Commutative Algebra

Dr. Thomas Markwig *

April 29, 2015

*LaTeXed by Simon Hampe in 2007/8

Contents

1. Rings and Ideals

A). Basics

Definition 1.1. A (commutative) *ring* (with 1) $(R, +, \cdot)$ is a set R with two binary operations, such that

(a) $(R, +)$ is an abelian group

(b) $(R, \cdot)$ is associative, commutative and contains a 1 - element.

(c) The distributive laws are satisfied.

Note.

- We will say "ring", instead of "commutative ring with 1".
- We will usually write "R", instead of "$(R, +, \cdot)$".
- Only the multiplicative inverses are missing for a field.
- If $0_R = 1_R$, then $R = \{0\}$

  Proof. Let $r \in R$. Then

$$\begin{aligned} 0 + r &= 0 + 1 \cdot r = (0 + 1) \cdot r \\ &= (1 + 1) \cdot r = r + r \\ &\implies r = 0 \end{aligned}$$

□

Example 1.2.

(a) Fields are rings, e.g. $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ for p prime.

(b) $\mathbb{Z}$ is a ring

(c) If R is a Ring $\implies R[\![\underline{x}]\!] = \{\sum_{|\alpha|=0}^{\infty} a_\alpha \underline{x}^\alpha \mid a_\alpha \in R\}$, where:

$$\begin{aligned}\underline{x} &:= (x_1, ..., x_n)\\ \alpha &:= (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n\\ \underline{x}^\alpha &:= x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}\\ |\alpha| &:= \alpha_1 + ... + \alpha_n\end{aligned}$$

is the ring of *formal power series* over R in the indeterminance $x_1, ..., x_n$. The operations are defined as

$$\sum_{|\alpha|=0}^{\infty} a_\alpha \underline{x}^\alpha + \sum_{|\alpha|=0}^{\infty} b_\alpha \underline{x}^\alpha = \sum_{|\alpha|=0}^{\infty} (a_\alpha + b_\alpha)\underline{x}^\alpha$$

$$\sum_{|\alpha|=0}^{\infty} a_\alpha \underline{x}^\alpha \cdot \sum_{|\beta|=0}^{\infty} b_\beta \underline{x}^\beta = \sum_{|\gamma|=0}^{\infty} (\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta)\underline{x}^\gamma$$

Notation:

$$\operatorname{ord}(\sum_{|\alpha|=0}^{\infty} a_\alpha \underline{x}^\alpha) := \begin{cases} \infty \text{ , if } a_\alpha = 0 \quad \forall\alpha \\ \min\{|\alpha| \text{ s.t. } a_\alpha \neq 0\} \text{ , otherwise}\end{cases}$$

(d) $\mathbb{R}\{\underline{x}\}, \mathbb{C}\{\underline{x}\}$ are the rings of convergent power series over $\mathbb{R}$ and $\mathbb{C}$.

(e) If M is a set and R a ring, then $R^M := \{f : M \to R \mid f \text{ is a map}\}$ is a ring with respect to :

$$\begin{aligned}(f+g)(m) &:= f(m) + g(m)\\ (f \cdot g)(m) &:= f(m)g(m)\end{aligned}$$

(f) If $R_\lambda, \lambda \in \Lambda$ is a family of rings, then $\prod_{\lambda\in\Lambda} R_\lambda = \{(a_\lambda)_{\lambda\in\Lambda} \mid a_\lambda \in R_\lambda\}$, the *direct product*, is a ring with respect to componentwise operations.

Definition 1.3. Let $(R, +, \cdot)$ be a ring, $I \subseteq R$

(a) I is a *subring* of $R :\iff (I, +, \cdot)$ is a ring with respect to the same operations restricted to I.

(b) I is an *ideal* of $R :\iff$

- $I \neq \emptyset$
- $\forall a, b \in I : \ a + b \in I$
- $\forall a \in I, r \in R : \ ra \in I$

Notation: $I \trianglelefteq R$

(c)

$$\begin{aligned}\langle I\rangle &:= \bigcap_{I\subseteq J\trianglelefteq R} J\\ &= \left\{\sum_{i=1}^{n} r_i a_i \,\middle|\, n\in\mathbb{N}_0, r_i\in R, a_i\in I\right\}\end{aligned}$$

is the ideal *generated by I*.

(d) If $I=\{a\}$, then $\langle a\rangle = aR := \{ar \,|\, r\in R\}$ is a *principal ideal*.

(e) If $I\trianglelefteq R$, then

$$R/I := \{r+I \,|\, r\in R\}$$

is the *quotient ring* and it's a ring with respect to operations via representatives.

Example 1.4.

(a) $\mathbb{Z}_p := \{\frac{a}{p^n} \,|\, a\in\mathbb{Z}, n\in\mathbb{N}\} \leq \mathbb{Q}$ for p prime

(b) Let R be a ring.

$$R[\underline{x}] := \{\sum_{|\alpha|=0}^{n} a_\alpha \underline{x}^\alpha \,|\, a_\alpha\in R, n\in\mathbb{N}\} \leq R[\![\underline{x}]\!]$$

is called the *polynomial ring* in the indeterminance $(x_1,...,x_n)=\underline{x}$. We define:

$$\deg(\sum_{|\alpha|=0}^{n} a_\alpha \underline{x}^\alpha) = \begin{cases}-\infty & \text{if } a_\alpha = 0\,\forall\alpha\\ \max\{|\alpha| \text{ s.t. } a_\alpha\neq 0\} & \text{else}\end{cases}$$

(c) R is a field $\iff$ $\{0\}$ and R are the only ideals.

Proof. We show two directions:
"$\implies$":

$$\begin{aligned}&I\trianglelefteq R, I\neq\{0\}\\ \implies&\exists a\in I: a\neq 0\\ \implies&\exists a^{-1}\in R\\ \implies&a^{-1}a = 1\in I\\ \implies&\forall r\in R: r\cdot 1 = r\in I\\ \implies&I = R\end{aligned}$$

"$\Longleftarrow$": Let $0 \neq r \in R$, then $0 \neq \langle r \rangle \trianglelefteq R$

$$\begin{aligned} &\Longrightarrow \langle r \rangle = R, \text{ but } 1 \in R \\ &\Longrightarrow \exists s \in R : sr = 1 \\ &\Longrightarrow \text{ R is a field.} \end{aligned}$$

□

(d) $I \trianglelefteq \mathbb{Z} \iff \exists n \in \mathbb{Z} : \langle n \rangle = I$. In particular, every ideal in $\mathbb{Z}$ is a principal ideal.

Proof.
"$\Longleftarrow$" is trivial.
"$\Longrightarrow$": If $I = \{0\}$, then $I = \langle 0 \rangle$, so let $I \neq \{0\}$. Choose $n \in I$ minimal, such that $n > 0$. We want to show that $I = \langle n \rangle$:

$$\begin{aligned} &\text{"}\supseteq\text{"} : \checkmark \\ &\text{"}\subseteq\text{"} : \text{Let } a \in I \\ &\qquad \overset{d.w.r.}{\Longrightarrow} \exists q, r \in \mathbb{Z} : a = qn + r, 0 \leq r < n \\ &\qquad \Longrightarrow r = a - qn \in I \\ &\qquad \overset{r<n}{\Longrightarrow} r = 0 \\ &\qquad \Longrightarrow a = qn \in \langle n \rangle \end{aligned}$$

□

(e) Let K be a field, then $I \trianglelefteq K[x] \iff \exists f \in K[x] : I =< f >$

Proof. As for the integers, just choose $f \in I \backslash \{0\}$ of minimal degree □

(f) Let K be a field, then: $I \trianglelefteq K [\![x]\!] \iff \exists n \geq 0 : I = \langle x^n \rangle$

Proof. postponed to 1.8 (c) □

Definition 1.5 (Operations on ideals)**.**

Let $I, J, J_\lambda \trianglelefteq R, \lambda \in \Lambda$

- $I + J := \langle I \cup J \rangle = \{a + b \,|\, a \in I, b \in J\} \trianglelefteq R$ is the *sum (of ideals)*.
- $I \cap J := \{a \,|\, a \in I, a \in J\} \trianglelefteq R$ is the *intersection (of ideals)*.
- $I \cdot J := \langle \{ab \,|\, a \in I, b \in J\} \rangle \trianglelefteq R$ is the *product (of ideals)*.
- $I : J := \{a \in R \,|\, aJ \subseteq I\} \trianglelefteq R$ is the *quotient (of ideals)*.
- $\sqrt{I} := rad(I) := \{a \in R \,|\, \exists n \geq 0 : a^n \in I\} \trianglelefteq R$ is the *radical* of I.

Proof. (that $\sqrt{I} \trianglelefteq R$)

- $0^1 \in I \implies 0 \in \sqrt{I} \implies \sqrt{I} \neq \emptyset$
- $a \in \sqrt{I}, r \in R \implies \exists n : a^n \in I \implies (ra)^n = r^n a^n \in I \implies ra \in \sqrt{I}$
- $a, b \in \sqrt{I} \implies \exists n, m : a^n, b^m \in I$
  $\implies (a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k} \in I$

□

Note.

- $\sqrt{I \cdot J} = \sqrt{I \cap J}$

  Proof.

  "$\subseteq$" : ✓
  "$\supseteq$" : $a \in \sqrt{I \cap J} \implies \exists n : a^n \in I \cap J \implies a^{2n} = a^n a^n \in I \cdot J \implies a \in \sqrt{I \cdot J}$

  □

- We call

  $ann_R(I) := ann(I) := \{0\} : I = \{a \in R \,|\, aI = \{0\}\} = \{a \in R \,|\, ab = 0 \forall b \in I\} \trianglelefteq R$

  the *annihilator* of I.
- $\sum_{\lambda \in \Lambda} J_\lambda := \left\langle \bigcup_{\lambda \in \Lambda} J_\lambda \right\rangle$

$$= \left\{ \sum_{\lambda \in \Lambda} a_\lambda \,|\, a_\lambda \in J_\lambda, \text{ and only finitely many } a_\lambda \text{ are non-zero.} \right\}$$

- $\bigcap_{\lambda \in \Lambda} J_\lambda \trianglelefteq R$
- I and J are called *coprime* $:\iff I + J = R \iff 1 \in I + J$

Example 1.6. Let $R = \mathbb{Z}, I = \langle n \rangle, J = \langle m \rangle$ for $n, m \neq 0$

- $I + J = \langle n, m \rangle = \langle \gcd(n, m) \rangle$
- $I \cap J = \langle lcm(n, m) \rangle$
- $I \cdot J = \langle nm \rangle$
- $I : J = \left\langle \frac{n}{\gcd(n,m)} \right\rangle = \left\langle \frac{lcm(n,m)}{m} \right\rangle$
- $\sqrt{I} = \langle p_1 \cdot \ldots \cdot p_k \rangle$, if $n = \prod_{i=1}^k p_i^{\alpha_i}$ is the prime factorization of n.
- $ann(I) = \{0\}$

- I, J are coprime $\iff \mathbb{Z} = I + J = \langle \gcd(n, m) \rangle \iff \gcd(n, m) = 1$

Definition 1.7. Let R be a ring, $r \in R$

(a) r is a *zero-divisor* $:\iff \exists 0 \neq s \in R : rs = 0 \iff ann(r) \neq \{0\}$
Note. If $R \neq \{0\}$, then 0 is a zero-divisor by definition. If r is *not* a zero-divisor, the cancellation laws hold: $ar = br \implies a = b$. (short proof: $ar = br \implies (a-b)r = 0 \implies a - b = 0$)

(b) R is an *integral domain*(*I.D.*), if 0 is the only zero-divisor.

(c) $r \in R$ is a *unit* $:\iff \exists s \in R : sr = 1$
Note. $R^* = \{a \in R \,|\, a \text{ is a unit}\}$ is a group with respect to multiplication.

(d) r is *nilpotent* $:\iff \exists n \geq 1$, s.t. $r^n = 0$
Note. If $R \neq \{0\}$, then we have:

- r nilpotent $\implies r$ is a zero-divisor
- $\sqrt{0} = \{a \in R \,|\, a \text{ is nilpotent}\}$

(e) r is *idempotent* $:\iff r^2 = r \iff r(1-r) = 0$
Note. If $r \notin \{0, 1\}$ is idempotent, then r is a zero-divisor. Furthermore, 0 and 1 are always idempotent.

Example 1.8.

(a) $\mathbb{Z}$ is an I.D., $\mathbb{Z}^* = \{1, -1\}$

(b) If K is a field, then $K[\underline{x}]$ is an I.D. and $K[\underline{x}]^* = K^* = K \backslash \{0\}$

(c) Consider $R\llbracket x \rrbracket$, R any ring.

(1) $R\llbracket x \rrbracket^* = \{f \in R\llbracket x \rrbracket \mid f(0) \in R^*\}$

(2) x is *not* a zero-divisor

(3) $f = \sum_{i=0}^{\infty} f_i x^i$ is nilpotent $\implies f_i$ are nilpotent $\forall i$

Proof. Exercise. □

(4) *Proof.* (of 1.4 (f))
Claim: $0 \neq I \trianglelefteq K\llbracket x \rrbracket$, K a field $\iff \exists n \geq 0 : I = \langle x^n \rangle$

- "$\Longleftarrow$ ": trivial

- "$\Longrightarrow$": Choose $0 \neq g \in I, g = \sum_{i=0}^{\infty} g_i x^i$ with minimal $\operatorname{ord}(g) = n$

$$
\begin{aligned}
&\Longrightarrow g = x^n \underbrace{\sum_{i=n}^{\infty} g_i x^{i-n}}_{:=h} \\
&\overset{1.8\,(c.1)}{\Longrightarrow} h \in K\,[\![x]\!]^* \text{ (since } h(0) = g_n \neq 0) \\
&\Longrightarrow x^n = gh^{-1} \in I, \text{ since } g \in I \\
&\Longrightarrow \langle x^n \rangle \subseteq I
\end{aligned}
$$

Now let $0 \neq f \in I$ be arbitrary

$$
\begin{aligned}
&\Longrightarrow \operatorname{ord}(f) \geq n, \text{ by definition of } g \\
&\Longrightarrow f = x^n \underbrace{\sum_{i=n}^{\infty} f_i x^{i-n}}_{\in K[\![x]\!], i-n \geq 0} \in \langle x^n \rangle
\end{aligned}
$$

$\square$

(d) $R = K[x]/\langle x^2 \rangle \Longrightarrow \bar{0} \neq \bar{x}$ is nilpotent, since $\bar{x}^2 = \bar{0}$

(e) $R = K[x,y]/\langle x \cdot y \rangle \Longrightarrow \bar{0} \neq \bar{x}$ is not nilpotent, but a zero-divisor, since $\bar{x}\bar{y} = \bar{0}$

(f) $R = \mathbb{Z} \oplus \mathbb{Z} \Longrightarrow (\bar{1}, \bar{0})$ is idempotent.

Definition 1.9. Let R and R' be rings.

(a) $\varphi : R \longrightarrow R'$ is a *ringhomomorphism* (or a *ring extension*) $:\Longleftrightarrow$

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_{R'}$

Notation: $\operatorname{Hom}(R, R') = \{\varphi : R \to R' \mid \varphi \text{ is a ringhom.}\}$
Note. R' is an R - module via $rr' = \varphi(r)r'$

(b) Let $\varphi \in \operatorname{Hom}(R, R')$

- $\operatorname{Im}(\varphi) := \varphi(R) \leq R'$ is the *image* of φ
- $\ker(\varphi) := \varphi^{-1}(0) \trianglelefteq R$ is the *kernel* of φ
- φ is a *monomorphism*/*epimorphism*/*isomorphism* $:\Longleftrightarrow$ φ is injective/surjective/bijective

Note. φ is a Monom. $\Longleftrightarrow \ker(\varphi) = \{0\}$

(c) Let $\varphi \in \operatorname{Hom}(R, R'), I \trianglelefteq R, J \trianglelefteq R'$. Then we define:

- $I^e := \langle \varphi(I) \rangle_{R'}$ the *extension* of I to R'
- $J^c := \varphi^{-1}(J) \trianglelefteq R$ the *contraction* of J to R

(d) Let $\varphi \in \operatorname{Hom}(R, R')$, then we call (R', φ) an R - *algebra*. Often we omit φ.

Given two R - algebras (R', φ) and (R'', ψ) an R - *algebra homomorphism* is a map $\alpha : R' \longrightarrow R''$, which is a ringhom. such that

$$\begin{tikzcd} R' \arrow[r, "\alpha"] & R'' \\ R \arrow[u, "\varphi"] \arrow[ur, "\psi"'] & \end{tikzcd}$$

commutes, i.e.: $\alpha \circ \varphi = \psi$

Lemma 1.10. *Let $\varphi \in \operatorname{Hom}(R, R'), I \trianglelefteq R, J \trianglelefteq R'$. Then:*

(a) $I^{ec} \supseteq I$

(b) $J^{ce} \subseteq J$

(c) $I^{ece} = I^e$

(d) $J^{cec} = J^c$

Proof.

(a) $a \in I \implies a \in \varphi^{-1}(\varphi(a)) \subseteq \varphi^{-1}(I^e) = I^{ec}$

(b) $J^{ce} = \left\langle \underbrace{\varphi(\varphi^{-1}(J))}_{\subseteq J} \right\rangle_{R'} \subseteq \langle J \rangle = J$

(c)

"$\supseteq$": 1.10 (a) $\implies I^{ec} \supseteq I \implies I^{ece} \supseteq I^e$
"$\subseteq$": Apply 1.10 (b) to $J := I^e$

(d)

"$\supseteq$": $J^c \trianglelefteq R' \overset{1.10}{\implies} J^{cec} \supseteq J^c$
"$\subseteq$": 1.10(b) $\implies J^{ce} \subseteq J \implies J^{cec} \subseteq J^c$

$\square$

Theorem 1.11 (Homomorphism Theorem)**.**

Let $\varphi \in \operatorname{Hom}(R, R')$

(a)

$$\bar{\varphi} : R/_{\ker(\varphi)} \xrightarrow{\cong} \mathrm{Im}(\varphi), \bar{r} \mapsto \varphi(r)$$

is a ringisomorphism.

(b) $I \trianglelefteq R \iff I$ *is the kernel of some ringhom.*

(c) If $I \trianglelefteq R$*, then:*

$$\begin{aligned} \{J \trianglelefteq R \,|\, I \subseteq J\} &\to \{\bar{J} \trianglelefteq R/I\} \\ J &\mapsto J/I \end{aligned}$$

is bijective.

Proof. (Easy exercise) □

Theorem 1.12 (Chinese remainder theorem)**.**

Let R *be a ring,* $I_1, ..., I_k \trianglelefteq R$*,*

$$\varphi : R \longrightarrow \prod_{i=1}^{k} R/_{I_i} : r \mapsto (\bar{r}, ..., \bar{r})$$

(a) If $I_1, ..., I_k$ *are pairwise coprime, then*

$$\bigcap_{i=1}^{k} I_i = I_1 \cdot ... \cdot I_k$$

(b) φ *is surjective* $\iff I_1, ..., I_k$ *are pairwise coprime.*

(c) φ *is injective* $\iff \bigcap_{i=1}^{k} I_i = \{0\}$

Note. In particular we have that for $I_1, ..., I_k$ pairwise coprime:

$$R/_{I_1 \cdot .. \cdot I_k} \cong \prod_{i=1}^{k} R/_{I_i}$$

Proof.

(a) We do an induction on k:

- $k = 2$: Show $I_1 \cap I_2 = I_1 \cdot I_2$

  "$\supseteq$": ✓

  "$\subseteq$": $R = I_1 + I_2 \implies 1 = a + b, a \in I_1, b \in I_2$. Let $c \in I_1 \cap I_2$ be arbitrary $\implies c = c \cdot 1 = \underbrace{ca}_{\in I_1 \cdot I_2} + \underbrace{cb}_{\in I_1 \cdot I_2} \in I_1 \cdot I_2$

- $k-1 \to k$: By assumption we have $a_2, ..., a_k \in I_1, b_i \in I_i$, such that $1 = a_i + b_i \;\forall i$.

$$\begin{aligned} \implies b_2 \cdot ... \cdot b_k &= (1-a_2) \cdot ... \cdot (1-a_k) \\ &= 1 + a \text{ for some } a \in I_1 \\ \implies 1 &= \underbrace{-a}_{\in I_1} + \underbrace{b_2 \cdot ... \cdot b_k}_{\in I_2 \cdot ... \cdot I_k} \in I_1 + (I_2 \cdot ... \cdot I_k) \end{aligned}$$

Thus we have that I_1 and $I_2 \cdot ... \cdot I_k$ are pairwise coprime.

$$\begin{aligned} \stackrel{k=2}{\implies} I_1 \cdot (I_2 \cdot ... \cdot I_k) &= I_1 \cap (I_2 \cdot ... \cdot I_k) \\ &\stackrel{Ind.}{=} I_1 \cap (I_2 \cap ... \cap I_k) \\ &= \bigcap I_i \end{aligned}$$

(b) We prove two directions:

"$\Longleftarrow$": Choose a_i, b_i as in the proof for (a).

$$\begin{aligned} &\implies b_2 \cdot ... \cdot b_k \equiv \begin{cases} 1 & \mod I_1 \\ 0 & \mod I_i, i \neq 1 \end{cases} \\ &\implies \varphi(b_2 \cdot ... \cdot b_k) = (\bar{1}, \bar{0}, ..., \bar{0}) \in \operatorname{Im}(\varphi) \\ &\implies \varphi(r b_2 \cdot ... \cdot b_k) = (\bar{r}, \bar{0}, ..., \bar{0}) \in \operatorname{Im}(\varphi) \end{aligned}$$

Analogously we have that $(\bar{0}, .., \underbrace{\bar{r}}_{\text{at } i}, .., \bar{0}) =: \bar{r} e_i \in \operatorname{Im}(\varphi) \,\forall r \in R, i = 1..k$

$$\implies (\bar{r_1}, ..., \bar{r_k}) = \sum_{i=1}^{k} \bar{r}_i e_i \in \operatorname{Im}(\varphi)$$

"$\implies$": Let $i \neq j \in \{1..k\}$ be arbitrary. Then we have the following surjective chain of homomorphisms:

$$\begin{array}{ccccc} R & \xrightarrow[\varphi]{} & \prod R/I_i & \xrightarrow[\pi]{} & R/I_i \oplus R/I_j \\ & & & & \\ r & \longmapsto & (\bar{r}, ..., \bar{r}); (\bar{r_1}, ..., \bar{r_k}) & \longmapsto & (\bar{r_i}, \bar{r_j}) \end{array}$$

$$\begin{aligned} \implies \exists a \in R, \text{ such that } (\pi \circ \varphi)(a) &= (\bar{1}, \bar{0}) = (\bar{a}, \bar{a}) \\ \implies a &\equiv 1 \mod I_i \\ &\equiv 0 \mod I_j \end{aligned}$$

$\implies a \in I_j$ and $\exists b \in I_i : a = 1 + b$. Thus we have $1 = a - b \in I_i + I_j \implies I_i, I_j$ are coprime.

(c)

$$\begin{aligned}\ker(\varphi) &= \{r \in R \,|\, \varphi(r) = (\bar{0}, ..., \bar{0})\} \\ &= \{r \in R \,|\, r \equiv 0 \mod I_i \ \forall i\} \\ &= \{r \in R \,|\, r \in I_i \ \forall i\} \\ &= \bigcap I_i\end{aligned}$$

$\square$

Example 1.13. $R = \mathbb{Z}, I_1 = \langle 2 \rangle, I_2 = \langle 3 \rangle, I_3 = \langle 11 \rangle$

$$\Longrightarrow \mathbb{Z}/\left\langle \underbrace{2 \cdot 3 \cdot 11}_{66} \right\rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z}$$

This means that, given $a_1, a_2, a_3 \in \mathbb{Z}$ there exists a unique $z \in \{0, .., 65\}$, such that

$$\begin{aligned}z &\equiv a_1 \ (2) \\ &\equiv a_2 \ (3) \\ &\equiv a_3 \ (11)\end{aligned}$$

B). Prime Ideals and Local Rings

Definition 1.14.

(a) $\mathfrak{m} \trianglelefteq R, \mathfrak{m} \subsetneq R$ is a *maximal ideal* $:\Longleftrightarrow \forall I \trianglelefteq R : (\mathfrak{m} \subsetneq I \implies I = R) \Longleftrightarrow R/\mathfrak{m}$ is a field (by 1.11 (c) and 1.4 (c))
Note. We write: $\mathfrak{m} \lhd \cdot R$ and $\mathfrak{m} - \mathrm{Spec}(R) := \{\mathfrak{m} \,|\, \mathfrak{m} \lhd \cdot R\}$

(b) $P \trianglelefteq R, P \subsetneq R$ is a *prime ideal* $:\Longleftrightarrow \forall I, J \trianglelefteq R : (I \cdot J \subseteq P \implies I \subseteq P$ or $J \subseteq P)$

$$\begin{aligned}&\overset{(*)}{\Longleftrightarrow} \forall a, b \in R : (ab \in P \implies a \in P \text{ or } b \in P) \\ &\Longleftrightarrow R/P \text{ is an I.D.} \\ &\Longleftrightarrow \forall I_1, ..., I_k \trianglelefteq R : (I_1 \cdot ... \cdot I_k \subseteq P \implies \exists i : I_i \subseteq P) \\ &\Longleftrightarrow \forall a_1, ..., a_k \in R : (\prod a_i \in P \implies \exists i : a_i \in P)\end{aligned}$$

Proof. (of (*))

- "$\Longrightarrow$": Let $a, b \in P$

$$\begin{aligned} &\Longrightarrow \langle ab \rangle = \langle a \rangle \langle b \rangle \subseteq P \\ &\Longrightarrow \langle a \rangle \subseteq P \text{ or } \langle b \rangle \subseteq P \\ &\Longrightarrow a \in P \text{ or } b \in P \end{aligned}$$

- "$\Longleftarrow$": Suppose $I, J \trianglelefteq R$, such that $I \cdot J \subseteq P$, but $I \nsubseteq P, J \nsubseteq P \implies \exists a \in I \backslash P, b \in J \backslash P$, but $ab \in P$ ↯

□

Note. $\operatorname{Spec}(R) = \{P \mid P \text{ is prime ideal of } R\}$ is called the *spectrum* of R.

(c)

$$J(R) := \bigcap_{\mathfrak{m} \lhd\cdot R} \mathfrak{m} \trianglelefteq R$$

is the *Jacobson radical* of R.

(d)

$$\mathfrak{R}(R) := \bigcap_{P \trianglelefteq R \text{ prime ideal}} P \overset{1.15}{=} \sqrt{\{0\}} = \{a \in R \mid \exists n : a^n = 0\}$$

is the *nilradical* of R.

Note.

$\mathfrak{R}\left(R/\mathfrak{R}(R) \right) = \{\bar{0}\}$

Proof. "$\supseteq$" is trivial, we only show the other inclusion:

$$\begin{aligned} &(a + \mathfrak{R}(R))^n = \bar{0} = a^n + \mathfrak{R}(R) \\ \Longrightarrow\ &a^n \in \mathfrak{R}(R) \\ \Longrightarrow\ &\exists m : (a^n)^m = 0 \\ \Longrightarrow\ &a \in \mathfrak{R}(R) \\ \Longrightarrow\ &\bar{a} = \bar{0} \end{aligned}$$

□

Proposition 1.15.

$$I \trianglelefteq R \implies \sqrt{I} = \bigcap_{P \trianglelefteq R \text{ prime}, I \subseteq P} P$$

Proof.

"$\subseteq$": $a \in \sqrt{I}$ and $P \trianglelefteq R$ prime, s.t. $I \subseteq P$. Show $a \in P$:

$$a \in \sqrt{I} \implies \exists n : a^n \in I \subseteq P$$

$\overset{P \text{ prime}}{\implies} a \in P$

"$\supseteq$": Let $r \in R \backslash \sqrt{I}$. Show: $\exists P \trianglelefteq R$ prime, s.t. $I \subseteq P$ and $r \notin P$: Therefore set

$$M := \{J \trianglelefteq R \,|\, I \subseteq J \text{ and } r^n \notin J \forall n \geq 1\}$$

Then $M \neq \emptyset$, since $I \in M$ and M is partially ordered with respect to inclusion of sets.

Note. We now have to use *Zorn's Lemma*:

"Let $(M, \leq)$ be a partially ordered set s.t. any totally ordered subset of M has an upper bound *in* M. Then M has a maximal element with respect to $\leq$."

If we now have a totally ordered subset $\mathcal{J} \subseteq M$, then:

$$\bigcup_{J \in \mathcal{J}} J \trianglelefteq R \text{ and } I \subseteq \bigcup_{J \in \mathcal{J}} J \text{ and } r^n \notin \bigcup_{J \in \mathcal{J}} J \;\; \forall n \geq 1$$

Thus $\bigcup_{J \in \mathcal{J}} J \in M$ and it is an upper bound for the chain. Thus, by Zorn's lemma, we have a $P \in M$, which is maximal in M with respect to "$\subseteq$". We claim: P is a prime ideal:

Suppose $a \cdot b \in P$, s.t. $a \notin P, b \notin P$

$$\begin{aligned}
&\implies \langle a, P \rangle, \langle b, P \rangle \supsetneq P \\
&\implies \langle a, P \rangle, \langle b, P \rangle \notin M, \text{ since } P \text{ is maximal in } M \\
&\implies \exists n, m : r^n \in \langle a, P \rangle, r^m \in \langle b, P \rangle \\
&\implies r^n r^m \in \langle a, P \rangle \langle b, P \rangle \subseteq \langle ab, P \rangle \subseteq P \lightning_{P \in M}
\end{aligned}$$

Hence P is prime and $I \subseteq P$ and $r \notin P$.

$\square$

Example 1.16.

(a) $\mathfrak{m} - \operatorname{Spec}(R) \subseteq \operatorname{Spec}(R)$

(b)
- $\mathfrak{m} - \operatorname{Spec}(\mathbb{Z}) = \{\langle p \rangle \,|\, p \text{ prime}\}$
- $\operatorname{Spec}(\mathbb{Z}) = \mathfrak{m} - \operatorname{Spec}(\mathbb{Z}) \cup \{\langle 0 \rangle\}$
- $J(\mathbb{Z}) = \{0\}$
- $\mathfrak{N}(\mathbb{Z}) = \{0\}$

(c)
- $\mathfrak{m} - \operatorname{Spec}(K[\![x]\!]) = \{\langle x \rangle\}$
- $\operatorname{Spec}(K[\![x]\!]) = \{\langle x \rangle, \langle 0 \rangle\}$

- $J(K\llbracket x\rrbracket) = \langle x\rangle$
- $\mathfrak{N}(K\llbracket x\rrbracket) = \langle 0\rangle$

(d)
- $\mathfrak{m}-\mathrm{Spec}(K[x]) = \{\langle f\rangle \mid f \text{ irred.}\}$
- $\mathrm{Spec}(K[x]) = \mathfrak{m}-\mathrm{Spec}(K[x]) \cup \{\langle 0\rangle\}$
- $J(K[x]) = \mathfrak{N}(K[x]) = \langle 0\rangle$

(e) Let K be algebraically closed. We will see in 7.19:
- $\mathfrak{m}-\mathrm{Spec}(K[x,y]) = \{\langle x-a, y-b\rangle \mid a,b \in K\}$ (by Hilbert's *Nullstellensatz*)
- $\mathrm{Spec}(K[x,y]) = \mathfrak{m}-\mathrm{Spec}(K[x,y]) \cup \{\langle f\rangle \mid f \text{ irred.}\} \cup \{\langle 0\rangle\}$
- $J(K[x,y]) = \mathfrak{N}(K[x,y]) = \langle 0\rangle$

(f) Let K be an algebraically closed field. One can show that:
- $\mathfrak{m}-\mathrm{Spec}(K[x,y]/\langle xy\rangle) = \{\langle \overline{x-a}, \overline{y-b}\rangle \mid a = 0 \text{ or } b = 0\}$
- $\mathrm{Spec}(K[x,y]/\langle xy\rangle) = \mathfrak{m}-\mathrm{Spec}(..) \cup \{\langle \bar{x}\rangle, \langle \bar{y}\rangle\}$
- $J(K[x,y]/\langle xy\rangle) = \mathfrak{N}(K[x,y]/\langle xy\rangle = \langle \bar{0}\rangle$

(g)
- $\mathrm{Spec}(K[x]/x^2) = \mathfrak{m}-\mathrm{Spec}(K[x]/x^2) = \{\langle \bar{x}\rangle\}$
- $J(K[x]/x^2) = \mathfrak{N}(K[x]/x^2) = \langle \bar{x}\rangle$

(h) $\mathrm{Spec}(\mathbb{Z}[x]) = \{\langle f,p\rangle \mid \bar{f} \text{ is irred in } \mathbb{Z}/p\mathbb{Z}[x], p \in \mathbb{P}\} \cup \{\langle f\rangle \mid f \text{ irred.}\} \cup \{\langle 0\rangle\}$

Proposition 1.17 (Prime Avoidance)**.** *Let $I \trianglelefteq R; P_1, ..., P_{k-2} \in \mathrm{Spec}(R); P_{k-1}, P_k \trianglelefteq R$. Then we have:*

$$I \subseteq \bigcup_{i=1}^{k} P_i \implies \exists i : I \subseteq P_i$$

Proof. We do an induction on k.

