Chapter II

Integral ring extensions

Convention 46 a) In this chapter a ring is always meant to be unital and commutative.

b) If we say subring we mean unital subring, i.e. it shares the unit element.

c) A ring extension $B|A$ is a ring B together with a subring $A \subseteq B$.

Def 47: Let $B|A$ be a ring extension. $b \in B$ is called *integral* over A, if $\exists$ *monic* polynomial $f(X) \in A[X]$, such that $f(b)=0$.

Def 48: Let A be a ring. An A-module M over A is called *faithful* if an element $a \in A$ which satisfies $\forall m \in M: am=0$ has to be zero.

(i.e. $\{a \in A \mid \forall m \in M: am=0\} = \{0_A\}$)

Example 49:

(a) $A = \mathbb{Z}$, $B = \mathbb{Q}[i]$.

$b := 2+3i$ is integral over $\mathbb{Z}$, because $b^2 - 4b + 13 = 0$

Question: Is $\frac{1}{5} + \frac{1}{3}i$ integral over $\mathbb{Z}$?

(b) Let $b \in B$ be integral over A.

Then $A[b]$ is finitely generated A-module.
(also say:
- A module of finite type,
- finite over A.)

Further $A[b]$ is faithful A because $1_A \in A \subseteq A[b]$ and if $a \in A$ satisfies $a\,A[b] = \{0\}$, then $a \cdot 1_A = 0$ $\Rightarrow a = 0$.

Prop. 50: Let $B|A$ be a ring extension and $b \in B$. T.a.e.:
1° b is integral over A
2° $A[b]$ is finite over A
3° $\exists$ faithful $A[b]$-module $M \subseteq B$, o.t. $b \in M$ and M is finite over A.
4° $\exists$ intermediate ring $B|B'|A$ such that $b \in B'$ and B' is finite $/A$.

Proof: 1° $\Rightarrow$ 2° easy
2° $\Rightarrow$ 4° Take $B' := A[b]$
4° $\Rightarrow$ 3° Take $M := B'$.
3° $\Rightarrow$ 1° Take a finite generating set $\{m_1, \dots, m_\ell\}$ of M, i.e.

$$M = A m_1 + \dots + A m_\ell.$$

Then $\exists$ matrix $(a_{ij}) \in A^{\ell \times \ell}$:

$$b \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_\ell \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1\ell} \\ \vdots & & \vdots \\ a_{\ell 1} & \cdots & a_{\ell\ell} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_\ell \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \left(\underbrace{I_\ell \cdot b - (a_{ij})}_{} \right) \begin{pmatrix} m_1 \\ \vdots \\ m_\ell \end{pmatrix}$$

Multiply with $\mathrm{Adj}(I_\ell b - (a_{ij}))$ from left.

$$\Rightarrow \begin{pmatrix} q \\ \vdots \\ 0 \end{pmatrix} = \det(I_\ell b - (a_{ij})) \begin{pmatrix} m_1 \\ \vdots \\ m_\ell \end{pmatrix}$$

$\Rightarrow \det(I_t \cdot b - (a_{ij})) = 0$.

↑ M is $A[b]$ faithful

$\Rightarrow$ b is integral over A $\square$

Remark 51: The strategy in the proof of $3° \Rightarrow 1°$ is called Noether's determinant trick.

Example 52: Which elements of $\mathbb{Q}$ are integral over $\mathbb{Z}$?

(1) All elts of $\mathbb{Z}$.

(2) These are all.

Pf: Take $\frac{p}{q} \in \mathbb{Q} \setminus \mathbb{Z}$ with

$\gcd(p,q) = 1$ and $q > 1$.

Assume $\frac{p}{q}$ is integral over $\mathbb{Z}$.

Then $\mathbb{Z}[\frac{p}{q}]$ is finite over $\mathbb{Z}$

Thus $\exists N \in \mathbb{N}: \forall z \in \mathbb{Z}[\frac{p}{q}]:$

$q^N z \in \mathbb{Z}$. ↯

as $q^N \left(\frac{p}{q}\right)^{N+1} = \frac{p^{N+1}}{q} \notin \mathbb{Z}$.

$\square$

Prop 53: In $B|A$ Let

$\overline{A}^B := \{b \in B \mid b \text{ integral over } A\}$

(integral closure of A in B)

Then $\overline{A}^B$ is a subring of B.

So we have the tower $B|\overline{A}^B|A$.

Proof: Let $b_1, b_2 \in \overline{A}^B$.

