Commutative Algebras

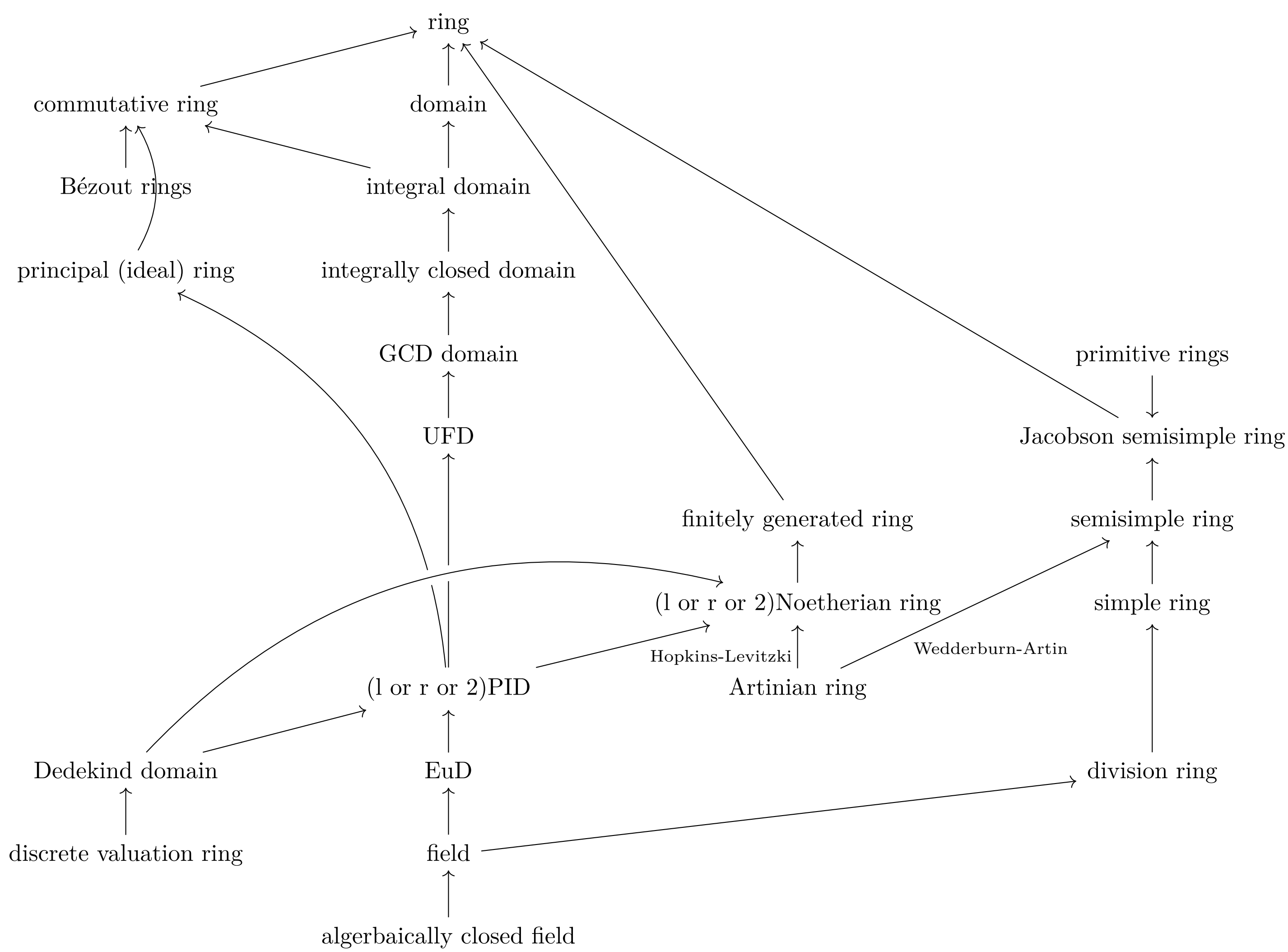
Guo Haoyang

January 2025

Contents

1 Preliminaries

One goal in this commutative algebra note is to see rings with different structures and to know the hierarchy:



2 Localization

2.1 Construction of localization

2.1.1 Localization of rings

Definition 2.1: Saturated multiplicative sets

Let $(R, +, \cdot)$ be a ring and S be. a multiplicative subset of R. S is saturated $\Leftrightarrow$ $(xy \in S \Leftrightarrow x \in S \wedge y \in S)$

Remark Since S is already closed under taking product, the definition can be rephrased as S is saturated if and only if S is *closed under taking divisors*: S is saturated $\Leftrightarrow$ $(xy \in S \Rightarrow x \in S \wedge y \in S)$
Taking divisors is a process of fetching little blocks of elements of the ring. So, the 'closed under taking divisor' property is saying that it contains all building blocks of elements of S.

2.1.2 Localization of modules

2.2 Local rings

Definition 2.2: Local rings

Local rings are 'closures' with respect to the operation localization.

Proposition 2.1: Characterisation of local rings

Let R be a commutative ring with unity. The followings are equal:
(1) R has the unique maximal ideal.
(2) R is non-trivial and any two sum of non-units is a non-unit.
(3) $R - R^{\times}$ is a proper ideal

3 Preservation property of localization

Many properties are preserved under localization, for example, integrally closed property (5.3)

4 Ideals

4.1 Ideal operations

Definition 4.1: Ideal operations [BGS24]

- **Intersection**
- **Sum**
- **Quotient and annihilator**: Let $I, J \trianglelefteq R$ be two ideals. The quotient or colon of I by J, $I : J$ is defined as

$$I : J := \{r \in R | rJ \subseteq I\}$$

- **Radical**

4.2 Extended and contracted ideals

Definition 4.2: Extended and contracted ideals

Let $f : R \to S$ be a ring homomorphism. Let $\mathfrak{a} \trianglelefteq R$ and $\mathfrak{b} \trianglelefteq S$. The extension of $\mathfrak{a}$, denoted $\mathfrak{a}^e$, is the ideal in S generated by $f(\mathfrak{a})$, i.e. $Sf(\mathfrak{a})$. The contraction of $\mathfrak{b}$, denoted $\mathfrak{b}^c$, is $f^{-1}(\mathfrak{b})$

Remark The preimage of an ideal is an ideal. But the image of an ideal under a ring homomorphism is not necessarily an ideal, so we consider the ideal generated by the image.

The homomorphism $f : R \to S$ can be factored into $R \xrightarrow{\widetilde{f}} f(R) \xrightarrow{\iota} S$, where $\widetilde{f}$ is surjective and ι is injective.
Question [1]: Under an injective ring homomorphism, $\iota : Q \hookrightarrow T$, we have already known that for a prime ideal, the preimage of a prime ideal is also a prime ideal. What is the answer of the inverse question, i.e. if $\mathfrak{p} \trianglelefteq Q$ is a prime ideal of Q, is $\mathfrak{p}^e$ a prime ideal of T? The following example answers no: consider an ideal $(2) \trianglelefteq \mathbb{Z}$ and $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$, $(2)^e = \mathbb{Q}$ and it is not a prime ideal of $\mathbb{Q}$.

Now, follow the notion that $f : R \to S$ is still a ring homomorphism.

$$\mathscr{C} := \{\mathfrak{a} \trianglelefteq R \big| \exists \mathfrak{b} \trianglelefteq S, \mathfrak{a} = \mathfrak{b}^c\} \quad \mathscr{E} := \{\mathfrak{b} \trianglelefteq S \big| \exists \mathfrak{a} \trianglelefteq R, \mathfrak{b} = \mathfrak{a}^e\}$$

[1] This is raised in [AM18] Chapter 1

i.e. $\mathscr{C}$ is the collection of all contracted ideals in R and $\mathscr{E}$ is the collection of all extended ideals in S.
As the following suggested, $\mathscr{E}$ is closed under addition and product; $\mathscr{C}$ is closed under intersection, taking radical and quotient/colon. Their 'closed' operations are complementary to each other.

