BULLETIN DE LA S. M. F.

E. CAHEN

Sur l'arithmétique du corps de tous les nombres algébriques

Bulletin de la S. M. F., tome 56 (1928), p. 7-17

<http://www.numdam.org/item?id=BSMF_1928__56__7_0>

SUR L'ARITHMÉTIQUE DU CORPS DE TOUS LES NOMBRES ALGÉBRIQUES ;

PAR M. EUGÈNE CAHEN.

On sait qu'on appelle *nombre algébrique* toute racine d'une équation algébrique à coefficients entiers rationnels (les entiers rationnels sont les nombres $0, \pm 1, \pm 2, \ldots$). On peut supposer et l'on supposera toujours ces coefficients premiers dans leur ensemble. Dans la suite il ne sera jamais question que de telles équations et pour simplifier nous les appellerons tout simplement « équations ».

Un nombre algébrique α satisfait à une infinité d'équations parmi lesquelles il y en a une de degré plus petit que ceux de toutes les autres. Cette équation est dite *irréductible*, et son degré est dit le *degré* du nombre algébrique α. Ses racines autres que α sont dites les nombres conjugués de α.

L'ensemble de *tous* les nombres algébriques forme un corps, c'est-à-dire que la somme, la différence, le produit, le rapport de deux nombres algébriques sont des nombres algébriques.

Un nombre algébrique est dit *entier* lorsqu'il satisfait à une équation irréductible dont le premier coefficient est 1. Si un nombre algébrique satisfait à une équation *non irréductible* dont le premier coefficient est 1, l'équation irréductible à laquelle il satisfait a aussi pour premier coefficient 1, et le nombre est entier. Mais une équation réductible peut avoir des racines qui soient des nombres algébriques entiers même si son premier coefficient n'est pas égal à 1.

Dans la suite le mot « entier » voudra dire « entier algébrique » en général.

Lorsqu'il s'agira spécialement d'un entier *rationnel* on ajoutera l'épithète « rationnel ».

L'ensemble des nombres *entiers* forme un anneau, c'est-à-dire que la somme, la différence, le produit de deux entiers sont des entiers.

Mais le rapport de deux entiers n'est pas en général un entier.

Un entier α est dit *divisible* par un entier β lorsque $\alpha = \beta\lambda$, λ étant lui-même un entier. On dit encore dans ce cas que α est un *multiple* de β et que β est un *diviseur* ou un *facteur* de α. Voici d'abord une propriété qui a son analogue dans la théorie des entiers rationnels et dans celle des entiers d'un corps : *Si* α, β, ... *sont divisibles par* γ, *il en est de même de* $\lambda\alpha + \mu\beta + \ldots$ *où* λ, μ, ... *sont des entiers quelconques.*

En voici maintenant une d'un caractère tout à fait différent :

Toute puissance à exposant rationnel d'un entier est elle-même un entier. En effet si un entier α satisfait à

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0,$$

$\alpha^{\frac{1}{k}}$ sera aussi un entier puisqu'il satisfait à

$$x^{nk} + a_1 x^{(n-1)k} + \ldots + a_n = 0.$$

Et $\alpha^{\frac{h}{k}}$ sera aussi un entier, puisque c'est le produit de h facteurs égaux à $\alpha^{\frac{1}{k}}$ ($\alpha^{\frac{1}{k}}$ a k déterminations, mais le théorème est vrai pour l'une quelconque d'entre elles).

L'étude de l'ensemble des nombres entiers algébriques n'a guère été faite.

Les résultats déjà obtenus se trouvent dans Dedekind (*Allegemeine Zahlentheorie*, supplément à *Vorlesungen über Zahlentheorie* de L. Dirichlet). Nous allons les rappeler d'abord.

On appelle *unités* les entiers qui divisent tous les autres. Ce sont les entiers définis par une équation dont le premier et le *dernier* coefficient sont égaux à + ou — 1. Le produit et le rapport des deux unités sont des unités. Toute puissance à exposant rationnel, positif, négatif ou nul d'une unité est une unité.

Deux entiers qui ne diffèrent que par un facteur unité sont dits *associés;* ils ont les mêmes diviseurs et les mêmes multiples. Deux entiers associés à un troisième sont associés entre eux et l'on peut partager l'ensemble de tous les entiers en systèmes d'entiers associés entre eux, de façon que, pour ce qui regarde les questions de divisibilité, tous les entiers d'un même système sont équiva-

lents entre eux. Quand deux entiers sont divisibles chacun l'un par l'autre ils sont associés.

