

D. LESEVRE, P. MONTAGNON
P. LE BARBENCHON, T. PIERRON

131 DÉVELOPPEMENTS POUR L'ORAL

**AGRÉGATION EXTERNE
MATHÉMATIQUES / INFORMATIQUE**

DUNOD

Conception de maquette de couverture : Hokus Pokus Création

Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.

Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements

d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour

les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée. Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du

Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).



© Dunod, Paris 2020

11 Rue Paul Bert, 92240 Malakoff

ISBN 978-2-10-079556-7

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Organisation de ce livre

Chapitres thématiques. Cet ouvrage a été organisé dans l'optique de faciliter sa consultation. Les développements sont regroupés par chapitres thématiques, qui correspondent essentiellement à la classification des leçons dans le programme. Ce choix d'organisation a été dicté par le thème principal et les méthodes mobilisées. Il ne restreint toutefois pas les développements au thème indiqué : un chapeau plus précis détaille la façon dont chaque sujet s'insère dans les différentes leçons qu'il est susceptible d'illustrer.

Structure des développements. Les développements ont été rédigés sous forme d'exercices, ce qui nous a paru pertinent pour plusieurs raisons. Le découpage en questions permet de donner une vision à plus haut niveau de la structure de la preuve et de l'enchaînement des arguments. Il est primordial pour l'agrégatif qui étudie un développement de trouver un juste milieu entre son apprentissage par cœur et sa relecture complète le jour de l'oral. Présenter le développement sous forme d'exercice permet d'éviter ces extrêmes : le candidat qui prépare le développement pendant l'année est invité à s'appuyer sur ces jalons pour le comprendre, et ces questions fournissent à leur tour un moyen efficace de retrouver la trame du développement lors de l'épreuve. Nous espérons ainsi avoir choisi un mode de présentation pédagogique et pratique, forçant à condenser chaque démonstration en l'enchaînement de quelques étapes clés scandées par les questions.

Chaque développement est suivi de commentaires tantôt mathématiques, tantôt culturels, ou discutant de l'organisation de la présentation au tableau et des variations possibles. Ces commentaires ont été écrits dans l'esprit d'ouverture que nous souhaitons conserver : chacun demeure libre de présenter différemment chaque résultat, par exemple en ne sélectionnant qu'une partie de l'exercice proposé ou en développant plus avant un point abordé en commentaire. Nous ne pouvons qu'encourager ces divergences, qui participent à une présentation plus personnelle et donc plus adaptée.

Enfin, des exercices sont présents à la fin de chaque développement, et représentent des questions qui pourraient être posées par le jury. Notre but est d'aider le lecteur à s'assurer de sa bonne compréhension des détails du raisonnement, notamment lorsque la correction passe un peu rapidement sur un point ou contourne une difficulté dont il est important d'être conscient. Les questions posées invitent donc tantôt à éclaircir un argument classique utilisé dans la preuve, tantôt à en proposer une variation, et parfois, à des fins d'approfondissement, à considérer une question indépendante mais sur le même thème. Nous nous sommes également

efforcés de donner une indication lorsque les arguments nécessaires à la résolution de la question posée nous ont semblé moins immédiats.

Niveau de difficulté. Nous avons déjà souligné que la grande liberté laissée lors des épreuves orales peut — et doit — mener à de nombreuses disparités de niveau quant aux contenus présentés. C'est la raison pour laquelle nous avons choisi de faire figurer un niveau de difficulté indicatif pour chaque développement, entre ★ et ★★★. Un développement de niveau ★ est élémentaire en tout point, dans son objet comme ses arguments, sans être particulièrement long et sans faire intervenir d'astuce ; nous avons par ailleurs fait un effort particulier pour détailler chaque étape du raisonnement dans ce cas. Un développement de niveau ★★★ est plus difficile, souvent à cause d'aspects techniques ou de passages sur lesquels il est nécessaire de passer rapidement pour se concentrer sur le cœur de la preuve, et parfois à cause de prérequis non triviaux ou moins classiques. Ces choix demeurent bien sûr subjectifs, et certains pourraient trouver ardu un développement marqué ★ portant sur des notions avec lesquelles ils sont peu familiers, ou aisé un développement marqué ★★★ et mobilisant des idées et techniques qu'ils maîtrisent déjà.

Par ailleurs, de nombreuses déclinaisons de chaque développement sont possibles : on peut choisir de n'en exposer qu'une partie, de varier le niveau de détails ou, dans certains cas, d'utiliser les commentaires fournis pour présenter une preuve alternative. Ces modulations peuvent changer le niveau de difficulté, et nous incitons le lecteur à consulter des développements sur des sujets ou leçons qui l'intéressent indépendamment du niveau de difficulté indiqué. Ainsi, certains développements indiqués comme étant de niveau ★★★ contiennent des parties autonomes ou admettent des variations de preuves fournies en commentaires qui pourraient constituer un développement ★ ou ★★, et réciproquement. Les choix de rédaction ont été faits pour respecter un équilibre entre les niveaux de difficulté à l'échelle du livre, de sorte que celui-ci puisse proposer à chacun des développements intéressants et adaptés à son niveau. Il fait toutefois partie du travail de chaque agrégatif de juger par lui-même du niveau auquel il souhaite placer sa présentation et de revisiter chaque développement à son gré.

Correspondances entre développements et leçons. L'objectif principal de ce livre demeure de permettre à chaque agrégatif de composer son corpus de développements en fonction de ses préférences et de ses besoins. Chaque leçon du programme doit être illustrée par au moins deux développements que le jury pourra demander d'exposer en détails après la présentation de la leçon. De manière à aider le candidat à faire son choix, comprendre ses possibilités et déterminer les développements les mieux adaptés pour illustrer ses leçons, nous avons présenté des tableaux de correspondance entre développements et leçons à la fin de l'ouvrage. Ainsi, il n'est pas nécessaire de consulter un développement pour retrouver les leçons correspondantes, ni de parcourir tout l'ouvrage pour trouver un développement adapté à une leçon donnée. Enfin, une présentation de cette correspondance a également été fournie sous forme de graphes, permettant une cartographie différente et utile pour choisir ses développements.

Table des matières

Avant-propos	iii
Liste des notations	xiii
Développements d'algèbre	1
Groupes, actions et représentations	3
1. Incertitude de Heisenberg pour les groupes ★	5
2. Théorème de Dixon ★	10
3. Générateurs de $SL_2(\mathbb{Z})$ ★	14
4. Ensembles de transpositions engendrant \mathfrak{S}_n ★	18
5. Paires génératrices de sous-groupes de \mathfrak{S}_n ★★	23
6. Ordre maximum des permutations ★★	28
7. Commutativité de permutations aléatoires ★★	35
8. Cyclicité des groupes d'ordre pq ★	41
9. Groupes d'ordre 105 ★★★	44
10. Table des caractères des groupes diédraux ★	49
11. Théorème $p^a q^b$ de Burnside ★★★	54
Anneaux, corps et théorie des nombres	61
12. Théorème de Cohn ★	63
13. Lemme de Hensel ★	69
14. Méthodes polynomiales en combinatoire ★★	73
15. \mathbb{C} est algébriquement clos ★	78
16. Lemme d'intersection de Krull ★★	81
17. Cyclicité de \mathbb{F}_p^\times ★★	84
18. Automorphismes de \mathbb{F}_{p^m} ★	89
19. Automorphismes d'un corps cyclotomique ★	92
20. Automorphismes sauvages de \mathbb{C} ★★★	96
21. Théorème d'Artin ★★★	103
22. L'unique entier entre un carré et un cube ★★	109
23. Valeurs absolues sur \mathbb{Q} ★★	114
24. Théorème de Fermat et cyclotomie ★★★	120
25. Problème de Waring modulo q ★★★	128
Algèbre linéaire	133
26. Perturbation par des matrices de rang un ★	135
27. Quaternions et isomorphismes ★	138
28. Lemmes de Schwartz-Zippel et de Kakeya ★★	147
29. Calculs de polynômes caractéristiques ★	155
30. Endomorphismes conservant le déterminant ★	163

