3

ETUDES

Une présentation des nombres réels

par Pierre SAMUEL, Université Paris-Sud, 91405 ORSAY

Les programmes en vigueur dans le Premier Cycle Universitaire et dans les Classes Préparatoires, et surtout les habitudes prises, font que l'on consacre beaucoup de temps et d'énergie à la construction de **R** et à la démonstration de ses propriétés élémentaires. Ce qui suit est l'esquisse d'un mode de présentation *économique*, qui vise à obtenir rapidement une propriété forte (l'existence de bornes supérieures) et dont les retombées immédiates sont nombreuses (unicité de **R**, multiplication, exponentielle et logarithme, mesure des grandeurs, exposé facile de la topologie de **R**, ...).

§ 1. Notions sur les groupes ordonnés.

On appelle *groupe ordonné* un groupe G (non nécessairement commutatif, ici noté multiplicativement) muni d'une relation d'ordre $x \leqslant y$ telle que :

(1) $x,y,z \in G$ et $x \leqslant y \Rightarrow xz \leqslant yz$ et $zx \leqslant zy$.

On en déduit aussitôt que l'ordre est *invariant* par translations (à droite et à gauche) et qu'il est *renversé* par passage à l'inverse. Les formules (1) montrent que la manipulation des inégalités obéit aux règles usuelles, compte tenu de l'ordre des facteurs.

Un groupe ordonné G est dit *archimédien* si, quels que soient les éléments a,b plus grands que e (e : élément neutre) de G, il existe un entier $n \geqslant 0$ tel que $b \leqslant a^n$.

On dit qu'un ensemble ordonné G est *dense* si, entre deux éléments quelconques de G, on peut en insérer un troisième (en sabir formalisé : $a,b \in G$ et $a < b \Rightarrow (\exists\ c)(a < c < b)$). Ainsi $\mathbf{Q}$ est dense, mais $\mathbf{Z}$ ne l'est pas.

Nous porterons particulièrement notre attention sur les groupes *totalement ordonnés* G jouissant des deux propriétés suivantes :

a) G est *dense*.

b) Toute partie non vide majorée A de G admet une *borne supérieure* (c'est-à-dire un plus petit majorant) (notation : sup(A)). Pour alléger, un tel groupe sera dit *parfait* dans ce qui suit, mais on pourra oublier ce mot ensuite. Le passage à l'inverse montre que toute partie non vide minorée de G admet une borne inférieure.

Théorème 1. *Tout groupe parfait* G *est archimédien.*

Donnons-nous $a,b \in G$ tels que $a,b > e$ (élément neutre). Si aucun a^n ($n \in \mathbf{N}$) ne dépasse b, l'ensemble P des a^n est majoré par b. Posons alors $s = \sup(P)$. On a $a^{n+1} \leqslant s$ pour tout n, donc $a^n \leqslant sa^{-1}$; de sorte que sa^{-1} est un majorant de P. Mais $sa^{-1} < s$ et s n'est pas le plus petit majorant de P. Contradiction.

§ 2. **Construction d'un groupe parfait.**

Partons du groupe additif $\mathbf{Q}$ des nombres rationnels. Celui des nombres décimaux (les $\frac{p}{10^n}$ avec $p \in \mathbf{Z}$, $n \in \mathbf{N}$) ou des nombres dyadiques (les $\frac{p}{2^n}$) peut jouer ici le même rôle que $\mathbf{Q}$. C'est un groupe totalement ordonné dense et archimédien qui n'est *pas* parfait : l'ensemble des nombres rationnels r tels que $r^2 < 5$ n'admet pas de borne supérieure dans $\mathbf{Q}$.

Nous appellerons *section* de $\mathbf{Q}$ (ou "section commençante ouverte" pour alourdir) toute partie S de $\mathbf{Q}$ qui jouit des propriétés suivantes :

a) S est distincte de ϕ et de $\mathbf{Q}$ tout entier ;

b) $x \in S$ et $y \leqslant x \Rightarrow y \in S$;

c) S n'a pas de plus grand élément.

