CAHIERS DU SÉMINAIRE D'HISTOIRE DES MATHÉMATIQUES

JEAN-PIERRE SOUBLIN

Préhistoire des idéaux

Cahiers du séminaire d'histoire des mathématiques 1re série, tome 5 (1984), p. 13-20

<http://www.numdam.org/item?id=CSHM_1984__5__13_0>

PRÉHISTOIRE DES IDÉAUX

PAR JEAN-PIERRE SOUBLIN*

A l'origine de la notion ensembliste d'*idéal* se trouvent les *nombres idéaux* de Ernst Eduard Kummer (1810-1893)[1]. On peut s'amuser à dater leur naissance[2] au 18 octobre 1845, jour où Kummer écrivit à son élève et ami Kronecker une lettre contenant sa définition et l'annonce des principales propriétés de ces nombres idéaux[3]. Nous allons construire ces nombres en suivant l'ordre dans lequel Kummer les a découverts.

Soit p un nombre premier impair, et α un nombre complexe $\neq 1$ tel que $\alpha^p = 1$. Kummer définit $Z[\alpha]$, sans employer cette notation bien sûr, ni le mot anneau, ni aucun concept ensembliste. Les *nombres complexes composés de l'unité et d'une racine $p^{ième}$ de l'unité*, ou plus simplement les *nombres complexes*, i.e. les éléments de $Z[\alpha]$, sont toujours écrits sous la forme polynomiale $\varphi(\alpha)$, avec $\varphi \in Z[X]$, encore que la variable X n'apparaisse jamais. Assez souvent φ est de degré $\leqslant p-2$, auquel cas φ est uniquement déterminé par $\varphi(\alpha)$, et nous dirons que le nombre complexe est écrit sous forme canonique :

$$\varphi(\alpha) = a_0 + a_1\alpha + \ldots + a_{p-2}\alpha^{p-2} \quad (a_i \in Z).$$

Kummer définit les *conjugués* de $\varphi(\alpha)$ comme étant les $\varphi(\alpha^k)$, $1 \leqslant k \leqslant p-1$, nombres qui ne sont donc plus écrits en général sous forme canonique, car le degré de $\varphi(X^k)$ peut excéder $p-2$. Leur produit est la *norme*, notée $N(\varphi(\alpha))$. Il invoque Lejeune-Dirichlet pour la propriété $N(\varphi(\alpha)) \in N$.

Si $\varphi(\alpha)$ est sous forme canonique

$$a_0 + \ldots + a_{p-2}\,\alpha^{p-2} ,$$

il note $\varphi(1)$ la somme

$$a_0 + \ldots + a_{p-2} \in Z .$$

Un calcul élémentaire montre à Kummer que, si $\varphi(\alpha)$, $g(\alpha)$ et $h(\alpha)$ sont sous forme canonique, on a l'implication

$$\varphi(\alpha)\, g(\alpha) = h(\alpha) \;\Rightarrow\; \varphi(1)\, g(1) \equiv h(1) \quad (\text{mod.} p) ;$$

et de même, pour $1 \leqslant k \leqslant p-1$,

$$g(\alpha) = \varphi(\alpha^k) \;\Rightarrow\; g(1) \equiv \varphi(1) \quad (\text{mod.} p).$$

---

* Conférence donnée le 9 mars 1983 au Séminaire d'Histoire des Mathématiques.

Il en déduit la congruence

$$N(\delta(\alpha)) \equiv (\delta(1))^{p-1} \quad (\text{mod.}p).$$

Compte-tenu du petit théorème de Fermat, il y a donc deux cas possibles : ou bien

$$N(\delta(\alpha)) \equiv 0 \quad (\text{mod.}p),$$

ou bien

$$N(\delta(\alpha)) \equiv 1 \quad (\text{mod.}p).$$

Kummer cherche ensuite les *nombres complexes premiers*, c'est-à-dire les éléments $\delta(\alpha)$ de $Z[\alpha]$ dont la norme $N(\delta(\alpha))$ est un nombre premier q. Ainsi, ou bien $q = p$, ou bien $q \equiv 1 \quad (\text{mod.}p)$. Le cas $q = p$ est facile : on trouve le nombre complexe $1 - \alpha$, ses conjugués $1 - \alpha^k$ et les nombres associés à ces conjugués $\varepsilon(\alpha)(1 - \alpha^k)$, où $\varepsilon(\alpha)$ est une *unité* de $Z[\alpha]$.

