quelle figure décrit $s(z)$ lorsque le point d'affixe z décrit soit un cercle contenu dans P, soit un demi-cercle contenu dans P et centré sur l'axe réel, soit une demi-droite contenue dans P, limitée à l'axe réel, et orthogonale à celui-ci?

11. Soit G l'ensemble des permutations du demi-plan de Poincaré P données par

$$s(z) = \frac{az+b}{cz+d}$$

où a, b, c, d sont des *entiers rationnels* tels que $ad - bc = 1$ (cf. *Exercice* 10).

a) Montrer que G est un groupe de permutations de P (on l'appelle le **groupe modulaire arithmétique**) qui contient les applications u et v données par

$$u(z) = z + 1, \qquad v(z) = -1/z.$$

On se propose dans ce qui suit de démontrer que G *est engendré par u et v*. On note G_0 le sous-groupe de G engendré par u et v.

b) Pour tout $z \in P$, soit I_z l'ensemble des nombres $y > 0$ possédant la propriété suivante : il existe un $s \in G_0$ tel que $y = \mathrm{Im}(s(z))$. En utilisant la question *a*) de l'*Exercice* 10, montrer que pour tout $m > 0$ les éléments de I_z tels que $y > m$ sont en nombre fini.

c) Montrer que pour tout $z \in P$ il existe un $s \in G_0$ tel que le nombre $z_0 = s(z)$ vérifie

$$\mathrm{Im}\,(t(z_0)) \leqslant \mathrm{Im}\,(z_0) \qquad \text{pour tout } t \in G_0.$$

Montrer qu'on a les relations

$$|z_0| \geqslant 1, \qquad -\frac{1}{2} \leqslant \mathrm{Re}\,(z_0) \leqslant +\frac{1}{2}.$$

d) Soit D la partie de P définie par les inégalités précédentes (de sorte que l'orbite par G_0 de tout élément de P rencontre D). Soit z un point « intérieur » à D, i.e. tel que

$$|z| < 1, \qquad -\frac{1}{2} < \mathrm{Re}\,(z) < +\frac{1}{2};$$

montrer que le seul $s \in G$ tel que $s(z) \in D$ est l'élément neutre. Pour tout $t \in G$, montrer qu'il existe un $t' \in G_0$ tel que $t'(t(z)) \in D$. En déduire que $t \in G_0$, et donc que $G = G_0$ comme annoncé.

e) Montrer que, pour tout $s \in G$, l'ensemble $s(D)$ est un triangle (sic) limité par des demi-cercles orthogonaux à l'axe réel (certains de ces demi-cercles pouvant dégénérer en demi-droites), que le demi-plan P est réunion de $s(D)$, $s \in G$, et que deux domaines $s(D)$, $t(D)$ distincts (i.e. pour lesquels $s \neq t$) ne peuvent avoir en commun qu'un de leurs côtés. Tracer à la règle et au compas, *avec la plus grande exactitude possible*, la figure formée par ce « pavage » du demi-plan P — on partira de D, puis on construira les ensembles $u^n(D)$, puis les ensembles $vu^n(D)$, puis les ensembles $u^n vu^n(D)$, etc... [La figure obtenue, excessivement compliquée si on en poursuit la construction suffisamment loin, a servi de point de départ aux travaux de F. Klein et de H. Poincaré sur la théorie des « fonctions automorphes ».]

12. Soit K le sous-anneau de $\mathbf{C}$ formé des nombres de la forme $x + iy$ avec $x, y \in \mathbf{Z}$ (on les appelle des **entiers de Gauss**).

a) Soient $u, v \in K$ avec $v \neq 0$; on pose

$$u/v = x + iy$$

avec x, y rationnels, puis on détermine des entiers rationnels m et n tels que

$$|x - m| \leqslant \frac{1}{2}, \qquad |y - n| \leqslant \frac{1}{2};$$

enfin, on pose

$$q = m + in, \qquad r = u - qv.$$

Montrer qu'on a $N(r) < N(v)$ ou, si l'on préfère, $|r| < |v|$.

b) Déduire de là que tout idéal de l'anneau K est principal (imiter les raisonnements utilisés dans l'Exemple 8 du § 7).

13. Pour tout nombre premier p, on désigne par $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$. Trouver les $d \in \mathbf{F}_p$ tels que l'anneau $\mathbf{F}_p[\sqrt{d}]$ soit un corps pour

$$p = 2, 3, 5, 7, 11.$$

Voyez-vous un rapport avec l'*Exercice* 11 du § 8?

14. Soient K un corps commutatif, u et v des éléments de K qui ne sont pas des carrés dans K. Pour qu'il existe un isomorphisme f du corps $K[\sqrt{u}]$ sur le corps $K[\sqrt{v}]$ tel que l'on ait $f(x) = x$ pour tout $x \in K$, il faut et il suffit que u/v soit le carré d'un élément de K.
Application : en considérant les corps construits dans l'*Exercice* **13**, montrer que deux quelconques de ces corps sont isomorphes dès qu'ils ont le même nombre d'éléments.
(Ce résultat est un cas particulier du fait que deux corps finis ayant le même nombre d'éléments sont toujours isomorphes).

15. Soient K un corps commutatif et d un élément de K, qui n'est pas un carré dans K. On suppose que l'élément $2 = 1 + 1$ de K n'est pas nul (ce qui exclut par exemple le corps

$\mathbf{Z}/n\mathbf{Z}$). Montrer que, pour qu'un élément x du corps $K[\sqrt{d}]$, n'appartenant pas à K, soit un carré dans $K[\sqrt{d}]$, il faut et il suffit que $N(x)$ soit un carré dans K.
Application : on prend $K = \mathbf{Z}/11\mathbf{Z}$ et $d = 7$. Trouver tous les éléments $u + v\sqrt{d}$ $(u, v \in K)$ qui sont des carrés dans $K[\sqrt{d}]$ (on pourra rassembler dans un tableau à double entrée les valeurs de $u^2 - 7v^2$ lorsque u et v décrivent K). Déduire de là des exemples de corps finis à 14 641 éléments... et vérifiez que tous les corps que vous aurez obtenus sont deux à deux isomorphes.

16. Soit K un corps commutatif dans lequel -1 est un carré. Soit d un élément de K qui n'est pas un carré dans K. Montrer que $\sqrt{d}$ n'est pas un carré dans $K[\sqrt{d}]$.
Application : construire un corps à 17^4 éléments.

17. Soit K un corps commutatif fini à q éléments; on suppose q impair.

a) Montrer que les éléments 1 et -1 de K sont distincts (observer que dans le cas contraire on aurait $2x = qx = 0$ pour tout $x \in K$, et noter que 2 et q sont premiers entre eux).

b) Montrer que $x \to x^2$ est un homomorphisme du groupe multiplicatif K^* des éléments non nuls de K dans lui-même, dont le noyau se compose de 1 et -1. En déduire que les carrés non nuls dans K forment un sous-groupe H à

$$\frac{q-1}{2}$$

éléments de K^* (utiliser l'*Exercice* 21 du § 7), et que le groupe quotient K^*/H a deux éléments.

c) Montrer que, pour tout $x \in K^*$, on a

$$x^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si } x \text{ est un carré} \\ -1 & \text{si } x \text{ n'est pas un carré.} \end{cases}$$

d) Soit p un nombre premier impair. On dit qu'un entier n non divisible par p est un **reste quadratique** modulo p s'il existe un $x \in \mathbf{Z}$ tel que

$$x^2 \equiv n \pmod{p}.$$

Montrer que les restes quadratiques se répartissent en $\frac{p-1}{2}$ classes modulo p, et que pour tout entier n non divisible par p on a

$$n^{\frac{p-1}{2}} \equiv \begin{cases} +1 \pmod{p} & \text{si } n \text{ est reste quadratique mod } p \\ -1 \pmod{p} & \text{si } n \text{ n'est pas reste quadratique mod } p. \end{cases}$$

(critère d'Euler). Montrer que -1 est reste quadratique mod p si et seulement si

$$p \equiv 1 \pmod{4}.$$

[L'étude, au XVIII^e siècle et au début du XIX^e, de la théorie des restes quadratiques a été l'un des points de départ de toute l'Arithmétique et de toute l'Algèbre « modernes ». Le résultat le plus célèbre dans cette voie est la **loi de réciprocité quadratique** conjecturée par Euler, et démontrée par Gauss à l'âge de 19 ans — un beau début. Pour l'énoncer, on doit d'abord introduire le **symbole de Legendre**

$$\left(\frac{n}{p}\right) = \begin{cases} +1 & \text{si } n \text{ est reste quadratique mod } p \\ -1 & \text{sinon.} \end{cases}$$

La loi de réciprocité est alors que, si p et q sont des nombres premiers impairs et distincts, on a

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Pour une démonstration de ce résultat, et plus généralement pour tout ce qui concerne l'Arithmétique élémentaire, voir par exemple G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford, 1938).
Après Gauss, les mathématiciens se sont efforcés d'étendre la loi de réciprocité quadratique aux anneaux d'entiers algébriques (§ 34, *Exercice* 48), ce qui est incomparablement plus difficile que le cas des entiers rationnels traité par Gauss. Les résultats complets, qui constituent la « théorie du corps de classe », après avoir été conjecturés par Hilbert, ont été obtenus vers 1920-1925 par Takagi, Artin et Hasse; la théorie a été grandement améliorée une dizaine d'années plus tard par Chevalley, et est encore actuellement l'objet de recherches très actives.]

1. Montrer que, dans $\mathbf{R}^3$, le vecteur $x = (6, 2, -7)$ est combinaison linéaire des vecteurs

$$a = (2, 1, -3), \qquad b = (3, 2, -5), \qquad c = (1, -1, 1);$$

les vecteurs a, b, c forment-ils une base de $\mathbf{R}^3$?
Mêmes questions dans $\mathbf{R}^4$ pour les vecteurs $x = (7, 14, -1, 2)$ et

$$a = (1, 2, -1, -2), \qquad b = (2, 3, 0, -1), \qquad c = (1, 2, 1, 3), \qquad d = (1, 3, -1, 0).$$

Montrer que les vecteurs a, b, c forment une base de $\mathbf{R}^3$, et trouver les coordonnées du vecteur x par rapport à cette base, dans chacun des cas suivants :

$a = (1, 1, 1)$, $b = (1, 1, 2)$, $c = (1, 2, 3)$, $x = (6, 9, 14)$,
$a = (2, 1, -3)$, $b = (3, 2, -5)$, $c = (1, -1, 1)$, $x = (6, 2, -7)$.

Même question dans $\mathbf{R}^4$ pour les vecteurs

$$a = (1, 2, -1, -2), \qquad b = (2, 3, 0, -1), \qquad c = (1, 2, 1, 4), \qquad d = (1, 3, -1, 0)$$

et

$$x = (7, 14, -1, 2).$$

2. Pour que deux vecteurs (a, b) et (c, d) de $\mathbf{R}^2$ forment une base de $\mathbf{R}^2$ il faut et il suffit que

$$ad - bc \neq 0.$$

3. Soit M l'espace vectoriel réel formé des vecteurs d'origine donnée O dans l'espace usuel. Soit $M' \subset M$ l'ensemble des vecteurs d'origine O dont l'extrémité est située sur un plan donné dans l'espace. M' est-il un sous-espace vectoriel de M?

4. Soit K un anneau. On considère dans K^n l'ensemble M des vecteurs $(x_1, \ldots, x_n)$ vérifiant la relation

$$x_1 + \cdots + x_n = 0;$$

est-ce un sous-module de K^n? Même question en remplaçant la relation précédente par

$$x_1 + \cdots + x_n = 1.$$

5. On considère dans $\mathbf{C}^n$ des vecteurs

$$x_k = (\xi_{k1}, \ldots, \xi_{kn}) \quad (1 \leqslant k \leqslant r)$$

dont les composantes vérifient les inégalités

$$|\xi_{kk}| > \sum_{\substack{1 \leqslant j \leqslant r \\ j \neq k}} |\xi_{kj}| \quad (1 \leqslant k \leqslant r);$$

montrer que ces vecteurs sont linéairement indépendants sur $\mathbf{C}$.

6. Quel est le sous-espace vectoriel de $\mathbf{R}^4$ engendré par les vecteurs

$$a = (1, -1, 1, 0), \qquad b = (1, 1, 0, 1), \qquad c = (2, 0, 1, 1)?$$

7. Traduire les notions de module de type fini, de module libre de type fini, et de base d'un tel module, dans le langage des groupes commutatifs écrits multiplicativement (un tel groupe étant regardé comme un $\mathbf{Z}$-module conformément à l'*Exemple* 5 du § 10).

