Read Math

Kenji Nakagawa

July 2019

Introduction

Notes are based on the second edition of Number Fields by Daniel A. Marcus, and at times may reference Neukirch. These are not meant to be comprehensive, but rather serve as a summary.

1 Fermat's Conjecture

Fermat's last theorem has proved to be elusive, and to have inspired a great deal of algebraic number theory. It states that there does not exist nontrivial solutions to $x^n + y^n = z^n$ whenever $n > 2$. Kummer saw that the left hand side factored into $\prod_{i=1}^{p}(x + \zeta_p^i y)$, and naturally, wanted to show that $\mathbb{Z}[\zeta_p]$ had a unique factorization, and thus, that the case in which p does not divide x, y, or z. However, this is only true for regular primes.

Definition 1

A prime is *regular* if $p \nmid h$, where h denotes the class number of the ring $\mathbb{Z}[\zeta]$, which is the number of equivalence classes of the ideals, with equivalence between ideals A, B being defined $A \sim B$ iff $aA = bB,\ a \in A, b \in B$.

It can be shown that if $p \nmid x, y, z$ (referred to as Case 1 in this context, and Case 2 when p divides one of x, y, z), then there are no solutions given that $\mathbb{Z}[\zeta]$ is a unique factorization domain which implies that $x + y\zeta$ has the form $u\alpha^p$ for some $\alpha \in \mathbb{Z}[\zeta]$

2 Number Fields and Number Rings

Definition 2

A *number field* is a subfield of $\mathbb{C}$ having finite degree (dimension as a vector space) over $\mathbb{Q}$. We refer to $Q[\zeta]$, $Q[\sqrt{m}]$ as cyclotomic fields, and quadratic fields, with the latter having a subdistinction of real versus imaginary.

As a result of the following equivalences:

1. α is an algebraic integer
2. The additive group is finitely generated
3. α is a member of some subring of $\mathbb{C}$ having a finitely generated additive group
4. $\alpha A \subset A$ for some finitely generated additive subgroup $A \subset \mathbb{C}$

we can show that the sum and product of two algebraic numbers is yet another algebraic number. As a more general result, the ring of algebraic integers, notated as $\mathbb{A}$ in this text or, more commonly, as $\mathcal{O}$. Furthermore, we may denote the algebraic numbers over some ring as $\mathbb{A} \cup K$ or as $\mathcal{O}_K$.

Something that is rather intuitive, but is of note is that $\text{Gal}\left(\mathbb{Q}[\zeta_m]/\mathbb{Q}\right) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$. This implies that the Galois group is transitive, and furthermore, that the subfields correspond to the subgroups, as well as that when $m = p$, a prime, that it contains a unique subfield of each degree dividing $p-1$, and that there it contains a unique quadratic field, which are $\sqrt{\pm p}$ depending on p.

Sometimes it's useful to replace embeddings of a number field with automorphisms. One way to do his is to extend the number field to a normal extension of $\mathbb{Z}$, which is always possible. As a reminder, a normal extension is an extension that any irreducible polynomial in the original field is either still irreducible, or it factors completely into linear terms. As an example, $L = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$ is a normal extension of $\mathbb{Q}[\sqrt[3]{2}]$.

Definition 3

We define the trace and the norm as $T(\alpha) = \sum_i^n \sigma_i(\alpha)$ and $N(\alpha) = \prod_i^n \sigma_i(\alpha)$, where $\sigma_i(\alpha)$ is the image of α in the ith embedding.

It is easy to show that both are always rational based on the minimal polynomial, and to show that the norm of an algebraic integer is an integer.

Some applications of this is that in general (except for two cases), that the imaginary integer fields have the property that a number is a unit iff it has norm ± 1.

Definition 4

The relative trace and relative norm is essentially the same, T_K^L, N_K^L are the embeddings of L in $\mathbb{C}$ which keep K fixed.

Similarly to field extensions, the relative trace, and relative norm are also transitive.

Additionally, we define the discriminant of an n-tuple as $\text{disc}(\alpha_1, \ldots, \alpha_n = |\sigma_i(\alpha_j)|^2$, where σ_i are the embeddings of the field that α_i are in, where $|a_{ij}|$ represents the determinant of the matrix $[a_{ij}]$, which has a_{ij} in the standard position. By some linear algebra stuff, we can define $\text{disc}(\alpha_1, \ldots \alpha_n) = |T(\alpha_i \alpha_j)|$. This has some nice properties which include that if the argument are all algebraic integers, then it is an integer, and if the determinant is nonzero, then the arguments are linearly independent over the rationals.

3 Prime Decomposition in Number Rings

Definition 5

A *Dedekind domain* is an integral domain R such that

(a) R is Noetherian. This is equivalent to every ideal being finitely generated, every increasing sequence of ideals is eventually constant, or every non-empty set S of ideals has a maximal member ($\exists M \in S$ such that $M \subset I \in S \implies M = I$.

(b) Every nonzero prime ideal is a maximal ideal;

(c) R is integrally closed in its field of fractions $K = \{\alpha/\beta : \alpha, \beta \in R, \beta \neq 0\}$.

Theorem 6

Every number ring is a Dedekind domain

Proof. Every number ring, R, as well as its ideals, with number field K is a free abelian group of finite rank, implying the first condition. For the second condition, we need only prove that R/I is finite (in the case of I prime, this gives a finite field, implying maximality). Let $\alpha \in I$, then $N(\alpha) \in \mathbb{Z},\ m = \alpha\beta \implies \beta = \frac{m}{\alpha} \in K$. Furthermore, it can be shown that $\beta \in \mathbb{A}$. Since $R/(m)$ is finite, so is R/I. Finally observe that if α/β is a root of a monic polynomial over R, then it is an algebraic integer. Thus $\alpha/\beta \in K \cap \mathbb{A} = R$. $a * b$

□