LIVRE III CHAPITRE V
GROUPES A UN PARAMETRE.
NOMBRES COMPLEXES

Rédaction n° 025

Nombre de pages : 62

Nombre de feuilles : 62

Chapitres V - VI - VII - VIII

A 25 2

LIVRE III

(Ancien CHAPITRE V.)

Etat 2

GROUPES A UN PARAMETRE. NOMBRES COMPLEXES.

§ 1. Le groupe additif R, ses sous-groupes et groupes quotients.

Automorphismes et automorphismes locaux de R. Soit f un automorphisme local (chap.III, § 1, déf.2) du groupe topologique R. Il existe donc un intervalle $[-a,+a] = I$ tel que f soit un homéomorphisme de I sur un voisinage V de 0 dans R, et que $f(x+y)=f(x)+f(y)$ pour tout couple de points x,y tels que $x \in I$, $y \in I$, $x+y \in I$.

Si p et q sont deux entiers >0 tels que $p \leqslant q$, on a $(p/q)a \in I$, donc, par récurrence sur p, $f(pa/q)=pf(a/q)$; en particulier $f(a)=qf(a/q)$, d'où $f(pa/q)=(p/q)f(a)$. Autrement dit, pour tout nombre rationnel r tel que $0 \leqslant r \leqslant 1$, $f(ra)=rf(a)$. Si maintenant λ est un nombre réel quelconque tel que $0 \leqslant \lambda \leqslant 1$, il est adhérent à $Q \cap I$, donc, en vertu de la continuité de f dans I

$$f(\lambda a)=\lim_{r\to\lambda, r\in Q} f(ra) = \lim_{r\to\lambda, r\in Q}(rf(a))=f(a).\lim_{r\to\lambda, r\in Q} r= \lambda f(a)$$

On a évidemment $f(a)\neq 0$; on peut donc écrire, pour tout nombre réel x tel que $0 \leqslant x \leqslant a$, $f(x)=\alpha x$, avec $\alpha=f(a)/a\neq 0$. Comme, pour $-a \leqslant x \leqslant 0$, on a $-x \in I$, $-x+x = 0 \in I$, on en tire $f(-x)+f(x)=0$, d'où $f(x)=-f(-x)=\alpha x$. Ainsi :

Proposition 1. *Si f est un automorphisme local du groupe topologique R (groupe additif de la droite numérique), il existe un intervalle $[-a,+a]$ $(a>0)$ et un nombre réel $\alpha\neq 0$ tels que, pour tout x tel que $-a \leqslant x \leqslant a$, $f(x) = \alpha x$.*

Proposition 2. *Tout automorphisme du groupe topologique R est de la forme $x \to \alpha x$, où α est un nombre réel $\neq 0$.*

Autrement dit, tout automorphisme de $\mathbb{R}$ est une <u>homothétie</u> de rapport $\neq 0$.

Le <u>groupe des automorphismes</u> du groupe additif $\mathbb{R}$ est donc isomorphe au <u>groupe multiplicatif</u> $\mathbb{R}^*$.

En effet, si f est un automorphisme de $\mathbb{R}$, il existe un intervalle $[-a,a]$ $(a>0)$ tel que, pour $-a \leqslant x \leqslant a$, $f(x)=ax$ $(a\neq 0)$. Si maintenant x est quelconque dans $\mathbb{R}$, il existe un entier n tel que $-a \leqslant x/n \leqslant a$, donc $f(x/n) = ax/n$, et comme $f(x)=nf(x/n)$, $f(x)=ax$. La réciproque est évidente.

<u>Corollaire</u>. <u>Etant donné un nombre réel</u> $a\neq 0$, <u>il existe un automorphisme</u> <u>f de</u> $\mathbb{R}$, <u>et un seul, tel que</u> $f(1)=a$.

On a en effet $f(x)=ax$, et a est déterminé par la condition $a=a$.

<u>Remarque</u>. La démonstration de la prop.1 montre, plus généralement, que si f est <u>continue</u> dans $I=[-a,+a]$, et telle que $f(x+y)=f(x)+f(y)$ lorsque $x\in I$, $y\in I$, $x+y\in I$, il existe un nombre réel a tel que $f(x)=ax$ pour tout $x\in I$. On en conclut que toute <u>représentation continue</u> f de $\mathbb{R}$ <u>dans</u> $\mathbb{R}$ est de la forme $x \to ax$; si elle n'est pas identiquement nulle, elle est un automorphisme.

<u>Sous-groupes fermés de</u> $\mathbb{R}$. <u>Théorème 1</u>. <u>Tout sous-groupe fermé du groupe topologique</u> $\mathbb{R}$, <u>distinct de</u> $\mathbb{R}$ <u>et de</u> $\{0\}$, <u>est formé des multiples entiers d'un nombre</u> $a>0$ (autrement dit, est de la forme $a\mathbb{Z}$).

Soit H un sous-groupe fermé de $\mathbb{R}$, et supposons d'abord H <u>non discret</u>. Alors, pour tout entier $n>0$, il existe $\varepsilon \in H$ tel que $0<\varepsilon \leqslant 1/n$. Soit x un point quelconque de $\mathbb{R}$, et q la partie entière (chap.IV, § 8) de x/ε; on a $|x-q\varepsilon| \leqslant 1/n$, et $q\varepsilon \in H$, ce qui montre que x est adhérent à H, et comme H est supposé fermé, $H = \mathbb{R}$.

Supposons maintenant H <u>discret</u> et non réduit à 0. L'ensemble $H \cap \mathbb{R}_+^*$ n'est pas vide, et sa borne inférieure a est >0, puisque H est discret

d'autre part, $a \in H$, puisque H est fermé. Si x est un point quelconque de H , et n la partie entière de x/a , on a $0 \leqslant x-na < a$, et comme $x-na \in H$, $x-na = 0$ d'après la définition de a , ce qui achève la démonstration.

Corollaire. Tout sous-groupe non discret de R est partout dense.

Considérons en particulier deux nombres a et b non nuls, tels que le rapport b/a soit irrationnel. Le sous-groupe de R engendré par l'ensemble $\{a,b\}$ n'est autre que l'ensemble des nombres $ma+nb$, où m et n sont des entiers (positifs ou négatifs). Ce sous-groupe ne peut être discret, car il existerait alors un nombre $c>0$ et deux entiers p,q tels que $a=pc$, $b=qc$, d'après le th.1 ; et cela entraînerait $b/a = q/p$, contrairement à l'hypothèse. Le corollaire du th.1 conduit donc au résultat suivant :

Proposition 3. (théorème de Kronecker). Soient a et b deux nombres $\neq 0$ tels que le rapport b/a soit irrationnel ; quels que soient les nombres réels x et $\varepsilon > 0$, il existe deux entiers m,n , tels que

$$(1) \qquad x < ma + nb < x+\varepsilon .$$

Nous allons donner de cette proposition une seconde démonstration qui précise davantage l'ordre de grandeur des entiers m et n , en fonction de x et ε (voir aussi exerc. 2). Nous nous limiterons au cas où $a=1$, $b=\omega>0$ et irrationnel (on y ramène le cas général par une homothétie).

Etant donné un entier $n>0$, nous allons montrer qu'il existe deux entiers p,q tels que $1 \leqslant q \leqslant n$, et que

$$(2) \qquad |q\omega - p| < 1/n .$$

Considérons en effet les n nombres $u_k = k\omega - [k\omega]$, où k prend toutes les valeurs entières telles que $1 \leqslant k \leqslant n$.

On a $0 \leqslant [nu_k] < n$ d'après la définition de u_k . S'il existe un entier k tel que $[nu_k] = 0$, la proposition est démontrée ; sinon, les n entiers $[nu_k]$ ne peuvent prendre que les n-1 valeurs 1,2,...,n-1 ; il y a donc deux entiers distincts k',k" tels que $[nu_{k'}] = [nu_{k''}]$, c'est-à-dire $|n(u_{k'} - u_{k''})| < 1$. on peut supposer par exemple $k' > k''$; si on pose $q = k' - k''$, $p = [k'\omega] - [k''\omega]$, on a bien $1 \leqslant q \leqslant n$, et l'inégalité (2) est vérifiée.

De la relation (2), on déduit sans peine la prop.3 . En effet supposons $1/n \leqslant \varepsilon$, et p et q entiers choisis de sorte que $0 < p + q\omega < 1/n$; si on pose $\alpha = p + q\omega$, soit h la partie entière de x/α ; on a donc $k\alpha = hp + hq\omega \leqslant x < h\alpha + \alpha$, d'où $x < (h+1)p + (h+1)q\omega \leqslant x + \alpha < x + \varepsilon$.

Le mode de raisonnement utilisé pour démontrer l'inégalité (2) est dû à Dirichlet, et est appelé principe des tiroirs ("si n objets sont rangés dans n-1 tiroirs, il y a au moins un tiroir qui contient au moins deux objets") ; il joue un grand rôle dans la théorie des approximations diophantiennes (*).

Groupes quotients de $\mathbf{R}$. Tout groupe quotient séparé de $\mathbf{R}$ étant un groupe quotient de $\mathbf{R}$ par un de ses sous-groupes fermés (chap.III, § 2, th.), on voit d'après le th.1 que les seuls groupes quotients séparés de $\mathbf{R}$ autres que $\mathbf{R}$ et $\{0\}$, sont les groupes $\mathbf{R}/a\mathbf{Z}$, où $a > 0$.

Définition 1. Le groupe $\mathbf{R}/a\mathbf{Z}$ est appelé groupe additif des nombres réels modulo a .

(*) Voir J.F.Koksma, Diophantische Approximationen (Ergeb. der Math., t.IV, fasc.4, Berlin, 1936), chap.I, § 2, p.5-8 . Une autre méthode de démonstration de l'inégalité (2) s'appuie sur la théorie des fractions continuelles, qui sort du cadre de la 1ère partie de ce Traité (cf. Koksma, loc. cit., chap.III) .

La relation $x \equiv y$ (mod. $a\mathbb{Z}$) s'écrit plus souvent $x \equiv y$ (mod.a) et se lit "x et y sont congrus modulo a" ; elle signifie donc que $x-y$ est un multiple entier de a .

Si a et b sont des nombres >0 distincts, l'automorphisme $x \to (b/a)x$ de $\mathbb{R}$ transforme $a\mathbb{Z}$ en $b\mathbb{Z}$; donc (chap.III, § 2) les groupes quotients $\mathbb{R}/a\mathbb{Z}$ et $\mathbb{R}/b\mathbb{Z}$ sont isomorphes ; autrement dit :

Proposition 4. Tout groupe quotient séparé de $\mathbb{R}$, distinct de $\mathbb{R}$ et de $\{0\}$, est isomorphe au groupe additif $\mathbb{R}/\mathbb{Z}$ des nombres réels modulo 1 .

Définition 2. L'espace topologique $\mathbb{R}/\mathbb{Z}$ est appelé tore numérique à une dimension et se note $\mathbb{T}$ (par abus de langage, on appelle souvent aussi "tore numérique à une dimension" le groupe topologique" $\mathbb{R}/\mathbb{Z}$) .

* Comme nous le verrons au § 4, $\mathbb{T}$ est un espace topologique homéomorphe au cercle $x^2+y^2=1$ du plan numérique $\mathbb{R}^2$; le produit $\mathbb{T}^2$ est donc homéomorphe à un tore de révolution dans $\mathbb{R}^3$ (chap.VI, § , exerc.) ; d'où le nom de "tore numérique à une dimension" employé pour désigner $\mathbb{T}$ (au chap.VI, § 2 , nous appellerons de même $\mathbb{T}^n$ le "tore numérique à n dimensions"). *

Etude topologique de $\mathbb{T}$. Désignons par S la relation d'équivalence induite par la relation $x \equiv y$ (mod.1) sur l'intervalle $A = \left(-\frac{1}{2}, +\frac{1}{2}\right)$. Tout ensemble B fermé par rapport à A est fermé par rapport à $\mathbb{R}$; pour le saturer pour la relation $x \equiv y$ (mod.1), dans $\mathbb{R}$, il faut prendre l'ensemble $B+\mathbb{Z}$, c'est-à-dire la réunion des ensembles $B+n$ ($n \in \mathbb{Z}$) ; or, un point quelconque de $\mathbb{R}$ ne peut être évidemment adhérent qu'à deux de ces ensembles au plus ; $B+\mathbb{Z}$ est donc fermé dans $\mathbb{R}$, et si B est saturé par rapport à S , B est la trace de $B+\mathbb{Z}$ sur A . Par suite (chap.I, §9, prop. 2) :

Proposition 5. Le tore numérique $\mathbb{T}$ est homéomorphe à l'espace quotient de l'intervalle $\left(-\frac{1}{2}, +\frac{1}{2}\right)$, obtenu en identifiant ses deux extrémités (fig. 1)

Proposition 6. Le tore numérique T est un espace compact, connexe et localement connexe.

En effet T est séparé, et homéomorphe à A/S ; comme A est compact, T est compact (chap.I, § 10, prop.6) ; comme A est connexe T est connexe (chap.I, § 11, prop.7). Enfin, comme Z est discret, $T = R/Z$ est localement isomorphe au groupe R, et en particulier localement connexe (chap. III, § 2, prop.).

On notera encore que l'application canonique φ de R sur $T = R/Z$, restreinte à un intervalle semi-ouvert $I = [a, a+1[$ (a point quelconque de R) est une application biunivoque et continue de I sur T ; son application réciproque est continue en tout point autre que $\varphi(a)$, discontinue au point $\varphi(a)$. Un tel intervalle I, image biunivoque de T dans R, est appelé domaine fondamental de T dans R. On identifie souvent T avec un de ses domaines fondamentaux, muni de la topologie image réciproque de celle de T par l'application φ.

Fonctions périodiques. **Définition 3.** On dit qu'une fonction f, définie dans R, et prenant ses valeurs dans un ensemble quelconque E, est périodique, s'il existe un nombre $a \neq 0$ tel que

$$f(x+a) = f(x) \tag{3}$$

quel que soit $x \in R$. Tout nombre a pour lequel la relation (3) est une identité en x, est appelé une période de f.

Il est immédiat que l'ensemble G des périodes d'une fonction périodique f est un sous-groupe (non réduit à 0 par hypothèse) du groupe additif R. Si G_x désigne l'ensemble des $a \in R$ tels que $f(x+a)=f(x)$ pour une valeur donnée de x, G n'est autre que l'intersection des G_x, lorsque x parcourt R.

Envisageons maintenant le cas où f est une application continue de $\mathbb{R}$ dans un espace topologique E ; chacun des ensembles G_x est alors fermé, donc le groupe G des périodes de f est fermé. Si $G=\mathbb{R}$, on a $f(x)=f(y)$ quels que soient x et y dans $\mathbb{R}$, donc f est constante.

En particulier, on voit qu'une fonction continue dans $\mathbb{R}$ ne peut avoir deux périodes a et b ayant un rapport irrationnel que si elle est constante (prop. 3).

Si $G=\mathbb{R}$, il existe un nombre $a>0$ tel que $G=a\mathbb{Z}$; a est appelé la période principale de f : c'est la plus petite période strictement positive de f ; l'application $x \to f(ax)$ étant alors de période principale égale à 1, on peut toujours se ramener ainsi à ce cas particulier.

Toute fonction f définie dans $\mathbb{R}$ et de période a (principale ou non) est compatible (Ens. R, § 5, n°7) avec la relation $x \equiv y \pmod{a}$; par passage au quotient, il lui correspond une fonction $\dot{f}$ définie dans $\mathbb{R}/a\mathbb{Z}$ et prenant ses valeurs dans le même ensemble E que f ; on définit ainsi une application biunivoque $f \to \dot{f}$ de l'ensemble des fonctions de période a, définies dans $\mathbb{R}$ et à valeurs dans E, sur l'ensemble des applications de $\mathbb{R}/a\mathbb{Z}$ dans E. Pour que $\dot{f}$ soit continue (lorsque E est un espace topologique), il faut et il suffit que f soit continue dans $\mathbb{R}$ (chap. 1, § 9, th. 1).

Sous-groupes et groupes quotients de $\mathbb{T}$. Soit φ l'homomorphisme canonique de $\mathbb{R}$ sur $\mathbb{T}=\mathbb{R}/\mathbb{Z}$; si H est un sous-groupe de $\mathbb{T}$, $G=\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{R}$ contenant $\mathbb{Z}$, et réciproquement, si G est un sous-groupe de $\mathbb{R}$ contenant $\mathbb{Z}$, $\varphi(G)$ est un sous-groupe de $\mathbb{T}$, isomorphe (en tant que groupe topologique) à $G/\mathbb{Z}$ (chap. III, § 2, prop.). Pour que H soit fermé dans $\mathbb{T}$, il faut et il suffit que $G=\varphi^{-1}(H)$ soit fermé dans $\mathbb{R}$; si on écarte le cas où $G=\mathbb{R}$, on a donc $G=a\mathbb{Z}$ avec $a>0$ (th. 1).

en outre, comme G contient Z, il existe un entier p tel que $1=pa$, d'où $a=1/p$. $H=\varphi(G)$ est identique à l'image de l'intersection de G et du domaine fondamental $[0,1[$; c'est donc un groupe à p éléments, et comme p est le plus petit entier m tel que $ma \equiv 1 \pmod 1$, G est un groupe cyclique discret d'ordre p.

Tout groupe quotient séparé de T étant de la forme T/H, où H est un sous-groupe fermé de T, est isomorphe au groupe R/G, où $G=\varphi^{-1}(H)$ (chap.III, § 2, prop.). Si $H \neq T$, c'est-à-dire si on écarte le cas du groupe quotient réduit à l'unité, $G=a\,Z$ $(a>0)$, donc R/G est isomorphe à T. Ainsi :

Proposition 7. Tout sous-groupe fermé de T, non identique à T, est à un groupe cyclique fini. Tout groupe quotient séparé de T et non réduit à l'unité, est isomorphe à T.

Corollaire. Tout sous-groupe infini de T est partout dense dans T.

