

Université de Montréal

**La propriété de Northcott de fonctions zêta sur des
familles d'extensions**

par

Xavier Généreux

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en mathématiques

20 août 2023

© Xavier Généreux, 2023

Université de Montréal

Faculté des arts et des sciences

Ce mémoire intitulé

La propriété de Northcott de fonctions zêta sur des familles d'extensions

présenté par

Xavier Généreux

a été évalué par un jury composé des personnes suivantes :

Dimitrios Koukoulopoulos

(président-rapporteur)

Matilde Lalin

(directeur de recherche)

Andrew Granville

(membre du jury)

Résumé

En mathématiques, une hauteur est une fonction utilisée pour mesurer la complexité d'un objet. Lorsqu'uniquement un nombre fini d'éléments possèdent une hauteur bornée, on dit alors que cette hauteur possède la propriété de Northcott. Un des intérêts de cette propriété est que les hauteurs la possédant peuvent être utilisées pour distinguer des sous-ensembles finis d'une famille infinie d'objets. Récemment, Pazuki et Pengo [47] ont étudié la propriété de Northcott où la hauteur considérée était l'évaluation de fonctions zêta de Dedekind en un entier n .

Ce mémoire contient, en premier lieu, une étude similaire sur l'évaluation de fonctions zêta de corps de fonctions. Ce premier article pousse cette réflexion sur un plus grand domaine en considérant l'évaluation sur n'importe quel point s du plan complexe au lieu de valeurs entières n . On y montre que pour les points appartenant à une certaine région $\{s \in \mathbb{C} : \operatorname{Re}(s) < \sigma_0\}$ où $0 < \sigma_0 < 1/2$, la hauteur considérée possède la propriété de Northcott et que ceux qui appartiennent à la région $\{s \in \mathbb{C} : \operatorname{Re}(s) > 1/2\}$ ne la possèdent pas. En prenant comme contexte les résultats du premier article, nous retournerons ensuite, dans un deuxième article, à la première situation des fonctions zêta de Dedekind pour étudier la question sur ce domaine étendu. Les résultats sur la propriété de Northcott sont différents et on trouve que le scénario sur les corps de fonctions est taché de disques non Northcott autour des entiers négatifs. Ces deux articles seront précédés d'une introduction à la théorie des corps de nombres et des corps de fonctions jusqu'à la définition de leur fonction zêta respective. Enfin, nous incluerons également une discussion des différences entre ces deux théories qui culminera à des définitions alternatives de leur fonction zêta. Ultiment, cette introduction pourvoira tous les outils nécessaires pour attaquer la question de la propriété de Northcott abordée dans les articles.

Mots-clés: Théorie des nombres; Propriété de Northcott; Fonctions zêta; Corps de nombres; Corps de fonctions

Abstract

In mathematics, heights are functions used to measure the complexity of an object. When only a finite number of elements have a bounded height, we say that this height has the Northcott property. One of the advantages of this property is that the heights possessing it can be used to distinguish finite subsets of an infinite family of objects. Recently, Pazuki and Pengo [47] studied the Northcott property where the height considered was the evaluation of Dedekind zeta functions at an integer n .

This thesis contains, first of all, an article describing a similar study on the evaluation of zeta functions of function fields. This first article pushes this reflection on a larger domain by considering the evaluation on any point s of the complex plane instead of integer values n . We show that for points belonging to a certain region $\{s \in \mathbb{C} : \operatorname{Re}(s) < \sigma_0\}$ where $0 < \sigma_0 < 1/2$, the considered height has the Northcott property, while for those belonging to the region $\{s \in \mathbb{C} : \operatorname{Re}(s) > 1/2\}$, the height does not have the Northcott property. Taking as context the results of the first article, we will then return, in a second article, to the initial situation of Dedekind zeta functions to study the question on this extended domain. The results on the Northcott property are different and the scenario on function fields is found to be stained with non-Northcott disks around the negative integers. These two articles will be preceded by an introduction to the theory of number fields and function fields up to the definition of their respective zeta functions. Finally, we will also include a discussion of the differences between these two theories culminating in alternative definitions of their zeta function. Ultimately, this introduction will provide all the tools necessary to attack the questions on the Northcott property discussed in the articles.

Keywords: Number Theory; Northcott property; Zeta functions; Number fields; Function fields

Table des matières

Résumé	5
Abstract	7
Liste des tableaux	13
Liste des figures	15
Remerciements	17
Chapitre 1. Introduction	19
1.1. Les corps de nombres	22
1.1.1. Extension des rationnels	22
1.1.2. Outils et définitions	27
1.1.3. Le point de vue des idéaux	30
1.1.4. Les premiers dans les corps de nombres	34
1.1.5. La théorie de Minkowski	37
1.1.6. La fonction zêta de Dedekind	40
1.2. L'analogie des corps de fonctions	42
1.2.1. Propriétés de $\mathbb{F}_q[t]$	42
1.2.2. Les corps algébriques de fonctions	44
1.2.3. Diviseurs	48
1.2.4. Les conjectures de Weil	49
1.3. Une question de définition	53
1.3.1. La théorie des valuations	53
1.3.1.1. <i>Les corps de fonctions</i>	54
1.3.1.2. <i>Les corps de nombres</i>	55

1.3.2.	Les diviseurs d'Arakelov et leur fonction zêta.....	56
1.3.3.	S-Anneaux des entiers et S-fonctions-zêta.....	60
1.3.3.1.	<i>Exemple: Les extensions quadratiques</i>	62
1.3.3.2.	<i>S-fonction-zêta</i>	62
1.4.	Les hauteurs et la propriété de Northcott.....	64
1.4.1.	La propriété de Northcott de fonctions zêta sur des familles d'extensions ..	68
Chapitre 2. On the Northcott property of zeta functions over function fields		73
2.1.	Introduction.....	74
	Acknowledgements.....	77
2.2.	Some background on $\zeta_K(s)$	77
2.3.	The left side of the critical strip.....	80
2.4.	The right side of the critical strip.....	83
2.5.	Inside the critical strip.....	87
2.5.1.	The Northcott property at the pole $s = 1$	87
2.5.2.	The segment of the real line inside the right side of the critical line.....	88
2.5.3.	The Northcott property at $s = 1/2$	89
2.5.4.	The Northcott property in the right of the critical line.....	90
2.5.5.	The Northcott property at $\text{Re}(s) = 1$	92
Chapitre 3. On the Northcott property of Dedekind zeta functions		99
3.1.	Introduction.....	100
	Acknowledgements.....	107
	Disclosure statement.....	107
	Data availability statement.....	107
3.2.	Some background.....	107
3.3.	The right side of the critical strip.....	110
3.4.	The left side of the critical strip.....	111

3.4.1.	Away from the real line	116
3.4.2.	The neighborhood of the real line and away from the integers	118
3.4.2.1.	The negative even integers	119
3.4.2.2.	The negative odd integers	122
3.4.3.	The neighborhood of the negative integers	125
3.4.4.	The case of $\sigma_0 \leq \sigma \leq 0$	127
3.5.	Inside the critical strip	129
3.5.1.	The case of $s = 1$	129
3.5.2.	The case of $1/2 < \sigma < 1$	131
3.5.3.	The case of $\text{Re}(s) = 1$	134
Appendix A.	The left side neighborhood of zero	135
	An application of Proposition A.0.5	139
Conclusion	147
Références bibliographiques	149

Liste des tableaux

A.1	Tableau comparant différents résultats autour des entiers négatifs	141
-----	--	-----

Liste des figures

1.1	Image dépeignant le Théorème principal du Chapitre 2.....	21
1.2	Image dépeignant le Théorème principal du Chapitre 3.....	22
1.3	Graphique donnant un exemple de la notion d'effectivité sur un corps de nombres.	58
1.4	Image dépeignant le Théorème principal du Chapitre 2.....	70
1.5	Image dépeignant le Théorème principal du Chapitre 3.....	71
2.1	Image dépeignant le Théorème principal du Chapitre 2.....	75
3.1	Image dépeignant le Théorème principal du Chapitre 2.....	101
3.2	Image dépeignant le Théorème principal du Chapitre 3.....	102
3.3	Illustration de la propriété Northcott vérifiée par les trois premiers éléments du Théorème 3.1.1.	104
3.4	Illustration de l'écart entre les théorèmes 3.1.1 et 3.1.4. Comme d'habitude, la propriété Northcott est vérifiée dans la zone bleue (cela inclut le centre du cercle), tandis que la zone rouge est connue pour être non-Northcott.	106
3.5	Illustration comparant la condition (3.4.10) dans la preuve du Théorème 3.4.9 (en bleu) et la condition (3.4.1) provenant de la Proposition 3.4.4 (en gris).	117
3.6	Illustration de la condition (3.4.10) dans la preuve du Théorème 3.4.9.	118
3.7	Le rayon minimal nécessaire pour couvrir la bande restante $ \tau \leq \tau_0$ est $\sqrt{\frac{1}{4} + \tau_0^2}$. ..	119
3.8	Représentation graphique de la condition non-Northcott (3.4.17) près de $\sigma = -1$. ..	125
3.9	Représentation graphique des points respectant la condition (3.4.1) sur la propriété de Northcott (en bleu).	128
3.10	Représentation graphique des conditions (3.4.23) et (3.4.24).	130

A.1	Représentation de la limite de la condition (3.4.1) et du cercle de centre 0.5 et de rayon 1.1 employé dans le lemme A.0.1.....	136
A.2	Comparaison entre le théorème 3.4.27 (violet), la remarque A.0.6 (vert) et la courbe par morceaux trouvée avec les méthodes de cette section (bleu).	142
A.3	Comparaison entre le théorème 3.4.27 (violet), la remarque A.0.7 (vert) et la courbe par morceaux trouvée avec les méthodes de cette section (bleu).	143
A.4	Calcul assistée par ordinateur de la frontière pour l'intervalle $(-1.2, -0.8)$. Tout ce qui se trouve au-dessus de la ligne bleue est Northcott.....	144
A.5	Calcul assistée par ordinateur de la frontière pour l'intervalle $(-0.8, -0.5)$. Tout ce qui se trouve au-dessus de la ligne bleue est Northcott.....	145

Remerciements

J'aimerais tout simplement remercier ma directrice, Matilde Lalín. Son support, tout au long des deux dernières années, est la réelle fondation de mes apprentissages. Merci pour tous les outils, conseils, avertissements et encouragements. Je chéris chacun d'entre eux.

Chapitre 1

Introduction

Ce mémoire met en relation deux concepts:

Les hauteurs sont un outil mathématique utilisé pour mesurer la taille ou la complexité d'un objet. La *propriété de Northcott* est une caractéristique associée à certaines hauteurs qui stipule que pour un objet donné, quelle que soit sa mesure de complexité, seul un nombre fini d'objets se situent «en dessous».

Les *corps de nombres* sont l'objet d'étude de la théorie algébrique des nombres. En termes simples, ils sont des extensions des nombres rationnels \mathbb{Q} auxquels on rajoute des racines de polynômes, comme $\sqrt{2}$. À chacune de ces extensions est associée ce qu'on appelle leur fonction zêta de Dedekind qui est d'importance particulière puisqu'elle emmagasine énormément d'informations par rapport à l'arithmétique de leur corps de nombres. Ces fonctions généralisent la fonction zêta de Riemann qui fascine à la fois néophytes et experts par ses caractéristiques surprenantes et sa nature indomptable.

La question la plus connue associée à la fonction zêta de Riemann est sans doute l'hypothèse de Riemann. Ce défi motiva l'élaboration d'une multitude de théories, toutes avec l'objectif d'apprivoiser ce dragon. Parmi elles, la théorie des *corps de fonctions* se présente comme une sœur bienveillante aux corps de nombres. Débordante de similitudes mais avec un avantage clé: de nombreux résultats sont plus facilement démontrés dans le cadre des corps de fonctions. Justement, bien que sa preuve n'avait rien de facile, c'est pendant les années 40 qu'André Weil maîtrisa l'hypothèse de Riemann sur les corps de fonctions.

L'idée de Pazuki et Pengo [47] était d'utiliser l'évaluation à un entier n de la valeur absolue de fonctions zêta de Dedekind comme mesure de complexité pour un corps de nombres

K . Plus spécifiquement, ils étudièrent la hauteur

$$[K] \mapsto |\zeta_K^*(n)| \text{ où } n \in \mathbb{Z} \text{ et } \zeta_K^*(n) = \lim_{t \rightarrow n} \frac{\zeta_K(t)}{(t-n)^{\text{ord}_n(\zeta_K(t))}.$$

Ici, ζ_K est la fonction zêta de Dedekind, mentionnée plus haut, qu'on détaillera à la Section 1.1.6. Aux fins de cette introduction, notons simplement que si $s \in \mathbb{C}$ n'est pas un zéro de ζ_K et fait partie de son domaine, alors $\zeta_K^*(s) = \zeta_K(s)$. Finalement, $[K]$ représente la classe d'isomorphisme du corps de nombres K . Cette considération est prise pour rassembler tous les corps qui sont «algébriquement les mêmes» dans une seule boîte pour éviter de les compter plusieurs fois.

Dans leur article, Pazuki et Pengo montrent le résultat suivant:

Théorème 1.0.1. [47] *Soit $n \in \mathbb{Z}$. Si $n \leq 0$, alors il existe seulement un nombre fini de classes d'isomorphismes de corps de nombres $[K]$ tels que $|\zeta_K^*(n)| \leq B$, et ce, peu importe $B \in \mathbb{R}_{>0}$. C'est-à-dire que la hauteur $[K] \mapsto |\zeta_K^*(n)|$ possède la propriété de Northcott. Si $n \geq 1$ alors la hauteur ne possède pas la propriété de Northcott.*

La question étant résolue sur les corps de nombres pour l'ensemble des $\mathbb{Z} \subset \mathbb{C}$, une question proposée par Wanlin Li fut de considérer le problème analogue sur les corps de fonctions.

Problème 1.0.2. Considérons l'ensemble

$$S_{q,B,s} = \{[K] : |\zeta_K^*(s)| \leq B\},$$

où $[K]$ représente la classe d'isomorphismes de corps de fonctions avec \mathbb{F}_q comme corps des constantes et ζ_K la fonction zêta associée. Cette fonction est analogue à la fonction zêta de Dedekind sur les corps de nombres. Elle sera introduite en détails à la Section 1.2.4. Maintenant, on a le même objectif: En fixant q une puissance de premier et $s \in \mathbb{C}$, l'ensemble $S_{q,B,s}$ est-il fini pour tout $B \in \mathbb{R}_{>0}$? Dans ce cas, on dit que la propriété de Northcott est respectée en s . Sinon, on appelle un tel point non Northcott.

Notons qu'ici, les points d'évaluation sont pris parmi l'entièreté du plan complexe \mathbb{C} au lieu de \mathbb{Z} . Ce problème est le sujet d'étude du Chapitre 2. Pour une impression qualitative des résultats du Chapitre 2, le lecteur est invité à consulter la Figure 1.1. Consulter le Théorème 1.4.16 pour plus de détails.

Après avoir étudié la question sur les corps de fonctions, une question naturelle fut de tenter de généraliser le Théorème 1.0.1 en considérant n'importe quel élément $s \in \mathbb{C}$ comme point d'évaluation. Nous étudierons donc la généralisation suivante de ce problème:

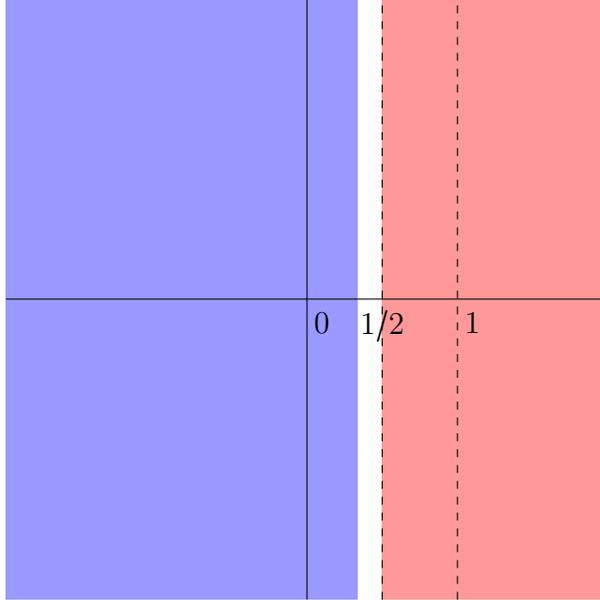


Fig. 1.1. Pour le corps de base \mathbb{F}_q , où q est une puissance de premier fixé, la propriété de Northcott est respectée pour tous les points appartenant à la zone bleue. Dans la zone rouge, $S_{q,B,s}$ est infini dès que B est assez grand. Finalement, la bande blanche disparaît quand $q \rightarrow \infty$.

Problème 1.0.3. Considérons l'ensemble

$$S_{B,s} = \{[K] : |\zeta_K^*(s)| \leq B\},$$

où $[K]$ représente la classe d'isomorphismes de corps de nombres et ζ_K la fonction zêta de Dedekind. En fixant $s \in \mathbb{C}$, l'ensemble $S_{B,s}$ est-il fini pour tout $B \in \mathbb{R}_{>0}$? Dans ce cas, on dit que la propriété de Northcott est respectée en s . Sinon, on appelle un tel point non Northcott.

Nous étudierons cette question au Chapitre 3. Une représentation qualitative des résultats est disponible sous la forme de la Figure 1.2. Consulter le Théorème 1.4.17 pour plus de détails. Avant tout, nous consacrerons le reste du Chapitre 1 à une présentation concise des concepts utilisés dans les Chapitres 2 et 3.

Les deux premières sections de l'introduction servent de rappel à la théorie des nombres algébrique sur les corps de nombres et sur les corps de fonctions respectivement. Les résultats sont donnés avec preuve lorsqu'elles sont immédiates ou utiles à l'exposition. On peut trouver le reste des preuves dans [30, 38] pour la Section 1.1, [51, 57] pour la Section 1.2

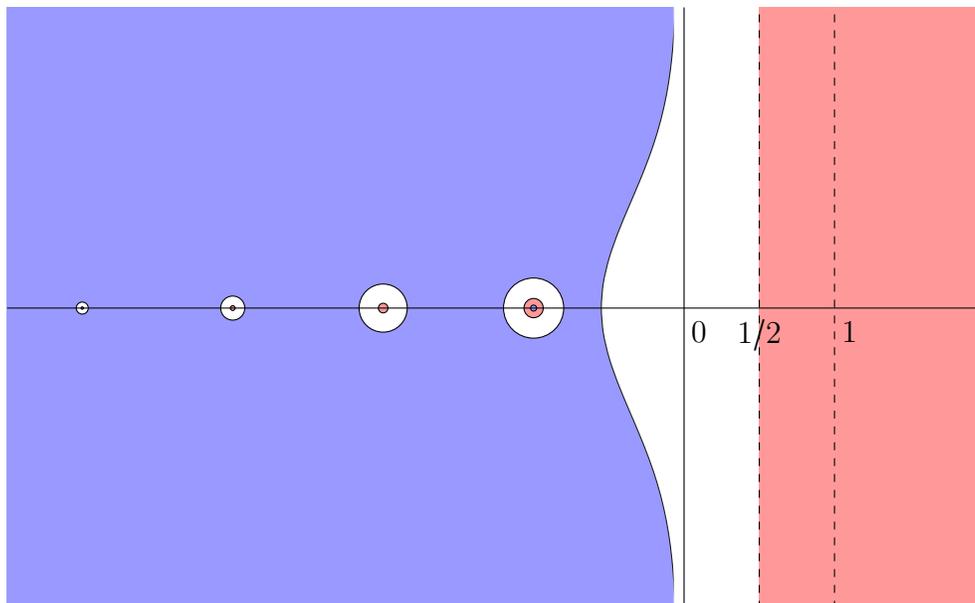


Fig. 1.2. Illustration approximative des résultats du Chapitre 3 par rapport à la propriété de Northcott sur les fonctions zêta de Dedekind. En bleu, les points qui respectent la propriété de Northcott; en rouge, les points qui ne la respectent pas.

et, finalement, [41, 51, 59] pour la Section 1.3. Une fois la mise en place achevée, nous retournerons à la propriété de Northcott de fonctions zêta dans la Section 1.4.

1.1. Les corps de nombres

1.1.1. Extension des rationnels

Les corps de nombres, qu'on notera avec la lettre K , sont des extensions finies des nombres rationnels \mathbb{Q} . Dans ce chapitre, nous considérerons les extensions suivantes: si α est un zéro d'un polynôme irréductible de degré n sur les rationnels alors il est possible de montrer [16, Théorème 25] qu'on a la représentation unique des éléments du corps

$$K = \mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}\}.$$

Dans ce contexte, on dira que K est de degré n et on appellera la réunion de ces extensions, pour tout n , $\overline{\mathbb{Q}} = \bigcup_{\alpha} \mathbb{Q}(\alpha)$, les nombres algébriques.

Exemple 1.1.1. L'extension quadratique $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ est un corps de nombres. Ici, $\sqrt{2}$ est la racine du polynôme irréductible $x^2 - 2$.

Pour chaque nombre algébrique α , il existe un polynôme de degré minimal tel que $f(\alpha) = 0$. De plus, on peut normaliser $f(x)$ pour que son coefficient principal soit 1. Avec ces critères, on obtient un polynôme déterminé uniquement qu'on appelle le **polynôme minimal** de α et on le note $m_\alpha(x)$. Notons que le polynôme donné à l'Exemple 1.1.1 est $m_{\sqrt{2}}(x)$.

La normalisation survenant dans la définition du polynôme minimal est commune. Pour un anneau unitaire A , on dit que $f(x) \in A[x]$ est **monique** si le coefficient principal de $f(x)$ est 1.

Définition 1.1.2. Soit $z \in \mathbb{C}$. On dit que z est un **entier algébrique** lorsqu'il est la racine d'un *polynôme monique* sur \mathbb{Z} . On notera l'ensemble des entiers algébriques par $\mathbb{A} \subset \mathbb{C}$. On dit également que \mathbb{A} est la fermeture intégrale de \mathbb{Z} dans \mathbb{C} .

Il se trouve que dans certains contextes, il est pratique d'avoir d'autres caractérisations d'un entier algébrique:

Proposition 1.1.3. Soit $\alpha \in \overline{\mathbb{Q}}$, alors $\alpha \in \mathbb{A}$ si et seulement si $\mathbb{Z}[\alpha]$ est un \mathbb{Z} -module de type fini.

DÉMONSTRATION. (\implies) Si α est la racine d'un polynôme f monique de degré m alors $\mathbb{Z}[\alpha]$ est généré par $1, \alpha, \dots, \alpha^{m-1}$. En effet, considérons un terme α^r . Si $r \leq m-1$, on a terminé; sinon, on peut substituer

$$\alpha^r = \alpha^{r-m}\alpha^m = \alpha^{r-m}(\alpha^m - f(\alpha)).$$

Le terme $\alpha^m - f(\alpha)$ est un polynôme en α sur \mathbb{Z} de degré $\leq m-1$. En répétant cette procédure au plus $r-m$ fois supplémentaires on a obtenu la représentation

$$\alpha^r = \sum_{i=0}^{m-1} a_i \alpha^i \text{ pour } a_i \in \mathbb{Z}.$$

(\impliedby) Soient $f_1(\alpha), \dots, f_n(\alpha) \in \mathbb{Z}[\alpha]$ des éléments qui génèrent le \mathbb{Z} -module $\mathbb{Z}[\alpha]$. Si $N = \max\{\deg(f_i) : 1 \leq i \leq n\}$, alors comme $\mathbb{Z}[\alpha]$ est un \mathbb{Z} -module, il existe $b_i \in \mathbb{Z}$ tels que

$$\alpha^{N+1} = \sum_{i=1}^n b_i f_i(\alpha).$$

En d'autres mots, α est la solution d'un polynôme monique sur \mathbb{Z} . □

De plus, les nombres algébriques sont fermés sous l'addition et la multiplication.

Proposition 1.1.4. L'ensemble des nombres algébriques \mathbb{A} forme un sous-anneau de \mathbb{C} .

DÉMONSTRATION. Soit $\alpha, \beta \in \mathbb{A}$. Il suffit de montrer que $\alpha + \beta$ et $\alpha\beta$ sont des entiers algébriques. Si $1, \alpha, \dots, \alpha^{n-1}$ génèrent le \mathbb{Z} -module $\mathbb{Z}[\alpha]$ et $1, \beta, \dots, \beta^{m-1}$ le \mathbb{Z} -module $\mathbb{Z}[\beta]$ alors l'ensemble $\alpha^i \beta^j, 0 \leq i < n, 0 \leq j < m$ génère le \mathbb{Z} -module $\mathbb{Z}[\alpha, \beta]$. $\mathbb{Z}[\alpha + \beta]$ et $\mathbb{Z}[\alpha\beta]$ étant des \mathbb{Z} -sous-modules de $\mathbb{Z}[\alpha, \beta]$, ils sont également de type fini par le fait très général que les sous-modules d'un \mathbb{Z} -module de type fini sont de type fini [27, Théorème 6.47]. Ainsi, $\alpha + \beta, \alpha\beta \in \mathbb{A}$ par la Proposition 1.1.3. \square

Enfin, on peut caractériser les éléments de \mathbb{A} avec leur polynôme minimal. Pour ce faire, on a besoin d'un petit lemme:

Lemme 1.1.5. *Soit $m(x) \in \mathbb{Z}[x]$ un polynôme monique. Si $\alpha \in \mathbb{Q}$ est une racine de $m(x)$ alors $\alpha \in \mathbb{Z}$.*

DÉMONSTRATION. Posons $\alpha = r/s \in \mathbb{Q}$ tel que $(r, s) = 1$. Comme α est une racine de $m(x)$, elle satisfait l'équation

$$m(\alpha) = (r/s)^n + a_{n-1}(r/s)^{n-1} + \dots + a_0 = 0 \iff r^n + a_{n-1}sr^{n-1} + \dots + a_0s^n = 0.$$

De cette relation, il découle que $s|r^n$. Or, r et s sont copremiers donc $s = \pm 1$ et $r/s \in \mathbb{Z}$. \square

Proposition 1.1.6. *Soit $\alpha \in \overline{\mathbb{Q}}$, alors $\alpha \in \mathbb{A}$ si et seulement si $m_\alpha(x) \in \mathbb{Z}[x]$.*

DÉMONSTRATION. Si $\alpha \in \mathbb{A}$, alors on sait qu'il existe $f(x) \in \mathbb{Z}[x]$ monique tel que $f(\alpha) = 0$. Une conséquence de la division euclidienne sur $\mathbb{Q}[x]$ est que $m_\alpha(x)$ divise $f(x)$, mais alors toutes les racines de $m_\alpha(x)$ sont des éléments de \mathbb{A} car elles sont aussi des racines de $f(x) = m_\alpha(x)q(x)$, où $q(x)$ est un certain polynôme sur $\mathbb{Q}[x]$. Puisque $m_\alpha(x) \in \mathbb{Q}[x]$ et que ses coefficients sont une combinaison de somme et de produit des racines, les coefficients de $m_\alpha(x)$ sont dans $\mathbb{A} \cap \mathbb{Q}$. On a montré dans le Lemme 1.1.5 précédant cette proposition que cette intersection est \mathbb{Z} . Ainsi, $m_\alpha(x) \in \mathbb{Z}[x]$. \square

Définition 1.1.7. Soit K , un corps de nombres. On définit $O_K = \mathbb{A} \cap K$, l'**anneau des entiers** de K . Dans ce contexte, O_K est la fermeture intégrale de \mathbb{Z} dans K .

L'anneau O_K peut être vu comme un analogue aux nombres entiers dans K .

Exemple 1.1.8.

- Dans la preuve de la Proposition 1.1.6, on a montré que $O_{\mathbb{Q}} = \mathbb{Z}$.
- Pour le corps quadratique $\mathbb{Q}(\sqrt{2})$, $\alpha = a + b\sqrt{2} \notin \mathbb{Q}$ si $b \neq 0$. Dans ce cas, le polynôme minimal ne peut pas être de degré 1, par contre

$$m_\alpha(x) = (x - a - b\sqrt{2})(x - a + b\sqrt{2}) = x^2 - 2ax + a^2 - 2b^2.$$

Les coefficients de ce polynôme sont des éléments de \mathbb{Q} , ainsi $\alpha \in O_{\mathbb{Q}(\sqrt{2})}$ ssi $2a$ et $a^2 - 2b^2$ sont des entiers. Si $2a$ est pair, alors $a \in \mathbb{Z}$ et on conclut que $2b^2 \in \mathbb{Z}$; qui implique que $b \in \mathbb{Z}$. Sinon, $2a$ est impair et $a^2 = \frac{(2n+1)^2}{4}$. Si $a^2 - 2b^2 \in \mathbb{Z}$, alors il existe $m \in \mathbb{Z}$ tel que

$$\frac{4n^2 + 4n + 1}{4} - 2b^2 = m \iff 4(n^2 + n - m) + 1 = 8b^2.$$

Mais ceci est impossible puisque $\frac{4(n^2+n-m)+1}{8}$ est une fraction réduite et 8 n'est pas un carré. On conclut que $O_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$.

- Considérons maintenant $\mathbb{Q}(\sqrt{5})$. L'élément $\phi = \frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ appartient à l'anneau des entiers $O_{\mathbb{Q}(\sqrt{5})}$. En effet, son polynôme minimal est donné par

$$m_\phi(x) = x^2 - x - 1.$$

En conséquence, l'inclusion $\mathbb{Z}[\sqrt{5}] \subset O_{\mathbb{Q}(\sqrt{5})}$ est stricte.

La dernière proposition de cette courte introduction sur les corps de nombres et leurs anneaux des entiers peut sembler assez anodine. On l'interprète comme la généralisation de «multiplier un nombre rationnel par son dénominateur».

Proposition 1.1.9. *Soit K un corps de nombres et O_K son anneau des entiers. Posons, $\alpha \in K$ et $m_\alpha(x) = x^n + a_{n-1}x^{n-1} \cdots + a_1x + a_0$ son polynôme minimal. Si $a_i = \frac{r_i}{s_i}$ est la représentation en fraction réduite des coefficients a_i et $s = \text{ppcm}(s_{n-1}, \dots, s_0)$, alors l'élément $s\alpha$ est un entier algébrique.*

DÉMONSTRATION. En effet, si on pose $\beta = s\alpha$, on remarque que

$$\begin{aligned} & \beta^n + sa_{n-1}\beta^{n-1} + s^2a_{n-2}\beta^{n-2} + \cdots + s^na_0 \\ &= s^n\alpha^n + s^na_{n-1}\alpha^{n-1} + s^na_{n-2}\alpha^{n-2} + \cdots + s^na_0 \\ &= s^n(m_\alpha(\alpha)) = 0. \end{aligned}$$

Par définition de s , les coefficients $s^{n-i}a_i \in \mathbb{Z}$. Ainsi, β est la racine d'un polynôme monique sur \mathbb{Z} . □

Corollaire 1.1.10. *Soit $\alpha \in K$, alors $\alpha = a/b$, où $a \in O_K$ et $b \in \mathbb{Z}$.*

On tourne maintenant notre attention vers le théorème fondamental de l'arithmétique. La décomposition des entiers en nombres premiers est à la base d'une multitude de résultats en théorie des nombres. C'est une histoire très populaire que Kummer, motivé probablement

par l'ambition du dernier Théorème de Fermat [7, p.120], essaya de généraliser cette notion aux anneaux $\mathbb{Z}[\zeta]$, où ζ est une racine p -ème de l'unité [7, p. 122]. Ces anneaux possédaient plusieurs difficultés à surmonter et parmi elles, le fait qu'ils n'étaient pas toujours des anneaux principaux. Ceci avait l'effet suivant, qu'on souligne avec le cas similaire des anneaux des entiers quadratiques:

Soit l'anneau $\mathbb{Z}[\sqrt{-5}]$, on va montrer qu'il est possible de trouver plus d'une factorisation en éléments irréductibles. On peut considérer

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Ces éléments sont bel et bien irréductibles. Pour le vérifier, on introduit la fonction norme $N(a + b\sqrt{-5}) := (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$. Il est possible de vérifier explicitement que cette fonction est multiplicative, de plus, il découle de sa définition que l'image de $\mathbb{Z}[\sqrt{-5}]$ est contenue dans les entiers. Maintenant, supposons qu'il soit possible de séparer le nombre 2 en des éléments non inversibles d_1, d_2 . Les propriétés de N impliquent alors que $N(2) = N(d_1)N(d_2)$ ou encore que $N(d_i) = \pm 2$. Or, ceci est impossible, car on sait que les éléments de $\mathbb{Z}[\sqrt{-5}]$ ont la forme $x + y\sqrt{-5}$ et la norme

$$N(x + y\sqrt{-5}) = x^2 + 5y^2.$$

Seulement, comme x^2, y^2 sont positifs, on peut vérifier qu'il n'existe pas d'entiers $x, y \in \mathbb{Z}$ tels que $x^2 + 5y^2 = \pm 2$. En répétant l'exercice pour les autres facteurs, on peut montrer que les 4 sont irréductibles. Ensuite, on rappelle que dans les entiers, la factorisation unique ne distingue pas $4 = 2 \cdot 2 = (-2) \cdot (-2)$. Il reste donc la tâche de vérifier que nos deux factorisations ne diffèrent pas par des éléments inversibles. Or, comme on le verra sous peu (Exemple 1.1.14), les éléments inversibles sont de norme 1 et on a terminé puisque les éléments des deux factorisations n'ont pas la même norme.

Pour réparer ce problème, l'idée de Kummer était d'introduire des *nombre idéal* qui serviraient tout de même à décomposer les éléments jusqu'à ce qu'on obtienne la factorisation unique. Même si sa méthode fut fructueuse pour les anneaux cyclotomiques [7, p.122], il faudra attendre la clarification de la notion d'entier algébrique (Définition 1.1.7) puis les travaux de Dedekind [7, p.126-130] avant de voir apparaître la théorie que nous présenterons dans les prochaines section. Nous explorerons ces notions en détails après avoir développé les outils nécessaires.

1.1.2. Outils et définitions

Soit α un nombre algébrique et $m_\alpha(x)$ son polynôme minimal. Le corps $\mathbb{Q}(\alpha)$ possède exactement $n = \deg(m_\alpha(x))$ injections $\sigma_1, \dots, \sigma_n$ dans \mathbb{C} . (Voir [16, Chapitre 13] pour un rappel sur la théorie des corps.) Ces injections sont facilement décrites par les racines de $m_\alpha(x)$,

Proposition 1.1.11. *Si σ est une injection de $\mathbb{Q}(\alpha)$ dans \mathbb{C} alors σ fixe \mathbb{Q} et $\sigma(\alpha) = \alpha'$, une racine de $m_\alpha(x)$. Chaque racine β de $m_\alpha(x)$ détermine une injection unique de $\mathbb{Q}(\alpha)$ dans \mathbb{C} .*

DÉMONSTRATION. Soit σ une telle injection. Immédiatement, $\sigma(1) = \sigma(1)\sigma(1)$. Ainsi, $\sigma(1) = 1$ et σ fixe \mathbb{Z} . Si $r/s \in \mathbb{Q}$, alors comme $s\sigma(r/s) = \sigma(r) = r$, on voit que l'injection fixe \mathbb{Q} au complet. Mais alors, $\sigma(m_\alpha(\alpha)) = m_\alpha(\sigma(\alpha))$, car par la Proposition 1.1.6, on sait que $m_\alpha(x) \in \mathbb{Z}[x]$. Donc $\sigma(\alpha)$ est aussi une racine de $m_\alpha(x)$. Finalement, comme il existe précisément n racines distinctes de $m_\alpha(x)$ [16, Chapitre 13], on voit en fait que chaque racine détermine une injection de $\mathbb{Q}(\alpha)$ dans \mathbb{C} . \square

Maintenant, pour un élément $\alpha \in K$ et la même notation pour les injections, on définit la **norme** et la **trace** par

$$\begin{aligned} N^K(\alpha) &= \sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha) \\ T^K(\alpha) &= \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha) \end{aligned}$$

Lorsque l'extension est dépourvue d'ambiguïté dans le contexte, on notera simplement $N(\alpha)$ et $T(\alpha)$. De ces définitions suivent que $N(\alpha\beta) = N(\alpha)N(\beta)$ et que $T(\alpha + \beta) = T(\alpha) + T(\beta)$.

Proposition 1.1.12. *Soit K un corps de nombres et $\alpha_1 \in K$. Si $\alpha_2, \dots, \alpha_d$ sont les conjugués de α_1 alors*

$$\begin{aligned} N(\alpha_1) &= (\alpha_1 \cdots \alpha_d)^{[K:\mathbb{Q}(\alpha_1)]} \in \mathbb{Q} \\ T(\alpha_1) &= [K:\mathbb{Q}(\alpha_1)](\alpha_1 + \cdots + \alpha_d) \in \mathbb{Q}. \end{aligned}$$

IDÉE DE LA PREUVE. Ce résultat suit du fait que les injections de $\mathbb{Q}(\alpha_1)$ dans \mathbb{C} s'étendent à $[K:\mathbb{Q}(\alpha_1)]$ injections de K dans \mathbb{C} [16, Chapitre 14] et parce que $N^{\mathbb{Q}(\alpha_1)}(\alpha_1) = \alpha_1 \cdots \alpha_d$ et $T^{\mathbb{Q}(\alpha_1)}(\alpha_1) = \alpha_1 + \cdots + \alpha_d$ (car les injections distinctes de $\mathbb{Q}(\alpha_1)$ dans \mathbb{C} envoient α_1 à des conjugués distincts). Finalement, ces quantités sont dans \mathbb{Q} puisque $m_\alpha(x) \in \mathbb{Q}[x]$. En effet, si on développe $(x - \alpha_1) \cdots (x - \alpha_d)$, $T^{\mathbb{Q}(\alpha)}(\alpha)$ et $N^{\mathbb{Q}(\alpha)}(\alpha)$ correspondent respectivement au deuxième et dernier coefficient de $m_\alpha(x)$. \square

Corollaire 1.1.13. *En fait, si $\alpha \in O_K$ alors $m_\alpha(x) \in \mathbb{Z}[x]$. Donc $N(\alpha), T(\alpha) \in \mathbb{Z}$.*

Exemple 1.1.14.

- Si $K = \mathbb{Q}(\sqrt{2})$, les injections de K dans \mathbb{C} sont les automorphismes identités ainsi que le conjugué donné par $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. En terminant, on remarque que $-\sqrt{2}$ est l'autre racine de $m_{\sqrt{2}}(x)$.
- Les éléments inversibles de K sont tels que $N(u)N(u^{-1}) = 1$. Or, $N(K) \subset \mathbb{Z}$ donc $N(u) = N(u^{-1}) = \pm 1$ si u est inversible. La réciproque est également vraie, si $N(u) = \sigma_1(u) \cdots \sigma_n(u) = 1$ alors on peut poser $\sigma_1 = id_K$, l'automorphisme identité et on trouve que le produit $\sigma_2(u) \cdots \sigma_n(u)$ est un inverse dans \mathbb{C} . C'est un élément de K puisque c'est $1/u$ et de \mathbb{A} puisque c'est un produit des conjugués de u par la Proposition 1.1.12 qui sont des entiers algébriques par la Proposition 1.1.11.
- On peut utiliser la trace pour montrer que $\sqrt{3} \notin \mathbb{Q}(\sqrt[4]{2})$. Sinon, posons $\sqrt{3} = a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}$ et d'une part, la Proposition 1.1.11 combinée avec la définition de la trace donne que $T(\sqrt{3}) = 4a$. Mais alors la Proposition 1.1.12 implique de $T(\sqrt{3}) = 0$, car $m_{\sqrt{3}}(x) = x^2 - 3$, donc $a = 0$. Mais alors on peut diviser $\sqrt{3} = b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}$ par $\sqrt[4]{2}$ et encore une fois, la Proposition 1.1.12 implique de $T\left(\frac{\sqrt{3}}{\sqrt[4]{2}}\right) = 0$, car $m_{\frac{\sqrt{3}}{\sqrt[4]{2}}}(x) = 2x^4 - 9$. En répétant l'argument, on trouve que $c = d = 0$ également, une contradiction.

Maintenant, supposons que K soit de degré n sur \mathbb{Q} . Si, comme plus haut, $\sigma_1, \dots, \sigma_n$ sont les injections de K dans \mathbb{C} , alors on définit le **discriminant** de $\alpha_1, \dots, \alpha_n$, des éléments de K , comme

$$d(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2,$$

où $\sigma_i(\alpha_j)$ représente la matrice $n \times n$ avec coefficient $\sigma_i(\alpha_j)$ à la rangée i et la colonne j . On sait qu'interchanger une paire de rangées ou de colonnes ne fait que changer le signe du discriminant. Ainsi, la valeur de $d(\alpha_1, \dots, \alpha_n)$ est indépendante de l'ordre des σ_i et des α_j .

Un résultat immédiat des définitions de la trace et du discriminant est

Proposition 1.1.15.

$$d(\alpha_1, \dots, \alpha_n) = \det(T(\alpha_i \alpha_j)).$$

DÉMONSTRATION. Rappelons que $\det(a_{i,j}) = \det(a_{j,i})$ et que $\det(AB) = \det(A)\det(B)$. Ainsi,

$$d(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 = \det(\sigma_j(\alpha_i)) \det(\sigma_i(\alpha_j)) = \det\left(\sum_{l=1}^n \sigma_l(\alpha_i \alpha_j)\right) = \det(T(\alpha_i \alpha_j)).$$

□

Proposition 1.1.16. *Le discriminant $d(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$. Si les $\alpha_i \in O_K$, alors $d(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$. De plus, le discriminant est non nul si et seulement si $\alpha_1, \dots, \alpha_n$ est une base de K sur \mathbb{Q} .*

DÉMONSTRATION. La première remarque découle de la Proposition 1.1.15 ainsi que du Corollaire 1.1.13. Ensuite, si $1, \alpha, \dots, \alpha^{n-1}$ est une autre base de K , (donc $K = \mathbb{Q}(\alpha)$) alors on sait qu'il existe une matrice inversible $U \in M_n(\mathbb{Q})$ telle que $(\alpha_1, \dots, \alpha_n) = U(1, \alpha, \dots, \alpha^{n-1})$. Cette égalité peut être vue comme un système de n équations. Il est possible d'appliquer chacun des σ_i à ces équations pour obtenir l'équation matricielle $\sigma_i(\alpha_j) = U\sigma_i(\alpha^j)$. En prenant le déterminant et le carré, on trouve que le discriminant des deux bases ne diffère que de $\det(U)^2 \neq 0$. Finalement, $d(1, \alpha, \dots, \alpha^{n-1}) \neq 0$ puisque $d(1, \alpha, \dots, \alpha^{n-1}) = \det(\sigma_i(\alpha^{j-1}))^2$ qui est un déterminant de Vandermonde. Or, $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ si $i \neq j$ donc le déterminant est non nul. □

On peut utiliser le discriminant pour montrer un résultat structurel important de O_K ,

Proposition 1.1.17. *L'anneau des entiers O_K forme un \mathbb{Z} -module libre de rang n .*

DÉMONSTRATION. Voir [38, Théorème 9]. Une autre stratégie, qui utilise la trace au lieu du discriminant, revient à montrer que O_K est un \mathbb{Z} -module de type fini [30, Proposition 6]. Le résultat suit alors de la théorie sur les anneaux principaux [27, Théorème 7.1]: Les modules sans torsion de type fini sur des anneaux principaux sont libres. □

Une conséquence de ce résultat est que,

Proposition 1.1.18. *Si B est une base de O_K comme \mathbb{Z} -module alors le discriminant $d(B)$ est invariant du choix de la base. On le note alors $d(O_K)$ ou Δ_K .*

DÉMONSTRATION. Si B_1 et B_2 sont deux bases de O_K , alors par la Proposition 1.1.17, il existe une matrice $U \in M_n(\mathbb{Z})$ telle que $B_1 = UB_2$. Pour exactement les mêmes raisons que dans la preuve de la Proposition 1.1.16, les discriminants diffèrent de $\det U^2$. Puisque les coefficients de U sont des entiers, son déterminant aussi. Par la première partie de la Proposition 1.1.16, il en est de même pour $d(B_1)$ et $d(B_2)$. Ceci montre que $d(B_2)$ divise $d(B_1)$ et ils ont le même signe, car $\det U^2$ est nécessairement un nombre positif. Un argument analogue nous permet de conclure que $d(B_1)$ divise $d(B_2)$ et ils sont donc égaux. □

On aura également besoin d'outils analogues au niveau des **idéaux** des anneaux des entiers. Rappelons que, si A est un anneau commutatif, ses idéaux sont par définition les A sous-modules du A -module A . Lorsqu'un idéal $\mathfrak{a} \subset A$ est cyclique, c'est-à-dire qu'il est généré par un seul élément $\alpha \in A$, on écrit $\mathfrak{a} = (\alpha)$ et on dit qu'il est principal. S'il est préférable de spécifier l'anneau (ou qu'on juge les parenthèses encombrantes), on priorisera la notation $\mathfrak{a} = \alpha A$. Finalement, pour un rappel sur la théorie des anneaux on réfère le lecteur aux excellentes notes [27]. Elles contiennent en particulier les concepts importants d'idéaux premiers et maximaux.

Maintenant, on définit la **norme d'un idéal** $\mathcal{N}(\mathfrak{a})$ par l'indice de \mathfrak{a} dans O_K en tant que sous-groupe: $[O_K : \mathfrak{a}] = |O_K/\mathfrak{a}|$. Voir [16, Section 3.2] pour un rappel sur la théorie des groupes.

Proposition 1.1.19. *Soit K un corps de nombres de degré n et \mathfrak{a} un idéal non trivial de O_K . La norme $\mathcal{N}(\mathfrak{a}) = [O_K : \mathfrak{a}]$ est bien définie. C'est à dire que $\mathcal{N}(\mathfrak{a}) \in \mathbb{N}$.*

DÉMONSTRATION. Si $m \in \mathbb{Z}$, alors l'indice $[O_K, (m)]$ est fini. En effet, par la Proposition 1.1.17, O_K est un \mathbb{Z} -module de rang n et le quotient par (m) contiendra m^n classes d'équivalences. Avec ceci en tête, on montre que pour chaque idéal $\mathfrak{a} \subseteq O_K$, il existe $m \in \mathbb{Z}$ tel que $(m) \subset \mathfrak{a}$. (Donc l'indice $[O_K : \mathfrak{a}]$ est également fini).

Soit $\alpha \in \mathfrak{a} \setminus \{0\}$ et posons $m = N(\alpha)$. Par définition, $m = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$ où $\sigma_1(\alpha) = \alpha$. Ainsi, $m \in \mathfrak{a}$ si $\sigma_2(\alpha) \cdots \sigma_n(\alpha) \in O_K$. Mais ce produit est un élément de \mathbb{A} puisque chaque $\sigma_i(\alpha) \in \mathbb{A}$ par la Proposition 1.1.11 et de K , car c'est m/α . Donc $(m) \subset \mathfrak{a}$ comme voulu. \square

Le nom que l'on donne à cette quantité provient du fait que pour les entiers, la norme $\mathcal{N}(n\mathbb{Z}) = [\mathbb{Z} : n\mathbb{Z}] = |n|$ coïncide avec la valeur absolue du générateur n . Avant d'explorer ses propriétés en plus grands détails, on aura besoin d'une meilleure compréhension des idéaux de O_K . C'est donc un bon moment pour revenir à la factorisation unique des idéaux.

1.1.3. Le point de vue des idéaux

Pour pouvoir considérer la factorisation d'idéaux, on aura besoin d'une notion de produit d'idéaux. Ainsi, on définit le produit de deux idéaux comme

Définition 1.1.20. Soit $\mathfrak{a}, \mathfrak{b}$ des idéaux. On dénote le produit de \mathfrak{a} et \mathfrak{b} par

$$\mathfrak{ab} = \left\{ \sum_{\alpha \in \mathfrak{a}, \beta \in \mathfrak{b}} \alpha\beta \right\}$$

Dans ce contexte, il est possible de réobtenir la factorisation en éléments irréductibles sous la forme de la factorisation en idéaux premiers.

Théorème 1.1.21. Soit $\mathfrak{a} \subset O_K$ un idéal différent de (0) et de (1). L'idéal \mathfrak{a} admet la factorisation

$$\mathfrak{a} = \mathcal{P}_1 \cdots \mathcal{P}_k$$

en idéaux premiers non nuls. Cette factorisation est unique modulo une permutation des facteurs.

