Algebraic Number Theory

Lecture 5, 5th November 2021

Last lecture:

Definition 2.2 Let $A \subseteq B$ be an extension of rings. An element $b \in B$ is called <u>integral over A</u>, if it satisfies a monic equation

$$x^n + a_1 x^{n-1} + \dots + a_n = 0 \quad , \; n \geq 1$$

with coefficients $a_i \in A$. The ring B is called integral over A if all elements $b \in B$ are integral over A.

Proposition 2.3 Elements $b_1, \dots, b_n \in B$ are all integral over A if and only if $A[b_1, \dots, b_n]$ is finitely generated as a A-module.

Corollary 2.5 If b_1 and b_2 are integral over A, then $b_1 + b_2$ and $b_1 \cdot b_2$ are also integral over A.

Definition 2.6 Let $A \subseteq B$ be a ring extension,

i) The ring $\overline{A} = \{ b \in B \mid b \text{ integral over } A \}$ is called the <u>integral closure of A in B</u>.

ii) If $\overline{A} = A$ then A is called <u>integrally closed</u> in B.

$K/\mathbb{Q}$ finite

K: alg. number field

$\mathcal{O}_K \subset K$

$\mathcal{O}_K$ = integral closure of $\mathbb{Z}$ in K.

Proposition 2.7. Let $A \subseteq B \subseteq C$ be two ring extensions. If B is integral over A and C is integral over B, then C is integral over A.

Proof: Let $c \in C$ with

$$c^n + b_1 c^{n-1} + \ldots + b_n = 0$$

for some $b_1, \ldots, b_n \in B$. Since $b_1 \ldots b_n$ are integral over A, we have by Prop. 2.3 that $R = A[b_1, \ldots, b_n]$ is a fin. gen. A-module. But $R[c]$ is a fin. gen. R-module and therefore also a fin. gen. A-module. By Prop. 2.3 c is therefore also integral over A. $\square$

Corollary 2.8

If $A \subset B$ is an extension of rings, then the integral closure $\bar{A}$ of A <u>in B</u> is integrally closed in B.

Proof: Let $\bar{\bar{A}}$ be the integral closure of $\bar{A}$. Then $A \subset \bar{A} \subset \bar{\bar{A}} \subset B$. By Prop. 2.7 we have $\bar{A}/A$ and $\bar{\bar{A}}/\bar{A}$ are integral $\Rightarrow$ $\bar{\bar{A}}/A$ integral $\Rightarrow$ $\bar{\bar{A}} \subset \bar{A} \Rightarrow \bar{\bar{A}} = \bar{A}$ $\square$

We will recall some facts about fields and the construction of the field of fractions.

Definition 2.9

Let R be a com. unitary ring and let $S \subset R$ be a multiplicative set, i.e $1 \in R$ and $x, y \in S \Rightarrow x \cdot y \in S$.

On $R \times S$ we define the following equivalence relation

$$(r, s) \sim (r', s') :\Longleftrightarrow \exists t \in S : t(rs' - r's) = 0.$$

We define the <u>localization of R by S</u> as the set of equivalence classes

$$S^{-1}R := R \times S / \sim .$$

We write the elements (r,s) of $S^{-1}R$ as fractions $\frac{r}{s}$. $S^{-1}R$ is a com. unitary ring with

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'}$$

$$\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$$

and $0 = \frac{0}{1}$, $1 = \frac{1}{1}$.

<u>Remark 2.10</u> i) The map

$$\varphi_S : R \longrightarrow S^{-1}R$$
$$r \longmapsto \frac{r}{1}$$

is a ring homomorphism.

If $0 \in S$ $\Rightarrow S^{-1}R = \{0\}$

φ_S is injective iff S does not contain zero divisors.