Theorem 4.1: Identities and operations on extension and contraction

Let $f : R \to S$ still be a ring homomorphism. Then,
(1) $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ and $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$
(2) $\mathfrak{a}^e = \mathfrak{a}^{ece}$ and $\mathfrak{b}^c = \mathfrak{b}^{cec}$
(3) $\mathscr{C} = \{\mathfrak{a} \trianglelefteq R \big| \mathfrak{a}^{ec} = \mathfrak{a}\}$ and $\mathscr{E} = \{\mathfrak{b} \trianglelefteq S \big| \mathfrak{b}^{ce} = \mathfrak{b}\}$. $\exists$ a bijection $\mathscr{C} \to \mathscr{E}$, $\mathfrak{a} \mapsto \mathfrak{a}^e$ with inverse $\mathfrak{b}^c \mapsfrom \mathfrak{b}$
(4) operations on $\mathscr{C}$ and $\mathscr{E}$: Let $\mathfrak{a}_1, \mathfrak{a}_2 \trianglelefteq R$ and $\mathfrak{b}_1, \mathfrak{b}_2 \trianglelefteq S$. Then,

$$\begin{aligned}
&(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e && (\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c \\
&(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e && (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c \\
&(\mathfrak{a}_1 \mathfrak{a}_2)^e = \mathfrak{a}_1^e \mathfrak{a}_2^e && (\mathfrak{b}_1 \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c \mathfrak{b}_2^c \\
&\left(\sqrt{\mathfrak{a}}\right)^e \subseteq \sqrt{\mathfrak{a}^e} && \left(\sqrt{\mathfrak{b}}\right)^e \subseteq \sqrt{\mathfrak{b}^e} \\
&(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e) && (\mathfrak{b}_1 : \mathfrak{b}_2)^e \subseteq (\mathfrak{b}_1^e : \mathfrak{b}_2^e)
\end{aligned}$$

Remark Is there any ring homomorphism $R \to S$ and any ideal $I \trianglelefteq R$ such that $I \subsetneq I^{ec}$. In general, there is no bijection $I \mapsto I^e$, even not for prime ideals. But I cannot give an example
Proof: □

4.2.1 Extension and contraction behavior under localization

Here is a special but useful case of extension and contraction. Set R, T as commutative rings with $R \leq T$ and $S \subseteq R$ to be one of its multiplicative subsets. When we restrict to

$$f : R \to R[S^{-1}] \quad r \mapsto \frac{r}{1}$$

In this context, we should demystify the extension and contraction. Suppose that $I \trianglelefteq R$ and $J \trianglelefteq R[S^{-1}]$, then by definition,

$$J^c = f^{-1}(J) = \{r \in R | \frac{r}{1} \in J\}$$

Contraction is easier, it is just preimage. The extension is a bit complex.

$$I^e = \langle f(I) \rangle = I[S^{-1}] = \left\{\frac{r}{s} | r \in I, s \in S\right\}$$

Following the definition 4.2,

Theorem 4.2: Correspondence between ideals in a ring and its localization

Let R be a commutative ring and S be its multiplicative subset. Consider the map $f : R \to R[S^{-1}]$ by $r \mapsto \frac{r}{1}$ and its associated extension and contraction. Then there is a bijection:

$$\left\{\text{prime ideals of } R \text{ disjoint from } S\right\} \longleftrightarrow \left\{\text{prime ideals of } R[S^{-1}]\right\}$$
$$I \mapsto I^e$$
$$J^c \mapsfrom J$$

Proof: First, given a prime ideal $J \trianglelefteq R[S^{-1}]$, want to show that J^c is a prime ideal of R disjoint from S.
We have alerady known that $J^c \trianglelefteq R$.

(1.1) J^c is prime: Consider the map $R/J^c \to R[S^{-1}]/J$ is a ring homomorphism. J is prime $\Leftrightarrow$ $R[S^{-1}]/J$ is an integral domain $\Rightarrow$ R/J^c is an integral domain. $\Leftrightarrow$ J^c is prime.

(1.2) J^c is disjoint from S. Suppose $S \cap J^c \neq \varnothing$, then $\exists s \in J^c \cap S \Rightarrow f(s) = \frac{s}{1}$ is a unit in $R[S^{-1}]$. So, $J = R[S^{-1}]$, contradiction.

Second, we want to show that given a prime ideal $I \trianglelefteq R$ disjoint from S, then I^e is a prime ideal of $R[S^{-1}]$.
$\forall$ $\frac{m_1}{s_1}, \frac{m_2}{s_2} \in R[S^{-1}]$ such that $\frac{m_1 m_2}{s_1 s_2} \in I^e \Leftrightarrow \exists \frac{i}{s_3} \in I^e = IR[S^{-1}] \Leftrightarrow \exists s \in S$, $s m_1 m_2 s_3 = s_1 s_2 i s \in I$ since $I \trianglelefteq R$. I is prime, so at least one of s, m_1, m_2, s_3 belongs to I. Notice that I is disjoint from S, so at least one of $m_1, m_2 \in I$,

which shows that one of $\frac{m_1}{s_1}, \frac{m_2}{s_2}$ is in I^e. Hence, I^e is a prime ideal.
This map is well-defined, it remains to show it is bijection, i.e. $I = I^{ec}$ and J^{ce}

(2.1) From theorem 4.1, $I \subseteq I^{ec}$. $I^{ec} \subseteq I$: $\forall m \in I^{ec}$, $\frac{m}{1} \in I^e \Leftrightarrow \exists \frac{i}{s} \in I^e$, $\frac{m}{1} = \frac{i}{s} \Leftrightarrow \exists s' \in S$, $s'sm = s'i \in I$. Using that $I \cap S = \varnothing$ and $I \trianglelefteq R$ is prime, $m \in i$.

(2.2) From theorem 4.1, $J^{ce} \subseteq J$. $J \subseteq J^{ce}$: $\forall \frac{m}{s} \in J$, $\frac{m}{1} = \frac{s}{1} \cdot \frac{m}{s} \in J \Leftrightarrow m \in J^c$. Then, $\frac{m}{s} = \frac{1}{s} f(m) \in \langle f(J^c) \rangle = J^{ce}$ □

4.3 Primary decomposition of ideals

Despite the obsoleteness, primary ideals are of interest in itself. There are two motivations for studying primary ideals: [AM18] (1) Algebraic foundation for decomposing an algebraic variety into its irreducible components. (2) Generalising the factorisation of an integer as a product of prime powers.

Definition 4.3: Primary ideal

Let R be a commutative ring and $\mathfrak{p} \trianglelefteq_{\mathbf{Ring}} R$. $\mathfrak{p}$ is a primary ideal $\Leftrightarrow$
- $\mathfrak{p} \neq R$
- $\forall x, y \in R, xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $\exists n > 0, y^n \in \mathfrak{p}$

Equivalently, this can be reformulated as, $\mathfrak{p}$ is a primary ideal $\Leftrightarrow R/\mathfrak{p} \neq \{0\}$ and every zero divisor of $R/\mathfrak{p}$ is nilpotent.

Remark • Every prime ideal is primary.
• Contraction of a primary ideal is primary: $\forall$ ring homomorphism $f : A \to B$, $\mathfrak{q}$ is a primary ideal of B, then the contraction with respect to f, $\mathfrak{q}^c$ is a primary ideal in A.

Proposition 4.1: Correspondence between primary and prime ideals

Let R be a commutative ring and $\mathfrak{q}$ be a primary ideal of R. Then, $\sqrt{\mathfrak{q}}$ is the smallest prime ideal containing $\mathfrak{q}$.

5 Integral extension

5.1 Basic properties

Definition 5.1: Integral extension

Proposition 5.1: Characterisation of integral elements

Let B/A be a ring extension with B being commutative. For an element $\alpha \in B$. The followings are equivalent:
(1) α is integral over A
(2) $A[\alpha]$ is a finitely generated A-module.
(3) $\exists$ a subring C of B such that $A \subseteq C \subseteq B$ and $\alpha \in C$.

Proposition 5.2: Closed property of integral elements

Let B/A be a ring extension with B being commutative and $\alpha, \beta \in B$ be two elements that are integral over A. Then, $\alpha + \beta$ and $\alpha\beta$ are integral over A.