En revenant à l'exemple introduit au début de cette section, on trouve que l'idéal engendré par 6 admet désormais une factorisation similaire aux nombres idéaux proposés par Kummer.

$$\begin{aligned} (2)(3) &= (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5}) (3, 1 - \sqrt{-5}) \\ &= (2, 1 + \sqrt{-5}) (3, 1 + \sqrt{-5}) (2, 1 + \sqrt{-5}) (3, 1 - \sqrt{-5}) = (1 + \sqrt{-5}) (1 - \sqrt{-5}). \end{aligned}$$

Remarque 1.1.22. Dans cette factorisation, les idéaux premiers ne peuvent pas être décrits comme des idéaux générés par un seul élément. En d'autres mots, ce ne sont pas des idéaux principaux. Si c'était le cas, il suit directement du Théorème 1.1.21 que O_K est un anneau factoriel.

En général, la preuve du Théorème 1.1.21 procède comme suit: On commence par faire ressortir trois propriétés structurelles importantes de O_K , puis, on montre que les anneaux intègres possédant ces trois propriétés possèdent la propriété de factorisation unique de leurs idéaux. Avec cette stratégie en tête, on définit

Définition 1.1.23. Un **anneau de Dedekind** est un anneau intègre A tel que

- (1) Tous les idéaux de A sont de type fini.
- (2) Tous les idéaux premiers non triviaux de A sont maximaux.
- (3) A est intégralement clos dans son corps des fractions

$$K = \{a/b : a, b \in A, b \neq 0\}.$$

(C'est à dire que si $\alpha \in K$ est la racine d'un polynôme monique sur A alors $\alpha \in A$.)

Théorème 1.1.24. Soit K un corps de nombres. Son anneau des entiers, O_K , est un anneau de Dedekind.

DÉMONSTRATION. Pour débiter, par la Proposition 1.1.17, O_K est un \mathbb{Z} -module libre. Comme \mathbb{Z} est un anneau principal, O_K respecte les critères de [27, Théorème 6.47] et les \mathbb{Z} -sous-modules de O_K (et en particulier ses idéaux) sont de type fini comme \mathbb{Z} -modules. Avec ceci en tête, puisque les idéaux de O_K sont de type fini comme \mathbb{Z} -modules, ils le seront nécessairement comme O_K -module.

Ensuite, si \mathcal{P} est un idéal premier, on considère le quotient O_K/\mathcal{P} . Par la théorie des anneaux, on sait que ce quotient est un anneau intègre; \mathcal{P} sera maximal si c'est un corps. Or, on a vu à la Proposition 1.1.19 que le quotient O_K/\mathcal{P} est un anneau fini. Un exercice classique montre qu'il est un corps et \mathcal{P} est maximal.

Finalement, supposons que $\alpha \in K$ soit la solution de l'équation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \text{ pour quelques } a_0, \dots, a_{n-1} \in O_K.$$

On affirme que l'anneau $\mathbb{Z}[a_0, \dots, a_{n-1}, \alpha]$ est un \mathbb{Z} -module de type fini. En effet, les produits $a_0^{m_0} \cdots a_{n-1}^{m_{n-1}} \alpha^m$ génèrent $\mathbb{Z}[a_0, \dots, a_{n-1}, \alpha]$ comme \mathbb{Z} -module, et ce même si on se restreint à un nombre fini de choix pour les exposants. Pour rendre ceci explicite, on remarque qu'il est possible de suivre une procédure semblable à celle de la preuve de la Proposition 1.1.3 pour trouver la substitution

$$\alpha^r = \sum_{i=0}^{n-1} \gamma_i \alpha^i \text{ pour } \gamma_i \in \mathbb{Z}[a_0, \dots, a_{n-1}] \text{ et } r \in \mathbb{N}.$$

Après cette substitution, il est possible que les puissances des a_i soient plus hautes que dans l'expression initiale. Ceci ne cause pas de problème puisque si on utilise les mêmes idées pour réduire les puissances des a_i , le fait que $m_{a_i}(x) \in \mathbb{Z}[x]$ implique que la procédure pour les a_i n'a aucune influence sur les autres puissances. En somme, ceci nous permet de représenter les termes $a_0^{m_0} \cdots a_{n-1}^{m_{n-1}} \alpha^m$ en une somme sur \mathbb{Z} de ces mêmes termes où $m_i \leq l_i - 1$ et $m \leq n - 1$. \square

La notion d'anneau de Dedekind a pour avantage de faire ressortir des propriétés importantes sur les idéaux de O_K . À partir de celle-ci, on peut finalement montrer

Théorème 1.1.25. *Soit A un anneau de Dedekind. Chaque idéal propre de A admet une factorisation unique en idéaux premiers similaire au Théorème 1.1.21.*

DÉMONSTRATION. Consulter [38, Théorème 16] ou [41, Théorème 3.3] pour la preuve complète. \square

Bien que l'on ne présente pas cette preuve dans ce mémoire, le point de vue d'anneau de Dedekind est très pratique et sera utilisé dans ce qui suit.

On termine cette section en introduisant une notion d'inverse pour les idéaux de O_K .

Définition 1.1.26. Un **idéal fractionnaire** de K est un O_K sous-module $\mathfrak{a} \neq 0$ de K qui est de type fini.

Lorsqu'un idéal $\mathfrak{a} \subset O_K$, c'est-à-dire qu'il est un idéal au sens classique, on dit que l'idéal \mathfrak{a} est **entier**.

Exemple 1.1.27. Si $K = \mathbb{Q}$, on montre que les idéaux fractionnaires sont les \mathbb{Z} -modules cycliques $(a) = a\mathbb{Z}$ pour $a \in \mathbb{Q}^*$. En effet, si $\frac{r}{s}, \frac{r'}{s'} \in \mathbb{Q}$ tels que $(r,s) = 1$ et $(r',s') = 1$ alors on a l'égalité d'ensembles suivante:

$$\begin{aligned} \left\{ \frac{nr}{s} + \frac{mr'}{s'} : n, m \in \mathbb{Z} \right\} &= \left\{ \frac{\text{pgcd}(r,r')}{\text{ppcm}(s,s')} \left(\frac{nr s' + mr' s}{\text{pgcd}(s,s') \text{pgcd}(r,r')} \right) : n, m \in \mathbb{Z} \right\} \\ &= \frac{\text{pgcd}(r,r')}{\text{ppcm}(s,s')} \mathbb{Z} \end{aligned}$$

où la dernière égalité suit du Théorème de Bézout et le résultat par récurrence.

Muni du produit de la Définition 1.1.20, c'est facile de se convaincre que l'ensemble des idéaux fractionnaires de l'Exemple 1.1.27 forme un groupe multiplicatif. En général,

Théorème 1.1.28. *L'ensemble des idéaux fractionnaires de K forme un groupe abélien qu'on note J_K , le **groupe des idéaux** de K . L'identité est donnée par $(1) = O_K$ et les inverses par*

$$\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subset O_K\}.$$

De plus, les $\mathfrak{a} \in J_K$ admettent la représentation unique

$$\mathfrak{a} = \prod_{\mathcal{P}} \mathcal{P}^{v_{\mathcal{P}}}.$$

pour $v_{\mathcal{P}} \in \mathbb{Z}$ et $v_{\mathcal{P}} \neq 0$ pour seulement un nombre fini de \mathcal{P} .

DÉMONSTRATION. La preuve est disponible à la suite de la [41, Proposition 3.8]. □

Évidemment, si O_K n'est pas principal, le groupe J_K ne sera pas constitué uniquement de sous-modules cycliques comme dans l'Exemple 1.1.27. Par contre, ceux-ci forment un sous-groupe de J_K , P_K le sous-groupe des idéaux fractionnels principaux. On s'intéresse au groupe quotient

$$Cl_K = J_K/P_K$$

le groupe des classes (d'idéaux) de K . Le **nombre de classes**, $h_K = |Cl_K|$ est un invariant important du corps de nombres K . Suivant notre discussion au paragraphe précédant, $h_K = 1$ si et seulement si O_K est un anneau factoriel. A priori, ce nombre n'est pas bien défini ($|Cl_K|$ pourrait ne pas être fini!), nous montrerons à la Section 1.1.5 que $h_K \in \mathbb{N}$.

1.1.4. Les premiers dans les corps de nombres

Nous avons énoncé, sous la forme du Théorème 1.1.21, que les idéaux de O_K se factorisent de façon unique en un produit d'idéaux premiers. Une question naturelle est de tenter de mettre en relation ces idéaux premiers avec ceux du corps de base \mathbb{Q} .

Soient K un corps de nombres et O_K son anneau des entiers. Évidemment, si l'idéal $(m) \subseteq \mathbb{Z}$ est décomposable comme produit d'idéaux premiers dans \mathbb{Z} , il le sera également dans $\mathbb{Z} \subseteq O_K$. Ainsi, on s'intéressera particulièrement à la décomposition des idéaux premiers de \mathbb{Z} dans O_K .

À la Section 1.1.3, on avait utilisé la fonction norme sur les éléments de O_K pour déterminer s'ils étaient irréductibles. Il se trouve que la notion de norme sur les idéaux peut également être utilisée à cette fin.

Proposition 1.1.29. *Soient \mathfrak{a} et \mathfrak{b} des idéaux entiers de O_K ,*

$$\mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathfrak{a}) \mathcal{N}(\mathfrak{b}).$$

De plus,

$$\mathcal{N}(\alpha O_K) = |N(\alpha)|.$$

DÉMONSTRATION. La preuve de ce fait n'est pas immédiate. On délègue donc le travail à [38, Théorème 22] ou [41, Chapitre 1: Section 6]. \square

Corollaire 1.1.30. *Si $\mathcal{N}(\mathfrak{a}) = p$, un nombre premier, alors \mathfrak{a} est un idéal premier de O_K .*

Exemple 1.1.31. Nous avons vu, dans la discussion suivant le Théorème 1.1.21, que dans l'anneau des entiers $O_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ nous avons la factorisation

$$(2) = (2, 1 + \sqrt{-5})^2$$

$$(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Reste donc à montrer que ces facteurs sont premiers. Or, c'est facile de vérifier que $\mathcal{N}((2, 1 + \sqrt{-5})) = 2$ et $\mathcal{N}((3, 1 \pm \sqrt{-5})) = 3$, ainsi les idéaux sont premiers par le Corollaire 1.1.30.

Pour parler de la décomposition de l'exemple précédant, on introduit les expressions \mathcal{P} est **au-dessus** de p ou p est **au-dessous** de \mathcal{P} lorsque $\mathcal{P}|p$. En particulier, dans l'exemple précédent, l'idéal premier $(2, 1 + \sqrt{-5})$ est au-dessus de 2.

Proposition 1.1.32. *Chaque premier \mathcal{P} de O_K est au-dessus d'un unique premier p de \mathbb{Q} ; Chaque premier p de \mathbb{Q} est au-dessous d'au moins un premier \mathcal{P} de O_K .*

DÉMONSTRATION. Consulter [38, Théorème 20]. □

Maintenant, en général si (p) admet la décomposition en idéaux premiers

$$(p) = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}$$

alors les éléments \mathcal{P}_i seront au-dessus de p . Lorsque $r > 1$ on dit que le premier p se **sépare** dans O_K et lorsqu'un des e_i est tel que $e_i > 1$ on dit que le premier p se **ramifie** dans O_K . On appellera donc e_i le **degré de ramification** de \mathcal{P}_i sur p .

Proposition 1.1.33. *Soit K un corps de nombres et O_K son anneau des entiers. Si \mathcal{P} est un premier au-dessus de p , alors il existe un entier $f \in \mathbb{N}$ tel que $\mathcal{N}(\mathcal{P}) = p^f$.*

DÉMONSTRATION. Supposons que K soit de degré n . Comme \mathcal{P} est au-dessus de p , on sait que $(p) \subset \mathcal{P}$. Ceci implique que $\mathcal{N}(\mathcal{P}) | \mathcal{N}(pO_K)$. Mais, $\mathcal{N}(pO_K) = p^n$ et $\mathcal{N}(\mathcal{P}) \neq 1$, car $\mathcal{P} \neq O_K$. La norme de l'idéal \mathcal{P} est donc une puissance positive de p . □

La puissance apparaissant à la Proposition 1.1.33 est appelé **degré d'inertie** f de \mathcal{P} sur p .

Remarque 1.1.34. Une autre façon de trouver le degré d'inertie est de considérer la composition de morphismes $\mathbb{Z} \hookrightarrow O_K \twoheadrightarrow O_K/\mathcal{P}_i$ donnée par l'inclusion des entiers dans O_K et le morphisme quotient par \mathcal{P}_i . Évidemment, le noyau est donné par $\mathbb{Z} \cap \mathcal{P}_i$. Notons que si p est le premier au-dessus de \mathcal{P}_i , on a vu que $\mathcal{P}_i | (p)$ et donc $(p) \subseteq \mathbb{Z} \cap \mathcal{P}_i$. Or (p) est maximal et $1 \notin \mathcal{P}_i$ donc le noyau est (p) . Ceci donne lieu à l'inclusion de corps finis $\mathbb{Z}/(p) \hookrightarrow O_K/\mathcal{P}_i$ et le degré d'inertie est précisément la dimension de cette extension.

Soit K un corps de nombres. Les nombres r , e_i et f_i sont intimement reliés avec le degré du corps de nombres K .

Théorème 1.1.35. *Soient K un corps de nombres et n son degré. Si $p \in \mathbb{Z}$ est un premier admettant la décomposition en idéaux premiers $(p) = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}$ dans O_K . Alors*

$$\sum_{i=1}^r e_i f_i = n.$$

DÉMONSTRATION. Remarquons que si K est de degré n sur \mathbb{Q} , alors par la Proposition 1.1.17, on a $\mathcal{N}(pO_K) = p^n$. On calcule,

$$\mathcal{N}(pO_K) = \mathcal{N}(\mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}) \implies p^n = p^{f_1 e_1} p^{f_2 e_2} \dots p^{f_r e_r}.$$

□

Lorsque l'extension K est galoisienne, l'index de ramification et le degré d'inertie dépendent uniquement de p .

Théorème 1.1.36. Soient K une extension galoisienne de \mathbb{Q} et p un nombre premier. Le groupe de Galois, $Gal(K)$ agit comme une permutation des premiers \mathcal{P}_i au-dessus de p . Ainsi, les index de ramification et les degrés d'inertie sont égaux pour tout index i . En écrivant e pour l'index de ramification et f pour le degré d'inertie, on trouve

$$ref = n.$$

DÉMONSTRATION. [38, Théorème 23] montre la première partie de l'énoncé. La factorisation unique implique que $e_i = e_j$. Si $\sigma \in Gal(K)$ et $\sigma(\mathcal{P}) = \mathcal{P}'$, alors la composition de σ avec le morphisme quotient

$$O_K \cong O_K \twoheadrightarrow O_K/\mathcal{P}'$$

est surjective. De plus, comme $\sigma(\mathcal{P}) = \mathcal{P}'$, l'idéal \mathcal{P} est le noyau et on a l'isomorphisme

$$O_K/\mathcal{P} \cong O_K/\mathcal{P}'.$$

Ainsi, $\mathcal{N}(\mathcal{P}) = \mathcal{N}(\mathcal{P}')$ et le degré d'inertie sera le même pour tout \mathcal{P}_i . □

On dit alors que e est l'**index de ramification de \mathfrak{p}** dans K et f le **degré d'inertie de \mathfrak{p}** dans K .

Exemple 1.1.37. Plus tôt, on avait vu que $(2) = \mathcal{P}_1\mathcal{P}_2 = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$. On sait que les deux éléments du groupe de Galois sont donnés par l'application identité ainsi que $\sigma(a + b\sqrt{-5}) = a - b\sqrt{-5}$. Bref, les éléments τ de $Gal(\mathbb{Q}(\sqrt{-5}))$ sont tels que $\tau(\mathcal{P}_i) = \mathcal{P}_j$ pour $i, j \in \{1, 2\}$.

Il se trouve qu'on peut classifier les premiers p de \mathbb{Z} qui se ramifient dans K .

Théorème 1.1.38. Soit K un corps de nombres. Un premier p de \mathbb{Z} est ramifié dans K ssi $p|\Delta_K$.

DÉMONSTRATION. Consulter [38, Théorème 24 (\implies) et 34 (\impliedby)] pour la preuve. Notons que la preuve (\impliedby) utilise de la théorie Galois que nous ne couvrons pas dans ce mémoire. □

Plus particulièrement, on peut classifier complètement la décomposition des premiers impairs dans les extensions $\mathbb{Q}(\sqrt{m})$ de \mathbb{Q} .

Théorème 1.1.39. Soit $K = \mathbb{Q}(\sqrt{m})$ tel que m ne possède pas de carré dans sa factorisation. Si $p|m$, alors (p) se ramifie. Sinon, si p est impair, alors (p) se sépare lorsque m est un carré (mod p) et reste premier sinon.

DÉMONSTRATION. Voir [38, Théorème 25]. □

1.1.5. La théorie de Minkowski

La théorie de Minkowski repose sur l'idée fondamentale que les éléments des extensions de corps de nombres peuvent être étudiés géométriquement. En conséquence, cette théorie est aussi appelée la géométrie des nombres. Spécifiquement, on considérera l'injection d'un corps de nombres K de degré n dans \mathbb{R}^n . Soient $\sigma_1, \dots, \sigma_n$, les injections de K dans \mathbb{C} . Si $\sigma_i(K) \subseteq \mathbb{R}$ alors on dit que σ_i est une injection réelle. Sinon, on dira qu'elle est une injection complexe. On a toujours un nombre pair d'injections complexes puisque chacune est associée à son injection conjuguée $\bar{\sigma}$.

Pour les différencier, on note $\sigma_1, \dots, \sigma_{r_1}$ les r_1 injections réelles $K \hookrightarrow \mathbb{R}$ et $\tau_1, \bar{\tau}_1, \dots, \tau_{r_2}, \bar{\tau}_{r_2}$ les $2r_2$ injections complexes $K \hookrightarrow \mathbb{C}$. L'injection convoitée est donnée par

$$K \rightarrow \mathbb{R}^n, \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \operatorname{Re} \tau_1(\alpha), \operatorname{Im} \tau_1(\alpha), \dots, \operatorname{Re} \tau_{r_2}(\alpha), \operatorname{Im} \tau_{r_2}(\alpha)).$$

On s'intéresse à l'image de O_K par l'injection $K \rightarrow \mathbb{R}^n$. Elle aura la forme de ce qu'on appelle un réseau:

Définition 1.1.40. Un **réseau** de dimension n est un \mathbb{Z} -module libre sur une base générant le \mathbb{R} -espace vectoriel \mathbb{R}^n . Pour $\lambda_1, \dots, \lambda_n$ une base de Λ_K , le **paralléloépe fondamental** est l'ensemble

$$\left\{ \sum_{j=1}^n a_j \lambda_j : 0 \leq a_j < 1 \right\}.$$

Théorème 1.1.41. L'image de O_K par l'injection $K \rightarrow \mathbb{R}^n$ forme un **réseau** de dimension n noté Λ_K . Le volume du paralléloépe fondamental est donné par

$$\frac{1}{2^{r_2}} \sqrt{|\Delta_K|}.$$

DÉMONSTRATION. Si $\alpha_1, \dots, \alpha_n$ est une base de O_K comme \mathbb{Z} -module alors le résultat équivaut à montrer que les images des éléments α_j dans \mathbb{R}^n sont linéairement indépendantes sur \mathbb{R} . Pour ce faire, on calcule le déterminant de la matrice $n \times n$ ayant comme rangée j l'image de α_j dans \mathbb{R}^n . Mais alors, pour chaque paire d'injections complexes, on peut ajouter la colonne $-i \operatorname{Im} \tau_k(\alpha_j)$ à la colonne $\operatorname{Re} \tau_k(\alpha_j)$ pour trouver $\bar{\tau}_k(\alpha_j)$ et finalement, si on multiplie la colonne $\operatorname{Im} \tau_k(\alpha_j)$ par $2i$, on peut y ajouter la colonne $\bar{\tau}_k(\alpha_j)$ pour trouver la matrice $[\sigma_k(\alpha_j)]$. Le déterminant de cette matrice diffère de notre matrice initiale par un facteur de $\frac{1}{(2i)^{r_2}}$ et est non nul par la Proposition 1.1.16. \square

Exemple 1.1.42. On a montré plus tôt que $O_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$. Une base de $\mathbb{Z}[\sqrt{2}]$ était donné par $\{1, \sqrt{2}\}$ et comme les injections de K sont l'identité et $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, l'image

de la base par $K \rightarrow \mathbb{R}^2$ est $\{(1,1), (\sqrt{2}, -\sqrt{2})\}$. Le volume de son paralléloétope fondamental est $2\sqrt{2}$.

Un résultat clé donné par la théorie de Minkowski est

Théorème 1.1.43. *Chaque idéal non trivial \mathfrak{a} de O_K contient un élément $\alpha \in \mathfrak{a}$ différent de zéro tel que*

$$|N(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|} \mathcal{N}(\mathfrak{a}).$$

DÉMONSTRATION. Consulter [38, Théorème 37]. \square

Rappelons la définition de h_K , l'ordre du groupe des classes $Cl_K = J_K/P_K$. Une des conséquences du Théorème 1.1.43 est le résultat

Théorème 1.1.44. *Le nombre de classes h_K est fini.*

DÉMONSTRATION. Pour obtenir ce résultat, on montre les deux faits suivants:

(1) Soit $B \in \mathbb{R}_{>0}$. Il existe un nombre fini d'idéaux $\mathfrak{a} \subset O_K$ tels que $\mathcal{N}(\mathfrak{a}) \leq B$.

(2) Si $[\mathfrak{a}] \in Cl_K$ alors il existe un représentant de la classe $\tilde{\mathfrak{a}}$ tel que $\mathcal{N}(\tilde{\mathfrak{a}}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}$.

Il est immédiat que ces deux faits impliquent que le nombre de classes est fini.

D'une part, on a vu au Théorème 1.1.21 que pO_K se factorise en un nombre fini de premiers; le nombre d'idéaux premiers $\mathcal{P} \subset O_K$ au-dessus de chaque premier p est fini. De plus, pour un idéal \mathcal{P} au-dessus de p , la Proposition 1.1.33 implique que $\mathcal{N}(\mathcal{P}) \geq p$. Ainsi, comme il existe un nombre fini de nombres premiers tels que $p \leq B$ on conclut qu'il existe un nombre fini d'idéaux premiers \mathcal{P} de O_K qui sont bornés par B . On les dénote ici par $\mathcal{Q}_1, \dots, \mathcal{Q}_m$. Maintenant, par la factorisation unique des idéaux et puisque la norme sur les idéaux est multiplicative, les seuls idéaux ayant leur norme bornée par B sont engendrés par la liste $\mathcal{Q}_1, \dots, \mathcal{Q}_m$. Ils sont tels que

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathcal{Q}_1)^{v_1} \dots \mathcal{N}(\mathcal{Q}_m)^{v_m} \geq q_1^{v_1} \dots q_m^{v_m}.$$

et $v_i \geq 0$. Comme il existe seulement un nombre fini de choix de v_1, \dots, v_m positifs tels que $q_1^{v_1} \dots q_m^{v_m} \leq B$, on conclut qu'il existe un nombre fini d'idéaux bornés par B .

D'autre part, si \mathfrak{a} est un représentant de $[\mathfrak{a}] \in Cl_K$, on peut toujours choisir $\gamma \in O_K \setminus \{0\}$ tel que $\gamma\mathfrak{a}^{-1} \subset O_K$. En effet, \mathfrak{a}^{-1} est de type fini et on peut écrire $\mathfrak{a}^{-1} = (\alpha_1, \dots, \alpha_l)$. Ainsi, pour chacun de ses générateurs α_i , il existe γ_i tel que $\gamma_i\alpha_i \in O_K$ par la Proposition 1.1.9. Ceci suggère $\gamma = \gamma_1 \dots \gamma_l$. Maintenant, par le Théorème 1.1.43, il existe $\alpha \in \gamma\mathfrak{a}^{-1}$ tel que

$$|N(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|} \mathcal{N}(\gamma\mathfrak{a}^{-1}) \iff |N(\alpha)| \mathcal{N}(\gamma\mathfrak{a}^{-1})^{-1} = \mathcal{N}(\alpha\gamma^{-1}\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}.$$

L'idéal $\alpha\gamma^{-1}\mathbf{a}$ ne diffère de \mathbf{a} que par la multiplication d'idéaux principaux; ils sont dans la même classe. \square

Une conséquence de la partie (2) de la preuve précédente et du fait que la norme des idéaux est toujours strictement positive est

Corollaire 1.1.45. *Soit $n = [K : \mathbb{Q}] = r_1 + 2r_2$. Le discriminant de K , Δ_K , possède la borne inférieure*

$$\left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!} \leq \sqrt{|\Delta_K|}.$$

Remarque 1.1.46. Notons que puisque $\pi \leq 4$ et que $r_2 \leq n/2$ on peut obtenir une borne inférieure plus faible qui ne dépend que de n :

$$\left(\frac{\pi}{4}\right)^{\frac{n}{2}} \frac{n^n}{n!} \leq \sqrt{|\Delta_K|}$$

À partir de l'approximation de Stirling [2], on remarque que le terme dominant de cette borne inférieure est donné par $\left(\frac{\sqrt{\pi e}}{2}\right)^n \approx 2.41^n$. En ignorant un nombre fini d'exceptions, on peut obtenir une meilleure borne inférieure. Soit

$$\delta(n) = \min_{d_K=n} |\Delta_K|,$$

le minimum de la valeur absolue du discriminant parmi les corps de nombres de degré n . Maintenant, si

$$D = \liminf_{n \rightarrow \infty} \delta(n)^{1/n}.$$

alors c'est, entre autres, la combinaison des efforts de Hajir, Maire, Ramakrishna, Martinet et Odlyzko [18, 39, 45] que,

$$22 \leq D \leq 79.$$

Une dernière conséquence de la théorie de Minkowski est ce qu'on appelle le théorème d'Hermite.

Théorème 1.1.47 (Hermite). *Il existe un nombre fini de corps de nombres avec discriminant Δ_K borné.*

Par le Corollaire 1.1.45, on est réduit à montrer qu'il existe un nombre fini de corps possédant un discriminant Δ_K donné. La preuve est aussi basée sur la théorie de Minkowski [41].

En terminant, il est possible de faire une étude analogue sur le groupe K^* . Dans ce cas, l'injection que l'on considère est donnée par

$$K^* \rightarrow \mathbb{R}^{r_1+r_2}, \quad \text{où } \alpha \mapsto (\log |\sigma_1(\alpha)|, \dots, \log |\sigma_{r_1}(\alpha)|, \log |\tau_1(\alpha)|^2, \dots, \log |\tau_{r_2}(\alpha)|^2).$$

Ici, la remarque intéressante est que pour un élément $\alpha \in \mathbb{Q}$, le logarithme de la valeur absolue de sa norme est donnée par

$$\log |N(\alpha)| = \log |\sigma_1(\alpha)| + \dots + \log |\sigma_{r_1}(\alpha)| + \log |\tau_1(\alpha)| + \log |\overline{\tau_1(\alpha)}| + \dots + \log |\overline{\tau_{r_2}(\alpha)}|.$$

Si $u \in K^*$ est un élément inversible, $\log |N(u)| = 0$ (Exemple 1.1.14) et on voit que les éléments de K^* sont tous envoyés dans l'hyperplan

$$x_1 + x_2 + \dots + x_{r_1+r_2} = 0.$$

En particulier, on peut montrer que O_K^* forme un réseau dans H . Ceci implique

Théorème 1.1.48 (Théorème des unités de Dirichlet). *Le groupe O_K^* est un \mathbb{Z} -module de type fini et de rang $r_1 + r_2 - 1$.*

DÉMONSTRATION. Voir [38, Théorème 38]. □

1.1.6. La fonction zêta de Dedekind

La fonction zêta de Riemann est une fonction qui suscite beaucoup d'intérêt en théorie des nombres. Pour un corps de nombres K , on définit la **fonction zêta de Dedekind**.

$$\zeta_K(s) = \sum_{\mathfrak{a} \neq 0} \frac{1}{\mathcal{N}(\mathfrak{a})^s},$$

où la somme est prise sur les idéaux de O_K et $\mathcal{N}(\mathfrak{a})$ représente la norme de ces idéaux.

Comme pour la fonction zêta de Riemann, il est possible d'exprimer ζ_K sous la forme d'un produit eulérien

Proposition 1.1.49. *La série ζ_K converge absolument et uniformément lorsque $\text{Re}(s) > 1$. Dans cette région, on peut écrire la série comme un produit eulérien*

$$\zeta_K(s) = \prod_{\mathcal{P}} \frac{1}{1 - \mathcal{N}(\mathcal{P})^{-s}}.$$

DÉMONSTRATION. Voir [41, Chapitre 7]. En fait, [30, Chapitre 8] prend cette expression comme définition. □

Exemple 1.1.50. Soit \mathbb{Q} les nombres rationnels, on vérifie que $\zeta_{\mathbb{Q}} = \zeta$. Dans ce cas, les idéaux peuvent être représentés par les nombres naturels $n \in \mathbb{N}$. On aura donc un unique

n pour chaque \mathbf{a} tel que $\mathbf{a} = (n)$. De plus, la norme de ces idéaux est tout simplement $\mathcal{N}(n\mathbb{Z}) = n$. On retrouve ainsi la fonction zêta de Riemann.

On note toujours les injections de K dans \mathbb{C} , $\sigma_1, \dots, \sigma_n$ et on appelle le couple (r_1, r_2) la signature de K lorsque r_1 est le nombre d'injections réelles et r_2 est le nombre de paires d'injections complexes.

Bien que dans ce qui précède, la somme ne soit restreinte à $\operatorname{Re}(s) > 1$, il existe une continuation analytique à tout le plan complexe \mathbb{C} sauf un pôle à $s = 1$. Le résidu de ce pôle est donné par ce qu'on appelle l'équation du nombre de classes.

Théorème 1.1.51 (Formule du nombre de classes). *Soient Δ_K , le discriminant de K , ω_K le nombre de racines de l'unité dans K , (r_1, r_2) la signature de K ainsi que l'invariant R_K qu'on appelle le régulateur. On a la limite*

$$\lim_{s \rightarrow 1} (s-1)\zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} R_K h_K}{\omega_K \Delta_K^{1/2}}$$

DÉMONSTRATION. [30, Chapitre 8] □

Le nombre h_K associé au corps K est très important, en particulier, on sait que $h_K = 1$ ssi l'anneau des entiers est principal. Cette formule nous donne donc une autre méthode pour déterminer si nous avons la factorisation unique dans l'anneau des entiers.

Au-delà de la continuation analytique, il est possible d'obtenir une formule concrète qui relie la section du plan complexe $\sigma > 1$ à la section $\sigma < 0$. Cette formule fait apparaître, entre autre, la fonction Gamma définie par

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt. \tag{1.1.1}$$

C'est une fonction très importante en théorie des nombres puisqu'elle étend la fonction factorielle sur les entiers. Sur ceux-ci, on a la relation $\Gamma(n) = (n-1)!$. Nous approfondirons l'étude de cette fonction au Chapitre 3.

On termine cette section en présentant la formule concrète mentionnée quelques lignes plus haut

Théorème 1.1.52. *Soient (r_1, r_2) la signature de K et Δ_K le discriminant. La fonction zêta de Dedekind ζ_K est une fonction méromorphe sur $\mathbb{C} \setminus \{1\}$. Elle satisfait une équation fonctionnelle*

$$\zeta_K(s) = \zeta_K(1-s) \frac{\Gamma_{\mathbb{R}}(1-s)^{r_1} \Gamma_{\mathbb{C}}(1-s)^{r_2}}{\Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2}} |\Delta_K|^{\frac{1}{2}-s}$$

avec

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2), \quad \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s} \Gamma(s).$$

Enfin, en posant $\xi_K(s) = \zeta_K(s) \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} |\Delta_K|^{\frac{s}{2}}$ on peut écrire tout simplement

$$\xi_K(s) = \xi_K(1-s).$$

DÉMONSTRATION. Ce résultat requiert beaucoup de travail. Le [30, Chapitre 13] présente la preuve plus classique d'Hecke alors que le [30, Chapitre 14] présente ce qu'on appelle « la thèse de Tate ». La Section 1.3 présentera en surface des idées qui prennent un point de vue similaire à celui pris par Tate dans sa preuve. \square

Ce théorème nous donne beaucoup d'information sur le comportement de la fonction zêta de Dedekind dans la section $\sigma < 0$. Elle jouera un rôle central dans le Chapitre 3. Enfin, on peut énoncer l'hypothèse de Riemann généralisée que nous avons mentionnée dans l'introduction:

Conjecture 1.1.53. *Soit K un corps de nombres. Si s est un zéro de ζ_K tels que $0 \leq \operatorname{Re}(s) \leq 1$ alors $\operatorname{Re}(s) = 1/2$.*

Cette conjecture suscite l'attention de beaucoup de mathématiciens à travers le monde et reste ouverte à ce jour. Consulter le texte [26, Chapitre 6] pour de plus amples détails.

Ceci termine notre aperçu sur la théorie algébrique des nombres élémentaire sur les corps de nombres. Dans la prochaine section, on va voir qu'il existe d'autres objets mathématiques qui ressemblent aux corps de nombres.

1.2. L'analogie des corps de fonctions

L'analogie des corps de fonctions provient des multiples ressemblances entre $\mathbb{F}_q[t]$, l'anneau des polynômes à une variable avec coefficients dans le corps fini \mathbb{F}_q , et \mathbb{Z} , les nombres entiers. On parle d'analogie puisque, d'une part, plusieurs théorèmes sont vrais dans les deux environnements et d'autre part, ils sont en général plus facilement prouvés sur $\mathbb{F}_q[t]$. Plusieurs exemples de la première affirmation seront présentés d'entrée de jeu, mais on devra attendre un peu avant de voir apparaître des preuves plus simples.

1.2.1. Propriétés de $\mathbb{F}_q[t]$

Soit \mathbb{F}_q , le corps fini à $q = p^n$ éléments, une puissance d'un nombre premier. L'exemple le plus simple est tout simplement le corps $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ et les corps \mathbb{F}_{p^r} peuvent être compris comme des extensions de \mathbb{F}_p .

Les éléments de $\mathbb{F}_q[t]$ sont donc tous de la forme $a_n t^n + \dots + a_1 t + a_0$ avec $a_i \in \mathbb{F}_q$. Quand le coefficient dominant, a_n , est non nul, on dit que le degré du polynôme est n .

Le théorème suivant résume des résultats de base sur cet objet.

Théorème 1.2.1. *L'anneau $\mathbb{F}_q[t]$ possède les propriétés suivantes:*

- *C'est un anneau euclidien.*
- *Soit $f(t) \in \mathbb{F}_q[t]$ non nul, le quotient $\mathbb{F}_q[t]/f\mathbb{F}_q[t]$ contient exactement $q^{\deg(f)}$ éléments.*
- *L'ensemble des éléments inversibles de $\mathbb{F}_q[t]$ est \mathbb{F}_q^* .*

Une conséquence directe, analogue aux entiers, est la factorisation unique en éléments premiers (c'est-à-dire, des polynômes moniques irréductibles). Plus précisément, tout élément non nul s'écrit

$$f = \alpha p_1^{e_1} p_2^{e_2} \dots p_k^{e_k},$$

pour $\alpha \in \mathbb{F}_q^*$ un élément inversible de l'anneau, $e_i \in \mathbb{Z}_{\geq 0}$ des entiers et p_i des éléments premiers.

Exemple 1.2.2. Dans l'anneau $\mathbb{F}_2[t]$, on peut factoriser le polynôme $x^2 + 1 = (x + 1)^2$.

Définition 1.2.3. Soit $f \in \mathbb{F}_q[t] \setminus \{0\}$. On définit $|f| = q^{\deg(f)}$ et $|0| = 0$.

Remarquons que cette norme est la même que $\mathcal{N}(f\mathbb{F}_q[t])$, car $[\mathbb{F}_q[t] : f\mathbb{F}_q[t]] = q^{\deg(f)}$ par le Théorème 1.2.1. On termine cette introduction avec des théorèmes qui ont tous des analogues sur les nombres entiers. On commence avec le nombre d'éléments inversibles modulo p^e ,

Proposition 1.2.4. *Le groupe des éléments inversibles $\left(\frac{\mathbb{F}_q[t]}{p^e\mathbb{F}_q[t]}\right)^*$ contient $|p|^e(|p| - 1)$ éléments.*

DÉMONSTRATION. Voir [51, Proposition 1.6]. □

Dans les entiers, l'indicatrice d'Euler, ϕ , qui pour tout entier n compte le nombre d'éléments $1 \leq a \leq n$ coprimiers à n peut être définie comme la fonction

$$\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|.$$

On aimerait définir une fonction Φ analogue sur les éléments de $\mathbb{F}_q[t]$. Pour tout élément non nul $f \in \mathbb{F}_q[t]$, on comptera le nombre d'éléments de $\mathbb{F}_q[t]$ coprimiers à f qui ont un degré strictement inférieur à $\deg(f)$. Il est immédiat que ces polynômes forment un ensemble de

représentants pour $(\mathbb{F}_q[t]/f\mathbb{F}_q[t])^*$ et on peut récupérer une analogie claire

$$\Phi(f) := |(\mathbb{F}_q[t]/f\mathbb{F}_q[t])^*|.$$

On liste finalement des identités qui ont une forme bien familière [51, Propositions 1.7 et 1.8]

$$\Phi(f) = |f| \prod_{p|f} (1 - |p|^{-1}).$$

Si $f, a \in \mathbb{F}_q[t]$, f non nul et $(a, f) = 1$ alors

$$a^{\Phi(f)} \equiv 1 \pmod{f}. \text{ (Théorème de Euler)}$$

En particulier, si p est un polynôme monique et irréductible et $a \in \mathbb{F}_q[t]$ est copremier à p ,

$$a^{|p|-1} \equiv 1 \pmod{p}. \text{ (Petit Théorème de Fermat)}$$

1.2.2. Les corps algébriques de fonctions

Le passage aux corps de fonctions est souvent expliqué comme le passage des rationnels aux corps de nombres. Une différence clé dans cette section est que l'on mettra moins d'emphase sur le corps de base. Nous avons la définition suivante,

Définition 1.2.5. Soit \mathbb{F}_q un corps fini. Un **corps de fonctions** K à une variable sur \mathbb{F}_q est une extension algébrique finie et séparable de $\mathbb{F}_q(x)$ pour un certain élément $x \in K$ transcendant sur \mathbb{F}_q .

Remarque 1.2.6. Pour un rappel sur la théorie des corps, voir [16, Section 13].

En particulier, le théorème de l'élément primitif [16] nous permet de reformuler cette définition de la manière suivante: Un corps de fonctions $K = \mathbb{F}_q(x, \alpha)$ est tel que

- $x \in K$ transcendant sur \mathbb{F}_q .
- $\alpha \in K$ algébrique sur $\mathbb{F}_q(x)$.

Si K est un corps de fonctions sur \mathbb{F}_q , remarquons que l'ensemble $F = \{z \in K : z \text{ algébrique sur } \mathbb{F}_q\}$ est un sous-corps de K car les éléments algébriques sont fermés sous la somme, le produit et l'inversion. On appelle F le corps des constantes de K . Comme $\mathbb{F}_q \subseteq F \subsetneq K$, on voit que K est également un corps de fonctions sur F . Si $F = \mathbb{F}_q$, on dira que \mathbb{F}_q est algébriquement clos dans K . En remplaçant \mathbb{F}_q par F au besoin, on supposera toujours que \mathbb{F}_q est algébriquement clos dans K . (Il est clair que $[F : \mathbb{F}_q]$ est fini, car $[F : \mathbb{F}_q] = [F(x) : \mathbb{F}_q(x)] \leq [K : \mathbb{F}_q(x)]$.)

Exemple 1.2.7. Le corps des fractions de $\mathbb{F}_q[t]$, $\mathbb{F}_q(t)$ est un corps de fonctions.

Exemple 1.2.8. Soit l'anneau $\mathbb{F}_q[x, y]$. On peut considérer l'idéal $(y^2 - x^3 + x)$. Si K est le corps des fractions du quotient $\mathbb{F}_q[x, y]/(y^2 - x^3 + x)$ alors K est un corps de fonctions. Notons qu'ici, on peut représenter K comme $\mathbb{F}_q(x, \sqrt{x^3 - x})$.

Remarque 1.2.9. Le choix de x n'est pas nécessairement unique. Ainsi, la notion de degré $[K : \mathbb{F}_q(x)]$ dépend du choix de x . En effet, bien que dans l'exemple précédent $[K : \mathbb{F}_q(x)] = 2$, il est intéressant de noter que $[K : \mathbb{F}_q(y)] = 3$.

Exemple 1.2.10. De manière similaire aux corps de nombres, si $[K : \mathbb{F}_q(x)] = n$, on peut écrire

$$\mathbb{F}_q(x, \alpha) = \{f_0 + f_1\alpha + \dots + f_{n-1}\alpha^{n-1} : f_i \in \mathbb{F}_q(x)\}.$$

On tourne maintenant notre attention vers le concept de primalité dans les corps de fonctions. L'anneau des entiers était un concept focal de notre traitement des corps de nombres à la Section 1.1. Un problème survient dans les corps de fonctions puisque la Définition 1.1.7 d'anneau des entiers dépendrait d'un anneau analogue aux entiers et, comme on l'a vu à la Remarque 1.2.9, il dépendrait de notre choix d'élément transcendant.

Pour obtenir ce qu'on appelle les premiers de K , on utilise alors une autre approche que dans le contexte des corps de nombres, où l'on considérerait les idéaux premiers de l'anneau des entiers:

Définition 1.2.11. Soit K , un corps de fonctions. Un **premier** de K est un anneau principal A tel que:

- (1) $\mathbb{F}_q \subset A \subset \text{frac}(A) = K$ où $\text{frac}(A)$ est le corps des fractions de A .
- (2) A possède un unique idéal maximal \mathcal{P} .

Il est commun d'identifier l'anneau principal A à son idéal maximal \mathcal{P} . En fait, lorsque le contexte n'est pas ambigu, on écrira \mathcal{P} au lieu de A pour signifier l'anneau principal en même temps que son idéal maximal.

Exemple 1.2.12. Dans $\mathbb{F}_q(t)$, la localisation à un polynôme irréductible $p(t)$ définie par

$$[\mathbb{F}_q(t)]_{p(t)} := \left\{ \frac{a(t)}{b(t)} \in \mathbb{F}_q(t) : p(t) \nmid b(t) \right\}$$

est un premier de K contenant l'idéal maximal $(p(t))$ tel que $\mathbb{F}_q \subset [\mathbb{F}_q(t)]_{p(t)} \subset \mathbb{F}_q(t)$.

Soit \mathcal{P} un premier, son degré est défini comme l'index de son corps résiduel avec le corps de base $\text{deg}(\mathcal{P}) = [A/\mathcal{P} : \mathbb{F}_q]$.

L'exemple 1.2.12 nous permet déjà de retrouver les polynômes irréductibles qu'on avait mentionné à la Section 1.2.1.

Il est utile d'avoir une autre description des premiers de K .

Définition 1.2.13. Une **valuation discrète** de K est une fonction $v : K^* \rightarrow \mathbb{Z}$ telle que

- (1) $v(xy) = v(x) + v(y)$.
- (2) L'application v est surjective.
- (3) Si $x, y \in K^*$ sont tels que $x + y \neq 0$, alors $v(x + y) \geq \min\{v(x), v(y)\}$.

On montre que les premiers de K donnent tous lieu à des valuations discrètes.

Proposition 1.2.14. *Si \mathcal{P} est un premier de K . Il existe une fonction $v_{\mathcal{P}}$ associée à son idéal maximal qui est une valuation discrète de K .*

DÉMONSTRATION. Les anneaux de la Définition 1.2.11 possèdent un unique idéal maximal principal \mathcal{P} . Si t est un générateur de cet idéal, les éléments de K s'écrivent uniquement comme $z = ut^n$ pour $u \in A^*$ et on peut définir $v_{\mathcal{P}} : K^* \rightarrow \mathbb{Z}$ comme $v_{\mathcal{P}}(z) = v_{\mathcal{P}}(ut^n) := n$. Cette fonction respecte déjà les propriétés (1) et (2) de la Définition 1.2.13 et on peut montrer qu'elle respecte aussi la troisième: Soient $x, y \in K^*$ tels que $x + y \neq 0$. On peut écrire $x + y = u_1t^n + u_2t^m = t^n(u_1 + u_2t^{m-n})$. Ici, SPDG, on peut prendre $n \leq m$ pour que $m - n$ soit non négatif. L'élément $u_1 + u_2t^{m-n}$ est donc un élément de A et $v_{\mathcal{P}}(u_1 + u_2t^{m-n}) \geq 0$. Ainsi par la propriété 1,

$$v_{\mathcal{P}}(x + y) = n + v_{\mathcal{P}}(u_1 + u_2t^{m-n}) \geq n.$$

Or on avait pris $n = \min\{v_{\mathcal{P}}(x), v_{\mathcal{P}}(y)\}$ d'où le résultat. \square

Inversement, on peut montrer que toutes les valuations discrètes donnent lieu à des premiers de K .

Proposition 1.2.15. *Soit v , une valuation discrète de K . L'ensemble*

$$O = \{z \in K : v(z) \geq 0\},$$

est un premier de K .

DÉMONSTRATION. Consulter [41, Proposition 3.9]. \square

Exemple 1.2.16. Soit $a(t) \in \mathbb{F}_q[t]$. Par la remarque suivant le Théorème 1.2.1, on peut écrire $a(t) = p_1(t)^{e_{p_1}} \cdots p_r(t)^{e_{p_r}}$ où $e_{p_i} \in \mathbb{Z}$ et $p_i(t)$ sont des polynômes irréductibles sur $\mathbb{F}_q[t]$. La valuation attachée aux premiers de l'Exemple 1.2.12 est donnée par

$$v_p(a(t)) = v_p(u(t)p(t)^{e_p}) := e_p$$

où $p(t)$ ne divise pas $u(t)$ ou son inverse.

Ceci couvre presque tous les premiers de $\mathbb{F}_q(t)$. En fait, il n'en existe qu'un autre:

Théorème 1.2.17. *Les premiers de $\mathbb{F}_q(t)$ sont donnés par la localisation de $\mathbb{F}_q[t]$ à ses irréductibles ou par la localisation de $\mathbb{F}_q[1/t]$ à $(1/t)$.*

DÉMONSTRATION. Consulter [57, Proposition 1.2.2] pour plus de détails. Cette preuve est pratique puisqu'elle propose une simplification de $[\mathbb{F}_q(1/t)]_{1/t}$. En effet, on trouve que

$$\begin{aligned} [\mathbb{F}_q(1/t)]_{1/t} &= \left\{ \frac{a(t^{-1})}{b(t^{-1})} \in \mathbb{F}_q(t^{-1}) : t^{-1} \nmid b(t^{-1}) \right\} \\ &= \left\{ \frac{u(t)}{v(t)} \in \mathbb{F}_q(t) : \deg(u) \leq \deg(v) \right\}. \end{aligned}$$

□

Remarque 1.2.18. On appellera ce dernier le premier à l'infini et on le notera P_∞ . La valuation attachée à P_∞ est donnée par $v_\infty(a) = v_\infty(f(t)/g(t)) = \deg(g) - \deg(f)$. En effet, on peut voir explicitement v_∞ de la manière suivante: Soit

$$\frac{f(x)}{g(x)} = \frac{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0}{b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0},$$

avec $a_n, b_m \neq 0$. En écrivant $x = t^{-1}$, on trouve

$$\begin{aligned} \frac{f(t^{-1})}{g(t^{-1})} &= \frac{a_n (t^{-1})^n + a_{n-1} (t^{-1})^{n-1} + \cdots + a_1 t^{-1} + a_0}{b_m (t^{-1})^m + b_{m-1} (t^{-1})^{m-1} + \cdots + b_1 t^{-1} + b_0} \\ &= \frac{t^{-n} a_n + a_{n-1} t + \cdots + a_1 t^{n-1} + a_0 t^n}{t^{-m} b_m + b_{m-1} t + \cdots + b_1 t^{m-1} + b_0 t^m} \\ &= t^{m-n} \frac{a_n + a_{n-1} t + \cdots + a_1 t^{n-1} + a_0 t^n}{b_m + b_{m-1} t + \cdots + b_1 t^{m-1} + b_0 t^m}. \end{aligned}$$

Une remarque importante est que t ne divise pas $a_n + a_{n-1}t + \cdots + a_1 t^{n-1} + a_0 t^n$ et $b_m + b_{m-1}t + \cdots + b_1 t^{m-1} + b_0 t^m$ car $a_n, b_m \neq 0$. Une conséquence de cette transformation est que

$$[\mathbb{F}_q(1/x)]_{1/x} = [\mathbb{F}_q(t)]_t = \left\{ \frac{a(t)}{b(t)} \in \mathbb{F}_q(t) : t \nmid b(t) \right\}$$

Ici, on voit que v_∞ est simplement $v_{(t)}$. Ainsi, comme $v_{(t)}\left(\frac{f(t^{-1})}{g(t^{-1})}\right) = m - n$ alors $v_\infty\left(\frac{f(x)}{g(x)}\right) = \deg(g) - \deg(f)$.