- $k = 1$: ✓
- $k = 2$: First, we'll need the following argument: W.l.o.g. we have that $I \nsubseteq \bigcup_{i\neq j} P_j$ for all i, since otherwise the respective P_i can be removed, so that we can apply induction and are done. So assume

$$\exists\, a_i \in I \backslash \bigcup_{i\neq j} P_j \subseteq P_i$$

Let $a_1 + a_2 \in I \subseteq P_1 \cup P_2$.

$$\begin{aligned} &\Longrightarrow a_1 + a_2 \in P_1 \text{ or } a_1 + a_2 \in P_2 \\ &\Longrightarrow a_2 = (a_1 + a_2) - a_1 \in P_1 \text{ or } a_1 \in P_2 \end{aligned}$$

This is a contradiction to the choice of the a_i.↯

- $k \geq 3$ Choose the a_i as above and let $a := a_1 + a_2 \cdot \ldots \cdot a_k \in I \subseteq \bigcup_{i=1}^k P_i \implies \exists i: \; a \in P_i$. We consider two cases:
  - $(i = 1)$

$$\begin{aligned} &\Longrightarrow a_1 + a_2 \cdot \ldots \cdot a_k \in P_1 \\ &\Longrightarrow a_2 \cdot \ldots \cdot a_k \in P_1 \text{ since } a_1 \in P_1 \\ &\Longrightarrow \exists j \neq 1 : a_j \in P_1 \text{↯} \end{aligned}$$

  - $(i > 1)$. Since $a_2 \cdot \ldots \cdot a_k \in P_i \implies a_1 = a - a_2 \cdot \ldots \cdot a_k \in P_i$↯. So there exists an i, such that $I \subseteq \bigcup_{i \neq j} P_j$ and we can apply induction.

□

Lemma 1.18. *Let $I \trianglelefteq R, I \subsetneq R$*

$$\implies \exists \mathfrak{m} \lhd \cdot R: \; I \subseteq \mathfrak{m}$$

Proof. Let $M = \{J \trianglelefteq R \,|\, J \subsetneq R, I \subseteq J\} \neq \emptyset$, since $I \in M$. M is partially ordered with respect to inclusion.

Now let

$$\mathcal{J} \subseteq M$$

be any totally ordered subset of M and

$$J := \bigcup_{J' \in \mathcal{J}} J' \trianglelefteq R$$

It is clear that $I \subseteq J$. We need to show, that $J \neq R$ (then $J \in M$ and J is an upper bound for the chain):

Suppose $J = R \ni 1 \implies \exists J' \in \mathcal{J} : J' \ni 1 \implies J' = R$ ↯

$\implies J \neq R \overset{\text{Zorn}}{\implies} \exists \tilde{J} \in M$ maximal with respect to inclusion. Our claim is now, that $\tilde{J} \lhd \cdot R$ and $I \subseteq \tilde{J}$:

- $I \subseteq \tilde{J} : \checkmark$, since $\tilde{J} \in M$
- Suppose $\exists J' \trianglelefteq R, J' \subsetneq R$ and $\tilde{J} \subsetneq J'$. Then we have $J' \in M$, which is a contradiction, since $\tilde{J}$ is maximal in M. Thus $\tilde{J}$ is a maximal ideal.

□

Lemma 1.19.
$$a \in J(R) \iff \forall b \in R : 1 - ab \in R^*$$

Proof.

- "$\Longrightarrow$": Suppose $1 - ab \notin R^*$ for some $b \in R$, but $a \in J(R)$

$$\begin{aligned} &\Longrightarrow \langle 1 - ab \rangle \neq R \\ &\overset{1.18}{\Longrightarrow} \exists \mathfrak{m} \lhd \cdot R : \langle 1 - ab \rangle \subseteq \mathfrak{m} \\ &\Longrightarrow 1 = \underbrace{(1 - ab)}_{\in \mathfrak{m}} + \underbrace{ab}_{\in J(R) \subseteq \mathfrak{m}} \in \mathfrak{m} \lightning, \text{ since } \mathfrak{m} \neq R \end{aligned}$$

- "$\Longleftarrow$": Suppose $\exists \mathfrak{m} \lhd \cdot R$, such that $a \notin \mathfrak{m}$.

$$\begin{aligned} &\Longrightarrow \mathfrak{m} \subsetneq \langle \mathfrak{m}, a \rangle \\ &\overset{\mathfrak{m} \lhd \cdot R}{\Longrightarrow} \langle \mathfrak{m}, a \rangle = R \\ &\Longrightarrow 1 = m + ab \text{ with } m \in \mathfrak{m}, b \in R \\ &\Longrightarrow \underbrace{1 - ab}_{\in R^*} = m \in \mathfrak{m} \\ &\Longrightarrow \mathfrak{m} = R \lightning \end{aligned}$$

□

Definition 1.20. A ring R is called *local* $:\iff$ R has a *unique* maximal ideal ($\iff$ $J(R) \lhd \cdot R$)

Example 1.21.

(a) Fields are local rings, $J(K) = \langle 0 \rangle$

(b) $K[\![x]\!]$ is a local ring, since $J(K[\![x]\!]) = \langle x \rangle$

(c) $\mathbb{R}\{x\} and \mathbb{C}\{x\}$ are local rings with Jacobson radical $\langle x \rangle$

(d) $K[x]$ and $\mathbb{Z}$ are not local, since for example $\langle 2 \rangle, \langle 3 \rangle \lhd \cdot \mathbb{Z}$ and $\langle x \rangle, \langle x + 1 \rangle \lhd \cdot K[x]$.

Lemma 1.22. *The following statements are equivalent (for $R \neq 0$):*

(a) R is local

(b) $\exists \mathfrak{m} \lhd \cdot R : \forall a \in \mathfrak{m}, b \in R : 1 - ab \in R^*$

(c) $\exists \mathfrak{m} \lhd \cdot R : \forall a \in \mathfrak{m} : 1 + a \in R^*$

(d) $R \backslash R^* \trianglelefteq R$ (in that case we have $J(R) = R \backslash R^*$)

Proof.

- "$(a) \implies (b)$": See 1.19, since $J(R) = \mathfrak{m}$
- "$(b) \implies (c)$": clear with $b = -1$
- "$(c) \implies (d)$": We have to show that $\mathfrak{m} = R \backslash R^*$:

  "$\subseteq$": $\checkmark$, since otherwise $\mathfrak{m} = R$

  "$\supseteq$": Let $b \notin \mathfrak{m}$

$$\begin{aligned}
&\Longrightarrow \mathfrak{m} \subsetneq \langle \mathfrak{m}, b \rangle \\
&\Longrightarrow \langle \mathfrak{m}, b \rangle = R (\text{ since } \mathfrak{m} \lhd \cdot R) \\
&\Longrightarrow 1 = m + ab \\
&\Longrightarrow ba = 1 - m = \underbrace{1 + (-m)}_{\in R^*} \\
&\Longrightarrow ba \in R^* \implies b \in R^*
\end{aligned}$$

- "$(d) \implies (a)$": Let $\mathfrak{m} \lhd \cdot R$

$$\begin{aligned}
&\Longrightarrow \mathfrak{m} \subseteq R \backslash R^* \trianglelefteq R \\
&\Longrightarrow \mathfrak{m} = R \backslash R^* \text{ since } \mathfrak{m} \text{ is maximal and } R \backslash R^* \subsetneq R
\end{aligned}$$

$\square$

2. Modules and linear maps

A). Basics

Definition 2.1. Let R be a ring.

(a) An *R-module* or *module* is a tuple $(M, +, \cdot)$, where $M \neq \emptyset$ is a set, $+ : M \times M \longrightarrow M, \cdot : R \times M \longrightarrow M$ binary operations such that $\forall m, m' \in M, r, s \in R :$

(1) $(M, +)$ is an abelian group

(2) (Generalized distributivity:)

$$\begin{aligned} r \cdot (m + m') &= r \cdot m + r \cdot m' \\ (r + s) \cdot m &= r \cdot m + s \cdot m \end{aligned}$$

(Generalized associativity:)

$$r \cdot (s \cdot m) = (r \cdot s) \cdot m$$

(3) $1 \cdot m = m$

(b) Let M be an R-module and $N \subseteq M$. Then N is a *submodule* of M

$$\begin{aligned} :\Longleftrightarrow & (N, +_{|N}, \cdot_{|N}) \text{ is an } R \text{ - module} \\ \Longleftrightarrow & (N, +) \text{ is a group and } rn \in N \ \forall r \in R, n \in N \\ \Longleftrightarrow & \forall n, n' \in N, r, r' \in R : rn + r'n' \in N \end{aligned}$$

In that case we write $N \leq M$.

(c) Let M be an R-module, $N \leq M$. Define on the quotient group $({}^{M}\!/\!{}_{N}, +)$ a scalar multiplication by

$$r\overline{m} = \overline{rm}$$

Then this is well-defined and $({}^{M}\!/\!{}_{N}, +, \cdot)$ is an R-module, the *quotient module* of M by N.

(d) Let M be an R-module, $J \subseteq M$.

$$\langle J \rangle := \bigcap_{J \subseteq N \leq M} N = \{\sum_{i=1}^{n} r_i m_i \,|\, n \in \mathbb{N}, r_i \in R, m_i \in J\} \leq M$$

the *submodule generated by J*.

(e) An R-module M is *fintely generated*

$$\iff \exists m_1, ..., m_n \in M : M = \langle m_1, ..., m_n \rangle$$

(f) Let M, N be an R-module. Then a map $\varphi : M \to N$ is called *R-linear* or an *R-module homomorphism*

$$:\iff \forall r, r' \in R, m, m' \in M : \varphi(rm + r'm') = r\varphi(m) + r'\varphi(m')$$

Notation: $\mathrm{Hom}_R(M, N) = \{\varphi : M \to N \mid \varphi \text{ is linear}\}$

(g) Let $\varphi \in \mathrm{Hom}_R(M, N)$. Then we call φ a *monomorphism*,*epimorphism*,*isomorphism* $:\iff$ φ is injective, surjective, bijective.

- $\ker(\varphi) := \varphi^{-1}(0) \leq M$ is the *kernel* of φ
- $\mathrm{Im}(\varphi) := \varphi(M) \leq N$ is the *image* of φ
- $\mathrm{Coker}(\varphi) := {}^{N}\!\big/_{\mathrm{Im}(\varphi)}$ is the *cokernel* of φ

Note. $\mathrm{Coker}(\varphi) = 0 \iff \varphi$ is surjective

(h) Let M, N, P be R-modules, $\varphi \in \mathrm{Hom}_R(M, N)$. Then:

$$\varphi^* : \mathrm{Hom}_R(N, P) \to \mathrm{Hom}_R(M, P) : \psi \mapsto \psi \circ \varphi$$
$$\varphi_* : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N) : \psi \mapsto \varphi \circ \psi$$

(i) An R-module M is *simple* if it contains only the trivial submodules $\{0\}$ and M.

Example 2.2.

(a) K-vector spaces correspond to K-modules (where K is a field)

(b) Ideals are *the* submodules of the R-module R

(c) $\varphi \in \mathrm{Hom}(R, R')$, M an R'-module, then

$$\underbrace{r}_{\in R}\underbrace{m}_{\in M} := \varphi(r)m$$

makes M an R-module.

(d) $(M, +, \cdot)$ is a $\mathbb{Z}$-module $\iff$ $(M, +)$ is an abelian group

Proof. (only for "$\Longleftarrow$")
$z \in \mathbb{Z}, m \in M \implies z \cdot m := m^z$ in $(M, +)$ □

(e) $\mathrm{Hom}_R(M, N)$ is an R-module via

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m)$$
$$(r\varphi)(m) = r\varphi(m)$$

(f) φ^*, φ_* are R-linear

(g) $M \cong \operatorname{Hom}_R(R, M)$ by $m \mapsto (R \to M, r \mapsto rm)$

Proof. Exercise $\square$

(h) Let M an R-module, $\varphi \in \operatorname{Hom}_R(M, M)$. Then M becomes an $R[x]$-module via

$$x \cdot m := \varphi(m)$$

(Then $(\sum a_i x^i)m = \sum a_i \varphi^i(m)$)

(i) In general we have $M \not\cong \operatorname{Hom}_R(M, R)$, e.g. $R = \mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z}$.

Definition 2.3 (Operations on modules)**.**

(a) Let M_λ be an R-module, $\lambda \in \Lambda$

$$\prod_{\lambda\in\Lambda} M_\lambda := \{(m_\lambda)_{\lambda\in\Lambda} \,|\, m_\lambda \in M_\lambda \;\forall \lambda \in \Lambda\}$$

is an R-module by componentwise operations and is called the *direct product* of the M_λ's.

$$\bigoplus_{\lambda\in\Lambda} M_\lambda := \{(m_\lambda)_{\lambda\in\Lambda} \,|\, \text{ only finitely many } m_\lambda \text{ are non-zero}\} \leq \prod_{\lambda\in\Lambda} M_\lambda$$

the *direct sum* of the M_λ

(b) Let $I \trianglelefteq R, M$ an R-module, $N, N', M_\lambda \leq M, \lambda \in \Lambda$

- $\bigcap\limits_{\lambda\in\Lambda} M_\lambda \leq M$
- $\sum\limits_{\lambda\in\Lambda} M_\lambda := \left\langle \bigcup\limits_{\lambda\in\Lambda} M_\lambda \right\rangle = \{\sum\limits_{\lambda\in\Lambda} m_\lambda \,|\, m_\lambda \in M_\lambda \text{ finitely many non-zero}\}$
- $\operatorname{Tor}(M) := \{m \in M \,|\, \exists r \in R : rm = 0 \text{ and } r \text{ is not a zero-divisor}\} \leq M$ is the *torsion module* of M

  Proof. $m, m' \in \operatorname{Tor}(M); r, r' \in R$ not zero-div. and $rm = r'm' = 0$

  $$\underbrace{rr'}_{\text{not zero-div.}} (m + m') = 0$$

  $\implies m + m' \in \operatorname{Tor}(M)$ $\square$

- $I \cdot M := \langle am \,|\, a \in I, m \in M\rangle \leq M$
- $N : N' := \{r \in R \,|\, rN' \subseteq N\} \trianglelefteq R$ is the *module quotient* of N by N'

- $\operatorname{ann}_R(M) := \operatorname{ann}(M) := \{r \in R \,|\, rm = 0 \ \forall m \in M\} \trianglelefteq R$ is the *annihilator* of M.
- Let M be an R-module, $m_\lambda \in M, \lambda \in \Lambda. M$ is called *free* with generators $(m_\lambda, \lambda \in \Lambda)$

$$:\iff \quad \begin{tikzcd} \bigoplus_{\lambda\in\Lambda} R \arrow[r, "\cong"] & M \\ e_\lambda \arrow[r, mapsto] & m_\lambda \end{tikzcd}$$

is an isomorphism.

$\iff \forall R-$ modules N and $n_\lambda \in N, \lambda \in \Lambda$:

$$\exists_1 R - \text{linear map } M \to N, m_\lambda \mapsto n_\lambda$$

Notation: $\operatorname{rank}(M) := |\Lambda|$
Note. $\operatorname{rank}(M)$ is well-defined and $\operatorname{rank}(M) = n < \infty \iff M \cong R^n$ (by def.)

Proof. (well-definedness:)
Let M be free with respect to $(m_\lambda)_{\lambda\in\Lambda}$ and with respect to $(m_\lambda)_{\lambda\in\Lambda'}$

We have to show: $|\Lambda| = |\Lambda'|$

(1) "$|\Lambda| = \infty$":

$$m_\mu = \sum_{\lambda\in T_\mu} a_\lambda m_\lambda;\ T_\mu \subseteq \Lambda \text{ finite, } \forall\, \mu \in \Lambda'$$

$$\implies \Lambda = \bigcup_{\mu\in\Lambda'} T_\mu, \text{ since } (m_\lambda) \text{ is a minimal set of generators}$$

$$\implies |\Lambda| \leq \sum_{\mu\in\Lambda'} |T_\mu| \leq |\Lambda'|\,|\mathbb{N}| = |\Lambda'| \ \ (\text{since } |\Lambda'| < \infty \implies |\Lambda| < \infty ⚡)$$

$$\implies |\Lambda| \leq |\Lambda'|$$

Analogously $|\Lambda'| \leq |\Lambda| \implies |\Lambda| = |\Lambda'|$

(2) "$|\Lambda| < \infty$" postponed to 2.14.

$\square$

Example 2.4.

(a) M an R-module $\implies M$ is an $R/_{\operatorname{ann}(M)}$-module via

$$\bar{r}m := rm$$

(b) $R = K[x,y], M = {}^{R}\!/\!_{\langle x\rangle} \oplus {}^{R}\!/\!_{\langle y\rangle}$

$$\implies \operatorname{ann}_R(M) = \langle xy\rangle$$

(c) $N : N' = \operatorname{ann}_R({}^{N+N'}\!/\!_{N})$

(d) $\mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module.

(e) A minimal set of generators in a module is in general not a basis, e.g. $\mathbb{Z} = \langle 2,3\rangle$, this is a minimal generating set but no basis.

Theorem 2.5 (Isomorphism theorem)**.** *Let N, N', M, L modules.*

(a) $\varphi \in \operatorname{Hom}_R(M,N)$

$$\implies {}^{M}\!/\!_{\ker(\varphi)} \cong \operatorname{Im}(\varphi)$$

by: $\overline{m} \mapsto \varphi(m)$

In particular: $\ker(\varphi) = \{0\} \iff \varphi$ *is injective*

(b) $N \le M \le L$

$$\implies {}^{({}^{L}\!/\!_{N})}\!/\!_{({}^{M}\!/\!_{N})} \cong {}^{L}\!/\!_{M}$$

(c) $N, N' \le M$

$$\implies {}^{N}\!/\!_{N\cap N'} \cong {}^{N+N'}\!/\!_{N'}$$

(d) $N \le M$

$$\implies \{N' \le M \mid N \subseteq N'\} \longrightarrow \{\overline{N}' \mid \overline{N}' \le {}^{M}\!/\!_{N}\}, N' \mapsto {}^{N'}\!/\!_{N}$$

is bijective.

Proof. As for vector spaces □

B). Finitely generated modules

Theorem 2.6 (Cayley-Hamilton)**.** *Let M be a finitely gen. R-module, $I \trianglelefteq R, \varphi \in \operatorname{Hom}_R(M,M)$.*

If $\varphi(M) \subseteq I \cdot M$, then there exists

$$\chi_\varphi := x^n + p_1 x^{n-1} + \ldots + p_n \in R[x]$$

such that $p_i \in I^i$ and $\chi_\varphi(\varphi) = 0 \in \operatorname{Hom}_R(M,M)$

Proof. Consider M as an $R[x]$-module via

$$xm := \varphi(m) \tag{*}$$

Let $M = \langle m_1, ..., m_n \rangle$

$$\implies \varphi(m_i) = \sum_{j=1}^{n} a_{ij} m_j,\ a_{ij} \in I, \text{since } \varphi(M) \subseteq I \cdot M$$

$$\overset{A:=(a_{ij})}{\implies} \underbrace{(x \cdot I_n - A)}_{\in Mat(n \times n, R[x])} \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} xm_1 - \sum_{i=1}^{n} a_{1i} m_i \\ \vdots \end{pmatrix} = \begin{pmatrix} \varphi(m_1) - \varphi(m_1) \\ \vdots \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

where I_n is the identity matrix. Thus by Cramer's rule we have that

$$\begin{aligned} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} &= \underbrace{(xI_n - A)^{\#}}_{\text{adjoined matrix}} (xI_n - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \\ &= \det(xI_n - A) \cdot I_n \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \\ &= \begin{pmatrix} \det(...)m_1 \\ \vdots \\ \det(...)m_n \end{pmatrix} \\ &\implies \det(xI_n - A)m = 0\ \forall m \in M \\ &\implies \underbrace{\det(xI_n - A)}_{=:\chi_\varphi} \in \operatorname{ann}_{R[x]}(M) \end{aligned}$$

Then by the Leibniz formula we have that

$$R[x] \ni \chi_\varphi = x^n + p_1 x^{n-1} + ... + p_n,\ p_i \in I^i$$

and thus $\chi_\varphi(\varphi)(m) \overset{(*)}{=} \chi_\varphi \cdot m = 0$

$\implies \chi_\varphi(\varphi) = 0 \in \operatorname{Hom}_R(M, M)$ $\square$

Remark 2.7. *Let M be finitely generated and $\varphi : M \to M$ R-linear. If φ is injective $\not\Rightarrow$ φ is bijective, e.g.*

$$\varphi : \mathbb{Z} \to \mathbb{Z}, z \mapsto 2z$$

is injective, but not surjective.

Corollary 2.8. *Let M be a fin. gen. R-module, $\varphi \in \mathrm{Hom}_R(M, M)$. Then:*

$$\varphi \text{ is surjective} \iff \varphi \text{ is bijective}$$

Proof. We only need to show "$\Longrightarrow$":

Consider M as an $R[t]$-module via $tm := \varphi(m)$ and let $I = \langle t \rangle \trianglelefteq R[t]$ and $\mathrm{id}_M \in \mathrm{Hom}_{R[t]}(M, M)$

Since φ is surjective $\Longrightarrow I \cdot M = t \cdot M = \varphi(M) = M = \mathrm{id}_M(M)$. Then by 2.6 there exists

$$\chi_{\mathrm{id}_M} = x^n + \sum_{i=0}^{n-1} p_{n-i} x^i \in R[t][x]$$

with $p_j \in \left\langle t^j \right\rangle$ and

$$0 = \chi_{\mathrm{id}_M}(\mathrm{id}_M) = \mathrm{id}_M + \sum_{i=0}^{n-1} p_{n-i} \,\mathrm{id}_M$$

Now set $q := \frac{p_1 + \ldots p_n}{t} \in R[t]$ (by def. of the p_j). Then we have:

$$\begin{aligned}
\mathrm{id}_M(m) &= (-\sum_{i=0}^{n-1} p_{n-i} \,\mathrm{id}_M)(m) \\
&= (-\sum_{i=0}^{n-1} p_{n-i})m \\
&= t \cdot (-q) \cdot m = (\varphi \circ (-q(\varphi)))(m) \\
&= (-q) \cdot t \cdot m = ((-q(\varphi)) \circ \varphi)(m)
\end{aligned}$$

Thus $id_M = \varphi \circ (-q(\varphi)) = (-q(\varphi)) \circ \varphi$ □

Corollary 2.9 (Lemma of Nakayama, NAK)**.** *Let M be a fin. gen. R-module and $I \trianglelefteq R$, such that $I \subseteq J(R)$. Then:*

$$I \cdot M = M \Longrightarrow M = 0$$

Proof. Apply 2.6 to $\varphi = \mathrm{id}_M$

$$\begin{aligned}
&\Longrightarrow \exists p_1, ..., p_n \in I : (1 + p_1 + ... + p_n) \,\mathrm{id}_M = 0 \\
&\Longrightarrow \forall m \in M : (1 + p_1 + ... + p_n)m = 0 \\
&\Longrightarrow \underbrace{1 + \underbrace{p_1 + ... + p_n}_{\in I \subseteq J(R)}}_{\in R^* \text{ by } 1.19} \in \mathrm{ann}_R(M) \\
&\Longrightarrow \mathrm{ann}_R(M) = R \\
&\Longrightarrow M = 0, \text{ since } 1 \cdot m = 0
\end{aligned}$$

□

Corollary 2.10 (NAK 1)**.** *If $(R, \mathfrak{m})$ is local, M a fin. gen. R-module, $\mathfrak{m}M = M$, then*

$$M = 0$$

Proof. $J(R) = \mathfrak{m}$ □

Corollary 2.11 (NAK 2)**.** *If $(R, \mathfrak{m})$ is local, M a fin. gen. R-module, $N \leq M$ and $N + \mathfrak{m}M = M$, then*

$$N = M$$

Proof.

$$\begin{aligned} &\mathfrak{m}(M/N) = (\mathfrak{m}M + N)/N = M/N \\ \Longrightarrow\ & M/N = 0 \text{ (by NAK 1)} \\ \Longrightarrow\ & M = N \end{aligned}$$

□

Corollary 2.12 (NAK 3)**.** *Let $(R, \mathfrak{m})$ be local, $0 \neq M$ a fin. gen. R-module. Then:*

$$\begin{aligned} &(m_1, ..., m_n) \textit{ is a minimal set of generators for } M \\ \Longleftrightarrow\ &(\overline{m_1}, ..., \overline{m_n}) \textit{ is a minimal set of generators for } M/\mathfrak{m}M \end{aligned}$$

Note. $\mathfrak{m} \lhd \cdot R \Longrightarrow R/\mathfrak{m}$ is a field $\Longrightarrow M/\mathfrak{m}M$ is a fin. gen. $R/\mathfrak{m}$-module $\Longrightarrow M/\mathfrak{m}M$ is a finite dimensional vector space over $R/\mathfrak{m}$.

Proof. We show two directions:

- "$\Longleftarrow$": Set $N := \langle m_1, ..., m_n \rangle \leq M$

$$\begin{aligned} \Longrightarrow\ & (N + \mathfrak{m}M)/\mathfrak{m}M = \langle \overline{m_1}, ..., \overline{m_n} \rangle = M/\mathfrak{m}M \\ \Longrightarrow\ & N + \mathfrak{m}M = M \overset{NAK2}{\Longrightarrow} N = M \\ \Longrightarrow\ & m_1, ..., m_n \text{ is a generating system of } M \end{aligned}$$

  Suppose that m_j is superfluos. Then

$$\langle \overline{m_1}, ..., \overline{m_{j-1}}, \overline{m_{j+1}}, ..., \overline{m_n} \rangle = M/\mathfrak{m}M \ \lightning$$

- "$\Longrightarrow$": Clear $\langle \overline{m_1}, \cdots, \overline{m_n} \rangle = M/\mathfrak{m}M$. Suppose $\overline{m_j}$ is superfluos. Then by "$\Longleftarrow$"

$$\langle m_1, \cdots, m_{j-1}, m_{j+1}, \cdots, m_n \rangle = M \ \lightning$$

□

Corollary 2.13 (NAK 4)**.** *Let $(R, \mathfrak{m})$ be a local ring; N, M fin. gen. R-modules, $\varphi \in \operatorname{Hom}_R(M, N)$. Then:*

$$\varphi \textit{ is surjective} \iff \overline{\varphi} : M/_{\mathfrak{m}M} \to N/_{\mathfrak{m}N} \textit{ is surjective}$$

Proof. We only need to show "$\Longleftarrow$":

Let $\overline{\varphi}$ be surjective

$$\implies 0 = \operatorname{Coker}(\overline{\varphi}) = {}^{(N/_{\mathfrak{m}N})}/_{\operatorname{Im}(\overline{\varphi})} = {}^{(N/_{\mathfrak{m}N})}/_{(\operatorname{Im}(\varphi) + \mathfrak{m}N/_{\mathfrak{m}N})} \cong N/_{(\operatorname{Im}(\varphi) + \mathfrak{m}N)}$$

$\implies N = \operatorname{Im}(\varphi) + \mathfrak{m}N$ and by NAK 2: $N = \operatorname{Im}(\varphi)$ and thus φ is surjective. $\square$

Remark 2.14.

$$R^m \overset{\psi}{\cong} R^n \implies m = n$$

In particular the rank of a free and finitely generated module is well-defined

Proof. Suppose $n > m$. Consider

$$\varphi : R^n \to R^m, e_i \mapsto \begin{cases} e_i, i \leq m \\ 0, \text{ else} \end{cases}$$

$\implies \varphi$ is a surjective, R-linear map.

Then $\psi \circ \varphi : R^n \to R^n$ is surjective and and by 2.8 bijective. But $(\psi \circ \varphi)(e_n) = \psi(0) = 0 \lightning$. $\square$

Proposition 2.15. *M is finitely generated $\iff \exists \varphi : R^n \twoheadrightarrow M$ R-linear*

Proof. We show two directions:

- "$\Longrightarrow$": $M = \langle m_1, ..., m_n \rangle \implies \varphi : R^n \to M, e_i \mapsto m_i$
- "$\Longleftarrow$": $\varphi : R^n \twoheadrightarrow M \implies M = \langle \varphi(m_1), ..., \varphi(m_n) \rangle$

$\square$

Remark 2.16 (Fundamental thm. of fin. gen. modules over P.I.D.'s)**.** *Let R be a P.I.D., M a fin. gen. R-module. Then:*

(a) $M \cong \mathit{Tor}(M) \oplus R^n$ *for a unique* $n \in \mathbb{N}_0$.

(b) $\mathit{Tor}(M) \cong \bigoplus_{i=1}^r R/_{\langle p_i^{\alpha_i} \rangle}$, *where p_i is prime, $\alpha_i \geq 1$ uniquely determined.*

Proof. too hard. $\square$

Example. $R = \mathbb{Z}$

$\implies M$ is an abelian group, fin. gen.

$\implies M = \mathbb{Z}^n \oplus \mathbb{Z}/\langle p_i^{\alpha_i}\rangle \oplus ... \oplus \mathbb{Z}/\langle p_r^{\alpha_r}\rangle, p_i$ prime.

C). Exact Sequences

Definition 2.17.

(a) A sequence $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ of R-linear maps is called *exact* at N

$$:\iff \operatorname{Im}(\varphi) = \ker(\psi)$$

(b) A sequence $M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \xrightarrow{\varphi_3} ... \xrightarrow{\varphi_{n-1}} M_n$ of R-linear maps is called *exact* $:\iff$ Is is exact at M_i $\forall i \in \{2, ..., n-1\}$

(c) An exact sequence of R-linear maps of the form $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ is called a *short exact sequence*.

(d) A short exact sequence $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$ is called *split exact* $:\iff \exists\, \psi \in \operatorname{Hom}_R(M'', M)$, such that $p \circ \psi = \mathrm{id}_{M''}$.

Example 2.18.

(a) $M \xrightarrow{\varphi} N \longrightarrow 0$ is exact at $N \iff \varphi$ is surjective

(b) $0 \longrightarrow M \xrightarrow{\varphi} N$ is exact at $M \iff \varphi$ is injective.

(c) $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ is exact $\iff \varphi$ is injective, ψ is surjective and $\operatorname{Im}(\varphi) = \ker(\psi)$

(d) $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ is exact.

(e) $\varphi \in \operatorname{Hom}_R(M, N) \implies:$

$0 \longrightarrow \ker(\varphi) \longrightarrow M \xrightarrow{\varphi} N \longrightarrow \operatorname{Coker}(\varphi) \longrightarrow 0$ is exact.

$0 \longrightarrow \ker(\varphi) \longrightarrow M \xrightarrow{\varphi} \operatorname{Im}(\varphi) \longrightarrow 0$ is short exact.

(f) $N \leq M \implies$

$$0 \longrightarrow N \hookrightarrow M \twoheadrightarrow M/N \longrightarrow 0 \text{ is exact.}$$

(g) Every "long" exact sequence splits into short ones and is composed by short ones. Thus, studying exact sequences is reduced to studying short exact sequences! How to do this (the 'triangular' sequence is the resulting short sequence, all these short sequences are 'stitched together' at the 0's):

$$\begin{tikzcd}
\dots \arrow[r] & M_{i-1} \arrow[r, "\varphi_{i-1}"] \arrow[d, two heads] & M_i \arrow[r, "\varphi_i"] \arrow[dr, two heads, "\varphi_i"] & M_{i+1} \arrow[r] & \dots \\
& \mathrm{Im}(\varphi_{i-1}) = \ker(\varphi_i) \arrow[ur] \arrow[dr] & & \mathrm{Im}(\varphi_i) = \ker(\varphi_{i+1}) \arrow[u] \arrow[dr] & \\
0 \arrow[ur] & & 0 \arrow[ur] & & 0
\end{tikzcd}$$

Conversely, if we have given:

$$0 \longrightarrow K_{n-1} \xrightarrow{i_{n-1}} M_{n-1} \xrightarrow{\pi_{n-1}} M_n$$

$$0 \longrightarrow K_{n-2} \xrightarrow{i_{n-2}} M_{n-2} \xrightarrow{\pi_{n-2}} K_{n-1} \longrightarrow 0$$

$$\vdots$$

$$0 \longrightarrow K_1 \xrightarrow{i_1} M_1 \xrightarrow{\pi_1} K_2 \longrightarrow 0$$

$$M_0 \xrightarrow{\pi_0} K_1 \longrightarrow 0$$

we construct an exact sequence

$$M_0 \xrightarrow{i_1 \circ \pi_0} M_1 \xrightarrow{i_2 \circ \pi_1} \dots \longrightarrow M_{n-1} \xrightarrow{\pi_{n-1}} M_n$$

Definition 2.19. Let $\mathfrak{M}$ be a class of R-modules, which is closed under submodules, quotient modules and isomorphisms. A function $\lambda : \mathfrak{M} \to \mathbb{N}$ is called *additive* on $\mathfrak{M}$ $:\Longleftrightarrow$ for all $M, M', M'' \in \mathfrak{M}$:

For all exact sequences $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ we have that

$$\lambda(M) = \lambda(M') + \lambda(M'')$$

or equivalently: $\forall\, M \in \mathfrak{M}$ and $N \leq M$ we have:

$$\lambda(M) = \lambda(N) + \lambda(M/N)$$

Example 2.20. $R = K$ a field, $\mathfrak{M} := \{V \mid V \text{ is a } K\text{−vector space with } \dim_K(V) < \infty\}$. Then:

$$\lambda = \dim_K$$

is additive.

Proposition 2.21. *If λ is additive on $\mathfrak{M}$ and*

$$0 \longrightarrow M_0 \xrightarrow{\varphi_0} M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \dots \xrightarrow{\varphi_{n-1}} M_n \xrightarrow{\varphi_n} 0$$

is exact with $M_i \in \mathfrak{M}$, then:

$$\sum_{i=0}^{n}(-1)^i\lambda(M_i) = 0$$

Proof. Since

$$0 \longrightarrow \ker(\varphi_i) \longrightarrow M_i \longrightarrow \operatorname{Im}(\varphi_i) \longrightarrow 0$$

is exact, we have that

$$\lambda(M_i) = \lambda(\operatorname{Im}(\varphi_i)) + \lambda(\ker(\varphi_i))$$

Thus

$$\begin{aligned}
\sum_{i=0}^{n}(-1)^i\lambda(M_i) &= \sum_{i=0}^{n}(-1)^i(\underbrace{\lambda(\ker(\varphi_i))}_{=\lambda(\operatorname{Im}(\varphi_{i-1}))} + \lambda(\operatorname{Im}(\varphi_i))) \\
&= \lambda(\underbrace{\ker(\varphi_0)}_{=0}) + (-1)^n\lambda(\underbrace{\operatorname{Im}(\varphi_n)}_{=0}) \\
&= \lambda(0) + (-1)^n\lambda(0) = 0
\end{aligned}$$

Note. Since $0 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0$ is exact, we know that $\lambda(0) = \lambda(0) + \lambda(0) = 2\lambda(0)$ and thus $\lambda(0) = 0$.