31. Endomorphismes conservant le rang ★★	167
32. Théorème de Chebotarev ★★★	172
33. Images par l'exponentielle ★★	178
34. Décomposition polaire ★	185
35. Réduction des endomorphismes nilpotents ★	190
36. Décomposition de Dunford ★	194
37. Forme normale de Smith ★★	201
38. Sous-algèbres réduites de $\mathcal{M}_n(\mathbb{C})$ ★★	207
39. Théorème d'Engel ★★★	212
Formes quadratiques et géométrie	217
40. Billard circulaire ★	219
41. Le plongeur le plus long ★★	225
42. Théorèmes de Helly et de Carathéodory ★	235
43. Théorème des trois réflexions ★	239
44. Théorème de Killing-Hopf ★	243
45. Isométries directes des solides de Platon ★★	251
46. Théorème d'Hermite ★	260
47. Formes quadratiques semi-réduites ★★	264
48. Théorème de Minkowski pour les formes quadratiques ★★★	268
Développements d'analyse	273
Analyse fonctionnelle et topologie	275
49. Compacts d'un espace de Hilbert séparable ★★	277
50. Opérateurs compacts d'un espace de Hilbert ★★	281
51. Décomposition de Mityagin ★★	285
52. Une isométrie de $L^2(\mathbb{R}_+)$ non surjective ★★	290
53. Logarithme et théorème de Brouwer ★★	296
54. Théorème de Riesz-Fischer ★	303
Calcul différentiel, équations différentielles et EDP	309
55. Théorème de Cartan-von Neumann ★	313
56. Théorème de stabilité de Liapounov ★	318
57. Des extrema liés au consommateur ★★	323
58. Théorème de Cauchy-Peano ★★	332
59. Modèle de croissance de Solow-Swan ★	341
60. Croissance logistique et prédation ★	347
61. Modèle épidémiologique SIS ★★	353
62. Modèle épidémiologique SIR ★★	361
63. Étude qualitative d'une équation de Riccati ★★	367
64. Modèle de Lotka-Volterra ★★★	372
65. Équation des ondes pour une corde vibrante ★	381
66. Caractère bien posé : équation de transport ★★★	388
67. Dualité contrôlabilité-observabilité ★★★	396
Analyse classique et complexe	407
68. Une méthode archimédienne pour approcher π ★	409
69. Convergence d'une suite de polygones ★★	413

TABLE DES MATIÈRES

70. Développement en fractions continues ★★	417
71. Théorèmes de Choquet et de Birkhoff ★★	423
72. Théorème de Nash ★★	429
73. Formules de Frenet-Serret ★	437
74. Méthode de descente de gradient ★	441
75. Méthode de Gauss-Seidel ★	445
76. Méthode de relaxation ★	451
77. Méthode de Kaczmarz ★	455
78. Prolongement analytique suivant une courbe ★	461
79. Domaines d'holomorphie à une variable ★★	464
80. Forme normale de Jordan et résidus ★★★	469
81. Espace des formes modulaires ★★★	477
Intégration et approximation de fonctions	485
82. Calcul des intégrales de Fresnel ★	487
83. Racine carrée de la primitivation ★	496
84. Méthode de la phase stationnaire ★	502
85. Théorème de Paley-Wiener ★	509
86. Théorème de Plancherel ★★	514
87. Prolongement de la fonction ζ de Riemann ★★	522
88. Théorème de Fejér-Cesàro ★	531
89. Théorème de Minkowski pour les réseaux ★★	539
90. Théorème taubérien de Hardy-Littlewood ★	545
91. Divergence de l'interpolation de Lagrange ★★	552
92. Meilleure approximation polynomiale ★★	557
Probabilités et statistiques	563
93. Aiguille de Buffon ★	565
94. Paradoxe de Penney ★	570
95. Formule de Stirling par la limite centrale ★	580
96. Une marche aléatoire sur $[0, 1]$ ★★	588
97. Loi forte des grands nombres ★★	594
98. Théorème de Pólya — version dénombrement ★★	599
99. Théorème de Pólya — version analytique ★★	606
100. Un théorème de grandes déviations ★★	613
101. Théorème de Cramér-Chernoff ★★★	617
Développements d'informatique	623
Algorithmique	625
102. Autour du tri rapide ★★	627
103. Tri par tas ★	634
104. Distance de Kendall et tri par insertion ★★	640
105. Tirage aléatoire de population ★★	644
106. Transformée de Fourier rapide ★★	651
107. B-arbres ★★	658
Modèles de calcul	665
108. Complexité du langage des palindromes ★	683

109. Turing-calculable implique μ -récursive ★★	687
110. Caractérisation de RE ★★	692
111. μ -récursive implique λ -définissable ★★	696
112. Théorème de Scott-Curry ★★	700
Théorie des graphes	705
113. Polynôme chromatique ★	717
114. Théorème de Turán ★★	724
115. Formule d'Euler par déchargement ★★	731
116. Problème du voyageur de commerce ★	738
117. Tri topologique ★	743
118. Séquençage ADN et graphe de De Bruijn ★	747
Langages réguliers et algébriques	753
119. Recherche de motif ★★	763
120. Problème de séparation par automate ★	768
121. Universalité d'un automate ★★	774
122. Algorithme de Cocke-Younger-Kasami ★	779
123. Caractérisation de PREMIER en analyse LL(1) ★★	783
Logique et preuves	789
124. Théorème de Cook-Levin ★	791
125. Transformation de Tseitin ★	797
126. 2SAT est NL-dur ★★	802
127. Compacité de la logique propositionnelle ★	807
128. Indécidabilité du problème VALIDFO ★★	812
129. Indécidabilité du problème RELSAT ★★★	817
130. Complétude de la logique de Hoare ★★★	824
131. Équivalence entre deux sémantiques ★★★	830
Compléments d'informatique	835
Schémas algorithmiques	836
Bases de données	839
Sémantiques des langages de programmation	847
Problèmes indécidables	855
Réductions classiques	859
Problèmes NP-complets	863
Annexes	869
Liste des leçons	871
Correspondances entre leçons et développements	881
Bibliographie	897
Index	901

Développement 13 (Lemme de Hensel ★)

a) Considérons un polynôme $P \in \mathbb{Z}[X]$.

(i) Soit $a \in \mathbb{Z}$. Montrer qu'il existe $Q \in \mathbb{Z}[X]$ tel que

$$P(X + a) = P(a) + P'(a)X + Q(X)X^2.$$

(ii) Soient $a, b \in \mathbb{Z}$ et un nombre premier p . Montrer que

$$\forall k \geq 1, \quad P(a + bp^k) \equiv P(a) + P'(a)bp^k \pmod{p^{k+1}}.$$

b) En déduire le lemme de Hensel :

Soit $P \in \mathbb{Z}[X]$. S'il existe $x \in \mathbb{Z}$ tel que

$$P(x) \equiv 0 \pmod{p} \quad \text{et} \quad P'(x) \not\equiv 0 \pmod{p}, \quad (1)$$

alors pour tout $k \geq 1$, il existe $x_k \in \mathbb{Z}$ tel que

$$P(x_k) \equiv 0 \pmod{p^k} \quad \text{et} \quad x_k \equiv x \pmod{p}.$$

Leçons concernées : 120, 121, 126, 144

Le lemme de Hensel est un des résultats centraux de l'analyse p -adique. Ce développement en propose une preuve dans le langage classique de l'arithmétique modulaire. Il s'agit, connaissant la solution d'une équation polynomiale modulo p , d'en tirer récursivement des solutions de l'équation modulo p^k pour tout $k \geq 1$. Cela en fait une illustration de la leçon sur les équations en arithmétique (126) ainsi que sur celle des racines de polynômes (144). Les méthodes sont celles de l'arithmétique modulaire et reposent fortement sur le fait que p soit premier, rendant le développement adéquat pour les leçons 120 et 121.

Correction.

a) On souhaite prouver que X^2 divise le polynôme $P(X+a) - P(a) - P'(a)X$ (cette quantité peut être interprétée comme l'erreur dans la première approximation affine de P). Par linéarité en P de cette expression, il suffit de le prouver le résultat pour les monômes X^n pour $n \geq 1$. On a alors par la formule du binôme de Newton, pour tout $n \geq 1$ et $P = X^n$,

$$\begin{aligned} P(X+a) - P(a) - P'(a)X &= (X+a)^n - a^n - na^{n-1}X \\ &= \sum_{k=0}^n \binom{n}{k} X^k a^{n-k} - a^n - na^{n-1}X = \sum_{k=2}^n \binom{n}{k} X^k a^{n-k}, \end{aligned}$$

et cette quantité est divisible par X^2 puisque que chacun de ses termes l'est. On obtient ainsi le résultat voulu.

b) Par la question précédente, il existe un polynôme $Q \in \mathbb{Z}[X]$ tel que

$$P(X+a) - P(a) - P'(a)X = X^2Q(X).$$

En substituant X par bp^k , pour un $k \geq 1$, il vient

$$\begin{aligned} P(a+bp^k) &= P(a) + P'(a)bp^k + Q(bp^k)b^2p^{2k} \\ &\equiv P(a) + P'(a)bp^k \pmod{p^{k+1}}. \end{aligned}$$

c) On raisonne par récurrence sur $k \geq 1$. Le cas $k = 1$ est l'hypothèse (1). Supposons la propriété vraie pour $k \geq 1$ et prouvons-la au rang $k+1$. Il existe donc, par l'hypothèse de récurrence, $x_k \in \mathbb{Z}$ tel que

$$P(x_k) \equiv 0 \pmod{p^k} \quad \text{et} \quad x_k \equiv x \pmod{p}.$$

On peut alors écrire $P(x_k) = ap^k$ pour un certain entier $a \in \mathbb{Z}$. Si $p \mid a$, alors on a déjà la congruence $P(x_k) \equiv 0 \pmod{p^{k+1}}$ et cela suffit pour avoir la propriété de récurrence au rang $k+1$ en posant $x_{k+1} = x_k$.

