bulletin de l'association des

professeurs de mathématiques

de l'enseignement public

"de la Maternelle aux Facultés"

Connecteurs logiques • Des cours d'arithmétique • La continuité • Expérience en Quatrième • RAPPORT DE LA COMMISSION MINISTÉRIELLE • Programmes pour les classes élémentaires • Vive Euclide ! • Les collègues écrivent • L'Assemblée générale

bimestriel - 46e année - mai-septembre 1967

n° 258

Sur l'organisation d'un cours d'arithmétique

Pierre Samuel,

Faculté des Sciences, Paris,

Malgré la prétendue difficulté de ce sujet, il est très fructueux d'enseigner de l'Arithmétique à de grands élèves scientifiques de l'enseignement secondaire. Par exemple, en France, les programmes de la classe « Terminale C » (correspondant à l'ancienne « Mathématiques Elémentaires ») en comportent. L'intérêt de l'Arithmétique est d'autant plus grand qu'elle permet d'illustrer, par des exemples nombreux et concrets, les notions d'Algèbre dite « moderne » (groupes, anneaux, corps, homomorphismes) qui prennent progressivement leur place dans les programmes de l'enseignement secondaire.

Les programmes français comprennent, très raisonnablement, les trois blocs suivants :

(*a*) Congruences, anneaux $\mathbb{Z}/n\mathbb{Z}$;

(*b*) L'unique décomposition des entiers en facteurs premiers ;

(*c*) L'étude des diviseurs (resp. multiples) communs à deux ou plusieurs nombres, et du p.g.c.d. (resp. p.p.c.m.).

Le but de cet article est de montrer qu'on peut mettre ces trois blocs dans un ordre à peu près arbitraire. Cependant, quelques définitions et faits préliminaires, sont nécessaires.

1. *Préliminaires.*

On utilise les notations classiques $\mathbb{N}$ pour l'ensemble des entiers naturels et $\mathbb{Z}$ pour l'anneau des entiers relatifs. On commence par définir la relation de divisibilité dans $\mathbb{Z}$; on introduit les mots « divise », « diviseur », « multiple », et la très commode notation $x|y$. On remarque que la restriction à $\mathbb{N}$ de la relation $x|y$ est une relation d'*ordre*. On définit enfin un nombre premier comme un nombre $p > 1$ dont les seuls diviseurs (dans $\mathbb{N}$) sont p et 1. On notera qu'il y a grand intérêt à entendre la relation de divisibilité au sens large (ainsi x divise x), et qu'il n'est pas recommandé de considérer 1 comme un nombre premier.

A propos des ensembles finis, on aura mis en évidence l'importante propriété suivante : toute application injective (resp. surjective) d'un ensemble *fini* dans lui-même est *bijective*. On pourra dire aux élèves que cette propriété caractérise les ensembles finis, et leur montrer une application injective (resp. surjective) f de $\mathbb{N}$ dans lui-même qui n'est pas bijective ; par exemple :

$$f(n) = 2n \text{ (resp. } f(n) = n - 1 \text{ pour } n \geqslant 1 \text{ et } f(0) = 0).$$

Enfin, étant donnés un groupe G (commutatif pour simplifier, et noté additivement) et un sous-groupe H de G, on aura montré que la relation $x - y \in H$ est une relation d'équivalence dans G (bien entendu des exemples seront les bienvenus ici, les congruences si l'on veut). La classe de x est l'ensemble traditionnellement noté $x + H$, et est en correspondance biunivoque avec H. Avec la notation card(E) pour le nombre d'éléments d'un ensemble fini E, on en déduit aussitôt :

Théorème. — *Si* G *est un groupe commutatif fini et si* H *est un sous-groupe de* G, *alors* card(H) *divise* card(G).

Bien entendu, l'hypothèse de commutativité est inutile.

2. *L'ordre* (a), (b), (c).