□

Proposition 2.22 (Snake lemma)**.** *Let the following commutative diagram of R-linear maps be given:*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "\alpha"] \arrow[d, "\varphi'"] & M \arrow[r, "\beta"] \arrow[d, "\varphi"] & M'' \arrow[r] \arrow[d, "\varphi''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "\alpha'"] & N \arrow[r, "\beta'"] & N'' \arrow[r] & 0
\end{tikzcd}$$

Then consider the following diagram:

$$
\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
(\diamond) & 0 \arrow[r] & \ker(\varphi') \arrow[r, "\alpha_|"] \arrow[d] & \ker(\varphi) \arrow[r, "\beta_|"] \arrow[d] & \ker(\varphi'') \arrow[r, dotted, "\delta"] \arrow[d] & \ldots \\
(*) & 0 \arrow[r] & M' \arrow[r, "\alpha"] \arrow[d, "\varphi'"] & M \arrow[r, "\beta"] \arrow[d, "\varphi"] & M'' \arrow[r] \arrow[d, "\varphi''"] & 0 \\
(*) & 0 \arrow[r] & N' \arrow[r, "\alpha'"] \arrow[d] & N \arrow[r, "\beta'"] \arrow[d] & N'' \arrow[r] \arrow[d] & 0 \\
(\diamond) & \ldots \arrow[r, dotted, "\delta"] & \operatorname{Coker}(\varphi') \arrow[r, "\overline{\alpha'}"] \arrow[d] & \operatorname{Coker}(\varphi) \arrow[r, "\overline{\beta'}"] \arrow[d] & \operatorname{Coker}(\varphi'') \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 & 0 &
\end{tikzcd}
$$

If the two (*) -rows are exact, then the $(\diamond)$ *- sequence is exact for a suitable "connecting homomorphism"* δ*.*

Proof. At first, we have to define δ (To make the following more clear, it might prove helpful to retrace the following, formal steps by hand in the diagram - a so-called 'diagram chase'):

Let $m'' \in \ker(\varphi'') \subseteq M''$

$$
\begin{aligned}
&\Longrightarrow \exists\, m \in M : \beta(m) = m'', \text{ since } \beta \text{ is surj.}\\
&\Longrightarrow \beta'(\varphi(m)) = \varphi''(\beta(m)) = \varphi''(m'') = 0\\
&\Longrightarrow \varphi(m) \in \ker(\beta') = \operatorname{Im}(\alpha')\\
&\Longrightarrow \exists_1\, n' \in N' : \alpha'(n') = \varphi(m)
\end{aligned}
$$

Now define: $\delta(m'') := \overline{n'} = n' + \operatorname{Im}(\varphi')$

We have to show that $\delta(m'')$ is independent of the choice of m:

Let $m, \tilde{m} \in M$, such that $\beta(m) = \beta(\tilde{m}) = m''$.

$$
\begin{aligned}
&\Longrightarrow \beta(m - \tilde{m}) = m'' - m'' = 0\\
&\Longrightarrow m - \tilde{m} \in \ker(\beta) = \operatorname{Im}(\alpha)\\
&\Longrightarrow \exists\, m' \in M' : \alpha(m') = m - \tilde{m}\\
&\Longrightarrow \varphi(m - \tilde{m}) = \varphi(\alpha(m')) = \alpha'(\varphi'(m')) \text{ and}\\
&\qquad \varphi(m - \tilde{m}) = \varphi(m) - \varphi(\tilde{m}) =: \alpha'(n') - \alpha'(\tilde{n}')
\end{aligned}
$$

if we set $n' := (\alpha')^{-1}(\varphi(m)), \tilde{n}' := (\alpha')^{-1}(\varphi(\tilde{m}))$. Thus we get:

$$\begin{aligned} &\Longrightarrow \alpha'(n' - \tilde{n}') = \alpha'(\varphi'(m')) \\ &\Longrightarrow n' - \tilde{n}' = \varphi'(m') \in \mathrm{Im}(\varphi'), \text{ since } \alpha' \text{ is inj.} \end{aligned}$$

$$\Longrightarrow \overline{n'} = \overline{\tilde{n}'} \in \mathrm{Coker}(\varphi')$$

Thus δ is well-defined.

Next we show that δ is R-linear:

Let $m'', \tilde{m}'' \in \ker(\varphi''); r, \tilde{r} \in R$ and let $m, \tilde{m} \in M$ and $n', \tilde{n}' \in N'$ as in the definition of δ.

$$\begin{aligned} &\Longrightarrow \beta(rm + \tilde{r}\tilde{m}) = rm'' + \tilde{r}\tilde{m}'', \text{ since } \beta \text{ is linear} \\ &\Longrightarrow \alpha'(rn' + \tilde{r}\tilde{n}') = \varphi(rm + \tilde{r}\tilde{m}), \text{ since } \alpha', \varphi \text{ are linear} \\ &\Longrightarrow \delta(rm'' + \tilde{r}\tilde{m}'') = r\overline{n'} + \tilde{r}\overline{\tilde{n}'} = r\delta(m'') + \tilde{r}\delta(\tilde{m}'') \end{aligned}$$

It remains to show, that the sequence is exact - we only prove this for the interesting part $ker(\delta) = \mathrm{Im}(\beta_|)$:

- "$\supseteq$": Let $m'' \in \mathrm{Im}(\beta_|)$

  $\Longrightarrow \exists\, m \in \ker\varphi : \beta(m) = m''$ and thus

  $\overline{(\alpha')^{-1}(\varphi(m))} = \delta(m'') = 0$
- "$\subseteq$": Let $m'' \in \ker(\delta)$ and let $m \in M, n' \in N'$ as in the definition of δ.

$$\begin{aligned} &\Longrightarrow \overline{n}' = 0 \\ &\Longrightarrow n' \in \mathrm{Im}(\varphi') \\ &\Longrightarrow \exists\, m' \in M' : \varphi'(m') = n' \\ &\Longrightarrow m - \alpha(m') \in \ker(\varphi) \\ &\qquad \text{since } \varphi(m) = \alpha'(n') = \alpha'(\varphi'(m')) = \varphi(\alpha(m')) \\ &\Longrightarrow \beta_|(m - \alpha(m')) = \underbrace{\beta(m)}_{=m''} - \underbrace{(\beta \circ \alpha)(m')}_{=0 \text{ by exactn.}} = m'' \end{aligned}$$

$$\Longrightarrow m'' \in \mathrm{Im}(\beta_|)$$

□

Corollary 2.23 (Special 5-lemma)**.** *Suppose that in 2.22 two of the maps $\varphi, \varphi', \varphi''$ are isomorphisms. Then so is the third one.*

Proof. Assume φ', φ'' are isom. We know the following sequence is exact:

$$\ker(\varphi') \longrightarrow \ker(\varphi) \longrightarrow \ker(\varphi'') \xrightarrow{\delta} \mathrm{Coker}(\varphi') \longrightarrow \mathrm{Coker}(\varphi) \longrightarrow \mathrm{Coker}(\varphi'')$$

$$\begin{aligned}
&\Longrightarrow 0 \longrightarrow \ker(\varphi) \longrightarrow 0 \text{ is exact} \\
&\Longrightarrow \ker(\varphi) = 0 \\
&\text{and } 0 \longrightarrow \mathrm{Coker}(\varphi) \longrightarrow 0 \text{ is exact} \\
&\Longrightarrow \mathrm{Coker}(\varphi) = 0
\end{aligned}$$

Thus φ is an isomorphism. The remaining cases work analogously. □

Corollary 2.24 (9-lemma)**.** *Consider*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 & (*) \\
0 \arrow[r] & N' \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & N'' \arrow[r] \arrow[d] & 0 & \\
0 \arrow[r] & P' \arrow[r] \arrow[d] & P \arrow[r] \arrow[d] & P'' \arrow[r] \arrow[d] & 0 & (**) \\
 & 0 & 0 & 0 & &
\end{tikzcd}$$

with exact columns.

If the middle row and one of *(*),(**) is exact, then so is the other row.*

Proof. If (*) is exact, then by 2.22 and exactness of columns:

$$0 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow P' \longrightarrow P \longrightarrow P'' \longrightarrow 0$$

is exact. Analogously, if (**) is exact, then

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0$$

is exact. □

Corollary 2.25. *For a short exact sequence* $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\varphi} M'' \longrightarrow 0$ *the following are equivalent:*

(a) *The sequence is split exact, i.e.* $\exists\, \psi \in \operatorname{Hom}(M'', M) : \varphi \circ \psi = \mathrm{id}_{M''}$

(b) $\exists\, j \in \operatorname{Hom}(M, M') : j \circ i = \mathrm{id}_{M'}$

In both cases we have: $M \cong M' \oplus M''$

Proof.

- "(a) $\implies$ (b)":

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] \arrow[d, "\cong"] & M' \oplus M'' \arrow[r] \arrow[d, "i\oplus\psi"] & M'' \arrow[r] \arrow[d, "\cong"] & 0 & \text{exact} \\ 0 \arrow[r] & M' \arrow[r, "i"] & M \arrow[r, "\varphi"] & M'' \arrow[r] & 0 & \text{exact} \end{tikzcd}$$

  This commutes. Thus, by 2.23 $i \oplus \psi$ is an isomorphism and we set

$$j := \pi_{M'} \circ (i \oplus \psi)^{-1}$$

- "(b) $\implies$ (a)":

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "i"] \arrow[d, "\cong"] & M \arrow[r, "\varphi"] \arrow[d, "j\oplus\varphi"] & M'' \arrow[r] \arrow[d, "\cong"] & 0 & \text{exact} \\ 0 \arrow[r] & M' \arrow[r] & M' \oplus M'' \arrow[r] & M'' \arrow[r] & 0 & \text{exact} \end{tikzcd}$$

  Analogously $j \oplus \varphi$ is an isomorphism and we set:

$$\psi := (j \oplus \varphi)^{-1}_{|M''}$$

□

Proposition 2.26.

(a) *Let*

$$\begin{tikzcd} M' \arrow[r, "\alpha"] \arrow[d, "\varphi'"] & M \arrow[r, "\beta"] \arrow[d, "\varphi"] & M'' \arrow[r] \arrow[d, dotted, "\varphi''"] & 0 \\ N' \arrow[r, "\alpha'"] & N \arrow[r, "\beta'"] & N'' & \end{tikzcd}$$

be a commutative diagram of R*-linear maps, such that the first row is exact and* $\beta' \circ \alpha' = 0$.

Then there exists $\varphi'' : M'' \to N''$ R*-linear, such that* $\beta' \circ \varphi = \varphi'' \circ \beta$ *(i.e.: the diagram commutes).*

(b) Let

$$\begin{tikzcd} & M' \arrow[r, "\alpha"] \arrow[d, dotted, "\varphi'"] & M \arrow[r, "\beta"] \arrow[d, "\varphi"] & M'' \arrow[d, "\varphi''"] \\ 0 \arrow[r] & N' \arrow[r, "\alpha'"] & N \arrow[r, "\beta'"] & N'' \end{tikzcd}$$

be a commutative diagram, such that the second row is exact and $\beta \circ \alpha = 0$.

Then there exists a $\varphi' : M' \to N'$ *R-linear, such that* $\alpha' \circ \varphi' = \varphi \circ \alpha$*(i.e.: the diagram commutes).*

Proof.

(a) Let $m'' \in M''$. Then by exactness $\exists\, m \in M : \beta(m) = m''$.

Define $\varphi''(m'') := \beta'(\varphi(m))$

Show: φ'' is well-defined

Let $m, \tilde{m} \in M$, such that $\beta(m) = \beta(\tilde{m}) = m''$

$$\begin{aligned} &\Longrightarrow m - \tilde{m} \in \ker(\beta) = \mathrm{Im}(\alpha) \\ &\Longrightarrow \exists m' \in M' : \alpha(m') = m - \tilde{m} \\ &\Longrightarrow \varphi(\alpha(m')) = \varphi(m - \tilde{m}) = \varphi(m) - \varphi(\tilde{m}) \\ &\qquad = \alpha'(\varphi'(m')) \in \mathrm{Im}(\alpha') = \ker(\beta') \\ &\Longrightarrow \beta'(\varphi(m)) = \beta'(\varphi(\tilde{m})) \end{aligned}$$

Note. φ'' is obviously R-linear.

(b) Exercise.

□

D). Tensor Products

Definition 2.27. Let $M_1, ..., M_n, T$ be R-modules. A multilinear map

$$\varphi : M_1 \times ... \times M_n \to T$$

is called a *tensor product* of $M_1, ..., M_n$

$:\Longleftrightarrow$ $\forall$ multilinear $\psi : M_1 \times ... \times M_n \to M$ (where M is an R-module) $\exists_1\, \alpha \in \mathrm{Hom}_R(T, M)$,such that $\alpha \circ \varphi = \psi$, i.e. the following diagram commutes:

$$\begin{tikzcd} M_1 \times ... \times M_n \arrow[rr, "\psi"] \arrow[dr, "\varphi"'] & & M \\ & T \arrow[ur, dotted, "\alpha"'] & \end{tikzcd}$$

$\iff \forall$ R-modules M the map

$$\mathrm{Hom}_R(T, M) \xrightarrow{1:1} Mult(M_1 \times ... \times M_n, M); \alpha \mapsto \alpha \circ \varphi$$

is bijective.

Proposition 2.28 (Existence)**.** *If $M_1, ..., M_n$ are R-modules, then there exists a tensor product.*

Proof. Let $P := M_1 \times .. \times M_n$ and let $F := \bigoplus_{\lambda \in P} R$ be the free module of rank $\#P$.

By abuse of notation we denote the free generators corresponding to the λ-component by $\lambda = (m_1, ..., m_n)$.

$$\begin{aligned} \implies F &= \left\{ \sum_{\lambda \in P} a_\lambda \lambda \,|\, \text{only finitely many } a_\lambda \text{ are non-zero} \right\} \\ &= \left\{ \sum_{(m_1,...,m_n) \in P} a_{(m_1,...,m_n)}(m_1, ..., m_n) \,|\, ... \right\} \end{aligned}$$

Careful! These are formal sums, so we can't pull $a_{(m_1,...,m_n)}$ into the vector $(m_1, ..., m_n)$!

Now consider the submodule

$$N := \left\langle \begin{array}{l} (m_1, ..., m_i + m_i', ..., m_n) - (m_1, ..., m_n) - (m_1, ..., m_i', ..., m_n), \\ (m_1, ..., am_i, ..., m_n) - a(m_1, ..., m_n) \; \forall m_1, ..., m_n, m_i'; i \in \{1..n\}; a \in R \end{array} \right\rangle$$

The quotient module is called $T := {}^{F}\!/_{N}$

Let $\varphi : P \to T : (m_1, ..., m_n) \mapsto \overline{(m_1, ..., m_n)}$. Then φ is multilinear by definition of T.

Let $\psi : P \to M$ be multilinear. Then define:

$$\alpha' : F \to M : \sum_{\lambda \in P} a_\lambda \lambda \mapsto \sum_{\lambda \in P} a_\lambda \psi(\lambda)$$

Then $\alpha'(N) = 0$, since ψ is multilinear.

$$\implies \alpha : T \to M, \bar{t} \mapsto \alpha'(t)$$

is well-defined and R-linear and

$$(\alpha \circ \varphi)(m_1, ..., m_n) = \alpha(\overline{(m_1, ..., m_n)}) = \psi(m_1, ..., m_n)$$

and α is obviously unique, since any other α' making the diagram commute would by definition map the generators $\overline{(m_1, ..., m_n)}$ of T to the same image, i.e. $\psi(m_1, ..., m_n)$. $\square$

Proposition 2.29 (Uniqueness)**.** *If $\varphi : M_1 \times ... \times M_n \to T$ and $\varphi' : M_1 \times ... \times M_n \to T'$ are two tensor products of $M_1, ..., M_n$, then there exists a unique isomorphism $\alpha : T \xrightarrow{\cong} T'$, such that*

$$\begin{tikzcd}
T \arrow[rr, "\cong", "\alpha"'] & & T' \\
& M_1 \times ... \times M_n \arrow[ul, "\varphi"] \arrow[ur, "\varphi'"'] &
\end{tikzcd}$$

commutes.

Proof. Consider the following diagram:

$$\begin{tikzcd}
M_1 \times ... \times M_n \arrow[r, "\varphi"] \arrow[dd, "\varphi'"'] \arrow[dr, "\varphi'"] \arrow[ddr, "\varphi"] & T \arrow[d, dotted, "\exists_1 \alpha"] \arrow[dd, dotted, bend left=60, "\exists_1 \mathrm{id}_T"] \\
& T' \arrow[d, dotted, "\exists_1 \beta"] \arrow[dl, dotted, "\exists_1 \mathrm{id}_{T'}"'] \\
T' & T \arrow[l, dotted, "\exists_1 \alpha"]
\end{tikzcd}$$

where the four unique homomorphisms are deduced by choosing either T or T' as tensor product and replacing the M in the definition of the tensor product each time by T and T'. Thus we get $\alpha \circ \beta = \mathrm{id}_{T'}, \beta \circ \alpha = \mathrm{id}_T$ and thus α is an isomorphism. □

Remark 2.30. *We choose the following notation:*

The tensor product of $M_1, ..., M_n$ we denote by $M_1 \otimes_R \cdots \otimes_R M_n$.

The image of $(m_1, ..., m_n)$ we denote by $m_1 \otimes \cdots \otimes m_n$ and call it a pure tensor*.*

Note.

- Every element in $M_1 \otimes_R \cdots \otimes_R M_n$ is a finite linear combination of pure tensors
- A linear map on $M_1 \otimes_R \cdots \otimes_R M_n$ can be definded simply by specifying the images of the pure tensors, as long as this behaves multilinearly
- If $M = \langle m_1, ..., m_k \rangle, N = \langle n_1, ..., n_l \rangle$

$$\implies M \otimes_R N = \langle m_i \otimes n_j \,|\, i = 1..k, j = 1..l \rangle_R$$

- We have

$$(r \cdot m) \otimes n = r \cdot (m \otimes n) = m \otimes (r \cdot n)$$

and

$$(m + m') \otimes n = m \otimes n + m' \otimes n.$$

Example 2.31.

(a) $M = R^n, N = R^m$ two finitely generated free modules

$$M \otimes_R N \cong Mat(n \times m, R) \text{ by } \underline{x} \otimes \underline{y} \mapsto \underline{x} \cdot \underline{y}^t$$

Thus $\{e_i \otimes e_j \mid i = 1..n, j = 1..m\}$ is a basis for $M \otimes_R N$.

(b) $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$, since:

$$\begin{aligned} \overline{a} \otimes \overline{b} &= (3\overline{a}) \otimes \overline{b} = \overline{a} \otimes (3\overline{b}) \\ &= \overline{a} \otimes \overline{0} = \overline{a} \otimes 0 \cdot \overline{0} \\ &= 0 \cdot \overline{a} \otimes \overline{0} = \overline{0} \otimes \overline{0} \end{aligned}$$

(c) Let $R = \mathbb{Z}, M = \mathbb{Z}, M' = 2\mathbb{Z}$ and $N = \mathbb{Z}/2\mathbb{Z}$. Then $2 \otimes \overline{1} \in M \otimes_R N$ and $2 \otimes \overline{1} \in M' \otimes_R N$, but:

In $M \otimes_R N : 2 \otimes \overline{1} = 2 \cdot 1 \otimes \overline{1} = 1 \otimes 2 \cdot \overline{1} = 1 \otimes \overline{0} = 0 \otimes \overline{0}$

In $M' \otimes_R N : 2 \otimes \overline{1} \neq 0 \otimes \overline{0}$

(d) Let M be an R-module, $I \trianglelefteq R$

$$M \otimes_R R/I \cong M/I \cdot M \text{ by } m \otimes \overline{r} \mapsto \overline{rm}$$

Proof.

- The map $M \times R/I \to M/I \cdot M, (m, \overline{r}) \mapsto \overline{rm}$ is bilinear, so there exists a unique
$$\varphi : M \otimes_R R/I \to M/I \cdot M, m \otimes \overline{r} \mapsto \overline{rm}$$
- φ is clearly surjective, since $\overline{m} = \varphi(m \otimes \overline{1})$.
- Show: φ is injective:

$$\begin{aligned} \ker(\varphi) \ni \sum_{i=1}^n a_i(m_i \otimes \overline{r_i}) &= \sum_i ((a_i m_i) \otimes \overline{r_i}) \\ &= \sum_i ((r_i a_i m_i) \otimes \overline{1}) \\ &= (\sum_i r_i a_i m_i) \otimes \overline{1} \end{aligned}$$

Thus we get:

$$
\begin{aligned}
&\Longrightarrow \varphi((\sum_i a_i r_i m_i) \otimes \overline{1}) = \overline{0} \\
&\Longrightarrow \overline{\sum_i a_i r_i m_i} = \overline{0} \\
&\Longrightarrow \sum_i a_i r_i m_i \in I \cdot M \\
&\Longrightarrow \exists\, n_j \in M, b_j \in I : \sum_i a_i r_i m_i = \sum_j b_j n_j \\
&\Longrightarrow (\sum_i r_i a_i m_i) \otimes \overline{1} = (\sum_j b_j n_j) \otimes \overline{1} = \sum_j (b_j n_j \otimes \overline{1}) \\
&\quad = \sum_j (n_j \otimes \overline{b_j}) = \sum_j (n_j \otimes \overline{0}) \\
&\quad = \sum_j (0 \otimes \overline{0}) = 0 \otimes \overline{0}
\end{aligned}
$$

$\Longrightarrow$ Injectivity

□

(e) Let R' be an R-algebra and let M be an R-module. Then:

$M \otimes_R R'$ is actually an R'-module via:

$$\underbrace{r'}_{\in R'}(m \otimes r) := m \otimes (r'r)$$

E.g.: $M = \mathbb{Z}^n, R = \mathbb{Z}, R' = \mathbb{Q}$

$$\Longrightarrow \mathbb{Z}^n \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^n$$

Proposition 2.32. *Let $M, N, P; M_\lambda, \lambda \in \Lambda$ be R-modules. Then:*

(a) $M \otimes_R N \cong N \otimes_R M$ *via:*

$m \otimes n \mapsto n \otimes m$

(b) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P) \cong M \otimes_R N \otimes_R P$ *via:*

$(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p) \mapsto m \otimes n \otimes p$

(c) $M \otimes (\bigoplus_{\lambda \in \Lambda} M_\lambda) \cong \bigoplus_{\lambda \in \Lambda}(M \otimes M_\lambda)$ *via:*

$m \otimes (m_\lambda)_{\lambda \in \Lambda} \mapsto (m \otimes m_\lambda)_{\lambda \in \Lambda}$

In particular: $M \otimes_R R^n \cong M^n$

(d) $\operatorname{Hom}_R(M \otimes N, P) \cong \operatorname{Hom}_R(M, \operatorname{Hom}_R(N, P))$ *via:*

$\varphi \mapsto (\tilde{\varphi} : M \to \operatorname{Hom}_R(N, P) : m \mapsto (N \to P : n \mapsto \varphi(m \otimes n)))$

Proof.

(a) clear, since $N \otimes_R M$ satisfies the universal property.

(b) Exercise

(c) $M \times \bigoplus_\lambda M_\lambda \xrightarrow{\text{bilin.}} \bigoplus_\lambda (M \otimes M_\lambda)$ via:

$(m, (m_\lambda)_\lambda) \mapsto (m \otimes m_\lambda)_\lambda$

So there exists a unique $\alpha : M \otimes \bigoplus_\lambda M_\lambda$, such that:

$m \otimes (m_\lambda)_\lambda \mapsto (m \otimes m_\lambda)_\lambda$

Show: α is surjective:

$$\begin{aligned}\bigoplus_\lambda (M \otimes M_\lambda) &= \langle (m \otimes m_\lambda)_\lambda \,|\, m \in M, m_\lambda \in M_\lambda, \text{only fin. many } m_\lambda \text{ non-zero}\rangle \\ &= \operatorname{Im}(\alpha)\end{aligned}$$

Show: α is injective:

Since $M \times M_\lambda \to M \otimes \bigoplus_{\mu \in \Lambda} M_\mu$

$(m, m_\lambda) \mapsto m \otimes (m_\mu)_{\mu \in \Lambda}$ with $m_\mu = \begin{cases} m_\lambda & , \lambda = \mu \\ 0 & , \lambda \neq \mu \end{cases}$

is bilinear, there exists a unique $a_\lambda : M \otimes M_\lambda \to M \otimes \bigoplus_{\mu \in \Lambda} M_\mu$, such that:

$m \otimes m_\lambda \mapsto m \otimes (m_\mu)_{\mu \in \Lambda}$, with m_μ as above.

So there is a unique

$$\begin{aligned}\alpha' : \bigoplus_{\lambda \in \Lambda} M \otimes M_\lambda &\to M \otimes \bigoplus_{\mu \in \Lambda} M_\mu \\ (m \otimes m_\lambda)_{\lambda \in \Lambda} &\mapsto \sum_{\lambda \in \Lambda} a_\lambda (m \otimes m_\lambda)\end{aligned}$$

Obviously: $(\alpha' \circ \alpha)(m \otimes (m_\lambda)_\lambda) = ... = m \otimes (m_\lambda)_\lambda$

$\implies \alpha' \circ \alpha = \mathrm{id} \implies \alpha$ is injective.

(d) Clearly $\gamma : \varphi \mapsto \tilde{\varphi}$ is an R-linear map. Our claim is now, that γ is bijective:
If $\psi : M \to \mathrm{Hom}_R(N, P)$ is R-linear, then

$$\begin{aligned}\psi' :&M \times N \to P \\ &(m, n) \mapsto \psi(m)(n)\end{aligned}$$

is bilinear. Thus there exists a unique homomorphism

$$\begin{aligned}\varphi :&M \otimes N \to P \\ &m \otimes n \mapsto \psi(m)(n) = \varphi(m \otimes n) = \tilde{\varphi}(m)(n) = \gamma(\varphi)(m)(n)\end{aligned}$$

Thus $\psi = \gamma(\varphi) \in \mathrm{Im}(\gamma)$ and γ is surjective. Injectivity is obvious.

$\square$

Proposition 2.33 (Exactness)**.** *Let M, M', M'', N be R-modules.*

(a) $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ *is exact* $\iff$

$\forall\, P$ *R-module:* $0 \longrightarrow \mathrm{Hom}_R(M'', P) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, P) \xrightarrow{\varphi^*} \mathrm{Hom}_R(M', P)$ *is exact.*

(b) If $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ *is exact, then:*

$M' \otimes N \xrightarrow{\varphi \otimes \mathrm{id}_N} M \otimes N \xrightarrow{\psi \otimes \mathrm{id}_N} M'' \otimes N \longrightarrow 0$ *is exact (i.e. the tensor product is* right exact*!).*

(c) If $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ *is split exact, then:*

$0 \longrightarrow M' \otimes N \xrightarrow{\varphi \otimes \mathrm{id}_N} M \otimes N \xrightarrow{\psi \otimes \mathrm{id}_N} M'' \otimes N \longrightarrow 0$ *is split exact.*

Proof.

(a) Exercise

(b)

$$
\begin{aligned}
& M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \text{ is exact} \\
\overset{(a)}{\Longrightarrow}\ & 0 \longrightarrow \mathrm{Hom}_R(M'', \mathrm{Hom}_R(N,P)) \longrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P)) \longrightarrow \dots \\
& \dots \longrightarrow \mathrm{Hom}_R(M', \mathrm{Hom}_R(N,P)) \\
& \text{is exact } \forall P \\
\overset{2.32}{\Longrightarrow}\ & 0 \longrightarrow \mathrm{Hom}_R(M'' \otimes N, P) \longrightarrow \mathrm{Hom}_R(M \otimes N, P) \longrightarrow \dots \\
& \dots \longrightarrow \mathrm{Hom}_R(M' \otimes N, P) \\
& \text{is exact } \forall P \\
\overset{(a)}{\Longrightarrow}\ & M' \otimes N \longrightarrow M \otimes N \longrightarrow M'' \otimes N \longrightarrow 0 \text{ is exact}
\end{aligned}
$$

(c) Too long and tedious, skipped.

□

Example 2.34. (The tensor product is not left exact in general) The sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

is exact, but

$$0 \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$$

is not exact, since $i(1 \otimes \overline{1}) = 2 \otimes \overline{1} = 0$, so i is not injective!

Definition 2.35. Let R be a ring, P be an R-module.

(a) P is called *flat* over R

$:\Longleftrightarrow$ For all exact sequences $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ the sequence

$$0 \longrightarrow M' \otimes P \xrightarrow{\varphi \otimes \mathrm{id}_P} M \otimes P \xrightarrow{\psi \otimes \mathrm{id}_P} M'' \otimes P \longrightarrow 0$$

is also exact.

$\Longleftrightarrow$ For all exact sequences $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$ the sequence

$$M' \otimes P \xrightarrow{\varphi \otimes \mathrm{id}_P} M \otimes P \xrightarrow{\psi \otimes \mathrm{id}_P} M'' \otimes P$$

is also exact.

$\iff$ For all injective maps $\varphi : M' \hookrightarrow M$ the map

$$\varphi \otimes \mathrm{id}_P : M' \otimes P \to M \otimes P$$

is also injective.

(b) P is called *projective*

$:\iff \forall\ M \overset{\varphi}{\twoheadrightarrow} N\ , \psi : P \to N \,\exists\, \alpha$, such that

$$\begin{tikzcd} M \arrow[r, two heads, "\varphi"] & N \\ & P \arrow[u, "\psi"'] \arrow[ul, dotted, "\alpha"] \end{tikzcd}$$

commutes.

(c) P is called *finitely presented*

$:\iff \exists\, k, l \in \mathbb{N}, \varphi$, such that:

$$R^k \longrightarrow R^l \xrightarrow{\varphi} P \longrightarrow 0 \text{ is exact.}$$

Proposition 2.36. *For an R-module P the following are equivalent:*

(a) P is projective

(b) For all surjective maps $M \overset{\varphi}{\twoheadrightarrow} N$ the map $\varphi_* : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$ is surjective.

(c) If $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ is exact, then it is split exact.

(d) There exists an R-module M, such that $M \oplus P$ is free.

Proof. Exercise. □

Example 2.37.

(a) P is fintely presented $\iff$ P is finitely generated and $\ker(\varphi)$ is finitely generated by $(\varphi : R^l \to P, r_i \mapsto p_i)$.

(b) P is free $\implies$ P is projective. In particular R^n is projective.

(c) P free $\implies$ P flat

Proof. Let $P = \bigoplus_\lambda R, \varphi : M' \to M$ injective.

$$\begin{tikzcd}
M' \otimes_R P \arrow[r, "\varphi \otimes \mathrm{id}_P"] \arrow[d, "\cong"] & M \otimes_R P \arrow[d, "\cong"] \\
\bigoplus_\lambda (M' \otimes_R R) \arrow[d, "\cong"] & \bigoplus_\lambda (M \otimes_R R) \arrow[d, "\cong"] \\
\bigoplus_\lambda M' \arrow[r, "\tilde{\varphi}"] & \bigoplus_\lambda M
\end{tikzcd}$$

$$(m'_\lambda)_\lambda \longmapsto (\varphi(m'_\lambda))_\lambda$$

So $(m'_\lambda) \in \ker(\tilde{\varphi}) \iff \varphi(m'_\lambda) = 0 \forall\, \lambda$

$\iff m'_\lambda \in \ker(\varphi) \forall\, \lambda \overset{\varphi \text{ inj.}}{\iff} m'_\lambda = 0 \forall\, \lambda$

Hence P is flat. $\square$

(d) Let $R = K[x], P = {K[x,y]}/{\langle xy \rangle}$ and consider the map

$\varphi :\ M' := K[x] \xhookrightarrow{\cdot x} K[x] =: M$. Then:

$(\mathrm{id}_P \otimes \varphi)(\overline{y} \otimes 1) = \overline{y} \otimes x = \overline{xy} \otimes 1 = \overline{0} \otimes 1 = 0$, so $\mathrm{id}_P \otimes \varphi : P \otimes_R M' \to P \otimes_R M$ is not injectice. Thus, P is not flat.

Proposition 2.38. *P projective $\implies$ P flat*

Proof. P projective $\overset{2.36}{\implies} \exists\, N : P \oplus N$ is free.