Supposons désormais $p \nmid a$. On parcourt la classe de x_k modulo p^k de sorte à trouver des candidats pour x_{k+1} . Autrement dit on considère un élément de la forme $x_{k+1} = x_k + tp^k$ pour un t entier. Il reste à déterminer un tel t de sorte que $P(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$.

Par les questions précédentes,

$$P(x_k + tp^k) \equiv P(x_k) + P'(x_k)tp^k \equiv (a + tP'(x_k))p^k \pmod{p^{k+1}}.$$

On peut alors choisir t qui annule le membre de droite puisque $p \nmid P'(x_k)$. Plus explicitement, $P'(x_k)$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$, on peut donc choisir $t = -aP'(x_k)^{-1}$ où $P'(x_k)^{-1}$ désigne l'inverse dans $\mathbb{Z}/p\mathbb{Z}$, et t convient alors. Ceci achève la récurrence et la preuve du lemme de Hensel.

Commentaires.

◆ L'un des grands thèmes de l'arithmétique et de la théorie des nombres est l'étude des équations diophantiennes. Un outil puissant pour leur étude est la possibilité de les étudier modulo les puissances de nombres premiers p^k et, en s'autorisant des puissances tendant vers l'infini, dans les nombres p -adiques \mathbb{Q}_p , voir Développement 23. L'espoir est de pouvoir en tirer des informations sur les solutions globales, dans \mathbb{Z} ou \mathbb{Q} . Un résultat dans cette direction est le *principe de Hasse*, qui est un principe local-global pour les équations diophantiennes polynomiales de degré deux :

Soit $P \in \mathbb{Z}[X_1, \dots, X_n]$ de degré 2. Alors P admet une racine sur \mathbb{Q} si, et seulement si, il admet des racines dans tous les \mathbb{Q}_p et dans \mathbb{R} .

◆ Toutefois, ce principe cesse d'être vérifié pour les degrés supérieurs. Déjà pour le degré trois (le problème est alors celui de trouver les points rationnels d'une courbe elliptique), certaines équations admettent des solutions locales, modulo tout p^k , et des solutions réelles, mais aucune solution rationnelle. C'est le cas par exemple pour l'équation de Selmer,

$$3x^3 + 4y^3 + 5z^3 = 0.$$

Le lemme de Hensel permet justement de construire des solutions non-triviales de l'équation de Selmer modulo tout p^k , autrement dit dans les corps p -adiques. Toutefois, cette équation n'admet pas de solution rationnelle non-triviale.

◆ Le lemme de Hensel connaît de nombreuses variations. Il peut par exemple être affiné pour prendre en compte le cas où la dérivée première, voire les suivantes, s'annulent modulo p . De plus, le polynôme peut être pris à coefficients dans \mathbb{Z}^p .

◆ Le lemme de Hensel doit être pensé et interprété comme une méthode de Newton p -adique : la preuve en est une mimique modulo p . En particulier, l'idée du lemme de Hensel est de construire des solutions approchées (dans un véritable sens topologique, lorsqu'on se place dans le corps des rationnels p -adiques \mathbb{Q}_p) itérativement. En effet, une solution modulo p^{k+1} est plus précise qu'une solution modulo p^k , par l'injection $\mathbb{Z}/p^k\mathbb{Z} \rightarrow \mathbb{Z}/p^{k+1}\mathbb{Z}$. La limite (pour la topologie p -adique) d'une telle suite de solutions $(x_k)_k$ est un élément $x_\infty \in \mathbb{Z}_p$, dont les x_k doivent justement être pensés comme l'approximation numérique, tronquant x_k à k chiffres dans la décomposition p -adique. Voir [Kob84] pour une ouverture vers l'analyse p -adique.

◆ Le résultat de la question **a)(i)** est une première approximation affine polynomiale, et celui de la question **a)(ii)** une première approximation affine modulaire. Il faut garder en tête que p^k est petit lorsque k grandit (au sens de la norme p -adique), de sorte que l'analogie avec la méthode de Newton et les développements limités conserve tout leur sens.

◆ Le lemme de Hensel admet une pléthore d'applications qui foisonnent dans la littérature de théorie algébrique des nombres. Certaines sont illustrées dans les exercices. Nous précisons ici une application dans l'anneau des entiers p -adiques \mathbb{Z}_p , qui peut très bien être intégrée — comme d'autres exemples — au développement si le temps le permet. On a la conséquence suivante :

Les $u \in \mathbb{Z}_p$ tels que $u \equiv 1 \pmod{p\mathbb{Z}_p}$ sont des puissances n -ièmes dans \mathbb{Z}_p , pour tout $n \geq 1$ non divisible par p .

En effet, appliquons le lemme de Hensel au polynôme $X^n - u$, en commençant avec $X = 1$. On a bien $P(1) = 1 - u \equiv 0 \pmod{p\mathbb{Z}_p}$ et $P'(1) = n \not\equiv 0 \pmod{p\mathbb{Z}_p}$. Il existe donc une solution $\alpha \in \mathbb{Z}$ telle que $\alpha^n = u$ dans \mathbb{Z}_p avec $\alpha \equiv 1 \pmod{p\mathbb{Z}_p}$.

◆ La structure topologique des corps p -adiques \mathbb{Q}_p est très différente de celle des corps archimédiens tels que \mathbb{R} . Par exemple, la boule unité est un anneau où les séries sont convergentes dès que leur terme général tend vers zéro. Voir le Développement 23 pour plus de détails sur les nombres p -adiques.

◆ Nous donnons ici une version plus fine du lemme de Hensel, utilisant la valeur absolue p -adique et les nombres p -adiques :

Soit $P \in \mathbb{Z}[X]$. S'il existe $x \in \mathbb{Z}_p$ tel que

$$P(x) \equiv 0 \pmod{p} \quad \text{et} \quad |P(x)|_p < |P'(x)|_p^2, \quad (2)$$

alors il existe $y \in \mathbb{Z}_p$ tel que

$$P(y) = 0 \quad \text{et} \quad |x - y|_p < |P'(x)|_p.$$

Ainsi, il est possible de se passer de la condition $P'(x) \not\equiv 0 \pmod{p}$ (qui signifie que p ne divise pas $P'(x)$, autrement dit que $|P'(x)|_p \geq 1$) : il suffit de s'assurer que la dérivée $P'(x)$ n'est pas trop proche de zéro.

Questions.

1. Soit p un nombre premier impair. Montrer que si $u \in \mathbb{Z}_p^*$ est un carré modulo p , alors c'est un carré dans \mathbb{Z}_p . Généraliser ce résultat à toute racine simple d'un polynôme unitaire.

2. Trouver les solutions de l'équation

$$5x^3 + x^2 - 1 \equiv 0 \pmod{125}.$$

3. Trouver une solution à l'équation

$$x^3 - 2x \equiv 1 \pmod{125}.$$

4. Montrer que $a \in \mathbb{Z}_p$ est inversible dans \mathbb{Z}_p si et seulement si son coefficient a_0 de degré zéro est inversible sur $\mathbb{Z}/p\mathbb{Z}$.

Indication : appliquer le lemme de Hensel au polynôme $aX - 1$.

5. Montrer que \mathbb{Z}_p contient toutes les racines de $X^{p-1} - 1$.

6. Si m est premier à $p(p-1)$, montrer que tout élément de \mathbb{Q}_p^* admet une racine m -ième dans \mathbb{Q}_p .

7. Montrer que \mathbb{Q}_p ne contient pas de racine primitive p -ième de l'unité si $p > 2$.

8. Montrer que \mathbb{Q}_p n'a pas d'endomorphisme non trivial.

Indication : on peut utiliser les propriétés prouvées aux questions précédentes, notamment constater que les unités de \mathbb{Q}_p ont des racines m -ièmes pour une infinité de valeurs de m .

