ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

Η ειδική περίπτωση Kummer του Τελευταίου Θεωρήματος του Fermat

της Ιωάννας Βουλκούδη

Επιβλέπουσα: Σοφία Λαμπροπούλου

Συνεπιβλέπων: Αριστείδης Κοντογεώργης

Ιούνιος 2019

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

Η ειδική περίπτωση Kummer του Τελευταίου Θεωρήματος του Fermat

της Ιωάννας Βουλκούδη

Επιβλέπουσα: Σοφία Λαμπροπούλου, Καθηγήτρια Σ.Ε.Μ.Φ.Ε. ΕΜΠ

Συνεπιβλέπων: Αριστείδης Κοντογεώργης, Καθηγητής Μαθηματικού Τμήματος, Ε.Κ.Π.Α.[1]

Εγκρίθηκε από την τριμελή επιτροπή:

Σοφία Λαμπροπούλου, Καθηγήτρια Σ.Ε.Μ.Φ.Ε. ΕΜΠ ____________________

Παναγιώτης Ψαρράκος, Καθηγητής Σ.Ε.Μ.Φ.Ε. ΕΜΠ ____________________

Δημήτριος Κοντοκώστας, Επ. Καθηγητής Σ.Ε.Μ.Φ.Ε. ΕΜΠ ____________________

[1] Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Ιωάννα Βουλκούδη, ______________________________

Τα συμπεράσματα που παρουσιάζονται αντιστοιχούν σε προσωπική στάση και δεν θα έπρεπε να θεωρηθεί πως εκπροσωπούν την επίσημη στάση του ιδρύματος.

Abstract in English

The path towards proving Fermat's Last Theorem led to the introduction of Algebraic Numbers and Algebraic Number Theory, as they are known today. We unfold the theory until the critical point of Kummer's contribution to Fermat's Last Theorem. In the first two Chapters 1, 2, we give some basic definitions of algebraic numbers and algebraic integers and we present the results which helped to produce new algebraic integers out of known ones. The main result is that every number field K can be expressed as $K = \mathbb{Q}(\theta)$, for some algebraic integer θ. Then, we focus on quadratic and cyclotomic fields. In particular, the cyclotomic fields are related to many results in Number Theory, including the introduction of ideal numbers by Kummer. The important step of unique factorization is introduced in Chapter 3. Namely, in Chapter 3 we discuss an early misunderstanding among mathematicians about the definition of prime numbers. Additionally, we explain how the misunderstanding was fixed, when proper definitions of primes and irreducible elements in a domain D were provided. Furthermore, Unique Factorization Domains (UFDs) are defined and examples of UFDs are provided. Chapter 4 explains how the absence of unique factorization in every ring of integers, motivated Kummer to introduce *ideal numbers.* Later Dedekind, influenced by Kummer, developed the theory of *ideals* in ring theory. The term *Dedekind ring* is presented along with the work that led to the proof that factorization is unique in them. The most important result of Dedekind's theory of ideals is theorem 4.6, which states that factorization into irreducibles is unique for elements of a ring of integers $\mathfrak{O}$, if and only if every ideal is principal. This theorem demonstrates the strong relationship between ideals and unique factorization. Chapter 5 discusses how geometric representation of algebraic numbers provides a result, which can be used as a measure of non-uniqueness of factorization. In Chapter 6 we provide proofs of special cases of FLT for $n = 4$ and $n = 3$, as they were given by Fermat and Euler respectively. We also present the Sophie Germain Theorem for infinitely many prime exponents. Finally, the last Chapter 7 is devoted to Kummer's proof, which has been the main target of this thesis all along.

Περίληψη στα Ελληνικά

Η προσπάϑεια να αποδειχϑεί το Τελευταίο Θεώρημα του Fermat οδήγησε στην ανάπτυξη της Αλγεβρικής Θεωρίας Αριϑμών, όπως την γνωρίζουμε σήμερα. Θα ακολουϑήσουμε την πορεία αυτής της ανάπτυξης, έως το κρίσιμο σημείο της απόδειξης της ειδικής περίπτωσης Kummer. Στα δύο πρώτα Κεφάλαια 1, 2 δίνονται οι ορισμοί των αλγεβρικών αριϑμών και των ακέραιων αλγεβρικών και παρουσιάζονται σχετικά αποτελέσματα. Το βασικό αποτέλεσμα του Κεφαλαίου 2 είναι το πόρισμα 2.1, σύμφωνα με το οποίο κάϑε σώμα αριϑμών μπορεί να γραφεί ως το σώμα των ρητών αριϑμών με επισύναψη ενός ακέραιου αλγεβρικού. Έπειτα επικεντρωνόμαστε στα τετραγωνικά και κυκλοτομικά σώματα. Ιδιαίτερα τα τελευταία σχετίζονται με πολλά αποτελέσματα στη Θεωρία Αριϑμών, αλλά και με την εισαγωγή των *ιδεωδών αριϑμών* από τον Kummer. Στο Κεφάλαιο 3, μελετάται η σημαντική ιδιότητα της παραγοντοποίησης και πότε αυτή είναι μοναδική. Δίνονται δύο ορισμοί του πρώτου αρϑμού, αναλύεται η παρανόηση των μαϑηματικών σχετικά με τους δύο ορισμούς, πώς ανακαλύφϑηκε και πώς αντιμετωπίστηκε. Δίνονται έγκυροι ορισμοί του ανάγωγου στοιχείου και του πρώτου σε μία ακέραια περιοχή D. Ορίζονται οι Περιοχές Μοναδικής Αναπαράστασης (UFD) και δίνονται παραδείγματα αυτών. Το Κεφάλαιο 4 περιγράφει πώς η έλλειψη μοναδικής παραγοντοποίησης σε κάϑε δακτύλιο ακεραίων κινητοποίησε τον Kummer να δημιουργήσει τους *ιδεώδεις αριϑμούς*. Έπειτα, ο Dedekind επηρεασμένος από τον Kummer, ανέπτυξε τη ϑεωρία των *ιδεωδών* στη ϑεωρία δακτυλίων. Το πιο σημαντικό αποτέλεσμα της ϑεωρίας των *ιδεωδών* που ανέπτυξε ο Dedekind είναι το ϑεώρημα 4.6 σύμφωνα με το οποίο η παραγοντοποίηση των στοιχείων ενός δακτυλίου ακεραίων $\mathfrak{O}$ σε ανάγωγα στοιχεία είναι μοναδική, αν και μόνον αν κάϑε ιδεώδες είναι κύριο. Το παραπάνω ϑεώρημα δείχνει την στενή σχέση μεταξύ των ιδεωδών και της μοναδικής παραγοντοποίησης. Στο Κεφάλαιο 5 παρουσιάζεται *η ομάδα κλάσης* και *ο αριϑμός κλάσης* και δίνεται ένα αποτέλεσμα, με το οποίο μπορούμε να «μετρήσουμε» κατά κάποιο τρόπο τη μη-μοναδικότητα της παραγοντοποίησης. Στο Κεφάλαιο 6 δίνονται οι αποδείξεις των ειδικών περιπτώσεων του Τελευταίου Θεωρήματος του Fermat για τους εκϑέτες $n = 4$, $n = 3$, όπως έχουν δοϑεί από τον Fermat και τον Euler αντίστοιχα. Ακόμη παρουσιάζεται το Θεώρημα της Sophie Germain. Τέλος, το Κεφάλαιο 7 είναι αφιερωμένο στην απόδειξη του Θεωρήματος του Kummer, η οποία άλλωστε υπήρξε και ο βασικός στόχος αυτής της εργασίας. Για ελληνική βιβλιογραφία, παραπέμπουμε τον αναγνώστη στην αναφορά [20].

Εκτεταμένη περίληψη στα Ελληνικά

Η προσπάθεια να αποδειχθεί το Τελευταίο Θεώρημα του Fermat οδήγησε στην ανάπτυξη της Αλγεβρικής θεωρίας Αριθμών, όπως την γνωρίζουμε σήμερα. Σε αυτήν την εργασία θα ακολουθήσουμε την πορεία αυτής της ανάπτυξης, έως το κρίσιμο σημείο της απόδειξης της ειδικής περίπτωσης Kummer.

Στο πρώτο Κεφάλαιο 1 ορίζονται οι αλγεβρικοί αριθμοί και σύμφωνα με το πόρισμα 2.1 αποδεικνύεται πως κάθε αλγεβρικό σώμα αριθμών μπορεί να γραφεί ως το σώμα των ρητών αριθμών στο οποίο έχουμε επισυνάψει έναν αλγεβρικό αριθμό. Το σώμα των αλγεβρικών αριθμών συμβολίζεται με $\mathbb{A}$ και αποτελεί υπόσωμα του σώματος των μιγαδικών αριθμών $\mathbb{C}$.

Στο Κεφάλαιο 2 δίνεται ο ορισμός του ακέραιου αλγεβρικού αριθμού. Οι ακέραιοι αλγεβρικοί αριθμοί σχηματίζουν έναν υποδακτύλιο του σώματος των αλγεβρικών αριθμών $\mathbb{A}$ και το σύνολό τους συμβολίζεται με $\mathbb{B}$. Παρουσιάζονται δύο αποτελέσματα που οδηγούν στην δημιουργία νέων ακέραιων αλγεβρικών από γνωστούς. Συγκεκριμένα, το γεγονός ότι το $\mathbb{B}$ είναι υποδακτύλιος του $\mathbb{A}$ μας επιτρέπει να βρούμε καινούριους ακέραιους αλγεβρικούς αριθμούς. Επίσης εάν ένας μιγαδικός αριθμός είναι λύση ενός μονικού πολυωνύμου, του οποίου οι συντελεστές περιέχονται στο σώμα $\mathbb{B}$, τότε αυτός ο μιγαδικός αριθμός είναι ακέραιος αλγεβρικός. Ένα σημαντικό αποτέλεσμα του Κεφαλαίου 2 είναι το πόρισμα 2.1, σύμφωνα με το οποίο κάθε σώμα αριθμών μπορεί να γραφεί ως το σώμα των ρητών αριθμών με επισύναψη ενός ακέραιου αλγεβρικού αριθμού. Επισημαίνεται ότι κάθε αλγεβρικό σώμα αριθμών έχει έναν δακτύλιο ακεραίων $\mathfrak{O}$, ο οποίος αποτελεί την τομή του αλγεβρικού σώματος με τον υποδακτύλιο $\mathbb{B}$. Επιπλέον, δίνεται ένα κριτήριο με το οποίο ελέγχουμε εάν ένας αλγεβρικός αριθμός είναι ακέραιος αλγεβρικός ή όχι. Έπειτα επικεντρωνόμαστε στα τετραγωνικά και κυκλοτομικά σώματα, τα οποία σχετίζονται με πολλά αποτελέσματα στη Θεωρία Αριθμών. Ιδιαίτερα τα κυκλοτομικά σώματα σχετίζονται μεταξύ άλλων και με την εισαγωγή των *ιδεωδών αριθμών* από τον Kummer. Αποδεικνύεται πως ένα αλγεβρικό σώμα αριθμών είναι τετραγωνικό, αν και μόνον αν ισούται με το σώμα των ρητών στο οποίο έχουμε επισυνάψει την τετραγωνική ρίζα ενός ελεύθερου τετραγώνου (squarefree) ακεραίου και υπολογίζεται ο δακτύλιος των ακεραίων των τετραγωνικών σωμάτων. Δίνεται ο ορισμός 2.9, σύμφωνα με τον οποίο τα κυκλοτομικά σώματα γράφονται ως $\mathbb{Q}(\zeta)$, όπου $\zeta = e^{2pii/n}$ είναι η πρωταρχική ρίζα της μονάδας. Υπολογίζεται η νόρμα και το ίχνος της πρωταρχικής ρίζας της μονάδας και σημειώνεται ο δακτύλιος των κυκλοτομικών σωμάτων, ο οποίος ισούται με $\mathbb{Z}[\zeta]$.

Στο Κεφάλαιο 3, μελετάται η σημαντική ιδιότητα της παραγοντοποίησης και πότε αυτή είναι μοναδική. Δίνουμε δύο ορισμούς του πρώτου αριθμού, οι οποίοι είναι μεν ισοδύναμοι στο σώμα των ακεραίων $\mathbb{Z}$, αλλά όχι σε κάθε δακτύλιο ακεραίων $\mathfrak{O}$. Σύμφωνα με τον πρώτο ορισμό 3.1, ένας αριθμός p λέγεται πρώτος εάν $p = ab \Rightarrow$ ο a ή ο b είναι *μονάδα*. Ο δεύτερος ορισμός 3.2 δηλώνει ότι πρώτος λέγεται ένας αριθμός p, όταν $p|ab \Rightarrow p|a$ ή $p|b$. Στην αρχή της ανάπτυξης της Αλγεβρικής Θεωρίας Αριθμών, οι μαθηματικοί, ανάμεσά τους και ο σπουδαίος Euler, απέτυχαν να κατανοήσουν πως οι δύο ορισμοί δεν είναι ισοδύναμοι σε κάθε δακτύλιο ακεραίων $\mathfrak{O}$. Αυτό είχε ως αποτέλεσμα να παρανοήσουν και την έννοια της παραγοντοποίησης. Η μοναδική παραγοντοποίηση σε πρώτους αριθμούς θεωρήθηκε δεδομένη αλλά οι πρώτοι αριθμοί είχαν οριστεί λανθασμένα. Αναφέρονται κάποια παραδείγματα όπου φαίνεται ετούτη η παρανόηση των μαθηματικών. Ο Euler έδωσε την απόδειξη του Τελευταίου Θεωρήματος του Fermat για εκθέτη ίσο με 3, έχοντας παραλείψει να αποδείξει τη μοναδική παραγοντοποίηση στον δακτύλιο όπου εργαζόταν. Επίσης ο Lamé ανακοίνωσε πως απέδειξε το Τελευταίο Θεώρημα του Fermat, λαμβάνοντας τη μοναδική παραγοντοποίηση ως δεδομένη. Φυσικά η απόδειξη που έδωσε ήταν λάθος. Κατόπιν, παρατηρούμε πως αρχίζει να γίνεται κατανοητό το λάθος από κάποιους μαθηματικούς. Για παράδειγμα, ο Gauss απέδειξε ότι στους λεγόμενους Γκαουσιανούς ακεραίους $\mathbb{Z}[i]$ η παραγοντοποίηση είναι μοναδική. Ο Kummer απέδειξε πως η μοναδική παραγοντοποίηση αποτυγχάνει όταν παραγοντοποιούμε κυκλοτομικούς ακεραίους. Ακόμη, ο Eisenstein φαίνεται να έχει κατανοήσει την ανάγκη να ελέγχεται η μοναδική παραγοντοποίηση και όχι να λαμβάνεται ως δεδομένη σε κάθε δακτύλιο ακεραίων. Προς την αποκατάσταση της αλήθειας δόθηκαν νέοι ορισμοί. Ο νέος έγκυρος ορισμός των πρώτων ισχυρίζεται ότι ένα στοιχείο p το οποίο ανήκει σε μία ακέραια περιοχή D λέγεται πρώτος εάν $p|ab \Rightarrow p|a$ ή $p|b$. Επιπλέον, με τον ορισμό 3.3 εισήχθηκε η έννοια του ανάγωγου στοιχείου σε μία ακέραια περιοχή D. Ένας στοιχείο p το οποίο ανήκει σε μία ακέραια περιοχή D λέγεται ανάγωγο εάν $p = ab \Rightarrow$ ο a ή ο b είναι μονάδα. Η ιδιότητα του πρώτου είναι πιο ισχυρή από αυτήν του ανάγωγου στοιχείου. Μάλιστα, όταν ένα στοιχείο σε μία ακέραια περιοχή D είναι πρώτος, τότε είναι και ανάγωγο στοιχείο, ενώ το αντίστροφο δεν ισχύει. Η παραγοντοποίηση σε πρώτους, όταν είναι δυνατή είναι μοναδική. Η παραγοντοποίηση σε ανάγωγα στοιχεία δεν είναι πάντα μοναδική. Οπότε έχει ενδιαφέρον να ασχοληθούμε με την παραγοντοποίηση σε ανάγωγα στοιχεία. Η παρανόηση έχει πλέον ξεκαθαρίσει. Σημαντικότατο αποτέλεσμα είναι το θεώρημα 3.3 που δηλώνει ότι σε μία ακέραια περιοχή D η παραγοντοποίηση σε ανάγωγα στοιχεία, όταν είναι δυνατή, είναι μοναδική, αν και μόνον αν κάθε ανάγωγο στοιχείο είναι και πρώτος. Επιπλέον, ορίζονται οι Περιοχές Μοναδικής Αναπαράστασης (ΠΜΑ/ UFD), στις οποίες η παραγονοποίηση σε ανάγωγα στοιχεία είναι μοναδική. Σύμφωνα με τα παραπάνω, σε μια ΠΜΑ κάθε ανάγωγο στοιχείο είναι και πρώτος. Παραδείγματα ΠΜΑ είναι οι Ευκλείδιες Περιοχές και οι Περιοχές Κύριων Ιδεωδών (Principal Ideal Domain).

Η έλλειψη μοναδικής παραγοντοποίησης σε ανάγωγα στοιχεία σε κάθε ακέραια περιοχή υπήρξε ιδιαιτέρως απογοητευτική για τους μαθηματικούς, καθώς τους απομάκρυνε ακόμη περισσότερο από την πολυπόθητη απόδειξη του Τελευταίου Θεωρήματος του Fermat. Στο κεφάλαιο 4 θα παρουσιάσουμε πώς η έλλειψη μοναδικής παραγοντοποίησης κινητοποίησε την περαιτέρω εξέλιξη της Αλγεβρικής Θεωρίας Αριθμών. Με αφορμή την έλλειψη μοναδικής παραγοντοποίησης σε κάθε δακτύλιο ακεραίων, ο Kummer και αργότερα ο Dedekind, επηρεασμένος από τη δουλεία του προηγούμενου ανέπτυξαν σημαντικές θεωρίες. Η ιδέα του Kummer ήταν να επεκταθεί ο δακτύλιος στον οποίο δεν παραγοντοποιείται κάποιο στοιχείο μοναδικά, με τέτοιον τρόπο ώστε να εξασφαλίζεται η μοναδική παραγοντοποίηση του εν λόγω στοιχείου στον εκτεταμένο δακτύλιο. Για να εφαρμόσει την ιδέα του, ο Kummer εισήγαγε την έννοια του *ιδεώδους αριθμού*, με την οποία δεν θα ασχοληθούμε σε αυτό το κείμενο. Για περαιτέρω μελέτη σχετικά με τη θεωρία που ανέπτυξε ο Kummer, παραπέμπουμε τον αναγνώστη στις αναφορες [4] και [3]. Επηρεασμένος από τους *ιδεώδεις αριθμούς* του Kummer, ο Dedekind ανέπτυξε την θεωρία των *ιδεωδών*, όπως είναι γνωστή σήμερα στη θεωρία δακτυλίων. Η προσέγγιση του Dedekind είναι πολύ πιο κοντά στη σύγχρονη θεωρία. Στον ορισμό 4.7 ορίζεται ο *δακτύλιος Dedekind* και παρουσιάζεται η πορεία που οδήγησε ο Dedekind προς την απόδειξη ότι η παραγοντοποίηση είναι μοναδική στους εν λόγω δακτυλίους. Το πιο σημαντικό αποτέλεσμα της θεωρίας των *ιδεωδών* που ανέπτυξε ο Dedekind είναι το θεώρημα 4.6 σύμφωνα με το οποίο η παραγοντοποίηση των στοιχείων ενός δακτυλίου ακεραίων $\mathfrak{O}$ σε ανάγωγα στοιχεία είναι μοναδική, αν και μόνον αν κάθε ιδεώδες είναι κύριο. Στο παραπάνω θεώρημα φαίνεται η στενή σχέση μεταξύ των ιδεωδών και της μοναδικής παραγοντοποίησης σε ανάγωγα στοιχεία.