Thus, by 2.37(c) and for any injective map $\varphi : M' \to M$:

$$\begin{tikzcd}
M' \otimes (P \oplus N) \arrow[r, hook] \arrow[d, "\cong"] & M \otimes (P \oplus N) \arrow[d, "\cong"] \\
(M' \otimes P) \oplus (M' \otimes N) \arrow[r, hook] & (M \otimes P) \oplus (M \otimes N)
\end{tikzcd}$$

$\implies \varphi \otimes \mathrm{id}_P$ is injective $\implies$ P is flat. $\square$

Proposition 2.39. *If $(R, \mathfrak{m})$ is local and P is finitely presented, then:*

$$P \text{ projective } \iff P \text{ free}$$

Proof. We only have to show "$\Longrightarrow$": Choose a minimal set of generators for P, say $(m_1, ..., m_n)$. Thus the sequence

$$0 \longrightarrow \ker(\varphi) \longrightarrow R^n \xrightarrow{\varphi} P \longrightarrow 0$$

is exact (where $\varphi(e_i) = m_i$ and $\ker(\varphi)$ is finitely generated). Thus, by 2.36 the sequence is also split exact and by 2.31, 2.33 tensorizing with $R/\mathfrak{m}$ yields the following split exact sequence:

$$0 \longrightarrow \ker(\varphi) \otimes R/\mathfrak{m} \longrightarrow R^n \otimes R/\mathfrak{m} \longrightarrow P \otimes R/\mathfrak{m} \longrightarrow 0$$

which is isomorphic to

$$0 \longrightarrow \ker(\varphi)/\mathfrak{m}\ker(\varphi) \longrightarrow (R/\mathfrak{m})^n \longrightarrow P/\mathfrak{m}P \longrightarrow 0$$

Since these are vector spaces, $(R/\mathfrak{m})^n = \ker(\varphi)/\mathfrak{m}\ker(\varphi) \oplus P/\mathfrak{m}P$ and $\dim(R/\mathfrak{m})^n = \dim P/\mathfrak{m}P = n$ by Nakayama's lemma we have that

$$\begin{aligned} &\ker(\varphi)/\mathfrak{m}\ker(\varphi) = 0 \\ \Longrightarrow\ &\ker(\varphi) = \mathfrak{m}\ker(\varphi) \overset{\text{NAK}}{\Longrightarrow} \ker(\varphi) = 0 \end{aligned}$$

Thus φ is an isomorphism and $P \cong R^n$ $\square$

Remark 2.40. *With some homological algebra, we get*

$$0 \longrightarrow Tor_1^R(P, R/\mathfrak{m}) \longrightarrow \ker(\varphi) \otimes R/\mathfrak{m} \longrightarrow R^n \otimes R/\mathfrak{m} \longrightarrow P \otimes R/\mathfrak{m} \longrightarrow 0$$

is exact and:

$$\begin{aligned} P \text{ flat } &\iff Tor_1^R(P, R/\mathfrak{m}) = 0 \\ &\iff P \text{ free} \end{aligned}$$

3. Localisation

Motivation. How did we construct the rational numbers?

Let $R = \mathbb{Z}, S = \mathbb{Z} \backslash \{0\}$

$$\implies \mathbb{Q} = {R \times S}/{\sim}$$

with

$$(r, s) \sim (r', s') :\iff rs' = r's$$

The operations on $\mathbb{Q}$ are defined by

- $\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}$
- $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$

Note. $s, s' \in S$ implies $ss' \in S$

Definition 3.1. Let R be a ring.

(a) A subset $S \subseteq R$ is called *multiplicatively closed* $:\iff \forall s, s' \in S:\ ss' \in S$ *and* $1_R \in S$.

(b) If $S \subseteq R$ is multipl. closed, then we define for $(r, s), (r', s') \in R \times S$:

$$(r, s) \sim (r', s') :\iff \exists u \in S : u(rs' - r's) = 0$$

Note. The '$\exists u$...' is only really needed to ensure transitivity in the following proof.

Our claim is now, that $\sim$ is an equivalency relation:

Proof.

- *Reflexivity:* $1(rs - rs) = 0 \implies (r, s) \sim (r, s)$
- *Symmetry:*

$$\begin{aligned} &(r, s) \sim (r', s') \\ \implies &\exists u \in S : u(rs' - r's) = 0 \\ \implies &u(r's - rs') = 0 \\ \implies &(r', s') \sim (r, s) \end{aligned}$$

- *Transitivity:*

$$\begin{aligned} &(r,s) \sim (r',s'), (r',s') \sim (r'',s'') \\ \Longrightarrow &\exists u, v \in S : u(rs' - r's) = 0, v(r's'' - r''s') = 0 \\ \Longrightarrow &0 = vu(rs's'' - r'ss'') + (r's''s - r''s's)vu \\ &= \underbrace{uvs'}_{\in S}(rs'' - r''s) \\ \Longrightarrow &(r,s) \sim (r'',s'') \end{aligned}$$

□

We then write

$$[(r,s)] =: \frac{r}{s}$$

and

$$S^{-1}R := {R \times S}/{\sim} = \left\{ \frac{r}{s} \mid r \in R, s \in S \right\}$$

Define operations on $S^{-1}R$ by:

- $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$
- $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$

We claim, that $(S^{-1}R, +, \cdot)$ is a commutative ring with $1_{S^{-1}R} = \frac{1_R}{1_R} = \frac{s}{s} \forall s \in S$ (without proof).

We call $S^{-1}R$ the *localisation of R at S*.

Remark 3.2. *There is a natural ring extension*

$$i : R \longrightarrow S^{-1}R : r \mapsto \frac{r}{1}$$

Note.

(a) $s \in S \implies i(s) = \frac{s}{1}$ is a unit

(b) $i(r) = 0 \iff \exists u \in S : ur = 0.$

In particular: i is injective $\iff$ S contains no zero-divisors.

(c) Every element of $S^{-1}R$ has the form $i(s)^{-1}i(r) = \frac{r}{s}$ for some $r \in R, s \in S$.

(d) Let $j : R \longrightarrow R'$, s.t. $j(S) \subseteq (R')^*$. Then there exists a *unique* linear $\varphi : S^{-1}R \longrightarrow R'$ such that

$$\begin{tikzcd} R \arrow[r, "j"] \arrow[dr, "i"'] & R' \\ & S^{-1}R \arrow[u, "\exists_1 \varphi"'] \end{tikzcd}$$

commutes.

Moreover, if j satisfies the first three criteria, then φ is an isomorphism.

(e) $J \trianglelefteq S^{-1}R \implies (J^c)^e = J$

(f) $I \trianglelefteq R \implies (I^e \neq S^{-1}R \iff I \cap S = \emptyset)$

Proof.

- (a)-(d) hold by definition

(e):

"$\subseteq$": By 1.10

"$\supseteq$": $a = \frac{r}{s} \in J \implies \frac{r}{1} = \frac{s}{1}a \in J$

$\implies r \in i^{-1}(J) = J^c \implies \frac{r}{1} \in (J^c)^e \implies a = \frac{1}{s}\frac{r}{1} \in (J^c)^e$

(f):

"$\implies$": Suppose $I \cap S \neq \emptyset$ Then $\frac{s}{1} \in I^e$, which is a unit. Therefore $I^e = S^{-1}R$↯

"$\impliedby$": Suppose $\{\frac{a}{s}, a \in I, s \in S\} = I^e = S^{-1}R \ni \frac{1}{1}$. Then $\exists a \in I, s \in S : \frac{a}{s} = \frac{1}{1}$ and therefore $\exists u \in S : \underbrace{ua1}_{\in I} = \underbrace{us1}_{\in S} \implies I \cap S \neq \emptyset$↯

□

Example 3.3.

(a) $0 \neq R$ any ring, $S = \{r \in R \,|\, r \text{ is not a zero-divisor}\}$

$$\implies \mathrm{Quot}(R) := S^{-1}R$$

is the *total ring of fractions* or *total quotient ring*.

In particular: If R is an I.D., then $S = R\backslash\{0\}$ and $\mathrm{Quot}(R)$ is a field (the *quotient field* of R).

E.g.:

- $R = \mathbb{Z} \implies \mathrm{Quot}(R) = \mathbb{Q}$
- $R = K[\underline{x}] \implies \mathrm{Quot}(R) = \{\frac{f}{g} \,|\, f, g \in K[\underline{x}], g \neq 0\} =: K(\underline{x})$

(b) R ring, $f \in R, S := \{f^n \,|\, n \geq 0\}$

$$\implies R_f := S^{-1}R = \{\frac{r}{f^n} \,|\, n \geq 0, r \in R\}$$

is the *localisation at f*.

E.g.: $R = \mathbb{Z}, f = p \in P \implies \mathbb{Z}_p = \{\frac{z}{p^n} \,|\, z \in \mathbb{Z}, n \geq 0\} \leq \mathbb{Q}$

(c) R ring, $P \in \operatorname{Spec}(R), S = R \backslash P$

$$R_P := S^{-1}R = \left\{ \frac{r}{s} \mid s, r \in R, s \notin P \right\}$$

is the *localisation at* P.

E.g.: $R = \mathbb{Z}, P = \langle p \rangle, p \in \mathbb{P}$. Then:

- $\mathbb{Z}_P = \{\frac{z}{s} \mid z \in \mathbb{Z}, p \nmid s\}] \leq \mathbb{Q}$
- $\mathbb{Z}_p \cap \mathbb{Z}_{\langle p \rangle} = \mathbb{Z}$

If R is an I.D., $P = \langle 0 \rangle \implies R_{\langle 0 \rangle} = \operatorname{Quot}(R)$

(d) $S^{-1}R = 0 \iff 0 \in S$

Proof. We show two directions:

- "$\Longleftarrow$": $0 \in S \implies \frac{a}{s} = \frac{0}{1}\ \forall a \in R, s \in S$, since $0 \cdot (a \cdot 1) = 0 \cdot (s \cdot 0)$
- "$\Longrightarrow$": $\frac{1}{1} = \frac{0}{1} \implies \exists u \in S : u \cdot 1 \cdot 1 = u \cdot 1 \cdot 0 = 0 \implies u = 0 \in S$

$\square$

Proposition 3.4. *$P \in \operatorname{Spec}(R) \implies R_P$ is a local ring with $P \cdot R_P = P^e \lhd \cdot R_P$.*

Proof. We have to show: $R_P \backslash P^e = R_P^*$:

"$\supseteq$": $P \cap (R \backslash P) = \emptyset \overset{3.2}{\implies} P^e \subsetneq R_P$. Thus, P^e contains no units $\implies R_P^* \subseteq R_P \backslash P^e$

"$\subseteq$": $\frac{r}{s} \in R_P \backslash P^e \implies r, s \notin P \implies \frac{s}{r} \in R_P$ and $\frac{r}{s}\frac{s}{r} = 1 \implies \frac{r}{s} \in R_P^*$

$\square$

Example.

$$K := \mathbb{R}, R := K[x,y], P := \langle x-1, y-1 \rangle, R_P = \left\{ \frac{f}{g} \mid f, g \in K[x,y], g(1,1) \neq 0 \right\}$$

Then $\frac{f}{g} : U_\epsilon(1,1) \longrightarrow R, p \mapsto \frac{f(p)}{g(p)}$ is well-defined.

Definition 3.5. Let R be a ring, $S \subseteq R$ multipl. closed and M, N, P be R-modules.

(a) Define

$$S^{-1}M := \left\{ \frac{m}{s} \mid m \in M, s \in S \right\} = {}^{M \times S}\!/\!_{\sim}$$

where

- $(m,s) \sim (m',s') :\iff \exists u \in S : u(ms' - m's) = 0$
- $\frac{m}{s} := [(m,s)]$
- $\frac{m}{s} + \frac{m'}{s'} = \frac{ms' + m's}{ss'}$

- $\frac{m}{s} \cdot \frac{m'}{s}' = \frac{mm'}{ss'}$

Note.
- $\sim$ is an equivalence relation
- $+, \cdot$ are well defined
- $(S^{-1}M, +, \cdot)$ is an $S^{-1}R$-module

(b) $\varphi \in \mathrm{Hom}_R(M, N)$. Define:

$$\mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \ni S^{-1}\varphi : S^{-1}M \longrightarrow S^{-1}N : \frac{m}{s} \mapsto \frac{\varphi(m)}{s}$$

Note.

- If $\varphi \in \mathrm{Hom}_R(M, N), \psi \in \mathrm{Hom}_R(N, P)$, then $S^{-1}(\psi \circ \varphi) = S^{-1}\psi \circ S^{-1}\varphi$.
- $S^{-1}(\mathrm{id}_M)) = \mathrm{id}_{S^{-1}M}$
- Thus: S^{-1} is a *covariant functor.*

(c) *Notation:* If $S = \{f^n \,|\, n \geq 0\}$, then
- $S^{-1}M =: M_f$
- $S^{-1}\varphi =: \varphi_f$

If $S = R \backslash P, P \in \mathrm{Spec}(R)$, then $M_P := S^{-1}M, \varphi_P := S^{-1}\varphi$

Proposition 3.6. *(S^{-1} is an exact functor) Let $S \subseteq R$ be multipl. closed and $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$ an exact, R-linear sequence. Then*

$$S^{-1}M' \xrightarrow{S^{-1}\varphi} S^{-1}M \xrightarrow{S^{-1}\psi} S^{-1}M''$$

is also exact.

Proof. We need to show: $\mathrm{Im}(S^{-1}\varphi) = \ker(S^{-1}\psi)$

"$\subseteq$": $S^{-1}\psi \circ S^{-1}\varphi = S^{-1}(\underbrace{\psi \circ \varphi}_{=0}) = 0$. Thus $\mathrm{Im}(S^{-1}\varphi) \subseteq \ker(S^{-1}\psi)$.

"$\supseteq$": Let $\frac{m}{s} \in \ker(S^{-1}\psi) \implies \frac{\psi(m)}{s} = S^{-1}\psi(\frac{m}{s}) = \frac{0}{1}$

$$\begin{aligned}
&\Longrightarrow \exists u \in S : \underbrace{u\psi(m)}_{=\psi(um)} = us \cdot 0 = 0 \\
&\Longrightarrow um \in \ker(\psi) \\
&\Longrightarrow \text{(by exactn.) } um \in \mathrm{Im}(\varphi) \implies \exists m' \in M' : \varphi(m') = um \\
&\Longrightarrow \frac{m}{s} = \frac{um}{us} = \frac{\varphi(m')}{us} = S^{-1}\varphi(\frac{m'}{us}) \in \mathrm{Im}(S^{-1}\varphi)
\end{aligned}$$

□

Corollary 3.7. *Let R be a ring, M_λ, M, M' R - modules, $\lambda \in \Lambda, N, N' \leq M, \varphi \in \mathrm{Hom}_R(M, M')$. Then:*

(a) $S^{-1}R \otimes_R M \cong S^{-1}M$
(by $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$*)*

(b) $S^{-1}N + S^{-1}N' = S^{-1}(N + N')$

(c) $S^{-1}N \cap S^{-1}N' = S^{-1}(N \cap N')$

(d) $S^{-1}(M/N) \cong S^{-1}M / S^{-1}N$

(e) $S^{-1}(\bigoplus_{\lambda\in\Lambda} M_\lambda) \cong \bigoplus_{\lambda\in\Lambda} S^{-1}M_\lambda$

(f) $\ker(S^{-1}\varphi) = S^{-1}\ker(\varphi)$
$\mathrm{Im}(S^{-1}\varphi) = S^{-1}\mathrm{Im}(\varphi)$

Proof.

(a)

Note. $S^{-1}R \times M \longrightarrow S^{-1}M, (\frac{r}{s}, m) \mapsto \frac{rm}{s}$ is bilinear.

Thus $\exists_1 \alpha : S^{-1}R \otimes_R M \longrightarrow S^{-1}M : \frac{r}{s} \otimes m \mapsto \frac{rm}{s}$. Our claim is, that α is an isomorphism.

α is clearly surjective, since $\frac{m}{s} = \frac{1m}{s} = \alpha(\frac{1}{s} \otimes m) \in \mathrm{Im}(\alpha)$. It remains to show that α is injective:

Let $x = \sum_{i=1}^k \frac{r_i}{s_i} \otimes m_i \in \ker\alpha$. Now we transform all fractions to a common denominator, i.e. $\exists \tilde{r}_i \in R, s \in S : \frac{r_i}{s_i} = \frac{\tilde{r}_i}{s}$

$$\begin{aligned} \Longrightarrow x &= \sum_{i=1}^k \frac{\tilde{r}_i}{s} \otimes m_i \\ &= \sum_{i=1}^k \frac{1}{s} \otimes \tilde{r}_i m_i \\ &= \frac{1}{s} \otimes (\sum_{i=1}^k \tilde{r}_i m_i), x \in \ker\alpha \end{aligned}$$

Thus

$$\frac{0}{1} = \alpha(x) = \frac{\sum_{i=1}^k \tilde{r}_i m_i}{s} \Longrightarrow \exists u \in S : \underbrace{u \cdot \sum_{i=1}^k \tilde{r}_i m_i}_{=\sum(u\tilde{r}_i)m_i} = 0$$

$\Longrightarrow x = \frac{1}{su} \otimes \sum_{i=1}^k u\tilde{r}_i m_i = 0$

(b) clear

(c) We show two inclusion:

"$\supseteq$": ✓

"$\subseteq$": Let $\frac{n}{s} = \frac{n'}{s'}$ with $n \in N, n' \in N', s, s' \in S$.

$\implies \exists u \in S : \underbrace{us'n}_{\in N} = \underbrace{usn'}_{\in N'} \in N \cap N'$

$\implies \frac{n}{s} = \frac{us'n}{us's} \in S^{-1}(N \cap N')$

(d) We know that

$$0 \longrightarrow N \longrightarrow M \longrightarrow {}^{M}\!/_{N} \longrightarrow 0$$

is exact. Thus, by 3.6 we know that

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}({}^{M}\!/_{N}) \longrightarrow 0$$

is exact.

$$\implies S^{-1}({}^{M}\!/_{N}) \cong {}^{S^{-1}M}\!/_{S^{-1}N}$$

(e) Follows from (a) and 2.32

(f) We know that

$$0 \longrightarrow \ker(\varphi) \longrightarrow M \xrightarrow{\varphi} M' \longrightarrow \mathrm{Coker}(\varphi) \longrightarrow 0$$

is exact and by 3.6

$$0 \longrightarrow S^{-1}(\ker(\varphi)) \longrightarrow S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}M' \longrightarrow S^{-1}(\mathrm{Coker}(\varphi)) \longrightarrow 0$$

is exact

$\implies \ker(S^{-1}\varphi) = S^{-1}(\ker(\varphi)), \mathrm{Coker}(S^{-1}\varphi) = S^{-1}(\mathrm{Coker}(\varphi))$

$\square$

Example 3.8. Let $R = \mathbb{Z}, p$ prime, $N_p := \langle p \rangle \trianglelefteq \mathbb{Z}, S = \mathbb{Z}\backslash\{0\}$. Then:

- $\bigcap\limits_{p \text{ prime}} N_p = \{0\}$, thus $S^{-1}(\bigcap\limits_{p \text{ prime}} N_p = \{0\}) = 0$, but
- $S^{-1}N_p = \mathbb{Q} \,\forall\, p \implies \bigcap\limits_{p \text{ prime}} S^{-1}N_p = \mathbb{Q}$

So localisation does *not* commute with arbitrary intersections!

Proposition 3.9. *$S \subseteq R$ multiplicatively closed, then:*

$$\{P \in \operatorname{Spec}(R) \mid P \cap S = \emptyset\} \xrightarrow{1:1} \operatorname{Spec}(S^{-1}R),\ P \mapsto P^e = S^{-1}P = \langle P \rangle_{S^{-1}R}$$

is bijective

Proof. Exercise □

Philosophy 3.10. *Let ($\mathcal{P}$) be a property of R - modules or of R-linear maps (e.g. "finitely generated", "injective",...). We call ($\mathcal{P}$)* local, *iff:*

$$M(\textit{or } \varphi) \textit{ has } (\mathcal{P}) \iff M_P(\textit{or } \varphi_P) \textit{ has } (\mathcal{P})\ \forall P \in \operatorname{Spec}(R)$$

Proposition 3.11 ("being 0" is a local property)**.** *For an R-module M the following are equivalent:*

(a) $M = 0$

(b) $M_P = 0\ \forall\, P \in \operatorname{Spec}(R)$

(c) $M_{\mathfrak{m}} = 0\ \forall\, \mathfrak{m} \in \mathfrak{m} - \operatorname{Spec}(R)$

Proof.

- "(a) $\implies$ (b)": ✓
- "(b) $\implies$ (c)": ✓
- "(c) $\implies$ (a)": Suppose $M \neq 0$

$$\begin{aligned}
&\implies \exists 0 \neq m \in M \implies \operatorname{ann}(m) \trianglelefteq R, \operatorname{ann}(m) \subsetneq R \\
&\implies \exists\, \mathfrak{m} \lhd \cdot R : \operatorname{ann}(m) \subseteq \mathfrak{m} \\
&\implies um \neq 0 \forall u \in R \backslash \mathfrak{m} \\
&\implies \frac{m}{1} \neq \frac{0}{1} \text{ in } M_{\mathfrak{m}} \implies M_{\mathfrak{m}} \neq 0 \lightning
\end{aligned}$$

□

Corollary 3.12 (Injectivity and Surjectivity are local)**.** *For an R -linear map $\varphi : M \longrightarrow N$ the following are equivalent:*

(a) φ is injective (surjective)

(b) φ_P is injective (surjective) $\forall\, P \in \operatorname{Spec}(R)$

(c) $\varphi_{\mathfrak{m}}$ is injective (surjective) $\forall\, \mathfrak{m} \in \mathfrak{m} - \operatorname{Spec}(R)$

Proof. By 3.7 and 3.11, since φ inj $\iff \ker(\varphi) = 0$ etc. □

Proposition 3.13. *Let R be an I.D., $f \in R$*

$$\Longrightarrow R_f = \bigcap_{P \in \mathrm{Spec}(R), f \notin P} R_P \quad \leq Quot(R)$$

In particular: $R \overset{f=1}{=} \bigcap_{P \in \mathrm{Spec}(R)} R_P$.

Proof. $S = \{f^n \mid n \geq 0\}$

"$\subseteq$": $f \notin P \implies S \subseteq R \backslash P$ and thus, since R is an I.D. $S^{-1}R = R_f \subseteq R_P \ \forall P \in \mathrm{Spec}(R)$

"$\supseteq$": Let $x \in \mathrm{Quot}(R)$,

$$I_x := \{r \in R \mid rx \in R\} \trianglelefteq R$$

Then

$$\begin{aligned} x \in R_P &\iff \exists\, a \in R, s \notin P : x = \frac{a}{s} \\ &\iff \exists\, s \in R \backslash P : sx \in R \\ &\iff I_x \nsubseteq P \end{aligned}$$

So if $x \in \bigcap_{P \in \mathrm{Spec}(R), f \notin P} R_P \implies I_x \nsubseteq P \ \forall P$ with $f \notin P$

$$\begin{aligned} &\overset{3.9}{\Longrightarrow} (I_x)_f \nsubseteq \mathfrak{m} \ \forall \mathfrak{m} \in \mathfrak{m} - \mathrm{Spec}(R_f) \\ &\Longrightarrow (I_x)_f = R_f \\ &\Longrightarrow I_x \cap S \neq \emptyset \\ &\Longrightarrow \exists f^n \in I_x \implies f^n \cdot x = a \in R \\ &\Longrightarrow x = \frac{a}{f^n} \in R_f \end{aligned}$$

$\square$

Proposition 3.14. *Let $S \subseteq R$ be multipl. closed; M, N R-modules s.t. M is finitely presented. Then:*

$$S^{-1}(\mathrm{Hom}_R(M,N)) \cong \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$$

by $\frac{\varphi}{s} \mapsto \frac{S^{-1}\varphi}{s}$.

Proof. Since M is finitely presented, there is an exact sequence

$$R^k \xrightarrow{\alpha} R^l \xrightarrow{\beta} M \longrightarrow 0\ .$$

Setting $m_i = \beta(e_i)$ and $v_j = \alpha(e'_j)$, where the e_i are the standard basis vectors in R^l and the e'_j are the standard basis vectors in R^k, we get

$$M = \langle m_1, \ldots, m_l \rangle \quad \text{and} \quad \ker(\beta) = \operatorname{Im}(\alpha) = \langle v_1, \ldots, v_k \rangle.$$

We consider now the map

$$\Phi : S^{-1}\mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) : \frac{\varphi}{u} \mapsto \frac{1}{u} \cdot S^{-1}\varphi.$$

This map is obviously well-defined and $S^{-1}R$-linear. We claim, that it is also bijective.

Let us first show that Φ is injective. For this we choose $\frac{\varphi}{u} \in \ker(\Phi)$. Then

$$0 = \Phi\left(\frac{\varphi}{u}\right) = \frac{1}{u} \cdot S^{-1}\varphi$$

implies that $\frac{\varphi(m_i)}{u} = 0$ for all $i = 1, \ldots, l$. By definition there exist therefore elements $s_1, \ldots, s_l \in S$ such that $s_i \cdot \varphi(m_i) = 0$ for $i = 1, \ldots, l$. With $s = s_1 \cdots s_l \in S$ we therefore get

$$s \cdot \varphi(m_i) = 0 \quad \forall\, i = 1, \ldots, l.$$

Since $m_1, \ldots, m_l$ is a generating set of M, we deduce, that the morphism $s \cdot \varphi$ is the zero-morphism, and hence

$$\frac{\varphi}{u} = \frac{s \cdot \varphi}{s \cdot u} = 0.$$

But then the Kernel of Φ is zero and Φ is injective.

We next want to show that Φ is surjective. For this we choose some

$$\psi \in \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

There are $n_i \in N$ and $s_i \in S$ such that

$$\psi\left(\frac{m_i}{1}\right) = \frac{n_i}{s_i} = \frac{n'_i}{s},$$

where $s = s_1 \cdots s_l$ and $n'_i = \frac{n_i \cdot s}{s_i}$. For arbitrary $a_1, \ldots, a_l \in R$ we therefore get

$$s \cdot \psi\left(\frac{\sum_{i=1}^l a_i m_i}{1}\right) = s \sum_{i=1}^l a_i \cdot \psi\left(\frac{m_i}{1}\right) = \frac{\sum_{i=1}^l a_i \cdot n'_i}{1}. \tag{3.1}$$

Let now $v_i = (v_{i1}, \ldots, v_{il})$. The exactness of the free presentation of M induces

$$0 = (\beta \circ \alpha)(e'_i) = \beta(v_i) = \sum_{j=1}^l v_{ij} \cdot m_j.$$

Applying $s \cdot \psi$ we get

$$0 = s \cdot \psi \left(\frac{\sum_{j=1}^{l} v_{ij} \cdot m_j}{1} \right) = \frac{\sum_{j=1}^{l} v_{ij} \cdot n'_j}{1}.$$

This fraction being zero means that there exists a $u_i \in S$ such that $u_i \cdot \sum_{j=1}^{l} v_{ij} \cdot n'_j = 0$, and setting $u = u_1 \cdots u_k$ we get

$$u \cdot \sum_{j=1}^{l} v_{ij} \cdot n'_j = 0.$$

Since the kernel of β is generated by $v_1, \ldots, v_k$ we deduce that actually

$$u \cdot \sum_{j=1}^{l} a_j \cdot n'_j = 0 \quad \forall\, a = (a_1, \ldots, a_l) \in \ker(\beta) = \langle v_1, \ldots, v_k \rangle.$$

If now $\sum_{i=1}^{l} a_i m_i = \sum_{i=1}^{l} b_i m_i$, then $(a_1 - b_1, \ldots, a_l - b_l) \in \ker(\beta)$ and we get

$$u \cdot \sum_{j=1}^{l} a_j \cdot n'_j = u \cdot \sum_{j=1}^{l} b_j \cdot n'_j.$$

This shows that the map

$$\varphi : M \longrightarrow N : \sum_{i=1}^{l} a_i \cdot m_i \mapsto u \cdot \sum_{i=1}^{l} b_i \cdot n'_i$$

is well-defined, and it is obviously R-linear. By (3.1) we have $u \cdot s \cdot \psi = S^{-1}\varphi$, and we thus get

$$\psi = \frac{u \cdot s \cdot \psi}{u \cdot s} = \frac{S^{-1}\varphi}{u \cdot s} \in \mathrm{Im}(\Phi).$$

Hence, the map Φ is surjective. □

Corollary 3.15. *Let M be finitely presented. Then:*

$$M \text{ is projective} \iff M \text{ is locally free}$$

whereas locally free *means M_P is free* $\forall P \in \mathrm{Spec}(R)$.

Proof.

- "$\Longrightarrow$": Assume M is projective

  $\Longrightarrow \exists\, N$, s.t. $M \oplus N \cong \bigoplus_{\lambda \in \Lambda} R$ is free

  $\Longrightarrow M_P \oplus N_P \cong \bigoplus_{\lambda \in \Lambda} R_P$

  $\Longrightarrow M_P$ is projective and by 2.39 we have that M_P is free.

- ”$\Longleftarrow$“: We know that if $N \xrightarrow{\varphi} N'$, then $N_P \xrightarrow{\varphi_P} N'_P$. And since (M_P free $\Longrightarrow$ M_P projective) and M finitely presented, we have that:

$$\begin{tikzcd} \mathrm{Hom}_{R_P}(M_P, N_P) \arrow[r, "(\varphi_P)_*", two heads] & \mathrm{Hom}_{R_P}(M_P, N_P) \\ (\mathrm{Hom}_R(M,N))_P \arrow[r, "(\varphi_*)_P"] \arrow[u, leftrightarrow, "\cong"'] & (\mathrm{Hom}_R(M,N))_P \arrow[u, leftrightarrow, "\cong"] \end{tikzcd}$$

commutes.

$\Longrightarrow$ $(\varphi_*)_P$ is surjective $\forall\, P \in \mathrm{Spec}(R)$

$\Longrightarrow$ φ_* is surjective

$\Longrightarrow$ M is projective.

□

Example 3.16. Let $I = \langle 2, 1 - \sqrt{-5} \rangle \trianglelefteq \mathbb{Z}[\sqrt{-5}]$, then I is projective, but not free.

Proof. Exercise. □

Proposition 3.17 (Flatness is a local property)**.** *Let M be an R-module, then the following are equivalent:*

(a) *M is flat as an R-module*

(b) *M_P is flat as R_P-module* $\forall P \in \mathrm{Spec}(R)$

(c) *$M_{\mathfrak{m}}$ is flat as $R_{\mathfrak{m}}$-module* $\forall \mathfrak{m} \in \mathfrak{m} - \mathrm{Spec}(R)$

Proof. Exercise. □

4. Chain conditions

A). Noetherian and Artinian rings and modules

Definition 4.1. Let R be any ring, M an R-module

(a) M is a *noetherian R-module* $:\Longleftrightarrow$ M satisfies the ACC (*ascending chain condition*) on submodules, i.e.:

$$\forall\, M_1 \subseteq M_2 \subseteq ..., M_i \leq M : \exists\, n : M_i = M_n \forall\, i \geq n$$

$\overset{!}{\Longleftrightarrow}$ every non-empty set of submodules of M has a maximal element.

(b) M is an *artinian R-module* $:\Longleftrightarrow$ M satisfies the DCC (*descending chain condition*) on submodules, i.e.:

$$\forall\, M_1 \supseteq M_2 \supseteq ..., M_i \leq M : \exists\, n : M_i = M_n \forall i \geq n$$

$\overset{!!}{\Longleftrightarrow}$ Every non-empty set of submodules of M has a minimal element.

(c) R is a *noetherian* (rsp. *artinian*) *ring* $:\Longleftrightarrow$ R is noetherian (rsp. artinian) as an R-module $\Longleftrightarrow$ R satisfies ACC (or DCC) on ideals

(d) A *composition series* of M is a finite strict chain

$$0 = M_n < M_{n-1} < \ldots < M_0 = M$$

of submodules of M that cannot be refined. We call n the *length* of the composition series. Note that in such a chain the quotient of two successive submodules is simple.

(e) We define the *length* of M

$$\operatorname{length}(M) := \sup\{n \mid M \text{ has a composition series of length } n\} \in \mathbb{N} \cup \{\infty\}$$

as the maximal length of a composition series, if one exists, respectively ∞ otherwise.

Proof of the equivalence denoted by ! and !!: Suppose first that there is a set X of submodules of M without a maximal element, then this can be used to create an ascending chain of submodules which does not become stationary. If conversely every set of submodules of M has a maximal element and $M_1 \subseteq M_2 \subseteq \ldots$ is an ascending chain of submodules of M, then $\{M_i \mid i \geq 1\}$ has a maximal element, say M_n, and it follows $M_i = M_n$ for all $i \geq n$. This proves the equivalence denoted by !, and that denoted by !! follows analogously. □

Example 4.2.

(a) Fields are noetherian and artinian as rings

(b) V a K-vector space, then:

$$\dim_K V = \text{length}(V) < \infty \iff V \text{ noetherian } \iff V \text{ artinian}$$

since $M \subsetneq M' \iff \dim(M) < \dim(M')$

(c) $\mathbb{Z}/_{n\mathbb{Z}}, n > 0$ as $\mathbb{Z}$-module is noetherian and artinian

(d) $K[x_i \,|\, i \in \mathbb{N}] := \bigcup_{n=0}^{\infty} K[x_0, \cdots, x_n]$ is neither noetherian nor aritinian, since:

$$\langle x_0 \rangle \subsetneq \langle x_0, x_1 \rangle \subsetneq \langle x_0, x_1, x_2 \rangle \subsetneq ...$$

$$\langle x_0 \rangle \supsetneq \langle x_0^2 \rangle \supsetneq \langle x_0^3 \rangle \supsetneq ...$$

Proposition 4.3. *Let M be an R-module. Then:*

$$M \textit{ is noetherian} \iff \textit{every submodule of } M \textit{ is finitely generated}$$

Proof.

- "$\Longrightarrow$": Suppose $N \leq M$ is not finitely generated, choose $0 \neq m_0 \in N$ and recursively choose $m_i \in N \backslash \langle m_0, ..., m_{i-1} \rangle$. Then:

$$\langle m_0 \rangle \subsetneq \langle m_0, m_1 \rangle \subsetneq ... \lightning$$

- $\Longleftarrow$": Let $M_1 \subseteq M_2 \subseteq M_3 \subseteq ...$ with $M_i \leq M$. Define

$$\tilde{M} := \bigcup_{i=1}^{\infty} M_i \leq M$$

Then by assumption $\tilde{M} = \langle m_1, ..., m_n \rangle$ and thus $\exists j : m_1, ..., m_n \in M_j$ and finally: $M_k = M_j = \tilde{M} \,\forall\, k \geq j$.

□

Example 4.4. Let R be a P.I.D., but not a field. Then R is noetherian, but not artinian. Choose $0 \neq p \in R$, such that p is irreducible (or $p \in R \backslash R^*$). Then

$$\langle p \rangle \supsetneq \langle p^2 \rangle \supsetneq \langle p^3 \rangle \supsetneq ...$$

In particular: $\mathbb{Z}, K[x], \mathbb{Z}[i], K[\![x]\!]$ are all noetherian and not artinian.