9. Retrouver la version du lemme de Hensel prouvée dans le développement à partir de la version p -adique donnée dans le dernier commentaire.

Développement 62 (Modèle épidémiologique SIR ★★)

On souhaite étudier la propagation d'une épidémie au sein d'une population de $N > 0$ individus, composée au temps t d'un nombre $S(t)$ d'individus sains (aussi dits *susceptibles*), d'un nombre d'individus $I(t)$ d'individus infectés et d'un nombre $R(t)$ d'individus anciennement infectés, rétablis et immunisés contre la maladie. On modélise cette situation par deux fonctions dérivables notées $S : \mathbb{R}_+ \rightarrow [0, N]$ et $I : \mathbb{R}_+ \rightarrow [0, N]$ qui vérifient le système d'équations différentielles suivant :

$$\begin{cases} \dot{S} &= -\beta \frac{IS}{N} \\ \dot{I} &= \beta \frac{IS}{N} - \gamma I, \end{cases} \quad (1)$$

où \dot{S} (resp. \dot{I}) représente la dérivée de S (resp. I) par rapport au temps et où $\beta, \gamma \in \mathbb{R}_+^*$ sont des paramètres. On pose par ailleurs $R := N - S - I$.

- a) Commenter le formalisme adopté.
- b) Montrer que S, I et R sont bien définies sur \mathbb{R}_+ et à valeurs positives pour tout choix de conditions initiales $S(0), I(0) \in [0, N]$ vérifiant $S(0) + I(0) \leq N$.
- c) On introduit à présent la fonction

$$\begin{aligned} H : \mathbb{R}_+ &\longrightarrow \mathbb{R} \\ x &\longmapsto S(t) \exp\left(\frac{\beta}{\gamma} \frac{R(t)}{N}\right). \end{aligned}$$

- (i) Montrer que H est constante.
- (ii) En déduire que lorsque $R(0) = 0$ et $S(0) > 0$, la *taille totale de l'épidémie* définie par $R_\infty := \lim_{t \rightarrow +\infty} R(t)$ est caractérisée par l'équation

$$(N - R_\infty) \exp\left(\frac{\beta}{\gamma} \frac{R_\infty}{N}\right) = S(0).$$

Leçons concernées : 220,229

Ce développement, complémentaire du Développement 61 qui étudie le modèle SIS, propose d'étudier de façon purement qualitative un modèle épidémiologique déterministe régi par un système d'équations différentielles ordinaires. En cela, il illustre adéquatement les leçons 220 et 229.

Correction.

On utilise dans le développement la notion de *sur-solution* d'une équation différentielle, dont la définition est donnée à la page 312.

- a) On considère que chaque individu infecté de la population entreprend un contact infectieux avec un autre individu choisi au hasard dans la population à un taux temporel β , ce qui occasionne entre les temps t et $t + dt$ un nombre

d'interactions infectieuses entre des individus infectés et des individus sains proportionnel à $\beta I(t) \frac{S(t)}{N} dt$. Dans cette équation, le facteur β traduit à la fois la fréquence des contacts et la proportion (déterministe ou statistique) des contacts entre individus sains et individus infectés qui donne lieu à une infection. Par ailleurs, la guérison des individus infectés intervient à taux γ : une fraction γdt de l'ensemble des $I(t)$ individus infectés au temps t est guérie en une unité de temps infinitésimale dt , ce que traduit la présence du terme $-\gamma I(t)$ dans l'expression de $\dot{I}(t)$. On peut réécrire le système différentiel de façon plus symétrique sous la forme

$$\begin{cases} \dot{S} &= -\beta \frac{IS}{N} \\ \dot{I} &= \beta \frac{IS}{N} - \gamma I \\ \dot{R} &= \gamma I. \end{cases} \quad (2)$$

La différence entre le modèle SIS présenté dans le Développement 61 et le modèle SIR étudié ici réside dans le fait que les individus infectés profitant d'une guérison ne retournent pas au statut sain (compartiment S) mais deviennent *rétablis* (compartiment R), comme on l'a représenté sur la Figure 2.15.

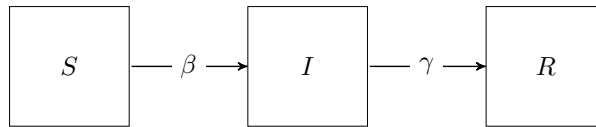


FIGURE 2.15 – Représentation schématique du modèle compartimental SIR. Les nombres apparaissant sur les flèches sont les taux instantanés de passage d'un compartiment à l'autre par individu.

Cette hypothèse est pertinente dans le cas de pathogènes qui provoquent la production d'anticorps assurant une immunité pendant une certaine période chez les sujets remis, comme la rougeole ou la rubéole. Le choix du formalisme (1), dans lequel aucun individu ne quitte le compartiment R , correspond à l'hypothèse d'une immunité complète et non limitée dans le temps.

b) Soient $s_0, i_0 \in [0, N]$ tels que $s_0 + i_0 \leq N$. On cherche à montrer que le système d'équations différentielles (1) admet une unique solution (S, I) définie sur \mathbb{R}_+ tout entier vérifiant $S(0) = s_0$ et $I(0) = i_0$, et que $S + I$ est à valeurs dans l'intervalle $[0, N]$, ce qui montrera que $R := N - S - I$ l'est aussi.

D'après le théorème de Cauchy-Lipschitz, comme l'application

$$F : \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ (s, i) \longmapsto \left(-\beta \frac{is}{N}, \beta \frac{is}{N} - \gamma i \right)$$

est de classe \mathcal{C}^1 , le système d'équations différentielles

$$\begin{cases} f' &= -\beta \frac{fg}{N} \\ g' &= \beta \frac{fg}{N} - \gamma g \end{cases} \quad (3)$$

admet une unique solution maximale (f, g) telle que $f(0) = s_0$ et $g(0) = i_0$. On note $J \subset \mathbb{R}$ son intervalle de vie.

Traisons tout d'abord deux cas particuliers :

- Si $s_0 = 0$, f est constante et égale à 0 et $g(t) = e^{-\gamma t} i_0$ pour tout $t \in J$. On a dans ce cas $J = \mathbb{R}$, donc (S, I) est bien définie comme restriction de (f, g) à \mathbb{R}_+ , est à valeurs dans $[0, N]^2$ et vérifie $S(t) + I(t) = e^{-\gamma t} i_0 \leq i_0 \leq N$ pour tout $t \geq 0$.
- Si $i_0 = 0$, alors (f, g) est la solution constante égale à $(s_0, 0)$. On a dans ce cas $J = \mathbb{R}$, donc (S, I) est bien définie comme restriction de (f, g) à \mathbb{R}_+ , est bien à valeurs dans $[0, N]^2$ et vérifie bien $S + I = s_0 \leq N$.

On suppose donc désormais que $s_0 > 0$ et $i_0 > 0$. Montrons dans un premier temps que (f, g) est à valeurs dans $]0, N[^2$ sur $J \cap \mathbb{R}_+^*$. Pour ce faire, raisonnons par l'absurde et supposons que cela ne soit pas le cas. On pose alors

$$\tau := \inf \left\{ t \in J \cap \mathbb{R}_+^* : (f(t), g(t)) \notin]0, N[^2 \right\}.$$

Remarquons d'emblée que comme $f(0), g(0) \in]0, N[$, par continuité de (f, g) on a $\tau > 0$, et f et g sont à valeurs dans $]0, N[^2$ sur $]0, \tau[$.

On sait que $(f + g)' = -\gamma g$, donc $f + g$ est strictement décroissante sur $[0, \tau]$, si bien que $(f + g)(\tau) < N$ et donc $f(\tau) < N$ et $g(\tau) < N$ puisque $f \geq 0$ et $g \geq 0$.

Par ailleurs, on a $f' = -\beta f \frac{g}{N}$ donc f est une sur-solution de l'équation différentielle $y' = -\beta y$ sur $]0, \tau[$; on en déduit que $f(t) \geq s_0 e^{-\beta t} > 0$ pour tout $t \in [0, \tau]$, donc en particulier que $f(\tau) > 0$.

Enfin, comme $g' = \beta \frac{fg}{N} - \gamma g$, la fonction g est une sur-solution de l'équation différentielle $g' = -\gamma g$ sur $]0, \tau[$, donc $g(t) \geq i_0 e^{-\gamma t}$ pour tout $t \in [0, \tau]$, et en particulier $g(\tau) > 0$.