Examinons alors ce qu'on peut dire des nombres complexes

$$\delta(\alpha) = a_0 + a_1\alpha + \ldots + a_{p-2}\alpha^{p-2}$$

dont la norme $N(\delta(\alpha))$ est un nombre premier $q \equiv 1 \quad (\text{mod.}p)$. Comme p divise alors l'ordre $q-1$ du groupe cyclique F_q^*, on peut trouver p racines $p^{\text{ièmes}}$ de l'unité dans F_q : $1, u_1, \ldots, u_{p-1}$. En fait Kummer ne parle jamais du corps F_q ; il prend les u_i dans Z et leur demandera de vérifier $u_i^p \equiv 1$ et $u_i \not\equiv u_j \quad (\text{mod.}q)$. Kummer montre alors que δ "annule modulo q" l'un de ces u_i, disons u_1 :

$$\delta(u_1) \equiv 0 \quad (\text{mod.}q)$$

[en effet un calcul "moderne" montre aisément que

$$N(\delta(\alpha)) = q \Rightarrow \delta(u_1)\delta(u_2)\ldots\delta(u_{p-1}) = 0$$

dans F_q]. Il renumérote alors les u_i en imposant

$$(u_k)^k \equiv u_1 \quad (\text{mod.}q).$$

On a alors

$$\delta_k(u_k) \equiv 0 \quad (\text{mod.}q),$$

où je note $\delta_k(\alpha)$ le nombre $\delta(\alpha^k)$. Mais Kummer exprime ainsi cette dernière congruence :

" $\delta(\alpha^k) \equiv 0 \quad (\text{mod.}q)$ pour $\alpha = u_k$ " !

Restons dans le cas que nous venons d'examiner :

$$N(\mathfrak{d}(\alpha)) = q \equiv 1 \pmod{p} .$$

Kummer se demande alors à quelle condition un nombre complexe

$$g(\alpha) = b_0 + b_1\alpha + \ldots + b_{p-2}\alpha^{p-2}$$

est-il divisible dans $Z[\alpha]$ par $\mathfrak{d}(\alpha)$, ou plus généralement par $\mathfrak{d}_k(\alpha)$? Il répond par le

Théorème : $\mathfrak{d}_k(\alpha)$ *divise* $g(\alpha)$ *dans* $Z[\alpha]$ *si et seulement si* q *divise* $g(u_k) = b_0 + b_1u_k + \ldots + b_{p-2}u_k^{p-2}$ *dans* Z .

C'est un exemple de ce qu'il recherche toujours : expliciter les divisibilités mystérieuses de $Z[\alpha]$ en termes de congruences dans Z , et surtout donner des propriétés opératoires. Il était donc bien éloigné des idées ensemblistes et non-constructives qui permettront à Dedekind de bâtir ses idéaux.

Soit toujours q un nombre premier congru à 1 selon le module p , mais qui n'est plus nécessairement la norme d'un élément de $Z[\alpha]$ .Il est clair que,si un nombre complexe $g(\alpha)$ est écrit sous forme canonique

$$g(\alpha) = b_0 + b_1\alpha + \ldots + b_{p-2}\alpha^{p-2} \text{ , on a l'équivalence}$$

$$q \text{ divise } g(\alpha) \text{ dans } Z[\alpha] \Leftrightarrow q \text{ divise } b_0, b_1, \ldots, b_{p-2} \text{ dans } Z.$$

Mais Kummer démontre aussi le résultat facile :

Proposition : q divise $g(\alpha)$ dans $Z[\alpha] \Leftrightarrow q$ divise $g(u_1), \ldots, g(u_{p-1})$ dans Z .