Proposition 4.5. *Let* $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ *be an exact sequence of R-linear maps. Then:*

(a) M is noetherian $\Longleftrightarrow$ M' and M'' are noetherian

(b) M is artinian $\Longleftrightarrow$ M' and M'' are artinian

Proof.

(a)

- "$\Longrightarrow$": First we show that M' is noetherian:

  Suppose $M_0 \subsetneq M_1 \subsetneq ..., M_i \leq M'$. Then $\alpha(M_0) \subsetneq \alpha(M_1) \subsetneq ... \lightning$, since M is noetherian.

  Now we show that M'' is noetherian:

  Suppose $M_0 \subseteq M_1 \subseteq M_2 \subseteq ..., M_i \leq M''$. Then $\beta^{-1}(M_0) \subseteq \beta^{-1}(M_1) \subseteq \beta^{-1}(M_2) \subseteq ...$ are submodules of M and by assumption:

  $$\begin{aligned} \exists\, j :& \beta^{-1}(M_j) = \beta^{-1}(M_i)\, \forall i \geq j \\ \Longrightarrow& \beta(\beta^{-1}(M_j)) = \beta(\beta^{-1}(M_i))\, \forall i \geq j \\ \Longrightarrow& M_j = M_i\, \forall i \geq j \end{aligned}$$

  Thus M'' is noetherian

- "$\Longleftarrow$": Let $M_1 \subseteq M_2 \subseteq M_3 \subseteq ..., M_i \leq M$. Then by assumption there exists a k, such that $\forall i \geq k$ we have $\alpha^{-1}(M_i) = \alpha^{-1}(M_k)$ and $\beta(M_i) = \beta(M_k)$. Now we need to show that $M_k = M_i\, \forall\, i \geq k$, in particular we need to show "$\supseteq$":

  Let $m \in M_i$

  $$\begin{aligned} &\Longrightarrow \beta(m) \in \beta(M_i) = \beta(M_k) \\ &\Longrightarrow \exists \tilde{m} \in M_k : \beta(\tilde{m}) = \beta(m) \\ &\Longrightarrow \tilde{m} - m \in \ker(\beta) = \operatorname{Im}(\alpha) \text{ and } \tilde{m} - m \in M_i \text{ since } M_k \subseteq M_i \\ &\Longrightarrow \exists m' \in \alpha^{-1}(M_i) = \alpha^{-1}(M_k) : \alpha(m') = \tilde{m} - m \\ &\Longrightarrow m = \underbrace{\tilde{m}}_{\in M_k} - \underbrace{\alpha(m')}_{\in M_k} \in M_k \end{aligned}$$

(b) Analagous

□

Example 4.6.

(a)

$$\begin{aligned}\mathbb{Z}_{p^\infty} &:= \left\{ \left[\frac{a}{b}\right] \in \mathbb{Q}/\mathbb{Z} \,|\, \mathrm{ord}(\left[\frac{a}{b}\right]) = p^n, n \geq 0 \right\}, p \in \mathbb{P} \\ &= \left\{ \left[\frac{a}{p^n}\right] \in \mathbb{Q}/\mathbb{Z} \,|\, a \in \{0, ..., p^n - 1\}, n \geq 0 \right\}\end{aligned}$$

is artinian, but not noetherian (the so-called *Prüfer group*). To prove this, we claim that:

$$N \lneqq \mathbb{Z}_{p^\infty} \text{ a } \mathbb{Z}\text{- submodule} \iff \exists\, n \in \mathbb{N} : N = \left\langle \left[\frac{1}{p^n}\right] \right\rangle_{\mathbb{Z}} =: N_n$$

Proof.

- "$\Longleftarrow$": ✓
- "$\Longrightarrow$": Let $\left[\frac{a}{p^n}\right] \in N$, such that $p \nmid a$.

$$\begin{aligned}&\Longrightarrow \gcd(a, p^n) = 1 \\ &\Longrightarrow \exists\, b, q \in \mathbb{Z} : 1 = ba + qp^n \\ &\Longrightarrow \left[\frac{1}{p^n}\right] = b\left[\frac{a}{p^n}\right] + q\underbrace{\left[\frac{p^n}{p^n}\right]}_{=0} = b\left[\frac{a}{p^n}\right] \in N \\ &\Longrightarrow \left\langle \left[\frac{1}{p^n}\right] \right\rangle \subseteq N\end{aligned}$$

  We now have to consider two cases:

  (1) $\exists\, n$ maximal, such that there exists $\left[\frac{a}{p^n}\right] \in N$ with $p \nmid a$. Then

$$N = \left\langle \left[\frac{1}{p^n}\right] \right\rangle_{\mathbb{Z}}$$

  (2) $\left\langle \left[\frac{1}{p^n}\right] \right\rangle \subseteq N \,\forall n \geq 0$. Then:

$$\mathbb{Z}_{p^\infty} = \bigcup_{n=0}^{\infty} \left\langle \left[\frac{1}{p^n}\right] \right\rangle \subseteq N \;\lightning_{N \lneqq \mathbb{Z}_{p^\infty}}$$

□

Note.

$$N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq \mathbb{Z}_{p^\infty}$$

$\Longrightarrow$ $\mathbb{Z}_{p^\infty}$ is artinian (every descending chain is a "subchain" of this) but not noetherian (the chain above does not become stationary).

In particular, $\mathbb{Z}_{p^\infty}$ is not finitely generated (by 4.5).

(b) The sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{a \mapsto \frac{a}{1}} \mathbb{Z}_p \xrightarrow{\frac{a}{p^n} \mapsto \left[\frac{a}{p^n}\right]} \mathbb{Z}_{p^\infty} \longrightarrow 0$$

is exact, so by 4.3, 4.4 and the above example $\mathbb{Z}_p$ is neither noetherian nor artinian as a $\mathbb{Z}$-module

Corollary 4.7. *Let $M_1, ..., M_n, M$ be R-modules*

(a) $M_1, ..., M_n$ are noetherian (rsp. artinian)

$$\Longrightarrow M_1 \oplus \cdots \oplus M_n \textit{ is noeth. (rsp. artinian)}$$

(b) R is a noetherian (rsp. artinian) ring, M is a finitely gen. R-module

$$\Longrightarrow M \textit{ is noeth. (rsp. artinian)}$$

(c) R noetherian and M finitely generated, then M is finitely presented.

Proof.

(a) We do an induction on n:

$$0 \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow M_n \longrightarrow 0$$

is exact. Since $\bigoplus_{i=1}^{n-1} M_i$ is noeth./artin. by induction and M_n is noeth./artin. by assumption, we know by 4.5 that $\bigoplus_{i=1}^{n} M_i$ is noetherian (rsp. artinian).

(b) $M = \langle m_1, ..., m_n \rangle_R$. Then:

$$0 \longrightarrow \ker(\alpha) \longrightarrow R^n \overset{\alpha}{\twoheadrightarrow} M \longrightarrow 0$$

is exact and by (a) R^n is noetherian (rsp. artinian). Thus, by 4.5, M is noetherian (rsp. artinian).

(c) If $M = \langle m_1, \ldots, m_n \rangle_R$ then the map

$$\alpha : R^n \longrightarrow M : e_i \mapsto m_i$$

has a finitely generated kernel, say $\ker(\alpha) = \langle k_1, \ldots, k_l \rangle$, since R^n is noetherian. Thus the sequence

$$R^l \xrightarrow{\beta} R^n \xrightarrow{\alpha} M \longrightarrow 0$$

with $\beta(e_j) = k_j$ is exact and thus a finite presentation of M.

$\square$

Proposition 4.8. *Let R be a noetherian (artinian) ring, $S \subseteq R$ multipl. closed and $I \trianglelefteq R$. Then:*

(a) ${}^{R}\!/_{I}$ *is a noetherian (artinian) ring*

(b) $S^{-1}R$ *is a noetherian (artinian) ring*

Proof.

(a) clear, since any ideal $J \trianglelefteq {}^{R}\!/_{I}$ corresponds to an ideal $\tilde{J} \trianglelefteq R$ with $I \subseteq J$ and vice versa.

(b) Let $J_0 \subseteq J_1 \subseteq J_2 \subseteq ..., J_i \trianglelefteq S^{-1}R$.

$$\begin{aligned}
&\Longrightarrow J_0^c \subseteq J_1^c \subseteq J_2^c \subseteq ..., J_i^c \trianglelefteq R \\
&\Longrightarrow \exists\, k : J_k^c = J_i^c \,\forall\, i \geq k, \text{ since } R \text{ is noeth.} \\
&\Longrightarrow \quad \underbrace{(J_k^c)^e}_{=J_k \text{ by } 3.2} = \underbrace{(J_i^c)^e}_{=J_i} \forall i \geq k \\
&\Longrightarrow J_k = J_i \,\forall i \geq k
\end{aligned}$$

Analogously for artinian.

□

B). Noetherian Rings

Theorem 4.9 (Hilbert's Basis Theorem)**.**

$$R \text{ noetherian} \implies R[x] \text{ noetherian}$$

Proof. Notation: Let $0 \neq f = \sum_{i=1}^{n} f_i x^i \in R[x], f_i \in R, f_n \neq 0$. Then let

$$f_n =: \mathrm{lc}(f) \text{ the } \textit{leading coefficent}$$

Let $J \trianglelefteq R[x], J \neq 0 \implies I := \langle \mathrm{lc}(f) \,|\, 0 \neq f \in J \rangle_R \trianglelefteq R$. So, since R is noetherian, there exist $f_1, ..., f_k \in J$, such that

$$I = \langle \mathrm{lc}(f_1), \cdots, \mathrm{lc}(f_k) \rangle_R$$

Our claim is now that

$$J = \langle f_1, \cdots, f_k \rangle_{R[x]} + (\langle 1, x, x^2, \cdots, x^{d-1} \rangle_R \cap J)$$

as R-modules, where $d = \max\{\deg(f_i) \,|\, i = 1..k\}$

- "$\supseteq$": ✓
- "$\subseteq$": We have to show that for all $f \in J$ there exists $r \in J$ such that $f - r \in \langle f_1, \cdots, f_k \rangle_{R[x]}$ and $\deg(r) < d$. For that we do an induction on $\deg(f)$:

– $\deg(f) = d = 0 : f = \mathrm{lc}(f) \in I = \langle f_1 = \mathrm{lc}(f_1), \cdots, f_k = \mathrm{lc}(f_k)\rangle \subseteq \langle f_1, \cdots, f_k\rangle_{R[x]} \implies r := 0$

– $\deg(f) < d : \implies r := f$

– $\deg(f) \geq d$: Since $\mathrm{lc}(f) \in I$ there exist $a_i \in R$. such that

$$\mathrm{lc}(f) = \sum_{i=1}^{k} a_i \mathrm{lc}(f_i)$$

Set

$$f' := f - \sum_{i=1}^{k} a_i f_i x^{\deg(f)-\deg(f_i)}$$

Then $\deg(f') < \deg(f)$ and by induction there exists an $r \in J$, such that:

$$f' - r \in \langle f_1, \cdots, f_k\rangle_{R[x]}, \deg(r) < \deg(f') < \deg(f)$$

$$\implies f - r = (f' - r) + \sum_{i=1}^{k} a_i f_i x^{\deg(f)-\deg(f_i)} \in \langle f_1, \cdots, f_k\rangle_{R[x]}$$

and $\deg(r) < \deg(f)$.

Thus we get: Since $\langle 1, x, x^2, x^3, \cdots, x^{d-1}\rangle$ is a finitely generated R-module and R is noetherian, it is also a noetherian R-module and by 4.5:

$$\underbrace{\langle 1, x, x^2, x^3, \cdots, x^{d-1}\rangle_R \cap J}_{=\langle g_1, \cdots, g_l\rangle_R \text{ by } 4.3}$$

is a noetherian R-module and thus finitely generated.

$$\implies J = \langle f_1, \cdots, f_k, g_1, \cdots, g_l\rangle_{R[x]}$$

is finitely generated and therefore $R[x]$ is noetherian.

□

Corollary 4.10.

- *K field $\implies K[x_1, ..., x_n]$ noetherian*
- *R noeth. $\implies R[x_1, ..., x_n]$ noetherian*

Remark 4.11. *Is $K[\![x_1, \cdots, x_n]\!]$ noetherian? Yes! Using the Weyerstraß-Division Theorem one reduces the proof to $K[\![x_1, \cdots, x_{n-1}]\!][x_n]$ being noetherian!*

Skipped: 4.12.

Skipped: 4.13.

Skipped: 4.14.

Proposition 4.15.

$$R \textit{ noeth.} \implies \mathfrak{N}(R) \textit{ nilpotent} \implies \exists\, n \geq 1 : \mathfrak{N}(R)^n = 0$$

Proof. R noeth.

$$\begin{aligned} &\Longrightarrow \mathfrak{N}(R) \text{ is finitely generated.} \Longrightarrow \qquad \mathfrak{N}(R) = \langle a_1, \cdots, a_k \rangle_R \\ &\Longrightarrow \exists \alpha_i : a_i^{\alpha_i} = 0 \,\forall\, i \end{aligned}$$

Now let $n := \max\{\alpha_i, i = 1..k\}$, then $(\sum_{i=1}^k b_i a_i)^{kn} = 0$. □

C). Artinian rings

Definition 4.16 (will be used again from 6.17 on)**.** Let R be a ring, then

$$\dim(R) := \sup\{n \in \mathbb{N} \,|\, \exists\, P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n, P_i \in \operatorname{Spec}(R)\}$$

is the *Krull dimension* of R.

Example 4.17.

(a) K a field $\implies \dim(K) = 0$

(b) R a P.I.D., R not a field $\implies \dim(R) = 1$.

In particular: $\dim(\mathbb{Z}) = \dim(K[x]) = \dim(K[\![x]\!]) = \dim(\mathbb{Z}[i]) = 1$

Proposition 4.18. *If $0 \neq R$ is artinian, then:*

$$\dim(R) = 0$$

$(\iff \mathfrak{m} - \operatorname{Spec}(R) = \operatorname{Spec}(R))$. *In particular:* $\mathfrak{N}(R) = J(R)$

Proof. $P \in \operatorname{Spec}(R) \implies R/P$ is artinian by 4.8. We claim, that R/P is actually a field:

Let $0 \neq \overline{a} \in R/P \overset{\text{artin.}}{\Longrightarrow} \exists\, n : \langle \overline{a}^n \rangle = \langle \overline{a}^{n+1} \rangle$

$$\begin{aligned} &\Longrightarrow \overline{a}^n \in \langle \overline{a}^{n+1} \rangle \\ &\Longrightarrow \exists\, \overline{b} : \overline{1} \cdot \overline{a}^n = \overline{a}^n = \overline{b}\overline{a}^{n+1} = \overline{b}\overline{a} \cdot \overline{a}^n \\ &\Longrightarrow \overline{1} = \overline{b}\overline{a} \text{ since } R/P \text{ is an I.D.} \end{aligned}$$

Thus R/P is a field. □

Proposition 4.19.
$$R \text{ artinian } \implies |\mathfrak{m} - \mathrm{Spec}(R)| < \infty$$

Proof. W.l.o.g. $R \neq 0$.

$$\begin{aligned}
&\implies M := \{\mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_k \mid k \geq 1, \mathfrak{m}_i \lhd \cdot R\} \neq \emptyset \\
&\overset{R \text{ artin.}}{\implies} \exists\, \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_k \in M \text{ minimal with respect to inclusion} \\
&\implies \forall\, \mathfrak{m} \lhd \cdot R : \mathfrak{m} \supseteq \mathfrak{m} \cdot \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_k = \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_k \text{ (by minimality)} \\
&\overset{\mathfrak{m} \text{ prime}}{\implies} \exists\, i : \mathfrak{m}_i \subseteq \mathfrak{m} \\
&\overset{\mathfrak{m}_i \text{ max.}}{\implies} \mathfrak{m}_i = \mathfrak{m}
\end{aligned}$$

□

Proposition 4.20.

$$R \text{ artinian} \implies \mathfrak{N}(R) = J(R) \text{ is nilpotent}$$

Proof. We have:
$$\mathfrak{N}(R) \supseteq \mathfrak{N}(R)^2 \supseteq \mathfrak{N}(R)^3 \supseteq \ldots$$
So, since R is artinian, there exists an n, such that $\mathfrak{N}(R)^n = \mathfrak{N}(R)^k =: I \,\forall\, k \geq n$.

Suppose $I \neq 0$
$$\implies M := \{J \trianglelefteq R \mid J \cdot I \neq 0\} \neq \emptyset$$
since $\mathfrak{N}(R) \in M$.

$$\begin{aligned}
&\implies \exists J_0 \in M \text{ minimal} \\
&\implies \exists 0 \neq a \in J_0 : a \cdot I \neq 0 \\
&\implies \langle a \rangle \in M, \text{ and since } J_0 \text{ is minimal:} \\
&\implies J_0 = \langle a \rangle
\end{aligned}$$

Now we get:

$$\begin{aligned}
&(a \cdot I) \cdot I = a \cdot I^2 \overset{I=I^2}{=} a \cdot I \neq 0 \\
&\implies a \cdot I \in M, \text{ and since } a \cdot I \subseteq \langle a \rangle : \\
&\implies \langle a \rangle = a \cdot I \\
&\implies \exists\, b \in I : a = ab = (ab)b = ab^2 = ab^k \,\forall k \geq 1 \text{ by induction} \\
&\implies \exists\, k : a = a \cdot b^k = a \cdot 0 = 0 \,\lightning
\end{aligned}$$

since $b \in I$ and $I \subseteq \mathfrak{N}(R)$. □

Lemma 4.21. *If there are* $\mathfrak{m}_1, \cdots, \mathfrak{m}_k \lhd \cdot R$*, such that* $\mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_k = 0$*, then:*

$$R \text{ is artinian} \iff R \text{ is noetherian}$$

Note. The $\mathfrak{m}_i$ are not necessarily pairwise different!

Proof. We do an induction on k. For $k = 1$ R is a field and the statement holds trivially. So assume the statement is true for $k-1$ and $\mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_k = 0$.

Let $I_{k-1} = \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_{k-1}$ and $I_k = \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_k = 0$.

$$\begin{aligned}
&\Longrightarrow I_{k-1} = {}^{I_{k-1}}\!/_{I_k} \text{ is an } {}^{R}\!/_{\mathfrak{m}_k}\text{- vector space}\\
&\overset{4.2(b)}{\Longrightarrow} ({}^{I_{k-1}}\!/_{I_k} \text{ is a noeth. } {}^{R}\!/_{\mathfrak{m}_k} \text{ - module} \iff {}^{I_{k-1}}\!/_{I_k} \text{ is an artin. } {}^{R}\!/_{\mathfrak{m}_k} \text{ - module})\\
&\Longrightarrow ({}^{I_{k-1}}\!/_{I_k} \text{ is a noeth. } R \text{ - module} \iff {}^{I_{k-1}}\!/_{I_k} \text{ is an artin. } R \text{ - module})\\
&\Longrightarrow (I_{k-1} \text{ is a noeth. } R \text{ - module} \iff I_{k-1} \text{ is an artin. } R \text{ - module})
\end{aligned}$$

By 1:1 - correspondence of prime (and maximal) ideals $\overline{\mathfrak{m}}_1, ..., \overline{\mathfrak{m}}_{k-1} \lhd \cdot {}^{R}\!/_{I_{k-1}}$ and $\overline{\mathfrak{m}}_1 \cdot \ldots \cdot \overline{\mathfrak{m}}_{k-1} = \overline{0}$. Hence by induction ${}^{R}\!/_{I_{k-1}}$ is noetherian if and only if it is artinian. Now consider the exact sequence

$$0 \longrightarrow I_{k-1} \hookrightarrow R \twoheadrightarrow {}^{R}\!/_{I_{k-1}} \longrightarrow 0$$

By the considerations above and 4.5 follows the statement. □

Theorem 4.22 (Theorem of Hopkins)**.**

$$R \text{ is artinian } \iff (R \text{ is noetherian and } \dim(R) = 0)$$

Proof.

- "$\Longrightarrow$": By 4.19 $\mathfrak{m} - \operatorname{Spec}(R) = \{\mathfrak{m}_1, \cdots, \mathfrak{m}_k\}$

$$\overset{4.20}{\Longrightarrow} \exists n : 0 = \mathfrak{N}(R)^n = J(R)^n = (\bigcap_{i=1}^{k} \mathfrak{m}_i)^n \supseteq \bigcap_{i=1}^{k} \mathfrak{m}_i^n \supseteq \mathfrak{m}_1^n \cdot \ldots \mathfrak{m}_k^n$$

$$\overset{4.21}{\Longrightarrow} R \text{ is noeth.}, \dim(R) = 0 \text{ by } 4.18$$

- "$\Longleftarrow$": postponed

□

Theorem 4.23 (Structure Thm. for artinian rings)**.** *If R is artinian, then:*

$$R \cong \bigoplus_{i=1}^{k} R_i$$

with R_i local and artinian.

Moreover, the decomposition is unique, i.e.: If $R \cong \bigoplus_{j=1}^{l} S_j$ with S_j local, artinian, then $l = k$ and $\exists\, \Pi \in \mathbb{S}_k$:

$$R_i \cong S_{\Pi(i)}$$

Note that the decompositon can actually be described as

$$R \cong \bigoplus_{\mathfrak{m} \in \mathfrak{m}-\mathrm{Spec}(R)} R_{\mathfrak{m}}.$$

Proof.

(a) (Existence:)

By 4.19 $\mathfrak{m} - \mathrm{Spec}(R) = \{\mathfrak{m}_1, \cdots, \mathfrak{m}_k\}$. We claim:

$$\mathfrak{m}_i^n + \mathfrak{m}_j^n = R\ \forall\, n \geq 1, i \neq j$$

Suppose this is not true. Then there exists $\mathfrak{m} \lhd \cdot R$, such that $\mathfrak{m}_i^n + \mathfrak{m}_j^n \subseteq \mathfrak{m}$ and since $\mathfrak{m}$ is prime: $\mathfrak{m}_i, \mathfrak{m}_j \subseteq \mathfrak{m}$ and thus $\mathfrak{m}_i = \mathfrak{m} = \mathfrak{m}_j$ ↯

Thus, by 4.20 there exists an n, such that

$$0 = J(R)^n = (\bigcap_{i=1}^{k} \mathfrak{m}_i)^n \supseteq \bigcap_{i=1}^{k} (\mathfrak{m}_i^n) \supseteq \mathfrak{m}_1^n \cdot \ldots \cdot \mathfrak{m}_k^n$$

$$\Longrightarrow \bigcap_{i=1}^{k} \mathfrak{m}_i^n = \mathfrak{m}_1^n \cdot \ldots \cdot \mathfrak{m}_k^n = 0$$

$$\Longrightarrow R \cong R \big/ \bigcap_{i=1}^{k} \mathfrak{m}_i^n \cong \bigoplus_{i=1}^{k} R/\mathfrak{m}_i^n \text{ by 1.12}$$

and $R/\mathfrak{m}_i^n$ is local and artinian.

Note moreover, that

$$R_{\mathfrak{m}_i} \cong \bigoplus_{j=1}^{k} \left(R/\mathfrak{m}_j^n\right)_{\mathfrak{m}_i} \cong R/\mathfrak{m}_i^n,$$

since $\left(R/\mathfrak{m}_j^n\right)_{\mathfrak{m}_i} = 0$ if $j \neq i$ and $\left(R/\mathfrak{m}_j^n\right)_{\mathfrak{m}_i} \cong R/\mathfrak{m}_i^n$ if $j = i$.

(b) (Uniqueness:) Postponed to 5.22

□

Example 4.24.

(a) $R = {}^{K[x]}\!\big/_{\langle x^2\rangle}$, $\mathrm{Spec}(R) = \{\langle \overline{x} \rangle\}$. This ring is artinian by Hopkins.

(b) $\dim(R) = 0 \not\Rightarrow R$ is noetherian:

Let $S := K[x_i \,|\, i \in \mathbb{N}], I := \langle x_0, x_1^2, x_2^2, \cdots \rangle$ and $R := {}^{S}\!\big/_{I}$. Claim: $\mathrm{Spec}(R) = \{\langle \overline{x_0}, \overline{x_1}, \cdots \rangle\}$:

If ${}^{P}\!\big/_{I}$ is prime

$$\begin{aligned}&\Longrightarrow (\overline{x_i}^i = \overline{0} \in {}^{P}\!\big/_{I} \Longrightarrow \overline{x_i} \in {}^{P}\!\big/_{I})\\ &\Longrightarrow \langle \overline{x_0}, \overline{x_1}, \cdots \rangle \subseteq {}^{P}\!\big/_{I}\\ &\Longrightarrow \dim(R) = 0\end{aligned}$$

But R is not noetherian, since:

$$\langle \overline{x_0} \rangle \subsetneq \langle \overline{x_0} . \overline{x_1} \rangle \subsetneq \langle \overline{x_0}, \overline{x_1}, \overline{x_2} \rangle \subsetneq ...$$

(c) R noetherian $\not\Rightarrow \dim(R) < \infty$:

$A := K[x_i, 0 \neq i \in \mathbb{N}], m_n = \frac{n(n+1)}{2}, P_n := \langle x_{m_n+1}, \cdots, x_{m_{n+1}} \rangle \in \mathrm{Spec}(A)$.

$S := A \setminus \bigcup_{n=0}^{\infty} P_n, R := S^{-1}A$

Then R is noetherian, but $\dim(R) = \infty$.

D). Modules of finite length

Theorem 4.25 (Theorem of Jordan-Hölder)**.** *If an R-module M has a composition series, then all composition series have the same length* length(M) *and every strict chain of submodules can be refined to a composition series.*

Proof. We denote by

$$l(M) := \min\{n \mid M \text{ has a composition series of length } n\}$$

the minimal length of a composition series of M.

We claim that $l(N) < l(M)$ holds for every strict submodule $N < M$. For this we consider a composition series

$$0 = M_n < M_{n-1} < \ldots < M_0 = M$$

of M of length $l(M) = n$, and we set $N_i := M_i \cap N \leq M_i$ for $i = 0, \ldots, n$. It follows that

$$\alpha_i : N_{i-1}/N_i = (M_{i-1} \cap N)/(M_i \cap N) \longrightarrow M_{i-1}/M_i : \overline{x} \mapsto \overline{x}$$

is a well-defined R-linear map and since M_{i-1}/M_i is simple, either $N_{i-1} = N_i$ or α_i is an isomorphism and N_{i-1}/N_i is simple. Omitting superflous terms the N_i define thus a composition series of N, which implies that $l(N) \leq n = l(M)$. Suppose now that we have the equality $l(N) = l(M)$, then no N_i was superflous and each α_i is an isomorphism. We claim that then $M_i = N_i$ for all $i = 0, \ldots, n$, leaving us with the contradition $N = N_0 = M_0 = M$. The proof of this claim works by descending induction on i, where $M_n = 0 = N_n$ gives the case $i = n$. If we now have $N_i = M_i$ and

$$\alpha_i : N_{i-1}/N_i = N_{i-1}/M_i \longrightarrow M_{i-1}/M_i : \overline{x} \mapsto \overline{x}$$

is an isomorphism, then obviously $N_{i-1} = M_{i-1}$, finishing the indcution. We have thus shown that $l(N) < l(M)$.

Suppose now that $M_k < M_{k-1} < \ldots < M_0$ is any strict chain of submodules in M, then due to

$$0 \leq l(M_k) < l(M_{k-1}) < \ldots < l(M_0) \leq l(M)$$

we must have $k \leq l(M)$. On the other hand, if the chain is a composition series, then $k \geq l(M)$ by the definition of $l(M)$. This shows that all composition series have the same length, which then is $\mathrm{length}(M)$ by definition.

It remains to show that any strict chain

$$M_k < M_{k-1} < \ldots < M_0$$

of submodules can be refined to a composition series. We have already seen that $k \leq l(M) = \mathrm{length}(M)$. If the chain is not yet a composition series, we can refine it and its length will still be bounded by $l(M)$, so that we can do so only finitely many times. But once it cannot be refined anymore, it is a composition series. □

Corollary 4.26. *An R-module M has finite length if and only if it is artinian and noetherian.*

Proof. If M has finite length then by the Theorem of Jordan-Hölder every chain of submodules of M has at most length $\mathrm{length}(M)$. Thus there are no infinite descending or ascending chains of submodules, and M is artinian and noetherian.

Suppose now conversely that M is artinian and noetherian. Then the set of strict submodules of $M_0 := M$ has a maximal element M_1, since M is noetherian. By maximality the quotient M_0/M_1 is simple. Moreover, M_1 is noetherian as well and if it is non-zero, we can find in the same way a maximal strict submodule M_2 of M_1. Continuing in this way we construct a descending chain of submodules

$$M_0 > M_1 > M_2 > \ldots$$

where every quotient M_{i-1}/M_i is simple. Since the module is artinian, the sequence must stop eventually, say with M_n, which implies that $M_n = 0$. But then

$$0 = M_n < M_{n-1} < \ldots < M_0 = M$$

is a composition series of M, and by the Theorem of Jordan-Hölder M has finite length. □

Corollary 4.27. *For a ring R the following are equivalent:*

(a) R is artinian.

(b) R is noetherian of dimension $\dim(R) = 0$.

(c) R has finite length as an R-module.

Proof. This follows immediately from Corollary 4.26 and the Theorem of Hopkins 4.22. □

5. Primary decomposition and Krull's Principle Ideal Theorem

A). Primary decomposition

Motivation. in $R = \mathbb{Z}$ we had

$$z = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$$

as prime factorisation, similarly in any U.F.D. How can we generalize this?

The problem is: In general we cannot find such a decomposition for each element. So maybe we could rephrase the above formula to

$$\langle z \rangle = \langle p_1^{n_1} \rangle \cap \cdots \cap \langle p_r^{n_r} \rangle$$

Our hope is, that any ideal $I \trianglelefteq R$ can be written as

$$I = Q_1 \cap \cdots \cap Q_r$$

with the Q_i somehow "uniquely" determined and a generalized notion of powers of prime ideals.

In a general ring this will fail. In a noetherian ring, however, this actually works! We will find Q_i, such that $\sqrt{Q_i}$ is a prime ideal. However, Q_i will only *contain* a prime power and uniqueness will only work up to a certain point

Definition 5.1. Let R be a ring, $Q \trianglelefteq R, I \trianglelefteq R$.

(a) Q is *primary*

$$\begin{aligned} &:\Longleftrightarrow Q \neq R \text{ and } (ab \in Q \implies a \in Q \text{ or } b \in \sqrt{Q}) \\ &\Longleftrightarrow Q \neq R \text{ and } (ab \in Q \implies a \in Q \text{ or } \exists\, n : b^n \in Q) \\ &\Longleftrightarrow R/Q \neq 0 \text{ and } (\bar{b} \in R/Q \text{ is a zero-divisor } \implies \bar{b} \text{ is nilpotent}) \end{aligned}$$

If Q is primary and $P = \sqrt{Q}$, we call Q *P-primary.*

(b) A *primary decomposition* (PD) of I is a finite collection of primary ideals $Q_1, \cdots, Q_n$, such that

$$I = Q_1 \cap \cdots \cap Q_n$$

(c) A primary decomposition is *minimal* $:\Longleftrightarrow$

(1) $\sqrt{Q_i} \neq \sqrt{Q_j}, i \neq j$

(2) $\bigcap_{i\neq j} Q_j \nsubseteq Q_i, \forall\, i = 1..n$

Note. $\sqrt{Q_i} \subsetneq \sqrt{Q_j}$ is allowed! (see 5.16)

Example 5.2. Let R be a U.F.D. Then $0 \neq Q = \langle q \rangle$ is primary $\iff \exists\, p \in R$ prime, $n \geq 1$, such that $q = p^n \cdot r, r \in R^*$

Proof. We show two directions:

- "$\Longleftarrow$":

$$\begin{aligned} ab \in Q &\implies p^n \mid ab \\ &\implies p^n \mid a \text{ or } p \mid b \\ &\implies a \in Q \text{ or } b \in \langle p \rangle = \sqrt{Q} \end{aligned}$$

- "$\Longrightarrow$": Let $q = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ be the prime factorization of q. Suppose $r > 1$ (otherwise we're done).

  Then $\underbrace{p_1^{\alpha_1}}_{=a} \cdot \underbrace{p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}}_{=b} \in Q$, but $a \notin Q, b \notin \langle p_1 \cdot \ldots \cdot p_r \rangle = \sqrt{Q}$ ↯.

$\square$

In particular:

- R P.I.D $\implies$ (Q primary $\iff \exists\, p$ prime, such that $Q = \langle p^n \rangle$)
- R U.F.D., $q = e \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ prime factorisation.

$$\implies \langle q \rangle = \bigcap_{i=1}^{r} \langle p_i^{\alpha_i} \rangle \text{ is a minimal PD.}$$

Proposition 5.3. *Let R be a ring, $Q \trianglelefteq R$ primary. Then $\sqrt{Q}$ is the smallest prime ideal containing Q*

Proof. Suppose $a, b \in \sqrt{Q}$

$$\begin{aligned} &\implies \exists\, n : a^n b^n = (ab)^n \in Q \\ &\implies a^n \in Q \text{ or } b^n \in \sqrt{Q} \\ &\implies a \in \sqrt{Q} \text{ or } b \in \sqrt{Q} \end{aligned}$$

Thus $\sqrt{Q}$ is prime. Since

$$\sqrt{Q} = \bigcap_{Q \subseteq P \text{ prime}} P$$

it is also the smallest prime ideal containing Q. $\square$

Lemma 5.4. *Let R be a ring, $S \subseteq R$ multipl. closed, $Q, Q' \trianglelefteq R$ with $Q, Q' \subsetneq R; I_1, \cdots, I_n, J \trianglelefteq R$*

(a) $\sqrt{Q}$ *is a maximal ideal* $\Longrightarrow Q$ *is* $\sqrt{Q}$*-primary*

(b) $\mathfrak{m} \lhd \cdot R \Longrightarrow \mathfrak{m}^n$ *is* $\mathfrak{m}$*-primary* $\forall\, n \geq 1$

(c) Q *is* P*-primary,* $a \in R \backslash Q \Longrightarrow (Q : a)$ *is* P*-primary*

(d) Q *is* P*-primary and*

(1) $S \cap P = \emptyset \Longrightarrow S^{-1}Q$ *is an* $S^{-1}P$*-primary ideal in* $S^{-1}R$ *and* $S^{-1}Q \cap R = Q$

(2) $S \cap P \neq \emptyset \Longrightarrow S^{-1}Q = S^{-1}R$

(e) Q, Q' *are* P*-primary* $\Longrightarrow Q \cap Q'$ *is* P*-primary.*

(f) $\sqrt{I_1 \cap \cdots \cap I_n} = \sqrt{I_1} \cap \cdots \cap \sqrt{I_n}$

(g) $(\bigcap_{i=1}^n I_i) : J = \bigcap_{i=1}^n (I_i : J)$

(h) $\sqrt{I_1 + \cdots + I_n} \supseteq \sqrt{I_1} + \cdots + \sqrt{I_n}$

Proof.