Automorphismes de T. Soient φ l'homomorphisme canonique de R sur T, et I l'intervalle $\left]-1/4,+1/4\right[$; la restriction de φ à I est un isomorphisme local de R dans T ; soit ψ son application réciproque. Si f est un automorphisme du groupe topologique T, il existe un voisinage V de l'origine dans T, contenu dans $\varphi(I)$ tel que $f(V)$ soit également contenu dans $\varphi(I)$; il en résulte que $g=\psi \circ f \circ \varphi$ est un automorphisme local de R, défini dans le voisinage $\varphi^{-1}(V) \subset I$, de 0 ; donc (prop.1) il existe un voisinage W de 0 dans R, contenu dans $\varphi^{-1}(V)$, et un nombre réel $a \neq 0$, tels que $g(x)=ax$ quel que soit $x \in W$. Or, pour tout $x \in R$, il existe un entier n tel que $x/n \in W$; donc $ax/n = \psi(f(\varphi(x/n)))$, ou encore $\varphi(ax/n) = f(\varphi(x/n))$, d'où, en multipliant les deux membres par n, $\varphi(ax)=f(\varphi(x))$; si, dans cette identité, on fait $x=1$, il en résulte, puisque f est un automorphisme, la relation $\varphi(a)=\varphi(0)$, c'est-à-dire $a \equiv 0 \pmod 1$. Autrement dit, a doit être un entier ;

mais, si $|a| > 1$, on aurait, pour $x=1/a$, $\varphi(1)=\varphi(0)=f(\varphi(1/a))$, et $\varphi(0)\neq\varphi(1/a)$, contrairement à l'hypothèse que f est biunivoque. Donc :

Proposition 8. Les seuls automorphismes du groupe topologique T sont l'application identique, et la symétrie $x \to -x$.

Homomorphismes de R sur T . Soit h une représentation continue de R dans T ; avec les mêmes notations que ci-dessus, on voit immédiatement que $\psi \circ h$ est une fonction continue dans un voisinage W de 0 dans R , à valeurs dans R et telle que $h(x+y)=h(x)+h(y)$ si x,y et $x+y$ sont dans W ; donc (prop.1), il existe un voisinage W' de 0 dans R , et un nombre réel a tels que $\psi(h(x))=ax$ quel que soit $x \in W'$; on en conclut comme ci-dessus que $h(x)=\varphi(ax)$ pour tout $x \in R$. Autrement dit

Proposition 9. Si φ est l'homomorphisme canonique de R sur $T = R/Z$, toute représentation continue de R dans T est de la forme $x \to \varphi(ax)$ où $a \in R$; si elle n'est pas identiquement nulle, c'est un homomorphisme de R sur T .

Groupes localement isomorphes à R . Théorème 2. Tout groupe connexe G localement isomorphe à R est isomorphe à R ou à T .

En effet, soit f un isomorphisme local de R dans G , appliquant un intervalle $I = \left(-a,+a\right)$ sur un voisinage V de l'unité dans G . Comme G est connexe, il est engendré par tout voisinage de l'unité (chap.III, § 2, prop.) ; si W est un voisinage de l'unité tel que $W^2 \subset V$, deux éléments quelconques de W sont permutables, puisqu'ils sont images par f de deux éléments x,y de I , et que $f(x)f(y)=f(y)f(x)=f(x+y)$; donc G est abélien, et on peut désormais le noter additivement. Nous allons prolonger f à R ; pour cela, considérons un point quelconque $x \in R$; il existe un entier n tel que $x/n \in I$; nous poserons $f(x)=nf(x/n)$. Cette définition est bien indépendante de l'entier n considéré ; en effet, si m est un second entier tel que $x/m \in I$,

on a a fortiori $x/mn \in I$, et $f(x/n)=mf(x/mn)$, $f(x/m)=nf(x/mn)$, d'où $nf(x/n)=mf(x/m)$. Si x et y sont deux points quelconques de $\mathbb{R}$, il existe un entier n tel que x/n , y/n et $(x+y)/n$ appartiennent à I ; donc $f(x+y) = nf((x+y)/n) = n(f(x/n)+f(y/n)) = f(x)+f(y)$, ce qui montre que f est une <u>représentation</u> de $\mathbb{R}$ dans G . Elle applique $\mathbb{R}$, qui est engendré par le voisinage I , sur le groupe engendré par V , c'est-à-dire <u>sur</u> G , en outre, comme l'image par f de tout voisinage de 0 dans $\mathbb{R}$, contenu dans I , est un voisinage de l'origine dans G , f est un <u>homomorphisme de</u> $\mathbb{R}$ <u>sur</u> G (chap.III, § 2, th.). G est donc isomorphe à un groupe quotient séparé de $\mathbb{R}$; comme il n'est pas réduit à l'origine, il est isomorphe à $\mathbb{R}$ ou à $\mathbb{T}$.

<u>Exercices</u>. 1) Soit $(a_i)_{1 \leqslant i \leqslant n}$ une suite finie de nombres réels; montrer que, pour tout nombre entier $t > 0$, il existe $n+1$ entiers $x_1, x_2, \ldots, x_n$, y tels que

$$\left| \sum_{i=1}^{n} a_i x_i - y \right| \leqslant 1/t^n$$

et $$|x_i| \leqslant t \quad \text{pour} \quad 1 \leqslant i \leqslant n$$

(utiliser le principe des tiroirs).

¶ 2) On appelle <u>suite de Farey d'ordre</u> n (n entier > 0) l'ensemble F_n des nombres rationnels irréductibles p/q tels que $0 < q \leqslant n$. Deux points r, r' de F_n $(r < r')$ sont dits <u>consécutifs</u> si l'intervalle ouvert $]r, r'[$ ne contient aucun point de F_n .

a) Si $r=p/q$, $r'=p'/q'$ $(r < r')$ sont deux points consécutifs de F_n , on a $p'q-pq'=1$; s'il existe dans l'intervalle $]r, r'[$ un point p''/q'' de F_{n+1} , on a nécessairement $p''=p+p'$, $q''=q+q'=n+1$; sinon, $q+q' > n+1$ (procéder par récurrence sur n, en démontrant d'abord la seconde partie de la proposition : remarquer que, si $p'q-pq'=1$, on a $p'' = \lambda p + \mu p'$,

$q''=\lambda q+\mu q'$ avec λ et μ entiers >0 pour tout nombre rationnel irréductible p''/q'' tel que $p/q<p''/q''<p'/q'$). Réciproquement, si r et r' sont deux nombres rationnels tels que $p'q-pq'=1$, et si n est le plus petit entier tel que r et r' appartiennent à F_n, r et r' sont consécutifs dans F_n.

b) Pour tout nombre réel θ et tout entier $n \geqslant 1$, il existe au moins un nombre rationnel irréductible p/q tel que $1 \leqslant q \leqslant n$ et $|\theta-p/q| \leqslant 1/(n+1)q$. Il ne peut exister deux nombres rationnels satisfaisant à ces conditions que si θ est rationnel.

c) Si p/q est un nombre rationnel irréductible, et θ un nombre réel tel que $|\theta-p/q| < 1/q^2$, θ appartient à l'intervalle ouvert dont les bornes sont les deux termes de la suite de Farey F_q, consécutifs à p/q.

¶ 3) Pour tout couple de nombres réels (θ,β), il existe une infinité de triplets (p,q,r) d'entiers >0, tels que $-1<r(\theta q+p-\beta)<1$, et $|q| \leqslant r/2$ (si m et n sont des entiers tels que $|n\theta-m| < 1/n$, prendre $r=n$, et choisir p et q de sorte que $pn+qm$ diffère de $n\beta$ de moins de $\frac{1}{2}$).

¶ 4) Soient θ un nombre irrationnel, λ un nombre réel, tels que $0 \leqslant \theta < 1$, $0 \leqslant \lambda < 1$; on pose $x_n = n\theta+\lambda-[n\theta+\lambda]$, $y_n=n\theta-[n\theta]$, pour tout entier $n>0$. Si α et β sont deux nombres réels tels que $0 \leqslant \alpha < \beta \leqslant 1$, on désigne par $\varphi(\alpha,\beta;n)$ le nombre des indices p tels que $1 \leqslant p \leqslant n$ et $\alpha \leqslant x_p < \beta$.

a) Montrer que $\varphi(0,\theta;n) = [n\theta+\lambda]$.

b) Plus généralement, on a

$$\varphi(0,y_m;n) = \sum_{k=0}^{m-1}([(n-k)\theta+\lambda]-[-k\theta+\lambda])-n[m\theta]$$

(évaluer la quantité $\varphi(y_k,y_{k+1};n)$ si $0 \leqslant y_k < y_{k+1} \leqslant 1$, la somme $\varphi(0,y_{k+1};n)+\varphi(y_k,1;n)$ si $0 \leqslant y_{k+1} < y_k \leqslant 1$, et en déduire la formule).

c) En déduire que, quels que soient les nombres réels α et β tels que $0 \leqslant \alpha < \beta \leqslant 1$, $\lim_{n\to\infty} \varphi(\alpha,\beta;n)/n = \beta-\alpha$ (approcher α et β par des y_m).

5) Soit φ l'application canonique de $\mathbb{R}$ sur $\mathbb{T} = \mathbb{R}/\mathbb{Z}$; si A est une partie connexe de $\mathbb{T}$, montrer qu'il existe un domaine fondamental $[a,a+1[$ de $\mathbb{T}$ tel que l'intersection de ce domaine et de $\varphi^{-1}(A)$ soit un intervalle.

¶ 6) a) Un intervalle compact I de $\mathbb{R}$ n'est pas homéomorphe à $\mathbb{T}$ (raisonner par l'absurde, en montrant que l'intervalle ouvert I' ayant mêmes bornes que I serait homéomorphe à un ensemble ouvert connexe et partout dense de $\mathbb{T}$, et en utilisant l'exerc. 5).

b) En déduire qu'un homéomorphisme de $\mathbb{T}$ <u>dans</u> $\mathbb{T}$ est nécessairement un homéomorphisme de $\mathbb{T}$ <u>sur</u> $\mathbb{T}$.

c) Soit f un homéomorphisme de $\mathbb{T}$ sur $\mathbb{T}$, φ l'application canonique de $\mathbb{R}$ sur $\mathbb{T}$. Montrer qu'il existe une application continue et strictement monotone g de $\mathbb{R}$ dans $\mathbb{R}$ telle que $f\circ\varphi = \varphi\circ g$, et que l'on ait, soit $g(x+1)=g(x)+1$ (si g est strictement croissante), soit $g(x+1)=g(x)-1$ (si g est strictement décroissante), quel que soit $x \in \mathbb{R}$.

¶ 7) Soit f une application continue strictement croissante de $\mathbb{R}$ sur $\mathbb{R}$, telle que $0 \leqslant f(0) < 1$ et $f(x+1)=f(x)+1$ quel que soit $x \in \mathbb{R}$. On pose $f_1=f$, et pour $n>1$, on définit par récurrence $f_n = f\circ f_{n-1}$.

a) Montrer que f_n est strictement croissante et continue, et que $f_n(x+1)=f_n(x)+1$ quel que soit $x \in \mathbb{R}$.

b) Si p et n sont deux entiers ($n>0$) tels que $f_n(0) \geqslant p$ (resp. $f_n(0)<p$) montrer que, pour tout entier $k>0$, on a $f_{kn}(0) \geqslant kp$ (resp. $f_{kn}(0)<kp$) ; en déduire qu'il existe un nombre

réel $\theta \leqslant 1$ tel que $\lim_{n\to\infty} f_n(0)/n = \theta$ (prendre pour θ la borne inférieure des nombres rationnels p/n $(n>0)$ tels que $f_n(0)<p$; on montrera d'abord que cette borne est $\leqslant 1$). Montrer ensuite que, pour tout $x \in \mathbb{R}$, on a aussi $\lim_{n\to\infty} f_n(x)/n = \theta$.

c) Si $\theta = m/n$ est rationnel (irréductible), montrer qu'il existe $x \in [0,1[$ tel que $f_n(x)=m+x$ (raisonner par l'absurde : en supposant $f_n(x)-(x+m) \geqslant \alpha > 0$ pour $0 \leqslant x \leqslant 1$, montrer qu'on en déduit $\lim_{p\to\infty} f_p(x)/p \geqslant (m+\alpha)/n$).

d) On suppose désormais θ <u>irrationnel</u>, et on pose pour $p \geqslant 1$ $a_p = p\theta - [p\theta]$, $u_p(x) = f_p(x) - [f_p(x)]$ pour tout $x \in [0,1[$. Montrer que la relation $a_h < a_k$ entraîne $u_h(x) < u_k(x)$. En déduire que l'ensemble P_x des valeurs d'adhérence de la suite $(u_p(x))$ est <u>parfait</u> (remarquer qu'entre deux points de la suite $(u_p(x))$, il y a une infinité d'autres points de cette suite, donc un point de P_x).

e) On pose, pour $0 \leqslant x < 1$, $g(x)=f(x)-[f(x)]$, puis $h(x)=\inf a_p$, où l'indice $p \geqslant 1$ parcourt l'ensemble des indices tels que $u_p(0) \geqslant x$. Montrer que h est croissante et continue dans $[0,1[$, et que

(1) $\qquad h(g(x)) \equiv h(x)+\theta \pmod 1$

Soit A l'ensemble des points de $[0,1[$ tels que $h^{-1}(y)$ soit un intervalle I_y non réduit à un point ; montrer que A est partout dense dans $[0,1[$ s'il n'est pas vide. Soit U l'ensemble ouvert, réunion des intérieurs $\mathring{I}_y$ des intervalles compacts I_y pour $y \in A$; montrer que, si U n'est pas vide, il est partout dense dans $[0,1[$ (s'il existait un intervalle ouvert ne contenant aucun point de U , montrer que h serait constante dans cet intervalle, contrairement à la définition de U) . Montrer que les ensembles parfaits P_x sont tous identiques au complémentaire de U par rapport à $[0,1[$ (utiliser l'identité (1), en distinguant le cas où $x \in U$ et celui où $x \notin U$).

f) Soit inversement h une fonction continue et strictement croissante dans $[0,1]$, telle que $h(0)=0$, $h(1)=1$; et soit θ un nombre irrationnel tel que $0 \leqslant \theta < 1$. Il existe une et une seule fonction f strictement croissante et continue dans $\mathbb{R}$, telle que $0 \leqslant f(0) < 1$, $f(x+1)=f(x)+1$, et que, si on pose $g(x)=f(x)-[f(x)]$, l'identité (1) soit vérifiée ; montrer que, pour la fonction f ainsi définie, $\lim_{n\to\infty} f_n(x)/n = \theta$, et que les ensembles parfaits P_x sont tous identiques à $[0,1]$.

g) De même, soit P un ensemble parfait contenu dans $[0,1]$, et dont le complémentaire U par rapport à cet intervalle soit partout dense. Montrer qu'on peut ranger les intervalles contigus à P en une suite (I_p) telle que la relation $a_h < a_k$ entraîne $x<y$ pour $x \in I_h$ et $y \in I_k$; en déduire qu'il existe une et une seule fonction h continue et croissante dans $[0,1[$ et telle que $h(x)=a_p$ pour $x \in I_p$. Montrer enfin qu'on peut définir une fonction f , strictement croissante et continue dans $\mathbb{R}$, telle que $f(x+1)=f(x)+1$, $0 \leqslant f(0) < 1$ et que, si on pose $g(x)=f(x)-[f(x)]$, l'identité (1) soit vérifiée ; mais ici il y a une infinité de fonctions vérifiant ces conditions ; pour chacune d'elles, on a $\lim_{n\to\infty} f_n(x)/n = \theta$ et les ensembles parfaits P_x sont tous identiques à P .

§2. Groupes à un paramètre.

On sait (chap.III, §1) que deux groupes topologiques peuvent être, en général, localement homéomorphes sans être localement isomorphes . Mais nous allons démontrer, dans ce paragraphe, le théorème fondamental suivant :

Théorème 1. Un groupe topologique localement homéomorphe à $\mathbb{R}$ est localement isomorphe à $\mathbb{R}$.

Ce théorème sera lui-même une conséquence du suivant :

Théorème 2. Soit E un espace topologique satisfaisant aux conditions suivantes :

1° Il existe un homéomorphisme f de l'intervalle $[0,1]$ sur E .

2° Il existe un voisinage V de $\omega=f(0)$ dans E , et une application continue $(x,y)\to xy$ de $V\times V$ dans E telle que :

a) $x(yz)=(xy)z$ lorsque les deux membres sont définis ;

b) $\omega x=x\omega=x$ quel que soit $x\in V$;

c) quels que soient x,y,z dans V, chacune des relations $xy=xz$, $yx=zx$, entraîne $y=z$.

Dans ces conditions, il existe un voisinage $W\subset V$ de ω , et un homéomorphisme φ de W sur l'intervalle $[0,1]$, tel que $\varphi(xy)=\varphi(x)+\varphi(y)$ pour tout couple de points (x,y) tel que $x\in W$, $y\in W$ et $xy\in W$.

Démonstration du théorème 2. Nous procéderons en plusieurs étapes.

1) Définition d'une relation d'ordre dans E . Soit g l'application réciproque de f ; par définition, la relation $x\leqslant y$ dans E sera équivalente à $g(x)\leqslant g(y)$; autrement dit, nous transportons sur E la structure d'ordre de $[0,1]$, au moyen de l'application biunivoque f (Ens. R, §8) ; E est ainsi totalement ordonné, et f est un isomorphisme de la structure d'ordre et de la structure topologique de $[0,1]$ sur celles de E . Il en résulte que toute propriété de $[0,1]$ qui ne fait intervenir que ces deux structures, se transporte à E . En particulier, les intervalles ouverts dans E ne sont pas vides ; les intervalles ouverts contenant un point x forment un système fondamental de voisinages de x .

On peut toujours supposer que V est un intervalle fermé $[\omega,a]$ de E , qui est donc compact et connexe ; on a $g(V)=[0,a]$.