On voit dès maintenant comment la théorie dont nous nous occupons se distingue essentiellement soit de celle de l'ensemble de tous les nombres, soit de celle de l'ensemble des nombres fractionnaires d'un corps algébrique, soit de celle de l'ensemble des entiers d'un corps algébrique.

Elle se distingue de la théorie de l'ensemble de tous les nombres en ce que tout entier n'est pas divisible par tout autre différent de zéro.

Elle se distingue de la théorie de l'ensemble des nombres fractionnaires d'un corps algébrique en ce que la racine $k^{\text{ième}}$ d'un entier algébrique est encore un entier algébrique.

Enfin elle se distingue de la théorie de l'ensemble des entiers d'un corps algébrique d'abord par la propriété précédente et ensuite parce qu'il n'y a pas d'entier algébrique indécomposable en facteurs différents de lui-même ou d'une unité. En effet α est toujours divisible au moins par les entiers $\alpha^{\frac{h}{k}}\left(0 < \frac{h}{k} < 1\right)$.

Voici un théorème, plus caché que les précédents, que Dedekind a tiré de la théorie des idéaux, et pour la démonstration duquel nous renvoyons à l'ouvrage cité plus haut :

Si l'on considère deux entiers α, β, *on peut trouver un entier* δ *qui jouit des propriétés suivantes. D'abord il divise* α *et* β, *et ensuite il peut se mettre sous la forme*

$$\delta = \lambda\alpha + \mu\beta, \tag{1}$$

λ, μ *étant des entiers.*

Il existe même une infinité de ces entiers, mais ils sont associés entre eux; on peut donc dire que δ *est déterminé à un facteur unité près.*

Cet entier δ s'appellera le *plus grand commun diviseur* (p. g. c. d.) de α et β. Il est facile en effet de voir qu'il jouit des deux propriétés caractéristiques du plus grand commun diviseur :

1° *Tout diviseur de* δ *est un diviseur commun à* α *et* β, puisque δ divise α et β;

2° *Tout diviseur commun à* α *et* β *est un diviseur de* δ à cause de l'égalité (1).

Lorsque δ est une unité, les entiers α et β n'ont d'autre communs diviseurs que les unités; ils seront dits *premiers* entre eux. Une condition nécessaire et suffisante pour que cela soit, est qu'il existe deux entiers λ et μ tels que

$$\lambda\alpha + \mu\beta = 1. \tag{2}$$

Il en résulte que deux entiers rationnels, premiers entre eux dans le domaine des entiers rationnels, le sont encore dans le domaine de tous les entiers algébriques.

De l'égalité (2), résulte comme pour les entiers rationnels les théorèmes suivants (nous ne citons que ceux dont nous aurons à nous servir) :

Quand on divise deux entiers par leur p. g. c. d. les quotients obtenus sont premiers entre eux.

Si un entier divise un produit de deux facteurs et est premier avec l'un deux il divise l'autre.

Quand deux entiers sont premiers entre eux un diviseur de l'un et un diviseur de l'autre le sont aussi.

Tout multiple commun à deux entiers α, β *est multiple de* $\frac{\alpha\beta}{D(\alpha, \beta)}$ [nous désignons par $D(\alpha, \beta)$ le plus grand commun diviseur de α et β] et réciproquement. Cet entier $\frac{\alpha\beta}{D(\alpha, \beta)}$ sera le plus petit commun multiple (p. p. c. m.) de α et β.

Le p. g. c. d. et le p. p. c. m. de plus de deux entiers se définissent comme pour les entiers rationnels.

Quand un entier est premier à plusieurs autres il est premier à leur produit.

De tous ces théorèmes résulte que la théorie des équations diophantiennes et celle des formes linéaires, telle qu'elle est traitée, par exemple, dans le Tome I de notre *Théorie des Nombres* (1), jusqu'à la page 368, c'est-à-dire jusqu'à la considération des nombres premiers absolus, se généralise ici (avec quelques modifi-

(1) Hermann, Paris, 1914.

cations, bien entendu). Ce n'est qu'à partir de là, où s'est arrêté Dedekind, que se manifestent les différences fondamentales car, comme nous l'avons déjà dit, dans l'ensemble des entiers algébriques il n'y a pas de nombres indécomposables.