Then $A[b_1]$ is finite over A

and $A[b_1,b_2]$ —"— $A[b_1]$

Thus $A[b_1,b_2]$ —"— A.

50 ($4° \Rightarrow 1°$) $\Rightarrow A[b_1,b_2] \subseteq \overline{A}^B$ $\square$

Example 54: $\overline{\mathbb{Z}}^{\mathbb{Q}} = \mathbb{Z}$.

Def 55: An integral domain A is called integrally closed if $\overline{A}^{Q(A)} = A$.

(Example: UFD's)

How to get $\overline{\mathbb{Z}}^{\mathbb{Q}(i)}$?

Prop 56: Let σ be integrally closed with quotient field F. Let $\alpha \in \overline{F}$

T.a.e.:

1° α is integral over σ

2° all coeff. of the minpol $f(X)$ of α / F are in σ.

Proof: 2° $\Rightarrow$ 1° $f(X)$ is monic.
Now 1° follows from Def. 47, because $f(X) \in \sigma[X]$.

1° $\Rightarrow$ 2° α is integral $/\sigma$.
Take any $\varphi \in \mathrm{Aut}(\overline{F}/F)$.
Then $\varphi(\alpha)$ is integral $/\sigma = \varphi(\sigma)$

Thus all roots of $f(X)$ are integral $/\sigma$.

53 $\Rightarrow$ $\overline{\sigma}^{F}$ is a ring.

$\Rightarrow$ All coeff. of $f(X)$ are in $\overline{\sigma}^{F}$.

$\Rightarrow$ All coeff. of $f(X)$ are integral over σ

$\Rightarrow$ — " — are in σ.

σ is int. closed. □

Example 57: We compute $\overline{\mathbb{Z}}^{\mathbb{Q}(i)}$.

Claim $\overline{\mathbb{Z}}^{\mathbb{Q}(i)} = \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z} i$

Proof: "$\supseteq$" ✓

"$\subseteq$" Take $\overbrace{a+ib}^{\alpha} \in \overline{\mathbb{Z}}^{\mathbb{Q}(i)}$

$(a, b \in \mathbb{Q})$

Case $b = 0$: Then $\alpha = a \in \overline{\mathbb{Z}}^{\mathbb{Q}} = \mathbb{Z}$.

Case $b \neq 0$: The minpol of $\alpha/\mathbb{Q}$

is given by

$$(X-\alpha)(X-\overline{\alpha})$$
$$= X^2 - 2aX + (a^2+b^2).$$

56 ($1^\circ \Rightarrow 2^\circ$) $\Rightarrow$ $2a,\ a^2+b^2 \in \mathbb{Z}$.

$\Rightarrow$ $2a,\ a^2+b^2,\ 2b \in \mathbb{Z}$.

First: If $a \in \mathbb{Z}$ or $b \in \mathbb{Z}$, then a^2 and $b^2 \in \mathbb{Z}$ and thus a and $b \in \mathbb{Z}$.

Second: Assume $a \notin \mathbb{Z}$ and $b \notin \mathbb{Z}$.

$\Rightarrow$ $a = \frac{p}{2}$, $b = \frac{p'}{2}$

with odd $p, p' \in \mathbb{Z}$.

$\Rightarrow$ $\mathbb{Z} \ni a^2+b^2 = \frac{p^2+p'^2}{4}$ ↯

as $p^2 + p'^2 \equiv_4 1+1 = 2 \not\equiv_4 0$

□

Exercise 58: Take $D \in \mathbb{Z}$,

s.t. $\forall p$ prime: $p^2 \nmid D$.

(D is called squarefree)

Show that

$$\overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{D})} = \begin{cases} \mathbb{Z}[\sqrt{D}], & D \equiv_4 2,3 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right], & D \equiv_4 1 \end{cases}$$

Prop 59 (tower law)
Let $C|B|A$ be a tower of ring extensions. T.a.e.:

1° $C|B$ and $B|A$ are integral.
2° $C|A$ is integral.

Proof: 2° ⇒ 1° ✓

1° ⇒ 2° Take $c \in C$. and $f(X) \in B[X]$ monic st. $f(c) = 0$.

$$f(X) = X^\ell + b_{\ell-1} X^{\ell-1} + \dots + b_1 X + b_0$$

⇒ c integral over $A[b_0, \dots, b_{\ell-1}]$

⇒ $A[b_0, \dots, b_{\ell-1}, c]$ finite over $A[b_0, \dots, b_{\ell-1}]$.

