# § 8. Anneaux et corps

## 1. Définition des anneaux, exemples

*On appelle* **anneau** *un triplet formé d'un ensemble* K *et de deux lois de composition sur* K, *notées* $(x, y) \to x + y$ (« addition » dans K) *et* $(x, y) \mapsto xy$ (« multiplication » dans K), *ces données devant vérifier les conditions suivantes :*
(A 1) : *le couple formé de l'ensemble* K *et de la loi de composition* $(x, y) \mapsto x + y$ *sur* K *est un groupe commutatif;*
(A 2) : *la loi de composition* $(x, y) \to xy$ *est associative et admet un élément neutre* (*);
(A 3) : *quels que soient* $x, y, z \in K$, *on a les relations* (dites de « distributivité de la multiplication par rapport à l'addition »)

$$x(y + z) = xy + xz, \qquad (x + y)z = xz + yz.$$

L'axiome (A 1) des anneaux s'explicite comme suit : on a les identités

$$x + (y + z) = (x + y) + z$$
$$x + y = y + x;$$

il existe d'autre part dans K un élément noté 0, tel que l'on ait

$$x + 0 = x$$

pour tout $x \in K$; enfin, quel que soit $x \in K$, il existe un élément de K, noté $-x$, tel que l'on ait

$$x + (-x) = 0.$$

Il s'ensuit que, quels que soient $a, b \in K$, l'équation

$$a + x = b$$

(*) Certains auteurs omettent, dans la définition d'un anneau, d'exiger l'existence d'un élément neutre pour la multiplication; on obtient ainsi une notion d'anneau plus générale que celle du texte; mais la pratique montre, et la théorie le confirme, qu'on peut toujours se limiter, comme nous le ferons dans cet ouvrage, à des anneaux *avec* élément unité.

possède une et une seule solution dans K, à savoir $b + (-a)$; on l'écrit

$$x = b - a.$$

L'axiome (A 2) des anneaux signifie que, dans un anneau, on a l'identité

$$x(yz) = (xy)z,$$

et qu'il existe un élément de K, noté 1, tel que l'on ait

$$x1 = 1x = x$$

pour tout $x \in K$. On dit que 1 est l'*élément unité* de K.

On dit qu'un anneau K est **commutatif** si l'on a

$$xy = yx \quad \text{quels que soient } x, y \in K;$$

on rencontrera dans la théorie des matrices d'importants exemples d'anneaux non commutatifs. On dit que deux éléments $x, y$ d'un anneau quelconque K **commutent** si l'on a $xy = yx$.

Dans un anneau, on a les relations

$$(-1)x = -x, \qquad 0x = 0$$

pour tout $x$; pour établir la première, il suffit de prouver que $(-1)x + x = 0$; or

$$(-1)x + x = (-1)x + 1x = (-1 + 1)x = 0x,$$

de sorte qu'on est ramené à prouver la seconde relation $0x = 0$. Pour cela on calcule

$$0x + x = 0x + 1x = (0 + 1)x = 1x = x,$$

ce qui montre que $0x = x - x = 0$ comme dans tout groupe additif.

Donnons maintenant des exemples d'anneaux.

*Exemple* 1. Si l'on munit l'ensemble **Z** des entiers rationnels des deux lois de composition usuelles (addition et multiplication) on obtient évidemment un anneau commutatif; on l'appelle l'**anneau des entiers rationnels.** Les ensembles **Q** (nombres rationnels) et **R** (nombres réels), munis de l'addition et de la multiplication usuelles, sont aussi des anneaux commutatifs.

*Exemple* 2. Soit K l'ensemble des nombres réels $x$ qui possèdent la propriété suivante : il existe des *entiers rationnels* $a, b, c$ tels que l'on ait

$$x = a + br + cr^2, \qquad \text{où} \qquad r = \sqrt[3]{2}.$$

On vérifie immédiatement que, si $x, y \in K$, alors $x + y$ et $xy$ sont encore dans K, ce qui permet de munir l'ensemble K de deux lois de composition, à savoir l'addition et la multiplication usuelles. Cela dit, l'ensemble K, avec ces deux lois de composition, est un anneau commutatif.



*Exemple* 3. Soient X un ensemble quelconque, K un anneau quelconque, et désignons par A l'ensemble de toutes les applications de X dans K. Pour $f, g \in A$, définissons comme suit des éléments $f + g$ et $fg$ de A : l'élément $f + g$ sera l'application

$$x \mapsto f(x) + g(x)$$

de X dans K, et $fg$ sera l'application

$$x \mapsto f(x)g(x)$$

de X dans K. Cela dit, l'ensemble A, muni des deux lois de composition

$$(f, g) \mapsto f + g \qquad \text{et} \qquad (f, g) \mapsto fg$$

qu'on vient de définir, est un *anneau* (commutatif si et seulement si K est commutatif). Vérifions par exemple la formule de distributivité

$$f(g + h) = fg + fh;$$

il suffit de montrer que les deux membres (qui sont des applications de X dans K) ont la même valeur en chaque $x \in X$; la valeur du premier membre est $f(x)\,(g(x) + h(x))$, celle du second membre est $f(x)g(x) + f(x)h(x)$; on voit donc que l'axiome de distributivité est vérifié dans A parce qu'il l'est déjà dans K.

