Emmy Noether

Noether fut l'une des mathématiciennes les plus importantes et influentes du XIXe siècle, notamment connue pour ses contributions à l'algèbre et à la physique mathématique. Malgré son génie, elle fit face à de nombreux obstacles dans sa vie académique en raison du fait qu'elle était une femme, et dut travailler sans salaire pendant plusieurs années. Elle fit beaucoup pour façonner l'algèbre abstraite alors qu'elle était relativement sous-développée, y compris les théories de base des anneaux et des corps qui sont maintenant si bien connues des étudiants en mathématiques de premier cycle. Si l'on considère l'état dans lequel se trouvait l'algèbre abstraite à l'époque, la difficulté de cette tâche ne peut être surestimée. Les chercheurs dans d'autres domaines comme la dynamique des fluides, la physique mathématique ou la géométrie différentielle ont généralement des indices avec lesquels travailler, ou des analogies et des images simples sur lesquelles s'appuyer. Même avec quelque chose comme le groupe fondamental en topologie algébrique, il y a une idée géométrique simple à la base du concept abstrait : celle de compter le nombre de trous entourés par une boucle fermée. Ces indices ont tendance à disparaître lorsqu'on étudie l'algèbre abstraite pure, surtout pour le débutant.

Noether a posé les fondations d'une grande partie de la théorie des anneaux commutatifs, connue sous le nom d'algèbre commutative. C'est encore une branche fondamentale et importante de l'algèbre, et il faut connaître une quantité raisonnable d'algèbre commutative avant même de commencer à envisager d'étudier des problèmes en géométrie algébrique. Un anneau R en général est un ensemble muni d'une addition et d'une multiplication telles que R forme un groupe abélien pour l'addition (R contient un élément zéro et tout élément de l'anneau a un inverse additif qui peut lui être ajouté pour obtenir l'élément zéro). De plus, la multiplication est associative

$$(xy)z = x(yz),$$

et distributive sur l'addition

$$x(y+z) = xy + xz, \qquad (y+z)x = yx + zx,$$

pour tout $x, y, z \in R$. On peut également exiger que l'anneau ait un élément identité noté 1 et que $xy = yx$. Cette dernière exigence signifie que l'anneau est commutatif, et la première est également souvent supposée pour simplifier. Un homomorphisme d'anneaux est une application f envoyant un anneau A dans un autre anneau B telle que

$$f(x+y) = f(x) + f(y),$$

$$f(xy) = f(x)f(y),$$

$$f(1) = 1.$$

Le premier critère signifie que f est un homomorphisme de groupes abéliens. Comme vous pouvez vous y attendre, vous pouvez former un sous-ensemble d'un anneau qui est alors un sous-anneau si

Synthèse et traduction des pages 169 à 178 de l'article arXiv https://arxiv.org/pdf/1910.01730 (fichiers de 1910.01730v3_page-0169.jpg à 1910.01730v3_page-0178.jpg).

Transcription en LaTeX : Madame Denise Vella-Chemla.

le produit de la somme de deux éléments est également un élément de l'ensemble et si l'ensemble contient l'élément identité pour l'anneau original R. Une composition d'homomorphismes d'anneaux est également un homomorphisme d'anneaux.

Une autre définition de base dont on a besoin est celle d'idéal : ce sont des objets simples, mais ils ont été utilisés avec beaucoup d'effet par Noether. Un idéal r d'un anneau R est un sous-ensemble de l'anneau tel que r est un sous-groupe additif (c'est-à-dire qu'une combinaison linéaire d'éléments de r avec des coefficients pris dans R est encore dans r). On pourrait écrire (x, y) pour l'idéal engendré de cette manière par deux éléments de R. Un idéal est également défini de telle sorte que

$$R\tau \subseteq \tau.$$

Si $r \subset R$ est un idéal, alors le groupe quotient R/r hérite de la multiplication de R de telle sorte qu'il devient un anneau en soi, appelé l'anneau quotient. Il existe un homomorphisme d'anneaux surjectif ϕ de R vers R/r qui envoie un élément de R vers sa classe et l'anneau quotient avec l'homomorphisme quotient sont définis de manière unique modulo isomorphismes. C'est un fait important et utile que l'application ϕ^{-1} qui envoie les idéaux de R/r vers les idéaux de R qui contiennent r est une correspondance bijective et croissante. Comme exemple d'un fait qui utilise les anneaux et les idéaux, prenons un anneau R qui n'est pas l'anneau nul. C'est l'anneau dont le seul élément est 0, ce qui ne peut se produire que si l'on permet à l'élément identité d'être égal à 0, puisque cela signifie que