Further
$A[b_0][b_1] \dots [b_{\ell-1}]$ is finite over A.

So $A[b_0, \dots, b_{\ell-1}, c]$ is finite over A.
⇒ $c \in \overline{A}^C$. □

Example 60: $\mathbb{Z}[i]$ is integrally closed.

Proof: $C := \overline{\mathbb{Z}[i]}^{\mathbb{Q}[i]}$.

$C | \mathbb{Z}[i] | \mathbb{Z}$ tower of integral extensions

59 ⇒ $C|\mathbb{Z}$ is integral.

$$\Rightarrow C \subseteq \overline{\mathbb{Z}}^{\mathbb{Q}(i)} \overset{57}{=} \mathbb{Z}[i]$$

□

II 2. Extension Theory under integral ring extensions

II 2.1. Recap Localization

Ref 61: R a ring.

$$\operatorname{Spec}(R) := \{ \mathfrak{p} \subseteq R \mid \mathfrak{p} \text{ is a prime ideal of } R \}$$

$$\operatorname{Specm}(R) := \{ \mathfrak{m} \subseteq R \mid \mathfrak{m} \text{ is a maximal ideal of } R \}$$

Example 62: $\operatorname{Spec}(\mathbb{Z}) = \{ p\mathbb{Z} \mid p \text{ prime} \} \cup \{ \{0\} \}$

$$\operatorname{Specm}(\mathbb{Z}) = \{ p\mathbb{Z} \mid p \text{ prime} \}$$

K a field, $\operatorname{Spec}(K) = \operatorname{Specm}(K) = \{(0)\}$

(0) = ideal generated by 0.

$(= \{0\})$

Def 63: Let R be a ring and $S \subseteq R$ be a multiplicative system, i.e.
- $1 \in S$ and
- $\forall s_1, s_2 \in S: s_1 s_2 \in S$

Let M be an R-module. The relation on $M \times S$:

$$(m_1, s_1) \sim (m_2, s_2) \overset{\text{Def}}{\Leftrightarrow} s_2 m_1 = s_1 m_2$$

is an equivalence relation.

Pf:
- $(m, s) \sim (m, s)$, as $1(sm - sm) = 0$.
- $(m_1, s_1) \sim (m_2, s_2) \Rightarrow (m_2, s_2) \sim (m_1, s_1)$ (easy)
- $(m_1, s_1) \sim (m_2, s_2) \sim (m_3, s_3)$

$\Rightarrow \exists s_1, s_2 \in S: s_1(s_2 m_1 - s_1 m_2) = 0$
$s_2(s_3 m_2 - s_2 m_3) = 0$

$\Rightarrow \underbrace{s_1 s_2 s_3}_{\in S}(s_3 m_1 - s_1 m_3) = 0$

$\Rightarrow (m_1, s_1) \sim (m_3, s_3)$. $\square$

We write: $\frac{m}{s}$ for the equivalence class, and M_S (or $S^{-1}M$) for the factor set $M \times S / \sim$.

Example 64: a) $\mathbb{Z} = R$, $S := \mathbb{Z} \setminus p\mathbb{Z}$

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, p \nmid b \right\} =: \mathbb{Z}_{(p)}$$

b) $R := \mathbb{Z}$, $S := \mathbb{Z} \setminus \{0\}$
$S^{-1}\mathbb{Z} = \mathbb{Q}$.

c) Let R be a ring, $S \subseteq R$ a mult. sys.. Suppose $0 \in S$. Then

$$R_S = 0$$

and $M_S = 0$, for all R-modules M.

Pf: To show $\frac{m}{s} = \frac{0_M}{1}$ in M_S, i.e. $(m,s) \sim (0_M, 1)$.

We have

$$0_R(1 \cdot m - s \cdot 0_M) = 0_M$$

So $(m,s) \sim (0_M, 1_R)$. ∎

d) $R = K[X,Y]$, K a field

$$S = R \setminus \big((X) \cup (Y)\big)$$

Union of the ideals one generated by X and the other by Y.

S is a multiplicative system, as (X) and (Y) are prime ideals in R.

Exercise: Describe

$$S^{-1}K[X,Y].$$

Def 65: (local ring) A ring R is called local ring if

$$|\mathrm{Specm}(R)| = 1.$$

Prop 66: Let R be a ring. Put $\mathfrak{X} := R \setminus R^\times = \{r \in R \mid r \notin R^\times\}$ = set of elts of R which are not invertible in R.

T.a.e.:

1° R is a local ring

2° $\mathfrak{X}$ is an ideal of R.