Pour $r \in \mathbf{Q}$, l'ensemble S_r des nombres rationnels x tels que $x < r$ est une section (la propriété c) est vraie car $\mathbf{Q}$ est dense). Nous noterons $\mathbf{R}$ *l'ensemble des sections de* $\mathbf{Q}$.

Nous munissons **R** :

— d'une relation *d'ordre* qui est tout simplement l'inclusion ;

— de la *loi de composition* + où S+S' est l'ensemble des sommes s+s' où s parcourt S et s' parcourt S'. En effet S+S' est bien une section :

a) Si a (resp. a') majore S (resp. S'), a+a' majore S+S', d'où a+a' ∉ S+S'.

b) Si $y \leqslant s+s'$ $(s \in S, s' \in S')$, on a
$y = (s-(s+s'-y)) + s'$ où $s-(s+s'-y) \leqslant s$ et donc
$s-(s+s'-y) \in S$.

c) Si S+S' a un plus grand élément, il s'écrit $s_0+s'_0$ $(s_0 \in S, s'_0 \in S')$ et on voit que s_0 est le plus grand élément de S ; contradiction (1).

Théorème 2. Muni de cette structure, **R** *est un groupe totalement ordonné commutatif parfait. L'application* $r \mapsto S_r$ *est un isomorphisme strictement croissant de* **Q** *sur un sous-groupe dense de* **R**.

L'associativité $(S+(S'+S'') = (S+S')+S'')$, la commutativité $(S+S' = S'+S)$ et la traduction de (1) (voir § 1) $(S \subset S' \Rightarrow S+T \subset S'+T)$ sont évidentes. Comme **Q** est dense, on a $S_{r+r'} = S_r + S_{r'}$ $(r,r' \in \mathbf{Q})$. Entre deux sections S,S' telles que $S \subsetneq S'$, on peut insérer une section S_r (prendre $r \in S'$, $r \notin S$). Une famille majorée $(S_\alpha)_{\alpha \in I}$ de sections a une borne supérieure, qui est tout simplement leur réunion $\bigcup_{\alpha \in I} S_\alpha$.

La densité de **Q** montre que la section S_0 (formée des rationnels plus petits que 0) est élément neutre de **R**. Reste à montrer que toute section S admet une section "opposée". Or la voici :

$$S' = \left\{ x \in \mathbf{Q} \mid x+S \subsetneq S_0 \right\}$$

On vérifie en effet que S' est bien une section : $S' \neq \phi$ car S admet un majorant a et on prend $x = -(a+1)$; $S' \neq \mathbf{Q}$ car n'importe quel $-s$, $s \in S$, majore strictement S' ; b) est évidente ; pour tout élément x_0 de S', $x_0 + S$ est une section strictement majorée par un rationnel plus petit que 0, de sorte que $x_0 - \frac{a}{2} + S \subsetneq S_0$, et que x_0 n'est pas le plus grand élément de S'. Enfin on a bien $S+S' = S_0$. En effet $S+S' \subset S_0$ est clair.

(1) Désormais les vérifications ayant cet ordre de difficulté seront laissées au lecteur.

Inversement, pour tout rationnel a plus grand que 0, il y a un plus grand entier $n \in \mathbf{Z}$ tel que $n\frac{a}{2} \in S$; alors $(n+1)\frac{a}{2}$ majore S, $-(n+1)\frac{a}{2} + S \subset S_+$, $-(n+\epsilon)\frac{a}{2} + S \subsetneq S_+$, $-(n+\epsilon)\frac{a}{2} \in S'$; d'où $-a = n\frac{a}{2} + (-(n+\epsilon)\frac{a}{2}) \in S+S'$. C.Q.F.D.

On identifie **Q** à son image par $r \mapsto S_r$, de sorte que **Q** est regardé comme un sous-groupe de **R**.

Les éléments de **R** s'appellent *les nombres réels.*

§ 3. Un théorème fondamental et ses premières conséquences.