1.2.3. Diviseurs

La factorisation des idéaux dans les corps de nombres était un résultat central. On a une version similaire, mais pas tout à fait analogue, qu'on présente sous la forme des **diviseurs**.

Définition 1.2.19. Le groupe des diviseurs de K , \mathcal{D}_K est défini comme le groupe abélien libre généré par les premiers de K . On notera $D \in \mathcal{D}_K$ additivement: $D = \sum_{\mathcal{P}} n_{\mathcal{P}} \mathcal{P}$ avec $n_{\mathcal{P}} \in \mathbb{Z}$.

Dans ce contexte, D est complètement déterminé par ses coefficients $n_{\mathcal{P}}$ qu'on notera parfois $v_{\mathcal{P}}(D)$. Lorsque que la multiplicité des facteurs premiers est positive pour tout \mathcal{P} , c'est-à-dire que $n_{\mathcal{P}} \geq 0$, on écrira $D \geq 0$. On appelle ces diviseurs les **diviseurs effectifs**.

Définition 1.2.20. Le degré d'un diviseur est défini par

$$\deg(D) = \sum_{\mathcal{P}} n_{\mathcal{P}} \deg(\mathcal{P}),$$

où \deg est un homomorphisme de \mathcal{D}_K à \mathbb{Z} .

Soit $a \in K^*$, le diviseur de a est défini par $(a) = \sum_{\mathcal{P}} v_{\mathcal{P}}(a) \mathcal{P}$. C'est bien un diviseur, car $v_{\mathcal{P}}(a)$ est non nul uniquement pour un nombre fini de \mathcal{P} . On appelle ces diviseurs les diviseurs principaux et on note Pr_K l'ensemble des diviseurs principaux de K .

Si \mathcal{P} est un premier K tel que $v_{\mathcal{P}}(a) > 0$, on dit que \mathcal{P} est un zéro de a . Si $v_{\mathcal{P}}(a) < 0$, on dit que \mathcal{P} est un pôle de a . Dans les deux cas, $|v_{\mathcal{P}}(a)|$ est ce qu'on appelle l'ordre du zéro/pôle. Il peut être pratique de séparer les zéros des pôles. On dénote donc

$$(a)_0 = \sum_{\mathcal{P} \text{ zéro de } a} v_{\mathcal{P}}(a) \mathcal{P} \quad \text{et} \quad (a)_{\infty} = - \sum_{\mathcal{P} \text{ pôle de } a} v_{\mathcal{P}}(a) \mathcal{P}.$$

De cette définition, il suit que $(a) = (a)_0 - (a)_{\infty}$.

Exemple 1.2.21. Soit le corps des fonctions rationnelles $\mathbb{F}_q(t)$. On peut calculer le degré des diviseurs principaux. Si $a \in \mathbb{F}_q$, alors $\deg(a) = 0$ puisque $\text{ord}_P(a) = 0$ pour tout P . Sinon $a(t) = \frac{f(t)}{g(t)}$ tels que $f(t) \in \mathbb{F}_q[t]$ et $g(t) \in \mathbb{F}_q[t] \setminus \{0\}$. Ainsi, on peut factoriser ces polynômes en irréductibles et on trouve que $a(t) = \prod p(t)^{v_p(a)}$. Dans ce contexte, $\deg(P) = \deg(p(t))$ et on trouve que le degré du diviseur principal est donné par $\deg(a) = \deg(f) - \deg(g) + v_{P_{\infty}}(a)$. Or, on a mentionné plus tôt à la Remarque 1.2.18 que $v_{P_{\infty}}(a) = \deg(g) - \deg(f)$ et le degré des diviseurs principaux est $\deg(a) = 0$.

C'est aussi le cas en général,

Théorème 1.2.22. Soit $a \in K^*$, on a la formule $\deg(a) = 0$.

IDÉE DE LA PREUVE. En général, pour les éléments $a \in K \setminus \mathbb{F}_q$, on considère la fermeture algébrique A de $\mathbb{F}_q[a]$ dans K . On peut montrer que dans cet anneau, l'idéal engendré par a admet la factorisation $(a) = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \cdots \mathcal{P}_r^{e_r}$ et que la localisation de A à ces idéaux \mathcal{P}_i coïncide avec les zéros de a . Finalement, un résultat analogue au Théorème 1.1.35 nous permet de conclure que $\deg(a)_0 = [K : \mathbb{F}_q[a]]$. Le même raisonnement sur $\mathbb{F}_q[1/a]$ donne que $\deg(a)_\infty = \deg(a)_0$. Pour plus de détails consulter [51, Théorème 7.6]. Une autre approche donne une généralisation de ce résultat, en permettant que le corps des constantes ne soit pas parfait: [57, Théorème 1.4.11]. (Notons que comme notre corps des constantes est fini, il est toujours parfait [16, Chapitre 13].) \square

Une façon d'interpréter cette formule est que les éléments $a \in K^*$ possèdent autant de pôles que de zéros. Le quotient des diviseurs de K par les diviseurs principaux, $Cl_K := \mathcal{D}_K / Pr_K$ est le groupe de classes des diviseurs de K . Puisque les diviseurs principaux sont de degré 0, la fonction de degré sera bien définie sur Cl_K . Son noyau, Cl_K^o est appelé le groupe de classes des diviseurs de degré 0. Un invariant important de K est le nombre de classes de degré zéro $h_K = |Cl_K^o|$. C'est un résultat non trivial de F.K. Schmidt [52] que l'application $\deg : Cl_K \rightarrow \mathbb{Z}$ sur les diviseurs de K , un corps de fonctions sur \mathbb{F}_q est surjective. Ainsi, h_K est aussi le nombre de classes de degré n .

Finalement, il sera utile d'introduire une norme pour les diviseurs qu'on définit par $|D| := q^{\deg D}$. Dans $\mathbb{F}_q(t)$, si on considère uniquement les diviseurs finis, cette norme coïncide avec le nombre d'éléments dans le corps résiduel par $(p_1(t))^{n_{p_1(t)}} \cdots (p_k(t))^{n_{p_k(t)}}$, où les $p_i(t)$ sont les générateurs des idéaux premiers dans $\mathbb{F}_q[t]$. On peut comprendre cette norme comme un analogue à celle introduite à la Section 1.1 pour les idéaux.

1.2.4. Les conjectures de Weil

Comme on l'avait fait dans les corps de nombres, on définit une fonction zêta.

Définition 1.2.23. La fonction zêta associé au corps de fonctions K est donnée par

$$\zeta_K(s) = \sum_{A \geq 0} |A|^{-s}$$

où la somme est sur les diviseurs effectifs.

En général, il est commun de réécrire la somme de la fonction ζ_K en fonction du degré,

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{b_n}{q^{ns}}$$

où b_n représente le nombre de diviseurs effectifs ($A \geq 0$) tels que $\deg(A) = n$.

On ne connaît pas encore le domaine de convergence ζ_K . On commence par le cas le plus simple,

Exemple 1.2.24. Si $K = \mathbb{F}_q(t)$ alors ζ_K converge lorsque $\operatorname{Re}(s) > 1$. Dans ce domaine, elle respecte $\zeta_K(s) = \frac{1}{(1-q^{1-s})(1-q^{-s})}$.

DÉMONSTRATION. En effet, dans ce cas, les diviseurs de K sont générés par l'ensemble des polynômes moniques de $\mathbb{F}_q(t)$, qu'on dénote par V_f , ainsi que par \mathcal{P}_∞ , le premier à l'infini. Les diviseurs effectifs $A = \sum_{\mathcal{P}} n_{\mathcal{P}} \mathcal{P}$ sont donc des sommes sur $A = \sum_{V_f \cup \{\mathcal{P}_\infty\}} n_{\mathcal{P}} \mathcal{P}$.

Cette remarque nous permet de réécrire

$$\begin{aligned} \zeta_K(s) &= \sum_{A \geq 0} |A|^{-s} = \sum_{\substack{A \geq 0 \\ \operatorname{ord}_{\mathcal{P}_\infty}(A)=0}} |A|^{-s} + \sum_{\substack{A \geq 0 \\ \operatorname{ord}_{\mathcal{P}_\infty}(A)=1}} |A|^{-s} + \dots \\ &= \sum_{\substack{A \geq 0 \\ \operatorname{ord}_{\mathcal{P}_\infty}(A)=0}} |A|^{-s} + |\mathcal{P}_\infty|^{-s} \sum_{\substack{A \geq 0 \\ \operatorname{ord}_{\mathcal{P}_\infty}(A)=0}} |A|^{-s} + \dots \end{aligned}$$

Ainsi, on peut mettre en évidence la somme sur les premiers finis pour trouver

$$\zeta_K(s) = \left(\sum_{n \geq 0} |\mathcal{P}_\infty|^{-ns} \right) \sum_{\substack{A \geq 0 \\ \operatorname{ord}_{\mathcal{P}_\infty}(A)=0}} |A|^{-s} = \left(\sum_{n \geq 0} q^{-ns} \right) \sum_{\substack{A \geq 0 \\ \operatorname{ord}_{\mathcal{P}_\infty}(A)=0}} |A|^{-s}$$

On tente maintenant d'évaluer la somme contenant uniquement les premiers finis. Si on fixe le degré, $\deg A = n$, on peut montrer ces éléments sont en correspondances avec les polynômes moniques $f(t) \in \mathbb{F}_q[t]$ de degré n . Comme il y en a q^n , on trouve

$$\zeta_K(s) = \left(\sum_{n \geq 0} q^{-ns} \right) \sum_{\substack{A \geq 0 \\ \operatorname{ord}_{\mathcal{P}_\infty}(A)=0}} |A|^{-s} = \frac{1}{1-q^{-s}} \sum_{\substack{A \geq 0, \deg A=n \\ \operatorname{ord}_{\mathcal{P}_\infty}(A)=0}} \frac{q^n}{q^{-ns}} = \frac{1}{(1-q^{-s})(1-q^{1-s})}.$$

Remarquons que ce sont des séries géométriques donc le domaine de convergence est clair. De plus, ce résultat donne une continuation méromorphe à la série. \square

Pour être en mesure d'étudier la fonction zêta d'un corps de fonctions en général, et en particulier, trouver son domaine de convergence, on fait un bref détour.

Définition 1.2.25. Soit D un diviseur. On définit $L(D) = \{a \in K^* : (a) + D \geq 0\} \cup \{0\}$.

L'ensemble $L(D)$ est un espace vectoriel de dimension finie sur \mathbb{F}_q . Sa dimension sur \mathbb{F}_q est dénotée par $l(D)$.

Théorème 1.2.26 (Riemann-Roch). *Il existe un diviseur C , appelé le diviseur canonique, tel que pour tout $D \in D_K$,*

$$l(D) = \deg(D) - l(C) + 1 + l(C - D).$$

*De plus, la dimension du diviseur canonique $l(C)$ est un invariant important de K , on le notera par g , le **genre** de K . Finalement, $\deg(C) = 2g - 2$.*

DÉMONSTRATION. Voir [51, Théorème 5.4]. □

Maintenant pour $[A] \in Cl_K$ la classe ayant le diviseur A comme représentant, on a que

Lemme 1.2.27. *Le nombre de diviseurs $D \in [A]$ tels que $D \geq 0$ est donné par $\frac{q^{l(A)} - 1}{q - 1}$.*

DÉMONSTRATION. Si $l(A) = 0$, évidemment, $[A]$ ne contient pas de diviseurs effectifs. Sinon, $l(A) > 0$ et on remarque que chaque diviseur effectif $D \in [A]$ s'écrit comme $D = (a) + A$ donc $a \in L(A) \setminus \{0\}$. Le choix de a est déterminé par D modulo un élément de \mathbb{F}_q^* . On a trouvé que

$$\#\{D \in [A] : D \geq 0\} \# \mathbb{F}_q^* = \#L(A) \setminus \{0\}.$$

□

On avait vu que le degré était bien défini sur les classes de diviseurs. Par définition, la norme le sera également et on peut réécrire

$$\zeta_K(s) = \sum_{D \geq 0} |D|^{-s} = \sum_{[A] \in Cl_K} \#\{D \in [A] : D \geq 0\} |A|^{-s} = \sum_{[A] \in Cl_K} \frac{q^{l(A)} - 1}{q - 1} |A|^{-s}.$$

On a vu que le nombre de classes de degré n dans Cl_K est donné par h_K . De plus, dès que $\deg(A) > 2g - 2$ on trouve que $l(A) = \deg(A) - g + 1$. En effet, lorsque $\deg(A) > 2g - 2$, le diviseur $C - A$ apparaissant dans le Théorème de Riemann-Roch est tel que $\deg(C - A) < 0$. Mais alors, $l(C - A) = 0$, puisque si $a \in L(C - A)$, on a $0 \leq \deg((a) + C - A) = \deg(C - A) < 0$, car le degré est un morphisme et les diviseurs principaux sont de degré zéro; ce qui est impossible. On peut donc séparer la somme

$$\zeta_K(s) = \sum_{\substack{[A] \in Cl_K \\ \deg(A) \leq 2g-2}} \frac{q^{l(A)} - 1}{q - 1} |A|^{-s} + \sum_{n > 2g-2} h_K \frac{q^{n-g+1} - 1}{q - 1} q^{-ns}$$

La somme à droite est géométrique et on peut retrouver le résultat analogue à la Proposition 1.1.49 sur la fonction zêta de Dedekind.

Proposition 1.2.28. *La série ζ_K converge absolument et uniformément lorsque $\operatorname{Re}(s) > 1$. Dans cette région, on peut écrire la série comme un produit eulérien*

$$\zeta_K(s) = \prod_{\mathcal{P}} \left(1 - \frac{1}{|\mathcal{P}|^s} \right)^{-1}.$$

DÉMONSTRATION. La convergence suit immédiatement de la série géométrique. Pour le produit eulérien, la multiplicativité de la norme ainsi que le fait que le groupe des diviseurs est un groupe libre sur l'ensemble des premiers de K nous informe que la preuve est la même qu'à la Proposition 1.1.49. \square

Sans surprise, le fait que la série soit géométrique nous apprend bien plus sur ζ_K que son domaine de convergence.

Théorème 1.2.29. *Soit K un corps de fonctions sur \mathbb{F}_q et g_K le genre K . Il existe un polynôme $L_K(u) \in \mathbb{Z}[u]$ de degré $2g_K$ tel que*

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1 - q^{1-s})(1 - q^{-s})}.$$

Cette relation est vraie lorsque $\operatorname{Re}(s) > 1$ et le côté droit de l'égalité nous fournit une continuation analytique sur tout \mathbb{C} . De plus,

- ζ_K possède des pôles simples à $s = \frac{2\pi in}{\log q}$ et $s = \frac{2\pi im}{\log q} + 1$ pour $m, n \in \mathbb{Z}$.
- $L_K(0) = 1$ et $L_K(1) = h_K$.
- Posons $\xi_K(s) = q^{(g_K-1)s} \zeta_K(s)$ alors $\xi_K(1-s) = \xi_K(s)$.

DÉMONSTRATION. On montre la première affirmation. Pour le reste de la preuve, consulter [51, Théorème 5.9].

Soit $u = q^{-s}$. On avait trouvé la relation,

$$\zeta_K(s) = \sum_{\substack{[A] \in Cl_K \\ \deg(A) \leq 2g-2}} \frac{q^{l(A)} - 1}{q-1} |A|^{-s} + \sum_{n > 2g-2} h_K \frac{q^{n-g+1} - 1}{q-1} q^{-ns}.$$

Remarquons que le terme gauche est un polynôme de degré $2g-2$ en u . Ainsi, en multipliant par le polynôme $(1-u)(1-qu)$ pour avoir le bon dénominateur, on a bel et bien un polynôme de degré $2g$ au numérateur. On peut donc concentrer notre attention sur le terme de droite,

$$\sum_{n > 2g-2} h_K \frac{q^{n-g+1} - 1}{q-1} q^{-ns} = \frac{h_K}{q-1} \left(\frac{q^g}{1-qu} - \frac{1}{1-u} \right) u^{2g-1} = \frac{h_K}{q-1} \frac{q^g - 1 - uq(q^{g-1} - 1)}{(1-qu)(1-u)} u^{2g-1}.$$

On doit donc montrer que $\frac{h_K}{q-1} (q^g - 1 - uq(q^{g-1} - 1)) u^{2g-1}$ est un polynôme de degré $2g$ appartenant à $\mathbb{Z}[u]$. Le degré est clair et le fait que les coefficients sont entiers découle du fait

que $q - 1$ divise $(q^g - 1)$ et $q(q^{g-1} - 1)$ dès que $g \geq 1$. Le cas $g = 0$ provient de l'exemple 1.2.24. \square

Exemple 1.2.30. Lorsque $K = \mathbb{F}_q(t)$, le polynôme $L_K(u) = 1$, ainsi $h_K = 1$ et par le Théorème 1.2.22, les diviseurs de degré zéro sont les diviseurs principaux.

Un résultat très important, vérifié sur les corps de fonctions, est le suivant

Théorème 1.2.31 (L'hypothèse de Riemann pour les corps de fonctions). *Soit K un corps de fonctions sur \mathbb{F}_q . La partie réelle des zéros de ζ_K est $1/2$.*

DÉMONSTRATION. Voir [51, Théorème 5.10]. Ce théorème est dû à Artin pour le cas particulier $g = 1$ puis en général à Weil. Pour un résumé de l'histoire entourant ce résultat voir la discussion juste après [51, Théorème 5.10]. \square

On termine cette courte introduction avec une conséquence de ces théorèmes.

Proposition 1.2.32. *Soit h_K le nombre de classes de diviseurs de degré 0. On a*

$$(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}.$$

DÉMONSTRATION. Par le Théorème 1.2.29, on sait que $h_K = L_K(1) = \prod_{i=1}^{2g} (1 - \pi_i)$. Par l'hypothèse de Riemann sur les corps de fonctions, $|\pi_i| = \sqrt{q}$, ainsi le résultat suit par l'inégalité du triangle. \square

Cette idée fera un retour dans le Chapitre 2.

1.3. Une question de définition

Les Sections 1.1 et 1.2 sont riches en similitudes. Or, les deux présentations reposent sur des idées et des définitions différentes. Cette section a pour but de donner une présentation unifiée des deux derniers chapitres. Paradoxalement, ceci mettra en évidence les différences entre les corps de nombres et les corps de fonctions.

1.3.1. La théorie des valuations

La définition des premiers de la Section 1.2 était basée sur les valuations discrètes. Dans le but de généraliser cette notion aux corps de nombres, on introduit le concept de valuation multiplicative ou encore de valeur absolue.

Définition 1.3.1. Une **valeur absolue** sur un corps K est une application $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$ telle que

- (1) $|\alpha| \geq 0$ pour tout $\alpha \in K$ et $|\alpha| = 0 \iff \alpha = 0$.
- (2) $|\alpha\beta| = |\alpha||\beta|$ pour tout $\alpha, \beta \in K$.
- (3) $|\alpha + \beta| \leq |\alpha| + |\beta|$ pour tout $\alpha, \beta \in K$.

Une valeur absolue sur K introduit une métrique sur l'espace avec la distance $|\alpha - \beta|$.

Définition 1.3.2. On dit que deux valeurs absolues sont équivalentes si la topologie induite par leur métrique respective est la même.

Une question naturelle est d'énumérer les valeurs absolues possibles modulo l'équivalence pour un corps K .

Remarque 1.3.3. Tout corps K possède la valeur absolue triviale donnée par $|\alpha| = 1$ pour tout $\alpha \in K^*$ qui induit la topologie discrète sur K . Lorsqu'on classifera les valeurs absolues sur K on ignorera toujours la valeur absolue triviale.

1.3.1.1. *Les corps de fonctions.* Dans les corps de fonctions, comme les premiers \mathcal{P} sont des anneaux de valuations discrètes, on peut prendre la valuation associée à \mathcal{P} pour obtenir une valeur absolue $|\cdot|_{\mathcal{P}}$ définie, pour $a \in K$ par

$$|a|_{\mathcal{P}} = \mathcal{N}(\mathcal{P})^{-v_{\mathcal{P}}(a)}.$$

Pour ce type de valeur absolue on a une propriété plus forte que l'inégalité du triangle qui découle directement de la propriété (3) donnée dans la Définition 1.2.13,

$$(3') \quad |\alpha + \beta| \leq \max\{|\alpha|, |\beta|\} \text{ pour tout } \alpha, \beta \in K.$$

On appelle les valeurs absolues qui respectent la propriété (3') *ultramétriques* ou *non archimédienne*.

Dans $\mathbb{F}_q(t)$, on avait trouvé que les seuls anneaux de valuation discrète du genre de la Définition 1.2.11 étaient données par la localisation aux irréductibles de $\mathbb{F}_q[t]$ et de $(1/t)$ dans $\mathbb{F}_q[1/t]$. Il se trouve que, dans ce contexte, ces localisations donnent lieu aux seules valeurs absolues de $\mathbb{F}_q(t)$. En d'autres mots, elles possèdent toutes la propriété (3'). C'est aussi le cas pour tous les corps de fonctions,

Théorème 1.3.4. *Soit K un corps de fonctions, l'ensemble des valeurs absolues de K , modulo l'équivalence de la Définition 1.3.2, consiste des valeurs absolues obtenues à partir des valuations \mathcal{P} -adiques.*

DÉMONSTRATION. Soit $|\cdot|$ une valeur absolue. Si elle respecte (3'), en prenant le log et en renormalisant, c'est facile de voir qu'elles sont en bijection avec les valuations (additive). Or,

on montre que toutes les valeurs absolues sur K possèdent la propriété (3'). Considérons la formule du binôme

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k.$$

Si p est la caractéristique de K , alors le coefficient $\binom{n}{k} \in \{0, 1, \dots, p-1\}$. Mais $|1| = 1$ et $|\binom{n}{k}| \leq p-1$ par (1) et (3) respectivement. En utilisant la propriété (3) successivement on obtient

$$|(a + b)|^n \leq \sum_{k=0}^n (p-1) |a|^{n-k} |b|^k \leq n(p-1) \max\{|a|, |b|\}^n.$$

Finalement, en prenant la racine n -ième et en laissant n tendre vers l'infini, on devait avoir (3') comme voulu. \square

1.3.1.2. *Les corps de nombres.* Dans les corps de nombres la situation est bien différente, par exemple, sur \mathbb{Q} on a la valeur absolue classique.

$$|\alpha| = \begin{cases} \alpha & \text{lorsque } \alpha \geq 0, \\ -\alpha & \text{sinon.} \end{cases}$$

Cette valeur absolue est différente de celles qu'on retrouve sur les corps de fonctions puisqu'elle ne respecte pas la propriété (3'). On les appellera *archimédienne*.

Ceci étant dit, on a tout de même les valeurs absolues associées aux premiers p sur \mathbb{Q} . Pour $\alpha \in \mathbb{Q}$ on les définit par

$$|\alpha|_p = p^{-v_p(\alpha)}$$

où v_p réfère à la valuation p -adique usuelle. C'est un théorème d'Ostrowski que toutes les valeurs absolues non triviales de \mathbb{Q} sont équivalentes à une de celles que l'on vient d'énoncer.

En général, si K est un corps de nombres, on rappelle qu'il existe r_1 injections $K \hookrightarrow \mathbb{R}$ et $2r_2$ injections $K \hookrightarrow \mathbb{C}$ où $n = r_1 + 2r_2$. Une généralisation du théorème d'Ostrowski donne le résultat suivant:

Théorème 1.3.5. *Soit K un corps de nombres. L'ensemble des valeurs absolues de K , modulo l'équivalence, consiste de r_1 valeurs absolues associées à chaque injection réelle, de r_2 valeurs absolues associées à chaque paire d'injections complexes ainsi qu'aux valuations \mathcal{P} -adiques.*

DÉMONSTRATION. Voir [41, Chapitre 3]. \square

Pour K un corps de nombres, on notera V_K l'ensemble des classes de valeurs absolues modulo l'équivalence. Cet ensemble est l'union disjointe des ensembles V_f des valeurs absolues non archimédiennes et de V_∞ des valeurs absolues archimédiennes. Les éléments de V_f sont appelés les premiers finis de K et ceux de V_∞ les premiers infinis de K . On les note $p \nmid \infty$ et $p | \infty$ respectivement.

Il existe un choix canonique de représentants pour ces valeurs absolues v . Si $v \in V_\infty$, on choisit $|\cdot|_v = |\sigma(\cdot)|$ si σ est une injection réelle et $|\cdot|_v = |\sigma(\cdot)|^2$ sinon. Dans le cas $v \in V_f$, on choisit $|\cdot|_v = |\mathcal{N}(\mathcal{P})|^{-v_P(\cdot)}$ pour v_P la valuation additive associée à P . Ces choix de normalisation ont pour conséquence

Théorème 1.3.6 (Formule du produit). *Soit $\alpha \in K^*$, on a la relation*

$$\prod_v |\alpha|_v = 1$$

où le produit est pris sur les représentants normalisés de tous les premiers de V_K .

DÉMONSTRATION. Si $\alpha \in K$, il existe uniquement un nombre fini de valeurs absolues $|\cdot|_v$ telles que $|\alpha|_v \neq 1$. En effet, $v_P(\alpha) = 0$ pour toutes les valuations $v_P \in V_f$ associées aux premiers qui n'apparaissent pas dans la factorisation de αO_K . Maintenant, on a vu que l'idéal fractionnaire αO_K se factorise un produit $\prod \mathcal{P}^{v_P(\alpha)}$. Ainsi, la norme $\mathcal{N}(\alpha O_K) = N(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$, mais aussi $\mathcal{N}(\alpha O_K) = \prod \mathcal{N}(\mathcal{P})^{v_P(\alpha)}$; d'où le résultat. \square

1.3.2. Les diviseurs d'Arakelov et leur fonction zêta

Avec ce nouveau point de vue, on considère maintenant les premiers de K comme une classe d'équivalence de valeurs absolues. Comme on vient de le voir, cette présentation est équivalente à celle donnée pour les corps de fonctions. Dans les corps de nombres, nous sommes désormais prêts à définir la notion de diviseur, comme nous l'avons fait à la Section 1.2. On présente les idées de Van Der Geer et Schoof [59].

Définition 1.3.7. Soit K un corps de nombres. On définit le groupe des **diviseurs d'Arakelov** par la somme formelle

$$\mathcal{D}_K = \left\{ \sum_{\mathcal{P} \in V_K} n_{\mathcal{P}} \mathcal{P} : n_{\mathcal{P}} \in \mathbb{Z} \text{ si } \mathcal{P} \nmid \infty, n_{\mathcal{P}} \in \mathbb{R} \text{ si } \mathcal{P} | \infty, n_{\mathcal{P}} = 0 \text{ pour presque tout } \mathcal{P} \right\}.$$

Dans cette définition, *pour presque tout \mathcal{P}* signifie que seul un nombre fini de $n_{\mathcal{P}}$ sont non nuls. Cette propriété mimique la situation des entiers qui possède une décomposition en un nombre fini de premiers. Finalement, pour rappeler que les coefficients de $\mathcal{P} | \infty$ sont continus, on priorisera $x_{\mathcal{P}}$ comme écriture au lieu de $n_{\mathcal{P}}$.

Le degré d'un diviseur est donné par

$$\deg(D) = \sum_{\mathcal{P} \in V_f} n_{\mathcal{P}} \log(\mathcal{N}(P)) + \sum_{\mathcal{P} \in V_{\infty}} x_{\mathcal{P}}.$$

Immédiatement, on a une projection du groupe \mathcal{D}_K vers le groupe des idéaux fractionnels donné par

$$\pi_A(D) = \prod_{\mathcal{P} \in V_f} \mathcal{P}^{-n_{\mathcal{P}}},$$

un diviseur de \mathcal{D}_K est déterminé par son idéal fractionnaire associé $\pi_A(D)$ et les $r_1 + r_2$ coefficients $x_{\mathcal{P}}$, $\mathcal{P} \in V_{\infty}$. Pour $\alpha \in K^*$, on définit le diviseur d'Arakelov principal par

$$(\alpha) = \sum_{\mathcal{P} \in V_f} v_{\mathcal{P}}(\alpha) \mathcal{P} + \sum_{\mathcal{P} \in V_{\infty}} -\log |\alpha|_{v_{\mathcal{P}}} \mathcal{P}.$$

Une motivation pour l'écriture des coefficients de $\mathcal{P} \in V_{\infty}$ est simplement que $v_{\mathcal{P}}(\alpha) = -\log_{\mathcal{N}(\mathcal{P})} |\alpha|_{v_{\mathcal{P}}}$. La projection d'un diviseur principal est donné par $\pi_A(\alpha) = \prod_{\mathcal{P} \in V_f} \mathcal{P}^{-v_{\mathcal{P}}(\alpha)} = \frac{1}{\alpha} O_K$. Finalement, on peut décomposer \mathcal{D}_K en deux parties: Soit la partie finie,

$$\mathcal{D}_K^f = \left\{ \sum_{\mathcal{P} \in V_f} n_{\mathcal{P}} \mathcal{P} : n_{\mathcal{P}} \in \mathbb{Z}, n_{\mathcal{P}} = 0 \text{ pour presque tout } \mathcal{P} \right\},$$

et la partie infinie,

$$\mathcal{D}_K^{\infty} = \left\{ \sum_{\mathcal{P} \in V_{\infty}} x_{\mathcal{P}} \mathcal{P} : x_{\mathcal{P}} \in \mathbb{R} \right\}.$$

Ces deux parties sont canoniquement isomorphes à des sous-groupes de \mathcal{D}_K et $\mathcal{D}_K = \mathcal{D}_K^f \times \mathcal{D}_K^{\infty}$. Si $D \in \mathcal{D}_K$, on peut donc décomposer $D = D_f + D_{\infty}$.

Le but étant de définir une fonction zêta associée à ces diviseurs, on doit définir une notion analogue à celle des diviseurs effectifs. À la Section 1.2, on avait pris comme diviseurs effectifs les $D \geq 0$. Le nouvel élément à gérer ici est, bien entendu, l'ensemble des premiers archimédiens. On pourrait utiliser la même définition, mais pour des raisons qui seront apparentes momentanément, on utilise plutôt la notion **d'effectivité** des diviseurs d'Arakelov proposée par Van Der Geer et Schoof [59].

Le concept de diviseur effectif est binaire: Un diviseur est effectif ou ne l'est pas. Une différence clé du concept de l'effectivité est qu'il est continu. Pour fixer les idées, on peut

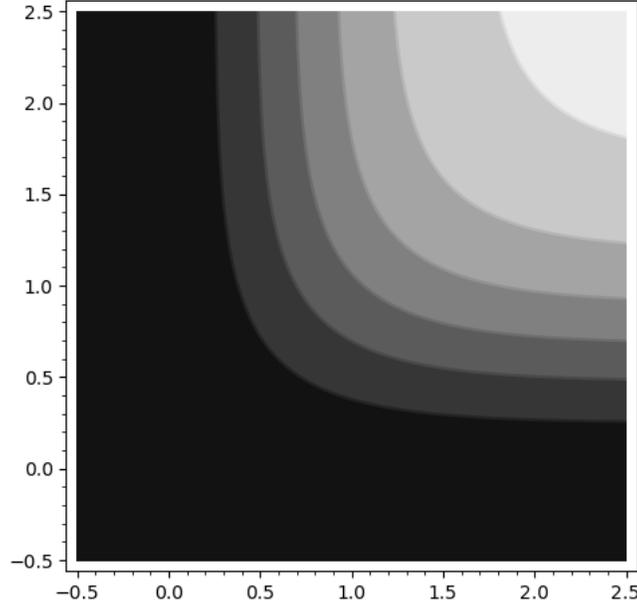


Fig. 1.3. Graphique représentant l'effectivité des diviseurs tels que $O_K \subset \pi_A(D)$ d'une extension possédant exactement deux premiers archimédiens réels. Les axes sont les coefficients $x_{\mathcal{P}}$ de chacun des premiers archimédiens. Le ton de gris représente la valeur de $e(D)$: pâle lorsque $e(D)$ est près de 1; foncé lorsque $e(D)$ est près de 0.

créer une fonction qui distingue les diviseurs effectifs sur les corps de fonctions:

$$e(D) = \begin{cases} 1 & \text{lorsque } D \geq 0 \\ 0 & \text{sinon.} \end{cases} \quad (1.3.1)$$

L'effectivité d'un diviseur d'Arakelov (qui est sur un corps de nombres) sera donc une fonction similaire qui permettra des valeurs entre 0 et 1. Elle est définie par,

$$e(D) = \begin{cases} \exp\left(-\pi \sum_{\mathcal{P} \text{ réel}} e^{-2x_{\mathcal{P}}} - \pi \sum_{\mathcal{P} \text{ complexe}} 2e^{-x_{\mathcal{P}}}\right) & \text{lorsque } O_K \subset \pi_A(D) \\ 0 & \text{sinon.} \end{cases}$$

Cette définition se veut adaptée au caractère continu des premiers archimédiens. Explicitement, on a que $0 \leq e(D) < 1$ et $e(D) = 0$ dès que, pour $\mathcal{P} \in V_f$, $n_{\mathcal{P}} < 0$. (C'est-à-dire que la partie finie de $D \in \mathcal{D}_K$ n'est pas effective!).

On interprète les diviseurs d'effectivité grande ($e(D)$ près de 1), comme les diviseurs effectifs. Si $O_K \subset \pi_A(D)$, alors $e(D)$ est très petit dès qu'un des coefficients de $\mathcal{P} \in V_{\infty}$ est négatif et se rapproche de 1 lorsqu'ils sont tous grands. (Voir la Figure 1.3.)

Remarque 1.3.8. On peut utiliser cette définition d'effectivité pour construire un espace analogue à l'espace $L(D)$ de la Définition 1.2.25. Ceci donne lieu à un analogue du Théorème de Riemann-Roch 1.2.26, voir [59] pour un exposé en profondeur.

Avec ces notions, on peut maintenant définir une fonction zêta similaire à la Définition 1.2.23 où on sommait sur les diviseurs effectifs,

$$Z_K(s) = \int_{\mathcal{D}_K} |D|^{-s} d\mu_{\text{eff}}.$$

Ici, $d\mu_{\text{eff}}$ dénote la mesure de Haar sur le groupe $\text{Div}(K)$ pondérée par l'effectivité des diviseurs. Il se trouve que la fonction $Z_K(s)$ est intimement liée à la fonction zêta de Dedekind.

Proposition 1.3.9. *L'intégrale survenant dans la définition de la fonction Z_K converge dès que $\text{Re}(s) > 1$ et on a la relation*

$$Z_K(s) = \zeta_K(s) \left(\frac{1}{2} \pi^{-s/2} \Gamma(s/2) \right)^{r_1} ((2\pi)^{-s} \Gamma(s))^{r_2}.$$

IDÉE DE LA PREUVE. La preuve est inspirée de [59]. Le lecteur intéressé peut également consulter [25] pour un traitement similaire au niveau de ce que l'on appelle les idèles (qui sont une construction différente, mais similaire aux diviseurs d'Arakelov.)

Par définition, $d\mu_{\text{eff}} = e(D)dD$. Donc,

$$Z_K(s) = \int_{\mathcal{D}_K} |D|^{-s} e(D) dD.$$

Maintenant, $|D| = e^{\deg D} = \prod_{\mathcal{P} \in V_f} \mathcal{N}(P)^{n_{\mathcal{P}}} \exp(\sum_{\mathcal{P} \in V_{\infty}} x_{\mathcal{P}})$. Comme $\mathcal{D}_K = \mathcal{D}_K^f \times \mathcal{D}_K^{\infty}$, on peut séparer l'intégrale:

$$Z_K(s) = \int_{\mathcal{D}_K^f} |D_f|^{-s} e(D_f) dD_f \int_{\mathcal{D}_K^{\infty}} |D_{\infty}|^{-s} e(D_{\infty}) dD_{\infty}.$$

Puisque la mesure de Haar sur les groupes discrets est la mesure de dénombrement, on trouve que

$$\int_{\mathcal{D}_K^f} |D_f|^{-s} e(D_f) dD_f = \prod_{\mathcal{P} \in V_f} \sum_{n=0}^{\infty} \mathcal{N}(\mathcal{P})^{-ns}.$$

On peut donc continuer à simplifier notre expression pour $Z_K(s)$ pour trouver,

$$Z_K(s) = \prod_{\mathcal{P} \in V_f} (1 - \mathcal{N}(\mathcal{P})^{-s})^{-1} \int_{\mathcal{D}_K^{\infty}} \prod_{\mathcal{P} \in V_{\infty}} (e^{x_{\mathcal{P}}})^{-s} e(D_{\infty}) dD_{\infty}.$$

Ici, en intégrant chaque coordonnée de \mathcal{D}_K^∞ séparément et posant $t_{\mathcal{P}} = e^{-x_{\mathcal{P}}}$, on retrouve des termes qui sont à peu près des fonctions Γ qu'on avait défini dans (1.1.1):

$$Z_K(s) = \prod_{\mathcal{P} \in V_f} (1 - \mathcal{N}(\mathcal{P})^{-s})^{-1} \prod_{p \text{ réel}} \int_0^\infty t_{\mathcal{P}}^s e^{-\pi t_{\mathcal{P}}^2} \frac{dt_{\mathcal{P}}}{t_{\mathcal{P}}} \prod_{p \text{ complexe}} \int_0^\infty t_{\mathcal{P}}^s e^{-2\pi t_{\mathcal{P}}} \frac{dt_{\mathcal{P}}}{t_{\mathcal{P}}}.$$

On a trouvé,

$$Z_K(s) = \zeta_K(s) \left(\frac{1}{2} \pi^{-s/2} \Gamma(s/2) \right)^{r_1} ((2\pi)^{-s} \Gamma(s))^{r_2}.$$

□

Cette définition est beaucoup plus rapprochée de celle proposée à la Section 1.2 puisque son équation fonctionnelle est donnée par

$$\Delta_K^{\frac{s}{2}} Z_K(s) = \Delta_K^{\frac{1-s}{2}} Z_K(1-s).$$

Comme c'était le cas pour la fonction de la Définition 1.2.23 sur les corps de fonctions, la fonction $Z_K(s)$ est définie sur un diviseur portant sur tous les premiers de K , incluant les premiers infinis! Une conséquence de cette définition sur les corps de nombres est que les termes associés aux premiers archimédiens sont maintenant inclus dans le terme $Z_K(s)$. De plus, elle ne possède pas de zéros à l'extérieur de la bande critique $0 \leq \operatorname{Re}(s) \leq 1$.

Remarque 1.3.10. Cette fonction est intimement liée au Théorème 1.1.52. En fait, on peut comparer les deux pour trouver qu'elles ne diffèrent que d'une constante dans les facteurs Γ . Ceci a peu d'effets et on retrouve plusieurs normalisations différentes dans la littérature. (Voir par exemple Serre [53] où on justifie le choix de normalisation du Théorème 1.1.52 pour avoir un lien plus simple entre $\Gamma_{\mathbb{C}}$ et $\Gamma_{\mathbb{R}}$.)

1.3.3. S-Anneaux des entiers et S-fonctions-zêta

La section précédente introduisait des définitions qui rapprochaient la théorie sur les corps de nombres à celle vue à la Section 1.2 sur les corps de fonctions. Cette section nous permettra de considérer la procédure inverse en considérant des objets sur les corps de fonctions qu'on voudra analogue au traitement de la Section 1.1. La présentation suit approximativement le chapitre 14 de Rosen [51].

Soit $x \in K$ transcendant sur \mathbb{F}_q , on peut ainsi considérer K comme une extension de $\mathbb{F}_q(x)$. La paire $\mathbb{F}_q[x] \subset \mathbb{F}_q(x)$ jouera ici le rôle de la paire $\mathbb{Z} \subset \mathbb{Q}$. On verra que le choix de x distingue un nombre fini de premiers de K qui sont précisément les premiers au-dessus de \mathcal{P}_∞ ; qu'on avait défini comme la localisation de $\mathbb{F}_q[1/x]$ à $(1/x)$.

Remarque 1.3.11. Contrairement à \mathbb{Q} , \mathcal{P}_∞ n'est pas un premier archimédien. En effet, on avait vu dans la preuve du Théorème 1.3.4 que l'image de \mathbb{Z} était bornée par rapport à $|\cdot|_\infty$ et que ceci impliquait l'inégalité ultramétrique.

Ceci étant dit, l'image de $\mathbb{F}_q[x]$ n'est pas bornée par rapport à $|\cdot|_\infty$. Avec la philosophie que $\mathbb{F}_q[x]$ est supposé remplacer \mathbb{Z} , \mathcal{P}_∞ est en quelque sorte analogue à un premier archimédien sur $\mathbb{F}_q[x]$. Cette sorte de similitude explique, entre autres raisons, pourquoi les premiers archimédiens sont souvent appelés les premiers à l'infini.

À la Section 1.1, on avait défini (Déf. 1.1.7) l'anneau des entiers d'un corps de nombres K comme $\mathbb{A} \cap K$, la fermeture algébrique de \mathbb{Z} dans K . Maintenant, si K est un corps de fonctions, on définit O_K comme étant la fermeture algébrique de $\mathbb{F}_q[x]$ dans le corps de fonctions K . Le but de ce chapitre sera de reproduire les différents objets abordés dans les autres chapitres en fonction de O_K .

Il existe une description plus générale de l'anneau des entiers.

Définition 1.3.12. Soit V_K l'ensemble des premiers d'un corps de fonctions K au sens des valeurs absolues modulo l'équivalence. Si S est un ensemble fini de premiers alors on appellera

$$O_S = \{a \in K : |a|_{v_P} \leq 1, \forall P \notin S\}$$

l'anneau des **S-entiers**.

Exemple 1.3.13. Si $S = \emptyset$, le fait que le degré des diviseurs principaux soit zéro implique que $O_S = \mathbb{F}_q$. On ne considérera pas ce cas dans notre traitement.

Théorème 1.3.14. Soit K un corps de fonctions et $S \subset V_K$ un ensemble non vide et fini de premiers dans K . Il existe toujours des éléments x de K qui possèdent comme pôles les premiers de S et seulement ceux-ci. Pour un tel $x \in K$, si O_K est la fermeture algébrique de $\mathbb{F}_q[x]$ dans K alors $O_S = O_K$.

DÉMONSTRATION. La preuve est accessible mais un peu longue, voir [51, Théorème 14.5]. □

En choisissant d'abord les premiers de K , ce théorème montre que tout ensemble fini peut servir de premiers au-dessus de l'infini en effectuant un changement de variable.

Exemple 1.3.15. Soit $K = \mathbb{F}_q(x)$. Notons \mathcal{P}_0 et \mathcal{P}_∞ , respectivement la localisation de $\mathbb{F}_q[x]$ à (x) et $\mathbb{F}_q[1/x]$ à $(1/x)$. L'élément $w = x + x^{-1}$ possède précisément \mathcal{P}_0 et \mathcal{P}_∞ comme pôles et le Théorème 1.3.14 implique que la fermeture algébrique de $\mathbb{F}_q[w]$ dans $\mathbb{F}_q(x)$ est $O_{\{\mathcal{P}_0, \mathcal{P}_\infty\}}$.

On peut montrer que $O_{\{\mathcal{P}_0, \mathcal{P}_\infty\}} = \mathbb{F}_q[x, x^{-1}]$ et que le polynôme minimal de x, x^{-1} sur $\mathbb{F}_q[w]$ est donnée par $x^2 - wx + 1$. $\mathbb{F}_q(x)$ est une extension galoisienne de degré 2 sur $\mathbb{F}_q(w)$ et si \mathcal{Q}_∞ dénote la localisation de $\mathbb{F}_q[1/w]$ à $(1/w)$, alors \mathcal{Q}_∞ se sépare en \mathcal{P}_0 et \mathcal{P}_∞ dans K .

1.3.3.1. *Exemple: Les extensions quadratiques.* Supposons que q est impair et soit $f(x) \in \mathbb{F}_q[x]$ un polynôme démuné de carrés. On définit l'extension $K = \mathbb{F}_q(x, \sqrt{f(x)})$. Suivant l'Exemple 1.1.8, on peut calculer O_K : D'une part on sait K est un espace vectoriel de dimension 2 sur $\mathbb{F}_q(x)$,

$$K = \{a + b\sqrt{f(x)} : a, b \in \mathbb{F}_q(x)\}$$

Soit $\alpha = a + b\sqrt{f(x)} \in K$. Si $b \neq 0$, le polynôme minimal de $\alpha \in K$ est donné par

$$y^2 - 2ay + a^2 - f(x)b^2$$

et $\alpha \in O_K$ ssi $2a$ et $a^2 - f(x)b^2$ sont des éléments de $\mathbb{F}_q[x]$. Or, dans ce cas 2 est un élément inversible de $\mathbb{F}_q[x]$ et $a \in \mathbb{F}_q[x]$. Finalement, $b \in \mathbb{F}_q[x]$ aussi puisque $f(x)$ est sans carré. On a montré que

$$O_K = \{n + m\sqrt{f(x)} : n, m \in \mathbb{F}_q[x]\}.$$

On peut s'intéresser à la décomposition des premiers dans O_K . En particulier pour \mathcal{P}_∞ , on a le résultat

Proposition 1.3.16. *Soit $K = \mathbb{F}_q(x, \sqrt{f(x)})$ avec q impair et $f(x)$ démuné de carré. Maintenant, si $d = \deg(f)$ et a_d est le coefficient de tête de $f(x)$ alors \mathcal{P}_∞ est ramifié dans K dès que d est impair. Sinon, \mathcal{P}_∞ se sépare dans K lorsque a_d est un carré dans \mathbb{F}_q^* et reste premier si a_d n'est pas un carré dans \mathbb{F}_q^* .*

DÉMONSTRATION. Consulter [51, Proposition 14.6] pour la preuve. □

Exemple 1.3.17. Si $f(x) = x^2 - 4$ alors on a vu que \mathcal{P}_∞ se sépare dans $K = \mathbb{F}_q(x, \sqrt{x^2 - 4})$.

1.3.3.2. *S-fonction-zêta.* On a quelques définitions

Définition 1.3.18. Soit $S \in V_K$ un ensemble fini de premiers de K . L'ensemble

$$E(S) = \{a \in K^* : |a|_{v_{\mathcal{P}}} = 1, \forall \mathcal{P} \notin S\}$$

est appelé le groupe des **S-unités** de K .

En effet, c'est clair que $E(S) = O_S^*$ puisque: α et $\alpha^{-1} \in O_S$ ssi $1 \leq |\alpha|_{v_{\mathcal{P}}} \leq 1$ pour tout $\mathcal{P} \notin S$.

Soit K un corps de fonctions. On rappelle également \mathcal{D} , le groupe des diviseurs de K , et Pr , le sous-groupe des diviseurs principaux. Une remarque au niveau de la notation est que l'on n'écrit pas explicitement K dans \mathcal{D}_K puisque le corps K est fixe dans notre discussion. De plus, dans ce qui suit, l'ensemble $S \subset V_K$ dépend de K et il n'y a pas d'ambiguïté.

Définition 1.3.19. On pose \mathcal{D}_S , les **S-diviseurs** de K comme le groupe libre généré par les premiers $V_K \setminus S$. Évidemment, ceci donne un sous-groupe de \mathcal{D} et pour $a \in K^*$ on définit son S -diviseur comme

$$(a)_S = \sum_{\mathcal{P} \notin S} v_{\mathcal{P}}(a)\mathcal{P}.$$

L'ensemble des diviseurs de la forme $(a)_S$ sont les S -diviseurs principaux Pr_S . Finalement, on définit le groupe des S -classes, $Cl_S = \mathcal{D}_S/Pr_S$.