Lemme 1. Si x,y,z appartiennent à V , la relation $x \leqslant y$ entraîne $xz \leqslant yz$ et $zx \leqslant zy$.

Il suffit de prouver que $x<y$ entraîne $xz<yz$ et $zx<zy$, c'est-à-dire $g(xz)<g(yz)$ et $g(zx)<g(zy)$. Posons $g(z)=\xi$; les fonctions numériques $g(xf(\xi))-g(yf(\xi))$ et $g(f(\xi)x)-g(f(\xi)y)$ sont continues pour $\xi \in [0,a]$; pour $\xi=0$, elles sont <0 par hypothèse ; d'autre part, elles ne peuvent s'annuler dans $[0,a]$, puisqu'il en résulterait $xz=yz$ ou $zx=zy$, donc $x=y$, contrairement à l'hypothèse. D'après le théorème de Bolzano (chap.IV, §6, th.1), ces fonctions sont strictement négatives dans $[0,a]$, ce qui démontre le lemme.

2) L'"axiome d'Archimède" dans V. D'après l'hypothèse, le carré x^2 de tout élément $x \in V$ est défini ; par récurrence, on définit pour un entier $p>0$, l'élément x^p comme égal à $x^{p-1}x$, lorsque $x^{p-1} \in V$. On voit par récurrence que, si $x_0 \in V$ est tel que $x_0^{p-1}<a$ la fonction x^p est définie et continue dans un intervalle ouvert contenant x_0 ; en particulier comme $\omega^p=\omega$ quel que soit p , la fonction x^p est définie et continue dans un intervalle $V_p=[\omega,a_p]$ $(a_p>\omega)$. Si $p=q+r$ (p et r entiers >0) et si x^p est définie, on a $x^p=x^qx^r$ d'après l'associativité du produit ; si $x>\omega$ et $p>q$, $x^q<x^p$; enfin, si $x<y \leqslant a$, et si y^p est défini, il en est de même de x^p et on a $x^p<y^p$ (en effet, si $x^{p-1}<y^{p-1}$, on a $x^p<y^{p-1}x<y^p$) .

Pour un $x \in V$ donné, l'ensemble des entiers $p>0$ tels que x^p soit défini et appartienne à V ne peut être qu'un intervalle $[1,n]$ de $\mathbb{N}$, ou l'ensemble $\mathbb{N}$ lui-même. Nous allons montrer que c'est toujours le premier de ces deux cas qui se présente ; de façon plus précise, nous démontrerons pour E la proposition correspondant à l'"axiome d'Archimède dans $\mathbb{R}$ (chap. IV, §2, th. 1) :

Lemme 2. Si $\omega < x < y \leqslant a$, il existe un entier n tel que $x^n \in V$ et $x^n \leqslant y < x^{n+1}$.

Supposons au contraire que l'on ait $x^p \leqslant y$ quel que soit p ; la suite (x^p) est croissante et majorée dans E, elle a donc (chap.IV, § 5, th.2) une limite $b \leqslant y$. Comme $b \in V$, bx est définie et on a $b < bx$, puisque $x > \omega$; mais $bx = (\lim_{p\to\infty} x^p).x = \lim_{p\to\infty} x^{p+1}$ (d'après la continuité du produit au point (b,x)) ; donc $bx = b$, contrairement à ce qui précède.

3) Définition de la racine $p^{ème}$ dans V. Etant donné l'entier $p > 0$ soit b_p la borne supérieure, dans V, de l'ensemble des $x \in V$ tels que x^p soit défini et appartienne à V. Montrons que $(b_p)^p = a$. En effet, on ne peut avoir $(b_p)^p < a$, car x^p serait alors continue au point b_p, et comme c'est une fonction strictement croissante, il existerait $x > b_p$ tel que $(b_p)^p < x^p < a$, contrairement à la définition de b_p. D'autre part, supposons que $q < p$ soit le plus grand entier tel que $(b_p)^q \leqslant a$; la fonction x^{q+1} étant alors continue au point b_p, il existerait $x < b_p$ tel que $a < x^{q+1} < (b_p)^{q+1}$, contrairement à l'hypothèse, puisque $x^{q+1} \leqslant x^p \leqslant a$. On a donc bien $(b_p)^p = a$.

Il en résulte que l'application $x \to x^p$ est strictement croissante et continue dans l'intervalle $W_p = [\omega, b_p]$ de E ; c'est donc un homéomorphisme de W_p sur V (chap.IV, § 2, th.5) ; on désignera par $x^{1/p}$ la valeur de son application réciproque pour $x \in V$ ("racine $p^{ème}$ de x") ; cette application est strictement croissante et continue dans V.

4) Définition de φ. Soit $r = p/q$ un nombre rationnel tel que $0 \leqslant r \leqslant 1$. Posons $a^r = (a^{1/q})^p$, définition qui a un sens d'après ce qui précède ; cette définition ne dépend bien que de r et non de sa représentation comme quotient de deux entiers, car pour tout entier $k > 0$, on a $(a^{1/kq})^{kq} = a$, donc $((a^{1/kq})^k)^q = a$, $a^{1/q} = (a^{1/kq})^k$, $a^{1/kq} = (a^{1/q})^{1/k}$;

donc $(a^{1/kq})^{kp} = ((a^{1/kq})^k)^p = (a^{1/q})^p$. Nous définirons la fonction ψ dans $Q \cap [0,1]$ en posant $\psi(r)=a^r$. C'est une application <u>strictement croissante</u> de $Q \cap [0,1]$ dans V , car si $p/q < p'/q'$, on a

$$a^{p/q} = (a^{1/qq'})^{pq'} < (a^{1/qq'})^{p'q} = a^{p'/q'}$$

En outre, si $r=p/q$ et $r'=p'/q'$ sont tels que $r+r' \leqslant 1$, on a

$$a^{r+r'} = (a^{1/qq'})^{pq'+p'q} = ((a^{1/qq'})^{pq'}).((a^{1/qq'})^{p'q}) = a^r . a^{r'}$$

autrement dit $\psi(r+r') = \psi(r)\psi(r')$.

Soit maintenant ρ un point quelconque de $[0,1]$; lorsque r tend vers ρ en restant dans Q , nous allons voir que $\psi(r)$ a une limite dans V. En effet, si r tend vers ρ en restant $\leqslant \rho$, $\psi(r)$ tend vers une limite b , d'après le théorème de la limite monotone (ch.IV, §5, th.2) . Soit $]c,d[$ un intervalle ouvert quelconque de V , contenant b ; il existe $x > \omega$ tel que $b < bx < d$; d'après le lemme 2 il existe un entier n tel que $a^{1/n} < x$; si alors r et r' sont deux nombres rationnels tels que $r \leqslant \rho \leqslant r'$ et $r'-r \leqslant 1/n$,,on aura $a^r \leqslant b$ et $a^{r'} = a^r a^{r'-r} < a^r a^{1/n} < a^r x \leqslant$ $\leqslant bx < d$; comme d'ailleurs $a^{r'} \geqslant b$, on voit que a^r tend aussi vers b lorsque r tend vers ρ en restant $\geqslant \rho$. D'après le théorème de prolongement (chap.I, §6, th.1), on peut prolonger ψ en une application <u>continue</u> de $[0,1]$ dans V .

En vertu du principe de prolongement des inégalités (chap.IV, §5, th1) ψ est croissante dans $[0,1]$; si $0 \leqslant \rho < \rho' \leqslant 1$, il existe deux nombres rationnels r,r' tels que $\rho \leqslant r < r' \leqslant \rho'$, donc $\psi(\rho) \leqslant \psi(r) < \psi(r') \leqslant$ $\leqslant \psi(\rho')$ autrement dit ψ est <u>strictement croissante</u> dans $[0,1]$, et par suite (chap.IV, §2, th.5) est un <u>homéomorphisme</u> de $[0,1]$ <u>sur</u> V . D'autre part, si ρ et ρ' sont tels que $\rho+\rho' \leqslant 1$, on a , par passage à la limite $\psi(\rho+\rho') = \psi(\rho)\psi(\rho')$, d'après la continuité de xy dans $V \times V$.

Soit alors φ l'application réciproque de ψ . C'est un homéomorphisme de V sur $[0,1]$; soient x et y deux points de V tels que $xy \in V$ et posons $\xi = \varphi(x)$, $\eta = \varphi(y)$, $\zeta = \varphi(xy)$; on a $\xi \leqslant \zeta$, donc on peut écrire $\zeta = \xi + \eta'$, d'où $xy = \psi(\zeta) = \psi(\xi)\psi(\eta') = x.\psi(\eta')$; donc $y = \psi(\eta')$, $\eta' = \varphi(y) = \eta$ et par suite $\varphi(xy) = \varphi(x) + \varphi(y)$.

C. Q. F. D.

Démonstration du théorème 1. Soit V un voisinage de l'unité e d'un groupe G , tel qu'il existe un homéomorphisme f de l'intervalle $[-1,+1]$ sur V . De même que dans la première partie de la démonstration du th.2, on transporte sur V la structure d'ordre de $[-1,+1]$, au moyen de l'application biunivoque f ; si W est un voisinage symétrique de e tel que $W^2 \subset V$, on démontre, comme dans le lemme 1, que pour $x \in W$, $y \in W$ et $z \in W$, la relation $x \leqslant y$ entraîne $xz \leqslant yz$ et $zx \leqslant zy$; en particulier, comme $x \in W$ entraîne $x^{-1} \in W$ par hypothèse, les relations $x \geqslant e$ et $x^{-1} \leqslant e$ sont équivalentes ; de même, si $x \in W$ et $y \in W$, les relations $x \geqslant e$, $y \geqslant e$ entraînent $xy \geqslant e$. On peut évidemment supposer que l'ensemble W_+ des éléments $x \geqslant e$ de W est l'image par f d'un intervalle $[0,a)$. D'après le th.2, il existe donc un homéomorphisme φ de W_+ sur $[0,1]$, tel que les conditions $x \in W_+$, $y \in W_+$, $xy \in W_+$, entraînent $\varphi(xy) = \varphi(x) + \varphi(y)$. Si $x \in W$ est tel que $x \leqslant e$, on a $x^{-1} \in W_+$; nous prolongerons φ à W en posant alors $\varphi(x) = -\varphi(x^{-1})$; en vertu de la continuité de x^{-1} , il est clair que φ , ainsi prolongée, est un homéomorphisme de W sur $[-1,+1]$.

D'autre part, soient x et y deux éléments de W tels que $x \geqslant e$, $y \leqslant e$; on a donc $y^{-1} \in W_+$. Supposons d'abord $y^{-1} \leqslant x$; alors $e \leqslant xy \leqslant x$, donc $xy \in W_+$, et $(xy)y^{-1} = x \in W_+$; d'où $\varphi(x) = \varphi(xy) + \varphi(y^{-1}) = \varphi(xy) - \varphi(y)$, $\varphi(xy) = \varphi(x) + \varphi(y)$. Si au contraire $x \leqslant y^{-1}$, on a $e \leqslant (xy)^{-1} \leqslant y^{-1}$

et $(xy)^{-1}x=y^{-1}\in W_+$, donc $\varphi(y^{-1})=\varphi((xy)^{-1})+\varphi(x)$, ce qui démontre encore $\varphi(xy)=\varphi(x)+\varphi(y)$. Enfin, si $x\leqslant e$, $y\leqslant e$, et $xy\in W$, on a $y^{-1}\in W_+$, $x^{-1}\in W_+$, $(xy)^{-1}=y^{-1}x^{-1}\in W_+$, donc $\varphi((xy)^{-1})=\varphi(x^{-1})+\varphi(y^{-1})$, d'où $\varphi(xy)=\varphi(x)+\varphi(y)$. L'application φ est donc un <u>isomorphisme local</u> de G dans R .

C.Q.F.D.

<u>Corollaire</u>. <u>Dans un groupe localement homéomorphe à R , il existe un voisinage de l'unité dont deux points quelconques sont permutables</u>.

<u>Groupes à un paramètre</u>. <u>Définition 1</u>. <u>On dit qu'un groupe topologique est un groupe à un paramètre s'il est localement homéomorphe au groupe additif R</u> .

Le théorème 1 montre que tout groupe à un paramètre est <u>localement isomorphe</u> à R ; d'après le th.2 du §1 , on voit donc que :

<u>Théorème 3</u>. <u>Un groupe connexe à un paramètre est isomorphe à R ou à T</u>.

<u>Remarque</u>. La dénomination traditionnelle de "groupe à un paramètre" ne doit pas faire perdre de vue que l'hypothèse que le groupe est <u>connexe</u> est essentielle pour la validité du th.3 . Il est clair, par exemple, que le <u>produit</u> de R (ou T) et d'un groupe <u>discret</u> quelconque G , est un groupe (non connexe) à un paramètre ; on peut prendre, par exemple pour G le groupe additif des nombres réels, muni de la topologie discrète ; la structure de <u>groupe</u> de $G\times R$ est alors isomorphe à celle de $R\times R$ mais $G\times R$ est un groupe topologique à un paramètre, alors qu'il n'en est pas de même du groupe topologique $R\times R$, comme nous le verrons au chap. VI (§ 1).

Soit G un groupe topologique isomorphe à R , noté <u>multiplicativement</u> et a un élément quelconque de G , distinct de l'élément unité e de G .

Il existe par hypothèse un isomorphisme f de $\mathbf{R}$ sur G ; soit $a \neq 0$ l'élément de $\mathbf{R}$ tel que $f(a)=a$; l'application $\xi \to f(a\xi)$ est encore un isomorphisme f_a de $\mathbf{R}$ sur G tel que $f_a(1)=a$. Inversement, si g est un isomorphisme de $\mathbf{R}$ sur G tel que $g(1)=a$, et si φ_a est l'application réciproque de f_a , $h = \varphi_a \circ g$ est un automorphisme de $\mathbf{R}$ tel que $h(1)=1$, donc (§ 1, prop. 2) h est l'application identique et $g=f_a$; d'où :

Proposition 1. Si G est un groupe à un paramètre isomorphe à $\mathbf{R}$, et a un point $\neq e$ de G , il existe un isomorphisme et un seul f_a de $\mathbf{R}$ sur G , tel que $f_a(1)=a$.

Lorsqu'on a choisi un isomorphisme f de $\mathbf{R}$ sur G , l'élément $a=f(1)=f_a(1)$ est parfois appelé "unité de mesure" dans G (voir Appendice). Soit b un élément de G distinct de e et de a ; si φ_a est l'isomorphisme réciproque de f_a , l'application $\xi \to f_a(\xi . \varphi_a(b))$ est un isomorphisme de $\mathbf{R}$ sur G , dont la valeur pour $\xi = 1$ est b ; on a donc identiquement

$$f_b(\xi) = f_a(\xi . \varphi_a(b)) \tag{1}$$

formule dite "du changement d'unité" ; elle est équivalente à l'identité

$$\varphi_a(x) = \varphi_a(b).\varphi_b(x) \tag{2}$$

Soit maintenant G un groupe à un paramètre, noté multiplicativement , et isomorphe à $\mathbf{T}$. Si f et g sont deux isomorphismes de $\mathbf{T}$ sur G , et h l'application réciproque de g , $h \circ f$ est un automorphisme de $\mathbf{T}$, donc (§ 1, prop.8) est l'application identique ou la symétrie $x \to -x$; les seuls isomorphismes de $\mathbf{T}$ sur G sont donc f et $x \to f(-x) = (f(x))^{-1}$.

D'après la prop.9 du § 1, on en déduit que tout homomorphisme de $\mathbf{R}$ sur G est de la forme $\xi \to f(\varphi(a\xi))$, où a est un nombre réel $\neq 0$ (φ application canonique de $\mathbf{R}$ sur $\mathbf{T}$) ; l'intervalle $\left]-\frac{|a|}{2}, +\frac{|a|}{2}\right[$

est <u>le plus grand intervalle ouvert symétrique</u> de $\mathbb{R}$ que cet homomorphisme applique <u>biunivoquement</u> dans G . Les seuls homomorphismes de $\mathbb{R}$ sur G pour lesquels l'intervalle $\left]-\frac{|a|}{2}, +\frac{|a|}{2}\right[$ ait cette propriété sont donc $\xi \to f(\varphi(a\,\xi))$ et $\xi \to f(\varphi(-a\,\xi))$. Supposons $a>0$, et désignons par u l'un des deux points de G tels que $u^4=e$, $u^2\neq e$; u est l'image de $a/4$ par l'un des homomorphismes précédents, de $-a/4$ par l'autre ; nous désignerons par f_a celui de ces deux homomorphismes pour lequel $f_a(a/4)=u$. Ainsi :

<u>Proposition 2</u>. <u>Si G est un groupe à un paramètre isomorphe à</u> $\mathbb{T}$, <u>et</u> a <u>un nombre réel</u> >0, <u>il existe un homomorphisme et un seul</u> f_a <u>de</u> $\mathbb{R}$ <u>sur G tel que</u> : 1° $\left]-\frac{a}{2}, +\frac{a}{2}\right[$ <u>soit le plus grand intervalle ouvert symétrique dont l'image par</u> f_a <u>soit biunivoque</u> ; 2° $f_a(a/4)=u$.

Il est clair que, si β est un second nombre >0 , l'application $\xi \to f_a(\beta\,\xi/a)$ est un homomorphisme de $\mathbb{R}$ sur G tel que l'intervalle $\left]-\frac{\beta}{2}, +\frac{\beta}{2}\right[$ soit le plus grand intervalle ouvert symétrique dont l'image dans G soit biunivoque ; en outre l'image de $\beta/4$ par cet homomorphisme est égal à u ; donc on a l'identité

$$(5) \qquad f_\beta(\xi) = f_a(\beta\,\xi/a)$$

qu'on appelle encore "formule du changement d'unité" .

<u>Exercices</u>. 1) Si G est un groupe à un paramètre, la composante connexe de l'unité dans G est un sous-groupe distingué H isomorphe à $\mathbb{R}$ ou $\mathbb{T}$, et G/H est un groupe discret.