$$x = x1 = x0 = 0.$$

En excluant cette possibilité, les trois énoncés suivants sont équivalents : R est un corps (c'est-à-dire que tout élément non nul de l'anneau est une unité), les seuls idéaux que contient l'anneau sont les idéaux engendrés par 0 et 1, et tout homomorphisme de R dans un anneau non nul A est une injection. Gardez à l'esprit que alors que l'idéal engendré par 1 est noté (1), l'idéal engendré par 0 est généralement noté simplement 0 (tout comme l'anneau nul). Peut-être que la partie la plus difficile à prouver dans cette chaîne est que le troisième énoncé implique le premier. Par définition, tout idéal r est le noyau de l'homomorphisme quotient de R vers R/r. Nous avons supposé que l'homomorphisme est injectif, mais cela implique que le seul idéal propre est (0), où un idéal propre est un idéal plus petit que l'anneau. Pour tout idéal propre $(x), x = 0$. Cela implique que tout x non nul est inversible, ce qui signifie que l'anneau est un corps. Alternativement, nous pourrions prouver à peu près la même chose par un argument de contradiction. Supposons que le troisième énoncé est vrai, mais que R n'est pas un corps. Cela signifie qu'il doit y avoir un élément de R qui n'est pas une unité. S'il n'est pas une unité, l'idéal (x) ne contient pas 1, donc (x) est un idéal propre de R. Si nous prenons l'homomorphisme quotient ϕ, cet homomorphisme n'est pas une injection par définition car $\phi(x) = 0$ et x n'est pas 0. (x) n'est pas un idéal propre, donc l'anneau quotient $R/(x)$ n'est pas l'anneau nul (puisque la seule façon d'obtenir l'anneau nul d'un quotient est via le quotient R/R et nous venons de dire que (x) est plus petit que R). C'est une contradiction, ce qui prouve l'affirmation [1].

Nous n'avons pas tout à fait terminé avec les définitions préliminaires, car nous devons encore définir les modules. La définition des modules peut sembler un peu étrange au début, mais ils sont essentiels à l'algèbre commutative moderne et ils aident à unifier de nombreux concepts que

1. Michael Atiyah and Ian MacDonald, Introduction to Commutative Algebra (USA : Westview Press, 1969).

vous avez peut-être vus auparavant en algèbre linéaire sans vraiment savoir ce qui se passait ou pourquoi les calculs produisaient les bonnes réponses. Commençons par un anneau commutatif R. Un R-module est un groupe abélien M sur lequel R agit via des transformations linéaires. Plus formellement, c'est un groupe abélien M muni d'une application de $M \times R$ vers R telle que pour des éléments x, y dans M et a, b dans R, les axiomes suivants sont vérifiés :

$$(x + y)a = xa + ya,$$

$$x(a + b) = xa + xb,$$

$$x(ab) = (xa)b,$$

$$x1 = x.$$

Vous pourriez voir ces axiomes écrits de telle sorte que les opérateurs se produisent dans l'ordre opposé : cela donne un R-module à gauche, alors que nous avons énoncé les axiomes pour un R-module à droite. L'exemple classique d'un module que vous avez peut-être vu est un espace vectoriel sur un corps : cet espace vectoriel est un R-module, où R est un corps. Comme autre exemple, si $R = \mathbb{Z}$, alors le R-module est un groupe abélien.