Proof: (**Version 1**)

(**Version 2**: Construct two simpler rings)
Let $f \in A[x]$ and $g \in A[y]$ be such that $f(\alpha) = 0$ and $g(\beta) = 0$. Write f and g explicitly as:

$$f(x) = a_0 + a_1 x + \cdots + x^m \qquad g(y) = b_0 + b_1 y + \cdots + y^n$$

Construct $A' := \mathbb{Z}[a_0, a_1, \dots, a_{m-1}, b_0, b_1, \dots, b_{n-1}]$ and $B' := A'[x,y]/\langle f(x), g(y)\rangle$. From the universal property of polynomial rings, $\exists!$ ring homomorphism $\Phi : A' \to A$ sending $a_i \mapsto a_i$ and $b_j \mapsto b_j$; $\exists!$ ring homomorphism $\psi : A'[x,y] \to B$ by sending a_i to a_i, b_j to b_j, $x \mapsto \alpha$ and $y \mapsto \beta$. Since $\langle f(x), g(y)\rangle \subseteq \ker\psi$, the universal property of quotient ring induces a ring homomorphism $\Psi : A'[x,y]/\langle f(x), g(y)\rangle =: B' \to B$. Now consider the ring extension $B'/\iota(A')$ (or we can identify $\iota(A')$ with A'), where $\iota : A' \hookrightarrow B'$ is the canonical inclusion. $\overline{x}$ and $\overline{y}$ are integral over $\iota(A')$. If we can show that $\overline{x}+\overline{y}$ and $\overline{xy}$ are integral over $\iota(A')$, then $\exists$ polynomials $h_1(z), h_2(z) \in \iota(A)[z]$ making $h_1(\overline{x+y}) = \overline{0}$ and $h_2(\overline{xy}) = \overline{0}$. Then, $\Psi(h_1(\overline{x+y})) = \Psi(h_1)(\alpha+\beta) = 0$ and $\Psi(h_2)(\alpha+\beta) = 0$.[2] Since $\Psi(\iota(A')) \subset A$, both polynomials have coefficients in A. This implies that $\alpha+\beta$ and $\alpha\beta$ are integral over A.
Now let's show both of them are integral over $\iota(A')$. Let's consider the algebraic closure $\overline{\mathrm{Frac}(\iota(A'))}$ of $\iota(A')$. Then, factor the $f(z)$ and $g(z)$ into linear factors: $f(z) = \prod_{0\le i\le m}(z-\alpha_i)$ and $g(z) = \prod_{0\le j\le n}(z-\beta_j)$. In B', $\overline{x}$ and $\overline{y}$ are roots of $f(z)$ and $g(z)$ respectively. Consider the polynomial

$$h(z) = \prod_{i,j}(z - (\alpha_i + \beta_j))$$

The coefficients of $h(z)$ are polynomials in symmetric functions of α_i and β_j, i.e. coefficients of a_i and b_j. $\overline{x}$ and $\overline{y}$ equals to some α_i and β_j. Hence, $h(\overline{x+y}) = 0$ and $\overline{x+y}$ is integral over A'. Similarly, consider $h(z) = \prod_{i,j}(z - \alpha_i\beta_j)$, $h(xy) = 0$. □

The last one is a little reward for integral extension:

Theorem 5.1: Integral extension and field

Let A, B be commutative rings with B/A be an integral extension. If B is an integral domain, then A is a field $\Leftrightarrow$ B is a field

Proof: (1) The first part is to show that every non-zero element of B is in $B^\times$.
Suppose A is a field, $\forall b \in B : b \neq 0$, since B is an integral extension of A, b is integral over A, then $\exists$ a monic polynomial with minimal n: $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in A[x]$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0 = 0$$

Reformulating it, $b^n + a_{n-1}b^{n-1} + \cdots + a_1b = -a_0 \Leftrightarrow b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = -a_0$
†: $a_0 \neq 0$ since if $a_0 = 0$, then $b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = 0$ and B is an integral domain, then

$$b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 = 0$$

contradicting the assumption that $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is the polynomial with the least degree that b solves. Then

$$b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)(-a_0)^{-1} = 1$$

i.e. $b^{-1} = (b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)(-a_0)^{-1} \in B$
(2) show that every non-zero element of A is in $A^\times$.
Suppose that B is a field, then $\forall a \in A - \{0\}$, $a \in B$, hence $a^{-1} \in B$, and since B is an integral extension A, a^{-1} is integral over A, then $\exists$ a monic polynomial with minimal n: $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in A[x]$ such that

$$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_1a^{-1} + a_0 = 0$$

Reformulating it, $a^{-1} = -a^{n-1}(a_{n-1}(a^{-1})^{n-1} + \cdots + a_1a^{-1} + a_0) = -(a_{n-1} + \cdots + a_1a^{n-2} + a_0a^{n-1}) \in A$

□

5.1.1 Integral closedness

As in the theory of algebraic extension, there is an algebraic closure. Here there is a counterpart in integral extension, called integral closure.

Definition 5.2: Integral closure

Let's compare the two concepts, integral closure 5.2 and integral extension 5.1. It is illustrated in the diagram: Let B/A still be a ring extension.

[2] Let $h(z) = \sum_i c_i z^i$. Then, $\Psi(h)(z) := \sum_i \Psi(c_i)z^i$

$$
\begin{tikzcd}
A \arrow[rr, dash, "\text{ring extension}"'] \arrow[rr, bend left, leftrightarrow, "\overline{A}^B"] \arrow[d, rightsquigarrow] & & B \arrow[d, rightsquigarrow] \\
A = \overline{A}^B \arrow[d, equal] & & B = \overline{A}^B \arrow[d, equal] \\
A \text{ is integrally closed} & & B \text{ is an integral extension}
\end{tikzcd}
$$

What kind of rings are integrally closed? $\mathbb{Z}$, every UFD, every valuation ring. We are going to finish this section by showing these are integrally closed.

Proposition 5.3: $\mathbb{Z}$ is integrally closed

The ring $\mathbb{Z}$ is integrally closed.

Proof: $\forall \frac{r}{s} \in \mathbb{Q}$ with $\gcd(r,s)=1$ being integral over $\mathbb{Z}$, $\exists$ a polynomial $f(x)=\sum_{0\le i\le n} a_i x^i \in \mathbb{Z}[x]$ such that

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

Eliminating the denominators yields $r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$. So, $r^n = -(a_{n-1}r^{n-1} + \cdots + a_1 r s^{n-2} + a_0 s^{n-1})s$ is a multiple of s. Since r and s are coprime, the only possibility is $s=\pm 1$. Hence $\frac{r}{s}\in\mathbb{Z}$. $\square$

Corollary 5.1: UFD is integrally closed

Every unique factorization domain is integrally closed. In particular, every PID is integrally closed.

Remark This corollary has some extra effect: It can be used to show some rings are not UFD. For example, $\mathbb{Z}[\sqrt{5}]$ is not a UFD since it is not integrally closed: $\phi := \frac{\sqrt{5}+1}{2} \in \mathrm{Frac}(\mathbb{Z}[\sqrt{5}])$, it satisfies $\phi^2-\phi-1=0$. Hence, it is integral over $\mathbb{Z}[\sqrt{5}]$. But $\phi \notin \mathbb{Z}[\sqrt{5}]$ implies $\mathbb{Z}[\sqrt{5}]$ is not integrally closed.
Proof: $\square$

This implies that every discrete valuation ring is integrally closed. In fact, every valuation ring is integrally closed.

Proposition 5.4: Valuation rings are integrally closed

Proof: Let R be a valuation ring. $\forall \alpha \in \mathrm{Frac}(R)$ that is integrally closed over R. If $\alpha \notin R$, then $\alpha^{-1}\in R$. Let $f(x)=\sum_i a_i x^i \in R[x]$ be the monic polynomial that α makes it vanish. Then,

$$\alpha = -(a_{n-1} + a_{n-2}\alpha^{-1} + \cdots + a_1\alpha^{-(n-2)} + a_0\alpha^{-(n-1)})$$

implies that $\alpha \in R$, impossible. Hence, $\alpha\in R$. It follows that R is integrally closed. $\square$

Theorem 5.2: Transitivity of integral closure

Let $A \subseteq B \subseteq C$ be commutative rings and R be the integral closure of A in B, S be the integral closure of A in C. Then S is also the integral closure of R in C. In short, $R=\overline{A}^B$ and $S=\overline{A}^C$, then $S=\overline{R}^C$.

