§ 4. Relations d'équivalence

1. Relations d'équivalence

Soit R une relation faisant intervenir deux variables x, y. On dit que c'est une **relation d'équivalence** lorsque les conditions suivantes sont remplies :

a) *la relation* $R\{x, x\}$ *est vraie pour tout* x;

b) *la relation* $R\{x, y\}$ *implique la relation* $R\{y, x\}$;

c) *les relations* $R\{x, y\}$ *et* $R\{y, z\}$ *impliquent la relation* $R\{x, z\}$.

Il est clair par exemple que la relation $x = y$ est une relation d'équivalence.

Une notion voisine de la précédente, et plus utile dans la pratique, est celle de **relation d'équivalence sur un ensemble** E; on appelle ainsi une relation $R\{x, y\}$ faisant intervenir deux variables x, y, et vérifiant les conditions suivantes :

(R 0) : *la relation* $R\{x, y\}$ *implique* $x \in E$ *et* $y \in E$;
(R 1) : *la relation* $R\{x, x\}$ *est vraie pour tout* $x \in E$;
(R 2) : *la relation* $R\{x, y\}$ *implique* $R\{y, x\}$;
(R 3) : *les relations* $R\{x, y\}$ *et* $R\{y, z\}$ *impliquent la relation* $R\{x, z\}$.

Si R est une relation d'équivalence sur un ensemble E, on appelle **graphe de R** l'ensemble $G \subset E \times E$ des couples $(x, y) \in E \times E$ tels que la relation $R\{x, y\}$ soit vraie; la relation $R\{x, y\}$ est alors équivalente à $(x, y) \in G$, et la condition (R 1) signifie que G contient la *diagonale* du produit $E \times E$.

Pour construire un exemple (qui, on le montrera plus loin, conduit à *toutes* les relations d'équivalence sur un ensemble E), considérons une application f de E dans un ensemble quelconque M, et prenons pour $R\{x, y\}$ la relation

$$f(x) = f(y);$$

on obtient évidemment une relation d'équivalence sur E, appelée la **relation d'équivalence associée à l'application** f.

Donnons maintenant quelques autres exemples.

Exemple 1. Pour tout ensemble E, la diagonale de $E \times E$ (§ 2, n° 6, *Exemple* 2) est le graphe d'une relation d'équivalence sur E — à savoir de la relation

$$x = y.$$

Exemple 2. Pour tout ensemble E, l'ensemble $E \times E$ est le graphe d'une relation d'équivalence sur E — à savoir la relation $(x, y) \in E \times E$; dans ce cas la relation $R\{x, y\}$ est donc vraie pour tout $x \in E$ et tout $y \in E$.

Exemple 3. On dit qu'un ensemble X est **équipotent** à un ensemble Y s'il existe une bijection de X sur Y. La relation « X est équipotent à Y » est une relation d'équivalence; en effet X est équipotent à X (considérer la bijection j_X, application identique); si X est équipotent à Y, alors Y est équipotent à X (car si f est une bijection de X sur Y, alors f^{-1} est une bijection de Y sur X); enfin si X est équipotent à Y et si Y est équipotent à Z, alors X est équipotent à Z (car si f est une bijection de X sur Y, et g une bijection de Y sur Z, alors $g \circ f$ est une bijection de X sur Z, en vertu du § 2, Théorème 7). Voir le § suivant.

Exemple 4. Soit **Z** l'ensemble des **entiers rationnels,** i.e. des nombres entiers positifs ou négatifs..., -2, -1, 0, 1, 2,.... Choisissons un entier $p \geqslant 1$ et considérons la relation

$$p \text{ divise } x - y$$

entre deux éléments x et y de **Z**; c'est une relation d'équivalence sur **Z**. En effet, il est clair que la relation « p divise $x - x$ » est toujours vraie; la relation « p divise $x - y$ » implique évidemment la relation « p divise $y - x$ »; enfin, si p divise $x - y$ et $y - z$, il est clair que p divise $x - z = (x - y) + (y - z)$.

