§ 9. Nombres complexes

1. Racines carrées

Soit K un anneau commutatif. On dit qu'un élément d de K est un **carré dans** K s'il existe un $x \in K$ tel que

$$x^2 = d;$$

on dit alors que x est une **racine carrée** de d dans K. Il est clair que si x est une racine carrée de d dans K, il en est de même de $-x$; si de plus l'anneau K est intègre, d ne peut admettre plus de deux racines carrées dans K, car la relation $x^2 = y^2$, qui s'écrit dans tous les cas sous la forme $(x-y)\ (x+y) = 0$, implique soit $y = x$ soit $y = -x$ lorsque l'anneau K est intègre.

Il peut naturellement arriver qu'un élément d d'un anneau commutatif K ne soit pas un carré dans K : si K est le corps $\mathbf{R}$ des nombres réels, d est un carré dans K si et seulement si $d \geqslant 0$. Dans le corps $\mathbf{Q}$ des nombres rationnels, 2 n'est pas un carré (cependant, 2 est un carré dans le corps $\mathbf{R}$ des nombres réels).

On est ainsi conduit à examiner le problème suivant : *soient* K *un anneau commutatif et d un élément de* K *qui n'est pas un carré dans* K*; peut-on construire un anneau commutatif* L *possédant les propriétés suivantes :* K *est un sous-anneau de* L, *et d est un carré dans* L*?*

C'est la résolution de ce problème lorsque $K = \mathbf{R}$ et $d = -1$ qui, historiquement, a conduit à l'invention des « nombres complexes » que nous définirons dans la suite de ce §. Pour comprendre vraiment la construction de ces « nombres », il est indispensable (et il n'est pas plus difficile) d'étudier le problème général que nous venons d'énoncer.

2. Préliminaires

Soit donc d un élément d'un anneau commutatif K; dans ce n° nous supposerons résolu le problème énoncé au n° précédent, et désignerons par L un anneau commutatif dont K soit un sous-anneau, et par ω une racine carrée de d dans L.

Désignons alors par L′ l'ensemble des éléments z de L possédant la propriété

suivante : il existe $x, y \in K$ tels que

$$z = x + \omega y. \tag{1}$$

Alors, L′ *est un sous-anneau de* L *contenant* K, *et dans lequel d possède une racine carrée.*

Il est en effet clair que L′ contient K (faire $y = 0$ dans la relation précédente) ainsi que ω (faire $x = 0$ et $y = 1$); il reste donc à faire voir que L′ est un sous-anneau de L; comme L′, contenant K, contient -1, il suffit pour cela de montrer que si L′ contient deux éléments de L, il contient aussi leur somme et leur produit; mais cela résulte aussitôt des formules

$$(x' + \omega y') + (x'' + \omega y'') = (x' + x'') + \omega(y' + y''), \tag{2}$$
$$(x' + \omega y').(x'' + \omega y'') = (x'x'' + dy'y'') + \omega(x'y'' + x''y'), \tag{3}$$

évidentes compte-tenu de la relation

$$\omega^2 = d. \tag{4}$$

Le résultat précédent montre que, si le problème posé admet une solution, autrement dit si l'on a construit un sur-anneau commutatif L de K et un $\omega \in L$ vérifiant (4), alors on peut même construire L de telle sorte que *tout* élément de L puisse se mettre sous la forme (1), avec $x, y \in K$. Autrement dit, si l'on introduit l'application $f : K \times K \to L$ donnée par

$$f(x, y) = x + \omega y,$$

on peut supposer *f surjective*.

Remarque 1. Si K est un corps et si d n'est pas un carré dans K, l'application f est en outre *injective*; en effet, la relation $x' + \omega y' = x'' + \omega y''$ s'écrit

$$x + \omega y = 0 \quad \text{avec} \quad x = x' - x'', \quad y = y' - y'';$$

si $y \neq 0$, alors y est inversible dans K (puisque K est un corps), à *fortiori* dans L, et la relation $x + \omega y = 0$ implique

$$\omega = -y^{-1}x \in K;$$

contrairement à l'hypothèse que d n'est pas un carré dans K. On a donc $y = 0$, et donc $x = 0$, autrement dit $x' = x''$ et $y' = y''$, ce qui montre bien que f est injective.

On remarquera qu'en introduisant l'application f, les formules (2) et (3) s'écrivent

$$f(x', y') + f(x'', y'') = f(x' + x'', y' + y''), \tag{2 bis}$$
$$f(x', y').f(x'', y'') = f(x'x'' + dy'y'', x'y'' + x''y'). \tag{3 bis}$$

Ces formules (obtenues en supposant le problème résolu) vont maintenant nous servir de point de départ pour construire effectivement une solution du problème posé.