Le lecteur débutant fera bien de traiter cet Exemple en détail, et de s'assurer du fait que, pour montrer que A est un anneau, on a effectivement besoin de se servir du fait que K vérifie *tous* les axiomes des anneaux. On comprendra facilement pourquoi en examinant le cas où X est un ensemble à un élément...

L'anneau A qu'on vient de définir s'appelle **l'anneau des applications de l'ensemble X dans l'anneau K.**

*Exemple* 4. On prend $X = K = \mathbf{R}$ dans l'*Exemple* 3, mais au lieu de considérer toutes les applications de X dans K on se borne à considérer celles qui vérifient certaines conditions de « régularité » données d'avance, par exemple : être continue en un point donné; être continue partout; avoir une dérivée troisième continue partout; etc... Dans chaque cas, on obtient un anneau commutatif.

*Exemple* 5. On verra plus loin (§ 15) que les matrices carrées à $n$ lignes et $n$ colonnes, à coefficients dans un anneau donné K, forment un nouvel anneau (non commutatif si $n \geqslant 2$, même si K est commutatif) pourvu qu'on définisse l'addition et la multiplication des matrices à l'aide des formules des §§ 14 et 15.

Soit K un anneau; on appelle **sous-anneau de** K toute partie A de K qui vérifie les conditions suivantes : A *est un sous-groupe du groupe additif* K; *les relations* $x \in A$ *et* $y \in A$ *impliquent la relation* $xy \in A$; *on a* $1 \in A$. S'il en est ainsi, il est clair que les applications

$$(x, y) \mapsto x + y \qquad \text{et} \qquad (x, y) \mapsto xy$$

de K × K dans K appliquent A × A dans A, donc définissent deux lois de composition sur l'ensemble A. Cela dit, *l'ensemble* A, *muni de ces deux lois de composition, est un anneau.*

En effet, l'ensemble A muni de l'addition est un groupe commutatif en vertu du § 7, n° 3; d'autre part, la multiplication est associative dans K, donc *a fortiori* dans A, et A admet un élément neutre pour la multiplication puisqu'il contient l'élément 1 de K; enfin, les identités de distributivité, étant vérifiées dans K, le sont à plus forte raison dans A.

Il est clair que, dans l'*Exemple* 1 ci-dessus, **Z** est un sous-anneau de **Q**, lui-même sous-anneau de **R**. D'autre part, les anneaux de l'*Exemple* 4 ci-dessus sont des sous-anneaux de l'anneau de toutes les applications de l'ensemble X = **R** dans l'anneau K = **R**.

On notera que, pour vérifier qu'une partie A d'un anneau K est un sous-anneau de K, il suffit de vérifier les conditions suivantes : *si* A *contient deux éléments x et y de* K, *il contient aussi leur somme x + y et leur produit xy; en outre,* A *contient* — 1.

En effet, supposons remplies ces conditions; pour $x \in A$, on a alors $-x \in A$ vu que $-x = (-1)x$; mais alors, si A contient $x$ et $y$, donc aussi $x$ et $-y$, il contient également $x + (-y) = x - y$, ce qui prouve que A est un sous-groupe du groupe additif K, autrement dit vérifie la première condition figurant dans la définition d'un sous-anneau. D'autre part, comme A contient — 1, il contient $-(-1) = 1$, donc vérifie la troisième condition figurant dans la définition d'un sous-anneau. La seconde, enfin, est vérifiée par hypothèse.

### 2. *Anneaux d'intégrité et corps*

Considérons dans un anneau K l'équation

$$ax = b, \tag{1}$$

où $a$, $b$ sont des éléments donnés, et $x$ un élément « inconnu » de K.

Un premier cas simple est celui où $a = 0$; comme $0x = 0$ pour tout $x \in K$, il est clair qu'alors deux cas seulement sont possibles : ou bien $b = 0$, et alors tout $x \in K$ vérifie l'équation (1); ou bien $b \neq 0$, et alors l'équation (1) n'a aucune solution.

Un second cas très simple est celui où $a$ admet un inverse relativement à la multiplication, i.e. où il existe un (et un seul) élément de K, noté $a^{-1}$, vérifiant

$$a^{-1}a = aa^{-1} = 1;$$

alors le Théorème 4 du § 6 s'applique : l'équation (1) possède, quel que soit $b$, une et seule solution

$$x = a^{-1}b.$$

Dans ce cas, on dit que $a$ est un **élément inversible** de K (on dit aussi souvent que $a$ est un élément *unitaire* ou une *unité* de K, mais nous n'utiliserons pas cette terminologie dangereuse).