La relation d'équivalence ainsi obtenue sur **Z** s'appelle la **congruence modulo** p, et elle se note classiquement

$$x \equiv y \pmod{p},$$

ce qui se lit « x est congru à y modulo p »; cela signifie que x et y ne diffèrent que d'un multiple de p. La théorie des congruences joue un rôle fondamental en Arithmétique depuis deux siècles. es.

Exemple 5. On obtient sur l'ensemble **R** des nombres réels une relation d'équivalence en écrivant

$$\text{il existe un entier } n \text{ tel que } x - y = 2\pi n;$$

on l'appelle la **congruence modulo** 2π. Cette relation d'équivalence est à la base de la définition *mathématique* des angles.

Exemple 6. Prenons pour E l'ensemble des couples (p, q) avec $p, q \in \mathbf{Z}$ et $q \neq 0$, et, pour $x = (p, q), y = (p', q')$, notons $R\{x, y\}$ la relation

$$pq' = p'q;$$

on obtient ainsi une relation d'équivalence sur E (ce n'est pas évident, mais on peut le démontrer à l'aide de quelques calculs élémentaires). Cette relation d'équivalence est à la base de la définition *mathématique* des nombres rationnels à partir des nombres entiers, comme on le verra plus tard (§ 29). On conseille au lecteur de vérifier lui-même, à titre d'exercice, que R est bien une relation d'équivalence sur l'ensemble E considéré.

Exemple 7. Prenons pour E l'ensemble des points de l'espace usuel et, une droite D étant choisie une fois pour toutes, considérons la relation

$$\text{il existe une droite parallèle à D passant par } x \text{ et } y;$$

on obtient alors une relation d'équivalence sur E.

Exemple 8. On prend pour E l'ensemble des triangles dans le plan, et pour $R\{x, y\}$ la relation

$$\text{les triangles } x \text{ et } y \text{ sont égaux,}$$

l'égalité des triangles étant définie (sic) comme en Géométrie élémentaire, i.e. en exigeant qu'il existe un déplacement qui transforme x en y (ce qui suppose qu'on sait ce qu'est un déplacement...). On obtient alors une relation d'équivalence dans E.

Soit R une relation d'équivalence sur un ensemble E; au lieu d'écrire $R\{x, y\}$, nous écrirons le plus souvent dans ce qui suit

$$x \equiv y \pmod{R},$$

notation inspirée de celle de l'Exemple 4. On a donc les propriétés suivantes : la relation

$$x \equiv x \pmod{R}$$

est vraie pour tout $x \in E$; la relation

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

implique (donc, par symétrie, est équivalente à) la relation

$$y \equiv x \pmod{R};$$

enfin, les relations

$$x \equiv y \pmod{R} \qquad \text{et} \qquad y \equiv z \pmod{R}$$

impliquent la relation

$$x \equiv z \pmod{R}.$$

2. *Quotient d'un ensemble par une relation d'équivalence*

Nous allons démontrer un résultat qui indique comment on obtient toutes les relations d'équivalence sur un ensemble :

THÉORÈME 1. *Soit* R *une relation d'équivalence sur un ensemble* E. *Il existe un ensemble* M *et une application* $f : E \to M$ *tels que les relations*

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

Exemple 2. Pour tout ensemble E, l'ensemble $E \times E$ est le graphe d'une relation d'équivalence sur E — à savoir la relation $(x, y) \in E \times E$; dans ce cas la relation $R\{x, y\}$ est donc vraie pour tout $x \in E$ et tout $y \in E$.

Exemple 3. On dit qu'un ensemble X est **équipotent** à un ensemble Y s'il existe une bijection de X sur Y. La relation « X est équipotent à Y » est une relation d'équivalence; en effet X est équipotent à X (considérer la bijection j_X, application identique); si X est équipotent à Y, alors Y est équipotent à X (car si f est une bijection de X sur Y, alors f^{-1} est une bijection de Y sur X); enfin si X est équipotent à Y et si Y est équipotent à Z, alors X est équipotent à Z (car si f est une bijection de X sur Y, et g une bijection de Y sur Z, alors $g \circ f$ est une bijection de X sur Z, en vertu du § 2, Théorème 7). Voir le § suivant.