Ici $u_1, \ldots, u_{p-1}$ sont toujours des entiers appartenant à Z dont les classes sont les $p-1$ racines primitives $p^{\text{ièmes}}$ de l'unité dans F_q , numérotées de façon à ce que $u_k^k \equiv u_1 \pmod{q}$.

Lorsque q n'est la norme d'aucun nombre complexe, Kummer introduit la

Définition : Le nombre complexe $g(\alpha)$ sera dit *divisible par le nombre complexe idéal premier* $\mathfrak{d}(\alpha^k)$ si et seulement si q divise $g(u_k)$ dans Z .

Les nombres idéaux, en tant que tels, ne sont jamais définis ; seule la divisibilité par eux est définie. Par ailleurs le symbole $\mathfrak{d}(\alpha^k)$ est un tout, la lettre $\mathfrak{d}$ isolée n'ayant aucune signification.

Ainsi la proposition et la définition précédentes montrent que q divise $g(\alpha)$ si et seulement si $\mathfrak{d}_1(\alpha),\ldots,\mathfrak{d}_{p-1}(\alpha)$ divisent $g(\alpha)$, que les *nombres* $\mathfrak{d}_k(\alpha) = \mathfrak{d}(\alpha^k)$ soient des nombres "existants" (premier cas envisagé), ou "idéaux". Bien sûr, Kummer considère que le nombre idéal $\mathfrak{d}(\alpha^k) = \mathfrak{d}_k(\alpha)$ est le $k^{\text{ième}}$ *conjugué* du nombre idéal $\mathfrak{d}(\alpha)$, et que sa *norme* est q ; et ces conjugués sont pensés déjà comme les *facteurs premiers* de q.

Kummer va alors s'employer à définir les autres diviseurs premiers idéaux d'un nombre complexe existant quelconque $g(\alpha)$, diviseurs dont la norme ne sera plus supposée égale à un nombre premier congru à 1 selon le module p.

Soit donc q un nombre premier qui ne soit congru ni à 0 ni à 1 selon le module p. On note alors $\mathfrak{f}$ l'ordre de q dans le groupe F_p^* ; c'est un diviseur de l'ordre $p-1$ de ce groupe : $p-1 = e\mathfrak{f}$ [$\mathfrak{f}$ sera plutôt défini par Kummer comme étant le plus petit entier $\geqslant 1$ tel que $q^{\mathfrak{f}} \equiv 1 \pmod{p}$]. Kummer introduit alors tout un attirail malcommode ; à commencer par les *périodes de Gauss* $\eta = \eta_0, \eta_1, \ldots, \eta_{e-1}$ définies par

$$\eta_i = \alpha^{g^i} + \alpha^{g^{e+i}} + \alpha^{g^{2e+i}} + \ldots + \alpha^{g^{(\mathfrak{f}-1)e+i}},$$

où $g \in Z$ est un générateur quelconque, mais fixé, du groupe cyclique F_p^*. Les $p-1 = e\mathfrak{f}$ conjugués de η se répartissent en e paquets de $\mathfrak{f}$ conjugués chacun, les éléments d'un paquet étant égaux à un certain η_i. Ce que ne dit pas Kummer, faute des concepts *ad hoc* (notamment d'*entier algébrique*), c'est que les η_i forment une Z-base (normale donc) de l'anneau A des entiers de l'unique sous-corps $\mathbb{Q}(\eta) = \mathbb{Q}(\eta_i)$ de $\mathbb{Q}(\alpha)$ qui soit de degré e sur $\mathbb{Q}$. Il emploie une notation particulièrement scabreuse pour les éléments de cet anneau d'entiers A ; un tel élément est noté $\varphi(\eta)$; cela ne signifie pas que ce nombre est de la forme

$$a_0 + a_1\eta + \ldots + a_{e-1}\eta^{e-1}$$

avec les $a_i \in Z$ comme le pense Bourbaki dans la *Note Historique* de son *Algèbre Commutative* (Chapitre 7, page 116) ; non, cela signifie que ce nombre est de la forme

$$a_0 + a_1\eta_1 + \ldots + a_{e-1}\eta_{e-1},$$

avec les a_i dans Z. Sous cette forme canonique, les a_i sont parfaitement déterminés. Cette conception de l'écriture $\varphi(\eta)$ n'empêche pas Kummer de substituer à η certains autres nombres ! ce qui nécessite à chaque fois une explication. Par exemple $\varphi(\eta_i)$ désigne l'image de $\varphi(\eta)$ par l'un des automorphismes de $\mathbb{Q}(\alpha)$ qui envoye η en η_i.