Nous appellerons *plus petit multiple rationnel* (p. p. m. r.) d'un entier α le plus petit entier rationnel positif qui soit multiple de α. Il est facile à déterminer connaissant l'équation irréductible qui définit α. Soit

$$x^m + a_1 x^{m-1} + \ldots + a_m = 0$$

cette équation. Soit M un entier rationnel positif. $\frac{M}{\alpha}$ est racine de l'équation, irréductible aussi,

$$a_m y^m + M a_{m-1} y^{m-1} + \ldots + M^{m-1} a_1 y + M^m = 0.$$

Pour que M soit un multiple de α, il faut et il suffit que

$$M a_{m-1}, \quad M^2 a_{m-2}, \quad \ldots, \quad M^{m-1} a_1, \quad M^m$$

soient divisibles par a_m. Le p. p. m. r. cherché sera le plus petit entier positif satisfaisant à ces conditions. Il est facile à trouver. On voit tout de suite qu'il ne contient que des facteurs premiers de a_m et qu'il les contient tous. Soient p l'un de ces facteurs premiers, λ_i son exposant dans a_i ($\lambda_i = 0$ si a_i ne contient pas le facteur p, $\lambda_i = \infty$ si $a_i = 0$), soit λ son exposant dans M. On doit avoir

$$(3) \qquad \begin{cases} \lambda + \lambda_{m-1} \geqq \lambda_m, & 2\lambda + \lambda_{m-2} \geqq \lambda_m, & \ldots, \\ (m-1)\lambda + \lambda_1 \geqq \lambda_m, & m\lambda \geqq \lambda_m. \end{cases}$$

Des conditions analogues devront être remplies pour tous les facteurs premiers de a_m. Pour toutes valeurs entières des λ satisfaisant à toutes ces conditions, M sera un multiple rationnel de α, et l'on aura le p. p. m. r. en prenant pour chaque λ le plus petit entier sastisfaisant aux conditions. Nous désignerons le p. p. m. r. de α par $M(\alpha)$.

Nous avons dit que $M(\alpha)$ ne contient que les facteurs premiers de a_m. On voit de plus qu'il les contient tous

La valeur $\lambda = \lambda_m$ satisfait à toutes les conditions (3). Donc $M(\alpha)$ est un diviseur de a_m. D'ailleurs cette propriété résulte aussi de ce que a_m est égal au produit de α par ses conjugués et du théorème suivant :

Tout multiple rationnel de $M(\alpha)$ *est un multiple de* α, *et réciproquement tout multiple rationnel de* α *est un multiple de* $M(\alpha)$. La première partie de ce théorème est évidente et la seconde résulte des conditions (3), ou encore peut se démontrer de la façon suivante :

Soit M un multiple rationnel de α; divisons-le par $M(\alpha)$ et soit

$$M = M(\alpha).q + r \qquad [0 \leq r < M(\alpha)].$$

Puisque M et $M(\alpha)$ sont divisibles par α, l'entier rationnel r le sera aussi et comme il est plus petit que $M(\alpha)$ il faut que $r = 0$ pour que $M(\alpha)$ soit le p. p. m. r. de α.

k désignant un entier rationnel positif, on a

$$M(k\alpha) = kM(\alpha).$$

En effet, si l'on considère un multiple rationnel positif de α et qu'on le multiplie par k, on obtient un multiple rationnel positif de $k\alpha$. Réciproquement, si l'on considère un multiple rationnel positif de $k\alpha$, il est divisible par k, et son quotient par k est un multiple rationnel positif de α. Il en résulte que tous les multiples rationnels positifs de $k\alpha$ s'obtiennent en multipliant tous les multiples rationnels positifs de α par k. Et, en particulier, le p. p. m. r. de $k\alpha$ s'obtient en multipliant le p. p. m. r. de α par k.

$M(\alpha\beta)$ *est divisible* $M(\alpha)$ *et par* $M(\beta)$. En effet tout multiple de $\alpha\beta$ est aussi un multiple de α et de β.

$M(\alpha\beta)$ *est un diviseur de* $M(\alpha)M(\beta)$. En effet puisque $M(\alpha)$ est divisible par α et $M(\beta)$ par β il en résulte que $M(\alpha)M(\beta)$ est divisible par $\alpha\beta$.

Des deux théorèmes précédents on déduit que si $M(\alpha)$ *et* $M(\beta)$ *sont premiers entre eux on a*

$$M(\alpha\beta) = M(\alpha)M(\beta).$$

Nous appellerons *plus grand diviseur rationnel* (p. g. d. r.) d'un entier algébrique α *le plus grand entier rationnel positif qui divise* α.

Soit encore

$$x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = 0$$

l'équation irréductible qui définit α. Soit D un entier rationnel

positif. $\frac{\alpha}{D}$ est racine de l'équation, irréductible aussi,

$$D^m y^m + D^{m-1} a_1 y^{m-1} + \ldots + D a_{m-1} y + a_m = 0.$$

Pour que D soit un diviseur de α il faut et il suffit que

a_1 soit divisible par D, a_2 par D^2, ..., a_{m-1} par D^{m-1} et a^m par D^m.