3. *L'anneau* $K[\sqrt{d}]$

Soit d un élément d'un anneau commutatif K; nous allons construire un nouvel anneau L, qu'on note traditionnellement

$$K[\sqrt{d}],$$

et qui est défini comme suit : l'ensemble L est le produit cartésien $K \times K$, de sorte qu'un élément de L est un couple (x, y) d'éléments de K; et les deux opérations fondamentales dans L sont *définies* par les formules

$$(2\ ter) \qquad (x', y') + (x'', y'') = (x' + x'', y' + y''),$$
$$(3\ ter) \qquad (x', y') \cdot (x'', y'') = (x'x'' + dy'y'', x'y'' + x''y'),$$

lesquelles font intervenir à la fois l'élément donné d et les lois de composition dans l'anneau K.

Bien entendu, il n'est nullement évident que les formules (2 *ter*) et (3 *ter*) font de l'ensemble $K \times K$ un *anneau commutatif*, et on doit le démontrer (y compris dans le cas classique où $K = \mathbf{R}$ et $d = -1$; la démonstration dans ce cas particulier n'est ni plus facile ni plus difficile que dans le cas général).

Tout d'abord, l'ensemble $K \times K$ muni de l'addition (2 *ter*) est un groupe commutatif : cela résulte du § 7, nº 2 (produit direct de groupes), et du fait que l'ensemble K, muni de l'addition donnée, est un groupe commutatif.

Montrons maintenant que la multiplication (3 *ter*) est associative. On a en effet par définition

$$\begin{aligned}(x, y)\,[(x', y')\,(x'', y'')] &= (x, y)\,(x'x'' + dy'y'', x'y'' + x''y')\\ &= (x(x'x'' + dy'y'') + dy(x'y'' + x''y'), x(x'y'' + x''y') + y(x'x'' + dy'y''))\end{aligned}$$

et d'autre part

$$\begin{aligned}[(x, y)\,(x', y')](x'', y'') &= (xx' + dyy', xy' + x'y)\,(x'', y'')\\ &= ((xx' + dyy')x'' + d(xy' + x'y)y'', (xx' + dyy')y'' + x''(xy' + x'y));\end{aligned}$$

l'associativité s'obtient trivialement en comparant les résultats obtenus (et, bien entendu, en utilisant les règles de calcul dans K). On établirait par des calculs analogues la commutativité de la multiplication, et sa distributivité par rapport à l'addition.

Enfin, la relation

$$(1, 0)\,(x, y) = (x, y)$$

montre que l'ensemble $K \times K$, muni de la loi de composition (3 *ter*), admet un élément neutre.

L'ensemble $K \times K$, muni des lois de composition (2 *ter*) et (3 *ter*), est donc bien un anneau commutatif.

Montrons maintenant que $K \times K$ *contient un sous-anneau isomorphe à* K; pour cela, considérons l'application $j : K \to K \times K$ donnée par

$$j(x) = (x, 0);$$

il est clair qu'elle est injective; de plus, un calcul facile montre qu'on a

$$j(x') + j(x'') = j(x' + x''),\ j(x') . j(x'') = j(x'x''),\ j(-1) = (-1, 0) = -1$$

où, dans le dernier membre de la dernière relation, -1 désigne l'opposé de l'élément unité $1 = (1, 0)$ de l'anneau $K \times K$; cela fait, les formules précédentes montrent évidemment que j est un *isomorphisme de* K *sur un sous-anneau de* $K \times K$.

Comme j transforme les lois de compositions de K en celles du sous-anneau $j(K)$ de $K \times K$, il n'y a aucun inconvénient à identifier chaque élément x de K à l'élément $j(x)$ de $K \times K$; c'est ce que nous ferons désormais (*).

Pour montrer qu'on a ainsi résolu le problème posé au nº 1, il reste à faire voir que *l'élément d de* K *est un carré dans* $K[\sqrt{d}]$. Or considérons l'élément

$$(5) \qquad \omega = (0, 1)$$

de L; un calcul trivial montre que

$$\omega^2 = (0, 1)\,(0, 1) = (0.0 + d.1.1, 0.1 + 1.0) = (d, 0) = j(d),$$

et comme on a convenu d'une manière générale d'identifier chaque $x \in K$ à l'élément $j(x)$ de L, notre assertion est démontrée.

Nous avons ainsi non seulement résolu le problème posé au nº 1, mais même construit une solution « canonique » de ce problème, à savoir l'anneau $K[\sqrt{d}]$. On dit qu'il s'obtient par **adjonction à K d'une racine carrée de** d; un anneau de la forme $K[\sqrt{d}]$ s'appelle une **extension quadratique de K**.