Comme chaque fois, le premier résultat qu'on vise est que le nombre de classes est fini,

Proposition 1.3.20. *Soit K un corps de fonctions, si $S \subset V_K$ est un ensemble fini de premiers de K alors Cl_S est un groupe fini. De plus, $E(S)$ est un groupe libre de rang $|S| - 1$.*

DÉMONSTRATION. Voir [51, Proposition 14.2]. □

On peut maintenant définir une fonction zêta relative à S . Plus tôt, on avait trouvé que

$$\zeta_K(s) = \prod_{\mathcal{P} \in V_K} (1 - \mathcal{N}(\mathcal{P})^{-s})^{-1}.$$

Cependant, pour éviter la confusion avec l'ensemble S , on utilisera la variable $z \in \mathbb{C}$ au lieu de s . Ainsi,

Définition 1.3.21. Soit K un corps de fonctions et $S \subset V_K$ un sous-ensemble fini des premiers de K . On définit

$$\zeta_S(z) = \prod_{\mathcal{P} \notin S} (1 - \mathcal{N}(\mathcal{P})^{-z})^{-1},$$

la **S-fonction-zêta**.

Une conséquence de cette définition, qu'on avait remarqué à la Proposition 1.2.28, est que

$$\zeta_S(z) = \prod_{\mathcal{P} \in S} (1 - \mathcal{N}(\mathcal{P})^{-z}) \zeta_K(s). \tag{1.3.2}$$

En fait, on peut reproduire des résultats très similaires aux résultats classiques sur la fonction ζ_K sur les corps de nombres.

Une autre conséquence directe est une nouvelle équation fonctionnelle,

Proposition 1.3.22. *Soit K un corps de fonctions, si $S \subset V_K$ est un ensemble fini de premiers de K alors la fonction $\zeta_S(z)$ admet l'équation fonctionnelle*

$$\zeta_S(z) = \zeta_S(1-z) \prod_{\mathcal{P} \in S} \frac{(1 - \mathcal{N}(\mathcal{P})^{-z})}{(1 - \mathcal{N}(\mathcal{P})^{1-z})} q^{(g-1)(1-2z)}.$$

DÉMONSTRATION. Cette équation fonctionnelle suit du Théorème 1.2.29 et de l'équation (1.3.2). \square

Cette forme de l'équation fonctionnelle se veut analogue au Théorème 1.1.52. En effet, la fonction $\zeta_S(z)$ exclue les termes associés aux premiers $\mathcal{P} \in S$. C'est-à-dire, les termes qui ne sont pas associés à des premiers au-dessus des irréductibles de $\mathbb{F}_q[x]$. Cette situation rappelle l'équation fonctionnelle du Théorème 1.1.52 où les premiers associés aux valeurs absolues archimédiennes sont exclus de la fonction zêta. Cette relation est une des raisons pour laquelle on donne le nom *premiers infinis* aux valeurs absolues archimédiennes.

Remarque 1.3.23. Une fonction similaire S -zêta peut également être définie sur les corps de nombres. Nous n'en faisons pas l'exposition ici puisque le but était d'exclure spécifiquement les premiers au-dessus de l'infini; à l'instar des premiers archimédiens de la fonction zêta de Dedekind.

1.4. Les hauteurs et la propriété de Northcott

La question principale de ce mémoire s'intéresse aux hauteurs et, plus spécifiquement, à savoir si certaines hauteurs associées aux fonctions zêta possèdent ce qu'on appellera la propriété de Northcott.

Les hauteurs sont un outil mathématique servant d'échelle pour mesurer la complexité d'un objet. Outre la norme usuelle d'un vecteur en d dimensions, une hauteur classique souvent considérée dans les cours d'introduction à la théorie des nombres est la hauteur naïve sur les nombres rationnels [21]. Pour $\frac{a}{b} \in \mathbb{Q}$ une fraction réduite, cette norme est donnée par la quantité $\log \max\{|a|, |b|\}$.

En général, on définit

Définition 1.4.1. Une fonction $h : S \rightarrow \Gamma$ est dite fonction de hauteur sur l'ensemble S lorsque le codomaine Γ est un ensemble partiellement ordonné.

On dit qu'une hauteur possède la **propriété de Northcott** lorsque, pour tout $\gamma \in \Gamma$, il existe seulement un nombre fini d'éléments $s \in S$ tels que $h(s) \leq \gamma$.

Exemple 1.4.2. La hauteur naïve définie sur les nombres rationnels possède la propriété de Northcott.

Exemple 1.4.3. Dans la preuve du Théorème 1.1.44, on avait besoin de montrer que la hauteur norme $\mathcal{N}(\cdot)$ sur les idéaux de O_K possède la propriété de Northcott.

Exemple 1.4.4. Le discriminant d'un corps de nombres K peut être vu comme une hauteur en considérant

$$[K] \mapsto \Delta_K$$

pour $[K]$ la classe d'isomorphisme de corps de nombres. Elle possède la propriété de Northcott par le Théorème d'Hermite.

En agrandissant la famille, on risque de perdre la propriété de Northcott.

Exemple 1.4.5. La hauteur naïve est définie sur les nombres algébriques par

$$h(\alpha) = \log \max_j |a_j|$$

où les $a_j \in \mathbb{Z}$ sont les coefficients du polynôme minimal de α . Cette fonction de hauteur ne respecte pas la propriété de Northcott puisqu'il existe un nombre infini de $\omega \in \overline{\mathbb{Q}}$ tels que $h(\omega) = 0$. Pour s'en convaincre, il suffit de considérer les racines de l'unité ω_p d'ordre p : On sait que le polynôme minimal de ces éléments est $x^{p-1} + x^{p-2} + \dots + x + 1$.

Exemple 1.4.6. Le degré d'un nombre algébrique défini par $\deg(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ ne possède pas la propriété de Northcott: Il existe un nombre infini d'éléments $\alpha \in \overline{\mathbb{Q}}$ avec $\deg(\alpha) = 2$.

On peut quand même prendre un plus grand domaine qu'à l'Exemple 1.4.2.

Exemple 1.4.7 (Le théorème de Northcott [42]). La hauteur combinée sur les nombres algébriques définie par

$$(h, \deg)(\alpha) : \overline{\mathbb{Q}} \rightarrow (\mathbb{R}_{\geq 0}, \mathbb{N})$$

où l'ordre partiel dans $(\mathbb{R}_{\geq 0}, \mathbb{N})$ est donné par $(a, n) < (b, m) \iff a < b$ et $n < m$, possède la propriété de Northcott. Une autre façon d'énoncer ce résultat est simplement que la hauteur naïve sur l'ensemble $\overline{\mathbb{Q}}_n$ des nombres algébriques de degré borné par n possède la propriété de Northcott.

Dans le contexte de hauteurs sur les nombres algébriques, une question naturelle suivant l'Exemple 1.4.7 est de catégoriser les ensembles S sur lesquels la hauteur naïve est Northcott. Ce type de questions est toujours d'actualité et les travaux de Bombieri et Zannier [6]

présentent des ensembles S qui sont Northcott dans lesquels le degré *n'est pas borné*. Checcoli et Fehm [11] amenèrent ces idées plus loin en montrant que certains ensembles surprenants possèdent la propriété de Northcott.

Théorème 1.4.8. [6, Théorème 1] *Soit K un corps de nombres et $d \in \mathbb{N}$. Si $C^{(d)}$ est l'ensemble des extensions de K de degré borné par d , alors on appelle*

$$K^{(d)} = \bigcap_{\substack{L \text{ sous-corps de } \overline{\mathbb{Q}} \\ \forall F \in C^{(d)}, F \subset L}} L.$$

le compositum de $C^{(d)}$. L'extension abélienne maximale de K contenu de $K^{(d)}$, $K_{ab}^{(d)}$ possède la propriété de Northcott.

Corollaire 1.4.9. *Le corps $K^{(2)}$ possède la propriété de Northcott.*

IDÉE DE LA PREUVE. En principe, on peut montrer que $K_{ab}^{(2)} = K^{(2)}$ [6]. □

On dit qu'une extension L de \mathbb{Q} est de degré local fini à un premier p si, pour un premier \mathcal{P} de L au-dessus de p , la complétion de L par rapport à la valeur absolue $|\cdot|_{\mathcal{P}}$, $L_{\mathcal{P}}$, est une extension finie de \mathbb{Q}_p (Ici, \mathbb{Q}_p signifie les nombres p -adiques. Ce corps peut être compris comme la complétion de \mathbb{Q} par rapport à la valeur absolue non archimédienne $|\cdot|_p$. Voir [41, Chapitre 2, Section 2] pour plus de détails). Dans le même article Bombieri et Zannier montrent

Théorème 1.4.10. [6, Théorème 2] *Soient L une extension Galoisienne de \mathbb{Q} et $S(L)$, l'ensemble des nombres premiers sur lesquels L est de degré local fini. Alors la quantité*

$$\mathcal{G}(L) := \sum_{p \in S(L)} \frac{\log p}{e_p(p^{f_p} + 1)},$$

où e_p et f_p dénotent respectivement l'index de ramification et le degré d'inertie de p dans L , est telle que

$$\liminf_{\alpha \in L} h(\alpha) \geq \frac{1}{2} \mathcal{G}(L).$$

Une remarque importante qui découle de ce théorème est que l'extension L possède la propriété de Northcott dès que la somme $\mathcal{G}(L)$ diverge. En effet, sinon, il existe une constante $B \in \mathbb{R}_{>0}$ et une suite d'éléments $(\alpha_n)_{1 \leq n}$ de L distincts tels que $h(\alpha_n) \leq B$ pour tout $n \geq 1$. En d'autres mots, la $\liminf_{\alpha \in L} h(\alpha)$ est finie puisqu'elle est bornée supérieurement par B . En général, les questions attachées à la propriété de Northcott et ses variantes sont souvent exprimables en termes de problèmes équivalents impliquant des limites inférieures.

Le résultat surprenant de Checcoli et Fehm [11] est que la somme $\mathcal{G}(L)$ peut diverger même lorsque l'on considère des extensions de \mathbb{Q} qui ne sont pas finies.

Théorème 1.4.11. [11, Théorème 3] *Il existe une extension L totalement réelle de \mathbb{Q} telle que le degré local de L est fini à tous les premiers et $\mathcal{G}(L) = \infty$.*

On s'intéresse également à la propriété de Northcott sur d'autres types de hauteurs. Intimement liée à la mesure de complexité des nombres algébriques, on peut aussi prendre une hauteur sur une extension algébrique. C'est en quelque sorte la même chose, puisqu'on peut voir cette hauteur comme une mesure sur les nombres algébriques contenus dans le corps. On a déjà vu l'Exemple 1.4.4 avec le discriminant de K et on va explorer d'autres mesures sur un corps de nombres K .

C'est une observation de Pazuki et Pengo [47] que le résultat de Akhtari et Vaaler [3] combiné avec la formule de classes présenté plus haut (Théorème 1.1.51) permettent de mettre en relation la notion de hauteur avec la fonction ζ_K définie dans la Section 1.1. Plus précisément, ces résultats montrent que la valeur spéciale

$$|\zeta_K^*(0)| = \lim_{t \rightarrow 0} \frac{\zeta_K(t)}{t^{\text{ord}_n(\zeta_K(t))}}$$

est commensurable par un produit de hauteurs de Weil. En effet,

Théorème 1.4.12. [3, Théorème 1.1 et 1.2] *Supposons que \mathcal{O}_K^\times le groupes des unités de \mathcal{O}_K soit de rang positif $r = r_1 + r_2 - 1$. Il existe une base $\gamma_1, \dots, \gamma_r$ de $\mathcal{O}_K^\times / \text{Tor}(\mathcal{O}_K^\times)$ telle que*

$$\text{Reg}_S(K) \leq [K : \mathbb{Q}]^r \prod_{j=1}^r h(\gamma_j) \leq \frac{2(r!)^4}{(2r)!} \text{Reg}_S(K) \quad (1.4.1)$$

Ainsi, la combinaison de ce résultat avec l'équation de classes donne

$$\frac{h_K [K : \mathbb{Q}]^r (2r)!}{2w_K (r!)^4} \prod_{i=1}^r h(\gamma_i) \leq |\zeta_K^*(0)| \leq \frac{h_K [K : \mathbb{Q}]^r}{w_K} \prod_{i=1}^{r_K} h(\gamma_i)$$

pour h_K le nombre de classes et, finalement, w_K le nombre de racines de l'unité de K . Notons que même si le Théorème 1.4.12 ne s'applique que si r est positif, on obtient trivialement (1.4.1) lorsque $r = 0$.

Cette observation est intéressante puisqu'elle met en relation la fonction zêta de Dedekind et un produit de hauteurs naïves. Elle suggère que la fonction zêta pourrait être utilisée comme mesure de complexité.

1.4.1. La propriété de Northcott de fonctions zêta sur des familles d'extensions

On rappelle maintenant les questions introduites au début du texte. La hauteur d'intérêt dans ce mémoire fût introduite par Pazuki et Pengo [47] sur l'ensemble des classes d'isomorphismes de corps de nombres et est définie par

$$[K] \mapsto |\zeta_K^*(n)| \text{ où } n \in \mathbb{Z} \text{ et } \zeta_K^*(n) = \lim_{t \rightarrow n} \frac{\zeta_K(t)}{(t-n)^{\text{ord}_n(\zeta_K(t))}}.$$

Dans leur article, Pazuki et Pengo montrent

Théorème 1.4.13. [47] *Soit $n \in \mathbb{Z}$. Si $n \leq 0$, alors il existe seulement un nombre fini de classes d'isomorphismes de corps de nombres tels que $|\zeta_K^*(n)| \leq B$, et ce, peu importe $B \in \mathbb{R}_{>0}$. C'est-à-dire que la hauteur $[K] \mapsto |\zeta_K^*(n)|$ possède la propriété de Northcott. Si $n \geq 1$ alors la hauteur ne possède pas la propriété de Northcott.*

On peut généraliser le problème de la manière suivante,

Problème 1.4.14. Considérons l'ensemble

$$S_{B,s} = \{[K] : |\zeta_K^*(s)| \leq B\},$$

où $[K]$ représente la classe d'isomorphismes de corps de nombres et ζ_K la fonction zêta de Dedekind. En fixant $s \in \mathbb{C}$, l'ensemble $S_{B,s}$ est-il fini pour tout $B \in \mathbb{R}_{>0}$? Dans ce cas, on dit que la propriété de Northcott est respectée en s . Sinon, on appelle un tel point non Northcott.

La question étant résolue sur les corps de nombres pour l'ensemble des $\mathbb{Z} \subset \mathbb{C}$, une question proposée par Wanlin Li fut de considérer le problème analogue sur les corps de fonctions.

Problème 1.4.15. Considérons l'ensemble

$$S_{q,B,s} = \{[K] : |\zeta_K^*(s)| \leq B\},$$

où $[K]$ représente la classe d'isomorphismes de corps de fonctions avec \mathbb{F}_q comme corps des constantes et ζ_K la fonction zêta de la Définition 1.2.23. Maintenant, on a le même objectif: En fixant q une puissance de premier et $s \in \mathbb{C}$, l'ensemble $S_{q,B,s}$ est-il fini pour tout $B \in \mathbb{R}_{>0}$? Dans ce cas, on dit que la propriété de Northcott est respectée en s . Sinon, on appelle un tel point non Northcott.

Le chapitre 2 se concentrera sur le Problème 1.4.15. En particulier, on montre que l'analogue du Théorème 1.4.13 sur les corps de fonctions est vrai lorsque $q > 4$. On a le théorème suivant:

Théorème 1.4.16. *Soit $s = \sigma + i\tau$.*

- a) *Lorsque $\sigma < \frac{1}{2} - \frac{\log 2}{\log q}$, le point s satisfait la propriété de Northcott.*
b) *Lorsque $\sigma > 1$, le point s est non Northcott. Plus spécifiquement, l'ensemble $S_{q,B,s}$ est infini pour*

$$B \geq \frac{1}{(1 - q^{-\sigma})(1 - q^{1-\sigma})^2}.$$

- c) *Si $q \equiv 1 \pmod{4}$, alors le point $s = 1$ est non Northcott.*
d) *Soit $q \equiv 1 \pmod{4}$ et $\sigma > 1/2$ (sauf $q^s = q$). Le point s est non Northcott.*

Voir la Figure 1.4 pour une représentation graphique de ce théorème. Le résultat a) est une conséquence de l'hypothèse de Riemann pour les corps de fonctions. Pour b), on distingue la sous-famille des corps de fonctions quadratiques, qu'on pourra borner explicitement. L'énoncé c) dépend de résultats importants sur la distribution de fonctions-L de Dirichlet quadratiques par Lumley [34, 36] et Li [31]. Finalement, d) découle de résultats récents sur la conjecture des moments translatsés sur les corps de fonctions [24]. La condition que $q \equiv 1 \pmod{4}$ est commune et on la retrouve entre autre dans [4, 35, 37]. Elle permet de simplifier les formules puisque la réciprocité quadratique devient triviale. Une version plus détaillée est disponible au Chapitre 2 sous la forme du Théorème 2.1.3. Ce théorème couvre entre autre un résultat partiel sur la ligne $\sigma = 1/2$.

Ensuite, dans le chapitre 3, nous retournerons au Problème 1.4.14 pour tenter d'agrandir l'ensemble \mathbb{Z} couvert par [47]. Il se trouve que la situation est plus complexe que sur les corps de fonctions. Ceci est dû, entre autres, aux zéros triviaux de la fonction zêta de Dedekind. Le théorème suivant présente un résumé qualitatif des résultats du Chapitre 3.

Théorème 1.4.17. *Soit $s = \sigma + i\tau$. On distingue deux situations dans lesquelles s possède la propriété de Northcott:*

- (1) *Si $\sigma < -1.5$ et le point s se trouve à l'extérieur de certains disques D_n centrés autour des entiers négatifs.*
(2) *Si $-1.5 \leq \sigma < 0$ et $|\tau| > C(\sigma)$, où $C(\sigma)$ est une certaine fonction croissante telle que $C(\sigma) \rightarrow \infty$ lorsque $\sigma \rightarrow 0^-$.*

On distingue une fois de plus deux cas pour lesquels s ne possède pas la propriété de Northcott:

- (1) *Si $\sigma > 1/2$ et $\sigma \neq 1$.*

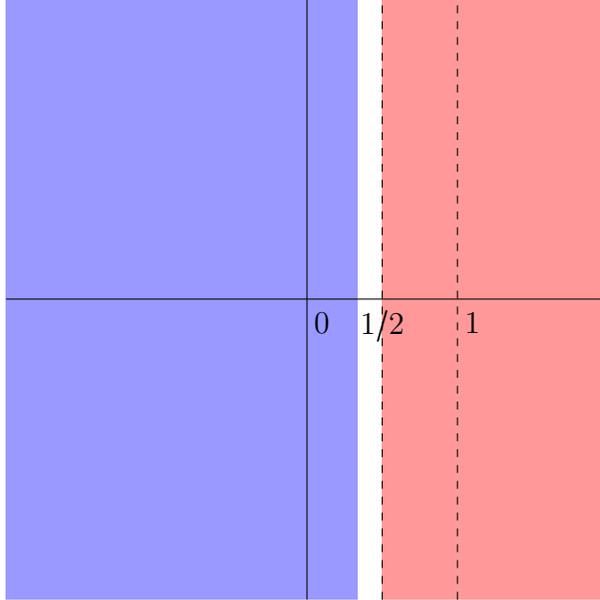


Fig. 1.4. Pour le corps de base \mathbb{F}_q , où q est une puissance de premier fixé, la propriété de Northcott est respectée pour tous les points appartenant à la zone bleue. Dans la zone rouge, $S_{q,B,s}$ est infini dès que B est assez grand. Finalement, la bande blanche disparaît quand $q \rightarrow \infty$.

(2) Si le point s se trouve à l'intérieur de certains disques d_n centrés autour des entiers négatifs.

Évidemment, $d_n \subset D_n$. De plus, le rayon de ces disques tend vers 0 lorsque $n \rightarrow -\infty$. Parmi les disques D_n , le plus grand rayon est atteint lorsque $n = -2$ et vaut $r \approx 0.0633$; pour d_n , c'est plutôt lorsque $n = -1$ et vaut $r \approx 3.415 \times 10^{-6}$.

Les résultats pour $\sigma < 0$ proviennent de l'étude des différents termes apparaissant dans l'équation fonctionnelle de la fonction zêta de Dedekind. Il faudra donc comprendre et contrôler $\zeta_K(s)$ lorsque $\sigma > 1$, les termes $\Gamma_{\mathbb{R}}$ et Γ_C ainsi que le discriminant Δ_K . Pour $\sigma > 1/2$, il dépend de la combinaison d'un résultat de Lamzouri [28] sur la distribution de valeurs extrêmes sur des familles de fonctions-L de Dirichlet quadratiques, ainsi que d'une stratégie similaire à celle utilisée sur les corps de fonctions, où on bornait la sous-famille de fonctions zêta des extensions quadratiques par un borne explicite. Consulter les Théorèmes 3.1.1, 3.1.3, 3.1.4 et 3.1.6 pour une description complète des résultats et, en particulier, une formule explicite pour les disques d_n et D_n ainsi que pour la fonction $C(\sigma)$. Notons finalement que les résultats sur les points qui possèdent la propriété de Northcott sont une conséquence de la même Proposition 3.4.4. Les résultats présentés dans le Théorème 1.4.17 sont plus

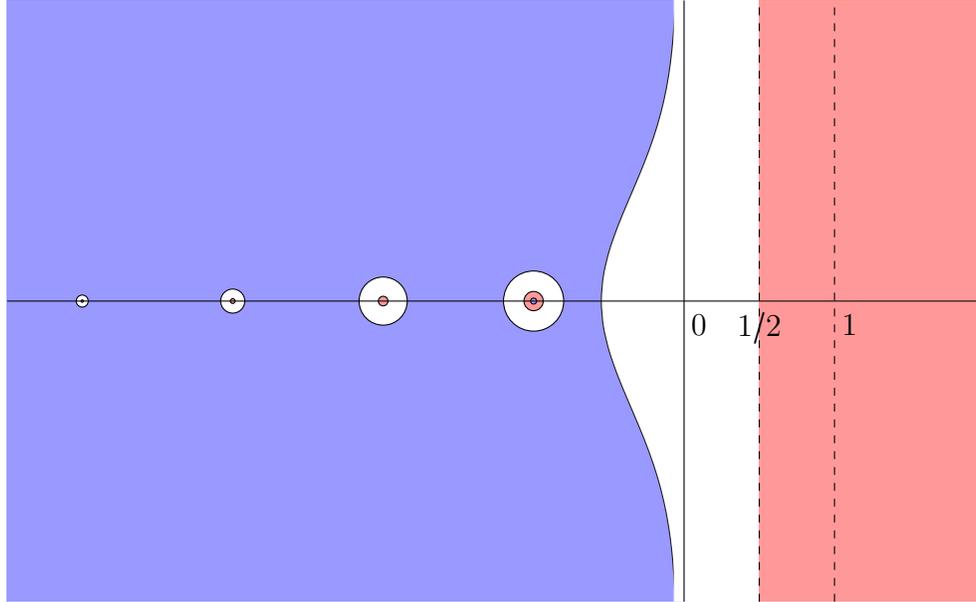


Fig. 1.5. Illustration approximative des résultats du Chapitre 3 par rapport à la propriété de Northcott sur les fonctions zêta de Dedekind. En bleu, les points qui respectent la propriété de Northcott; en rouge, les points qui ne la respectent pas.

faibles mais plus explicites que cette Proposition. Dans le but d'obtenir des résultats plus précis, l'Annexe A approche la Proposition 3.4.4 avec un point de vue numérique. La Figure 1.5 reflète cette analyse.

En comparant les résultats des Théorèmes 1.4.16 et 1.4.17, il est immédiat que la section $\sigma < 0$ possède des différences importantes. La question se pose à savoir pourquoi la propriété de Northcott agit différemment selon le problème. Est-ce parce que les corps de nombres et les corps de fonctions sont intrinsèquement différents? Ou peut-être parce que les fonctions ζ considérées ne sont pas tout à fait analogues? Les autres fonctions zêta introduites à la Section 1.3 servent de candidates pour répondre à cette dernière question. Plus spécifiquement, ce sont les facteurs Γ de l'équation fonctionnelle 1.1.52 qui sont responsables des disques non Northcott autour des entiers négatifs. En effet, par la formule de réflexion d'Euler (3.2.3), on remarque que le rapport $\frac{\Gamma(1-s)}{\Gamma(s)} = \Gamma(1-s)^2 \frac{\sin(\pi s)}{\pi}$ s'annule aux entiers négatifs. Ceci implique que le rapport $\frac{\Gamma_{\mathbb{C}}(1-s)}{\Gamma_{\mathbb{C}}(s)}$ s'annule également sur les entiers négatifs et on voit similairement que $\frac{\Gamma_{\mathbb{R}}(1-s)}{\Gamma_{\mathbb{R}}(s)}$ s'annule aux entiers pairs. C'est parce que ces termes tendent vers 0 près des entiers négatifs que le respect des Équations (3.4.1) et (3.4.17) change dans cette région. Une question naturelle se pose donc: quel serait l'effet sur la propriété de Northcott si les premiers à l'infini étaient inclus dans la définition de la fonction zêta comme c'est le

cas dans la Section 1.3.2 pour $Z_K(s)$. Une conséquence immédiate est que cette fonction ne possède pas de zéros triviaux! Évidemment, la question inverse se pose tout autant: quel serait l'effet sur la propriété de Northcott si on exclut les premiers à l'infini de la fonction zêta comme c'est le cas à la Définition 1.3.21?

Chapitre 2

On the Northcott property of zeta functions over function fields

par

Xavier G n reux, Matilde Lal n, Wanlin Li¹

- (¹) Xavier G n reux: D partement de math matiques et de statistique, Universit  de Montr al. CP 6128, succ. Centre-ville. Montreal, QC H3C 3J7, Canada
- (²) Matilde Lal n: D partement de math matiques et de statistique, Universit  de Montr al. CP 6128, succ. Centre-ville. Montreal, QC H3C 3J7, Canada
- (³) Wanlin Li: Centre de recherches math matiques, Universit  de Montr al. CP 6128, succ. Centre-ville. Montreal, QC H3C 3J7, Canada

Xavier G n reux, Matilde Lal n, Wanlin Li, On the Northcott property of zeta functions over function fields, *Finite Fields and Their Applications*, Volume 83, 2022, 102080, ISSN 1071-5797.

Chacun des auteurs a contribu    part  gale   la publication.

ABSTRACT. Pazuki and Pengo defined a Northcott property for special values of zeta functions of number fields and certain motivic L -functions. We determine the values for which the Northcott property holds over function fields with constant field \mathbb{F}_q outside the critical strip. We then use a case by case approach for some values inside the critical strip, notably $\operatorname{Re}(s) < \frac{1}{2} - \frac{\log 2}{\log q}$ and for s real such that $1/2 \leq s \leq 1$, and we obtain a partial result for complex s in the case $1/2 < \operatorname{Re}(s) \leq 1$ using recent advances on the Shifted Moments Conjecture over function fields.

Keywords: Zeta function over function fields; Northcott property

2.1. Introduction

The Northcott property [42] implies that a set of algebraic numbers with bounded height and bounded degree must be finite. In [47], Pazuki and Pengo study a variant of the Northcott property for number fields using special values of the Dedekind zeta function to measure the height. For a field K and $s \in \mathbb{C}$ denote

$$\zeta_K^*(s) := \lim_{t \rightarrow s} \frac{\zeta_K(t)}{(t-s)^{\operatorname{ord}_s(\zeta_K(t))}},$$

the first nonzero coefficient of the Taylor series for $\zeta_K(s)$ around s .

For a fixed $s = n \in \mathbb{Z}$, Pazuki and Pengo consider, for B a fixed positive real number, the set of isomorphism classes of number fields

$$\{[K] : |\zeta_K^*(n)| \leq B\}, \tag{2.1.1}$$

and discuss the finiteness of this set under various conditions of BB and nn. For number fields, they prove that a Northcott property holds for nn located at the left of the critical strip, but does not hold for nn to the right of the critical strip, and they show that such a property does not hold for $n = 1$, but holds for $n = 0$. They also estimate the size of this set when the Northcott property holds.

We are interested in exploring the Northcott property for global function fields, more precisely, we consider the set of isomorphism classes of function fields K with constant field \mathbb{F}_q , and we aim at considering the value of its zeta function at any complex number $s \in \mathbb{C}$. To this end, we define

$$S_{q,s,B} = \{[K] : |\zeta_K^*(s)| \leq B\},$$

where $[K]$ denotes the isomorphism class of K , a global function field in one variable over a finite constant field \mathbb{F}_q with q elements, where q is fixed. The Northcott property of \mathbb{F}_q at s is equivalent to having $S_{q,s,B}$ finite for all $B \in \mathbb{R}_{>0}$. More generally, we consider the following definition.

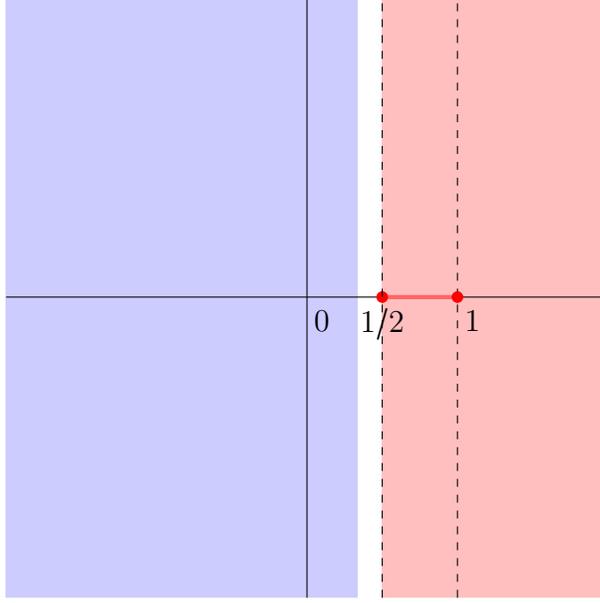


Fig. 2.1. For the base field \mathbb{F}_q , the Northcott property holds in the area in blue. Bright red indicates that $S_{q,s,B}$ is infinite for all B . This involves the real segment $[1/2,1]$, where for $s = 1/2$, we take the Northcott property with $\zeta_K(1/2)$. Light red means that $S_{q,s,B}$ is infinite for B greater than a certain constant. The dashed line at $\text{Re}(s) = 1$ indicates the boundary of the critical strip. More elementary results are available for $\text{Re}(s) > 1$. Remark that the white gap corresponding to $\frac{1}{2} - \frac{\log 2}{\log q} \leq \sigma < \frac{1}{2}$ disappears as $q \rightarrow \infty$.

Definition 2.1.1. Let q be a power of a prime, $s \in \mathbb{C}$, and $\mathcal{I} \subset \mathbb{R}_{\geq 0}$. We say that the triple (q,s,\mathcal{I}) has the Northcott property if the set $S_{q,s,B}$ is finite for all $B \in \mathcal{I}$. We say that (q,s,\mathcal{I}) is non-Northcott if the set $S_{q,s,B}$ is infinite for all $B \in \mathcal{I}$.

The Riemann hypothesis implies that the zeros of $\zeta_K(s)$ are included in $\text{Re}(s) = 1/2$. While working with the Northcott property on s such that $\text{Re}(s) = 1/2$ we will sometimes replace $\zeta_K^*(s)$ by $\zeta_K(s)$ in the definition of Northcott property. This will allow us to conclude that the Northcott property is not satisfied when there are infinitely many zeros. More precisely, we consider the following definition.

Definition 2.1.2. Let q be a power of a prime, $s \in \mathbb{C}$ such that $\text{Re}(s) = 1/2$, and $\mathcal{I} \subset \mathbb{R}_{\geq 0}$. We say that the triple (q,s,\mathcal{I}) has the Northcott property with $\zeta_K(s)$ if the set

$$\{[K] : |\zeta_K(s)| \leq B\} \tag{2.1.2}$$

is finite for all $B \in \mathcal{I}$. We say that (q,s,\mathcal{I}) is non-Northcott with $\zeta_K(s)$ if the set (2.1.2) is infinite for all $B \in \mathcal{I}$.

We prove the following results.

Theorem 2.1.3. *Let $\sigma = \text{Re}(s)$.*

- a) *If $q > 4$, then $(q, 0, \mathbb{R}_{>0})$ satisfies the Northcott property.*
- b) *When $\sigma < \frac{1}{2} - \frac{\log 2}{\log q}$, then $(q, s, \mathbb{R}_{>0})$ satisfies the Northcott property.*
- c) *Let $\sigma > 1$ and*

$$B = \frac{1}{(1 - q^{-\sigma})(1 - q^{1-\sigma})^2}.$$

Then $(q, s, \mathbb{R}_{\geq B})$ is non-Northcott.

- d) *For $q \equiv 1 \pmod{4}$, $(q, 1, \mathbb{R}_{>0})$ is non-Northcott.*
- e) *For $q \equiv 1 \pmod{4}$ and $1/2 < \sigma < 1$, $(q, \sigma, \mathbb{R}_{>0})$ is non-Northcott.*
- f) *$(q, 1/2, \mathbb{R}_{>0})$ is non-Northcott with $\zeta_K(1/2)$ (as opposed to $\zeta_K^*(1/2)$).*
- g) *For $q \equiv 1 \pmod{4}$ and $1/2 < \sigma$ (except $s = \frac{2\pi im}{\log q} + 1$ for $m \in \mathbb{Z}$), let*

$$B = \left| \frac{1}{(1 - q^{-s})(1 - q^{1-s})} \right| \times \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left[\frac{1}{2} \left(\left(1 - \frac{1}{|P|^{s-\frac{1}{2}}}\right)^{-1} \left(1 - \frac{1}{|P|^{\bar{s}-\frac{1}{2}}}\right)^{-1} + \left(1 + \frac{1}{|P|^{s-\frac{1}{2}}}\right)^{-1} \left(1 + \frac{1}{|P|^{\bar{s}-\frac{1}{2}}}\right)^{-1} \right) + \frac{1}{|P|} \right]^{1/2} \times \left(1 + \frac{1}{|P|}\right)^{-1/2}.$$

Then $(q, s, \mathbb{R}_{>B})$ is non-Northcott.

In the list of Theorem 2.1.3, statements d), e), and f) depend on deep results on the distribution of quadratic Dirichlet L -functions due to Lumley [35, 37] and Li [32], while g) for $\sigma < 1$ depends on the Shifted Moments Conjecture for quadratic Dirichlet L -functions, which was formulated by Andrade and Keating [4] for the function field case, and has been recently proven under certain constraints by Bui, Florea, and Keating [10]. The result of g) for $\sigma \geq 1$ follows directly from a moment computation and improves upon the set given in c). The result of f) is with $\zeta_K(1/2)$ as it rests on the existence of infinitely many $[K]$ such that $\zeta_K(1/2) = 0$, instead of working with $\zeta_K^*(1/2)$.

In addition, we discuss bounds for $\#S_{q,s,B}$ in the cases of a) and b). More precisely, we use a result of Couveignes [14] to prove that there is an absolute computable constant \mathcal{Q} (independent of q) such that

$$\#S_{q,s,B} \leq q^{\mathcal{Q}c_\sigma(\log B)^3 B}, \tag{2.1.3}$$

where

$$c_\sigma = \frac{1}{(\log q) \log \left(q^{\frac{1}{2}-\sigma} - 1 \right)}.$$

(We recall that the cases *a*) and *b*) only occur when $\sigma \neq 1/2$, and therefore the value for c_σ above is well-defined.)

Pazuki and Pengo [47] study the Northcott, Bogomolov, and Lehmer properties for special values of L -functions evaluated at $n \in \mathbb{Z}$. They prove that the Northcott property holds at the left of the critical strip for a general family of motivic L -functions (assuming meromorphic continuation and functional equation), which can be compared to our result of Theorem 2.1.3 *b*). They also focus on the Northcott property for Dedekind zeta functions of number fields evaluated at integer numbers and prove that it is not satisfied for $n \in \mathbb{Z}_{\geq 1}$, in a result analogous to our Theorem 2.1.3 *c*). When $n \in \mathbb{Z}_{\leq 0}$, they obtain bounds for the size of the set given in (2.1.1) which are better than (2.1.3) in the case of $n < 0$, but worse than (2.1.3) in the case of $n = 0$. Our results are limited by the lack of understanding on the number of smooth, projective curves of genus g over a fixed finite field.

This article is organized as follows. Section 3.2 covers standard background on the zeta function attached to a global function field. Sections 3.4 and 3.3 treat the left and right sides of the critical strip, while Section 2.5 considers the critical strip.

Acknowledgements

The authors are grateful to Jordan Ellenberg, Alexandra Florea, Allysa Lumley, and Timothy Trudgian for many useful discussions. We would like to thank the referee for their dedicated work and many helpful remarks and corrections. This work was supported by the Centre de recherches mathématiques and the Institut des sciences mathématiques (CRM-ISM postdoctoral fellowship to WL, ISM summer internship to XG), the Natural Sciences and Engineering Research Council of Canada (Discovery Grant 355412-2013 to ML), and the Fonds de recherche du Québec - Nature et technologies (Projet de recherche en équipe 256442 and 300951 to ML).

2.2. Some background on $\zeta_K(s)$

In this section we recall some background on function fields with constant field \mathbb{F}_q . More details can be found in [51].

Let K be a global function field in one variable with a finite constant field \mathbb{F}_q with q elements. A prime of K is a discrete valuation ring R with maximal ideal P such that

$\mathbb{F}_q[T] \subset R$ and the quotient field of R equals K . The degree of a prime P , denoted by $\deg(P)$ is the (finite) dimension of R/P over \mathbb{F}_q . The group of divisors of K is the free abelian group generated by the primes. Thus, a divisor is an element of the form $A = \sum_P a(P)P$. In this case, $\sum_P a(P) \deg(P)$ is called the degree of A , denoted $\deg(A)$. The norm of A is equal to $q^{\deg(A)}$ and is denoted by $|A|$. The divisor A is said to be effective if $a(P) \geq 0$ for all P . We write $A \geq 0$ to indicate that A is effective.

The zeta function of K is defined for $\operatorname{Re}(s) > 1$ by

$$\zeta_K(s) := \sum_{A \geq 0} \frac{1}{|A|^s} = \sum_{n=0}^{\infty} \frac{b_n}{q^{ns}},$$

where the sum is taken over all the effective divisors, and b_n is the number of effective divisors of degree n . Notice that $\zeta_K(s)$ satisfies an Euler product

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1},$$

where the product takes over the primes of K .

From this, we have

$$\log \zeta_K(s) = \sum_P \sum_{j=1}^{\infty} \frac{1}{j|P|^{js}} = \sum_{A \geq 0} \frac{\Lambda(A)}{\deg(A)|A|^s}, \quad (2.2.1)$$

where $\Lambda(A)$ is the von Mangoldt function, equal to $\deg(P)$ if $A = P^j$ (or $A = jP$ if written additively) for P prime and 0 otherwise.

By the Weil conjectures ([51, Theorem 5.9]), there is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$, where g is the genus of the curve whose function field is K , such that

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}. \quad (2.2.2)$$

The right hand side provides a meromorphic continuation for $s \in \mathbb{C}$. We immediately see that $\zeta_K(s)$ has simple poles at $s = \frac{2\pi in}{\log q}$ and $s = \frac{2\pi im}{\log q} + 1$ for $m, n \in \mathbb{Z}$. If we set

$$\xi_K(s) = q^{(g-1)s} \zeta_K(s),$$

then we have the functional equation

$$\xi_K(1-s) = \xi_K(s). \quad (2.2.3)$$

The Riemann Hypothesis, which is known to be true in this context, implies that the zeros of $\zeta_K(s)$ occur only at $\operatorname{Re}(s) = 1/2$.

The function $\zeta_K(s)$ admits certain symmetry inherited from the functional equation. This symmetry centers on the critical line $\operatorname{Re}(s) = 1/2$. It is natural to analyze the behavior of $|\zeta_K(s)|$ depending on the position of s respect to the critical strip.

After making the change of variables $u = q^{-s}$, we can write

$$L_K(u) = \prod_{j=1}^{2g} (1 - \pi_j u), \quad (2.2.4)$$

where $|\pi_j| = \sqrt{q}$. In addition, it is known that $L_K(0) = 1$ and $L_K(1) = h_K$, the class number of K . By the functional equation, the π_j 's can be separated in pairs of complex conjugates, so that $\pi_j = \overline{\pi_{2g-j}}$. Notice that we also have ([51, Theorem 5.12])

$$\sum_{j=1}^{2g} \pi_j^\ell = q^\ell + 1 - \sum_{d|\ell} da_d, \quad (2.2.5)$$

where

$$a_d = \#\{P : \deg(P) = d\}. \quad (2.2.6)$$

Thus, we can write the Euler product for $\zeta_K(s)$ as

$$\zeta_K(s) = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-a_n}. \quad (2.2.7)$$

In particular for $K = \mathbb{F}_q(T)$ we have

$$\zeta_{\mathbb{F}_q(T)}(s) = \prod_P \left(1 - \frac{1}{|P|}\right)^{-1},$$

where the product is over all the primes of $\mathbb{F}_q(T)$, namely, the monic irreducible polynomials and the prime at infinity. When P is a monic irreducible polynomial, we have that $|P| = q^{\deg(P)}$, while the prime at infinity has norm q , since its degree is 1. Notice that

$$\zeta_{\mathbb{F}_q(T)}(s) = \frac{1}{(1 - q^{-s})(1 - q^{1-s})}.$$

We will also denote by $\zeta_{\mathbb{F}_q[T]}$ the zeta function without the prime at infinity. In this case

$$\zeta_{\mathbb{F}_q[T]}(s) = \frac{1}{1 - q^{1-s}}.$$

Throughout this paper we will write $s = \sigma + i\tau$, where σ, τ are real numbers.

2.3. The left side of the critical strip

Starting with the left side of the critical strip, we obtain a positive result for a large subset of $\mathbb{C}_{\sigma < 1/2}$ that contains $\mathbb{C}_{\sigma \leq 0}$ (for $q > 4$). More precisely, we prove in Theorems 2.3.3 and 2.3.4 that for s in the blue area of Figure 2.1, $(q, s, \mathbb{R}_{>0})$ has the Northcott property.

Lemma 2.3.1. *The polynomial $L_K(u) \in \mathbb{Z}[u]$ satisfies the following bounds*

$$(\sqrt{q}|u| - 1)^{2g} \leq |L_K(u)| \leq (\sqrt{q}|u| + 1)^{2g}. \quad (2.3.1)$$

PROOF. This follows immediately from equation (2.2.4) and the triangle inequality on each factor. \square

Lemma 2.3.2. *Let q be a power of a prime p . For a fixed g there are finitely many isomorphism classes of global function fields over \mathbb{F}_q with genus g .*

PROOF. The statement follows from the fact that there exists a moduli stack \mathcal{M}_g over \mathbb{F}_p classifying smooth proper curves of genus $g \geq 2$. (See for example [15].) \square

We are ready to prove the main result of this section. First we treat the case $s = 0$ separately.

Theorem 2.3.3. *Let q be a power of a prime such that $q > 4$. We have that $(q, 0, \mathbb{R}_{>0})$ satisfies the Northcott property.*

PROOF. We remark that

$$\zeta_K^*(0) = \lim_{s \rightarrow 0} \frac{sL_K(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})} = \frac{h_K}{1 - q} \lim_{s \rightarrow 0} \frac{s}{1 - q^{-s}} = \frac{h_K}{(1 - q) \log q}.$$

By Lemma 2.3.1, we have that

$$\frac{(\sqrt{q} - 1)^{2g}}{(q - 1) \log q} \leq |\zeta_K^*(0)|. \quad (2.3.2)$$

Since $q > 4$, $\sqrt{q} - 1 > 1$, and we conclude that $|\zeta_K^*(0)| \rightarrow \infty$ as long as $g \rightarrow \infty$. Therefore, if $[K] \in S_{q,0,B}$, we must have that $g(K)$ is bounded. By Lemma 2.3.2, there are only finitely many $[K]$ for each g , and we conclude that $S_{q,0,B}$ must be finite. \square

Theorem 2.3.4. *Let $s = \sigma + i\tau \in \mathbb{C}^*$ such that*

$$\sigma < 1/2 - \frac{\log 2}{\log q},$$

then $(q, s, \mathbb{R}_{>0})$ satisfies the Northcott property.

PROOF. First notice that if $\sigma < 1/2 - \frac{\log 2}{\log q}$, then we have that $2 < q^{\frac{1}{2}-\sigma}$. From here, we deduce that

$$\sqrt{q}|u| - 1 > 1.$$

By Lemma 2.3.1, we conclude that $|L_K(u)| \rightarrow \infty$ as long as $g \rightarrow \infty$. We reach the same conclusion as long as $s \neq 0$, since the denominator in $\zeta_K(s)$ is non-zero and bounding $|\zeta_K(s)|$ is therefore equivalent to bounding $|L_K(u)|$. Thus, if $[K] \in S_{q,s,B}$, we must have that $g(K)$ is bounded. By Lemma 2.3.2, there are only finitely many $[K]$ for each g , and we conclude that $S_{q,s,B}$ must be finite. □

A natural question is to bound the size of $S_{q,s,B}$ in the cases when it is finite. We will need the following result of Couveignes [14].

Theorem 2.3.5. [14, Theorem 2 (simplified version)] *There exists an absolute and computable constant \mathcal{Q} such that the following is true. Let $K = \mathbb{F}_q(T)(\mathcal{C}) = \mathbb{F}_q(T, X)$ be a function field of genus $g \geq 2$ and degree $[\mathbb{F}_q(T, X) : \mathbb{F}_q(T)] = n$. Then K is determined by at most*

$$\mathcal{Q}(\log n)^2(g + n(1 + \log_q n))$$

parameters of \mathbb{F}_q .

Although Couveignes does not give the value of \mathcal{Q} , this constant is only related to the technicalities of the proof and is independent of the base field. In our context this means that it is independent of q .

Using Theorem 3.4.6, we can prove the following bound.

Theorem 2.3.6. *Let $\varepsilon > 0$ and $s \in \mathbb{C}$ such that $\sigma < 1/2 - \frac{\log 2}{\log q}$. Then, as $B \rightarrow \infty$, we have*

$$\#S_{q,s,B} \leq q^{\mathcal{Q}c_\sigma(\log B)^3 B},$$

where

$$c_\sigma = \frac{1}{(\log q) \log \left(q^{\frac{1}{2}-\sigma} - 1 \right)}.$$

PROOF. By Theorem 3.4.6, the number of possible fields K of genus g and degree n is bounded by

$$q^{\mathcal{Q}(\log n)^2(g+n(1+\log_q n))}.$$

We need to count over all possible values of n . We can take n as the gonality of the curve \mathcal{C} , defined as the smallest possible degree of a dominant map $\mathcal{C} \rightarrow \mathbb{P}^1(\mathbb{F}_q(T))$, and known

to be bounded by $2g-2$ when $g > 1$ (see [49, Proposition A.1]). For $g = 1$, we have an elliptic curve, and we can bound the degree of the function field by 2. Thus, we have a bound for the number of isomorphism classes of fields under consideration with fixed genus g given by

$$\sum_{n=2}^{2g-2} q^{\mathcal{Q}(\log n)^2(g+n(1+\log_q n))} \leq q^{\mathcal{Q}(\log(2g-2))^2(g+(2g-2)(1+\log_q(2g-2))+1)} \quad (g \geq 2).$$

For $g = 1$ this number is bounded by

$$1 + q^{\mathcal{Q}(\log 2)^2(1+2(1+\log_q 2))},$$

and for $g = 0$, we have just one field.

We proceed to let g vary. First consider the case $s = 0$ with $q > 4$. By equation (2.3.2), we have

$$\frac{(\sqrt{q} - 1)^{2g}}{(q - 1) \log q} \leq B,$$

and this gives

$$g \leq \frac{\log((q-1)(\log q)B)}{2 \log(\sqrt{q}-1)} = a_0 \log B + b_0,$$

where $a_0 = \frac{1}{2 \log(\sqrt{q}-1)}$ and $b_0 = \frac{\log((q-1)(\log q))}{2 \log(\sqrt{q}-1)}$ denote constants that are only dependent on q .