Reste à examiner, dans la mesure où c'est possible, le cas où $a$ n'est ni nul ni inversible. Tout d'abord ce cas peut fort bien ne pas se produire — autrement dit, il peut arriver que *tout élément non nul de* K *soit inversible;* on dit alors que K est un **corps** (*). Les anneaux **Q** et **R** sont des corps (**corps des nombres rationnels** et **corps des nombres réels**), par contre l'anneau **Z** n'est pas un corps (pour qu'un $x \in \mathbf{Z}$ soit inversible dans l'anneau **Z**, il faut et il suffit qu'il existe un $y \in \mathbf{Z}$ tel que $xy = 1$; ce n'est évidemment possible que si $x = +1$ ou $x = -1$).

Revenant au cas général, on peut se demander s'il est possible que l'équation (1) admette plusieurs solutions. Si $x$ et $y$ sont deux telles solutions, on aura évidemment $ax = ay$, donc

$$a(x - y) = 0;$$

ceci conduit à introduire la notion suivante : on dit qu'un anneau K est **intègre** ou est un **anneau d'intégrité,** lorsque, pour $u \in K$ et $v \in K$, la relation

$$uv = 0 \quad \text{implique} \quad u = 0 \quad \text{ou} \quad v = 0$$

(autrement dit lorsqu'un produit d'éléments de K ne peut être nul sans qu'un au moins des facteurs du produit le soit). L'anneau **Z** est évidemment un anneau d'intégrité. Un corps est nécessairement un anneau d'intégrité, car de la relation $uv = 0$ résulte, si $u \neq 0$, que $v = u^{-1}0 = 0$.

Dans un anneau d'intégrité, l'équation (1), pour $a \neq 0$, possède *au plus* une solution comme le montre le raisonnement ci-dessus. Mais il peut naturellement arriver qu'elle n'en possède aucune — c'est le cas par exemple de l'équation $2x = 3$ dans l'anneau **Z** — et on ne peut rien dire de général sur les conditions de résolubilité de l'équation (1) dans un anneau d'intégrité qui n'est pas un corps.

Il existe des anneaux qui ne sont pas intègres. Prenons par exemple l'anneau de toutes les applications de l'ensemble **R** dans l'anneau **R** (*Exemple* 3 ci-dessus) et considérons les deux éléments $f$ et $g$ de cet anneau définis comme suit :

$$f(x) = \begin{cases} x & \text{pour } x \geqslant 0, \\ 0 & \text{pour } x \leqslant 0, \end{cases} \qquad g(x) = \begin{cases} 0 & \text{pour } x \geqslant 0, \\ x & \text{pour } x \leqslant 0; \end{cases}$$

il est clair que

$$f(x)g(x) = 0 \quad \text{pour tout} \quad x \in \mathbf{R},$$

et par suite que $fg = 0$ dans l'anneau considéré; néanmoins on a $f \neq 0$ et $g \neq 0$ (car l'élément 0 de l'anneau des applications d'un ensemble X dans un anneau K est la fonction qui, en *chaque* $x \in X$ *sans exception,* prend la valeur 0 — ce qui, ici, n'est le cas ni de $f$ ni de $g$).

*Remarque* 1. Soit K un anneau; on désigne habituellement l'ensemble des éléments inversibles de K par la notation

$$K^*$$

(cf. le passage de **Q** à **Q*** ou de **R** à **R***). D'après le Théorème 3 du § 6, si $K^*$

(*) En fait, dans un corps, on exige aussi que $1 \neq 0$, de sorte qu'un corps possède toujours au moins *deux* éléments.

contient deux éléments $x$ et $y$ il contient aussi $xy$; on peut donc munir l'ensemble $K^*$ de la loi de composition $(x, y) \mapsto xy$. Cela dit, l'ensemble $K^*$, muni de cette loi de composition, est un *groupe*. Il est clair en effet que la loi de composition considérée sur $K^*$ est associative (car elle l'est déjà dans K); d'autre part, on a évidemment $1 \in K^*$, de sorte que la loi de composition considérée sur l'ensemble $K^*$ admet un élément neutre; enfin, si $x \in K^*$, on a aussi $x^{-1} \in K^*$ d'après le Théorème 3 du § 6, et comme on a

$$x^{-1}x = xx^{-1} = 1,$$

élément neutre de $K^*$, on voit que tout élément de $K^*$ est inversible (dans $K^*$, et pas seulement dans K !) pour la loi de composition considérée.

L'ensemble $K^*$, muni de la loi de composition $(x, y) \mapsto xy$, s'appelle le **groupe multiplicatif de l'anneau** K (ou, parfois, le **groupe des unités** de K). Si K est un *corps*, on a

$$K^* = K - \{0\}.$$

Par contre, on a

$$\mathbf{Z}^* = \{1, -1\},$$

avec la table de multiplication suivante :

$$1.1 = 1; \qquad -1.1 = 1.-1 = -1; \qquad -1.-1 = 1.$$

*Remarque* 2. Soit K un corps. On appelle **sous-corps** de K toute partie A de K vérifiant les conditions suivantes : A *est un sous-anneau de* K, *et pour* $x \neq 0$ *la relation* $x \in A$ *implique* $x^{-1} \in A$. Il est clair qu'alors l'ensemble A, muni des lois de composition « induites » par celles de K, est non seulement un anneau mais un corps.