Ainsi, $(f, g)(\tau) \in]0, N[^2$, ce qui contredit le fait que (f, g) soit continue et $]0, N[^2$ ouvert. La solution (f, g) est donc bien à valeurs dans le pavé $]0, N[^2$ sur $J \cap \mathbb{R}_+^*$.

Comme (f, g) est à valeurs dans $]0, N[^2$ sur $J \cap \mathbb{R}_+^*$, le théorème d'explosion implique bien que l'intervalle de vie J contient \mathbb{R}_+ tout entier, ce qui permet de définir de manière unique les restrictions S et I de f et g à \mathbb{R}_+ . On a par ailleurs montré que f et g (et donc S et I) sont à valeurs positives sur \mathbb{R}_+ . Enfin, pour prouver que $S + I \leq N$, il suffit d'appliquer à nouveau l'argument selon lequel l'égalité $(f + g)' = -\gamma g < 0$ implique que $f + g$ est décroissante sur \mathbb{R}_+ et donc que $S + I$ est à valeurs inférieures à $S(0) + I(0) = s_0 + i_0 \leq N$.

c) (i) On remarque que la première équation du système (1) peut se réécrire sous la forme

$$\forall t \in \mathbb{R}_+, \quad \dot{S}(t) + \frac{\beta}{N} S(t)I(t) = 0.$$

En calculant la dérivée de H par rapport au temps, on obtient alors

$$\begin{aligned} \forall t \in \mathbb{R}_+, \quad \dot{H}(t) &= \left(\dot{S}(t) + \frac{\beta \dot{R}(t)}{\gamma N} S(t) \right) \exp\left(\frac{\beta R(t)}{\gamma N}\right) \\ &= \left(\dot{S}(t) + \frac{\beta}{N} I(t)S(t) \right) \exp\left(\frac{\beta R(t)}{\gamma N}\right) = 0 \end{aligned}$$

grâce à la troisième équation de (2), ce qui montre que H est constante sur \mathbb{R}_+ .

(ii) Notons tout d'abord que d'après le système (2), la fonction S est décroissante et R est croissante, ce qui assure que leurs limites en $+\infty$ existent. Comme on a $S + I + R = N$, il en va donc de même pour I . On note S_∞ , I_∞ et R_∞ les limites respectives de S , I et R en $+\infty$, et on remarque que l'équation $\dot{R} = \gamma I$ implique que $I_\infty = 0$, si bien que $S_\infty + R_\infty = N$.

On suppose désormais que $R(0) = 0$. On a alors $H \equiv H(0) = S(0)$ d'après la question précédente, soit

$$\forall t \in \mathbb{R}_+, \quad S(t) \exp\left(\frac{\beta R(t)}{\gamma N}\right) = S(0)$$

d'où, par passage à la limite,

$$S_\infty \exp\left(\frac{\beta R_\infty}{\gamma N}\right) = S(0),$$

soit encore

$$(N - R_\infty) \exp\left(\frac{\beta R_\infty}{\gamma N}\right) = S(0) \quad (4)$$

qui est bien la relation recherchée. Il est aisé de voir par une étude de fonction que cette équation admet une unique solution sur $[0, N]$, et donc qu'elle caractérise bien R_∞ .

Commentaires.

◆ On pourra à l'envi raccourcir la présentation heuristique effectuée dans la question a) pour libérer le temps nécessaire à l'exposé de la question b), riche en arguments analytiques simples mais précis.

◆ Il est utile d'étudier le Développement 61 ainsi que les commentaires et les questions qui le suivent pour acquérir davantage de recul sur les modèles épidémiologiques compartimentaux et se préparer à satisfaire la curiosité du jury.

◆ Contrairement au cas du processus SIS décrit dans le Développement 61, le comportement asymptotique du processus SIR ne présente pas de phénomène de seuil, et l'équation (4) montre que R_∞ est une fonction strictement croissante et continue du rapport $R_0 := \frac{\beta}{\gamma}$, appelé *nombre de reproduction de base*.

♦ La Figure 2.16 illustre le champ de vecteurs associé au système (1) et peut servir de support visuel au traitement de la question **b**). Notons que le champ de vecteurs n'est pas rentrant sur les bords du triangle $\{(s, i) \in [0, N]^2 : s + i \leq N\}$, c'est-à-dire que les frontières du triangle ne sont pas répulsives pour le système dynamique associé, ce qui contraint à trouver des barrières exponentielles pour f et g dans la question **b**).

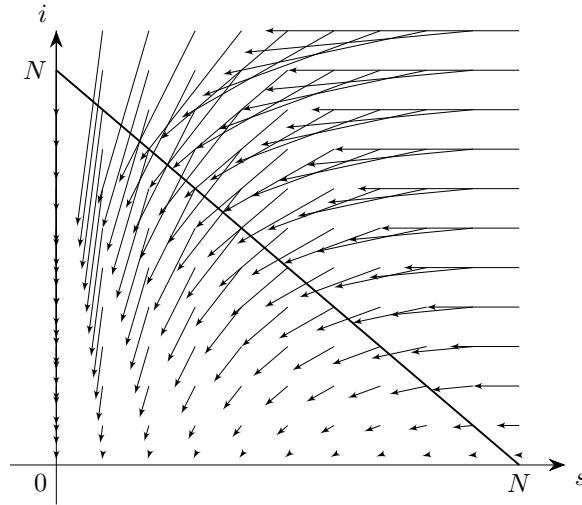
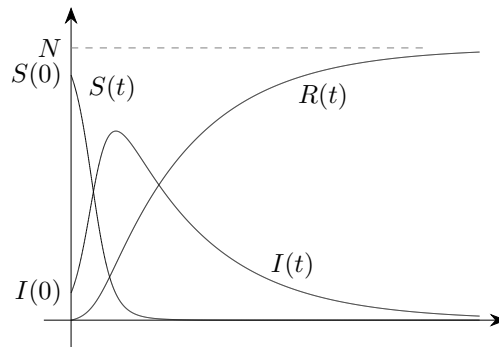


FIGURE 2.16 – Représentation du champ de vecteurs associé au système (1) pour le choix de paramètres $N = 20$ et $\beta = \gamma = 5$.

♦ La Figure 2.17 représente les fonctions S , I et R dans le cas où l'infection est introduite dans la population par un nombre réduit d'individus et où $R_0 := \frac{\beta}{\gamma} > 1$. Dans ce cas, la croissance du nombre d'individus infectés est d'abord exponentielle, puis est limitée par la décroissance du nombre d'individus susceptibles, ce qui donne au graphe de I une allure de courbe logistique (voir Développements 60 et 61). Contrairement à ce que l'on observe dans le cas du modèle SIS (voir Développement 61), l'infection finit par s'éteindre puisque les individus infectés ne redeviennent pas susceptibles mais sont immunisés.

Questions.

1. Supposons que $(i_0, s_0) \in]0, N[^2$ avec $i_0 + s_0 \leq N$. La solution maximale (f, g) étudiée dans la question **b**) est-elle à valeurs dans $]0, N[$ sur J tout entier ?
2. Détailler l'utilisation faite dans la question **b**) du résultat sur les sur-solutions exposé à la page 2.
3. Quelle est la taille finale de l'épidémie si $S(0) = N$?
4. Dans le modèle SIR, montrer que I est décroissante sur \mathbb{R} si et seulement si on a $\beta S(0) - \gamma \leq 0$, et que dans le cas contraire le maximum de I est atteint à l'unique temps $t \geq 0$ tel que $S(t) = \frac{\gamma}{\beta}$.

FIGURE 2.17 – Courbes représentatives des fonctions S , I et R .

5. Détailler l'étude de fonction permettant de conclure dans la question **c**).
6. Pourquoi le réel R_∞ est-il nommé *taille totale de l'épidémie*?
7. Proposer un algorithme d'approximation de R_∞ .
8. Adapter le résultat de la question **c**) au cas où $R(0) > 0$. Est-il toujours pertinent de parler de R_∞ comme de la *taille totale de l'épidémie* dans ce cas?
9. Quel serait l'effet sur la taille totale de l'épidémie d'une politique de vaccination portant sur une proportion $\lambda \in [0, 1]$ des individus initialement susceptibles?
10. En utilisant l'équation (4) et le tableau de variations de la fonction H , déterminer le rôle des coefficients β et γ sur la valeur de R_∞ et interpréter ce résultat.
11. Proposer une modélisation probabiliste d'un phénomène épidémique inspirée du modèle SIR.