Exemple 4. Soit **Z** l'ensemble des **entiers rationnels**, i.e. des nombres entiers positifs ou négatifs..., -2, -1, 0, 1, 2,.... Choisissons un entier $p \geqslant 1$ et considérons la relation

$$p \text{ divise } x - y$$

entre deux éléments x et y de **Z**; c'est une relation d'équivalence sur **Z**. En effet, il est clair que la relation « p divise $x - x$ » est toujours vraie; la relation « p divise $x - y$ » implique évidemment la relation « p divise $y - x$ »; enfin, si p divise $x - y$ et $y - z$, il est clair que p divise $x - z = (x - y) + (y - z)$.

La relation d'équivalence ainsi obtenue sur **Z** s'appelle la **congruence modulo** p, et elle se note classiquement

$$x \equiv y \pmod{p},$$

ce qui se lit « x est congru à y modulo p »; cela signifie que x et y ne diffèrent que d'un multiple de p. La théorie des congruences joue un rôle fondamental en Arithmétique depuis deux siècles. es.

Exemple 5. On obtient sur l'ensemble **R** des nombres réels une relation d'équivalence en écrivant

$$\text{il existe un entier } n \text{ tel que } x - y = 2\pi n;$$

on l'appelle la **congruence modulo** 2π. Cette relation d'équivalence est à la base de la définition *mathématique* des angles.

Exemple 6. Prenons pour E l'ensemble des couples (p, q) avec $p, q \in \mathbf{Z}$ et $q \neq 0$, et, pour $x = (p, q), y = (p', q')$, notons $R\{x, y\}$ la relation

$$pq' = p'q;$$

on obtient ainsi une relation d'équivalence sur E (ce n'est pas évident, mais on peut le démontrer à l'aide de quelques calculs élémentaires). Cette relation d'équivalence est à la base de la définition *mathématique* des nombres rationnels à partir des nombres entiers, comme on le verra plus tard (§ 29). On conseille au lecteur de vérifier lui-même, à titre d'exercice, que R est bien une relation d'équivalence sur l'ensemble E considéré.

Exemple 7. Prenons pour E l'ensemble des points de l'espace usuel et, une droite D étant choisie une fois pour toutes, considérons la relation

$$\text{il existe une droite parallèle à D passant par } x \text{ et } y;$$

on obtient alors une relation d'équivalence sur E.

Exemple 8. On prend pour E l'ensemble des triangles dans le plan, et pour $R\{x, y\}$ la relation

$$\text{les triangles } x \text{ et } y \text{ sont égaux,}$$

l'égalité des triangles étant définie (sic) comme en Géométrie élémentaire, i.e. en exigeant qu'il existe un déplacement qui transforme x en y (ce qui suppose qu'on sait ce qu'est un déplacement...). On obtient alors une relation d'équivalence dans E.

Soit R une relation d'équivalence sur un ensemble E; au lieu d'écrire $R\{x, y\}$, nous écrirons le plus souvent dans ce qui suit

$$x \equiv y \pmod{R},$$

notation inspirée de celle de l'Exemple 4. On a donc les propriétés suivantes : la relation

$$x \equiv x \pmod{R}$$

est vraie pour tout $x \in E$; la relation

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

implique (donc, par symétrie, est équivalente à) la relation

$$y \equiv x \pmod{R};$$

enfin, les relations

$$x \equiv y \pmod{R} \qquad \text{et} \qquad y \equiv z \pmod{R}$$

impliquent la relation

$$x \equiv z \pmod{R}.$$

2. *Quotient d'un ensemble par une relation d'équivalence*

Nous allons démontrer un résultat qui indique comment on obtient toutes les relations d'équivalence sur un ensemble :

THÉORÈME 1. *Soit* R *une relation d'équivalence sur un ensemble* E. *Il existe un ensemble* M *et une application* $f : E \to M$ *tels que les relations*

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

et

$$f(x) = f(y)$$

soient équivalentes.