We have $\varphi_S(S) \subset (S^{-1}R)^\times$ since $\left(\frac{s}{1}\right)^{-1} = \frac{1}{s}$ for $s \in S$

(In general $\not\subseteq$
e.g. $S = \{1, 4, 4^2, \dots\}$, $2 \in (S^{-1}\mathbb{Z})^\times$)

ii) If R is a domain then $S = R \setminus \{0\}$ is a multiplicative set. In this case $S^{-1}R$ is a field, called the <u>field of fractions of R</u> and denoted by $\mathrm{Frac}(R) := S^{-1}R$.

In particular $\varphi_S : R \to \mathrm{Frac}(R)$ is injective and we can view R as a subring of $\mathrm{Frac}(R)$.

e.g. $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

iii) If $\mathfrak{p} \subset R$ is a prime ideal then

$S_{\mathfrak{p}} := R \setminus \mathfrak{p}$ is multiplicative, since

$1 \notin \mathfrak{p}$ and $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

implies $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p} \Rightarrow xy \notin \mathfrak{p}$.

The localization of R by $S_{\mathfrak{p}}$ is denoted by

$$R_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1} R.$$

This is a so-called <u>local ring</u>, which means that it has exactly one maximal ideal given by

$$m = \left\{ \frac{r}{s} \,\middle|\, s \notin \mathfrak{p},\ r \in \mathfrak{p} \right\}.$$

Definition 2.11 Let A be a domain with field of fractions $K = \mathrm{Frac}(A)$.

i) The integral closure $\overline{A}$ of A in K is called the <u>normalization of A</u>.

ii) If $A = \overline{A}$ then A is simply called <u>integrally closed</u>.

Proposition 2.12 Every factorial ring (UFD) is integrally closed.

Proof: Let A be a UFD and $K = \mathrm{Frac}(A)$. If $\frac{a}{b} \in K$ is integral over A, then

$$\left(\frac{a}{b}\right)^n + a_1 \left(\frac{a}{b}\right)^{n-1} + \ldots + a_n = 0$$

for $a_1, \ldots, a_n \in A$. Therefore

$$a^n + a_1 b a^{n-1} + \ldots + a_n b^n = 0. \quad (\star)$$

If $\pi \in A$ is prime and $\pi \mid b$ then $(\star)$ implies $\pi \mid a$. Assuming that $\frac{a}{b}$ is reduced (a, b are coprime) we therefore obtain $b \in A^\times$ and $\frac{a}{b} \in A$. $\square$

§3 Trace, Norm & Discriminant

Definition Remark 3.1

We will recall now some facts about fields and their extensions.

i) Let R be a ring and $K \subseteq R$ a field.

$x \in R$ is called <u>algebraic over K</u> if it is the zero of a polynomial in $K[X]$.

Otherwise it is called <u>transcendental</u> over K.

R is called algebraic over K if all elements in R are algebraic over K.

ii) Let $K \subset L$ be a field extension, which is denoted L/K "L over K".

We call $[L:K] := \dim_K L$ the <u>degree</u> of the extension L/K.

$(K \subset L \subset M)$

If $[L:K] < \infty$ then L/K is called finite.

and in particular L/K is algebraic.

Given two finite extensions L/K and M/L we have

$$[M:K] = [M:L] \cdot [L:K].$$

iii) Let R again be a ring and $K \subseteq R$ a field.
For any $\alpha \in R$ we have a ring homomorphism

$$\varphi_\alpha : K[X] \longrightarrow R$$
$$f \longmapsto f(\alpha) .$$

We have $\operatorname{Ker} \varphi_\alpha \neq (0) \iff \alpha$ is algebraic over K.

Since $K[X]$ is a PID we can find for each algebraic α a monic polynomial, the <u>minimal polynomial of α</u>, $\min_K(\alpha) \in K[X]$ with

$$\operatorname{Ker} \varphi_\alpha = (\min_K(\alpha)) .$$

We have $K[X] / (\min(\alpha)) \cong K(\alpha)$.

iv) A field K is called <u>algebraically closed</u> if any non-constant $f(X) \in K[X]$ splits into linear factors

$$f(X) = k \cdot (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$$

for some $k, \alpha_1, \ldots, \alpha_n \in K$.

