Introduction to Algebraic Number Theory
Lecture 2

Andrei Jorza

2014-01-17

Today: overview of fields. Textbook here is `http://wstein.org/books/ant/ant.pdf`

1 Fields

(1.1) A field K is a ring such that $K - \{0\} = K^\times$ is the group of invertible elements. If L/K is a finite extension of fields (i.e., $L \supset K$) then $[L : K] = \dim_K L$. If $M/L/K$ are finite extensions then $[M : K] = [M : L][L : K]$.

(1.2) An element α is said to be algebraic over K is $P(\alpha) = 0$ for some monic $P \in K[X]$. For α algebraic the field $K(\alpha)$ is the minimal field containing both K and α. Every algebraic α has a minimal polynomial, monic in $K[X]$ obtained as the generator of the (proper) principal ideal in the PID $K[X]$ consisting of all polynomials which vanish at α, in which case $[K(\alpha) : K]$ equals the degree of this minimal polynomial.

Definition 1. A number field is defined to be a finite extension of $\mathbb{Q}$.

For any finite extension L/K of fields of characteristic 0 or of finite fields there exists a so-called primitive element $\alpha \in L$ such that $L = K(\alpha)$.

E.g., every quadratic extension L/K, by the quadratic formula, is of the form $L = K(\sqrt{\alpha})$ for some $\alpha \in K$.

(1.3) An extension L/K is said to be algebraic if every element of L is algebraic over K.

Fact 2. An element α is algebraic over K if and only if $K(\alpha)/K$ is an algebraic extension if and only if $K(\alpha)/K$ is a finite extension.

As an application we present:

Corollary 3. *If α is algebraic of degree d then*

$$K(\alpha) = K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} | a_i \in K\}$$

Proof. Every element of $K(\alpha)$ is of the form $P(\alpha)/Q(\alpha)$. Write $\beta = Q(\alpha)$. Since α is algebraic it follows that $K(\beta) \subset K(\alpha)$ is finite over K and so β is algebraic over K. Let $b_0 + b_1X + \cdots + b_mX^m$ be its minimal polynomial in which case $b_0 \neq 0$. Then

$$1/Q(\alpha) = \beta^{-1} = -b_0^{-1}(b_1 + b_2\beta + \cdots b_m\beta^{m-1}) \in K[\beta] \subset K[\alpha]$$

Thus $K(\alpha) = K[\alpha]$ and every polynomial of α can be reduced to a polynomial of degree at most $d - 1$ of alpha using the minimal polynomial of α over K. $\square$

Every field K has an algebraic closure $\overline{K}$ which is algebraically closed. If L is any algebraically closed field (such as $\mathbb{C}$) containing K then there is a unique algebraic closure $\overline{K} \subset L$ consisting of all the elements of L which are algebraic over K. This is how we will think of $\overline{\mathbb{Q}}$ as the closure of $\mathbb{Q}$ in $\mathbb{C}$.

(1.4) Embeddings. A number field $K/\mathbb{Q}$ can sit inside $\overline{\mathbb{Q}} \subset \mathbb{C}$ in more than one way. For example, $\mathbb{Q}(i) \to \mathbb{C}$ given by $a + bi \mapsto a \pm bi$ provides two distinct embeddings (i.e., injective homomorphisms) of fields which invary $\mathbb{Q}$.

Fact 4. If α is algebraic with minimal polynomial $f(X)$ over K then the embeddings of $K(\alpha)$ into $\overline{K}$ which fix K are parametrized by the roots of $f(X)$. If β is any root the associated embedding fixes K and takes α to β. This produces a unique isomorphism $K(\alpha) \cong K(\beta)$.

Theorem 5. *If L/K is finite there are exactly $[L : K]$ embeddings $L \to \overline{K}$ fixing K.*

If $M/L/K$ are finite extensions and α_i are the embeddings of L into $\overline{K}$ fixing K and τ_j are the embeddings of M into $\overline{L} = \overline{K}$ fixing L then the embeddings of M into $\overline{K}$ fixing K are $\sigma_i\tau_j$.

2 Number Rings

(2.1)

Definition 6. An algebraic integer is an element α satisfying $P(\alpha) = 0$ for some monic $P \in \mathbb{Z}[X]$. For a number field K we write $\mathcal{O}_K$ for the set of algebraic integers in K.

Recall Gauss' lemma that if $P \in \mathbb{Z}[X]$ is monic and irreducible in $\mathbb{Z}[X]$ then P is irreducible in $\mathbb{Q}[X]$.

(2.2)

Proposition 7. *An element α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a finite $\mathbb{Z}$-module.*

Proof. Done in class. See textbook Proposition 2.3.4 □

Corollary 8. *If α, β are algebraic integers then $\alpha \pm \beta, \alpha \cdot \beta$ are algebraic integers.*

Proof. Done in class. See textbook Proposition 2.3.5 □

The conclusion is that the set $\mathcal{O}_K$ of algebraic integers in the number field K is in fact a ring.