Le p. g. d. r. cherché sera le plus grand entier positif satisfaisant à ces conditions. Il ne peut contenir que des facteurs premiers communs à $a_1, a_2, \ldots, a_m$.

Soit μ l'exposant d'un tel facteur dans D, μ doit satisfaire aux conditions

$$\mu \leqq \lambda_1, \qquad 2\mu \leqq \lambda_2, \qquad \ldots, \qquad m\mu \leqq \lambda_m,$$

les λ ayant la même signification que plus haut. Pour toutes valeurs entières rationnelles des μ satisfaisant à ces conditions, D sera un diviseur rationnel de α et l'on aura le p. g. d. r. en prenant pour chaque λ le plus grand entier rationnel satisfaisant à ces conditions. Nous désignerons le p. g. d. r. de α par $D(\alpha)$.

On voit immédiatement que $D(\alpha)$ *est un diviseur de* $M(\alpha)$.

$D(\alpha)$ *est égal à* $M(\alpha)$ *quand* α *est associé à un entier rationnel, et dans ce cas seulement.*

Quand $D(\alpha) = 1$ l'entier α sera dit *primitif.*

k désignant un entier rationnel, on a

$$D(k\alpha) = k D(\alpha).$$

La démonstration est analogue à celle donnée pour $M(\alpha)$.

On en déduit que *le quotient d'un entier algébrique par son p. g. d. r. est un entier primitif.* Ainsi tout entier est le produit d'un entier primitif par un entier rationnel positif.

$D(\alpha\beta)$ *est un multiple de* $D(\alpha)D(\beta)$.

En effet on a

$$\alpha = D(\alpha)\alpha', \qquad \beta = D(\beta)\beta',$$

α' et β' étant primitifs. Alors

$$\alpha\beta = D(\alpha)\,D(\beta)\,\alpha'\beta'$$

et, par suite,

$$D(\alpha\beta) = D(\alpha)\,D(\beta)\,D(\alpha'\beta').$$

ce qui démontre le théorème. On voit de plus que si le produit des

deux entiers primitifs α' et β' est lui-même primitif, $D(\alpha\beta)$ est égal à $D(\alpha)D(\beta)$. Mais le produit de deux entiers primitifs n'est pas toujours primitif. Par exemple $(\sqrt{2})^2 = 2$.

Tout diviseur rationnel d'un entier α est un diviseur de son p. g. d. r.

Cela résulte immédiatement de la façon dont on trouve le p. g. d. r.

Si le produit de deux entiers algébriques α, β est égal à un entier rationnel positif M, *on a*

$$M = \alpha\beta = M(\alpha)D(\beta) = M(\beta)D(\alpha).$$

En effet, puisque M est un multiple de α c'est un multiple de $M(\alpha)$.

$$M = M(\alpha)k,$$

k étant un entier rationnel positif. Donc

$$\alpha\beta = M(\alpha)k,$$

d'où

$$\frac{\beta}{k} = \frac{M(\alpha)}{\alpha}.$$

Puisque $M(\alpha)$ est divisible par α on voit que β est divisible par k, donc k est un diviseur de $D(\beta)$. Soit

$$k = \frac{D(\beta)}{h}.$$

Alors

$$\frac{M(\alpha)}{h} = \alpha\frac{\beta}{D(\beta)},$$

ceci montre que le nombre rationnel positif $\frac{M(\alpha)}{h}$ est entier. C'est d'ailleurs un entier rationnel positif et il est multiple de α; donc, puisque $M(\alpha)$ est le p. p. m. r. de α c'est que $h = 1$. Alors $k = D(\beta)$ et l'on a

$$\alpha\beta = M(\alpha)D(\beta).$$

On verrait de même que

$$\alpha\beta = M(\beta)D(\alpha).$$

Comme cas particulier on voit que si $M = M(\alpha)$ on a $D(\beta) = 1$. Ainsi le quotient du p. p. m. r. d'un entier par cet entier est un entier primitif. Réciproquement, si le quotient d'un multiple

rationnel d'un entier par cet entier est primitif, ce multiple est le p. p. m. r. D'ailleurs ce cas particulier se démontrerait directement avec la plus grande facilité.