Proof: $R=\{b\in B \mid b \text{ is integral over } A\}$ $S=\{c\in C \mid c \text{ is integral over } A\}$ WTS: $S=\{c\in C\mid c \text{ is integral over } R\}$
$\subseteq$: $\forall s\in S$, s is integral over $A \Leftrightarrow \exists\, p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \in A[x]\subseteq R[x]$ such that $p(s)=0 \Rightarrow s$ is integral over R
$\supseteq$: If c is integral over R, c satisfies a polynomial

$$p(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 \in R[x]$$

The ring $A[r_0, r_1, \cdots, r_{n-1}]$ is a finitely generated A-module because each r_i is integral over A. Notice that c is integral over $A[r_0, r_1, \cdots, r_{n-1}]$ because the polynomial

$$p(x) \in A[r_0, r_1, \cdots, r_{n-1}][x]$$

Hence $A[r_0, r_1, \cdots, r_{n-1}][c]$ is a finitely generated as an $A[r_0, r_1, \cdots, r_{n-1}]$-module and $A[r_0, r_1, \cdots, r_{n-1}]$ is finitely generated as a A module, then $A[r_0, r_1, \cdots, r_{n-1}][c] = A[r_0, r_1, \cdots, r_{n-1}, c]$ is finitely generated as an A-module. $A[c] \subseteq A[c, r_0, \cdots, r_{n-1}] \subseteq C$, $A[c]$ is contained in a finitely generated A-module $A[r_0, r_1, \cdots, r_{n-1}, c]$. This is equivalent to the fact that c is integral over A.

$\square$

5.2 Integrally closedness as a local property

Theorem 5.3: Local property: integrally closed

Let A be an integral domain and $B = \mathrm{Frac}(A)$. The followings are equivalent: (1) A is integrally closed.
(2) $\forall$ prime ideals $\mathfrak{p} \trianglelefteq A$, $A_\mathfrak{p}$ is integrally closed.
(3) $\forall$ maximal ideal $\mathfrak{m} \trianglelefteq A$, $A_\mathfrak{m}$ is integrally closed.

5.3 Cohen-Seidenberg theory: Behaviour of prime ideals under integral extension

Theorem 5.4: Maximal going down

Let A, B be two rings and B/A be an integral extension. Consider the inclusion $\iota : A \hookrightarrow B$. Let $\mathfrak{q} \trianglelefteq B$ be prime, and $\mathfrak{q}^c$ is the contraction of $\mathfrak{q}$ wrt ι. $\mathfrak{q}$ is maximal over $B \Leftrightarrow \mathfrak{q}^c$ is maximal over A

Theorem 5.5: Existence of prime ideals going up

Let A, B be two commutative rings and B/A be an integral extension. If $\exists\ \mathfrak{p} \trianglelefteq A$ is prime, then $\exists\ \mathfrak{q} \trianglelefteq B$, s.t. $\mathfrak{q} \cap A = \mathfrak{p}$

Theorem 5.6: (Cohen-Seidenberg) Going-up theorem

Let A, B be two rings and B/A be an integral extension. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain of prime ideals of A and $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ be a chain of prime ideals of B $(m < n)$, such that $\forall 1 \le i \le m$, $\mathfrak{q}_i \cap A = \mathfrak{p}_i$. Then the chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ can be extended to the chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ such that $\forall 1 \le i \le n$, $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.

Remark Usually, this theorem is split into a two-ideal version and a multiple-ideal version. For simplicity, they are compressed into one. But in the proof, we do the two cases.
Proof: We first prove the $n = 2$ case and then it easily extends to arbitrary n.
When $n = 2$
Applying $n = 2$ case to get $\mathfrak{q}_{m+1}$ such that $\mathfrak{q}_{m+1} \cap A = \mathfrak{p}_{m+1}$, $\mathfrak{q}_{m+2}, \cdots$,till $\mathfrak{q}_n$ such that

$$\forall^{m \le i \le n} i,\ \mathfrak{q}_i \cap A = \mathfrak{p}_i$$

$\square$

Theorem 5.7: (Cohen-Seidenberg) Going-down theorem

Let $A \subseteq B$ be an integral extension and A is **integrally closed**. $\mathfrak{p}_1, \mathfrak{p}_2 \trianglelefteq A$ are prime with $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ and $\mathfrak{q}_2 \trianglelefteq B$ is prime such that $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. Then $\exists$ prime $\mathfrak{q}_1 \trianglelefteq B$, such that $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.

6 Chain conditions

6.1 Noetherian

6.2 Artinian

7 Normalization

8 Decomposition

8.1 Irreducible, Noetherian topological spaces

Definition 8.1: Irreducible topological spaces

Let X be a topological space. X is irreducible (or hyperconnected) $\Leftrightarrow$
- X is not the union of any two closed proper subsets. i.e. $\nexists$ closed proper sets $U, V \subsetneq X$, $X = U \cup V$
- Equivalently, $\nexists$ open sets $U, V (\neq \varnothing)$, $U \cap V = \varnothing$

Remark This is also equivalent to every non-empty open set is dense in X.
Why does U, V require to be closed here?

Lemma 8.1: Closure and irreducibility

If Y is an irreducible subspace of X, then the closure $\overline{Y}$ in X is also irreducible.

Proof: Take any open set U in $\overline{Y}$, then $U \cap Y$ is open in Y. Since Y is irreducible, then $\overline{U \cap Y} = \overline{Y}$. Hence,

$$\overline{Y} \subseteq \overline{\overline{U \cap Y}} = \overline{U \cap Y} \subseteq \overline{U} \subseteq \overline{Y}$$

$(A \subseteq B \Rightarrow \overline{A} \subseteq \overline{B})$ which implies that $\overline{U} = \overline{Y}$, showing that every open set in $\overline{Y}$ is dense. $\square$

Lemma 8.2: Maximal irreducible space

Every irreducible subspace belongs to some maximal irreducible space with respect to $\subseteq$.

Proof: Pick any irreducible subspace Y in X. Let $\mathscr{Y} := \{U \subseteq X | U \text{ irreducible}, Y \subseteq U\}$. i.e. $\mathscr{Y}$ is the collection of all irreducible subspaces in X containing Y. Then, of course, $Y \in \mathscr{Y}$. Let $\{Y_\alpha\}_\alpha$ be a chain in $\mathscr{Y}$, then claim that $\bigcup_\alpha Y_\alpha$ is the upper bound of this chain. Using Zorn's lemma, one can tell that $\exists$ a maximal element in $\mathscr{Y}$. The reason why $\bigcup_\alpha Y_\alpha$ is the upper bound is: $\forall$ open set U in $\bigcup_\alpha Y_\alpha$, $U \cap Y_\alpha$ is an open set in Y_α.

$$\bigcup_\alpha Y_\alpha \cap U \subseteq U \Rightarrow \bigcup_\alpha Y_\alpha \cap U \subseteq \overline{\bigcup_\alpha Y_\alpha \cap U} = \bigcup_\alpha \overline{Y_\alpha \cap U} \subseteq \overline{U}$$

Also, $\bigcup_\alpha Y_\alpha \cap U$ is closed in itself, so $\overline{U} \subseteq \bigcup_\alpha Y_\alpha \cap U$. Hence, $\overline{U} = \bigcup_\alpha Y_\alpha \cap U$ which implies that $\bigcup_\alpha Y_\alpha \cap U$ is irreducible and $\in \mathscr{Y}$. $\square$

The notion of Noetherian ring and module is transported to topological spaces.

Definition 8.2: Noetherian topological space

Let X be a topological space. Then, X is **Noetherian** if the closed sets of X satisfy the descending chain condition or the open sets of X satisfies the ascending chain condition. i.e.
- DCC: $\forall$ closed subsets $Y_1, Y_2, \ldots, Y_n \subseteq X$, with $\forall i$, $Y_{i+1} \subseteq Y_i$, then $\exists$ n, such that $\forall j \geq n$, $Y_j = Y_n$
- ACC: $\forall$ open subsets $Y_1, Y_2, \ldots, Y_n \subseteq X$, with $\forall i$, $Y_i \subseteq Y_{i+1}$, then $\exists$ n, such that $\forall j \geq n$, $Y_j = Y_n$

What is the connection between irreducible topological space and Noetherian space?
If X is the topological space that is dealt with in normal analysis, then it could almost be neither a Noetherian

space nor an irreducible space. However, if X is equipped with the Zariski topology, then it would have much better properties.

In the next, we give a very important theorem which is the core of this decomposition chapter.

Theorem 8.1: Decomposition of Noetherian topological space

Let X be a Noetherian topological space.
$\exists!$ non-negative many closed, irreducible maximal subsets $Z_1, Z_2, \dots, Z_n \subseteq X$ with $\forall i, j$, $Z_i \not\subseteq Z_j$,

$$X = Z_1 \cup Z_2 \cup \cdots \cup Z_n$$

the uniqueness is up to permutation and those maximal irreducible topological spaces are called **irreducible components** of X.

