Integral ring extensions

Consider a number field $K|\mathbb{Q}$. Our goal was to find an analogue of $\mathbb{Z}\subseteq\mathbb{Q}$ in K, i.e. a "ring of integers" $\mathcal{O}_K\subseteq K$ such that $K=\mathrm{Frac}(\mathcal{O})$. Last time we gave a definition as $\mathcal{O}_K$ being the maximal order in K. Exercise $\mathbb{Z}=\mathcal{O}_{\mathbb{Q}}$.

Q: What is an integer?

We will discuss this more generally. In what follows, rings are assumed to be commutative.

Proposition:

Let $A\hookrightarrow R$ a ring extension, $z\in R$. TFAE:

(i) $\exists P\in A[X]$ monic such that $P(z)=0$.

(ii) $A[z]$ is an A-module of finite type.

(iii) $\exists A\subseteq B\subseteq R$ subring s.t. $z\in B$ and B is of finite type over A.

Pf: (i) $\Rightarrow$ (ii): $A[z]=\{Q(z): Q\in A[X]\}$. But $A[X]$ admits division with remainder w.r.t. P, i.e.,

$$Q(z)=K(z).P(z)+T(z) \qquad (\deg T<\deg P)$$

Let P as in (i). As P is monic, we have division with remainder w.r.t. P, i.e., for all $Q\in A[X]$ there are $K,T\in A[X]$ s.t.

- $\deg(T)<\deg(P)$, and
- $Q=KP+T$.

Therefore, any element in $A[z]$ is an A-linear combination of $(1,\dots,z^{\deg(P)-1})$:

$$Q(z)=K(z).P(z)+T(z)=T(z).$$

(ii) $\Rightarrow$ (iii): Choose $B=A[z]$.

(iii) $\Rightarrow$ (i): Let $B = A.z_1 + \dots + A.z_d$. $B \curvearrowright B$ by multiplication, i.e., we have $[\times \circ]: B \to \mathrm{End}_A(B)$ given by $[\times \tilde{z}](u) = \tilde{z}.u$.

For our given $z \in B$, the endomorphism $[\times z]$ admits a matrix representation $M_z \in A^{d \times d}$ in the following sense: If $b = a_1 z_1 + \dots + a_d z_d$, $v = (a_1, \dots, a_d)$, $v.M_z = (a_1', \dots, a_d')$, then

$$z.b = [\times z](b) = a_1' . z_1 + \dots + a_d' . z_1 .$$

⌜ $\forall i \; \exists (a_{ij})_{j=1}^{d} \in A^d$ s.t. $z.z_i = \sum_{j=1}^{d} a_{ij}.z_j$. Set $M_z = (a_{ij})$. Then

$$z.b = \sum_{i=1}^{d} a_i . z . z_i = \sum_{i,j=1}^{d} a_i a_{ij} . z_j = \sum_{j=1}^{d} \underbrace{\left(\sum_{i=1}^{d} a_i . a_{ij} \right)}_{= a_j'} . z_j$$

⌟

The characteristic polynomial of M_z is a monic polynomial in $A[X]$ that vanishes at z, i.e., $\det(z.\mathrm{Id} - M_z) = 0$.

The exact argument for the latter is complicated by B not necessarily being free over A, i.e., the matrix is not uniquely determined by the choice $(z_1, \dots, z_d)$. Therefore, the map $B \to \mathrm{Mat}_d(A)$, $z \mapsto M_z$ is not well-defined. The argument follows the proof of Cramer's rule.

⌜ We have that

$$\forall i \quad z \cdot z_i = \sum_{j=1}^{d} a_{ij} \cdot z_j$$

and thus

$$\forall j \qquad \sum_{j=1}^{d} (\delta_{ij} \cdot z - a_{ij}) \cdot z_j = 0.$$

Define $C(z) \in B^{d \times d}$ by $C(z) = (\delta_{ij} \cdot z - a_{ij})_{i,j=1}^{d}$. Then

$$C(z) \cdot \begin{pmatrix} z_1 \\ \vdots \\ z_d \end{pmatrix} = 0.$$

Let $v_j = C(z)^{(j)}$, $w_j = \begin{cases} v_j & \text{if } j \neq i, \\ v_j \cdot z_i & \text{if } j = i, \end{cases}$, $\tilde{\omega}_j = \begin{cases} \omega_j & \text{if } j \neq i, \\ \sum_{k=1}^{d} C(z)^{(k)} \cdot z_k & \text{if } j = i. \end{cases}$ Then multilinearity

and the alternating property of the determinant yield

$$(\det C(z)) \cdot z_i = \det(\omega_1, \dots, \omega_d) = \det(\tilde{\omega}_1, \dots, \tilde{\omega}_d) = 0$$

as $\tilde{\omega}_i = C(z) \cdot \begin{pmatrix} z_1 \\ \vdots \\ z_d \end{pmatrix}$. As i was arbitrary, $(\det C(z)) \cdot 1_B = 0$ and therefore $\det C(z) = 0$. ⌟

