NOUVELLES ANNALES DE MATHÉMATIQUES

P. L. CIRODDE

Note sur la théorie du plus grand commun diviseur algébrique

Nouvelles annales de mathématiques 1re série, tome 4 (1845), p. 497-507

<http://www.numdam.org/item?id=NAM_1845_1_4__497_0>

NOTE

sur la théorie du plus grand commun diviseur algébrique.

PAR M. P. L. CIRODDE,
Professeur au college de Henri IV.

—

Rappelons d'abord quelques définitions et quelques principes qu'il est important d'avoir bien présents à l'esprit.

1. *On appelle* quantité entière *celle dont l'expression ne renferme ni dénominateur, ni radical.* Telles sont $2a^3b$, $3a^2 - bc$, etc.

2. *On nomme* quantité première *toute quantité entière qui n'est divisible par aucune autre quantité entière qu'elle-même ou l'unité.* Ainsi $3a^2 - 2b$ est une quantité première, mais $a^2 - b^2$ n'en est pas une.

3. *Pour qu'un polynôme entier soit divisible par un diviseur entier, indépendant de la lettre par rapport à laquelle il est ordonné, il faut et il suffit que ce diviseur divise chacun des coefficients de cette lettre.*

4. *Toute quantité première qui divise le produit de plusieurs facteurs entiers divise l'un d'eux.*

5. *Une quantité entière n'est décomposable qu'en un seul système de facteurs premiers.*

6. *Le* plus grand commun diviseur *de plusieurs quantités algébriques est le produit de* tous *leurs facteurs premiers communs tant égaux qu'inégaux.*

7. Nous distinguerons deux cas dans la théorie du plus grand commun diviseur algébrique, selon que les quantités entre lesquelles on le cherchera seront monômes ou polynômes.

Si les quantités proposées sont monômes, on cherchera le P. G. C. *diviseur de leurs coefficients, et on le fera suivre de toutes les lettres communes à ces monômes, en donnant à chacune d'elles le plus petit exposant dont elle s'y trouve affectée. Ce produit sera le* P. G. C. *diviseur demandé*, car il est clair qu'il satisfait à la définition du n° 6.

8. Examinons actuellement le cas où les quantités proposées sont polynômes, et d'abord nous observerons qu'il suit immédiatement de la définition (6) que *la recherche du* P. G. C. *diviseur de plusieurs polynômes ne dépend que de la détermination de celui de deux polynômes.*

Soient en effet les quatre polynômes A, B, C, D. *Opérons comme il est prescrit au n° 79 de nos* Leçons d'Arithmétique (*), et désignons en conséquence par E le P. G. C. diviseur entre A et B, par F celui de E et de C et enfin par G celui de F et de D; G sera le P. G. C. diviseur des quatre polynômes A, B, C, D, car il est évidemment le produit de *tous* leurs facteurs premiers communs.

9. Scholie. Dans la pratique, on devra, après avoir ordonné les polynômes proposés par rapport aux puissances d'une même lettre, chercher d'abord le P. G. C. diviseur entre les deux polynômes du plus faible degré; puis celui de ce P. G. C. diviseur et du plus simple des polynômes restants, et ainsi de suite.

10. Lemme. *On n'altère pas le* P. G. C *diviseur de deux quantités* A *et* B *en multipliant ou en divisant l'une d'elles par un facteur premier avec l'autre.*

En effet si M est une quantité première avec B, le produit MA n'ayant pas d'autres facteurs premiers que ceux de M et de A (5), les facteurs premiers qui sont communs à MA et

(*) ***Leçons d'arithmétique***, par P. L. Cirodde, professeur au college de Henri IV, ***sixième édition***, augmentée de la méthode de division abregee de M. le capitaine Guy

à B sont ceux mêmes qui l'étaient à A et à B ; donc le P. G. C. diviseur de MA et de B est le même que celui de A et de B (6).

On verrait de même qu'en supposant A divisible par M, le P. G. C. diviseur de $\frac{A}{M}$ et de B est identique avec celui de A et de B.