On va non seulement démontrer l'existence de f et de M, mais construire explicitement un ensemble M et une application f satisfaisant à la condition énoncée.

Étant donné un $x \in E$, appelons **classe de x modulo R** l'ensemble $F_x \subset E$ formé des $y \in E$ tels que la relation

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

soit vraie — de sorte que les relations

$$x \equiv y \pmod{R}, \qquad y \in F_x$$

sont équivalentes. On va montrer que, pour $x, y \in E$, *les relations*

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

et

$$F_x = F_y$$

sont équivalentes.

Supposons en effet $x \equiv y \pmod{R}$; alors la relation $z \in F_y$, qui signifie $y \equiv z \pmod{R}$, implique $x \equiv z \pmod{R}$, donc $z \in F_x$; par suite, la relation $x \equiv y \pmod{R}$ implique $F_y \subset F_x$, donc aussi $F_x \subset F_y$, donc $F_x = F_y$. Inversement, supposons $F_x = F_y$; comme on a toujours $y \equiv y \pmod{R}$, et donc $y \in F_y$, il vient $y \in F_x$, donc $x \equiv y \pmod{R}$, et notre assertion est démontrée.

Nous pouvons maintenant démontrer le Théorème 1. Dans l'ensemble $\mathfrak{P}(E)$ des parties de E, considérons l'ensemble formé des parties F de E telles que l'on ait

$$F = F_x$$

pour au moins un $x \in E$ — c'est donc l'ensemble des classes d'équivalence des divers éléments de E; cet ensemble se note E/R et s'appelle le **quotient de l'ensemble E par la relation d'équivalence R**; définissons maintenant une application

$$f : E \to E/R$$

en posant

$$f(x) = F_x$$

i.e. en associant à chaque $x \in E$ sa classe modulo R; on a vu plus haut que la relation

$$x \equiv y \pmod{R},$$

équivaut à $F_x = F_y$; mais ceci s'écrit encore

$$f(x) = f(y),$$

et le Théorème est démontré.

L'application f qu'on vient de définir s'appelle **l'application canonique de E sur E/R**; elle est évidemment *surjective*, par construction même de E/R.

Notons que les classes F_x possèdent deux propriétés importantes : *la réunion des F_x est* E *tout entier* (en vertu du fait qu'on a $x \in F_x$ pour tout $x \in E$); d'autre part, *deux classes F_x et F_y quelconques sont ou bien identiques ou bien disjointes*, car si $F_x \cap F_y$ contient au moins un élément z, on a les relations

$$x \equiv z \pmod{R} \qquad \text{et} \qquad y \equiv z \pmod{R}$$

d'où, en faisant usage de (R 2) et (R 3), la relation

$$x \equiv y \pmod{R},$$

laquelle entraîne $F_x = F_y$ comme on l'a vu dans la démonstration du Théorème 1.

Remarque 1. La méthode de démonstration du Théorème 1 repose essentiellement sur la construction d'une application de l'ensemble E dans l'ensemble $\mathfrak{P}(E)$ des parties de E, à savoir l'application $x \to F_x$. On ne pourrait évidemment pas effectuer ce genre de construction si l'on ne connaissait que les fonctions classiques (d'une variable réelle, à valeurs réelles), et c'est ce genre de démonstration qui montre la nécessité de considérer des fonctions dont les ensembles de départ et d'arrivée sont arbitraires.

Notons d'autre part que la méthode de construction de E/R, qui pourra sembler étrange au débutant, s'utilise cependant dans la vie de tous les jours, comme le montre l'exemple (non mathématique !) que voici : on prend pour E la collection des hommes, et pour R la relation « x et y sont compatriotes »; on obtient ainsi évidemment une relation d'équivalence sur E. Pour un $x \in E$, la classe F_x est l'ensemble de tous les compatriotes de x; autrement dit c'est la nation à laquelle x appartient; par suite, l'ensemble quotient E/R est ici la collection des diverses nations existantes, et l'application canonique de E sur E/R consiste à associer à chaque homme la nation à laquelle il appartient...