Nous allons maintenant chercher à établir quelque chose d'analogue à la décomposition des entiers rationnels en facteurs premiers et, pour cela, nous démontrerons d'abord le théorème suivant :

Tout entier α dont le p. p. m. r. est MM' *où* M *et* M′ *sont premiers entre eux se décompose en un produit de deux facteurs dont les p. p. m. r. sont respectivement* M *et* M′. *Cette décomposition n'est possible que d'une seule manière (à des facteurs unités près).*

En effet, soit

$$MM' = \alpha\beta \qquad [D(M, M') = 1].$$

1° On a

$$\alpha = \frac{M'}{D(\beta, M')} \times \frac{\alpha}{\dfrac{M'}{D(\beta, M')}}.$$

Le premier facteur du second membre est évidemment entier, et comme M′ en est un multiple, il a pour p. p. m. r. un diviseur de M′, soit D′.

Le second facteur est aussi entier. En effet M′ divise $\alpha\beta$, c'est-à-dire $\alpha D(\beta, M') \times \frac{\beta}{D(\beta, M')}$. Donc $\frac{M'}{D(\beta, M')}$ divise $\alpha \times \frac{\beta}{D(\beta, M')}$. Mais $\frac{M'}{D(\beta, M')}$ est premier à $\frac{\beta}{D(\beta, M')}$, donc il divise α.

Je dis maintenant que ce second facteur admet M comme multiple, c'est-a-dire que $\frac{MM'}{\alpha D(\beta, M')}$ est entier. En effet, puisque $MM' = \alpha\beta$, cette expression est égale à $\frac{\beta}{D(\beta, M')}$.

Ce second facteur qui est entier et qui a M pour multiple a donc pour p. p. m. r. un diviseur de M, soit D.

Ainsi α est décomposé en un produit de deux facteurs ayant respectivement pour p. p. m. r. un diviseur D de M et un diviseur D′ de M′. Ces nombres D et D′ sont premiers entre eux puisque leurs multiples M et M′ le sont. Donc α a pour p. p. m. r. le

nombre DD'. On a donc

$$DD' = MM',$$

ce qui exige $D = M$ et $D' = M'$.

2° Cette décomposition n'est possible que d'une seule manière. En effet, soit

$$\alpha = \gamma\gamma' = \delta\delta',$$

γ et δ ayant pour p. p. m. r. l'entier M, γ' et δ' ayant pour p. p. m. r. l'entier M'.

Puisque M et M' sont premiers entre eux, γ et δ' qui en sont respectivement des diviseurs le sont aussi. Alors γ divisant le produit $\delta\delta'$ et étant premier à δ' divise δ. On voit de même que δ divise γ. Donc γ et δ sont associés. De même γ' et δ'.

Ce théorème se généralise facilement de proche en proche : *Tout entier dont le p. p. m. r. est* MM'M'', ... *où* M, M', M'', ... *sont premiers entre eux deux à deux se décompose en un produit de facteurs dont les p. p. m. r. sont respectivement* M, M', M'', ... *Cette décomposition n'est possible que d'une seule manière* (*à des facteurs unités près*), et, en particulier :

Soit $p^\lambda q^\mu r^\nu \ldots$ *le p. p. m. r. décomposé en facteurs premiers d'un entier* α. *Cet entier se décompose en un produit de facteurs dont les p. p. m. r. sont respectivement* p^λ, q^μ, r^ν, ... *Cette décomposition n'est possible que d'une seule manière* (à des facteurs unités près).

Nous appellerons *nombre primaire* tout entier dont le p. p. m. r. est une puissance d'un nombre premier. Le théorème précédent s'énonce alors, en considérant comme identiques deux entiers associés.

Tout entier algébrique est décomposable et d'une seule façon en un produit de facteurs primaires. C'est l'analogue du théorème sur les entiers rationnels : *Tout entier rationnel est décomposable et d'une seule façon en un produit de puissances de nombres premiers.*

Si l'on convient de dire qu'un nombre primaire dont le p. p. m. r. est une puissance de p *appartient* à l'exposant p, on voit qu'on peut ajouter que dans la décomposition précédente *deux quel-*

conques des facteurs appartiennent à des nombres premiers différents.

Si l'on considère deux nombres primaires appartenant à un même nombre premier p, leur produit est un nombre primaire appartenant à ce même nombre.

Si l'on considère un nombre primaire appartenant à un nombre premier p, toute puissance à exposant rationnel positif de ce nombre primaire est elle-même un nombre primaire appartenant au nombre premier p.

Ainsi les nombres primaires appartenant à un même nombre premier p forment un ensemble tel que si l'on appelle π, π', ... des nombres de cet ensemble et r, r' des exposants rationnels positifs, le nombre $\pi^r \pi'^{r'} \ldots$ appartient à l'ensemble. Reste à savoir s'il faut un nombre fini ou un nombre infini d'éléments π, π' ... pour que l'expression $\pi^r \pi'^{r'}$ puisse représenter *tous* les éléments de l'ensemble.