11. Ce Lemme étant ainsi établi, occupons-nous de la recherche du P. G. C. diviseur de deux polynômes, et, pour considérer d'abord le cas le plus simple, *supposons que les deux polynômes ne renferment qu'une seule lettre, et que de plus tous les termes de chacun soient premiers entre eux.*

Désignons-les par A et par B, et admettons que B soit au plus du même degré que A. D'après la définition, le P. G. C. diviseur demandé est le produit de tous les facteurs premiers communs à A et à B ; donc si B divise exactement A, ce polynôme sera le P. G. C. diviseur de A et de B, puisqu'un polynôme ne peut être décomposé qu'en un seul système de facteurs premiers. Effectuons donc la division de A par B : soient Q le quotient et R_1 le reste ; nous aurons

$$A = BQ + R_1$$

or, je dis que, si le quotient Q ne renferme que des termes entiers, le P. G. C. diviseur de A et de B est le même que celui de B et de R_1. En effet, tout facteur commun à A et à B divise A et BQ et par conséquent leur différence R_1 ; de même tout facteur commun à B et à R_1 divise A ; donc les facteurs premiers communs à A et à B sont les mêmes que ceux qui sont communs à B et à R_1, et par conséquent le P. G. C. diviseur de B et de R_1 est le même que celui de A et de B.

Donc *lorsque la division de deux polynômes s'effectue, sans admettre de termes fractionnaires au quotient, le* P. G. C. *diviseur de ces deux polynômes est le même que celui qui existe entre le reste de leur division et le polynôme qui a servi de diviseur.*

La question est ainsi ramenée à chercher le P. G. C. diviseur entre les polynômes B et R_1. On divisera donc B par R_1; si la division réussit, R_1 sera le P. G. C. diviseur demandé; si non, ce P. G. C. diviseur sera le même que celui de R_1 et du reste R_2 de cette deuxième division (on suppose *toujours* que l'on n'ait écrit que des termes entiers au quotient). On divisera donc R_1 par R_2, puis le reste R_2 par celui R_3 de la troisième division, puis R_3 par le reste R_4 de la quatrième, et on continuera ainsi de suite, jusqu'à ce que l'on soit arrivé à un reste indépendant de la lettre ordonnatrice. Si ce reste est nul, le dernier diviseur est le P. G. C. diviseur demandé; sinon, les polynômes proposés sont premiers entre eux, sans quoi le P. G. C. diviseur qui, s'il existe, est dépendant de cette lettre (3), puisque tous les termes de chacun sont premiers entre eux, par hypothèse, devrait diviser ce dernier reste, qui est indépendant de cette même lettre.

12. La démonstration du principe sur lequel est fondée la méthode que nous venons de développer suppose essentiellement que les quotients successifs aient tous leurs termes entiers, car si le quotient Q de la division de A par B était fractionnaire, on n'aurait pas le droit de dire que tout facteur qui divise B divise BQ. Or on sent qu'il arrivera très-souvent que la division du coefficient du premier terme d'un dividende partiel par celui du premier terme du diviseur ne s'effectuera pas exactement. Dans ce cas, on multipliera le dividende par un facteur tel que le terme correspondant du quotient soit entier (nous indiquerons tout à l'heure (13) comment on peut déterminer ce facteur), et cette opération n'altèrera pas le P. G. C. diviseur que l'on cherche, si ce facteur est premier avec le diviseur (10). Or pour que le facteur que l'on introduit ainsi soit certainement premier avec le diviseur, il suffit que les coefficients de tous les termes de ce diviseur soient premiers entre eux, puisque notre facteur est indépendant de la lettre or-

donnatrice. En conséquence *avant de prendre un reste pour diviseur, on aura soin de chercher le* P. G. C. *diviseur des coefficients de tous ses termes, et de le diviser par ce* P. G. C. *diviseur, ce qu'il est permis de faire* (10), *puisque le dividende correspondant a déjà tous ses termes premiers entre eux.*

13. *Si le coefficient du premier terme d'un dividende partiel est premier avec le coefficient du premier terme du diviseur, on n'aura qu'à multiplier ce dividende par ce coefficient, et alors le coefficient du terme correspondant du quotient sera évidemment entier. Mais si les deux coefficients dont il s'agit ne sont pas premiers entre eux, il vaudra mieux chercher leur* P. G. C. *diviseur et multiplier le dividende partiel par le quotient obtenu en divisant le coefficient du premier terme du diviseur par ce* P. G. C. *diviseur.* On conçoit en effet qu'en opérant ainsi, on aura rendu le coefficient du premier terme du dividende divisible par celui du premier terme du diviseur, et que le facteur introduit de cette manière dans ce dividende sera le plus simple possible. (*Leçons d'Arithmétique*, 6ᵉ édit., n° 93.)