Ainsi, $\mathbf{Q}$ est un sous-corps de $\mathbf{R}$.

*Exemple* 6. Soit $K \subset \mathbf{R}$ l'ensemble des nombres réels $x$ possédant la propriété suivante : il existe des nombres *rationnels* $a$ et $b$ tels que l'on ait

$$x = a + br, \qquad \text{où} \qquad r = \sqrt{2}.$$

Le lecteur vérifiera facilement que K est un sous-corps de $\mathbf{R}$.

### 3. *L'anneau des entiers modulo p*

Au § 4, *Exemple* 9, nous avons défini, pour tout entier rationnel $p$, l'*ensemble* $\mathbf{Z}/p\mathbf{Z}$ des entiers modulo $p$, et, dans l'*Exemple* 14 du même §, nous avons défini sur cet ensemble deux lois de composition appelées addition et multiplication; celles-ci sont liées aux lois de composition sur les entiers ordinaires par le fait suivant : *si* $\theta$ *désigne l'application canonique de* $\mathbf{Z}$ *sur* $\mathbf{Z}/p\mathbf{Z}$, *on a*

$$\theta(x + y) = \theta(x) + \theta(y), \qquad \theta(xy) = \theta(x)\theta(y)$$

*quels que soient* $x, y \in \mathbf{Z}$.

On va déduire de là que *l'ensemble* $\mathbf{Z}/p\mathbf{Z}$ *des entiers modulo* $p$, *muni de l'addition et de la multiplication définies au* § 4, *est un anneau commutatif.*

Montrons d'abord que l'addition dans $\mathbf{Z}/p\mathbf{Z}$ est associative; soient $\xi$, $\eta$, $\zeta$ trois éléments de cet ensemble; il existe $x, y, z \in \mathbf{Z}$ tels que $\xi = \theta(x)$, $\eta = \theta(y)$, $\zeta = \theta(z)$; on a alors

$$\xi + \eta = \theta(x) + \theta(y) = \theta(x + y), \qquad \eta + \zeta = \theta(y) + \theta(z) = \theta(y + z),$$

donc

$$(\xi + \eta) + \zeta = \theta(x + y) + \theta(z) = \theta((x + y) + z),$$
$$\xi + (\eta + \zeta) = \theta(x) + \theta(y + z) = \theta(x + (y + z)),$$

et l'associativité de l'addition dans $\mathbf{Z}/p\mathbf{Z}$ résulte donc de l'associativité de l'addition dans $\mathbf{Z}$.

On prouverait de même l'associativité de la multiplication, la commutativité de l'addition et de la multiplication, et la distributivité de la multiplication par rapport à l'addition dans $\mathbf{Z}/p\mathbf{Z}$.

Il est clair, vu la relation

$$\theta(1)\theta(x) = \theta(1x) = \theta(x),$$

que $\theta(1)$ est élément neutre pour la multiplication dans $\mathbf{Z}/p\mathbf{Z}$, et de même que $\theta(0)$ est élément neutre pour l'addition.

Pour établir que $\mathbf{Z}/p\mathbf{Z}$ est un anneau commutatif, il reste donc à montrer que tout élément $\xi$ de $\mathbf{Z}/p\mathbf{Z}$ admet un opposé; pour cela, on écrit $\xi = \theta(x)$ pour un $x \in \mathbf{Z}$ convenablement choisi, et il est alors clair, vu la relation

$$\theta(-x) + \theta(x) = \theta(-x + x) = \theta(0),$$

que $\xi$ admet effectivement un opposé, à savoir $\theta(-x)$.

Les résultats qu'on vient d'établir permettent de parler de **l'anneau** $\mathbf{Z}/p\mathbf{Z}$ **des entiers modulo** $p$; cet anneau possède un nombre fini seulement d'éléments si $p \neq 0$, à savoir $p$ (on suppose $p$ positif, ce qui ne restreint pas la généralité).