¶ 8. Soit V un espace vectoriel de dimension finie sur le corps $\mathbf{Q}$ des nombres rationnels. On dit qu'une partie M de V est un **réseau** dans V si M est un sous-groupe de type fini du groupe additif V, et si M contient un système de générateurs de V.

a) Soit M un sous-groupe de type fini de V. Pour que M soit un réseau de V, il faut et il suffit que, pour tout $x \in V$, il existe un entier rationnel $r \neq 0$ tel que $rx \in M$. Montrer qu'alors l'ensemble des $r \in \mathbf{Z}$ tels que $rx \in M$ est un idéal (non nul) de l'anneau $\mathbf{Z}$.

b) Soient p un nombre premier et M un réseau de V. On note M_p l'ensemble des $x \in V$ vérifiant la condition suivante : il existe un entier r non multiple de p tel que $rx \in M$. Montrer que M_p est un sous-module de V regardé comme module sur l'anneau $\mathbf{Z}_p$ du § 8, *Exercice* 5.

c) Montrer que, si M est un réseau de V, on a

$$M = \bigcap_{p \text{ premier}} M_p.$$

d) Soient M et N deux réseaux de V. Montrer que les nombres premiers p tels que

$$M_p \neq N_p$$

sont en nombre fini.
(On trouvera des propriétés supplémentaires des réseaux dans l'*Exercice* 1 du § 18.)

9. Soit A un sous-anneau d'un corps commutatif K; on suppose que tout élément de K puisse se mettre sous la forme uv^{-1} avec $u, v \in A$, $v \neq 0$, et que K soit un A-module de type fini. Montrer qu'alors $A = K$.

¶ 10. Soient K un anneau, M un K-module à gauche et M' un sous-module de M.

a) Montrer que

$$x - y \in M'$$

est une relation d'équivalence sur l'ensemble M [on l'appelle la **congruence modulo M'** et on l'écrit souvent sous la forme

$$x \equiv y \pmod{M'};$$

voir § 7, n° 6].

b) On note M/M′ l'ensemble quotient de M par cette relation d'équivalence, et p l'application canonique de M sur M/M′. Montrer qu'il existe sur M/M′ une et une seule structure de K-module à gauche telle que l'on ait

$$p(x+y) = p(x) + p(y), \qquad p(\lambda x) = \lambda p(x)$$

quels que soient $x, y \in M$ et $\lambda \in K$ (utiliser le § 4, n° 3; voir aussi § 7, *Exercice* 16 et § 8, *Exercice* 7 pour des constructions analogues). On dit que M/M′, muni de cette structure de module, est le **module quotient** de M par le sous-module M′.

c) A chaque sous-module de M/M′ on associe son image réciproque par l'application p; montrer qu'on obtient ainsi une bijection de l'ensemble des sous-modules de M/M′ sur l'ensemble des sous-modules de M contenant M′.

d) Montrer que si M est de type fini il en est de même de M/M′ quel que soit M′. Si M est libre de type fini, en est-il de même de M/M′?

11. Soit M un module à gauche sur un anneau K.

a) Pour tout $x \in M$, on appelle **annulateur** de x l'ensemble des $\lambda \in K$ tels que $\lambda x = 0$. Montrer que c'est un idéal à gauche de K.

b) On suppose K intègre. Montrer que les $x \in M$ dont l'annulateur ne se réduit pas à 0 forment un sous-module T de M (on dit que T est le **sous-module de torsion** de M, et que M est **sans torsion** si $T = \{0\}$).

c) Montrer que le module quotient M/T (*Exercice* 10) est sans torsion.

d) Calculer T lorsque $K = \mathbf{Z}$ et $M = \mathbf{Z}^2/L$, où L est le sous-groupe de $\mathbf{Z}^2$ engendré par le vecteur (4,6).

12. On dit qu'un module à gauche M sur un anneau K est **de torsion** si, pour tout $x \in M$, il existe un scalaire *non nul* $\lambda \in K$ tel que $\lambda x = 0$.

a) Soient M un K-module à gauche et M′ un sous-module de K. On suppose que M′ et M/M′ sont des modules de torsion. Montrer que, si K est intègre, M est alors un module de torsion.

b) On suppose $K = \mathbf{Z}$. Montrer que, pour qu'un K-module de type fini soit de torsion, il faut et il suffit qu'il soit fini.

13. Soit M un module sur un anneau K. Une partie B de M (finie ou non) est appelée un **ensemble de générateurs** de M si le seul sous-module de M contenant B est M tout entier ou, ce qui revient au même, si chaque élément de M est combinaison linéaire d'éléments de B en nombre fini.
On suppose M de type fini. Montrer que l'on peut alors extraire de B un ensemble *fini* de générateurs de M (choisir dans M un système fini de générateurs x_i, et exprimer chaque x_i à l'aide d'éléments de B).

14. Soient K un corps commutatif et A un sous-anneau de K; on suppose que K est le corps des fractions de A i.e. que, pour tout $x \in K$, il existe des éléments u et v de A tels que $v \neq 0$ et

$$x = uv^{-1}.$$

Dans ce qui suit on regarde K comme un A-module, et on dit qu'une partie I de K est un **idéal fractionnaire** de l'anneau A si elle ne se réduit pas à 0, si c'est un sous-module de K, et si, enfin, il existe un élément $d \neq 0$ de K tel que l'on ait

$$dI \subset A$$

(où dI désigne l'ensemble des produits dx avec $x \in I$).

a) Pour qu'une partie J de K soit un idéal fractionnaire il faut et il suffit qu'il existe un idéal non nul J de l'anneau A et un $d \in A$ non nul tels que

$$I = d^{-1}J.$$

b) Soient I et J des idéaux fractionnaires, et soit $(I : J)$ l'ensemble des $x \in K$ tels que $xJ \subset I$; montrer que c'est un idéal fractionnaire (souvent appelé le **transporteur** de J dans I).

c) Soient I et J deux idéaux fractionnaires; on note $I + J$ l'ensemble des sommes $x + y$ avec $x \in I$ et $y \in J$, et IJ l'ensemble des éléments de K qui peuvent s'écrire comme somme (finie) de produits xy avec $x \in I$ et $y \in J$ (cf. § 8, *Exercice* 10 pour le cas où $I, J \subset A$). Montrer que $I + J$, IJ et $I \cap J$ sont des idéaux fractionnaires de l'anneau A. Étendre les formules du § 8, *Exercice* 10, (*a*).

d) On dit qu'un idéal fractionnaire I est **inversible** s'il existe un idéal fractionnaire J tel que

$$I.J = A;$$

montrer qu'alors J est unique, et donné par la relation

$$J = (A : I)$$

(on dit alors que J est l'**inverse** de I, et on le note I^{-1}). Autrement dit, pour que I soit inversible, il faut et il suffit que

$$(A : I).I = A.$$

e) Pour qu'un idéal I soit inversible il faut et il suffit qu'il existe des éléments $x_k \in I$ et $y_k \in (A : I)$ en nombre fini, tels que

$$1 = \sum x_k y_k;$$

les x_k forment alors un système de générateurs du A-module I (un idéal fractionnaire inversible est donc de type fini — on convient de dire qu'un idéal fractionnaire est **de type fini** s'il est de type fini comme A-module).

f) On dit que A est un **anneau de Dedekind** si tout idéal fractionnaire de A est inversible. Montrer que l'ensemble des idéaux fractionnaires de A, muni de la loi de composition $(I, J) \to I.J$, est alors un groupe.

g) Si A est un anneau de Dedekind, tout idéal *premier* non nul de A est *maximal*.
[Les anneaux de Dedekind se sont introduits d'abord dans la théorie des nombres algébriques — cf. § 34, *Exercice* — et on n'en a donné une définition générale et abstraite que beaucoup plus tard. La principale propriété de ces anneaux, est que *dans un anneau de Dedekind tout idéal s'écrit, d'une façon unique à des permutations près, sous la forme d'un produit d'idéaux premiers*; cf. § 18, *Exercice* 7. Inversement, cette propriété caractérise les anneaux de Dedekind. Une troisième caractérisation, beaucoup plus maniable dans la pratique, sera donnée au § 34, *Exercice* 50. Notons enfin que les anneaux de Dedekind interviennent non seulement dans la théorie des nombres algébriques, mais aussi dans l'étude des courbes algébriques et en beaucoup d'autres questions de Géométrie algébrique; c'est ce qui justifie l'introduction et l'étude des anneaux de Dedekind « abstraits ».
Comme exemple aussi élémentaire que possible d'un anneau de Dedekind, mis à part bien entendu l'anneau $\mathbf{Z}$, citons les anneaux $\mathbf{Z}[\sqrt{d}]$ où

$$d \equiv 2 \text{ ou } 3 \pmod 4.]$$

15. Soient K un anneau et X un ensemble. On désigne par

$$K^{(X)}$$

l'ensemble de toutes les applications

$$u : X \to K$$

telles que les $x \in X$ vérifiant $u(x) \neq 0$ soient en nombre *fini*. Montrer que $K^{(X)}$ est un sous-module du K-module à gauche K^X (formé de toutes les applications de K dans X). Pour chaque $x \in X$, on considère l'élément e_x de $K^{(X)}$ défini par

$$e_x(y) = \begin{cases} 1 & \text{si } y = x \\ 0 & \text{si } y \neq x; \end{cases}$$

montrer que la famille $(e_x)_{x \in X}$ est une *base* du K-module à gauche $K^{(X)}$, et que les composantes par rapport à cette base de tout $u \in K^{(X)}$ sont les scalaires $u(x)$, autrement dit qu'on a

$$u = \sum_{x \in X} u(x) \cdot e_x$$

pour tout $u \in K^{(X)}$.
Soit f une application de X dans un K-module à gauche M; montrer qu'il existe un et un seul homomorphisme

$$\bar{f} : K^{(X)} \to M$$

tel que l'on ait

$$\bar{f}(e_x) = f(x) \quad \text{pour tout } x \in X.$$

(Les éléments du module $K^{(X)}$ sont généralement appelés les **combinaisons linéaires formelles** d'éléments de X à coefficients dans K, et on identifie le plus souvent l'élément de base e_x de ce module à l'élément $x \in X$ correspondant).

16. Soient K et L deux anneaux commutatifs, et $j_1, \ldots, j_n$ des homomorphismes deux à deux distincts de K dans L. Montrer que $j_1, \ldots, j_n$ sont linéairement indépendants dans le L-module de toutes les applications de K dans L (théorème de Dedekind) (écrire une relation linéaire entre $j_1, \ldots, j_n$ et utiliser l'identité $j_k(xy) = j_k(x) j_k(y)$ pour se ramener au cas de $n - 1$ homomorphismes).

17. Soient G un groupe commutatif, K un anneau commutatif, et $\rho_1, \ldots, \rho_n$ des homomorphismes deux à deux distincts de G dans le groupe multiplicatif K^*. Montrer que $\rho_1, \ldots, \rho_n$ sont linéairement indépendants sur K, i.e. que si $\alpha_1, \ldots, \alpha_n \in K$ vérifient

$$\alpha_1 \rho_1(s) + \ldots + \alpha_n \rho_n(s) = 0 \quad \text{pour tout } s \in G,$$

alors $\alpha_1 = \ldots = \alpha_n = 0$ (raisonner par récurrence sur n).
Exemple : soient $c_1, \ldots, c_n$ des nombres complexes deux à deux distincts; on considère les fonctions

$$e^{c_1 t}, \ldots, e^{c_n t}$$

pour $t \in \mathbf{R}$; montrer qu'elles sont linéairement indépendantes sur $\mathbf{C}$.

1. On considère les matrices (à coefficients dans $\mathbf{C}$)

$$I_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad I_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$
$$I_4 = \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix}, \quad I_5 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad I_6 = \begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix}.$$

Établir les quinze relations suivantes :

$$\begin{array}{lll} [I_1, I_3] = 2I_3, & [I_1, I_4] = 2I_4, & [I_2, I_3] = 2I_4 \\ [I_1, I_5] = -2I_5, & [I_1, I_6] = -2I_6, & [I_2, I_5] = -2I_6 \\ [I_3, I_5] = I_1, & [I_3, I_6] = I_2, & [I_4, I_5] = I_2 \\ [I_2, I_4] = -2I_3, & [I_2, I_6] = 2I_5, & [I_4, I_6] = -I_1 \\ [I_1, I_2] = 0, & [I_3, I_4] = 0, & [I_5, I_6] = 0, \end{array}$$

où l'on pose d'une façon générale

$$[X, Y] = XY - YX.$$

Trouver toutes les matrices carrées d'ordre 2 qui commutent aux six matrices $I_1, \ldots, I_6$.

2. Établir les formules de l'*Exercice* précédent pour les matrices

$$I_1 = 2\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad I_2 = 2\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad I_3 = \begin{pmatrix} 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$
$$I_4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad I_5 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad I_6 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

3. Trouver toutes les matrices carrées d'ordre 3 commutant à la matrice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 1 & 2 \end{pmatrix}$$

(on prendra comme anneau de base soit le corps $\mathbf{C}$, soit un corps commutatif quelconque, soit un anneau arbitraire — au choix...).

4. Soit K un anneau commutatif. Montrer que l'application de $M_2(K)$ dans $M_4(K)$ qui transforme chaque matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ en la matrice

$$\begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{pmatrix}$$

est un isomorphisme de l'anneau $M_2(K)$ sur un sous-anneau de $M_4(K)$. Interprétation en termes de modules?