14. On voit donc que *pour trouver le* P. G. C. diviseur *de deux polynômes il faut leur appliquer la méthode des divisions successives*, comme on le fait dans l'arithmétique, *avec les modifications nécessaires pour que les termes des quotients successifs que l'on obtiendra soient tous entiers* (13), *et avoir bien soin de diviser chaque reste par le* P. G. C. *diviseur des coefficients de tous ses termes, avant de le prendre pour diviseur. On arrêtera cette série d'opérations, quand on sera parvenu à un reste indépendant de la lettre ordonnatrice : si ce reste est nul, le dernier diviseur est le* P. G. C. *diviseur demandé ; sinon, les polynômes proposés sont premiers entre eux.*

15. L'application de cette règle ne saurait présenter de difficultés, dans le cas particulier où nous nous sommes placés ; car les coefficients du polynôme B étant supposés être

tous premiers entre eux, le facteur par lequel on pourra multiplier A pour rendre la division par B possible en termes entiers, sera nécessairement premier avec B, de sorte que l'introduction de ce facteur n'altèrera pas le P. G. C. diviseur cherché. D'un autre côté, les coefficients des différents termes de chaque reste sont numériques et la recherche de leur P. G. C. diviseur se réduit par conséquent à une simple opération d'arithmétique.

16. Passons actuellement au cas général et considérons ainsi deux polynômes entiers quelconques A et B. Représentons par A_1 le P. G. C. diviseur monôme des différents termes de A et par A' le quotient de la division de A par A_1; nous aurons

$$A = A_1 A'.$$

Désignons de même par B_1 le P. G. C. diviseur monôme de tous les termes de B, et par B' le quotient de la division de B par B_1, de sorte que

$$B = B_1 B'.$$

Cela posé, supposons que l'on ait ordonné les polynômes A' et B' par rapport aux puissances d'une même lettre, et appelons A_2 le P. G. C. diviseur de tous les coefficients de cette lettre dans A', et A_3 le quotient de la division de A' par A_2, nous aurons

$$A' = A_2 A_3, \quad \text{et par conséquent} \quad A = A_1 A_2 A_3.$$

Supposons que l'on ait agi sur B' comme on a fait sur A' et soit

$$B' = B_2 B_3, \quad \text{et partant} \quad B = B_1 B_2 B_3;$$

je dis alors que si l'on cherche le P. G. C. diviseur d_1 de A_1 et de B_1; celui d_2 de A_2 et de B_2, et celui d_3 de A_3 et de B_3, le produit

$$d_1 d_2 d_3$$

sera le P. G. C. diviseur des quantités A et B. En effet tout facteur polynôme premier dépendant de la lettre ordonnatrice qui divise $A = A_1A_2A_3$ et $B = B_1B_2B_3$, ne pouvant diviser aucune des quantités A_1, A_2, B_1, B_2, divise nécessairement A_3 et B_3 (4), et est par conséquent un facteur de leur P. G. C. diviseur d_3; donc d_3 est le produit de tous les facteurs polynômes premiers qui, fonction de la lettre ordonnatrice, sont communs à A et à B. On démontrerait de même que d_1 et d_2 sont, l'un le produit de tous les facteurs monômes premiers communs à A et à B, et l'autre celui de tous les facteurs polynômes premiers, communs à A et à B, qui sont indépendants de la lettre ordonnatrice. Donc $d_1d_2d_3$ est bien le produit de *tous* les facteurs premiers communs à A et à B; donc il est leur P. G. C. diviseur.