Développement 115 (Formule d'Euler par déchargement ★★)

Soit $G = (S, A)$ un graphe simple planaire. On fixe un plongement de G dans le plan, et on note $q(G) = |S| - |A| + |F|$ où F est l'ensemble des faces de G . Le but de cet exercice est de montrer que $q(G) = 2$ et de fournir quelques applications de ce résultat.

a) **Formule d'Euler.**

(i) Montrer qu'il suffit de prouver le résultat dans le cas où G est une triangulation, c'est-à-dire quand toutes les faces de G sont des triangles.

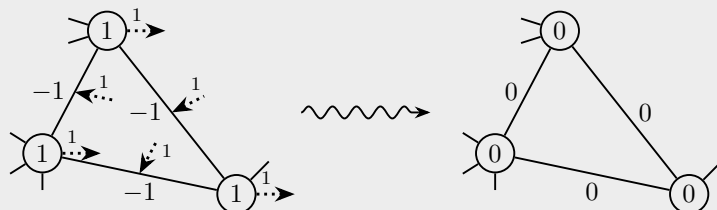
On suppose maintenant que G est triangulé.

(ii) Montrer qu'il existe un plongement de G dans le plan où aucune arête n'est horizontale. En particulier, pour tout sommet s (resp. arête a), il existe une unique face à droite de s (resp. a)⁴⁰.

(iii) On associe un poids à chaque sommet, arête et face de G en définissant une fonction $\omega : S \cup A \cup F \rightarrow \mathbb{R}$ telle que

$$\omega(x) = \begin{cases} 1 & \text{si } x \in S \cup F, \\ -1 & \text{si } x \in A. \end{cases}$$

On déplace ensuite le poids selon la règle suivante : chaque sommet transfère un poids de 1 à la face à sa droite et chaque arête reçoit un poids de 1 depuis la face à sa droite, comme illustré ci-après.



Calculer le poids final de chaque face et en déduire que $q(G) = 2$.

b) **Applications.**

(i) En déduire que pour tous $a, b \in \mathbb{R}$, on a :

$$\sum_{s \in S} (a \cdot d(s) - 2(a + b)) + \sum_{f \in F} (b \cdot \ell(f) - 2(a + b)) = -4(a + b),$$

où $d(s)$ est le degré du sommet s et $\ell(f)$ la longueur de la face f .

(ii) Montrer qu'il n'y a que 5 polyèdres réguliers convexes.

(iii) Soit G un fullerène, i.e. un graphe planaire dont tous les sommets sont de degré 3 et dont les faces ont pour longueur 5 ou 6. Montrer que G a exactement 12 faces pentagonales.

Leçons concernées : 190, 925

40. Cette face peut être définie formellement comme l'unique face contenant un segment horizontal suffisamment petit dont l'extrémité gauche est s ou le milieu de a .

On s'intéresse ici à un grand classique de théorie des graphes : la formule d'Euler pour les graphes planaires. Ce résultat et ses conséquences permettent d'illustrer la leçon 925, en montrant que les graphes planaires possèdent des propriétés structurelles fortes. La formule d'Euler, quant à elle, connaît un très grand nombre de démonstrations et d'applications en combinatoire, ce qui justifie une inclusion dans la leçon 190. On a choisi ici une méthode dite « par déchargement », très utilisée en théorie structurelle des graphes. Le fonctionnement de cette méthode sera développé dans les questions en fin d'exercice.

Correction.

a) (i) Supposons que $q(T) = 2$ pour toute triangulation planaire T . Comme G est simple, toutes ses faces ont taille au moins 3. On peut construire itérativement une triangulation en ajoutant des arêtes à G selon la procédure suivante. Tant que G possède une face non triangulaire, on ajoute une arête séparant cette face en deux. La quantité $q(G)$ reste inchangée car on ajoute une face et une arête. Lorsque cette procédure se termine, le graphe H obtenu est une triangulation. On a alors $q(G) = q(H) = 2$. On peut donc supposer que G est triangulé.

(ii) Pour $\theta \in [0, 2\pi[$, on note r_θ la rotation de \mathbb{R}^2 de centre $(0, 0)$ et d'angle θ . Considérons les images du plongement de G par r_θ .

Pour chaque arête a de G , son image par r_θ est horizontale pour seulement deux valeurs de θ . Il existe ainsi au plus $2|A|$ valeurs de θ telles que l'image par r_θ du plongement de G contienne une arête horizontale. L'intervalle $[0, 2\pi[$ étant infini, on peut choisir une valeur de θ pour laquelle cette situation n'arrive pas.

(iii) Soit f une face de G . Comme G est une triangulation, f est un triangle. Comme il n'y a pas d'arête horizontale dans le plongement de G choisi, il existe exactement un sommet x du plongement de f d'ordonnée maximum et un sommet y d'ordonnée minimum. Soit z le troisième sommet de f . On distingue deux cas selon que f est la face extérieure f_{ext} ou une face interne.

- Supposons que f est une face interne. Si (le plongement de) z est à gauche (du plongement) de xy , alors f reçoit 1 par z et donne 1 à xz et yz . Sinon, f donne seulement 1 à xy . Dans les deux cas, f perd un poids de 1 et son poids final est 0.

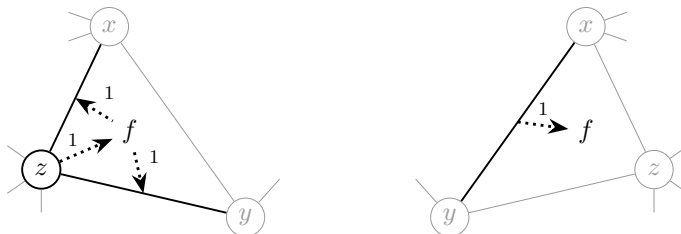


FIGURE 3.21 – Déchargement : cas d'une face interne.

- Supposons que $f = f_{ext}$. Si z est à gauche de xy , f reçoit 1 de x et y et donne 1 à xy . Sinon f reçoit 1 de la part de x, y et z et donne 1 à xz et yz . Dans les deux cas, f reçoit un poids de 1 et son poids final est 2.

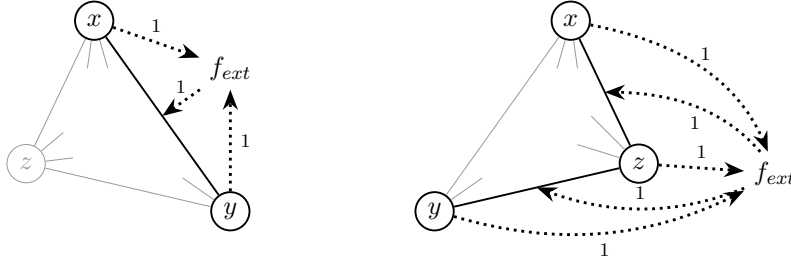


FIGURE 3.22 – Déchargement : cas de la face externe.

La somme des poids était initialement

$$\sum_{s \in S} 1 + \sum_{a \in A} (-1) + \sum_{f \in F} 1 = |S| - |A| + |F| = q(G).$$

La somme des poids finaux est

$$\sum_{s \in S} 0 + \sum_{a \in A} 0 + \sum_{f \in F} 2\delta_{f, f_{ext}} = 2.$$

Comme le déplacement des poids a préservé le poids total, on obtient finalement le résultat recherché, à savoir $q(G) = 2$.

b) (i) Par linéarité de la somme, on remarque qu'il suffit de prouver que :

$$a \sum_{s \in S} d(s) + b \sum_{f \in F} \ell(f) = 2(a + b)(2 - |S| - |F|).$$

On utilise tout d'abord une permutation de sommes :

$$\sum_{s \in S} d(s) = \sum_{s \in S} \sum_{\substack{a \in A \\ s \in A}} 1 = \sum_{a \in A} 2 = 2|A| \tag{1}$$

car chaque arête de A apparaît dans les sommes correspondant à exactement deux sommets (à savoir ses extrémités). De manière similaire, on obtient que

$$\sum_{f \in F} \ell(f) = 2|A|. \tag{2}$$

Ainsi, on en déduit que

$$a \sum_{s \in S} d(s) + b \sum_{f \in F} \ell(f) = 2(a + b)|A| = 2(a + b)(|S| + |F| - 2)$$

par le résultat de la question précédente.

(ii) À partir d'un solide S , on peut construire un graphe connexe simple G qui utilise les mêmes sommets et arêtes. En utilisant une projection stéréographique, on peut obtenir un plongement de G dans \mathbb{R}^2 , qui est donc planaire. Par définition, si S est un solide régulier, alors toutes ses faces sont des polygones réguliers de même taille, et tous ses sommets sont incidents au même nombre d'arêtes. Cela se traduit par le fait que tous les sommets de G ont même degré $q \geq 1$ et que toutes les faces de G ont même degré p . De plus, on a $p \geq 3$ car les faces de S sont au moins triangulaires. Si $q = 1$, alors G ne contient qu'une arête, et si $q = 2$, comme G est simple alors G est un cycle. Or G est construit à partir d'un solide donc il n'est ni réduit à une arête ni un cycle. Il reste donc le cas $q \geq 3$.