5. Calculer le produit des trois matrices

$$\begin{pmatrix} 0 & 2 & -1 \\ -2 & -1 & 2 \\ 3 & -2 & -1 \end{pmatrix}, \quad \begin{pmatrix} 70 & 34 & -107 \\ 52 & 26 & -68 \\ 101 & 50 & -140 \end{pmatrix}, \quad \begin{pmatrix} 27 & -18 & 10 \\ -46 & 31 & -17 \\ 3 & 2 & 1 \end{pmatrix}.$$

Effectuer le même calcul en prenant pour anneau de base l'anneau $\mathbf{Z}/7\mathbf{Z}$ des entiers modulo 7.

6. Calculer le cube de la matrice carrée d'ordre n

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

7. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice carrée d'ordre 2 à coefficients dans un anneau commutatif quelconque. Montrer qu'on a la relation

$$A^2 - (a+d)A + (ad - bc)\mathbf{1}_2 = 0.$$

8. Étant donnée une matrice carrée

$$A = (\alpha_{ij})_{1 \leqslant i,j \leqslant n}$$

à coefficients dans un anneau *commutatif* K, on appelle **trace** de A le scalaire

$$\mathrm{Tr}(A) = \alpha_{11} + \alpha_{22} + \dots + \alpha_{nn},$$

somme des éléments diagonaux de A. Montrer qu'on a

$$\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B), \qquad \mathrm{Tr}(AB) = \mathrm{Tr}(BA)$$

quelles que soient les matrices A et B.
On suppose $K = \mathbf{C}$. Déduire de ce qui précède qu'il est impossible de trouver des matrices carrées X et Y d'ordre n telles que

$$XY - YX = \mathbf{1}_n.$$

9. Soient K un anneau commutatif et d un élément de K. Montrer que les matrices

$$\begin{pmatrix} x & dy \\ y & x \end{pmatrix}$$

(où x et y sont des éléments arbitraires de K) forment un sous-anneau L de $M_2(K)$, et que L est isomorphe à l'anneau $K[\sqrt{d}]$ du § 9. Cas où $K = \mathbf{R}$, $d = -1$?

10. On dit qu'une matrice carrée X d'ordre n à coefficients dans un anneau K est **nilpotente** s'il existe un entier $r \geqslant 1$ tel que $X^r = 0$, et **unipotente** si la matrice $1_n - X$ est nilpotente. On suppose $K = \mathbf{C}$ dans ce qui suit. Étant données une matrice carrée nilpotente N, et une matrice carrée unipotente U, on pose (cf. § 8, *Exercice* 2)

$$\exp(N) = 1 + \frac{N}{1!} + \frac{N^2}{2!} + \dots \frac{N^k}{k!} + \dots,$$

$$\log(U) = -\frac{1-U}{1} - \frac{(1-U)^2}{2} - \dots - \frac{(1-U)^k}{k} - \dots.$$

On prend

$$N = \begin{pmatrix} 0 & a & c \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix};$$

vérifier que N est nilpotente, que U est unipotente, et qu'on a les relations

$$\exp(\log(U)) = U, \qquad \log(\exp(N)) = N$$

[on calculera effectivement les matrices $\exp(\log(U))$ et $\log(\exp(N))$, sans utiliser le résultat général de l'*Exercice* 2 du § 8].

11. Pour tout nombre complexe t, on pose

$$U(t) = \begin{pmatrix} 1 & t & 2t + 2t^2 & 3t + \frac{17}{2}t^2 + 4t^3 \\ 0 & 1 & 4t & 5t + 12t^3 + 3t^4 \\ 0 & 0 & 1 & 6t \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

montrer qu'on a

$$U(s)\,U(t) = U(s+t)$$

quels que soient $s, t \in \mathbf{C}$ et que $U(t) = \exp(tN)$ où N est une matrice nilpotente qu'on calculera.

q 12. Soit z un nombre algébrique, i.e. (§ 11, *Exemple* 11) un nombre complexe racine d'une équation algébrique à coefficients rationnels non tous nuls.

a) Montrer qu'il existe un entier $n \geqslant 1$ et des nombres rationnels $a_0, \dots, a_{n-1}$ tels que l'on ait une relation de la forme

$$z^n = a_0 + a_1 z + \dots + a_{n-1} z^{n-1}.$$

b) Soit K le sous-anneau de $\mathbf{C}$ engendré par $\mathbf{Q}$ et z; montrer que K, considéré comme espace vectoriel sur $\mathbf{Q}$, est engendré par les éléments $1, z, \dots, z^{n-1}$.

c) On suppose n minimum dans ce qui précède. Montrer qu'alors $1, z, \dots, z^{n-1}$ forment une base de K regardé comme espace vectoriel sur $\mathbf{Q}$.

d) Soit f l'application de K dans K donnée par

$$f(u) = zu \qquad \text{pour tout } u \in K.$$

Montrer que c'est un endomorphisme de K regardé comme espace vectoriel sur $\mathbf{Q}$. Calculer la matrice de f par rapport à la base de K définie dans la question *c*).

¶ **13.** Soient L et M deux modules à gauche sur un anneau K ; on suppose donnés un sous-module L′ de L et un homomorphisme f de L dans M. Prouver que les deux conditions suivantes sont équivalentes : *a*) L′ est contenu dans le noyau de f, i.e. on a $f(x) = 0$ pour tout $x \in L'$; *b*) f est composé de l'application canonique de L sur le module quotient L/L′ (§ 10, *Exercice* 10) et d'un homomorphisme de L/L′ dans M.

14. Soient K un anneau, L, M et N trois K-modules à gauche, f un homomorphisme de L dans M, et p un homomorphisme de L dans N ; on suppose p surjectif. Montrer que les deux conditions suivantes sont équivalentes : *a*) on a $\mathrm{Ker}(f) \supset \mathrm{Ker}(p)$; *b*) f est composé de p et d'un homomorphisme de N dans M.

15. Soient L l'espace vectoriel réel formé des vecteurs d'origine donnée O dans l'espace usuel, et L′ le sous-espace vectoriel de L formé des vecteurs portés par une droite donnée (resp. un plan donné) passant par O. Pour tout $x \in L$, on note $f(x)$ le vecteur projection orthogonale de x sur L′. Montrer que l'application f de L dans L′ est linéaire. Quel est son noyau ?

¶¶ **16.** Soit K un anneau. On dit qu'un K-module à gauche M est **simple** ou **irréductible** s'il n'est pas réduit à 0 et si les seuls sous-modules de M sont $\{0\}$ et M tout entier.

a) Pour que M, supposé non nul, soit simple, il faut et il suffit que, quels que soient $a, b \in M$ avec $a \neq 0$, il existe un $\lambda \in K$ tel que $b = \lambda a$. En déduire que, si K est un *corps*, tout K-module simple est isomorphe à K.

b) Soit M un K-module simple. On choisit dans M un élément $a \neq 0$, et on note I l'ensemble des $\lambda \in K$ tels que $\lambda a = 0$. Montrer que I est un idéal à gauche *maximal* de K (§ 8, *Exercice* 7). Montrer que l'application $\lambda \to \lambda a$ de K dans M est composée de l'application canonique de K sur K/I, et d'un isomorphisme du K-module à gauche K/I sur M.
Montrer inversement que, pour tout idéal à gauche maximal I de K, le K-module à gauche K/I est simple.

c) Soient L et M deux K-modules à gauche simples, et f un homomorphisme de L dans M. Montrer que, si f n'est pas nul, c'est un isomorphisme de L sur M (lemme de Schur). (On examinera le noyau et l'image de f.)

d) Soit L un K-module à gauche simple. Montrer que l'anneau des endomorphismes de L est un *corps* (en général non commutatif).

1. L'anneau de base étant **R**, trouver les inverses des matrices suivantes (*) :

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}; \quad \begin{pmatrix} 2 & 5 & 7 \\ 6 & 3 & 4 \\ 5 & -2 & -3 \end{pmatrix}; \quad \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}; \quad \begin{pmatrix} 2 & 2 & 3 \\ 1 & -1 & 0 \\ -1 & 2 & 1 \end{pmatrix}.$$

2. Calculer l'inverse de la matrice

$$\begin{pmatrix} 1 & a & a^2 & \dots & a^n \\ 0 & 1 & a & \dots & a^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

3. Soit N une matrice carrée nilpotente (i.e. dont une puissance est nulle) à coefficients dans un anneau. Montrer que la matrice $1 - N$ est inversible, et que

$$(1 - N)^{-1} = 1 + N + N^2 + \cdots$$

Application : calculer l'inverse de la matrice

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

4. Calculer l'inverse de la matrice

$$\begin{pmatrix} 1 + a_1 & 1 & 1 & \dots & 1 \\ 1 & 1 + a_2 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1 + a_n \end{pmatrix}$$

(*) Le lecteur plus avancé pourra aussi résoudre cet *Exercice* en utilisant les formules de Cramer.

¶ 5. Soit $\omega = \cos(2\pi/n) + i.\sin(2\pi/n)$. Montrer que l'inverse de la matrice

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)^2} \end{pmatrix}$$

s'obtient en remplaçant ω par ω^{-1} dans cette matrice, et en divisant par n la matrice ainsi obtenue.

6. Trouver une matrice carrée X d'ordre 3 telle que (*)

$$\begin{pmatrix} 2 & -3 & 1 \\ 4 & -5 & 2 \\ 5 & -7 & 3 \end{pmatrix} X \begin{pmatrix} 9 & 7 & 6 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & -2 \\ 18 & 12 & 9 \\ 23 & 15 & 11 \end{pmatrix}.$$

7. Montrer que les vecteurs

$$(1, 2, 1), \quad (2, 3, 3), \quad (3, 7, 1)$$

forment une base de $\mathbf{R}^3$, ainsi que les vecteurs

$$(3, 1, 4), \quad (5, 2, 3), \quad (1, 1, -6),$$

et calculer la matrice de passage de la première base à la seconde.
Même problème, dans $\mathbf{R}^4$, pour les vecteurs

$$(1, 1, 1, 1), \quad (1, 2, 1, 1), \quad (1, 1, 2, 1), \quad (1, 3, 2, 3)$$

et

$$(1, 0, 3, 3), \quad (-2, -3, -5, -4), \quad (2, 2, 5, 4), \quad (-2, -3, -4, -4).$$

8. Les matrices

$$\begin{pmatrix} x+y & 4y \\ -y & x-y \end{pmatrix}$$

où x et y sont des nombres rationnels arbitraires, forment un sous-corps de l'anneau $M_2(\mathbf{Q})$.

9. Les matrices

$$\begin{pmatrix} x & y & z \\ 2z & x & y \\ 2y & 2z & x \end{pmatrix}$$

où x, y, z sont des nombres rationnels, forment un sous-corps de $M_3(\mathbf{Q})$.

¶ 10. Soient K un anneau commutatif, p et q deux éléments donnés de K. On considère l'anneau

$$L = K[\sqrt{p}]$$

et l'ensemble $M \subset M_2(L)$ des matrices de la forme

$$z = \begin{pmatrix} x & qy \\ \bar{y} & \bar{x} \end{pmatrix} \quad \text{avec } x, y \in L$$

(pour les notations, voir le § 9).

(*) Voir note page précédente.

a) Montrer que M est un sous-anneau de $M_2(L)$.

b) Pour toute matrice

(1) $$z = \begin{pmatrix} x & qy \\ \bar{y} & \bar{x} \end{pmatrix}$$

de M on pose

$$z^* = \begin{pmatrix} \bar{x} & -qy \\ -\bar{y} & x \end{pmatrix};$$

montrer qu'on a $(z_1 z_2)^* = z_2^* z_1^*$ quels que soient $z_1, z_2 \in M$.

c) Pour la matrice (1), calculer le produit $z^* z$, et montrer que z est un élément inversible de l'anneau M si et seulement si

$$N(z) = \bar{x}x - q\bar{y}y$$

est un élément inversible de l'anneau L.

d) On suppose que K soit un corps commutatif et que p ne soit pas un carré dans K. Montrer que les assertions suivantes sont équivalentes : (*i*) l'anneau M est un corps (*ii*) il n'existe aucun couple d'éléments x, y de K tels que

$$q = x^2 - py^2.$$

e) On suppose $K = \mathbf{R}$. Montrer que M est un corps si et seulement si l'on a

$$p < 0, \qquad q < 0.$$

Montrer que le corps M ainsi obtenu est isomorphe à celui qu'on obtiendrait en prenant $p = q = -1$ (et qu'on appelle le **corps des quaternions**, premier exemple, historiquement, d'un corps non commutatif).

f) On suppose $K = \mathbf{Q}$ et p et q entiers. Montrer que, pour que M soit un corps, il faut et il suffit que l'équation

$$px^2 + qy^2 = z^2$$

ne possède aucune solution (x, y, z) *entière* autre que $(0, 0, 0)$. Montrer que cette condition est satisfaite dans les cas suivants par exemple :

$$p = 5, \quad q \equiv 2 \pmod 5; \qquad p = 5, \quad q \equiv 3 \pmod 5;$$
$$p = 11, \quad q \equiv 2, 6, 7, 8 \text{ ou } 10 \pmod{11}.$$

¶ 11. Montrer que les matrices de la forme

$$\begin{pmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix},$$

où x, y, z, t sont des nombres réels arbitraires, forment un sous-corps de $M_4(\mathbf{R})$, et que ce sous-corps est isomorphe au corps des quaternions défini dans l'*Exercice* précédent. Montrer que, considéré comme espace vectoriel réel, ce corps admet une base formée de quatre éléments e, i, j, k vérifiant les formules suivantes :

$$e^2 = e, \qquad i^2 = j^2 = k^2 = -e,$$
$$ei = ie = i, \qquad ej = je = j, \qquad ek = ke = k,$$
$$ij = -ji = k; \qquad jk = -kj = i; \qquad ki = -ik = j.$$

Obtiendrait-on encore un corps si l'on autorisait les variables x, y, z, t à prendre des valeurs complexes quelconques ?