Στο Κεφάλαιο 5 αναλύουμε την γεωμετρική αναπαράσταση των αλγεβρικών αριθμών. Ορίζουμε την έννοια του lattice στο $\mathbb{R}^n$, επίσης τους μονομορφισμούς από ένα αλγεβρικό σώμα αριθμών στο σώμα των μιγαδικών αριθμών και ιδιότητες αυτών. Προκειμένου να «μετρηθεί» κατά κάποιο τρόπο η έλλειψη μοναδικής παραγοντοποίησης, μέσω των ορισμών 5.3 και 5.4 παρουσιάζεται *η ομάδα κλάσης* των ιδεωδών σε ένα αλγεβρικό σώμα και *ο αριθμός κλάσης*. Η ομάδα κλάσης ορίζεται ως η ομάδα-πηλίκο των κλασματικών ιδεωδών ενός δακτυλίου ακεραίων ενός αλγεβρικού σώματος K ως προς την υποομάδα των κύριων ιδεωδών του. Ο αριθμός κλάσης ορίζεται ως η τάξη της αντίστοιχης ομάδας κλάσης, η οποία είναι πάντα πεπερασμένη. Παρουσιάζεται το θεώρημα 5.2, σύμφωνα με το οποίο η παραγοντοποίηση σε έναν δακτύλιο ακεραίων είναι μοναδική, αν και μόνον αν ο αριθμός των κλάσεων ισούται με τη μονάδα. Μάλιστα όσο μεγαλύτερος είναι ο αριθμός κλάσης τόσο πιο πολύπλοκη γίνεται η μη μοναδικότητα της παραγοντοποίησης. Ο Gauss είχε δώσει διάφορες εικασίες σχετικά με τον αριθμό των κλάσεων. Συγκεκριμένα θεωρούσε ότι σε ένα τετραγωνικό σώμα $K = \mathbb{Q}(\sqrt{d})$, ο αριθμός κλασης μεγαλώνει $h(d) \to \infty$, όσο ο ακέραιος d μικραίνει, $d \to -\infty$. Η εικασία αυτή αποδείχθηκε αργότερα από τον Heilbronn. Επίσης ο Gauss ασχολήθηκε με το πρόβλημα της εύρεσης κάθε τετραγωνικού σώματος με συγκεκριμένο αριθμό κλάσης. Το Gauss Class Number One Problem είναι η αναζήτηση κάθε τετραγωνικού σώματος με αριθμό κλάσης ίσο με 1. Σύμφωνα με το θεώρημα 5.10 των Baker, Heegner, Stark ο αριθμός

κλάσης των τετραγωνικών σωμάτων $K = \mathbb{Q}(\sqrt{d})$ ισοδυναμεί με 1 αν και μόνον αν το d παίρνει τις εξής εννέα τιμές:
$-1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163.$ Αργότερα δίνεται το θεώρημα 5.11 από τους Goldfeld, Gross, Zagier, σύμφωνα με το οποίο ο αριθμός κλάσης ευρίσκεται από συγκεκριμένη σχέση. Η μέθοδος που χρησιμοποιήθηκε για την απόδειξη του θεωρήματος 5.11 σχετίζεται με ελλειπτικές καμπύλες.

Το Κεφάλαιο 6 αναφέρεται σε τρεις ειδικές περιπτώσεις του Τελευταίου Θεωρήματος του Fermat, οι οποίες αντιμετωπίστηκαν πριν την συνεισφορά του Kummer. Συγκρίνονται οι μέθοδοι που χρησιμοποιήθηκαν καθώς και το εύρος των αποτελεσμάτων. Στην πρώτη ενότητα 6.1, παρουσιάζεται η μοναδική απόδειξη που έχει γράψει ο Fermat. Ο Fermat αποδεικνύει το θεώρημα 6.1 από το οποίο προκύπτει άμεσα η απόδειξη του Τελευταίου Θεωρήματος του Fermat για εκθέτη ίσο με 4. Η εν λόγω απόδειξη δεν έχει δημοσιευτεί από τον ίδιο τον Fermat, αλλά από τον γιο του, μετά το θάνατό του. Στην απόδειξη χρησιμοποιείται η «μέθοδος της άπειρης καθόδου», την οποία εισήγαγε ο ίδιος ο Fermat. Σύμφωνα με την «μέθοδο της άπειρης καθόδου», υποθέτωντας ότι υπάρχει μία θετική ακέραια λύση μίας εξίσωσης, καταλήγουμε στην εύρεση μίας επιπλέον λύσης της ίδιας εξίσωσης, η οποία είναι μικρότερη από την πρώτη. Με αυτόν το τρόπο φτιάχνουμε μια συνεχώς φθίνουσα ακολουθία θετικών ακέραιων, το οποίο είναι αδύνατο. Στην επόμενη ενότητα 6.2, δίνεται η απόδειξη του Euler για το τελευταίο θεώρημα του Fermat όταν ο εκθέτης είναι ίσος με 3. Η απόδειξη του θεωρήματος 6.2, αν και σωστή, περιέχει μία σημαντική παράλειψη. Ο Euler, όπως αναφέραμε σε προηγούμενο κεφάλαιο, είχε πέσει στην παγίδα μαζί με άλλους μαθηματικούς της εποχής του, να θεωρήσει πως η μοναδική παραγοντοποίηση ισχύει σε κάθε δακτύλιο ακεραίων. Αν και περιέχει αυτό το σημαντικό λάθος, η απόδειξη που έδωσε ο Euler για την περίπτωση όπου ο εκθέτης ισούται με 3, είναι σωστή, διότι τυχαίνει ο δακτύλιος στον οποίο εργάζεται να είναι ΠΜΑ. Ο Euler χρησιμοποιεί επίσης τη «μέθοδο της άπειρης καθόδου» στη απόδειξή του. Παρακάτω, στην ενότητα 6.3 παρουσιάζουμε το Θεώρημα της Sophie Germain. Η δουλειά της Sophie Germain στη Θεωρία Αριθμών οδήγησε στην διχοτόμηση του Τελευταίου Θεωρήματος του Fermat σε δύο περιπτώσεις. Στην πρώτη περίπτωση ο εκθέτης δεν διαιρεί κανένα όρο της εξίσωσης $x^n + y^n = z^n$. Στην δεύτερη περίπτωση, ο εκθέτης διαιρεί ένα και μόνο ένα από τα $x,\ y,\ z$. Η Sophie Germain αποδεικνύει το Τελευταίο Θεώρημα του Fermat στην πρώτη περίπτωση, υπό κάποιες ειδικές υποθέσεις για τον εκθέτη, όπως περιγράφονται στο θεώρημα 6.3. Η διαφορά με τις προηγούμενες δύο περιπτώσεις βρίσκεται στο γεγονός ότι το Θεώρημα της Sophie Germain αποδεικνύει το Τελευταίο Θεώρημα του Fermat για άπειρα πολλούς πρώτους εκθέτες, ενώ οι προηγούμενες δύο περιπτώσεις παρείχαν απόδειξη περιορισμένη μόνο σε έναν εκθέτη. Παρόλαυτα το εύρος των αποτελεσμάτων του θεωρήματος της Sophie Germain περιορίζεται αρκετά εξαιτίας των υποθέσεων.

Το τελευταίο Κεφάλαιο 7, είναι αφιερωμένο στην απόδειξη του Kummer. Πριν δοθεί η απόδειξη, ορίζονται οι *κανονικοί (ή ομαλοί) πρώτοι αριθμοί*, τους οποίους εισήγαγε ο Kummer. Σύμφωνα με τον ορισμό 7.2, ένας κανονικός πρώτος είναι ένας πρώτος αριθμός, ο οποίος δεν διαιρεί τον αριθμό κλάσης $h(p)$ του κυκλοτομικού σώματος $\mathbb{Q}(\zeta)$, όπου $\zeta = e^{2pii/p}$ είναι μία πρωταρχική ρίζα της μονάδας. Ένας πρώτος αριθμός, ο οποίος δεν είναι κανονικός, λέγεται μη κανονικός πρώτος. Δίνεται ένα κριτήριο κανονικότητας από τον ίδιο τον Kummer, σύμφωνα με το οποίο ένας πρώτος αριθμός είναι κανονικός, αν και μόνον αν δεν διαιρεί τους αριθμητές των αριθμών Bernoulli B_2, $B_4, \cdots$, B_{p-3}. Χρησιμοποιώντας το παραπάνω κριτήριο, ο Kummer βρήκε τους 10 πρώτους μη κανονικούς πρώτους αριθμούς, οι οποίοι είναι οι εξής: 37, 59, 67, 101, 103, 131, 149, 157, 233, 257. Παρατηρούμε ότι οι κανονικοί πρώτοι, τουλάχιστον σε αυτό το μικρό δείγμα που παρουσιάζουμε παραπάνω, είναι περισσότεροι από τους μη κανονικούς. Σύμφωνα με μία εικασία που τέθηκε από τον Siegel και η οποία δεν έχει αποδειχθεί ακόμη, υπάρχουν άπειροι κανονικοί πρώτοι αριθμοί. Ενώ ο Jensen και αργότερα ο Carlitz απέδειξαν την ύπαρξη άπειρων μη κανονικών πρώτων. Για την απόδειξη του θεωρήματος του Kummer δίνονται τρία λήμματα, 7.1, 7.2 και το λήμμα του Kummer 7.3. Με το Θεώρημα του Kummer 7.1 αποδεικνύεται ότι για έναν περιττό κανονικό πρώτο αριθμό p, δεν υπάρχουν ακέραιοι αριθμοί x, y, z που να επιλύουν την εξίσωση $x^p + y^p = z^p$, τέτοιοι ώστε ο p να μην διαιρεί κανέναν από τους x, y, z. Σε αυτό το σημείο αξίζει να σημειωθεί ότι, ως συνέπεια των παρατηρήσεων (**Remarks**) στην αρχή του Κεφαλαίου 6.1, το Τελευταίο Θεώρημα του Fermat αρκεί να αποδειχθεί για εκθέτη n περιττό πρώτο αριθμό και για $n = 4$. Από την παραπάνω διαπίστωση, συμπεραίνουμε ότι το θεώρημα του Kummer αποτελεί σημαντικότατο αποτέλεσμα με μεγάλο εύρος. Η πλήρης απόδειξη του Θεωρήματος του Kummer δίνεται μέσα στο κείμενο. Η κατανόηση της απόδειξης του Θεωρήματος του Kummer 7.1 υπήρξε άλλωστε ο βασικός στόχος αυτής της εργασίας. Για ελληνική βιβλιογραφία, παραπέμπουμε τον αναγνώστη στην αναφορά [20].

Ευχαριστίες

Ιδιαίτερες ευχαριστίες οφείλω στον κύριο Αριστείδη Κοντογεώργη, καθηγητή του Μαθηματικού Τμήματος, του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών για το χρόνο που αφιέρωσε, ούτως ώστε να ολοκληρώσω την διπλωματική μου εργασία. Ο κύριος Κοντογεώργης, ως συνεπιβλέπων της διπλωματικής εργασίας μου, με συνέστησε με την «Αλγεβρική Θεωρία Αριθμών» και σε κάθε στάδιο ήταν ιδιαίτερα πρόθυμος να μου λύσει απορίες και να με συμβουλέψει. Επίσης, θα ήθελα να ευχαριστήσω θερμά την κυρία Λαμπροπούλου, επιβλέπουσα της διπλωματικής μου εργασίας, για την υπομονή και την καθοδήγησή της. Η υποστήριξη και οι συμβουλές που μου προσέφερε καθ΄ όλη τη διάρκεια των σπουδών μου συνέβαλαν σημαντικά στη ολοκλήρωση αυτού του κύκλου της ζωής μου. Τέλος, να ευχαριστήσω τον κύριο Vita Kala, επίκουρο καθηγητή του Μαθηματικού Τμήματος του Πανεπιστημίου του Καρόλου για τις παρατηρήσεις του, για όσο διάστημα δούλευα μαζί του στο Πανεπιστήμιο του Καρόλου της Πράγας

Contents

Chapter 1

Algebraic Numbers

The main path towards Fermat's Last Theorem leaded to the introduction of Algebraic Numbers and Algebraic Number Theory, as we know it today. We are going to follow that journey and unfold the theory until the critical point of Kummer's contribution to Fermat's Last Theorem.

Let's begin with giving a good understanding of *algebraic number fields* (or simply *number fields*), which are of great importance in algebraic number theory. The field of rational numbers $\mathbb{Q}$ is an example of a number field.

Definition 1.1. A *number field* F is a finite degree field extension of the field $\mathbb{Q}$, which means that $F \supseteq \mathbb{Q}$. Also F, when considered as a vector space over $\mathbb{Q}$, has finite dimension.

For more information and study of number fields, see Refs. [5] and [11].

Definition 1.2. *Algebraic numbers* are defined as the solutions of polynomial equations with integer coefficients. The set of algebraic numbers is symbolized as $\mathbb{A}$.

From now on, we will assume that a complex number a is algebraic when it is algebraic over $\mathbb{Q}$ (equivalently over $\mathbb{Z}$). First we give a result concerning factorization of polynomials, that is going to be useful later.

Theorem 1.1. *Suppose that K is a field of characteristic zero and f is a non-zero polynomial over K. There exists another polynomial, of degree > 0, whose square divides f, if and only if, f and the derivative of f have a common factor of degree > 0.*

Theorem 1.2 (*Eisenstein's criterion*)**.** *If $f = a_n t^n + \cdots + a_1 t + a_0$ is a polynomial over $\mathbb{Z}$ and p a prime number such that*

$$p \nmid a_n, \quad p^2 \nmid a_0 \quad \& \quad p | a_i, \; \forall i \in [0, n-1], \tag{1.1}$$

then $f(t)$ is irreducible over $\mathbb{Z}$, which equivalently means that $f(t)$ is irreducible over $\mathbb{Q}$ (except for possible constant factors).f

Definition 1.3. As *field extension* of K, we define a larger field L, which includes K as a subfield. The *degree of the extension* L over K is symbolized $[L : K]$ and is equal to the dimension of L as a vector space over K.

Theorem 1.3. *Suppose $L : K$ is a field extension and $\alpha \in L$. Then, α is algebraic over K, if and only if, $K(\alpha)$ is a finite extension of K. In that case, $[K(\alpha) : K]$ is equal to the degree of the minimum polynomial of α over K. Also $K(\alpha) = K[\alpha]$.*

Theorem 1.4. *If H is a subgroup of G, where G is a free abelian group of rank n, then H is free of rank $\leq n$.*

For the proof of theorems 1.1,1.2, 1.3, 1.4, see Ref [19].

Theorem 1.5. *The set $\mathbb{A}$ is a subfield of the complex field $\mathbb{C}$.*

Proof. According to theorem 1.3, the number a is algebraic, if and only if, $[\mathbb{Q}(a) : \mathbb{Q}]$ is finite.

Now, suppose that a, b are two algebraic numbers. Then,

$$[\mathbb{Q}(a, b) : \mathbb{Q}] = [\mathbb{Q}(a, b) : \mathbb{Q}]\ [\mathbb{Q}(a) : \mathbb{Q}] \tag{1.2}$$

But, b is algebraic over $\mathbb{Q}$, which implies that it is also algebraic over $\mathbb{Q}(a)$. Hence, $[\mathbb{Q}(a, b) : \mathbb{Q}]$ as well as $[\mathbb{Q}(a) : \mathbb{Q}]$ are finite. Therefore, according to (1.2), $[Q(a, b) : Q]$ is finite.

According to theorem 1.3, all the elements of $\mathbb{Q}(a, b)$ are algebraic. Hence $a+b$, $a-b$, ab, a/b (for $b \neq 0$), which belong to $\mathbb{Q}(a, b)$, are algebraic. And that completes the proof that $\mathbb{A}$ is a subfield of $\mathbb{C}$. □

For further details on the proof, see Ref. [18].

Theorem 1.6. *Every number field K is equal to $\mathbb{Q}(\theta)$, where θ is an algebraic number.*

Proof. Every number field K can be written as

$$K \equiv \mathbb{Q}(a_1, \cdots, a_n)\,,$$

where a_i are algebraic numbers, $\forall i \in [1, n]$ (e.g. a basis for K over $\mathbb{Q}$). We will use the method of induction for this proof. In particular, we will show that

$$K = K_1(a, b) \Rightarrow K = K_1(\theta), \text{ for some } \theta,$$

where K_1 is a subfield of K.

Let p, q be the minimum polynomials of a, b over K_1, respectively. Further suppose that they factorize over $\mathbb{C}$ as

$$p(t) = (t - a_1) \cdots (t - a_n), \quad q(t) = (t - b_1) \cdots (t - b_m) \tag{1.3}$$

Then, for some integer i, we must have $a_i = a$ and for some j, $b_j = b$. We choose (without loss of generality) $a_1 = a$ and $b_1 = b$. Since an irreducible polynomial over a subfield of $\mathbb{C}$ has no repeated zeros in $\mathbb{C}$, it follows that $a_i \neq a_j$ and $b_i \neq b_j$, $\forall i, j \in \mathbb{Z}$.

Let $k \neq 1$, equivalently $b_1 \neq b_k$. Then $\forall k \neq 1$ and $\forall i \in \mathbb{Z}$, there is exactly one, or none, $x \in K_1$, such that

$$\begin{aligned} x &= \frac{a_i - a_1}{b_1 - b_k} \\ &\Leftrightarrow a_i - a_1 = (b_1 - b_k)\ x \\ &\Leftrightarrow a_i + xb_k = a_1 + xb_1. \end{aligned} \tag{1.4}$$

Since there is a finite number of such equations, we can choose $c \in K_1$, such that $c \neq 0$ and $c \neq x$ and we can prove that $\forall x$ which satisfies equation (1.4). Then, it follows that $a_i + cb_k \neq a_1 + cb_1$, $\forall\, i \in [1, n]$ and $\forall\, k \in [2, m]$.

Claim: $K_1(a + cb) \equiv K_1(a, b)$

Proof of the claim: Define $a + cb = \theta$. It is obvious that $K_1(\theta) \subseteq K_1(a, b)$. It suffices to prove that

$$K_1(a, b) \subseteq K_1(\theta). \tag{1.5}$$

It holds that

$$\theta = a + cb \Rightarrow a = \theta - cb \Rightarrow p(\theta - cb) = p(a) = 0,$$

since $p(t)$ is the minimum polynomial of a over K_1. If we define $r(t) = p(\theta - ct) \in K_1(\theta)[t]$, we get that $q(b) = r(b) = 0$. But, $r(t)$, $q(t)$ have only one common zero. Since if $q(\xi) = r(\xi) = 0$, with $\xi \neq b$, then $\xi = b_i$, for some $i \in [2, m]$. However, $r(\xi) = p(\theta - c\xi) = 0$ and therefore $\theta - c\xi = a_i$, for some $i \in [1, n]$. Now, $\theta = a + cb$, hence $\xi = b$, which contradicts the assumption that $\xi \neq b$. Therefore, we have proved that

$$q(t) = r(t) = 0 \Leftrightarrow t = b.$$

Let $h(t)$ be the minimum polynomial of b over $K_1(\theta)$. Then, $h(t)|q(t)$ and $h(t)|r(t)$. Since $q(t)$, $r(t)$ have exactly one common zero in $\mathbb{C}$, the degree of $h(t)$ is 1. Hence, $h(t) = t + \mu$, where $\mu \in K_1(\theta)$ and

$$h(b) = 0 \ \Leftrightarrow b + \mu = 0 \ \Leftrightarrow b = -\mu \cdots \tag{1.6}$$

$\mu \in K_1(\theta)$ implies that $b \in K_1(\theta)$. Additionally, $c \in K_1$, where $K_1 \subseteq K_1(\theta)$. Thus, $c \in K_1(\theta)$. Finally, obviously $a = \theta - cb$ belongs to $K_1(\theta)$. This proves relation (1.5) and therefore also the claim. ■

By induction, it follows that every number field can be written as $\mathbb{Q}(\theta)$, where θ is an algebraic number. □

Chapter 2

Algebraic Integers

What is an algebraic integer?

Definition 2.1. The solutions of polynomial equations with integer coefficients, with the leading coefficient being 1, are called *algebraic integers.*

Equivalently, a complex number θ is an algebraic integer, if there is a monic polynomial $p(x)$ with integer coefficients such that $p(\theta) = 0$. We denote as $\mathbb{B}$ the set of algebraic integers.

Lemma 2.1. *Let $\theta \in \mathbb{C}$. The complex number θ is an algebraic integer if and only if the additive group generated by $1, \theta, \theta^2, \cdots$ is finitely generated.*

See Ref. [19] for the proof of lemma 2.1, which will be used for the proof of theorem 2.1.

Theorem 2.1. *$\mathbb{B}$ is a subring of $\mathbb{A}$.*

Proof.

Let $\theta, \phi \in \mathbb{B}$ (θ, ϕ algebraic integers). In order to show that $\mathbb{B}$ is a subring of $\mathbb{A}$, it suffices to show that $\theta + \phi \in \mathbb{B}$ and $\theta\phi \in \mathbb{B}$.