Kummer prouve à grand hahan que :

(i) Le polynôme

$$F_{p,e} = (X-\eta_0)(X-\eta_1)\dots(X-\eta_{e-1})$$

appartient à $Z[X]$.

[Avec les concepts modernes cette propriété est facile ; dans le cas précédent $q \equiv 1 \pmod{p}$, où $f = 1$ et $e = p-1$, les η_i sont les α^i et $F_{p,p-1}$ est le polynôme cyclotomique Φ_p].

(ii) Ce polynôme se décompose complètement dans $F_q[X]$:

$$F_{p,e} = (X-u_0)\dots(X-u_{e-1}) .$$

[Contrairement à ce qu'affirme Bourbaki (ibid.), les u_i ne sont pas nécessairement distincts dans F_q ; bien sûr chez Kummer les u_i sont pris dans Z].

(iii) Comme dans le cas $q \equiv 1$, une fois choisi u_0 , Kummer numérote d'une certaine façon les autres u_i .

(iv) Si

$$\varphi(\eta) = a_0\eta_0 + \dots + a_{e-1}\eta_{e-1} \in A ,$$

Kummer introduit les entiers $\varphi(u_i) \in Z$ par

$$\varphi(u_i) = a_0 u_{\sigma_i(0)} + \dots + a_{e-1} u_{\sigma_i(e-1)} ,$$

où σ_i est une certaine permutation de $\{ 0, 1, \dots, e-1 \}$.

(v) Tout $g(\alpha) \in Z[\alpha]$ peut s'écrire, de façon unique, sous la forme

$$\varphi_0(\eta) + \alpha\varphi_1(\eta) + \dots + \alpha^{f-1}\varphi_{f-1}(\eta)$$

avec les $\varphi_j(\eta)$ dans A .

(vi) Avec les notations ci-dessus on a la double équivalence

q divise $g(\alpha)$ dans $Z[\alpha]$ $\Leftrightarrow$

(trivial)

q divise les $\varphi_j(\eta)$ dans A [ce qui correspond à chaque fois à e congruences] $\Leftrightarrow$

q divise les $\varphi_j(u_i)$ dans Z , $0 \leqslant j \leqslant f-1$, $0 \leqslant i \leqslant e-1$.

Et Kummer introduira de nouveaux nombres premiers idéaux par la

Définition. Soit $0 \leqslant i \leqslant e-1$. Le nombre complexe

$$g(\alpha) = \varphi_0(\eta) + \ldots + \alpha^{\delta-1}\varphi_{\delta-1}(\eta)$$

sera dit *divisible par le nombre complexe idéal premier* $\mathfrak{p}_i(\alpha) = \mathfrak{p}(\alpha^i)$ si et seulement si q divise les δ entiers $\varphi_j(u_i)$ dans Z $(0 \leqslant j \leqslant \delta-1)$.

Cette dernière condition est exprimée ainsi par Kummer : " $g(\alpha) \equiv 0 \pmod{q}$ pour $\eta = u_i$ " !

Désormais, Kummer dispose de sa panoplie de nombres premiers existants (= éléments de $Z[\alpha]$) et idéaux, indicés par les nombres premiers q , et, pour chaque q , par un indice variant de 0 à $e-1$ (ou plutôt $e(q)-1$). Il n'aura plus besoin d'autres nombres premiers idéaux.