Pour terminer ces constructions, indiquons une notation commode pour les éléments de $K[\sqrt{d}]$. Tout d'abord l'identification de tout $x \in K$ à l'élément $(x, 0)$ de L permet d'écrire

$$(6) \qquad (x, 0) = x$$

(ce qui, à strictement parler, est aussi faux que possible...). Mais un calcul immédiat montre que, quels que soient $x, y \in K$, on a la formule

$$(x, y) = (x, 0) + (0, 1)\,(y, 0);$$

(*) La méthode utilisée ici est analogue à celle qui permet d'identifier les nombres entiers à des nombres rationnels particuliers (ou les nombres rationnels à des nombres réels particuliers). Quels que soient les procédés utilisés pour définir mathématiquement les nombres entiers et les nombres rationnels, il n'est jamais vrai que le nombre entier n et le nombre rationnel représenté par la fraction $\frac{n}{1}$ soient *identiques*; on peut simplement dire que l'application $n \to \frac{n}{1}$ est injective et transforme les opérations algébriques sur des nombres entiers en les opérations algébriques analogues sur les nombres rationnels correspondants. C'est ce qui explique pourquoi, dans la pratique, on ne fait pas de distinction entre n et $\frac{n}{1}$.

celle-ci s'écrit, compte-tenu de (5) et (6), sous la forme

$$(x, y) = x + \omega y, \tag{7}$$

et on est ainsi ramené à la situation étudiée au nº 2 en supposant le problème résolu.

En conclusion, tout élément de l'anneau $K[\sqrt{d}]$ s'écrit d'une façon et d'une seule sous la forme $x + \omega y$, et ce fait, joint aux axiomes des anneaux commutatifs et à la relation

$$\omega^2 = d, \tag{4}$$

suffit pour effectuer tous les calculs dont on peut avoir besoin : autrement dit le lecteur peut maintenant oublier la *construction* effective de l'anneau $K[\sqrt{d}]$ pour n'en retenir que les *propriétés*.

Exemple 1. Le cas le plus important est celui où $K = \mathbf{R}$, corps des nombres réels, et $d = -1$. L'anneau $\mathbf{R}[\sqrt{-1}]$ ainsi obtenu se note $\mathbf{C}$, et ses éléments s'appelent les **nombres complexes**; un nombre complexe est donc un couple (x, y) de nombres réels, et on calcule sur les nombres complexes à l'aide des formules (2 *ter*) et (3 *ter*) pour $d = -1$, i.e. on pose

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

Dans la pratique on n'utilise pas ces formules; on utilise seulement les propriétés suivantes des nombres complexes :

a) *les nombres complexes forment un anneau commutatif* $\mathbf{C}$ (on verra plus loin que $\mathbf{C}$ est même un corps);

b) *le corps* $\mathbf{R}$ *des nombres réels est un sous-anneau de* $\mathbf{C}$;

c) *il existe un nombre complexe* i (cette notation traditionnelle remplace la notation ω utilisée pour les extensions quadratiques générales) *tel que*

$$i^2 = -1;$$

d) *tout nombre complexe* z *s'écrit d'une façon et d'une seule sous la forme*

$$z = x + iy$$

où x *et* y *sont réels.*

Il n'y a rien de plus à savoir pour calculer sur les nombres complexes. Par exemple :

$$\begin{aligned}(2 + 3i)(5 - 7i) &= 2.5 - 2.7i + 3i.5 - 3i.7i \\ &= 10 - 14i + 15i - 21i^2 = 10 + i + 21 = 31 + i.\end{aligned}$$

Étant donné un nombre complexe

$$z = x + iy$$

avec x, y réels, on dit que x est la **partie réelle** et y la **partie imaginaire** de z; on les désigne par les notations

$$x = \mathrm{Re}(z), \qquad y = \mathrm{Im}(z).$$

On dit que z est **imaginaire pur** si $\mathrm{Re}(z) = 0$; dire par contre que z est **réel** (i.e. appartient au sous-anneau $\mathbf{R}$ de $\mathbf{C}$) se traduit par la relation $\mathrm{Im}(z) = 0$.

4. *Éléments inversibles d'une extension quadratique*

Soient K un anneau commutatif et d un élément de K; considérons l'extension quadratique

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

construite au nº précédent. Étant donné un élément

$$z = x + \omega y \quad (x, y \in K)$$

de L, on appelle **conjugué de** z l'élément

$$\bar{z} = x - \omega y \tag{8}$$

de L, et **norme de** z l'élément

$$N(z) = \bar{z}.z = (x - \omega y)(x + \omega y) = x^2 - \omega^2 y^2 = x^2 - dy^2 \tag{9}$$

de K.