According to lemma 2.1, all the powers of θ (as well as ϕ) lie in a finitely generated group. This group will be called Γ_θ (respectively Γ_ϕ) and it is a subgroup of $\mathbb{C}$. Note that all powers of $\theta + \phi$ and $\theta\phi$ are integer linear combinations of elements $\theta^i\phi^j$, which lie in the group $\Gamma_\theta\Gamma_\phi$ (also subgroup of $\mathbb{C}$). But, because of lemma 2.1, Γ_θ has a finite number of generators: $u_1, u_2, \cdots u_n$. For the same reason, Γ_ϕ has generators: $v_1, v_2, \cdots, v_m$. Thus, $\Gamma_\theta\Gamma_\phi$ is the additive group generated by all $u_i v_j$, $\forall i \in [1, n]$, $\forall j \in [1, m]$.

This means that all powers of $\theta+\phi$ and $\theta\phi$ lie in a finitely generated additive subgroup of $\mathbb{C}$.

Again according to lemma 2.1, the above is equivalent to $\theta+\phi$ and $\theta\phi$ being algebraic integers. □

Theorem 2.2. *Suppose that $\theta \in \mathbb{C}$. If θ is a solution of a monic polynomial equation with coefficients which belong to $\mathbb{B}$, then $\theta \in \mathbb{B}$.*

Proof. Let $\theta \in \mathbb{C}$ such that

$$\theta^n + \psi_{n-1}\theta^{n-1} + \cdots + \psi_0 = 0,$$

where ψ_i are algebraic integers, $\forall i \in [0, n-1]$. Obviously, ψ_i generates a subring of $\mathbb{B}$, $\forall i \in [0, n-1]$.

By lemma 2.1, all powers of θ lie inside a finitely generated Ψ-submodule M of $\mathbb{C}$, spanned by $1, \theta, \cdots, \theta^{n-1}$.

Reminder: Suppose that M is a left R-module and N a subgroup of M. Then, N is called an R-submodule if $\forall n \in N$, $\forall r \in R$, $rn \in N$.

As a consequence of theorem 2.1, each ψ_i and all its powers lie inside a finitely generated additive group Γ_i, with generators γ_{i_j}, where $j \in [1, n_i]$. Therefore, M lies inside the additive group generated by all elements $\gamma_{1j_1}, \gamma_{2j_2}, \cdots, \gamma_{n-1_{j_{n-1}}}\theta^k$, where $j_i \in [1, u_i]$, $i \in [0, n-1]$, $k \in [0, n-1]$ and this group is also a finite set. Hence, M is a finitely generated additive group and thus, lemma 2.1 implies that θ is an algebraic integer. □

Theorems 2.1 and 2.2 provide useful ways to construct many algebraic integers out of known ones.

Lemma 2.2. *For every $\alpha \in K$, $\exists\, c \in \mathbb{Z} \setminus \{0\}$, such that $c\alpha \in \mathfrak{O}$.*

In theorem 1.6, it is proved that every number field can be written in the form $K = \mathbb{Q}(\theta)$, for some algebraic number θ. Now we can replace algebraic number θ with algebraic integer θ.

Corollary 2.1. *If K is a number field, then there is an algebraic integer $\theta \in \mathbb{B}$, such that $K = \mathbb{Q}(\theta)$.*

Proof. By theorem 1.6, $K = \mathbb{Q}(\phi)$, for some algebraic number ϕ. Now, by lemma 2.2, $\exists\, c \in \mathbb{Z} \setminus \{0\}$, such that $c\phi \in \mathfrak{O}$. By denoting $c\phi = \theta$, it follows that $\mathbb{Q}(\phi) \equiv \mathbb{Q}(\theta)$. □

Definition 2.2. Every number field K has a *ring of integers* $\mathfrak{O}$, which is defined as $\mathfrak{O} = K \cap \mathbb{B}$.

Definition 2.3. If K is an number field of degree n over $\mathbb{Q}$, a *basis* of K is a basis for K as a vector space over $\mathbb{Q}$. That means that $[K : \mathbb{Q}] = n$, where $K : \mathbb{Q}$ is a field extension and operates as a vector space over $\mathbb{Q}$.

Definition 2.4. The ring of integers $\mathfrak{O}$ forms an abelian group under addition. A $\mathbb{Z}$-basis for $(\mathfrak{O}, +)$ is called an *integral basis* for K, where K is a number field with degree n over $\mathbb{Q}$. Equivalently, $\big\{a_1, \cdots, a_s\big\}$ is an *integral basis*, if and only if, $a_i \in \mathfrak{O}$, $\forall\ i \in [1, s]$ and every $x \in \mathfrak{O}$ can be expressed as

$$x = z_1 a_1 + \cdots + z_s a_s, \text{ where } z_1, \cdots, z_s \in \mathbb{Z}.$$

Note that any integral basis for K is $\mathbb{Q}$-basis. Therefore $s = n$.

Theorem 2.3. *Every number field K has an integral basis. If the degree of K is n, then the additive group of the ring of integers $(\mathfrak{O}, +)$ is free abelian of rank n.*

Remark: $\mathbb{Z} \subseteq \mathbb{B}$ and $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$. Thus $\mathbb{Z} \subseteq K \cap \mathbb{B} \equiv \mathfrak{O}$.

There is a great criterion for an algebraic number to be an algebraic integer and it is given in the following lemma.

Lemma 2.3. *Let $a \in \mathbb{A}$. Then, a is an algebraic integer if and only if the coefficients of the minimum polynomial of a over $\mathbb{Q}$ belong to $\mathbb{Z}$.*

Agreement: From now on, when we refer to a *rational integer*, we mean an element of $\mathbb{Z}$, while an algebraic integer will be simply called an *integer*.

Lemma 2.4. *Let a be an integer (algebraic integer). Then $a \in \mathbb{Q}$, if and only if a is a rational integer (which means $a \in \mathbb{Z}$). Equivalently $B \cap \mathbb{Q} = \mathbb{Z}$.*

For proof of lemmas 2.3, 2.4 see Ref. [19].

Definition 2.5. For every number field $K = \mathbb{Q}(\theta)$, there are several distinct monomorphisms $\sigma_i : K \to \mathbb{C}$. The elements $\sigma_i(\alpha)$, where $\alpha \in K = \mathbb{Q}(\theta)$, are called the K-conjugates of α.

Definition 2.6. Let K be a number field of degree n, $K = \mathbb{Q}(\theta)$ and $\{a_1, a_2, \cdots, a_n\}$ a basis of K, as a vector space over $\mathbb{Q}$. The *discriminant* of this basis is given by the formula $\Delta[a_1, \cdots, a_n] = det(\sigma_i(a_j))^2$.

Some important properties of the discriminant:

- For another basis $\{b_1, \cdots, b_n\}$ of K, it holds that

$$\begin{aligned} &b_k = \sum_{i=1}^{n} c_{ik} a_i, \text{ where } c_{ik} \in \mathbb{Q},\ k \in [i, n],\ det(c_{ik}) \neq 0 \\ &\text{and } \Delta[b_1, \cdots, b_n] = (det(c_{ik}))^2 \cdot \Delta[a_1, \cdots, a_n]. \end{aligned} \tag{2.1}$$

- If K is a number field, then for every basis of it, the discriminant is rational and non-zero.

- If K has a basis $\{a_1, a_2, \cdots, a_n\}$, where a_i are integers, $\forall i \in [1, n]$, then

$$\Delta[a_1, a_2, \cdots, a_n] \in \mathbb{Z} \setminus \{0\}$$

  (equivalently the discriminant is a non-zero rational integer).

Definition 2.7. A rational integer a is called *squarefree*, if there is no prime number p such that $p^2|a$.

Theorem 2.4. *Suppose $a_1, \cdots, a_n \in \mathfrak{O}$ form a $\mathbb{Q}$-basis for K and $\Delta\big[a_1, \cdots, a_n\big]$ is squarefree. Then $\big\{a_1, \cdots, a_n\big\}$ is an integral basis for K.*

Proof. Let $b_1, \cdots, b_n$ form an integral basis for K. It follows, from the properties of the discriminant, that there exist $c_{ij} \in \mathbb{Q}$ such that

$$a - i = \sum c_{ij} b_j \quad \& \quad \Delta[a_1, \cdots, a_n] = (det(c_{ij}))^2 \cdot \Delta[b_1, \cdots, b_n].$$

But, $\Delta[a_1, a_2, \cdots, a_n]$ is squarefree. Therefore, $det(c_{ij}) = \pm 1$, which means that (c_{ij}) is unimodular. It follows that $\{a_1, \cdots, a_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{O}$, equivalently an integral basis for K. □

Theorem 2.5. *Every subgroup H of a free abelian group G, of rank n, is free of rank $s \leq n$. Also there is a basis $\{u_1, \cdots, u_n\}$ for G such that $a_1 u_1, \cdots, a_s u_s$, where a_i are positive integers, form a basis for H.*

For more details on theorem 2.5, see Ref. [19].

We will now introduce some results which allow to find the ring of integers of a given number field.

Theorem 2.6. *Let G be an additive subgroup of $\mathfrak{O}$. Suppose that the rank of G is equal to the degree of K and $\big\{a_1, \cdots a_n\big\}$ is a $\mathbb{Z}$-basis for G.*

Then

$$|\mathfrak{O}/G|^2 \textit{ divides } \Delta\big[a_1, \cdots, a_2\big].$$

Proof. According to theorem 2.5, there is a $\mathbb{Z}$-basis $\{b_1, \cdots, b_n\}$ for $\mathfrak{O}$, such that $\exists\ \mu_i$ positive integers, with $\{\mu_1 b_1, .., \mu_n b_n\}$ a $\mathbb{Z}$-basis for G.

$$\text{eq. (2.1)} \Rightarrow \Delta[a_1, \cdots, a_n] = (\, det(c_{ij}))^{\,2} \Delta[\mu_1 b_1, \cdots, \mu_n b_n]. \tag{2.2}$$

Since a basis change has unimodular matrix, we have that

$$\begin{aligned} \text{eq. (2.2)} \Rightarrow\ & \Delta[a_1, \cdots, a_n] = (\,\pm 1)^{\,2} \Delta[\mu_1 b_1, \cdots, \mu_n b_n] \\ \Rightarrow\ & \Delta[a_1, \cdots, a_n] = (\,\mu_1 \cdots \mu_n)^{\,2} \Delta[b_1, \cdots, b_n]. \end{aligned}$$

Since $|\mu_1 \cdots \mu_n| = |\mathfrak{O}/G|$, it is easy to see that $|\mathfrak{O}/G|^2$ divides $\Delta[a_1, \cdots, a_n]$. □

Proposition 2.1. *If $G \neq \mathfrak{O}$, there exists an algebraic integer x such that*

$$x = \frac{(\lambda_1 a_1 + \cdots + \lambda_n a_n)}{p}, \ \textit{where}\ \lambda_i \in \big[0, p-1], \ \ \lambda_i \in \mathbb{Z}, \ \ p \ \textit{prime},$$

with $p^2 | \Delta_G$.

Proof. Since $G \neq \mathfrak{O}$, $|\mathfrak{O}/G| > 1$, then $\exists\, p$ prime, such that p divides $|\mathfrak{O}/G|$ and $u \in \mathfrak{O}/G$. Thus every element $g \in G$ can be written as $g = pu$. Using the result of theorem 2.6, we get that $p^2 | \Delta_G$.

Since $a_1, \cdots, a_n$ form a $\mathbb{Z}$-basis for G, we have that

$$u = \frac{1}{p} g = \frac{1}{p}(\,\lambda_1 a_1 + \cdots + \lambda_n a_n).$$

Thus, we found an algebraic integer as needed. □

2.1 Quadratic fields

We turn our attention at quadratic fields, which are an important special case of number fields.

Definition 2.8. A *quadratic field* is an algebraic number field K of degree 2 over $\mathbb{Q}$.

The next result describes quadratic fields adequately.

Proposition 2.2. *A number field K is quadratic, if and only if, $K = \mathbb{Q}(\sqrt{d})$, where d is a squarefree rational integer.*

Proof. Let K be a number field of degree 2 over $\mathbb{Q}$ (quadratic). According to corollary 2.1, for every number field, $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer. But, K is of degree 2, which means that θ satisfies an equation of the form:

$$t^2 + at + b = 0,\ where\, a, b \in \mathbb{Z}$$
$$\Rightarrow \theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2} \tag{2.3}$$

Suppose that $a^2 - 4b = r^2 d$, where $r, d \in \mathbb{Z}$ and d is squarefree (this is possible because of prime factorization in $\mathbb{Z}$).

$$\begin{aligned} \text{eq. (2.3)} \Rightarrow \theta &= \frac{-a \pm \sqrt{r^2 d}}{2} \\ \Rightarrow \theta &= \frac{-a \pm r\sqrt{d}}{2} \\ \Rightarrow \theta &= -\frac{a}{2} \pm \frac{r}{2}\sqrt{d} \end{aligned}$$

Thus, it follows that $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$

The inverse can be proved in exactly the opposite way. □

Theorem 2.7. *The ring of integers of quadratic fields (equivalently of $\mathbb{Q}(\sqrt{d})$, where d is a squarefree rational integer) is*

$$\mathbb{Z}\big[\sqrt{d}\big],\ \ if\, d \not\equiv 1\,(mod\, 4)\ \ and$$

$$\mathbb{Z}\big[\frac{1}{2} + \frac{1}{2}\sqrt{d}\big],\ \ if\, d = 1\,(mod\, 4).$$

Proof. Let $a \in \mathbb{Q}(\sqrt{d})$. For some $r, s \in \mathbb{Q}$,

$$\begin{aligned} a &= r + s\sqrt{d} \\ \Leftrightarrow a &= \frac{e}{c} + \frac{b}{c}\sqrt{d} \\ \Leftrightarrow a &= \frac{e + b\sqrt{d}}{c},\ where\ a, b, c \in \mathbb{Z}. \end{aligned}$$

We additionally assume that $c > 0$ and that $\nexists\, p$ prime such that $p|e$ & $p|b$ & $p|c$, at the same time. Since a is an algebraic integer, the coefficients of the minimum polynomial are integers. The minimum polynomial is

$$\begin{aligned}&(t-a)(t-\frac{e-b\sqrt{d}}{c}) \\ =&(t-\frac{e+b\sqrt{d}}{c})(t-\frac{e-b\sqrt{d}}{c}) = t^2 - \frac{2e}{c}t + \frac{e^2-b^2d}{c^2}.\end{aligned} \tag{2.4}$$

$$\text{Thus, the coefficients } \frac{2e}{c},\ \frac{e^2-b^2d}{c^2} \text{ are rational integers.} \tag{2.5}$$

Suppose there is a prime p such that $p|c$ and $p|e$. Then, since (2.5) holds, $c^2|(e^2-b^2d) \Rightarrow p^2|(e^2-b^2d)$. Additionally $p|e \Rightarrow p^2|e^2$. Since d is squarefree, p should also divide b. This is a contradiction to an earlier assumption. Hence, $e,\ c$ cannot have any common prime factors.

Furthermore, since $\frac{2e}{c} \in \mathbb{Z}$, we must have $c|2$, equivalently $c = 1$ or $c = 2$.

- If $c = 1$, a is an algebraic integer of K in any case.
- If $c = 2$, we must have $e,\ b$ both odd. In the case where one of them is even, then the other is also even. Thus 2 divides all of them, which is a contradiction. It also holds that

  $$\frac{e^2-b^2d}{4} \in \mathbb{Z} \Rightarrow 4|(e^2-b^2d) \Rightarrow e^2-b^2d \equiv 0(mod\,4) \tag{2.6}$$

  Moreover, it is easy to see that

  $$e^2 \equiv 1\,(mod\,4), \tag{2.7}$$

  $$\text{and } b^2 \equiv 1\,(mod\,4), \text{ since they are odd.} \tag{2.8}$$

  By (2.6), (2.7), (2.8) we get that $d \equiv 1\,(mod\,4)$.

  Conversely, for $d \equiv 1\,(mod\,4)$ and for $e,\ b$ odd, (2.5) implies that a is an algebraic integer.

In conclusion, when $d \not\equiv 1\,(mod\,4)$, we have $c = 1$ and the ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$. When $d \equiv 1\,(mod\,4)$, c might also be 2 and if $e,\ b$ are odd, it easily follows that the ring of integers is $\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{d}]$.

□

2.2 Cyclotomic fields

The cyclotomic fields affected the development of Abstract Algebra and Number Theory. In particular, we focus on the arithmetic of those cyclotomic fields, which are generated by p_{th} roots of unity, when p is a prime number. The failure of unique factorization in their rings of integers, motivated Kummer to introduce the ideal numbers. Moreover, Wile's proof is related to cyclotomic fields.

Definition 2.9. A *cyclotomic field* $\mathbb{Q}(\zeta)$ is a number field obtained by adjoining a primitive complex n_{th} root of unity $\zeta = e^{2\pi i/n}$ to the field of rational numbers $\mathbb{Q}$.

The word "cyclotomic" refers to the equal spacing of powers of ζ around the unit circle in the complex plane.

Since we consider that p is a rational prime number, we can begin with

$$p = 2 \Rightarrow \zeta = e^{\pi i} = \cos\pi + \sin\pi = -1.$$

We easily realize that we have created nothing more than the set of rational numbers, since $\mathbb{Q}(-1) \equiv \mathbb{Q}$. Therefore, we can forget about $p = 2$ and from now on, we consider p to be an odd prime.

Lemma 2.5. *The minimum polynomial of $\zeta = e^{2\pi i/p}$ over $\mathbb{Q}$, where p is an odd prime, is*

$$f(t) = t^{p-1} + t^{p-2} \cdots + t + 1\,. \tag{2.9}$$

Proof. First, we check whether ζ is a root of the given $f(t)$. We can rewrite the polynomial as

$$f(t) = \frac{t^p - 1}{t - 1}\,. \tag{2.10}$$

Note that $f(\zeta)$ is well defined. Namely, the denominator is not equal to zero. Indeed,

$$\zeta - 1 \neq 0 \Leftrightarrow e^{2\pi i/p} \neq e^0 \Leftrightarrow 2\pi i/p \neq 0$$

is true for every prime p.

Moreover, ζ satisfies the polynomial equation, since

$$f(\zeta) = \frac{\zeta^p - 1}{\zeta - 1} = \frac{e^{2\pi i - 1}}{\zeta - 1} = \frac{\cos 2\pi + i\sin 2\pi - 1}{\zeta - 1} = 0\,.$$

In order to complete the proof, it suffices to show that $f(t)$ is irreducible.

Notice that

$$f(t+1) = \frac{(t+1)^p}{t} = \sum_{r=1}^{p} \left(\begin{array}{c} p \\ r \end{array} \right), \qquad t^{r-1} = p + \cdots + t^{p-1}\,.$$

It can be checked that the conditions of Eisenstein's criterion (theorem 1.2) are satisfied. Thus, $f(t+1)$ is irreducible. Hence, in turn $f(t)$ is irreducible. So this is the minimum polynomial of ζ over $\mathbb{Q}$.

According to the theorem 1.3, $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ should be equal to the degree of f, which is $p - 1$. Thus, the result has been verified. □

Finding the norm and the trace of ζ:

Recall that the expressions for norm and trace are

$$N(a) = \prod_{i=1}^{p-1} \sigma_i(a), \qquad T(a) = \sum_{i=1}^{p-1} \sigma_i(a),$$

where $\sigma_i(a)$ are the conjugates of a.

The first step is to find the conjugates of ζ. Note that $\zeta, \zeta^2, \cdots, \zeta^{p-1}$ are p^{th} roots of unity (different than 1). Thus, $f(t)$ is a minimum polynomial for them also. Equation (2.10) can be rewritten as

$$f(t) = (t-\zeta)(t-\zeta^2)\cdots(t-\zeta^{p-1}). \tag{2.11}$$

Thus, the conjugates of ζ are the the powers of ζ from 1 to $p-1$, which means that the monomorphisms from $\mathbb{Q}(\zeta) \to \mathbb{C}$ are

$$\sigma_i(\zeta) = \zeta^i\,, \text{ for } \ i \in [1, p-1].$$

The minimum polynomial has degree $p-1$. Therefore, a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is

$$\{1, \zeta, \cdots, \zeta^{p-2}\}.$$

This means that any element x can be written as

$$x = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}, \text{ for some}\, a_i \in \mathbb{Q}$$

$$\Leftrightarrow \sigma_i(a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}) = a_0 + a_1\zeta^i + \cdots + a_{p-2}\zeta^{p-2}.$$

- Now, lets calculate $N(\zeta)$.

