II. L'ordre (a), (b), (c)

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 N dans lui-même qui n'est pas bijective; par exemple $f(n) = 2n$ (resp. $f(n) = n - 1$ pour $n \geqslant 1$ 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.

II. L'ORDRE (a), (b), (c)

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

On démontre alors le théorème de la *division euclidienne* (« tout entier $x \in Z$ s'écrit, d'une façon et d'une seule, sous la forme $x = bn + r$ avec $b, r \in Z$ et $0 \leqslant r \leqslant n - 1$ »). On en déduit aussitôt que Z/nZ *a exactement* n *éléments*, à savoir les classes de 0, 1, ..., $n - 1$. 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 Z/nZ 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* « Z/pZ *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 Z/pZ n'est pas inversible. Si p est

premier, on considère un élément non nul x de Z/pZ, et le sous-groupe additif H formé de $x, 2x, 3x, \ldots$; comme card (H) divise card $(Z/pZ) = p$ (§ I), on en déduit que card $(H) = p$, donc $H = Z/pZ$; ainsi x est inversible et Z/pZ 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 mains tous les ingrédients nécessaires pour démontrer, de façon très classique, l'unique décomposition des entiers en facteurs premiers. Il serait donc presque 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 prop. 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 prop. 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

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

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

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

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

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

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 Z. L'énoncé suivant fait bien le lien avec les congruences:

THÉOREME. *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* $\mathbf{Z}/a\mathbf{Z}$;
c) *il existe* $u, v \in \mathbf{Z}$ *tels que* $au + bv = 1$.

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

III. L'ORDRE (b), (c), (a)

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

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. C.Q.F.D.