2) Si G est un groupe <u>compact</u> à un paramètre, la composante connexe de l'unité dans G est un sous-groupe distingué H isomorphe à $\mathbb{T}$, et G/H est un groupe fini.

§ 3. Exponentielles et logarithmes.

On a vu au chap. IV (§ 3) que la topologie induite par celle de $\mathbf{R}$ sur le groupe multiplicatif $\mathbf{R}_+^*$ des nombres réels strictement positifs, est compatible avec la structure de groupe de $\mathbf{R}_+^*$, et définit donc une structure de groupe topologique sur $\mathbf{R}_+^*$. Tout intervalle ouvert contenu dans $\mathbf{R}_+^*$ et contenant l'unité +1 de $\mathbf{R}_+^*$ est homéomorphe à un voisinage de 0 dans $\mathbf{R}$, donc $\mathbf{R}_+^*$ est un groupe à un paramètre ; comme il est connexe et non compact, il est isomorphe à $\mathbf{R}$. D'après la prop. 1 du § 2, quel que soit le nombre $a>0$ et $\neq 1$, il existe un isomorphisme et un seul f_a de $\mathbf{R}$ sur $\mathbf{R}_+^*$, tel que $f_a(1)=a$. Quels que soient x et y dans $\mathbf{R}$, on a donc

(1) $$f_a(x+y) = f_a(x).f_a(y)$$

(2) $$f_a(-x) = 1/f_a(x)$$

et en particulier, pour tout n entier (positif ou négatif)

(3) $$f_a(n) = a^n$$

En raison de cette relation, on pose, pour tout $x \in \mathbf{R}$, $f_a(x)=a^x$; les fonctions a^x (pour toutes les valeurs >0 et $\neq 1$ de a) sont dites fonctions exponentielles ; on pose aussi $1^x=1$ pour tout $x \in \mathbf{R}$.

L'isomorphisme de $\mathbf{R}_+^*$ sur $\mathbf{R}$, réciproque de a^x, s'appelle logarithme de base a, et sa valeur pour $x \in \mathbf{R}_+^*$ se note $\log_a x$. On a donc, avec ces notations

(4) $a^{x+y}=a^x a^y$ quels que soient $x \in \mathbf{R}$, $y \in \mathbf{R}$;

(5) $a^{-x}=1/a^x$ quel que soit $x \in \mathbf{R}$;

(6) $\log_a 1 = 0$, $\log_a a=1$;

(7) $\log_a(xy)=\log_a x + \log_a y$ quels que soient $x>0$, $y>0$;

(8) $\log_a(1/x)=-\log_a x$ quel que soit $x>0$;

(9) $a^{\log_a x} = x$ quel que soit $x>0$;

(10) $\log_a(a^x)=x$ quel que soit $x \in \mathbf{R}$.

D'après la prop.1 du § 2, tout isomorphisme de $\mathbf{R}$ sur $\mathbf{R}_+^*$ est une exponentielle ; la formule (1) du § 2 s'écrit ici

(11) $\quad x^y = a^{y.\log_a x}$ quels que soient $x > 0$ et $y \in \mathbf{R}$

ou encore, en changeant les notations

(12) $\quad (a^x)^y = a^{xy}$ quels que soient $x \in \mathbf{R}$, $y \in \mathbf{R}$ et $a > 0$.

En particulier, on a, pour tout entier $n > 0$, $(a^{1/n})^n = a$, ce qui montre que $a^{1/n}$ est identique à la racine $n^{\text{ème}}$ $\sqrt[n]{a}$ définie au chap. IV, § 3.

De même, la formule (2) du § 2 s'écrit ici

(13) $\quad \log_a x = \log_a b . \log_b x$ pour tout $x > 0$

(formule dite du changement de base) ; elle est évidemment équivalente à (11) et(12), ou encore, en changeant les notations, à

(14) $\quad \log_a(x^y) = y.\log_a x$ quels que soient $x > 0$ et $y \in \mathbf{R}$.

Cherchons enfin les automorphismes du groupe topologique $\mathbf{R}_+^*$; si g est un tel automorphisme, $\log_a(g(a^x))$ est un automorphisme de $\mathbf{R}$, et réciproquement ; donc (§ 1, prop.2), il existe $\alpha \in \mathbf{R}$ tel que $\log_a(g(a^x)) = \alpha x$ quel que soit $x \in \mathbf{R}$; d'où, en vertu de (12) on tire l'identité $g(x) = x^\alpha$ quel que soit $x > 0$. On a donc identiquement

(15) $\quad (xy)^\alpha = x^\alpha y^\alpha$ quels que soient $x > 0$, $y > 0$.

Les formules (7), (8) et (14) font des logarithmes un instrument précieux en Calcul numérique, où l'addition est la seule opération à laquelle soit vraiment adapté le système de numération en usage. On a donc construit des tables donnant (avec une certaine approximation) le logarithme d'un nombre donné, ou inversement un nombre dont on connaît le logarithme; pour leur construction et leur usage, nous renvoyons à la partie de cet ouvrage consacrée au Calcul numérique.

Le choix de la base a obéit à des considérations de nature diverse ; pour la commodité des calculs dans le système décimal, on emploie le plus souvent les logarithmes de base $a=10$ (logarithmes décimaux, ou de Briggs) ; mais en mathématique, on est amené, par des considérations de calcul différentiel, à utiliser de préférence les logarithmes ayant pour base un nombre noté e (et égal à 2,718...), qui est défini comme le seul nombre $a>0$ tel que $\lim_{x\to 0, x\neq 0} (a^x-1)/x=1$ (voir Livre V); les logarithmes de base e sont dits logarithmes naturels ou népériens.

Variation des fonctions a^x et $\log_a x$. Comme $x \to a^x$ est un homéomorphisme de $\mathbf{R}$ sur l'intervalle $\mathbf{R}_+^* =]0,+\infty[$, a^x est strictement monotone (chap.IV, § 2, th.5) ; si $a>1$, on a $a^1 > a^0$, donc a^x est strictement croissante ; en outre, $\mathbf{R}_+^*$ n'étant pas borné supérieurement, a^x n'est pas bornée supérieurement dans $\mathbf{R}$, donc

(16) $$\lim_{x\to+\infty} a^x = +\infty \qquad (a>1)$$

et, d'après (5)

(17) $$\lim_{x\to-\infty} a^x = 0 \qquad (a>1)$$

Au contraire, si $a<1$, a^x est strictement décroissante dans $\mathbf{R}$, tend vers 0 lorsque x tend vers $+\infty$, vers $+\infty$ quand x tend vers $-\infty$ (fig.).

De ces propriétés, et de (15), on déduit que, si $0<a<b$, on a $a^x<b^x$ pour $x>0$, $a^x>b^x$ pour $x<0$; cela revient en effet à constater que $(b/a)^x>1$ pour $x>0$, $(b/a)^x<1$ pour $x<0$.

La variation de $\log_a x$ dans $\mathbf{R}_+^*$ se déduit de celle de a^x dans $\mathbf{R}$; si $a>1$, $\log_a x$ est strictement croissante, tend vers $-\infty$ quand x tend vers 0 , vers $+\infty$ quand x tend vers $+\infty$; si $a<1$, $\log_a x$

est strictement décroissante, tend vers $+\infty$ quand x tend vers 0, vers $-\infty$ quand x tend vers $+\infty$ (fig.).

On peut <u>prolonger par continuité</u> la fonction a^x (resp. $\log_a x$) dans $\overline{R}$ (resp. dans l'intervalle $[0,+\infty]$ de $\overline{R}$), en lui donnant aux points $+\infty$ et $-\infty$ (resp. 0 et $+\infty$) ses valeurs limites en ces points.

Plus généralement, la formule (11) montre que la fonction x^y est <u>continue</u> dans le sous-espace $R_+^* \times R$ de R^2 ; en outre, elle tend vers une limite lorsque (x,y) tend vers un point (a,b) de $\overline{R} \times \overline{R}$ adhérent à $R_+^* \times R$, à l'exception des points (0,0), $(+\infty,0)$, $(1,+\infty)$, $(1,-\infty)$; autrement dit, l'expression x^y a un sens pour tout $x \geqslant 0$ (fini ou non) et pour tout $y \in \overline{R}$, à l'exception des expressions 0^0, $(+\infty)^0$, $1^{+\infty}$, $1^{-\infty}$ (qu'on appelle encore "formes indéterminées").

On vérifie immédiatement que, dans les formules (4),(7) et (12), si l'un des deux membres a un sens, il en est de même de l'autre, qui lui est alors égal.

Pour une valeur donnée $y=a$, finie et $\neq 0$, x^a est fonction continue de x dans $[0,+\infty]$; elle est <u>strictement croissante</u> si $a>0$, <u>strictement décroissante</u> si $a<0$ (fig.).

<u>Familles multipliables de nombres positifs</u>. Les relations (4) et (7) étant vérifiées chaque fois que l'un des membres de ces relations est défini, on voit que, <u>pour qu'une famille</u> (x_ι) <u>de nombres réels positifs</u> (finis ou non) <u>soit multipliable, il faut et il suffit que la famille</u> $(\log_a x_\iota)$ <u>soit sommable dans</u> $\overline{R}$; et on a alors

$$\prod_\iota x_\iota = a^{\sum_\iota \log_a x_\iota} \tag{18}$$

De même, pour que le produit infini défini par la suite $(1+u_n)$ de nombres $\geqslant 0$ soit <u>convergent</u> dans $[0,+\infty]$, il faut et il suffit que

la série définie par la suite $(\log_a(1+u_n))$ soit <u>convergente</u> dans R, et on a

$$(19) \qquad \prod_{n=0}^{\infty}(1+u_n) = a^{\sum_{n=0}^{\infty}\log_a(1+u_n)}$$

Ces propositions, qui résultent immédiatement de l'isomorphisme des groupes R et R_+^*, ramènent donc l'étude des produits infinis à celle des sommes infinies de nombres réels, dont les termes sont des logarithmes ; nous verrons au Livre V que ces dernières s'étudient aisément à l'aide des propriétés différentielles du logarithme.

<u>Exercices</u>. 1) Soit (a_i) une suite finie de nombres $\geqslant 0$, r et s deux nombres réels tels que $0<r<s$; montrer que

$$\left(\sum_{i=1}^{n} a_i^s\right)^{1/s} \leqslant \left(\sum_{i=1}^{n} a_i^r\right)^{1/r}$$

l'égalité n'ayant lieu que si tous les a_i sauf un sont nuls. (se ramener au cas où $\sum_{i=1}^{n} a_i^r = 1$).

2) Si $a>0$ et $a\neq 1$, on a, pour $0<x<y$

$$(a^x-1)/x < (a^y-1)/y$$

(le démontrer d'abord pour x entier >0 et $y=x+1$, puis en déduire la proposition pour x et y rationnels, et passer enfin au cas général). En déduire que la fonction $(a^x-1)/x$ (définie pour $x\neq 0$), a une limite quand x tend vers 0 en restant $\neq 0$; si h(a) est cette limite, montrer que, pour a et b strictement positifs, $h(b)=h(a).\log_a b$.

3) Soit (a_n) une suite de nombres >0 ; on appelle <u>exposant de convergence</u> de cette suite, la borne supérieure λ de l'ensemble des nombres σ tels que la somme $\sum_{n=0}^{\infty} a_n^{-\sigma}$ soit finie. Montrer que $\lambda = \lim_{n\to\infty}\sup(\log n/\log a_n)$ (les logarithmes étant pris par rapport à une base quelconque).

4) Si la suite (x_n) de nombres réels est telle que $|x_i - x_j| \geqslant \delta > 0$ pour $i \neq j$, l'exposant de convergence de la suite $(|x_n|)$ est inférieur à 1.

5) Soit (r_n) une suite croissante de nombres >0, telle que $\lim_{n\to\infty} r_n = +\infty$; on désigne par $N(r)$, pour tout $r \geqslant 0$, le plus grand indice n tel que $r_n \leqslant r$. Montrer que

$$\limsup_{r\to\infty}(\log N(r)/\log r) = \limsup_{n\to\infty}(\log n/\log r_n)$$
$$\liminf_{r\to\infty}(\log N(r)/\log r) = \liminf_{n\to\infty}(\log n/\log r_n).$$

¶ 6) Soit f une fonction finie, strictement positive, définie dans l'intervalle $[0,+\infty[$, croissante et telle que

$$\lim_{x\to+\infty}(f(2x)/f(x)) = 1.$$

Montrer que, pour tout nombre $c>0$, $\lim_{x\to+\infty}(f(cx)/f(x))=1$ (le démontrer d'abord pour $c=2^k$, puis pour $c \geqslant 1$). Montrer que $\lim_{x\to+\infty}(\log f(x)/\log x)=0$ (se ramener au cas où x ne prend que les valeurs 2^k).

§ 3. Nombres complexes. Angles.

Définition des nombres complexes. On a vu (chap.IV, § 3) que le corps R des nombres réels est un corps ordonné, donc quasi-réel (Alg., chap.VI).

Proposition 1. Le corps des nombres réels R est un corps quasi-réel maximal (Alg., chap. VI).

Pour le voir, il suffit (Alg., chap.VI) de montrer d'une part que tout élément $\geqslant 0$ a une racine carrée dans R, et d'autre part que tout polynome de degré impair à coefficients dans R possède au moins une racine dans R. Nous avons déjà démontré la première de ces propositions (chap. IV, § 3). D'autre part, si $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ est un polynome de degré impair n $(a_0\neq 0)$, en le prolongeant par continuité à $\overline{R}$ (chap. IV, § 4), on obtient une fonction qui prend

des valeurs infinies de signes opposés aux points $+\infty$ et $-\infty$; comme $\overline{R}$ est connexe, cette fonction s'annule dans R, d'après le théorème de Bolzano (chap.IV, § 6, th.2).

On sait donc (Alg.,chap.VI) qu'en adjoignant à R une racine i de l'équation $x^2+1=0$, on obtient un corps algèbriquement clos.

Définition 1. On appelle corps des nombres complexes, et on désigne par C, le corps algèbriquement clos obtenu par adjonction algèbrique d'une racine i du polynome x^2+1, au corps R des nombres réels ; les éléments de C sont appelés nombres complexes.

On sait que R peut être considéré comme un sous-corps de C, et que tout élément $z \in C$ peut se mettre d'une manière et d'une seule sous la forme $x+iy$, où x et y sont réels ; x est appelé partie réelle de z, et se note $\mathcal{R}(z)$, y la partie imaginaire de z et se note $\mathcal{I}(z)$; les nombres complexes de la forme yi (y réel) sont dits imaginaires purs.

La relation $x+iy=0$ (x et y réels) est donc équivalente à "$x=0$ et $y=0$". Comme $i^2=-1$, les éléments de C, donnés par leurs parties réelles et imaginaires, satisfont évidemment aux règles de calcul suivantes :

$$(1) \qquad (x+iy)+(x'+iy') = (x+x')+i(y+y')$$

$$(2) \qquad (x+iy)(x'+iy') = (xx'-yy')+i(xy'+yx')$$

En particulier $(x+iy)(x-iy)=x^2+y^2 \in R$; d'où, si $x+iy \neq 0$

$$(3) \qquad 1/(x+iy) = (x/(x^2+y^2))+i(y/(x^2+y^2))$$

On a donc, pour tout entier n

$$i^{4n}=+1 \ , \quad i^{4n+1}=i \ , \quad i^{4n+2}=-1 \ , \quad i^{4n+3}=-i \ .$$

La seconde racine du polynome x^2+1 dans C n'est autre que -i ; on en conclut (alg.,chap.VI), que le seul automorphisme de C, distinct de l'application identique, et qui laisse invariants les éléments de R,

est l'application faisant correspondre à tout nombre complexe $z=x+iy$, le nombre complexe $x-iy$, qu'on note $\bar{z}$, et qu'on appelle nombre complexe <u>conjugué</u> de z ; on a $\mathcal{R}(z) = (z+\bar{z})/2$, $\mathcal{I}(z) = (z-\bar{z})/2i$. En vertu de cet automorphisme, si $f(z)$ est un polynome à coefficients <u>réels</u>, on a $f(\bar{z}) = \overline{f(z)}$ quel que soit $z \in \mathbb{C}$.

Un nombre complexe $z=x+iy$ est racine de l'équation du second degré $(t-z)(t-\bar{z})=0$, qui s'écrit encore $t^2-2xt+(x^2+y^2)=0$, et a donc ses coefficients réels. Conformément aux définitions générales (Alg., chap.VI), le terme constant $x^2+y^2=z\bar{z}$ de cette équation s'appelle la <u>norme</u> de z ; c'est un nombre $\geqslant 0$, qui n'est nul que si $z=0$. Le nombre positif $\sqrt{z\bar{z}} = \sqrt{x^2+y^2}$ se réduit à la valeur absolue de z lorsque z est réel ; aussi l'appelle-t-on encore <u>valeur absolue</u> de z et le note-t-on $|z|$ dans le cas où z est un nombre complexe quelconque. La relation $|z| = 0$ est équivalente à $z=0$. Si z et z' sont deux nombres complexes, le conjugué de zz' est $\bar{z}.\bar{z}'$, donc $|zz'|^2 = zz'\overline{zz'} = |z|^2|z'|^2$ d'où $|zz'| = |z|.|z'|$: <u>la valeur absolue d'un produit est le produit des valeurs absolues des facteurs</u> (cf. Alg.,chap.VI, pour la propriété générale correspondante des <u>normes</u>).

En particulier, si on fait $z'= 1/z$ dans cette relation $(z\neq 0)$, on a $|1/z| = 1/|z|$.

On remarquera que le quotient z'/z de deux nombres complexes $(z\neq 0)$ peut s'écrire $z'\bar{z}/z\bar{z} = z'\bar{z}/|z|^2$, ce qui permet de calculer aisément sa partie réelle et sa partie imaginaire.