  We have

  $$N(\zeta) = \zeta\zeta^2\cdots\zeta^{p-1}\,.$$

  Equation (2.9) gives $f(0) = 1$, while if we put $t = 0$ in equation (2.11) we get

  $$f(0) = (-\zeta)(-\zeta^2)\cdots(-\zeta^{p-1}) = (-1)^{p-1}\zeta\zeta^2\zeta^3\cdots\zeta^{p-1}.$$

  Since p is odd, we have that $p-1$ is even. So $(-1)^{p-1} = 1$.

  $$f(0) = 1 \Rightarrow \zeta\zeta^2\cdots\zeta^{p-1} = 1 \Rightarrow N(\zeta) = 1\,.$$

  Since ζ, ζ^i are conjugates, $\forall i \in [1, p-1]$, it follows that

  $$N(\zeta) = N(\zeta^i) = 1, \quad \forall i \in [1, p-1].$$

- In a similar way, the trace $T(\zeta)$ is calculated.

  $$T(\zeta) = \zeta + \zeta^2 + \cdots + \zeta^{p-1}.$$

  $$f(\zeta) = 0 \Rightarrow 1 + \zeta + \cdots + \zeta^{p-1} = 0 \Rightarrow T(\zeta) = -1.$$

  Since ζ, ζ^i are conjugates, it holds that

  $$T(\zeta^i) = T(\zeta) = -1, \quad \forall i \in [1, p-1]\,.$$

Theorem 2.8. *The ring of integers of* $\mathbb{Q}(\zeta)$ *is* $\mathbb{Z}[\zeta]$.

For the proof of theorem 2.8, see Ref. [19].

Chapter 3

Factorization

In the beginning of Algebraic Number Theory, mathematicians have assumed that factorization in the ring of integers of an algebraic number field is unique. Is it?

Why even the bright Euler believed that factorization of algebraic integers is unique, leading himself to many false results?

In order to reveal what was the starting fallacy of the above assumption, we will have to remember the definition of a prime number.

Definition 3.1. A number p *was* called a prime if

$$p = ab \Rightarrow a \,\mathrm{or}\, b \text{ is a unit.}$$

Definition 3.2. A number p is called a *prime* if,

$$p|ab \Rightarrow p|a \text{ or} \, p|b.$$

Although definitions 3.1 and 3.2 are equivalent in $\mathbb{Z}$ (where the only units are ± 1), they are not in every ring of integers of an algebraic number field. At that time, mathematicians failed to distinguish the difference between the above definitions. They considered a prime to be defined as 3.1 and were led to many wrong conclusions. For example,

- Euler has given many applications following the uniqueness of factorization and "proved" falsely some results in Number Theory. One example is his false proof of Fermat's Last Theorem (FLT) for $n = 3$, given in 1770, which will be further discussed in chapter 6.2.

- In 1847, Lamé thought wrongly and announced that he had proved FLT, taking uniqueness of factorization as a fact.

On the other hand, some mathematicians realized the need to prove unique factorization. For example,

- In 1832, Gauss introduced the “Gaussian integers” $\mathbb{Z}[i]$ and proved that factorization in $\mathbb{Z}[i]$ is unique.
- In 1844, Kummer proved that factorization is not unique for cyclotomic integers. However, his proof has been unnoticed at the time.
- Also in 1844, Eisenstein realized the importance to check the property of unique factorization.

The truth was restored, when a new term was coined and clarified the difference between definitions 3.1 and 3.2.

Definition 3.3. A number p is called *irreducible* if $p = ab$ implies that a or b is a unit.

Definition 3.4. An element u of an integral domain D is called a *unit* of D if $u|1$, equivalently if u has an inverse in D.

Note that definition 3.3 is identical to definition 3.1, which used to define primes. Let us mention some relations between primes and irreducibles, which we will revisit in more detail later on:

1. Irreducibility is not as strong quality as being a prime element.
2. If p is a prime, then it is also irreducible.
3. If p is irreducible, it is not necessarily a prime.
4. Factorization into primes, when possible, is unique. Whereas factorization into irreducibles is not always unique.

An example of non-unique factorization into irreducibles: In $\mathbb{Z}[\sqrt{-6}]$, $2 \cdot 3 = \sqrt{-6} \cdot \sqrt{-6} = 6$. We are going to verify that 2, 3, $\sqrt{-6}$ are not prime, but irreducible. In $\mathbb{Z}[\sqrt{-6}]$, $\sqrt{-6} \,|\, (2 \cdot 3)$ but $\sqrt{-6} \nmid 2$ and $\sqrt{-6} \nmid 3$. Therefore $\sqrt{-6}$ is not a prime in $\mathbb{Z}[\sqrt{-6}]$. Since it is impossible to find elements of $\mathbb{Z}[\sqrt{-6}]$, which are non-units and their product equal to $\sqrt{-6}$, then $\sqrt{-6}$ is irreducible.

In a similar way, it can be proved that elements 2, 3 are not primes, but irreducible. ■

Definition 3.5. Let $x \in R$, $x = yz$ is a *proper factorization* if neither y nor z is a unit.

Definition 3.6. A factorization of $x \in R$ is called *trivial* when it is not proper, which means that one of the factors is a unit and the other is an associate of x.

Definition 3.7. An element y is called an *associate* of x if $x = uy$, u being a unit.

At this point, it is useful to give a formal definition of *unique factorization into irreducibles.*

Definition 3.8. In a domain D, factorization into irreducibles is unique,

$$\text{if } p_1 \cdots p_r = q_1 \cdots q_s, \tag{3.1}$$

where $p_i,\ q_j$ are irreducible in D, $\forall i, j$. Equation (3.1) implies that

(a) $r = s$.

(b) $\exists$ permutation π of $1, \cdots, r$ such that $\forall i \in [1, r]$ $p_i,\ q_{\pi(i)}$ are associates.

Note that unique factorization into irreducibles is not affected by the units or by the order in which the factors appear.

Proposition 3.1. *Let D be a domain. Then*

(a) x is a unit $\Leftrightarrow x|1$.

(b) any two units are associates and any associate of a unit is a unit.

(c) x, y are associates $\Leftrightarrow x|y$ and $y|x$.

(d) x is irreducible $\Leftrightarrow$ every divisor of x is a unit or an associate of x.

(e) if x is irreducible, then its associate is also irreducible.

Proof. (a), (b): These two can be easily proved, using only the definition of associates.

(c): If $x|y$ and $y|x$ then $y = ax$ and $x = by$, for some $a, b \in D$. Hence

$$\begin{aligned} & x = bax \\ \Leftrightarrow & x\ (1 - ba) = 0 \\ \Leftrightarrow & x = 0 \textit{ or } 1 = ba. \end{aligned}$$

In the case that $x = 0$, $y = 0$ also and so they are trivially associates. In the case that $1 = ba$, then a, b are units, which means that they are also associates. If x, y are associates, then by definition $x = uy$ and $y = vx$, where u, v are units. Equivalently $y|x$ *and* $x|y$.

(d): It is trivial.

(e): Let y be an associate of x. Then $x = uy$, where u is a unit. □

The respective result, in terms of ideals is given in proposition 3.2. For definitions and more results on ideals, see chapter 4.

Proposition 3.2. *Suppose that D is a domain and $x, y \in D$, $x, y \neq 0$. Then,*

(a) $x|y \Leftrightarrow \langle x \rangle \supseteq \langle y \rangle$.

(b) x, y are associates $\Leftrightarrow \langle x \rangle = \langle y \rangle$.

(c) x is a unit $\Leftrightarrow \langle x \rangle = D$.

(d) x is irreducible $\Leftrightarrow \langle x \rangle$ is the maximal proper principal ideal of D.

Proof. (a): If $x|y$, then $\exists z \in D$ such that

$$\begin{aligned} & y = zx \\ & \Rightarrow y \in \langle x \rangle \\ & \Rightarrow \langle y \rangle \subseteq \langle x \rangle \\ & \Rightarrow y \in \langle x \rangle \\ & \Rightarrow y = zx, \ for\ some\ x \in D. \end{aligned}$$

(b): If x, y are associates then $\exists\ z, w \in D$ such that

$$\begin{aligned} x = yz\ and\ y = wx & \Leftrightarrow y|x\ and\ x|y \\ & \overset{(a)}{\Leftrightarrow} \langle y \rangle \subseteq \langle x \rangle\ and\ \langle x \rangle \subseteq \langle y \rangle \\ & \Leftrightarrow\ \langle x \rangle = \langle y \rangle\,. \end{aligned}$$

If $\langle x \rangle = \langle y \rangle$ then $\langle y \rangle \subseteq \langle x \rangle$ & $\langle x \rangle \subseteq \langle y \rangle$ and by following the reverse procedure, it can be shown that x, y are associates.

(c): If x is a unit, then $\exists\ v \in D$ such that $xv = 1$. Thus, for any $y \in D$

$$y = xv\ y \Rightarrow y \in \langle x \rangle\,.$$

Therefore, $D \subseteq \langle x \rangle$ and since $\langle x \rangle \subseteq D$, $D \equiv \langle x \rangle$.

Conversely, if $D = \langle x \rangle$, then every element of D is an element of $\langle x \rangle$. So, since $1 \in D$

$$\begin{aligned} & \Rightarrow 1 = zx \\ & \Leftrightarrow\ \ x \text{ is a unit.} \end{aligned}$$

(d): If x is irreducible and not the maximal proper ideal of D then $\exists\ y \in D$ such that

$$\langle x \rangle \subset \langle y \rangle \subset D\,.$$

This means that $y|x$, while y is not a unit neither an associate of x. But, according to proposition 3.1, an associate of an irreducible is an irreducible, which is a contradiction.

If $\langle x \rangle$ is the maximal proper ideal of D then x is either a unit or an associate, therefore irreducible. □

Note that the set $\mathbb{B}$ of algebraic integers has no irreducibles. Therefore, factorization into irreducibles is impossible there.

Definition 3.9. A domain D is called *noetherian* if every ideal in D is finitely generated.

Theorem 3.1. *If a domain D is noetherian, then factorization into irreducibles is possible in D.*

Proof. If D is a noetherian domain , every ideal in it is finitely generated. Let $\langle x\rangle$ be the maximal ideal such that $x \in D/\{0\}$, non-unit for which factorization into irreducibles cannot stand (equivalently it cannot be expressed as the product of a finite number of irreducibles).

This ideal exists because of the *maximal condition*, according to which any non-empty collection of ideals in a noetherian domain D has a maximal element.

Proof of the *maximal condition*: Suppose that $S \neq \emptyset$ is a set of ideals, which live in D, and that S has no maximal element. If I_0 is an ideal in S, then

$$\exists\ I_1 \in S\,\text{such that}\,I_1 \supseteq I_0.$$

We can continue this way and construct a chain of ideals in D, such that

$$I_0 \supseteq I_1 \supseteq \cdots \supseteq I_k\,,$$

with none of the ideals being maximal. Therefore, this chain can extend forever. But, this obviously contradicts the fact that D is finitely generated, since it is noetherian. Thus, the statement is proved. ■

Suppose that $x = yz$, with y, z non-units. Then, by proposition 3.2,

$$\langle x\rangle \subseteq \langle y\rangle\,.$$

In the case that $\langle x\rangle = \langle y\rangle$, again by proposition 3.2, y, x are associates, which means that z is a unit, which contardicts our hypothesis. Therefore, $\langle x\rangle \subset \langle y\rangle$ (not equal). By similar argument, $\langle x\rangle \subset \langle z\rangle$.

Since $\langle x\rangle$ is the maximal ideal, such that x cannot be expressed as a product of a finite number of irreducibles, elements y and z should factorize into irreducibles. So,

$$\begin{aligned} y &= p_1 \cdots p_r \\ z &= q_1 \cdots q_s\,. \end{aligned}$$

However,

$$x = yz \Rightarrow x = (p_1 \cdots p_r)(q_1 \cdots q_s)\,.$$

Thus, it has been proved that x is also a product of irreducibles, which contradicts our very first hypothesis. □

Theorem 3.2. *The ring of integers $\mathfrak{O}$ in any number field K is noetherian.*

Proof. We are going to show that every ideal I of $\mathfrak{O}$ is finitely generated. According to theorem 2.3, $(\mathfrak{O}, +)$ is a free abelian group of rank n, which is equal to the degree of the number field K. Therefore, in line with theorem 1.4, $(I, +)$ is also free abelian of rank $s \leq n$. A possible $\mathbb{Z}$-basis for $(I, +)$ is

$$\{x_1, \cdots x_s\}\,.$$

Furthermore,

$$\langle x_1, .., x_s \rangle \equiv I \,,$$

which implies that I is finitely generated, thus, $\mathfrak{O}$ noetherian. □

Corollary 3.1. *Factorization into irreducibles is possible in $\mathfrak{O}$.*

Proof. This corollary is a consequence of theorems 3.1, 3.2. □

However, factorization into irreducibles is not always unique in a ring of integers of a number field, and that is the reason, why we prefer to work in $\mathfrak{O}$ instead of $\mathbb{B}$.

We will give some examples of quadratic fields, in which factorization into irreducibles is not unique.

- Imaginary quadratic fields, where factorization into irreducibles is not unique: $\mathbb{Q}(\sqrt{d})$, for

  $$d = -5, -6, -10, -13, -14, -15, -17, -21, -22, -23, -26, -29, -30.$$

  It has been proved later on that $\mathbb{Q}(\sqrt{d})$ has unique factorization only for

  $$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

- Real quadratic fields, in which unique factorization into irreducibles is not valid: $\mathbb{Q}(\sqrt{d})$, for $d = 10, 15, 26$. In the case of real quadratic fields, it is shown that factorization is unique in many cases, but it remains unknown whether it holds for infinitely many $d > 0$.

One has to be very careful with the terms prime and irreducible. Let us revisit more thoroughly the relations between them.

In $\mathbb{Z}$, if x is an irreducible element, then x is a prime. Therefore, if $x|\ pq$, then we have

$$x|p \quad \text{or} \quad x|q \,.$$

While, in a domain D, x is a prime if it is non-zero, non-unit and

$$x|ab \Rightarrow x|a \quad \text{or} \quad x|b.$$

Proposition 3.3. *If x is a prime in a domain D, then x is also irreducible.*

Proof. Let $x \in D$ be prime and suppose that it can be reduced as

$$x = ab. \tag{3.2}$$

Because of the definition of a prime, $x|a$ or $x|b$.

If $x|a$, then $a = cx$ for some $c \in D$ and

$$\text{eq. (3.2)} \Leftrightarrow x = cxb \Leftrightarrow x(1 - cb) = 0 \Leftrightarrow cb = 1 \,,$$

since we set $x \neq 0$. This means that b is a unit and constitutes the factorization of x not proper.

If $x|b$, in a similar way, we get that a is a unit and the factorization of x is not proper.

Since we are led to a contradiction in both cases, we infer that our hypothesis, that x is not irreducible, is false. □

Note that the converse of proposition 3.3 is not true. An example was given by Eisenstein in 1844. Namely, let us assume that $\mathbb{Z}(\sqrt{-5})$ is a domain which contains irreducibles that are not primes, like element 2. It is straightforward to obtain that

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

Obviously 2 is an irreducible in $\mathbb{Z}(\sqrt{-5})$, but is it a prime? The answer is negative, since it does not divide neither $(1 + \sqrt{-5})$ nor $(1 - \sqrt{-5})$, while it divides their product, which is 6.

Theorem 3.3. *If in a domain D, factorization into irreducibles is possible, then it is also unique if and only if every irreducible is a prime.*

Proof. First, we may give an equivalent definition for the factorization of $x \neq 0$ in a domain D, that is

$$x = u\, p_1 \cdots p_r, \text{ where } u \text{ is a unit and } p_i \text{ are irreducibles}, \forall i \in\ [1, r\,].$$

For $r = 0$, we have $x = u$ (a unit), hence it is irreducible. While, for $r \geq 1$, $x = (up_1)\ p_2 \cdots p_r$, so x is a product of irreducibles.

Suppose that factorization is unique in D and p is irreducible. We will prove that p is also prime. Note that

$$p|ab \ \Rightarrow\ \exists\ c \in D, \text{ such that } ab = cp \tag{3.3}$$

and suppose that $a, b, c \neq 0$. We can factorize the elements into irreducibles as:

$$a = u_1 p_1 \cdots p_r$$
$$b = u_2 q_1 \cdots q_m$$
$$c = u_3 r_1 \cdots r_s,$$

where all u_i are units and $p_i,\ q_i,\ r_i$ are irreducibles. Equation (3.3) gives

$$(u_1 p_1 \cdots p_r)\ (u_2 q_1 \cdots q_s) = (u_3 r_1 \cdots r_s) p$$

and because of unique factorization in D, p should be an associate with one of the p_i, q_j. This implies that

$$\begin{aligned} &p|q_j \quad \text{or} \quad p|p_i, \text{ for some } i \text{ or } j \\ \Rightarrow\, &p|a \quad \text{or} \quad p|b. \end{aligned}$$

Hence, p is a prime.

Now, suppose that every irreducible is a prime. We will show that, in D, factorization into irreducibles is unique. Equivalently, we will show that if

$$u_1 p_1 \cdots p_m = u_2\ q_1 \cdots q_n, \tag{3.4}$$
$$\text{where } u_1, u_2 \text{ are units and } p_i, q_j \text{ are irreducibles,}$$

then $m = n$ and there exists a permutation π of $\{1, \cdots, m\}$, such that $p_i, q_\pi(i)$ are associates, $\forall i \in [1, m\,]$.

- For $m = 0$, it is trivial.
- For $m \geq 1$, eq. (3.4) $\Rightarrow$ $p_m | u_2\ q_1 \cdots q_n$, where p_m is irreducible, hence prime, because of the hypothesis. Therefore, by definition of a prime, either $p_m | u_2$, which means that p_m is a unit, and this leads to a contradiction, or $p_m | q_j$, for some $j \in [1, n]$, which is acceptable.

  Suppose that $j = n$. Then,

  $$\begin{aligned} & p_m | q_n \\ \Rightarrow & q_n = p_m u, \text{ where } u \text{ is a unit and } q_n \text{ irreducible} \\ \Rightarrow & u_1 p_1 \cdots p_m = u_2\ q_1 \cdots q_{n-1} p_m u \\ \Rightarrow & u_1 p_1 \cdots p_{m-1} = (u_2 u)\ q_1 \cdots q_{n-1} \end{aligned}$$

  By induction, let $m-1 = n-1$ and suppose that there exists a permutation π of $1, \cdots, m-1$, such that $p_i,\ q_\pi(i)$ are associates, $\forall i \in [1, m-1]$. By extending π to $1, \cdots, m$, the proof is completed.

□

The importance of unique factorization in a domain made it necessary to name these domains.

Definition 3.10. A domain in which factorization into irreducibles is unique, is called a *unique factorization domain.*

A UFD is an integral domain in which every non-zero, non-unit element can be written as a product of prime elements (equivalently irreducible elements) uniquely, up to order and units. In a *unique factorization domain* (UFD), primes are irreducibles and vice versa.

It is not difficult to notice the analogy to the fundamental theorem of arithmetic for the integers. As it was proved by Euclid in his *Elements*, according to the "Fundamental Theorem of Arithmetic", every integer $x > 1$, either is a prime number, or it can be expressed as a product of primes, in a unique way, up to order of factors.

Some examples of UFDs are *the principal ideal domains*, where every ideal is principal and *the Euclidean domains*, which are *integral domains*[1] granted with

[1] An *integral domain* is a nonzero commutative ring (a ring in which the multiplication operation is commutative), in which the product of any two nonzero elements is nonzero. Particularly, if a, b, c are elements of an integral domain and $a \neq 0$, then $ab = ac \Rightarrow b = c$. Integral domains are generalizations of the ring of integers.

at least one Euclidean function. We will give the relevant theorems right away. First, let us remember the definition of an Euclidean function.

Definition 3.11. An *Euclidean function* of a domain D is defined as
$\phi : D \setminus \{0\} \to \mathbb{N}$. If $a, b \in D \setminus \{0\}$, with $b \neq 0$, then there exist $q, r \in D$ such that $a = bq + r$, with either $r = 0$ or $\phi(r)\langle\phi(b)$.

The Euclidean function allows the use of Euclidean division in the domain.

Theorem 3.4. *If D is Euclidean, then it is also a principal ideal domain.*

Proof. Suppose D is an Euclidean domain and I is an ideal of D. If $I = \emptyset$, then it is principal and we are done. If $I \neq \emptyset$, then $\exists\ x \in I$, $x \neq 0$ and we can choose it to be the one for which the Euclidean function $\phi(x)$ is minimum. Then, if $y \in I$, by definition of the Euclidean function, we have that

$$y = qx + r,$$

where either $r = 0$ or $\phi(r) < \phi(x)$. Since we assumed that $\phi(x)$ is minimum, $r = 0$. Hence $y = qx$. This means that I is principal and in particular
$I = \langle x \rangle$. □

Theorem 3.5. *If D is a principal ideal domain, then it is a Unique Factorization Domain (UFD).*

Proof. If D is a principal ideal domain, it is also noetherian and by theorem 3.1, factorization into irreducibles is possible in D. In order to prove that it is also unique, we have to show that every irreducible is prime.