Now consider the case $s \neq 0$ such that $\sigma < 1/2 - \frac{\log 2}{\log q}$. By equation (2.3.1),

$$\frac{(q^{\frac{1}{2}-\sigma} - 1)^{2g}}{|(1 - q^{-\sigma-i\tau})(1 - q^{1-\sigma-i\tau})|} \leq B,$$

and this gives

$$g \leq \frac{\log(|(1 - q^{-\sigma-i\tau})(1 - q^{1-\sigma-i\tau})| B)}{2 \log(q^{\frac{1}{2}-\sigma} - 1)} \leq a_\sigma \log B + b_\sigma,$$

where $a_\sigma = \frac{1}{2 \log(q^{\frac{1}{2}-\sigma} - 1)}$ and $b_\sigma = \frac{\log((1+q^{-\sigma})(1+q^{1-\sigma}))}{2 \log(q^{\frac{1}{2}-\sigma} - 1)}$ are constants that are only dependent on σ and q .

Finally, we need to consider the bound summing all the possible values g up to $aB + b$. This gives

$$\begin{aligned} & 2 + q^{\mathcal{Q}(\log 2)^2(1+2(1+\log_q 2))} + \sum_{2 \leq g \leq aB+b} q^{\mathcal{Q}(\log(2g-2))^2(g+(2g-2)(1+\log_q(2g-2))+1)} \\ & \leq 2 + q^{\mathcal{Q}(\log 2)^2(1+2(1+\log_q 2))} + q^{\mathcal{Q}(\log(2(aB+b-1)))^2(aB+b+2(aB+b-1)(1+\log_q(2(aB+b-1))))+2}. \end{aligned}$$

As $B \rightarrow \infty$ the above is bounded by

$$\leq q^{\frac{2a(1+a(1))}{\log q} (\log B)^3 B}.$$

We conclude by noticing that the formula for a_0 is simply the result of specializing a_σ at $\sigma = 0$. \square

Remark 2.3.7. Lipnowski and Tsimerman [33, Lemma 2.1, Corollary 2.2] estimate the number of possible $L_K(u)$ of fixed genus g to be at most $(2g)^g q^{\frac{1}{4}g(g+1)}$. In the same article, [33, Eq. (28)] gives a bound for the number of isomorphism classes on each isogeny class of $p^{\frac{33}{4}g^2(1+o(1))}$. Combining these two estimates gives a bound of

$$(2g)^g q^{\frac{1}{4}g(g+1)} p^{\frac{33}{4}g^2(1+o(1))}$$

for the number of isomorphism classes of fields under consideration with fixed genus g . While this formula is more explicit than the bound given by Theorem 3.4.6, the final bound for $\#S_{q,s,B}$ is asymptotically worse as it has g^2 in the exponent. In fact, this leads to

$$\#S_{q,s,B} \leq q^{\frac{17}{2}a_\sigma^2(1+o(1))B^2}.$$

Remark 2.3.8. The result of Theorem 2.3.6 can be in principle improved if we use the argument by de Jong and Katz [15], which claims that the number of smooth proper curves of genus $g \geq 2$ is bounded by

$$g^{c_1 g} q^{c_2 g},$$

where c_1, c_2 are (non-effective) positive constants. This leads to

$$\#S_{q,s,B} \leq q^{c_1 a_\sigma (1+o(1))(\log B)B},$$

This bound has a slightly better asymptotic than the result of Theorem 2.3.6, but it has the disadvantage that we can not compute c_1 .

2.4. The right side of the critical strip

We now consider the right side of the critical strip, that is, $\mathbb{C}_{\sigma>1}$, where we obtain a result conditionally on the value of B . More precisely, we prove that for the s in the pale shade of red of Figure 2.1, the Northcott property does not hold for B sufficiently large.

The first result allows us to compare $\zeta_K(s)$ with $\zeta_K(\sigma)$.

Lemma 2.4.1. *Let $s = \sigma + i\tau \in \mathbb{C}$ with $\sigma > 1$. Then*

$$\frac{1}{\zeta_K(\sigma)} \leq |\zeta_K(s)| \leq \zeta_K(\sigma).$$

PROOF. We start by proving the upper bound. Since $\sigma > 1$, the Dirichlet series for $\zeta_K(s)$ converges and we can directly bound

$$|\zeta_K(\sigma + i\tau)| = \left| \sum_{n=1}^{\infty} \frac{b_n}{q^{n(\sigma+i\tau)}} \right| \leq \sum_{n=1}^{\infty} \left| \frac{b_n}{q^{n(\sigma+i\tau)}} \right| = \sum_{n=1}^{\infty} \frac{b_n}{q^{n\sigma}} = \zeta_K(\sigma).$$

Now we proceed to prove the lower bound. Notice that for any θ , $1 + \cos(\theta) \geq 0$. By considering the logarithm of the Euler product (2.2.1), we have that

$$\log \zeta_K(\sigma) + \operatorname{Re} \log \zeta_K(\sigma + i\tau) = \sum_P \sum_{j=1}^{\infty} \frac{1 + \cos(\tau \log |P^j|)}{j|P|^{j\sigma}} \geq 0.$$

Taking the exponential, we conclude that

$$\zeta_K(\sigma) |\zeta_K(s)| \geq 1 \tag{2.4.1}$$

as desired. \square

Corollary 2.4.2. *For $\sigma > 1$,*

$$1 \leq \zeta_K(\sigma).$$

PROOF. This follows directly from setting $s = \sigma$ in (2.4.1). \square

Lemma 2.4.1 shows that if we can control $\zeta_K(\sigma)$, then we can also control $|\zeta_K(s)|$. We now focus on estimating $\zeta_K(\sigma)$.

Lemma 2.4.3. *Let a_ℓ be defined by equation (2.2.6). Then*

$$a_\ell \leq \frac{q^\ell}{\ell} + q^{\ell/3} + \frac{2g}{\ell} q^{\ell/2} + 2gq^{\ell/4}.$$

PROOF. This proof follows from combining various elements from [51, Theorem 5.12]. By applying Möbius inversion to (2.2.5), we have, for $\ell > 1$,

$$\ell a_\ell = \sum_{d|\ell} \mu(d) q^{\ell/d} + \sum_{d|\ell} \mu(d) \left(\sum_{j=1}^{2g} \pi_j^{\ell/d} \right). \tag{2.4.2}$$

We focus on the first term. The highest power of q is q^ℓ and the second highest power is $q^{\ell/2}$ that only appears when $2 \mid \ell$ and in that case, it has coefficient -1 . All the other powers are at most $q^{\ell/3}$. The total number of terms is bounded by $\sum_{d|\ell} |\mu(d)|$, which is seen to be $2^{\omega(\ell)}$, where $\omega(\ell)$ is the number of distinct prime divisors of ℓ . If $p_1, \dots, p_{\omega(\ell)}$ are the distinct primes dividing ℓ , then one has that $2^{\omega(\ell)} \leq p_1 \cdots p_{\omega(\ell)} \leq \ell$. Combining all of this, we obtain

$$\sum_{d|\ell} \mu(d) q^{\ell/d} \leq q^\ell + \ell q^{\ell/3}. \tag{2.4.3}$$

Similarly, we have

$$\left| \sum_{d|\ell} \mu(d) \left(\sum_{j=1}^{2g} \pi_j^{\ell/d} \right) \right| \leq 2gq^{\ell/2} + 2g\ell q^{\ell/4}. \quad (2.4.4)$$

The result follows by combining equations (2.4.3) and (2.4.4). \square

We use the previous estimate to give an upper bound for $\zeta_K(\sigma)$.

Remark 2.4.4. By employing a better estimate for $\omega(\ell)$ given by Robin in [50, Theorem 11]

$$\omega(\ell) \leq 1.3841 \frac{\log \ell}{\log \log \ell} \quad \ell \geq 3,$$

one can actually prove

$$\sum_{d|\ell} \mu(d) q^{\ell/d} \leq q^\ell + \ell^{\frac{0.96}{\log \log \ell}} q^{\ell/3}, \quad (2.4.5)$$

and we remark that the above bound is true for $\ell \geq 1$. This leads to

$$a_\ell \leq \frac{q^\ell}{\ell} + \frac{q^{\ell/3}}{\ell^{1-\frac{0.96}{\log \log \ell}}} + \frac{2g}{\ell} q^{\ell/2} + 2gq^{\ell/4}.$$

This is a much better bound when ℓ is large. For our purposes, the biggest terms will come from $g \rightarrow \infty$, and therefore we will continue to work with the inequality from Lemma 2.4.3.

Proposition 2.4.5. *Let $\sigma > 1$. Then we have*

$$\zeta_K(\sigma) \leq \left(\frac{\exp\left(\frac{1}{q^{\sigma-\frac{1}{3}}-1} + \frac{2g}{q^{\sigma-\frac{1}{4}}-1}\right)}{(1-q^{1-\sigma})(1-q^{\frac{1}{2}-\sigma})^{2g}} \right)^{\frac{q^\sigma}{q^\sigma-1}}.$$

PROOF. We apply Lemma 2.4.3 to the Euler product (2.2.7) and obtain

$$\begin{aligned} \log \zeta_K(\sigma) &= - \sum_{n=1}^{\infty} a_n \log \left(1 - \frac{1}{q^{n\sigma}} \right) \\ &\leq - \sum_{n=1}^{\infty} \left(\frac{q^n}{n} + q^{n/3} + \frac{2g}{n} q^{n/2} + 2gq^{n/4} \right) \log \left(1 - \frac{1}{q^{n\sigma}} \right). \end{aligned}$$

By using the estimate $1 - \frac{1}{x} \leq \log(x)$ for $x \in \mathbb{R}_{\geq 0}$, we obtain

$$\log \zeta_K(\sigma) \leq \sum_{n=1}^{\infty} \left(\frac{q^n}{n} + q^{n/3} + \frac{2g}{n} q^{n/2} + 2gq^{n/4} \right) \frac{1}{q^{n\sigma} - 1}.$$

Now we further use the bound

$$\frac{q^{n\sigma}}{q^{n\sigma} - 1} \leq \frac{q^\sigma}{q^\sigma - 1}$$

and get

$$\begin{aligned} \log \zeta_K(\sigma) &\leq \frac{q^\sigma}{q^\sigma - 1} \sum_{n=1}^{\infty} \left(\frac{q^n}{n} + q^{n/3} + \frac{2g}{n} q^{n/2} + 2gq^{n/4} \right) q^{-n\sigma} \\ &= \frac{q^\sigma}{q^\sigma - 1} \left(-\log(1 - q^{1-\sigma}) - 2g \log(1 - q^{\frac{1}{2}-\sigma}) + \frac{1}{q^{\sigma-\frac{1}{3}} - 1} + \frac{2g}{q^{\sigma-\frac{1}{4}} - 1} \right), \end{aligned}$$

and thus

$$\zeta_K(\sigma) \leq \left(\frac{\exp\left(\frac{1}{q^{\sigma-\frac{1}{3}}-1} + \frac{2g}{q^{\sigma-\frac{1}{4}}-1}\right)}{(1 - q^{1-\sigma})(1 - q^{\frac{1}{2}-\sigma})2g} \right)^{\frac{q^\sigma}{q^\sigma-1}}.$$

□

The result of Proposition 2.4.5 gives an upper bound for $\zeta_K(\sigma)$ when $\sigma > 1$. This upper bound tends to infinity as $g \rightarrow \infty$, and therefore it gives a weak result in terms of the Northcott property.

We close this section by focusing on the case of quadratic fields, where we obtain a better upper bound, independent of g .

Proposition 2.4.6. *Let $\sigma > 1$ and K be a quadratic extension of $\mathbb{F}_q(T)$ with constant field \mathbb{F}_q . Then*

$$|\zeta_K(\sigma)| \leq \frac{1}{(1 - q^{-\sigma})(1 - q^{1-\sigma})^2}.$$

PROOF. Since K is quadratic, we can write

$$\zeta_K(s) = \frac{L(s, \chi_D)}{(1 - q^{-s})(1 - q^{1-s})}, \quad (2.4.6)$$

where χ_D is the quadratic character associated to the extension and

$$L(s, \chi_D) = \sum_{f \text{ monic}} \frac{\chi_D(f)}{|f|^s}.$$

To be concrete, we can think of $\chi_D(f) := \left(\frac{D}{f}\right)_2$, the Legendre symbol, with $D \in \mathcal{H}_{2g+1}$, the set of monic square-free polynomials of degree $2g + 1$. Furthermore, we can think of $K = \mathbb{F}_q(T)(\sqrt{D})$.

We have

$$|L(s, \chi_D)| \leq \sum_{f \text{ monic}} \left| \frac{\chi_D(f)}{|f|^s} \right| \leq \sum_{f \text{ monic}} \frac{1}{|f|^\sigma} = \zeta_q(\sigma) = \frac{1}{1 - q^{1-\sigma}}.$$

Considering the denominator of $\zeta_K(s)$ in (2.4.6), we obtain the result.

□

Theorem 2.4.7. *Let $\sigma > 1$, and*

$$B \geq \frac{1}{(1 - q^{-\sigma})(1 - q^{1-\sigma})^2}.$$

Then (q, s, B) does not satisfy the Northcott property.

PROOF. By Proposition 2.4.6, $|\zeta_K(\sigma)| \leq B$ for all quadratic fields provided that B is larger than $\frac{1}{(1 - q^{-\sigma})(1 - q^{1-\sigma})^2}$. This gives an infinite family of quadratic fields with $|\zeta_K(\sigma)| \leq B$.

For complex s , we use the upper bound in Lemma 2.4.1 to conclude. \square

2.5. Inside the critical strip

In this section we use results of Lumley [35, 37], Li [32], and Bui, Florea, and Keating [10] to get information on some specific values inside the critical strip. Unless otherwise stated, we assume that $q \equiv 1 \pmod{4}$. This is a common assumption made in [4, 35, 37] that allows cleaner formulas as quadratic reciprocity becomes trivial.

2.5.1. The Northcott property at the pole $s = 1$

Here we treat the case of $s = 1$ and, of course, $s = \frac{2\pi im}{\log q} + 1$ for $m \in \mathbb{Z}$. This corresponds to the right bold point in red of Figure 2.1 and is repeated periodically on the line $\operatorname{Re}(s) = 1$. We consider the following result of Lumley.

Theorem 2.5.1. [35, Corollary 1.8] *For g large and $1 \leq \tau \leq \log g - 2\log(\log g) - \log(\log(\log g))$, the number of $D \in \mathcal{H}_{2g+1}$ such that*

$$\frac{h_D}{q^g} < \frac{\zeta_{\mathbb{F}_q[T]}(2)}{e^{\gamma\tau}}$$

is given by

$$(\#\mathcal{H}_{2g+1}) \exp\left(-C_1(q^{\{\log \kappa(\tau)\}}) \frac{q^{\tau - C_0(q^{\{\log \kappa(\tau)\}})}}{\tau} \left(1 + O\left(\frac{\log \tau}{\tau}\right)\right)\right). \quad (2.5.1)$$

Above, we have written h_D instead of $h_{\mathbb{F}_q(T)(\sqrt{D})}$ for short, and γ denotes the Euler—Mascheroni constant. We will not discuss κ , C_0 , and C_1 . It suffices to say that $C_0(q^{\{\log \kappa(\tau)\}})$ and $C_1(q^{\{\log \kappa(\tau)\}})$ are positive functions depending on τ .

Theorem 2.5.2. *Let $B > 0$. Then $(q, 1, B)$ does not satisfy the Northcott property.*

PROOF. Given $B > 0$, fix τ large enough such that

$$\frac{\zeta_{\mathbb{F}_q[T]}(2)}{e^{\gamma\tau}} \cdot \frac{q}{(1-q^{-1})\log q} < B.$$

Since τ is fixed, we can evaluate the exponential factor in (2.5.1) and it gives a fixed positive constant $c(\tau)$ (that can be very small).

We have that (see for example, [51, Proposition 2.3])

$$\#\mathcal{H}_n = \begin{cases} q^n(1-q^{-1}) & n \geq 2, \\ q^n & n = 0, 1. \end{cases} \quad (2.5.2)$$

Applying this, we get that for g large enough (so that τ satisfies the right conditions) there are at least

$$q^{2g+1}(1-q^{-1})c(\tau)$$

possible $D \in \mathcal{H}_{2g+1}$ satisfying that

$$\frac{h_D q^{-g}}{(1-q^{-1})\log q} < B.$$

We will combine this with the fact that

$$\zeta_K^*(1) = \lim_{s \rightarrow 1} \frac{(s-1)L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})} = \frac{L_K(q^{-1})}{1-q^{-1}} \lim_{s \rightarrow 0} \frac{s-1}{1-q^{1-s}} = \frac{L_K(q^{-1})}{(1-q^{-1})\log q} = \frac{h_K q^{-g}}{(1-q^{-1})\log q},$$

where the equality $L_K(q^{-1}) = h_K q^{-g}$ follows from the functional equation (2.2.3).

Finally, we obtain

$$\zeta_K^*(1) < B.$$

Letting $g \rightarrow \infty$, we have that $S_{q,1,B}$ is infinite for any choice of $B > 0$. \square

2.5.2. The segment of the real line inside the right side of the critical line

For $1/2 < \sigma < 1$ we use another result of Lumley that is very similar to the result we had at the pole $s = 1$. This corresponds to the red segment in Figure 2.1.

Theorem 2.5.3. [37, Theorem 1.3, partial statement] *Let N be large and $1/2 < \sigma < 1$ be fixed. There exist a constant $\beta_q(\sigma) > 0$ and an irreducible polynomial P of degree N , such that*

$$\log(L(\sigma, \chi_P)) \leq -\beta_q(\sigma) \frac{(\log_q |P|)^{1-\sigma}}{(\log_q \log_q |P|)^\sigma}.$$

With this, we can prove the following.

Theorem 2.5.4. *Let $B > 0$ and $1/2 < \sigma < 1$. Then (q, σ, B) does not satisfy the Northcott property.*

PROOF. Given $B > 0$ and $\sigma \in (\frac{1}{2}, 1)$ we can choose N such that

$$|\zeta_{K_P}(\sigma)| \leq \frac{1}{|(1 - q^{-\sigma})(1 - q^{1-\sigma})|} e^{-\beta_q(\sigma) \frac{(\log_q |P|)^{1-\sigma}}{(\log_q \log_q |P|)^\sigma}} \leq B.$$

Then, we can construct a sequence of irreducible polynomials P_k where P_0 is a polynomial of degree N and P_k is of degree $N + k$ such that for all the polynomials in the sequence

$$|\zeta_{K_{P_k}}(\sigma)| \leq B.$$

Thus, we see that $S_{q, \sigma, B}$ is infinite for any choice of $B > 0$. □

2.5.3. The Northcott property at $s = 1/2$

Now we consider the case of $s = 1/2$, more precisely, we look at $\zeta_K(1/2)$. For this case, we use the following result of Li.

Theorem 2.5.5. [32, Theorem 1.3, simplified version] *For any $\varepsilon > 0$ there exist nonzero constants B_ε and N_ε such that if $N > N_\varepsilon$,*

$$\#\{D \in \mathbb{F}_q[T] : D \text{ monic, square-free, } |D| < N, L(\frac{1}{2}, \chi_D) = 0\} \geq B_\varepsilon N^{1/5-\varepsilon}.$$

The above result immediately implies the following.

Theorem 2.5.6. *Let $B > 0$. Then $(q, 1/2, B)$ does not satisfy the Northcott property with $\zeta_K(1/2)$.*

PROOF. By Theorem 2.5.5, there are infinitely many K for which $|\zeta_K(1/2)| = 0$ and therefore we obtain infinitely many K such that $|\zeta_K(1/2)| < B$. □

Remark 2.5.7. The above result does not cover the case of $\zeta_K^*(1/2)$. To do this, we would have to consider the first nonzero coefficient of the Taylor series for $\zeta_K(s)$ around $s = 1/2$.

Remark 2.5.8. It would be interesting to see if Theorem 2.5.6 has a counterpart in the number field case. This is not clear, as there is no vanishing result analogous to Theorem 2.5.5 in the number field case. We speculate that understanding the result over number fields

is equivalent to understanding the standard Northcott property with $\zeta_K^*(1/2)$ as opposed to the current results involving the Northcott property with $\zeta_K(1/2)$.

Theorem 2.5.6 can be extended to a more general class of s . An algebraic integer α is called a **Weil integer** if $|\alpha| = \sqrt{q}$ under every complex embedding.

Theorem 2.5.9. *For any $B > 0$ and q^s a Weil integer, the triple (q, s, B) does not satisfy the Northcott property with $\zeta_K(1/2)$.*

PROOF. The statement follows from the fact that for any Weil integer q^s , there exist infinitely many function fields K such that $\zeta_K(s) = 0$.

By the theory of Honda–Tate, for every Weil integer q^s , there exists an abelian variety A/\mathbb{F}_q such that q^s is a Frobenius eigenvalue for A . By the work of Gabber [19, Corollary 2.5], for any abelian variety A/\mathbb{F}_q , there exists a smooth projective curve C/\mathbb{F}_q such that A is an isogeny factor of the Jacobian of C (see also [8] for an effective statement). Hence $\zeta_{K_C}(s) = 0$ where K_C is the function field of C . The theorem follows from the fact that $\zeta_L(s) = 0$ for any field L which is an extension of K with constant field \mathbb{F}_q . \square

2.5.4. The Northcott property in the right of the critical line

Here we consider the set $1/2 < \operatorname{Re}(s) < 1$. This case will be studied in the context of the Shifted Moments Conjecture, formulated over function fields by Andrade and Keating [4] and recently proven for products of up to three factors and $\operatorname{Re}(s) < 1$ by Bui, Florea, and Keating [10].

For simplicity of notation we will write $\zeta_q(s)$ instead of $\zeta_{\mathbb{F}_q[T]}(s)$. Here, as before, it is assumed that $q \equiv 1 \pmod{4}$ for simplicity.

We start by recalling a simplified version of one of the results of Bui, Florea, and Keating.

Theorem 2.5.10. [10, Theorem 1.2, simplified version of a particular case] *Let $\alpha_1, \alpha_2 \in \mathbb{C}$ such that $|\operatorname{Re}(\alpha_j)| < 1/2$. Denote $A = \{\alpha_1, \alpha_2\}$. For a set $\mathfrak{A} \subseteq A$, let $\mathfrak{A}^- = \{-\mathfrak{a} : \mathfrak{a} \in \mathfrak{A}\}$ and $q^{-2g\mathfrak{A}} = q^{-2g \sum_{\mathfrak{a} \in \mathfrak{A}} \mathfrak{a}}$. We have*

$$\frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} L\left(\frac{1}{2} + \alpha_1, \chi_D\right) L\left(\frac{1}{2} + \alpha_2, \chi_D\right) = \sum_{\mathfrak{A} \subseteq A} q^{-2g\mathfrak{A}} S_{(A \setminus \mathfrak{A}) \cup \mathfrak{A}^-} + E_2,$$

where if $C = \{\gamma_1, \gamma_2\}$,

$$S_C = \mathcal{A}_C(1) \prod_{1 \leq i \leq j \leq 2} \zeta_q(1 + \gamma_i + \gamma_j),$$

$$\mathcal{A}_C(u) = \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \prod_{1 \leq i \leq j \leq 2} \left(1 - \frac{u^{2 \deg(P)}}{|P|^{1+\gamma_i+\gamma_j}} \right) \left(1 + \left(1 + \frac{1}{|P|} \right)^{-1} \sum_{\ell=1}^{\infty} \frac{\tau_C(P^{2\ell})}{|P|^\ell} u^{2\ell \deg(P)} \right),$$

$$\tau_C(f) = \sum_{\substack{f=f_1 f_2 \\ f_i \text{ monic}}} \frac{1}{|f_1|^{\gamma_1} |f_2|^{\gamma_2}} \quad (2.5.3)$$

and, for $\varepsilon > 0$,

$$E_2 \ll_\varepsilon q^{-(1+2 \min\{|\operatorname{Re}(\alpha_1)|, |\operatorname{Re}(\alpha_2)|\})g+\varepsilon g}.$$

Remark that the various sets of the form $(A \setminus \mathfrak{A}) \cup \mathfrak{A}^-$ should be taken as multi-sets in the case where a parameter is repeated. Therefore, in our case, they always have cardinality 2.

We stress that the result of Bui, Florea, and Keating is much more general than Theorem 2.5.10, as it considers a product of k factors of the form $L(\frac{1}{2} + \alpha, \chi_D)$ and it includes a twist by $\chi_D(h)$, where h is a polynomial of degree $\ll g$. We have written a simplified version that is sufficient for our purposes. The error term that we give in Theorem 2.5.10 is more detailed than the term in the original statement in [10] and has been taken from the proof.

Theorem 2.5.11. *Assume $q \equiv 1 \pmod{4}$. Let $0 < \operatorname{Re}(\alpha) < \frac{1}{2}$ be fixed and*

$$B > \left| \frac{1}{\left(1 - q^{-\frac{1}{2}-\alpha}\right) \left(1 - q^{\frac{1}{2}-\alpha}\right)} \right|$$

$$\times \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left[\frac{1}{2} \left(\left(1 - \frac{1}{|P|^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 - \frac{1}{|P|^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} + \left(1 + \frac{1}{|P|^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 + \frac{1}{|P|^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} \right) + \frac{1}{|P|} \right]^{1/2}$$

$$\times \left(1 + \frac{1}{|P|}\right)^{-1/2}.$$

Then $(q, 1/2 + \alpha, B)$ does not satisfy the Northcott property.

PROOF. In Theorem 2.5.10 we fix $\alpha = \alpha_1, \alpha_2 = \bar{\alpha}$. Since $\operatorname{Re}(\alpha) > 0$ is fixed, we have that $\operatorname{Re}(\alpha)g \rightarrow \infty$ as $g \rightarrow \infty$, and therefore the dominant term occurs when \mathfrak{A} is the empty set. We have

$$\frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} |L(\frac{1}{2} + \alpha, \chi_D)|^2 = \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left(1 + \left(1 + \frac{1}{|P|} \right)^{-1} \sum_{\ell=1}^{\infty} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(P^{2\ell})}{|P|^\ell} \right) (1 + o(1)). \quad (2.5.4)$$

We can give a more precise expression for the Euler product above. Notice that

$$\begin{aligned}
& \frac{1}{2} \left(\left(1 - \frac{1}{|P|^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 - \frac{1}{|P|^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} + \left(1 + \frac{1}{|P|^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 + \frac{1}{|P|^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} \right) \\
&= \frac{1}{2} \left(\sum_{j_1=0}^{\infty} \frac{1}{|P|^{j_1(\frac{1}{2}+\alpha)}} \sum_{j_2=0}^{\infty} \frac{1}{|P|^{j_2(\frac{1}{2}+\bar{\alpha})}} + \sum_{j_1=0}^{\infty} \frac{(-1)^{j_1}}{|P|^{j_1(\frac{1}{2}+\alpha)}} \sum_{j_2=0}^{\infty} \frac{(-1)^{j_2}}{|P|^{j_2(\frac{1}{2}+\bar{\alpha})}} \right) \\
&= 1 + \frac{1}{2} \left(\sum_{\ell=1}^{\infty} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(P^\ell)}{|P|^{\frac{\ell}{2}}} + \sum_{\ell=1}^{\infty} \frac{(-1)^\ell \tau_{\{\alpha, \bar{\alpha}\}}(P^\ell)}{|P|^{\frac{\ell}{2}}} \right).
\end{aligned}$$

This allows us to write

$$\frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} |L(\frac{1}{2} + \alpha, \chi_D)|^2 = C_\alpha(1 + o(1)),$$

where

$$\begin{aligned}
C_\alpha &= \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left[\frac{1}{2} \left(\left(1 - \frac{1}{|P|^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 - \frac{1}{|P|^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} + \left(1 + \frac{1}{|P|^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 + \frac{1}{|P|^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} \right) + \frac{1}{|P|} \right] \\
&\quad \times \left(1 + \frac{1}{|P|}\right)^{-1}.
\end{aligned}$$

In other words, the average value of $|L(\frac{1}{2} + \alpha, \chi_D)|^2$ is given by $C_\alpha(1 + o(1))$.

Finally, given $\varepsilon > 0$, we can guarantee that for g large enough, there is a $D \in \mathcal{H}_{2g+1}$ such that

$$|L(\frac{1}{2} + \alpha, \chi_D)| \leq C_\alpha^{1/2} + \varepsilon.$$

Taking ε arbitrarily small we can construct an infinite sequence of D 's satisfying this property, and leading to bounded $|\zeta_K(\frac{1}{2} + \alpha)|$. This implies that $S_{q, 1/2+\alpha, B}$ is infinite. \square

2.5.5. The Northcott property at $\text{Re}(s) = 1$.

In this section we examine the behaviour at the boundary of the critical strip, namely $\text{Re}(s) = 1$. We need a result along the lines of Theorem 2.5.10. Since we have not found this in the literature, we start by computing the average of $|L(\frac{1}{2} + \alpha, \chi_D)|^2$ where $\text{Re}(\alpha) \geq \frac{1}{2}$. When $\text{Re}(\alpha) > \frac{1}{2}$ this also gives an alternative better bound for Theorem 2.4.7.

In this section we will use \mathcal{M} to denote the monic polynomials in $\mathbb{F}_q[T]$, \mathcal{M}_n to denote the monic polynomials of degree n , and $\mathcal{M}_{\leq n}$ to denote those of degree up to n .

Our main result here is the following.

Theorem 2.5.12. *Let $\operatorname{Re}(\alpha) \geq \frac{1}{2}$. Then for $\varepsilon > 0$,*

$$\frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} |L(\frac{1}{2} + \alpha, \chi_D)|^2 = \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left(1 + \left(1 + \frac{1}{|P|} \right)^{-1} \sum_{\ell=1}^{\infty} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(P^{2\ell})}{|P|^\ell} \right) + O(q^{(\varepsilon - \operatorname{Re}(\alpha))g} + \min\{q^{(\varepsilon-1)g}, q^{-g} + 4^g q^{(\varepsilon-2\operatorname{Re}(\alpha))g}\}),$$

where for a set C , τ_C is defined by (2.5.3).

We remark that the main term in the above formula is the same as in equation (2.5.4), with a difference in the conditions, namely that we now have $\operatorname{Re}(\alpha) \geq \frac{1}{2}$. In the above result we *do not assume* that $q \equiv 1 \pmod{4}$.

Before proceeding to the proof of Theorem 2.5.12, we consider some auxiliary results.

Lemma 2.5.13. [10, Lemma 2.1, particular case] *We have*

$$|L(\frac{1}{2} + \alpha, \chi_D)|^2 = \sum_{f \in \mathcal{M}_{\leq 2g}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} + q^{-4g \operatorname{Re}(\alpha)} \sum_{f \in \mathcal{M}_{\leq 2g-1}} \frac{\tau_{\{-\alpha, -\bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}},$$

where for a set C , τ_C is defined by (2.5.3).

PROOF. This follows from [10, Lemma 2.1] by setting $k = 2$ and $\alpha_1 = \alpha$, $\alpha_2 = \bar{\alpha}$. □

Lemma 2.5.14. [17, Lemma 2.1] *Let χ_f be a non-trivial Dirichlet character modulo f . Then for $n < \deg(f)$,*

$$\left| \sum_{B \in \mathcal{M}_n} \chi_f(B) \right| \leq \binom{\deg(f) - 1}{n} q^{\frac{n}{2}}.$$

Lemma 2.5.15. [9, Lemma 3.7] *For $f \in \mathcal{M}$ we have*

$$\frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \chi_D(f^2) = \prod_{\substack{P \text{ monic} \\ \text{irreducible} \\ P|f}} \left(1 + \frac{1}{|P|} \right)^{-1} + O(q^{-2g}).$$

Lemma 2.5.16. *For any $\varepsilon > 0$,*

$$|\tau_{\{\alpha, \bar{\alpha}\}}(f)| \ll |f|^{\varepsilon - \operatorname{Re}(\alpha)} \tag{2.5.5}$$

and similarly

$$|\tau_{\{-\alpha, -\bar{\alpha}\}}(f)| \ll |f|^{\varepsilon + \operatorname{Re}(\alpha)}. \tag{2.5.6}$$

PROOF. We have that

$$|\tau_{\{\alpha, \bar{\alpha}\}}(f)| = \left| \sum_{\substack{f=f_1 f_2 \\ f_i \text{ monic}}} \frac{1}{|f_1|^\alpha |f_2|^{\bar{\alpha}}} \right| \leq \frac{d_2(f)}{|f|^{\operatorname{Re}(\alpha)}},$$

where d_2 is the divisor function. We can use that $d_2(f) = o(|f|^\varepsilon)$. The bound for $\tau_{\{-\alpha, -\bar{\alpha}\}}(f)$ is proven similarly. \square

We are now ready to proceed with the proof of the main result of this section.

PROOF OF THEOREM 2.5.12. By Lemma 2.5.13, we can split the sum under consideration in two Dirichlet sums of approximate length $2g$ as follows

$$\begin{aligned} \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} |L(\tfrac{1}{2} + \alpha, \chi_D)|^2 &= \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \sum_{f \in \mathcal{M}_{\leq 2g}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} \\ &\quad + \frac{q^{-4\operatorname{Re}(\alpha)g}}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \sum_{f \in \mathcal{M}_{\leq 2g-1}} \frac{\tau_{\{-\alpha, -\bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} \\ &= S_{2g, \alpha} + S_{2g-1, -\alpha}. \end{aligned}$$

We can further split each of the above sums into a sum where the character is evaluated in squares and a sum where it is not as follows

$$\begin{aligned} S_{2g, \alpha} &= \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g} \\ f = \square}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} + \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g} \\ f \neq \square}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} \\ &= S_{2g, \alpha}(\square) + S_{2g, \alpha}(\neq \square), \\ S_{2g-1, -\alpha} &= \frac{q^{-4\operatorname{Re}(\alpha)g}}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g-1} \\ f = \square}} \frac{\tau_{\{-\alpha, -\bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} + \frac{q^{-4\operatorname{Re}(\alpha)g}}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g-1} \\ f \neq \square}} \frac{\tau_{\{-\alpha, -\bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} \\ &= S_{2g-1, -\alpha}(\square) + S_{2g-1, -\alpha}(\neq \square). \end{aligned}$$

The main term comes from $S_{2g, \alpha}(\square)$, while the other three terms are smaller. We do not need to estimate them for our purposes, so we will bound them to get an error term.

We start by focusing on the main term, coming from $S_{2g,\alpha}(\square)$. We apply Lemma 2.5.15 and obtain

$$\begin{aligned} \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g} \\ f = \square}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} &= \sum_{h \in \mathcal{M}_{\leq g}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(h^2)}{|h|} \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \chi_D(h^2) \\ &= \sum_{h \in \mathcal{M}_{\leq g}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(h^2)}{|h|} \left(\prod_{P|h} \left(1 + \frac{1}{|P|} \right)^{-1} + O(q^{-2g}) \right). \end{aligned}$$

We remark that there are q^n monic polynomials of degree n . Applying inequality (2.5.5), we obtain

$$\sum_{h \in \mathcal{M}_{\leq g}} \frac{|\tau_{\{\alpha, \bar{\alpha}\}}(h^2)|}{|h|} O(q^{-2g}) \leq \sum_{n=1}^g q^{2n(\varepsilon - \operatorname{Re}(\alpha))} O(q^{-2g}) \ll O(q^{-2g}).$$

Now we consider the generating function

$$\mathcal{A}(u) = \sum_{h \in \mathcal{M}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(h^2)}{|h|} \prod_{P|h} \left(1 + \frac{1}{|P|} \right)^{-1} u^{\deg(h)} = \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left(1 + \left(1 + \frac{1}{|P|} \right)^{-1} \sum_{\ell=1}^{\infty} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(P^{2\ell})}{|P|^\ell} u^{2\ell \deg(P)} \right).$$

Since $|\tau_{\{\alpha, \bar{\alpha}\}}(P^{2\ell})| \leq \frac{2\ell+1}{|P|^{2\ell \operatorname{Re}(\alpha)}}$, it can be seen that $\mathcal{A}(u)$ converges for $|u| < q^{\operatorname{Re}(\alpha)}$.

By Perron's formula, for $r < 1$,

$$\sum_{h \in \mathcal{M}_{\leq g}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(h^2)}{|h|} \prod_{P|h} \left(1 + \frac{1}{|P|} \right)^{-1} = \frac{1}{2\pi i} \oint_{|u|=r} \frac{\mathcal{A}(u)}{u^g(1-u)} du.$$

We move the integral to the circle $|u| = q^{\operatorname{Re}(\alpha) - \varepsilon}$ encountering the pole at $u = 1$. This gives

$$\sum_{h \in \mathcal{M}_{\leq g}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(h^2)}{|h|} \prod_{P|h} \left(1 + \frac{1}{|P|} \right)^{-1} = -\operatorname{Res}_{u=1} \frac{\mathcal{A}(u)}{u^{g+1}(1-u)} + O(q^{(\varepsilon - \operatorname{Re}(\alpha))g}) = \mathcal{A}(1) + O(q^{(\varepsilon - \operatorname{Re}(\alpha))g}).$$

Putting all of the above together, we finally write

$$S_{2g,\alpha}(\square) = \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left(1 + \left(1 + \frac{1}{|P|} \right)^{-1} \sum_{\ell=1}^{\infty} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(P^{2\ell})}{|P|^\ell} \right) + O(q^{(\varepsilon - \operatorname{Re}(\alpha))g}). \quad (2.5.7)$$

Now we consider $S_{2g-1,-\alpha}(\square)$. Following similar steps as before and applying (2.5.6),

$$\begin{aligned} \left| \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g-1} \\ f = \square}} \frac{\tau_{\{-\alpha, -\bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} \right| &= \left| \sum_{h \in \mathcal{M}_{\leq g-1}} \frac{\tau_{\{-\alpha, -\bar{\alpha}\}}(h^2)}{|h|} \prod_{P|h} \left(1 + \frac{1}{|P|} \right)^{-1} \right| + O(q^{-2g}) \\ &\ll \sum_{h \in \mathcal{M}_{\leq g-1}} |h|^{2\operatorname{Re}(\alpha) - 1 + \varepsilon} + O(q^{-2g}) \\ &\ll q^{(2\operatorname{Re}(\alpha) + \varepsilon)g}. \end{aligned}$$

Combining with the term $q^{-4\operatorname{Re}(\alpha)g}$, this gives

$$S_{2g-1,-\alpha}(\square) \ll q^{(\varepsilon-2\operatorname{Re}(\alpha))g}. \quad (2.5.8)$$

Our next step is to bound $S_{2g,\alpha}(\neq \square)$. We follow the proof of [5, Lemma 3.2].

$$\begin{aligned} \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g} \\ f \neq \square}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} &= \sum_{n=0}^{2g} q^{-\frac{n}{2}} \sum_{\substack{f \in \mathcal{M}_n \\ f \neq \square}} \tau_{\{\alpha, \bar{\alpha}\}}(f) \sum_{D \in \mathcal{H}_{2g+1}} \chi_D(f) \\ &= \sum_{n=0}^{2g} q^{-\frac{n}{2}} \sum_{\substack{f \in \mathcal{M}_n \\ f \neq \square}} \tau_{\{\alpha, \bar{\alpha}\}}(f) \sum_{D \in \mathcal{M}_{2g+1}} \sum_{\substack{A \in \mathcal{M} \\ A^2 | D}} \mu(A) \chi_D(f) \\ &= \sum_{n=0}^{2g} q^{-\frac{n}{2}} \sum_{\substack{f \in \mathcal{M}_n \\ f \neq \square}} \tau_{\{\alpha, \bar{\alpha}\}}(f) (-1)^{\frac{(q-1)\deg(f)}{2}} \sum_{\substack{A \in \mathcal{M}_{\leq g} \\ (A, f)=1}} \mu(A) \sum_{B \in \mathcal{M}_{2g+1-2\deg(A)}} \chi_f(B), \end{aligned} \quad (2.5.9)$$

where in the last line we have applied quadratic reciprocity and the fact that $\deg(B)$ is odd.

We can apply Lemma 2.5.14 in the innermost sum when $2g+1-2\deg(A) < \deg(f)$. Note that the sum is zero otherwise, since it is a full character sum. Also applying (2.5.5), we obtain

$$\begin{aligned} \left| \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g} \\ f \neq \square}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} \right| &\leq \sum_{n=0}^{2g} q^{-\frac{n}{2}} \sum_{\substack{f \in \mathcal{M}_n \\ f \neq \square}} |\tau_{\{\alpha, \bar{\alpha}\}}(f)| \sum_{A \in \mathcal{M}_{\leq g}} \binom{\deg(f)-1}{2g+1-2\deg(A)} q^{\frac{2g+1-2\deg(A)}{2}} \\ &\ll q^g \sum_{n=0}^{2g} q^{-\frac{n}{2}} \sum_{f \in \mathcal{M}_n} |f|^{\varepsilon - \operatorname{Re}(\alpha)} 2^{\deg(f)-1} \\ &\ll q^g \sum_{n=0}^{2g} 2^n q^{(\frac{1}{2} - \operatorname{Re}(\alpha) + \varepsilon)n} \\ &\ll q^g + 2^{2g} q^{(2-2\operatorname{Re}(\alpha) + \varepsilon)g}. \end{aligned}$$

Combining with equation (2.5.2), we get

$$S_{2g,\alpha}(\neq \square) \ll q^{-g} + 2^{2g} q^{(\varepsilon-2\operatorname{Re}(\alpha))g}. \quad (2.5.10)$$

When $q < 5$ and $\operatorname{Re}(\alpha)$ is close to $\frac{1}{2}$, the bound above is sub-optimal, since it becomes $\gg q^{cg}$ for some positive c . To solve this, we bound the innermost sum in (2.5.9) using the

Riemann Hypothesis instead, to obtain

$$\begin{aligned}
\left| \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g} \\ f \neq \square}} \frac{\tau_{\{\alpha, \bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} \right| &\ll \sum_{n=0}^{2g} q^{-\frac{n}{2}} \sum_{\substack{f \in \mathcal{M}_n \\ f \neq \square}} |\tau_{\{\alpha, \bar{\alpha}\}}(f)| \sum_{A \in \mathcal{M}_{\leq g}} q^{(1+\varepsilon) \frac{2g+1-2 \deg(A)}{2}} \\
&\ll q^{(1+\varepsilon)g} \sum_{n=0}^{2g} q^{-\frac{n}{2}} \sum_{f \in \mathcal{M}_n} |f|^{\varepsilon - \operatorname{Re}(\alpha)} \\
&\ll q^{(1+\varepsilon)g} \sum_{n=0}^{2g} q^{(\frac{1}{2} - \operatorname{Re}(\alpha) + \varepsilon)n} \\
&\ll q^{(1+\varepsilon)g}.
\end{aligned}$$

This gives

$$S_{2g, \alpha}(\neq \square) \ll q^{(\varepsilon-1)g}. \quad (2.5.11)$$

Finally we consider $S_{2g-1, -\alpha}(\neq \square)$. The computation is similar as before and applying the Riemann Hypothesis gives

$$\begin{aligned}
\left| \sum_{D \in \mathcal{H}_{2g+1}} \sum_{\substack{f \in \mathcal{M}_{\leq 2g-1} \\ f \neq \square}} \frac{\tau_{\{-\alpha, -\bar{\alpha}\}}(f) \chi_D(f)}{|f|^{\frac{1}{2}}} \right| &\ll q^{(1+\varepsilon)g} \sum_{n=0}^{2g-1} q^{-\frac{n}{2}} \sum_{f \in \mathcal{M}_n} |\tau_{\{-\alpha, -\bar{\alpha}\}}(f)| \\
&\ll q^{(1+\varepsilon)g} \sum_{n=0}^{2g-1} q^{-\frac{n}{2}} \sum_{f \in \mathcal{M}_n} |f|^{\varepsilon + \operatorname{Re}(\alpha)} \\
&\ll q^{(2+2 \operatorname{Re}(\alpha) + \varepsilon)g},
\end{aligned}$$

where we have used equation (2.5.6). Again, combining with the extra factor $\frac{q^{-4 \operatorname{Re}(\alpha)g}}{\#\mathcal{H}_{2g+1}}$, this leads to

$$S_{2g-1, -\alpha}(\neq \square) \ll q^{(\varepsilon-2 \operatorname{Re}(\alpha))g}. \quad (2.5.12)$$

The result follows by combining equations (2.5.7), (2.5.8), (2.5.10), (2.5.11), and (2.5.12) \square

With Theorem 2.5.12 proven, we can now proceed to study the corresponding Northcott property.

Theorem 2.5.17. *Let $\operatorname{Re}(\alpha) \geq \frac{1}{2}$ with $\alpha \neq \frac{1}{2}$ and*

$$B > \left| \frac{1}{(1 - q^{-\frac{1}{2}-\alpha})(1 - q^{\frac{1}{2}-\alpha})} \right| \\
\times \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left[\frac{1}{2} \left(\left(1 - \frac{1}{|P|^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 - \frac{1}{|P|^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} + \left(1 + \frac{1}{|P|^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 + \frac{1}{|P|^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} \right) + \frac{1}{|P|} \right]^{1/2} \\
\times \left(1 + \frac{1}{|P|}\right)^{-1/2}.$$

Then $(q, 1/2 + \alpha, B)$ does not satisfy the Northcott property.

We remark that, as in the case of Theorem 2.5.12, we do not assume that $q \equiv 1 \pmod{4}$.

PROOF. The proof follows the same lines as the proof of Theorem 2.5.11. \square

Remark 2.5.18. As a final remark, for $\operatorname{Re}(\alpha) > \frac{1}{2}$, Theorem 2.5.17 provides a better result than Theorem 2.4.7. In the case of Theorem 2.4.7, the bound is chosen to control all the quadratic $\zeta_K(s)$, while in the case of Theorem 2.5.17 the bound is chosen according to the average, and is, therefore, less restricted.

Chapitre 3

On the Northcott property of Dedekind zeta functions

par

Xavier G n reux, Matilde Lal n¹

- (¹) Xavier G n reux: D partement de math matiques et de statistique, Universit  de Montr al. CP 6128, succ. Centre-ville. Montreal, QC H3C 3J7, Canada
- (²) Matilde Lal n: D partement de math matiques et de statistique, Universit  de Montr al. CP 6128, succ. Centre-ville. Montreal, QC H3C 3J7, Canada

Cet article a  t  soumis dans The Ramanujan Journal. Il est disponible   l'adresse <https://arxiv.org/abs/2209.13854>.

Chacun des auteurs a contribu    part  gale   la publication.

ABSTRACT. The Northcott property for special values of Dedekind zeta functions and more general motivic L -functions was defined by Pazuki and Pengo. We investigate this property for any complex evaluation of Dedekind zeta functions. The results are more delicate and subtle than what was proven for the function field case in previous work of Li and the authors, since they include some surprising behavior in the neighborhood of the trivial zeros. The techniques include a mixture of analytic and computer assisted arguments.

Keywords: Dedekind zeta function; Northcott property

3.1. Introduction

Recently Pazuki and Pengo [47] considered a variant of the Northcott property for special values of L -functions attached to mixed motives. Usually the Northcott property [42] refers to the fact that a set of algebraic numbers with bounded height and bounded degree must be finite. In the number field case, the problem studied by Pazuki and Pengo concerns special values of the Dedekind zeta function. For a field K and $s \in \mathbb{C}$ denote by

$$\zeta_K^*(s) := \lim_{t \rightarrow s} \frac{\zeta_K(t)}{(t-s)^{\text{ord}_{t=s}(\zeta_K(t))}},$$

the first nonzero coefficient of the Taylor series for ζ_K around s .

For a fixed $s = n \in \mathbb{Z}$ and a fixed positive real number B , Pazuki and Pengo study the set of isomorphism classes of number fields K given by

$$S_{B,n} = \{[K] : |\zeta_K^*(n)| \leq B\},$$

and discuss the finiteness of this set under various conditions of B and n . For number fields, they prove that the Northcott property holds for n a negative integer or $n = 0$, and it does not hold if n is a positive integer. They also estimate the size of this set for the integers n such that the Northcott property holds.

In [20] Li and the authors of this note consider the analogous problem for isomorphism classes of function fields K with constant field \mathbb{F}_q . However, instead of restricting to special values with $s = n \in \mathbb{Z}$, they work directly with $\zeta_K^*(s)$ with s a fixed arbitrary complex number. They are able to establish or partially establish the question of the Northcott property *outside* the set $\frac{1}{2} - \frac{\log 2}{\log q} \leq \text{Re}(s) < \frac{1}{2}$. More precisely, the Northcott property holds when $\text{Re}(s) < \frac{1}{2} - \frac{\log 2}{\log q}$ and the set $S_{B,s}$ is infinite for B larger than a certain constant depending on s in $\text{Re}(s) \geq \frac{1}{2}$. This is illustrated by Figure 3.1. Moreover, remark that the gap corresponding to $\frac{1}{2} - \frac{\log 2}{\log q} \leq \text{Re}(s) < \frac{1}{2}$ shrinks to the empty set as q tends to infinity. These results are consistent with what Pazuki and Pengo obtained for the cases $s = n \in \mathbb{Z}$.

