Integral elements

Definition

L ring. $A \leq L$ subring. $\alpha \in L$ is integral over A if $\exists$ nonzero monic polynomial $f(y) \in A[y]$ s.t. $f(\alpha) = 0$.

Definition

A subring of a ring C. C is integral over A if every $\alpha \in C$ is integral over A.

Definition

A domain A is integrally closed if it's equal to its integral closure in $\operatorname{Frac} A$.

Observation

A domain with $K = \mathrm{Frac}\, A$. L/K finite extension.

Let $\alpha \in L$. If α's min poly $\in A[y]$ then α is integral over A.

If $0 \neq f(y) \in A[y]$ with $f(\alpha) = 0$ then $g(y) \mid f(y)$ in $K[x]$. Now, if A UFD

Gauss' Lemma $\Rightarrow$ $g(y) \in A[y]$.

So in A UFD α is integral over $A \iff$ its min-poly $\in A[y]$.

Example

Let $d \in \mathbb{Z}$ be a square free integer. $d \neq 0, 1$. $L = \mathbb{Q}(\sqrt{d})$ be the associated quadratic field. Then

all elements in $\mathbb{Q}(\sqrt{d})$ integral over $\mathbb{Z}$

$$\begin{array}{ccc} ?? = B & & \mathbb{Q}(\sqrt{d}) \\ & & | \\ \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

$$B = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv_4 2, 3 \\ \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right] & d \equiv_4 1 \end{cases}$$

Proof

Let $\alpha = m + n\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ $\mathbb{Z}$ UFD (even PID and even Euclidean). So, α integral over $\mathbb{Z}$ iff its min-poly $\in \mathbb{Z}[y]$. If $n = 0$ α is integral over $\mathbb{Z}$ iff $\alpha \in \mathbb{Z}$.

So assume $\alpha \notin \mathbb{Q}$ and so $f(y)$ not linear. Then

$$f(y) = (y - (m + n\sqrt{d}))(y - (m - n\sqrt{d})) = y^2 - 2my + m^2 - n^2 d.$$

$\Rightarrow \alpha$ integral over $\mathbb{Z}$ iff $\begin{cases} 2m \in \mathbb{Z} \\ m^2 - n^2 d \in \mathbb{Z} \end{cases}$ $\Longleftarrow$ what's argued above

check

In the previous example, the set of elements integral over $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ formed a ring. This is a general property of rings which we'll prove. This is similar to algebraic elements forming a field. There this is proved by proving a finiteness condition on the dimension of the extension. We'll use the same idea here. It will require an idea called the determinant trick.

Proposition

A subring of a field L. $\alpha \in L$. TFAE:

(1) α is integral over A

easy

(2) The subring $A[\alpha]$ of L is a f.g. A-module.

obvious

(3) $\exists$ f.g A-submodule M of L with $\alpha M \subseteq M$.

Proof of $3 \Rightarrow 1$

Say $M = Ae_1 + \cdots + Ae_n$. Fix $i \in [n]$

$\alpha e_i \in M \implies \alpha e_i = \sum_{j=1}^{n} b_{ij} e_j \qquad b_{ij} \in A$.

Let $B = (b_{ij})$. Then,

$$\alpha \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = B \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \implies (\alpha I - B) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

So $\alpha I - B$ is singular. Since its entries are in the field L, $\det(\alpha I - B) = 0$.

But $f(y) = \det(yI - B)$ is a monic poly in $A[y]$ $\implies$ α integral over A.

Corollary

A subring of a field L. The set B consisting of all elements of L that are integral over A form a ring

Proof

$\alpha \in A$ integral $(x - \alpha \in A[x])$ so $1 \in B$.

Let α, β integral over A. Then $A[\alpha], A[\beta]$ are f.g A-modules

$\Rightarrow$ $A[\alpha, \beta]$ f.g. A-module and $\alpha\beta \in A[\alpha, \beta]$

$\Rightarrow$ $\alpha + \beta$, $\alpha \cdot \beta$ are integral over A

∎

The corollary above leads to the following natural definition.

Definition

A subring of a field L. The <u>integral closure</u> B of A in L is the ring of elements of L integral over A.

Definition

A domain A is <u>integrally closed</u> if it is equal to its integral closure in $\operatorname{Frac} A$.

Corollary

A UFD $\implies A$ integrally closed

Proof

Denote $k = \mathrm{Frac}\, A$. Let $\alpha \in k$. Using Gauss' Lemma we proved that α is integral over A $\iff$ its min poly $\in A[y]$. But α's min poly is $x - \alpha$. ∎

We'll see another proof for UFD $\implies$ integrally closed below.

Since $\mathbb{Z}$, $k[x]$ are UFDs (even Euclidean) they are integrally closed.

Example

For $d \equiv_4 1$ $\mathbb{Z}[\sqrt{d}]$ is not i.c. $\frac{1+\sqrt{d}}{2}$ is integral over $\mathbb{Z}[\sqrt{d}]$ yet not in $\mathbb{Z}[\sqrt{d}]$.