Let p be irreducible. This means that $\langle p \rangle$ is maximal principal ideal of D and since all ideals are principal, $\langle x \rangle$ is the maximal ideal.

If $p|ab$, with $p \nmid a$, then $\langle p, a \rangle \supset \langle p \rangle$ (not equal). Since $\langle p \rangle$ is the maximal, $\langle p, a \rangle = D$. Then, every element of D belongs to $\langle p, a \rangle$ as well. It holds that

$$\begin{aligned} &1 \in \langle p, a \rangle \\ \Rightarrow &1 = cp + da, \ \text{ for some } c, d \in D. \end{aligned} \tag{3.5}$$

If we multiply (3.5) by b, we get that

$$\begin{aligned} &b = cpb + dab \\ \Rightarrow &p|cpb + dab, \text{ since}\, p|ab \\ \Rightarrow &p|b \end{aligned}$$

This means that p is prime as we assumed that $p|ab$ and $p \nmid a$. □

Theorem 3.6. *Every Euclidean domain is a Unique Factorization Domain (UFD).*

Proof. The proof follows directly by theorems 3.4 and 3.5. □

Now, let us display a rather impressive example, which shows how properties of unique factorization serve to get results in Diophantine equations. The next theorem was introduced by Ramanujan as a conjecture and proved later on by Nagell, Ref. [13].

Theorem 3.7 (The Ramanujan-Nagell Theorem)**.**
Equation $x^2 + 7 = 2^n$, with x, n integers, has only the following solutions:

$$x = \pm 1,\ 3,\ 5,\ 11,\ 181, \quad n = 3,\ 4,\ 5,\ 7,\ 15.$$

Chapter 4

Introduction of Ideals

4.1 Basic definitions

The fact that unique factorization into irreducibles holds **only** in some rings of integers was quite disappointing. On the other hand, this obstacle motivated the introduction of ideals. Let us give some definitions and start revealing the history.

Definition 4.1. A subset I of a ring R is called an *ideal*, if it is an additive subgroup of I and

$$rx \in I \,\&\; xr \in I, \forall r \in R\,, \forall x \in I.$$

Ideals are symbolized with small Gothic letters $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ etc. For example, the set of even numbers, as a subset of the ring of integers $\mathbb{Z}$, form an ideal.

Definition 4.2. Every ideal has an *inverse*, which is defined as

$$\mathfrak{a}^{-1} = \{x \in K | xa \subseteq \mathfrak{O}\}.$$

Definition 4.3. A *principal ideal* is an ideal I in a ring R that is generated by a single element a of R in the following way: $I = \{ar : r \in R\}$.

Some examples of principal ideals are the ideals $n\mathbb{Z}$ of the ring of integers $\mathbb{Z}$. Actually, it has been proved that every ideal of $\mathbb{Z}$ is principal.

4.2 Revealing the history

We can start now revealing the history of how the theory of ideals was developed.

Kummer's idea: If a number cannot be factorized uniquely in a given ring of integers, Kummer suggested to extend that ring, so that the number does factorize uniquely in the bigger one. In particular, when an element a in the number field K cannot be factorized uniquely, we can extend K to L, so that

$\mathfrak{O}_K \subseteq \mathfrak{O}_L$ and a factorizes uniquely into elements in $\mathfrak{O}_L$. That is how *ideal numbers* were introduced. Of course, Kummer had a different point of view. He introduced ideal prime factors for elements which may have no prime factors in their number field, by using detailed computations. For more information see Refs. [4] and [3]. Below, through a specific example, we will try to understand what was the need to introduce ideal numbers.

Example: In $\mathbb{Q}(\sqrt{15})$,

$$10 = 2 \cdot 5 = (5+\sqrt{15})(5-\sqrt{15}).$$

How can we guarantee unique factorization for 10? By extending $\mathbb{Q}(\sqrt{15})$ to $\mathbb{Q}(\sqrt{3},\sqrt{5})$, factorization of 10 is unique. Indeed,

$$10 = \sqrt{5} \cdot \sqrt{5} \cdot (\sqrt{5}+\sqrt{3}) \cdot (\sqrt{5}-\sqrt{3})$$

and there is no other way to factorize 10 in the extended field. ■

Let us stress that, even the extended rings of integers do not need to be UFDs and this makes the theory very useful. It suffices that an element of a ring of integers $\mathfrak{O}$, not uniquely factorized in $\mathfrak{O}$, can be uniquely factorized in elements of the extended number field.

Dedekind's contribution: Dedekind introduced the term of an *ideal* in ring theory, influenced by Kummer's ideal numbers. He developed a theory of unique factorization for ideals, in which 'prime ideals' play the role of a 'prime'. Dedekind's approach is the closest to our modern view of ideals. According to that, the product

$$x = p_1\ p_2 \cdots\ p_n, \text{ where } p_i \text{ belong in a ring } R, \tag{4.1}$$

corresponds to

$$\langle x\rangle = \langle p_1\rangle\ \langle p_2\rangle \cdots \langle p_n\rangle, \text{where } \langle p_i\rangle \text{ are principal ideals.} \tag{4.2}$$

Replacing (4.1) with (4.2), eliminates the problem. In particular, according to Proposition 3.2,

$$\langle p_1\rangle = \langle u\ p_1\rangle.$$

This means that, if the multiplication is unique up to units and order, then the multiplication of ideals is unique up to order.

Definition 4.4. An ideal $\mathfrak{a}$ of a ring R is called *maximal* if it is a proper ideal and there is no ideal of R strictly between $\mathfrak{a}$ and R.

Definition 4.5. An ideal $\mathfrak{a}$ of a ring R, with $\mathfrak{a} \neq R$, is called *prime ideal*, if for every $\mathfrak{b}, \mathfrak{c}$ ideals of R holds that $\mathfrak{bc} \subseteq \mathfrak{a} \Rightarrow \mathfrak{b} \subseteq \mathfrak{a}$ or $\mathfrak{c} \subseteq \mathfrak{a}$.

Proposition 4.1. *Let $x, y \neq 0$ be elements of a domain D. Then*

(a) $x|y \Leftrightarrow \langle x\rangle \supseteq \langle y\rangle$,

(b) x, y are associates $\Leftrightarrow \langle x\rangle = \langle y\rangle$,

(c) x is a unit $\Leftrightarrow \langle x\rangle = D$,

(d) x is irreducible $\Leftrightarrow \langle x\rangle$ is maximal, among the proper principal ideals of D.

For the proof of the above proposition, see Ref. [19]. Moreover, because of proposition 4.1, a prime ideal can also be defined as follows:

Definition 4.6. If $\mathfrak{p}$ is a prime ideal, $\mathfrak{p}|\mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p}|\mathfrak{a}$ or $\mathfrak{p}|\mathfrak{b}$.

Lemma 4.1. *Suppose $\mathfrak{a}$ is an ideal of a ring R. Then,*

(a) $\mathfrak{a}$ is maximal $\Leftrightarrow \frac{R}{\mathfrak{a}}$ is a field,

(b) $\mathfrak{a}$ is prime $\Leftrightarrow \frac{R}{\mathfrak{a}}$ is a domain.

Proof. (a): There is an one-to-one correspondence between ideals of $R/\mathfrak{a}$ and ideals of R, which lie between $\mathfrak{a}$ and R. This constitutes $\mathfrak{a}$ a maximal ideal, if and only if $R/\mathfrak{a}$ does not have non-zero proper ideals. Therefore, any ring is a field, if and only if it does not have non-zero ideals.

(b): If $\mathfrak{a}$ is prime and $x, y \in R$ such that $(\mathfrak{a}+x)(\mathfrak{a}+y) = 0,\ \text{in}\, R/\mathfrak{a}$, then $xy \in \mathfrak{a}$. Therefore,

$$\begin{aligned}&\langle x\rangle\langle y\rangle \subseteq \mathfrak{a}\\ \Rightarrow&\langle x\rangle \subseteq \mathfrak{a}\ \text{ or } \langle y\rangle \subseteq \mathfrak{a}\\ \Rightarrow& x \in \mathfrak{a}\ \textit{ or }\ y \in \mathfrak{a}.\end{aligned}$$

Hence, either $(\mathfrak{a}+x) = 0$ or $(\mathfrak{a}+y) = 0$ in $R/\mathfrak{a}$, which means that $R/\mathfrak{a}$ has no zero divisors and therefore is a domain.

Conversely, if we suppose that $R/\mathfrak{a}$ is a domain, it follows that

$$|R/\mathfrak{a}| \neq 1 \ \Rightarrow\ \mathfrak{a} \neq R.$$

If $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}$ and at the same time $\mathfrak{b} \nsubseteq \mathfrak{a}$, $\mathfrak{c} \nsubseteq \mathfrak{a}$, then there exist elements $b \in \mathfrak{b}$ and $c \in \mathfrak{c}$, with $b, c \notin \mathfrak{a}$, while their product $b \cdot c \in \mathfrak{a}$. Hence, it is proved that $(\mathfrak{a}+b)$ as well as $(\mathfrak{a}+c)$ are zero-divisors in $R/\mathfrak{a}$, which contradicts the fact that $R/\mathfrak{a}$ is a domain. □

Corollary 4.1. *Every maximal ideal is prime.*

In the following theorem we will show some important properties of the ring of integers $\mathfrak{O}$ of a number K, with degree n.

Theorem 4.1. *(a) The ring of integers $\mathfrak{O}$ of a number field K is a domain, with field of fractions K,*

(b) $\mathfrak{O}$ is noetherian,

(c) if $\mathfrak{a} \in K$ satisfies a monic polynomial equation with coefficients in $\mathfrak{O}$ then $\mathfrak{a} \in \mathfrak{O}$,

(d) every non-zero prime ideal of $\mathfrak{O}$ is maximal.

Proof. (a): is quite obvious. Note that the field of fractions of an integral domain is the smallest field, in which the domain can be embedded.

(b): by theorem 2.3, we have that $(\mathfrak{O},+)$ is free abelian of rank n. By theorem 1.4, it follows that $(\mathfrak{a},+)$ is free abelian of rank less or equal to n, $\forall \mathfrak{a}$ ideal of $\mathfrak{O}$. Since any $\mathbb{Z}$-basis for $(\mathfrak{a},+)$ generates the ideal $\mathfrak{a}$, $\mathfrak{O}$ is noetherian (because every ideal in it is finitely generated).

(c): follows immediately by theorem 2.2.

(d): let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}$. We will prove that $R/\mathfrak{p}$ is a field, which is equivalent to $\mathfrak{p}$ maximal by lemma 4.1. Suppose that there exists $a \in \mathfrak{p}$, such that $a \neq 0$. Then, since $a_1 = a$,

$$\begin{aligned} &N(a) = N = a_1 \cdots a_n \in \mathfrak{p}, \text{ where } a_i \text{ are the conjugates of } a.\\ \Rightarrow &\langle N \rangle \subseteq \mathfrak{p}\\ \Rightarrow &\mathfrak{O}/\mathfrak{p} \text{ is a quotient ring of } \mathfrak{O}/N\mathfrak{O}. \end{aligned}$$

This is a finitely generated abelian group and every element, which belongs to it, is of finite order. Therefore, the group $\mathfrak{O}/\mathfrak{p}$ is finite . According to lemma 4.1, $\mathfrak{O}/\mathfrak{p}$ is a domain, since $\mathfrak{p}$ is a prime ideal. Finally, by theorem 1.1, since $\mathfrak{O}/\mathfrak{p}$ is a domain and finite, it is also a field and the proof is completed. □

Theorem 4.1 gives a quite characteristic property of the ring of integers, which does not apply in all rings.

Definition 4.7. A ring of integers which satisfies all the properties of theorem 4.1 is called a *Dedekind Ring.*

We will show that in a Dedekind ring, every nonzero proper ideal factors into a product of prime ideals in a unique way, up to order of the factors. First, we need to study the behaviour of non-zero ideals of $\mathfrak{O}$, which creates the need to introduce fractional ideals of $\mathfrak{O}$. Since an ideal can be described as an $\mathfrak{O}$-submodule of $\mathfrak{O}$, we turn our attention to $\mathfrak{O}$-submodules of the field K. In order to get the group structure that we want, we are going to use fractional ideals.

Definition 4.8. An $\mathfrak{O}$-submodule $\mathfrak{a}$ of K is called a *fractional ideal* of $\mathfrak{O}$ if

$$\exists\, c \in \mathfrak{O},\ c \neq 0 \text{ such that } c\mathfrak{a} \subseteq \mathfrak{O}.$$

Equivalently, the set $\mathfrak{b} = c\mathfrak{a}$ is an ideal of $\mathfrak{O}$. It follows that $\mathfrak{a} = c^{-1}\mathfrak{b}$ and the fractional ideals of $\mathfrak{O}$ are of the form $c^{-1}\mathfrak{b}$. For example, the fractional ideals of $\mathbb{Z}$ are of the form $r\mathbb{Z}$, with r being a rational number.

Interesting facts about fractional ideals:

- If every ideal of $\mathfrak{O}$ is a principal ideal and d is a generator, then fractional ideals have the following form

$$c^{-1}\langle d \rangle = c^{-1}d\ \mathfrak{O}.$$

- Every ideal is a fractional ideal.
- A fractional ideal is an ideal, if and only if $\mathfrak{a} \subseteq \mathfrak{O}$.
- When we multiply fractional ideals, the result is a fractional ideal. In particular, if $\mathbf{a_1}, \mathbf{a_2}$ are fractional ideals with $\mathfrak{a}_1 = c_1^{-1}\mathbf{b_1}$, $\mathfrak{a}_2 = c_2^{-1}\mathbf{b_2}$, their product will be
$$\mathfrak{a}_1\mathfrak{a}_2 = (c_1c_2)^{-1}\mathfrak{b}_1\mathfrak{b}_2.$$
- Multiplication of fractional ideals is commutative and associative. Also, $\mathfrak{O}$ is the identity of multiplication of fractional ideals.
- Every fractional ideal $\mathfrak{a}$ has an inverse $\mathfrak{a}^{-\mathbf{1}}$, such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$.

Theorem 4.2. *The non-zero fractional ideals of $\mathfrak{O}$ form an abelian group under multiplication.*

Theorem 4.3. *Every non-zero ideal of $\mathfrak{O}$ is possible to be written as a product of prime ideals, in a unique way (up to order of factors).*

Theorem 4.3 is a very important result. Uniqueness of factorization for ideals provides a great tool, which enables further progress towards proving FLT. For the proof of theorems 4.2, 4.3 see Ref. [19].

As a consequence of theorem 4.3, the following corollary is valid.

Corollary 4.2. *Every fractional ideal of $\mathfrak{O}$ can be written as a product of prime ideals, in a unique way, up to order of factors.*

Proof. Let $\mathfrak{a}$ be a fractional ideal and $c \in \mathfrak{O} \setminus \{0\}$, such that $c\mathfrak{a}$ is an ideal. Then, according to theorem 4.3, $\exists\ \mathfrak{p}_i,\ \mathfrak{q}_j$ prime ideals, with $i \in [1,\ r]$, $j \in [1,\ s]$, such that $\langle c \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ and $c\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Hence, $\mathfrak{a} = {\mathfrak{p}_1}^{-1} \cdots {\mathfrak{p}_r}^{-1}\mathfrak{q}_1 \cdots \mathfrak{q}_s$. □

Proposition 4.2. *Suppose $\mathfrak{a}, \mathfrak{b}$ are ideals of $\mathfrak{O}$. Then,*

$$\mathfrak{a}|\mathfrak{b} \ \Leftrightarrow\ \mathfrak{b} \subseteq \mathfrak{a}.$$

The uniqueness of factorization for ideals combined with proposition 4.2 provide the following conclusions:

(a) Let $\mathfrak{a}, \mathfrak{b}$ be ideals of $\mathfrak{O}$. $\mathfrak{a}|\mathfrak{b}$ if $\exists\, \mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, where $\mathfrak{c}$ is an ideal of $\mathfrak{O}$. Equivalently $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{a} \supseteq \mathfrak{b}$, which means that the factors of an ideal are precisely the ideals that contain it.

(b) If $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}$, then
$$\mathfrak{p}|\mathfrak{a}\mathfrak{b} \ \Rightarrow\ \mathfrak{p}|\mathfrak{a} \ \text{or}\, \mathfrak{p}|\mathfrak{b},$$
which is completely analogous to the definition of a prime number.

(c) The greatest common factor of two ideals is the smallest ideal that contains them.

(d) The least common multiple of two ideals is the largest ideal that is contained to them.

Definition 4.9. The *norm* of a non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}$ is defined as

$$N(\mathfrak{a}) = \left|\frac{\mathfrak{O}}{\mathfrak{a}}\right|,$$

where $\frac{\mathfrak{O}}{\mathfrak{a}}$ is finite, $\forall \mathfrak{a} \in \mathfrak{O}$.

Useful results about Norms of Ideals:

(a) Every non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}$ has a $\mathbb{Z}$-basis $\{a_1, \cdots, a_n\}$, where n is equal to the degree of K. In particular,

$$N(\mathfrak{a}) = \left|\frac{\Delta[a_1, \cdots, a_n]}{\Delta}\right|^{1/2}, \tag{4.3}$$

where Δ is the discriminant of K.

(b) $\forall\, \mathfrak{a}$ ideal of $\mathfrak{O}$, $\mathfrak{a} = \langle a \rangle$ (principal ideal) $\Rightarrow$ $N(\mathfrak{a}) = |N(a)|$.

(c) $\forall\, \mathfrak{a}, \mathfrak{b}$ pair of ideals of $\mathfrak{O}$,

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b}) \tag{4.4}$$

From now on $\mathfrak{a}|\langle b \rangle$ will be denoted as $\mathfrak{a}|b$, where $\mathfrak{a}$ is an ideal and b is an element of $\mathfrak{O}$.

Theorem 4.4. *For an ideal $\mathfrak{a} \neq 0$ of $\mathfrak{O}$, the following are valid:*

(a) if $N(\mathfrak{a})$ is prime, then $\mathfrak{a}$ is also a prime,

(b) $N(\mathfrak{a})$ is an element of $\mathfrak{a}$ (which is equivalent to $\mathfrak{a}|N(\mathfrak{a})$),

(c) if $\mathfrak{a}$ is prime, then $\mathfrak{a}|p$, for only one rational prime p and $N(\mathfrak{a}) = \mathfrak{p}^m$, where m is the degree of K $(m \leq n)$.

Proof. (a): Every ideal is a product of prime ideals, which means that

$$a = p_1 \cdots p_r.$$

By properties of the norm of an ideal,

$$N(\mathfrak{a}) = N(p_1 \cdots p_r) = N(p_1) \cdots N(p_r).$$

Since $N(\mathfrak{a})$ is prime, then $N(\mathfrak{a}) = N(p_i)$, for some $i \in [1, r]$. But, p_i is prime, $\forall i \in [1, r]$. Therefore $\mathfrak{a} = p_i$ is prime.

(b): By definition, $N(\mathfrak{a}) = |\mathfrak{O}/\mathfrak{a}|$. Then, $\forall x \in \mathfrak{O}$,

$$N(\mathfrak{a}) \cdot x \in \mathfrak{a}\,. \tag{4.5}$$

If we put $x = 1$ in (4.5), we have that $N(a) \in x$.

(c): From (b) and for p_i rational primes, it follows that

$$\begin{aligned} \mathfrak{a}|N(a) &\Rightarrow \mathfrak{a}|N(p_1 \cdots p_r) \\ &\Rightarrow \mathfrak{a}|N(p_1) \cdots N(p_r) \\ &\Rightarrow \mathfrak{a}|p_1^{m_1} \cdots p_r^{m_r} \\ &\Rightarrow \mathfrak{a}|N(p_i), \text{ for some } i \in [1, r] \\ &\Rightarrow \mathfrak{a}|p_i, \text{ for some } i \in [1, r]. \end{aligned} \tag{4.6}$$

Now, we will prove that i, in equation (4.6), is unique. Let p, q be primes, with $p \neq q$, such that $\mathfrak{a}|p$ and $\mathfrak{a}|q$. Since $p \neq q$, $\exists\ u, v$ integers, such that

$$\begin{aligned} &up + vq = 1 \\ &\Rightarrow \mathfrak{a}|up + vq \\ &\Rightarrow \mathfrak{a}|1 \\ &\Rightarrow \mathfrak{a} = \mathfrak{O}, \end{aligned}$$

which is a contradiction. Then, $N(\mathfrak{a})|N(\langle p\rangle) = p^n$, where m is equal to the degree of K and therefore

$$N(\mathfrak{a}) = p^m, \text{ for some } m \leq n.$$

□

Theorem 4.5. *(a) Every non-zero ideal of $\mathfrak{O}$ has a finite number of divisors.*

(b) A non-zero rational integer is possible to belong only to a finite number of ideals of $\mathfrak{O}$.