1) Soit $n \geqslant 1$ un entier naturel. Les multiples de n forment un sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$. La relation d'équivalence $x - y \in n\mathbb{Z}$ dans $\mathbb{Z}$ est appelée la relation de *congruence* modulo n et est notée $x \equiv y$ (mod. n). On définit, sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ de ces classes d'équivalence, une structure de groupe additif, puis une structure *d'anneau* déduites de celles de $\mathbb{Z}$. Tout ceci est bien classique.

On démontre alors le théorème de la *division euclidienne* (« tout entier $x \in \mathbb{Z}$ s'écrit, d'une façon et d'une seule, sous la forme $x = bn + r$ avec $b, r \in \mathbb{Z}$ et $0 \leqslant r \leqslant n - 1$ »). On en déduit aussitôt que $\mathbb{Z}/n\mathbb{Z}$ *a exactement* n *éléments*, à savoir les classes de $0, 1, \ldots, n - 1$. On illustre ici le cours par des exercices de calculs modulo de petits entiers n, et par l'établissement des tables d'addition et de multiplication de $\mathbb{Z}/n\mathbb{Z}$ correspondantes. La recherche d'inverses dans ces tables de multiplication amène très naturellement au théorème suivant :

Théorème. — *Soit* p *un entier* $\geqslant 2$. *Alors* « p *premier* » *équivaut à* « $\mathbb{Z}/p\mathbb{Z}$ *est un corps* ».

Esquisse de démonstration : Si p n'est pas premier, on écrit $p = ab$ avec $a, b > 1$, et la classe de a dans $\mathbb{Z}/p\mathbb{Z}$ n'est pas inversible. Si p est premier, on considère un élément non nul x de $\mathbb{Z}/p\mathbb{Z}$, et le sous-groupe additif H formé de $x, 2x, 3x, \ldots$; comme card(H) divise card($\mathbb{Z}/p\mathbb{Z}$) $= p$ (par 1), on en déduit que card(H) $= p$, donc $H = \mathbb{Z}/p\mathbb{Z}$; ainsi x est inversible et $\mathbb{Z}/p\mathbb{Z}$ est un corps. Enfin, la traduction de « un corps n'a pas de diviseurs

de zéro » donne le bien classique corollaire : si un nombre premier p divise un produit ab, il divise l'un des facteurs a ou b.

2) Le corollaire précédent montre que nous avons maintenant en main tous les ingrédients nécessaires pour démontrer, de façon très classique, l'unique décomposition des entiers en facteurs premiers. Il serait donc presqu'inutile de développer, s'il ne fallait pas mettre en garde les professeurs contre d'inutiles et traditionnelles dichotomies.

On commencera par établir *l'existence* de la décomposition en facteurs premiers :

Proposition 1. — *Tout nombre* $a > 1$ *admet un diviseur premier.*

En effet, l'ensemble des diviseurs $n > 1$ de a n'est pas vide (il contient a). Donc, il contient un plus petit élément p, et on voit que p est premier. Il n'y a pas besoin de séparer les cas « a premier », « a non-premier ».

Proposition 2. — *Tout nombre* $a > 1$ *est produit de nombres premiers.*

On procède par récurrence en supposant l'assertion vraie pour tout entier b tel que $1 < b < a$. Dans cette forme du raisonnement par récurrence, il n'est pas logiquement nécessaire de « commencer la récurrence » ; mais, comme il y a de la « logique de l'ensemble vide » là-dessous, le professeur préférera peut-être épargner cette subtilité à ses élèves ; alors, la vérification du cas $a = 2$ n'est pas fatigante ! Ceci étant, la proposition 1 montre qu'on peut écrire $a = bp$ avec p premier et $b < a$; si $b > 1$, on applique l'hypothèse de récurrence.

N. B. — Il faut ici faire comprendre aux élèves qu'on admet des produits d'*un* facteur. Ceci compris, il faudra introduire la convention qu'un produit de *zéro* facteurs est le nombre 1.