The goal of this article is to return to the case considered by Pazuki and Pengo in [47] and to explore the special values $\zeta_K^*(s)$ associated to Dedekind zeta functions at any complex number. The motivation for considering such questions comes naturally from a desire to better understand the results in [20]. Figure 3.2 gives an approximate (not to scale) illustration of the results obtained in this article over number fields.

We will say that s satisfies the Northcott property for B a real positive number if $S_{B,s}$ is finite.

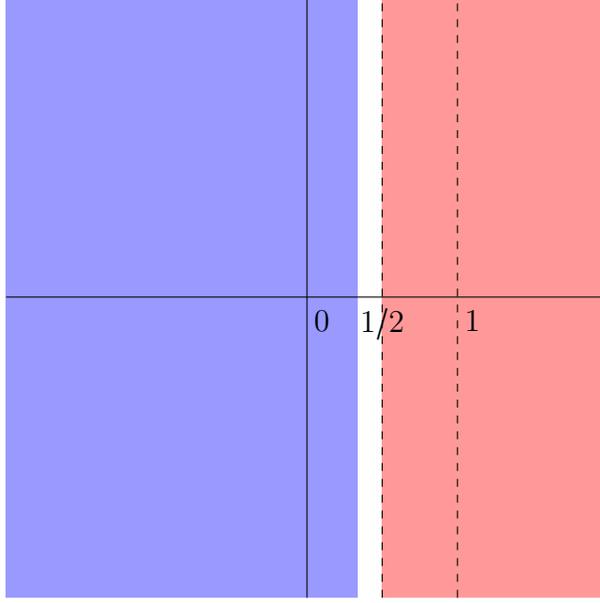


Fig. 3.1. For the base field \mathbb{F}_q , with q a fixed prime power, the Northcott property holds in the blue area. In the red area, $S_{B,s}$ is infinite for B greater than a certain constant (which is zero in the case of the real segment $[1/2,1]$). The white gap disappears when $q \rightarrow \infty$.

Occasionally, we will work with $\zeta_K(s)$ instead of $\zeta_K^*(s)$. We will say that s satisfies the Northcott property for values of ζ_K if the set

$$\{[K] : |\zeta_K(s)| \leq B\}$$

is finite. When $\zeta_K(s) \neq 0$, we have that $\zeta_K(s) = \zeta_K^*(s)$. The above definition is only different from the standard Northcott property when working with values of s where $\zeta_K(s)$ may have zeros or poles.

We prove the following statements.

Theorem 3.1.1. *The Northcott property is satisfied for $s = \sigma + i\tau$ with $\sigma, \tau \in \mathbb{R}$ and any $B > 0$ under the following conditions:*

- When $s = \sigma + i\tau$ with

$$\sigma < -1.5 \quad \text{and} \quad |\tau| > \tau_0 := \frac{2}{\pi} \tanh^{-1} \left(\frac{\zeta\left(\frac{5}{2}\right)}{3\sqrt{2}e^{2\gamma}} \right) = 0.063666\dots,$$

where

$$\gamma = \lim_{n \rightarrow \infty} \left(-\log n + \sum_{k=1}^n \frac{1}{k} \right) \tag{3.1.1}$$

is the Euler–Mascheroni constant given by $\gamma = 0.577215\dots$

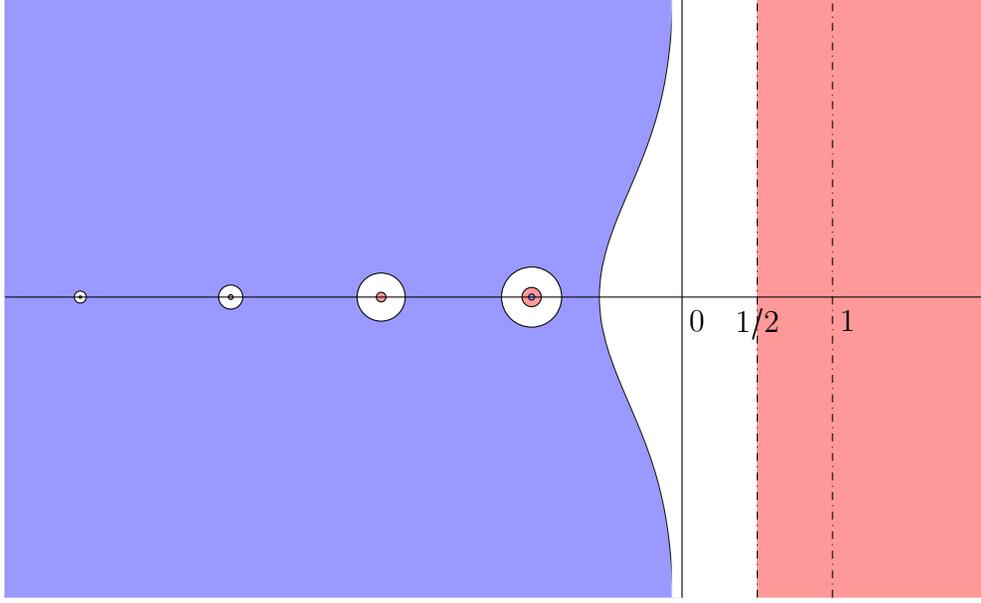


Fig. 3.2. Approximate (not to scale) illustration summarizing what is proven in the whole article regarding the Northcott property for Dedekind zeta functions. The Northcott property holds in the blue area. In the red area, $S_{B,s}$ is infinite for B greater than a certain constant. Unlike the function field case, we do not have information regarding the situation when $\text{Re}(s) = 1$ and $s \neq 1$ as well as when $\text{Re}(s) = \frac{1}{2}$.

- When $s = \sigma + i\tau = -2n + re^{i\theta}$ with $n \in \mathbb{Z}_{>0}$ and satisfying the following conditions

$$-2n - \frac{1}{2} \leq \sigma \leq -2n + \frac{1}{2}, \quad \text{and} \quad |\tau| \leq \tau_0,$$

as well as

$$r > \max \left\{ \frac{\sin^{-1}(C_{\mathbb{C}}(n))}{\pi}, \frac{2 \sin^{-1}(C_{\mathbb{R}}(n))}{\pi} \right\}$$

where

$$C_{\mathbb{C}}(n) = \pi \left(\frac{e^{-2\gamma}}{2} \right)^{4n} \frac{\zeta\left(2n + \frac{1}{2}\right)^2}{\Gamma\left(2n + \frac{1}{2}\right)^2} \frac{18e^{4\gamma} + \zeta\left(\frac{5}{2}\right)^2}{18e^{4\gamma} - \zeta\left(\frac{5}{2}\right)^2},$$

and

$$C_{\mathbb{R}}(n) = \sqrt{\pi} \left(\frac{e^{-2\gamma}}{2} \right)^{2n} \frac{\zeta\left(2n + \frac{1}{2}\right)}{\Gamma\left(2n + \frac{1}{2}\right)} \frac{3e^{2\gamma}}{\left(18e^{4\gamma} - \zeta\left(\frac{5}{2}\right)^2\right)^{\frac{1}{2}}}.$$

- When $s = \sigma + i\tau = -2n + 1 + re^{i\theta}$ with $n \in \mathbb{Z}_{>1}$ and satisfying the following conditions

$$-2n + \frac{1}{2} \leq \sigma \leq -2n + \frac{3}{2}, \quad \sigma < \sigma_0, \quad \text{and} \quad |\tau| \leq \tau_0,$$

as well as

$$r > \frac{1}{\pi} \sin^{-1} \left(\pi \left(\frac{e^{-\gamma}}{2} \right)^{4n-2} \frac{\zeta \left(2n - \frac{1}{2} \right)^2 18e^{4\gamma} + \zeta \left(\frac{5}{2} \right)^2}{\Gamma \left(2n - \frac{1}{2} \right)^2 18e^{4\gamma} - \zeta \left(\frac{5}{2} \right)^2} \right).$$

- When $s = \sigma + i\tau$ with $\sigma < 0$ and

$$|\tau| > \frac{(2e^\gamma)^{2\sigma-1} \zeta(1-\sigma)^2}{\tanh\left(\frac{\pi}{2} (2e^\gamma)^{2\sigma-1} \frac{\zeta(1-\sigma)^2}{\Gamma(1-\sigma)^2}\right) \Gamma(1-\sigma)^2}.$$

The idea behind Theorem 3.1.1 is to use the functional equation of the Dedekind zeta function in order to compare the value of $\zeta_K(s)$ with that of $\zeta_K(1-s)$, where $\text{Re}(1-s) = 1-\sigma > 0$, which is easier to understand and control. However, this strategy requires the control of the discriminant Δ_K and the Γ -factors. To control the discriminant we use a result of Odlyzko [45] that gives a lower bound for the inferior limit of the root discriminant $|\Delta_K|^{\frac{1}{[K:\mathbb{Q}]}}$ as the degree $[K:\mathbb{Q}]$ goes to infinity. With these bounds in hand, it remains to control the Γ -factors, which is done in stages, first when the imaginary part τ is sufficiently away from zero, and then in discs centered at negative integers, and chosen in such a way that they cover all the strip around the real negative axis, except for some smaller concentric discs. There are several strategies to bound τ and to choose the discs. For Theorem 3.1.1, the choice of σ_0 determines the choice of τ_0 , but the choice of $\sigma_0 = -1.5$ is arbitrary. It is related with the fact that this method yields very sub-optimal results if we try to reach -1 , in the sense that the τ_0 must be very large. Given that we do our analysis over intervals of length 1 centered at negative integers, the choice of $\sigma_0 = -1.5$ is then natural. Figure 3.3 illustrates the strategy and results of Theorem 3.1.1, except for the last item, which removes the condition $\sigma < \sigma_0$, but it gives a relatively bad bound for τ .

More precise results can be obtained by studying the region where the Northcott property holds with a computer-generated graph (see Figure 3.9) and by approximating its boundary with analytic methods. A strategy following this idea is described in Section A, and this allows us to numerically prove that if $s = \sigma + i\tau = -1 + re^{i\theta}$ is such that

$$-1.5 \leq \sigma \leq \sigma_1,$$

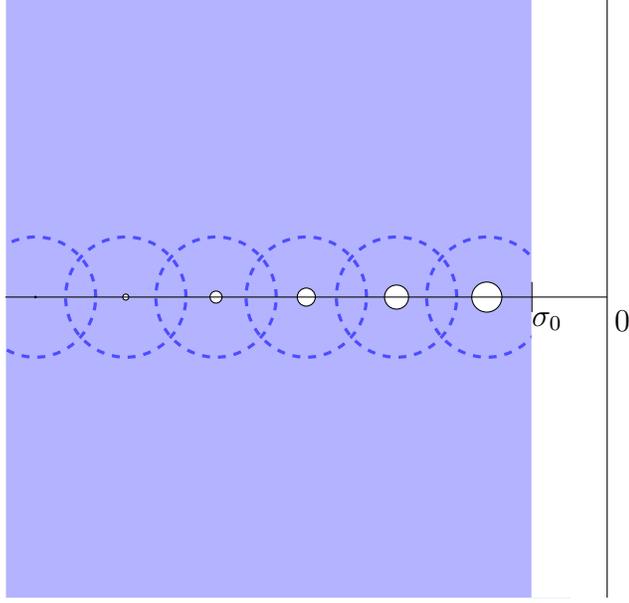


Fig. 3.3. Illustration of the Northcott property as verified by the first three items in Theorem 3.1.1.

where $\sigma_1 \approx -0.68$ is a solution to

$$\frac{(2e^\gamma)^{\frac{1}{2}-\sigma}}{\zeta(1-\sigma)} \left| \frac{\Gamma(1-\sigma)}{\Gamma(\sigma)} \right|^{\frac{1}{2}} = 1$$

and

$$r > 9.260\,260\,274\,818 \times 10^{-2},$$

then s satisfies the Northcott property for any $B > 0$, which complements the statement of Theorem 3.1.1. In fact, we can be more precise about this, and give information in the interval $-1.5 \leq \sigma \leq \varepsilon$ (see Remarks A.0.6 and A.0.7 and the discussions following them). Table A.1 exhibits a comparison of the numerical results and the results of Theorem 3.1.1.

In addition, we provide an estimate for the number of elements in $S_{B,s}$ in the cases considered in Theorem 3.1.1.

Theorem 3.1.2. *Let $s = \sigma + i\tau$ such that any of the conditions in Theorem 3.1.1 are satisfied. Then, there are constants b_s, f_s depending only on s such that*

$$\#S_{B,s} \leq \exp\left(b_s(\log B)(\log(f_s \log B))^3\right).$$

Theorem 3.1.2 is obtained by applying a result of Couveignes [14] giving a bound for the number of K of fixed degree over \mathbb{Q} and fixed discriminant. This strategy was already

employed both in [47] and in [20], and Theorem 3.1.2 has the same strength as the equivalent results obtained in these articles.

The simplest negative result to examine is the right side of the critical strip.

Theorem 3.1.3. *The Northcott property does not hold for $s = \sigma + i\tau$ with $\sigma, \tau \in \mathbb{R}$, $\sigma > 1$ and $B \geq \zeta(\sigma)^2$.*

This follows from the fact that, for quadratic fields, $\zeta_K(\sigma + i\tau) \leq \zeta(\sigma)^2$.

We also have negative results on the left side of the critical strip, in the neighborhood of negative integers, but not on the negative integers themselves (where the Northcott property holds as proven in [47]).

Theorem 3.1.4. *The Northcott property does not hold for $s = \sigma + i\tau = -n + re^{i\theta}$ with $n \in \mathbb{Z}_{>0}$, and satisfying that*

$$0 < r < \frac{1}{\pi} \sinh^{-1} \left(\frac{\pi}{\Gamma\left(n + \frac{3}{2}\right)^2 \zeta\left(n + \frac{1}{2}\right)^2} \left(\frac{2\pi}{D_M}\right)^{2n+2} \right),$$

where

$$D_M = 3^{\frac{1}{8}} \cdot 7^{\frac{1}{12}} \cdot 13^{\frac{1}{12}} \cdot 19^{\frac{1}{8}} \cdot 23^{\frac{1}{3}} \cdot 29^{\frac{1}{12}} \cdot 31^{\frac{1}{12}} \cdot 35509^{\frac{1}{8}} = 78.4269 \dots$$

Remark 3.1.5. We remark that the radii of the circles appearing in Theorems 3.1.1 and 3.1.4 are both tending to zero as $n \rightarrow \infty$.

Theorem 3.1.4 is obtained by applying a result of Hajir, Maire, and Ramakrishna [18], which is an improvement of results of Martinet [39] giving upper bounds for the inferior limit of the root discriminant $|\Delta_K|^{\frac{1}{[K:\mathbb{Q}]}}$ as the degree $[K:\mathbb{Q}]$ goes to infinity. We remark here that the set where we can prove that the Northcott property is not verified is a punctured disc around each negative integer.

There is a ring representing a gap of knowledge between Theorems 3.1.1 and 3.1.4 (see Figure 3.4). This lack of knowledge originates from the gap between the lower and upper bounds for the inferior limits of the root discriminants of number fields. Also rough bounds for the Γ -factors contribute to this gap, but these in principle could be improved.

Finally, inside the critical strip, we have the following result.

Theorem 3.1.6. *Assume the Generalized Riemann Hypothesis. Then the Northcott property does not hold for $s = \sigma + i\tau$ with $1/2 < \sigma < 1$.*

Moreover, unconditionally, there is a $B(s) > 0$ (given by (3.5.1)) such that s does not satisfy the Northcott property for the values of ζ_K for $B > B(s)$.

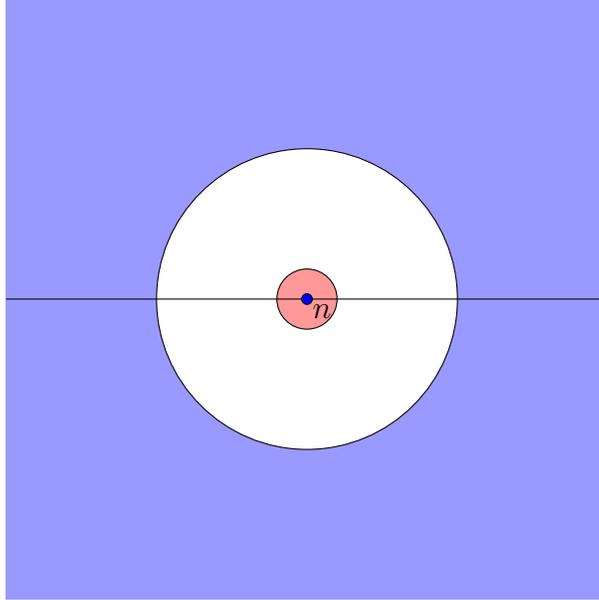


Fig. 3.4. Illustration of the knowledge gap between Theorems 3.1.1 and 3.1.4. As usual, the Northcott property is verified in the blue area (this includes the center of the circle), while the red area is known to be non-Northcott.

The first part of Theorem 3.1.6 is obtained by applying a result of Lamzouri [29] on the distribution of extreme values in families of quadratic Dirichlet L -functions that allows to construct arbitrarily many quadratic extensions with bounded Dirichlet L -function at s . A result of Sono [55] on the second moment of quadratic Dirichlet L -functions allows us to prove the second part.

The main difference between the results for number fields and the analogue results for function fields from [20] lies when $\text{Re}(s) < 0$. While the function field case has a relatively straightforward verification of the Northcott property for $\text{Re}(s) < \frac{1}{2} - \frac{\log 2}{\log q}$, this verification fails in a neighborhood of each negative integer in the number field case. This surprising difference comes from the Γ -factors in the functional equation. Another difference lies in the interior of critical strip. More precisely, in the strip where $1/2 < \text{Re}(s) < 1$, we have, conditionally on the Generalized Riemann Hypothesis, non-Northcott for any $B > 0$ in the number field case, as opposed to results that are partial (for B larger than certain value) for $\text{Im}(s) \neq 0$ in the function field case. This is due to the strength of the result in [29] and can likely be translated to the function field case as well, where the Riemann Hypothesis is known.

This article is organized as follows. Section 3.2 includes some necessary background on the Dedekind zeta function, the Γ function, and hyperbolic trigonometric functions. The right side of the critical strip is considered in Section 3.3, while Section 3.4 treats the left side. Section 3.5 considers the behavior inside the critical strip. Finally, we include an Appendix where the case $-1.5 < \sigma$ is discussed with numerical methods.

Acknowledgements

The authors are grateful to Chantal David, Alexandra Florea, Wanlin Li, and Riccardo Pengo for many helpful discussions. The authors would like to also thank the anonymous referee for the numerous suggestions and corrections which greatly improved the exposition of this article. This work was supported by the Natural Sciences and Engineering Research Council of Canada, Discovery Grant 355412-2022, and the Fonds de recherche du Québec - Nature et technologies, Projet de recherche en équipe 300951.

Disclosure statement

The authors report there are no competing interests to declare.

Data availability statement

The datasets generated and analysed during the current study are available in the GitHub repository:

<https://github.com/Louddy/-The-northcott-property-of-dedekind-zeta-functions>

3.2. Some background

In this section we recall some background regarding the Dedekind zeta function $\zeta_K(s)$, the Gamma function, and some inequalities involving trigonometric and hyperbolic functions. Let K be a number field, that is, a finite extension of \mathbb{Q} of degree $d_K = r_1 + 2r_2$, where r_1 denotes the number of real embeddings and r_2 , the number of pairs of complex embeddings. The Dedekind zeta function of K is given by

$$\zeta_K(s) := \sum_{\substack{I \subseteq \mathcal{O}_K \\ I \neq (0)}} \frac{1}{N_{K/\mathbb{Q}}(I)^s} = \prod_{P \subseteq \mathcal{O}_K} (1 - N_{K/\mathbb{Q}}(P)^{-s})^{-1}, \quad \text{Re}(s) > 1, \quad (3.2.1)$$

where the sum takes place over all the ideals in the integral domain \mathcal{O}_K and the Euler product goes over the prime ideals of \mathcal{O}_K .

Let Δ_K denote the discriminant of K/\mathbb{Q} . The Dedekind zeta function $\zeta_K(s)$ satisfies the following functional equation

$$\zeta_K(s) = \zeta_K(1-s) \frac{\Gamma_{\mathbb{R}}(1-s)^{r_1} \Gamma_{\mathbb{C}}(1-s)^{r_2}}{\Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2}} |\Delta_K|^{\frac{1}{2}-s},$$

where

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2), \quad \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s} \Gamma(s).$$

Here

$$\Gamma(s) := \int_0^{\infty} x^{s-1} e^{-x} dx, \quad \operatorname{Re}(s) > 1$$

is the gamma function, which has a meromorphic continuation to the whole complex plane, with simple poles at 0 and at the negative integers. When n is a positive integer, we have

$$\Gamma(n) = (n-1)!$$

The value at a complex number can be controlled by the value at a real argument. More precisely, writing $s = \sigma + i\tau$, we have,

$$|\Gamma(s)| \leq |\Gamma(\sigma)|, \quad (\text{see [2, Eq. 6.1.26]}); \quad (3.2.2)$$

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}, \quad s \notin \mathbb{Z}, \quad (\text{Euler's reflection formula [2, Eq. 6.1.17]}); \quad (3.2.3)$$

$$\Gamma(s)\Gamma\left(s + \frac{1}{2}\right) = 2^{1-2s} \sqrt{\pi} \Gamma(2s), \quad (\text{Lagrange's duplication formula [2, Eq. 6.1.18]}); \quad (3.2.4)$$

$$|\Gamma(s)| \geq \frac{\Gamma(\sigma)}{|\cosh(\pi\tau)|^{\frac{1}{2}}}, \quad \sigma \geq \frac{1}{2}, \quad (\text{see [1, Eq. 5.6.7]}); \quad (3.2.5)$$

$$\frac{1}{\Gamma(z)} = z e^{\gamma z} \prod_{k=1}^{\infty} \left(1 + \frac{z}{k}\right) e^{-z/k}, \quad (\text{Euler's infinite product [2, Eq. 6.1.3]}). \quad (3.2.6)$$

In the last formula, γ is the Euler–Mascheroni constant $\gamma = 0.577215\dots$ given by (3.1.1).

The digamma function is the logarithmic derivative of the gamma function:

$$\psi(s) = \frac{d}{ds} \log(\Gamma(s)). \quad (3.2.7)$$

It can be expressed with the following series ([2, Eq. 6.3.16])

$$\psi(s+1) = -\gamma + \sum_{k=1}^{\infty} \left(\frac{1}{k} - \frac{1}{k+s}\right), \quad (3.2.8)$$

for $s \neq -1, -2, \dots$

We will need some bounds relating trigonometric functions and hyperbolic functions. For example, we have

$$|\sin(s)| \geq |\sinh(\tau)|. \quad (3.2.9)$$

(See [2, Eq. 4.3.83].)

The following result will be used to bound $|\sin(z)|$ and $|\cos(z)|$ in terms of $|z|$.

Lemma 3.2.1. *For any $z \in \mathbb{C}$, we have*

$$|\sin(|z|)| \leq |\sin(z)|, \quad (3.2.10)$$

$$|\sin(z)| \leq \sinh(|z|). \quad (3.2.11)$$

Similarly we have

$$|\cos(|z|)| \leq |\cos(z)|, \quad (3.2.12)$$

$$|\cos(z)| \leq \cosh(|z|). \quad (3.2.13)$$

PROOF. Notice that the upper bound on $|\sin(z)|$ and $|\cos(z)|$ are well-known (see for example [2, Eq. 4.3.87, Eq. 4.3.86]).

Write for simplicity $z = re^{it}$, where $r \geq 0$ and $t \in [0, 2\pi)$. Consider

$$|\sin(z)|^2 = |\sin(re^{it})|^2 = \sin(r \cos(t))^2 \cosh(r \sin(t))^2 + \cos(r \cos(t))^2 \sinh(r \sin(t))^2 =: f(t).$$

The derivatives with respect to t give

$$\begin{aligned} f'(t) &= r \sinh(2r \sin(t)) \cos(t) - r \sin(2r \cos(t)) \sin(t), \\ f''(t) &= 2r^2 \cosh(2r \sin(t)) \cos(t)^2 + 2r^2 \cos(2r \cos(t)) \sin(t)^2 \\ &\quad - r \sinh(2r \sin(t)) \sin(t) - r \sin(2r \cos(t)) \cos(t). \end{aligned}$$

We can focus on $[0, 2\pi)$. Studying the derivatives, we find minima at 0 and π as well as maxima at $\frac{1}{2}\pi$ and $\frac{3}{2}\pi$. Thus, we obtain

$$\sin(r)^2 \leq f(t) \leq \sinh(r)^2.$$

By taking square roots everywhere in the above inequality we obtain the result.

Similarly, consider

$$|\cos(z)|^2 = |\cos(re^{it})|^2 = \cos(r \cos(t))^2 \cosh(r \sin(t))^2 + \sin(r \cos(t))^2 \sinh(r \sin(t))^2 =: g(t).$$

As before, we have

$$\begin{aligned} g'(t) &= r \sinh(2r \sin(t)) \cos(t) + r \sin(2r \cos(t)) \sin(t), \\ g''(t) &= 2r^2 \cosh(2r \sin(t)) \cos(t)^2 - 2r^2 \cos(2r \cos(t)) \sin(t)^2 \\ &\quad - r \sinh(2r \sin(t)) \sin(t) + r \sin(2r \cos(t)) \cos(t). \end{aligned}$$

We study the derivatives on $[0, 2\pi)$, and we find minima at 0 and π and maxima at $\frac{1}{2}\pi$ and $\frac{3}{2}\pi$. This gives

$$\cos(r)^2 \leq g(t) \leq \cosh(r)^2.$$

By taking square roots everywhere in the above inequality we obtain the result. \square

3.3. The right side of the critical strip

To begin, we consider the Northcott property on the right side of the critical strip, that is, $\mathbb{C}_{\sigma > 1}$, where we obtain a result conditionally on the value of B . The result will follow from a comparison between $\zeta_K(s)$ and $\zeta(\sigma)^{d_K}$, where d_K is the degree of the extension K/\mathbb{Q} .

Lemma 3.3.1. *Let $s = \sigma + i\tau$ with $\sigma > 1$. Then*

$$\frac{1}{\zeta(\sigma)^{d_K}} \leq |\zeta_K(s)| \leq \zeta(\sigma)^{d_K}.$$

Notice that this result bounds $|\zeta_K(s)|$ by small constants except near $\sigma = 1$. In addition, since d_K can be arbitrary, the above bounds are not absolute for s .

PROOF. We start by proving bounds in terms of $\zeta_K(\sigma)$. Since $\sigma > 1$, we have

$$|\zeta_K(\sigma + i\tau)| = \left| \sum_{n=1}^{\infty} \sum_{\substack{I \in \mathcal{O}_K \\ N_{K/\mathbb{Q}}(I)=n}} \frac{1}{n^{\sigma+i\tau}} \right| \leq \sum_{n=1}^{\infty} \sum_{\substack{I \in \mathcal{O}_K \\ N_{K/\mathbb{Q}}(I)=n}} \frac{1}{n^{\sigma}} = \zeta_K(\sigma), \quad (3.3.1)$$

and this yields an upper bound.

To get a lower bound, we take the logarithm of the Euler product (3.2.1) and use the fact that $1 + \cos(\theta) \geq 0$ for any θ to get

$$\begin{aligned} \log \zeta_K(\sigma) + \operatorname{Re} \log \zeta_K(\sigma + i\tau) &= \sum_P -\log(1 - N_{K/\mathbb{Q}}(P)^{-\sigma}) - \operatorname{Re} \log(1 - N_{K/\mathbb{Q}}(P)^{-\sigma-i\tau}) \\ &= \sum_P \sum_{j=1}^{\infty} \frac{1 + \operatorname{Re}(N_{K/\mathbb{Q}}(P)^{-i\tau j})}{j |N_{K/\mathbb{Q}}(P)^j|^{\sigma}} \\ &= \sum_P \sum_{j=1}^{\infty} \frac{1 + \cos(\tau \log |N_{K/\mathbb{Q}}(P)^j|)}{j |N_{K/\mathbb{Q}}(P)^j|^{\sigma}} \geq 0. \end{aligned} \quad (3.3.2)$$

By combining (3.3.1) and the exponential of (3.3.2), we conclude that

$$\frac{1}{\zeta_K(\sigma)} \leq |\zeta_K(\sigma + i\tau)| \leq \zeta_K(\sigma). \quad (3.3.3)$$

Finally, using the fact that $N_{K/\mathbb{Q}}(P)$ is a power of the prime $p \in \mathbb{Z}$ lying under the prime ideal $P \subseteq \mathcal{O}_K$, we have that

$$\zeta_K(\sigma) = \prod_{P \subseteq \mathcal{O}_K} (1 - N_{K/\mathbb{Q}}(P)^{-\sigma})^{-1} \leq \prod_p (1 - p^{-\sigma})^{-d_K} = \zeta(\sigma)^{d_K},$$

since there are at most d_K prime ideals P lying over each p . By combining with (3.3.3), we get the desired result. \square

Combining the above, we arrive at the following result.

Theorem 3.3.2. *Let $s = \sigma + i\tau$ with $\sigma > 1$. Then the Northcott property does not hold at s for any $B \geq \zeta(\sigma)^2$.*

PROOF. Fix $B \geq \zeta(\sigma)^2$. The upper bound in Lemma 3.3.1 implies that for any quadratic field K ,

$$|\zeta_K(s)| = |\zeta_K(\sigma + i\tau)| \leq \zeta(\sigma)^2.$$

This gives an infinite family of isomorphism classes of number fields with $|\zeta_K(s)| \leq B$ and the result follows. \square

3.4. The left side of the critical strip

We now turn our attention to the left side of the critical strip, namely, $\mathbb{C}_{\sigma < 0}$. In this set, Pazuki and Pengo [47] proved that the Northcott property is satisfied at the negative integers and zero. We will extend this result to show that the Northcott property is satisfied away from the negative integers. We will then see that the Northcott property is not satisfied in a neighborhood around each negative integer that excludes the integer itself.

Before proceeding to these considerations, we recall some results giving bounds to discriminants in terms of degrees, and prove some basic lemmas. We start by recalling the following statement.

Theorem 3.4.1 ([45],[18]). *Consider*

$$\delta(n) = \min_{d_K=n} |\Delta_K|,$$

that is, the minimum of the absolute values of the discriminants of all the numbers fields of fixed degree n over \mathbb{Q} . Let

$$D = \liminf_{n \rightarrow \infty} \delta(n)^{1/n}.$$

Then we have

$$D_m \leq D \leq D_M,$$

where

$$D_m := 4\pi e^\gamma = 22.3816\dots,$$

$$D_M := 3^{\frac{1}{8}} \cdot 7^{\frac{1}{12}} \cdot 13^{\frac{1}{12}} \cdot 19^{\frac{1}{6}} \cdot 23^{\frac{1}{3}} \cdot 29^{\frac{1}{12}} \cdot 31^{\frac{1}{12}} \cdot 35509^{\frac{1}{6}} = 78.4269\dots,$$

and γ is the Euler–Mascheroni constant $\gamma = 0.577215\dots$ given by (3.1.1).

Remark 3.4.2. The lower bound appeared as a culmination of a series of articles by Odlyzko [43–45]. (See also the surveys of Poitou [48] and Odlyzko [46].) Odlyzko’s method is a refinement, using ideas of Serre [54], of an analytic method of Stark [56]. This method was a substantial improvement over previous ideas coming directly from Minkowski’s bounds. A better lower bound, $8\pi e^\gamma$, is known under the Generalized Riemann Hypothesis.

The upper bounds come from constructing infinite towers of fields with controlled root discriminant. This idea was due to Martinet [39], and for a long time, his bound of $2^{3/2} \cdot 11^{4/5} \cdot 23^{1/2} = 93.38\dots$ was the best known. It was later improved by Hajir and Maire [23] and finally by Hajir, Maire, and Ramakrishna [18]. The bound in question is obtained by constructing an infinite tower of fields over the totally imaginary field $k = \mathbb{Q}(\alpha)$ with α a root of $x^{12} + 339x^{10} - 19752x^8 - 2188735x^6 + 284236829x^4 + 4401349506x^2 + 15622982921$, that has degree $d_k = 12$ and discriminant $|\Delta_k| = 7 \cdot 13 \cdot 19^2 \cdot 23^4 \cdot 29 \cdot 31 \cdot 35509^2$.

We begin with a simple lemma that transforms the bounds under consideration from field dependent to degree dependent. Together with Lemma 3.3.1, the following statement gives bounds for each of the three factors involved in the functional equation of $\zeta_K(s)$.

Lemma 3.4.3. *Let $s \in \mathbb{C}$ and*

$$\Gamma_m(s) = \min \left\{ \left| \frac{\Gamma_{\mathbb{R}}(1-s)}{\Gamma_{\mathbb{R}}(s)} \right|, \sqrt{\left| \frac{\Gamma_{\mathbb{C}}(1-s)}{\Gamma_{\mathbb{C}}(s)} \right|} \right\}.$$

We have the following bound

$$\Gamma_m(s)^{d_K} \leq \left| \frac{\Gamma_{\mathbb{R}}(1-s)^{r_1} \Gamma_{\mathbb{C}}(1-s)^{r_2}}{\Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2}} \right|.$$

We remark that the above bound is only dependent on the degree of the extension K/\mathbb{Q} and the number of complex and real embeddings, but it is independent of the field itself.

PROOF. To show this, we consider two cases. Writing $\gamma_{\mathbb{R}}(s) = \left| \frac{\Gamma_{\mathbb{R}}(1-s)}{\Gamma_{\mathbb{R}}(s)} \right|$ and $\gamma_{\mathbb{C}}(s) = \left| \frac{\Gamma_{\mathbb{C}}(1-s)}{\Gamma_{\mathbb{C}}(s)} \right|^{\frac{1}{2}}$, we first suppose that $\gamma_{\mathbb{R}}(s) \leq \gamma_{\mathbb{C}}(s)$ so that $\Gamma_m(s) = \gamma_{\mathbb{R}}(s)$. Then

$$|\gamma_{\mathbb{R}}^{r_1}(s)\gamma_{\mathbb{C}}^{2r_2}(s)| \geq |\gamma_{\mathbb{R}}^{r_1}(s)\gamma_{\mathbb{R}}^{2r_2}(s)| = \Gamma_m(s)^{d_K}.$$

Similarly, if $\gamma_{\mathbb{C}}(s) \leq \gamma_{\mathbb{R}}(s)$, we find

$$|\gamma_{\mathbb{R}}^{r_1}(s)\gamma_{\mathbb{C}}^{2r_2}(s)| \geq |\gamma_{\mathbb{C}}^{r_1}(s)\gamma_{\mathbb{C}}^{2r_2}(s)| = \Gamma_m(s)^{d_K}.$$

□

The combination of Lemmas 3.3.1 and 3.4.3 yields the following key result, which gives a sufficient condition for having the Northcott property on the left side of the critical strip.

Proposition 3.4.4. *Let $s = \sigma + i\tau$ with $\sigma < 0$, and suppose that we have*

$$\frac{\Gamma_m(s)}{\zeta(1-\sigma)} D_m^{\frac{1}{2}-\sigma} > 1. \quad (3.4.1)$$

Then the Northcott property holds at s for any $B > 0$.

PROOF. Let $s \in \mathbb{C}_{\sigma < 0}$ such that condition (3.4.1) is true. Then, for $\varepsilon > 0$ sufficiently small, we have that

$$\frac{\Gamma_m(s)}{\zeta(1-\sigma)} (D_m - \varepsilon)^{\frac{1}{2}-\sigma} > 1. \quad (3.4.2)$$

By Theorem 3.4.1 there are only finitely many number fields such that

$$\Delta_K \leq (D_m - \varepsilon)^{d_K}.$$

Combining this with (3.4.2), we conclude that for all but finitely many fields K , we have that

$$|\zeta_K(s)| \geq |\zeta_K(1-s)| \Gamma_m(s)^{d_K} |\Delta_K|^{\frac{1}{2}-\sigma} \geq \frac{\Gamma_m(s)^{d_K}}{\zeta(1-\sigma)^{d_K}} (D_m - \varepsilon)^{d_K(\frac{1}{2}-\sigma)}, \quad (3.4.3)$$

where we have applied Lemmas 3.3.1 and 3.4.3. The statement follows from the fact that for large enough degrees, the number on the right hand side of (3.4.3) is arbitrarily large and that for a fixed degree, there are only finitely many fields with discriminant bounded by any constant. □

Remark 3.4.5. We remark that inequality (3.4.1) is never satisfied when $s \in \mathbb{Z}_{<0}$. Thus, the $s \in \mathbb{C}_{\sigma < 0}$ for which (3.4.1) is true satisfy that $\zeta_K(s) = \zeta_K^*(s)$.

A natural question is to bound the size of $S_{B,s}$ in the cases when it is finite. This was done by Pazuki and Pengo [47] for the case $s = n \in \mathbb{Z}_{n < 0}$ using the following result of Couveignes [14].

Theorem 3.4.6. [14, Theorem 4, simplified version] *There exists an absolute and computable constant \mathcal{Q} such that the following is true. Let K be a number field of degree $d \geq \mathcal{Q}$ and discriminant Δ_K . Then, there are at most*

$$(d^d |\Delta_K|)^{\mathcal{Q}(\log d)^2}$$

possibilities for K .

Although Couveignes does not give the value of \mathcal{Q} , this constant is only related to the technicalities of the proof and is independent of the field.

Using Theorem 3.4.6, we can prove the following bound, which extends the result of [47].

Theorem 3.4.7. *Let $s = \sigma + i\tau$ with $\sigma < 0$ and suppose that*

$$\frac{\Gamma_m(s)}{\zeta(1-\sigma)} D_m^{\frac{1}{2}-\sigma} > 1. \quad (3.4.4)$$

Then, we have

$$\#S_{B,s} \leq \exp\left(2\mathcal{Q}\left(\frac{1}{\frac{1}{2}-\sigma} + \frac{c_s}{a_s}(1 + \log D_m)\right)(\log B)\left(\log\left(\frac{c_s}{a_s} \log B\right)\right)^3\right)$$

where

$$a_s = \log\left(\frac{\Gamma_m(s) D_m^{\frac{1}{2}-\sigma}}{\zeta(1-\sigma)}\right),$$

and c_s is a constant depending on s and chosen so that

$$c_s^{2/3} a_s \left(1 - \frac{1}{c_s}\right) > 8.6 \left(\frac{1}{2} - \sigma\right).$$

PROOF. By Theorem 3.4.6, we have that

$$\#\{[K] : |\Delta_K| = x, d_K = d\} \leq d^{\mathcal{Q}d(\log d)^2} x^{\mathcal{Q}(\log d)^2}.$$

Thus, we have

$$\begin{aligned} \#\{[K] : |\Delta_K| \leq X, d_K \leq D\} &\leq \sum_{x=1}^X \sum_{d=1}^D d^{\mathcal{Q}d(\log d)^2} x^{\mathcal{Q}(\log d)^2} \\ &\leq D^{\mathcal{Q}D(\log D)^2+1} X^{\mathcal{Q}(\log D)^2+1} \\ &\leq \exp\left(2\mathcal{Q}D(\log D)^3 + 2\mathcal{Q}(\log X)(\log D)^2\right). \end{aligned}$$

Now suppose that

$$|\zeta_K(s)| \leq B.$$

By equation (3.4.3), we must have

$$|\zeta_K(1-s)|\Gamma_m(s)^{d_K}|\Delta_K|^{\frac{1}{2}-\sigma} \leq B.$$

Combining the above with (3.4.4), we must have

$$|\zeta_K(1-s)| \left(\frac{\zeta(1-\sigma)}{D_m^{\frac{1}{2}-\sigma}} \right)^{d_K} |\Delta_K|^{\frac{1}{2}-\sigma} \leq B.$$

Now we apply Lemma 3.3.1 to conclude

$$\frac{|\Delta_K|^{\frac{1}{2}-\sigma}}{D_m^{d_K(\frac{1}{2}-\sigma)}} \leq B. \quad (3.4.5)$$

From the lower bound

$$\log |\Delta_K| \geq d_K \log(D_m) + r_1(K) - 8.6d_K^{1/3},$$

(see [48, Equation 22]) and Lemma 3.3.1, one can deduce that

$$B \geq |\zeta_K(1-s)|\Gamma_m(s)^{d_K}|\Delta_K|^{\frac{1}{2}-\sigma} \geq \left(\frac{\Gamma_m(s)D_m^{\frac{1}{2}-\sigma}}{\zeta(1-\sigma)} \right)^{d_K} e^{-8.6d_K^{1/3}(\frac{1}{2}-\sigma)}.$$

The term involving $d_K^{1/3}$ in the exponent decreases at a much lower speed than the other term.

Letting

$$a_s := \log \left(\frac{\Gamma_m(s)D_m^{\frac{1}{2}-\sigma}}{\zeta(1-\sigma)} \right),$$

we have

$$d_K a_s \leq \log B + 8.6d_K^{1/3} \left(\frac{1}{2} - \sigma \right).$$

Suppose that $d_K a_s > c_s \log B$. Then we have

$$d_K^{2/3} a_s \left(1 - \frac{1}{c_s} \right) \leq 8.6 \left(\frac{1}{2} - \sigma \right).$$

But this implies that for $B \geq e$,

$$c_s^{2/3} a_s \left(1 - \frac{1}{c_s} \right) \leq (c_s \log B)^{2/3} a_s \left(1 - \frac{1}{c_s} \right) \leq 8.6 \left(\frac{1}{2} - \sigma \right),$$

which gives a contradiction if we choose c_s sufficiently large (depending only on s).

Thus we have that

$$d_K \leq \frac{c_s}{a_s} \log B \quad \text{and} \quad |\Delta_K| \leq B^{\frac{1}{2}-\sigma} B^{\frac{c_s}{a_s} \log D_m},$$

where the second inequality comes from (3.4.5). Setting

$$D = \frac{c_s}{a_s} \log B \quad \text{and} \quad X = B^{\frac{1}{2}-\sigma + \frac{c_s}{a_s} \log D_m},$$

we obtain

$$\begin{aligned} \#S_{B,s} &\leq \exp\left(2\mathcal{Q}\frac{c_s}{a_s}(\log B)\left(\log\left(\frac{c_s}{a_s}\log B\right)\right)^3 + 2\mathcal{Q}\left(\frac{1}{\frac{1}{2}-\sigma} + \frac{c_s}{a_s}\log D_m\right)(\log B)\left(\log\left(\frac{c_s}{a_s}\log B\right)\right)^2\right) \\ &\leq \exp\left(2\mathcal{Q}\left(\frac{1}{\frac{1}{2}-\sigma} + \frac{c_s}{a_s}(1+\log D_m)\right)(\log B)\left(\log\left(\frac{c_s}{a_s}\log B\right)\right)^3\right) \end{aligned}$$

□

3.4.1. Away from the real line

The next step is to give a general idea of the values of s that respect the condition in Proposition 3.4.4. To do this, it is useful to search for lower bounds for $\Gamma_m(s)$, which follow from individual bounds for the ratios $\gamma_{\mathbb{R}}(s) = \left|\frac{\Gamma_{\mathbb{R}}(1-s)}{\Gamma_{\mathbb{R}}(s)}\right|$ and $\gamma_{\mathbb{C}}(s) = \left|\frac{\Gamma_{\mathbb{C}}(1-s)}{\Gamma_{\mathbb{C}}(s)}\right|^{\frac{1}{2}}$.

Lemma 3.4.8. *Let $s = \sigma + i\tau \in \mathbb{C} \setminus \mathbb{Z}$ with $\sigma < 0$. Then*

$$\gamma_{\mathbb{C}}(s) \geq \frac{(2\pi)^{\sigma-\frac{1}{2}}}{\sqrt{\pi}} \Gamma(1-\sigma) \tanh(\pi\tau)^{\frac{1}{2}}.$$

and

$$\gamma_{\mathbb{R}}(s) \geq \sqrt{2} \frac{(2\pi)^{\sigma-\frac{1}{2}}}{\sqrt{\pi}} \Gamma(1-\sigma) \left| \tanh\left(\frac{\pi\tau}{2}\right) \right|.$$

PROOF. First consider the bound for $\Gamma_{\mathbb{C}}$. By applying Euler's reflection formula (3.2.3), we have

$$\gamma_{\mathbb{C}}(s)^2 = \left| \frac{2(2\pi)^{s-1}\Gamma(1-s)}{2(2\pi)^{-s}\Gamma(s)} \right| = (2\pi)^{2\sigma-1} |\Gamma(1-s)|^2 \frac{|\sin(\pi s)|}{\pi}. \quad (3.4.6)$$

Now we apply inequalities (3.2.5) and (3.2.9) and we obtain

$$\begin{aligned} \gamma_{\mathbb{C}}(s)^2 &\geq \frac{(2\pi)^{2\sigma-1}}{\pi} \Gamma(1-\sigma)^2 \left| \frac{\sin(\pi s)}{\cosh(\pi\tau)} \right| \\ &\geq \frac{(2\pi)^{2\sigma-1}}{\pi} \Gamma(1-\sigma)^2 |\tanh(\pi\tau)|. \end{aligned} \quad (3.4.7)$$

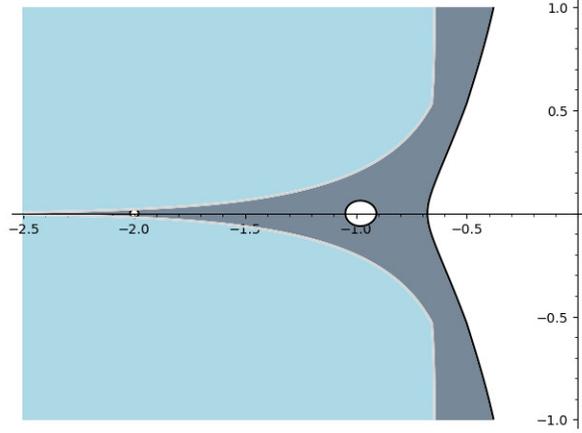


Fig. 3.5. Illustration comparing condition (3.4.10) in the proof of Theorem 3.4.9 (in blue) and condition (3.4.1) from Proposition 3.4.4 (in grey).

Now consider the bound for $\Gamma_{\mathbb{R}}$. Again we apply Euler's reflection formula (3.2.3) as well as inequalities (3.2.5) and (3.2.9), together with Lagrange's duplication formula (3.2.4).

$$\begin{aligned} \gamma_{\mathbb{R}}(s) &= \pi^{\sigma-\frac{1}{2}} \left| \frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)} \right| \\ &= \pi^{\sigma-\frac{1}{2}} \left| \Gamma\left(\frac{1-s}{2}\right) \Gamma\left(1-\frac{s}{2}\right) \right| \frac{|\sin(\frac{\pi s}{2})|}{\pi} \end{aligned} \quad (3.4.8)$$

$$\begin{aligned} &\geq \pi^{\sigma-\frac{1}{2}} \frac{\Gamma\left(\frac{1-\sigma}{2}\right)}{|\cosh\left(\frac{\pi\tau}{2}\right)|^{\frac{1}{2}}} \frac{\Gamma\left(1-\frac{\sigma}{2}\right)}{|\cosh\left(\frac{\pi\tau}{2}\right)|^{\frac{1}{2}}} \frac{|\sin(\frac{\pi s}{2})|}{\pi} \\ &\geq \frac{\pi^{\sigma-\frac{1}{2}}}{\sqrt{\pi}} 2^{\sigma} \Gamma(1-\sigma) \left| \frac{\sin\left(\frac{\pi s}{2}\right)}{\cosh\left(\frac{\pi\tau}{2}\right)} \right| \quad (3.4.9) \\ &\geq \sqrt{2} \frac{(2\pi)^{\sigma-\frac{1}{2}}}{\sqrt{\pi}} \Gamma(1-\sigma) \left| \tanh\left(\frac{\pi\tau}{2}\right) \right|. \end{aligned}$$

□

The previous results allow us to give a large region to the left of the critical strip where the Northcott property is satisfied.