(a)
$$\sqrt{Q}/_{Q} = \bigcap_{\overline{P} \in \operatorname{Spec}(R/_{Q})} \overline{P} = \mathfrak{N}(R/_{Q}) \lhd \cdot R/_{Q}$$

$\Longrightarrow \operatorname{Spec}(R/_{Q}) = \left\{\sqrt{Q}/_{Q}\right\}$

$\Longrightarrow R/_{Q}$ is local $\Longrightarrow (R/_{Q})^* = R/_{Q} \backslash \sqrt{Q}/_{Q}$

$\Longrightarrow$ every zero-divisor of $R/_{Q}$ is nilpotent, i.e. is in $\sqrt{Q}/_{Q}$

$\Longrightarrow Q$ primary.

(b) $\sqrt{\mathfrak{m}^n} = \mathfrak{m} \lhd \cdot R$ and by (a) $\mathfrak{m}^n$ is $\mathfrak{m}$-primary

(c) We have to show: $\sqrt{Q : a} = P$. Since "$\supseteq$" is clear, we only need to show "$\subseteq$":

$$\begin{aligned} & b \in Q : a \\ \Longrightarrow\ & ab \in Q \\ \Longrightarrow\ & a \in Q \text{ or } b \in \sqrt{Q}, \text{ but } a \notin Q \\ \Longrightarrow\ & b \in \sqrt{Q} \\ \Longrightarrow\ & Q : a \subseteq \sqrt{Q} = P \\ \Longrightarrow\ & \sqrt{Q : a} \subseteq \sqrt{\sqrt{Q}} = \sqrt{Q} = P \end{aligned}$$

Now show that $Q : a$ is primary:

$$\begin{aligned}
& bc \in Q : a \\
\Longrightarrow\, & (ab)c \in Q \\
\Longrightarrow\, & ab \in Q \text{ or } c \in \sqrt{Q} = \sqrt{Q : a} \\
\Longrightarrow\, & b \in Q : a \text{ or } c \in \sqrt{Q : a} \implies Q : a \text{ primary}
\end{aligned}$$

(d)
- $P \cap S \neq \emptyset$:

  $\implies \exists\, b \in P \cap S$

  $\implies \exists\, n : b^n \in Q \cap S$, since $P = \sqrt{Q}$

  $\implies S^{-1}Q = S^{-1}R$
- $P \cap S = \emptyset$: We have to show $S^{-1}Q \cap R = Q$ (or rather $Q^{ec} = Q$). Since "$\supseteq$" holds by 1.10, we only have to show "$\subseteq$":

$$\begin{aligned}
& \frac{a}{s} = \frac{b}{1} \in S^{-1}Q \cap R; a \in Q, s \in S, b \in R \\
\Longrightarrow\, & \exists t \in S : ta = tbs \\
\Longrightarrow\, & Q \ni ta = b(ts), \text{ where } ts \in S, \text{ thus } ts \notin P \\
\Longrightarrow\, & b \in Q \text{ since } Q \text{ is primary.}
\end{aligned}$$

Now we need to show $\sqrt{S^{-1}Q} = S^{-1}\sqrt{Q}$:

  - "$\supseteq$": $b^n \in Q \implies (\frac{b}{s})^n = \frac{b^n}{s^n} \in S^{-1}Q \implies \frac{b}{s} \in \sqrt{S^{-1}Q}$
  - "$\subseteq$":

$$\begin{aligned}
& \frac{a}{s} \in \sqrt{S^{-1}Q} \implies (\frac{a}{s})^n \in S^{-1}Q \\
\Longrightarrow\, & \frac{a^n}{1} = s^n(\frac{a}{s})^n \in S^{-1}Q \cap R = Q \\
\Longrightarrow\, & a^n \in Q \implies a \in \sqrt{Q} \\
\Longrightarrow\, & \frac{a}{s} \in S^{-1}\sqrt{Q}
\end{aligned}$$

Now we need to show that $S^{-1}Q$ is primary, so let $\frac{a}{s}\frac{b}{t} \in S^{-1}Q$ and assume $\frac{b}{t} \notin \sqrt{S^{-1}Q} = S^{-1}\sqrt{Q}$. Then $b \notin \sqrt{Q}$.

$ab = st\frac{a}{s}\frac{b}{t} \in S^{-1}Q \cap R = Q \implies ab \in Q$ and since $b \notin \sqrt{Q}$ we know that $a \in Q$ and thus $\frac{a}{s} \in S^{-1}Q$

(e) $\sqrt{Q \cap Q'} = \sqrt{Q} \cap \sqrt{Q'} = P$ by (f).

$ab \in Q \cap Q'$ and $b \notin P \implies a \in Q \cap Q'$

(f) - (h): Exercise

□

Example 5.5.

(a) "P prime $\not\Rightarrow P^n$ primary":

Let $R = {}^{K[x,y,z]}\!/\!_{\langle xy - z^2 \rangle}, P = \langle \overline{x}, \overline{z} \rangle \in \operatorname{Spec}(R)$

Then $\overline{xy} = \overline{z}^2 \in P^2$, but $\overline{x} \notin P^2$ and $\overline{y} \notin P = \sqrt{P^2}$.

We see in particular that the condition ($a \cdot b \in Q \implies a \in \sqrt{Q}$ or $b \in \sqrt{Q}$) does not imply that Q is primary, since the power of a prime ideal satisfies this condition!

(b) "Q is P-primary $\not\Rightarrow Q = P^n$":

Let $R = K[x,y], Q = \langle x, y^2 \rangle$

$$\begin{aligned}
&\implies \langle x,y \rangle^2 = \langle x^2, xy, y^2 \rangle \subsetneq Q \subsetneq \langle x,y \rangle \\
&\implies \sqrt{Q} = \langle x,y \rangle \lhd \cdot\, K[x,y] \\
&\implies Q \text{ is primary and } Q \neq \langle x,y \rangle^n
\end{aligned}$$

Corollary 5.6. *Let R be a noetherian ring, $P \in \operatorname{Spec}(R), Q \trianglelefteq R, Q \subsetneq R, \mathfrak{m} \lhd \cdot\, R$*

(a) If Q is P-primary then there exists an $n \geq 1$, such that

$$P^n \subseteq Q$$

(b) The following are equivalent:

(1) Q is $\mathfrak{m}$-primary

(2) $\sqrt{Q} = \mathfrak{m}$

(3) $\exists\, n \geq 1 : \mathfrak{m}^n \subseteq Q \subseteq \mathfrak{m}$

Proof. (a) Since ${}^{R}\!/\!_{Q}$ is noetherian, by 4.15

$${}^{P}\!/\!_{Q} = {}^{\sqrt{Q}}\!/\!_{Q} = \mathfrak{N}({}^{R}\!/\!_{Q})$$

is nilpotent.

$\implies \exists\, n \geq 1 : {}^{P^n + Q}\!/\!_{Q} = ({}^{P}\!/\!_{Q})^n = {}^{Q}\!/\!_{Q}$

$\implies \exists\, n : P^n \subseteq Q$

(b) • "(1) $\implies$ (2)": ✓

- "(2) $\implies$ (3)": By 5.4, Q is $\mathfrak{m}$-primary and thus (3) follows from (a)
- "(3) $\implies$ (1)": Since (3) implies $\sqrt{Q} = \mathfrak{m} \lhd \cdot R$, (1) follows from 5.4

□

Corollary 5.7. *Let R be a ring and $I \trianglelefteq R, I \subsetneq R$. If I has a PD, it has a minimal PD.*

Proof. Assume $I = Q_1 \cap \cdots \cap Q_n$ is a PD.

- Step 1: Delete recursively all those Q_i, for which $\bigcap_{j \neq i} Q_j \subseteq Q_i$
- Step 2: Replace the Q_i with the same radical by their intersection.

□

Lemma 5.8. *Let R be any ring, $I \trianglelefteq R, a \in R$. If $I : a = I : a^2$; then:*

$$I = (I : a) \cap (I + \langle a \rangle)$$

Proof. "$\subseteq$" is clear, we only show "$\supseteq$":

$$\begin{aligned}
&r \in (I : a) \cap (I + \langle a \rangle) \\
\implies &\exists\, b \in I, c \in R : r = b + ca \text{ and } ar \in I \\
\implies &I \ni ar = \underbrace{ab}_{\in I} + ca^2 \implies ca^2 \in I \\
\implies &c \in I : a^2 = I : a \implies ca \in I \implies r \in I
\end{aligned}$$

□

Theorem 5.9 (Existence of PD in noetherian rings)**.** *In a noetherian ring every ideal has a minimal PD.*

Proof. Let $M := \{I \trianglelefteq R \,|\, I \subsetneq R, I \text{ has no PD}\}$. Suppose $M \neq \emptyset$. Since R is noetherian, there exists an $I_0 \in M$ maximal with respect to inclusion. In particular I_0 is not primary, i.e. there exist $a, b \in R$ such that $ab \in I_0$, but $a \notin I_0, b^n \notin I_0 \forall n \geq 1$.

Now consider the chain:

$$I_0 : b \subseteq I_0 : b^2 \subseteq I_0 : b^3 \subseteq \ldots$$

Since R is noetherian, there exists an $n \geq 1$, such that

$$I_0 : b^n = I_0 : b^k = I_0 : (b^n)^2 \,\forall k \geq n$$

and by 5.8 we have:

$$I_0 = \underbrace{(I_0 : b^n)}_{\supsetneq I_0,\text{ since } a \notin I_0} \cap \underbrace{(I_0 + \langle b^n \rangle)}_{\supsetneq I_0,\text{ since } b^n \notin I_0}$$

$\Longrightarrow (I_0 : b^n), (I_0 + \langle b^n \rangle) \notin M$ since I_0 was maximal
$\Longrightarrow$ Let $I_0 : b^n = Q_1 \cap \cdots Q_k, I_0 + \langle b^n \rangle = Q_1' \cap \cdots \cap Q_l'$ be the PD's of these
$\Longrightarrow I_0 = Q_1 \cap \cdots \cap Q_k \cap Q_1' \cap \cdots \cap Q_l'$ is a PD $\lightning$

□

Example 5.10.

(a) $R := K[x, y, z], I = \langle xz, yz \rangle = \langle x, y \rangle \cap \langle z \rangle$ is a PD

(b) $R = K[x, y], I = \langle x^2, xy \rangle$ is *not* radical.

$$I = \underbrace{\langle x \rangle}_{\text{prime}} \cap \underbrace{\langle x, y \rangle^2}_{\text{primary}} = \langle x \rangle \cap \underbrace{\langle x^2, y \rangle}_{\text{primary}}$$

are two *different* minimal PD's.

Thus, the PD is *not unique!*

Definition 5.11. Let R be a ring, $I \trianglelefteq R$

(a)

$$\begin{aligned}\mathrm{Ass}(I) &:= \left\{ P \in \mathrm{Spec}(R) \,|\, \exists\, a \in R : \sqrt{I : a} = P \right\} \\ &= \left\{ P \in \mathrm{Spec}(R) \,|\, \exists\, \overline{a} \in {}^{R}\!/_{I} : P = \sqrt{\mathrm{Ann}(\overline{a})} \right\}\end{aligned}$$

is the set of *associated primes* of I

(b)

$$\mathrm{Min}(I) := \{ P \in \mathrm{Ass}(I) \,|\, \nexists Q \in \mathrm{Ass}(I) : Q \subsetneq P \}$$

is the set of *minimal primes* of I or *isolated primes*

(c)

$$\mathrm{Emb}(I) := \mathrm{Ass}(I) \backslash \mathrm{Min}(I)$$

is the set of *embedded primes* of I.

Remark 5.12. *If $I = Q_1 \cap \cdots \cap Q_r$ is a minimal PD of I, then:*

$$\forall\, k\, \exists\, a_k \in \Big(\bigcap_{j \neq k} Q_j\Big) \backslash Q_k$$

And thus:

$$I : a_k = \bigcap_{j=1}^{r} \underbrace{(Q_j : a_k)}_{=R \ for \ j \neq k} = (Q_k : a_k)$$

which is $\sqrt{Q_k}$-primary.

In particular:

- $\forall\, k\, \exists\, a_k \in R : I : a_k$ *is* $\sqrt{Q_k}$*-primary*
- *If* $a_k \notin \sqrt{Q_k}$*, then* $I : a_k = Q_k$ *is a primary component*

Theorem 5.13 (First Uniqueness Theorem)**.** *Let R be any ring, $I \trianglelefteq R, I \subsetneq R$ with minimal PD*

$$I = Q_1 \cap \cdots \cap Q_r$$

Then $\operatorname{Ass}(I) = \left\{\sqrt{Q}, \cdots, \sqrt{Q_r}\right\}$.

In particular: The number of primary components of I and their radicals do not *depend on the chosen minimal PD.*

Proof.

- "$\subseteq$":

$$\begin{aligned}\operatorname{Spec}(R) \ni \sqrt{I : a} &\overset{5.4}{=} \bigcap_{i=1}^{r} \sqrt{Q_i : a}, \text{ where } \sqrt{Q_i : a} \overset{5.4(c)}{=} \begin{cases} R, & a \in Q_i \\ \sqrt{Q_i}, & a \notin Q_i \end{cases} \\ &= \bigcap_{a \notin Q_i} \sqrt{Q_i} \supseteq \prod_{a \notin Q_i} \sqrt{Q_i} \\ &\Longrightarrow \exists\, i : \sqrt{Q_i} \subseteq \sqrt{I : a} \subseteq \sqrt{Q_i : a} = \sqrt{Q_i} \\ &\Longrightarrow \sqrt{I : a} = \sqrt{Q_i}\end{aligned}$$

- "$\supseteq$": Let $k \in \{1, \cdots, r\}$.

$$\begin{aligned}&\overset{5.12}{\Longrightarrow} \exists\, a \in R : (I : a) = Q_k : a \text{ which is } \sqrt{Q_k}\text{-primary} \\ &\Longrightarrow \sqrt{Q_k} = \sqrt{I : a} \in \operatorname{Ass}(I)\end{aligned}$$

$\square$

Corollary 5.14. *If $I = Q_1 \cap \cdots \cap Q_k$ minimal PD, then:*

$$\operatorname{Min}(I) = \{P \in \operatorname{Spec}(R) \,|\, I \subseteq P \ and \ \nexists Q \in \operatorname{Spec}(R) : I \subseteq Q \subsetneq P\}$$

are the minimal ones among the prime ideals containing I.

In particular:

(a) $\mathfrak{R}(R/I) = \bigcap_{P \in \mathrm{Min}(I)} P/I$

(b) R is noetherian $\implies$ *R has only finitely many minimal prime ideals*

Proof.

- "$\subseteq$": Let $\mathrm{Min}(I) \ni P \overset{5.13}{=} \sqrt{Q_j}$ for some j. Now assume there exists a $P' \in \mathrm{Spec}(R) \backslash \mathrm{Ass}(I) : \prod Q_i \subseteq I \subseteq P' \subsetneq P$

$$\begin{aligned} &\implies \exists\, l : Q_l \subseteq P' \\ &\implies \sqrt{Q_l} \subseteq \sqrt{P'} = P' \subsetneq P = \sqrt{Q_j}\ \lightning \end{aligned}$$

- "$\supseteq$:" Let $P \in \mathrm{Spec}(R)$ be in the right hand set. By the argument above there exists an l, such that $P \supseteq \sqrt{Q_l} \supseteq Q_l \supseteq I$ and since P is minimal we get $P = \sqrt{Q_l}$

□

Corollary 5.15. *If $I = Q_1 \cap \dots \cap Q_k$ minimal PD, then*

$$\bigcup_{i=1}^{k} \sqrt{Q_i} = \left\{ a \in R \,|\, \overline{a} \in R/I \text{ is a zero-divisor} \right\} = \{ a \in R \,|\, I : a \supsetneq I \}$$

In particular: If $I = 0$, then

$$\bigcup_{i=1}^{r} \sqrt{Q_i} = \{ a \in R \,|\, a \text{ is a zero-divisor} \}$$

Proof. We show

$$\left\{ a \in R \,|\, \overline{a} \in R/I \text{ is a zero-divisor} \right\} = \bigcup_{a \notin I} \sqrt{I : a}$$

- "$\subseteq$": Let b in the set on the left hand side. Then there exists an $a \notin I$, such that $ab \in I$. Thus $b \in I : a \subseteq \sqrt{I : a}$ and b is in the set on the right hand side.
- "$\supseteq$": Let b be in the set on the r.h.s.

$$\begin{aligned} &\implies \exists\, a \notin I : b \in \sqrt{I : a} \\ &\implies \exists\, m : b^m \in I : a \\ &\implies b^m a \in I \\ &\implies \text{ choose } m \text{ minimal } (m \geq 1, \text{ since otherwise } a \in I) \\ &\implies b(\underbrace{b^{m-1}a}_{\notin I}) \in I \end{aligned}$$

and thus $\overline{b}$ is a zero-divisor in R/I

Now we claim: $\bigcup_{a \notin I} \sqrt{I : a} = \bigcup_{i=1}^{r} \sqrt{Q_i}$:

- "$\supseteq$": By 5.13
- "$\subseteq$": Let $a \notin I = Q_1 \cap \cdots \cap Q_k \implies \exists\, l$ s.t. $a \notin Q_l$

$$\implies \sqrt{I : a} = \bigcap_{j=1}^{k} \sqrt{Q_j : a} \subseteq \sqrt{Q_l : a} \overset{5.4}{=} \sqrt{Q_l}$$

$\square$

Example 5.16. Let $R = K[x, y], I = \left\langle x^2, xy \right\rangle$

$$I = \underbrace{\langle x \rangle}_{\sqrt{\langle x \rangle} = \langle x \rangle} \cap \underbrace{\left\langle x^2, y \right\rangle}_{\sqrt{\langle x^2, y \rangle} = \langle x, y \rangle}$$

is a minimal PD. Thus:

- $\mathrm{Ass}(I) = \{\langle x \rangle, \langle x, y \rangle\}$
- $\mathrm{Min}(I) = \{\langle x \rangle\}$
- $\mathrm{Emb}(I) = \{\langle x, y \rangle\}$

Proposition 5.17 (PD commutes with localisation)**.** *Let R be a ring, $S \subseteq R$ multipl. closed, $I \trianglelefteq R, I \neq R$ with minimal PD $I = Q_1 \cap \cdots \cap Q_r$. Then:*

$$S^{-1}I = \bigcap_{Q_i \cap S = \emptyset} S^{-1}Q_i \text{ and } S^{-1}I \cap R = \bigcap_{Q_i \cap S = \emptyset} Q_i$$

are minimal PD's.

Proof.

$$S^{-1}I \overset{3.7}{=} \bigcap_{i=1}^{r} S^{-1}Q_i = \bigcap_{Q_i \cap S = \emptyset} S^{-1}Q_i$$

Note.

$$S \cap Q_i = \emptyset \iff S \cap \sqrt{Q_i} = \emptyset$$

since $a \in S \cap \sqrt{Q_i} \implies a^n \in S \cap Q_i$.

Thus, by 5.4, $S^{-1}Q_i$ is primary, if $S \cap Q_i = \emptyset$

Moreover $I = \bigcap_{i=1}^{r} Q_i$ is a minimal PD, i.e. the $\sqrt{Q_i}$ are pairwise different. and so the $S^{-1}\sqrt{Q_i}$ are pairwise different (if $\sqrt{Q_i} \cap S = \emptyset$).

Now suppose $\bigcap_{j\neq i} S^{-1}Q_j \subseteq S^{-1}Q_i$ with $Q_i \cap S = \emptyset$. Then:

$$\bigcap_{j\neq i} Q_j \subseteq (\bigcap_{i\neq j} S^{-1}Q_j) \cap R \subseteq S^{-1}Q_i \cap R = Q_i \lightning$$

And we have:

$$\begin{aligned} R \cap S^{-1}I &= R \cap \bigcap_{Q_j \cap S = \emptyset} S^{-1}Q_j \\ &= \bigcap_{Q_j \cap S = \emptyset} \underbrace{(R \cap S^{-1}Q_j)}_{=Q_j} \\ &\overset{5.4}{=} \bigcap_{Q_j \cap S = \emptyset} Q_j \end{aligned}$$

□

Definition 5.18. Let R be a ring, $I \trianglelefteq R, I \neq R, \Sigma \subseteq \operatorname{Ass}(I)$. Then:

$$\Sigma \text{ is called } \textit{isolated} :\iff (\operatorname{Ass}(I) \ni P' \subseteq P \in \Sigma \implies P' \in \Sigma)$$

E.g.: If $P \in \operatorname{Ass}(I)$, then

$$\Sigma_P := \{P' \in \operatorname{Ass}(I) \mid P' \subseteq P\}$$

is obviously isolated and

$$P \in \operatorname{Min}(I) \iff \Sigma_P = \{P\}$$

Corollary 5.19. *Let R be a ring, $I \trianglelefteq R, I \neq R$ with minimal PD $I = Q_1 \cap \cdots \cap Q_r$ and $\Sigma \subseteq \operatorname{Ass}(I)$ isolated. Then:*

$$S_\Sigma := R \setminus \bigcup_{P \in \Sigma} P$$

is multipl. closed and

$$S_\Sigma^{-1} I \cap R = \bigcap_{\sqrt{Q_i} \in \Sigma} Q_i$$

In particular: $\bigcap\limits_{\sqrt{Q_i}\in\Sigma} Q_i$ is independent of the chosen PD

Proof.

$$\begin{aligned} & S_\Sigma \cap Q_i = \emptyset \\ \iff & S_\Sigma \cap \sqrt{Q_i} = \emptyset \\ \iff & \sqrt{Q_i} \subseteq \bigcup_{P \in \Sigma} P \\ \overset{1.17}{\iff} & \exists P \in \Sigma : \sqrt{Q_i} \subseteq P \\ \iff & \sqrt{Q_i} \in \Sigma. \end{aligned}$$

The rest follows from 5.17 □

Corollary 5.20 (Second Uniqueness Theorem)**.** *The isolated (minimal) primary components of a minimal PD are independent of the chosen PD*

Proof 5.21 (of 4.22, "$\Longleftarrow$")**.** Show: R noeth and $\dim R = 0 \implies R$ is artinian.

$$\begin{aligned}
&\dim R = 0\\
\Longrightarrow\; &\mathfrak{m} - \operatorname{Spec}(R) = \operatorname{Spec}(R) = \{P \mid P \text{ minimal}\}\\
&\overset{5.14}{=} \{\mathfrak{m}_1, \cdots, \mathfrak{m}_n\} \text{ finite}\\
\Longrightarrow\; &\mathfrak{R}(R) = \bigcap_{i=1}^{n} \mathfrak{m}_i\\
\overset{4.15}{\Longrightarrow}\; &\exists\, m : 0 = \mathfrak{R}(R)^m = \mathfrak{m}_1^m \cdot \ldots \cdot \mathfrak{m}_n^m\\
\overset{4.21}{\Longrightarrow}\; &R \text{ artinian}
\end{aligned}$$

Proof 5.22 (of 4.23, "Uniqueness")**.** Let

$$R \xrightarrow[\cong]{\psi} \bigoplus_{i=1}^{r} R_i$$

We intend to show: $R_i \cong R/I_i$, where $I_1, \cdots, I_r$ are the isolated (minimal) primary components of $\langle 0 \rangle$.

Consider $\varphi_k : R \overset{\psi}{\twoheadrightarrow} \bigoplus_{i=1}^{r} R_i \overset{\text{proj.}}{\twoheadrightarrow} R_k$, where $\ker(\varphi_k) =: I_k$. Then:

$\Longrightarrow\; R_k \cong R/I_k$ local, artinian ring

$\Longrightarrow\; \exists_1\, \mathfrak{m}_k \lhd \cdot R : I_k \subseteq \mathfrak{m}_k$ and $\exists\, n_k : \mathfrak{m}_k^{n_k} \subseteq I_k$

$\overset{5.6}{\Longrightarrow}\; I_k$ is $\mathfrak{m}_k$-primary

$$\Longrightarrow\; \langle 0 \rangle = \ker(\psi) = \bigcap_{k=1}^{r} I_k$$

is a PD

By the C.R.T. (1.12) I_i, I_j are pairwise coprime $\forall\, i \neq j$. Thus $\mathfrak{m}_i \neq \mathfrak{m}_j \,\forall\, i \neq j$. Thus the radicals of the I_j are pairwise different.

Suppose now that some I_j was redundant in the PD of 0. Then the map

$$\alpha : R \longrightarrow \bigoplus_{i \neq j} R_i : a \mapsto (\varphi_i(a) \mid i \neq j)$$

would be surjective with kernel $\bigcap_{i\neq j} I_i = \langle 0\rangle$, i.e. it would be an isomorphism. In turn also the map $\alpha\circ\psi^{-1}$ would be an isomorphism which would map the j-th unit vector $e_j \in \bigoplus_{i=1}^r R_i$ to zero. This is clearly impossible.

Thus the PD is minimal and all primary components are actually isolated, i.e. minimal and by 5.20 $r, I_1, \cdots, I_r$ only depend on R and thus $R_1, \cdots, R_r$ only depend on R.

B). Krull's Principal Ideal Theorem

Definition 5.23. Let R be a ring, $P \in \operatorname{Spec}(R), I \trianglelefteq R, n \geq 1; a_1, ..., a_k \in P$

(a)

$$\begin{aligned} P^{(n)} &:= P^n \cdot R_P \cap R = (P^n)^{ec} \\ &= \{a \in R \mid \exists\, b \in R\backslash P : ab \in P^n\} \end{aligned}$$

is the *n-th symbolic power* of P.
Note.

- $P^n \subseteq P^{(n)} \subseteq P$. Thus $P^{(1)} = P$ and $\sqrt{P^{(n)}} = P$
- $(P^{(n)})^e = (P^n)^{ece} = (P^n)^e$

(b) P is *minimal over* $a_1, ..., a_k$

$$:\iff \nexists Q \in \operatorname{Spec}(R) : a_1, ..., a_k \in Q \subsetneq P$$

(c)

$$\operatorname{codim}(P) := \operatorname{ht}(P) := \sup\{m \mid \exists\, P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_m \subseteq P, P_i \in \operatorname{Spec}(R)\}$$

is the *codimension* or *height* of P.

(d)

$$\operatorname{codim}(I) := \operatorname{ht}(I) := \min\{\operatorname{codim}(P) \mid I \subseteq P \in \operatorname{Spec}(R)\}$$

is the *codimension* or *height* of I.

Proposition 5.24. *Let R be any ring, $P \in \operatorname{Spec}(R), n \geq 1$*

$$\Longrightarrow P^{(n)} \text{ is } P\text{-primary}$$

Proof. Exercise. □

Theorem 5.25 (Krull's Principal Ideal Theorem)**.** *Let R be a noeth. ring, $P \in \operatorname{Spec}(R)$ minimal over $a \in R\backslash R^*$. Then:*

$$\operatorname{codim}(P) \leq 1$$

Proof. Suppose $Q' \subseteq Q \subsetneq P$ are prime ideals. We need to show. $Q = Q'$.

Localising with respect to P and dividing by Q' we may assume w.l.o.g. (by 1:1 - correspondence of prime ideals):

- R local, $P = J(R) \lhd \cdot R$
- $Q' = 0$
- R is an I.D.

The idea is to show $Q = 0$ by showing $Q^{(k)} = Q^{(k+1)}$, then from this $(Q \cdot R_Q)^k = (Q \cdot R_Q)^{k+1}$ and then using Nakayama's lemma. Since $Q^{(k+1)} \subseteq Q^{(k)}$ is obvious, we only need to show the other inclusion:

P is minimal over a, so we get:

$$\begin{aligned}
&\Longrightarrow \dim(R/\langle a\rangle) = 0 \\
&\overset{4.22}{\Longrightarrow} R/\langle a\rangle \text{ is artinian, since it is noeth. by assumption} \\
&\Longrightarrow Q^{(k)} + \langle a\rangle = Q^{(k+1)} + \langle a\rangle \text{ for some } k \\
&\qquad \text{(just consider: } Q + \langle a\rangle \supseteq Q^{(2)} + \langle a\rangle \supseteq \ldots \text{ in } R/\langle a\rangle) \\
&\Longrightarrow Q^{(k)} \subseteq Q^{(k+1)} + \langle a\rangle
\end{aligned}$$

Now let $y = x + at$ with $y \in Q^{(k)}, x \in Q^{(k+1)}, t \in R$.

$\Longrightarrow$ $at = y - x \in Q^{(k)}$, and since P is minimal: $a \notin Q = \sqrt{Q^{(k)}}$. As $Q^{(k)}$ is primary, we get $t \in Q^{(k)}$ by 5.24.

$$\Longrightarrow \; Q^{(k)} \subseteq Q^{(k+1)} + \underbrace{a}_{\in P} \cdot Q^{(k)} \subseteq Q^{(k+1)} + PQ^{(k)} \subseteq Q^{(k)}$$

Thus we have $Q^{(k+1)} + P \cdot Q^{(k)} = Q^{(k)}$ and by 2.11 we get:

$$Q^{(k)} = Q^{(k+1)}$$

.

Thus we can derive:

$$\begin{aligned}
(Q \cdot R_Q)^k &= Q^k R_Q = Q^{(k)} \cdot R_Q \text{ by definition, as } (P^n)^e = (P^n)^{ece} = (P^{(n)})^e \\
&= Q^{(k+1)} \cdot R_Q = Q^{k+1} \cdot R_Q = (Q \cdot R_Q)^{k+1} \\
&= (Q \cdot R_Q)^k \cdot (Q \cdot R_Q) \\
&\overset{2.9}{\Longrightarrow} (Q \cdot R_Q)^k = 0 \\
&\Longrightarrow Q \cdot R_Q \text{ is nilpotent} \\
&\Longrightarrow Q \cdot R_Q = 0 \text{ since } R \text{ is an I.D.} \\
&\Longrightarrow Q = 0 \text{ again, since } R \text{ is an I.D.}
\end{aligned}$$

□

Note. NAK can only be applied, since R is noetherian and thus every ideal is finitely generated!

Corollary 5.26. *R noetherian, $P_1, P_2, P_3 \in \operatorname{Spec}(R), P_1 \subsetneq P_2 \subsetneq P_3; a \in P_3 \backslash P_2$. Then*

$$\exists\, P \in \operatorname{Spec}(R) : a \in P \text{ and } P_1 \subsetneq P \subsetneq P_3$$

Proof. $\operatorname{codim}({}^{P_3}\!/\!_{P_1}) \geq 2$ by assumption.

By 5.25 ${}^{P_3}\!/\!_{P_1}$ is not minimal over $\overline{a} \in {}^{P_3}\!/\!_{P_1}$ and thus there exists a $P \in \operatorname{Spec}(R)$, such that $\overline{a} \in {}^{P}\!/\!_{P_1}$ and ${}^{P}\!/\!_{P_1} \subsetneq {}^{P_3}\!/\!_{P_1}$. □

Corollary 5.27. *Let R be a noeth. ring, $P \in \operatorname{Spec}(R)$ minimal over $a_1, ..., a_r \in R\backslash R^*$. Then:*

$$\operatorname{codim}(P) \leq r$$

Proof. We do an induction on r. For $r = 1$ see 5.25. Now let $r > 1$:

Let $P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_{r'} = P$. By 5.26 and induction we may assume that $a_r \in P_1$.

Thus ${}^{P}\!/\!_{\langle a_r \rangle}$ is minimal over $\overline{a_1}, ..., \overline{a_{r-1}} \in {}^{R}\!/\!_{\langle a_r \rangle}$ and

$${}^{P_1}\!/\!_{\langle a_r \rangle} \subsetneq {}^{P_2}\!/\!_{\langle a_r \rangle} \subsetneq ... \subsetneq {}^{P_{r'}}\!/\!_{\langle a_r \rangle} = {}^{P}\!/\!_{\langle a_r \rangle}$$

Thus $r' - 1 \leq \operatorname{codim}({}^{P}\!/\!_{\langle a_r \rangle}) \overset{\text{Ind.}}{\leq} r - 1$, and we get

$$r \geq \sup\{r' \mid \exists\, P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_{r'} = P, P_i \text{ prime}\} = \operatorname{codim}(P).$$

□

Corollary 5.28. *Let R be a noeth. ring, $a \in R\backslash R^*$ not a zero-divisor and $P \in \operatorname{Spec}(R)$ minimal over a. Then*

$$\operatorname{codim}(P) = 1$$

Proof. $\operatorname{Ass}(0) = \{P_1, ..., P_n\} \implies a \notin P_i \,\forall\, i$ by 5.15.