Bien que le théorème suivant ne soit pas énoncé dans le langage des mathématiciens de l'antiquité, il est juste de l'attribuer au mathématicien grec Eudoxe de Cnide (4ème siècle av. J.C.), car sa "théorie des grandeurs" est justement fondée sur les manipulations d'inégalités qui nous conduiront à sa démonstration (voir la Note Historique de Bourbaki, Topologie Générale, chap. IV).

Théorème 3 (Eudoxe). *Soient* G *et* G' *deux groupes totalement ordonnés,* e *et* e' *leurs éléments neutres,* $a > e$ *et* $a' > e'$ *des éléments donnés de* G *et* G'. *On suppose* G *archimédien et* G' *parfait. Il existe alors un unique homomorphisme strictement croissant* $\varphi : G \to G'$ *tel que* $\varphi(a) = a'$.

Afin de se donner du courage pour aborder la démonstration assez longue du théorème d'Eudoxe (voir § 6), on va d'abord en déduire un bon nombre de conséquences faciles et importantes.

Corollaire 1. *Tout groupe totalement ordonné archimédien* G *est isomorphe à un sous-groupe (additif) de* **R** *et est commutatif.*

Prendre $G' = \mathbf{R}$ dans le th. 3 ; noter que φ est injective (car strictement croissante) et définit un isomorphisme de G sur $\varphi(G)$.

Corollaire 2. *Deux groupes totalement ordonnés parfaits quelconques* G,G' *sont isomorphes (et donc isomorphes à* **R**).

Fixons $a > e$ et $a' > e'$ dans G et G'. Comme G est archimédien (th. 1) on a un homomorphisme strictement croissant $\varphi : G \to G'$ tel que $\varphi(a) = a'$. Inversant les rôles, on obtient $\Psi : G' \to G$ tel que $\Psi(a') = a$. L'assertion d'unicité du th. 3 montre que $\varphi \circ \Psi$ et $\Psi \circ \varphi$ sont les applications identiques de G' et de G. C'est "fonctoriel", comme on dit parfois.

On peut donc dire que **R** est "le seul" groupe totalement ordonné parfait. Ainsi, lorsqu'on vous définit R par un autre procédé que celui du § 2 (par exemple suites de Cauchy, filtres de Cauchy, ...) ou qu'on vous le caractérise axiomatiquement, vous pourrez être sûrs que cet "autre **R**" est isomorphe à celui d'ici *dès que* vous vous serez assuré que c'est un groupe totalement ordonné parfait. Cela fait, "mes" nombres réels sont "les mêmes" que ceux de tous mes collègues.

§ 4. **Multiplication dans R, exponentielle, logarithme.**

Comme il est habituel, on notera + la loi de composition de **R** et $\leqslant$ sa relation d'ordre. Comme à la fin du § 2, on convient que $\mathbf{Q} \subset \mathbf{R}$. Pour $a \in \mathbf{R}$, $a > 0$, on note f_a *l'unique endomorphisme* (homomorphisme de **R** dans **R**) strictement croissant de **R** qui amène 1 en a ($f_a(1) = a$) (th. 3). Pour $a < 0$, on pose $f_a = -f_{-a}$ (l'endomorphisme $-f$ est défini par $(-f)(x) = -f(x)$). On pose enfin $f_0 = 0$ (endomorphisme "nul" amenant tout le monde en 0). On définit une *multiplication* dans **R** au moyen de la formule :

$$ab = f_a(b). \tag{2}$$

Théorème 4. *Cette multiplication prolonge celle de* **Q**.

Pour $n \in \mathbf{N}$, $n > 0$, l'application $x \mapsto x + x + \ldots + x$ (n fois) est un endomorphisme strictement croissant de **R** qui amène 1 en n ; donc $f_n(x) = nx$, formule encore valable pour tout $n \in \mathbf{Z}$. Pour $r = p/q \in \mathbf{Q}$ $(p,q \in \mathbf{Z}, q > 0)$, on voit de même que $qf_r \leqslant f_p$. Donc, pour r et $r' \in \mathbf{Q}$, on a $qf_r(r') = f_p(r') = pr'$ d'où $f_r(r') = \dfrac{pr'}{q} = rr'$. C.Q.F.D.