Donnons quelques exemples de construction d'un ensemble quotient.

Exemple 9. Considérons sur **Z** la relation d'équivalence de l'*Exemple* 4 (congruence modulo p); pour tout $x \in \mathbf{Z}$, la classe F_x se compose évidemment des entiers de la forme $x + np$, où n est un entier arbitraire; ces classes sont en nombre p exactement (on suppose $p \geqslant 1$). En effet, pour tout $x \in \mathbf{Z}$ on peut écrire (« division avec reste de x par p »)

$$x = np + r \qquad (0 \leqslant r < p),$$

et la connaissance du reste r de la division de x par p détermine évidemment la classe F_x — autrement dit, toute classe modulo p est l'une des classes

$$F_0, \quad F_1, \quad \cdots, \quad F_{p-1};$$

ces p classes sont de plus deux à deux distinctes, car si des entiers r et r' compris entre 0 et $p - 1$ sont congrus modulo p, ils sont évidemment égaux.

On voit donc bien qu'ici l'ensemble E/R, qu'on désigne par la notation

$$\mathbf{Z}/p\mathbf{Z},$$

comporte exactement p éléments, éléments qu'on appelle les **entiers modulo** p. Un entier modulo p est donc un ensemble d'entiers ordinaires, à savoir l'ensemble de tous les entiers se déduisant d'un entier x donné par addition d'un multiple quelconque de p; on dit alors que l'entier x est un **représentant** de l'entier modulo p considéré. Tout entier modulo p admet un et un seul représentant compris entre 0 et $p-1$, ce qui permet de numéroter les entiers modulo p à l'aide des entiers $0, 1, \ldots, p-1$ qui les représentent. Par exemple, on représente les éléments de $\mathbf{Z}/6\mathbf{Z}$ à l'aide des entiers 0, 1, 2, 3, 4, 5; quand on parle de l'élément 4 de $\mathbf{Z}/6\mathbf{Z}$, cela signifie qu'on parle de « la classe de l'entier 4 pour la congruence modulo 6 », ou encore de « l'ensemble des nombres de la forme $6n+4$ ». Avec ces conventions de langage, *l'application canonique de* $\mathbf{Z}$ *sur* $\mathbf{Z}/p\mathbf{Z}$ *consiste à associer à chaque entier rationnel le reste de sa division par* p.

Exemple 10. Dans le cas de l'*Exemple* 5 du n° 1, l'ensemble quotient se note

$$\mathbf{R}/2\pi\mathbf{Z},$$

et ses éléments s'appellent les **nombres réels modulo** 2π. Un nombre réel modulo 2π est donc un ensemble de nombres réels — à savoir tous ceux qui se déduisent d'un nombre réel donné par addition d'un multiple quelconque de 2π. Il est clair que la mesure d'un angle est précisément un nombre réel modulo 2π (et non pas un nombre réel usuel).

Exemple 11. Dans l'*Exemple* 7 du n° 1, les classes sont les droites parallèles à D, et l'ensemble quotient est l'ensemble des droites parallèles à D.

3. *Fonctions définies sur un ensemble quotient* (*)

Le résultat que voici est très utile :

THÉORÈME 2. *Soient* E *un ensemble,* R *une relation d'équivalence sur* E, *p l'application canonique de* E *sur* E/R, *et f une application de* E *dans un ensemble* X. *Les propriétés suivantes sont équivalentes:*

a) la relation $x \equiv y \pmod{R}$ *implique* $f(x) = f(y)$;

b) il existe une application

$$\bar{f}\colon \mathrm{E/R} \to \mathrm{X}$$

telle que $f = \bar{f} \circ p$.