Example 67: (a) $\mathbb{Z} \setminus \mathbb{Z}^\times = \mathbb{Z} \setminus \{\pm 1\}$

is not an ideal in $\mathbb{Z}$, because $1 = 3 - 2 \notin \mathbb{Z} \setminus \mathbb{Z}^\times$.

So $\mathbb{Z}$ is not a local ring.
We know: $|\mathrm{Specm}(\mathbb{Z})| = \infty$.

(a) K a field $\Rightarrow |\mathrm{Specm}(K)| = 1$

(zero ideal) $\Rightarrow$ K is a local ring.

(c) $R := \mathbb{Q}[X]/(X^n)$ $(n \in \mathbb{N})$

is a local ring with max. ideal

$$(X)/(X^n).$$

Pf: Take $\overline{P} \in R$ s.t. $X \nmid P$.

We use that $\mathbb{Q}[X]$ is a Euclidean ring.
$\gcd(X^n, P) \Rightarrow$
$\exists\, f(X), g(X) \in \mathbb{Q}[X]$:

$$1 = X^n f(X) + P(X) g(X).$$

(Bézout)

$\Rightarrow \overline{P(X)}\,\overline{g(X)} = \overline{1}$ in R.

$\Rightarrow \overline{P} \in R^\times$ □

Proof of (Prop 66): $2^\circ \Rightarrow 1^\circ$ ✓

$1^\circ \Rightarrow 2^\circ$ Take $x_1, x_2 \in \mathfrak{X}$.
$\Rightarrow \exists\, m_1, m_2 \in \mathrm{Specm}(R)$:
$x_1 \in m_1$, $x_2 \in m_2$.

R is a local ring $\Rightarrow m_1 = m_2$.
$\Rightarrow x_1 \pm x_2 \in m_1 \subseteq \mathfrak{X}$
and $Rx_1 \subseteq m_1 \subseteq \mathfrak{X}$ □

II 2.2. Extension of a prime ideal.

Prop 68: Let $B|A$ be an integral ring extension and $\mathfrak{p} \in \mathrm{Spec}(A)$. Then $\exists\, \mathfrak{q} \in \mathrm{Spec}(B) : \mathfrak{q} \cap A = \mathfrak{p}$.

Before we give a proof, just consider the following example.

Example 69: $A = \mathbb{Z}$, $B = \mathbb{Z}[i]$

Note at first that $\mathbb{Z}[i]$ is a Euclidean ring w.r.t.

$N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}$ $\quad N(a+ib) = a^2+b^2$

[Pf:— $\alpha, \beta \overset{\neq 0}{\in} \mathbb{Z}[i]$. We need to find $\gamma \in \mathbb{Z}[i]$, $\delta \in \mathbb{Z}[i]$, s.t. $N(\delta) < N(\beta)$ and $\alpha = \gamma\beta + \delta$

$\frac{\alpha}{\beta} \in \mathbb{Q}[i]$. Take $\gamma \in \mathbb{Z}[i]$, s.t. $\mathrm{Re}\left(\frac{\alpha}{\beta} - \gamma\right), \mathrm{Im}\left(\frac{\alpha}{\beta} - \gamma\right) \in \left[-\frac{1}{2}, \frac{1}{2}\right]$.

$$\Rightarrow N(\alpha - \beta\gamma) \leq N(\beta)\left(\frac{1}{4} + \frac{1}{4}\right) < N(\beta)$$

□]

Thus B is a PID. (exercise)

Claim: $\mathrm{Specm}(B) = \left\{ (x+iy)B \;\middle|\; x^2+y^2 \text{ prime in } \mathbb{Z} \right\} \cup \left\{ pB \;\middle|\; p \equiv_4 3 \text{ prime in } \mathbb{Z} \right\}$

$\cdot\ \mathrm{Spec}(B) = \mathrm{Specm}(B) \cup \{(0)\}$

Proof: "$\supseteq$" Take $x+iy \in B$ s.t. x^2+y^2 prime.

Assume $(x+iy)$ is not maximal ideal.

PID $\Rightarrow \exists\, \alpha \in \mathbb{Z}[i] : (\alpha)$ is maximal and $(\alpha) \supsetneq (x+iy)$

$\Rightarrow \exists\, \beta \in \mathbb{Z}[i] : \alpha\beta = x+iy$

$\Rightarrow N(\alpha)N(\beta) = p.$

$\Rightarrow N(\beta) = 1 \iff \beta \in \mathbb{Z}[i]^\times$

$\uparrow$ $\qquad\qquad$ $\uparrow$ $\beta \in B$

$\alpha \notin \mathbb{Z}[i]^\times$

$\Rightarrow (\alpha) = (x+iy)$ $\lightning$.