Montrons enfin que l'on a encore, quels que soient les nombres complexes z,z', l'<u>inégalité du triangle</u>

$$|z+z'| \leqslant |z| + |z'| \tag{4}$$

Si on pose $z=x+iy$, $z'=x'+iy'$, cela revient à vérifier que

$$(xx'+yy')^2 \leqslant (x^2+y^2)(x'^2+y'^2)$$

c'est-à-dire $$(xy'-yx')^2 \geqslant 0$$

On voit en même temps que les deux membres de (4) ne peuvent être égaux que si $xy'-yx'=0$; cette condition nécessaire signifie que l'on a , soit $z=0$, soit $z'=0$, soit $z'=\lambda z$ avec λ réel; mais dans ce dernier cas, on a $|z+z'| = |1+\lambda| . |z|$ et $|z| + |z'| = (1+|\lambda|).|z|$; donc il faut en outre, pour que les deux membres de (4) soient égaux, que λ soit un nombre positif, et cette condition est alors suffisante.

Topologie de $\mathbb{C}$. L'application $(x,y) \to x+iy$ du plan numérique $R^2 = R \times R$ sur $\mathbb{C}$ est biunivoque ; si on munit R^2 de la topologie produit de la topologie de la droite numérique par elle-même, on peut transporter à $\mathbb{C}$ cette topologie au moyen de l'application précédente. Cette topologie est compatible avec la structure de corps de $\mathbb{C}$ (chap.III, § 5) ; en effet, d'après (1) et (2) (les fonctions $z+z'$ et zz' sont continues dans $\mathbb{C} \times \mathbb{C}$ chap.I, § 8, cor.2 du th.1) ; et de même, d'après (3), $1/z$ est continue dans le complémentaire $\mathbb{C}^*$ du point $z=0$ dans $\mathbb{C}$.

En munissant l'ensemble $\mathbb{C}$ de cette topologie et de la structure de corps définie plus haut (déf. 1), on définit donc sur $\mathbb{C}$ une structure de corps topologique (chap.III, § 5) ; quand nous parlerons de la topologie de $\mathbb{C}$, c'est toujours de la topologie précédente qu'il sera question.

On notera que la définition de la structure de corps topologique de $\mathbb{C}$ est indépendante du fait que $\mathbb{C}$ est un corps algèbriquement clos ; et on peut, en s'appuyant sur les propriétés topologiques de $\mathbb{C}$, démontrer que $\mathbb{C}$ est algèbriquement clos ("théorème de d'Alembert")

sans utiliser la théorie des corps quasi-réels (voir exerc.2, et aussi la partie de cet ouvrage consacrée à la Topologie combinatoire où le théorème de d'Alembert sera démontré comme conséquence de résultats sur le degré d'application).

Dans la suite, on identifiera très souvent les ensembles $\mathbb{C}$ et $\mathbb{R}^2$, considérés comme espaces topologiques. Le corps topologique $\mathbb{R}$ est un sous-corps topologique de $\mathbb{C}$; quand on identifie $\mathbb{R}^2$ et $\mathbb{C}$, il se trouve identifié avec la partie de $\mathbb{R}^2$ définie par $y=0$, que l'on appelle pour cette raison axe réel de $\mathbb{R}^2$; on appelle de même axe imaginaire de $\mathbb{R}^2$ l'ensemble défini par $x=0$, et qui est un sous-espace homéomorphe à $\mathbb{R}$ (mais non un sous-corps de $\mathbb{C}$) ; on notera que ces deux ensembles sont fermés dans $\mathbb{R}^2$.

Pour illustrer par des figures ce qui sera dit de $\mathbb{C}$ ou de $\mathbb{R}^2$, on utilisera la représentation, bien connue en géométrie analytique élémentaire, de $\mathbb{R}^2$ par les points d'un plan où l'on a fixé deux axes de coordonnées rectangulaires, qui représentant respectivement l'axe réel et l'axe imaginaire de $\mathbb{R}^2$ (fig.) ; ces figures n'interviendront naturellement jamais dans les raisonnements.

Comme dans tout corps topologique (chap.III, §5), toute fonction rationnelle de n variables complexes, à coefficients complexes, est continue en tout point de $\mathbb{C}^n$ où son dénominateur n'est pas nul.

Les fonctions $\mathcal{R}(z)$, $\mathcal{I}(z)$ ne sont autres que les fonctions projections dans $\mathbb{R}^2$; elles sont donc continues ; il en est de même de la valeur absolue $|z|$. La permutation $z \to \bar{z}$ de $\mathbb{C}$ est continue ; c'est donc un automorphisme de la structure de corps topologique de $\mathbb{C}$.

L'expression $|z-z'| = \sqrt{(x-x')^2+(y-y')^2}$ est ce qu'on appelle la <u>distance</u> des points z et z' en géomètrie analytique élémentaire (voir chap. VI, § 3).

<u>Le groupe multiplicatif de $\mathbb{C}$</u>. Nous allons étudier la structure de groupe topologique du groupe multiplicatif des nombres complexes. En premier lieu, le groupe multiplicatif $\mathbb{C}^*$ des nombres réels >0 est un <u>sous-groupe</u> de $\mathbb{C}^*$. Un autre sous-groupe est formé de l'ensemble U des nombres complexes <u>de valeur absolue égale à 1</u>, en vertu de la formule donnant la valeur absolue d'un produit. Dans $\mathbb{R}^2$, l'ensemble U est identifié à l'ensemble des points (x,y) tels que $x^2+y^2=1$, que nous appellerons <u>cercle unité</u> (voir chap. VI, § 3).

<u>Proposition 2</u>. <u>Le groupe topologique $\mathbb{C}^*$ est isomorphe au produit des groupes topologiques $\mathbb{R}_+^*$ et U</u>.

En effet, tout $z \in \mathbb{C}^*$ peut se mettre d'une manière et d'une seule sous la forme $z=\rho.\zeta$, où ρ est un nombre réel >0, et $|\zeta|=1$; car on tire de cette relation $|z| = \rho$, $\zeta = z/|z|$. La structure de <u>groupe</u> de $\mathbb{C}^*$ est donc isomorphe au produit des structures de groupe de $\mathbb{R}_+^*$ et de U. D'autre part, les applications $z \to |z|$, $z \to z/|z|$ sont continues dans $\mathbb{C}$, l'application $(\rho, \zeta) \to \rho\zeta$ est continue dans $\mathbb{R}_+^* \times U$, ce qui démontre que l'application $z \to (|z|, z/|z|)$ est un isomorphisme de la structure de <u>groupe topologique</u> de $\mathbb{C}^*$ sur celle du produit $\mathbb{R}_+^* \times U$.

L'étude du groupe topologique $\mathbb{C}^*$ est donc ramenée à celle du groupe U.

<u>Théorème 1</u>. <u>Le groupe multiplicatif U des nombres complexes de valeur absolue égale à un, est un groupe topologique isomorphe au groupe additif $\mathbb{T}$ des nombres réels modulo 1</u>.

D'après le th.3 du § 2, il nous suffira de prouver que U est <u>localement homéomorphe à</u> R , <u>connexe</u> et <u>compact</u> .

1) U <u>est localement homéomorphe à</u> R. Soit V l'intersection du cercle unité U et du "demi-plan" défini par $x>0$; ce dernier est un ensemble ouvert dans R^2 contenant le point (1,0) , élément unité de U ; donc V est un voisinage de l'unité dans U . Or V est l'image biunivoque de l'intervalle $]-1,+1[$ de R par l'application $y \to (\sqrt{1-y^2}, y)$ qui est bicontinue ; d'où la proposition.

2) U <u>est connexe</u>. D'après la prop.2, il suffit de montrer que C^*, homéomorphe à $R_+^* \times U$, est connexe (chap.I, § 11, prop.6) . Or, soient z et z' deux points de C^* ; si le rapport z'/z n'est pas un nombre réel négatif, l'image de l'intervalle $[0,1]$ de R par l'application $t \to tz+(1-t)z'$ est contenue dans C^*, et comme cette application est continue, on voit qu'il existe un ensemble connexe contenu dans C^* et contenant z et z' . Si au contraire z'/z est réel négatif, il existe une partie connexe A de C^* contenant z et iz , et une partie connexe B de C^* contenant iz et z' ; donc $A \cup B$ est connexe et contient z et z' (fig.), d'où la proposition.

3) U <u>est compact</u>. En effet, U est défini par la relation $x^2+y^2-1=0$, donc est <u>fermé</u> dans R^2 (chap.I, § 8, cor. de la prop.6). D'autre part, ses projections sur les espaces facteurs de R^2 sont identiques à l'intervalle $[-1,+1]$, qui est compact, donc U est compact (chap.I, § 10, cor. du th.2) .

C. Q. F. D.

<u>Corollaire</u>. <u>Le groupe topologique</u> C^* <u>est isomorphe au groupe produit</u> $R \times T$.

D'après la prop.2 du § 2, il existe un homomorphisme et un seul de R sur U tel que l'intervalle $]-\frac{1}{2}, +\frac{1}{2}[$ soit le plus grand intervalle ouvert symétrique dont l'image soit biunivoque, et que l'image du nombre réel 1/4 soit le nombre i ; nous le désignerons par e . On sait (§ 2) que tout autre homomorphisme de R sur U est de la forme $\xi \to e(a\xi)$, où a est un nombre réel $\neq 0$. D'après la définition de e , on a les identités.

(5) $\quad e(x+y) = e(x)\,e(y)$ quels que soient $x \in R$, $y \in R$

(6) $\quad |e(x)| = 1$ quel que soit $x \in R$

ainsi que les relations

(7) $\quad e(0)=1$, $e(1/4)=i$, $e(1/2)=-1$, $e(3/4)=-i$, $e(1)=1$.

De (5) et (6) on tire les identités

(8) $\quad \overline{e(x)} = 1/e(x) = e(-x)$

(9) $\quad e(px) = (e(x))^p$ quel que soit l'entier p

Enfin, de (5) et (7) on déduit que

(10) $\quad e(x+k) = e(x)$ quel que soit l'entier k

(11) $\quad e(x+1/4) = i\,e(x)$ (12) $\quad e(x+1/2) = -e(x)$

La formule (10) peut encore s'exprimer en disant que e est une fonction <u>périodique</u> de période principale 1 .

* On a $e(x)=e^{2\pi i x}$ quel que soit $x \in R$, comme nous le verrons dans la partie de cet ouvrage consacrée aux fonctions analytiques, où e^z sera définie pour les valeurs complexes de z . *

<u>Angles de demi-droites</u>. Le plan numérique R^2 est muni d'une structure d'<u>espace vectoriel à deux dimensions</u> par rapport au corps R (Alg., chap.II, § 3), le produit λx d'un nombre réel λ et d'un point $x = (x_1, x_2)$ de R^2 étant le point $(\lambda x_1, \lambda x_2)$. Les <u>variétés linéaires à une dimension</u> de cet espace vectoriel sont appelées <u>droites</u> du plan numérique .

Une droite contenant deux points distincts x, y de R^2 est donc l'ensemble des points $\lambda x + \mu y$, où (λ, μ) parcourt l'ensemble des couples de nombres réels tels que $\lambda + \mu = 1$. L'ensemble des points de cette droite tels que $\mu > 0$ (resp. $\mu \geqslant 0$) est dit <u>demi-droite ouverte</u> (resp. <u>demi-droite fermée</u>) d'origine x et passant par y. En particulier, une demi-droite ouverte (resp. fermée) passant par l'origine 0 et un point $x \neq 0$ est l'ensemble des points λx, où λ parcourt l'ensemble des nombres réels > 0 (resp. $\geqslant 0$). Si D est une droite quelconque, il y a évidemment deux demi-droites fermées (resp. ouvertes) distinctes, contenues dans D, et ayant pour origine un point x de D ; on dit qu'elles sont <u>opposées</u>. En particulier, R_+ et $-R_+$ sont deux demi-droites fermées opposées, qu'on appelle respectivement <u>demi-axe réel positif fermé</u>, et <u>demi-axe réel négatif fermé</u> ; de même R_+^* et $-R_+^*$ sont deux demi-droites ouvertes opposées, dites respectivement <u>demi-axe réel positif ouvert</u> et <u>demi-axe réel négatif ouvert</u>.

On sait (Alg., chap. X) que deux droites D, D' dans R^2 sont dites <u>parallèles</u> s'il existe une translation $x \to x + a$ transformant D en D'. Deux demi-droites sont dites <u>parallèles</u> si les droites qui les contiennent sont parallèles ; elles sont dites <u>parallèles et de même sens</u> s'il existe une translation transformant l'une en l'autre ; si elles sont parallèles et non de même sens, elles sont dites <u>de sens opposés</u>. Il existe toujours une demi-droite (resp. droite) et une seule ayant comme origine 0 (resp. passant par 0), et qui soit parallèle à une demi-droite donnée et de même sens (resp. parallèle à une droite donnée).

Identifions R^2 et C, et considérons, dans le groupe multiplicatif C^*, les classes d'équivalence modulo le sous-groupe R_+^* : ce sont les demi-droites ouvertes d'origine 0. Le groupe quotient C^*/R_+^* est un groupe topologique isomorphe à U, donc à T ; on le note additivement et on appelle angles de demi-droites ses éléments (qu'on n'identifie donc pas ici avec les classes mod. R_+^*). On désigne par $Am(z)$, et on appelle amplitude de z, la valeur pour $z \neq 0$ de l'homomorphisme canonique de C^* sur C^*/R_+^* ; $Am(z)$ est donc continue dans C^*, et on a $Am(zz')=Am(z)+Am(z')$ $(zz' \neq 0)$ et $Am(\bar{z})=Am(1/z)=-Am(z)$. L'application $z \to Am(z)$, restreinte à U, est un isomorphisme de U sur C^*/R_+^*.

L'angle $Am(i)$ est appelé angle droit positif (plus brièvement angle droit, ou simplement droit, si aucune confusion n'est possible) ; on a $Am(-1)=2\,Am(i)$, et $4nAm(i)=0$, quel que soit l'entier n.

Considérons maintenant deux demi-droites ouvertes D, D', et soient D_1, D_1' les demi-droites ouvertes ayant pour origine 0, respectivement parallèles à D, D' et de même sens. Quels que soient les nombres complexes $z \in D_1$, $z' \in D_1'$, $Am(z'/z)$ a la même valeur, qui ne dépend que de D et D' ; on l'appelle angle de D et D', et on le désigne par la notation $\widehat{(D,D')}$; on a évidemment $\widehat{(D,D')} = \widehat{(D_1,D_1')}$, $\widehat{(D',D)} = -\widehat{(D,D')}$, $\widehat{(D,D')}+\widehat{(D',D'')} = \widehat{(D,D'')}$ (relation de Chasles). L'angle de deux demi-droites parallèles et de même sens est nul ; l'angle de deux demi-droites parallèles et de sens opposés est égal à deux droits.

Si D et D' sont deux demi-droites quelconques (ouvertes ou fermées) on appelle angle de D et D' l'angle $\widehat{(D_0,D_0')}$, où D_0 (resp. D_0') désigne la demi-droite ouverte obtenue en enlevant éventuellement de D (resp. D') son origine.

Mesure des angles de demi-droites. Tout homomorphisme de R sur le groupe additif $\mathbb{C}^*/R_+^*$ des angles de demi-droites est de la forme $x \to \mathrm{Am}(e(x/a))$, où a est un nombre réel $\neq 0$; l'angle $\omega = \mathrm{Am}(e(1/a))$ est appelé unité d'angle correspondant à cet homomorphisme. Etant donné un angle $\alpha \in \mathbb{C}^*/R_+^*$, tout nombre réel x tel que $\mathrm{Am}(e(x/a)) = \alpha$ est appelé mesure de l'angle α, avec l'unité d'angle ω ; si x est une mesure de α avec cette unité, toute autre mesure de α avec la même unité est de la forme $x + ka$, où k est un entier quelconque (positif ou négatif) ; en particulier, l'unité d'angle ω a pour mesures les nombres $1 + ka$, l'angle droit a pour mesures $a/4 + ka$. Tout angle a une mesure et une seule dans un intervalle semi-ouvert de la forme $[x_0, x_0 + a[$; en particulier, il a une mesure et une seule dans l'intervalle $[0, a[$; on l'appelle sa mesure réduite.

Si θ est une mesure quelconque de $\mathrm{Am}(z)$ $(z \neq 0)$, on peut écrire $z = |z| \cdot e(\theta/a)$; on dit que z, exprimé ainsi à l'aide de sa valeur absolue et d'une mesure de son amplitude, est mis sous forme trigonométrique. Si α et β sont deux nombres réels quelconques $(\alpha < \beta)$, l'ensemble $S(\alpha, \beta) = S$ des points $z \neq 0$ tels que $\alpha < \theta < \beta$ est appelé secteur angulaire ouvert de sommet 0 (ou angle ouvert de sommet 0, par abus de langage) ; si $\beta - \alpha > a$, cet ensemble est identique à $\mathbb{C}^*$; sinon, on appelle ouverture de ce secteur l'angle dont une mesure est $\beta - \alpha$. L'adhérence de ce secteur dans $\mathbb{C}$ est la réunion de S et des demi-droites fermées D, D' faisant respectivement avec le demi-axe réel positif des angles de mesure α et β ; on l'appelle secteur angulaire formé de sommet 0 et d'ouverture $\beta - \alpha$; D et D' sont appelés les cotés de S et de $\bar{S}$. La demi-droite issue de 0 et passant par $e((\alpha+\beta)/2a)$ est appelée la bissectrice de S (et $\bar{S}$).

Un secteur angulaire d'ouverture a/4 est appelé quadrant (ou, par abus de langage, angle droit) ; en particulier, le quadrant S(0,a/4) (resp. S(a/4,a/2), S(a/2,3a/4), S(3a/4,a)) est dit premier (resp. deuxième, troisième, quatrième) quadrant. Un secteur angulaire d'ouverture a/2 est appelé demi-plan ; en particulier S(0,a/2) (resp. S(a/2,a), S(-a/4,a/4), S(a/4,3a/4)) est appelé demi-plan supérieur (resp. inférieur, positif, négatif) ; si la bissectrice d'un demi-plan ouvert (resp. fermé) fait avec le demi-axe réel positif un angle de mesure φ , on notera que le demi-plan est l'ensemble des z tels que $\mathcal{R}(z\,e(-\varphi/a)) > 0$ (resp. $\mathcal{R}(z\,e(-\varphi/a)) \geqslant 0$). Un secteur angulaire d'ouverture φ est dit aigu (resp. obtus, méplat) si $\varphi < a/4$ (resp. $a/4 < \varphi < a/2$, $a/2 < \varphi < a$).