Afin d'obtenir des résultats plus significatifs sur les modules et les anneaux, il faut utiliser des conditions de finitude pour des ensembles partiellement ordonnés appelées conditions de chaîne [2]. Si S est un ensemble muni d'un ordre partiel pour la relation $\leq$ tel que $x \leq y$ et $y \leq x$ implique que $y = x$, alors les conditions suivantes sont équivalentes : premièrement, pour une suite croissante dans l'ensemble,

$$x_1 \leq x_2 \leq \dots$$

il existe n_0 tel que $x_m = x_n$ pour tout $n, m \geq n_0$. Deuxièmement, tout sous-ensemble non vide de S contient un élément maximal. La première condition est connue sous le nom de condition de chaîne ascendante, et la seconde est la condition maximale. L'application particulière que nous avons en vue est lorsque S est l'ensemble des sous-modules d'un module et que la relation d'ordre partiel est donnée par l'inclusion de sous-ensembles fermés. Un module qui satisfait l'une ou l'autre des conditions ci-dessus est noethérien. Si nous ordonnons l'ensemble via l'inclusion opposée, les conditions deviennent la condition de chaîne descendante et la condition minimale et un module qui satisfait l'une ou l'autre est artinien. Si l'on prend un ensemble dans lequel la condition maximale est vérifiée, le principe de récurrence noethérienne dit que si X est un sous-ensemble de S qui contient un élément s de S chaque fois qu'il contient tous les éléments $x \in S$ tels que $x > s$, alors $X = S$. Techniquement, ceci est basé sur le fait que l'ensemble de tous les sous-modules forme un treillis modulaire sous l'ordre partiel par inclusion, et c'est ce treillis qui satisfait alors l'une des conditions [3]. Les modules noethériens sont plus utiles que les modules artiniens, car la condition noethérienne est celle qui est requise pour de nombreux théorèmes et propositions. Par exemple, M étant un R-module noethérien implique que tout sous-module de M est de type fini.

Dans de nombreux cas, cependant, les propriétés de base des modules noethériens et artiniens sont les mêmes. Si l'on prend une suite exacte courte de R-modules,

$$0 \to M' \to M \to M'' \to 0$$

2. Emmy Noether, 'Idealtheorie in Ringbereichen', Mathematische Annalen, 83 (1), 24 – 66 (1921).
3. Paul Cohn, Basic Algebra : Groups, Rings and Fields (Trowbridge : Springer, 2003).

le fait que M soit noethérien ou artinien implique que M' et M'' le sont également. Si un ensemble de modules M_i sont tous noethériens ou artiniens, alors la somme directe l'est également. Cela peut être prouvé en utilisant une suite exacte courte similaire.

$$0 \to M_n \to \prod_{i=1}^{n} M_i \to \prod_{i=1}^{n-1} M_i \to 0.$$

Nous pouvons prendre un anneau R et le considérer comme un R-module à droite en soi, et par la même terminologie, l'anneau est dit noethérien ou artinien, où les conditions maximale et minimale sont définies par rapport aux idéaux à droite. Si R est un anneau noethérien à droite, alors un R-module de type fini est également noethérien (ou artinien, respectivement). La plupart des anneaux que l'on utilise lorsqu'on applique l'algèbre commutative sont noethériens : en particulier, les anneaux qui sont utilisés en géométrie algébrique lorsque l'on souhaite étudier les liens entre les anneaux et les objets géométriques sont noethériens. Il vaut peut-être la peine de mentionner que la condition de chaîne ascendante a également des applications en topologie : un espace topologique X est noethérien si les sous-ensembles ouverts de l'espace satisfont la condition de chaîne ascendante ou maximale. Puisque les sous-ensembles fermés sont des compléments de sous-ensembles ouverts (et vice versa), il est équivalent d'exiger que les sous-ensembles fermés de l'espace satisfassent la condition de chaîne descendante ou minimale. On peut montrer que tout sous-espace d'un espace topologique noethérien est également noethérien, et que l'espace est compact.

Il y a trois conditions équivalentes pour qu'un anneau A soit noethérien : nous avons déjà établi leur équivalence dans le cadre des modules. Premièrement, tout ensemble non vide d'idéaux dans l'anneau contient un élément maximal. Deuxièmement, toute chaîne ascendante d'idéaux dans l'anneau est stationnaire : c'est-à-dire que la chaîne d'idéaux

$$a_1 \subset a_2 \subset \cdots \subset a_k \subset \ldots$$

s'arrête à un certain point, donc nous aboutissons à $a_k = a_{k+1}$ pour un certain k. Troisièmement, tout idéal $a \in A$ est de type fini. Si A est noethérien et ϕ est un homomorphisme d'anneaux de A sur un autre anneau B, alors B est également noethérien. Si A est un sous-anneau de B tel que A est noethérien et B est de type fini comme A-module, alors B est un anneau noethérien. Un exemple trivial d'un anneau qui n'est pas noethérien est l'anneau de polynômes $k[X_1, \ldots, X_n, \ldots]$ formé à partir de l'ensemble des polynômes en un nombre infini d'indéterminées, où les coefficients sont tirés du corps k (plus généralement, d'un autre anneau).