Definition

Let $A \hookrightarrow B$ a ring extension, $z \in B$. We call z integral (over A) if $A[z]$ is A-f.t.
The extension $A \hookrightarrow B$ is an integral extension if every element in B is A-integral.

Remark: If A is a field, integrality and algebraicity are the same.

Proposition:

Let $A \hookrightarrow B$ a ring extension, $\mathcal{O}_B(A) \subseteq B$ the set of A-integral elements in B. $\mathcal{O}_B(A)$ is a ring containing A.

clear: $\forall a \in A$ $A[a] = A$ is A f.t.

Lemma:

Suppose $A \hookrightarrow B \hookrightarrow R$ are ring extensions and B/A, R/B are of finite type. Then R/A is of finite type.

Proof: $R = B.r_1 + \dots + B.r_e = \sum_{i=1}^{d} \sum_{j=1}^{e} A.(b_i . r_j)$ $\square$

Proof of the proposition:

Let $z, z' \in \mathcal{O}_B(A)$, i.e., $A[z], A[z']$ are A-f.t. Then z' is $A[z]$-f.t. and thus $\overset{\text{by the lemma}}{A[z][z'] = A[z,z']}$ is A-f.t.
In particular, $z+z'$ and $z.z'$ are contained in an A-f.t. subring of B, therefore $z+z'$, $z.z'$ are integral over A. $\square$

Proposition:

If B/A and C/B are integral, then so is C/A.

Proof: Let $z \in C$, then $B[z]$ is B-f.t. by assumption. By the lemma, $B[z]$ is A-f.t. and thus z is integral over A. As z was arbitrary, C/A is integral.

Definition:

Let $A \hookrightarrow B$ a ring extension. $\mathcal{O}_B(A)$ is called the integral closure of A in B. A is integrally closed in B if $\mathcal{O}_B(A) = A$.

Suppose A is a domain, $Q = \mathrm{Frac}(A)$. The integral closure of A is $\mathcal{O}_Q(A)$ and A is integrally closed if A equals its integral closure.

Corollary

The integral closure of a domain is integrally closed.

Examples:

- $\mathbb{Z}$ is integrally closed.
- $\mathbb{Z}[i]$ is integrally closed.
- $\mathbb{Z}[2i]$ is not integrally closed.
- $\mathbb{Z}[\sqrt{-5}]$ is integrally closed.
- $\mathbb{Z}[\sqrt{-20}]$ is not integrally closed.

Proposition

If A is a PID, then A is integrally closed.

Let $z \in \mathcal{O}_Q(A)$, $a_0, \dots, a_{d-1} \in A$ with $a_0 \neq 0$ and $z^d = -a_{d-1}z^{d-1} - \dots - a_0$. Let $z = \frac{a}{b}$ with a, b coprime, then

$$a^d = -a_{d-1}b(bz)^{d-1} - \dots - a_0 b^d = bk$$

for some $k \in A \Rightarrow b \mid a$ ↯

Dedekind rings

Recall: We are interested in number fields $K/\mathbb{Q}$ and mainly hope to understand $\mathcal{O}_K(\mathbb{Z})$, the ring of integers in K.
Moreover, an important piece of information is given by the factorization of rational primes p viewed as elements in $\mathcal{O}_K = \mathcal{O}_K(\mathbb{Z})$.
This was relatively easy for $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(j)$, mostly because in these cases $\mathcal{O}_K$ was a PID. This is not true in general.

Definition:

A ring A is Dedekind if

(i) A is a domain,
(ii) A is integrally closed,
(iii) Every non-zero prime ideal is maximal, and
(iv) A is noetherian.

consequences of PID

relaxation of PID

cf. exercises

Recall: A is noetherian iff every ideal (i.e., A-submod) is of finite type.