L'un des buts poursuivis étant d'écrire chaque "nombre complexe" comme produit de facteurs irréductibles, idéaux ou non, il peut seulement, à ce stade, dire quels facteurs vont intervenir dans la décomposition, mais pas avec quelle *multiplicité*. Il semblerait que la définition de cette multiplicité soit due à une collaboration entre Kummer et son élève Kronecker, dont elle constituerait la Thèse de Doctorat.

Pour bien comprendre l'idée, d'ailleurs très simple, de Kronecker, on peut reprendre une image développée par Hensel, un autre élève de Kummer. Soit à définir une théorie satisfaisante des irréductibles dans le monoïde multiplicatif $\mathfrak{E}$ des entiers $\geqslant 1$ dont le nombre de facteurs premiers est pair. Dans ce monoïde, il n'y a pas unicité de la décomposition en facteurs irréductibles, car, par exemple,

$$210 = 6\times35 = 10\times21 = 14\times15 .$$

Il s'agit de chercher à définir des facteurs premiers "idéaux", dont l'ensemble $\mathfrak{J}$ rajouté aux éléments "existants" de $\mathfrak{E}$ fourniront un monoïde $\mathfrak{M} = \mathfrak{E} \cup \mathfrak{J}$ où il y aura unicité de la décomposition. Ici bien sûr on prendra $\mathfrak{M} = \mathbf{N}^*$, et on aura $210 = 2\times3\times5\times7$.

Soit par exemple à introduire le nombre "idéal" premier 2 . Ce n'est pas tant ce nombre 2 que Kummer, ou Hensel, va construire, que la relation

" le nombre existant e est divisible par le nombre idéal 2 ".

Et ceci de la façon suivante :

" le nombre existant e est divisible par 2 si et seulement si le nombre existant 15 e est divisible, dans $\mathfrak{E}$, par le nombre existant 6 ".

Ainsi, à supposer qu'on ait pu, par un procédé *ad hoc*, déceler la présence commune de 3 (et non de 2) dans 6 et 15 , et celle de 2 (et non de 4) dans

6 , la divisibilité par 2 revient à un pur problème interne au monoïde donnée $\mathfrak{E}$. Nous venons précisément de décrire un tel procédé, où l'on remplace $\mathfrak{E}$ par $Z[\alpha] \setminus \{ 0 \}$ et 2 par $\mathfrak{b}_i(\alpha)$.

Cette idée conduit aux facteurs multiples, car il est clair que,"pour tout entier $n \geqslant 1$, le nombre existant e est divisible par 2^n (dans $\mathfrak{M}$) si et seulement si $(15)^n e$ est divisible par 6^n dans $\mathfrak{E}$ ". Cette analogie (due à Hensel ?) fait comprendre la définition suivante de Kummer (due à Kronecker ?) :

Définition. Soit n un entier $\geqslant 1$. Le nombre idéal premier $\mathfrak{b}(\alpha)$ sera dit diviser n fois le nombre $g(\alpha) \in Z[\alpha]$ si et seulement si q^n divise $(\psi(\eta))^n g(\alpha)$ dans $Z[\alpha]$.

Dans cette définition, q et $\Psi(\eta)$ jouent les rôles de 6 et 15 dans l'analogie précédente, et sont définis ainsi :

- q est le nombre premier dont il a été question précédemment, et qui a servi à construire le nombre idéal $\mathfrak{b}(\alpha)$ (dont la norme sera q^6) ;
- Kummer construit *explicitement* (page 409 du tome 1 de ses Oeuvres) un $\psi(\eta)$ dans $A = Z[\eta_0, \ldots, \eta_{e-1}]$ tel que le produit $\psi(\eta)\psi(\eta_1)\ldots\psi(\eta_{e-1})$ (qui est la norme sur $\mathbb{Q}$ de cet élément de $\mathbb{Q}(\eta)$, donc dans Z) soit divisible (dans Z) par q mais non par q^2 , et tel que $\mathfrak{b}(\alpha)$ divise $\psi(\eta)$.
- Il pose alors $\Psi(\eta) = \psi(\eta_1)\ldots\psi(\eta_{e-1}) \in A \subset Z[\alpha]$. Ce nombre $\Psi(\eta)$ est donc construit pour que $\mathfrak{b}(\alpha)$ divise q mais non $\Psi(\eta)$, et que q divise $\mathfrak{b}(\alpha)\Psi(\eta)$.