The case pB $(p \equiv_4 3)$ is an exercise.

"$\subseteq$" exercise

For the second assertion: In a PID a non-zero prime ideal is automatic a maximal ideal. $\square$

Now we have

(1) For $\underbrace{x^2+y^2}_{=p}$ prime in $\mathbb{Z}$.

$$\left((x+iy)\mathbb{Z}[i]\right) \cap \mathbb{Z} = p\mathbb{Z}.$$

(2) For p prime $\equiv_4 3$:

$$\left(p\mathbb{Z}[i]\right) \cap \mathbb{Z} = p\mathbb{Z}.$$

(Pf: The LHS contains $p\mathbb{Z}$ but not 1, and $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$.) $\square$

Lem 70: Let $B \mid A$ be integral and B be an integral domain. T.a.e.:

1° A is a field.

2° B is a field

Pf: $2° \Rightarrow 1°$ $a \in A \setminus \{0\}$, $a^{-1} \in B$. $\Rightarrow \exists\, a_i \in A, n \in \mathbb{N}$

$a^{-n} + \sum_{i=0}^{n-1} a_i a^{-i} = 0$. multiply with a^{n-1}:

$\Rightarrow a^{-1} \in A$.

$1° \Rightarrow 2°$ $b \in B \setminus \{0\}$: $b\left(b^{n-1} + \sum_{i=1}^{n-1} a_i b^{i-1}\right) = -a_0 \in A^\times$ $\square$

Proof of Prop 6.8:

We localize A and B w.r.t. $A \setminus \mathfrak{p}$.

$B_{\mathfrak{p}} \mid A_{\mathfrak{p}}$ is an integral ring extension and $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$

Note that under $A \xrightarrow{\varphi} A_{\mathfrak{p}}$, $a \longmapsto \frac{a}{1}$

we have $\varphi^{-1}(\mathfrak{p}A_{\mathfrak{p}}) = \mathfrak{p}$.
(Why?)

Thus we can assume w.l.o.g.:
A is local with maximal ideal $\mathfrak{p}$.

Now take $\mathfrak{m} \in \operatorname{Specm}(B)$.
Then $A/A\cap\mathfrak{m} \subseteq B/\mathfrak{m}$
is integral.

$B/\mathfrak{m}$ field $\Rightarrow$ $A/A\cap\mathfrak{m}$ field
(Lem 7.0)

$\Rightarrow A\cap\mathfrak{m} \in \operatorname{Specm}(A) = \{\mathfrak{p}\}$

$\Rightarrow A\cap\mathfrak{m} = \mathfrak{p}$ □

II 2.3. Extension of ring homomorphisms under integral ring extensions

Theorem 72: Let $(B,\mathfrak{q})|(A,\mathfrak{p})$ be integral. Suppose $\mathfrak{p}$ is maximal. Let $\varphi: A \longrightarrow L$ be a ring homomorphism with $\mathfrak{p} = \ker(\varphi)$.

Then $\exists\ \Phi: B \longrightarrow \overline{L}$ ring hom. s.t. $\ker(\Phi) = \mathfrak{q}$ and $\Phi|_A = \varphi$.

Proof: We decompose φ:

$$A \xrightarrow{\pi} A/\mathfrak{p} \xrightarrow{\overline{\varphi}} L$$

So we obtain a diagram

$$\begin{array}{ccccc} B & \xrightarrow{\Pi} & B/\mathfrak{q} & \dashrightarrow^{\exists\,\overline{\Phi}} & \overline{L} \\ \cup & & \uparrow & & \cup \\ A & \xrightarrow{\pi} & A/\mathfrak{p} & \xrightarrow{\overline{\varphi}} & L \end{array}$$

$\mathfrak{p} \in \mathrm{Spec}_m(A)$, $B/\mathfrak{q}|A/\mathfrak{p}$ integral

$\overset{70}{\Longrightarrow}$ $B/\mathfrak{q}$ field $\Rightarrow \mathfrak{q} \in \mathrm{Spec}_m(B)$.

Thus $B/\mathfrak{q}|A/\mathfrak{p}$ is an algebraic field extension.

$\Rightarrow \exists\ \overline{\Phi}: B/\mathfrak{q} \hookrightarrow \overline{L} : \overline{\Phi}|_{A/\mathfrak{p}} = \overline{\varphi}$.