12. L'anneau de base étant $\mathbf{C}$, calculer l'inverse de la matrice

$$\begin{pmatrix} 1 & 1+i & -i \\ 0 & i & 1-2i \\ 1 & 1 & i \end{pmatrix}.$$

13. On considère la matrice $U(t)$ de l'*Exercice* 11 des §§ 12, 13, 14. Calculer son inverse en effectuant le moins possible de calculs.

14. Soit K un anneau commutatif. Montrer que les matrices de la forme

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

$(x, y, z \in K)$ forment un sous-groupe de $GL(3, K)$. Déterminer le centre de ce sous-groupe.

¶ **15.** Soient K un anneau commutatif et n un entier. Montrer que les matrices carrées d'ordre n, à coefficients dans K, et de la forme

$$\begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \dots & * \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

(où les signes * désignent des éléments arbitraires de K) forment un sous-groupe de $GL(n, K)$, dont on déterminera le centre.

16. Soit K un corps. On désigne par H le sous-groupe de $GL(n, K)$ formé des matrices diagonales de $GL(n, K)$. Trouver le normalisateur (§ 7, *Exercice* 13) de H dans $GL(n, K)$.

¶ **17.** Pour que des éléments (a, b) et (c, d) de $\mathbf{Z}^2$ forment une base de $\mathbf{Z}^2$ il faut et il suffit que $ad - bc = +1$ ou -1.

18. Soient K un anneau commutatif et I un idéal de K. Soit H l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, à coefficients dans K, qui vérifient

$$ad - bc = 1, \qquad a \equiv d \equiv 1 \pmod{I}, \qquad b \equiv c \equiv 0 \pmod{I}.$$

Montrer que H est un sous-groupe invariant de $GL(2, K)$.

¶¶ **19.** Soit K un corps fini à q éléments. Calculer le nombre d'éléments du groupe $GL(n, K)$.

¶ **20.** Pour tout entier $n \geqslant 1$, on note G_n l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec

$$a, b, c, d \in \mathbf{Z}, \qquad ad - bc = n,$$

et on pose $G_1 = G$.

a) Montrer que G est un sous-groupe de $GL(2, \mathbf{Z})$. En est-il de même de G_n pour $n \geqslant 2$?

b) Montrer que si $X \in G_n$ on a $UXV \in G_n$ quelles que soient $U, V \in G$.

c) Montrer que, pour toute $X \in G_n$, il existe $U, V \in G$ telles que UXV soit diagonale.

¶ **17.** Soit $u = (a, b)$ un élément du $\mathbf{Z}$-module $\mathbf{Z}^2$.

a) Montrer que s'il existe une base de $\mathbf{Z}^2$ qui contient u, alors il existe une forme linéaire f sur le module considéré telle que $f(u) = 1$. En déduire qu'alors les entiers a et b sont premiers entre eux.

b) On suppose inversement a et b premiers entre eux. Montrer qu'il existe une forme linéaire f sur $\mathbf{Z}^2$ telle que $f(u) = 1$. Montrer qu'il existe un vecteur v tel que $\mathrm{Ker}(f)$ soit l'ensemble des multiples entiers de v. Prouver que les vecteurs u et v forment une base de $\mathbf{Z}^2$.

c) On prend $u = (6, 35)$; trouver un vecteur v tel que u et v forment une base de $\mathbf{Z}^2$.

18. Soient L et M deux modules à gauche sur un anneau quelconque K, et

$$f : M \to L$$

un homomorphisme *surjectif*. On suppose L libre de type fini. Montrer qu'il existe un homomorphisme

$$g : L \to M$$

tel que

$$f \circ g = id.$$

¶ **19.** Soient L et M deux modules à gauche sur un anneau, L' et M' des sous-modules de L et M, et u un homomorphisme de L dans M tel que $u(L') \subset M'$. On note p et q les applications canoniques de L sur L/L' et de M sur M/M' (§§ 10, 11, *Exercice* 10). Montrer qu'il existe un et un seul homomorphisme

$$\bar{u} : L/L' \to M/M'$$

tel que l'on ait

$$q \circ u = \bar{u} \circ p$$

(on dit que $\bar{u}$ est l'homomorphisme déduit de u par passage aux quotients). A quelles conditions $\bar{u}$ est-il injectif, ou surjectif, ou bijectif?

20. Soit k un corps commutatif. Dans le groupe $SL(2, k)$ des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients dans k et telles que $ad - bc = 1$, on considère les matrices

$$x_+(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \qquad x_-(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

où $t \in k$. Désignant par α l'un des deux symboles $+$ ou $-$, et par $-\alpha$ le symbole opposé, on définit pour $t \neq 0$ les matrices

$$w_\alpha(t) = x_\alpha(t) x_{-\alpha}(-1/t) x_\alpha(t), \qquad h_\alpha(t) = w_\alpha(t) w_\alpha(1)^{-1}.$$

a) Calculer ces matrices, et montrer que les matrices $x_+(t)$ et $x_-(t)$ engendrent $SL(2, k)$.

b) Établir les relations suivantes :

(R 1) $\quad x_\alpha(t+u) = x_\alpha(t)\, x_\alpha(u)$ $\quad$ pour $\quad t, u \in k$;

(R 2) $\quad w_\alpha(t)\, x_\alpha(u)\, w_\alpha(t)^{-1} = x_{-\alpha}(-u/t^2)$ $\quad$ pour $\quad t, u \in k,\ t \neq 0$;

(R 3) $\quad h_\alpha(tu) = h_\alpha(t)\, h_\alpha(u)$ $\quad$ pour $\quad t, u \in k,\ t \neq 0,\ u \neq 0$.

c) Montrer que toute matrice $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, k)$ peut se mettre d'une façon et d'une seule soit sous la forme $g = h_+(t) x_+(u)$, soit sous la forme $g = h_+(t)\, x_+(u)\, w x_+(v)$, où l'on pose $w = w_+(1)$ (distinguer deux cas, suivant que $c = 0$ ou que $c \neq 0$).

d) On appelle *groupe dérivé* d'un groupe G le sous-groupe G' de G engendré par les « commu-

tateurs $c(x, y) = xyx^{-1}y^{-1}$ de ses éléments. Montrer que $\mathrm{SL}(2, k)$ est égal à son groupe dérivé pourvu que k contienne au moins 4 éléments.

21. On considère dans $\mathrm{SL}(2, k) = \mathrm{G}$ le sous-groupe U formé des $x_+(t)$, et le sous-groupe H formé des $h_+(t)$; on a donc $\mathrm{G} = \mathrm{HU} \cup \mathrm{HU}w\mathrm{U}$ d'après la question *c*) de l'*exercice* précédent. On se propose de montrer que *si k possède au moins 4 éléments le groupe* G *contient un seul sous-groupe invariant* M *autre que* $\{e\}$ *et* G, *à savoir le sous-groupe* Z *formé des matrices* 1 *et* -1 (qui se réduit d'ailleurs à l'élément neutre en caractéristique 2; noter que, dans tous les cas, ce sous-groupe est le centre de G, comme on le vérifiera facilement). On pose $\mathrm{B} = \mathrm{HU}$.

a) Montrer que $\mathrm{B} \cap w\mathrm{B}w^{-1} = \mathrm{H}$, et en déduire que si $\mathrm{M} \subset \mathrm{B}$ alors on a $\mathrm{M} \subset \mathrm{H}$.

b) On suppose $\mathrm{M} \subset \mathrm{H}$. Supposons $h = h_+(t) \in \mathrm{M}$. En calculant le commutateur de h et de $x_+(u)$ montrer que M contient $x_-(u - u/t^2)$, et en déduire que $\mathrm{M} \subset \mathrm{Z}$.

c) On suppose M non contenu dans B. Montrer, à l'aide de la question *c*) de l'*exercice* précédent, que $\mathrm{G} = \mathrm{MB}$, et en déduire (§ 7, exercice 16) que le groupe quotient G/M est isomorphe à $\mathrm{B}/\mathrm{B} \cap \mathrm{M}$.

d) On suppose $\mathrm{Card}(k) \geqslant 4$, et donc $\mathrm{G} = \mathrm{G}'$ d'après l'*exercice* précédent. Montrer que le groupe G/M est égal à son groupe dérivé. Déduire de là et de la question précédente que $\mathrm{M} = \mathrm{G}$ si M n'est pas contenu dans B (remarquer que $\mathrm{B}' \subset \mathrm{U}$ et que $\mathrm{U}' = \{e\}$, et observer que le seul sous-groupe invariant L de B tel que B/L soit son propre groupe dérivé est B lui-même).

22. Dans un groupe G, on considère deux familles d'éléments que l'on notera $\hat{x}_+(t)$ et $\hat{x}_-(t)$ et qui dépendent d'un paramètre t qui varie dans un corps commutatif k donné. A partir des éléments $\hat{x}_\alpha(t)$ de G on définit des éléments $\hat{w}_\alpha(t)$ et $\hat{h}_\alpha(t)$ de G par les formules de l'*exercice* 20, i.e. en posant

$$\hat{w}_\alpha(t) = \hat{x}_\alpha(t)\hat{x}_{-\alpha}(-1/t)\hat{x}_\alpha(t), \qquad \hat{h}_\alpha(t) = \hat{w}_\alpha(t)\hat{w}_\alpha(1)^{-1},$$

et on suppose vérifiées les relations

$$(\mathrm{R}\,1)\quad \hat{x}_\alpha(t+u) = \hat{x}_\alpha(t)\hat{x}_\alpha(u), \qquad (\mathrm{R}\,2)\quad \hat{w}_\alpha(t)\hat{x}_\alpha(u)\hat{w}_\alpha(t)^{-1} = \hat{x}_{-\alpha}(-u/t^2)$$

de l'*exercice* 20.

a) Démontrer les formules suivantes :

$$\hat{w}_\alpha(t)\hat{w}_\alpha(u)\hat{w}_\alpha(t)^{-1} = \hat{w}_{-\alpha}(-u/t^2), \qquad \hat{w}_\alpha(t)\hat{h}_\alpha(u)\hat{w}_\alpha(t)^{-1} = \hat{h}_{-\alpha}(-u/t^2)\hat{h}_{-\alpha}(-1/t^2)^{-1},$$
$$\hat{w}_\alpha(t)\hat{x}_\alpha(u)\hat{w}_\alpha(t)^{-1} = \hat{x}_{-\alpha}(-u/t^2), \qquad \hat{h}_\alpha(t)\hat{x}_\alpha(u)\hat{h}_\alpha(t)^{-1} = \hat{x}_\alpha(t^2u),$$
$$\hat{h}_\alpha(t)\hat{w}_\alpha(u)\hat{h}_\alpha(t)^{-1} = \hat{w}_\alpha(t^2u), \qquad \hat{h}_\alpha(t)\hat{h}_\alpha(u)\hat{h}_\alpha(t)^{-1} = \hat{h}_\alpha(t^2u)\hat{h}_\alpha(t^2)^{-1},$$
$$\hat{w}_\alpha(-1/t) = \hat{w}_{-\alpha}(t), \qquad \hat{w}_\alpha(t)^{-1} = \hat{w}_\alpha(-t),$$
$$\hat{h}_\alpha(-1/t) = \hat{h}_{-\alpha}(t), \qquad \hat{h}_\alpha(t)\hat{h}_\alpha(-1/t) = \hat{h}_\alpha(-1),$$
$$\hat{w}_\alpha(1)\hat{h}_\alpha(t)\hat{w}_\alpha(1)^{-1} = \hat{h}_\alpha(1/t), \qquad \hat{w}_\alpha(1)^{-2} = \hat{h}_\alpha(-1).$$

b) Soient U le sous-groupe de G formé par les $\hat{x}_-(t)$, et H le sous-groupe engendré par les $\hat{h}_-(t)$. On pose $\hat{w} = \hat{w}_1(1)$ et $\mathrm{N} = \mathrm{H} \cup \hat{w}\mathrm{H}$. Montrer que N est un sous-groupe de G et que H est invariant dans N. Montrer que l'on a $\hat{w}\mathrm{U}\hat{w} \subset \mathrm{UNU}$ (ensemble des produits $u'nu''$ avec $u' \in \mathrm{U}$, $u'' \in \mathrm{U}$ et $n \in \mathrm{N}$), et que l'ensemble $\mathrm{UH} \cup \mathrm{UH}\hat{w}\mathrm{U}$ est le sous-groupe de G engendré par les $x_\alpha(t)$.