Lemma (again)

UFD $\Rightarrow$ i.c

Proof

A UFD, $z \in K \coloneqq \mathrm{Frac}\,A$ integral over A. Write $z = \frac{b}{c}$ $b, c \in A$ coprime. Then,

$$\left(\frac{b}{c}\right)^n + a_{n-1}\left(\frac{b}{c}\right)^{n-1} + \cdots + a_0 = 0 \qquad a_i \in A$$

$$\Rightarrow \quad -b^n = c\,(a_{n-1} b^{n-1} + \cdots + a_0 c^{n-1})$$

Since A UFD, every prime factor of c divides b $\Rightarrow$ c is a unit $\Rightarrow z \in A$ ∎

We'll sharpen the remark regarding integral elements & their min-poly in UFD:

Lemma

A i.c. α algebraic over K with min-poly $g(y) \in K[y]$. Then,

$$\alpha \text{ integral over } A \iff g(y) \in A[y]$$

Proof

$\Leftarrow$ obvious

$\Rightarrow$ Let $f(y) \in A[y]$ monic with $f(\alpha) = 0$.

Let L be a splitting field for $g(y)$. Let $\alpha_1, \dots, \alpha_n$ conjugates of α in L. That is,

$$g(y) = \prod_i (y - \alpha_i)$$

Since $g \mid f$, each α_i is integral over A. The coefficients of g are polynomials in the α_i's and so are in B - the ring of integral elements over A. However, these coefficients are clearly also in K, so $g(y) \in (B \cap K)[y]$. But $B \cap K = A$ since A is i.c $\Rightarrow g(y) \in A[y]$ ∎

Proposition

$A \subseteq B \subseteq C$ domains. Then, C integral over $A \iff \begin{cases} C \text{ integral over } B \\ \quad \& \\ B \text{ — " — } A \end{cases}$

Proof

$\Rightarrow$ obvious

$\Leftarrow$ Take $\alpha \in C$. C integral over $B \Rightarrow \exists\, g(y) = y^n + b_{n-1}y^{n-1} + \dots + b_0 \in B[y]$ $g(\alpha) = 0$

Let $B' = A[b_0, \dots, b_{n-1}]$. Since each b_i is integral over A, using induction,

we can show that B' is a f.g. A-module

Consider $B'[\alpha]$. It is a f.g. B'-module: $B'[\alpha] = B' + \alpha B' + \dots + \alpha^{n-1} B'$. So it is a f.g

A-module. Since $\alpha B'[\alpha] \subseteq B'[\alpha]$ we get that α is integral over A.

To summarize:

Proposition

A domain, $K = \mathrm{Frac}\, A$. L/K finite extension. B the integral closure of A in L.

Then

1) $L = \mathrm{Frac}\, B$. In fact, $\alpha \in L \Rightarrow \exists\, b \in B$ $a \in A$ s.t. $\alpha = \frac{b}{a}$.

2) B is i.c.

3) A i.c $\Longrightarrow$ $B \cap K = A$.

$$\begin{array}{ccc} B & \hookrightarrow & L \\ | & & | \\ A & \hookrightarrow & K \end{array}$$

Proof

1) $\alpha \in L$. $g(y) \in K[y]$ its min poly:

$$g(y) = y^n + \frac{c_{n-1}}{d_{n-1}} y^{n-1} + \dots + \frac{c_0}{d_0} \qquad c_i, d_i \in A \quad d_i \neq 0$$

Let $d = \prod d_i$. $d^n g(\alpha) = 0 \Longrightarrow (d\alpha)^n + \underset{\in A}{\left(\frac{c_{n-1}}{d_{n-1}} d\right)} (d\alpha)^{n-1} + \dots + \underset{\in A}{\left(\frac{c_0}{d_0} d^n\right)} = 0$. $\Longrightarrow d\alpha \in B$

$\Longrightarrow \alpha = \frac{b}{d} \in \frac{B}{A}$

2) Let C be the integral closure of B in L.

So C integral over A $\Rightarrow$ $C = B$.

$$\text{integral}\left\{ \Leftarrow \begin{array}{c} C \\ | \\ B \\ | \\ A \end{array} \right. \begin{array}{l} \left.\vphantom{\begin{array}{c} C \\ | \end{array}}\right\} \text{integral} \\ \left.\vphantom{\begin{array}{c} | \\ A \end{array}}\right\} \text{integral} \end{array}$$

3) By definition

Corollary

A domain, $K = \operatorname{Frac} A$. L/K deg n extension. B integral closure of A in L. Then B contains a K-vector space basis of L.

Proof

Let $e_1, \dots, e_n \in L$ be any basis of L over K. $e_i = \frac{b_i}{a_i}$ $b_i \in B$ $a_i \in A$.

$\Rightarrow$ $b_1, \dots, b_n \in B$ is also a basis of L over K.