Vient alors le joli complément que l'ensemble P des nombres premiers est infini : classiquement, on prend n nombres premiers distincts $p_1, \ldots, p_n$ et on forme le nombre $1 + p_1 p_2 \ldots p_n$; par la proposition 1, il admet un diviseur premier q (pas besoin de séparer les cas !) ; on montre que q est distinct de $p_1, \ldots, p_n$.

L'unicité de la décomposition en facteurs premiers se démontre alors bien classiquement, au moyen du dernier corollaire du 1). Ici, il est souhaitable que les élèves aient atteint une capacité d'abstraction telle qu'il leur soit possible d'utiliser la très commode notation

$$(1) \qquad x = \prod_{p \in P} p^{v_p(x)}$$

pour la décomposition de x en facteurs premiers ; dans celle-ci P désigne l'ensemble des nombres premiers, et les exposants $v_p(x)$ sont des entiers naturels, tous nuls à l'exception d'un nombre fini.

3) L'application aux diviseurs et aux multiples a alors la même armature logique (sinon les mêmes notations) que dans la classe française de Quatrième (où l'on admet l'unicité de la décomposition en facteurs premiers). Avec la notation de (1), on a :

$$v_p(xy) = v_p(x) + v_p(y) \qquad \text{pour tout } p \in P.$$

De plus, la condition de divisibilité $x|y$ s'écrit : $v_p(x) \leqslant v_p(y)$ pour tout $p \in$ P. On en déduit aussitôt l'existence du pgcd d et du ppcm m de a et b, avec :

(2) $\qquad v_p(d) = \inf(v_p(a), v_p(b)) \qquad v_p(m) = \sup(v_p(a), v_p(b))$.

Des propriétés très faciles des inf et des sup donnent sans peine l'associativité du pgcd et du ppcm, la formule pgcd $(ab, ac) = a$ pgcd (b, c), et (si l'on veut) la distributivité du pgcd par rapport au ppcm et inversement. Arrivés à ce point, on peut utiliser la méthode classique, ou des considérations sur les inf, pour démontrer le fameux « lemme d'Euclide » : si ***a* divise *bc* et est premier à *b***, il divise c (ce résultat est parfois improprement appelé « lemme de Gauss », mais il est explicitement dans les Eléments d'Euclide ; d'ailleurs, s'il avait fallu attendre Gauss pour connaître un résultat aussi fondamental, on se demanderait comment des arithméticiens comme Euclide, Diophante, Fermat ou Euler auraient pu travailler). De même, pour les autres résultats classiques sur les nombres premiers entre eux, s'ils sont de nature purement multiplicative.

Reste l'importante *identité de Bezout* *. Celle-ci n'est pas une conséquence formelle de l'unique décomposition en facteurs premiers ; en effet, l'analogue de cette unique décomposition est vrai dans tous les anneaux qu'on appelle factoriels, en particulier dans l'anneau des polynômes à plusieurs variables sur un corps ; mais l'identité de Bezout n'est pas vraie dans cet anneau, qui n'est pas un anneau principal. On doit donc utiliser des propriétés plus précises de $\mathbb{Z}$. L'énoncé suivant fait bien le lien avec les congruences :

Théorème. — Soient a, b deux entiers $\geqslant 1$. *Les assertions suivantes sont équivalentes :*

a) *a et b sont premiers entre eux ;*

b) *la classe* $\bar{b}$ *de b est inversible dans* $\mathbb{Z}/a\mathbb{Z}$;

c) *il existe* $u, v \in \mathbb{Z}$ *tels que* $au + bv = 1$.