Put $\Phi := \overline{\Phi} \circ \Pi$ □

Remark 73: (a) The statement in Thm 72 is still true if we skip the assumption that $\mathfrak{p}$ is maximal. (Exercise)

(b) Suppose $(B,\mathfrak{q})|(A,\mathfrak{p})$ is integral and $L|K = Q(\sigma)$ is a field ext. and we have a diagramm

$$\begin{array}{ccc} B & \xrightarrow{\Phi_\sigma} & L \\ | & & | \\ A & \xrightarrow{\varphi} & \sigma \subseteq K \end{array}$$

of ring hom's s.th. $\ker(\varphi) = \mathfrak{p}$ and $\ker(\Phi) = \mathfrak{q}$. Then $\mathrm{im}(\Phi) \subseteq \overline{\sigma}^L$.

Example 74 We can extend

$$\begin{array}{ccc} \mathbb{Z}[i] & \xhookrightarrow{(\cdot)} & \mathbb{C} \\ \alpha & \longmapsto & \overline{\alpha} \end{array} \quad \text{to} \quad \begin{array}{ccc} \overline{\mathbb{Z}}^{\mathbb{C}} & \xhookrightarrow{(\cdot)} & \mathbb{C} \\ | & \sigma & \| \\ \mathbb{Z}[i] & \xhookrightarrow{(\cdot)} & \mathbb{C} \end{array}$$

via $(\cdot)$.

(The prime ideal here is the zero ideal in $\mathbb{Z}[i]$ and — " — in $\overline{\mathbb{Z}}^{\mathbb{C}}$)

We have more extensions

$$\begin{array}{ccc} \overline{\mathbb{Z}}^{\mathbb{C}} & \xhookrightarrow{\Phi} & \mathbb{C} \\ | & & \| \\ \mathbb{Z}[i, \sqrt{2}] & \xhookrightarrow{} & \mathbb{C} \\ \cup & \sigma & \| \\ \mathbb{Z}[i] & \xhookrightarrow{(\cdot)} & \mathbb{C} \end{array}$$

$\sqrt{2} \mapsto -\sqrt{2}$, $i \mapsto -i$

The Φ exists by 72, applied on the upper rectangle.

II 2.4. Integral elements and valuation rings

Def 75: Let K be a field. A subring $\sigma \subseteq K$ is called valuation ring if

$\forall x \in K \setminus \{0\}: \; x \in \sigma$ or $x^{-1} \in \sigma$.

A proper val. ring of K is a val. ring σ s.t. $\sigma \neq K$.

Example 76 (a) $K = \mathbb{Q} = Q(\mathbb{Z})$.

$\mathbb{Z}$ is not a val. ring of $\mathbb{Q}$, as $\frac{2}{3}, \frac{3}{2} \notin \mathbb{Z}$.

Take p a prime in $\mathbb{Z}$

Claim $\mathbb{Z}_{(p)} = \{ \frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b \}$ is a val. ring of $\mathbb{Q}$.

Pf: Take $\frac{a}{b} \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, $b \neq 0$, $\gcd(a, b) = 1$.

If $p \nmid a$ then $\frac{b}{a} \in \mathbb{Z}_{(p)}$
If $p \mid a$ then (as $\gcd(a,b)=1$) $p \nmid b$. So $\frac{a}{b} \in \mathbb{Z}_{(p)}$.

□

Claim: Those are all proper val. rings of $\mathbb{Q}$.

(Note that $\mathbb{Q}$ is also a val. ring of $\mathbb{Q}$.)

Pf: Take $B \subsetneq \mathbb{Q}$ a val. ring of $\mathbb{Q}$.

$1 \in B \Rightarrow \mathbb{Z} \subseteq B$

$B \subsetneq \mathbb{Q} \Rightarrow \exists$ prime $p \in \mathbb{Z}$: $\frac{1}{p} \notin B$.

Now we show that $B = \mathbb{Z}_{(p)}$.

"$\subseteq$" ✓ easy.

"$\supseteq$" To show $\forall q$ prime in $\mathbb{Z}$, $q \neq p$: $\frac{1}{q} \in B$.

Assume $\exists q$ prime $\neq p$: $\frac{1}{q} \notin B$

Bézout $\Rightarrow \exists a, b \in \mathbb{Z}$: $aq + bp = 1$

$\Rightarrow \frac{q}{p} \notin B$, as $a\frac{q}{p} + b = \frac{1}{p} \notin B$

and $\frac{p}{q} \notin B$, as $a + b\frac{p}{q} = \frac{1}{q} \notin B$.