(c) Only a finite number of ideals of $\mathfrak{O}$ have given norm.

Proof. The proof of theorem 4.5 follows directly as a result of theorem 4.4 and basic properties of prime factorization. □

Theorem 4.6. *Factorization of elements of $\mathfrak{O}$ into irreducibles is unique, if and only if every ideal is principal.*

Proof. According to theorem 3.5, every principal ideal domain is a unique factorization domain (UFD). Therefore, if every ideal of $\mathfrak{O}$ is principal, unique factorization follows.

Conversely, suppose that factorization into irreducibles is unique in $\mathfrak{O}$. We are going to prove that every ideal is principal. In fact, it suffices to show that every prime ideal is principal, because every ideal is a product of prime ideals. If $p \neq 0$ is a prime ideal of $\mathfrak{O}$, according to 4.4, $N(p)$ is an element of p and as a consequence, $p|N(p)$. Since $N(p)$ is a rational integer and because of the initial hypothesis,

$$N(p) = \pi_1 \cdots \pi_s, \text{ where } \pi_i \text{ are irreducible elements of } \mathfrak{O}.$$

Since $p|N$, where p is a prime ideal, it follows that, for some $i \in [1, s]$

$$\begin{aligned} &p|\pi_i \\ \Leftrightarrow &p|\langle \pi_i \rangle \,. \end{aligned}$$

Theorem 3.3 implies that every irreducible in a UFD is prime. Therefore, π_i is prime. Hence, $\langle \pi_i \rangle$ is prime. This in turn implies that $p = \langle \pi_i \rangle$ or that equivalently p is a principal ideal.

Since the prime ideal with which we started was randomly chosen, it is proved that every prime ideal is principal. □

Theorem 4.6 reveals the relation between ideals and factorization of elements.

Chapter 5

Geometric view of algebraic numbers and results

5.1 Geometric representation of algebraic numbers

Reminder: As a *lattice L^{st} in* $\mathbb{R}^n$, we define a subgroup of the additive group $\mathbb{R}^n$, which is isomorphic to the additive group $\mathbb{Z}^n$. L^{st} generalizes the way $\mathbb{Z}$ is embedded in $\mathbb{R}$.

This chapter starts by investigating how a number field K, of degree n, can be embedded into a real vector space of dimension equal to n, so that the ideals in K will map to lattices in this vector space.

We define as $\sigma_1, \sigma_2, \cdots, \sigma_n$ the monomorphisms from the number field $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer, to $\mathbb{C}$.

Definition 5.1. A monomorhism σ_i is called *real monomorphism*, if $\sigma_i(K) \subseteq \mathbb{R}$. Otherwise, σ_i is called *complex monomorphism.*

Properties of σ_i :

- $\overline{\sigma_i}(a) = \overline{\sigma_i(a)}$,
- $\overline{\sigma_i} = \sigma_i \Leftrightarrow \sigma_i$ is real,
- $\overline{\overline{\sigma_i}} = \sigma_i$,
- $n = s + 2t$, where s is the number of real monomorphisms, $2t$ is the number of complex monomorphisms. We write it as $2t$, because complex monomorphisms always appear in conjugate pairs.

Analytically, we define all the monomorphisms: $K \to \mathbb{C}$ as follows:

$$\underbrace{\sigma_1, \cdots, \sigma_s}_{\text{real}};\ \underbrace{\sigma_{s+1}, \overline{\sigma_{s+1}}, \cdots, \sigma_{s+t}, \overline{\sigma_{s+t}}}_{\text{complex monomorphisms}}.$$

Then, a lattice can be written as $L^{st} = \mathbb{R}^s \times \mathbb{C}^t$, which involves the elements of the form

$$x = (\underbrace{x_1, \cdots, x_s}_{\in \mathbb{R}}; \underbrace{x_{s+1}, \cdots, x_{s+t}}_{\in \mathbb{C}}).$$

Obviously, L^{st} is a vector space over $\mathbb{R}$, with dimension $n = s + 2t$.

Definition 5.2. We define as *norm* of x

$$N(x) = x_1 \cdots x_s |x_{s+1}|^2 \cdots |x_{s+t}|^2, \ \forall x \in L^{st}.$$

Properties of the Norm:

- $N(xy) = N(x)N(y)$, $\forall x, y \in L^{st}$,
- $N(x) \in \mathbb{R}, \ \forall x \in L^{st}$.

Let us define a map $\sigma : K \to L^{st}$,

$$\sigma(a) = (\sigma_1(a), \cdots, \sigma_s(a); \sigma_{s+1}(a), \cdots, \sigma_{s+t}(a)), \ \forall a \in K, \tag{5.1}$$

such that

(a) $\sigma(a + \beta) = \sigma(a) + \sigma(\beta), \ \forall a, \beta \in K$

(b) $\sigma(a\beta) = \sigma(a)\sigma(\beta), \ \forall a, \beta \in K$

(c) $\sigma(ra) = r\sigma(a), \ \forall a \in K, \ \forall r \in \mathbb{Q}$ ($\Rightarrow \sigma$ is a $\mathbb{Q}$-algebra homomorphism),

(d) $N(\sigma(a)) = N(a), \ \forall a, \beta \in K.$

Theorem 5.1. *Let $\{a_1, a_2, \cdots, a_n\}$ be a basis for K over $\mathbb{Q}$.*
Then, $\sigma(a_1), \cdots, \sigma(a_n)$ are linearly independent over $\mathbb{R}$.

The proof of theorem 5.1 can be found in Ref. [19].

Since L^{st} is a vector space, isomorphic to $\mathbb{R}^{s+2t}$, we can choose the following basis for L^{st}:

$$\begin{gathered}(1, 0, \cdots, 0; 0, \cdots, 0)\\(0, 1, \cdots, 0; 0, \cdots, 0)\\\vdots\\(0, \cdots, 1; 0, \cdots, 0)\\(0, \cdots, 0; 1, \cdots, 0)\\(0, \cdots, 0; i, \cdots, 0)\\\vdots\\(0, \cdots, 0; 0, \cdots, i)\end{gathered}$$

This way, an element $(x_1, \cdots, x_s; y_1 + iz_1, \cdots, y_t + iz_t)$ of L^{st} can be rewritten as $(x_1, \cdots, x_s, y_1, z_1, \cdots, y_t, z_t)$.

Lemma 5.1. *Let L be an n-dimensional lattice in $\mathbb{R}^n$, with $\mathbb{Z}$-basis $\{e_1, \cdots, e_n\}$, where $e_i = (a_{1_i}, \cdots, a_{n_i})$ and T is a fundamental domain of L. Then, the volume of T, which is defined by the above basis, is given by the formula $v(T) = |det(a_{ij})|$.*

5.2 About non-unique factorization.

In this section, we are going to discuss how non-unique factorization is approached. In particular, we are going to use the geometric ideas developed earlier in this chapter and we are going to relate them to unique factorization.

Definition 5.3. The *class-group* of a number field is the quotient of fractional ideals by the (normal) subgroup of principal fractional ideas.

Definition 5.4. The *class-number* is the order of the class-group.

Kummer's introduction of "ideal numbers" is related to the fact that every ideal can become principal with the appropriate field extension. Many results in Number theory, including the proof of Kummer's special case of Fermat's Last Theorem, are highly connected to the idea of the class-number.

Theorem 5.2. *Let $\mathfrak{O}$ be the ring of integers, in a number field K, of degree n. Factorization in $\mathfrak{O}$ is unique if and only if the class-number h is equal to 1.*

Proof. The theorem 4.6 suggests that factorization in $\mathfrak{O}$ is unique, if and only if every ideal is principal or, equivalently, if and only if every fractional ideal is principal.

Let $\mathcal{F}$ be the group of fractional ideals under multiplication and $\mathcal{P}$ be the set of principal fractional ideals. Then, it suffices to prove that $\mathcal{F} = \mathcal{P}$. But, $\mathcal{F} = \mathcal{P}$ is equivalent to $|\mathcal{H}| = h = 1$, where $|\mathcal{H}|$ is the order of $\mathcal{H}$. □

Theorem 5.2 states that factorization in a ring of integers is unique if and only if the corresponding class-number is 1. In other cases, i.e. when the class-number is greater than 1, the factorization is not unique. In particular, larger class-number corresponds to more complicated non-uniqueness of factorization. Using the latter statement, non-uniqueness of factorization can be measured somehow.

Theorem 5.3. *Let $\mathfrak{O}$ be the ring of integers of K, which is a number field of degree $n = s + 2t$. Let $\mathfrak{a} \neq 0$ be an ideal of $\mathfrak{O}$. The volume of a fundamental domain for $\sigma(\mathfrak{a})$ (as defined in equation (5.1)) in L^{st} is equal to*

$$2^{-t}\ N(\mathfrak{a})\sqrt{|\Delta|},$$

where Δ is the discriminant of K.

Proof. If $\{a_1, \cdots, a_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$, then a $\mathbb{Z}$-basis for $\sigma(\mathfrak{a})$ in L^{st} is the following:

$$\begin{aligned} &(x_1^{(1)}, \cdots, x_s^{(1)}, y_1^{(1)}, z_1^{(1)}, \cdots, y_t^{(1)}, z_t^{(1)})\,, \\ &\quad\vdots \qquad\qquad\qquad\qquad\qquad\qquad , \\ &(x_1^{(n)}, \cdots, x_s^{(n)}, y_1^{(n)}, z_1^{(n)}, \cdots, y_t^{(n)}, z_t^{(n)})\,. \end{aligned}$$

Let T be a fundamental domain for $\sigma(\mathfrak{a})$. As a consequence of lemma 5.1, $v(T) = |D|$, where

$$D = \begin{vmatrix} {x_1}^{(1)} & \cdots & {x_s}^{(1)} & {y_1}^{(1)} & {z_1}^{(1)} & \cdots & {y_t}^{(1)} & {z_t}^{(1)} \\ & \vdots & & & & & & \\ {x_1}^{(n)} & \cdots & {x_s}^{(n)} & {y_1}^{(n)} & {z_1}^{(n)} & \cdots & {y_t}^{(n)} & {z_t}^{(n)} \end{vmatrix}.$$

Moreover,

$$|D| = 2^{-t}|E|, \text{ with } E^2 = \Delta[a_1, .., a_n].$$

According to equation (4.3) (see the aforementioned **Useful Results about Norms of Ideals**), it holds that

$$N(\mathfrak{a}) = |\Delta[a_1, \cdots, a_n]/\Delta|^{1/2}.$$

Thus,

$$v(T) = 2^{-t}\Delta[a_1, \cdots, a_n]^{1/2} = 2^{-t}N(\mathfrak{a})|\Delta|^{1/2}.$$

□

Theorem 5.4. *Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}$, $\mathfrak{a} \neq 0$. Then, $\mathfrak{a}$ contains an integer b, for which*

$$|N(b)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

Proof. Let $\epsilon > 0$. We choose

$$x_1, \cdots x_{s+t},\ x_i \in \mathbb{R},\ x_i > 0,\ \forall i \in [1, s+t].$$

By theorem 5.3, it follows that there is an integer $b \in \mathfrak{a}$, with $b \neq 0$ such that

$$|\sigma_1(b)| < x_1,\ \cdots,\ |\sigma_s(b)| < x_s \tag{5.2}$$

$$\text{and } |\sigma_{s+1}|^2 < x_{s+1}, \cdots,\ |\sigma_{s+t}^2 < x_{s+t}| \tag{5.3}$$

By multiplying (5.2) with (5.3), we get

$$|N(b)| < x_1 \cdots x_s x_{s+1} \cdots x_{s+t} < \left(\frac{4}{\pi}\right)^t 2^{-t}N(\mathfrak{a})\sqrt{|\Delta|}$$

$$\Rightarrow |N(b)| < x_1 \cdots x_s x_{s+1} \cdots x_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|} + \epsilon \tag{5.4}$$

However, it is known that every lattice is discrete. Therefore, if we define A_ϵ as the set of all integers b, we have that A_ϵ is finite. Of course $A_\epsilon \neq \emptyset$, which means that the union of A_ϵ, $\forall \epsilon$ is also nonempty. If we define this union of sets as $A = \bigcup_\epsilon A_\epsilon$ and choose $b \in A$, we get that

$$|N(b)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

□

Corollary 5.1. *Every ideal* $\mathfrak{a}$ *of* $\mathfrak{O}$, $\mathfrak{a} \neq 0$ *is equivalent to an ideal with norm less than or equal to*

$$\left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

Proof. Consider the class of fractional ideals which are equivalent to $\mathfrak{a}^{-1}$. This class contains an ideal $\mathfrak{c}$ such that $\mathfrak{ac} \sim \mathfrak{O}$. According to theorem 5.4, there is an integer $d \in \mathfrak{c}$ such that

$$|N(d)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{c})\sqrt{|\Delta|}. \tag{5.5}$$

Yet, $\mathfrak{c}|d$ and therefore there exists an ideal $\mathfrak{b}$ with $\langle d\rangle = \mathfrak{c} \cdot \mathfrak{b}$.

By equation (4.4) (see **Results of Norms**), it holds that $N(\mathfrak{b})N(\mathfrak{c}) = N(\mathbf{bc}) = N(\langle d\rangle) = |N(d)|$. Further, by inequality (5.5),

$$N(\mathfrak{b})N(\mathfrak{c}) \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{c})\sqrt{|\Delta|}$$
$$\Rightarrow N(\mathfrak{b}) \leq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

Moreover, $\mathfrak{b} \sim \mathfrak{c}$, since $\mathfrak{c} \sim \mathfrak{a}^{-1}$ and $\mathfrak{b} \sim \mathfrak{c}^{-1}$. Therefore, the proof is completed. □

Theorem 5.5. *The class-group of a number field is a finite abelian group and the class-number is finite.*

Proof. Consider a number field K with discriminant Δ and degree $n = s + 2t$. The class group $\mathcal{H} = \mathcal{F}/\mathcal{P}$ is an abelian group. We have to prove that it is also finite. Let us define $[\mathfrak{c}]$ as an equivalence class. There is an ideals $\mathfrak{a}$ that is contained in $[\mathfrak{c}]$. As a consequence of corollary 5.1, $\mathfrak{a}$ is equivalent to an ideal $\mathfrak{b}$, such that

$$N(\mathfrak{b}) \leq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

As stated in theorem 4.5, only a finite number of ideals have a given norm. Therefore, there is only a finite number of choices for the ideal $\mathfrak{b}$. Further, it holds that

$$\begin{aligned} &\mathfrak{c} \sim \mathfrak{a} \sim \mathfrak{b} \\ \Rightarrow &[\mathfrak{c}] = [\mathfrak{a}] = [\mathfrak{b}] \,. \end{aligned}$$

Hence, there is a finite number of equivalence classes $[\mathfrak{c}]$, which is equivalent to $\mathcal{H}$ being a finite group. Thus, the class-number $h = |\mathcal{H}|$ is finite. □

One can find a more elementary proof of finiteness of the class-number in Ref. [12].

Proposition 5.1. *Let K be a number field of class-number h and let $\mathfrak{a}$ be an ideal of $\mathfrak{O}$. Then*

(a) $\mathfrak{a}^h$ is a principal ideal.

(b) If q is prime to h and $\mathfrak{a}^p$ is principal, then $\mathfrak{a}$ is principal.

Proof. (a): It holds that $h = |\mathcal{H}| \Rightarrow [\mathfrak{a}]^h = [\mathfrak{O}]$, $\forall$ $[\mathfrak{a}] \in \mathcal{H}$, since $[\mathfrak{O}]$ is the identity element of $\mathcal{H}$. Thus, $[\mathfrak{a}^h] = [\mathfrak{a}]^h = [\mathfrak{O}] \Rightarrow \mathfrak{a}^h \sim \mathfrak{O} \cdot \mathfrak{a}^h$, which means that $\mathfrak{a}^h$ is principal.

(b): We choose u, $v \in \mathbb{Z}$ such that $uh + vq = 1$. Therefore,

$$\begin{aligned} &[\mathfrak{a}]^q = [\mathfrak{O}] \\ \Rightarrow &[\mathfrak{a}] = [\mathfrak{a}]^{uh+vq} = ([\mathfrak{a}]^h)^u ([\mathfrak{a}]^q)^v = [\mathfrak{O}]^u [\mathfrak{O}]^v = [\mathfrak{O}], \end{aligned}$$

from which it follows that $\mathfrak{a}$ is principal.

□

By attempting to compute the class-number, many results have been produced.

Theorem 5.6. *(Dedekind) Let K be a number field of degree n, with ring of integers $\mathfrak{O} = Z[\theta]$, where θ is an element of $\mathfrak{O}$. Let p be a rational prime, f the minimum polynomial of θ over $\mathbb{Q}$, which causes the factorization into irreducibles over Z_p, as shown below*

$$\bar{f} = f_1^{\bar{e}_1} \cdots f_r^{\bar{e}_r},$$

where the bar symbolizes the natural map: $Z[t] \to Z_p[t]$. If $f_i \in Z[t]$ is a polynomial mapping onto $\bar{f}_i$, then the ideal $\mathfrak{p}_i = \langle p \rangle + \langle f_i(\theta) \rangle$ is prime and $\langle p \rangle$ factorizes in $\mathfrak{O}$ as $\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

Theorem 5.6 can be applied to quadratic and cyclotomic fields, which are of the form $Z[\theta]$, as well as many other fields. In particular, it provides a useful method for computing the factorization of $\bar{f}$, in a finite number of steps. Actually, if p is a prime number in $\mathbb{Z}$, it is not always true that $\langle p \rangle$ is a prime ideal in $\mathfrak{O}$. Thus, the need to factorize $\langle p \rangle$ arises. Let us investigate an example.

Example: In $\mathbb{Q}(\sqrt{-1})$, with ring of integers $\mathfrak{O} = \mathbb{Z}(\theta)$ $(\theta = \sqrt{-1})$, we are interested in factorizing $\langle 2\rangle$. The minimum polynomial of θ is t^2+1. Since $t^2+1 = (t+1)^2$ $(mod\, 2)$, according to Dedekind's theorem (5.6),
$\langle 2\rangle = \mathfrak{p}^2$, for some prime ideal $\mathfrak{p}$, such that $\mathfrak{p} = \langle 2\rangle + \langle\sqrt{-1}+1\rangle$. But, $2 = (1+\sqrt{-1})(\sqrt{-1}+1)$. Therefore, $\mathfrak{p} = \langle 1+\sqrt{-1}\rangle$ and finally $\langle 2\rangle = \langle 1+\sqrt{-1}\rangle^2$.
■

Theorem 5.7. *Let $\mathfrak{a} \neq 0$ be an ideal of $\mathfrak{O}$. Then, $\mathfrak{a}$ contains an element b, with norm*

$$|N(b)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\Delta|}\ N(\mathfrak{a}).$$

Definition 5.5. *Minkowski constants* are the constants given by the formula

$$M_{st} = \left(\frac{4}{\pi}\right)^t \frac{(s+2t)!}{(s+2t)^{s+2t}}\ . \tag{5.6}$$

Theorem 5.8. *Let $\mathfrak{O}$ be the ring of integers of a number field K of degree $n = s+2t$ and suppose that $\forall p \in Z$, p prime, with $p \leq M_{st}\sqrt{|\Delta|}$, every prime ideal dividing $\langle p\rangle$ is principal. Then, $\mathfrak{O}$ has class-number equal to* 1.

Theorem 5.8 provides a useful criterion for $h = 1$. Next, we will give some specific numerical applications of this theorem. In particular, 5.8 combined with 5.6 can lead to computational methods in cases with small degree and discriminant.

Example of application of theorems 5.6 and 5.8: In $\mathbb{Q}(\sqrt{-19})$, the ring of integers is $\mathbb{Z}(\theta)$ and θ is a root of the polynomial

$$t^2 - t + 5. \tag{5.7}$$

Therefore, the degree is $2 = 0 + 1\cdot 2$ and the discriminant is -19. Minkowski constants can be calculated directly by equation (5.6), for $s = 0$, $t = 1$,

$$\begin{aligned} M_{st} &= \left(\frac{4}{\pi}\right)^1 \frac{(0+2\cdot 1)!}{(0+2\cdot 1)^{0+2\cdot 1}} = \frac{2}{\pi} \simeq 0.637 \\ M_{st}\sqrt{|\Delta|} &= M_{st}\sqrt{|-19|} \simeq 2.777. \end{aligned}$$

Hence, theorem 5.8 provides information for prime p less or equal to 2.777, equivalently for $p \leq 2$. Next, we are going to use theorem 5.6. Since polynomial (5.7) is irreducible, modulo 2, $\langle 2\rangle$ is prime in $\mathfrak{O}$. This means that if a prime ideal divides $\langle 2\rangle$, then it is equal to $\langle 2\rangle$, hence principal. Polynomial (5.7) is also irreducible, modulo 3. Therefore, theorem 5.8 suggests that the class-number of $\mathfrak{O}$ is 1. ■

In 1801, in his "Disquisitiones Arithmeticae"[1], Gauss introduced several conjectures some of which remain unproved until today. In 1934, Heilbronn

[1] For the translated in English work (Arithmetical Investigations) see Ref [6].

proved the "Gauss Conjecture" that $h(d) \to \infty$, as $d \to -\infty$. Also, in 1934, Heilbronn and Linfoot came up with the following theorem Ref. [9].