Si ces conditions sont vérifiées, l'application $\bar{f}$ *est unique; pour qu'elle soit injective il faut et il suffit que les relations* $x \equiv y \pmod{R}$ *et* $f(x) = f(y)$ *soient équivalentes; pour qu'elle soit surjective il faut et il suffit que f le soit.*

D'après le Théorème 1 du § 2, une condition nécessaire et suffisante pour qu'il

(*) **Les résultats de ce n° ne seront pas indispensables avant le § 29.**

existe une application $\bar{f}$ satisfaisant à la condition de l'énoncé est que la relation $p(x) = p(y)$ implique la relation $f(x) \equiv f(y)$; or la relation $p(x) = p(y)$ équivaut à la relation $x \equiv y \pmod{R}$; les propriétés *a*) et *b*) sont donc bien équivalentes.

L'unicité de $\bar{f}$ provient de ce que p est surjective; supposons en effet trouvées deux applications g et h telles que $f = g \circ p = h \circ p$; pour tout $x \in \mathrm{E}$ on a alors $g(p(x)) = h(p(x))$; donc g et h coïncident sur l'image $p(\mathrm{E})$, i.e. sur E/R, d'où $g = h$ comme annoncé.

On a $f(\mathrm{E}) = \bar{f}(p(\mathrm{E})) = \bar{f}(\mathrm{E/R})$, de sorte que f est surjective si et seulement si $\bar{f}$ l'est. Pour que l'application f soit injective, il faut et il suffit, puisque tout élément de E/R est de la forme $p(z)$, que la relation

$$\bar{f}(p(x)) = \bar{f}(p(y)) \quad \text{implique} \quad p(x) = p(y),$$

autrement dit que $f(x) = f(y)$ implique $x \equiv y \pmod{R}$, ce qui achève la démonstration.

Le résultat suivant, analogue au Théorème précédent mais un peu plus compliqué, est fondamental quand on désire définir des opérations algébriques sur les éléments d'un ensemble quotient :

THÉORÈME 3. *Soient* X, Y, Z *trois ensembles,* R, S, T *des relations d'équivalence sur ces ensembles, et f une application de* $\mathrm{X} \times \mathrm{Y}$ *dans* Z. *Désignons par* $x \to \bar{x}$, $y \to \bar{y}$ *et* $z \to \bar{z}$ *les applications canoniques de* X, Y *et* Z *sur* X/R, Y/S *et* Z/T. *Les assertions suivantes sont équivalentes:*

a) les relations

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

impliquent la relation

$$f(x', y') \equiv f(x'', y'') \pmod{T};$$

b) il existe une application

$$\bar{f} : (\mathrm{X/R}) \times (\mathrm{Y/S}) \to \mathrm{Z/T}$$

telle que l'on ait

$$\bar{f}(\bar{x}, \bar{y}) = \overline{f(x, y)}$$

quels que soient $x \in \mathrm{X}$ *et* $y \in \mathrm{Y}$.

Si ces conditions sont vérifiées, l'application $\bar{f}$ *est unique.*

Considérons l'application $u : \mathrm{X} \times \mathrm{Y} \to \mathrm{Z/T}$ donnée par

$$u(x, y) = \overline{f(x, y)};$$

considérons d'autre part l'application $v : \mathrm{X} \times \mathrm{Y} \to (\mathrm{X/R}) \times (\mathrm{Y/S})$ donnée par

$$v(x, y) = (\bar{x}, \bar{y});$$

tout revient à construire une application $\bar{f}\colon (\mathrm{X/R}) \times (\mathrm{Y/S}) \to \mathrm{Z/T}$ telle que l'on

ait $u = \overline{f} \circ v$; pour cela, on applique le Théorème 1 du § 2 : $\overline{f}$ existe si et seulement si la relation

$$v(x', y') = v(x'', y'') \qquad \text{implique} \qquad u(x', y') = u(x'', y'');$$

or la première relation s'écrit $\overline{x}' = \overline{x}''$ et $\overline{y}' = \overline{y}''$, i.e.

$$x' \equiv x'' \pmod{R} \qquad \text{et} \qquad y' \equiv y'' \pmod{S},$$

et la seconde

$$f(x', y') \equiv f(x'', y'') \pmod{T};$$

le Théorème 1 du § 2 montre donc bien l'équivalence des conditions *a*) et *b*) de l'énoncé.