Pour certaines valeurs de $p$, l'anneau $\mathbf{Z}/p\mathbf{Z}$ est même un corps (ce qui prouvera l'existence de **corps finis**, i.e. de corps à un nombre fini d'éléments) :

THÉORÈME 1. *Soit* $p \geqslant 2$ *un entier. Les assertions suivantes sont équivalentes :*

*a) l'anneau* $\mathbf{Z}/p\mathbf{Z}$ *est intègre;*

*b) l'anneau* $\mathbf{Z}/p\mathbf{Z}$ *est un corps;*

*c) le nombre* $p$ *est premier.*

Soient $\xi$ et $\eta$ deux éléments *non nuls* de $\mathbf{Z}/p\mathbf{Z}$; on a donc $\xi = \theta(x)$, $\eta = \theta(y)$ avec

$$x \not\equiv 0 \pmod{p}, \qquad y \not\equiv 0 \pmod{p};$$

pour en déduire que $\xi\eta$, qui est égal à $\theta(xy)$, est aussi non nul, il faut montrer qu'on a aussi

$$xy \not\equiv 0 \pmod{p};$$

autrement dit, pour que $\mathbf{Z}/p\mathbf{Z}$ soit intègre, il faut et il suffit que la relation

$$xy \equiv 0 \pmod{p} \quad \text{implique} \quad x \equiv 0 \pmod{p} \quad \text{ou} \quad y \equiv 0 \pmod{p},$$

ou encore que si $p$ divise un produit $xy$, il divise soit $x$ soit $y$ : d'où l'équivalence des propriétés *a*) et *c*).

Il est d'autre part clair que *b*) implique *a*). Pour achever la démonstration, il suffit donc de montrer que *a*) implique *b*), ce qui résultera visiblement du Théorème plus général que voici :

THÉORÈME 2. *Tout anneau d'intégrité fini est un corps.*

Soit K un anneau d'intégrité fini; pour un élément $a \neq 0$ de K, considérons l'application $x \to ax$ de K dans K; comme $ax = ay$ implique $a(x-y) = 0$, donc $x - y = 0$ si K est intègre, on voit que l'application considérée est *injective*; mais comme l'ensemble K est *fini*, cette application est forcément *surjective* (§ 5, Théorème 4), et en particulier on peut résoudre $ax = 1$, ce qui montre que tout élément non nul de K possède un inverse à droite. On montrerait de même, à l'aide de l'application $x \to xa$, que tout élément non nul de K possède un inverse à gauche, ce qui achève la démonstration.

*Remarque* 3. On peut démontrer que *tout corps fini est commutatif*, mais les techniques nécessaires pour y parvenir dépassent de fort loin le niveau du présent ouvrage.

On peut d'autre part démontrer que le nombre d'éléments d'un corps fini est nécessairement une puissance d'un nombre premier, et que pour tout nombre premier $p$ et tout entier $n \geqslant 1$, il existe essentiellement un seul corps à $p^n$ éléments (ce qui veut dire qu'on sait construire explicitement tous les corps finis). La première étude détaillée des corps finis a été faite par Galois.

### 4. *Formule du binôme*

Les « identités remarquables » qu'on démontre dans l'enseignement secondaire lorsqu'il s'agit de nombres réels, sont pour la plupart encore valables dans tout anneau (en supposant parfois que les éléments $x, y, \cdots$ figurant dans ces identités commutent deux à deux). Par exemple, soient $x, y$ deux éléments d'un anneau K, et calculons

$$(x+y)^2 = (x+y)(x+y) = x^2 + xy + yx + y^2;$$

on voit que, si $x$ et $y$ commutent, on retrouve l'identité $(x+y)^2 = x^2 + 2xy + y^2$. On a alors

$$(x+y)^3 = (x^2 + 2xy + y^2)(x+y) = x^3 + 3x^2y + 3xy^2 + y^3$$

comme le montre un calcul trivial.

Plus généralement :

THÉORÈME 3. *Soient* K *un anneau, $x$ et $y$ deux éléments de* K, *et supposons que $x$ et $y$ commutent. On a alors, pour tout entier $n \geqslant 1$, la relation*

$$(x+y)^n = \sum_{p=0}^{p=n} \binom{n}{p} x^{n-p} y^p$$

*où l'on pose*

$$\binom{n}{p} = \frac{n(n-1)\dots(n-p+1)}{1.2\dots p} = \frac{n!}{p!(n-p)!} \quad (0 \leqslant p \leqslant n).$$

*Remarque* 4. Rappelons (§ 5, Théorème 10) que les nombres $\binom{n}{p}$ sont des *entiers* et pas seulement des nombres rationnels.

Le résultat à établir est trivial pour $n = 1$; il suffit donc de prouver que la formule

$$(x+y)^{n-1} = \sum_{p=0}^{p=n-1} \binom{n-1}{p} x^{n-1-p} y^p,$$

implique la formule analogue pour l'exposant $n$. Or, en multipliant par $x+y$ la relation précédente, il vient

$$(x+y)^n = \sum_{p=0}^{p=n-1} \binom{n-1}{p} x^{n-p} y^p + \sum_{p=0}^{p=n-1} \binom{n-1}{p} x^{n-1-p} y^{p+1};$$

si $r$ est un entier tel que $0 < r < n$, il y a au second membre de la relation précédente deux termes contenant le monôme

$$x^{n-r} y^r;$$

le premier s'obtient en prenant $p = r$ dans la première somme, ce qui introduit un facteur égal à

$$\binom{n-1}{r},$$

et le second s'obtient en prenant $p = r-1$ dans la seconde somme, ce qui introduit un facteur égal à