c) On reprend le groupe $\mathrm{SL}(2, k)$ de l'*exercice* 20 et les éléments $x_\alpha(t)$, $w_\alpha(t)$ et $h_\alpha(t)$ de ce groupe. Montrer, en utilisant la question *c*) de l'*exercice* 20, qu'il existe une application π de $\mathrm{SL}(2, k)$ dans G, et une seule, telle que

$$\pi(h_+(t)x_+(u)) = \hat{h}_+(t)\hat{x}_+(u), \qquad \pi(h_+(t)x_+(u)wx_+(v)) = \hat{h}_+(t)\hat{x}_+(u)\hat{w}\hat{x}_+(v).$$

Montrer que, pour que π soit un homomorphisme, il faut et il suffit que la relation

$$(\mathrm{R}\,3)\qquad \hat{h}_\alpha(tu) = \hat{h}_\alpha(t)\hat{h}_\alpha(u)$$

soit vérifiée. Autrement dit, *pour construire un homomorphisme de* $\mathrm{SL}(2, k)$ *dans un groupe quelconque* G, *il suffit de se donner des éléments* $\hat{x}_+(t)$ *et* $\hat{x}_-(t)$ *de* G *vérifiant les relations* (R 1), (R 2) *et* (R 3) (« définition de $\mathrm{SL}(2, k)$ par générateurs et relations »).

qq 23. On considère le groupe $\mathrm{G} = \mathrm{GL}(n, k)$ sur un corps commutatif k, le sous-groupe T de G formé des matrices diagonales, le sous-groupe B des matrices dont les termes situés en dessous de la diagonale sont tous nuls, et le sous-groupe U de B formé des matrices de B dont tous les termes diagonaux sont égaux à 1. Enfin on note N l'ensemble des $n \in \mathrm{G}$ tels que $n\mathrm{T}n^{-1} = \mathrm{T}$ (normalisateur de T dans G). On identifie les éléments de G aux automorphismes de l'espace vectoriel k^n, dont la base canonique sera notée $e_1, \ldots, e_n$.

a) Montrer que $g \in \mathrm{N}$ si et seulement s'il existe une permutation $w \in \mathfrak{S}_n$ et des scalaires $t_i \neq 0$ tels que l'on ait $g(e_i) = t_i e_{w(i)}$ pour $1 \leqslant i \leqslant n$. En déduire que le groupe quotient $\mathrm{N}/\mathrm{T} = \mathrm{W}$ est isomorphe au groupe symétrique $\mathfrak{S}_n$. Pour $1 \leqslant i \leqslant n-1$, soit $\omega_i \in \mathrm{G}$ la matrice qui permute les vecteurs de base e_i et e_{i+1} et laisse fixe e_j pour tout $j \neq i, i+1$. Montrer que N est engendré par T et les ω_i.

b) Pour $i \neq j$ et $t \in k$ on note $x_{ij}(t)$ l'élément de G défini par les formules suivantes :

$$x_{ij}(t)e_j = e_j + te_i, \qquad x_{ij}(t)e_k = e_k \quad \text{si} \quad k \neq j.$$

Quelle est la matrice de $x_{ij}(t)$? Montrer que l'on a $x_{ij}(t+u) = x_{ij}(t)x_{ij}(u)$ quels que soient $t, u \in k$, et que les $x_{ij}(t)$, pour i et j donnés et t variable, forment un sous-groupe U_{ij} de G. En posant d'une manière générale $(a, b) = aba^{-1}b^{-1}$ montrer qu'on a

$$(x_{ij}(t), x_{jk}(u)) = x_{ik}(tu) \quad \text{si } i, j, k \text{ sont deux à deux distincts.}$$
$$(x_{ij}(t), x_{kl}(u)) = 1 \quad \text{si } j \neq k \text{ et } i \neq l.$$

Montrer que U est engendré par les matrices $x_{i,i+1}(t)$ $(1 \leqslant i \leqslant n-1, t \in k)$. Calculer $nx_{ij}(t)n^{-1}$ pour $n \in \mathrm{N}$.

c) Soit B' le sous-groupe de G formé des matrices dont les termes situés au-dessus de la diagonale sont tous nuls. Montrer qu'il existe un $n \in \mathrm{N}$ tel que $\mathrm{B}' = n\mathrm{B}n^{-1}$, et que B' est engendré par T et les $x_{i+1,i}(t)$. Soit g un élément quelconque de G; montrer qu'il existe un $b \in \mathrm{B}$ et un $b' \in \mathrm{B}'$ tels qu'en posant $g = bb'g_1$ la matrice g_1 soit de la forme

$$g_1 = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & * & \ldots & * \\ \ldots & \ldots & \ldots & \ldots \\ 0 & * & \ldots & * \end{pmatrix}.$$

En déduire que G est engendré par B et B' ou, ce qui revient au même, par B et N (raisonner par récurrence sur n).

Montrer, en utilisant les formules de l'exercice 20, que le sous-groupe de G engendré par les $x_{i,i+1}(t)$ et les $x_{i+1,i}(t)$ est $\mathrm{SL}(n, k)$, ensemble des $g \in \mathrm{GL}(n, k)$ tels que $\det(g) = 1$ (cette question suppose le lecteur au courant de la théorie des déterminants, et ne sera pas utilisée par la suite).

d) On considère le sous-groupe $\mathrm{B}_i = \mathrm{B} \cap \omega_i^{-1}\mathrm{B}\omega_i$. Montrer que B_i est invariant dans B, et que tout $b \in \mathrm{B}$ s'écrit, de façon unique, comme produit d'un élément de $\mathrm{U}_{i,i+1}$ et de B_i. En déduire que la double classe $\mathrm{B}\omega_i\mathrm{B}$, ensemble des $b'\omega_i b''$ avec $b', b'' \in \mathrm{B}$, est réunion des classes $\mathrm{B}\omega_i x_{i,i+1}(t)$, $t \in k$.

e) En posant $n \cdot {}^t U_{i,i+1} n = U_{jk}$ montrer que l'ensemble $B\omega_i BnB$ (pour $n \in N$) est réunion des classes $B\omega_i n x_{jk}(t)B$, où t varie. En déduire que l'on a

$$B\omega_i BnB = B\omega_i nB \quad \text{si } j < k, \qquad \text{et} \qquad B\omega_i BnB = BnB \cup B\omega_i nB \quad \text{si } j > k$$

(on utilisera le fait, qu'il suffit de vérifier dans $GL(2, k)$, que $x_{i+1,i}(t) \in B\omega_i B$ si $t \neq 0$).

f) Soit G_0 la réunion des doubles classes BnB (lesquelles sont en nombre fini puisque N/T est fini). En utilisant le fait que N est engendré par T et les ω_i, montrer à l'aide de la question précédente que $nG_0 \subset G_0$ pour tout $n \in N$. Montrer que G_0 est un sous-groupe de G, et en déduire que

$$G = \bigcup BnB$$

(théorème de Bruhat pour le groupe linéaire).

24. Soit k un corps fini à q éléments, et soit V un espace vectoriel de dimension finie n sur k; soit m un entier compris entre 0 et n.

a) Soit X_m l'ensemble des familles $(x_1, \ldots, x_m)$ d'éléments de V linéairement indépendants. Montrer que l'on a :

$$\mathrm{Card}(X_m) = (q^n - 1)(q^n - q) \ldots (q^n - q^{m-1}).$$

(Raisonner par récurrence sur m.)

b) Montrer que l'ordre du groupe GL(V) des automorphismes de V est donné par la formule :

$$\mathrm{Card}\ GL(V) = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}) = q^{n^2} \prod_{i=1}^{i=n} \left(1 - \frac{1}{q^i}\right).$$

c) Soit $G_{n,m}$ l'ensemble des sous-espaces vectoriels de V de dimension m (« grassmannienne »). Montrer que l'on a :

$$\mathrm{Card}\ G_{n,m} = q^{n^2 - m^2} \prod_{i=n-1}^{i=n} \left(1 - \frac{1}{q^i}\right).$$

25. Soit V un espace vectoriel de dimension 2 sur le corps à 2 éléments; soient x, y, z les trois éléments non nuls de V.

a) Montrer que l'on a $x + x = y + y = z + z = 0$ et $x + y = z, y + z = x, z + x = y$.

b) En déduire que le groupe GL(V) des automorphismes de V est isomorphe au groupe des permutations de x, y, z.

26. Soit V un espace vectoriel de dimension 2 sur le corps à 3 éléments.

a) Montrer que V contient 4 sous-espaces de dimension 1, soient D_1, D_2, D_3, D_4.

b) Tout élément du groupe d'automorphismes GL(V) de V permute les D_i entre eux. On déduit de là un homomorphisme

$$\varepsilon : GL(V) \to S_4,$$

où S_4 désigne le groupe des permutations de $\{1, 2, 3, 4\}$. Montrer que le noyau de ε est $\{\pm 1\}$; en déduire que ε est surjectif (comparer les ordres des deux groupes).

c) Soit (LSV) le sous-groupe de GL(V) formé des éléments de déterminant 1. Montrer que ε définit un isomorphisme de SL(V) sur le groupe alterné A_4, formé des permutations paires; de S_4. [Cette question suppose le lecteur au courant de la théorie des déterminants.]

§ 16

1. On considère les trois formes linéaires

$$2x - y + 3z, \qquad 3x - 5y + z, \qquad 4x - 7y + z$$

sur $\mathbf{R}^3$, Forment-elles une base du dual de $\mathbf{R}^3$?

2. Montrer que les formes linéaires

$$x + 2y + z, \qquad 2x + 3y + 3z, \qquad 3x + 7y + z$$

forment une base du dual de $\mathbf{R}^3$, et trouver la base de $\mathbf{R}^3$ duale de celle-ci.

3. Soient K un anneau et $f_1, \ldots, f_n$ des formes linéaires sur le K-module à droite K^n. Pour que celles-ci forment une base du dual de K^n, il faut et il suffit qu'il existe des vecteurs $x_1, \ldots, x_n \in K^n$ tels que l'on ait

$$f_i(x_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases}$$

4. Soient K un anneau commutatif et U une matrice carrée d'ordre n à coefficients dans K.

a) Montrer que les relations

$${}^t U . U = 1_n, \qquad U . {}^t U = 1_n$$

sont équivalentes.

b) Montrer que les matrices $U \in M_n(K)$ vérifiant les conditions précédentes forment un sous-groupe de $GL(n, K)$ (**groupe orthogonal à n variables** sur l'anneau K).

c) On dit qu'une matrice $S \in M_n(K)$ est **symétrique** si ${}^t S = S$. Soient X et Y deux matrices symétriques; pour que XY soit symétrique, il faut et il suffit que $XY = YX$.

d) Montrer (en prenant $K = \mathbf{Q}$ ou un surcorps quelconque de $\mathbf{Q}$) que la matrice

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

est à la fois orthogonale et symétrique.

e) Trouver toutes les matrices orthogonales d'ordre 3 à coefficients entiers rationnels.

5. Soit $M_n(K)$ l'anneau des matrices carrées d'ordre n sur un anneau quelconque K; on regarde $M_n(K)$ comme un K-module à droite. Montrer que, pour toute forme linéaire f sur $M_n(K)$, il existe une et une seule matrice $A \in M_n(K)$ telle que

$$f(X) = \mathrm{Tr}(AX) \quad \text{pour tout } X \in M_n(K)$$

(voir l'*Exercice* 8 du § 12 pour une définition du symbole Tr). Pour que l'on ait

$$f(XY) = f(YX)$$

quelles que soient $X, Y \in M_n(K)$, il faut et il suffit, lorsque l'anneau K est commutatif, que la matrice A soit proportionnelle à 1_n.

1. Soient K un anneau, L un K-module et

$$L = M_1 \oplus \cdots \oplus M_n$$

une décomposition de L en somme directe de sous-modules.

a) Pour tout endomorphisme u de L, montrer qu'il existe un et un seul système d'homomorphismes

$$u_{ij} : M_i \to M_j \quad (1 \leqslant i, j \leqslant n)$$

tels que l'on ait

$$u(x) = u_{ij}(x) + \cdots + u_{nj}(x) \quad \text{pour tout } x \in M_j$$

et tout j tel que $1 \leqslant j \leqslant n$. Montrer inversement qu'étant donnés de tels homomorphismes u_{ij}, il existe un et un seul endomorphisme u de L vérifiant les conditions précédentes.

b) A tout endomorphisme u de L on associe la « matrice »

$$\begin{pmatrix} u_{11} & \cdots & u_{n1} \\ \cdots & \cdots & \cdots \\ u_{1n} & \cdots & u_{nn} \end{pmatrix}$$

formée avec les homomorphismes définis dans la question *a*). Étant donnés deux endomorphismes u et v de L, comment calcule-t-on la « matrice » de $v \circ u$ en fonction de celles de u et v?