S'il existe une application $\overline{f}$ possédant la propriété cherchée, cette application est unique parce que v est évidemment surjective. Ceci termine la démonstration.

Exemple 12. Prenons $X = Y = Z = \mathbf{Z}$, ensemble des entiers rationnels, et pour R, S et T la relation de congruence modulo p, où p est un entier non nul donné. Considérons les applications f, $g : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ données par

$$f(x, y) = x + y, \qquad g(x, y) = xy;$$

la condition *a*) du Théorème 3 est vérifiée par f et par g; pour le voir, on doit vérifier que les relations

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

impliquent

$$x' + y' \equiv x'' + y'' \pmod{p} \qquad \text{et} \qquad x'y' \equiv x''y'' \pmod{p},$$

ce qui est clair en vertu des identités

$$(x' + y') - (x'' + y'') = (x' - x'') + (y' - y''),$$
$$x'y' - x''y'' = (x' - x'')y' + x''(y' - y'').$$

On peut donc appliquer le Théorème 3 à f et à g, autrement dit il existe des applications

$$\overline{f}, \overline{g} : (\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z}) \to \mathbf{Z}/p\mathbf{Z}$$

qui sont caractérisées par les propriétés suivantes : étant donnés des éléments ξ et η de $\mathbf{Z}/p\mathbf{Z}$, représentés par des entiers rationnels x et y (de sorte qu'on a

$$\xi = \overline{x}, \qquad \eta = \overline{y}$$

avec les notations du Théorème 3), alors $\overline{f}(\xi, \eta)$ et $\overline{g}(\xi, \eta)$ sont représentés par $x + y$ et xy, dont les classes modulo p ne dépendent donc que des classes de x et y modulo p, et non du choix de x et y dans les classes ξ et η considérées.

Dans la pratique, on écrit

$$\overline{f}(\xi, \eta) = \xi + \eta, \qquad \overline{g}(\xi, \eta) = \xi\eta,$$

et on dit que $\xi + \eta$ et $\xi\eta$ sont la **somme** et le **produit** des éléments ξ et η de $\mathbf{Z}/p\mathbf{Z}$. Si l'on désigne par θ l'application canonique de $\mathbf{Z}$ sur $\mathbf{Z}/p\mathbf{Z}$, on voit donc que l'addition et la multiplication des entiers modulo p sont définies de telle sorte que l'on ait les relations

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

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

Pratiquement, l'addition et la multiplication dans $\mathbf{Z}/p\mathbf{Z}$ se calculent comme suit : on représente les entiers modulo p par les entiers ordinaires $0, 1, \ldots, p - 1$ (cf. *Exemple* 9); si des classes modulo p sont représentées par des entiers x et y (compris entre 0 et $p - 1$), la somme et le produit de ces classes seront alors représentées par les restes des divisions de $x + y$ et xy par p.

Voici par exemple les « tables d'addition et de multiplication » des entiers modulo 5 :

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Une formule telle que $2 \cdot 3 = 1$ signifie bien entendu que

$$2 \cdot 3 \equiv 1 \pmod{5}.$$

Le cas le plus simple (à part $p = 1$) est celui où $p = 2$; on a alors *deux* classes, qu'il s'impose d'appeler « pair » et « impair », et les règles de calcul sont alors données par les formules suivantes :

pair + pair = pair	pair × pair = pair
pair + impair = impair	pair × impair = impair
impair + pair = impair	impair × pair = pair
impair + impair = pair	impair × impair = impair.

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. 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

$$\text{les points O, P′ et P″ sont alignés.}$$

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 $\mathbf{R}$ dans $\mathbf{R}$ (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 $\mathbf{R}$ dans $\mathbf{R}$; 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.]