Esquisse de démonstration. On raisonne « en cercle » :

$$\text{a)} \implies \text{b)} \implies \text{c)} \implies \text{a)}.$$

Supposons a) ; la relation $\bar{b}\bar{x} = 0$ dans $\mathbb{Z}/a\mathbb{Z}$ veut dire $a|bx$, d'où $a|x$ par Euclide, et $\bar{x} = 0$; on en déduit, par différence, que, dans $\mathbb{Z}/a\mathbb{Z}$, la multiplication par $\bar{b}$ est injective ; elle est donc bijective (cf. 1), d'où l'inversibilité de $\bar{b}$. Si b) est vraie, il existe $v \in \mathbb{Z}$ tel que $bv \equiv 1$ (mod. a), et ceci équivaut à c). Enfin c) $\implies$ a) est immédiat.

3. *L'ordre* (b), (c), (a).

1) On commence par l'existence de la décomposition en facteurs premiers comme dans le 2) du § 2. Pour *l'unicité,* on peut utiliser l'ingénieuse démonstration suivante, due à E. Zermelo :

* Encore dite de Bachet (*N.D.L.R.*).

On montre, par récurrence sur n, que la décomposition de n en facteurs premiers est unique. Facile (mais inutile) départ pour $n = 1$ ou 2. On suppose l'unicité vraie pour tout entier naturel $n' < n$. Considérons deux décompositions de n en facteurs premiers.

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t,$$

et supposons-les distinctes. Alors, chacun des p_i est distinct de chacun des q_j : sinon l'on diviserait par ce facteur premier commun p_k et on obtiendrait deux décompositions distinctes du nombre n/p_k, contrairement à l'hypothèse de récurrence. On a donc, par exemple, $p_1 < q_1$; écrivons $n = p_1 p' = q_1 q'$ avec $p' = p_2 \dots p_s$ et $q' = q_2 \dots q_t$; alors $q' < p'$. Considérons le nombre $n' = (q_1 - p_1)q' = p_1(p' - q')$. On a $n' < n$, de sorte que la décomposition en facteurs premiers de n' est unique. Or, comme $n' = p_1(p' - q')$, p_1 figure dans cette décomposition ; écrivons alors $n' = (q_1 - p_1)q'$; comme p_1 est distinct de tous les facteurs premiers q_j de la décomposition $q' = q_2 \dots q_t$, et que celle-ci est unique par l'hypothèse de récurrence, p_1 doit figurer dans la décomposition (unique encore) de $q_1 - p_1$. Mais alors p_1 divise $q_1 - p_1$, donc aussi q_1. Contradiction. CQFD.

2) L'étude purement multiplicative des diviseurs et multiples peut alors procéder comme dans le 3) du § 2. Pour l'identité de Bezout, il semble préférable d'avoir la théorie des congruences.

3) Jusqu'au théorème disant que $\mathbb{Z}/p\mathbb{Z}$ est un corps, lorsque p est premier (exclu), on procède comme dans le 1) du § 2. Mais il n'est pas avantageux de démontrer directement ce théorème ; en effet, on en sait suffisamment pour démontrer un théorème plus fort, à savoir le dernier théorème du § 2 relatif à l'identité de Bezout. Alors l'énoncé relatif à $\mathbb{Z}/p\mathbb{Z}$ (p premier) vient en corollaire : en effet, un élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est la classe d'un entier premier à p, et est donc inversible dans $\mathbb{Z}/p\mathbb{Z}$ d'après l'assertion b) du théorème.

4. *L'ordre classique (c), (b), (a).*

1) L'exemple de l'ensemble $n\mathbb{Z}$ des multiples de n introduit la notion d'*idéal* de $\mathbb{Z}$ (et, plus généralement, d'un anneau commutatif quelconque). La division euclidienne permet alors de montrer le :

Théorème : tout idéal I *de* $\mathbb{Z}$ *est « principal », c'est-à-dire de la forme* $n\mathbb{Z}$.