Theorem:

Let $K/\mathbb{Q}$ a number field. Then $\mathcal{O}_K = \mathcal{O}_K(\mathbb{Z})$ is a Dedekind ring.

We will prove this later.

Key properties of Dedekind rings

1) Factorization of ideals: $\forall \underline{\mathfrak{a}} \in \mathcal{J}_A \; \exists! \, v_\bullet(\underline{\mathfrak{a}}) : \mathrm{Spec}(A)^* \longrightarrow \mathbb{N}_0$ s.t.

(i) $\forall \mathfrak{p} \in \mathrm{Spec}(A)^* \quad v_{\mathfrak{p}}(\underline{\mathfrak{a}}) = 0$

(ii) $\underline{\mathfrak{a}} = \prod_{\mathfrak{p} \in \mathrm{Spec}(A)^*} \mathfrak{p}^{v_{\mathfrak{p}}(\underline{\mathfrak{a}})}$.

2) Stability:

Thm

Let A Dedekind, $K/\mathbb{Q}$ finite separable. Then $\mathcal{O}_K(A)$ is A-f.t. and Dedekind.

Proof of factorisation into prime ideals

Lemma (Gauss' lemma for ideals)

Let A a domain, $\mathfrak{p} \triangleleft A$ prime. Let $\underline{\mathfrak{a}}, \underline{\mathfrak{b}} \triangleleft A$ such that $\mathfrak{p} \mid \underline{\mathfrak{a}} . \underline{\mathfrak{b}}$, then either $\mathfrak{p} \mid \underline{\mathfrak{a}}$ or $\mathfrak{p} \mid \underline{\mathfrak{b}}$.

Pf: Suppose $\mathfrak{p} \nmid \underline{\mathfrak{a}}$. Then there is $a \in \underline{\mathfrak{a}} - \mathfrak{p}$.

As $A/\mathfrak{p}$ is a domain, we need to show that $a.b \in \mathfrak{p}$ for all $b \in \underline{\mathfrak{b}}$. But

$$a.\underline{\mathfrak{b}} \subseteq \underline{\mathfrak{a}}.\underline{\mathfrak{b}} \subseteq \mathfrak{p}$$

$\blacksquare$

Lemma:

Let A noetherian and $\underline{\mathfrak{a}} \triangleleft A$ non-zero. Then $\underline{\mathfrak{a}}$ contains a product of non-zero prime ideals.

Proof: Consider the set of all non-zero ideals $\underline{\mathfrak{a}} \triangleleft A$ which do not contain any product of primes. Assume for the sake of contradiction that this set is non-empty.

every collection of A-submodules contains a max'l elmt.

A noetherian $\Longrightarrow$ there is $\underline{\mathfrak{a}} \triangleleft A$ maximal with respect to this property. In particular, $\underline{\mathfrak{a}}$ is not prime and therefore there are $x, y \notin \underline{\mathfrak{a}}$ s.t. $x.y \in \underline{\mathfrak{a}}$. Consider

$$\underline{\mathfrak{b}} = A.x + \underline{\mathfrak{a}} \quad \text{and} \quad \underline{\mathfrak{c}} = A.y + \underline{\mathfrak{a}}.$$

Both $\underline{\mathfrak{b}}$ and $\underline{\mathfrak{c}}$ contain products of prime ideals, say $\mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{q}_1 \cdots \mathfrak{q}_s$. Then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq (A.x + \underline{\mathfrak{a}}).(A.y + \underline{\mathfrak{a}}) = A.xy + x.\underline{\mathfrak{a}} + y.\underline{\mathfrak{a}} + \underline{\mathfrak{a}}^2 \subseteq \underline{\mathfrak{a}}.$$

$\lightning$

$\blacksquare$

Lemma "Integrality lemma"

Let A an integrally closed noetherian domain and $\mathfrak{a} \triangleleft A$ a non-zero ideal. If $x \in \mathrm{Frac}(A)$ satisfies $x.\mathfrak{a} \subseteq \mathfrak{a}$, then $x \in A$.

Proof: Exercise.

Definition:

Let A a domain. A subset $\mathfrak{f} \subseteq \mathrm{Frac}(A)$ is a fractional ideal if there is $b \in A - \{0\}$ such that $b.\mathfrak{f} \subseteq A$ is a non-zero ideal.

Proposition:

Let A Dedekind, $\mathfrak{p} \triangleleft A$ non-zero prime. Then there is a fractional ideal $\mathfrak{p}^{-1} \subseteq \overset{Q}{\mathrm{Frac}(A)}$ s.t.