Proof: (**Existence of decomposition**) First, we would show that X can be decomposed into closed, irreducible spaces. The maximality could be obtained from Lemma 8.2 or being proved later.
Let $\mathscr{M}$ be the collection of all closed subsets of X that are not a finite union of closed irreducible subsets. i.e.

$$\mathscr{M} := \{V \text{ closed in } X | V \text{ is not a finite union of closed irreducible subsets in } X\}$$

Notice that every **non-empty** collection of closed sets in X has a minimal element. Otherwise, it has an infinite endless descending chain, contradicting the Noetherianity of X.
Assume that $\mathscr{M}$ is not empty. Now take the minimal element of $\mathscr{M}$, say Y. Since Y is irreducible, then it can be written as a union of two closed proper subsets of Y, say Y_1, Y_2, by Definition 8.1. By minimality of Y, Y_1 and Y_2 could be written as a finite union of closed irreducible subsets in X. So is Y, contradicting the fact that Y is not a finite union of such sets.
So, $\mathscr{M} = \varnothing$ and every closed subset of X is a finite union of closed, irreducible subsets. In particular, X is a finite union of closed, irreducible subsets. i.e.

$$X = Z_1 \cup Z_2 \cup \cdots \cup Z_m$$

for some m and each Z_i is closed and irreducible. Using Lemma 8.2, we can replace every Z_i by a maximal one. By deleting all those Z_i such that $\exists j$, $Z_i \subseteq Z_j$, we get the desired form.
Even without putting 'maximal' in the condition, we can show every Z_i is inside some maximal irreducible subspace. Let Z be an irreducible subspace of X. Then,

$$Z = (Z \cap Z_1) \cup (Z \cap Z_2) \cup \cdots \cup (Z \cap Z_n)$$

each one of them is closed. By Definition 8.1, the only possibility is $\exists i$, $Z = Z \cap Z_i$, implying $Z \subseteq Z_i$.
(**Uniqueness of decomposition**) If there is another decomposition $X = W_1 \cup W_2 \cup \cdots \cup W_k$, $\forall W_i$, $\exists j_i$, $W_i \subseteq Z_{j_i}$. The only possibility for Z_{j_i} is $Z_{j_i} \subseteq W_i$. So, $Z_{j_i} = W_i$. Continuing the matching gives us a one-to-one correspondence between two decompositions. Hence it is a permutation. □

Remark As we saw, in the proof, we use the fact X is Noetherian only in existence part(even without word 'maximal'). So, if the decomposition exists, the 'maximal property' and uniqueness automatically holds.

9 Valuation

9.1 Valuation in general

9.1.1 Valuation

Definition 9.1: Discrete valuation

A **discrete valuation** over a field K, is the map $\nu : K \to \mathbb{Z} \cup \{\infty\}$ where ν satisfying the inequalities in definition 9.2.

As long as ν is non-trivial discrete valuation, $\nu(K^\times)$ is a non-zero subgroup of $\mathbb{Z}$, hence $\exists n$, $\nu(K^\times) = n\mathbb{Z}$. For $n\mathbb{Z} = \nu(K^\times)$, $n = 1 \Leftrightarrow \nu$ is surjective. In this case, ν is said to be **normalized**. If ν is not normalized, we can always consider $m^{-1}\nu : x \mapsto m^{-1} \cdot \nu(x)$, which is a normalized discrete valuation. (c.f. [Mil20])

Example (1) p-adic valuation:
(2)
Valuation is the generalization of discrete valuation by abstracting $\mathbb{Z}$ to Γ.

Definition 9.2: Valuation

Let K be a field and $(\Gamma, +, \geq)$ be a totally ordered abelian group. A **valuation** is a map $\nu : K \to \Gamma \cup \{\infty\}$ satisfies the following properties:
- $\nu(x) = +\infty \Leftrightarrow x = 0$, which is equivalent to $\nu(x) \in \Gamma \Leftrightarrow x \in K^\times$
- $\forall a, b \in K$, $\nu(ab) = \nu(a) + \nu(b)$
- $\forall a, b \in K$, $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$ with equality $\Leftrightarrow \nu(a) \neq \nu(b)$ When does the $=$ hold?

A valuation ν is **non-trivial** $\Leftrightarrow \forall x \in K^\times$, $\nu(x) = 0$. Otherwise, ν is non-trivial.

Remark Some explanations on each term in definitions.
(1) Geometrically, any non-empty germ of an analytic variety near a point contains that point.
(2) Valuation is a group homomorphism between $K^\times$ and Γ.
(3) A version of triangle inequality. Something. It can be extended to finite cases:

$$\nu(\sum_{i=1}^{n} a_i) \geq \min\left\{\nu(a_1), \nu(\sum_{i=2}^{n} a_i)\right\} \geq \cdots \geq \min_{i=1}^{n}\{\nu(a_i)\}$$

Example (1) A valuation on p-adic integers $\mathbb{Z}_p$:

Definition 9.3: Associated Structures to valuation

Let $\nu : K \to \Gamma \cup \{\infty\}$ be the valuation with the same setting in definition 9.2.
The **valuation group/ value group** is $\Gamma_\nu := \nu(K^\times)$. Since $x \in K^\times \Leftrightarrow \nu(x) \in \Gamma$, then $\nu(K^\times) \subseteq \Gamma$ and more, $\nu(K^\times) \leq \Gamma$.
The **valuation ring** $R_\nu := \{x \in K : \nu(x) \geq 0\}$. When $\Gamma = \mathbb{Z}$, R_ν is called a **discrete valuation ring**.
The **prime ideal**(in fact **maximal ideal**) $\mathfrak{m}_\nu := \{x \in K : \nu(x) > 0\}$
The **residual field** $k_\nu := R_\nu / \mathfrak{m}_\nu$
The place of K associated to ν

Theorem 9.1: Characterisation of valuation rings

Let R be an integral domain and $K := \mathrm{Frac}(R)$. Then the followings are equivalent:
(1) $\forall x \in K$, either $x^{-1} \in R$ or $x \in R$.
(2) The ideals of R are totally ordered by $\subseteq$.
(3) The principal ideals of R are totally ordered by $\subseteq$.
(4) $\exists$ a totally ordered abelian group Γ and a valuation on K, $\nu : K \to \Gamma \cup \{\infty\}$ such that $R = R_\nu$.

Proof: □

Now let ν be a discrete valuation temporarily. We just call the structure $\mathfrak{m}_\nu$ a maximal ideal but we do not see it is. Also the validity of residue field comes from that valuation ring is a local ring, so the maximal ideal is unique. Then, the quotient is unique on choosing the maximal ideal.

$$\begin{array}{ccc} (1) R_\nu \text{ is local} & & \\ \uparrow & & \\ (2) \mathfrak{m}_\nu \text{ is maximal} & \xrightarrow{(1)} & k_\nu := R_\nu / \mathfrak{m}_\nu \text{ unique quotient field} \end{array}$$

Theorem 9.2: R_ν is a local ring

Let K be a field, $(\Gamma, +, \geq)$ be a totally ordered abelian group, and $\nu : K \to \Gamma \cup \{\infty\}$ be a discrete valuation on K. Then, the valuation ring R_ν is a local ring.

Proof: $\forall x, y \in R - R^\times$, we would like to show $x + y \in R - R^\times$. The equivalence 2.1 tells that R is a local ring. If $x = 0$, then $x + y = y \in R - R^\times$. Similar argument for $y = 0$. So, let's assume both $x \neq 0$ and $y \neq 0$. By assumption, $x^{-1}, y^{-1} \notin R$ but $x^{-1}, y^{-1} \in K$. Consider xy^{-1}. From 9.1, either $xy^{-1} \in R$ or $yx^{-1} \in R$. Without loss of generality, assume $xy^{-1} \in R$. Then, suppose $x + y \in R^\times$, meaning $\exists u \in R$, $u(x+y) = 1$. Hence,

$$y^{-1} = u(x+y)y^{-1} = u(xy^{-1} + 1) \in R$$

which contradicts to the fact that $y \in R - R^\times$. Hence, $x + y$ cannot be a unit. $\square$ Is R_ν a PID?

Lemma 9.1 (Existence of uniformizer) *Exist*

Theorem 9.3: $\mathfrak{m}_\nu$ is a maximal ideal

Let K, Γ, ν be the same setting as above. Then, $\mathfrak{m}_\nu$ is the [a] maximal ideal of R_ν.

[a] The locality of R_ν makes $\mathfrak{m}_\nu$ 'a' maximal ideal 'the' maximal ideal.