$$\binom{n-1}{r-1};$$

pour achever la démonstration il reste donc à vérifier la relation

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}.$$

Or le second membre est égal à

$$\frac{(n-1)(n-2)\dots(n-r)}{1.2\dots r} + \frac{(n-1)(n-2)\dots(n-r+1)}{1.2\dots(r-1)}$$

$$= \frac{(n-1)\dots(n-r+1)(n-r) + (n-1)\dots(n-r+1)r}{r!}$$

$$= \frac{[(n-r)+r](n-1)\dots(n-r+1)}{r!} = \frac{n(n-1)\dots(n-r+1)}{r!} = \binom{n}{r},$$

ce qui achève la démonstration.

La relation

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

permet de calculer facilement les nombres $\binom{n}{r}$, qu'on appelle pour des raisons évidentes les **coefficients du binôme** d'indices $n$ et $r$. Ils sont donnés par le tableau suivant, appelé **triangle de Pascal** :

```
1  1
1  2  1
1  3  3  1
1  4  6  4  1
1  5  10 10 5  1
1  6  15 20 15 6  1
1  7  21 35 35 21 7  1
.....................;
```

la méthode, pour calculer le $p^e$ terme de la $n^e$ ligne, consiste à additionner le $p^e$ et le $(p-1)^e$ termes de la ligne précédente.

L'examen du tableau précédent suggère la formule

$$\binom{n}{r} = \binom{n}{n-r};$$

la vérification de celle-ci est immédiate puisque

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}, \qquad \binom{n}{n-r} = \frac{n!}{(n-r)!\,r!};$$

mais la véritable raison de la formule en question réside dans le fait que l'expression

$$\sum_{p=0}^{p=n} \binom{n}{p} x^{n-p} y^p$$

ne doit pas changer — vu sa signification — si l'on permute $x$ et $y$; il est donc naturel que les coefficients dans cette expression des « monômes » $x^{n-r}y^r$, $x^r y^{n-r}$ soient égaux, puisque ces monômes se déduisent l'un de l'autre par échange de $x$ et $y$.

On peut aussi observer que, X désignant un ensemble à $n$ éléments, $\binom{n}{r}$ est le nombre de parties à $r$ éléments de X; en associant à une telle partie Y son complémentaire X — Y, on obtient une *bijection* de l'ensemble des parties à $r$ éléments de X sur l'ensemble des parties à $n-r$ éléments de X; d'où la relation $\binom{n}{r} = \binom{n}{n-r}$.

### 5. *Développement d'un produit de sommes*

La formule du binôme est un cas particulier d'une formule plus générale que nous allons exposer maintenant.

Soient K un anneau commutatif, I un ensemble *fini*, et $(x_i)_{i\in I}$ et $(y_i)_{i\in I}$ deux familles d'éléments de K indexées par I. On se propose de « développer » le produit

$$\prod_{i\in I}(x_i + y_i).$$

Pour énoncer le résultat, introduisons d'abord la notation suivante : étant donnée une partie F de I, on posera

$$x_F = \prod_{i\in F} x_i, \qquad y_F = \prod_{i\in F} y_i$$

(étant entendu que $x_F = y_F = 1$ si F est vide). Ceci dit, la formule cherchée s'écrit

$$\prod_{i\in}(x_i + y_i) = \sum_{F\subset I} x_F y_{I-F},$$

la somme figurant au second membre étant étendue à toutes les parties de l'ensemble I.

En effet, pour multiplier des sommes les unes par les autres, on choisit, de toutes les façons possibles, un terme dans chacune de ces sommes, on effectue le produit des termes ainsi choisis, et on additionne les résultats ainsi obtenus pour tous les choix possibles.

Le produit des sommes $x_i + y_i$ sera donc une somme de termes obtenus en multipliant les $x_i$ figurant dans un certain nombre des sommes données par les $y_j$ figurant dans les autres. Pour un tel produit, notons F l'ensemble des valeurs de $i$ pour lesquelles on décide de choisir $x_i$, de sorte que I — F est l'ensemble des valeurs de $i$ pour lesquelles on décide de choisir $y_i$; il est clair que le produit des termes ainsi choisis est $x_F y_{I-F}$; en ajoutant les résultats ainsi obtenus on trouve donc la formule annoncée.

La formule du binône résulte comme suit de la relation qu'on vient d'établir : on prend pour I un ensemble à $n$ éléments, et on choisit $x_i = x, y_i = y$ pour tout $i \in$ I. Le premier membre de la formule générale est donc $(x+y)^n$. Au second membre, il est clair que

$$x_F y_{I-F} = x^r y^{n-r}$$

où $r$ est le nombre d'éléments de F. Il reste donc, pour obtenir la formule du binôme, à tenir compte du fait que, dans un ensemble à $n$ éléments, il y a $\binom{n}{r}$ parties à $r$ éléments.