De nombreux exemples d'anneaux noethériens peuvent être trouvés en utilisant le théorème de la base de Hilbert. Celui-ci stipule que l'anneau de polynômes $A[x]$ est noethérien si A est noethérien. On peut prouver cela en définissant des ensembles auxiliaires qui forment une chaîne ascendante d'idéaux et en montrant que tout idéal $a \subset A[x]$ est de type fini. (Le mot « base » a été utilisé historiquement pour désigner un ensemble générateur). Comme corollaire direct par récurrence sur n, si A est noethérien, alors $A[x_1, \ldots, x_n]$ l'est aussi. De plus, si A est un anneau noethérien et B est une B-algèbre de type fini, alors B est noethérienne. Tout anneau de type fini, et toute algèbre de type fini sur $\mathbb{Z}$ ou un corps k, est noethérien. On peut suivre des lignes similaires à la preuve du théorème de la base de Hilbert pour montrer que A étant un anneau noethérien implique que l'anneau des séries formelles $A[[x]]$ est noethérien [4].

4. Miles Reid, Undergraduate Commutative Algebra (Cambridge : Cambridge University Press, 2010).

Nous pouvons également énoncer que si k est un corps et E est une k-algèbre de type fini telle que E est aussi un corps, alors E est une extension algébrique finie de k. Une extension de corps est un monomorphisme $i : k \to l$, où k et l sont tous deux des sous-corps d'un corps plus grand (souvent pris comme $\mathbb{C}$). Nous pourrions dire que k est le petit corps et l le grand corps. Il y a de nombreux résultats intéressants pour les extensions de corps et on étudie ce type d'extension en détail dans la théorie de Galois : spécifiquement, le groupe des automorphismes de corps de l'extension. La célèbre loi des tours, par exemple, est un résultat sur les degrés des extensions où il y a une chaîne de sous-corps (le degré d'une extension de corps étant la dimension du grand corps considéré comme un espace vectoriel sur le petit corps) [5].

Une extension finie est une extension de degré fini et une extension (notée $l : k$) est algébrique si tout élément de l est algébrique sur k. Toute extension finie est algébrique, mais la réciproque n'est pas toujours vraie. Un élément est algébrique sur k s'il satisfait une relation de dépendance pour un polynôme de degré n dans l'anneau de polynômes sur le corps :

$$f(y) = a_n y^n + \cdots + a_1 y + a_0 = 0.$$

On peut diviser par a_n lorsqu'on travaille dans un corps, donc on peut supposer que $a_n = 1$: c'est-à-dire que le polynôme est unitaire. Cependant, un anneau de polynômes n'a pas à être sur un corps. Dans le cas où il est sur un anneau, la relation

$$f(y) = a_n y^n + \cdots + a_1 y + a_0 = 0,$$

où $a_n = 1$ est connue comme une relation de dépendance intégrale pour y. Il y a une relation utile entre la dépendance intégrale et les conditions de finitude dans une extension d'anneaux : comme exemple, si l'on sait que deux éléments d'une extension d'anneaux $B \subset A$ sont entiers sur A, on peut utiliser des conditions de finitude pour montrer que la somme et le produit des deux éléments sont entiers sur A sans avoir à calculer leurs relations de dépendance intégrale. On peut commencer avec une A-algèbre $\phi : A \to B$ et un élément $y \in B$ et montrer que les énoncés suivants sont tous équivalents : y est entier sur A, le sous-anneau de polynômes $A'[y] \subset B$ engendré par $A' = \phi(A)$ et y est fini sur A, et il existe une A-sous-algèbre $C \subset B$ telle que $A'[y] \subset C$ et C est fini sur A. On peut prouver la dernière équivalence en utilisant l'astuce du déterminant [6].

