ZAHLENTHEORIE SS 2019 - NOTE 3

INTEGRAL EXTENSIONS

def: INTEGRAL ELEMENTS

$A \subseteq B$ rings. An element $\alpha \in B$ is called integral over A if it is the root of a monic polynomial with coefficients in A:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$$

The extension $A \subseteq B$ is called integral if every element of B is integral over A.

Example; The element $\sqrt{d}$ is integral over $\mathbb{Z}$. Also S_n.

Rmk: Let $A \subseteq B$ be an extension and $\alpha \in B$ integral over A. Then $A[\alpha]$ is f.g. as an A-module

Indeed, if

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$$

then $A[\alpha]$ is generated by $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ as an A-module.

A converse of this statement holds as well, but we need some preparation:

Lemma [HAMILTON-CAYLEY]

Let M be a f.g. A-module and $\varphi: M \to M$ a homomorphism of A-modules. Then

$$\varphi^n + a_{n-1}\varphi^{n-1} + \dots + a_1\varphi + a_0 \, id_A = 0$$

for certain $a_i \in A$.

proof: Let $m_1, \dots, m_n$ be a set of generators of M. Then

$$\varphi(m_1) = a_{11}m_1 + \dots + a_{1n}m_n$$
$$\varphi(m_2) = a_{21}m_1 + \dots + a_{2n}m_n$$
$$\vdots$$
$$\varphi(m_n) = a_{n1}m_1 + \dots + a_{nn}m_n$$

We can write this in matrix form as

$$\begin{pmatrix} \varphi & & \\ & \varphi & \\ & & \ddots \\ & & & \varphi \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}$$

which is the same as

$$\begin{pmatrix} \varphi - a_{11} & -a_{12} & \dots \\ -a_{21} & \varphi - a_{22} & \dots \\ \vdots & \vdots & \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = 0$$

$$\| $$

$$(\varphi \cdot Id - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

Multiplying on the left by the cofactor matrix we get

$$\begin{pmatrix} \det(\varphi \mathrm{Id} - A) & & \\ & \ddots & \\ & & \det(\varphi I - A) \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0 \quad \text{i.e.}$$

$$\det(\varphi \mathrm{Id} - A)\, m_i = 0 \quad \forall i$$

Since the m_i generate M, it follows that

$$\det(\varphi \mathrm{Id} - A) = 0$$

Expanding the determinant we get

$$\varphi^n + a_{n-1}\varphi^{n-1} + \dots + a_0 \mathrm{id}_M = 0. \qquad \square$$

As a corollary we get this useful characterization of integrality:

Prop: Let $A \subseteq B$ be a ring extension and let $\alpha \in B$. Then TFAE

(1) α is integral over A

(2) $A[\alpha]$ is finite over A.

(3) $A[\alpha] \subseteq C$, with C finite over A.

proof: (1) $\Rightarrow$ (2) we know this already

(2) $\Rightarrow$ (3) take $C = A[\alpha]$

(3) $\Rightarrow$ (1) Consider the multiplication map

(3) $\Rightarrow$ (1) Consider the multiplication map $\varphi = \cdot\alpha : C \to C$, $x \mapsto \alpha x$. This is a homomorphism of A-modules, and since C is f.g. over A we know from Hamilton-Cayley that

$$\varphi^n + a_{n-1}\varphi^{n-1} + \dots + a_1\varphi + a_0 \cdot id_C = 0$$

but this means

$$(\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0)x = 0 \quad \forall x \in C.$$

Taking $x = 1$ gives what we want. □

Cor/def: INTEGRAL CLOSURE

Let $A \subseteq B$ be a ring extension. The set

$$\overline{A} = \{\alpha \in B \mid \alpha \text{ is integral over } A\}$$

is a ring extension of A. It is called the integral closure of A in B.

proof: we need to prove that $\overline{A}$ is a ring: Let $\alpha, \beta \in B$ integral over A. We need to show that $\alpha+\beta, \alpha\beta$ are both integral over A. However, we see that $\alpha+\beta, \alpha\beta \in A[\alpha,\beta]$ and since α, β are integers we know that $A[\alpha,\beta]$ is a finite extension of A. Hence $\alpha+\beta, \alpha\beta$ is integral.

def: INTEGRALLY CLOSED / NORMAL

Let $A \subseteq B$ be a ring extension. A is called integrally closed in B if $\overline{A} = A$.