### 6. *Homomorphismes d'anneaux*

Étant donnés deux anneaux K et L, on appelle **homomorphisme de K dans L** toute application $f$ de K dans L telle que l'on ait

$$f(x+y)=f(x)+f(y), \quad f(xy)=f(x)f(y) \quad \text{quels que soient} \quad x, y \in \mathrm{K}, \quad f(1)=1.$$

*Exemple* 7. L'application canonique de $\mathbf{Z}$ sur $\mathbf{Z}/p\mathbf{Z}$ est un homomorphisme d'anneaux (et du reste la structure d'anneau de $\mathbf{Z}/p\mathbf{Z}$ a été choisie de telle sorte qu'il en soit ainsi).

*Exemple* 8. Soient X un ensemble, K un anneau, et L l'anneau des applications de X dans K (*Exemple* 3); alors, pour tout $x \in \mathrm{X}$, l'application

$$f \mapsto f(x)$$

de L dans K est un homomorphisme.

Les propriétés des homomorphismes d'anneaux sont analogues à celles des homomorphismes de groupes (§ 7, n° 8 et 9). Étant donnés deux homomorphismes d'anneaux

$$f : \mathrm{K} \to \mathrm{L}, \qquad g : \mathrm{L} \to \mathrm{M},$$

l'application composée $g \circ f$ est encore un homomorphisme.

Si un homomorphisme $f : \mathrm{K} \to \mathrm{L}$ est bijectif, l'application réciproque est encore un homomorphisme; on dit alors que $f$ est un **isomorphisme**, et on dit que deux anneaux K et L sont **isomorphes** s'il existe un isomorphisme de K sur L; la relation

K et L sont isomorphes

est une relation d'équivalence entre anneaux.

Soit $f : \mathrm{K} \to \mathrm{L}$ un homomorphisme d'anneaux. On appelle **noyau** de $f$ l'ensemble, noté

$$\mathrm{Ker}(f),$$

des $x \in \mathrm{K}$ tels que $f(x) = 0$ (c'est donc le noyau de $f$ quand on regarde $f$ comme un homomorphisme du groupe additif K dans le groupe additif L). L'homomorphisme $f$ est injectif si et seulement si $\mathrm{Ker}(f) = \{0\}$.

Les relations

$$f(x-y)=f(x)-f(y), \qquad f(axb)=f(a)f(x)f(b)$$

montrent immédiatement que le noyau I d'un homomorphisme d'un anneau K dans un autre vérifie les deux conditions suivantes :

(i) : I *est un sous-groupe du groupe additif* K;

(ii) : *on a la relation* $axb \in \mathrm{I}$ *quels que soient* $a, b \in \mathrm{K}$ *et* $x \in \mathrm{I}$.

Une partie I d'un anneau K s'appelle un **idéal bilatère** lorsqu'elle vérifie les conditions (i) et (ii) ci-dessus.



*Remarque* 4. Une partie I d'un anneau K est appelée un **idéal à gauche de K** si c'est un sous-groupe de K et si l'on a $ax \in \mathrm{I}$ quels que soient $a \in \mathrm{K}$ et $x \in \mathrm{I}$ (autrement dit si les **multiples à gauche** de tout $x \in \mathrm{I}$ sont tous dans I); il revient au même de dire que I est une partie de K, non vide, qui possède la propriété suivante : on a

$$ux + vy \in \mathrm{I} \quad \text{quels que soient } u, v \in \mathrm{K} \text{ et } x, y \in \mathrm{I}.$$

On définirait de même les **idéaux à droite** de K comme étant les parties non vides I de K telles que l'on ait

$$xu + yv \in \mathrm{I} \quad \text{quels que soient } u, v \in \mathrm{K} \text{ et } x, y \in \mathrm{I}.$$

Les idéaux bilatères sont évidemment les parties de K qui sont à la fois des idéaux à gauche et des idéaux à droite.

Lorsque K est *commutatif*, les notions d'idéal à gauche, d'idéal à droite et d'idéal bilatère sont évidemment identiques; on dit alors simplement **idéal** au lieu d'idéal à gauche, ou à droite, ou bilatère.

*Exemple* 9. Si K est un corps, les seuls idéaux à gauche de K sont $\{0\}$ et K lui-même. Si en effet un idéal à gauche I contient un élément $a$ non nul, donc inversible, il contiendra $a^{-1}a = 1$, donc aussi $u.1 = u$ pour tout $u \in \mathrm{K}$, d'où $\mathrm{I} = \mathrm{K}$.

Le lecteur démontrera, à titre d'exercice, que lorsque $1 \neq 0$ cette propriété caractérise les anneaux qui sont des corps.

*Exemple* 10. Soit K un anneau commutatif; pour tout $x \in \mathrm{K}$, notons $x\mathrm{K}$ l'ensemble des **multiples de $x$ dans K**, i.e. des éléments de la forme $ux$, $u \in \mathrm{K}$. Cet ensemble est alors un idéal de K (les idéaux de ce type sont appelés les **idéaux principaux** de K).