Proof: To show $\mathfrak{m}_k$ is maximal, fix a proper ideal $I \trianglelefteq R$ with $\mathfrak{m}_\nu \subseteq I \subsetneq R_\nu$.
The lemma above gives the existence of uniformizer π of R_ν. Then, $\forall x \in I$,

$$\nu(x) = \nu(\pi \cdot \pi^{-1} x) = \nu(\pi) + \nu(\pi^{-1} x) = 1 + \nu(\pi^{-1} x) \overset{\dagger}{\geq} 1 > 0$$

$\dagger$: $\pi^{-1} x \in R_\nu$, then $\nu(\pi^{-1} x) \geq 0$. So, $x \in \mathfrak{m}_\nu$. $\square$
A question is raising: can we extend this fact to every valuation ν, not only discrete valuation? If the answer is yes, what kind of modification should we made? If the answer is no, to what level can we extend $\mathbb{Z}$? (Guessing a discrete subgroup of Γ is the upper bound) Note that in the proof of theorem 9.3, the crucial part relied is the existence of an element has valuation > 0. We do not even use the existence of uniformizer.
does uniformizer always exist in a totally-ordered abelian group? Does a element greater than zero always exist in a toag?

9.1.2 Discrete valuation

9.2 Absolute value

Definition 9.4: Real absolute value

A **real absolute value** on a field K is a map $|\cdot| : K \to \mathbb{R}_{>0} \cup \{0\}$ such that in the following:
(1) $|x| = 0 \Leftrightarrow x = 0_K$
(2) $\forall x, y \in K$, $|xy| = |x||y|$
(3) (Triangle inequality) $|x + y| \leq |x| + |y|$
(4) (Ultra triangle inequality) $|x + y| \leq \max\{|x|, |y|\}$ with equality $\Leftrightarrow |x| \neq |y|$
$(1), (2), (3)$ are satisfied.
If $|\cdot|$ satisfies one more (4), then $|\cdot|$ is called a **non-Archimedean real absolute value**; if (4) is not satisfied (only (1), (2) and (3)), then $|\cdot|$ is **Archimedean real absolute value**.

Remark The second part says that $|\cdot| : K^\times \to \mathbb{R}_{>0}$, $\mathbb{R}_{>0}$ as a multiplicative group, is a group homomorphism.

Definition 9.5: Absolute value

Let $(\Sigma, \cdot, \leq)$ be a multiplicative totally abelian group. Let K be a field. Joining O, put order relations between Σ and O: $\forall \alpha \in K$, $\alpha \in \Sigma, \alpha \geq O$ and $\alpha \cdot O = O \cdot \alpha = O$.
An **absolute value** on K is a map $|\cdot| : K \to \Gamma \cup \{O\}$ such that:
- $|x| = O \Leftrightarrow x = 0_K$
- $\forall x, y \in K$, $|xy| = |x||y|$
- $\forall x, y \in K$, $|x + y| \leq \max\{|x|, |y|\}$ with equality $\Leftrightarrow |x| \neq |y|$. By induction, $\left|\sum_i x_i\right| \leq \max_i\{|x_i|\}$

In this generalization, we choose the harsher inequality, ultra triangle inequality. So, this is exactly a generalization of a non-Archimedean absolute value. The reason is inside the following theorem: it tells us how to pass one from another, as illustrated in the diagram:

$$\begin{tikzcd} K \arrow[r, "\nu"] \arrow[rr, bend left, "|\cdot|_\nu = f\circ\nu"] & (\Gamma\cup\{\infty\},+,\leq) \arrow[r, shift left, "f"] & (\Sigma\cup\{O\},\cdot,\leq) \arrow[l, shift left, "g"] & K \arrow[l, "|\cdot|"'] \arrow[ll, bend left, "\nu_{|\cdot|}=g\circ|\cdot|"] \end{tikzcd} \quad \text{or} \quad \begin{tikzcd} (\Gamma\cup\{\infty\},+,\leq) \arrow[rr, shift left, "f"] & & (\Sigma\cup\{O\},\cdot,\leq) \arrow[ll, shift left, "g"] \\ & K \arrow[ul, "\nu"] \arrow[ur, "|\cdot|"'] & \end{tikzcd}$$

Theorem 9.4: Correspondence between valuation and absolute value

Set $(\Gamma,+,\leq)$ to be an totally ordered additive abelian group with ∞ having order relations with Γ, and $(\Sigma,\cdot,\leq)$ to be an totally ordered multiplicative abelian group with O having order relations with Σ. Let K be a field. Then, we have the correspondence:
• $\nu : K \to \Gamma\cup\{\infty\}$ is a valuation. $f : (\Gamma\cup\{\infty\},+,\leq) \to (\Sigma\cup\{O\},\cdot,\leq)$ is an order-reversing group homomorphism with $\infty \mapsto O$, then $\exists$ an absolute value $|\cdot|_\nu : K \to \Sigma\cup\{O\}$ depending on ν, $|\cdot|_\nu = f\circ\nu$.
• $|\cdot| : K \to \Sigma\cup\{O\}$ is an absolute value. $g : (\Sigma\cup\{O\},\cdot,\leq) \to (\Gamma\cup\{\infty\},+,\leq)$ is an order-reversing group homomorphism with $O \mapsto \infty$, then $\exists$ a valuation $\nu_{|\cdot|} : K \to \Gamma\cup\{\infty\}$ depending on $|\cdot|$, $\nu_{|\cdot|} = g\circ|\cdot|$.

Proof: Let ν and f have the above-mentioned settings. Then, we check:
(1) $|x|_\nu = O \Leftrightarrow f(\nu(x)) = O \Leftrightarrow \nu(x) = +\infty \Leftrightarrow x = 0_K$
(2) $|xy|_\nu = f(\nu(xy)) = f(\nu(x)+\nu(y)) = f(\nu(x))f(\nu(y)) = |x|_\nu \cdot |y|_\nu$
(3) $|x+y|_\nu = f(\nu(x+y)) \leq f(\min\{\nu(x),\nu(y)\}) = \max\{f(\nu(x)), f(\nu(y))\} = \max\{|x|_\nu, |y|_\nu\}$
Let $|\cdot|$ and g have the above-mentioned settings. Then, we check:
(1) $\nu_{|\cdot|}(x) = +\infty \Leftrightarrow g(|x|) = +\infty \Leftrightarrow |x| = O \Leftrightarrow x = 0_K$
(2) $\nu_{|\cdot|}(xy) = g(|xy|) = g(|x||y|) = g(|x|) + g(|y|) = \nu(x) + \nu(y)$
(3) $\nu_{|\cdot|}(x+y) = g(|x+y|) \geq g(\max\{|x|,|y|\}) = \min\{g(|x|), g(|y|)\} = \min\{\nu_{|\cdot|}(x), \nu_{|\cdot|}(y)\}$ □

9.3 Extension of valuations

Definition 9.6: Extension of valuation to field extension

Let L/K be a field extension (not necessarily finite). A valuation $w : L \to \Gamma\cup\{\infty\}$ on L is an **extension** of a valuation $v : K \to \Gamma\cup\{\infty\}$ on $K \Leftrightarrow w|_K = v$.

The set of all extensions of valuations of K is studied in the ramification theories of valuations. In general (for arbitrary field extension), we do not know how many (non-equivalent) extensions of a valuation are there. But, the answer is definite for finite field extensions and it is an application of 'trace and norm' in fields:

Theorem 9.5: Existence and uniqueness of the extension valuation

Definition 9.7: Associated structures to extensions of valuations

Let L/K be a finite field extension and $v : K \to \Gamma\cup\{\infty\}$, $w : L \to \Gamma\cup\{\infty\}$ are valuations on K and L respectively. w is an extension of v. Then,
the **ramification index** of w over v, denoted $e_{w/v}$, is $e_{w/v} := [\Gamma_w : \Gamma_v] := [w(L^\times) : v(K^\times)]$, which is the index of a valuation group in another.
the **relative/residue degree** of w over v, denoted $f_{w/v}$, is $f_{w/v} := [k_w : k_v] := [R_w/\mathfrak{m}_w : R_v/\mathfrak{m}_v]$, which is the degree of field extension between two residue fields.

Remark The two concepts are in some sense dual to each other. Ramification index studies the information in the group side of valuations. While relative degree studies the field side of valuations.