Théorème 5. *Pour la multiplication et la relation d'ordre* $\leqslant$, *l'ensemble* $\mathbf{R}_+^*$ *des nombres réels* > 0 *est un groupe totalement ordonné parfait, donc commutatif.*

En effet, $a,b > 0$ implique $ab = f_a(b) > 0$ en vertu de la stricte croissance de f_a. L'associativité équivaut à la formule $f_a \circ f_b = f_{ab}$ (faites le calcul !), qui résulte de ce que $f_a \circ f_b$ est un endomorphisme croissant qui amène 1 en $f_a(f_b(1)) = f_a(b) = ab$. Comme l'application identique de **R** n'est autre que f_1, 1 est élément neutre à gauche, et aussi à droite en vertu de a. $1 = f_a(1) = a$. Pour trouver l'inverse de a, considérons l'endomorphisme strictement croissant g de **R** tel

que $g(a) = 1$ (th. 3) et posons $a' = g(1)$; alors $g = f_{a'}$, $f_{a'} \circ f_a = f_1$, $a'a = 1$. Ainsi $\mathbf{R}_+^*$ est bien un groupe pour la multiplication.

Assurons-nous que c'est un groupe ordonné pour $\leqslant$ (relation (1) du § 1). La croissance de f_a $(a > 0)$ montre que $b \leqslant b'$ implique $ab \leqslant ab'$. D'autre part, pour $0 < a \leqslant a'$, $f_a + f_{a'-a}$ est un endomorphisme de $\mathbf{R}$, est croissant (comme somme de deux applications croissantes) et amène 1 en $a - (a'-a) = a'$; c'est donc $f_{a'}$; ainsi, pour tout $b > 0$, on a

$$a'b = f_{a'}(b) = f_a(b) + f_{a'-a}(b) \geqslant f_a(b) = ab.$$

Enfin les propriétés de densité et d'existence de bornes supérieures se transmettent de $\mathbf{R}$ à $\mathbf{R}_+^*$ (§ 1), qui est donc parfait et par conséquent commutatif (cor. 1 du th. 3).

Corollaire 1. *Pour tout nombre réel* $a > 1$, *il existe un unique isomorphisme croissant* $\exp_a$ *de* $\mathbf{R}$ *sur* $\mathbf{R}_+^*$ *tel que* $\exp_a(1) = a$.

C'est un cas particulier du théorème 3. On a $\exp_a(x+y) = \exp_a(x)\exp_a(y)$ pour tous $x,y \in \mathbf{R}$. On écrit souvent $\exp_a(x) = a^x$. L'isomorphisme $\mathbf{R}_+^* \to \mathbf{R}$ récirpoque de $\exp_a$ se note $\log_a$; on a $\log_a(xy) = \log_a(x) + \log_a(y)$.

Corollaire 2. *Muni de l'addition et de la multiplication* $ab = f_a(b)$, $\mathbf{R}$ *est un corps commutatif.*

Les formules $a(-b) = -ab$, $(-a)b = -ab$ (résulte de la définition de f_{-a}) et $(-a)(-b) = ab$, jointes au th. 5, montrent la commutativité de la multiplication dans $\mathbf{R}$ tout entier. Pour $a < 0$, on constate que $-(-a)^{-1}$ est inverse de a. Reste à vérifier une distributivité, la plus facile, $a(b+b') = ab+ab'$; or elle résulte de ce que f_a est un endomorphisme.

De plus $\mathbf{R}$ est un *corps ordonné*, ce qui signifie que la multiplication est "compatible" avec la relation d'ordre, au sens suivant :

(3) $$x \leqslant x',\ y > 0 \Rightarrow xy \leqslant x'y.$$

§ 5. Aperçu sur la mesure des grandeurs.