On remarquera que la donnée de l'angle ω détermine un nombre $a > 1$ et un seul tel que $\mathrm{Am}(e(1/a)) = \omega$; si on convient de se restreindre aux homomorphismes tels que $a > 1$, on voit qu'un tel homomorphisme est bien déterminé par l'unité d'angle correspondante.

Les unités d'angles utilisées en mathématique et dans les applications de la mathématique sont assez nombreuses. Celle qui semblerait la plus naturelle a priori serait l'angle droit, correspondant à $a=4$. En pratique, on utilise surtout le degré , qui correspond à $a=360$, et le grade, qui correspond à $a=400$; l'angle droit a donc pour mesure 90 degrés, ou 100 grades. En mathématique, on se sert plutôt d'une autre unité, le radian, qui correspond au nombre a défini par la condition $\lim_{x \to 0} (e(x/a)-1)/x = i$, nombre que l'on désigne par la notation 2π ; on a $\pi = 3,1415...$ (pour l'existence de ce nombre et le calcul de ses valeurs approchées, voir Livre V).

Fonctions trigonomètriques. Une fois choisie une unité d'angle ω , et par suite le nombre réel $a>1$ correspondant, à toute fonction f définie sur $\mathcal{C}^{\infty}/R_+^*$ correspond une fonction $\dot{f}$ définie sur R et admettant pour période a , et réciproquement ; f et $\dot{f}$ sont continues simultanément ; par un abus de langage très fréquent, lorsqu'on parle de la fonction f , c'est en réalité de la fonction $\dot{f}$ correspondante qu'il s'agit ; de même, on dira qu'un argument x figurant dans cette dernière fonction est un angle, au lieu de dire que c'est la mesure d'un angle ; en particulier, ce qu'on appelle le plus souvent amplitude d'un nombre complexe $z\neq 0$, n'est pas l'angle $\mathrm{Am}(z)$ lui-même, mais une mesure de cet angle avec une unité déterminée. Ces abus de langage n'ont pas d'inconvénient grave, lorsqu'on a bien précisé, une fois pour toutes, quelle unité d'angle on a choisi (en mathématique, c'est presque toujours le radian), et qu'on se souvient qu'une mesure d'angle n'est déterminée que mod. a .

On appelle fonctions trigonomètriques simples correspondant à un nombre $a>1$ déterminé, la fonction complexe $e(x/a)$, et les fonctions réelles suivantes qui s'en déduisent :

1° $\mathcal{R}(e(x/a))$, qu'on note $\cos_a x$, et qu'on appelle cosinus du nombre x , relatif à l'unité de mesure $\mathrm{Am}(e(1/a))$ (on dit encore cosinus de l'angle x , conformément à l'abus de langage que nous venons de signaler) ; on a donc, d'après (8) ,

$$\cos_a x = \frac{1}{2}(e(x/a)+e(-x/a)) \tag{13}$$

2° $\mathcal{I}(e(x/a))$, qu'on note $\sin_a x$, et qu'on appelle sinus du nombre (ou de l'angle) x , relatif à l'unité de mesure $\mathrm{Am}(e(1/a))$; on a

$$\sin_a x = (e(x/a)-e(-x/a))/2i \tag{14}$$

3° Les quotients $tg_a x = \sin_a x/\cos_a x$, et $cotg_a x = \cos_a x/\sin_a x$, définis lorsque les dénominateurs ne sont pas nuls, qu'on appelle respectivement <u>tangente</u> et <u>cotangente</u> de x (relatives à l'unité d'angle Am(e(1/a))) ; on a donc

(15) $$tg_a x = (e(x/a) - e(-x/a))/(e(x/a) + e(-x/a))$$

(16) $$cotg_a x = (e(x/a) + e(-x/a))/(e(x/a) - e(-x/a))$$

lorsque les dénominateurs ne sont pas nuls ; par suite

(17) $$tg_a x . cotg_a x = 1$$

lorsque le premier membre a un sens.

On peut donc écrire

(18) $$e(x/a) = \cos_a x + i \sin_a x$$

d'où, en vertu de (6)

(19) $$\cos_a^2 x + \sin_a^2 x = 1 .$$

Les fonctions $\cos_a x$ et $\sin_a x$ sont continues dans R ; elles sont périodiques de période a ; a est d'ailleurs <u>période principale</u> de ces fonctions ; en effet, la relation $\cos_a x = \cos_a y$ entraîne $\sin_a x = \sin_a y$ ou $\sin_a x = -\sin_a y$ d'après (19), c'est-à-dire $e(x/a) = e(y/a)$ ou $e(x/a) = e(-y/a)$, donc $x \equiv y \pmod a$ ou $x \equiv -y \pmod a$; on voit de même que $\sin_a x = \sin_a y$ est équivalente à $x \equiv y \pmod a$ ou $x+y \equiv a/2 \pmod a$. Les fonctions $\cos_a x$ et $\sin_a x$ appliquent R <u>sur</u> l'intervalle $[-1,+1]$, car les projections de U sur R sont des ensembles connexes contenus dans cet intervalle et en contenant les extrémités.

D'après ce qui précède, la fonction $\cos_a x$, restreinte à l'intervalle $[0,a/2]$ applique <u>biunivoquement</u> cet intervalle sur $[-1,+1]$; comme $\cos_a 0 = 1$, $\cos_a (a/2) = -1$, $\cos_a x$ est donc <u>strictement décroissante</u> dans l'intervalle $[0,a/2]$; elle s'annule pour $x = a/4$, est positive pour

$0 \leqslant x \leqslant a/4$, négative pour $a/4 \leqslant x \leqslant a/2$; comme $\cos_a x = \cos_a(-x)$, on en déduit la variation de $\cos_a x$ dans l'intervalle $\left[-a/2, 0\right]$, puis dans tout R par périodicité (fig.). Comme d'après (12), on a $\sin_a x = -\cos(x+a/4)$, on en déduit sans peine la variation de $\sin_a x$ dans R (fig.) .

La fonction $tg_a x$ est définie et continue pour toutes les valeurs de x distinctes des valeurs $a/4+ka/2$ (k entier quelconque), qui annulent $\cos_a x$. Elle admet pour période $a/2$, d'après (11), et on a $tg_a(-x) = -tg_a x$. Dans l'intervalle $\left[0, a/4\right]$, $\sin_a x$ croît de 0 à 1 , $\cos_a x$ décroît de 1 à 0 , donc $tg_a x$ est <u>strictement croissante</u>, et applique par suite $\left[0, a/4\right[$ <u>sur</u> $\left[0, +\infty\right[$; elle est donc strictement croissante dans $\left]-a/4, +a/4\right[$, et est un homéomorphisme de cet intervalle <u>sur</u> R ; d'où résulte en particulier que $a/2$ est <u>période principale</u> de $tg_a x$ (fig.).

On notera enfin que, si $b > 1$, on a, d'après la définition des fonctions trigonomètriques simples

(20) $$\cos_b x = \cos_a(ax/b) , \quad \sin_b x = \sin_a(ax/b) .$$

Comme on l'a déjà dit, les seules fonctions trigonomètriques qui interviennent en mathématique sont celles relatives au <u>radian</u>, c'est-à-dire les fonctions $\cos_{2\pi} x$, $\sin_{2\pi} x$, $tg_{2\pi} x$, $cotg_{2\pi} x$, qu'on note simplement cos x , sin x , tg x et cotg x . Les formules (5) à (12) , exprimés à l'aide de ces fonctions, donnent lieu, en les combinant, à une foule d'identités plus ou moins utiles, et que le lecteur trouvera dans un traité de Trigonomètrke élémentaire quelconque.

Angles de droites. Considérons, dans le groupe multiplicatif $\mathcal{C}^*$, le sous-groupe R^* ; les classes d'équivalence modulo R^* sont ici les droites passant par O , privées du point O . Le groupe quotient $\mathcal{C}^*/R^*$ est isomorphe à $(\mathcal{C}^*/R_+^*)/(R^*/R_+^*)$; or R^*/R_+^* est le sous-groupe de $\mathcal{C}^*/R_+^*$ formé de l'angle nul et de l'angle égal à 2 droits ; $\mathcal{C}^*/R^*$ est donc un groupe topologique isomorphe à T ; on le note encore additivement, et on l'appelle groupe additif des angles mod.2 droits ; ses éléments sont aussi appelés angles de droites.

Si D et D' sont deux droites quelconques, Δ et Δ' deux demi-droites arbitraires contenues dans D et D' respectivement, les angles $(\widehat{\Delta, \Delta'})$ sont tous congrus entre eux (mod.2 droits), et il leur correspond par suite un élément bien déterminé du groupe $\mathcal{C}^*/R^*$; cet élément se note $\widehat{[D,D']}$ et s'appelle angle de la droite D et de la droite D' ; on a encore $\widehat{[D',D]} = -\widehat{[D,D']}$, $\widehat{[D,D']} + \widehat{[D',D'']} = \widehat{[D,D'']}$ (formule de Chasles) ; si D_1 et D'_1 sont respectivement parallèle à D et D' , $\widehat{[D,D']} = \widehat{[D_1,D'_1]}$. Deux droites D,D' sont dites perpendiculaires (ou rectangulaires) si $\widehat{[D,D']}$ est égal à 1 droit.

Un nombre réel x sera encore dit la mesure d'un angle de droites α , avec l'unité d'angle $\omega = Am(e(1/a))$, si x est une mesure, avec cette unité d'angle, d'un des deux angles de demi-droites qui correspondent à α ; si x est une mesure de α , toutes les autres mesures de α sont donc les nombres $x+ka/2$, où k prend toutes les valeurs entières ; celle qui appartient à l'intervalle $\left[0, \frac{a}{2}\right[$ est dite mesure réduite de α .

A toute fonction définie dans $\mathcal{C}^*/R^*$ correspond (une fois l'unité d'angle choisie) une fonction définie dans R et admettant la période $a/2$, et réciproquement ; par un abus de langage analogue à celui

signalé plus haut, on identifie le plus souvent ces deux fonctions ; si l'une est continue, il en est de même de l'autre. En particulier, à la fonction $tg_a x$, définie pour x distinct des valeurs $a/4+ka/2$ correspond une fonction définie dans le sous-espace A de $\mathbb{C}^*/\mathbb{R}^*$, complémentaire de l'angle égal à 1 droit , et cette fonction est un <u>homéomorphisme</u> de A <u>sur</u> $\mathbb{R}$.

<u>Exercices</u>. 1) Soit a un nombre complexe $\neq 0$, n un entier >0 ; pour tout nombre positif r tel que $r^n \leqslant |a|$, montrer qu'il existe z tel que $|z| = r$, et $|a+z^n| = |a|-r^n$.

En déduire que, si f est un polynome à coefficients complexes de degré >0 , on ne peut avoir $|f(z_0)| \leqslant |f(z)|$ pour tous les points z d'un voisinage de z_0 que si $f(z_0)=0$.

¶ 2) Montrer que, pour tout polynome f à coefficients complexes non identiquement nul, il existe un nombre $r>0$ tel que, pour $|z|>r$, $f(z)\neq 0$ (mettre en facteur la plus haute puissance de z qui figure dans $f(z)$).

En déduire, à l'aide de l'exerc. 1 et du th. de Weierstrass (chap.IV, §6, th.1), que $\mathbb{C}$ est un corps algèbriquement clos (considérer la fonction $|f|$ dans l'ensemble compact des points z tels que $|z| \leqslant r$).

3) Soit $f(z)=z^n+a_1 z^{n-1}+\ldots+a_{n-1}z+a_n$ un polynome de degré n à coefficients complexes, et z_i $(1\leqslant i\leqslant n)$ ses racines.

a) Montrer que, si r est un nombre >0 tel que

$$r^n \geqslant |a_1| r^{n-1} + |a_2| r^{n-2} + \ldots + |a_n|$$

On a

$$r_0 = \operatorname*{Max}_{1\leqslant i\leqslant n} (|z_i|) \leqslant r \ .$$

b) Si $(\lambda_i)_{1\leqslant i\leqslant n}$ est une suite finie de n nombres >0, tels que $\sum_{i=1}^{n} 1/\lambda_i = 1$, montrer que

$$r_o \leqslant \operatorname{Max}_{1\leqslant k\leqslant n}((\lambda_k|a_k|)^{1/k})$$

(utiliser a)). En déduire que

$$r_o \leqslant \operatorname{Max}\left(1, \sum_{k=1}^{n}|a_k|\right)$$

c) Déduire de a) que, si les a_i sont tous $\neq 0$,

$$r_o \leqslant \operatorname{Max}(2|a_1|, 2|a_2/a_1|, \ldots, 2|a_{n-1}/a_{n-2}|, |a_n/a_{n-1}|).$$

d) Déduire de b) que l'on a

$$r_o \leqslant |a_1-1|+|a_2-a_1|+\ldots+|a_{n-1}-a_n|+|a_n|$$

(considérer le polynome $(z-1)f(z)$). En conclure que, si les a_i sont réels et >0, on a

$$r_o \leqslant \operatorname{Max}(a_1, a_2/a_1, \ldots, a_n/a_{n-1}).$$

¶ 4) Soit $f(z)=a_o z^n+a_1 z^{n-1}+\ldots+a_{n-1}z+a_n$ un polynome à coefficients complexes dont les n racines z_i $(1\leqslant i\leqslant n)$ sont telles que $\mathcal{I}(z_k)>0$ $(1\leqslant k\leqslant n)$. Si $\alpha_k = \mathcal{R}(a_k)$, $\beta_k = \mathcal{I}(a_k)$ $(0\leqslant k\leqslant n)$ et si on pose

$$u(z) = a_o z^n + a_1 z^{n-1}+\ldots+ a_n$$
$$v(z) = \beta_o z^n + \beta_1 z^{n-1}+\ldots+ \beta_n$$

les deux polynomes u et v n'ont que des racines réelles (si $\overline{f}(z)=\overline{a}_o z^n+\overline{a}_1 z^{n-1}+\ldots+\overline{a}_n$, montrer que pour une racine z de u ou de v, on a $|f(z)| = |\overline{f}(z)|$, et, en décomposant $f(z)$ et $\overline{f}(z)$ en facteurs du premier degré, montrer que cette relation entraîne que z est réel).

¶ 5) Soit $f(x)=a_o+a_1\cos x + b_1\sin x + \ldots + a_n\cos nx + b_n\sin nx$ un "polynome trigonomètrique" à coefficients réels ; si on pose $z = e(x/2\pi)$, on a $f(x) = g(z)/z^n$, où $g(z)=u_o+u_1 z+\ldots+u_{2n}z^{2n}$, est tel que $\overline{u}_k = u_{2n-k}$ $(0\leqslant k\leqslant 2n)$.

a) Montrer que, si pour tout $x \in R$, $f(x) > 0$, il existe un polynome $h(z)$ de degré n $(z = e(x/2\pi))$,

$$h(z) = c_0 + c_1 z + \ldots + c_n z^n$$

tel que $f(x) = |h(z)|^2$ quel que soit $x \in R$. Etendre ce résultat au cas où $f(x) \geqslant 0$ quel que soit $x \in R$ (considérer le polynome trigonomètrique $f(x)+\varepsilon$, où $\varepsilon > 0$, et faire tendre ε vers 0).

b) En déduire que, si $f(x) \geqslant 0$ quel que soit $x \in R$, et si $a_0 = 1$, on a

$$|f(x)| \leqslant n+1 \qquad \text{quel que soit } x \in R$$
$$a_k^2 + b_k^2 \leqslant 4 \qquad \text{pour } 1 \leqslant k \leqslant n-1$$
$$a_n^2 + b_n^2 \leqslant 1$$

c) Si $a_0 = 0$, on ne peut avoir $f(x) \geqslant 0$ pour tout $x \in R$ que si $a_k = b_k = 0$ pour tous les indices k .

6) Démontrer les identités

$$\sum_{k=1}^{n} \cos kx = \sin((2n+1)x/2)/2 \sin x/2 - \frac{1}{2}$$
$$= \sin nx/2 \,.\, \cos((n+1)x/2)/\sin x/2$$
$$\sum_{k=1}^{n} \cos(2k-1)x = \sin 2nx/2 \sin x$$
$$\sum_{k=1}^{n} \sin kx = \sin nx/2 \,.\, \sin((n+1)/2)x \,/ \sin x/2$$
$$\sum_{k=1}^{n} \sin(2k-1)x = (\sin nx)^2/\sin x$$
$$(n+1)/2 + \sum_{k=1}^{n}(n-k+1)\cos kx = \frac{1}{2}(\sin(n+1)x/2 \,/ \sin x/2)^2$$

§ 4. Sommes et produits infinis de nombres complexes.

Familles addibles de nombres complexes. **Théorème 1.** *Pour qu'une famille (z_ι) de nombres complexes soit addible* (dans $\mathbb{C}$), *il faut et il suffit que la somme des valeurs absolues $|z_\iota|$ soit finie* (autrement dit, que la famille $(|z_\iota|)$ soit addible dans R).

En effet, si on pose $z_\iota = x_\iota + iy_\iota$, pour que (z_ι) soit addible, il faut et il suffit (chap.III, § 4, prop.4) que chacune des familles

(x_ι) et (y_ι) le soit, donc (chap.IV, § 7, th.3) que les familles $(|x_\iota|)$ et $(|y_\iota|)$ soient addibles dans R . Or, on a $|x_\iota| \leqslant |z_\iota|$, $|y_\iota| \leqslant |z_\iota|$, et, d'après l'inégalité du triangle , $|z_\iota| \leqslant |x_\iota| + |y_\iota|$, d'où le théorème (chap.IV, § 7, th.2).