Theorem 5.9. *(Heilbronn-Linfoot theorem) The class-number of* $\mathbb{Q}(\sqrt{d})$ *is equal to* 1 *for* $d = -1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163$ *and exactly one more (unknown for now)* $d < 0$.

Definition 5.6. *Gauss' Class-Number one problem* is described as the problem of finding every complex quadratic field, which has class-number equal to 1.

Additionally, Gauss conjectured that there are infinitely many real quadratic fields with class-number one, which is not solved up to this day.

Gauss' Class-Number one problem was solved by Baker and Stark in 1967, although Heegner had already given almost the proof in 1952.

Theorem 5.10. *(Baker–Heegner–Stark theorem) The class-number of* $\mathbb{Q}(\sqrt{d})$ *is equal to* 1*, if and only if*

$$d = -1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163.$$

For further details on theorem 5.10 and Gauss Class Number problem, I refer the reader to Refs. [14], [17], [16], [1], [8].

Later on, the problem was connected to $L-$ functions of elliptic curves. Let us present a much stronger result, which was given by Gross and Zagier, see Ref. [7] .

Theorem 5.11. *(Goldfeld-Gross-Zagier)*

For every $\epsilon > 0$*,* $\exists c > 0$ *(which can be computed effectively) such that*

$$h(d) > c \cdot |log|d||^{1-\epsilon}.$$

Chapter 6

Special cases of Fermat's Last Theorem before Kummer

We present in this chapter some special cases of FLT, which have been proved before Kummer. We would like to stress the difference in the way of proving cases of Fermat's Last Theorem before and after Kummer.

It is clear that for $n = 2$ there are infinite examples of integers satisfying the Diophantine equation. These are the so-called Pythagorean triples. It has been revealed that Babylonians have calculated these triples, earlier than Pythagoras, with an unknown until now way. Apart from the case $n = 2$, we will present some other $n's$, which were proved (or almost proved) before Kummer.

6.1 Fermat ($n = 4$)

The case n=4 is the only proof that was ever given by Fermat. Actually the proof was not published by Fermat himself. Fermat's son, Samuel, published it after his father's death together with other mathematical work done by Fermat.

Remarks:

(a) If there is a solution to the Diophantine equation

$$x^n + y^n = z^n, \tag{6.1}$$

then there is also a solution to this equation, where x, y, z are pairwise coprime.

(b) If equation (6.1) is impossible for an exponent n, then it is also impossible for every exponent kn, where k is an integer.

(c) Every integer $n > 2$ is divisible by 4 or by an odd prime.

As a consequence of remarks (b) and (c), FLT may be reduced to the following: *Equation* (6.1) *is impossible for* $n = 4$ *and for every* n *odd prime.*

In order to prove the case $n = 4$ of FLT, we need the following lemma.

Lemma 6.1. *The solutions of the well known equation*

$$x^2 + y^2 = z^2, \tag{6.2}$$

where the integers x, y, z *are pairwise coprime, are given by*

$$x = 2rs,\ y = r^2 - s^2,\ z = r^2 + s^2, \tag{6.3}$$

where, r, s *are coprime and exactly one of them is odd.*

Proof. Consider $x, y, z > 0$ and note that they cannot all be odd (because $odd^2 = odd$, $even^2 = even$ and $odd + odd = even$). Thus, because of the fact that they are pariwise coprime, only one of them can (and should) be even.

- If we consider the case when z is even, therefore x, y are odd, there exist integers a, b, c, such that $x = 2a + 1$, $y = 2b + 1$, $z = 2c$. This leads equation (6.2) to a contradiction, i.e.

  $$\begin{aligned} (2a + b)^2 + (2b + 1)^2 &= (2c)^2 \qquad (6.4) \\ \Leftrightarrow 2(a^2 + a + b^2 + b) + 1 &= 2c^2, \end{aligned}$$

  which is impossible.

  We are left with two possible cases.

- We consider the case, in which x is even, while y, z are odd.

  Equation (6.2) can be rewritten as

  $$x^2 = z^2 - y^2 = (z - y)(z + y). \tag{6.5}$$

  Since $x, z + y, z - y$ are all even and positive, there exist u, v such that $x = 2u$, $z + y = 2v$, $z - y = 2w$. Therefore, we get

  $$\begin{aligned} \text{eq. (6.5)} &\Rightarrow (2u)^2 = (2v)(2w) \\ &\Rightarrow 4u^2 = 4vw \\ &\Rightarrow u^2 = vw. \qquad (6.6) \end{aligned}$$

  Note that $v = \dfrac{z + y}{2}$, $w = \dfrac{z - y}{2}$ are coprime.

  For if there was a common factor k such that $k|v$ and $k|w$, then

  $$\begin{aligned} &k|v + w \text{ and } k|v - w \\ \Leftrightarrow\, &k|z \text{ and } k|y \\ \Leftrightarrow\, &\text{z,y are not coprime, which is a contradiction.} \end{aligned}$$

Then, we factorize u, v, w into prime factors

$$\text{eq. (6.6)} \Rightarrow (p_1 p_2 \cdots p_{k1})^2 = (l_1 l_2 \cdots l_{k2})(m_1 m_2 \cdots m_{k3}). \tag{6.7}$$

Keeping in mind that v, w are coprime, they need to be squares, so that (6.7) is true. Therefore, there are r, s such that $v = r^2$ and $w = s^2$. It follows that r, s are also coprime, since v, w are coprime. Thus,

$$z = v + w = r^2 + s^2, \qquad y = v - w = r^2 - s^2.$$

Finally, since $y,\ z$ are odd, one of $r,\ s$ is odd. Indeed:

- If $r,\ s$ are even, then,

  $$z = (2a)^2 + (2b)^2,$$

  which means that z is even, that is contradicting our hypothesis.
- If $r,\ s$ are odd, then,

  $$z = (2a + 1)^2 + (2b + 1)^2,$$

  which means again z is even, that is contradicting our hypothesis.
- If r is even and s is odd (or r is odd and s is even), then

  $$z = (2a)^2 + (2b + 1)^2,$$

  which verifies that z is odd. This is the only acceptable case.

From equation (6.5) follows that

$$x^2 = (z - y) \cdot (z + y) = 2(s^2) \cdot 2(r^2) = 4 \cdot r^2 s^2,$$

where $x > 0$. Therefore, $x = 2rs$.

- In a similar way with the above case, it can be shown that when y is even and $x,\ z$ are odd, formulas (6.3) are satisfied.

□

Theorem 6.1. *Equation*

$$x^4 + y^4 = z^2 \tag{6.8}$$

has no integer solutions for $x, y, z \neq 0$.

Proof. We can rewrite equation (6.8) as follows

$$(x^2)^2 + (y^2)^2 = z^2.$$

The above is a Pythagorean equation.

According to lemma 6.1 and assuming without loss of generality that x is even, while y, z are odd, we get that $\exists\ r, s$ coprime, with only one of them odd, such that

$$x^2 = 2rs, \tag{6.9}$$
$$y^2 = r^2 - s^2, \tag{6.10}$$
$$z = r^2 + s^2. \tag{6.11}$$

We assume that r is odd and s is even. Equation (6.9) implies that $\exists\ c, d \in \mathbb{Z}$ such that $r = c^2,\ s = 2d^2$.

Moreover,

$$\text{eq. } (6.10) \Rightarrow y^2 = c^4 - 4d^4. \tag{6.12}$$

Equation (6.12) is equivalent to $(2d^2)^2 + y^2 = (c^2)^2$, which is a Pythagorean equation. Again lemma 6.1 implies that $\exists\ e, f$ coprime, with one of them odd, such that

$$2d^2 = 2ef \Leftrightarrow d^2 = ef, \tag{6.13}$$
$$y = e^2 - f^2, \tag{6.14}$$
$$c^2 = e^2 + f^2. \tag{6.15}$$

Since e, f are coprime, equation (6.13) implies that $\exists\ u, v \in \mathbb{Z}$ such that $e = u^2$, $f = v^2$. Then,

$$\text{eq. } (6.15) \Leftrightarrow c^2 = u^4 + v^4. \tag{6.16}$$

Obviously, equation (6.16) is an equivalent formula to equation (6.8).

At this point, Fermat made the important observation that $c < z$. This means that for every solution $(x,\ y,\ z)$ of equation (6.8), there is a *smaller* one (u, v, c), where $x,\ z,\ y,\ u,\ v,\ c$ are positive integers. This is impossible. The method used for this proof is called *method of infinite descent.* □

Proof of FLT, for $n = 4$: Theorem 6.1 implies that there are no integer solutions of equation (6.8). Suppose that equation (6.1) has solution for $n = 4$, equivalently that there exist $a, b, c \in \mathbb{Z}$ such that $a^4 + b^4 = c^4$. Then, $\exists\, d \in \mathbb{Z}$ such that $d = c^2$. Hence, $a^4 + b^4 = d^2$, which contradicts theorem 6.1. ■

6.2 Euler ($n = 3$)

This section presents Euler's proof of FLT, even if it contains a serious mistake. It is interesting to compare this proof with the methods used later, by Sophie Germain and by Kummer, in order to appreciate the progress made in Algebraic Number Theory.

Theorem 6.2. *Fermat's Last Theorem is true for exponent $n = 3$. Equivalently, equation*

$$x^3 + y^3 = z^3 \tag{6.17}$$

has no integer solutions.

Proof. Suppose that equation (6.17) has a solution $(x,\ y,\ z)$, where $x,\ y,\ z \in \mathbb{Z}$ pairwise relatively prime. This means that one and only one of the three is even.[1] We consider, without loss of generality, that z is even and $x,\ y$ are odd. Then, $x + y,\ x - y$ are even and can be written as

$$x + y = 2p,\ x - y = 2q \Leftrightarrow x = p + q,\ y = p - q.$$

Then,

$$\begin{aligned} \text{eq. (6.17)} &\Leftrightarrow (x+y)(x^2 + y^2 + 2xy) = z^3 \\ &\Leftrightarrow 2p[(p+q)^2 - (p+q)(p-q) + (p-q)^2] = z^3 \\ &\Leftrightarrow 2p(p^2 + 3q^2) = z^3. \end{aligned} \tag{6.18}$$

Note that:

- $p,\ q$ have opposite parity.

  Since $p + q$, $p - q$ are odd, they cannot have the same parity.

- $p,\ q$ are relatively prime.

  For if they have a common factor, then this would also divide $x,\ y$. But, we assumed earlier that $x,\ y$ are relatively prime.

- $p,\ q > 0$.

  Recall that

  $$p = \frac{x+y}{2}, \quad q = \frac{x-y}{2}. \tag{6.19}$$

  - If $x = y$, then $x = y = 1$, since they are relatively prime. Then, eq. (6.17) $\Leftrightarrow z^3 = 2$, which is impossible.
  - If $x > y$, then it follows directly from equations (6.19), that $p, q > 0$.
  - If $x < y$, then by interchanging them, we can still have $p, q > 0$.

To sum up until this point, we have proved that $\exists\ p, q > 0$, relatively prime, with opposite parity, such that $2p(p^2 + 3q^2) = z^3$ (see equation (6.18)).

We will consider, if there are any common factors between $2p$ and $p^2 + 3q^2$. Since p, q have opposite parity, $p^2 + 3q^2$ is odd, that can be trivially calculated.

[1] Since they are relatively prime, it cannot be that two of them or all of them is even. On the other hand, if two of them were odd, because of equation (6.17), the third one should be even.

Therefore, any common factor of $2p$ and p^2+3q^2, would also be common factor of p and p^2+3q^2. This means that this common factor would divide p but also $3q^2$, which can be trivially proved. Since $p,\ q$ are relatively prime, the only possible common factors which divide p and $3q^2$, or equivalently $2p$ and p^2+3q^2, is 3 and 1.

(i) Let us consider first the trivial case, where the common factor of $2p$, p^2+3q^2 is 1. In that case, we will prove that there is a smaller solution than $(x,\ y,\ z)$ for the original equation (6.17). Since $2p$, p^2+3q^2 are relatively prime, equation (6.18) implies that they must both be cubes.

A basic fact for sums of two squares is

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2.$$

In an analogous way, it has been proved (see Ref. [3]) that

$$(a^2+3b^2)(c^2+3d^2) = (ac-3bd)^2+3(ad+bc)^2. \tag{6.20}$$

Using formula (6.20), for $a=c$ and $b=d$ we get

$$\begin{aligned}(a^2+3b^2)^3 &= (a^2+3b^2)[(a^2-3b^2)^2+3(2ab)^2]\\ &= [a(a^2-3b^2)-3b(2ab)]^2+3[a(2ab)+b(a^2-3b^2)]^2\\ &= (a^3-9ab^2)^2+3(3a^2b-3b^3)^2.\end{aligned}$$

From the above formula, by setting

$$p=a^3-9ab^2,\ \ q=3a^2b-3b^3, \tag{6.21}$$

for random a,b, we get

$$p^2+3q^2=(a^2+3b^2)^3.$$

At that point, Euler assumed that this is the only way we can write p^2+3q^2 as a cube, but he failed to realize that this needed to be proved.[2]

Equation (6.21) suggests that

$$\begin{aligned}p=a(a-3b)(a+3b) \Leftrightarrow 2p &= 2a(a-3b)(a+3b), \qquad (6.22)\\ q &= 3b(a-b)(a+b).\end{aligned}$$

Moreover, it holds that

- $a,\ b$ are relatively prime. For if they had a common factor, that would also divide p and q, which is a contradiction, since $p,\ q$ are relatively prime.

[2] Euler's error is that he assumed that numbers of the form $a+b\sqrt{3}$, where $a,\ b\in\mathbb{Z}$ behave like integers. The main issue here is that unique factorization holds in $\mathbb{Z}$, but not in every algebraic field, as we have seen in chapter 3. However, Euler's proof happens to be correct, since unique factorization is unique in $\mathbb{Z}(\sqrt{3})$.

- $a,\ b$ are of opposite parities. For if they were of the same parity, then $p,\ q$ would both be even, which is a contradiction.
- $2a,\ a-3b,\ a+3b$ are relatively prime.
  - $2a$ is coprime with $a \pm 3b$.
    Both $a \pm 3b$ are odd, since a, b are of opposite parity. Therefore, if $2a, a \pm 3b$ have a common factor, this would also be a common factor of $a, a \pm 3b$. And then this factor would divide both a and b, which contradicts the fact that $a,\ b$ are relatively prime.
  - $a+3b$ is coprime with $a-3b$.
    For if they had a common factor, this would divide both a and b.
- Each one of $2a,\ a-3b,\ a+3b$ is a cube, since they are relatively prime and $2p$ is a cube. Thus, there exist $\alpha, \beta, \gamma \in \mathbb{Z}$, such that

  $$2a = \alpha^3, \tag{6.23}$$
  $$a-3b = \beta^3, \tag{6.24}$$
  $$a+3b = \gamma^3. \tag{6.25}$$

  eq. (6.22)$\Rightarrow$ $\alpha^3\beta^3\gamma^3 = 2a(a-3b)(a+3b) = 2p$. Additionally, eq. (6.18) $\Rightarrow$ $\alpha^3\beta^3\gamma^3 | z^3$. Therefore, $\alpha^3\beta^3\gamma^3 < z^3$. By adding together equations (6.24) with (6.25), we get

  $$\beta^3 + \gamma^3 = 2 \overset{(6.23)}{=} \alpha^3.$$

  This is another solution of the equation (6.17), which smaller than (x, y, z). Thus, by the method of infinite descent, we have proved that there is no integer solution to (6.17), for case (i).

(ii) In the case that $3|p$, we again conclude that there is a smaller solution of equation (6.17). The proof of this result is similar to the first case and can be found in Ref. [3].

Thus, it has been proved for both cases with the method of infinite descent. □

6.3 Sophie Germain

Sophie Germain contributed significantly to Number Theory and specifically to Fermat's Last Theorem. In contrast with previous approaches, Germain attempted to give a proof of FLT for infinitely many prime exponents. Her work led to dividing Fermat's Last Theorem into two cases:

FLT Case I: $x^n + y^n = z^n$ has no integer solutions such that $n \nmid x$, $n \nmid y$ and $n \nmid z$ at the same time.

FLT Case II: $x^n + y^n = z^n$ has no integer solutions such that n divides one and only one of $x,\ y,\ z$. Note that if n divides two of $x,\ y,\ z$, then it also divides the third one.

Theorem 6.3 (Sophie Germain's Theorem). *Let n be an odd prime and p an auxiliary prime, such that*

$$x^n + y^n + z^n \equiv 0 \ (mod\, p) \Rightarrow x \equiv 0 \ \ or\ y \equiv 0\ or\ z \equiv 0\ (mod\, p) \tag{6.26}$$

$$and\ \ x^n \equiv n\ (mod\, p)\ is\ impossible, \tag{6.27}$$

then FLT Case I *is true for this exponent n.*

Proof. Let n be an odd prime and p an auxiliary prime satisfying the conditions of the theorem.

Note that Fermat's Last Theorem for exponent n can be expressed equivalently as: "$x^n + y^n + z^n = 0$ is impossible for every triad of nonzero integers $(x,\ y,\ z)$."

Suppose that *FLT Case I* is not true for n. Equivalently, suppose that $\exists$ integers $x,\ y,\ z$ such that

$$x^n + y^n + z^n = 0, \tag{6.28}$$

where none of $x,\ y,\ z$ are divisible by n. We will show that the above assumptions lead to a contradiction.

Additionally, without loss of generality, we assume that $x,\ y,\ z$ are pairwise relatively prime. By reformulating equation (6.28), we get

$$\text{eq. } (6.28) \Leftrightarrow (-x)^n = y^n + z^n \tag{6.29}$$

$$\Leftrightarrow (-x)^n = (y+z)(y^{n-1} - y^{n-2}z + y^{n-3}z^2 - \cdots + z^{n-1}) \tag{6.30}$$

Since factors $y + z$ and $z^{n-1} - y^{n-2}z + y^{n-3}z^2 - \cdots + z^{n-1}$ are relatively prime, equation (6.30) implies that they are both of n^{th} power. Furthermore, equation (6.28) is equivalent to $(-y)^n = x^n + z^n$, as well as $(-z)^n = x^n + y^n$. Using the same argument as for equation (6.29), it follows that $\exists\ a_1,\ b_1,\ c_1,\ a_2,\ b_2,\ c_2$, such that

$$\begin{aligned} x &= -a_1a_2, \\ y &= -b_1b_2, \\ z &= -c_1c_2. \end{aligned}$$

Analytically, the relevant factors are written as

$$y + z = {a_1}^n, \tag{6.31}$$

$$z + x = {b_1}^n, \tag{6.32}$$

$$x + y = {c_1}^n, \tag{6.33}$$

$$\begin{aligned} y^{n-1} - y^{n-2}z + ... + z^{n-1} &= {a_2}^n, \\ z^{n-1} - z^{n-2}x + ... + x^{n-1} &= {b_2}^n, \\ x^{n-1} - x^{n-2}y + ... + y^{n-1} &= {c_2}^n. \end{aligned}$$

Since $x^n + y^n + z^n \equiv 0\ (mod\, p)$, because of initial assumption (6.26), it holds that one of $x,\ y,\ z$ is equal to $0\,(mod\, p)$. Without loss of generality, suppose that

$$\begin{aligned} x &\equiv 0\,(mod\, p) \\ \Rightarrow 2x &\equiv 0\,(mod\, p) \\ \Rightarrow \text{eq. } (6.32) + \text{eq. } (6.33) - \text{eq. } (6.31) \equiv 2x &\equiv 0\,(mod\, p) \\ \Rightarrow {b_1}^n + {c_1}^n + (-a_1)^n &\equiv 0\,(mod\, p). \end{aligned} \tag{6.34}$$

As a consequence of assumption (6.26) of the theorem, equation (6.34) leads to

$$a_1 \equiv 0 \ \text{ or } \ b_1 \equiv 0 \ \text{ or } \ c_1 \equiv 0\,(mod\, p).$$

- Suppose that $b_1 \equiv 0\,(mod\, p)$. Then, $y = -b_1 b_2 \equiv 0\,(mod\, p)$. Since $x \equiv 0\,(mod\, p)$, the latter contradicts the fact that $x,\ y$ are relatively prime.