On appelle **anneau principal** tout anneau d'intégrité commutatif dont tous les idéaux sont principaux. L'anneau $\mathbf{Z}$ est principal (un idéal de $\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$, donc est de la forme $n\mathbf{Z}$ d'après le § 7, *Exemple* 8). On verra au § 31 (que le lecteur peut, s'il le désire, étudier dès maintenant) que les propriétés de divisibilité des entiers rationnels s'étendent aux éléments d'un anneau principal.

Il existe des anneaux non principaux — l'exemple le plus simple est le sous-anneau de $\mathbf{R}$ formé des nombres de la forme

$$x + y\sqrt{10} \qquad \text{avec} \qquad x, y \in \mathbf{Z}.$$

L'étude de cet anneau et d'anneaux analogues mais plus compliqués (les anneaux d'entiers algébriques) a conduit les mathématiciens du siècle dernier — en premier lieu Dedekind — à inventer la notion d'idéal qui, par la suite, s'est révélée indispensable dans de nombreuses autres branches des Mathématiques.

# 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.** 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 l 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 $u^3(x) = 0$ pour tout $x \in \mathrm{K}$, et que si $a^3 = 0$ on a $u^5(x) = 0$ po tout $x \in \mathrm{K}$. Montrer d'une manière générale que, si $a$ est nilpotent, il existe un entier $q$ 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 $u, v \in$ sont unipotents et commutent, alors $uv$ est aussi unipotent. Montrer que tout élément unip tent 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 d §§ 12, 13 et 14 et l'*Exercice* 19 du § 19. En Analyse, la théorie des *développements limités* four aussi des exemples d'éléments nilpotents : considérer l'anneau des fonctions $f(t)$ d'une variab 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'anne quotient a évidemment des éléments nilpotents non nuls — par exemple l'image dans ce qu tient de la fonction $t$].

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

**q** **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

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

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 :

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

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

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

impliquent les relations

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

*c*) On note K/I l'ensemble quotient de K par la relation d'équivalence considérée, et $\theta$ 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 $\theta$ 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

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

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

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

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

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

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

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

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 $q_1, \ldots, q_h$ 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 $\mathrm{I} + \mathrm{J}$ (**somme** des idéaux I et J) l'ensemble des éléments de K qui peuvent se mettre sous la forme $x + y$ avec $x \in \mathrm{I}$ et $y \in \mathrm{J}$, et IJ (**produit** des deux idéaux I et J) l'ensemble des $z \in \mathrm{K}$ possédant la propriété suivante : il existe un entier $n \geqslant 1$, des éléments $x_1, \ldots, x_n$ de I, et des éléments $y_1, \ldots, y_n$ de J, tels que $z = x_1y_1 + \cdots + x_ny_n$.

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

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

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

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

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

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

¶ 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 $\mathrm{I}, \mathrm{J}_1, \ldots, \mathrm{J}_r$ des idéaux de K; on suppose I et $\mathrm{J}_k$ étrangers pour $1 \leqslant k \leqslant r$. Montrer que I est étranger au produit $\mathrm{J}_1 \cdots \mathrm{J}_r$.

*e*) Soient $\mathrm{J}_1, \ldots, \mathrm{J}_r$ des idéaux deux à deux étrangers. Montrer que

$$\mathrm{J}_1 \cdots \mathrm{J}_r = \mathrm{J}_1 \cap \cdots \cap \mathrm{J}_r.$$

*f*) Soient $\mathrm{J}_1, \ldots, \mathrm{J}_r$ des idéaux deux à deux étrangers. Montrer que, quels que soient $a_1, \ldots, a_r \in \mathrm{K}$ on peut trouver un $x \in \mathrm{K}$ tel que l'on ait

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

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

¶ **11.** Soient $\mathrm{I}_1, \ldots, \mathrm{I}_r$ des idéaux d'un anneau commutatif K. Si un idéal **premier** (*Exercice* 7, (*e*)) de K contient le produit $\mathrm{I}_1 \ldots \mathrm{I}_r$ il contient l'un au moins des idéaux $\mathrm{I}_1, \ldots, \mathrm{I}_r$.
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 $x \in \mathrm{K}$ tels que l'on ait

$$x^n \in \mathrm{I}$$

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

$$\sqrt{\mathrm{I}}$$

(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 $\mathrm{I} = \{0\}$? 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 :

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

*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 $\mathrm{I} \neq \mathrm{K}$ et si, quels que soient les éléments $x, y$ de K tels que l'on ait

$$xy \in \mathrm{I}, \qquad x \notin \mathrm{I},$$

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

$$y^n \in \mathrm{I}.$$

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

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

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 $\alpha$ un idéal $I_\alpha$ de telle sorte que, pour $\alpha < \beta$, l'idéal $I_\alpha$ soit *strictement* contenu dans $I_\beta$ — la construction est évidemment facile pour les $\alpha$ 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).