Quels que soient les éléments z' et z'' de L, on a les relations

$$\overline{z' + z''} = \bar{z}' + \bar{z}'', \tag{10}$$
$$\overline{z'z''} = \bar{z}'.\bar{z}'', \tag{11}$$

qui montrent comment calculer le conjugué d'une somme ou d'un produit d'éléments de L. Pour établir les relations (10) et (11), le plus simple est de partir des formules (2 *ter*) et (3 *ter*) du nº 3, et d'examiner ce qui se passe lorsqu'on y remplace y' et y'' par leurs opposés, sans modifier x' et x''.

La relation (11) montre qu'on a

$$N(z'z'') = N(z')N(z'') \tag{12}$$

quels que soient z' et z''; en effet

$$N(z'z'') = \overline{z'z''}.z'z'' = \bar{z}'.\bar{z}''.z'.z'' = \bar{z}'.z'.\bar{z}''.z'' = N(z')N(z'')$$

comme annoncé. On observera qu'on a aussi

$$N(1) = 1. \tag{13}$$

Théorème 1. *Soient* K *un anneau commutatif*, d *un élément de* K, *et* z *un élément de l'anneau* $K[\sqrt{d}]$. *Pour que* z *soit inversible dans* $K[\sqrt{d}]$, *il faut et il suffit que* $N(z)$ *le soit dans* K;

on a alors

(14) $$z^{-1} = N(z)^{-1}.\bar{z}.$$

Supposons z inversible; alors la relation $z^{-1}.z = 1$ donne, compte-tenu de (12) et (13), la relation

$$N(z^{-1}).N(z) = 1,$$

et $N(z)$ est donc bien un élément inversible de l'anneau K.

Inversement, supposons $N(z)$ inversible dans K; la relation

$$\bar{z}z = N(z)$$

implique alors

$$N(z)^{-1}\bar{z}.z = 1,$$

ce qui montre que z est inversible et que son inverse est donné par la relation (14); d'où le Théorème.

5. Cas d'un corps commutatif

Nous pouvons maintenant démontrer le résultat suivant :

THÉORÈME 2. *Soit d un élément d'un corps commutatif* K; *les propriétés suivantes sont équivalentes :*

a) l'anneau $K[\sqrt{d}]$ *est un corps;*

b) d n'est pas un carré dans K.

Pour montrer que *a*) implique *b*), supposons qu'il existe un $x \in K$ tel que

$$x^2 = d;$$

on a alors $x^2 = \omega^2$, donc $(x - \omega)(x + \omega) = 0$; si $K[\sqrt{d}]$ est un corps, donc un anneau d'intégrité, il s'ensuit qu'on a soit $\omega = x$, soit $\omega = -x$, ce qui est impossible puisque pour $x, y \in K$ la relation $x + \omega y = 0$ implique $x = y = 0$.

Montrons maintenant que *b*) implique *a*). Soit $z = x + \omega y$ un élément *non nul* de $K[\sqrt{d}]$; pour montrer qu'il est inversible il suffit (Théorème 1) de montrer que $N(z)$ est inversible dans K; comme K est un corps, tout revient donc à prouver que la relation $N(z) = 0$ implique $z = 0$, autrement dit que

$$x^2 - dy^2 = 0 \quad \text{implique} \quad x = y = 0;$$

or si l'on avait $y \neq 0$, l'élément y de K serait inversible, et il viendrait

$$d = (y^2)^{-1}x^2 = (y^{-1}x)^2$$

contrairement à l'hypothèse que d n'est pas le carré d'un élément de K. On a donc $y = 0$, donc $x^2 = 0$, donc $x = 0$, et ceci achève la démonstration du Théorème.

Exemple 2. Prenant $K = \mathbf{R}$ et $d = -1$ on voit donc que l'anneau $\mathbf{C}$ des nombres complexes est en fait un *corps* commutatif; pour cette raison, on dit que $\mathbf{C}$ est le corps des nombres complexes. Étant donné un nombre complexe