Theorem 3.4.9. *Let $s = \sigma + i\tau$ such that*

$$\sigma < \sigma_0 := -1.5 \quad \text{and} \quad |\tau| > \tau_0 := \frac{2}{\pi} \tanh^{-1} \left(\frac{\zeta\left(\frac{5}{2}\right)}{3\sqrt{2}e^{2\gamma}} \right) = 0.063666\dots$$

Then the Northcott property holds at s for any $B > 0$.

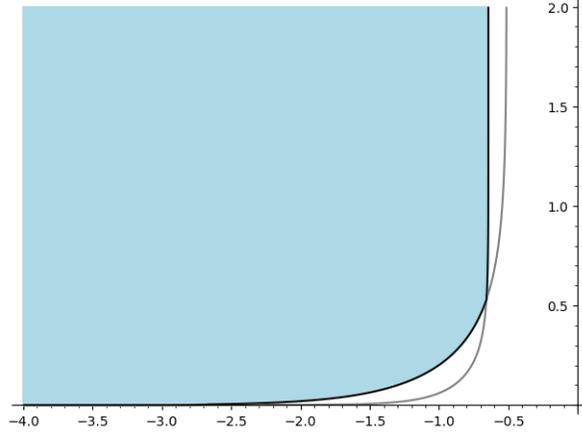


Fig. 3.6. Illustration of condition (3.4.10) in the proof of Theorem 3.4.9.

PROOF. In fact, for such values of σ, τ we have that

$$\frac{\sqrt{2}\Gamma(1-\sigma)|\tanh(\frac{\pi\tau}{2})|}{\sqrt{\pi}\zeta(1-\sigma)}\left(\frac{D_m}{2\pi}\right)^{\frac{1}{2}-\sigma} > 1 \quad \text{and} \quad \frac{\Gamma(1-\sigma)|\tanh(\pi\tau)|^{\frac{1}{2}}}{\sqrt{\pi}\zeta(1-\sigma)}\left(\frac{D_m}{2\pi}\right)^{\frac{1}{2}-\sigma} > 1. \quad (3.4.10)$$

Remark that the functions $\Gamma(1-\sigma)$, $\left(\frac{D_m}{2\pi}\right)^{\frac{1}{2}-\sigma} = (2e^\gamma)^{\frac{1}{2}-\sigma}$, and $\frac{1}{\zeta(1-\sigma)}$ all increase as σ decreases in the negative part of the real axis. Now $|\tanh(\frac{\pi\tau}{2})| = \tanh(\frac{\pi|\tau|}{2})$ and $|\tanh(\pi\tau)|^{\frac{1}{2}} = \tanh(\pi|\tau|)^{\frac{1}{2}}$ are increasing functions of $|\tau|$. Thus, the worse possible case is with $\sigma = \sigma_0$ and $\tau = \tau_0$. Fixing $\sigma = \sigma_0 := -1.5$, we evaluate in σ_0 and choose τ_0 accordingly so that the inequalities in (3.4.10) are satisfied. Figure 3.6 illustrates the condition (3.4.10).

We then combine the inequalities (3.4.10) with Proposition 3.4.4 and Lemma 3.4.8 to conclude.

□

3.4.2. The neighborhood of the real line and away from the integers

In this section we continue to restrict to the condition $\sigma < \sigma_0$ but we now focus on the case where $|\tau| \leq \tau_0$. Since $\Gamma_{\mathbb{R}}$ behaves very differently on odd and even integers, we consider the two cases separately. To cover the remaining strip that has not been covered in Section 3.4.1, we notice that it suffices to investigate the Northcott property in discs centered at negative integers and such that the radii are large enough to cover the whole strip $|\tau| \leq \tau_0$. In other words, if $s = -m + re^{i\theta}$, it then suffices to consider $r \leq \sqrt{\frac{1}{4} + \tau_0^2}$ (see Figure 3.7).

The strategy is to determine a specific criterion on s so that it respects the condition in Proposition 3.4.4.

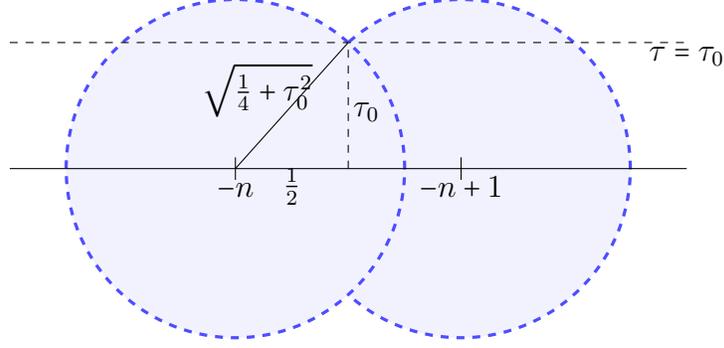


Fig. 3.7. The minimal radius needed to cover the remaining strip $|\tau| \leq \tau_0$ is $\sqrt{\frac{1}{4} + \tau_0^2}$.

3.4.2.1. The negative even integers. When we look at even integers, both cases of Γ_m are small near $-2n$. However, we will see that when we are sufficiently far from $-2n$, these terms can be compensated by large terms in order to satisfy condition (3.4.1). This motivates us to write $s = -2n + re^{i\theta}$, with the goal to get a criterion in terms of r . We proceed to establish these lower bounds.

Lemma 3.4.10. *Let $s = \sigma + i\tau = -2n + re^{i\theta} \in \mathbb{C}$ be such that it lies in the rectangle $-2n - \frac{1}{2} \leq \sigma \leq -2n + \frac{1}{2}$ and $|\tau| \leq \tau_0$, where $\tau_0 > 0$ is arbitrary. Then*

$$\gamma_{\mathbb{C}}(s) \geq \frac{(2\pi)^{\sigma - \frac{1}{2}}}{\sqrt{\pi}} \Gamma(1 - \sigma) \left| \frac{\sin(\pi r)}{\cosh(\pi \tau_0)} \right|^{\frac{1}{2}}$$

and

$$\gamma_{\mathbb{R}}(s) \geq \frac{\sqrt{2}}{\sqrt{\pi}} (2\pi)^{\sigma - \frac{1}{2}} \Gamma(1 - \sigma) \left| \frac{\sin\left(\frac{\pi r}{2}\right)}{\cosh\left(\frac{\pi \tau_0}{2}\right)} \right|.$$

Remark 3.4.11. While Lemma 3.4.10 is true for $\tau_0 > 0$ arbitrary, it will be applied to the τ_0 defined in Theorem 3.4.9. Because we have a precise formula for $\tanh\left(\frac{\pi \tau_0}{2}\right)$ from Theorem 3.4.9, identities such as $\cosh(2\alpha) = \frac{1 + \tanh^2(\alpha)}{1 - \tanh^2(\alpha)} = 2 \cosh^2(\alpha) - 1$ lead to

$$\cosh(\pi \tau_0) = \frac{18e^{4\gamma} + \zeta\left(\frac{5}{2}\right)^2}{18e^{4\gamma} - \zeta\left(\frac{5}{2}\right)^2} = 1.020069 \dots$$

and

$$\cosh\left(\frac{\pi \tau_0}{2}\right) = \frac{3\sqrt{2}e^{2\gamma}}{\left(18e^{4\gamma} - \zeta\left(\frac{5}{2}\right)^2\right)^{\frac{1}{2}}} = 1.005004 \dots$$

PROOF OF LEMMA 3.4.10. First we consider $\Gamma_{\mathbb{C}}$. By inequality (3.4.7), (3.2.10), and the increasing property of $\cosh(x)$ for $x > 0$, we have

$$\begin{aligned}\gamma_{\mathbb{C}}(s) &\geq \frac{(2\pi)^{\sigma-\frac{1}{2}}}{\sqrt{\pi}} \Gamma(1-\sigma) \left| \frac{\sin(\pi s)}{\cosh(\pi\tau)} \right|^{\frac{1}{2}} \\ &\geq \frac{(2\pi)^{\sigma-\frac{1}{2}}}{\sqrt{\pi}} \Gamma(1-\sigma) \left| \frac{\sin(\pi r)}{\cosh(\pi\tau_0)} \right|^{\frac{1}{2}}.\end{aligned}$$

Now we consider $\Gamma_{\mathbb{R}}$. By inequality (3.4.9), we have

$$\begin{aligned}\gamma_{\mathbb{R}}(s) &\geq \frac{\sqrt{2}}{\sqrt{\pi}} (2\pi)^{\sigma-\frac{1}{2}} \Gamma(1-\sigma) \left| \frac{\sin\left(\frac{\pi s}{2}\right)}{\cosh\left(\frac{\pi\tau}{2}\right)} \right| \\ &\geq \frac{\sqrt{2}}{\sqrt{\pi}} (2\pi)^{\sigma-\frac{1}{2}} \Gamma(1-\sigma) \left| \frac{\sin\left(\frac{\pi r}{2}\right)}{\cosh\left(\frac{\pi\tau_0}{2}\right)} \right|.\end{aligned}$$

where we have used again (3.2.10) and the fact that $\cosh(x)$ is an increasing function for $x > 0$. \square

We have what we need to show the following result.

Proposition 3.4.12. *Let $s = \sigma + i\tau = -2n + re^{i\theta} \in \mathbb{C}$ be such that it lies in the rectangle $-2n - \frac{1}{2} \leq \sigma \leq -2n + \frac{1}{2}$ and $|\tau| \leq \tau_0$. Define*

$$\rho(-2n) = \max \left\{ \frac{\sin^{-1}(C_{\mathbb{C}}(n))}{\pi}, \frac{2 \sin^{-1}(C_{\mathbb{R}}(n))}{\pi} \right\}$$

where

$$C_{\mathbb{C}}(n) = \pi \left(\frac{2\pi}{D_m} \right)^{4n} \frac{\zeta\left(2n + \frac{1}{2}\right)^2}{\Gamma\left(2n + \frac{1}{2}\right)^2} |\cosh(\pi\tau_0)|$$

and

$$C_{\mathbb{R}}(n) = \frac{\sqrt{\pi}}{\sqrt{2}} \left(\frac{2\pi}{D_m} \right)^{2n} \frac{\zeta\left(2n + \frac{1}{2}\right)}{\Gamma\left(2n + \frac{1}{2}\right)} \left| \cosh\left(\frac{\pi\tau_0}{2}\right) \right|.$$

Then if $r > \rho(-2n)$, the Northcott property holds at s for any $B > 0$.

We refer to Table A.1 for the values of $\rho(-2n)$ at small positive integers n .

PROOF. The result follows by combining the previous statements. More specifically, Proposition 3.4.4 together with Lemma 3.4.10 give certain criteria for the Northcott property that apply under the conditions of the statement. Here we take into account that

$\sigma \in [-2n - \frac{1}{2}, -2n + \frac{1}{2}]$ and the strategy will be to find bounds in terms of n by taking the worst possible cases.

First we consider the complex case. It follows that a sufficient condition for s to satisfy the Northcott property when $\Gamma_m(s) = \gamma_{\mathbb{C}}(s)$ is

$$\frac{1}{\sqrt{\pi}} \left(\frac{D_m}{2\pi} \right)^{\frac{1}{2}-\sigma} \frac{\Gamma(1-\sigma)}{\zeta(1-\sigma)} \left| \frac{\sin(\pi r)}{\cosh(\pi\tau_0)} \right|^{\frac{1}{2}} > 1.$$

By considering the worst case in each factor, we find

$$\frac{1}{\sqrt{\pi}} \left(\frac{D_m}{2\pi} \right)^{2n} \frac{\Gamma(2n + \frac{1}{2})}{\zeta(2n + \frac{1}{2})} \left| \frac{\sin(\pi r)}{\cosh(\pi\tau_0)} \right|^{\frac{1}{2}} > 1,$$

which is the same as requiring

$$C_{\mathbb{C}}(n) = \pi \left(\frac{2\pi}{D_m} \right)^{4n} \frac{\zeta(2n + \frac{1}{2})^2}{\Gamma(2n + \frac{1}{2})^2} |\cosh(\pi\tau_0)| < \sin(\pi r). \quad (3.4.11)$$

In the real case, a sufficient condition for s to satisfy the Northcott property when $\Gamma_m(s) = \gamma_{\mathbb{R}}(s)$ is

$$\frac{\sqrt{2}}{\sqrt{\pi}} \left(\frac{D_m}{2\pi} \right)^{\frac{1}{2}-\sigma} \frac{\Gamma(1-\sigma)}{\zeta(1-\sigma)} \left| \frac{\sin(\frac{\pi r}{2})}{\cosh(\frac{\pi\tau_0}{2})} \right| > 1.$$

Considering the worst case in each factor gives

$$\frac{\sqrt{2}}{\sqrt{\pi}} \left(\frac{D_m}{2\pi} \right)^{2n} \frac{\Gamma(2n + \frac{1}{2})}{\zeta(2n + \frac{1}{2})} \left| \frac{\sin(\frac{\pi r}{2})}{\cosh(\frac{\pi\tau_0}{2})} \right| > 1,$$

which is the same as requiring

$$C_{\mathbb{R}}(n) = \frac{\sqrt{\pi}}{\sqrt{2}} \left(\frac{2\pi}{D_m} \right)^{2n} \frac{\zeta(2n + \frac{1}{2})}{\Gamma(2n + \frac{1}{2})} \left| \cosh\left(\frac{\pi\tau_0}{2}\right) \right| < \sin\left(\frac{\pi r}{2}\right). \quad (3.4.12)$$

With inequalities (3.4.11) and (3.4.12) in place, we immediately get the following constraints for r

(a)

$$\frac{\sin^{-1}(C_{\mathbb{C}}(n))}{\pi} < r < 1 - \frac{\sin^{-1}(C_{\mathbb{C}}(n))}{\pi},$$

(b)

$$\frac{2 \sin^{-1}(C_{\mathbb{R}}(n))}{\pi} < r < 2 - \frac{2 \sin^{-1}(C_{\mathbb{R}}(n))}{\pi}.$$

Note that as long as

$$\sqrt{\frac{1}{4} + \tau_0^2} < \min \left\{ 1 - \frac{\sin^{-1}(C_{\mathbb{C}}(n))}{\pi}, 2 - \frac{2 \sin^{-1}(C_{\mathbb{R}}(n))}{\pi} \right\}, \quad (3.4.13)$$

the upper conditions in (a) and (b) are automatically verified. The minimum from the right hand side of (3.4.13) is achieved at $n = 1$, namely,

$$1 - \frac{1}{\pi} \sin^{-1} \left(\frac{\zeta \left(\frac{5}{2}\right)^2 e^{-4\gamma}}{9} |\cosh(\pi\tau_0)| \right) = 1 - \frac{1}{\pi} \sin^{-1} \left(\frac{\zeta \left(\frac{5}{2}\right)^2 \left(18 + e^{-4\gamma} \zeta \left(\frac{5}{2}\right)^2\right)}{9 \left(18e^{4\gamma} - \zeta \left(\frac{5}{2}\right)^2\right)} \right) = 0.993547 \dots,$$

but we have

$$\sqrt{\frac{1}{4} + \tau_0^2} = 0.504037 \dots,$$

and therefore (3.4.13) is satisfied.

In conclusion, it suffices to define the function ρ by

$$\max \left\{ \frac{\sin^{-1}(C_{\mathbb{C}}(n))}{\pi}, \frac{2 \sin^{-1}(C_{\mathbb{R}}(n))}{\pi} \right\}.$$

□

Remark 3.4.13. Proposition 3.4.12 gives the second item in Theorem 3.1.1.

Taking the worst case we have the following consequence.

Corollary 3.4.14. *With the same notation as in Proposition 3.4.12, the Northcott property holds for $-2n - \frac{1}{2} \leq \sigma \leq -2n + \frac{1}{2}$ and*

$$r > \rho(-2) = \frac{2}{\pi} \sin^{-1} \left(\frac{\zeta \left(\frac{5}{2}\right)}{\left(18e^{4\gamma} - \zeta \left(\frac{5}{2}\right)\right)^{\frac{1}{2}}} \right) = 0.063889 \dots$$

and any $B > 0$.

Remark 3.4.15. We observe that the $\rho(n)$ given in Proposition 3.4.12 satisfy $\rho(-2n) \rightarrow 0$ as $n \rightarrow \infty$ and this convergence is actually quite fast. Therefore the estimate from Corollary 3.4.14 is a very crude approximation of the region in which the Northcott property is known to hold.

3.4.2.2. The negative odd integers. In this case the lower bound for the term involving $\Gamma_{\mathbb{C}}$ will be similar to what we had in Lemma 3.4.10, while the lower bound for the term involving $\Gamma_{\mathbb{R}}$ will be different.

Lemma 3.4.16. *Let $s = \sigma + i\tau = -2n + 1 + re^{i\theta} \in \mathbb{C}$ be such that it lies in the rectangle $-2n + \frac{1}{2} \leq \sigma \leq -2n + \frac{3}{2}$ and $|\tau| \leq \tau_0$, where $\tau_0 > 0$ is arbitrary. Then*

$$\gamma_{\mathbb{C}}(s) \geq \frac{(2\pi)^{\sigma-\frac{1}{2}}}{\sqrt{\pi}} \Gamma(1-\sigma) \left| \frac{\sin(\pi r)}{\cosh(\pi\tau_0)} \right|^{\frac{1}{2}} \quad (3.4.14)$$

and

$$\gamma_{\mathbb{R}}(s) \geq \frac{\sqrt{2}}{\sqrt{\pi}} (2\pi)^{\sigma-\frac{1}{2}} \Gamma(1-\sigma) \left| \frac{\cos\left(\frac{\pi}{2}\sqrt{\frac{1}{4} + \tau_0^2}\right)}{\cosh\left(\frac{\pi\tau_0}{2}\right)} \right|. \quad (3.4.15)$$

Remark 3.4.17. As in Remark 3.4.11, while Lemma 3.4.16 is true for $\tau_0 > 0$ arbitrary, it will be applied to the τ_0 defined in Theorem 3.4.9. The precise formula for $\tanh\left(\frac{\pi\tau_0}{2}\right)$ from Theorem 3.4.9 gives us

$$\cos\left(\frac{\pi}{2}\sqrt{\frac{1}{4} + \tau_0^2}\right) = \cos\left(\frac{1}{2}\sqrt{\frac{\pi^2}{4} + \left(\log\left(\frac{3\sqrt{2}e^{2\gamma} + \zeta\left(\frac{5}{2}\right)}{3\sqrt{2}e^{2\gamma} - \zeta\left(\frac{5}{2}\right)}\right)\right)^2}\right) = 0.702608\dots$$

PROOF OF LEMMA 3.4.16. The inequality (3.4.14) is obtained by following the same steps as in the proof of Lemma 3.4.10. Remark that attempting to follow these ideas with $\Gamma_{\mathbb{R}}$ produces

$$\gamma_{\mathbb{R}}(s) \geq \frac{\sqrt{2}}{\sqrt{\pi}} (2\pi)^{\sigma-\frac{1}{2}} \Gamma(1-\sigma) \left| \frac{\sin\left(\pi \frac{-2n+1+re^{i\theta}}{2}\right)}{\cosh\left(\frac{\pi\tau_0}{2}\right)} \right|,$$

which is not small near odd integers. Actually we have

$$\left| \sin\left(\pi \frac{-2n+1+re^{i\theta}}{2}\right) \right| = \left| \cos\left(\pi \frac{re^{i\theta}}{2}\right) \right| \geq \cos\left(\frac{\pi r}{2}\right),$$

where the last inequality follows from (3.2.12).

Since the cosine function $\cos\left(\frac{\pi r}{2}\right)$ decreases from 0 to 1, it will be the smallest at $r = \sqrt{\frac{1}{4} + \tau_0^2} < 1$. We find

$$\gamma_{\mathbb{R}}(s) \geq \frac{\sqrt{2}}{\sqrt{\pi}} (2\pi)^{\sigma-\frac{1}{2}} \Gamma(1-\sigma) \left| \frac{\cos\left(\frac{\pi}{2}\sqrt{\frac{1}{4} + \tau_0^2}\right)}{\cosh\left(\frac{\pi\tau_0}{2}\right)} \right|,$$

which concludes the proof. □

Since the lower bound (3.4.15) does not tend to 0 as $r \rightarrow 0$, the fact that the Northcott property holds near odd integers when $\Gamma_m(s) = \gamma_{\mathbb{R}}(s)$ will only depend on n and τ_0 . In fact

Proposition 3.4.18. *Let $s = \sigma + i\tau = -2n + 1 + re^{i\theta} \in \mathbb{C}$ be such that it lies in the rectangle $-2n + \frac{1}{2} \leq \sigma \leq -2n + \frac{3}{2}$ and $|\tau| \leq \tau_0$, where $\tau_0 > 0$ is arbitrary. Suppose that $\Gamma_m(s) = \gamma_{\mathbb{R}}(s)$. Then if*

$$\frac{\sqrt{2} \Gamma(2n - \frac{1}{2})}{\sqrt{\pi} \zeta(2n - \frac{1}{2})} \left| \frac{\cos\left(\frac{\pi}{2} \sqrt{\frac{1}{4} + \tau_0^2}\right)}{\cosh\left(\frac{\pi\tau_0}{2}\right)} \right| \left(\frac{D_m}{2\pi} \right)^{2n-1} > 1,$$

the Northcott property holds for s and any $B > 0$.

Remark 3.4.19. We can see that in the worst case, namely $n = 2$, τ_0 must be at least 0.85 for the above condition to fail.

Proposition 3.4.20. *Let $s = \sigma + i\tau = -2n + 1 + re^{i\theta} \in \mathbb{C}$ with $\sigma < \sigma_0$ be such that it lies in the rectangle $-2n + \frac{1}{2} \leq \sigma \leq -2n + \frac{3}{2}$ and $|\tau| \leq \tau_0$, where $\tau_0 > 0$ is arbitrary. Suppose that $\Gamma_m(s) = \gamma_{\mathbb{C}}(s)$. Define*

$$\rho(-2n + 1) = \frac{1}{\pi} \sin^{-1} \left(\pi \left(\frac{2\pi}{D_m} \right)^{4n-2} \frac{\zeta(2n - \frac{1}{2})^2}{\Gamma(2n - \frac{1}{2})^2} |\cosh(\pi\tau_0)| \right).$$

Then if $r > \rho(-2n + 1)$, then the Northcott property holds at s for any $B > 0$.

Refer to Table A.1 for the values of $\rho(-2n + 1)$ at small positive integers n .

PROOF. The proof of this statement follows that same lines as the proof of Proposition 3.4.12, although it suffices to only consider $\Gamma_{\mathbb{C}}$ this time. Combining Proposition 3.4.4 with Lemma 3.4.16 we find

$$\frac{1}{\sqrt{\pi}} \left(\frac{D_m}{2\pi} \right)^{2n-1} \frac{\Gamma(2n - \frac{1}{2})}{\zeta(2n - \frac{1}{2})} \left| \frac{\sin(\pi r)}{\cosh(\pi\tau_0)} \right|^{\frac{1}{2}} > 1,$$

giving the condition

$$\sin(\pi r) > \pi \left(\frac{2\pi}{D_m} \right)^{4n-2} \frac{\zeta(2n - \frac{1}{2})^2}{\Gamma(2n - \frac{1}{2})^2} |\cosh(\pi\tau_0)|.$$

We reach the result with the same argument used at the end of the proof of Proposition 3.4.12. \square

Remark 3.4.21. Propositions 3.4.18 and 3.4.20 together form the third item in Theorem 3.1.1.

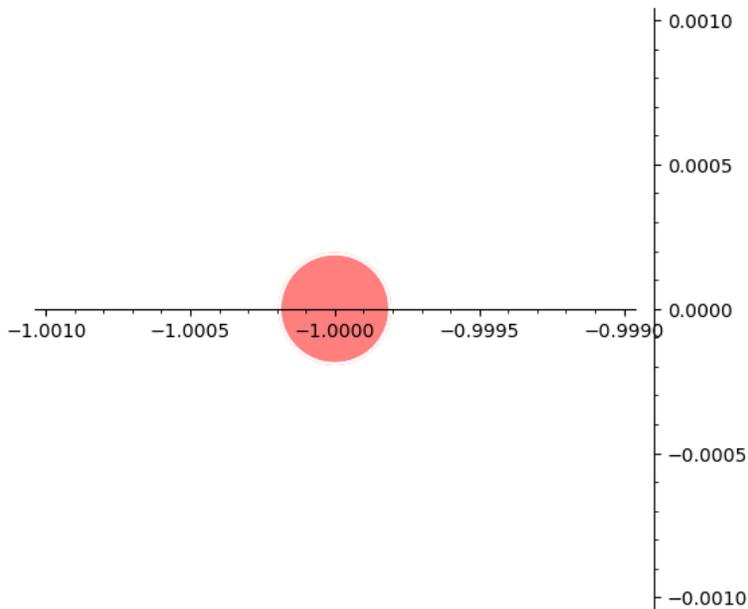


Fig. 3.8. Depiction of the non-Northcott condition (3.4.17) around $\sigma = -1$.

3.4.3. The neighborhood of the negative integers

The goal of this section is to prove non-Northcott near negative integers. To do this, we use the constant $D_M = 3^{\frac{1}{8}} \cdot 7^{\frac{1}{12}} \cdot 13^{\frac{1}{12}} \cdot 19^{\frac{1}{6}} \cdot 23^{\frac{1}{3}} \cdot 29^{\frac{1}{12}} \cdot 31^{\frac{1}{12}} \cdot 35509^{\frac{1}{6}} = 78.4269\dots$ given by Hajir, Maire, and Ramakrishna in [18], and associated to a tower of totally complex fields. More precisely, Hajir, Maire, and Ramakrishna give an infinite sequence of totally complex fields K_ℓ satisfying

$$\lim_{\ell \rightarrow \infty} |\Delta_{K_\ell}|^{\frac{1}{d_{K_\ell}}} = D_M. \quad (3.4.16)$$

The following result is a natural complement to Proposition 3.4.4.

Proposition 3.4.22. *Let $s = \sigma + i\tau$ with $\sigma < 0$ and suppose that we have*

$$\gamma_{\mathbb{C}}(s)\zeta(1-\sigma)D_M^{\frac{1}{2}-\sigma} < 1. \quad (3.4.17)$$

Then the Northcott property does not hold at s for any $B > 0$.

Figure 3.8 shows the region given by condition (3.4.17) in the case of $\sigma = -1$.

PROOF. Using the sequence of totally complex fields K_ℓ satisfying (3.4.16), and fixing an arbitrary $\varepsilon > 0$, we notice that there are infinitely many K_ℓ such that

$$\begin{aligned} |\zeta_{K_\ell}(s)| &= |\zeta_{K_\ell}(1-s)| \left| \frac{\Gamma_{\mathbb{R}}(1-s)^{r_1} \Gamma_{\mathbb{C}}(1-s)^{r_2}}{\Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2}} \right| \left| \Delta_{K_\ell}^{\frac{1}{2}-s} \right| \\ &\leq \gamma_{\mathbb{C}}(s)^{d_{K_\ell}} \zeta(1-\sigma) (D_M + \varepsilon)^{d_{K_\ell}(\frac{1}{2}-\sigma)} \end{aligned} \quad (3.4.18)$$

Here we have used Lemma 3.3.1 together with the fact that the fields K_ℓ are totally complex, and all but finitely many must have root discriminant less than $D_M + \varepsilon$. Now, by setting

$$f_\varepsilon(s) = \gamma_{\mathbb{C}}(s) \zeta(1-\sigma) (D_M + \varepsilon)^{\frac{1}{2}-\sigma},$$

we can write (3.4.18) as

$$|\zeta_{K_\ell}(s)| < f_\varepsilon(s)^{d_{K_\ell}}.$$

When inequality (3.4.17) is true, we can also find an $\varepsilon > 0$ such that it is still true with D_M replaced by $D_M + \varepsilon$. Therefore we have $f_\varepsilon(s) < 1$, and we find that for every $B > 0$ there is a sufficiently large d_B such that

$$|\zeta_{K_\ell}(s)| < f(s)^{d_{K_\ell}} < B \text{ for all } d_{K_\ell} > d_B.$$

□

Remark 3.4.23. The proof of Proposition 3.4.22 shows that the function $[K] \rightarrow |\zeta_K(s)|$ does not satisfy the Bogomolov property (in the sense of [47, Definition 2.8]) when condition (3.4.17) is true. The negation of the Bogomolov property implies the negation of the Northcott property, as discussed in [47].

Since $\Gamma_{\mathbb{C}}(s)$ has poles on the negative integers, the ratio $\frac{\Gamma_{\mathbb{C}}(1-s)}{\Gamma_{\mathbb{C}}(s)}$ vanishes on them and we expect the condition of Proposition 3.4.22 to hold in small discs around them. We will use similar ideas to those introduced in Section 3.4.2.

Consider $s = \sigma + i\tau = -n + re^{i\theta} \in \mathbb{C}$, where $n \in \mathbb{Z}_{>0}$ is chosen so that r is minimal. That is to say, we choose n so that $-n$ is the closest integer to σ , in other words, $\sigma \in [-n - \frac{1}{2}, -n + \frac{1}{2}]$.

Theorem 3.4.24. *Let $s = \sigma + i\tau = -n + re^{i\theta} \in \mathbb{C} \setminus \mathbb{Z}_{<0}$ be such that it verifies $-n - \frac{1}{2} \leq \sigma \leq -n + \frac{1}{2}$. If*

$$r < \frac{1}{\pi} \sinh^{-1} \left(\frac{\pi}{\Gamma(n + \frac{3}{2})^2 \zeta(n + \frac{1}{2})^2} \left(\frac{2\pi}{D_M} \right)^{2n+2} \right),$$

then the Northcott property does not hold at s for any $B > 0$.

PROOF. Starting from (3.4.6), applying (3.2.11) and (3.2.2), we obtain

$$\begin{aligned} \gamma_{\mathbb{C}}(s)\zeta(1-\sigma)D_M^{\frac{1}{2}-\sigma} &= |\Gamma(1-s)| \left(\frac{|\sin(\pi s)|}{\pi} \right)^{\frac{1}{2}} \zeta(1-\sigma) \left(\frac{D_M}{2\pi} \right)^{\frac{1}{2}-\sigma} \\ &\leq \Gamma(1-\sigma) \left(\frac{\sinh(\pi r)}{\pi} \right)^{\frac{1}{2}} \zeta(1-\sigma) \left(\frac{D_M}{2\pi} \right)^{\frac{1}{2}-\sigma}. \end{aligned}$$

Our goal is to guarantee the condition in Proposition 3.4.22. Thus we want,

$$\begin{aligned} \Gamma(1-\sigma) \left(\frac{\sinh(\pi r)}{\pi} \right)^{\frac{1}{2}} \zeta(1-\sigma) \left(\frac{D_M}{2\pi} \right)^{\frac{1}{2}-\sigma} &< 1 \\ \iff \sinh(\pi r) &< \frac{\pi}{\Gamma(1-\sigma)^2 \zeta(1-\sigma)^2} \left(\frac{2\pi}{D_M} \right)^{1-2\sigma}. \end{aligned} \quad (3.4.19)$$

Since $-n - \frac{1}{2} \leq \sigma \leq -n + \frac{1}{2}$, we obtain the result by optimizing each term in (3.4.19) under these restrictions. \square

These radii are rather small and decrease quickly. The first few values can be found in the third column in Table A.1. More values are available in [22].

3.4.4. The case of $\sigma_0 \leq \sigma \leq 0$

We now turn our attention to the remaining area outside the critical strip, that is, $\sigma_0 \leq \sigma < 0$. Remark that the restriction to $\sigma < \sigma_0$ in the last sections originates from requiring that $\Gamma(1-\sigma)$ be sufficiently large for condition (3.4.1) in Proposition 3.4.4 to be satisfied when τ is sufficiently large. As this is no longer the case we turn to other methods.

Direct calculation of condition (3.4.1) reveals that for fixed $\sigma < 0$, we expect the Northcott property to hold for $s = \sigma + i\tau$ with $|\tau| > T_\sigma$ for certain T_σ depending on σ . This is illustrated in Figure 3.9. We can provide an effective result of this statement by slightly modifying the proof of Lemma 3.4.8. Before doing this, we need the following auxiliary statements.

Lemma 3.4.25. *Let $s = \sigma + i\tau$ with $\sigma > 1$. Then we have*

$$|\Gamma(\sigma + i\tau)|^2 \geq |\Gamma(\sigma)|^2 \left| \frac{\pi\tau}{\sinh(\pi\tau)} \right|. \quad (3.4.20)$$

PROOF. By applying Euler's infinite product (3.2.6), and by using that $f(x) = \frac{x^2}{x^2 + \tau^2}$ is strictly increasing for $x > 0$, we have

$$\left| \frac{\Gamma(\sigma + i\tau)}{\Gamma(\sigma)} \right|^2 = \prod_{k=0}^{\infty} \frac{(k+\sigma)^2}{(k+\sigma)^2 + \tau^2} \geq \prod_{k=0}^{\infty} \frac{(k+1)^2}{(k+1)^2 + \tau^2} = \prod_{k=1}^{\infty} \frac{1}{1 + \frac{\tau^2}{k^2}} = \left| \frac{\pi i\tau}{\sin(\pi i\tau)} \right| = \left| \frac{\pi\tau}{\sinh(\pi\tau)} \right|.$$

\square

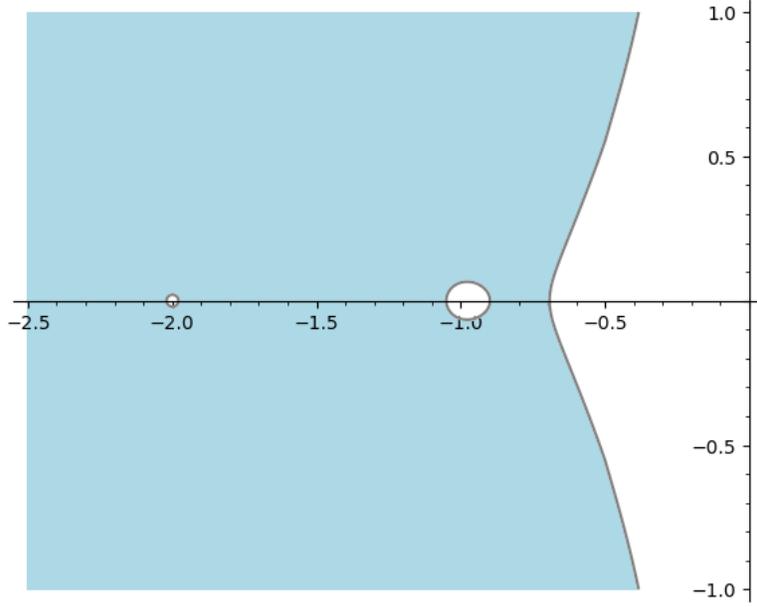


Fig. 3.9. Depiction of points satisfying condition (3.4.1) corresponding to the Northcott property (in blue).

Lemma 3.4.26. *Let $s = \sigma + i\tau$ such that $\sigma < 0$. Then we have*

$$\gamma_{\mathbb{C}}(s)^2 \geq (2\pi)^{2\sigma-1} \Gamma(1-\sigma)^2 |\tau| \quad (3.4.21)$$

$$\gamma_{\mathbb{R}}(s)^2 \geq (2\pi)^{2\sigma-1} \Gamma(1-\sigma)^2 |\tau| \left| \tanh\left(\frac{\pi\tau}{2}\right) \right|. \quad (3.4.22)$$

PROOF. Equation (3.4.21) follows immediately from equations (3.4.6), (3.2.9), and (3.4.20).

Equation (3.4.22) follows similarly from (3.4.8) and the duplication formula (3.2.4) since

$$\begin{aligned} \gamma_{\mathbb{R}}(s) &= \pi^{\sigma-\frac{1}{2}} \left| \Gamma\left(\frac{1-s}{2}\right) \Gamma\left(1-\frac{s}{2}\right) \right| \frac{|\sin(\frac{\pi s}{2})|}{\pi} \\ &= \pi^{\sigma-1} |2^s \Gamma(1-s)| \left| \sin\left(\frac{\pi s}{2}\right) \right| \\ &\geq \pi^{\sigma-\frac{1}{2}} 2^\sigma |\Gamma(1-\sigma)| \frac{|\sin(\frac{\pi s}{2})|}{|\sinh(\pi\tau)|^{\frac{1}{2}}} |\tau|^{\frac{1}{2}} \\ &\geq \pi^{\sigma-\frac{1}{2}} 2^\sigma |\Gamma(1-\sigma)| \frac{|\sinh(\frac{\pi\tau}{2})|}{|\sinh(\pi\tau)|^{\frac{1}{2}}} |\tau|^{\frac{1}{2}} \\ &= (2\pi)^{\sigma-\frac{1}{2}} |\Gamma(1-\sigma)| \left| \tanh\left(\frac{\pi\tau}{2}\right) \right|^{\frac{1}{2}} |\tau|^{\frac{1}{2}}, \end{aligned}$$

Where we have used inequality (3.2.9) and the well-known duplication formula $2 \frac{\sinh(\frac{\pi\tau}{2})^2}{|\sinh(\pi\tau)|} = |\tanh(\frac{\pi\tau}{2})|$. \square

Combining the result above with inequality (3.4.1), we have the following result.

Theorem 3.4.27. *Let $s = \sigma + i\tau$ with $\sigma < 0$ and*

$$|\tau| > \frac{1}{\tanh\left(\frac{\pi}{2} \left(\frac{D_m}{2\pi}\right)^{2\sigma-1} \frac{\zeta(1-\sigma)^2}{\Gamma(1-\sigma)^2}\right)} \left(\frac{D_m}{2\pi}\right)^{2\sigma-1} \frac{\zeta(1-\sigma)^2}{\Gamma(1-\sigma)^2}. \quad (3.4.23)$$

Then, the Northcott property holds at s for any $B > 0$.

PROOF. It suffices to check inequality (3.4.1), and therefore, by Lemma 3.4.26, it suffices to check that

$$|\tau| \min\left\{1, \left|\tanh\left(\frac{\pi\tau}{2}\right)\right|\right\} > \left(\frac{D_m}{2\pi}\right)^{2\sigma-1} \frac{\zeta(1-\sigma)^2}{\Gamma(1-\sigma)^2}. \quad (3.4.24)$$

This follows from the fact that

$$|\tau| > \frac{1}{\tanh\left(\frac{\pi}{2} \left(\frac{D_m}{2\pi}\right)^{2\sigma-1} \frac{\zeta(1-\sigma)^2}{\Gamma(1-\sigma)^2}\right)} \left(\frac{D_m}{2\pi}\right)^{2\sigma-1} \frac{\zeta(1-\sigma)^2}{\Gamma(1-\sigma)^2} > \left(\frac{D_m}{2\pi}\right)^{2\sigma-1} \frac{\zeta(1-\sigma)^2}{\Gamma(1-\sigma)^2},$$

and therefore

$$\left|\tanh\left(\frac{\pi\tau}{2}\right)\right| \geq \tanh\left(\frac{\pi}{2} \left(\frac{D_m}{2\pi}\right)^{2\sigma-1} \frac{\zeta(1-\sigma)^2}{\Gamma(1-\sigma)^2}\right).$$

\square

Remark 3.4.28. We remark that the region given by inequality (3.4.23) is much smaller than the region corresponding to the inequality (3.4.24), since the right hand side of inequality (3.4.23) tends to a non-zero limit (namely, $\frac{2}{\pi}$) as $\sigma \rightarrow -\infty$. This discrepancy is illustrated in Figure (3.10).

Corollary 3.4.29. *Let $s = \sigma + i\tau$ with $\sigma < 0$. There exists $T_\sigma \in \mathbb{R}_{>0}$ such that the Northcott property holds at s for any $B > 0$ as long as $|\tau| > T_\sigma$.*

3.5. Inside the critical strip

3.5.1. The case of $s = 1$

This case was established in [47] by using the asymptotics for the moment of the class numbers $h_{\mathbb{Q}(\sqrt{D})}$, which are directly related to $\zeta_{\mathbb{Q}(\sqrt{D})}^*(1)$ by the class number formula.

Another strategy is to employ the following result of Chowla.

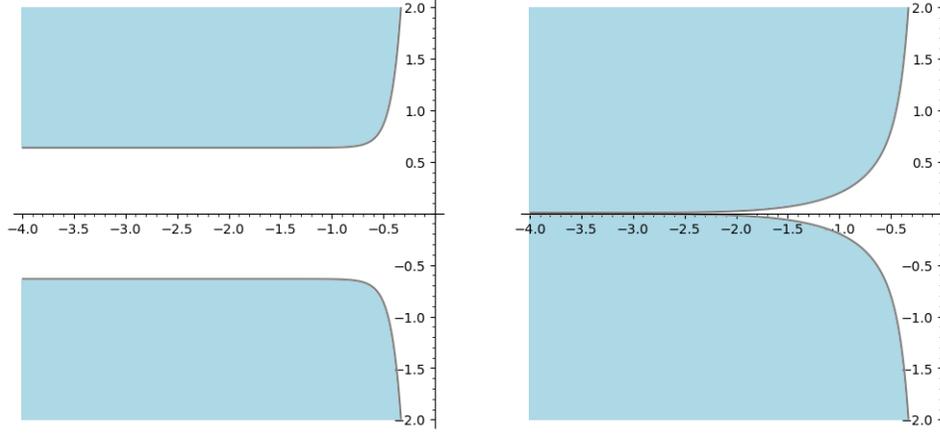


Fig. 3.10. Depiction of conditions (3.4.23) and (3.4.24).

Theorem 3.5.1. [12, Theorem 2] *For any x sufficiently large, there is a $x < d < 2x$ such that there is a real primitive character χ_d modulo d satisfying*

$$L(1, \chi_d) \leq (1 + o(1)) \frac{\zeta(2)}{e^\gamma \log(\log d)},$$

where γ denotes the Euler–Mascheroni constant.

We then have the following result.

Theorem 3.5.2. $s = 1$ *does not satisfy the Northcott property for any $B > 0$.*

PROOF. Recall that for a quadratic field K with corresponding quadratic character χ we have

$$\zeta_K^*(1) = \lim_{s \rightarrow 1} (s-1) \zeta_K(s) = \lim_{s \rightarrow 1} (s-1) \zeta(s) L(1, \chi) = L(1, \chi).$$

Given $B > 0$, choose x such that

$$(1 + o(1)) \frac{\zeta(2)}{e^\gamma \log(\log x)} \leq B.$$

By choosing x progressively larger, we can construct an infinite sequence of fundamental discriminants $D_k \in \mathbb{Z}_{>0}$ such that

$$|\zeta_{\mathbb{Q}(\sqrt{D_k})}^*(1)| \leq B,$$

and this process can be applied to any B arbitrary. Therefore, the Northcott property is not satisfied in this case.

□

Remark 3.5.3. Indeed, the above argument shows that Chowla's result (Theorem 3.5.1) implies that the Bogomolov property ([47, Definition 2.8]) fails at $s = 1$. From there, we deduce the failure of the Northcott property.

3.5.2. The case of $1/2 < \sigma < 1$

Let $\chi_p = \left(\frac{\cdot}{p}\right)$ denote the Legendre symbol modulo a prime p . We have the following result of Lamzouri.

Theorem 3.5.4. [29, Theorem 1.8, partial statement] *Assume the Generalized Riemann Hypothesis. Let $s = \sigma + i\tau$ where $1/2 < \sigma < 1$ and $\tau \in \mathbb{R}$. Then, there exists a constant $x_\sigma \in \mathbb{R}_{>0}$ (where x_σ depends on σ), such that for every $x \geq x_\sigma$ there are $\gg x^{\frac{1}{2}}$ primes $p \leq x$ such that*

$$\log |L(s, \chi_p)| \leq -(\beta(s) + o(1)) \frac{(\log x)^{1-\sigma}}{(\log(\log x))^\sigma},$$

where

$$\beta(\sigma) = \frac{(2 \log 2)^{\sigma-1}}{1-\sigma},$$

and for $\tau \neq 0$,

$$\beta(s) = \frac{\beta(\sigma)\tau^2}{(1-\sigma)^2 + 4\tau^2}.$$

With this result we can prove the following.

Theorem 3.5.5. *Assume the Generalized Riemann Hypothesis for the Dirichlet L-functions associated to real quadratic fields $\mathbb{Q}(\sqrt{p})$ where p runs over the positive rational primes. Let $s = \sigma + i\tau$ with $1/2 < \sigma < 1$, then s does not satisfy the Northcott property for any $B > 0$.*

PROOF. We first remark that the assumption of the Generalized Riemann Hypothesis allows one to say that $\zeta_{\mathbb{Q}(\sqrt{p})}(s) = \zeta_{\mathbb{Q}(\sqrt{p})}^*(s)$ for all the positive rational primes. Let $B > 0$ and s fixed with $1/2 < \sigma < 1$. Choose $x \geq x_\sigma$ such that

$$|\zeta(s)| \exp\left(-(\beta(s) + o(1)) \frac{(\log x)^{1-\sigma}}{(\log(\log x))^\sigma}\right) \leq B.$$

Thus, there are $\gg x^{\frac{1}{2}}$ primes $p \leq x$ such that

$$|\zeta_{\mathbb{Q}(\sqrt{p})}(s)| \leq B.$$

By choosing x progressively larger, we can construct an infinite sequence of primes p_k such that

$$|\zeta_{\mathbb{Q}(\sqrt{p_k})}(s)| \leq B,$$

and this process can be applied to any B arbitrary. Therefore, the Northcott property is not satisfied in this case. \square

Remark 3.5.6. We remark that due to the above argument, Theorem 3.5.5 shows that, under the Generalized Riemann Hypothesis, the Bogomolov property fails for every $s \in \mathbb{C}$ such that $1/2 < \sigma < 1$.

We can also give an unconditional partial result. For this we need the following statement of Sono.

Theorem 3.5.7. [55, Theorem 2.2, simplified version] *Let $\alpha_1, \alpha_2 \in \mathbb{C}$ such that $|\operatorname{Re}(\alpha_j)| < 1/2$. Let $\Phi : \mathbb{R}_{>0} \rightarrow \mathbb{R}$ be a smooth function supported in $[1/2, 3]$ and, for sufficiently large $X > 0$, set*

$$F(x) = \Phi\left(\frac{x}{X}\right).$$

Let $\chi_{8d} = \left(\frac{8d}{\cdot}\right)$, where d is square-free and odd ($8d$ is a fundamental discriminant). Then, for any $\varepsilon > 0$,

$$\sum_{\substack{d \square\text{-free} \\ \text{odd}}} L\left(\frac{1}{2} + \alpha_1, \chi_{8d}\right) L\left(\frac{1}{2} + \alpha_2, \chi_{8d}\right) F(d) = \sum_{\varepsilon_1, \varepsilon_2 \in \{\pm 1\}} A_{\varepsilon_1 \alpha_1, \varepsilon_2 \alpha_2} \Gamma_{\alpha_1}^{\delta_1} \Gamma_{\alpha_2}^{\delta_2} \frac{2\tilde{F}(1 - \delta_1 \alpha_1 - \delta_2 \alpha_2)}{3\zeta(2)} + O_{\alpha_1, \alpha_2}\left(X^{\frac{1}{2} + \varepsilon}\right),$$

where $\tilde{F}(w) = \int_0^\infty F(x)x^{w-1}dx$ is the Mellin transform of F ,

$$A_{\alpha_1, \alpha_2} = \sum_{(n, 2)=1} \frac{\sigma_{\alpha_1, \alpha_2}(n^2)}{n} \prod_{p|n} (1 + p^{-1})^{-1},$$

and

$$\sigma_{\alpha_1, \alpha_2}(n) = \sum_{n_1 n_2 = n} \frac{1}{n_1^{\alpha_1} n_2^{\alpha_2}}.$$

We also have

$$\delta_i = \begin{cases} 0 & \varepsilon_i = 1, \\ 1 & \varepsilon_i = -1. \end{cases}$$

Finally,

$$\Gamma_\alpha = \left(\frac{8}{\pi}\right)^{-\alpha} \frac{\Gamma\left(\frac{1-2\alpha}{4}\right)}{\Gamma\left(\frac{1+2\alpha}{4}\right)}.$$

The statement of Theorem 3.5.7 is deduced from the recipe of Conrey, Farmer, Keating, Rubinstein, and Snaith [13] and rigorously proven as an intermediate step in the estimate for the second moment of quadratic Dirichlet L -functions at $s = 1/2$ with a square-root savings in the error term. The original ideas for the proof are due to Young, who developed this method to obtain similar results for the first and third moments in [60, 61]. In its original

statement, Theorem 3.5.7 has the condition that the α_j be in the rectangle $|\operatorname{Re}(s)| \leq \frac{\varepsilon}{\log X}$, $|\operatorname{Im}(s)| \leq X^\varepsilon$. However, as explained by Young in [60], this condition is imposed to claim uniformity in terms of α . In our case, since the α_j will be fixed, we do not need to impose this condition, but we still need $|\operatorname{Re}(\alpha_j)| < 1/2$ for all the terms $A_{\varepsilon_1\alpha_1, \varepsilon_2\alpha_2}$ to converge.