2. Soient r un entier $\geqslant 1$ donné et $r_1, \ldots, r_n$ des entiers $\geqslant 1$ tels que

$$r = r_1 + \cdots + r_n.$$

Étant donnée une matrice carrée

$$U = \begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \cdots & \cdots & \cdots \\ a_{1r} & \cdots & a_{rr} \end{pmatrix}$$

à coefficients dans un anneau quelconque K, on désigne par U_{ij} $(1 \leqslant i, j \leqslant n)$ la matrice (à r_i colonnes et r_j lignes) formée avec ceux des termes a_{pq} de la matrice U pour lesquels on a à la fois

$$r_1 + \cdots + r_{i-1} < p \leqslant r_1 + \cdots + r_i$$
$$r_1 + \cdots + r_{j-1} < q \leqslant r_1 + \cdots + r_j,$$

ce qui permet, avec des conventions évidentes, d'écrire U sous la form

$$U = \begin{pmatrix} U_{11} & \dots & U_{n1} \\ \dots & \dots & \dots \\ U_{1n} & \dots & U_{nn} \end{pmatrix}.$$

Soit V une autre matrice carrée d'ordre n à coefficients dans K, et soit $W = VU$ la matrice produit. Montrer que les « blocs » W_{ii} qui composent W sont donnés par la formule

$$W_{ij} = V_{1j}U_{i1} + \dots + V_{nj}U_{in}$$

analogue à la règle de calcul usuelle des matrices (**formule de multiplication par blocs** des matrices). Peut-on étendre ce résultat à des produits de matrices rectangulaires?

3. Montrer qu'avec les notations de l'Exercice précédent, la transposée d'une matrice U est donnée par

$$^tU = \begin{pmatrix} {}^tU_{11} & \dots & {}^tU_{1n} \\ \dots & \dots & \dots \\ {}^tU_{n1} & \dots & {}^tU_{nn} \end{pmatrix}.$$

4. Soit K un corps commutatif. On considère la matrice carrée

$$J = \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix}$$

(où 0 est la matrice nulle à n lignes et n colonnes), et on cherche les matrices carrées

$$U = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

d'ordre $2n$, à coefficients dans K, telles que

$$^tU.J.U = J$$

(où A, B, C, D sont des matrices carrées d'ordre n à coefficients dans K). Écrire les relations que doivent vérifier A, B, C, D. Trouver les matrices U pour lesquelles $C = 0$.

5. Soit $S = {}^tS$ une matrice symétrique carrée d'ordre n à coefficients dans un corps commutatif K On pose

$$J = \begin{pmatrix} 0 & 0 & 1_p \\ 0 & S & 0 \\ 1_p & 0 & 0 \end{pmatrix}$$

(de sorte que J est une matrice carrée d'ordre $n + 2p$). A quelles conditions la matrice

$$M = \begin{pmatrix} U & X & Z \\ 0 & V & Y \\ 0 & 0 & W \end{pmatrix}$$

(où la décomposition en blocs de M est de même nature que celle de J) vérifie-t-elle la relation

$$^tM.J.M = J?$$

6. Soient K un anneau et $r_1, \dots, r_n$ des entiers $\geqslant 1$. On pose $r = r_1 + \dots + r_n$, et on considère les matrices

$$U = \begin{pmatrix} U_{11} & \dots & U_{n1} \\ \dots & \dots & \dots \\ U_{1n} & \dots & U_{nn} \end{pmatrix}$$

(avec U_{ij} à r_i colonnes et r_j lignes) qui vérifient les conditions suivantes : on a

$$U_{ij} = 0 \quad \text{pour } i < j,$$

et de plus les matrices U_{ii} sont inversibles. Montrer que les matrices U forment un sous-groupe du groupe linéaire GL(r, K). Même question pour les matrices telles que

$$U_{ij} = 0 \text{ si } i < j, \qquad U_{ii} = 1.$$

Montrer que le second sous-groupe est invariant dans le premier, et formé de matrices unipotentes.

7. Soit $L = M_1 \oplus \dots \oplus M_p$ une décomposition en somme directe de sous-modules d'un module à gauche L sur un anneau K. Dans le module à droite L*, dual de L, on considère pour chaque i tel que $1 \leqslant i \leqslant p$ l'ensemble M_i' des formes linéaires f sur L telles que

$$f(M_j) = 0 \quad \text{pour tout } j \neq i.$$

Montrer que les M_i' sont des sous-modules de L* et que $L^* = M_1' \oplus \dots \oplus M_p'$.

8. Soient M un module à gauche sur un anneau K et M' un sous-module M. On suppose que le module quotient M/M' (§§ 10, 11, *Exercice* 10) est libre de type fini. Montrer qu'alors M' est facteur direct dans M (considérer le sous-module de M engendré par des éléments dont les images dans M/M' forment une base de M/M'). Pour une application importante de ce résultat, voir § 29, *Exercice* 11, *g*).

9. Soient M un module à gauche sur un anneau K et a un élément de M tel que $\lambda a = 0$ implique $\lambda = 0$; pour que le sous-module Ka engendré par a soit facteur direct dans M, il faut et il suffit qu'il existe sur M une forme linéaire f telle que $f(a) = 1$; on a alors

$$M = Ka \oplus \mathrm{Ker}(f).$$

§ 18

1. Montrer que tout sous-groupe *de type fini* du groupe additif $\mathbf{Q}^n$ possède une *base* d'au plus n éléments (imiter la démonstration du Théorème 1).

2. Pour qu'il existe une base de $\mathbf{Z}^n$ contenant un élément donné $(a_1, \ldots, a_n)$ de $\mathbf{Z}^n$, il faut et il suffit que les entiers a_i soient premiers entre eux (choisir des $u_i \in \mathbf{Z}$ tels que $\sum u_i a_i = 1$ et considérer le sous-groupe de $\mathbf{Z}^n$ défini par l'équation $\sum u_i x_i = 0$).
Plus généralement, soit K un anneau; pour qu'il existe une base de K^n contenant un $a \in K^n$ donné, il est nécessaire qu'il existe une forme linéaire f sur K^n telle que $f(a) = 1$, et cette condition est suffisante si K est principal (cf. § 17, *Exercice* 9).

3. Pour qu'il existe une matrice $U \in GL(n, \mathbf{Z})$ ayant une première ligne donnée

$$a_{11} \quad a_{21} \quad \ldots \quad a_{n1},$$

il faut et il suffit que les entiers $a_{11}, a_{21}, \ldots, a_{n1}$ soient premiers entre eux.

4. Soient L et M deux modules de type fini sur un anneau commutatif noethérien K. Montrer que le K-module $\mathrm{Hom}_K(L, M)$ est de type fini (construire un homomorphisme injectif de ce module dans une puissance convenable de M).

5. Soit M un module de type fini sur un anneau noethérien K. Montrer que toute suite croissante de sous-modules de M est stationnaire, et que tout ensemble de sous-modules de M possède au moins un élément maximal.

6. Soit a un idéal d'un anneau commutatif noethérien K. Montrer qu'il existe une suite finie d'idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ (pas nécessairement deux à deux distincts) de K telle que l'on ait

$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \subset a$$

(raisonner par l'absurde, considérer un élément maximal de l'ensemble des idéaux ne possédant pas cette propriété, et lui appliquer l'*Exercice* 11 du § 8).

7. Soient K un corps commutatif et A un sous-anneau de K admettant K pour corps des fractions (i.e. tel que tout $x \in K$ soit quotient de deux éléments de A). On utilise dans ce qui suit les définitions et résultats de l'*Exercice* 14 des §§ 10, 11.

a) Si A est un anneau de Dedekind, A est noethérien.

b) On suppose A noethérien, et que tout idéal *maximal* de l'anneau A est inversible; montrer que tout idéal de A est produit d'un nombre fini d'idéaux maximaux (méthode analogue à celle de l'*Exercice* précédent). En déduire que A est un anneau de Dedekind.

c) Soit A un anneau de Dedekind. Montrer que tout idéal fractionnaire de A s'écrit sous la forme d'un produit fini de puissances (positives ou négatives) d'idéaux premiers de A, et que cette décomposition est unique à l'ordre près des facteurs.

d) Soit $\mathfrak{p}$ un idéal premier de l'anneau de Dedekind A. Pour tout $x \in K$ non nul, on désigne par $v_\mathfrak{p}(x)$ l'exposant (qui peut être nul) de $\mathfrak{p}$ dans la décomposition de l'idéal fractionnaire Ax de A en produit de facteurs premiers; et on définit $v_\mathfrak{p}(0) = +\infty$. Montrer que la fonction $v_\mathfrak{p}$ est une valuation discrète (§ 8, *Exercice* 6) du corps K.

¶ **8.** Soient K un anneau commutatif noethérien, M un K-module de type fini, et u l'homothétie de rapport $a \in K$ dans M, donnée par

$$u(x) = ax \quad \text{pour tout } x \in M.$$

a) Montrer qu'il existe un entier $p \geqslant 0$ tel que l'on ait $\mathrm{Ker}(u^n) = \mathrm{Ker}(u^{n+1})$ pour tout $n \geqslant p$ (utiliser l'*Exercice* 5).

b) Montrer qu'on a $\mathrm{Im}(u^n) \cap \mathrm{Ker}(u) = \{0\}$ pour tout $n \geqslant p$.

c) On dit que le module M est **primaire** si, dans M, toute homothétie est soit injective soit nilpotente. Montrer qu'il en est ainsi lorsque le module M possède la propriété suivante : l'intersection de deux sous-modules non nuls de M n'est jamais nulle.

d) Soit $\mathfrak{q}$ un idéal de l'anneau K. Pour que $\mathfrak{q}$ soit primaire (§ 8, *Exercice* 13) il faut et il suffit que le quotient $K/\mathfrak{q}$, regardé comme K-module, soit primaire.

e) Un idéal $\mathfrak{q}$ d'un anneau K est dit **irréductible** si $\mathfrak{q} \neq K$ et si, quels que soient les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de K, la relation

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{q} \text{ implique } \mathfrak{a} = \mathfrak{q} \text{ ou } \mathfrak{b} = \mathfrak{q}.$$

Montrer que tout idéal irréductible d'un anneau noethérien est primaire.

NB. — La réciproque est fausse.

¶¶ **9.** Soit K un anneau commutatif noethérien.

a) Montrer que tout idéal $\mathfrak{a} \neq K$ est intersection finie d'idéaux irréductibles (méthode de l'*Exercice* 6).

b) En déduire que *tout idéal d'un anneau commutatif noethérien est intersection finie d'idéaux primaires* (Emmy Noether).

¶¶ **10.** Soit M un module de type fini sur un anneau commutatif noethérien K. On dit qu'un idéal premier $\mathfrak{p}$ de K est **associé à** M s'il existe un $x \in M$ tel que $\mathfrak{p}$ soit l'annulateur de x dans M (i.e. tel que la relation $a \in \mathfrak{p}$ soit équivalente à la relation $ax = 0$).

a) Si $M \neq \{0\}$, il existe au moins un idéal premier associé à M (considérer les annulateurs des éléments non nuls de M et en prendre un maximal).

b) Il existe une suite croissante

$$0 = M_0 \subset M_1 \subset \cdots \subset M_r = M$$

de sous-modules de M et des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ de K tels que M_i/M_{i-1} soit isomorphe au module quotient $K/\mathfrak{p}_i$ pour tout i tel que $1 \leqslant i \leqslant r$ [observer que si l'annulateur d'un élément x d'un module est un idéal a de K, alors le sous-module Kx engendré par x est isomorphe à K/a].

c) Avec les notations de la question précédente, tout idéal premier associé à M est l'un des $\mathfrak{p}_i$.

d) Soit $u(x) = ax (a \in K)$ une homothétie dans M. Pour que u soit injective, il faut et il suffit que a n'appartienne à aucun des idéaux premiers associés à M. Pour que u soit nilpotente, il faut et il suffit que a appartienne à tous les idéaux premiers associés à M.

e) On prend dans ce qui précède $M = K$ et on note $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ les idéaux premiers associés à M. Montrer que

$$\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$$

est l'ensemble des diviseurs de zéro dans K, et que

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$$

est l'ensemble des éléments nilpotents de K.
Montrer que tout idéal premier de K contient l'un des $\mathfrak{p}_i$. En déduire que, dans un anneau noethérien, l'intersection de tous les idéaux premiers est l'ensemble des éléments nilpotents (ce résultat s'étend en fait à tous les anneaux commutatifs : §§ 27, 28, *Exercice* 9).