↯ as B is a val. ring □

Claim: $\bigcap_p \mathbb{Z}_{(p)} = \mathbb{Z}$

Pf: $\bigcap_p \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0,\ \gcd(a,b) = 1,\ \forall p \in \mathbb{N} \text{ prime}: p \nmid b \right\}$

$= \{ a \mid a \in \mathbb{Z} \} = \mathbb{Z}$. □

(b) $\mathcal{O} = \mathbb{Z}$, $K = \mathbb{Q}(i)$

A val. ring of $\mathbb{Q}(i)$ satisfies $\mathbb{Z} \subseteq B$ and $i \in B$ (as $i^{-1} = -i$)

So $\mathbb{Z}[i] \subseteq B$.

Thus $\bigcap_{B \text{ val. ring of } \mathbb{Q}(i)} B \overset{(*)}{=} \bigcap_{B \text{ val ring of } \mathbb{Q}(i),\ B \supseteq \mathbb{Z}[i]} B \overset{(*)}{=} \mathbb{Z}[i]$

$= \overline{\mathbb{Z}}^{\mathbb{Q}(i)}$.

(*) Same argument as in (a), because $\mathbb{Z}[i]$ is a PID.

Question: (c) Given a number field K, i.e. a finite extension of $\mathbb{Q}$, do we have

$$\overline{\mathbb{Z}}^{K} = \bigcap_{\substack{B \subseteq K \\ \text{val. ring of } K}} B \quad ?$$

(d) Are all val. rings local rings?

Lemma 77: Let B be a val. ring of K. Then B is a local ring.

Proof: $\mathfrak{I} := \{x \in B \mid x \notin B^\times\}$

Take $x, y \in \mathfrak{I}$. To show $x+y \in \mathfrak{I}$.
Assume $x+y \notin \mathfrak{I}$. Then
$x+y \in B^\times$, so $\frac{1}{x+y} \in B$.

Case $x^{-1}y \in B$: Then

$$x^{-1}y + x^{-1}\cdot x \in B$$
$$\| $$
$$x^{-1}(x+y)$$
$$\Rightarrow \quad x^{-1} \in B \ \lightning$$
$(x+y) \in B^\times$

Case $y^{-1}x \in B$: Similar. $\lightning$ □

Theorem 78: Let σ be a subring of a field K.

Then

$$\overline{\sigma}^K = \bigcap_{\substack{\sigma \subseteq B \\ B \text{ val. ring of } K}} B$$

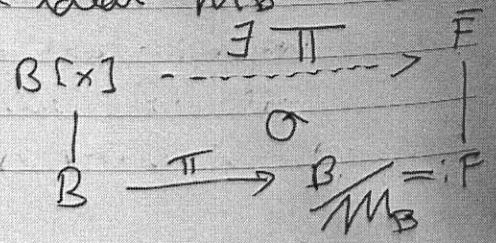
$$= \bigcap_{\substack{\sigma \subseteq B \\ B \text{ proper val. ring of } K}}$$

Proof: "$\subseteq$" Let $x \in \overline{\sigma}^K$

Take $B \supseteq \sigma$ a proper val. ring of K. Assume $x \notin B$.

By 77 B is a local ring with unique max ideal $\mathfrak{m}_B$

72 $\Rightarrow$



Note that $\frac{1}{x} \in B \setminus (B^\times) = \mathfrak{m}_B$

So $\pi(\frac{1}{x}) = 0_F$ and

$$1 \overset{!}{=} \pi(x \cdot \tfrac{1}{x}) = \pi(x)\,\pi(\tfrac{1}{x}) = \pi(x)\,0_F$$
$$= 0_F. \quad \lightning$$

"$\supseteq$" Take $x \in \bigcap_{\substack{B \supseteq \sigma \\ \text{proper val ring of } K}} B$, $x \neq 0$.

Case 1: $\frac{1}{x}$ is a unit in $\sigma[\frac{1}{x}]$.

Then x is integral over σ. ✓

Case 2: $\frac{1}{x}$ is not a unit in $\sigma[\frac{1}{x}]$.

Then take $m \in \operatorname{Specm}(\sigma[\frac{1}{x}])$ such that $\frac{1}{x} \in m$.