C'est clair si I est réduit à 0. Sinon, I contient des éléments > 0, donc un plus petit élément > 0, soit n. Par division euclidienne de $x \in \mathrm{I}$ par n, soit $x = nq + r$ avec $0 \leqslant r \leqslant n - 1$, on voit que $r \in \mathrm{I}$, donc $r = 0$; ainsi $x \in n\mathbb{Z}$, et $\mathrm{I} = n\mathbb{Z}$. CQFD.

L'existence du *ppcm* de deux entiers a et b est alors immédiate : en effet, $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc est de la forme $m\mathbb{Z}$. Pour le *pgcd*, on peut le déduire du *ppcm*, en vérifiant que l'entier $d = ab/ppcm(a, b)$, d'une part, divise a et b, d'autre part, est multiple de tout diviseur commun à a et

b. Mais il est plus fructueux et plus classique de noter que tout diviseur commun à a et b divise tous les éléments de l'idéal $a\mathbb{Z} + b\mathbb{Z}$ (ensemble des sommes $ua + vb$, où u et v parcourent $\mathbb{Z}$) ; or, cet idéal est de la forme $d\mathbb{Z}$; comme $a\mathbb{Z} \subset d\mathbb{Z}$, on voit que d divise a, et de même d divise b.

Ainsi, d a les propriétés classiques du *pgcd* ; de plus, il s'écrit :

$$(3) \qquad d = ua + vb \quad (u, v \in \mathbb{Z}).$$

N. B. — Il sera bon de dire que les mots « plus grand » et « plus petit » (dans « plus grand commun diviseur » et « plus petit commun multiple ») ne se rapportent qu'incidemment à la relation d'ordre usuelle de $\mathbb{N}$, mais se rapportent de façon essentielle à la relation d'ordre de la *divisibilité* sur $\mathbb{N}$. D'ailleurs, la théorie décrite ici s'applique à n'importe quel anneau principal A, et un tel anneau n'admet en général pas d'ordre analogue à l'ordre usuel de $\mathbb{Z}$.

On démontre alors, à la manière classique, les formules du type $pgcd(ab, ac) = a\, pgcd(b, c)$, le lemme d'Euclide, et les propriétés des entiers premiers entre eux. Un professeur soucieux de pureté s'efforcera de ne pas utiliser l'identité de Bezout dans des questions uniquement multiplicatives (comme le lemme d'Euclide), car il s'agit là de propriétés valables dans tout anneau factoriel, et pas seulement dans tout anneau principal.

On termine la partie (*c*) par l'*identité de Bezout*, qui affirme ici l'équivalence de :

a) a et b *sont premiers entre eux* ; c) il existe $u, v \in \mathbb{Z}$ *tels que* $au + bv = 1$. La démonstration résulte aussitôt de la formule (3).

2) On passe à l'étude des nombres *premiers*. Pour l'existence de la décomposition en facteurs premiers, on procède comme dans le 2) du § 2. Pour l'unicité on démontre le lemme « si p est premier et s'il divise ab, alors il divise a ou b », qui est une conséquence facile du lemme d'Euclide ; l'unicité en résulte de façon classique. On introduit la notation (cf. 2, du § 2) :

$$x = \prod_{p \in P} p^{v_p(x)}$$

où P désigne l'ensemble des nombres premiers, et où les exposants $v_p(x)$ sont nuls à l'exception d'un nombre fini. Comme dans le 3) du § 2, on donne la formule $v_p(xy) = v_p(x) + v_p(y)$, la condition de divisibilité « $v_p(x) \leqslant v_p(y)$ pour tout $p \in P$ », et les formules $v_p(pgcd(x, y)) = \inf(v_p(x), v_p(y))$ et $v_p(ppcm(x, y)) = \sup(v_p(x), v_p(y))$.