$$z = x + iy$$

non nul, son inverse est donné par la relation (14), et comme ici on a

$$N(z) = x^2 + y^2$$

il vient donc

$$z^{-1} = \frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2};$$

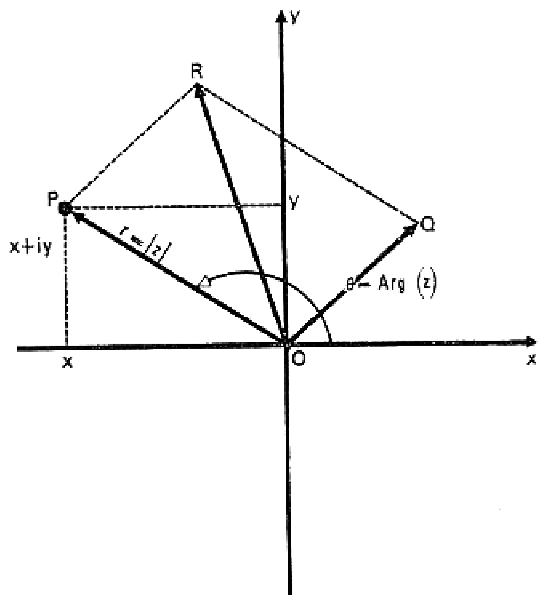
le dénominateur ne peut s'annuler (conformément à la démonstration du Théorème 2) que si $x = y = 0$, i.e. si $z = 0$.

Exemple 3. L'anneau $L = \mathbf{Q}[\sqrt{2}]$ est en fait un *corps* commutatif. On peut d'ailleurs l'identifier à un sous-corps de $\mathbf{R}$: il suffit d'associer à chaque élément $x + y\omega$ de L le nombre réel $x + y\sqrt{2}$ (où $\sqrt{2}$ désigne la racine carrée usuelle du nombre 2); l'application de L dans $\mathbf{R}$ ainsi définie est injective, et compatible avec les lois de composition qui interviennent dans la question. On retrouve ainsi le sous-corps de $\mathbf{R}$ défini au § 8, *Exemple* 6.

6. Représentation géométrique des nombres complexes

Considérons dans le plan deux axes de coordonnées rectangulaires Ox et Oy; il est naturel d'associer à tout nombre complexe

$$z = x + iy$$



le point de coordonnées x, y dans le plan; inversement, on associe à tout point P du plan, de coordonnées x et y, le nombre complexe $z = x + iy$, qu'on appelle traditionnellement l'affixe du point P. On obtient ainsi une bijection de l'ensemble $\mathbf{C}$ des nombres complexes sur l'ensemble des points du plan (une fois choisis des axes de coordonnées, ce qui a naturellement pour but d'identifier le plan à l'ensemble $\mathbf{R}^2$).

Cette « représentation géométrique » des nombres complexes permet d'interpréter facilement l'addition des nombres complexes : si P et Q sont, dans le plan, des points d'affixes u et v, alors le point R d'affixe $u + v$ est donné par la relation

$$\overrightarrow{OR} = \overrightarrow{OP} + \overrightarrow{OQ},$$

puisque pour additionner des vecteurs d'origine O il suffit d'additionner leurs composantes par rapport aux axes de coordonnées Ox, Oy.

Soit P le point d'affixe $z = x + iy$; le nombre

$$N(z) = \bar{z}z = x^2 + y^2$$

est visiblement donné par

$$N(z) = OP^2,$$

en vertu du théorème de Pythagore. La distance de P au point O, i.e. le nombre

$$r = OP = \sqrt{x^2 + y^2} = \sqrt{\bar{z}z} \tag{15}$$

s'appelle le **module** ou la **valeur absolue** de z, et se désigne par la notation

$$|z|;$$

on a toujours $|z| \geqslant 0$, et on a $|z| = 0$ si et seulement si $z = 0$; de plus, les inégalités classiques entre les côtés d'un triangle montrent, si l'on examine la figure, que l'on a $|u + v| \leqslant |u| + |v|$ quels que soient $u, v \in \mathbf{C}$, et plus généralement

$$\boxed{|z_1 + \cdots + z_n| \leqslant |z_1| + \cdots + |z_n|} \tag{16}$$

quels que soient les nombres complexes $z_1, \ldots, z_n$; ce résultat est souvent cité sous le nom d'**inégalité du triangle**

Supposons $z \neq 0$; l'angle

$$\theta = (\widehat{\overrightarrow{Ox}, \overrightarrow{OP}}),$$

qui est un nombre réel modulo 2π (§ 4, *Exemple* 10), s'appelle l'**argument** du nombre complexe $z \neq 0$, et se désigne souvent par la notation

$$\mathrm{Arg}(z).$$

La figure montre que les parties réelle et imaginaire de z sont données, en fonction de la valeur absolue r et de l'argument θ de z, par les formules

$$x = r.\cos\theta, \qquad y = r.\sin\theta, \tag{17}$$

de sorte qu'on peut aussi écrire

$$\boxed{z = r\,(\cos\theta + i.\sin\theta)}\,; \tag{18}$$

cette formule s'appelle la **représentation trigonométrique** de z. On notera qu'inversement la relation