Ces conditions de finitude nous conduisent à un lemme important, le lemme de normalisation de Noether (en réalité un théorème). Pour ce lemme, on prend un corps k et une k-algèbre de type fini A. Dans ce cas, il existe des éléments $x_1, \ldots, x_n$ dans A tels que $x_1, \ldots, x_n$ sont algébriquement indépendants sur k et A est indépendant sur $B = k[x_1, \ldots, x_n]$. Une k-algèbre est dite de type fini sur k si $A = k[x_1, \ldots, x_n]$ pour un certain ensemble fini $x_1, \ldots, x_n$. Plus en détail pour le cas où A est un domaine d'intégrité, le résultat dit que pour un corps infini k et $K = k(x_1, \ldots, x_n)$ le corps des fractions de k, il existe un entier non négatif d et d combinaisons linéaires $y_1, \ldots, y_d$ de $x_1, \ldots, x_n$ avec des coefficients de k tels que $y_1, \ldots, y_d$ sont algébriquement indépendants sur k et tels que tout élément de R est entier sur $k[y_1, \ldots, y_d]$. Si K est séparablement engendré sur k, alors les y_i peuvent être choisis tels que K est une extension séparable de $k(y_1, \ldots, y_d)$ [7]. Le corps

5. Ian Stewart, Galois Theory (USA : Chapman Hall, 2004).
6. Miles Reid, Undergraduate Commutative Algebra (Cambridge : Cambridge University Press, 2010).
7. Anthony Knapp, Advanced Algebra (New York : Birkhäuser, 2007).

des fractions de l'anneau R est un corps K contenant un sous-anneau isomorphe à R tel que tout élément de K peut être exprimé comme r/s où s est non nul et r et s appartiennent tous deux au sous-anneau. Noether a introduit ce lemme dans le contexte différent d'un article sur la théorie des invariants des groupes finis [8].

Une utilisation importante du lemme est d'établir un résultat connu sous le nom de Nullstellensatz de Hilbert (ou du moins sa forme faible). Celui-ci stipule que si k est un corps et K est une k-algèbre de type fini, alors K est algébrique sur k tel que k est une extension finie de corps. Une autre façon d'énoncer ceci est que si l'on prend un corps algébriquement clos k, chaque idéal maximal dans $R = k[x_1, \ldots, x_n]$ a la forme

$$\mathfrak{m} = (x_1 - \alpha_1, \ldots, x_n - \alpha_n).$$

Dans tous les cas, la preuve commence par utiliser le lemme de normalisation de Noether, car on utilise le fait que l'on a immédiatement un ensemble d'éléments dans K qui sont algébriquement indépendants, plus le fait que K est fini sur l'anneau de polynômes dans les indéterminées formées par ces éléments où les coefficients sont tirés de k. La forme complète du Nullstellensatz est un peu longue, mais elle peut être énoncée en quelques lignes en utilisant le concept de radical d'un idéal. Si I est un idéal contenu dans un anneau commutatif avec une identité, le radical de l'idéal $\sqrt{I}$ est l'ensemble des éléments dans l'anneau tels que la puissance k-ième est dans l'idéal pour un certain $k \geq 1$. En utilisant ce concept, commençons par $R = k[x_1, \ldots, x_n]$, un anneau de polynômes sur un corps algébriquement clos k. Il s'ensuit que pour tout idéal $I \subset R$,

$$IV(I) = \sqrt{I}.$$

Bien que cela ne soit pas évident à partir de l'énoncé utilisant les radicaux, ce théorème marque le début de la géométrie algébrique moderne (l'étude des propriétés géométriques définies par des équations algébriques), car il énonce le résultat de base selon lequel une famille de polynômes sur un corps algébriquement clos a une solution commune lorsque l'idéal qu'ils engendrent dans l'anneau de polynômes est propre. En général, un idéal propre n'a pas nécessairement besoin d'avoir un lieu de zéros non vide, donc le théorème fait en partie l'énoncé non trivial qu'un idéal propre a un lieu de zéros non vide si l'on suppose que le corps est algébriquement clos. Si l'on pense à un système d'équations polynomiales que l'on cherche à résoudre simultanément dans le corps approprié $F_i(x_1, \ldots, x_n)$, l'ensemble des solutions est le lieu de zéros pour le système. La clé est que l'augmentation de la taille du système n'affecte pas le lieu de zéros, donc on peut tout prendre comme membre d'un idéal dans l'anneau de polynômes $k[x_1, \ldots, x_n]$. Le théorème de la base de Hilbert nous dit déjà qu'un idéal $I \subset k[x_1, \ldots, x_n]$ est de type fini, donc étudier le lieu de zéros d'un idéal revient à étudier le lieu de zéros d'un ensemble de polynômes.