Corollaire 1. Si une famille (z_ι) de nombres complexes est addible, l'ensemble des indices ι tels que $z_\iota \neq 0$ est dénombrable.

C'est une conséquence du th.1 et du cor.2 du th.1 du § 7 du chap. IV.

Corollaire 2. Pour qu'une famille (z_ι) de nombres complexes soit addible il faut et il suffit que l'ensemble des valeurs absolues des sommes partielles finies de cette famille soit borné dans R .

La condition est évidemment nécessaire, d'après le th.1 et la relation $\left|\sum_{\iota \in H} z_\iota\right| \leqslant \sum_{\iota \in H} |z_\iota|$ (H partie finie quelconque de l'ensemble d'indices). Elle est suffisante, car on a $\left|\sum_{\iota \in H} x_\iota\right| \leqslant \left|\sum_{\iota \in H} |z_\iota|\right|$, et $\left|\sum_{\iota \in H} y_\iota\right| \leqslant \left|\sum_{\iota \in H} z_\iota\right|$, donc elle entraîne que les familles (x_ι) et (y_ι) sont addibles dans R (chap.IV, § 7, cor.1 du th.3).

Proposition 1. Si $(u_\lambda)_{\lambda \in L}$ et $(v_\mu)_{\mu \in M}$ sont deux familles addibles de nombres complexes, la famille $(u_\lambda v_\mu)_{(\lambda, \mu) \in L \times M}$ est addible, et on a

$$(1) \qquad \sum_{(\lambda, \mu) \in L \times M} u_\lambda v_\mu = \left(\sum_{\lambda \in L} u_\lambda\right)\left(\sum_{\mu \in M} v_\mu\right)$$

La démonstration étant identique à celle de la prop.2 du § 7 du chap. IV , nous y renvoyons le lecteur.

Familles multipliables dans C^*. Dans le groupe multiplicatif C^* des nombres complexes, une famille $(z_\iota)_{\iota \in I}$ ne peut être multipliable que si $\lim z_\iota = 1$ suivant le filtre des complémentaires des parties finies de I (chap.III, § 4, cor. du th. 1). Il en résulte que, si on pose $z_\iota = 1+u_\iota$, avec $u_\iota \neq -1$, on ne peut avoir $|u_\iota| \geqslant 1/n$ que pour un nombre fini d'indices ι , et par suite l'ensemble des ι tels que $u_\iota \neq 0$ est dénombrable si la famille $(1+u_\iota)$ est multipliable. Nous n'étudierons donc que la multiplicabilité des suites $(1+u_n)$.

Théorème 2. *Pour que la suite* $(1+u_n)$ *soit multipliable dans* $\mathbb{C}^*$, *il faut et il suffit que la suite* (u_n) *soit addible dans* $\mathbb{C}$.

Lemme. *Si* $(a_i)_{1\leqslant i\leqslant p}$ *est une suite finie de nombres complexes telle que* $\sum_{i=1}^{p}|a_i|<1$, *on a*

$$(2)\qquad \Big|\prod_{i=1}^{p}(1+a_i)-1-\sum_{i=1}^{p}a_i\Big|\leqslant\Big(\sum_{i=1}^{p}|a_i|\Big)^2/\Big(1-\sum_{i=1}^{p}|a_i|\Big)$$

On a en effet

$$\prod_{i=1}^{p}(1+a_i)=1+\sum_{i=1}^{p}a_i+\sum_{i<j}a_ia_j+\ldots+\sum_{i_1<i_2<\ldots<i_k}a_{i_1}a_{i_2}\ldots a_{i_k}+\ldots.$$
$$+a_1a_2\ldots a_p$$

Or, on a $\Big|\sum_{i_1<i_2<\ldots<i_k}a_{i_1}a_{i_2}\ldots a_{i_k}\Big|\leqslant\sum|a_{i_1}||a_{i_2}|\cdots|a_{i_k}|\leqslant$
$$\leqslant\Big(\sum_{i=1}^{p}|a_i|\Big)^k$$

donc, si on pose $s=\sum_{i=1}^{p}|a_i|$,

$$\Big|\prod_{i=1}^{p}(1+a_i)-1-\sum_{i=1}^{p}a_i\Big|\leqslant s^2+\ldots+s^k+\ldots+s^p\leqslant s^2\Big(\sum_{n=0}^{\infty}s^n\Big)=s^2/(1-s)$$

puisqu'on a supposé $s<1$.

Ce lemme étant démontré, posons $u_n=x_n+iy_n$, et désignons par I_1 (resp. I_2,I_3,I_4) l'ensemble des indices n tels que $-y_n<x_n$ et $y_n\leqslant x_n$ (resp. $x_n<y_n$ et $-x_n\leqslant y_n$, $x_n<-y_n$ et $x_n\leqslant y_n$, $y_n<x_n$ et $y_n\leqslant -x_n$) ; ces ensembles constituent une partition de l'ensemble des indices n tels que $u_n\neq 0$; donc (chap.III, §4, prop.1 et cor. de la prop.5) il suffit de démontrer le théorème pour chacune des suites partielles $(1+u_n)_{n\in I_k}$ $(k=1,2,3,4)$. Nous ferons le raisonnement pour I_1, il est tout à fait analogue pour les trois autres ensembles d'indices.

Nous sommes donc ramenés à démontrer le théorème dans le cas où $|y_n|\leqslant x_n$ quel que soit n ; on a alors $|u_n|\leqslant|x_n|+|y_n|\leqslant 2|x_n|=2x_n$, d'où, pour toute partie finie H de $\mathbb{N}$

$$(3)\qquad \sum_{n\in H}|u_n|\leqslant 2\Big|\sum_{n\in H}u_n\Big|$$

1° La condition est <u>suffisante</u>. En effet, si (u_n) est addible dans $\mathcal{C}$, il existe, d'après le th.1, une partie finie J de $\mathcal{N}$ telle que, pour toute partie finie H de $\mathcal{N}$ ne rencontrant pas J on ait $\sum_{n\in H} |u_n| \leqslant \varepsilon < 1$; d'après (2), on a donc

$$\left| \prod_{n\in H} (1+u_n) - 1 \right| \leqslant \varepsilon + \varepsilon^2/(1-\varepsilon) = \varepsilon/(1-\varepsilon)$$

d'où la proposition, d'après le critère de Cauchy, puisque $\mathcal{C}^*$ est un groupe complet.

2° La condition est <u>nécessaire</u>. Supposons en effet $(1+u_n)$ multiplisable dans $\mathcal{C}^*$; il existe alors une partie finie J de $\mathcal{N}$ telle que, pour toute partie finie H de $\mathcal{N}$ ne rencontrant pas J , on ait $\left| \prod_{n\in H} (1+u_n) - 1 \right| \leqslant \varepsilon$. Nous allons voir que, si on peut en conclure que $\left| \sum_{n\in H} u_n \right| \leqslant 1/20$, il en résultera, d'après (2) et (3), que $\left| \sum_{n\in H} u_n \right| \leqslant 2\varepsilon$ ce qui démontrera la proposition.

Posons en effet, pour simplifier, $a = \sum_{n\in H} |u_n|$, $b = \left| \sum_{n\in H} u_n \right|$; on a $a \leqslant 2b$ d'après (3), donc, d'après (2) et l'hypothèse sur H

$$b - \varepsilon \leqslant 2a^2/(1-a) \leqslant 8b^2/(1-2b)$$

c'est-à-dire $$b(1-10b)/(1-2b) \leqslant \varepsilon$$

et, si $b \leqslant 1/20$, $1-10b \geqslant \frac{1}{2}$, donc $\frac{1}{2} b \leqslant \varepsilon$.

Reste donc à montrer qu'en choisissant ε convenablement, on a bien $\left| \sum_{n\in H} u_n \right| \leqslant 1/20$ pour toute partie finie H ne rencontrant pas J . Nous ferons la démonstration par récurrence sur le nombre d'éléments m de H . Comme $\lim_{n\to\infty} u_n = 0$, on peut supposer que J a été choisi de sorte que, pour $n \notin J$, $|u_n| \leqslant \varepsilon$; si $\varepsilon \leqslant 1/80$, la proposition est vraie pour m=1 . Supposons-la démontrée pour $m < p$; soit H une partie finie de p éléments, ne rencontrant pas J ; on peut l'écrire $H = H' \cup \{n_o\}$, où H' a p-1 éléments On a par hypothèse $\left| \sum_{n\in H'} u_n \right| \leqslant 2\varepsilon \leqslant 1/40$, et $|u_{n_o}| \leqslant 1/40$, donc $\left| \sum_{n\in H} u_n \right| \leqslant 1/20$, ce qui achève la démonstration.

L'étude des propriétés différentielles des fonctions trigonométriques, que nous ferons au Livre V , nous permettra de retrouver le th. 2 par une autre voie plus simple.

Séries et produits infinis de nombres complexes. Définition 1. Une série de nombres complexes est dite absolument convergente si la série des valeurs absolues de ses termes est convergente (dans $\mathbb{R}$).

D'après le th.1, et la prop.9 du § 4 du chap.III, on voit que, pour qu'une série de nombres complexes soit commutativement convergente, il faut et il suffit qu'elle soit absolument convergente. Mais, d'après les exemples du chap.IV, § 7, une série de nombres complexes peut être convergente sans être absolument convergente.

Pour que la série de terme général $z_n=x_n+iy_n$ soit convergente, il faut et il suffit évidemment que chacune des deux séries de nombres réels (x_n) et (y_n) soit convergente.

Définition 2. Un produit infini défini par la suite $(1+u_n)$ de nombres complexes $\neq 0$ est dit absolument convergent si le produit défini par la suite de nombres réels $(1+|u_n|)$ converge dans $\mathbb{R}^*$.

Par suite, pour que le produit défini par la suite $(1+u_n)$ de nombres complexes $\neq 0$, soit commutativement convergent dans $\mathbb{C}^*$, il faut et il suffit, d'après les th. 1 et 2 et la prop. 9 du § 4 du chap.III, qu'il soit absolument convergent.

D'après la prop.2 du § 3 , pour que le produit $(1+u_n)$ soit convergent, il faut et il suffit que le produit $(|1+u_n|)$ soit convergent dans $\mathbb{R}^*$, et que la série de terme général $\mathrm{Am}(1+u_n)$ soit convergente dans $\mathbb{U}$.

Remarques. 1) Le produit $(|1+u_n|)$ peut être convergent, et même absolument convergent dans $\mathbb{R}^*$ sans que le produit $(1+|u_n|)$ le soit (ce qui ne peut se produire si tous les termes $1+u_n$ sont positifs) ; l'exemple le plus simple est fourni

en prenant $u_n=0$ si n est pair, $u_n=-2$ si n est impair (voir aussi exerc. 6).

2) Comme on l'a déjà signalé pour les produits de facteurs >0, la convergence de la série de terme général u_n n'est ni nécessaire ni suffisante pour assurer la convergence du produit de facteur général $(1+u_n)$.

Exercices. 1) Soit (z_n) une suite de nombres complexes $z_n=x_n+iy_n$, telle que $x_n \geqslant 0$ quel que soit n. Montrer que, si les séries définies par les suites (z_n) et (z_n^2) sont convergentes, la série de terme général z_n est absolument convergente. Donner un exemple où ce résultat tombe en défaut quand on remplace la condition $x_n \geqslant 0$ (qui s'écrit aussi $-\pi/2 \leqslant \mathrm{Am}(z_n) \leqslant +\pi/2$) par $-(1+\varepsilon)\pi/2 \leqslant \mathrm{Am}(z_n) \leqslant (1+\varepsilon)\pi/2$ quelque petit que soit le nombre $\varepsilon > 0$ (Am z étant la mesure en radians de l'amplitude de z).

¶ 2) Soit (z_n) une suite de nombres complexes telle que $\sum_{n=0}^{\infty} |z_n| = +\infty$. Montrer qu'il existe un angle α tel que, pour tout angle aigu arbitrairement petit ε, la suite partielle $(z_n)_{n\in H}$ formée des z_n tels que $\alpha-\varepsilon \leqslant \mathrm{Am}(z_n) \leqslant \alpha+\varepsilon$, soit telle que $\sum_{n\in H} |z_n| = +\infty$. La demi-droite faisant l'angle α avec le demi-axe réel positif est dite direction de condensation pour la suite donnée (pour la démonstration, utiliser la compacité du groupe U).

¶ 3)* Soit (z_n) une suite de nombres complexes telle que $\lim_{n\to\infty} z_n = 0$, et $\sum_{n=0}^{\infty} |z_n| = +\infty$. Si la demi-droite d'origine 0 passant par le point $e(\varphi)$ est direction de condensation de cette suite, montrer qu'il existe une suite partielle (z_{n_k}) extraite de (z_n), telle que la série de terme général $\mathcal{R}(z_{n_k}\, e(-\varphi))$ soit commutativement convergente vers $+\infty$, et que la série de terme général

$\mathcal{I}(z_{n_k} e(-\varphi))$ soit convergente dans R (se ramener au cas où $\varphi=0$; si on pose $z_n=x_n+iy_n=r_n\, e(\theta_n)$, définir la suite (z_{n_k}) de sorte qu'il existe une suite d'indices (k_p) strictement croissante telle que, pour $k_p \leqslant k < k_{p+1}$, $|\theta_{n_k}| \leqslant 1/2^p$, et que la somme des x_{n_k} d'indice k tel que $k_p \leqslant k < k_{p+1}$ soit comprise entre 1 et 2).

¶ 4) Soit (z_n) une suite de nombres complexes telle que la série de terme général z_n ne soit pas absolument convergente ; montrer qu'il existe au plus un angle φ tel que la série de terme général $\mathcal{R}(z_n\, e(-\varphi))$ soit absolument convergente. On suppose en outre que la série de terme général z_n soit convergente et de somme s ; s'il existe un angle φ ayant la propriété précédente, l'ensemble des nombres complexes s' tels qu'il existe une permutation σ de $\mathcal{N}$ telle que la série de terme général $z_{\sigma(n)}$ soit convergente et ait pour somme s' , est une droite passant par s et perpendiculaire à la droite passant par 0 et le point $e(\varphi)$ (utiliser l'exerc.17 du § 7 du chap. IV).

¶ 5) Soit (z_n) une suite de nombres complexes telle que la série de terme général z_n soit convergente, mais non absolument convergente, et qu'il n'existe <u>aucun</u> angle φ tel que la série de terme général $\mathcal{R}(z_n\, e(-\varphi))$ soit absolument convergente. Montrer que, pour <u>tout</u> nombre complexe s' , il existe une permutation σ de $\mathcal{N}$ telle que la série de terme général $z_{\sigma(n)}$ soit convergente et ait pour somme s' (montrer d'abord que, dans tout demi-plan $\mathcal{R}(z\, e(-\varphi))>0$, il y a une direction de condensation de la suite (z_n) ; en déduire qu'il existe, ou bien trois directions de condensation au moins non situées dans un même demi-plan fermé, ou bien deux directions de condensation opposées. Définir dans chacun des deux cas la permutation σ voulue, en utilisant l'exerc.3 ci-dessus, et l'exerc. 17 du § 7 du chap. IV).

6) Le produit infini de facteur général $(1+i\,n)$ n'est pas convergent, mais le produit des modules de ses facteurs est absolument convergent.

Appendice .

Mesure des grandeurs et caractérisations du groupe additif R .

Le théorème fondamental sur les groupes à un paramètre (§ 2, th. 3) montre en particulier que tout groupe topologique homéomorphe au groupe additif R des nombres réels lui est nécessairement isomorphe. On peut donc penser qu'il existe une caractérisation purement topologique (c'est-à-dire ne faisant appel qu'à des notions topologiques, mais non aux propriétés du groupe Q , ni à celles de la structure d'ordre de R), de la structure topologique du groupe R ; effectivement, une telle caractérisation est possible, mais comme elle exige d'assez longs développements et est plus curieuse qu'utile, nous ne la donnerons pas dans le texte de cet Appendice (voir exerc. 3).

Nous allons montrer par contre que la structure de groupe totalement ordonné de R peut être caractérisée par des propriétés ne faisant pas intervenir le groupe Q qui lui a donné naissance. Cette caractérisation peut être rattachée à une question plus générale, dont l'origine est le problème fondamental de la mesure des grandeurs dans les sciences expérimentales. Sous une forme schématique, ce problème est le suivant : les méthodes expérimentales, appliquées à certains phénomènes, permettent d'attacher (d'une manière tout idéale) à ces phénomènes un ensemble E , dont les éléments sont qualifiés de grandeurs (d'une certaine espèce, en rapport avec les phénomènes étudiés), et dans lequel sont définiss : 1^{o} une loi de composition (interne) ; 2^{o} une structure d'ordre. Il s'agit de savoir à quels axiomes doivent

satisfaire ces deux structures pour qu'on puisse affirmer qu'il existe un isomorphisme de E sur une partie E' de l'ensemble R, faisant correspondre à la loi de composition dans E l'addition dans E', et à la structure d'ordre de E la structure d'ordre induite sur E' par celle de R. Lorsque cela est possible, le nombre réel de E' associé à une grandeur de l'ensemble E par cet isomorphisme, sera dit sa mesure.

Abordons le problème d'une façon précise. Nous considérerons un ensemble E muni d'une structure d'ensemble totalement ordonné, et d'une loi de composition associative, notés multiplicativement ; nous supposerons en outre que les axiomes suivants sont vérifiés :

(GR_I) E a un plus petit élément ω, qui est élément unité de la loi de composition (autrement dit $\omega x = x\omega = x$ quel que soit $x \in E$).

(GR_{II}) La relation $x < y$ entraîne $xz < yz$ et $zx < zy$, quel que soit $z \in E$.

(GR_{III}) Quels que soient $x > \omega$, $y > \omega$, il existe un entier $n > 0$ tel que $y \leqslant x^n$ (axiome d'Archimède).