On utilise à nouveau les équations (1) et (2), qui fournit $q|S| = 2|A| = p|F|$. En réinjectant ces égalités dans la formule d'Euler, on obtient

$$\frac{1}{q} + \frac{1}{p} = \frac{1}{|A|} + \frac{1}{2}.$$

Comme p, q et $|A|$ sont des entiers positifs, cette équation n'a qu'un nombre fini de solutions :

- Si $p = q = 3$, alors $|A| = 6$, donc $|F| = |S| = 4$. Ceci correspond à un unique graphe, la clique sur 4 sommets. Le solide associé est le tétraèdre.
- Si $p = 4$ et $q = 3$, on obtient $|A| = 12$, d'où $|F| = 6$ et $|S| = 8$, ce qui correspond au cube.
- Si $p = 5$ et $q = 3$, on obtient $|A| = 30$, d'où $|F| = 12$ et $|S| = 20$, ce qui correspond au dodécaèdre.
- Si $p = 3$ et $q = 4$, on obtient $|A| = 12$, d'où $|F| = 8$ et $|S| = 6$, ce qui correspond à l'octaèdre.
- Si $p = 3$ et $q = 5$, on obtient $|A| = 30$, d'où $|F| = 20$ et $|S| = 12$, ce qui correspond à l'icosaèdre.

Dans chacun des cas, on a un unique candidat pour G , et il existe bien un solide régulier d'où G est issu. Il existe donc bien cinq types de solides réguliers convexes (voir Figure 3.23).

(iii) Soit G un fullerène, et notons f_5 (resp. f_6) son nombre de faces pentagonales (resp. hexagonales). En utilisant à nouveau les équations (1) et (2), on obtient

$$3|S| = 2|A| = 5f_5 + 6f_6.$$

Par la formule d'Euler, on a enfin

$$\begin{aligned} 12 &= 6|S| - 6|A| + 6|F| \\ &= 2 \times (5f_5 + 6f_6) - 3 \times (5f_5 + 6f_6) + 6 \times (f_5 + f_6) \\ &= f_5. \end{aligned}$$

Ainsi, G a bien 12 faces pentagonales, quelle que soit la taille de G .

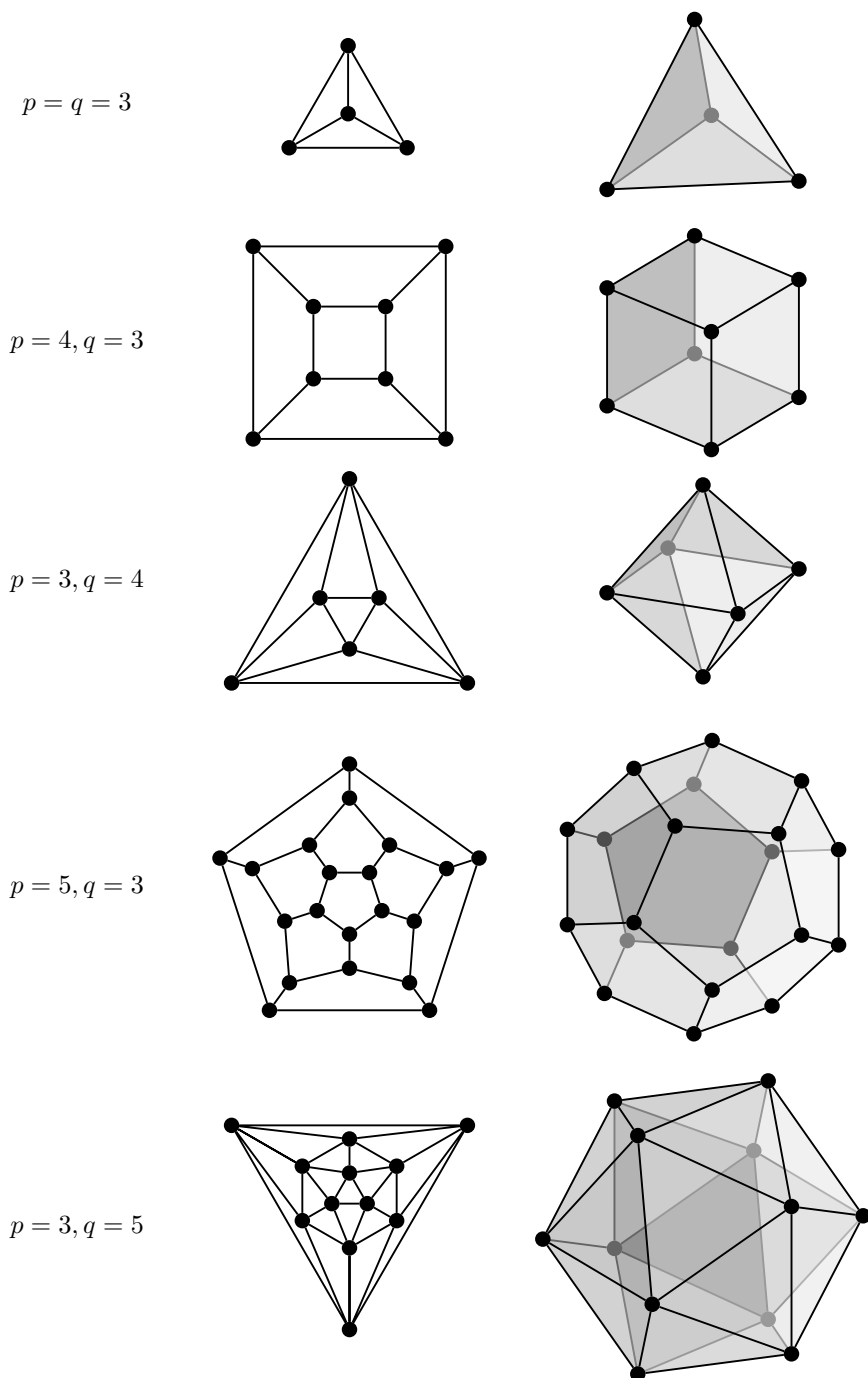


FIGURE 3.23 – Les graphes des solides de Platon.

Commentaires.

◆ La définition d'un plongement donnée en page 712 utilise des segments de droite pour les arêtes. Une autre définition classique utilise des chemins non nécessairement rectilignes, mais il s'avère que les deux définitions sont équivalentes : c'est le théorème de Fary. On utilise de manière implicite ce fait en question **a)(i)** quand on triangule la face extérieure.

◆ On peut étendre la définition de plongement à d'autres surfaces compactes même non orientables. On peut montrer en utilisant des arguments similaires mais plus évolués que la quantité $|S| - |A| + |F|$ reste un invariant qui dépend du genre de la surface considérée.

◆ La formule d'Euler peut être démontrée de nombreuses manières, par exemple par récurrence sur les sommets, arêtes ou encore faces.

◆ La méthode de déchargement présentée ici a de nombreuses applications. Elle est notamment utilisée pour montrer que tout graphe d'une certaine famille (par exemple planaire) contient certaines configurations. Ces résultats sont alors utilisés pour prouver inductivement des théorèmes de coloration ou de décomposition de graphes (voir les questions ci-après pour un exemple). C'est par exemple la base du célèbre théorème des quatre couleurs⁴¹.

◆ Le résultat de l'équation (1) est un grand classique de théorie des graphes et est connu comme le « lemme des poignées de main ».

◆ La formule de la question **b)(i)** peut aussi s'obtenir par déchargement, en donnant un poids initial de $-2(a + b)$ aux sommets et aux faces, et de $2(a + b)$ aux arêtes. On redistribue alors le poids de chaque arête en donnant a à chaque sommet qu'elle contient, et b à chaque face incidente.

◆ Les fullerènes trouvent des applications en chimie du carbone et en biologie : c'est notamment la structure des nanotubes de carbones et de certains virus. Lorsque les faces pentagonales sont deux à deux disjointes, le résultat de la question **b)(iii)** montre que le fullerène en question a au moins 60 sommets. Il existe un tel fullerène (c'est le graphe aisément reconnaissable à la surface des ballons de football).