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = A$$

and $A \subsetneqq \mathfrak{p}^{-1}$.

Proof: We will show that

$$\mathfrak{p}^{-1} = \{x \in Q : x.\mathfrak{p} \subseteq A\}$$

does the job.

Note: $\mathfrak{p}^{-1}$ is an A-module, $A \subseteq \mathfrak{p}^{-1}$ and $\forall b \in \mathfrak{p}$ $\mathfrak{p}^{-1}.b \subseteq A$. Therefore $\mathfrak{p}^{-1}$ is a fractional ideal.

$$\left.\begin{array}{l}
\bullet\ \mathfrak{p}^{-1}.\mathfrak{p} \subseteq A. \\[1em]
\bullet\ A \subseteq \mathfrak{p}^{-1} \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}^{-1}.\mathfrak{p} \subseteq A \\
\bullet\ \mathfrak{p}^{-1}.b \triangleleft A \Rightarrow \mathfrak{p}^{-1}.\mathfrak{p} \subseteq A \text{ is an } \underset{\text{(i.e., ideal)}}{A\text{-submodule}}.
\end{array}\right\} \Rightarrow \mathfrak{p}^{-1}.\mathfrak{p} \in \{A, \mathfrak{p}\} \text{ as } \mathfrak{p} \text{ is maximal.}$$

$\Rightarrow$ We only need to show that $\mathfrak{p}^{-1}\cdot\mathfrak{p} \neq \mathfrak{p}$.

Assume $\mathfrak{p}^{-1}\cdot\mathfrak{p}=\mathfrak{p}$, then the integrality lemma implies $\mathfrak{p}^{-1}\subseteq A$ (i.e., $\mathfrak{p}^{-1}=A$).

Let $a\in\mathfrak{p}-\{0\}$, then there are $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ prime s.t. r is minimal and

$$\mathfrak{p}_1\cdot\dots\cdot\mathfrak{p}_r \subseteq A.a \subseteq \mathfrak{p}$$

and by Gauss' lemma and maximality we assume w.l.o.g. that $\mathfrak{p}_1=\mathfrak{p}$ ($\mathfrak{p}_1\subseteq\mathfrak{p}$). Thus $\underbrace{\mathfrak{p}_2\cdot\dots\cdot\mathfrak{p}_r}_{=:\mathfrak{b}} \not\subseteq A.a$. Let $b\in\mathfrak{b}-A.a$.

Then $b.\mathfrak{p}\subseteq A.a \Rightarrow ba^{-1}.\mathfrak{p}\subseteq A \Rightarrow ba^{-1}\in\mathfrak{p}^{-1}=A \Rightarrow b\in A.a$ ↯.

Pf of factorization into prime ideals

non-zero

Suppose the claim is false. As A is noetherian, there is $\underline{\mathfrak{a}} \lhd A$ maximal among ideals without prime factorization. Let $\mathfrak{p} \in \mathrm{Spec}(A)$ s.t. $\underline{\mathfrak{a}} \subsetneq \mathfrak{p}$ (every ideal is contained in a max'l ideal).

Hence $\underline{\mathfrak{a}} \underset{A \subseteq \mathfrak{p}^{-1}}{\subseteq} \mathfrak{p}^{-1} \cdot \underline{\mathfrak{a}} \subseteq \mathfrak{p}^{-1} \cdot \mathfrak{p} = A$. If we can show that $\underline{\mathfrak{a}} \neq \mathfrak{p}^{-1} \cdot \underline{\mathfrak{a}}$, then we get the desired contradiction: $\underline{\mathfrak{a}} \neq \mathfrak{p}^{-1} \cdot \underline{\mathfrak{a}} \overset{\underline{\mathfrak{a}} \text{ max'l}}{\Rightarrow} \mathfrak{p}^{-1} \cdot \underline{\mathfrak{a}} = \mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_r \Rightarrow \underline{\mathfrak{a}} = \mathfrak{p} \cdot \mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_r$.

Suppose $\underline{\mathfrak{a}} = \mathfrak{p}^{-1} \cdot \underline{\mathfrak{a}}$, then $b \cdot \underline{\mathfrak{a}} \subseteq \underline{\mathfrak{a}}$ for all $b \in \mathfrak{p}^{-1}$. Hence, by the integrality lemma $\mathfrak{p}^{-1} \subseteq A$, which is absurd.

Uniqueness is left as an exercise.