Un autre domaine important de l'algèbre commutative auquel Noether a contribué est la théorie des décompositions d'idéaux dans les anneaux noethériens, où les décompositions sont primaires car elles décomposent les idéaux en idéaux primaires. Rappelons que les entiers peuvent être factorisés en produits de nombres premiers et de puissances de nombres premiers. Ce concept de factorisation se généralise aux idéaux, puisque l'on peut avoir des idéaux premiers et des idéaux qui sont analogues à des produits de puissances premières. Un idéal $p \subset A$ est premier si $p \neq (1)$ et si xy

8. Emmy Noether, 'Der Endlichkeitsatz der Invarianten endlicher linearer Gruppen der Charakteristik ρ', Nachr. Ges. Wissm, DE : 28 – 35 (1926).

appartenant à l'idéal implique que soit x soit y par eux-mêmes appartient à l'idéal. p est premier si et seulement si A/p est un domaine d'intégrité. On pourrait peut-être deviner cette équivalence, puisqu'un anneau R est un domaine d'intégrité si pour deux éléments x et y de l'anneau, $xy = 0$ implique que $x = 0$ ou $y = 0$. Un exemple classique est l'anneau $\mathbb{Z}$ (aussi évidemment un anneau commutatif), puisque le produit de deux entiers donnant zéro implique que l'un de ces entiers doit être nul. Un autre exemple est l'anneau de polynômes $\mathbb{Z}[t]$: on peut montrer par contradiction que l'on ne peut pas avoir $fg = 0$ tel que $f, g \neq 0$. Une autre façon d'énoncer ceci est que le domaine n'a pas de diviseurs de zéro, puisque l'on ne peut pas trouver un élément non nul qui peut être multiplié par un autre élément non nul pour obtenir zéro. En plus des idéaux premiers, on peut avoir des idéaux primaires. Un idéal $I \subset A$ est primaire si $I \neq A$ et si xy appartenant à A/I implique que soit x est dans I soit y^n est dans I pour un certain n positif.

Une autre façon d'énoncer la définition est que I est un idéal primaire si et seulement si $\frac{A}{I} \neq 0$ et tout diviseur de zéro dans le quotient est nilpotent (un élément d'un anneau x étant nilpotent s'il existe un n positif tel que $x^n = 0$). Par exemple, les idéaux primaires dans $\mathbb{Z}$ sont les idéaux engendrés par 0 et p^n, pour p premier. On a besoin du deuxième type d'idéal pour permettre des idéaux qui ne sont pas des radicaux. Une décomposition primaire d'un idéal I dans A est simplement l'expression de cet idéal comme une intersection finie d'idéaux primaires :

$$I = \bigcap_{i=1}^{n} q_i.$$

Tous les idéaux n'ont pas de décompositions primaires, mais Noether a prouvé le théorème d'existence de base selon lequel tout idéal contenu dans un anneau noethérien a une décomposition primaire. La preuve est une application d'un argument par récurrence noethérienne et utilise également le concept d'idéal indécomposable. Un idéal est indécomposable s'il ne peut pas être écrit comme l'intersection de deux idéaux plus grands, donc un idéal premier est évidemment indécomposable. Il y a également plusieurs options pour des théorèmes d'unicité ou d'unicité partielle. Par exemple, prenons un idéal décomposable α et écrivons une décomposition primaire minimale pour α :

$$\alpha = \bigcap_{i=1}^{n} q_i.$$

Une décomposition est dite minimale si les radicaux $r(q_i)$ sont tous distincts et si l'intersection $\cap_{j \neq i} q_i$ n'est pas proprement contenue dans q_i. Toute décomposition primaire peut être réduite à une décomposition minimale. Prenons $p_i = r(q_i)$, alors les p_i sont les idéaux premiers dans l'ensemble des idéaux $r(\alpha; x)$ et ne dépendent donc pas de la décomposition choisie pour α. Rappelons qu'un résultat d'unicité célèbre existe pour les entiers connu sous le nom de théorème fondamental de l'arithmétique (prouvé pour la première fois par Euclide) : tout entier est soit un nombre premier, soit peut être décomposé en un produit de nombres premiers unique modulo l'ordre. Le théorème fondamental a été utilisé par Gauss pour prouver un autre résultat de base, la loi de réciprocité quadratique. Celle-ci stipule que pour tout nombre premier impair p et q, la relation suivante est vérifiée