If A is a domain, A is called integrally closed or normal if it is integrally closed in $K = \mathrm{Fract}\, A$.

Example: (1) $\mathbb{Z}$ is integrally closed (EX. SESSION)
In general, any UFD is integrally closed.

Cor: $A \subseteq B \subseteq C$ ring extensions.
B integral over A
C integral over B
$\Rightarrow$ C is integral over A

proof: Let $\alpha \in C$. Since α is integral over B, we have

$$\alpha^n + b_{n-1}\alpha^{n-1} + \dots + b_1\alpha + b_0 = 0$$

Hence, α is integral over $A[b_0, b_1, \dots, b_{n-1}]$
This means that $A[b_0, \dots, b_{n-1}][\alpha]$ is finite over $A[b_0, \dots, b_{n-1}]$, which is finite over A because the b_i are integral over A. Hence $A[b_0, \dots, b_{n-1}, \alpha]$ is finite over A, and α is integral over A. □

Cor: Let $A \subseteq B$ be a ring extension and $\overline{A}$ the integral closure. Then $\overline{A}$ is integrally closed in B.

proof: $\alpha \in B$ integral over $\overline{A}$, which is integral over A. Hence α is integral over A, which means $\alpha \in \overline{A}$. □

We can use one exercise from Exercise sheet 1 to characterize integral elements in terms of the minimal polynomial:

Lemma: Let A be an UFD and $K = \operatorname{Frac} A$.
Let $f(x) = g(x)h(x)$ be a factorization in $K[x]$ with f, g, h monic. If f has coeff in A, then g, h have coeff in A as well.

Prop: A = UFD, $K = \operatorname{Frac} A$, $\alpha \in \overline{K}$.
α is integral over A $\iff$ $m_\alpha(x)$ has coefficients in A

proof: ($\Leftarrow$) clear.
($\Rightarrow$) α is a root of a monic polynomial $f(x)$ with coefficients in A. By definition of minimal polynomial, we have

$$f(x) = m_\alpha(x)\, g(x) \quad \text{in } K[x]$$

By the Lemma, $m_\alpha(x)$ has coefficients in A. □

Def: NUMBER FIELDS, RINGS of INTEGERS
A number field is a finite extension $K/\mathbb{Q}$.
The ring of integers $\mathcal{O}_K$ of K is the integral closure of $\mathbb{Z}$ in K.

Example: RING of INTEGERS of QUADRATIC

Example

EXTENSIONS

Let $d \in \mathbb{Z}$ be a sqfr integer. Then

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4 \end{cases}$$

proof: Let $\alpha = a + b\sqrt{d}$ an element of $\mathbb{Q}(\sqrt{d})$ with $a, b \in \mathbb{R}$, $b \neq 0$. The minimal polynomial of α is

$$(x - (a+b\sqrt{d}))(x - (a-b\sqrt{d})) =$$

$$= ((x-a) - b\sqrt{d})((x-a) + b\sqrt{d}) =$$

$$= (x-a)^2 - b^2 d = x^2 - 2ax + a^2 - b^2 d$$

Hence α is integral iff $\begin{cases} 2a \in \mathbb{Z} \\ a^2 - b^2 d \in \mathbb{Z} \end{cases}$

Since $2a \in \mathbb{Z}$ we can write $a = \frac{A}{2}$ so we can also write

$$(*) \quad \frac{A^2}{4} - b^2 d = k \qquad k \in \mathbb{Z}$$

hence

$$A^2 - (2b)^2 d = 4k$$

so

$$(2b)^2 d = A^2 - 4k$$

hence $(2b)^2 d$ is an integer. Since d is sqfr $2b$ must be an integer, hence we can write

$$b = \frac{B}{2}$$

Now we rewrite (*) as

$$\frac{A^2}{4} - \frac{B^2}{4} d = k$$

$$A^2 - B^2 d = 4k$$

which, modulo 4 means

$$A^2 - B^2 d \equiv 0 \quad (4)$$

$d \equiv 1 \ (4)$: $A^2 - B^2 \equiv 0 \quad (4)$

$A^2 \equiv B^2 \quad (4)$

i.e. A, B both even

or A, B both odd

$d \equiv 2 \ (4) \quad A^2 \equiv 2B^2 \ (4)$

only if $A^2 \equiv B^2 \equiv 0 \ (4)$

i.e. A, B both even

$d \equiv 3 \ (4) \quad A^2 \equiv 3B^2$

same as before. □