3) Pour la théorie des congruences on procède comme dans le 1) du § 2 jusqu'au théorème disant que $\mathbb{Z}/p\,\mathbb{Z}$ est un corps lorsque p est premier (exclu). Comme dans le 3) du § 3, on passe au théorème sur l'identité de Bezout (dernier théorème du § 2) ; ici la démonstration est quasiment faite car, dans le 1), on a démontré l'équivalence des assertions a) et c) ; reste l'assertion b) (« la classe $\bar{b}$ de b est inversible dans $\mathbb{Z}/a\,\mathbb{Z}$ »), mais ce n'est qu'une traduction de b). On donne en corollaire l'énoncé relatif à $\mathbb{Z}/p\,\mathbb{Z}$ pour p premier (cf. le 3, du § 3).

5. *Autres ordres. Mérites respectifs de ces ordres.*

La théorie des permutations nous dit qu'il y a $3\,! = 6$ ordres possibles des trois blocs (*a*), (*b*), (*c*). Nous en avons déjà examiné trois. Il me paraît pédagogiquement peu indiqué de séparer les blocs (*b*) (nombres premiers) et (*c*) (divisibilité) ; ceci exclut donc les ordres (*b*), (*a*), (*c*) et (*c*), (*a*), (*b*). Reste l'ordre (*a*), (*c*), (*b*) : il consiste à démarrer sur la partie élémentaire des congruences (c'est-à-dire la définition de $\mathbb{Z}/n\,\mathbb{Z}$ et de sa structure d'anneau), puis à suivre l'ordre indiqué dans les 1) et 2) du § 4 ; à la fin de ce 2) on peut donner l'énoncé complet concernant l'identité de Bezout (y compris la caractérisation des éléments inversibles de $\mathbb{Z}/a\,\mathbb{Z}$; quant à l'énoncé relatif à $\mathbb{Z}/p\,\mathbb{Z}$ pour p premier, il vient à la fin du 3). Ainsi l'ordre (*a*), (*c*), (*b*) ressemble assez à l'ordre (*c*), (*b*), (*a*) du § 4 ; mais il a le désavantage que des considérations sur les congruences viennent interrompre des propriétés uniquement multiplicatives.

Restent ainsi à comparer les ordres (*a*), (*b*), (*c*) décrits dans le § 2 (*b*), (*c*), (*a*) du § 3, et (*c*), (*b*), (*a*), du § 4. Le premier a l'avantage de l'économie ; aucune démonstration n'y est difficile ; la connaissance préalable de l'unique décomposition en facteurs premiers permet de donner un exposé à la fois très simple et complet de la théorie du *pgcd* et du *ppcm* (on obtient à la fois l'existence du *pgcd* ou du *ppcm*, et le moyen de le calculer à partir de décompositions en facteurs premiers). Le désavantage de cet ordre est que le théorème « $\mathbb{Z}/p\,\mathbb{Z}$ est un corps lorsque p est premier » y reçoit une démonstration *ad hoc*, particulière à $\mathbb{Z}$; il n'est donc pas généralisable à d'autres anneaux principaux.

L'ordre (*b*), (*c*), (*a*), du § 3 a encore l'avantage dû au fait que l'unique décomposition en facteurs premiers vient avant la théorie du *pgcd* et du *ppcm*. Mais il a le désavantage que la démonstration d'unicité de E. Zermelo est un peu trop ingénieuse, et risque de passer par-dessus la tête de la plupart des élèves. Comme l'ordre du § 2, il a aussi le désavantage de ne pas se prêter à la généralisation aux autres anneaux principaux.

