5. Algebraic integers

Def A number field is a finite ext. of $\mathbb{Q}$

$$\begin{array}{ccc} \mathbb{Q} & \subset & K \\ \cup & & \cup \\ \mathbb{Z} & \subset & \mathcal{O}_K \end{array} \leftarrow \text{integers in } K$$

What properties should $\mathcal{O}_K$ naturally have?

1) $\mathcal{O}_K$ should be a subring of K containing $\mathbb{Z}$.

2) If K_1, K_2 – number fields, $\sigma: K_1 \hookrightarrow K_2$ then $x \in \mathcal{O}_{K_1} \Leftrightarrow \sigma(x) \in \mathcal{O}_{K_2}$

Equivalently, $\mathcal{O}_{K_1} = K_1 \cap \mathcal{O}_{K_2}$

Note: 2) $\Rightarrow$ $\mathcal{O}_K$ is stable under automorph. of K, in part. if K is Galois / $\mathbb{Q}$ $x \in \mathcal{O}_K$, then $g(x) \in \mathcal{O}_K$ $\forall g \in Gal(K/\mathbb{Q})$

Then x is a root of the polynom.:

$$f = \prod_{g \in Gal(K/\mathbb{Q})} (X - g(x)) = X^n + a_1 X^{n-1} + \ldots + a_n$$

a_i are symm. poly's in $g(x)$, $g \in Gal(K/\mathbb{Q})$

$\Rightarrow a_i \in \mathbb{Q}$, 1) $\Rightarrow a_i \in \mathcal{O}_K$

2) $\Rightarrow a_i \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$

Def $x \in K$, where K is a number field, is called alg. integer if x is a root of some monic poly $f \in \mathbb{Z}[X]$

($f = a_0 X^d + \dots + a_d$ is monic if $a_0 = 1$)

Prop 5.1 For $x \in K$ the following are equivalent (TFAE):

1) x is an alg. integer (in the sense of the above def.)

2) the monic min. poly of x has integral coefficients.

Proof 2) $\Rightarrow$ 1) obvious

1) $\Rightarrow$ 2) Let x be a root of monic $f \in \mathbb{Z}[X]$, $h \in \mathbb{Q}[X]$ be the monic min poly of x.

Then $f = h \cdot g$ for some $g \in \mathbb{Q}[X]$

note: g is monic.

Assume $h \notin \mathbb{Z}[X]$. Then $\exists$ a prime p that appears in denominator of some

coeff. of h.

Define: n_1 = maxim exponent of p appearing in denominators of coeff of h

n_2 = —"— of z

then $n_1 \geq 1$ by assumption

$$p^{n_1+n_2} f = \underbrace{(p^{n_1} h)} \cdot \underbrace{(p^{n_2} z)}$$

have no p in denominators

$\Rightarrow$ can reduce coeff. mod p

$p^{n_1} \cdot h \pmod p = \bar{h} \in \mathbb{F}_p[x]$

$p^{n_2} \cdot z \pmod p = \bar{z} \in \mathbb{F}_p[x]$

By the choice of n_1, n_2 $\bar{h} \neq 0$, $\bar{z} \neq 0$

$p^{n_1+n_2} f \pmod p = 0$

$\Rightarrow$ get $0 = \bar{h} \cdot \bar{z}$ — contradiction, because $\mathbb{F}_p[x]$ has no zero divisors. □

We want to prove that $\mathcal{O}_K$ is a ring; first we generalize the notion of an integer. Let $R \subset S$ be two rings

Def 1) $x \in S$ is integral over R, if $\exists$ a monic $f \in R[x]$, s.t. $f(x) = 0$

2) $R \subset S$ is called integral ext., if $\forall x \in S$ is int / R

3) The integral closure of R in S

$$\overline{R} = \{x \in S \mid x \text{ is int. / } R\}$$

Prop. 5.2 In the above setting TFAE

1) $x \in S$ is int. / R

2) x is contained in some subring $S' \subset S$, s.t. S' is a finitely generated R-module.

Rmk 2) means: $\exists s_1 \dots s_n \in S'$, s.t.

$$R^{\oplus n} \longrightarrow S' \text{ is surj.}$$
$$(r_1, \dots, r_n) \longmapsto \sum_{i=1}^{n} r_i s_i$$

Proof of 5.2 1) $\Rightarrow$ 2) we have an equation of integral dependence

$$x^n + a_1 x^{n-1} + \dots + a_n = 0 \quad a_i \in R \quad (*)$$

Let S' be R-submodule of S spanned by $1, x, \dots x^{n-1}$.

Then S' is a subring:

x^N can be expressed as a linear comb of $1, x, \ldots, x^{n-1}$ using (*) for any $N \geq 0$

2) $\Rightarrow$ 1) Assume S' is generated by $s_1, \ldots, s_n$; $x \in S' \Rightarrow$

(**) $x \cdot s_i = \sum_{j=1}^{n} a_{ij} s_j$ for some $a_{ij} \in R$

Consider the matrix with elements in S'

$$A = \begin{pmatrix} a_{11} - x & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - x & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} - x \end{pmatrix}$$

Note: $A \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ by (**)

It follows (see Lemma below) that

$\forall i$: $\det A \cdot s_i = 0$

Since S' is a subring, we have

$1 = \sum_{i=1}^{n} \alpha_i s_i$ for some $\alpha_i \in R$

$\Rightarrow \det A = \sum \alpha_i \underbrace{s_i \det A}_{0} = 0$

$\det A = (-1)^n x^n + b_1 x^{n-1} + \dots + b_n \quad b_i \in R$

multiplying by $(-1)^n \Rightarrow$ get equation of int. depend. for x. $\square$