$$z = r(\cos\theta + i.\sin\theta) \quad \text{avec} \quad r > 0 \quad \text{implique} \quad r = |z|,\ \theta = \mathrm{Arg}\,(z);$$

car la relation considérée montre que les parties réelle et imaginaire de z sont

$$x = r.\cos\theta, \qquad y = r.\sin\theta,$$

d'où résulte d'abord que $r^2 = x^2 + y^2$, et, comme r est positif, $r = |z|$; notant θ' l'argument de z il vient alors $\cos\theta = \cos\theta'$, $\sin\theta = \sin\theta'$, d'où $\theta = \theta'$ à un multiple près de 2π, ce qui établit notre assertion.

On va déduire de là les formules

$$\boxed{|z_1 z_2| = |z_1|.|z_2|, \qquad \mathrm{Arg}\,(z_1 z_2) = \mathrm{Arg}\,(z_1) + \mathrm{Arg}\,(z_2)}\,, \tag{19}$$

qui permettent de calculer le module et l'argument d'un produit de nombres complexes. Pour cela, écrivons

$$z_1 = r_1\,(\cos\theta_1 + i.\sin\theta_1), \qquad z_2 = r_2\,(\cos\theta_2 + i.\sin\theta_2)$$

en mettant en évidence les modules et les arguments de z_1 et z_2; il vient

$$z_1 z_2 = r_1 r_2\,(\cos\theta_1 + i.\sin\theta_1)\,(\cos\theta_2 + i.\sin\theta_2)$$

et comme $r_1 r_2$ est positif, il suffit, pour établir le résultat cherché, de prouver la relation

$$(\cos\theta_1 + i.\sin\theta_1).(\cos\theta_2 + i.\sin\theta_2) = \cos(\theta_1 + \theta_2) + i.\sin(\theta_1 + \theta_2);$$

or, d'après les règles de multiplication des nombres complexes, la partie réelle du premier membre est égale à

$$\cos\theta_1.\cos\theta_2 - \sin\theta_1.\sin\theta_2 = \cos(\theta_1 + \theta_2),$$

et la partie imaginaire à

$$\cos\theta_1.\sin\theta_2 + \sin\theta_1.\cos\theta_2 = \sin(\theta_1 + \theta_2),$$

ce qui établit le résultat annoncé.

Ce résultat s'étend naturellement à un produit de plusieurs facteurs, sous la forme

$$\boxed{\prod_{p=1}^{p=n} (\cos\theta_p + i.\sin\theta_p) = \cos\theta + i.\sin\theta \quad \text{où} \quad \theta = \sum_{p=1}^{p=n} \theta_p}\,. \tag{20}$$

En particulier, si l'on suppose les θ_p égaux à un même angle θ, il vient la célèbre **formule de De Moivre**

$$\boxed{(\cos\theta + i.\sin\theta)^n = \cos(n\theta) + i.\sin(n\theta)}\,. \tag{21}$$

Remarque 2. Les formules

$$|z_1 z_2| = |z_1|.|z_2|, \qquad \mathrm{Arg}(z_1 z_2) = \mathrm{Arg}(z_1) + \mathrm{Arg}(z_2)$$

permettent de donner une interprétation « géométrique » de la multiplication des nombres complexes. Soit

$$z = r.(\cos\theta + i.\sin\theta), \qquad r \geqslant 0,$$

un nombre complexe; à tout point P du plan associons le point P′ dont l'affixe est le produit par z de l'affixe de P (l'application $P \to P'$ correspond donc, dans le plan, à l'application $u \to zu$ de $\mathbf{C}$ dans $\mathbf{C}$); alors la transformation faisant passer de P à P′ est une *similitude* et, de façon précise, c'est le produit de l'homothétie de centre O et de rapport r et de la rotation d'angle θ autour de O.

De même, les relations

$$|z^{-1}| = |z|^{-1}, \qquad \operatorname{Arg}(z^{-1}) = -\operatorname{Arg}(z)$$

(qu'on obtient en faisant $z_1 = z$, $z_2 = z^{-1}$ dans (19)), montrent qu'on passe du point d'affixe $z \neq 0$ au point d'affixe z^{-1} par une inversion de centre O et de puissance 1, suivie d'une symétrie par rapport à l'axe Oy.

Ces interprétations géométriques des opérations sur les nombres complexes sont souvent utiles en Analyse, et Gauss fut le premier, en 1799, à les utiliser systématiquement, notamment pour donner la première démonstration correcte du théorème de d'Alembert — Gauss (§ 33, n° 2).

