Introduction to Algebraic Number Theory

Lev Kruglyak

Contents

1 Motivation

1.1 Fermat's last theorem

1.2 Primes of the form $x^2 + ny^2$

2 Number Fields

2.1 Norm and trace

2.2 Discriminants

2.3 Cyclotomic number fields

3 Prime Decomposition

3.1 Galois theory applied to prime decompositions

3.2 Decomposition and inertia groups

4 The ideal class group

A Galois theory

A.1 Field extensions

Definition A.1. A ***field extension*** is a pair of fields $K \subset L$, and denoted L/K. The ***degree***, or ***index*** of the field extension, denoted $[L : K]$ is defined as the dimension of L as a vector space over K. A field extension is said to be ***finite*** if it has finite degree, and said to be ***infinite*** otherwise.

For example, $\mathbb{C}$ is a degree two extension of $\mathbb{R}$, and an infinite extension of $\mathbb{Q}$. An important class of field extensions we are usually interested are those defined by polynomial equations; for instance $\mathbb{C}$ could be considered as the smallest field containing $\mathbb{R}$ which has a solution to the polynomial equation $x^2 + 1 = 0$. In general, a simple way to generate field extensions is to start with a base field and construct extension fields which contain roots to some irreducible polynomial in the base field. This is motivated by the following theorem:

Theorem A.2. *Given some field K and irreducible polynomial $p(x) \in K[x]$, there exists a field extension of K which contains some root of $p(x)$.*

Proof. Consider the ring $L = K[x]/(p(x))$. This is a field because $p(x)$ is irreducible and so $(p(x))$ is maximal. Then $p(\theta) = 0$ in L, where $\theta = x \mod p(x)$. Note that there is an isomorphic copy of K in L so this is a field extension. □

To better understand this extension field, we can try writing out all of its elements explicitly.

Theorem A.3. *Let $p(x) \in K[x]$ be an irreducible polynomial of degree n, and let L be the field $F[x]/(p(x))$. Let $\theta = x \mod p(x)$. Then $1, \theta, \theta^2, \ldots, \theta^{n-1}$ are a basis for L as a K-vector space, so $[L : K] = n$.*

For example if $K = \mathbb{R}$, $L = \mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. If we were to replace $\mathbb{R}$ with $\mathbb{Q}$, then L would be $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}(i)$, i.e. the field of fractions of the Gaussian integers.

Definition A.4. Let L be an extension of K and let $\alpha_1, \alpha_2, \ldots \in L$ be some elements. Then the smallest subfield of L containing both K and the elements $\alpha_1, \alpha_2, \ldots$, denoted $K(\alpha_1, \alpha_2, \ldots)$ is called the field ***generated by*** $\alpha_1, \alpha_2, \ldots$ ***over*** K***.***

Definition A.5. If the field L is generated by a single element α over K, i.e. $L = K(\alpha)$, then L is said to be a ***simple*** extension of K and the element α is called a ***primitive element*** for the extension.

Theorem A.6. *Let K be a field and $p(x) \in K[x]$ a irreducible polynomial. Suppose L is an extension field of K containing a root of $p(x)$. Then $K(\alpha) \cong K[x]/(p(x))$.*

Proof. Use the natural evaluation homomorphism $\varphi : K[x] \to K(\alpha)$. □

Theorem A.7. *Let $\varphi : K \to K'$ be a field isomorphism. Let $p(x) \in K[x]$ and $p'(x) \in K'[x]$ be the irreducible polynomial obtained by applying φ to the coefficients of $p(x)$. Let α be some root of $p(x)$ in some extension and β be some root of $p'(x)$. Then there is a natural isomorphism $\sigma : K(\alpha) \to K'(\beta)$ which sends α to β.*

A.1.1 Algebraic extensions

Definition A.8. An element $\alpha \in L$ is said to be ***algebraic*** over K if α is the root of a nonzero polynomial $p(x) \in K[x]$. Otherwise α is ***transcendental*** over K. The extension L/K is said to be ***algebraic*** if every element of L is algebraic over K.

A.1.2 Splitting Fields