Lemma R arbitrary ring, $A = (a_{ij})$ a $n \times n$ matrix $a_{ij} \in R$, $s_1 \dots s_n \in R$

Assume $A \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Then

$\forall i \quad \det A \cdot s_i = 0$

Proof Let $A^+ = (A_{ij})$, where

$A_{ij} = (-1)^{i+j+1} \cdot \det(\underbrace{(j,i)\text{-th minor of } A}_{(n-1)\times(n-1) \text{ matrix obtained from } A \text{ by removing } j\text{-th row and } i\text{-th column}})$

Then: $A^+ \cdot A = \det A \cdot Id$

$\Rightarrow \quad 0 = \underbrace{A^+ \cdot A}_{0} \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} \det A \cdot s_1 \\ \vdots \\ \det A \cdot s_n \end{pmatrix}$ $\square$

Prop. 5.3 1) $R \subset S$ ring extension $\Rightarrow$ the int. closure $\bar{R}$ is a subring of S, containing R

2) $R \subset S \subset T$ rings, assume $R \subset S$ is an integral ext.

If $x \in T$ is int / $S \Rightarrow x$ is int / R

(transitivity of integrality)

Proof 1) Need: $x_1, x_2 \in \bar{R} \Rightarrow x_1 + x_2 \in \bar{R}$, $x_1 x_2 \in \bar{R}$

$$(*)\begin{cases} x_1^n + a_1 x_1^{n-1} + \dots + a_n = 0 & a_i \in R \\ x_2^m + b_1 x_2^{m-1} + \dots + b_m = 0 & b_i \in R \end{cases}$$

We can assume $n > 1$, $m > 1$

(case $n = 1$ or $m = 1$ — exercise)

Let S' be R-submodule of S generated by $x_1^i x_2^j$ for $i = 0 \dots n-1$, $j = 0 \dots m-1$

S' is fin. generated

Since any $x_1^u x_2^v$, $u, v \geq 0$ can be expressed as a lin. comb. of

$x_1^i x_2^j$ $i = 0 \dots n-1$, $j = 0 \dots m-1$

using (*). Hence S' is a subring.
By construction S' contains x_1+x_2
and x_1x_2 $\overset{\text{Prop. 5.2}}{\Rightarrow}$ $x_1+x_2, x_1\cdot x_2 \in \overline{R}$ □

2) $x \in T$ int $/S \Rightarrow x^n + s_1x^{n-1} + \dots + s_n = 0$
For some $s_i \in S$; s_i are int $/R$
$\Rightarrow$ the subring of S generated by
$s_1, \dots, s_n$ is spanned $/R$ by a
finite number of monomials

$$s_1^{k_1} \cdots s_n^{k_n}, \quad 0 \le k_i < N$$

Consider $T' =$ subring of T
spanned by $x^i s_1^{k_1} \cdots s_n^{k_n}$, $0 \le i < n$
$0 \le k_i < N$
T' is fin. gen $\overset{\text{Prop 5.2}}{\Rightarrow}$ x is int $/R$ □

Def For a ring ext $R \subset S$
R is int. closed in S if $\overline{R} = R$

Coz. from Prop 5.3 For $R \subset S$
then $\overline{R}$ is int. closed in S
i.e. $\overline{\overline{R}} = \overline{R}$

Proof Apply Prop 5.3 (2) to $R \subset \overline{R} \subset S$ □

Back to the number fields

$\mathbb{Z} \subset \mathbb{Q} \subset K$

$\Downarrow$

$\mathbb{Z} \subset K$ a ring extension;

By definition $\mathcal{O}_K$ = int. closure of $\mathbb{Z}$ in K

In part. Prop 5.3 $\Rightarrow$ $\mathcal{O}_K$ is a ring, int. closed in K ✓;

Example Let $K = \mathbb{Q}(i)$

Min poly of $z = a+ib \in \mathbb{Q}(i)$

$$X^2 - (\sigma_1(z)+\sigma_2(z))X + \sigma_1(z)\cdot\sigma_2(z)$$

$$= X^2 - 2aX + a^2 + b^2$$

$$z \in \mathcal{O}_K \Leftrightarrow \begin{cases} 2a \in \mathbb{Z} \\ a^2+b^2 \in \mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} a = \frac{n}{2},\ n \in \mathbb{Z} \\ \frac{n^2}{4} + b^2 = m \in \mathbb{Z} \end{cases}$$

$$\frac{n^2}{4} + b^2 = m \Rightarrow n^2 = 4m - 4b^2$$

$$n \equiv 0 \pmod 2 \Rightarrow a \in \mathbb{Z} \Rightarrow b^2 \in \mathbb{Z} \Rightarrow b \in \mathbb{Z}$$

$n \equiv 1 \pmod 2 \Rightarrow n^2 \equiv 1 \pmod 4$

from $n^2 = 4m - 4b^2$

$\Downarrow$

$4b^2 \in \mathbb{Z} \Rightarrow b = \frac{\ell}{2} \quad \ell \in \mathbb{Z}$

$m = \frac{n^2}{4} + b^2 = \frac{n^2 + \ell^2}{4} \in \mathbb{Z}$

ℓ^2 is either 0 or 1 mod 4

$\Rightarrow n^2 + \ell^2 \equiv 1 \pmod 4$

or $n^2 + \ell^2 \equiv 2 \pmod 4$

in any case $\frac{n^2+\ell^2}{4} \notin \mathbb{Z}$

$\Rightarrow n \equiv 1 \pmod 2$ can not happen.

$\Rightarrow \mathcal{O}_K \simeq \mathbb{Z}[i]$