Proposition 1: Si E satisfait aux axiomes (GR_I), (GR_{II}), (GR_{III}) il existe une représentation croissante f de E dans le groupe additif R.

Remarquons d'abord qu'il résulte de (GR_{II}) et (GR_I), par récurrence sur n, que $x > \omega$ entraîne $x^{n+1} > x^n$ quel que soit l'entier $n > 0$; d'autre part, $x < y$ entraîne $x^2 < xy < y^2$, donc $x^2 < y^2$, et on en déduit, par récurrence, que $x^n < y^n$ quel que soit l'entier $n > 0$. On notera enfin que tout élément z de E est régulier (Alg., chap.I, §) ; en effet la relation $xz = yz$ entraîne nécessairement $x = y$, sans quoi on aurait, soit $x < y$, et alors $xz < yz$, soit $y < x$, et $yz < xz$, contrairement à l'hypothèse ; de même, on voit que $zx = zy$ entraîne $x = y$.

Soit a un élément arbitraire $>\omega$ de E . Si m et n sont deux entiers positifs tels que $a^n \leqslant x^m$ (resp. $a^n \geqslant x^m$), on a aussi, pour tout entier $k>0$, $a^{kn} \leqslant x^{km}$ (resp. $a^{kn} \geqslant x^{km}$). Considérons alors, pour tout $x \in E$, l'ensemble A_x des nombres rationnels $r=p/q \geqslant 0$ tels que $a^p \leqslant x^q$; d'après ce qui précède, cette propriété de r ne dépend pas de sa représentation fractionnaire. A_x est <u>majoré</u> dans R , car si n est un entier tel que $x \leqslant a^n$ (qui existe d'après (GR_{III})) et si $a^p \leqslant x^q$, on a $a^p \leqslant a^{qn}$, donc $p/q \leqslant n$; soit f(x) sa <u>borne supérieure</u> ; nous allons voir que f est une représentation du type voulu.

Si $x \leqslant y$, on a $A_x \subset A_y$, car la relation $a^p \leqslant x^q$ entraîne $a^p \leqslant y^q$; donc $f(x) \leqslant f(y)$, f est <u>croissante</u> ; il suffit donc de montrer que $f(xy)=f(x)+f(y)$ quels que soient x et y dans E . Remarquons pour cela que, si $x^n \leqslant a^m$, m/n est un <u>majorant</u> de A_x , car si $a^p \leqslant x^q$, on a $a^{pn} \leqslant x^{qn} \leqslant a^{qm}$, donc $pn \leqslant qm$, $p/q \leqslant m/n$. Prenons alors arbitrairement un entier n ; d'après (GR_{III}), il existe un entier p tel que $a^p \leqslant x^n < a^{p+1}$, et un entier q tel que $a^q \leqslant y^n < a^{q+1}$; il en résulte que $p/n \leqslant f(x) \leqslant (p+1)/n$, $q/n \leqslant f(y) \leqslant (q+1)/n$. D'autre part, $a^{p+q} \leqslant x^n y^n < a^{p+q+2}$, et $a^{p+q} \leqslant y^n x^n \leqslant a^{p+q+2}$; nous allons voir qu'on peut en déduire que $a^{p+q} \leqslant (xy)^n < a^{p+q+2}$.

En effet, supposons par exemple qu'on ait $xy \leqslant yx$; on en déduit d'abord, par récurrence sur m , que $x^m y \leqslant yx^m$; en effet, on a $x^m y = x(x^{m-1}y) \leqslant x(yx^{m-1}) = (xy)x^{m-1} \leqslant (yx)x^{m-1} = yx^m$. On voit de même qu'on a $xy^m \leqslant y^m x$. Montrons alors qu'on a $x^n y^n \leqslant (xy)^n \leqslant (yx)^n \leqslant y^n x^n$. Il suffit de raisonner par récurrence sur n ; on a $x^n y^n = x(x^{n-1}y)y^{n-1} \leqslant x(yx^{n-1})y^{n-1} = (xy)(x^{n-1}y^{n-1}) \leqslant (xy)(xy)^{n-1} = (xy)^n$ $(xy)^n \leqslant (yx)^n = (yx)(yx)^{n-1} \leqslant (yx)(y^{n-1}x^{n-1}yx) = y(xy^{n-1})x^{n-1} \leqslant$ $\leqslant y(y^{n-1}x)x^{n-1} = y^n x^n$, ce qui démontre la proposition.

On raisonnerait de même lorsque $yx \leqslant xy$, et on voit qu'on a dans tous les cas

$$(p+q)/n \leqslant f(xy) \leqslant (p+q+2)/n$$

et par suite $|f(xy)-f(x)-f(y)| \leqslant 2/n$;

comme n est arbitraire, $f(xy)=f(x)+f(y)$, ce qui achève la démonstration.

La représentation f ainsi définie n'est pas biunivoque en général.

Prenons par exemple pour E la partie du produit $\mathcal{N} \times R_+$ formée du couple (0,0) et des couples (n,x) où $n \geqslant 1$; la loi de composition sera le produit des lois additives de $\mathcal{N}$ et R_+ ; nous ordonnerons E lexicographiquement, c'est-à-dire en posant $(n,x) < (m,y)$ si $n < m$ ou si $n = m$ et $x < y$. Il est immédiat que les axiomes (GR_I) et (GR_{II}) sont vérifiés ; quant à (GR_{III}), si (n,x) et (m,y) sont $> (0,0)$, on a $n > 0$ et $m > 0$, donc il existe p tel que $m < pn$, ce qui entraîne $(n,y) < p(n,x)$. Pourtant, si on prend $a=(1,0)$, la représentation f construite suivant le procédé de la démonstration qui précède, est telle que $f((n,x))=n$; elle n'est donc pas biunivoque.

Proposition 2. Il existe une représentation croissante et biunivoque f de E dans le groupe additif R , si E satisfait aux axiomes (GR_I), (GR_{II}) et (GR_{IIIa}) Quels que soient x,y,z, tels que $\omega \leqslant x < y$, $\omega \leqslant z$, il existe un entier $n > 0$ tel que $x^n z \leqslant y^n$ ou $zx^n \leqslant y^n$.

On notera que cet axiome entraîne (GR_{III}), en y faisant $x=\omega$. Il suffit d'établir que f est strictement croissante ; or, supposons $\omega \leqslant x < y$; supposons qu'il existe n tel que $x^n a^2 \leqslant y^n$; si p est le plus grand entier tel que $a^p \leqslant x^n$, on a $a^{p+2} \leqslant x^n a^2 \leqslant y^n$; mais $x^n < a^{p+1}$, donc $f(x) \leqslant (p+1)/n$ et $f(y) \geqslant (p+2)/n$, d'où la proposition. Démonstration analogue si $a^2 x^n \leqslant y^n$.

Corollaire. Si E satisfait aux axiomes (GR_I), (GR_{II}) et (GR_{IIIa}), la loi de composition dans E est commutative.

Au contraire, on peut donner des exemples d'ensembles E satisfaisant à (GR_I), (GR_{II}) et (GR_{III}), mais où la loi de composition n'est pas commutative (exerc. 1).

Proposition 3. L'axiome (GR_{IIIa}) est entraîné par les axiomes (GR_I) (GR_{II}), (GR_{III}) et

(GR_{IV}) Si $x \leqslant y$, il existe z tel que $y = zx$.

En effet, supposons $\omega \leqslant x < y$ et $\omega \leqslant z$; il existe t tel que $y=tx$. Supposons par exemple $tx \leqslant xt$; alors, d'après la démonstration de la prop. 1, $t^n x^n \leqslant (tx)^n = y^n$ quel que soit n. Prenons n tel que $z \leqslant t^n$, ce qui est possible d'après (GR_{III}) (on a en effet $t > \omega$) ; il en résulte que $zx^n \leqslant t^n x^n \leqslant y^n$, d'où (GR_{IIIa}). Démonstration analogue si $tx \geqslant xt$.

On notera que l'élément $a > \omega$ de E a été pris arbitrairement ; la représentation f construite dans la démonstration de la prop. 1 est telle que $f(a)=1$; c'est la seule représentation croissante de E dans R ayant cette propriété. En effet, si $a^p \leqslant x^q < a^{p+1}$, on a nécessairement, pour une représentation croissante g de E dans $\mathbb{R}$, telle que $g(a)=1$, $pg(a) \leqslant qg(x) \leqslant (p+1)g(a)$, autrement dit $p/q \leqslant g(x) \leqslant (p+1)/q$, ce qui montre que $g(x)$ est la borne supérieure de A_x, donc que $g=f$. La valeur de $f(x)$ est appelée la mesure de la grandeur x, lorsque a est pris comme grandeur unité.

Remarque. Toute partie E' de $\mathbb{R}_+$, stable pour l'addition et contenant 0, satisfait évidemment à (GR_I), (GR_{II}) et (GR_{IIIa}) (mais pas nécessairement à (GR_{IV}) ; ces trois axiomes sont donc nécessaires et suffisants pour que E soit isomorphe à une telle partie de $\mathbb{R}$.

Application aux groupes. Nous dirons qu'un groupe G (commutatif ou non, noté multiplicativement) est un groupe totalement ordonné s'il est muni d'une structure d'ensemble totalement ordonné telle que l'axiome (GR_{II}) soit satisfait. Si ω désigne l'élément unité de G, l'ensemble E des éléments $\geqslant \omega$ de G satisfait évidemment à (GR_I) et (GR_{II}) ; il satisfait aussi à (GR_{IV}), car si $\omega \leqslant x \leqslant y$, on a, d'après ($GR_{II}$), $\omega = xx^{-1} \leqslant yx^{-1}$ donc $t=yx^{-1} \in E$, et $y=tx$. Nous dirons que G est un groupe archimédien si E satisfait en outre à (GR_{III}) ; pour tout $a > \omega$ il existe alors une représentation croissante biunivoque et une seule, f, de E dans R_+, telle que $f(a)=1$. On prolonge f en une représentation croissante de G dans R en posant $f(x)=-f(x^{-1})$ pour $x \leqslant \omega$. On obtient évidemment une fonction strictement croissante, car $f(x)<0$ pour $x<\omega$. D'autre part, si $x \leqslant \omega \leqslant y$, et $xy \geqslant \omega$, on a $y=x^{-1}(xy)$, donc $f(y)=f(x^{-1})+f(xy)=f(xy)-f(x)$, $f(xy)=f(x)+f(y)$. Si au contraire $xy \leqslant \omega$, $x^{-1}=y(xy)^{-1}$, donc $f(x^{-1})=f(y)+f((xy)^{-1}$ c'est-à-dire $-f(x)=f(y)-f(xy)$, $f(xy)=f(x)+f(y)$. Enfin, si $x \leqslant \omega$, $y \leqslant \omega$, on a $xy \leqslant \omega$, donc $(xy)^{-1}=y^{-1}x^{-1}$, $f((xy)^{-1}=f(y^{-1}) + f(x^{-1})$, $-f(xy)=-f(x)-f(y)$, d'où encore $f(xy)=f(x)+f(y)$, ce qui montre que f est une représentation de G dans R. Ainsi :

Proposition 4. Pour qu'un groupe totalement ordonné G soit isomorphe à un sous-groupe du groupe additif R, il faut et il suffit qu'il soit archimédien.

Nous allons en déduire une caractérisation du groupe R lui-même :

Proposition 5. Pour qu'un groupe totalement ordonné G soit ismorphe au groupe additif R, il faut et il suffit qu'il ne soit pas discret, et que toute suite croissante majorée dans G admette une borne supérieure.

Montrons d'abord que la seconde de ces conditions entraîne que G est archimédien. Supposons en effet que, pour un $x > \omega$, il existe y tel que $x^n \leqslant y$ quel que soit n ; la suite croissante (x^n), étant majorée, aurait une borne supérieure a ; comme $x > \omega$, il existerait n tel que $ax^{-1} < x^n \leqslant a$, d'où $a < x^{n+1}$, contrairement à la définition de a, d'où la proposition. On peut donc supposer, d'après la prop.4, que G est un sous-groupe de $\mathbb{R}$ (noté désormais additivement). La seconde condition de l'énoncé entraîne que G est fermé ; en effet, soit a un point adhérent à G ; il existe, soit une suite croissante, soit une suite décroissante de points de G ayant pour limite a ; dans le premier cas, $a \in G$; dans le second, si (x_n) est une suite décroissante tendant vers a, $(-x_n)$ est une suite croissante tendant vers -a, donc $-a \in G$ et par suite $a \in G$. Donc G est, ou bien identique à $\mathbb{R}$, ou bien de la forme $a\mathbb{Z}$; mais le second de ces deux cas est exclu par l'hypothèse que G est non discret, d'où la proposition.

Exercices. 1) Soit G un groupe non commutatif totalement ordonné (voir p. ex. chap.IV, § 1, exerc. 3 et 4). On considère, dans le produit $\mathbb{N} \times G$, l'ensemble E formé du couple (0,e) (e unité de G) et des couples (n,x), où n parcourt l'ensemble des entiers $\geqslant 1$, et x parcourt G. On prend comme loi de composition dans G, $(n,x)(n',x') = (n+n', xx')$, et on ordonne E lexicographiquement ($(n,x) < (n',x')$ si $n < n'$ ou si $n = n'$ et $x < x'$). Montrer que l'ensemble E, muni de ces deux structures, satisfait aux axiomes (GR_I), (GR_{II}) et (GR_{III}).

¶ 2) Soit G un groupe totalement ordonné ayant plus d'un élément ; si, quand on munit G de la topologie $\mathcal{C}_0(G)$ (chap.I, § 1, exerc.3), G est connexe, G est isomorphe au groupe additif $\mathbb{R}$ (voir chap.IV, § 2, exerc. 8).

¶ 3) <u>Un groupe topologique G est isomorphe à $\mathbb{R}$ s'il est connexe et si le complémentaire de l'élément unité e dans G est non connexe</u>.

On montrera successivement que :

a) Si A est une composante connexe de $G^* = \complement\{e\}$, l'adhérence de A dans G est $A \cup \{e\}$.

b) Si A et B sont deux composantes connexes de G^*, $x \in A$, $y \in B$, l'ensemble $\{x\} \cup (xB) \cup (Ay) \cup \{y\}$ est connexe ; en conclure que $B = A^{-1}$, et que G^* a exactement <u>deux</u> composantes connexes A et A^{-1}.

c) La relation $yx^{-1} \in \bar{A}$ est une relation d'ordre faisant de G un groupe totalement ordonné (montrer que $A\bar{A}$ et $\bar{A}A$ sont contenus dans A et que $x\bar{A}x^{-1} \subset \bar{A}$ quel que soit $x \in G$).

d) La topologie $\mathfrak{T}_0(G)$ est moins fine que la topologie donnée $\mathfrak{T}$ sur G (montrer que A est ouvert dans $\mathfrak{T}$).

Conclure à l'aide de l'exerc. 2 du § 11 du chap.I, et de l'exerc.2 ci-dessus.

¶ 4) Soit E un ensemble totalement ordonné, satisfaisant aux conditions suivantes :

1° E a un plus petit élément ω ;

2° Il existe un élément $a > \omega$ de E et si on pose $V = [\omega, a]$ une application $(x,y) \to xy$ de $V \times V$ dans E telle que $\omega x = x\omega = x$ quel que soit $x \in V$, et $(xy)z = x(yz)$ lorsque les deux membres sont définis ;

3° Si x, y, z sont des éléments de V tels que $x < y$, on a $xz < yz$ et $zx < zy$;

4° Pour tout $x \in V$, il existe y tel que $\omega < y$, et que $y^2 \leqslant x$;

5° Quels que soient x et y dans V tels que $\omega < x$, $\omega \leqslant y$, l'ensemble des entiers $n > 0$ tels que x^n soit défini et $\leqslant y$, est fini.

Montrer qu'il existe une application croissante f de V dans l'intervalle $[0,1]$ de R telle que, pour tout couple x,y d'éléments de V tels que $xy \in V$, $f(xy)=f(x)+f(y)$, et que $f(a)=1$ (On établira d'abord qu'il existe une suite (ε_n) d'éléments de V telle que $\varepsilon_n^2 \leqslant \varepsilon_{n-1}$; on prouvera qu'il n'existe aucun élément b tel que $\omega < b \leqslant \varepsilon_n$ quel que soit n ; on désignera par $p_n(x)$, pour tout $x \in V$, le plus grand entier p tel que $\varepsilon_n^p \leqslant x$. On montrera que $\lim_{n\to\infty} p_n(x)=+\infty$, que $\lim_{n\to\infty} p_n(x)/p_n(a)$ existe et que si on désigne cette limite par f(x) , f satisfait aux conditions de l'énoncé).

¶ 5) Donner un exemple d'ensemble E satisfaisant aux conditions de l'exerc. 4, mais où l'application f ne soit pas biunivoque. Montrer que f est biunivoque si E satisfait à la condition supplémentaire :

6° Si $\omega \leqslant x \leqslant y \leqslant a$, il existe $t \in V$ tel que $y=tx$.

6) Soit E un ensemble ordonné satisfaisant aux conditions 1°, 2°, 3°, 4° et 6° des exerc. 4 et 5 , et tel en outre que toute suite croissante majorée d'éléments de V ait une borne supérieure. Montrer que E satisfait à la condition 5° , et que l'application f est une application strictement croissante de V sur $[0,1]$.

¶ 7) Soit G un groupe topologique possédant la propriété suivante : il existe trois voisinages ouverts, symétriques et connexes U,V,W de l'unité e de G , tels que $V^2 \subset U$ et $W^2 \subset V$, et que le complémentaire de e par rapport à U soit non connexe. Montrer que G est localement isomorphe à $\mathbb{R}$ (Raisonner comme dans l'exerc. 3, en définissant sur W une structure d'ensemble totalement ordonné, telle que $\mathscr{C}_0(W)$ soit moins fine que la topologie induite sur W par celle de G , et qu'on puisse appliquer à l'ensemble E des éléments $\geqslant e$ de W les exerc. 4 et 6).