- If $c_1 \equiv 0\,(mod\, p)$ we are led to a contradiction in a similar way.

- Let us consider the last possible case, i.e.

  $$\begin{aligned} a_1 &\equiv 0\,(mod\, p) \\ \Rightarrow y \equiv -z\,(mod\, p) \text{ and } {a_2}^n &\equiv n y^{n-1} \equiv n {c_2}^n\,(mod\, p). \end{aligned}$$

  Since $c_2 \not\equiv 0\,(mod\, p)$, $\exists\ k \in \mathbb{Z}$ such that

  $$\begin{aligned} c_2 k &\equiv 1\,(mod\, p) \\ \Rightarrow (a_2 k)^n &\equiv n\,(mod\, p). \end{aligned} \tag{6.35}$$

  Equation (6.35) contradicts the initial assumption (6.27) of the theorem, i.e. that equation $x^n \equiv n\,(mod\, p)$ is impossible. And the theorem is proved.

□

For more information on Germain's work on Number Theory, see Refs. [10] and [2].

Chapter 7

Kummer's special case of Fermat's Last Theorem

7.1 A first approach to the problem.

In order to tackle FLT, many mathematicians started with the idea of expressing $x^p + y^p$ as a product of pairwise relatively prime factors. It holds that

$$x^p + y^p = (x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{p-1} y),$$

where $\zeta \in \mathbb{C}$ represents the p_{th} root of unity, given by the following formula

$$\zeta = \cos(2\pi/p) + i \sin(2\pi/p).$$

Let us present two useful facts about ζ:

(a) There are exactly p p_{th} roots of unity and each one is a power of ζ.

(b) $1 + \zeta + \cdots + \zeta^{p-1} = 0$.

Kummer considered complex numbers, which can be obtained from ζ and the rational numbers, using the operations of addition, subtraction, multiplication and division. In this way, he produced numbers of the following form[1]

$$a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2}. \tag{7.1}$$

Definition 7.1. The numbers of the form (7.1), with $a_i \in \mathbb{Z}$, are called *cyclotomic integers* of $\mathbb{Q}(\zeta)$. Cyclotomic integers form the ring $\mathbb{Z}[\zeta]$.

It is true that, if $a \in \mathbb{Z}$, then a is a cyclotomic integer. Although divisibility of cyclotomic integers is very similar to the one of ordinary integers, there are two important differences:

[1] In equation (7.1), the term including ζ^{p-1} is ommited, since it can be expressed using formula (b).

1. the presence of units, which are different than ±1, in $\mathbb{Z}(\zeta)$,
2. the fact that unique factorization is not warranted for cyclotomic integers. The first example of this failure, which was discovered by Kummer, is the field of 23_{rd} roots of unity.

The need to prove that factors

$$(x+y),\ (x+\zeta y),\ (x+\zeta^2 y),\ \cdots,\ (x+\zeta^{p-1}y) \tag{7.2}$$

should be of p_{th} power, inspired Kummer to invent *ideal numbers.* Then, factors (7.2) are p_{th} powers of these ideals numbers, since he proved that unique factorization holds for ideal numbers.

7.2 Regular Primes

Kummer introduced regular primes. As we will present in section 7.3, Kummer succeeded to prove FLT in the case when the exponent is a regular prime and it does not divide any of $x,\ y,\ z$.

Definition 7.2. A *regular prime* is a prime number which does not divide the class-number $h(p)$ of the cyclotomic field $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/p}$ is a primitive p_{th} root of unity.

As we have stated earlier, FLT can be reduced to the following: *Equation* $x^n + y^n = z^n$ *is impossible for* $n = 4$ *and for every* n *odd prime.* Since FLT for case $n = 4$ was proved by Fermat (see section 6.1), we are only interested in the case where the exponent is an odd prime.

The first few regular odd primes are: 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 43, 47, 53, 61, 71, 73, 79, 83, 89, 97, 107, 109, 113, 127, 137, 139, 151, 163, 167, 173, 179, 181, 191, 193, 197, 199, $\cdots$

Definition 7.3. A prime which is not regular is called *irregular prime.*

The first few irregular primes are: 37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293, 307, 311, 347, 353, 379, 389, 401, 409, 421, 433, 461, 463, 467, 491, 523, 541, 547, 557, 577, 587, 593, $\cdots$

Some interesting facts about regular and irregular primes:

- "There are infinitely many regular primes."(*Conjecture*)

  More precisely, Carl Ludwig Siegel in (1964) (see Ref. [15]) conjectured that $e^{-1/2}$, or about 60.65% of all prime numbers, are regular in the asymptotic sense of natural density. Neither conjecture has been proved up to date.

- *"There are infinitely many irregular primes."*(Theorem)

  This theorem was proved by Jensen in 1915 and later by Carlitz in 1954. Actually, Jensen had proved a stronger result in 1915: that there exists an infinite number of irregular primes p such that $p \equiv 3\,(mod\,4)$.

Definition 7.4. The *Bernoulli numbers* B_n are a sequence of signed rational numbers that can be defined by the exponential generating function

$$\frac{x}{(e^x-1)}=\sum_{n=0}^{\infty}\frac{B_n x^n}{n!}.$$

The Bernoulli numbers are a special case of the Bernoulli polynomials.

The Bernoulli number B_n can also be defined by the contour integral

$$B_n=\oint \frac{n!}{2pi\, i}\frac{z}{(e^z-1)}\frac{1}{z^{(n+1)}}dz,$$

where the contour encloses the origin, has radius less than $2\pi i$ (to avoid the poles at $\pm 2\pi i$), and is traversed in a counterclockwise direction.

For every even $n \neq 0$, if $4|n$, then B_n is negative, otherwise it is positive. For every odd $n \neq 1$, $B_n = 0$. The first few Bernoulli numbers B_n are: $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42$, $B_8 = -1/30$, $B_{10} = 5/66$, $B_{12} = -691/2730$, $B_{14} = 7/6$, $B_{16} = -3617/510$, $B_{18} = 43867/798$,
$B_{20} = -174611/330$, $B_{22} = 854513/138$.

Kummer's Criterion for regularity: A number p is not a regular prime if and only if p divides the numerator of the Bernoulli number B_k for some $k \in \{2, 4, 6, \cdots, p-3\}$.

Using the above criterion, Kummer proved that the only irregular primes which are less than 100 are $37, 59, 67$. Later, he showed that 101, 103, 131, 149, 157 are the only irregular primes less than 164.

7.3 Kummer's proof

In this section, an analytical proof of Kummer's special case of Fermat's Last Theorem is presented. We are going to use three lemmas for Kummer's proof.

Definition 7.5. As $\mathfrak{l}$ we define the ideal which is generated by λ, i.e. $\mathfrak{l} = \langle\lambda\rangle$, in the ring of integers $\mathbb{Z}[\zeta]$ of K.

Lemma 7.1. *$\mathfrak{l}^{p-1} = \langle p\rangle$ and $N(\mathfrak{l}) = p$.*

Lemma 7.2. *For every $a \in \mathbb{Z}[\zeta]$, $\exists\, b \in \mathbb{Z}$, such that $a^p \equiv b$ (mod $\mathfrak{l}^p$), where $\mathfrak{l} = \langle\lambda\rangle = 1-\zeta$.*

Lemma 7.3. *(Kummer's Lemma) Every unit in $\mathbb{Z}[\zeta]$ can be written in the form $r\zeta^g$, where r is a real number and g is an integer.*

Proofs of lemmas 7.1, 7.2 and 7.3 can be found at Ref. [19].

Theorem 7.1. *(Kummer's Theorem) Let p be an odd regular prime. Then, there are no integers x, y, z satisfying the equation*

$$x^p + y^p = z^p,$$

such that $p \nmid x$, $p \nmid y$, $p \nmid z$.

Proof. Let us consider the equation

$$x^p + y^p + z^p = 0. \tag{7.3}$$

It is sufficient to show that there are no integer solutions for the equation (7.3), since then we can replace z by $-z$ in equation (7.3) and the theorem is proved. We will consider that there is a solution of equation (7.3), i.e. there are $x,\ y,\ z$ which satisfy equation (7.3) and also $x,\ y,\ z$ are prime to p. If we factortize equation (7.3) in $\mathbb{Q}(\zeta)$, we get

$$\prod_{j=0}^{p-1}(x+\zeta^j y) + z^p = 0$$

$$\Leftrightarrow \prod_{j=0}^{p-1}(x+\zeta^j y) = -z^p. \tag{7.4}$$

For the relation (7.4), we used the fact that $(x^p+y^p) = x(x+\zeta y)\cdots(x+\zeta^{p-1}y)$. By taking the ideals of the relation (7.4), we get

$$\prod_{j=0}^{p-1}\langle x+\zeta^j y\rangle = \langle z\rangle^p. \tag{7.5}$$

Claim: All the factors included in the product of (7.5) are coprime pairwise.

Proof of Claim: Consider $\mathfrak{p}$ as a prime ideal such that

$$\mathfrak{p}|\langle x+\zeta^k y\rangle \ \ \& \ \ \mathfrak{p}|\langle x+\zeta^l y\rangle, \text{ where } 0 \le k \le l \le p-1. \tag{7.6}$$

Relations (7.6) imply that the ideal $\mathfrak{p}$ includes the element

$$(x+\zeta^k y) - (x+\zeta^l y) = x + \zeta^k y - x - \zeta^l y = \zeta^k y(1-\zeta^{l-k}).$$

But, $(1-\zeta^{l-k})$ is an associate of $(1-\zeta)$ and ζ^k is a unit. Therefore, $\mathfrak{p}$ includes the element $y(1-\zeta) = y\lambda$. Since $\mathfrak{p}$ is a prime ideal, it follows that either $\mathfrak{p}|y$ or $\mathfrak{p}|\lambda$.

- In the case that $\mathfrak{p}|y$, equation (7.5) implies that $\mathfrak{p}|z$ also. However, $y,\ z$ are coprime integers. Hence, $\exists\ a,b \in Z$ such that

  $$az + by = 1. \tag{7.7}$$

  Since $y, z \in \mathfrak{p}$, (7.7) implies that $1 \in \mathfrak{p}$, which is a contradiction.

- In the case that $\mathfrak{p}|\lambda$, we note that $N(\mathfrak{l}) = p$ and now theorem 4.4 implies that $\mathfrak{l}$ is prime. Therefore, $\mathfrak{p}|\lambda \Rightarrow \mathfrak{p} = \mathfrak{l}$ and so $\mathfrak{l}|z$ and we have

  $$p = N(\mathfrak{l})|N(z) = z^{p-1}.$$

  Therefore, $p|z$, which contradicts with the hypothesis that $p \nmid z$.

We have proved that both cases fall to a contradiction, thus the claim is proved.■

Let us revisit equation (7.5). As a consequence of uniqueness of factorization for ideals, each factor of the product in equation (7.5) should be a p^{th} power of an ideal.[2] We can assume, e.g. for $j = 1$, that there exists an ideal $\mathfrak{a}$ such that

$$\langle x + \zeta y \rangle = \mathfrak{a}^p, \tag{7.8}$$

which directly implies that $\mathfrak{a}^p$ is principal. Now, since p is regular, $p \nmid h$, where h is the class-number of $\mathbb{Q}(\zeta)$. As a consequence of proposition 5.1, $\mathfrak{a}$ is also principal. Therefore, we can find δ such that $\mathfrak{a} = \langle \delta \rangle$. Equation (7.8) implies that

$$x + \zeta y = \epsilon \delta^p, \tag{7.9}$$

where ϵ is a unit. As a result of Kummer's Lemma 7.3, $\exists\, r \in \mathbb{R}$ and $g \in \mathbb{Z}$, such that $\epsilon = r\zeta^g$. Equation (7.9) implies that $x + \zeta y = r\ \zeta^g\ \delta^p$, $r \in \mathbb{R}$. Moreover, lemma 7.2 implies that, since $\delta \in \mathbb{Z}[\zeta]$ there exists $c \in \mathbb{Z}$, such that

$$\begin{aligned} \delta^p &= c\ (mod \mathfrak{l}^p) \\ \Rightarrow x + \zeta y &\equiv r\zeta^g c\ (mod \mathfrak{l}^p). \end{aligned} \tag{7.10}$$

Lemma 7.1 suggests that

$$\begin{aligned} \mathfrak{l}^{p-1} &= \langle p \rangle \\ \text{eq. (7.10)} &\Rightarrow x + \zeta y \equiv rc\zeta^g\ (mod\langle p \rangle) \\ &\Rightarrow \zeta^{-g}(x + \zeta y) \equiv rc\ (mod\langle p \rangle), && (7.11) \\ &\text{where we have multiplied by unit } \zeta^{-g}, \\ &\Rightarrow \zeta^{g}(x + \zeta^{-1} y) \equiv rc\ (mod\langle p \rangle), && (7.12) \\ &\text{where we have taken complex conjugates,} \\ &\overset{(7.11)-(7.12)}{\Rightarrow} x\zeta^{-g} + \zeta^{1-g}y - x\zeta^g - y\zeta^{g-1} \equiv 0\ (mod\langle p \rangle). && (7.13) \end{aligned}$$

Note that $(1 + \zeta)$ is a unit.[3]

Let us consider possible values of g in equation (7.13). If $g \equiv 0\ (mod\, p)$, we get that

$$\begin{aligned} \zeta^g &= 1 \\ \Rightarrow \zeta^{-g} &= 1 \\ \text{eq. (7.13)} \Rightarrow x1 + \zeta y - x1 - y\zeta^{-1} &= 0(mod\langle p \rangle) \\ \Rightarrow y(\zeta - \zeta^{-1}) &\equiv 0(mod\langle p \rangle) \\ \Rightarrow y(1 + \zeta)(1 - \zeta) &\equiv 0(mod\langle p \rangle). \end{aligned}$$

[2] Because on the right part of the equation, we have $\langle z \rangle^p$. Additionally, the claim which was proved earlier implies that all the aforementioned factors are pairwise coprime.

[3] This is proved by putting $t = -1$ in the polynomial equation $f(t) = (t - \zeta)(t - \zeta^2) \cdots (t - \zeta^{(p-1)})$.

Since $(1+\zeta)$ is a unit & $1-\zeta=\lambda$, the above relation reads

$$y\lambda \equiv 0(\,mod\langle p\rangle). \tag{7.14}$$

It holds that $\langle p\rangle = \langle\lambda\rangle^{p-1}$ & $p-1\geq 2$, since p is an odd prime. Thus $\lambda|y$. If we put norms at the above equation, we get that $p|y$, which contradicts an initial hypothesis of the theorem. Hence,

$$g \not\equiv 0(modp). \tag{7.15}$$

In a similar way, it can be proved that

$$g \not\equiv 1(modp). \tag{7.16}$$

We continue with equation (7.13) as follows. There exists $\alpha\in\mathbb{Z}[\zeta]$, such that

$$\begin{aligned} \alpha p &= x\zeta^{-g} + y\zeta^{1-g} - x\zeta^{g} - y\zeta^{g-1} \\ \Rightarrow \alpha &= \frac{x}{p}\zeta^{-g} + \frac{y}{p}\zeta^{1-g} - \frac{x}{p}\zeta^{g} - \frac{y}{p}\zeta^{g-1}. \end{aligned} \tag{7.17}$$

Note that p does not divide any of the exponents $-g,\ 1-g,\ g,\ g-1$. Additionally $\{1,\ \zeta,\ \zeta^2,\ \cdots,\ \zeta^{p-2}\}$ is a $\mathbb{Z}$-basis and $\alpha\in\mathbb{Z}[\zeta]$. Assume that all exponents $-g,\ 1-g,\ g,\ g-1$ are incongruent modulo p. This means that $x/p\in\mathbb{Z}$, which is impossible, since $p\nmid x$, by hypothesis. Thus, one pair of exponents is congruent modulo p. As a consequence of equations (7.15) and (7.16), it holds that $2g\equiv 1(mod\,p)$. Then,

$$\begin{aligned} \text{eq. (7.17)} \Rightarrow \alpha p\zeta^{g} &= \frac{x}{p}p\zeta^{g}\zeta^{-g} + \frac{y}{p}p\zeta^{g}\zeta^{1-g} - \frac{x}{p}p\zeta^{g}\zeta^{g} - \frac{y}{p}p\zeta^{g}\zeta^{g-1} \\ \Rightarrow \alpha p\zeta^{g} &= x + y\zeta - x\zeta^{2}g - y\zeta^{2g-1} \\ \Rightarrow \alpha p\zeta^{g} &= (x-y)\lambda \\ \Rightarrow |\alpha p\zeta^{g}| &= |(x-y)\lambda|. \end{aligned} \tag{7.18}$$

Equation (7.18) implies that $p|(x-y)$. Therefore,

$$x-y\equiv 0\,(mod\,p) \Rightarrow x\equiv y\,(mod\,p).$$

The symmetry of equation (7.3) delivers $y\equiv z\,(mod\,p)$. Hence,

$$0\equiv x^p+y^p+z^p\equiv 3z^p(\,mod\,p)$$

The above equation leads to $p=3$, since $p\nmid z$. We will show that this is impossible. Note that modulo 9, cubes of numbers that are prime to p (specifically $1,\ 2,\ 4,\ 5,\ 7,\ 8$) are congruent to ± 1.

Thus, if there is an integer solution to equation (7.3), it would lead to the following result

$$\pm 1\pm 1\pm 1\equiv 0\,(mod\,9).$$

This is impossible. Thus, it has been proved that there is no solution for equation (7.3) and the theorem is proved. □

Bibliography

[1] A. Baker. “Linear forms in the logarithms of algebraic numbers”. In: *Mathematika 13* (1966), pp. 204–216.

[2] Lane-Lise Daniloff. *The work of Sophie Germain and Niels Henrik Abel on Fermat’s Last Theorem.* Master Thesis, Department of Mathematics, University of Oslo, 2017.

[3] H. M. Edwards. *Fermat’s Last Theorem.* Springer-Verlag New York Inc, 1977.

[4] H. M. Edwards. *The background of Kummer’s proof of Fermat’s Last Theorem for regular primes.* Springer, 1975.

[5] John B. Fraleigh. *A First Course in Abstract Algebra.* Pearson, 1967.

[6] Carl Friedrich Gauss and Arthur A. Clarke. *Disquisitiones Arithmeticae.* Yale University Press, 1965.

[7] Dorian M. Goldfeld. “Gauss’ Class number problem for imaginary quadratic fields”. In: (1985).

[8] H. Heilbronn. “On the class-number in imaginary quadratic fields”. In: *Quart. J. Math. Oxford Ser. 5* (1934), pp. 150–160.

[9] H. Heilbronn and E. H. Linfoot. “On the imaginary quadratic corpora of class-number one”. In: *The Quarterly Journal of Mathematics* os-5.1 (Jan. 1934), pp. 293–301.

[10] Colleen Alkalay Houlihan. “Sophie Germain and Special Cases of Fermat’s Last Theorem”. In: (2014).

[11] N. Jacobson. *Basic Algebra I: Second Edition.* Dover Books on Mathematics. Dover Publications, 2012. ISBN: 9780486135229. URL: https://books.google.gr/books?id=JHFpv0tKiBAC.

[12] Serge Lang. *Algebraic Number Theory, 2nd edition.* Springer-Verlag New York Inc, 1994.

[13] T. Nagell. “The Diophantine equation $x^2 + 7 = 2^n$”. In: *Ark. Mat.* 4.2-3 (Apr. 1961), pp. 185–187. DOI: 10.1007/BF02592006. URL: https://doi.org/10.1007/BF02592006.

[14] Z. I. Borevic , I. R. Safarevic. *Number Theory.* Academic Press Inc, New York, 1966.

[15] C. L. Siegel. “Zum Beweise des Starkchen Satzes”. In: *Invent. Math. 5* (1968), pp. 169–179.

[16] H. M. Stark. “A complete determination of the complex quadratic fields of class-number one.” In: *The Michigan Mathematical Journal* 14.1 (1967), pp. 1–27.

[17] H. M. Stark. “The Gauss Class-Number Problems”. In: *Clay Mathematics Proceedings* 7 (2007).

[18] Ian Stewart. *The problems of mathematics.* Oxford University Press, 1987.

[19] Ian Stewart , David Tall. *Algebraic Number Theory and Fermat’s Last Theorem, 3rd edition.* A K Peters/CRC Press, 2001.

[20] Ιωάννης Αντωνιάδης και Αριστείδης Κοντογεώργης. *Θεωρία Αριθμών και εφαρμογές*. 2015. ISBN: 9786188212459.