Pour fixer les idées, occupons-nous des *masses*. Etant donnés deux objets matériels A,B, la relation "A et B mettent en équilibre les plateaux d'une (ou de toute) balance" est une relation d'équivalence (vérification expérimentale) ; notation $A \sim B$. La classe d'équivalence de A s'appelle la *masse* de A. Soit $\mathcal{M}$ l'ensemble des masses.

Notons A T B la juxtaposition de deux objets distincts (et dissociables ; sinon on remplace l'un d'eux par un objet "tout pareil"). On constate expérimentalement que, si $A \sim A'$, alors $A \top B \sim A' \top B$. Ainsi T "passe au quotient" et définit une loi de composition sur $\mathcal{M}$. Associativité et commutativité sont évidentes. La vérification (expérimentale) de $A \top B \sim A' \top B \Rightarrow A \sim A'$ montre que la propriété de simplification est vraie dans $\mathcal{M}$. Le théorème de symétrisation permet alors de plonger $\mathcal{M}$ dans un *groupe* G.

D'autre part la relation entre objets matériels A,B : "chargée de A sur un plateau et de B sur l'autre, une (ou toute) balance penche du côté de A", — définit une relation d'ordre total sur $\mathcal{M}$. Elle est compatible avec la loi de composition (vérification expérimentale). On la prolonge à G de la même façon qu'on prolonge à $\mathbb{Z}$ l'ordre de N. Ainsi G est un *groupe ordonné*.

Si l'on met suffisamment de grains de sable sur un plateau d'une balance, on parvient à équilibrer un éléphant placé sur l'autre. Des constatations (moins douteuses et plus élaborées !) de ce genre amènent à admettre que $\mathcal{M}$ (et donc G) est *archimédien*. On choisit alors un objet matériel bien déterminé A ("étalon de masse") et on note α sa classe d'équivalence dans $\mathcal{M}$. D'après le théorème d'Eudoxe (th. 3), il y a un unique homomorphisme croissant $m : G \to \mathbb{R}$ tel que $m(\alpha) = 1$. Pour toute masse $\mu \in \mathcal{M}$, $m(\mu)$ est la *mesure* de la masse μ. Mais on dit souvent que le nombre μ (classe de B) est la masse de l'objet B, identifiant ainsi β à son image $m(\beta)$ dans $\mathbb{R}$.

§ 6. Démonstration du théorème d'Eudoxe.

Réénonçons ce théorème :

Théorème 3 (Eudoxe). *Soit* G *et* G' *deux groupes totalement ordonnés, e et e' leurs éléments neutres, a > e et a' > e' des éléments donnés de* G *et* G'. *On suppose* G *archimédien et* G' *parfait. Il existe alors un unique homomorphisme strictement croissant* $\varphi : G \to G'$ *tel que* $\varphi(a) = a'$.

D'abord quelques lemmes :

Lemme 1. *Si* x *et* y *sont deux éléments d'un groupe dense* H *tels que* $x \leqslant yv$ (resp. vy) *pour tout* $v > e$, *alors* $x \leqslant y$.

Sinon $y < x$ et on insère $z : y < z < x$. Alors $v = y^{-1}z > e$ contredit l'hypothèse $x \leqslant yv$ car $yv = z$.

Lemme 2. Pour tout élément $u > e$ *d'un groupe dense* H *et tout entier* $q > 0$, *il existe* $v > e$ *dans* H *tel que* $v^q \leqslant u$.

Pour $q = 2$, on insère w entre e et u ($e < w < u$), et alors $v_1 = \inf(w, w^{-1}u)$ satisfait à $v_1^2 < u$ (si $u < w^2, w^{-1}u < w$, $(w^{-1}u)^2 = w^{-1}u\,w^{-1}u < ww^{-1}u = u$). Par récurrence, on obtient $v_n > e$ tel que $(v_n)^{2^n} \leqslant u$. On choisit n tel que $2^n \geqslant q$.