17. Occupons-nous de la recherche de ces différents P. G. C. diviseurs. La détermination de A_1, de B et de d_1 ne présente aucune difficulté (7). quant aux autres, je dis que si l'on savait trouver le P. G. C. diviseur des polynômes A′ et B′ qui ne renferment plus, chacun, de facteurs monômes communs à tous leurs termes, dans le cas où ils sont composés de n lettres *au plus*, il serait possible de le déterminer aussi, dans le cas où ils en contiendraient $n+1$. En effet, les coefficients de la lettre ordonnatrice dans A′ et dans B′ ne renfermant alors que n lettres, on pourrait, d'après notre hypothèse et en vertu du principe du n° 8. calculer A_2 et B_2, et par suite leur P. G. C diviseur d_2, ainsi que les quotients A_3 et B_3. Cela posé, j'observe que les différents termes de chacun de ces quotients étant premiers entre eux, on pourra appliquer à A_3 et à B_3 la méthode du n° 14; car, dans les raisonnements sur lesquels nous l'avons fondée, nous ne nous sommes nullement occupés du nombre des lettres qui pourraient entrer dans les polynômes proposés (10, 11, 12 et 13). Ainsi pour rendre possible la première division partielle, on multipliera

A_3 par une certaine quantité M qui sera un produit de facteurs premiers du coefficient du premier terme de B_3 (13), et cette opération ne saurait altérer le P. G. C. diviseur des polynômes A_3 et B_3, puisque tous les coefficients de la lettre ordonnatrice dans B_3 étant premiers entre eux, le facteur par lequel on multiplie A_3 est nécessairement premier avec B_3 (3). Ayant ainsi effectué entièrement la division de A_3 par B_3, on pourra supprimer, dans le reste de cette division, tous les facteurs monômes qu'il renfermera (7), ainsi que les facteurs polynômes indépendants de la lettre ordonnatrice qui leur seraient communs, car il suffira, pour cela, de chercher le P. G. C. diviseur de plusieurs polynômes de n lettres au plus (8). On procédera ensuite à la seconde division, en prenant pour diviseur ce reste ainsi modifié, et on continuera ainsi de suite. Donc on arrivera à la valeur de d_3.

Ainsi la détermination du P. G. C. diviseur de deux polynômes A' et B' qui contiennent un certain nombre de lettres et dont les termes de chacun n'ont d'ailleurs aucun facteur monôme commun, ne dépend que de celle du P. G. C. diviseur de pareils polynômes qui renfermeraient une lettre de moins. Or nous avons donné une méthode complète pour calculer le P. G. C. diviseur de deux polynômes d'une seule lettre, tels que tous les termes de chacun seraient premiers entre eux (14); donc on pourra trouver le P. G. C. diviseur de deux polynômes qui renfermeraient deux lettres, puis trois, puis quatre, et en général un nombre quelconque de lettres.

18. Règle générale. *Pour trouver le* P. G. C. *diviseur de deux polynômes* A *et* B, *cherchez le* P. G. C. *diviseur monôme* A_1 *de tous les termes de* A (7); *celui* B_1 *de tous les termes de* B; *puis le* P. G. C. *diviseur* d_1 *de* A_1 *et de* B_1. *Mettez* d_1 *de côté, et divisez* A *et* B *respectivement par* A_1 *et* B_1 : *vous obtiendrez des quotients* A' *et* B' *que vous ordonnerez par rapport aux puis-*

sances d'une même lettre. Calculez le P. G. C. *diviseur* A_2 *des coefficients du polynôme* A', *celui* B_2 *des coefficients du polynôme* B', *et le* P. G. C. *diviseur* d_2 *de* A_2 *et de* B_2. *Mettez* d_2 *de côté, et divisez* A' *et* B' *respectivement par* A_2 *et* B_2, *ce qui vous donnera des quotients* A_3 *et* B_3 *dont tous les termes seront premiers entre eux. Cherchez enfin le* P. G. C. *diviseur* d_3 *de ces deux quotients, d'après la règle du n° 14, et il ne s'agira plus ensuite que de multiplier entre elles les trois quantités* d_1, d_2 *et* d_3. *Leur produit résoudra la question.*

19. Dans le cas où les deux polynômes A' et B' ne renfermeront que deux lettres x et y, et c'est ce cas qui se présentera le plus souvent, on pourra simplifier les calculs de la manière suivante. On les ordonnera par rapport à y, par exemple, et on cherchera le P. G. C. diviseur X des coefficients de cette lettre dans A'; puis on divisera A' par X. On ordonnera le quotient A'' par rapport à x, et on cherchera le P. G. C. diviseur Y des coefficients des différents termes de A''; on divisera A'' par Y, et en appelant A''' le quotient de cette division, on aura

$$A' = XYA'''.$$

On mettra de même le polynôme B' sous la forme

$$B' = X'Y'B''',$$

et en formant ensuite le produit des P. G. C. diviseurs des quantités X et X', Y et Y', A''' et B''', on obtiendra le P. G. C. diviseur de A' et de B', comme il est facile de le démontrer, à l'aide de raisonnements analogues à ceux qu'on a employés au n° 16.