La définition précédente de Kummer est du type calculatoire : il ne se contente pas de la divisibilité dans $Z[\alpha]$, qui risquerait de n'être pas opératoire, mais se ramène en dernière analyse à des congruences modulo q^n dans Z , congruences entièrement explicitables en fonction des seuls coefficients de $g(\alpha)$ écrit sous forme canonique. Bien sûr ces calculs deviennent vite énormes et on peut douter de l'avantage d'une telle attitude. Mais il semble bien que Kummer avait fait par lui-même une masse de calculs explicites et qu'il disposait d'une table de certains facteurs premiers idéaux. Il émet le voeu de voir créer une telle table pour $p < 1000$ et $q < 1000$!

Rien de tout cela n'est publié en 1845, mais Kummer, dans sa lettre à Kronecker du 18 octobre, en connaît déjà les résultats essentiels. Notamment :

Théorème 1 : Un nombre complexe donné ne possède qu'un nombre fini de diviseurs premiers idéaux ou existants.

Théorème 2 : Si deux nombres complexes ont les mêmes diviseurs avec les mêmes multiplicités, ils ne diffèrent que par une unité.

Théorème 3 : Dans $Z[\alpha]$, $h(\alpha)$ divise $g(\alpha)$ si et seulement si les diviseurs

de $h(\alpha)$ apparaissent dans $g(\alpha)$ avec une multiplicié au plus égale.

Puis, plus tard, Kummer, qui n'employera jamais le langage des idéaux de Dedekind, étudiera de façon très approfondie les *classes* de nombres idéaux, dont il saura calculer le nombre $h(p)$ pour $p < 100$!

NOTES DE LA RÉDACTION

1 Sur E.E. Kummer et son oeuvre on peut lire avec profit : K.-R. Biermann, *Kummer, Ernst Eduard*, p.521-524 du t.VII du *Dictionary of Scientific Biography*, New York (Scribner), 1973 ; H.M. Edwards, *Fermat's Last Theorem*, Berlin(Springer), 1977 ; W.J. et F. Ellison, *Théorie des nombres*, p.165-334 du t.I de l'*Abrégé d'histoire des mathématiques*, Paris(Hermann), 1978 (en particulier p.195-200).

Toutefois, la source principale pour étudier l'oeuvre de Kummer sont ses *Collected Papers*, édités en deux volumes par André Weil, Berlin(Springer), 1975. Particulierement précieux est le tome I qui contient l'*Introduction* (p.1-14) d'André Weil, *Nachruf für Ernst Eduard Kummer* (p.15-30) de E. Lampe, *Gedächtnisrede auf Ernst Eduard Kummer* (p.33-69) de K. Hensel et *Kummers Briefe an Leopold Kronecker* (p.76-102). On y trouve également la très belle lettre de Kronecker à son ami Kummer du 9 septembre 1881, dans laquelle Kronecker écrit (p.133) que leur amitié, vieille de 36 ans, "constitue une part essentielle de mon bonheur".

2 Les premiers éléments de la théorie de Kummer sont développés dans son mémoire *De numeris complexis, qui radicibus unitatis et numeris integris realibus constant* (Sur les nombres complexes qui sont formés avec les nombres entiers réels et les racines de l'unité), publié à Breslau (aujourd'hui Wroclaw) en 1844 et dans le *Journal de Mathématiques pures et appliquées* de J. Liouville, t.12(1847) (p.165-192 du t.I des *Collected Papers*).

La première synthèse de sa théorie, "qui puisse servir de base sûre" (t.I,p.364), a été publié par Kummer, en français, dans le *Journal* de Liouville, t.16(1851) : *Mémoire sur le théorie des nombres complexes composés de racines de l'unité et de nombres entiers* (p.363-484 du t.I des *Collected Papers*).

3 P.94-98 du t.I des *Collected Papers*.