Lemme 3. Soit x,z *des éléments d'un groupe ordonné tels que* $xz \leqslant zx$; *alors, pour tout* $n \geqslant 1$, *on a :*

$$x^n z^n \leqslant (xz)^n \leqslant (zx)^n \leqslant z^n x^n. \tag{3}$$

On procède par récurrence sur n. De (3) on déduit $x^{n+1}z^{n+1} = xx^n z^n z \leqslant x(zx)^n z = xzxzx\ldots zxz = (xz)^{n+1}$. L'inégalité $(xz)^{n+1} \leqslant (zx)^{n+1}$ découle aussitôt de $xz \leqslant zx$. L'inégalité $(zx)^{n+1} \leqslant z^{n+1}x^{n+1}$ se démontre comme la première.

NB. Dans un groupe totalement ordonné, on a donc ou bien (3), ou bien l'analogue $z^n x^n \leqslant (zx)^n \leqslant (xz)^n \leqslant x^n z^n$.

Lemme 4. Soit a,x,y *des éléments d'un groupe archimédien* H *tels que* $x < y$ *et* $a > e$. *Il existe alors des entiers* p *et* q, $q > 0$, *tels que :*

$$x^q \leqslant a^p < y^q \leqslant a^{p+1}. \tag{5}$$

Soit $z = \inf(yx^{-1}, x^{-1}y)$; on a $z > e$. Comme H est archimédien, on peut choisir $q > 0$ tel que $a \leqslant z^q$. Notons $p+1$ le plus petit des entiers s tels que $y^q \leqslant a^s$; alors $a^p < y^q \leqslant a^{p+1}$. Comme xz et zx sont $\leqslant y$, on a $x^q z^q \leqslant y^q$ ou $z^q x^q \leqslant y^q$ (lemme 3) ; d'où $x^q a \leqslant y^q \leqslant a^{p+1}$ ou $ax^q \leqslant y^q \leqslant a^{p+1}$, et en tous cas $x^q \leqslant a^p$.

Démonstration d'unicité de φ. Pour $b \in G$, *nous noterons* B'(b) (ou B') *l'ensemble des* $x' \in G'$ *tels que l'on ait* $x'^q \leqslant a'^p$ *pour tous les couples d'entiers* p,q ($q > 0$) *vérifiant* $b^q \leqslant a^p$. On a $\varphi(b) \in B'(b)$ car $b^q \leqslant a^p$ implique $\varphi(b^q) \leqslant \varphi(a^p)$ (croissance de φ), c'est-à-dire $\varphi(b)^q \leqslant a'^p$.

D'autre part aucun élément $y' > \varphi(b)$ de G' n'est dans B'(b). En effet, comme G' est archimédien (th. 1), il existe des entiers p,q ($q > 0$) tels que $\varphi(b)^q \leqslant a'^p < y'^q$ (lemme 4) ; en particulier $\varphi(b^q) \leqslant \varphi(a^p)$, d'où $b^q \leqslant a^p$ car φ est strictement croissante. Comme $y'^q \leqslant a'^p$ n'est pas vraie, on en déduit $y' \notin B'(b)$.

On en conclut que $\varphi(b)$ *est le plus grand élément* de B'(b), d'où son unicité car B'(b) est défini indépendamment de φ.

Démonstration d'existence de φ. Ce qui précède amène, pour tout $b \in G$, à considérer encore l'ensemble $B'(b) \subset G'$ et à poser :

$$(*) \qquad \varphi(b) = \sup(B'(b)) .$$

C'est justifié car $B'(b)$ est non vide et majoré (si r est un entier tel que $b \leqslant a^r$, a'^r majore $B'(b)$).

On a bien $\varphi(a) = a'$, et même :

$$(6) \qquad \varphi(a^n) = a'^n \text{ pour tout } n \in \mathbf{Z} .$$

En effet $x' \in B'(a^n)$ veut dire que $a^{nq} \leqslant a^p$ implique $x'^q \leqslant a'^p$. Mais $a^{nq} \leqslant a^p$ équivaut à $nq \leqslant p$ $(a > e)$. Or "$nq \leqslant p \Rightarrow x'^q \leqslant a'^{np}$" implique $x'^q \leqslant a'^{np}$ (prendre $p = nq$) et donc $x' \leqslant a'^n$; inversement, si $x' \leqslant a'^n$ et si $nq \leqslant p$, on a $x'^q \leqslant a'^{nq} \leqslant a'^p$. Donc $x' \in B'(a^n)$ équivaut à $x' \leqslant a'^n$. Ainsi a'^n est le plus grand élément de $B'(a^n)$, et donc sa borne supérieure.