An algebraic closure $\overline{K}$ of a field K is an algebraic extension $\overline{K}/K$ which is algebraically closed.

An algebraic closure always exists and is unique up to isomorphisms.

Proposition 3.2 Let K be a field with $\mathrm{char}(K)=0$ or $|K|<\infty$.

characteristic of K defined by ($\mathrm{char}(K) = \mathrm{Ker}(\mathbb{Z} \to K)$)

i) If $f \in K[X]$ is irreducible and

$$f(x) = \prod_{i=1}^{n} (X - \alpha_i) \qquad (\alpha_i \in L)$$

in some extension L/K, then the α_i are all pairwise distinct.

ii) If L/K is an extension with $[L:K]=n$, then there exist exactly n different homomorphisms (K-embeddings) $\sigma : L \longrightarrow \overline{K}$, with $\sigma(x)=x$ $\forall x \in K$.

(Homomorphism between field extensions of K which fix the elements in K are called <u>K-homomorphisms</u>).

iii) If $[L:K]=n$, then there exists an element $\alpha \in L$ with $L = K(\alpha)$.

smallest subfield of L containing K and α.

α is called a <u>primitive element</u>.

Proof: Algebra course.

Examples 3.3. i) $K=\mathbb{Q}$, $L=\mathbb{Q}(i)$, $[L:K]=2$

$$\mathbb{Q}(i) = \mathbb{Q}[x]/(x^2+1) = (x+i)(x-i)$$

$\min(i)$

$\sigma_i : L \to \overline{\mathbb{Q}}$

$\sigma_1 : a+bi \mapsto a+bi$

$\sigma_2 : a+bi \mapsto a-bi$

ii) General: α algebraic $L=\mathbb{Q}(\alpha)$, $[L:K]=n$, $\min(\alpha)=\prod_{j=1}^{n}(x-\alpha_j)$

$$c_j \in \mathbb{Q} \quad \sum_{j=0}^{n-1} c_j \alpha^j \xmapsto{\sigma_i} \overline{\mathbb{Q}}$$

$$\alpha \longmapsto \alpha_i$$

iii) $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$. In this case we can choose $\alpha=\sqrt{2}+\sqrt{3}$ as a primitive element. $\sqrt{3}=\frac{11\alpha-\alpha^3}{2}$

$L=\mathbb{Q}(\alpha)$ $\quad \sqrt{2}=-\frac{9\alpha-\alpha^3}{2}$

Definition 3.4 Let L/K be a field extension with $[L:K]=n$.

For an $x\in L$ define the K-linear map

$$T_x : L \longrightarrow L$$
$$\alpha \longmapsto x\alpha .$$

Then we define the <u>trace</u> and <u>norm</u> of x by

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(T_x) \qquad N_{L/K}(x) = \det(T_x).$$

There are coefficients in the characteristic polynomial

$$f_x(\lambda) = \det(\lambda\, \mathrm{id} - T_x) = \lambda^n - a_1 \lambda^{n-1} + \dots + (-1)^n a_n \in K[\lambda]$$

$$a_1 = \mathrm{Tr}_{L/K}(x), \quad a_n = N_{L/K}(x).$$

For $x, y \in L$ we have

$$\mathrm{Tr}_{L/K}(x+y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$$

$$N_{L/K}(x \cdot y) = N_{L/K}(x)\, N_{L/K}(y),$$

i.e. we obtain group homomorphisms

$$\mathrm{Tr}_{L/K} : (L, +) \longrightarrow (K, +)$$

$$N_{L/K} : (L^\times, \cdot) \longrightarrow (K^\times, \cdot).$$

<u>Example 3.5</u> $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$ $n = 2$

$B = \{1, i\}$ basis of L

$x = a + bi$ $\quad [T_x]_B = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ matrix of T_x with respect to B

$$N_{L/K}(x) = \det [T_x]_B = a^2 + b^2$$

$$Tr_{L/K}(x) = Tr(T_x) = 2a$$