Now let $\operatorname{Ass}(0) \supseteq \operatorname{Min}(0) = \{P_1, ..., P_m\} \overset{5.14}{\implies} \exists\, i \in \{1..n\}$:

$$\underbrace{P_i}_{a\notin} \subseteq \underbrace{P}_{a\in}$$

$\implies P_i \subsetneq P \implies \operatorname{codim}(P) \geq 1$ and by the KPIT follows equality. □

Corollary 5.29. *Let R be a noeth I.D. Then R is a U.F.D. $\iff$ all prime ideals of codimension 1 are principal*

Proof. We show two directions:

- "$\Longrightarrow$": Let $\operatorname{codim}(P) = 1$

$$\begin{aligned}
&\Longrightarrow \exists\, 0 \neq f = f_1^{\alpha_1} \cdot \ldots \cdot f_r^{\alpha_r} \in P \text{ prime fact.}\\
&\Longrightarrow \exists\, i : f_i \in P \text{ since } P \text{ is prime}\\
&\Longrightarrow 0 \subsetneq \langle f_i \rangle \subseteq P\\
&\Longrightarrow P = \langle f_i \rangle \ \text{ since } \operatorname{codim}(P) = 1
\end{aligned}$$

- "$\Longleftarrow$": First we show, that if $0 \neq f \in R \backslash R^* \implies f$ is a product of irred. elements:

  Assume that

$$M := \{\langle f \rangle \mid f \text{ is not a product of irred. elements}\} \neq \emptyset$$

$$\begin{aligned}
&\Longrightarrow \exists\, \langle f \rangle \in M \text{ maximal with respect to inclusion, since } R \text{ is noeth.}\\
&\Longrightarrow f \text{ is not irred.}\\
&\Longrightarrow f = gh; g, h \notin R^*\\
&\Longrightarrow \langle g \rangle \supsetneq \langle f \rangle \subsetneq \langle h \rangle\\
&\Longrightarrow \langle g \rangle, \langle h \rangle \notin M \text{ by choice of } f\\
&\Longrightarrow g, h \text{ are products of irred. elements}\\
&\Longrightarrow f \text{ is a product of irred. elements } \lightning
\end{aligned}$$

  Now we need to show: f irreducible $\implies f$ prime:

  Choose: $P \in \operatorname{Spec}(R)$ minimal over f (this exists, since R is noetherian).

$$\begin{aligned}
&\overset{5.28}{\Longrightarrow} \operatorname{codim}(P) = 1\\
&\Longrightarrow P \text{ is principal by assumption}\\
&\Longrightarrow P = \langle p \rangle \ \text{ for some } p \text{ prime element}\\
&\Longrightarrow \exists a \in R : f = ap, \text{ since } f \in P\\
&\Longrightarrow a \in R^*, \text{ since } f \text{ is irred.}\\
&\Longrightarrow P = \langle f \rangle \implies f \text{ prime}
\end{aligned}$$

$\square$

Corollary 5.30 (Compare with Example 4.24 c))**.** *Let* $(R, \mathfrak{m})$ *be a local noeth. ring, then:*

$$\dim(R) \leq \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 < \infty$$

Proof.

$$\begin{aligned}
&R \text{ noeth.}\\
&\overset{NAK}{\Longrightarrow} \mathfrak{m} = \langle a_1, \cdots, a_r\rangle \text{ for some } a_i \in \mathfrak{m} \text{ and } r = \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2\\
&\Longrightarrow \mathfrak{m} \text{ is minimal over } a_1, \cdots, a_r\\
&\Longrightarrow \dim(R) = \operatorname{codim}(R) \leq r
\end{aligned}$$

□

Remark 5.31. *(a) If $P \in \operatorname{Spec}(R)$, we get*

(1) $\operatorname{codim}(P) + \dim({}^{R}\!/\!_{P}) \leq \dim(R)$

(2) $\operatorname{codim}(P) = \dim(R_P)$

(b) We call a local noetherian ring $(R, \mathfrak{m})$ regular *if $\dim(R) = \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$.*
Note, if R is the local ring of an algebraic variety at a point p, then $\mathfrak{m}/\mathfrak{m}^2$ is the dual of the tangent space of the variety at the point p and the above equality means that the point is a smooth or regular point of the variety!

Corollary 5.32. *Let $(R, \mathfrak{m})$ be a local, noetherian ring, $a \in R\backslash R^*$.*

(a) $\dim\left({}^{R}\!/\!_{\langle a\rangle}\right) \geq \dim(R) - 1$.

(b) If a is not a zero-divisor, then $\dim\left({}^{R}\!/\!_{\langle a\rangle}\right) = \dim(R) - 1$.

Proof. We show two inequalities:

- "$\geq$": Choose a chain $P_0 \subsetneq P_1 \subsetneq .. \subsetneq P_d$ of primes in R with $d = \dim(R)$, such that $a \in P_i$ with minimal i. Note, for this we need that R is local, so that a is contained in every maximal ideal! Otherwise possibly no chain of length $\dim(R)$ would contain a prime ideal which contains a!

  By 5.26 we get $i \leq 1$

  $\Longrightarrow {}^{P_1}\!/\!_{\langle a\rangle} \subsetneq ... \subsetneq {}^{P_d}\!/\!_{\langle a\rangle}$ are primes in ${}^{R}\!/\!_{\langle a\rangle}$. Thus:

  $\dim\left({}^{R}\!/\!_{\langle a\rangle}\right) \geq d - 1 = \dim(R) - 1$.

- "$\leq$": Choose $\langle a\rangle \subseteq P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_r$ a chain of prime ideals in R of maximal length, such that $a \in P_0$.

  $\Longrightarrow \dim\left({}^{R}\!/\!_{\langle a\rangle}\right) = r = \dim\left({}^{R}\!/\!_{P_0}\right) \overset{5.31}{\leq} \dim(R) - \operatorname{codim}(P_0) \overset{5.28}{=} \dim(R) - 1$

  Note, in order to apply Corollary 5.28, we need that a is not a zero-divisor.

□

Corollary 5.33.
$$\dim(K[x_1, \cdots, x_n]_{\langle x_1 - a_1, \cdots, x_n - a_n\rangle}) = n$$
In particular, $K[x_1, \ldots, x_n]_{\langle x_1 - a_1, \cdots, x_n - a_n\rangle}$ *is a regular ring.*

Proof. 5.32 + Induction. ☐

Geometrical interpretation 5.34.

Consider $0 \subsetneq \langle x\rangle \subsetneq \langle x, y\rangle \subsetneq K[x, y]$ and $R = {K[x,y,z]}\big/{\langle xz, yz\rangle}$, $P = \langle \overline{x}, \overline{y}, \overline{z-1}\rangle$. Then:

$$\begin{aligned} \operatorname{codim} P &= \dim R_P \\ &= \dim({K[x,y,z]}\big/{\langle xz, yz\rangle})_{\langle \overline{x}, \overline{y}, \overline{z-1}\rangle} \\ &= \dim({K[x,y,z]}\big/{\langle x, y\rangle})_{\langle \overline{x}, \overline{y}, \overline{z-1}\rangle} \\ &= \dim K[z]_{\langle \overline{z-1}\rangle} = 1 \end{aligned}$$

Since $\dim {R}/{P} = 0 \implies \operatorname{codim} P + \dim({R}/{P}) = 1 < \dim R = 2$.

Proposition 5.35. *A regular local ring* $(R, \mathfrak{m})$ *is an integral domain.*

Proof. We prove the statement by induction on $d = \dim(R)$. If $d = 0$ then by Nakayama's Lemma $\mathfrak{m}$ must be zero, since $\mathfrak{m}/\mathfrak{m}^2 = 0$.

Let thus $d > 0$. Since R is noetherian there are only finitely many minimal prime ideals $\operatorname{Min}(0) = \{P_1, \ldots, P_k\}$. By prime avoidance 1.17 there is an

$$x \in \mathfrak{m} \setminus \big(\mathfrak{m}^2 \cup P_1 \cup \ldots \cup P_k\big).$$

In the following sequence of inequalities we make use of the following identifications $R/\langle x\rangle\big/\mathfrak{m}/\langle x\rangle \cong R/\langle x\rangle$ and $\mathfrak{m}/\langle x\rangle\big/\mathfrak{m}^2 + \langle x\rangle/\langle x\rangle \cong \mathfrak{m}/\mathfrak{m}^2 + \langle x\rangle$ in order to determine that $R/\langle x\rangle$ is regular:

$$\begin{aligned} \dim_{R/\mathfrak{m}}\big(\mathfrak{m}/\mathfrak{m}^2 + \langle x\rangle\big) &= \dim_{R/\mathfrak{m}}\big(\mathfrak{m}/\mathfrak{m}^2\big) - 1 = \dim(R) - 1 \\ &\overset{5.32}{\leq} \dim\big(R/\langle x\rangle\big) \overset{5.30}{\leq} \dim_{R/\mathfrak{m}}\big(\mathfrak{m}/\mathfrak{m}^2 + \langle x\rangle\big). \end{aligned}$$

Thus the inequalities are indeed equalities and $R/\langle x\rangle$ is regular.

By induction $R/\langle x\rangle$ is then an integral domain and thus $\langle x\rangle$ is a prime ideal. It follows that some of the minimal prime ideals P_i is contained in $\langle x\rangle$, and since x is not contained in any minimal prime the inclusion is strict.

We now want to show that this P_i is indeed the zero ideal and therefore R is an integral domain. To this end we consider an arbitrary element $y \in P_i \subset \langle x\rangle$. There must be a $z \in R$ such that $y = x \cdot z$. Since P_i is prime and $x \notin P_i$ it follows that $z \in P_i$, and thus

$$y = x \cdot z \in x \cdot P_i \subseteq \mathfrak{m} \cdot P_i.$$

We have thus shown that

$$P_i \subseteq \mathfrak{m} \cdot P_i,$$

which by Nakayama's Lemma implies that $P_i = 0$. This finishes the proof. □

6. Integral Ring Extensions

A). Basics

Motivation. Let $K \subseteq K'$ be a field extension, $\alpha \in K'$ and

$$\varphi_\alpha : K[x] \twoheadrightarrow K[\alpha], x \longmapsto \alpha$$

Then we call α *transcendental* over K

$$\begin{aligned} &:\iff \varphi_\alpha \text{ is an isomorphism} \\ &\iff \ker(\varphi_\alpha) = 0 \\ &\iff \dim_K K[\alpha] = \infty \\ &\iff K[\alpha] \text{is } \textit{not} \text{ finitely generated as } K \text{ - vector space} \end{aligned}$$

We call α *algebraic* over K

$$\begin{aligned} &:\iff \varphi_\alpha \text{ is not injective} \\ &\iff 0 \neq \ker(\varphi_\alpha) = \langle \mu_\alpha \rangle \trianglelefteq K[x] \\ &\iff \exists 0 \neq \mu_\alpha \in K[x] : \mu_\alpha(\alpha) = 0 \\ &\overset{(*)}{\iff} \exists \mu_\alpha \text{ monic} : \mu_\alpha(\alpha) = 0 \\ &\iff \dim_K(K[\alpha]) < \infty \\ &\iff K[\alpha] \text{ is a finitely generated } K \text{ - vector space} \end{aligned}$$

Note. The step marked by (*) does not work in general rings!

Definition 6.1. Let $R \subseteq R'$ be a ring extension, $\alpha \in R', I \trianglelefteq R$,

$$\varphi_\alpha : R[x] \twoheadrightarrow R[\alpha] \subseteq R', x \longmapsto \alpha$$

(a) α is called *transcendental*$_{/R}$ or *algebraically independent*$_{/R}$ $:\iff$ φ_α is an isomorphism $\iff$ $\ker(\varphi_\alpha) = 0$

(b) α is called *integral*$_{/R}$

$$:\iff \exists 0 \neq f = x^n + \sum_{i=0}^{n-1} f_i x^i \in R[x] \text{ monic, such that } f(\alpha) = 0$$

(c) R' is *integral*$_{/R}$ $:\iff$ Every $\alpha \in R'$ is integral$_{/R}$

(d) R' is *finite*$_{/R}$ $:\Longleftrightarrow$ R' is finitely generated as an R-module,

$$:\Longleftrightarrow \exists \alpha_1, ..., \alpha_n \in R' : R' = \sum_{i=1}^{n} \alpha_i R$$

(e) R' is a *finitely generated R-algebra*

$$:\Longleftrightarrow \exists \alpha_1, ..., \alpha_n \in R' : R' = R[\alpha_1, ..., \alpha_n]$$

Example 6.2. Let R be a UFD, $R' := \mathrm{Quot}(R)$ and $\alpha = \frac{a}{b} \in R'; a, b \in R, b \neq 0$. Then we have that $0 \neq bx - a \in R[x]$ and since α is a zero of this polynomial, it is not transcendental. However, since we're not in a field, this does *not* imply automatically, that α is integral. It may well be that it is neither of these. In fact, we can show:

$$\alpha \text{ is integral}_{/R} \iff \alpha \in R$$

Proof. The implication "$\Longleftarrow$" is clear, we only have to show "$\Longrightarrow$":

W.l.o.g. we can assume, that $\gcd(a, b) \in R^*$. Since α is integral$_{/R}$ there exists a polynomial $0 \neq f = x^n + \sum_{i=0}^{n-1} f_i x^i \in R[x]$, such that $f(\alpha) = 0$. Thus we have:

$$\begin{aligned} 0 = f\left(\frac{a}{b}\right) &= \frac{a^n}{b^n} + \sum_{i=0}^{n-1} f_i \frac{a^i}{b^i} \\ \Longrightarrow a^n &= -\sum_{i=0}^{n-1} f_i a^i b^{n-i} \\ &= b \underbrace{\left(-\sum_{i=0}^{n-1} f_i a^i b^{n-i-1}\right)}_{\in R} \end{aligned}$$

Thus we know that $b \mid a^n$ and by the assumption above follows $b \in R^*$ and thus $\alpha \in R$ ☐

We summarize:

- The elements of $R' \backslash R$ are neither transcendental nor integral$_{/R}$
- If $\alpha \notin R$, then $R[\alpha]$ is *not* finitely generated as R-module (see 6.3). So

$$\alpha \text{ transcendental} \nLeftrightarrow R[\alpha] \text{ is not finitely generated}_{/R}$$

- E.g. $\alpha \in \mathbb{Q}$ integral$_{/R}$ $\iff \alpha \in \mathbb{Z}$

Proposition 6.3. *Let $R \subseteq R'$ be a ring extension, $\alpha \in R'$ Then the following are equivalent:*

- *α is integral$_{/R}$*
- *$R[\alpha]$ is finite$_{/R}$*
- *There exists an $R[\alpha]$-module M, such that $R[\alpha] \subseteq M$ and M is finite$_{/R}$*

Proof. We show three implications:

- "(a) $\implies$ (b)": $f = x^n + \sum_{i=0}^{n-1} f_i x^i \in R[x]$ with $f(\alpha) = 0$. Thus $R[\alpha] = \langle \alpha^{n-1}, ..., \alpha, 1 \rangle$
- "(b) $\implies$ (c)": Set $M = R[\alpha]$
- "(c) $\implies$ (a)": Apply 2.6 (Cayley-Hamilton) to $\varphi : M \to M, m \mapsto \alpha m$, $I = R$.

$$\begin{aligned} &\implies \exists \chi_\varphi \in R[x] \text{ monic, such that } \chi_\varphi(\varphi) = 0 \\ &\implies 0 = \chi_\varphi(\varphi)(\underbrace{1}_{\in M \supseteq R[\alpha]}) = \chi_\varphi(\alpha) \cdot 1 = \chi_\varphi(\alpha) \end{aligned}$$

□

Corollary 6.4 (Tower Law)**.** *Let $R \subseteq R' \subseteq R''$ be ring extensions. Then:*

(a) If R' is finite$_{/R}$ $\implies$ R' is integral$_{/R}$

(b) If R' is finite$_{/R}$, R'' finite$_{/R'}$ $\implies$ R'' is finite$_{/R}$

(c) $\alpha_1, ..., \alpha_n \in R'$ integral$_{/R}$ $\implies$ $R[\alpha_1, \cdots, \alpha_n]$ is finite$_{/R}$

(d) R' integral$_{/R}$, R'' integral$_{/R'}$ $\implies$ R'' integral$_{/R}$

(e) $\mathrm{Int}_{R'}(R) := \{\alpha \in R' \mid \alpha \text{ integral}_{/R}\}$, the integral closure *of R in R' is a subring of R'*

Proof.

(a) Let $\alpha \in R' \implies R \subseteq R[\alpha] \subseteq R'$. Applying 6.3 to $M := R'$ yields that α is integral$_{/R}$

(b) $R' = \langle \alpha_1, \cdots, \alpha_n \rangle_R, R'' := \langle \beta_1, \cdots, \beta_n \rangle_{R'}$

$$\implies R'' = \langle \alpha_i \cdot \beta_j \mid i = 1..m, j = 1..n \rangle_R$$

(c) We do an induction on n. For $n = 1$ we just have to apply 6.3. Now assume the statement is true for $n - 1$. We get:

$$R \underbrace{\subseteq}_{\text{finite by induction}} R[\alpha_1, \cdots, \alpha_{n-1}] \subseteq R[\alpha_1, \cdots, \alpha_n]$$

where the last inclusion is also finite by 6.3, since α_n is integral$_{/R}$ (and thus also integral$_{/R[\alpha_1, \cdots, \alpha_{n-1}]}$). With (b) we conclude that $R[\alpha_1, \cdots, \alpha_n]$ is finite$_{/R}$.

(d) Let $\alpha \in R''$

$$\begin{aligned}
&\Longrightarrow \exists b_0, \cdots, b_{n-1} \in R' : \alpha^n + b_{n-1}\alpha^{n-1} + ... + b_0 = 0 \\
&\Longrightarrow \alpha \text{ is integral}_{/R[b_0,\cdots,b_{n-1}]} \\
&\Longrightarrow R \subseteq R[b_0, \cdots, b_{n-1}] \text{ is finite by (c), since } R' \text{ is integral}_{/R} \text{ and} \\
&\quad\; R[b_0, \cdots, b_{n-1}] \subseteq R[b_0, \cdots, b_{n-1}, \alpha] \text{ finite by 6.3} \\
&\Longrightarrow R \subseteq R[b_0, \cdots, b_{n-1}, \alpha] \text{ is finite}_{/R} \text{ by (b) and by (a) integral}_{/R}, \\
&\quad\; \text{in particular, } \alpha \text{ is integral}_{/R}
\end{aligned}$$

(e) Let $\alpha, \beta \in \mathrm{Int}_{R'}(R)$. Then by (c) $R[\alpha, \beta]$ is finite$_{/R}$, in particular integral$_{/R}$. Thus $\alpha + \beta, \alpha \cdot \beta, -\alpha, 1 \in \mathrm{Int}_{R'}(R)$

□

Example 6.5.

(a) R' integral$_{/R}$ $\not\Rightarrow$ R' finite$_{/R}$. E.g. Let $R' := \mathrm{Int}_{\mathbb{C}}(\mathbb{Q}), R := \mathbb{Q}$

(b) $R' := {}^{K[x,y]}\!\diagup\!_{\langle x^2 - y^3 \rangle}, R := K[x]$. Consider $R \xhookrightarrow{i} R'$, $x \mapsto \overline{x}$. Thus

$$R' = \langle 1, \overline{y}, \overline{y}^2 \rangle_R$$

is finite, hence integral.

(c) $\overline{K}[x_1, \ldots, x_n]$ is integral over $K[x_1, \ldots, x_n]$, see Exercises.

Definition 6.6. Let $R \subseteq R'$ be a ring extension

(a) R is *integrally closed* in $R' :\Longleftrightarrow \mathrm{Int}_{R'}(R) = R$

(b) R is *reduced* $:\Longleftrightarrow \mathfrak{R}(R) = 0$

(c) R is *normal* $:\Longleftrightarrow$ R is reduced and integrally closed in $\mathrm{Quot}(R)$
Note. Some authors require R to be an ID as well

(d) If R is reduced, then $R \hookrightarrow \mathrm{Int}_{\mathrm{Quot}(R)}(R)$ is called the *normalisation* of R.

Example 6.7.

(a) R UFD $\overset{6.2}{\Longrightarrow}$ R is normal, e.g. $\mathbb{Z}$ and $K[\underline{x}]$ are normal.

(b) ${}^{K[x]}\!\diagup\!_{\langle x^2 \rangle}$ is *not* reduced, since $0 \neq \overline{x} \in \mathfrak{R}(R)$

(c) $R = {}^{K[x,y]}\!\diagup\!_{\langle x^2 - y^3 \rangle}$ is *not* normal (but reduced!), since R is not integrally closed in $\mathrm{Quot}(R)$.

Proof. Let $\alpha := \frac{\overline{x}}{\overline{y}} \in \mathrm{Quot}(R)$

$$\begin{aligned}&\Longrightarrow \alpha^2 - \overline{y} = \frac{\overline{x}^2}{\overline{y}^2} - \overline{y} = \frac{\overline{y}^3}{\overline{y}^2} - \overline{y} = \overline{0}\\ &\Longrightarrow \alpha \text{ is a zero of } z^2 - \overline{y} \in R[z], \text{ hence integral}_{/R}\end{aligned}$$

But suppose $\alpha \in R$

$$\begin{aligned}&\Longrightarrow \exists\, p \in K[x,y] : \overline{p} = \frac{\overline{x}}{\overline{y}} = \alpha\\ &\Longrightarrow \overline{yp} - \overline{x} = \overline{0}\\ &\Longrightarrow yp - x \in \left\langle x^2 - y^3 \right\rangle, \text{ but } \deg x = 1, \deg x^2 = 2 \lightning\\ &\Longrightarrow \alpha \notin R\end{aligned}$$

□

(d) $\mathrm{Int}_{R'}(\mathrm{Int}_{R'}(R)) = \mathrm{Int}_{R'}(R)$, i.e. $\mathrm{Int}_{R'}(R)$ is integrally closed in R'

Proof. Since "$\supseteq$" is clear, we only have to show "$\subseteq$":

We know:

$$R \underbrace{\subseteq}_{\text{integral}} \mathrm{Int}_{R'}(R) \underbrace{\subseteq}_{\text{integral}} \mathrm{Int}_{R'}(\mathrm{Int}_{R'}(R))$$

Hence, by 6.4, $R \subseteq \mathrm{Int}_{R'}(\mathrm{Int}_{R'}(R))$ is integral and thus

$$\mathrm{Int}_{R'}(\mathrm{Int}_{R'}(R)) \subseteq \mathrm{Int}_{R'}(R)$$

□

Proposition 6.8 (Integral dependence is preserved under localisation and quotients)**.** *Let $R \subseteq R'$ be a ring extension, $S \subseteq R$ multipl. closed and $I \trianglelefteq R'$. Then:*

(a) R' integral$_{/R}$ $\Longrightarrow$ ${R'}/{I}$ is integral$_{/R/_{I\cap R}}$

(b) R' integral$_{/R}$ $\Longrightarrow$ $S^{-1}R'$ is integral$_{/S^{-1}R}$

(c) $S^{-1}(\mathrm{Int}_{R'}(R)) = \mathrm{Int}_{S^{-1}R'}(S^{-1}R)$

(d) If $f \in K[\underline{x}]$, then $\overline{K}[\underline{x}]/\langle f\rangle$ is integral over $K[\underline{x}]/\langle f\rangle$.

Proof.

(a) $I \cap R \trianglelefteq R$ and ${R}/{I \cap R} \hookrightarrow {R'}/{I}$ is an inclusion. The rest is clear (just factorize all polynomial coefficients modulo $I \cap R$).

(b) Let $\frac{a}{s} \in S^{-1}R$. Since $a \in R'$, there exist $b_i \in R$, such that

$$a^n + b_{n-1}a^{n-1} + ... + b_0 = 0$$

and thus also

$$(\frac{a}{s})^n + \frac{b_{n-1}}{s} \cdot (\frac{a}{s})^{n-1} + ... + \frac{b_0}{s^n} = 0$$

which shows that $\frac{a}{s}$ is integral$_{/S^{-1}R}$.

(c) "$\subseteq$" follows from (b) and "$\supseteq$" is an exercise.

(d) By (a) it suffices to show that $\langle f \rangle_{\overline{K}[\underline{x}]} \cap K[\underline{x}] = \langle f \rangle_{K[\underline{x}]}$. This follows from the Exercises.

$\square$

Proposition 6.9 (Normality is a local property)**.** *For an integral domain R the following are equivalent:*

(a) R is normal

(b) R_P is normal $\forall\, P \in \mathrm{Spec}(R)$

(c) $R_{\mathfrak{m}}$ is normal $\forall\, \mathfrak{m} \in \mathfrak{m} - \mathrm{Spec}(R)$

Proof.

Note. $Q := \mathrm{Quot}(R) = \mathrm{Quot}(R_P)$ and by Exercise 26 R_P is a *reduced* ID!

- "(a) $\implies$ (b)":

$$\mathrm{Int}_Q(R_P) = \mathrm{Int}_{Q_P}(R_P) = (\mathrm{Int}_Q(R))_P = R_P$$

Hence R_P is normal.

- "(b) $\implies$ (c)" is clear
- "(c) $\implies$ (a)": Consider the map $i : R \hookrightarrow \mathrm{Int}_Q(R), r \mapsto \frac{r}{1}$. It induces maps $i_{\mathfrak{m}} : R_{\mathfrak{m}} \hookrightarrow (\mathrm{Int}_Q(R))_{\mathfrak{m}} : \frac{a}{b} \mapsto \frac{a}{b}$ and

$$\begin{aligned}(\mathrm{Int}_Q(R))_{\mathfrak{m}} &= \mathrm{Int}_{Q_{\mathfrak{m}}}(R_{\mathfrak{m}}) \\ &= \mathrm{Int}_Q(R_{\mathfrak{m}}) \\ &= R_{\mathfrak{m}}\end{aligned}$$

Thus, $i_{\mathfrak{m}}$ is surjective and since by 3.12 surjectivity is a local property, also i is surjective. Hence R is normal

$\square$

B). Going-Up Theorem

Proposition 6.10. *Let R' be integral$_{/R}$, $\alpha \in R$. Then:*

(a) $\alpha \in R^* \iff \alpha \in (R')^*$

(b) If R' is an ID then: R is a field $\iff$ R' is a field

(c) $\mathfrak{m} \lhd \cdot R' \iff \mathfrak{m} \in \operatorname{Spec}(R')$ *and* $\mathfrak{m} \cap R \lhd \cdot R$

Proof.

(a) "$\implies$" is clear, we only have to show "$\impliedby$": So let $\beta \in R'$, such that $\beta \cdot \alpha = 1$. Since β is integral$_{/R}$, there exist $a_i \in R$ such that $\beta^n + \sum_{i=0}^{n-1} a_i \beta^i = 0$

$$\implies \beta = \beta^n \cdot \alpha^{n-1} = \sum_{i=0}^{n-1} \underbrace{(-a_i)}_{\in R} \underbrace{\beta^i \alpha^{n-1}}_{=\alpha^{n-i} \in R} \in R$$

Thus $\beta \in R$ and $\alpha \in R^*$

(b) "$\impliedby$" follows from (a), it remains to show "$\implies$": Let $0 \neq \alpha \in R'$. Then there exists $0 \neq f = x^n + \sum_{i=0}^{n-1} f_i x^i \in R[x]$ such that $f(\alpha) = 0$ and f has minimal degree. Since R is an ID we can w.l.o.g. assume that $f_0 \neq 0$ (otherwise just "cancel out" x).

$$\begin{aligned} \implies f_0 &= -\alpha^n - \sum_{i=1}^{n-1} f_i \alpha^i \\ &= \alpha(-\alpha^{n-1} - \sum_{i=1}^{n-1} f_i \alpha^{i-1}) \end{aligned}$$

Since R is a field $f_0 \neq 0$ is a unit and thus

$$1 = \alpha \cdot \underbrace{f_0^{-1} \cdot (...)}_{\in R'}$$

(c) By 6.8 (a) $R/_{\mathfrak{m} \cap R} \hookrightarrow R'/_{\mathfrak{m}}$ is integral for all $\mathfrak{m} \in \mathfrak{m}-\operatorname{Spec}(R')$ and by (b) follows

$$R/_{\mathfrak{m} \cap R} \text{ is a field} \iff R'/_{\mathfrak{m}} \text{ is a field}$$

which is equivalent to saying:

$$\mathfrak{m} \cap R \lhd \cdot R \iff \mathfrak{m} \lhd \cdot R'$$

□

Example 6.11.

Let $R' = {}^{K[x,y]}\!\big/_{\langle x \cdot y\rangle}$, $R = K[x] \hookrightarrow R'$ by $x \mapsto \overline{x}$. Let $P := \langle \overline{x} \rangle \in \operatorname{Spec}(R')$. We see that $P \cap R = \langle x \rangle \lhd \cdot R$, but $\langle \overline{x} \rangle$ is *not* maximal in R'. Thus, $R \subseteq R'$ is *not* integral!

Remark 6.12. *Recall the 1:1 - correspondences:*

(a) $\{P \in \operatorname{Spec}(R) \mid I \subseteq P\} \xrightarrow{1:1} \operatorname{Spec}({}^{R}\!/_{I})$ *by* $P \mapsto \overline{P}$

(b) $\{P \in \operatorname{Spec}(R) \mid P \cap S = \emptyset\} \xrightarrow{1:1} \operatorname{Spec}(S^{-1}R)$ *by* $P \mapsto S^{-1}P$

Our aim is to find a similar correspondence for integral ring extensions.

Corollary 6.13. *Let R' be integral$_{/R}$, $Q, Q' \in \operatorname{Spec}(R'), Q \subsetneq Q'$*

$$\implies Q \cap R \subsetneq Q' \cap R$$

Proof. Suppose that $P := Q \cap R = Q' \cap R \in \operatorname{Spec}(R)$. Then by 6.8 R'_P is integral$_{/R_P}$, where $Q_P \subseteq Q'_P \in \operatorname{Spec}(R'_P)$ and $P_P \lhd \cdot R_P$, which can be written as:

$$\begin{aligned} P_P &= (Q' \cap R)_P = Q'_P \cap R_P \text{ and} \\ P_P &= (Q \cap R)_P = Q_P \cap R_P \end{aligned}$$

By 6.10 $Q_P, Q'_P \lhd \cdot R'_P$ and since one is contained in the other we know that $Q_P = Q'_P$. Thus, by 6.12(b) we derive that $Q = Q'$ ↯. ☐

Example 6.14.

(a) Choose R and R' as in 6.11. Let $Q := \langle \overline{x} \rangle \subsetneq \langle \overline{x}, \overline{y} \rangle =: Q'$, which are both prime. However $Q \cap R = \langle x \rangle = Q' \cap R$.

(b) Even if $Q \nsubseteq Q'$, it might be possible that $Q \cap R = Q' \cap R$: Let $R := K[x] \subseteq {}^{K[x,y]}\!\big/_{\langle x^2 - y^2 \rangle} =: R'$ by $x \mapsto \overline{x}$. Choose

$$\begin{aligned} P &:= \langle x - 1 \rangle \in \operatorname{Spec}(R) \\ Q &:= \langle \overline{x} - 1, \overline{y} - 1 \rangle \in \operatorname{Spec}(R') \\ Q' &:= \langle \overline{x} - 1, \overline{y} + 1 \rangle \in \operatorname{Spec}(R') \end{aligned}$$

Then $Q \cap R = \langle x - 1 \rangle = Q' \cap R$, but $Q \nsubseteq Q' \nsubseteq Q$.

Theorem 6.15 (Lying-Over and Going-Up)**.** *Let R' be integral$_{/R}$*

*(a) (*Lying-Over*)*

$$\forall\, P \in \operatorname{Spec}(R) \exists\, Q \in \operatorname{Spec}(R') : Q \cap R = P$$

*(b) (*Going-Up*)* $\forall P, P' \in \operatorname{Spec}(R), Q \in \operatorname{Spec}(R')$*, such that*

$$Q \supseteq Q \cap R = P \subsetneq P'$$

there exists a $Q' \in \operatorname{Spec}(R')$ *, such that* $Q \subsetneq Q', Q' \cap R = P'$

$$\begin{tikzcd} Q \arrow[r, dotted, "\subsetneq"] & \exists Q' \\ Q \cap R = P \arrow[u, dash] \arrow[r, "\subsetneq"] & P' = Q' \cap R \arrow[u, dotted, dash] \end{tikzcd}$$

Proof.

(a) Idea: Localise at P and choose a maximal ideal $\mathfrak{m} \lhd \cdot R'_P$. Then show that $\mathfrak{m} \cap R'$ is the desired ideal.

By 6.8(b) we know that $R_P \subseteq R'_P$ is an integral extension, where $P_P \lhd \cdot R_P$ is the unique maximal ideal. Now choose any maximal ideal $\mathfrak{m} \lhd \cdot R'_P$. By 6.10(c) we get

$$\begin{aligned} &\Longrightarrow \mathfrak{m} \cap R_P \lhd \cdot R_P \\ &\Longrightarrow \mathfrak{m} \cap R_P = P_P \end{aligned}$$

Now set $Q := \mathfrak{m} \cap R' \in \operatorname{Spec}(R')$

$$\begin{aligned} \Longrightarrow \; P &= P_P \cap R \\ &= (\mathfrak{m} \cap R_P) \cap R \\ &= \mathfrak{m} \cap R \\ &= (\mathfrak{m} \cap R') \cap R = Q \cap R \end{aligned}$$

(b) Idea: Reduce modulo Q and apply (a):

By 6.8(a) $R/P \subseteq R'/Q$ is integral and $P'/P \in \operatorname{Spec}\left(R/P\right)$. By (a) there exists a $\overline{Q'} \in \operatorname{Spec}\left(R'/Q\right)$, such that $\overline{Q'} \cap R/P = P'/P$ and by 6.12(b) this corresponds to a $Q' \in \operatorname{Spec}(R')$ with $Q \subsetneq Q'$ and $Q' \cap R = P'$.

$\square$

Example 6.16 (Geometrical interpretation)**.**

(a) If the component Q maps to the component P, then every point $P' \in P$ has a preimage Q' in Q.