¶ **11.** Soit $\mathfrak{a}$ un idéal d'un anneau commutatif noethérien K; on suppose $\mathfrak{a} \neq K$. On appelle **idéal premier minimal de** $\mathfrak{a}$ tout idéal premier $\mathfrak{p}$ de K qui contient $\mathfrak{a}$, et qui ne contient aucun idéal premier contenant $\mathfrak{a}$ autre que lui-même.
Montrer que les idéaux premiers minimaux de $\mathfrak{a}$ sont en nombre fini, et que leur intersection est le radical (§ 8, *Exercice* 12) de $\mathfrak{a}$ (appliquer à $K/\mathfrak{a}$ la question *e*) de l'*Exercice* précédent).
(Les anneaux noethériens ont été inventés vers 1920 par Emmy Noether et ont été l'un des principaux points de départ de l'Algèbre « abstraite » moderne. Leur théorie, aujourd'hui extraordinairement développée, est à la base de la Géométrie Algébrique; mais on les utilise aussi ailleurs, en particulier dans la théorie des fonctions analytiques de plusieurs variables complexes; en fait, l'invention de ces anneaux est certainement l'une des découvertes mathématiques les plus utiles des temps modernes. Avant l'introduction des anneaux noethériens, on se bornait à en démontrer certaines propriétés sur les anneaux de polynômes — ce qui conduisait fréquemment à des démonstrations beaucoup plus compliquées que celles qu'on connait aujourd'hui puisqu'on n'avait pas encore isolé l'idée fondamentale qui permet de les simplifier, à savoir les Théorèmes 3 et 4 de ce §.)

1. On considère dans $\mathbf{R}^4$ les vecteurs

$$(1, 0, 0, -1), \quad (2, 1, 1, 0), \quad (1, 1, 1, 1), \quad (1, 2, 3, 4), \quad (0, 1, 2, 3);$$

extraire de ces cinq vecteurs une base du sous-espace qu'ils engendrent.

2. On considère dans $\mathbf{R}^4$ le sous-espace L engendré par les vecteurs

$$(1, 1, 1, 1), \quad (1, -1, 1, -1), \quad (1, 3, 1, 3)$$

et le sous-espace M engendré par

$$(1, 2, 0, 2), \quad (1, 2, 1, 2), \quad (3, 1, 3, 1);$$

calculer les dimensions de $L \cap M$ et $L + M$.

3. Soient V un espace vectoriel de dimension n sur un corps et L un sous-espace de dimension r de V. Pour qu'un sous-espace M de V soit un supplémentaire de L dans V, il faut et il suffit qu'on ait

$$L \cap M = \{0\}, \quad \dim(M) = n - r.$$

4. Soient V un espace vectoriel de dimension finie sur un corps, $(a_i)_{1 \leqslant i \leqslant n}$ une base de V, et $x_1, \ldots, x_r$ des éléments de V en nombre $r \leqslant n$. Pour que les x_i soient linéairement indépendants il faut et il suffit qu'il existe un automorphisme u de V tel que l'on ait

$$u(a_i) = x_i \quad \text{pour } 1 \leqslant i \leqslant r.$$

¶ **5.** Soient L et M des espaces vectoriels de dimension finie sur un corps K, et f un homomorphisme de L dans M, de rang r. Montrer qu'il existe une base $(a_i)_{1 \leqslant i \leqslant p}$ de L et une base $(b_j)_{1 \leqslant j \leqslant q}$ de M telles que l'on ait les relations

$$f(a_i) = b_i \quad \text{pour } 1 \leqslant i \leqslant r$$
$$f(a_i) = 0 \quad \text{pour } r + 1 \leqslant i \leqslant p.$$

En déduire le résultat suivant : soit A une matrice à q lignes et p colonnes à coefficients dans K, de rang r; alors il existe des matrices

$$U \in GL(q, K) \quad \text{et} \quad V \in GL(p, K)$$

telles que

$$\mathrm{UAV} = \begin{pmatrix} 1_r & 0 \\ 0 & 0 \end{pmatrix}$$

(les 0 figurant au second membre désignent des matrices nulles ayant les nombres de lignes et de colonnes requis pour que le second membre soit une matrice à q lignes et p colonnes). Soient A et B deux matrices à q lignes et p colonnes à coefficients dans K; pour qu'il existe des matrices $\mathrm{U} \in \mathrm{GL}(q, \mathrm{K})$ et $\mathrm{V} \in \mathrm{GL}(p, \mathrm{K})$ telles que $\mathrm{B} = \mathrm{UAV}$, il faut et il suffit que A et B aient même rang.

6. Soient E et F deux sous-espaces vectoriels d'un espace vectoriel V de dimension finie; pour qu'il existe un automorphisme u de V tel que $\mathrm{F} = u(\mathrm{E})$, il faut et il suffit que $\dim(\mathrm{E}) = \dim(\mathrm{F})$.

7. Soient $x_1, \ldots, x_n$ des éléments d'un espace vectoriel; on suppose que $x_1, \ldots, x_r$ sont linéairement indépendants, et qu'on a des relations

$$x_j = \rho_{j1}x_1 + \cdots + \rho_{jr}x_r \quad (r+1 \leqslant j \leqslant n).$$

Soit L l'espace des relations linéaires entre $x_1, \ldots, x_n$, i.e. des systèmes de scalaires $(\lambda_1, \ldots, \lambda_n) \in \mathrm{K}^n$ tels que

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0.$$

Montrer que les $n - r$ éléments

$$(\rho_{j1}, \ldots, \rho_{jr}, 0, \ldots, 0, -1, 0, \ldots, 0),$$

où -1 se trouve à la j^e place, forment une base de L.

8. Soient $f_1, \ldots, f_n$ des formes linéaires sur un espace vectoriel; pour que le système d'équations

$$f_i(x) = \beta_i \quad (1 \leqslant i \leqslant n)$$

possède au moins une solution, il faut et il suffit qu'on ait

$$\lambda_1\beta_1 + \cdots + \lambda_n\beta_n = 0$$

pour toute relation linéaire $(\lambda_1, \ldots, \lambda_n)$ entre $f_1, \ldots, f_n$.

9. Soit K un corps commutatif.

a) Pour qu'une forme linéaire f sur $\mathrm{M}_n(\mathrm{K})$, regardé comme espace vectoriel de dimension n^2 sur K, vérifie

$$f(\mathrm{XY}) = f(\mathrm{YX}),$$

il faut et il suffit qu'il existe un scalaire $\lambda \in \mathrm{K}$ tel que

$$f(\mathrm{X}) = \lambda . \mathrm{Tr}(\mathrm{X}) \quad \text{pour tout } \mathrm{X} \in \mathrm{M}_n(\mathrm{K})$$

(on rappelle — § 12, *Exercice* 8 — que $\mathrm{Tr}(\mathrm{X})$ désigne la somme des coefficients diagonaux de X).

b) Déduire de là et du Théorème 3 du § 19 le résultat suivant : pour qu'une matrice $\mathrm{A} \in \mathrm{M}_n(\mathrm{K})$ puisse s'écrire comme somme de matrices de la forme $\mathrm{XY} - \mathrm{YX}$, il faut et il suffit que $\mathrm{Tr}(\mathrm{A}) = 0$.

10. Soient V un espace vectoriel de dimension finie sur un corps K et $(a_i)_{1 \leqslant i \leqslant n}$ une base de V.

a) Soit x un élément non nul de V. Montrer (sans utiliser les résultats du § 19) qu'il existe un indice i tel que les vecteurs $a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n$ forment encore une base de V.

b) Soient $x_1, \ldots, x_p$ des vecteurs linéairement indépendants dans V. A l'aide de la question *a*), et en raisonnant par récurrence sur p, montrer qu'il existe une base de V formée des p vecteurs x_j et de $n - p$ des vecteurs a_i. En déduire une nouvelle démonstration des Théorèmes 6 et 7 du § 19.

11. Démontrer directement le Corollaire du Théorème 7 en raisonnant par récurrence sur p (on utilisera l'une des équations pour exprimer une inconnue à l'aide des $p - 1$ autres, et on se ramènera à un système de $n - 1$ équations à $p - 1$ inconnues).

¶ **12.** Soient L et M deux espaces vectoriels de dimension finie sur un corps, f une application linéaire de L dans M, et

$${}^t f : \mathrm{M}^* \to \mathrm{L}^*$$

l'application transposée (§ 16). Montrer que $\mathrm{Im}({}^t f)$ est le sous-espace de L^* orthogonal à $\mathrm{Ker}(f)$, et que $\mathrm{Ker}({}^t f)$ est le sous-espace de M^* orthogonal à $\mathrm{Im}(f)$ (utiliser le Théorème 3). Déduire de là que f et sa transposée ont le même rang, et appliquer ce résultat pour obtenir une autre démonstration du Corollaire du Théorème 16. Montrer que si f est un endomorphisme de L, les noyaux de f et ${}^t f$ ont même dimension.

13. Soit K un corps. Pour qu'une matrice $\mathrm{A} \in \mathrm{M}_n(\mathrm{K})$ soit inversible, il faut et il suffit que A ne soit pas diviseur de zéro dans l'anneau $\mathrm{M}_n(\mathrm{K})$.

14. Soit X une matrice à coefficients dans un corps. Montrer que le rang de X n'est pas modifié lorsqu'on ajoute à une ligne (resp. colonne) de X une combinaison linéaire quelconque des autres lignes (resp. colonnes) de X, ou lorsqu'on fait subir une permutation quelconque aux lignes (resp. colonnes) de X.

15. Soient V un espace vectoriel complexe de dimension finie et $(a_k)_{1 \leqslant k \leqslant n}$ une base de V. On regarde V comme un espace vectoriel réel; montrer que les $2n$ vecteurs

$$a_1, \ldots, a_n, \qquad ia_1, \ldots, ia_n$$

forment une base de V sur $\mathbf{R}$. En conclure que

$$\dim_{\mathbf{R}}(\mathrm{V}) = 2 . \dim_{\mathbf{C}}(\mathrm{V}).$$

¶ **16.** Soient L un corps et K un sous-corps de L; on dit que L est une **extension de degré fini** de K si L, regardé comme espace vectoriel sur K, est de dimension finie; la dimension en question s'appelle alors le **degré de L sur** K, et se note $[\mathrm{L} : \mathrm{K}]$.
Soit V un espace vectoriel de dimension finie sur L. On regarde V comme un espace vectoriel sur K; montrer que, si L est extension finie de K, on a

$$\dim_{\mathrm{K}}(\mathrm{V}) = [\mathrm{L} : \mathrm{K}] . \dim_{\mathrm{L}}(\mathrm{V})$$

(imiter le raisonnement de l'*Exercice* précédent).
Soient K un corps, L un corps extension finie de K, et M un corps extension finie de L. Montrer que M est extension finie de K et que

$$[\mathrm{M} : \mathrm{K}] = [\mathrm{M} : \mathrm{L}] . [\mathrm{L} : \mathrm{K}].$$

17. Soit

$$L_1 \xrightarrow{f_1} L_2 \xrightarrow{f_2} L_3 \dots \xrightarrow{f_n} L_{n+1}$$

une suite formée d'espaces vectoriels de dimension finie sur un corps, et d'homomorphismes de chaque espace dans le suivant. On suppose que f_1 est injectif, f_n surjectif, et que

$$\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1}) \quad \text{pour } 1 \leqslant i \leqslant n.$$

Montrer qu'on a alors

$$\dim(L_1) - \dim(L_2) + \dim(L_3) - \dots + (-1)^n \dim(L_{n+1}) = 0.$$

¶ **18.** Soit p un nombre premier. Quelles conditions doivent vérifier les entiers u et v pour qu'on puisse résoudre les congruences

$$\begin{aligned} x + 2y + 3z &\equiv u \pmod{p} \\ 4x + 5y + 6z &\equiv v \pmod{p} ? \end{aligned}$$

¶ **19.** Soit V un espace vectoriel de dimension finie n sur un corps.

a) Soient $L_1, \dots, L_r$ des sous-espaces vectoriels de V tels que

$$L_1 \subset L_2 \subset \dots \subset L_r = V;$$

on pose $\dim(L_i) = d_i$; montrer qu'il existe une base de V telle que, pour chaque i, les d_i premiers éléments de cette base forment une base de L_i.

b) Soit u un endomorphisme nilpotent de V, i.e. tel que $u^k = 0$ pour un entier k au moins. Soit r le plus petit entier non nul tel que

$$u^r = 0;$$

on pose

$$L_1 = \mathrm{Ker}(u), \qquad L_2 = \mathrm{Ker}(u^2), \quad \dots, \quad L_r = \mathrm{Ker}(u^r).$$

Montrer que ces sous-espaces de V vérifient les hypothèses de la question *a*). En déduire qu'il existe une base de V par rapport à laquelle la matrice de u est de la forme (*)

$$\begin{pmatrix} 0 & * & * & * & \dots & * \\ 0 & 0 & * & * & \dots & * \\ 0 & 0 & 0 & * & \dots & * \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & . & 0 \end{pmatrix}.$$

Réciproque ?

c) Soit $N \in M_n(K)$ une matrice nilpotente. Montrer qu'il existe une matrice $U \in GL(n, K)$ telle que

$$UNU^{-1} = \begin{pmatrix} 0 & * & * & \dots & * \\ 0 & 0 & * & \dots & * \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Réciproque ?