Il sera utile de savoir *que* $\varphi(b) \in B'(b)$. Soit en effet p,q $(q > 0)$ deux entiers tels que $b^q \leqslant a^p$. Donnons-nous $u' > e'$ dans G' ; il existe $v' > e'$ tel que $v'^q \leqslant u'$ (lemme 2). Comme $\varphi(b) = \sup(B'(b))$, il existe $x' \in B'(b)$ tel que

$$\sup(\varphi(b)v'^{-1}, v'^{-1}\varphi(b)) \leqslant x'.$$

Par définition de $B'(b)$ on a $x'^q \leqslant a'^p$, d'où, par exemple, $\varphi(b)^q v'^{-q} \leqslant a'^p$ (lemme 3). Ainsi $\varphi(b)^q \leqslant a'^p v'^q \leqslant a'^p u'$. Comme ceci a lieu pour tout $u' > e'$, on en déduit $\varphi(b)^q \leqslant a'^p$ (lemme 1). Donc $b^q \leqslant a^p \Rightarrow \varphi(b)^q \leqslant a'^p$ et $\varphi(b) \in B'(b)$.

Pour $b \leqslant c$ dans G, on voit aisément que $B'(b) \subset B'(c)$, d'où la *croissance de* φ.

Vérifions maintenant que φ est un *homomorphisme* de groupes, c'est-à-dire que $\varphi(bc) = \varphi(b)\varphi(c)$ pour tous $b,c \in G$. Soit p et $q > 0$ des entiers tels que $(bc)^q \leqslant a^p$. Considérons les entiers r et s tels que $a^{r-1} < b^q \leqslant a^r$ et $a^{s-1} < c^q \leqslant a^s$. On a alors :

$$a^{r+s-2} < \inf(b^q c^q, c^q b^q) \leqslant (bc)^q \text{ (lemme 3)} \leqslant a^p,$$

d'où $r+s-2 < p$ et $r+s \leqslant p+1$. Comme $\varphi(b) \in B'(b)$ et $\varphi(c) \in B'(c)$, on a $\varphi(b)^q \leqslant a'^r$, $\varphi(c)^q \leqslant a'^s$, d'où, encore d'après le lemme 3, $(\varphi(b)\varphi(c))^q \leqslant a'^{r+s} \leqslant a'^{p+1}$. Posons $\varphi(b)\varphi(c) = d'$. Comme on peut remplacer le couple (p,q) par (np,nq) $(n > 0)$, on en déduit $d'^{nq} \leqslant a'^{np+1}$ pour tout $n \geqslant 0$. Pour tout $v' > e'$, on choisit un n tel que $v'^n \geqslant a'$, d'où $d'^{nq} < (a'^p v')^n$ (lemme 3). On en déduit $d'^q \leqslant a'^p v'$ pour tout $v' > e'$, d'où $d'^q \leqslant a'^p$ (lemme 1). Cela veut dire que $\varphi(b)\varphi(c) = d'$ est élément de $B'(bc)$.