Quant à l'invention des nombres complexes, elle est de beaucoup antérieure à Gauss, et remonte aux mathématiciens italiens du XVIe siècle.

7. *Formules de multiplication des fonctions trigonométriques*

La formule de De Moivre

$$(\cos t + i.\sin t)^n = \cos(nt) + i.\sin(nt)$$

établie ci-dessus pour tout nombre réel t permet de calculer $\cos(nt)$ et $\sin(nt)$ en fonction de $\cos t$ et $\sin t$. En effet, le premier membre s'écrit

$$\begin{aligned}\cos^n t &+ \binom{n}{1}\cos^{n-1}t.i\sin t + \binom{n}{2}\cos^{n-2}t\,(i.\sin t)^2 + \cdots + (i.\sin t)^n \\ &= \cos^n t + i.\binom{n}{1}\cos^{n-1}t.\sin t - \binom{n}{2}\cos^{n-2}t.\sin^2 t - i.\binom{n}{3}\cos^{n-3}t.\sin^3 t \\ &\quad + \binom{n}{4}\cos^{n-4}t.\sin^4 t + i.\binom{n}{5}\cos^{n-5}t.\sin^5 t + \cdots + i^n.\sin^n t;\end{aligned}$$

mais puisque les parties réelle et imaginaire de cette expression sont, d'après la formule de De Moivre, égales à $\cos(nt)$ et $\sin(nt)$, il vient

$$\cos(nt) = \cos^n t - \binom{n}{2}\cos^{n-2}t.\sin^2 t + \binom{n}{4}\cos^{n-4}t.\sin^4 t - \cdots \tag{22}$$

$$\sin(nt) = \binom{n}{1}\cos^{n-1}t.\sin t - \binom{n}{3}\cos^{n-3}t.\sin^3 t + \binom{n}{5}\cos^{n-5}t.\sin^5 + \cdots \tag{23}$$

d'où les formules cherchées. Dans ces formules, les derniers termes dépendent naturellement de la parité de n puisque i^n est réel si n est pair, et imaginaire pur si n est impair. Par exemple on a

$$\begin{aligned}\cos(4t) &= \cos^4 t - 6\cos^2 t.\sin^2 t + \sin^4 t,\\ \cos(5t) &= \cos^5 t - 10\cos^3 t.\sin^2 t + 10\cos t.\sin^4 t.\end{aligned}$$

Les formules obtenues pour $\cos(nt)$ et $\sin(nt)$ permettent naturellement de calculer

$$\operatorname{tg}(nt) = \frac{\sin(nt)}{\cos(nt)} = \frac{\binom{n}{1}\cos^{n-1}t.\sin t - \binom{n}{3}\cos^{n-3}t.\sin^3 t + \cdots}{\cos^n t - \binom{n}{2}\cos^{n-2}t.\sin^2 t + \binom{n}{4}\cos^{n-4}t.\sin^4 t - \cdots}, \tag{24}$$

et en divisant les deux membres de la dernière fraction par $\cos^n t$ il vient

$$\operatorname{tg}(nt) = \frac{\binom{n}{1}\operatorname{tg} t - \binom{n}{3}\operatorname{tg}^3 t + \binom{n}{5}\operatorname{tg}^5 t - \cdots}{1 - \binom{n}{2}\operatorname{tg}^2 t + \binom{n}{4}\operatorname{tg}^4 t - \cdots}.$$

Par exemple, on a

$$\operatorname{tg}(5t) = \frac{5\operatorname{tg} t - 10\operatorname{tg}^3 t + \operatorname{tg}^5 t}{1 - 10\operatorname{tg}^2 t + 5\operatorname{tg}^4 t}.$$

Appliquons maintenant la formule

$$1 + q + q^2 + \cdots + q^n = \frac{1 - q^{n+1}}{1 - q} \tag{25}$$

valable sur tout corps pourvu que $q \neq 1$, en prenant

$$q = r^2, \qquad r = \cos t + i.\sin t;$$

il vient d'une part

$$\frac{1 - q^{n+1}}{1 - q} = \frac{r^{2n+2} - 1}{r^2 - 1} = \frac{r^{2n+1} - r^{-1}}{r - r^{-1}} = r^n\,\frac{r^{n+1} - r^{-n-1}}{r - r^{-1}};$$

or la formule de De Moivre donne

$$\begin{aligned}r^{n+1} &= \cos(n+1)t + i.\sin(n+1)t\\ r^{-1} &= \cos t - i.\sin t\\ r^{-n-1} &= \cos(n+1)t - i.\sin(n+1)t\end{aligned}$$