¶¶ **20.** Soit V un espace vectoriel de dimension finie n sur $\mathbf{Q}$, et soit M un sous-*groupe* de type fini de V.

a) Montrer qu'il existe une base de V par rapport à laquelle les coordonnées de tout $x \in M$ soient entières.

(*) On trouvera un résultat plus précis au § 35.

b) Montrer qu'il existe un entier $r \leqslant n$ tel que M soit le sous-groupe de V engendré par r éléments linéairement indépendants convenablement choisis de V (autrement dit que le groupe M est isomorphe à $\mathbf{Z}^r$ pour un entier $r \leqslant n$). (Utiliser le Théorème 3 du § 18.)

c) Soit $(a_i)_{1 \leqslant i \leqslant n}$ une base de V. Montrer qu'il existe une base $(b_i)_{1 \leqslant i \leqslant n}$ de V telle que (*i*) M soit engendré par $b_1, \dots, b_r$ (*ii*) la matrice de passage de la base (a_i) à la base (b_i) soit triangulaire (imiter la démonstration du Théorème 3 du § 18).

d) En déduire que *toute matrice* $X \in M_n(\mathbf{Q})$ *est produit d'une matrice* $U \in GL(n, \mathbf{Z})$ *et d'une matrice triangulaire.*

¶ **21.** Soient A et B deux matrices carrées d'ordre n à coefficients dans un corps. Montrer qu'on a

$$\mathrm{rg}(A) + \mathrm{rg}(B) - n \leqslant \mathrm{rg}(AB) \leqslant \mathrm{Min}(\mathrm{rg}(A), \mathrm{rg}(B))$$

(inégalités de Sylvester).

22. Soit u un endomorphisme d'un espace vectoriel V de dimension finie sur un corps *commutatif* K; montrer que, si A et B sont les matrices de u par rapport à deux bases quelconques de V, on a

$$\mathrm{Tr}(A) = \mathrm{Tr}(B)$$

(§ 12, *Exercice* 8). La valeur commune des traces des matrices de u par rapport aux diverses bases de V s'appelle la **trace de l'endomorphisme** u, et se note

$$\mathrm{Tr}(u).$$

Montrer qu'on a

$$\mathrm{Tr}(u+v) = \mathrm{Tr}(u) + \mathrm{Tr}(v), \qquad \mathrm{Tr}(\lambda u) = \lambda \mathrm{Tr}(u) \quad \text{pour } \lambda \in K,$$
$$\mathrm{Tr}(u \circ v) = \mathrm{Tr}(v \circ u), \qquad \mathrm{Tr}(j_V) = \dim(V),$$

et que ces propriétés caractérisent entièrement l'application

$$\mathrm{Tr} : \mathcal{L}(V) \to K.$$

Montrer qu'on a aussi

$$\mathrm{Tr}(u) = \mathrm{Tr}({}^t u)$$

pour tout endomorphisme u de V.

¶ **23.** Pour qu'un système d'équations linéaires

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ \dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m \end{cases}$$

à coefficients dans un corps, possède au moins une solution, il faut et il suffit que les deux matrices

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} & b_m \end{pmatrix}$$

possèdent le même rang.

¶¶ **24.** Soient L un corps commutatif et A un sous-*anneau* de L; on suppose que, comme A-module, L est de type fini; on se propose d'en déduire que A est un sous-*corps* de L.

a) Soit K l'ensemble des $x \in L$ qui peuvent s'écrire sous la forme u/v avec $u, v \in A$ et $v \neq 0$.

Montrer que c'est un sous-corps de L, et que L est de dimension finie en tant qu'espace vectoriel sur K.

b) Soit $(u_1, \ldots, u_n)$ un système de générateurs du A-module L; on choisit une base $(v_0, v_1, \ldots, v_r)$ de L regardé comme espace vectoriel sur K, telle que $v_0 = 1$, et on pose

$$u_i = \sum_{0 \leqslant j \leqslant r} x_{ij} v_j$$

avec des $x_{ij} \in K$. Montrer que le A-module K est engendré par les éléments x_{i0}.

c) Terminer la démonstration à l'aide de l'*Exercice* 9 des §§ 10, 11.

Résoudre les systèmes d'équations linéaires suivants (*) par la méthode des éliminations successives (celle-ci consiste à utiliser une équation pour calculer une inconnue en fonction des autres, puis à reporter le résultat ainsi obtenu dans les autres équations, de façon à se ramener à un système comportant une inconnue et une équation de moins que le système initial).

1.
$$\begin{aligned} 2x - y + 3z &= 9 \\ 3x - 5y + z &= -4 \\ 4x - 7y + z &= 5 \end{aligned}$$

2.
$$\begin{aligned} 2x + 3y + 5z &= 10 \\ 3x + 7y + 4z &= 3 \\ x + 2y + 2z &= 3 \end{aligned}$$

3.
$$\begin{aligned} 5x + 2y + 3z &= -2 \\ 2x - 2y + 5z &= 0 \\ 3x + 4y + 2z &= -10 \end{aligned}$$

4.
$$\begin{aligned} 4bcx + acy - 2abz &= 0 \\ 5bcx + 3acy - 4abz &= -abc \\ 3bcx + 2acy - abz &= 4abc \end{aligned}$$
(on suppose $abc \neq 0$)

5.
$$\begin{aligned} x + y + z &= a \\ x + \omega y + \omega^2 z &= b \\ x + \omega^2 y + \omega z &= c \end{aligned}$$
(où ω est une racine cubique de l'unité)

6.
$$\begin{aligned} ax - 3y + 5z &= 4 \\ x - ay + 3z &= 2 \\ 9x - 7y + 8az &= 0 \end{aligned}$$
(discuter suivant les valeurs de a)

(*) Dans les *Exercices* 1 à 17 (extraits du recueil de Proskurjakov, où l'on en trouvera beaucoup d'autres) le corps de base est **C**. Toutefois, le lecteur désireux d'introduire plus de variété dans les calculs pourra se placer sur un corps commutatif K quelconque et tenir compte de la caractéristique de K, ou bien chercher les solutions dans l'anneau **Z** des entiers rationnels lorsque la question a un sens. Il va de soi d'autre part qu'après avoir étudié la théorie des déterminants, le lecteur devra l'appliquer à la résolution de ces *Exercices*.

7.
$$\begin{aligned} ax + 2z &= 2 \\ 5x + 2y &= 1 \\ x - 2y + bz &= 3 \end{aligned}$$
(discuter suivant les valeurs de a et b)

8.
$$\begin{aligned} 2x + 2y - z + t &= 4 \\ 4x + 3y - z + 2t &= 6 \\ 8x + 5y - 3z + 4t &= 12 \\ 3x + 3y - 2z + 2t &= 6 \end{aligned}$$

9.
$$\begin{aligned} 2x - y - 6z + 3t &= -1 \\ 7x - 4y + 2z - 15t &= -32 \\ x - 2y - 4z + 9t &= 5 \\ x - y + 2z - 6t &= -8 \end{aligned}$$

10.
$$\begin{aligned} 2x - 5y + 3z + t &= 5 \\ 3x - 7y + 3z - t &= -1 \\ 5x - 9y + 6z + 2t &= 7 \\ 4x - 6y + 3z + t &= 8 \end{aligned}$$

11.
$$\begin{aligned} 6x + 6y + 5z + 18t + 20u &= 14 \\ 10x + 9y + 7z + 24t + 30u &= 18 \\ 12x + 12y + 13z + 27t + 35u &= 32 \\ 8x + 6y + 6z + 15t + 20u &= 16 \\ 4x + 5y + 4z + 15t + 15u &= 11 \end{aligned}$$

12.
$$\begin{aligned} 2x + 7y + 3z + t &= 5 \\ x + 3y + 5z - 2t &= 3 \\ x + 5y - 9z + 8t &= 1 \\ 5x + 18y + 4z + 5t &= 12 \end{aligned}$$

13.
$$\begin{aligned} 2x + 5y - 8z &= 8 \\ 4x + 3y - 9z &= 9 \\ 2x + 3y - 5z &= 7 \\ x + 8y - 7z &= 12 \end{aligned}$$

14.
$$\begin{aligned} 6x + 3y + 2z + 3t + 4u &= 5 \\ 4x + 2y + z + 2t + 3u &= 4 \\ 4x + 2y + 3z + 2t + u &= 0 \\ 2x + y + 7z + 3t + 2u &= 1 \end{aligned}$$

(on déterminera en outre toutes les solutions *entières* de ce dernier système).

15.
$$\begin{aligned} 2x + 3y + z + 2t &= 3 \\ 4x + 6y + 3z + 4t &= 5 \\ 6x + 9y + 5z + 6t &= 7 \\ 8x + 12y + 7z + \lambda t &= 9 \end{aligned}$$
(discuter suivant les valeurs de λ)

16.
$$\begin{aligned} ax + y + z &= 1 \\ x + ay + z &= 1 \\ x + y + az &= 1 \end{aligned}$$
(discuter suivant les valeurs de a)

17.
$$\begin{aligned} (a+1)x + y + z &= a^2 + 3a \\ x + (a+1)y + z &= a^3 + 3a^2 \\ x + y + (a+1)z &= a^4 + 3a^3 \end{aligned}$$
(discuter suivant les valeurs de a).

18. Soit K un corps. On considère d'une part le système

$$(i) \qquad \begin{cases} a_{11}x_1 + \cdots + a_{n1}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{1n}x_1 + \cdots + a_{nn}x_n = b_n \end{cases}$$

de n équations linéaires à n inconnues, à coefficients dans K, et d'autre part le système

$$(ii) \qquad \begin{cases} a_{11}y_1 + \cdots + a_{n1}y_n - b_1 y_{n+1} = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{1n}y_1 + \cdots + a_{nn}y_n - b_n y_{n+1} = 0 \end{cases}$$

de n équations linéaires et homogènes à $n+1$ inconnues.

a) Montrer que si une solution de (ii) vérifie $y_{n+1} \neq 0$, alors les

$$x_i = y_i y_{n+1}^{-1}$$

forment une solution de (i), et que réciproquement toute solution de (i) permet de construire une solution de (ii) telle que $y_{n+1} \neq 0$.

b) Montrer que les deux propriétés suivantes sont équivalentes : le système homogène associé à (i) ne possède aucune solution non triviale; toute solution non triviale de (ii) vérifie $y_{n+1} \neq 0$.

c) En utilisant le Corollaire du Théorème 7 du § 19, déduire de là une démonstration du fait que les conditions *a*) et *e*) du Théorème 2 du § 20 sont équivalentes.

19. Si un système d'équations linéaires à coefficients réels admet au moins une solution complexe, il admet une solution réelle.

¶¶ **20.** Soient L un corps et K un sous-corps de L.

a) On considère un système de n équations linéaires et homogènes à n inconnues, à coefficients dans K. Montrer que si le système admet une solution non triviale dans L, il admet une solution non triviale dans K (raisonner par récurrence sur n en utilisant par exemple la méthode des éliminations successives).

b) Montrer que si une matrice $A \in M_n(K)$ est inversible dans l'anneau $M_n(L)$, elle est inversible dans l'anneau $M_n(K)$.

c) Si des éléments de K^n (resp. des formes linéaires sur K^n) sont linéairement indépendants sur K, ils sont aussi linéairement indépendants sur L, et réciproquement.

d) Pour qu'un système d'équations linéaires, à coefficients et seconds membres dans K, admette une solution dans K, il faut et il suffit qu'il admette une solution dans L.

e) Les solutions dans L d'un système d'équations linéaires et homogènes à coefficients dans K, sont les combinaisons linéaires, à coefficients dans L, des solutions dans K du système considéré.

f) Si un système d'équations linéaires et homogènes à coefficients dans $\mathbf{Z}$ admet une solution non triviale dans $\mathbf{C}$, il admet une solution non triviale dans $\mathbf{Z}$.

EXERCICES DU § 0 481
EXERCICES DU § 1 485
EXERCICES DU § 2 486
EXERCICES DU § 3 489
EXERCICES DU § 4 491
EXERCICES DU § 5 494
EXERCICES DU § 7 498
EXERCICES DU § 8 505
EXERCICES DU § 9 514
EXERCICES DU § 10 520
EXERCICES DU § 11 520
EXERCICES DU § 12 525
EXERCICES DU § 13 525
EXERCICES DU § 14 525
EXERCICES DU § 15 529
EXERCICES DU § 16 537
EXERCICES DU § 17 539
EXERCICES DU § 18 542
EXERCICES DU § 19 545
EXERCICES DU § 20 551
EXERCICES DU § 21 554
EXERCICES DU § 22 559
EXERCICES DU § 23 562
EXERCICES DU § 24 566
EXERCICES DU § 26 571
EXERCICES DU § 27 574
EXERCICES DU § 28 574
EXERCICES DU § 29 582
EXERCICES DU § 30 588
EXERCICES DU § 31 592
EXERCICES DU § 32 598
EXERCICES DU § 33 607
EXERCICES DU § 34 619
EXERCICES DU § 35 633
EXERCICES DU § 36 641

BIBLIOGRAPHIE 655

INDEX DES NOTATIONS 659

INDEX TERMINOLOGIQUE 661