Take (by Zorn's Lemma) a maximal pair (B, π), $\sigma[\frac{1}{x}] \subseteq B \subseteq K$ subring and

$\overline{\pi}: B \longrightarrow \overline{F}$ $(F := \sigma[\frac{1}{x}])$

a ring homomorphism,
s.t. $\overline{\pi}|_{\sigma[\frac{1}{x}]} = \pi : \sigma[\frac{1}{x}] \to F$

Claim: B is a local ring

Pf: Yes, because if not then localize by $\ker(\overline{\pi})$ and extend $\overline{\pi}$. ∎

Claim: B is a proper val. ring of K with $x \notin B$.

Pf: $x \notin B$, as otherwise

$1 = \overline{\pi}(1) = \overline{\pi}(x)\pi(\frac{1}{x}) = 0_F$ ↯.

If B is not a val. ring, i.e.
$\exists y \in K: \; y, y^{-1} \notin B$.
Then, by next Lemma, we can extend $\overline{\pi}$ to $B[y]$ or $B[y^{-1}]$ ↯ ∎∎

Lemma 79: Let σ be a subring of K and $x \in K \setminus \{0\}$.
Then a ring hom.

$\varphi: \sigma \longrightarrow L$ (alg. closed field)

can be extended to $\sigma[x]$ or $\sigma[x^{-1}]$.

Example 80: $\sigma = F$, $K|F$ a field extension. Take $x \in K \setminus \{0\}$.
Let $\varphi: F \hookrightarrow L = \overline{L}$ be a ring monomorphism.

a) If x is algebraic $/F$, then we can extend φ to $F[x]$ using a minpol of x $/F$ and root of $\varphi f \in \varphi(F)[X]$.

c) If x is not alg. $/F$
Take $y \in L$ and extend φ by $\varphi(x) := y$.

$$\varphi\Big(\sum_{i=0}^{n} a_i x^i\Big) := \sum_{i=0}^{n} \varphi(a_i)\, y^i$$

Proof (of Lemma 79): W.l.o.g. σ is local with $\operatorname{Spec_m}(\sigma) = \{\ker(\varphi)\}$

- If x is integral over σ, then we can extend φ by Thm 72.

- Suppose x is not integral over σ. Let $\mathfrak{a} \subseteq \sigma[x]$ be the ideal generated by $\ker(\varphi) \cup \{x\}$.

Then $1 \notin \mathfrak{a}$. or x^{-1} is integral $/\sigma$.

Pf: Assume $1 \in \mathfrak{a}$

$$\Rightarrow \exists_{n \in \mathbb{N}} \exists_{a_1, \dots, a_n \in \sigma} \; b \in \ker(\varphi)$$

$$1 = a_1 x + \dots + a_n x^n + b$$

σ is local $\Rightarrow 1 - b \in \sigma^\times$.

multiply with $x^{-n} \Rightarrow$ x^{-1} integral $/\sigma$. $\square$

If x^{-1} is integral $/\sigma \Rightarrow$ Use #2

If $1 \notin \mathfrak{a}$. Take a maximal ideal $\mathfrak{m}$ of $\sigma[x]$, s.t.

$$\mathfrak{m} \supseteq \mathfrak{a}.$$

Then $\bar{\varphi}$: $[x]_{\ker(\varphi)} \longmapsto [x]_{\mathfrak{m}}$

$$\frac{\sigma}{\ker(\varphi)} \longrightarrow \frac{\sigma[x]}{\mathfrak{m}}$$

$\bar{\varphi}$ is bijective.

Surjective: yes, because $x \in \mathfrak{m}$

Injective:

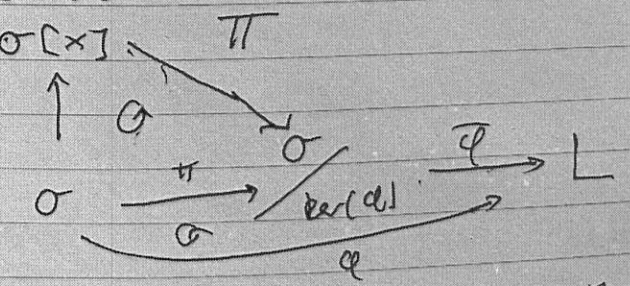
$$\ker(\varphi) \subseteq \mathfrak{m} \text{ and } 1 \notin \mathfrak{m}$$

$$\Rightarrow \mathfrak{m} \cap \sigma = \ker(\varphi).$$

$$\uparrow$$

$$\ker(\varphi) = \sigma \setminus \sigma^\times$$

So we have



$\bar{\varphi} \circ \pi$ extends φ. $\square$