Enfin, l'ordre (*c*), (*b*), (*a*), du § 4 a le grand avantage d'introduire l'importante notion d'idéal, et de se prêter à la généralisation aux anneaux principaux ; on peut, en compléments ou en exercices, étudier la divisibilité dans d'autres anneaux principaux, par exemple, l'anneau des polynômes à une variable sur un corps, l'anneau des nombres $a + b\sqrt{2}$ ($a, b \in \mathbb{Z}$), ou l'anneau des « entiers de Gauss » $a + bi$ ($a, b \in \mathbb{Z}$, $i^2 = -1$) ; ce dernier est particulièrement intéressant, car il permet d'étudier très élégamment la représentation des entiers comme sommes de deux carrés. Un professeur soucieux de pureté pourra même utiliser la variante esquissée dans le § 4 : du fait que $\mathbb{Z}$ est un anneau principal, il ne retiendra d'abord que l'énoncé « l'intersection $a\mathbb{Z} \cap b\,\mathbb{Z}$ de deux idéaux principaux est un idéal principal $m\mathbb{Z}$ » ; il aura ainsi le *ppcm*, en déduira le *pgcd*, puis l'unique décomposition en facteurs premiers ; cette variante a l'avantage d'être immédiatement généralisable, non seulement aux anneaux principaux, mais à tous les anneaux factoriels ; en effet, jointe à l'existence d'une décomposition en facteurs « irréductibles », la principalité des intersections de deux idéaux principaux caractérise les anneaux factoriels. Mais les désavantages de cet ordre sont qu'il est nettement moins économique que celui du § 2, que certaines démonstrations dans la théorie (*c*) du *pgcd* et du *ppcm* y sont un peu subtiles (encore plus subtiles si on utilise la variante ci-dessus), que l'existence du *pgcd* et du *ppcm* y est séparée de leur calcul à partir de décompositions en facteurs premiers, et qu'enfin la finitude des anneaux $\mathbb{Z}/n\mathbb{Z}$ n'y est pas utilisée (ce qui prive les élèves d'occasions de mieux comprendre les propriétés des ensembles finis).

Que peut-on maintenant conclure de cette discussion ? L'ordre du § 3, avec la démonstration de E. Zermelo, paraît un peu inférieur aux deux autres. Quant à ceux-ci, la simplicité du premier me paraît équilibrer la généralité du dernier ; le choix entre eux dépendra donc des préférences du professeur, de son tempérament, du niveau et de l'état d'esprit de ses élèves.

P. S.

Rotations normales, déplacements et orientations d'un plan métrique

Claude FRASNAY,

Faculté des Sciences de Toulouse.

Sommaire. — Dans une structure G-métrique plane (au sens de G. Choquet), le fait qu'une symétrie ne soit pas un déplacement constitue un théorème essentiel, qui ne résulte pas trivialement des axiomes de cette structure. Pour démontrer ce théorème, on peut effectuer au préalable une bipartition de l'ensemble des rotations normales. Une telle bipartition montre d'ailleurs immédiatement l'existence d'une double orientation du plan.

1. *Définition d'une G-métrique plane.*

1.1. Etant donné un groupe totalement ordonné G, une *G-métrique* sur un ensemble E est définie par une application d de $E \times E$ dans G vérifiant les trois conditions : $d(M, N) = 0 \iff M = N$, $d(M, N) = d(N, M)$, $d(M, N) \leqslant d(M, P) + d(P, N)$.

a) La notion d'*isométrie* entre deux espaces G-métriques D, F est évidente, et le cas F = G (muni de la distance $d(x, y) = |x - y|$) permet d'introduire les *G-droites* D (supportant chacune deux droites ordonnées opposées) ainsi que les *segments* [M, N] de ces droites.

b) L'espace G-métrique E est *réglé* s'il contient, avec deux points distincts quelconques, une droite et une seule passant par ces points. On dit que E est *pliable* autour d'un sous-espace F s'il existe une partition (F, F_1, F_2) de E et une isométrie σ de $F \cup F_1$ sur $F \cup F_2$ vérifiant les deux conditions :

$$\begin{cases} M \in F \implies \sigma(M) = M, \\ M_1 \in F_1 \text{ et } M_2 \in F_2 \implies F \text{ rencontre } [M_1, M_2]. \end{cases}$$

L'axiomatique de la géométrie plane prend alors une forme condensée :

DÉFINITION. — Un *G-plan* est un espace G-métrique réglé pliable autour de chacune de ses droites.