We choose a concrete $\Phi(x)$ in the next statement to make the result explicit.

Theorem 3.5.8. *Let $s \in \mathbb{C}$ such that $1/2 < \sigma < 1$ be fixed. Set*

$$\Phi(x) = \begin{cases} \exp\left(-\frac{1}{(2x-1)(3-x)}\right) & \frac{1}{2} < x < 3, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and } I = \int_0^\infty \Phi(y) dy.$$

Then s does not satisfy the Northcott property for values of ζ_K for any

$$B > |\zeta(s)| \left(\exp\left(\frac{1}{2}\right) A_{s-\frac{1}{2}, \bar{s}-\frac{1}{2}} \frac{8I}{9} \right)^{\frac{1}{2}}. \quad (3.5.1)$$

PROOF. Let $\alpha = s - \frac{1}{2}$. Then $0 < \operatorname{Re}(\alpha) < 1/2$, and we set $\alpha_1 = \bar{\alpha}_2 = \alpha$ in Theorem 3.5.7. We have

$$\tilde{F}(1 - \delta_1\alpha - \delta_2\bar{\alpha}) = \int_0^\infty \Phi\left(\frac{x}{X}\right) x^{-\delta_1\alpha - \delta_2\bar{\alpha}} dx = X^{1-\delta_1\alpha - \delta_2\bar{\alpha}} \int_0^\infty \Phi(y) y^{-\delta_1\alpha - \delta_2\bar{\alpha}} dy.$$

Remark that the dominant term in the formula for the mixed moment given in Theorem 3.5.7 occurs with $\delta_i = 0$. This gives

$$\sum_{\substack{d \square\text{-free} \\ \text{odd}}} \left| L\left(\frac{1}{2} + \alpha, \chi_{8d}\right) \right|^2 F(d) = A_{\alpha, \bar{\alpha}} \frac{2I}{3\zeta(2)} X + O\left(X^{1-\operatorname{Re}(\alpha)} + X^{\frac{1}{2}+\varepsilon}\right).$$

Then we get

$$\sum_{\substack{d \square\text{-free} \\ \text{odd} \\ X \leq d \leq \frac{5}{2}X}} \left| L\left(\frac{1}{2} + \alpha, \chi_{8d}\right) \right|^2 \leq \exp\left(\frac{1}{2}\right) A_{\alpha, \bar{\alpha}} \frac{2I}{3\zeta(2)} X + O\left(X^{1-\operatorname{Re}(\alpha)} + X^{\frac{1}{2}+\varepsilon}\right).$$

The number of d square-free, odd and such that $X \leq d \leq \frac{5}{2}X$ is $\sim \frac{3X}{4\zeta(2)}$ (see [40, Ex. 3.2.1.6]).

Thus, given $\varepsilon > 0$, we can guarantee that for X large enough there is a d such that $X \leq d \leq \frac{5}{2}X$ and for which

$$\left| L\left(\frac{1}{2} + \alpha, \chi_{8d}\right) \right| \leq \left(\exp\left(\frac{1}{2}\right) A_{\alpha, \bar{\alpha}} \frac{8I}{9} \right)^{\frac{1}{2}} + \varepsilon.$$

Taking ε arbitrarily small we can construct an infinite sequence of d 's satisfying this property, and leading to bounded $\left| L\left(\frac{1}{2} + \alpha, \chi_{8d}\right) \right|$. The conclusion follows by writing

$$\zeta_K\left(\frac{1}{2} + \alpha\right) = \zeta\left(\frac{1}{2} + \alpha\right) L\left(\frac{1}{2} + \alpha, \chi_{8d}\right).$$

□

Remark 3.5.9. Notice that, for every rational prime $p \in \mathbb{Z}_{>0}$, we have that

$$\begin{aligned} & \frac{1}{2} \left(\left(1 - \frac{1}{p^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 - \frac{1}{p^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} + \left(1 + \frac{1}{p^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 + \frac{1}{p^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} \right) \\ &= \frac{1}{2} \left(\sum_{j_1=0}^{\infty} \frac{1}{p^{j_1(\frac{1}{2}+\alpha)}} \sum_{j_2=0}^{\infty} \frac{1}{p^{j_2(\frac{1}{2}+\bar{\alpha})}} + \sum_{j_1=0}^{\infty} \frac{(-1)^{j_1}}{p^{j_1(\frac{1}{2}+\alpha)}} \sum_{j_2=0}^{\infty} \frac{(-1)^{j_2}}{p^{j_2(\frac{1}{2}+\bar{\alpha})}} \right) \\ &= 1 + \frac{1}{2} \left(\sum_{\ell=1}^{\infty} \frac{\sigma_{\alpha, \bar{\alpha}}(p^\ell)}{p^{\frac{\ell}{2}}} + \sum_{\ell=1}^{\infty} \frac{(-1)^\ell \sigma_{\alpha, \bar{\alpha}}(p^\ell)}{p^{\frac{\ell}{2}}} \right). \end{aligned}$$

Thus, $A_{\alpha, \bar{\alpha}}$ can be expressed as

$$\begin{aligned} A_{\alpha, \bar{\alpha}} &= \prod_{p \neq 2} \left(1 + \left(1 + \frac{1}{p}\right)^{-1} \sum_{\ell=1}^{\infty} \frac{\sigma_{\alpha, \bar{\alpha}}(p^{2\ell})}{p^\ell} \right) \\ &= \prod_{p \neq 2} \left[\frac{1}{2} \left(\left(1 - \frac{1}{p^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 - \frac{1}{p^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} + \left(1 + \frac{1}{p^{\frac{1}{2}+\alpha}}\right)^{-1} \left(1 + \frac{1}{p^{\frac{1}{2}+\bar{\alpha}}}\right)^{-1} \right) + \frac{1}{p} \right] \\ &\quad \times \left(1 + \frac{1}{p}\right)^{-1}. \end{aligned}$$

3.5.3. The case of $\operatorname{Re}(s) = 1$

In order to complete the analysis in this section, one should consider the general case $\operatorname{Re}(s) = 1$. This case was considered in [20, Section 5.5], where Theorem 5.17 shows in particular that s with $\operatorname{Re}(s) = 1$ does not satisfy the Northcott property for any B larger than a certain constant. We expect a similar result to hold (at least conditional on the Generalized Riemann Hypothesis) over number fields.

Appendix A

The left side neighborhood of zero

In the Subsection 3.4.4, Theorem 3.4.27 provided an answer for the Northcott property for the region $\sigma_0 := -1.5 \leq \sigma < 0$ but failed to capture the true boundary of condition (3.4.1) in Proposition 3.4.4. In particular, we expect that for some $\sigma \in [\sigma_0, 0)$, the Northcott property holds for all τ .

Using numerical methods, we can obtain substantially more precise results that are closer to the boundary given by Proposition 3.4.4. Namely, we can describe a circle around $s = -1$ in the style of the circles described in Propositions 3.4.12 and 3.4.20, and we can better describe the behavior for $\sigma < 0$ approaching the origin. Furthermore, we can also obtain improvements for the circles in the first few cases of $s = n$ with n a negative integer. The results in this section are better than the ones given in Theorem 3.4.27 but require a large number of steps, and ultimately rely on the help of a computer.

The strategy in this section is the following. We will numerically construct an approximation of a curve that is close to the boundary of the red region in Figure 3.9, such that we will be able to guarantee that the Northcott property is true for $s = \sigma + i\tau$ with $|\tau| > t > 0$ such that $\sigma + it$ is on the curve. This curve approximation will be made of small horizontal segments (see Figure A.4 for an example). In order to construct this approximation, we consider an interval around n , and we perform a sufficiently fine division into smaller intervals $[\alpha, \beta]$ where we can numerically control the behavior of the factors involved in inequality (3.4.1) due to monotonicity. To achieve this goal, we will need some auxiliary results about the growth of the factors involved in (3.4.1).

The first result will allow us to understand the growth of $|\Gamma(s)|$ as s moves in a horizontal line, outside a circle of center $\frac{1}{2}$.

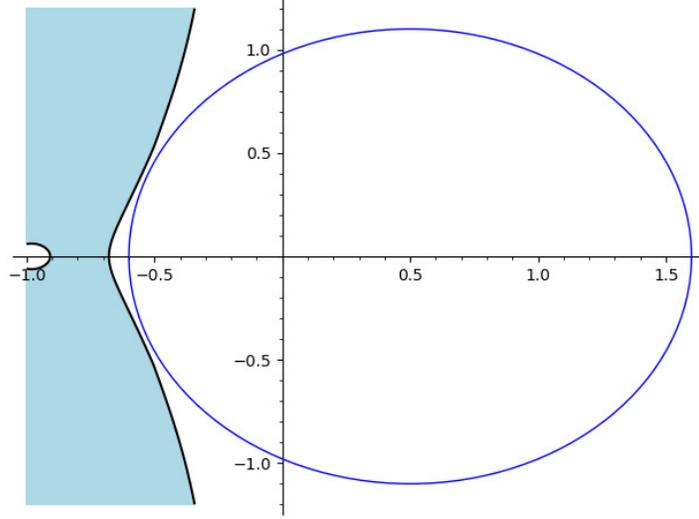


Fig. A.1. Depiction of the boundary of condition (3.4.1) and the circle of center 0.5 and radius 1.1 employed in Lemma A.0.1

Lemma A.0.1. Let $s = \sigma + i\tau \in \{z \in \mathbb{C}_{\sigma < 0} : |z - 0.5| \geq 1.1\}$. We have

$$\frac{d}{d\sigma} |\Gamma(1-s)|^2 \leq 0.$$

Remark A.0.2. The constant 1.1 has been numerically chosen by numerically adjusting a circle centered at 0.5 so that it satisfies the following conditions.

- The circle encapsulates the region of $\mathbb{C}_{\sigma < 0}$ where $\frac{d}{d\sigma} |\Gamma(1-s)|^2 \geq 0$.
- The boundary of the red region of Figure 3.9 entirely lies outside this circle (see Figure A.1 for more detail).

PROOF. After replacing $1-s$ by s , the statement to be proven is equivalent to $\frac{d}{d\sigma} |\Gamma(\sigma + i\tau)|^2 \geq 0$ for $s = \sigma + i\tau \in \mathcal{C} := \{z \in \mathbb{C}_{\sigma > 1} : |z - 0.5| \geq 1.1\}$. We have

$$\frac{d}{ds} \Gamma(s) \overline{\Gamma(s)} = (\psi(s) + \overline{\psi(s)}) |\Gamma(s)|^2,$$

where ψ denotes the digamma function (3.2.7). Therefore, the desired derivative is given by

$$\frac{d}{d\sigma} |\Gamma(\sigma + i\tau)|^2 = 2 \operatorname{Re}(\psi(\sigma + i\tau)) |\Gamma(\sigma + i\tau)|^2.$$

Our goal is to show that $\operatorname{Re}(\psi(\sigma + i\tau))$ is positive outside the circle \mathcal{C} . We consider the series (3.2.8) and truncate it to the first four terms:

$$\operatorname{Re}(\psi(s)) = -\gamma + \sum_{k=1}^{\infty} \frac{k(\sigma - 1) + (\sigma - 1)^2 + \tau^2}{k((k + \sigma - 1)^2 + \tau^2)} \geq -\gamma + \sum_{k=1}^4 \frac{k(\sigma - 1) + (\sigma - 1)^2 + \tau^2}{k((k + \sigma - 1)^2 + \tau^2)}, \quad (\text{A.0.1})$$

where we have chosen to keep four terms because numerical estimates suggest this level of truncation yields the needed precision.

Next, since we want to prove that the right-hand side of (A.0.1) is positive outside the circle \mathcal{C} , we consider polar coordinates centered at 0.5. After the change of variables $s = 0.5 + re^{ix}$, we now have

$$-\gamma + \sum_{k=1}^4 \frac{4r^2 + 4(k-1)r \cos(x) - 2k + 1}{4kr^2 + 4(2k^2 - k)r \cos(x) + 4k^3 - 4k^2 + k}. \quad (\text{A.0.2})$$

The derivative with respect to r of each term is

$$\frac{4(4k(k-1) \cos(x) + (4r^2 + 1) \cos(x) + 4r(2k-1))}{(4r^2 + 4(2k-1)r \cos(x) + 4k^3 - 4k^2 + k)^2}.$$

We see that the term above is always positive for $x \in [-\pi/2, \pi/2]$. Thus, if expression (A.0.2) is positive on this half circle of fixed radius, the result will follow. To see this, we compute the derivative of (A.0.2) with respect to x and remark that it can be expressed as $\sin(x)R(\cos(x))$, where $R(t)$ is a rational function with positive coefficients, and therefore $R(\cos(x)) \geq 0$ for $x \in [-\pi/2, \pi/2]$. From this we can deduce that for fixed r , equation (A.0.2) reaches its minimum when $x = 0$. Now we evaluate at $r = 1.1$ and $x = 0$ to obtain

$$-\gamma + \sum_{k=1}^4 \frac{4(1.1)^2 + 4(k-1)(1.1) - 2k + 1}{4k(1.1)^2 + 4k^3 + 4(2k^2 - k)(1.1) - 4k^2 + k} = 0.00133\dots$$

Thus, we conclude that $\operatorname{Re}(\psi(s)) \geq 0$ outside \mathcal{C} , and therefore the same is true for $\frac{d}{ds}|\Gamma(s)|^2$. \square

The next result allows us to understand the growth of $\gamma_{\mathbb{C}}(s)$ and $\gamma_{\mathbb{R}}(s)$ as s moves along a vertical line.

Lemma A.0.3. *Let $\sigma \leq 1/2$ be fixed. Then*

$$\frac{d}{d\tau} \gamma_{\mathbb{C}}(s)^4 \geq 0 \quad \text{and} \quad \frac{d}{d\tau} \gamma_{\mathbb{R}}(s)^2 \geq 0$$

for $\tau \in [0, \infty)$.

PROOF. Starting with the case of $\gamma_{\mathbb{C}}$, it suffices to check the sign of the derivative. Thus, we can ignore the positive constants and consider

$$\frac{d}{d\tau} \frac{|\Gamma(1-s)|^2}{|\Gamma(s)|^2}.$$

The above expression has the same sign as

$$\begin{aligned} & \left(\frac{d}{d\tau} \Gamma(1-s) \overline{\Gamma(1-s)} \right) |\Gamma(s)|^2 - \left(\frac{d}{d\tau} \Gamma(s) \overline{\Gamma(s)} \right) |\Gamma(1-s)|^2 \\ &= |\Gamma(1-s)|^2 \left(-i\psi(1-s) + i\overline{\psi(1-s)} \right) |\Gamma(s)|^2 - |\Gamma(s)|^2 \left(i\psi(s) - i\overline{\psi(s)} \right) |\Gamma(1-s)|^2. \end{aligned}$$

Ignoring positive terms once again, we are left to consider

$$\left(-i\psi(1-s) + i\overline{\psi(1-s)} \right) - \left(i\psi(s) - i\overline{\psi(s)} \right),$$

which is the same as

$$\operatorname{Im}(\psi(s) + \psi(1-s)).$$

Now, using (3.2.8), we reduce the problem to

$$\sum_{k=1}^{\infty} \frac{\tau}{(k+\sigma-1)^2 + \tau^2} - \sum_{k=1}^{\infty} \frac{\tau}{(k-\sigma)^2 + \tau^2} \geq 0.$$

We can show this by ignoring the sums and comparing the terms for each k . In doing so, we find

$$\frac{\tau}{(k+\sigma-1)^2 + \tau^2} \geq \frac{\tau}{(k-\sigma)^2 + \tau^2} \text{ when } \sigma \leq 1/2 \text{ and } \tau \geq 0.$$

The case of $\gamma_{\mathbb{R}}$ can be proven similarly. □

Corollary A.0.4. *Suppose that for fixed $t \geq 0$ and all $\sigma \in [\alpha, \beta]$ we have*

$$\frac{\Gamma_m(\sigma + it)}{\zeta(1-\sigma)} D_m^{\frac{1}{2}-\sigma} > 1.$$

Then, this inequality is also true for $\tau > t$.

PROOF. The statement follows directly from Lemma A.0.3. □

We are now ready to show the following key result.

Proposition A.0.5. *Let $s = \sigma + i\tau \in \{z \in \mathbb{C}_{\sigma < 0} : |z - 0.5| \geq 1.1\}$. Furthermore, let τ be fixed and $\sigma \in [\alpha, \beta] \subseteq \mathbb{R}$ and $n \in \mathbb{Z}_{< 0}$. The following statements are true:*

(1) Suppose $[\alpha, \beta] \subseteq [n, n + \frac{1}{2}]$, then for all $\sigma \in [\alpha, \beta]$

$$\frac{1}{\sqrt{\pi}} \left(\frac{D_m}{2\pi} \right)^{\frac{1}{2}-\beta} \frac{|\Gamma(1-\beta-i\tau)|}{\zeta(1-\beta)} |\sin(\pi(\alpha+i\tau))|^{\frac{1}{2}} > 1 \implies \frac{\gamma_{\mathbb{C}}(s)}{\zeta(1-\sigma)} D_m^{\frac{1}{2}-\sigma} > 1.$$

(2) Suppose $[\alpha, \beta] \subseteq [n - \frac{1}{2}, n]$, then

$$\frac{1}{\sqrt{\pi}} \left(\frac{D_m}{2\pi} \right)^{\frac{1}{2}-\beta} \frac{|\Gamma(1-\beta-i\tau)|}{\zeta(1-\beta)} |\sin(\pi(\beta+i\tau))|^{\frac{1}{2}} > 1 \iff \frac{\gamma_{\mathbb{C}}(s)}{\zeta(1-\sigma)} D_m^{\frac{1}{2}-\sigma} > 1. \quad (\text{A.0.3})$$

(3) Suppose $[\alpha, \beta] \subseteq [2n, 2n + 1]$, then

$$\frac{\sqrt{2}}{\sqrt{\pi}} \left(\frac{D_m}{2\pi} \right)^{\frac{1}{2}-\beta} \frac{|\Gamma(1-\beta-i\tau)|}{\zeta(1-\beta)} \left| \sin\left(\frac{\pi}{2}(\alpha+i\tau)\right) \right| > 1 \implies \frac{\gamma_{\mathbb{R}}(s)}{\zeta(1-\sigma)} D_m^{\frac{1}{2}-\sigma} > 1.$$

(4) Suppose $[\alpha, \beta] \subseteq [2n - 1, 2n]$, then

$$\frac{\sqrt{2}}{\sqrt{\pi}} \left(\frac{D_m}{2\pi} \right)^{\frac{1}{2}-\beta} \frac{|\Gamma(1-\beta-i\tau)|}{\zeta(1-\beta)} \left| \sin\left(\frac{\pi}{2}(\beta+i\tau)\right) \right| > 1 \iff \frac{\gamma_{\mathbb{R}}(s)}{\zeta(1-\sigma)} D_m^{\frac{1}{2}-\sigma} > 1.$$

PROOF. The proof follows by studying the growth of the terms in condition (3.4.1).

The functions under consideration are (up to a positive constant) the following.

(1) The expression

$$\left(\frac{D_m}{2\pi} \right)^{\frac{1}{2}-\sigma} \frac{|\Gamma(1-\sigma-i\tau)|}{\zeta(1-\sigma)}$$

is monotonously decreasing as a function of σ when $s \in \{z \in \mathbb{C}_{\sigma < 0} : |z - 0.5| \geq 1.1\}$ by Lemma A.0.1.

(2) The function $|\sin(\pi\sigma)|$ is increasing in $[n, n + \frac{1}{2}]$ and decreasing in $[n - \frac{1}{2}, n]$ for $n \in \mathbb{Z}$. For fixed τ this function has the same increasing/decreasing intervals as $|\sin(\pi(\sigma+i\tau))|^{\frac{1}{2}}$. This follows from the fact that $|\sin(\pi(\sigma+i\tau))|^{\frac{1}{2}} = \sqrt[4]{\sin(\pi\sigma)^2 + \sinh(\pi\tau)^2}$ and $\sinh(\pi\tau)^2$ is constant when τ is fixed.

(3) Similarly, $|\sin(\frac{\pi}{2}(\sigma+i\tau))|$ is increasing in $[2n, 2n + 1]$ and decreasing in $[2n - 1, 2n]$ for $n \in \mathbb{Z}$.

We get the result by combining the above facts together and by taking the minimum of each component in the interval $[\alpha, \beta]$. \square

An application of Proposition A.0.5

We can construct an effective approximation of the boundary of condition (3.4.1) by considering a very thin subdivision of the interval of interest and by applying Proposition

A.0.5 in each sub-interval. To illustrate this, Figures A.4 and A.5 have been constructed by subdividing the intervals $[-1.2, -0.8]$ and $[-0.8, -0.5]$ respectively.

To obtain these results, we first subdivide the interval $[-1.5, -0.1]$ into segments of length $\delta = 0.0025$. For each said segment $[\alpha, \alpha + \delta]$, we then find τ_α such that Proposition A.0.5 is satisfied. Since Lemma A.0.3 implies that Proposition A.0.5 is also satisfied for $|\tau| > |\tau_\alpha|$, we seek to find the smallest τ_α possible. In the case of the sub-interval $[-1.5, -0.68]$, the region where $\tau_\alpha > 0$ is close to a circle, and therefore we approximate its boundary by above with a circle. We showcase these results in the following remark.

Remark A.0.6. Let $s = \sigma + i\tau$ with $\sigma \in [-1.5, \sigma_1]$, where $\sigma_1 \approx -0.68$ satisfies

$$\frac{(2e^\gamma)^{\frac{1}{2}-\sigma_1}}{\zeta(1-\sigma_1)} \left| \frac{\Gamma(1-\sigma_1)}{\Gamma(\sigma_1)} \right|^{\frac{1}{2}} = 1.$$

(In other words, $\frac{\gamma_{\mathbb{C}}(\sigma_1)}{\zeta(1-\sigma_1)} D_m^{\frac{1}{2}-\sigma_1} = 1$.) We define

$$R(\sigma) = \begin{cases} 0 & \text{for } \sigma \in [-1.5, -1 - \rho(-1)) \\ \sqrt{\rho(-1)^2 - (\sigma + 1)^2} & \text{for } \sigma \in [-1 - \rho(-1), -1 + \rho(-1)] \\ 0 & \text{for } \sigma \in (-1 + \rho(-1), \sigma_1] \end{cases}$$

where $\rho(-1) \approx 9.5 \times 10^{-2}$. Then, as long as $|\tau| \geq R(\sigma)$ the Northcott property holds at s for any $B > 0$.

We stop at $\sigma_1 \approx -0.68$ because for $\sigma > \sigma_1$ we will again need that $|\tau_\alpha| > 0$ for Proposition A.0.5 to be satisfied. Figure A.5 illustrates this phenomenon. The value of σ_1 marks the beginning of the red region on the right of Figure 3.9. The complete list of τ_α used for the interval $[-1.5, \sigma_1]$ is available here [22]. Notice that in this list, the closest point to $s = 0.5$ is at a distance of $1.1227 > 1.1$, in particular, this justifies our use of Proposition A.0.5. Figure A.2 illustrates a comparison between Theorem 3.4.27, Remark A.0.6, and the numerical graph found with Proposition A.0.5 and more clearly depicted in Figure A.4.

For the interval $[\sigma_1, -0.1]$, the boundary of the Northcott region is more difficult to describe. The following remark aims at approximating the boundary described by bounding the segments by above with continuous functions. A comparison among Theorem 3.4.27, Remark A.0.7, and the numerical results found with Proposition A.0.5 is made in Figure A.3.

Center	Num. radius (Appendix A)	Northcott radius (Section 3.4)	Non-Northcott radius
-1	$9.260\,260\,274\,818 \times 10^{-2}$	-	$3.415\,443\,142\,941 \times 10^{-6}$
-2	$2.105\,502\,084\,026 \times 10^{-2}$	$6.388\,919\,396\,319 \times 10^{-2}$	$1.330\,026\,824\,001 \times 10^{-8}$
-3	$4.474\,651\,495\,645 \times 10^{-6}$	$5.742\,868\,294\,706 \times 10^{-5}$	$9.877\,567\,910\,286 \times 10^{-12}$
-4	$1.135\,531\,168\,473 \times 10^{-4}$	$4.516\,050\,376\,141 \times 10^{-4}$	$3.572\,719\,521\,466 \times 10^{-15}$
-5	$6.138\,786\,399\,296 \times 10^{-11}$	$1.190\,762\,805\,871 \times 10^{-9}$	$8.022\,539\,291\,403 \times 10^{-19}$

Table A.1. In the first column, we showcase the radii of the Northcott region obtained using the methods of this section. This means that the points outside of these circles satisfy the Northcott property. The second column is similarly constructed using the methods given by Propositions 3.4.12, 3.4.18 and 3.4.20 to calculate the radii. Finally, the third column shows the radii of the non-Northcott circles, also computed from the results in Section 3.4. In this case, the area inside these circles is proven to be non-Northcott.

Remark A.0.7. Let $s = \sigma + i\tau$ with $\sigma \in [\sigma_1, -0.1]$. We define

$$R(\sigma) = \begin{cases} \sqrt{\sigma - \sigma_1 + 0.1} & \text{for } \sigma \in (\sigma_1, -0.65] \\ 0.82 \left(\frac{D_m}{2\pi}\right)^{2\sigma-1} \frac{\zeta(1-\sigma)^2}{\Gamma(1-\sigma)^2} & \text{for } \sigma \in (-0.65, -0.1]. \end{cases}$$

Then, as long as $|\tau| \geq R(\sigma)$ the Northcott property holds at s for any $B > 0$.

The formula for $R(\sigma)$ was constructed ad hoc from a modification of the formula in Theorem 3.4.27 aimed at approximating the numerical graph from Figure A.5 (from above) combined with a simpler formula for values closer to σ_1 .

We have chosen to stop at -0.1 for the sake of clarity, as $\tau_\alpha \rightarrow \infty$ as $\alpha \rightarrow 0$. This method could have been used for any interval $[-1.5, \varepsilon]$ where $\varepsilon > 0$.

Remark A.0.8. Although the areas around the integers that do not satisfy the condition of Proposition 3.4.4 are not circles, they are approximate circles well enough suggesting that one should fit them in circles centered at the integers. Table A.1 compares this numerical method based on Proposition A.0.5 with the previous results based on Propositions 3.4.12, 3.4.18, and 3.4.20. We have used better precision than in Remarks A.0.6 and A.0.7, leading to more precision in the radii.

The source code for these calculations is available here [22]. The computations were performed with the aid of Sage [58].

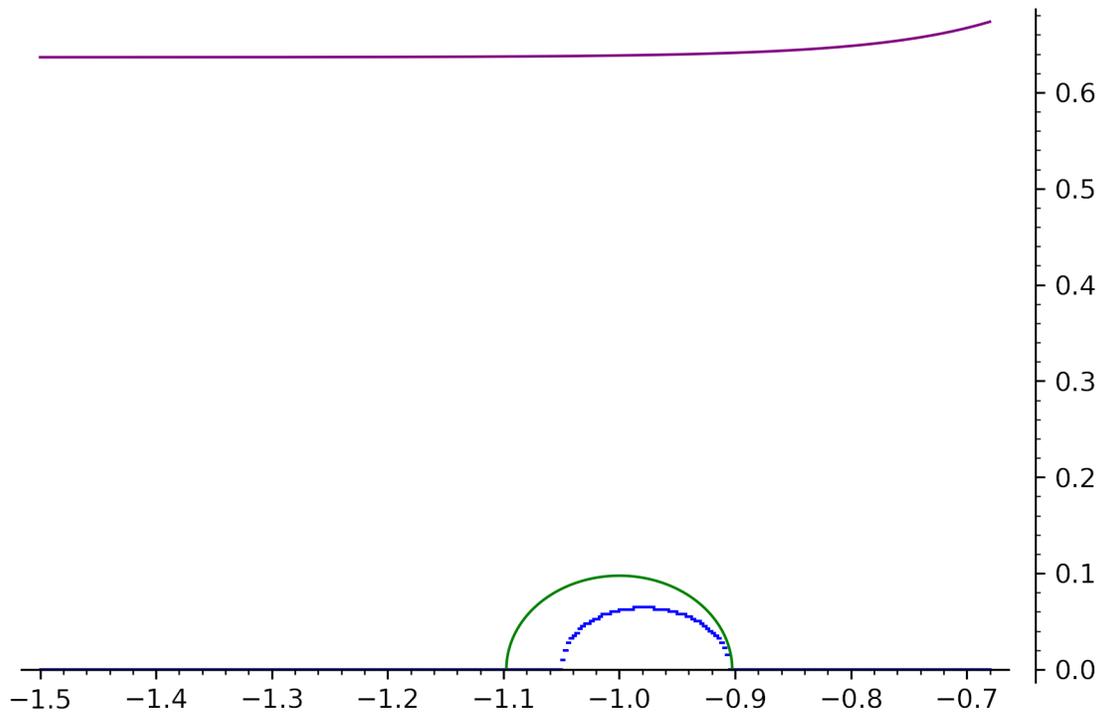


Fig. A.2. Comparison between Theorem 3.4.27 (purple), Remark A.0.6 (green) and the piece-wise curve found with the methods of this section (blue).

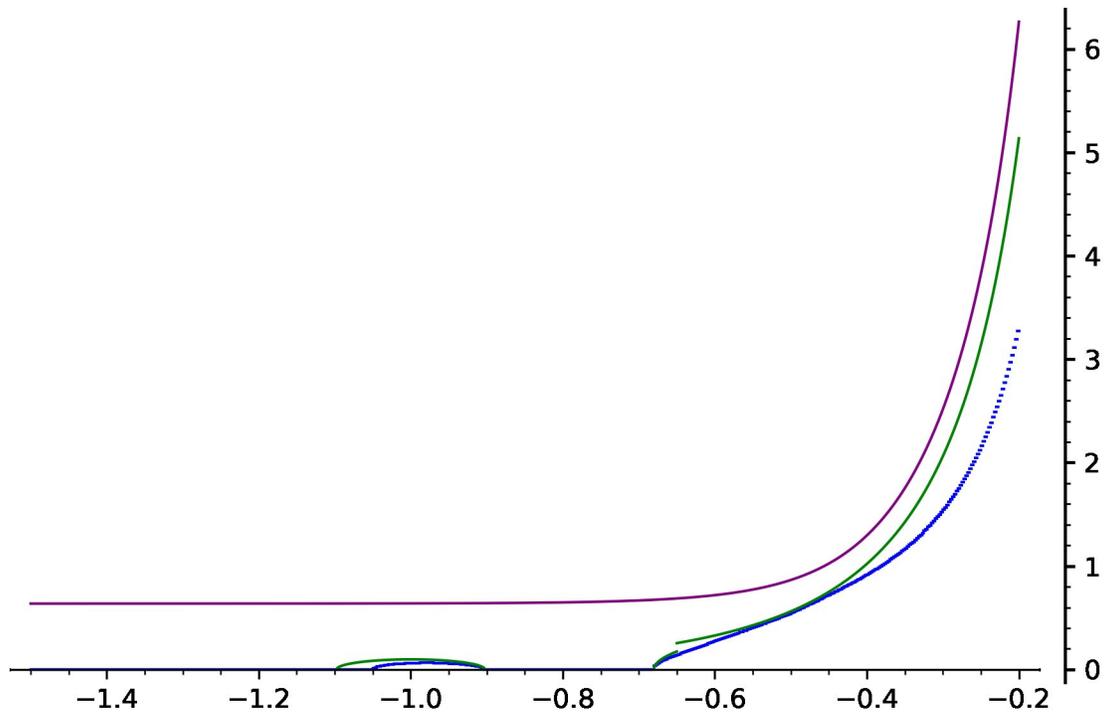


Fig. A.3. Comparison between Theorem 3.4.27 (purple), Remark A.0.7 (green) and the piece-wise curve found with the methods of this section (blue).

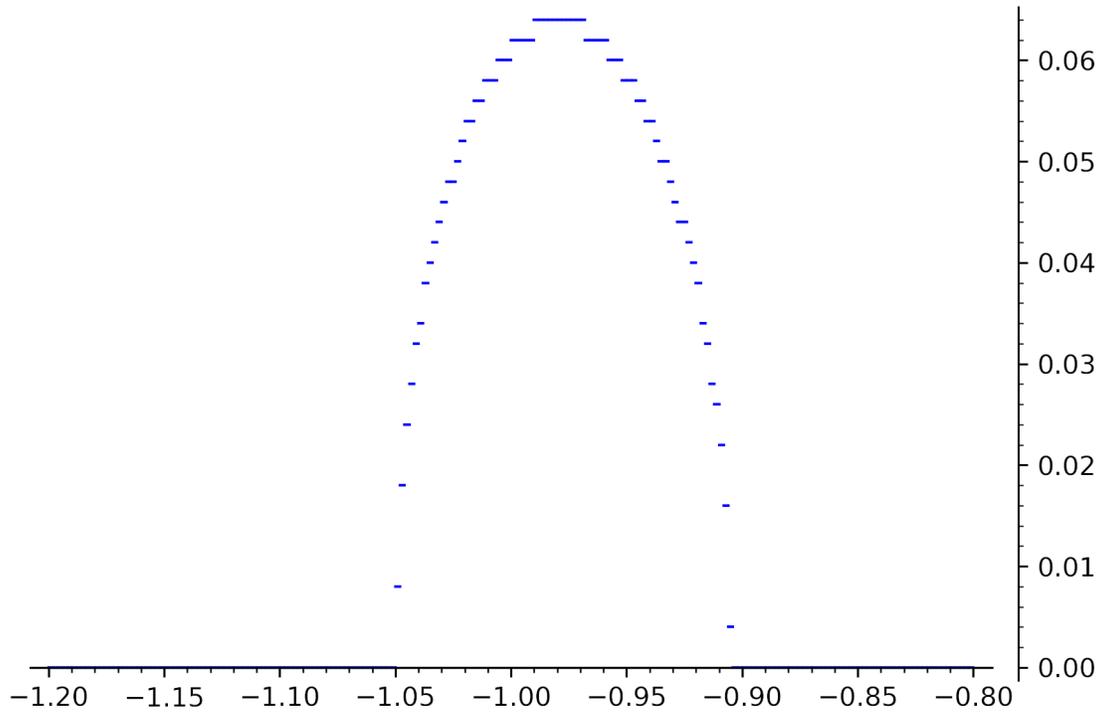


Fig. A.4. Computer assisted boundary for the interval $[-1.2, -0.8]$. Everything above the blue line is Northcott.

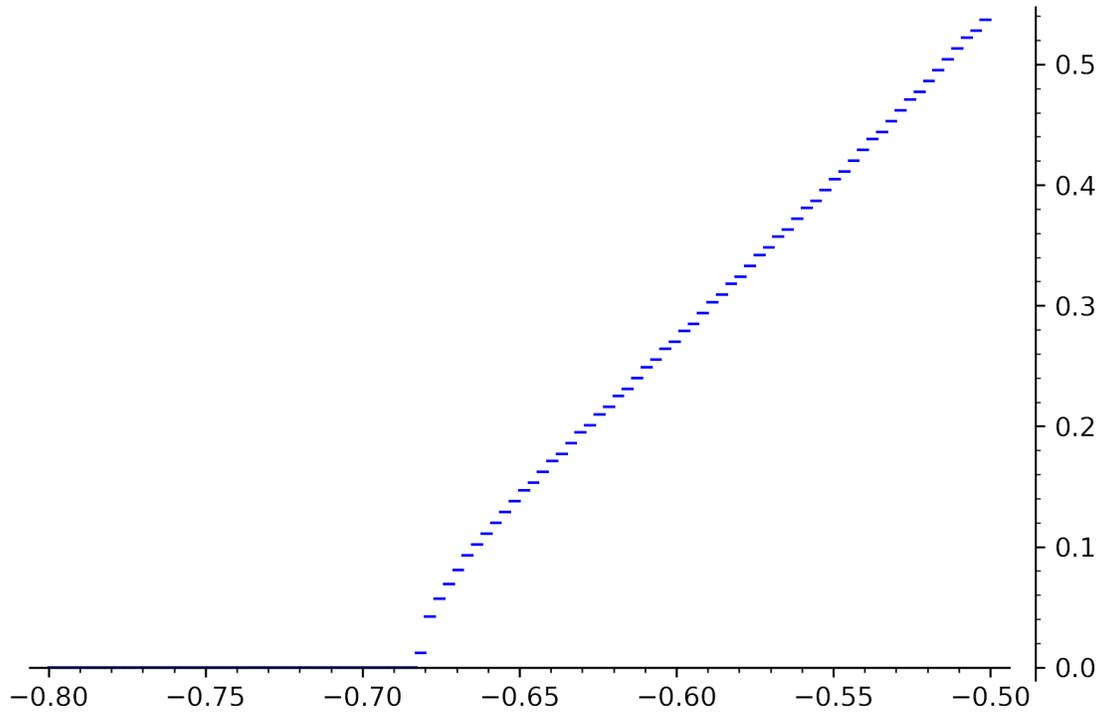


Fig. A.5. Computer assisted boundary for the interval $[-0.8, -0.5]$. Everything above the blue line is Northcott.

Conclusion

Ce mémoire présentait deux articles traitant de la Propriété de Northcott de fonctions zêta. Notre objectif principal était de déterminer pour quels points s du plan complexe uniquement un nombre fini de fonctions appartenant à la famille des fonctions zêta de Dedekind ou des fonctions zêta sur les corps de fonctions étaient bornés. Pour ce faire, nous avons utilisé une grande variété de résultats sur les corps de fonctions et les corps de nombres.

La présence des zéros triviaux de la fonction zêta de Dedekind étant une cause principale des différences entre les résultats du Chapitre 2 et 3, une étude plus approfondie sur les facteurs Γ nous fit remettre en question si les deux familles de fonctions zêta, c'est à dire la fonction de zêta de Dedekind et la fonction zêta de la Définition 1.2.23, sont les bons analogues sur les corps de nombres et les corps de fonctions. Cette différence nous poussa à considérer d'autres définitions de fonctions zêta (introduites aux Sections 1.3.2 et 1.3.3) avec comme but d'établir une comparaison fiable entre les deux familles. Il serait intéressant d'étudier la question de la propriété de Northcott sur ces familles de fonctions zêta dans le but de les comparer avec les résultats obtenus dans ce mémoire. Le fruit de ce projet nous permettrait de vérifier si les différences entre la réponse à la propriété de Northcott sur les corps de fonctions et celle sur les corps de nombres proviennent du fait qu'ils possèdent des différences intrinsèques ou de la définition de leur fonction zêta.

Références bibliographiques

- [1] *NIST Digital Library of Mathematical Functions*. F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller, B. V. Saunders, H. S. Cohl, and M. A. McClain, eds.
- [2] Milton Abramowitz and Irene A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, National Bureau of Standards Applied Mathematics Series, U. S. Government Printing Office, Washington, D.C., 1964. For sale by the Superintendent of Documents. MR0167642
- [3] Shabnam Akhtari and Jeffrey D. Vaaler, *Heights, regulators and schinzel's determinant inequality*, *Acta Arith.* **172** (2016), no. 3, 285–298. MR3460817
- [4] J. C. Andrade and J. P. Keating, *Conjectures for the integral moments and ratios of L -functions over function fields*, *J. Number Theory* **142** (2014), 102–148.
- [5] Julio Andrade, *A note on the mean value of L -functions in function fields*, *Int. J. Number Theory* **8** (2012), no. 7, 1725–1740.
- [6] Enrico Bombieri and Umberto Zannier, *A note on heights in certain infinite extensions of \mathbb{Q}* , *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **12** (2001), 5–14 (2002). MR1898444
- [7] Nicolas Bourbaki, *Éléments d'histoire des mathématiques*, Masson, Paris, 1984 (French). Reprints of the historical notes from the *Éléments*. MR782480
- [8] Juliette Bruce and Wanlin Li, *Effective bounds on the dimensions of jacobians covering abelian varieties*, *Proc. Amer. Math. Soc.* **148** (2020), no. 2, 535–551.
- [9] H. M. Bui and Alexandra Florea, *Zeros of quadratic dirichlet L -functions in the hyperelliptic ensemble*, *Trans. Amer. Math. Soc.* **370** (2018), no. 11, 8013–8045.
- [10] Hung M. Bui, Alexandra Florea, and Jonathan P. Keating, *The ratios conjecture and upper bounds for negative moments of L -functions over function fields*, arXiv:2109.1039.
- [11] S. Checcoli and A. Fehm, *On the northcott property and local degrees*, *Proc. Amer. Math. Soc.* **149** (2021), no. 6, 2403–2414. MR4246793
- [12] S. Chowla, *Improvement of a theorem of linnik and walfisz*, *Proc. London Math. Soc. (2)* **50** (1949), 423–429. MR27302
- [13] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubinstein, and N. C. Snaith, *Integral moments of L -functions*, *Proc. London Math. Soc. (3)* **91** (2005), no. 1, 33–104. MR2149530
- [14] Jean-Marc Couveignes, *Short models of global fields*.
- [15] A. J. de Jong and N. M. Katz, *Counting the number of curves over a finite field*.

- [16] David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236
- [17] Dmitry Faifman and Zeév Rudnick, *Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field*, *Compos. Math.* **146** (2010), no. 1, 81–101.
- [18] Ravi Ramakrishna Farshid Hajir Christian Maire, *Cutting towers of number fields*, *Ann. Math. Qué.* **45** (2021), no. 2, 321–345. MR4308183
- [19] O. Gabber, *On space filling curves and albanese varieties*, *Geom. Funct. Anal.* **11** (2001), no. 6, 1192–1200.
- [20] Xavier G en ereux, Matilde Lal ın, and Wanlin Li, *On the northcott property of zeta functions over function fields*, *Finite Fields Appl.* **83** (2022), Paper No. 102080. MR4444425
- [21] Andrew Granville, *Rational and integral points on curves*, 2022. Notes pour le cours de courbes elliptiques de l’Universit e de Montr eal en hiver 2022.
- [22] Xavier G en ereux and Matilde Lal ın, *The-northcott-property-of-dedekind-zeta-functions*, 2022. <https://github.com/Louddy/-The-northcott-property-of-dedekind-zeta-functions>.
- [23] Farshid Hajir and Christian Maire, *Tamely ramified towers and discriminant bounds for number fields*, *Compositio Math.* **128** (2001), no. 1, 35–53. MR1847664
- [24] Jonathan P. Keating Hung M. Bui Alexandra Florea, *The ratios conjecture and upper bounds for negative moments of L-functions over function fields*, arXiv:2109.1039.
- [25] Kenkichi Iwasawa, *Letter to j. dieudonn e*, *Zeta functions in geometry*, 1992, pp. 445–450. MR1210798
- [26] Dimitris Koukoulopoulos, *The distribution of prime numbers*, *Graduate Studies in Mathematics*, vol. 203, American Mathematical Society, Providence, RI, [2019]  2019. MR3971232
- [27] ———, *Alg ebre 2*, 2020. Notes pour le cours d’introduction   la th orie des anneaux et des modules de l’Universit e de Montr eal.
- [28] Youness Lamzouri, *On the distribution of extreme values of zeta and L-functions in the strip $\{\frac{1}{2} < \sigma < 1\}$* , *Int. Math. Res. Not. IMRN* **23** (2011), 5449–5503. MR2855075
- [29] ———, *On the distribution of extreme values of zeta and L-functions in the strip $\{\frac{1}{2} < \sigma < 1\}$* , *Int. Math. Res. Not. IMRN* **23** (2011), 5449–5503. MR2855075
- [30] Serge Lang, *Algebraic number theory*, 2nd ed., *Graduate Texts in Mathematics*, vol. 110, Springer-Verlag, New York, 1994. MR1282723
- [31] Wanlin Li, *Vanishing of hyperelliptic L-functions at the central point*, *J. Number Theory* **191** (2018), 85–103.
- [32] ———, *Vanishing of hyperelliptic L-functions at the central point*, *J. Number Theory* **191** (2018), 85–103.
- [33] Michael Lipnowski and Jacob Tsimerman, *How large is $a_g(\mathbb{F}_q)$?*, *Duke Math. J.* **167** (2018), no. 18, 3403–3453.
- [34] Allysa Lumley, *Complex moments and the distribution of values of $l(1, \chi_d)$ over function fields with applications to class numbers*, *Mathematika* **65** (2019), no. 2, 236–271.
- [35] ———, *Complex moments and the distribution of values of $l(1, \chi_d)$ over function fields with applications to class numbers*, *Mathematika* **65** (2019), no. 2, 236–271.

- [36] ———, *Moments and distribution of values for L-functions over function fields inside the critical strip*, Acta Arith. **201** (2021), no. 4, 329–369.
- [37] ———, *Moments and distribution of values for L-functions over function fields inside the critical strip*, Acta Arith. **201** (2021), no. 4, 329–369.
- [38] Daniel A. Marcus, *Number fields*, Universitext, Springer, Cham, 2018. Second edition of [MR0457396]; With a foreword by Barry Mazur. MR3822326
- [39] Jacques Martinet, *Tours de corps de classes et estimations de discriminants*, Invent. Math. **44** (1978), no. 1, 65–73. MR460281
- [40] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, 2007. MR2378655
- [41] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder. MR1697859
- [42] D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. **45** (1949), 502–509. MR33094
- [43] A. M. Odlyzko, *Some analytic estimates of class numbers and discriminants*, Invent. Math. **29** (1975), no. 3, 275–286. MR376613
- [44] ———, *Lower bounds for discriminants of number fields*, Acta Arith. **29** (1976), no. 3, 275–297. MR401704
- [45] ———, *Lower bounds for discriminants of number fields. II*, Tôhoku Math. J. **29** (1977), no. 2, 209–216. MR441918
- [46] ———, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: A survey of recent results*, Sémin. Théor. Nombres Bordeaux (2) **2** (1990), no. 1, 119–141. MR1061762
- [47] Fabien Pazuki and Riccardo Pengo, *On the northcott property for special values of L-functions*, arXiv:2012.00542.
- [48] Georges Poitou, *Minorations de discriminants (d’après A. M. Odlyzko)*, Séminaire Bourbaki, Vol. 1975/76 28ème année, exp. No. 479, 1977, pp. 136–153. Lecture Notes in Math., Vol. 567. MR0435033
- [49] Bjorn Poonen, *Gonality of modular curves in characteristic p* , Math. Res. Lett. **14** (2007), no. 4, 691–701.
- [50] Guy Robin, *Estimation de la fonction de tchebychef θ sur le k -ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n* , Acta Arith. **42** (1983), no. 4, 367–389.
- [51] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657
- [52] Friedrich Karl Schmidt, *Analytische zahlentheorie in körpern der charakteristik pp* , Math. Z. **33** (1931), no. 1, 1–32 (German). MR1545199
- [53] Jean-Pierre Serre, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)* (1970), 15.

- [54] ———, *Minorations de discriminants, note of october 1975, œuvres. Vol. III*, Springer-Verlag, Berlin, 1986. 1972–1984. MR926691
- [55] Keiju Sono, *The second moment of quadratic dirichlet L-functions*, J. Number Theory **206** (2020), 194–230. MR4013170
- [56] H. M. Stark, *Some effective cases of the brauer-siegel theorem*, Invent. Math. **23** (1974), 135–152. MR342472
- [57] Henning Stichtenoth, *Algebraic function fields and codes*, Second, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.
- [58] The Sage Developers, *Sagemath, the sage mathematics software system (version 9.3)*, 2022. <https://www.sagemath.org>.
- [59] Gerard van der Geer and René Schoof, *Effectivity of arakelov divisors and the theta divisor of a number field*, Selecta Math. (N.S.) **6** (2000), no. 4, 377–398. MR1847381
- [60] Matthew P. Young, *The first moment of quadratic Dirichlet L-functions*, Acta Arith. **138** (2009), no. 1, 73–99. MR2529465
- [61] ———, *The third moment of quadratic Dirichlet L-functions*, Selecta Math. (N.S.) **19** (2013), no. 2, 509–543. MR3090236