d'où

$$\begin{aligned}\frac{1 - q^{n+1}}{1 - q} &= (\cos(nt) + i.\sin(nt))\,\frac{2i.\sin(n+1)t}{2i.\sin t}\\ &= (\cos(nt) + i.\sin(nt))\,\frac{\sin(n+1)t}{\sin t};\end{aligned}$$

d'autre part, la formule de De Moivre donne aussi

$$1 + q + \cdots + q^n = \sum_{k=0}^{k=n} (\cos(2kt) + i.\sin(2kt));$$

en égalant les parties réelle et imaginaire de cette expression avec celles de l'expression trouvée auparavant, on obtient donc les formules

$$1 + \cos(2t) + \cos(4t) + \cdots + \cos(2nt) = \cos(nt)\frac{\sin(n+1)t}{\sin t}$$

$$\sin(2t) + \sin(4t) + \cdots + \sin(2nt) = \sin(nt)\frac{\sin(n+1)t}{\sin t}$$

ou, si l'on préfère,

$$(26) \qquad 1 + \cos t + \cos(2t) + \cdots + \cos(nt) = \frac{\cos\left(n\frac{t}{2}\right)\sin(n+1)\frac{t}{2}}{\sin\frac{t}{2}}$$

$$(27) \qquad \sin t + \sin(2t) + \cdots + \sin(nt) = \frac{\sin\left(n\frac{t}{2}\right)\sin(n+1)\frac{t}{2}}{\sin\frac{t}{2}}.$$

Ces formules supposent naturellement $\sin\frac{t}{2}$ non nul, i.e. t non multiple de 2π.

Modules sur un anneau

La notion de module sur un anneau fournit un cadre général et abstrait permettant de traiter les aspects purement algébriques des problèmes « linéaires » qu'on rencontre dans toutes les branches des Mathématiques : théorie des nombres, algèbre linéaire classique, calcul tensoriel, formes différentielles, équations aux dérivées partielles, équations intégrales, géométrie algébrique, fonctions analytiques, topologie algébrique, etc...

Certains résultats de la théorie des modules sur un anneau K ne sont valables que moyennant certaines hypothèses concernant l'anneau K : par exemple, la théorie de la « dimension » suppose que K est un corps.

Par contre, les résultats les plus simples sont valables pour *tout* anneau K; ce sont ces résultats qu'on trouvera dans ce chapitre (§§ 10 à 17). Le lecteur qui trouverait trop général et abstrait le point de vue adopté ici, et qui préférerait supposer que l'anneau de base K, est, par exemple, le corps **R** des nombres réels, ne parviendrait pas à simplifier de façon très substantielle les §§ en question : en faisant l'hypothèse que K = **R**, on pourra négliger les *Exemples* 5, 6, 9, 10 et le n° 4 du § 10, les *Exemples* 4, 5, 6, 11 du § 11, la *Remarque* 4 du § 16, et l'*Exemple* 2 du § 17, tout le reste demeurant sans aucun autre changement que le remplacement de la lettre K par la lettre **R**.

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.

§ 9

1 *a*) Montrer que tout nombre complexe $d \neq 0$ possède exactement deux racines carrées dans le corps $\mathbf{C}$ (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 $\mathbf{C}$, et en possède deux si

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

c) Résoudre dans $\mathbf{C}$ les équations

$$\begin{aligned} z^2 + (5 - 2i)z + 5 - 5i &= 0 \\ z^2 + (1 - 2i)z - 2i &= 0 \\ z^4 - 30z^2 + 289 &= 0 \end{aligned}$$

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

$$\frac{(1+2i)^2 - (1-i)^3}{(3+2i)^3 - (2+i)^2}; \qquad \frac{(1+i)^9}{(1-i)^7}; \qquad \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)^3; \qquad \sqrt[4]{2 - i\sqrt{12}};$$

$$(az^2 + bz)(bz^2 + az) \qquad \text{où} \qquad z = -\frac{1}{2} + \frac{i\sqrt{3}}{2}.$$

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) :

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

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 $\mathbf{U}$ l'ensemble des nombres complexes z tels que $|z| = 1$; montrer que c'est un sous-groupe du groupe multiplicatif $\mathbf{C}^*$ des nombres complexes non nuls. Construire un isomorphisme entre les groupes $\mathbf{U} \times \mathbf{R}_+^*$ et $\mathbf{C}^*$. Montrer que $\mathbf{U}$ 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 $u^p vu^n(D)$, 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 **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

$\mathbf{Z}/2\mathbf{Z}$). 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 XVIIIe siècle et au début du XIXe, 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.]