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

où le symbole de Legendre $\left(\frac{q}{p}\right)$ est défini comme 0 si q divise p, 1 si l'équation modulaire $x^2 \equiv q \pmod{p}$ a une solution, et -1 sinon. Les deux dernières possibilités sont équivalentes à q étant un

résidu quadratique [9].

Pour un autre théorème d'unicité, prenons un idéal décomposable α. Soit $\cap_{i=1}^{n} q_i$ une décomposition primaire minimale de α et $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_n}\}$ un ensemble d'idéaux premiers de α. Il s'ensuit que l'intersection $q_{i_1} \cap \ldots \cap q_{i_m}$ ne dépend pas de la décomposition. Comme corollaire, les composantes primaires q_i correspondant aux idéaux premiers minimaux sont déterminées de manière unique par α. Le terme « isolé » trouve son origine en géométrie algébrique, tout comme la notation Spec, se référant à un type d'espace topologique connu sous le nom de « spectre premier d'un anneau » où la topologie est la topologie de Zariski. En géométrie algébrique, on considère généralement des objets appelés variétés, où une variété est un objet géométrique découpé par un ensemble d'équations polynomiales homogènes en une ou plusieurs variables

$$\{P_1(x_1, \ldots, x_d) = \cdots = P_k(x_1, \ldots, x_d) = 0\}.$$

Si $A = k[x_1, \ldots, x_n]$ pour un corps k, l'idéal α découpe une variété X. Les composantes premières minimales $\mathfrak{p}_i$ correspondent aux composantes de la variété qui sont irréductibles, tandis que les premiers plongés correspondent à des sous-variétés plongées dans les composantes irréductibles. Bien que nous ayons dit que les composantes primaires isolées sont déterminées de manière unique par l'idéal, ce n'est généralement pas vrai pour les composantes primaires plongées [10].

Comme avec l'exemple des espaces topologiques noethériens, il existe d'autres objets « noethériens » qui suivent le type de condition de finitude associée à Noether. Par exemple, en géométrie algébrique, un schéma X est dit noethérien s'il a un recouvrement fini par des ensembles affines

$$X = \bigcup_i U_i, \quad \text{avec} U_i = \text{Spec} A_i,$$

tels que les A_i sont des anneaux noethériens. Ceci est équivalent à un schéma ayant une sorte de condition de finitude sur sa dimensionnalité. Si le schéma affine Spec A est noethérien, alors on peut prouver que A est un anneau noethérien en utilisant l'un de ces arguments standards avec une chaîne d'idéaux dont vous êtes probablement en train de vous habituer à entendre parler [11].

Un théorème célèbre de Noether concerne les invariants calculés dans les problèmes variationnels : il est généralement connu sous le nom de théorème de Noether et c'est l'un des résultats les plus importants de l'histoire des mathématiques et de la physique théorique (la physique moderne ne se serait certainement pas développée dans la même direction sans ce théorème) [12]. Dans la terminologie moderne, le théorème peut être énoncé comme suit : prenons f envoyant de $\Omega \times \mathbb{R}^m \times \mathbb{R}^{m \times d}$ vers $\mathbb{R}$ telle que f soit deux fois différentiable en v et A et satisfasse des bornes de croissance

$$|D_v f(x, v, A)|, |D_A f(x, v, A)| \leq C(1 + |v|^p + |A|^p),$$

pour un certain $C > 0$ et $p \in [1, \infty)$. Prenons une fonctionnelle associée pour f

$$F[u] \int_\Omega f(x, u(x), \nabla u(x)) \mathrm{d}x$$

9. Henryk Iwaniec and Emmanuel Kowalski, Analytic Number Theory (USA : American Mathematical Society, 2004).

10. Michael Atiyah and Ian MacDonald, Introduction to Commutative Algebra (USA : Westview Press, 1969).

11. Igor Shafarevich, Basic Algebraic Geometry : Schemes and Complex Manifolds (Berlin : Springer, 1994).

12. Emmy Noether, 'Invariante Variationsprobleme', Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, 235 – 257 (1918).