A naturally raised question is (1) to what extent the two numbers are relative to the degree $[L:K]$? The answers have already existed without giving a proof here: $e_{w/v} \leq [L:K]$ and $f_{w/v} \leq [L:K]$. This answer seems not satisfiable because it only answers inequalities. So, the next question is when the equalities hold in both cases.
(2) The relation between $e_{w/v}$ and $f_{w/v}$ also seems intriguing. When L/K is a separable extension, there is a make-up equality, $e_{w/v} = f_{w/v}[k_w : k_v]_i$, where $[k_w : k_v]_i$ is the inseparable degree of k_w over k_v.
The question raised here could be summarized in one diagram:

$$\begin{tikzcd} f_{w/v} \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow, "\leq"'] & & e_{w/v} \arrow[dl, leftrightarrow, "\leq"] \\ & {[L:K]} & \end{tikzcd}$$

10 Completion

In analysis, we complete rational numbers to get a complete ordered field, real numbers. One way is to use Cauchy sequences. To make completion an algebraic operation,
A filtration enables endowing an module a topology. With respect to this topology, we can complete the module.

10.1 Graded rings and modules

10.1.1 Basic definitions and gradations

Definition 10.1: Graded rings

Let R be a ring(not necessarily commutative). R is a **graded ring** $\Leftrightarrow$ R is equipped a direct decomposition (meaning it can be decomposed into inner direct products) of the underlying **additive** groups (which are abelian)

$$R = \bigoplus_{n\geq 0} R_n$$

such that $\forall m, n \in \mathbb{Z}_{\geq 0}$, $R_m R_n \subseteq R_{m+n}$

Remark In the decomposition into direct sum, we only use the group structure (only addition). For $R_m R_n$ condition, we use the multiplication in ring R.
Example (1) **Trivial gradation**: Let S be any ring. Then S can be given a gradation with $R_0 = R$ and $R_n = \{0\}$ for all $n > 0$.
(2) Polynomial rings: Consider a polynomial ring $R[t_1, \dots, t_n]$
Further, given R a graded ring, one can define graded R-module.

Definition 10.2: Graded left R-modules

Let R be a graded ring with decomposition $R = \bigoplus_{n\geq 0} R_n$. Let M be a left R-module.
M is a **graded** left R-module $\Leftrightarrow$ M has a decomposition into abelian groups

$$M = \bigoplus_{n\in\mathbb{Z}} M_n$$

such that $\forall m \in \mathbb{Z}_{\geq 0}$, $\forall n \in \mathbb{Z}$, $R_m M_n \subseteq M_{m+n}$. Elements of R_n are called **homogeneous** of degree n.

Example (1) If R is a graded ring, R is a graded left ideal(also a graded module) over itself.
(2) Let $I \trianglelefteq R$ be an ideal of R. I is a
There is a category of graded R-modules ([Uchicago]), where the objects are all graded left R-modules and the morphisms are the morphisms of left R-modules that preserve the grading (taking homogeneous elements to homogeneous elements of the same degree).

Definition 10.3: Graded algebra

Example (1) Polynomial rings:
(2) The tensor algebra T^*V of a vector space V
(3) The exterior algebra $\bigwedge^* V$ and the symmetric algebra S^*V
(4) The cohomology ring H^*

Definition 10.4: Graded submodule

Let R be a graded ring and M an R-graded module. Then, a submodule $N \leq M$ is a graded submodule of $M \Leftrightarrow \forall y \in N$, $\forall$ decomposition of $y = \sum_n y_n$ into homogeneous component of y with respect to M, $y_n \in N$.
An ideal $I \trianglelefteq R$ is **graded ideal** $\Leftrightarrow$ I is a graded submodule of R

Remark This definition looks trivial but it actually not. It can be translated in many ways: N is a graded submodule iff every element of N, written as a sum of elements belonging to graded components of M, M_n, belongs to some graded component of N, N_{k_n}. In other words, the graded submodule is not only closed under addition and scalar multiplication, but also closed under taking homogeneous components.
Another subtlety is that each homogeneous component of M, say M_n lying in N implies that it is a homogeneous component of N by taking $N_n := N \cap M_n$.
Example Let F be a field and $F[x, y]$ be the corresponding polynomial ring, which is a graded-ring, hence graded-module. Now consider the ideal $\langle x + y\rangle$, this is a submodule of $F[x, y]$ and a graded one. But, $\langle x + y^2\rangle$ is not a graded one
$F[x, y]$ has the gradation into collections of polynomials in certain degree. Consider $x + y^2$, it can be decomposed into itself or two components x and y^2, both are in M and are homogeneous of degree 1 and 2, respectively. But neither x nor y^2 belongs to $\langle x + y^2\rangle$.

From these two examples, we noticed that $\langle x + y\rangle$ is a graded ideal and it is generated by a homogeneous element. So, those ideals generated by homogeneous elements can be called **homogeneous ideals**.

Definition 10.5: Homogeneous ideal

The homogeneous ideals and graded ideals are actually synonymous.

Proposition 10.1: Characterisation of homogeneous ideal

Let R be a graded ring and M an R-graded module, and $I \trianglelefteq R$.
I is a homogeneous ideal $\Leftrightarrow$ I is a graded ideal.

Proof: Let I be an R-graded ideal. Then, I admits a gradation:

$$I = \bigoplus_{i\in\mathbb{Z}_{\geq 0}} I \cap R_i$$

So, I is generated by the set $\bigcup_{i\in\mathbb{Z}_{\geq 0}}\{I \cap R_i\}$, which are all homogeneous.
Let I be a homogeneous ideal, generated by the set $\{h_\alpha\}_\alpha$. So, $\forall x \in I$,

$$x = \sum_\alpha r_\alpha h_\alpha = \sum_\alpha \left(\sum_i (r_\alpha)_i\right) h_\alpha \overset{\dagger}{=} \sum_\alpha \left(\sum_j \sum_{i:i+\deg h_\alpha = j} (r_\alpha)_i h_\alpha\right) = \sum_\alpha \left(\sum_j (r_\alpha)_i h_\alpha\right) \overset{\ddagger}{=} \sum_j \sum_\alpha (r_\alpha)_{j-\deg h_\alpha} h_\alpha$$

†: Change of variable. After changing the variable, the i becomes a specific one, not an arbitrary index anymore;
‡: Because each $r_\alpha \in R$ and R is graded, so it can be written as a direct sum. So, the sum indexed by j is finite. Also, since x is generated by h_α, the sum indexed by α is finite as well.
Then, let $x_j := \sum_\alpha (r_\alpha)_{j-\deg h_\alpha} h_\alpha$, which is an homogeneous element of degree j. Each x_j is a linear combination of h_α so it lies in I. □

Lemma 10.1: Characterisation of homogeneous prime ideal

Let $\mathfrak{p}$ be a homogeneous ideal of a graded ring R. $\mathfrak{p}$ is a prime ideal $\Leftrightarrow$ $\forall$ homogeneous element $x, y \in R$, $xy \in R \Rightarrow x \in R$ or $y \in R$

Proof: $\Rightarrow$ is trivial. For $\Leftarrow$, let $\mathfrak{p}$ be a homogeneous prime ideal, and x, y be two arbitrary homogeneous elements. Suppose $xy \in \mathfrak{p}$.
Write x and y into sum of homogeneous components,

$$x = x_{m_1} + \cdots + x_{m_s} \quad y = y_{n_1} + \cdots + y_{n_t}$$

where each $x_{m_i} \in R_{m_i}$ and $y_{n_j} \in R_{n_j}$.
Now there are at most $s+t$ homogeneous components for xy in total. Induct on $s+t$:

- Base case: $m+n=0$, then $x=y=0$, both are in $\mathfrak{p}$.
- Inductive hypothesis: for every k, when $m+n=k$, $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.
- When $m+n=k+1$, consider $x_{m_s}y_{n_t}$, which is a homogeneous component and $\mathfrak{p}$ is a graded ideal(submodule) by proposition 10.1. This implies that $x_{m_s}y_{n_t} \in \mathfrak{p}$ by definition 10.4. Primity of $\mathfrak{p}$ implies $x_{m_s} \in \mathfrak{p}$ or $y_{n_t} \in \mathfrak{p}$. Without loss of generality, we assume that $x_{m_s} \in \mathfrak{p}$. On the other hand, $(x - x_{m_s})y \in \mathfrak{p}$ because both $xy \in \mathfrak{p}$ and $x_{m_s}y \in \mathfrak{p}$. Since $(x - x_{m_s})y$ has $m+n-1=k$ homogeneous components, $x - x_{m_s} \in \mathfrak{p}$ or $y \in \mathfrak{p}$. If it is the first case, $x = x - (x_{m_s}) + x_{m_s} \in \mathfrak{p}$. So, $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. □

Morphisms between two graded module and category

Definition 10.6: Morphisms between two graded module

So, now R-graded modules can be made into a category.
Instead of taking the index start from 0, we could set the starting point somewhere else and call it 'torsion'.