D'où déjà l'inégalité

(7) $$\varphi(b)\varphi(c) \leqslant \varphi(bc)\,.$$

Pour démontrer l'inégalité opposée, considérons des éléments $x' > \varphi(b)$ et $y' > \varphi(c)$. Comme $x' \notin B'(b)$ et $y' \notin B'(c)$, il existe deux couples d'entiers (p,q), (p',q') $(q,q' > 0)$ tels que $b^q \leqslant a^p$, $x'^q > a'^p$, $c^{q'} \leqslant a^{p'}$ et $y'^{q'} > a'^{p'}$. En utilisant le lemme 3 comme ci-dessus, on en déduit $(bc)^{qq'} \leqslant a^{pq'+qp'}$ et $(x'y')^{qq'} > a'^{pq'+qp'}$; ainsi $x'y' \notin B'(bc)$, d'où $x'y' > \varphi(bc)$. Soit alors $u' > e'$ dans G', arbitraire ; prenons $v' > e'$ tel que $v'^2 \leqslant u'$ (lemme 2) et $x' = v'\varphi(b)$, $y' = \varphi(c)v'$. L'inégalité $x'y' > \varphi(bc)$ s'écrit alors $\varphi(bc) < v'\varphi(b)\varphi(c)v'$. Or, suivant que $v'\varphi(b)\varphi(c)$ est $\leqslant$ ou $\geqslant$ à $\varphi(b)\varphi(c)v'$, $v'\varphi(b)\varphi(c)v'$ est $\leqslant$ à $\varphi(b)\varphi(c)v'^2$ ou à $v'^2\varphi(b)\varphi(c)$. Donc $\varphi(bc) < \sup(u'\varphi(b)\varphi(c), \varphi(b)\varphi(c)u')$. Comme ceci a lieu pour tout $u' > e'$, on en déduit que $\varphi(bc) \leqslant \varphi(b)\varphi(c)$.

Reste à montrer la croissance *stricte* de φ, c'est-à-dire, comme φ est un homomorphisme, que $e < b$ implique $e' < \varphi(b)$. En tous cas $e' \leqslant \varphi(b)$. Or, comme G est archimédien, il existe un entier n tel que $a \leqslant b^n$. Alors $a' = \varphi(a) \leqslant \varphi(b)^n$, ce qui exclut $\varphi(b) = e'$ car $e' < a'$. C.Q.F.D. Ouf !

Appendice — La déduction des propriétés topologiques de R .

On a rapidement obtenu une propriété forte de **R**, l'existence des bornes supérieures. Il est facile d'en déduire les propriétés topologiques fondamentales de **R**. Par exemple :

1) *Compacité.* Pour montrer que, de tout *recouvrement ouvert* (U_α) d'un intervalle fermé $[a,b]$, on peut extraire un recouvrement fini, on considère l'ensemble E des $x \in [a,b]$ tels que $[a,x]$ soit recouvrable par un nombre fini d'ensembles U_α ; sa borne supérieure c est égale à b car, sinon, un U_β qui contient c permettrait de le dépasser. Par dualité on en déduit que, de toute famille (F_α) de fermés de I d'intersection vide, on peut extraire une sous-famille finie d'intersection vide ; cela donne aussitôt le principe des *intervalles emboîtés*, et le fait que toute suite bornée $(a_1,\ldots,a_n,\ldots)$ admet une valeur d'adhérence (considérer les ensembles $A_n = \{a_n, a_{n+1}, \ldots\}$, leurs adhérences $\overline{A}_n$ et un point de l'intersection, non vide, des $\overline{A}_n$). Comme il est facile de voir qu'une valeur d'adhérence d'une *suite de Cauchy* est sa limite, et qu'une telle suite est bornée, le fait que **R** est complet s'ensuit aussitôt. La caractérisation des parties compactes de **R** comme fermés bornés vient du fait général que les parties compactes d'un espace compact ne sont autres que ses fermés.

2) *Connexion.* La seule chose délicate à montrer est que tout intervalle fermé $I = [a,b]$ est connexe (les intervalles des autres types sont réunions croissantes d'intervalles fermés). Pour cela, on suppose qu'on a une partition $I = A \cup B$, $A \cap B = \phi$, de I en deux ouverts A, B, et que $a \in A$. On considère l'ensemble E des $x \in I$ tels que $[a,x] \subset A$ et sa borne supérieure c ; en regardant un peu à gauche de c, on voit que $c \in B$ est impossible car $A \cap B = \phi$; donc $c \in A$; si $c < b$, E dépasse un peu c vers la droite, impossible ; donc $c = b$, $E = I = A$, $B = \phi$. Les conséquences habituelles (par exemple le théorème des valeurs intermédiaires) s'ensuivent classiquement.