◆ L'étude des graphes planaires a donné lieu à de nombreux résultats et conjectures. Leur structure permet par exemple d'obtenir de meilleurs algorithmes pour résoudre ou approximer les problèmes classiques de théorie des graphes. Un des exemples les plus extrêmes est fourni par la détermination de la plus grande clique, qui est un problème NP-complet en général, mais résoluble en temps polynomial dans les graphes planaires.

◆ L'équation de la question **b)(ii)** reliant p, q et $|A|$ est à rapprocher de l'équation fondamentale du Développement 45, qui détermine aussi les (groupes d'isométries des) polyèdres réguliers. En particulier, les cinq cas distingués ici correspondent aux trois cas présentés dans ce développement (quitte à échanger p et q). Cet échange peut se justifier grâce à la notion de *graphe dual* : le dual d'un graphe planaire G est le graphe dont les sommets sont les faces de G , et deux sommets

41. Tout graphe planaire admet une coloration propre à quatre couleurs.

sont adjacents si les faces correspondantes partagent une arête dans G . On se rend facilement compte du fait que cette opération échange p et q , et on retrouve le résultat établissant que le cube et l'octaèdre (resp. l'icosaèdre et le dodécaèdre) sont duaux.

Questions.

1. Montrer que la procédure de triangulation décrite en question **a**)(i) se termine.
2. Montrer que si S est un polyèdre régulier, il existe une projection stéréographique produisant un plongement planaire du graphe associé.
3. Montrer que tout graphe connexe simple dont tous les sommets ont degré 2 est un cycle.
4. Montrer que dans un graphe planaire, on a

$$\sum_{f \in F} \ell(f) = 2|A|.$$

5. Justifier que l'équation

$$\frac{1}{q} + \frac{1}{p} = \frac{1}{|A|} + \frac{1}{2}$$

n'admet qu'un nombre fini de solutions entières.

6. Dans la question **b**)(ii), où est utilisée la convexité des solides réguliers considérés?
7. Montrer la formule de la question **b**)(i) avec un argument de déchargement.
8. Quelle est la complexité du problème consistant à décider si un graphe est planaire?
9. Montrer que si $G = (S, A)$ est planaire, $|A| \leq 3|S| - 6$.
10. Montrer qu'il existe un nombre fini de graphes planaires de degré maximum 3 et dont toutes les faces ont taille au plus 5.
11. Montrer que tout graphe planaire a un sommet de degré au plus 5. En déduire que tout graphe planaire admet une coloration propre à 6 couleurs.
12. Améliorer le résultat précédent avec 5 couleurs. Donner un algorithme polynomial pour trouver une telle coloration.
Indication : si un graphe planaire G contient un sommet s de degré 5, on pourra montrer que le graphe obtenu à partir de $G - s$ en identifiant deux sommets non adjacents de $N_G(s)$ bien choisis est planaire.
13. Soit G un graphe planaire de degré minimum 3. Montrer que G contient un sommet de degré 3 sur une face de taille au plus 5 ou bien un sommet de degré au plus 5 sur un triangle.

	01	02	03	04	05	06	07	08	20	21	22	23	25	26	41	42	44	50	N° dvp.
Heisenberg				1			1												1
Dixon			1	1		1													2
Gén. $SL_2(\mathbb{Z})$	1					1		1	1		1					1		1	3
CNS transpo.					1			1											4
Groupes trans.	2			2	2			2											5
Landau	2			2	2					2									6
Permut. commutant	2			2	2														7
Groupes pq	1		1	1															8
Groupes 105	3		3	3						3									9
Caractères diédraux	1			1			1	1											10
Burnside	3		3	3			3											3	11
Cohn										1					1			1	12
Hensel									1	1				1				1	13
Chevalley-Waring												2						2	14
d'Alembert-Gauss													1		1			1	15
Krull											2								16
Cyclicité \mathbb{F}_p^*				2			2	2		2									17
Autom. \mathbb{F}_q											1	1			1				18
Morphismes cyclo.		1							1	1	1		1		1		1		19
Autom. \mathbb{C}													3		3		3		20
Artin													3		3		3		21
Entier carré-cube											2			2		2			22
Val. abs. \mathbb{Q}										2	2								23
Fermat cyclo.		3							3	3	3			3		3	3		24
Waring mod.				3				3	3	3				3					25
Sherman-Morrison																			26
Quaternions	1	1				1							1						27
Schwartz-Zippel										2							2		28
Faddeev																	1		29
Consv. det						1												1	30
Consv. rg																			31
Chebotarev		3								3							3		32
Image exp.																			33
Décomp. polaire						1												1	34
	01	02	03	04	05	06	07	08	20	21	22	23	25	26	41	42	44	50	N° dvp.

TABLE A.1 – Tableau de correspondance des leçons — Algèbre (1/4).
 Les leçons sont numérotées **1xx** mais ne font apparaître que la valeur de **xx**.
 Le numéro dans les cases correspond à la difficulté.

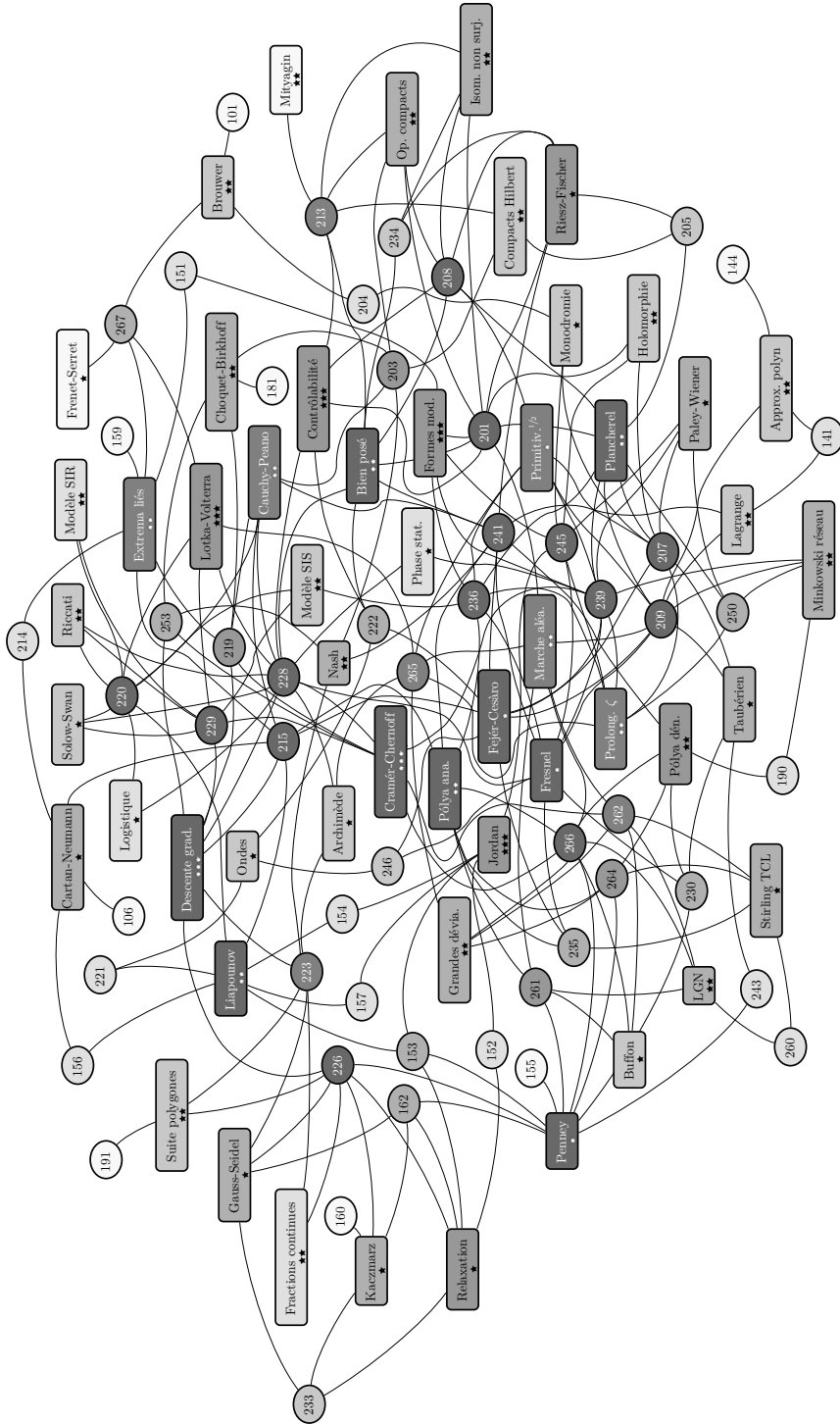


FIGURE A.2 – Graphe de correspondance des développements — Analyse.