Definition 10.7: Torsion graded module

What is the meaning of this definition?
In fact, from the origin R to this definition, we have actually defined a functor.

10.1.2 Finiteness condition

Definition 10.8: Irrelevant ideals

Let R be a graded ring with decomposition $R = \bigoplus_{i \in \mathbb{Z}_{\geq 0}} R_i$. The **irrelevant ideal** of R, denoted R_+, is $R_+ := \bigoplus_{i \in \mathbb{Z}_{>0}} R_i$

Remark R_+ is a graded ideal of R. First, R_+ is a submodule of R:
It is closed under $+$, since every R_i is an additive group.
It is closed under $\cdot$: take arbitrary $r \in R$ and $y \in R_+$, say $r = r_0 + \sum_i r_i$ and $y = \sum_j y_j$, with both being finite sums and $i, j > 0$. Then, $ry = r_0 y + \sum_i \sum_j r_i y_j$. Since each R_i is an R_0-module, $r_0 y \in R_+$. By definition 10.2, $r_i y_j \in R_i R_j \subseteq R_{i+j}$. So, each component is in some R_k with $k > 0$. Hence, $ry \in R_+$.
The last thing is R_+ is a graded ideal/submodule. This is because every element of R_+ can be decomposed into elements inside $R_i \subseteq R$ for some i. So, by 10.4, R_+ is a graded ideal.

10.1.3 Localization and Gradation

10.2 Filter, rings and modules

Now let's introduce a more general and weaker concept, 'filtration'.

Definition 10.9: Filtration and filtered rings

Let R be a ring. A **filtration** on a ring R is a sequence of ideals of R, $R = I_0 \supseteq I_1 \supseteq \dots$, such that $\forall m, n \geq 0$, $I_m I_n \subseteq I_{m+n}$. A ring R together with a filtration $\{I_n\}$ is a **filtered ring**.

Remark Filtered rings can be thought of as a generalization of graded rings because every graded rings has a canonical filtration. Let R be a graded ring with decomposition $R = \bigoplus_{i \in \mathbb{Z}_{\geq 0}} R_i$. Taking $I_m := \bigoplus_{i \geq m} R_i$, I_m is an ideal and this is a filtration, called the **filtration induced by grading**.
The 'weaker' embodies in the sense that: comparing to the gradation gives a precise description of components of a precise/certain degree, the filtration only tells the lowest degree. In other words, it gives elements of degree greater that a certain number. This would be manifested in the first example. From this perspective, we can say gradation is '**finer**' and the filtration is a '**coarser**' concept.

Example (1) Polynomial rings: Let R be a ring. $R[x]$ has a filtration $\{\langle x^i \rangle\}_i$. Each one is an ideal generated by an element of certain degree. So, the elements in ideal $\langle x^i \rangle$ has the least degree i. By in gradation, each components consist of homogeneous polynomial of degree exactly i for some i.
(2) I-**adic filtration**: Especially, let $I \trianglelefteq R$. We have a special filtration consists of power of I, i.e. $I_m := I^m$. (Here we abuse the notation I). This is especially important when R is a local ring and I is a maximal ideal of R. The example (1) is actually an $\langle x \rangle$-adic filtration.
(3) More generally, in ring $k[x_1, \dots, x_n]$, consider the $\langle x_1, x_2, \dots, x_n \rangle$-adic filtration. Then, this filtration coincides with the filtration induced by grading.
(4) Formal power series:

Definition 10.10: Filtration and filtered modules

10.2.1 Associative graded rings

As we did in definition 10.9, we saw how graded rings can be made into filtrations. Can we do the inverse process from a filtered ring to a graded ring?

$$\begin{tikzcd}
\text{filtered rings} \arrow[r, bend left, "?"] & \text{graded rings} \arrow[l, bend left, "\textbf{in Remark } 10.9"]
\end{tikzcd}$$

We are not be able to make R directly into a graded ring. However, we have a compensation:

Definition 10.11: Associated graded ring

Let $(R, \{I_n\})$ be a filtered ring (with filtration $\{I_n\}$). The **associated graded ring** of R, denoted $\mathrm{gr}(R)$, is defined to be
$$\mathrm{gr}(R) := \bigoplus_{m \in \mathbb{Z}_{\geq 0}} I_m / I_{m+1}$$

Remark For $\mathrm{gr}(R)$ we mentioned in this definition, $\mathrm{gr}(R)$ is a graded ring. When the filtration is the I-adic filtration, we stress the associated graded ring $\mathrm{gr}(R)$ by $\mathrm{gr}^I(R)$.

Theorem 1 *In the setting of definition 10.11,* $\mathrm{gr}(R)$ *is a graded ring.*

Proof: Define the multiplication of $\mathrm{gr}(R)$ component-wise: merely define multiplication for the component of sum of $\mathrm{gr}(R)$: $a_m \in I_m$ and $b_n \in I_n$ ($\overline{a_m} \in I_m/I_{m+1}$, $\overline{b_n} \in I_n/I_{n+1}$),
$$\overline{a_m} \cdot \overline{b_n} := \overline{a_m b_n} := a_m b_n + I_{m+n+1} \in I_{m+n}/I_{m+n+1}$$
We are going to show that this forms a ring.

• This definition is well-defined, since for another $a'_m \neq a_m$ and $b'_n \neq b_n$ but $\overline{a'_m} = \overline{a_m}$ and $\overline{b'_n} = \overline{b_n}$, $a'_m = a_m + u$ and $b'_n = b_n + v$ with $u \in I_{m+1}$ and $v \in I_{n+1}$. Then,
$$a'_m b'_n = (a_m + u)(b_n + v) = a_m b_n + \underbrace{a_m v}_{\in I_{m+1} \cdot I_n} + \underbrace{b_n u}_{\in I_m \cdot I_{n+1}} + \underbrace{uv}_{\in I_{m+1} \cdot I_{n+1}}$$
By definition 10.9, $I_{m+1} I_n, I_{n+1} I_m \subseteq I_{m+n+1}$ and $I_{m+1} I_{n+1} \subseteq I_{m+n+2} \subseteq I_{m+n+1}$.

$\mathrm{gr}(R)$ is an additive group. The associativity, distributivity come from R. Multiplicative identity is $\overline{1} \in I_0/I_1$. As we shown, the multiplication is a map $I_m/I_{m+1} \times I_n/I_{n+1} \to I_{m+n}/I_{m+n+1}$, so $\forall m, n$, $\mathrm{gr}(R)_m \cdot gr(R)_n \subseteq \mathrm{gr}(R)_{m+n}$. So, $\mathrm{gr}(R)$ is a graded ring. $\square$

Definition 10.12: Associated graded module

Let $(R, \{I_n\})$ be a filtered ring (with filtration $\{I_n\}$). The **associated graded ring** of R, denoted $\mathrm{gr}(R)$, is defined to be
$$\mathrm{gr}(R) := \bigoplus_{m \in \mathbb{Z}_{\geq 0}} I_m / I_{m+1}$$

Remark Fix a ring R. From this definition, the gr becomes a functor from the category of filtered R-module $\mathbf{filMod}_R$ to the category of graded $\mathrm{gr}(R)$-modules $\mathbf{gradMod}_{\mathrm{gr}(R)}$

10.2.2 Topology induced by filtration

11 Dimension theory

11.1 Length

11.2

References

[Uchicago] Shishir Agrawal etc. *The CRing Project*. https://math.uchicago.edu/~amathew/CRing.pdf. 2011.

[AM18] M.F. Atiyah and I.G. MacDonald. *Introduction To Commutative Algebra*. CRC Press, 2018. ISBN: 9780429962189. URL: https://books.google.ca/books?id=4nhQDwAAQBAJ.

[Mil20] James S. Milne. *Algebraic Number Theory (v3.08)*. Available at www.jmilne.org/math/. 2020.

[BGS24] Andrea Bandini, Patrizia Gianni, and Enrico Sbarra. "Rings". In: *Commutative Algebra through Exercises*. Cham: Springer International Publishing, 2024, pp. 3–19. ISBN: 978-3-031-56910-4. DOI: 10.1007/978-3-031-56910-4_1. URL: https://doi.org/10.1007/978-3-031-56910-4_1.