telle que u_* soit un minimiseur pour cette fonctionnelle et que cette fonctionnelle soit invariante sous les transformations spécifiées par les applications suivantes

$$g(x,0) = x,$$

$$H(x,0) = u_*(x).$$

Les équations pour g et H ressemblent à celles d'une homotopie, et on peut penser à la transformation de cette manière. Supposons qu'il existe une majorante h dans $L^p(\Omega)$ telle que

$$|\partial_\tau H(x,\tau)|, |\partial_\tau g(x,\tau)| \leq h(x)$$

pour presque tout x et tout réel τ. Il s'ensuit que pour tout minimiseur de la fonctionnelle $F[u]$, il y a une loi de conservation

$$\operatorname{div}[\mu^T D_A f(x, u_*, \nabla u_*) - \nu f(x, u_*, \nabla u_*)] = 0$$

presque partout dans Ω, où

$$\mu(x)\partial_\tau H(x,0),$$

$$\nu(x)\partial_\tau g(x,0),$$

sont connus comme les multiplicateurs de Noether. Cela signifie essentiellement que les invariances d'une fonctionnelle qui peut être différenciée donnent lieu à des lois de conservation. En termes plus quantitatifs, les invariances de la fonctionnelle donnent lieu à des équations différentielles qu'un minimiseur de la fonctionnelle doit satisfaire [13].
Le théorème peut également être énoncé en termes plus géométriques si on le préfère. Commençons par un groupe de mouvements à un paramètre $\phi_s : M \to M$ sur M, qui engendre un champ de vecteurs X par

$$X_q f = \frac{\partial f(\phi_s(q))}{\partial s},$$

lorsque la dérivée est évaluée en $s = 0$. Si cela semble étrange, rappelons que les champs de vecteurs sont des opérateurs sur l'espace des fonctions lisses tels qu'un champ de vecteurs agissant sur une fonction à valeurs réelles est une autre fonction à valeurs réelles Xf. L'application tangente (ϕ_s), induit un flot local sur le fibré tangent et le lagrangien est invariant sous le groupe à un paramètre si

$$L((\phi_s)_* u) = L(u),$$

pour tout u dans le fibré tangent TM. Le théorème de Noether stipule que (ω_u, X) est une constante du mouvement, où ω est une 1-forme sur M définie comme

$$\omega = \left(\frac{\partial L}{\partial \dot{q}^i}\right) \mathrm{d}q^i.$$

Ceci peut être prouvé en coordonnées locales sur le fibré tangent en posant

$$\dot{\mathbf{q}}(s,t) = \phi_s \mathbf{q}(t),$$

13. Filip Rindler, Calculus of Variations (Cham, Switzerland : Springer, 2018).

où $q^i(t)$ est une solution des équations d'Euler-Lagrange et en différenciant par rapport à t. Après un calcul et en supposant l'invariance du lagrangien, nous aboutissons à

$$\frac{\partial}{\partial t}\left(p_i X^i\right) = 0.$$

Cependant,

$$\langle \omega_u, X \rangle = g_{ij}\dot{q}^i X^j = p_i X^i.$$

Le terme le plus à droite doit être une constante d'après l'équation précédente, ce qui établit le résultat. Le groupe à un paramètre est généralement connu comme un groupe de symétrie pour le système, d'où une relation physique entre les lois de conservation d'un système et ses symétries mathématiques [14].

Je dois souligner qu'il s'agit d'un aperçu extrêmement bref et sélectif de l'œuvre de Noether et que, compte tenu des contraintes d'espace, j'ai choisi de me concentrer sur ses contributions les plus fondamentales et importantes à l'algèbre et à la physique mathématique. Noether a travaillé dans de nombreux autres domaines en plus de l'algèbre commutative et je n'ai pas abordé ses autres contributions : voir, par exemple, ses travaux sur la topologie algébrique précoce et la théorie des représentations des groupes et des algèbres.

14. Peter Szekeres, A Course in Modern Mathematical Physics : Groups, Hilbert Space and Differential Geometry (Cambridge : Cambridge University Press, 2004).