L'avantage de cette méthode consiste à faire appliquer la règle du n° 14 à des polynômes de degré plus faible que ceux sur lesquels on devrait opérer d'après la règle du n° 18.

20. Il y a encore un cas particulier que l'on peut traiter plus simplement que par la *règle générale;* c'est celui où *l'un*

des deux polynômes, A' *par exemple*, *renfermera une lettre* x *qui ne se trouvera pas dans l'autre* B'. *On ordonnera alors* A' *par rapport à* x, *et le* P. G. C. *diviseur demandé sera celui même qui existera entre* B' *et les coefficients de cette lettre* x. Il est évident en effet que B' étant indépendant de x, le P. G. C. diviseur demandé ne peut contenir cette lettre, et divise en conséquence tous les coefficients de x dans le polynôme A' (3), qui est de la forme

$$ax^{\alpha} + bx^{6} + cx^{\gamma} + \text{etc.} :$$

donc en cherchant le P.G.C. diviseur des quantités B', a, b, c, ... on aura celui de A' et de B'.

21. Dans la *théorie générale des équations*, on restreint la définition que nous avons donnée des quantités entières. *On y regarde comme entière toute quantité dans l'expression de laquelle les* inconnues *n'entrent dans aucun dénominateur, ni sous aucun radical, et pour qu'une quantité soit dite divisible par une autre, il suffit que leur division ne donne pas de reste et que le quotient soit entier par rapport aux inconnues, de même que les quantités proposées.* Ainsi $x^2 + \frac{xy}{\sqrt{2}} - 6y^2$, fonction entière de x et de y, est divisible par $\frac{2}{3}x - y\sqrt{2}$, parce que le reste de cette division est nul et que le quotient $\frac{3}{2}x + 3y\sqrt{2}$, est aussi une fonction entière de x et de y.

En partant de ces définitions, on démontre facilement : 1° que *tout facteur du premier degré* $ax + 6$ *qui divise le produit de deux fonctions entières de* x, *divise nécessairement l'une d'elles ;* 2° qu'*une fonction entière de* x *n'est décomposable qu'en un seul système de facteurs du premier degré par rapport à* x.

22. *On appelle* P. G. C. *diviseur de plusieurs fonctions*

entières de x *le produit de tous les facteurs du premier degré en* x *communs à ces fonctions.*

23. Si l'on applique à deux pareilles fonctions, les raisonnements du n° 11, on verra que *pour trouver leur* P. G. C. *diviseur, il faudra les soumettre à la méthode des divisions successives*, telle qu'on la pratique en arithmétique, *en arrêtant l'opération quand on sera parvenu à un reste indépendant de* x; *de telle sorte que si ce reste est nul, le dernier diviseur sera le* P. G. C. *diviseur demandé, et que s'il n'est pas nul, les fonctions proposées n'ont pas de diviseur commun en* x.

24. Remarquons qu'il ne sera pas *nécessaire* d'avoir recours aux modifications prescrites dans le n° 12, parce que la démonstration du principe fondamental (*le* P. G. C. *diviseur de deux fonctions entières de* x *est le même que celui qui existe entre le reste de leur division et celle qui a servi de diviseur*) n'exige pas que le quotient Q soit entier par rapport aux coefficients de x; il suffit qu'il le soit par rapport à cette lettre. Toutefois il sera plus simple de réduire tous les termes des deux fonctions proposées au même dénominateur, de chercher ensuite le P. G. C. diviseur des deux numérateurs, d'après la règle du n° 18, et enfin de diviser le P. G. C. diviseur trouvé par le dénominateur commun, parce qu'en le supprimant dans les fonctions proposées, on les a multipliées par ce dénominateur. Dans la plupart des applications, il sera inutile de tenir compte de ce dénominateur.

(*Extrait d'un ouvrage inédit.*)