(b) Let $R := K[x], R' := \mathrm{Quot}(R) = K(x)$ and $K = \overline{K}$. Then $\mathrm{Spec}(R') = \{\langle 0\rangle\}$ and $\mathrm{Spec}(R) = \{\langle 0\rangle\} \cup \{\langle x-a\rangle \mid a \in K\}$.

Now let $P := \langle 0\rangle \subsetneq \langle x-1\rangle =: P'$, where $P \subseteq Q = \langle 0\rangle$, but there is no prime ideal 'lying over' P'. In particular, this extension can not be integral.

(c) Let $R := K[x] \subseteq {}^{K[x,y]}\!\diagup_{\langle 1-xy\rangle} =: R'$ by $x \mapsto \overline{x}$. Now choose

- $Q := \langle\overline{0}\rangle \in \mathrm{Spec}(R')$
- $P := Q \cap R = \langle 0\rangle \in \mathrm{Spec}(R)$
- $P' := \langle x\rangle \in \mathrm{Spec}(R)$

Then $P \subsetneq P'$, but there is no prime ideal $Q' \supseteq Q$, such that $Q' \cap R = P'$, since otherwise, as $\overline{x} \in Q'$, also $\overline{xy} = \overline{1} \in Q'$ and thus $Q' = R' \lightning_{Q' \text{ prime}}$

Note. $\overline{y}$ is not integral$_{/R}$ and thus R' is not integral$_{/R}$

Corollary 6.17.

$$R' \ \textit{integral}_{/R} \implies \dim R = \dim R'$$

Proof.

"$\leq$" : Let $P_0 \subsetneq ... \subsetneq P_m$ be a chain in R, P_i prime. By 6.15 there exists a chain $Q_0 \subsetneq ... \subsetneq Q_m$ in R', Q_j prime.

"$\geq$" : Let $Q_0 \subsetneq ... \subsetneq Q_m$ be a chain in R', Q_j prime. By 6.13 we have that $Q_0 \cap R \subsetneq ... \subsetneq Q_m \cap R$ is a chain of prime ideals in R.

□

C). Going-Down Theorem

Motivation 6.18.

(a) We want to find a reverse statement to 'Going-Up', i.e. if we have $P \subsetneq P' \in \mathrm{Spec}(R)$ and $P' = Q' \cap R$ with $Q' \in \mathrm{Spec}(R')$, is there a $Q' \supsetneq Q \in \mathrm{Spec}(R')$, such that $Q \cap R = P$?

(b) The problem is, that R' integral over R is *not* sufficient! E.g. choose

$$i : R := {}^{K[x,y,z]}\!\diagup_{\langle x^2-y^2-z^2\rangle} \hookrightarrow K[t,z] =: R'$$

with

$$\overline{x} \mapsto t^3 - t,\ \overline{y} \mapsto t^2 - 1,\ \overline{z} \mapsto z$$

Then $R \cong \operatorname{Im}(i) = K[t^3-t, t^2-1, z] = K[t^3-t, t^2, z]$ and by choosing $f := X^2 - t^2 \in R[X]$ we get $f(t) = 0$ and thus t is integral$_{/R}$. Therefore, as R' is finite$_{/R}$, hence integral. Now choose

$$Q' = \langle t-1, z+1 \rangle \,.$$

Then

$$\begin{aligned} Q' \cap R &= \left\langle t^3 - t, t^2 - 1, z+1 \right\rangle =: P' \\ &= \langle x, y, z+1 \rangle \\ &\supsetneq \left\langle y - (z^2+1), x - zy \right\rangle \\ &= \left\langle t - z^2, (t-z)(t^2-1) \right\rangle \\ &= \langle t - z \rangle \cap R = P \end{aligned}$$

Now assume that there exists a $Q \in \operatorname{Spec}(R)$, such that $Q \cap R = P$ and $Q \subsetneq Q'$. Then

$$(t-1)(t+1)(t-z) = (t-z)(t^2-1) \in Q$$

Thus $t-1 \in Q$ or $t-z \in$ or $t+1 \in Q$. Also:

$$(t-z)(t+z) = t^2 - z^2 \in Q$$

and thus $t - z \in Q$ or $t + z \in Q$. We now have to consider three cases:

- 1st Case: $t - z \in Q \subset Q'$. Then:

$$2 = (t-z) - (t-1) + (z+1) \in Q' \;\lightning$$

- 2nd Case: $t+z, t-1 \in Q$. Then

$$z + 1 = (t+z) - (t-1) \in Q \text{ and thus } Q = Q' \;\lightning$$

- 3rd Case: $t+z, t+1 \in Q \subset Q'$. Then

$$2 = (t+1) - (t-1) \in Q' \;\lightning$$

Hence there is no $Q \in \operatorname{Spec}(R)$ as described a above
Note. $\langle z - t \rangle \cap R = P$, but $\langle z - t \rangle \subsetneq Q'$

The crucial reason for our failure is that R is not normal!

Theorem 6.19 (Going-Down). *Let $R \subseteq R'$ be ID's, R normal (i.e. $\operatorname{Int}_{\operatorname{Quot}(R)}(R) = R$) and R' integral$_{/R}$. Then, given $P, P' \in \operatorname{Spec}(R), Q' \in \operatorname{Spec}(R')$, such that $P \subsetneq P'$ and $P' = Q' \cap R$:*

$$\exists\, Q \in \operatorname{Spec}(R') : Q \subsetneq Q' \text{ and } Q \cap R = P$$

$$\begin{tikzcd} \exists\, Q \arrow[r, dotted, "\subsetneq"] & Q' \\ Q \cap R = P \arrow[u, dotted] \arrow[r, "\subsetneq"] & P' = Q' \cap R \arrow[u] \end{tikzcd}$$

Proof. postponed to 6.24 □

Definition 6.20. Let $R \subseteq R'$ be a ring extension, $I \trianglelefteq R$.

(a) $\alpha \in R'$ is *integral*$_{/I}$

$$:\Longleftrightarrow \exists\, f = x^n + \sum_{j=0}^{n-1} f_j x^j,\ f_j \in I \text{ and } f(\alpha) = 0$$

(b) $\mathrm{Int}_{R'}(I) := \{\alpha \in R' \,|\, \alpha \text{ is integral}_{/I}\}$ is the *integral closure* of I in R'.

Proposition 6.21. *Let $R \subseteq R'$ be a ring extension, $I \trianglelefteq R$. Then:*

$$\mathrm{Int}_{R'}(I) = \sqrt{I \cdot \mathrm{Int}_{R'}(R)} \trianglelefteq \mathrm{Int}_{R'}(R)$$

Proof.

"$\subseteq$": Let $\alpha \in \mathrm{Int}_{R'}(I)$. Then there exist $f_0, ..., f_{n-1} \in I$, such that

$$\alpha^n = -\sum_{j=0}^{n-1} \underbrace{f_j}_{\in I} \underbrace{\alpha^j}_{\in \mathrm{Int}_{R'}(R)} \in I \cdot \mathrm{Int}_{R'}(R)$$

Thus $\alpha \in \sqrt{I \cdot \mathrm{Int}_{R'}(R)}$.

"$\supseteq$": Let $\beta \in \sqrt{I \cdot \mathrm{Int}_{R'}(R)}$.

$$\Longrightarrow \exists\, n : \beta^n \in I \cdot \mathrm{Int}_{R'}(R)$$
$$\Longrightarrow \exists\, a_i \in I, b_i \in \mathrm{Int}_{R'}(R) : \beta^n = \sum_{i=1}^{m} a_i b_i$$

Set $M := R[b_1, ..., b_m]$, which is a finite R-module and consider

$$\varphi : M \to M, \tilde{m} \mapsto \beta^n \tilde{m},$$

which is R-linear. Obviously $\varphi(M) \subseteq I \cdot M$ and by 2.6 there exists

$$\chi_\varphi = x^n + \sum_{i=0}^{n-1} c_j x^j$$

with $c_j \in I^{k-j} \subseteq I$ and $\chi_\varphi(\varphi) = 0$. Thus

$$0 = \chi_\varphi(\varphi)(1) = \chi_\varphi(\beta^n)$$

Thus β^n is integral$_{/I}$ and therefore β is integral$_{/I}$ (just replace x by x^n in the polynomial).

□

Proposition 6.22. *Let R be a normal ID, $K = \operatorname{Quot}(R), K \subseteq K'$ a field extension, $I \trianglelefteq R$ and $\alpha \in \operatorname{Int}_{K'}(I)$. Then α is algebraic over K and the minimal polynomial of α over K is of the form*

$$\mu_\alpha = x^n + \sum_{i=0}^{n-1} a_i x^i \in K[x]$$

with $a_i \in \sqrt{I}$

Proof. Since α is integral$_{/I}$, there exists $0 \neq f = x^m + \sum_{j=0}^{m-1} f_j x^j$ with $f_j \in I$ and $f(\alpha) = 0$. Now let

$$\prod_{i=1}^{n}(x - \alpha_i) = \mu_\alpha = x^n + \sum_{i=0}^{n-1} a_i x^i \in K[x]$$

be the minimal polynomial of α over K, with $\alpha_i \in \overline{K}$, the algebraic closure of K. W.l.o.g. $\alpha_1 = \alpha$. Since $f(\alpha) = 0$, we know that $f \in \langle \mu_\alpha \rangle_{K[x]}$.

$\Longrightarrow \exists\, p \in K[x] : f = p \cdot \mu_\alpha$
$\Longrightarrow 0 = \mu_\alpha(\alpha_i) \cdot p(\alpha_i) = f(\alpha_i)\ \forall\, i = 1..n$
$\Longrightarrow \alpha_i$ integral$_{/I}$
$\Longrightarrow \{a_0, ..., a_{n-1}\} \subseteq \operatorname{Int}_{\overline{K}}(I)$, since $a_i \in \mathbb{Z}[\alpha_1, \cdots, \alpha_n]\, \forall i$
$\overset{a_i \in K}{\Longrightarrow} a_0, ..., a_{n-1} \in \operatorname{Int}_K(I) \overset{6.21}{=} \sqrt{I \cdot \operatorname{Int}_K(R)} = \sqrt{I \cdot R} = \sqrt{I}$, since R is normal.

□

Lemma 6.23. *Let $\varphi : R \to R'$ be a ringhomomorphism, $P \in \operatorname{Spec}(R)$. Then:*

$$\exists\, Q \in \operatorname{Spec}(R') : Q^c = P \iff (P^e)^c = P$$

Proof.

- "$\Longrightarrow$": $P = Q^c \implies P^{ec} = Q^{cec} \overset{1.10}{=} Q^c = P$
- "$\Longleftarrow$": $S := \varphi(R \backslash P) \subset R'$ is multipl. closed. First we show that $P^e \cap S = \emptyset$:

  Assume $\exists\, a \in P^e \cap S$. Then

  $$\varphi^{-1}(a) \subseteq P^{ec} = P$$

  and

  $$\emptyset \neq \varphi^{-1}(a) \cap \varphi^{-1}(S) \subseteq R \backslash P \text{ ↯}$$

  Thus we know that $S^{-1}P^e \subsetneq S^{-1}R'$. Therefore there exists a maximal ideal $\mathfrak{m} \lhd \cdot S^{-1}R'$, such that $S^{-1}P^e \subseteq \mathfrak{m}$.

Now let $Q := \mathfrak{m} \cap R' \in \operatorname{Spec}(R')$ and $Q \cap S = \emptyset$.

$$\begin{aligned}&\Longrightarrow Q^c \cap (R \backslash P) = \emptyset\\ &\Longrightarrow P \subseteq P^{ec} \subseteq Q^c \subseteq P\\ &\Longrightarrow Q^c = P\end{aligned}$$

$\square$

Proof 6.24 (of 6.19)**.** Consider the extensions $R \subseteq R' \subseteq R'_{Q'}$, where

$$P \subsetneq P' = Q' \cap R \subseteq Q' \subseteq Q'_{Q'}$$

By 6.23 and the 1:1 - correspondence of prime ideals under localisation, it suffices to show that

$$P \cdot R'_{Q'} \cap R = P$$

Proof.

"$\supseteq$": 1.10

"$\subseteq$": Let $0 \neq a = \frac{b}{s} \in P \cdot R'_{Q'} \cap R$ with $a \in R, b \in P \cdot R', s \in R' \backslash Q'$.

$$\begin{aligned}\Longrightarrow\ b \in P \cdot R' \subseteq \sqrt{P \cdot R'} = \sqrt{P \cdot \operatorname{Int}_{R'}(R)} &\overset{6.21}{=} \operatorname{Int}_{R'}(P)\\ &\subseteq \operatorname{Int}_{K'}(P) \text{ where } K' = \operatorname{Quot}(R')\end{aligned}$$

If we set $K := \operatorname{Quot}(R)$ and apply 6.22, we get that

$$\mu_b = x^n + \sum_{i=0}^{n-1} a_i x^i \in K[x], a_i \in \sqrt{P} = P$$

is the minimal polynomial of $b_{/K}$.

Now consider the isomorphism

$$\varphi : K[x] \to K[x], x \mapsto ax$$

Then

$$f := \frac{1}{a^n} \cdot \varphi(\mu_b) = x^n + \sum_{i=0}^{n-1} \frac{a_i}{a^{n-i}} x^i \in K[x] \text{ is irreducible}$$

Since $f(s) = \frac{1}{a^n}\mu_b(b) = 0$, we know that $f = \mu_s$ is the minimal polynomial of s over K. Furthermore, since $s \in \operatorname{Int}_{R'}(R) \subseteq \operatorname{Int}_{K'}(R)$ and by applying 6.22, we get that

$$b_i := \frac{a_i}{a^{n-i}} \in R$$

Thus

$$\underbrace{a^{n-i}}_{\in R}\underbrace{b_i}_{\in R} = a_i \in P \in \operatorname{Spec}(R)$$

Now assume $a \notin P$. Then $b_i \in P$ for all $i = 0, ..., n-1$.

$$\begin{aligned}
&\Longrightarrow s^n = \underbrace{f(s)}_{=0} - \sum_{i=0}^{n-1} \underbrace{b_i}_{\in P} s^i \in P \cdot R' \subseteq P' \cdot R' \subseteq Q' \\
&\Longrightarrow s \in Q', \text{since } Q' \in \operatorname{Spec}(R') \lightning
\end{aligned}$$

Thus $a \in P$.

$\square$

Example 6.25. Is also $\operatorname{codim}(Q) = \operatorname{codim}(Q \cap R)$?

Let $R = K[x,y] \hookrightarrow K[x,y,z]/\langle z(x-z), zy\rangle := R'$ and $Q = \langle \overline{z-1}, \overline{x-1}, \overline{y}\rangle \in \operatorname{Spec}(R')$. Then

- $\operatorname{codim}(Q) = \dim R_Q = 1$
- $\operatorname{codim}(Q \cap R) = \operatorname{codim}(\langle x-1, y\rangle) = 2 > \operatorname{codim}(Q)$

Proposition 6.26.

(a) R' integral$_{/R}$, $Q \in \operatorname{Spec}(R')$ $\Longrightarrow \operatorname{codim}(Q) \leq \operatorname{codim}(R \cap Q)$

(b) R' integral$_{/R}$, R normal and R, R' IDs, $Q \in \operatorname{Spec}(R)$

$$\Longrightarrow \operatorname{codim}(Q) = \operatorname{codim}(R \cap Q)$$

Proof.

(a) 6.13

(b) 6.19

$\square$

Philosophy 6.27. *Applying "going-up" preserves dimension and applying "going-down" preserves codimension.*

7. Hilbert's Nullstellensatz, Noether Normalisation, Krull Dimension

A). Hilbert's Nullstellensatz

Theorem 7.1 (Algebraic HNS)**.** *Let $K \subseteq K'$ be a field extension such that*

$$K' = K[\alpha_1, ..., \alpha_n]$$

is a finitely generated K-algebra. Then K' is finite$_{/K}$, in particular it is algebraic$_{/K}$.

Proof. (due to Zariski) We do an induction on n:

- ($n = 1$): Suppose α_1 is *not* algebraic$_{/K}$. Then α_1 is transcendental$_{/K}$. Then

  $$K[x] \cong K[\alpha_1] = K' \text{ by } x \mapsto \alpha_1 \ \lightning$$

  which is a contradiction, since K' is a field. Thus α_1 is algebraic$_{/K}$, hence $K[\alpha_1]$ is finite$_{/K}$ by 6.3/6.4.

- ($n - 1 \to n$):
  Note. K' finite$_{/K}$ $\iff$ $\alpha_1, ..., \alpha_n$ algebraic$_{/K}$

  Suppose that w.l.o.g. α_1 is *not* algebraic$_{/K}$. Then $R := K[\alpha_1] \cong K[x]$ is integrally closed in L. Now consider

  $$K \subseteq R = K[\alpha_1] \subseteq \mathrm{Quot}(R) = K(\alpha_1) =: L \subseteq K' = R[\alpha_2, ..., \alpha_n] = L[\alpha_2, ..., \alpha_n]$$

  (the last equality holds, since $L \subseteq K'$). By induction we get that $\alpha_2, ..., \alpha_n$ are algebraic$_{/L}$. Thus

  $$\exists\, \mu_{\alpha_i} = x^{n_i} + \sum_{j=0}^{n_i-1} \frac{a_{ij}}{b_{ij}} x^j \in L[x];\ \mu_{\alpha_i}(\alpha_i) = 0;\ a_{ij}, b_{ij} \in R = K[\alpha_1]$$

  Now set

  $$f := \prod_{i=2}^{n} \prod_{j=0}^{n_i-1} b_{ij} \in R \implies \mu_{\alpha_i} \in R_f[x]$$

  Therefore $\alpha_2, ..., \alpha_n$ are integral$_{/R_f}$ and by 6.4 $K' = R[\alpha_2, ..., \alpha_n] = R_f[\alpha_2, ..., \alpha_n]$ is integral$_{/R_f}$. Since $L \subseteq K'$, L is also integral$_{/R_f}$. Hence:

  $$K(x) \cong \mathrm{Quot}(R) = L = \mathrm{Int}_L(R_f) \overset{L=L_f}{=} \mathrm{Int}_{L_f}(R_f) = \underbrace{(\mathrm{Int}_L(R))}_{=R}{}_f = R_f \ \lightning$$

□

Corollary 7.2. *Let K be an algebraically closed field. Then:*

$$\mathfrak{m} \lhd \cdot K[x_1, ..., x_n] \iff \exists\, \underline{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n : \mathfrak{m} = \langle x_1 - a_1, \cdots, x_n - a_n \rangle$$

Proof.

- "$\Longleftarrow$": Consider the map $\varphi_{\underline{a}} : K[\underline{x}] \to K; x_i \mapsto a_i$, which is surjective, where $\ker(\varphi_{\underline{a}}) = \langle x_1 - a_1, \cdots, x_n - a_n \rangle$:

  Since "$\supseteq$" is clear, we only have to show "$\subseteq$": By applying the Horner Schema, every polynomial in $K[\underline{x}]$ can be written as

  $$f = \sum_{i=1}^{n} g_i (x_i - a_i) + r$$

  So obviously $f \in \ker(\varphi_{\underline{a}}) \iff r = f(\underline{a}) = 0$.

  Thus ${K[\underline{x}]}/{\mathfrak{m}} \cong K$, which is a field, hence $\mathfrak{m}$ is maximal.

- "$\Longrightarrow$": Let $\mathfrak{m} \lhd \cdot K[\underline{x}]$. Then $K' = {K[\underline{x}]}/{\mathfrak{m}}$ is a field and a finitely generated K - algebra via $i : K \to {K[\underline{x}]}/{\mathfrak{m}}, a \mapsto \overline{a}$, generated by $\overline{x_1}, ..., \overline{x_n}$. Then by 7.1 K' is algebraic$_{/K}$ and since K is algebraically closed we have that $K = K'$. In particular i is surjective.

  $$\Longrightarrow \exists\, a_1, ..., a_n \in K : \overline{a_i} = i(a_i) = \overline{x_i}$$

  Thus $\overline{x_i} - \overline{a_i} = \overline{0}$, i.e. $x_i - a_i \in \mathfrak{m}$. Thus $\langle x_1 - a_1, \cdots, x_n - a_n \rangle \subseteq \mathfrak{m}$ and since both are maximal, we know that $\langle x_1 - a_1, \cdots, x_n - a_n \rangle = \mathfrak{m}$

□

Corollary 7.3. *If $I \trianglelefteq K[\underline{x}] =: R, I \subsetneq K[\underline{x}]$, then:*

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{m} \lhd \cdot K[\underline{x}]} \mathfrak{m}$$

Proof. Since "$\subseteq$" is clear by 1.15, we only have to show "$\supseteq$":

Let $f \notin \sqrt{I}$

$$\begin{aligned} &\Longrightarrow I_f \subsetneq R_f \\ &\Longrightarrow \exists\, \mathfrak{n} \lhd \cdot R_f : I_f \subseteq \mathfrak{n} \not\ni f \\ &\Longrightarrow I \subseteq I_f \cap R \subseteq \mathfrak{n} \cap R =: \mathfrak{m} \not\ni f \end{aligned}$$

We need to show that $\mathfrak{m} \lhd \cdot R$: Consider the canonical inclusions:

$$K \hookrightarrow R/\mathfrak{m} \hookrightarrow R_f/\mathfrak{n} = K\left[\underline{x}, \frac{1}{f}\right]/\mathfrak{n} =: K'$$

where K' is a finitely generated K - algebra. By 7.1 $R_f/\mathfrak{n}$ is finite$_{/K}$, hence integral$_{/K}$ by 6.4. Thus $R_f/\mathfrak{n}$ is also integral$_{/R/\mathfrak{m}}$. By 6.10(b) $R/\mathfrak{m}$ is a field, thus $\mathfrak{m} \lhd \cdot R$. □

Notation 7.4. For $I \trianglelefteq K[\underline{x}]$ we set

$$V(I) := \{\underline{a} \in K^n \mid f(\underline{a}) = 0 \,\forall\, f \in I\}$$

the *vanishing set* of I.

For $V \subseteq K^n$ we set

$$I(V) := \{f \in K[\underline{x}] \mid f(\underline{a}) = 0 \,\forall\, \underline{a} \in V\}$$

the *vanishing ideal* of V.

Corollary 7.5 (Geometric HNS)**.** *If $K = \overline{K}$ and $I \trianglelefteq K[\underline{x}]$, then*

$$I(V(I)) = \sqrt{I}$$

Proof.

"$\supseteq$" Let $f \in \sqrt{I}$

$$\begin{aligned}
&\Longrightarrow \exists\, n : f^n \in I \\
&\Longrightarrow \forall\, \underline{a} \in V(I) : f^n(\underline{a}) = (f(\underline{a}))^n = 0^n = 0 \\
&\Longrightarrow f \in I(V(I))
\end{aligned}$$

"$\subseteq$" Let $f \notin \sqrt{I}$

$$\begin{aligned}
&\overset{7.3}{\Longrightarrow} \exists\, \mathfrak{m} \lhd \cdot K[\underline{x}], I \subseteq \mathfrak{m} : f \notin \mathfrak{m} \\
&\overset{7.2}{\Longrightarrow} \exists\, \underline{a} \in K^n : \mathfrak{m} = \langle x_1 - a_1, \cdots, x_n - a_n \rangle \not\ni f \\
&\overset{I \subseteq \mathfrak{m}}{\Longrightarrow} \forall\, g \in I : g(\underline{a}) = 0 \\
&\Longrightarrow \underline{a} \in V(I)
\end{aligned}$$

Now suppose that $f(\underline{a}) = 0$. Then $f \in I(\{\underline{a}\}) \supseteq \mathfrak{m}$. Thus, since $\mathfrak{m}$ is maximal and $f \notin \mathfrak{m}$ we have that $K[\underline{x}] = \langle \mathfrak{m}, f \rangle \subseteq I(\{a\})$ ↯, which is a contradiction to $1(\underline{a}) \neq 0$.

Thus $f(\underline{a}) \neq 0$ and $f \notin I(V(I))$.

□

Geometrical interpretation 7.6. When K is algebraically closed, we have:

- 7.2 $\Longrightarrow \mathfrak{m}-\mathrm{Spec}(K[\underline{x}]) \overset{1:1}{\longleftrightarrow} K^n$
- 7.5 $\Longrightarrow$

$$\{\text{prime ideals}\} \overset{1:1}{\longleftrightarrow} \{\text{irred. subvarieties of } K^n\}$$
$$\{\text{radical ideals}\} \overset{1:1}{\longleftrightarrow} \{\text{subvarieties of } K^n\}$$

Corollary 7.7. *Let K be a field and let $f \in K[x_1, \ldots, x_n] \setminus K$. Then:*

(a) $\dim(K[x_1, \ldots, x_n]) = n$.

(b) $\dim(K[x_1, \ldots, x_n]/\langle f\rangle) = n - 1$.

Proof. By Proposition 6.8 we know that for any $g \in K[x_1, \ldots, x_n]$ the ring extension

$$K[x_1, \ldots, x_n]/\langle g\rangle \hookrightarrow \overline{K}[x_1, \ldots, x_n]/\langle g\rangle$$

is integral. We thus get

$$\begin{aligned}\dim\left(K[\underline{x}]/\langle g\rangle\right) &\overset{6.17}{=} \dim\left(\overline{K}[\underline{x}]/\langle g\rangle\right)\\ &\overset{Def.}{=} \sup\left\{\mathrm{codim}(\mathfrak{m}/\langle g\rangle) \mid \mathfrak{m} \lhd \cdot\, \overline{K}[\underline{x}], g \in \mathfrak{m}\right\}\\ &\overset{7.2}{=} \sup\left\{\mathrm{codim}(\langle x_1 - a_1, \ldots, x_n - a_n\rangle/\langle g\rangle) \mid \underline{a} \in \overline{K}^n, g(\underline{a}) = 0\right\}.\end{aligned}$$

However, by Corollary 5.32 and 5.33 we know for $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n\rangle$

$$\mathrm{codim}\big(\mathfrak{m}/\langle g\rangle\big) \overset{5.31}{=} \dim\left(\overline{K}[\underline{x}]_{\mathfrak{m}}/\langle g\rangle\right) \overset{5.32/5.33}{=} \begin{cases} n, & \text{if } g = 0,\\ n-1, & \text{if } g = f,\end{cases}$$

since f is neither a unit, nor a zero-divisor in the localised ring $\overline{K}[\underline{x}]_{\mathfrak{m}}$. $\square$

B). Noether Normalisation

Definition 7.8.

(a) Let $R \subseteq R'$ be a ring extension; $\alpha_1, ..., \alpha_n \in R', n \geq 0$

(1) $\alpha_1, ..., \alpha_n$ are *algebraically independent*$_{/R}$

$$\begin{aligned}&:\Longleftrightarrow \varphi_{\underline{\alpha}} : R[x_1, ..., x_n] \twoheadrightarrow R[\alpha_1, \cdots, \alpha_n]\ , x_i \mapsto a_i \text{ is an isomorphism}\\ &\Longleftrightarrow \ker(\varphi_{\underline{\alpha}}) = \{0\}\\ &\Longleftrightarrow\ \nexists\, 0 \neq f \in R[\underline{x}] : f(\alpha_1, ..., \alpha_n) = 0\\ &\Longleftrightarrow \forall\ i = 1, \ldots, n\ :\ \alpha_i \text{ is transcendental }_{/R[\alpha_1, \ldots, \alpha_{i-1}]}\end{aligned}$$

(2) $\operatorname{trdeg}_R(R') := \sup\{d \mid \exists\, \alpha_1, ..., \alpha_d \in R' \text{ alg. indep.}_{/R}\}$ is the *transcendence degree* of R' over R.

(b) Let K be a field, R a K-algebra. A finite, injective K-algebra-homomorphism

$$\varphi : K[y_1, ..., y_d] \hookrightarrow R$$

is called a *Noether Normalisation* (NN) of R.
Note.

$$\varphi : R \to R' \text{ finite } \iff R' \text{ is a finitely gen. } \varphi(R)\text{-module}$$

If φ is injective, then $\varphi(R) \cong R$ and this is equivalent to saying that R' is a finitely generated R-module

Theorem 7.9 (NN)**.** *Let $|K| = \infty$ and R a finitely generated K-algebra. Then:*
$\exists\, \beta_1, \ldots, \beta_d \in R$ algebr. indep.$_{/K}$, such that

$$K[\beta_1, \ldots, \beta_d] \overset{\text{finite!}}{\hookrightarrow} R$$

is a NN. More precisely:

If $R = K[\alpha_1, ..., \alpha_n]$, then

$$\exists\, M = \begin{array}{c} \left(\begin{array}{c|c} I & * \\ \hline 0 & A \end{array}\right) \begin{array}{l} \}\, d \\ \}\, n-d \end{array} \\ \begin{array}{cc} \underbrace{\quad}_{d} & \underbrace{\quad}_{n-d} \end{array} \end{array} \in \operatorname{Mat}(n \times n, K), A = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix},$$

such that $\underline{\beta} := M\underline{\alpha}$ satisfies that

(a) $\beta_1, ..., \beta_d \in R$ are algebraically independent$_{/K}$, and

(b) β_i integral$_{/K[\beta_1,...,\beta_{i-1}]}$ for all $i > d$.

In particular, $K[\beta_1, \ldots, \beta_n] = R$ and $\dim(R) = d$.

Note. The main statement follows from the 'More precisely'-part, since:

- $\beta_1, ..., \beta_d$ algebr. indep.$_{/K}$ $\implies$ the inclusion $K[\beta_1, ..., \beta_d] \hookrightarrow R$ is injective
- $\underline{\beta} = M\underline{\alpha} \implies R = K[\beta_1, ..., \beta_n]$ (since $\alpha_n = \beta_n, \alpha_{n-1} = \beta_{n-1} - a_{n-1,n}\beta_n$, etc...)
- β_i integral$_{/K[\beta_1,...,\beta_{i-1}]}$ yields finiteness of the inclusion: $R = K[\beta_1, ..., \beta_n] = K[\beta_1, ..., \beta_{n-1}][\beta_n]$. Since β_n is algebraic$_{/K[\beta_1,...,\beta_{n-1}]}$, R is finite over $K[\beta_1, ..., \beta_{n-1}]$ by 6.4(c); induction and 6.4(b) yields that R is finite$_{/K[\beta_1,...,\beta_d]}$.

Proof. Postponed to 7.14 □

Remark 7.10.

(a) We will see later, that $\operatorname{trdeg}_K(R) = \dim R$*, the Krull dimension of* R.

(b) $\underline{\beta} = M\underline{\alpha}$ *implies that* β_i *is a linear combination of the* α_j*. The main statement also holds for* $|K| < \infty$*, but then we cannot choose the* β_i *as* linear *combinations of the* α_j.

(c) If we identify M *with a vector in* K^m*, where* $m = \frac{(n-d)(n+d-1)}{2}$ *is the number of* $*$*-elements, there exists a Zariski-open subset* $U \subseteq K^m$*, such that any* $M \in U$ *is a suitable coordinate change for 7.9, i.e. the non-suitable ones satisfy a polynomial relationship (*$\exists\, f_1, ..., f_m \in K[z_1, ..., z_m]$ *such that* $p \in U \iff f_i(p) \neq 0$ *for some* i*).*

(d) If K *is algebraically closed and* R *is an integral domain we can choose* $\beta_1, \dots, \beta_d$ *in such a way that the field extension* $K(\beta_1, \dots, \beta_d) \subseteq \operatorname{Quot}(R)$ *is separable.*

Example 7.11.

(a) $K[\overline{y+1}] \subseteq K[x,y]/\langle xy\rangle$ is *not* finite, since $\overline{x}$ is not integral$_{/K[\overline{y+1}]}$. Suppose that

$$\begin{aligned}
& x^k + \sum_{i=0}^{k-1} \underbrace{a_i}_{\in K[y+1]} x^i \in \langle xy\rangle \\
\Longrightarrow\, & x^k + \sum_{i=1}^{k-1} b_i x^i + \underbrace{a_0}_{\in K[y+1]} \in \langle xy\rangle \text{ with } b_i = \text{ const.term of } a_i \\
\Longrightarrow\, & a_0, b_i = 0 \,\forall\, i \\
\Longrightarrow\, & x^k \in \langle xy\rangle \ \lightning
\end{aligned}$$

(b) $K[\overline{x+y}] \subseteq K[x,y]/\langle xy\rangle$ is finite, thus a NN.

$$\begin{aligned}
& p = z^2 - (\overline{x+y})z \\
\Longrightarrow\, & p(\overline{x}) = p(\overline{y}) = 0 \\
\Longrightarrow\, & \overline{x}, \overline{y} \text{ integral}_{/K[\overline{x+y}]}, \text{ hence finite}
\end{aligned}$$

(c) (Geometric interpretation) Let $V = V(I) \subseteq K^n, I \trianglelefteq K[\underline{x}]$. Then

$$\exists \text{ a linear subspace } H = \left\langle \tilde{M}_1^t, ..., \tilde{M}_d^t \right\rangle \subseteq K^n$$

of dimension d, such that the projection of V to H has finite fibers. The idea is, that the inclusion $K[y_1, ..., y_d] \hookrightarrow K[\underline{x}]/I$ corresponds inversely to the projection $K^d = H \longleftarrow V(I)$.

Recall that for $M = \begin{pmatrix} I_n & A \\ 0 & B \end{pmatrix}$ we have $M^{-1} = \begin{pmatrix} I_n & -AB^{-1} \\ 0 & B^{-1} \end{pmatrix}$ and if we set $\tilde{M} := \begin{pmatrix} -AB^{-1} \\ B^{-1} \end{pmatrix}$, then $H = \ker(\tilde{M}^t)$.

(d) While NN corresponds to projection, normalisation corresponds to parametrisation: Let $I = \langle y^2 - xz, yx^2 - z^2, x^3 - yz \rangle \trianglelefteq K[x,y,z]$, then consider

$$R := K[x,y,z]/I \hookrightarrow K[t], x \mapsto t^3, y \mapsto t^4, z \mapsto t^5$$

Then $R \cong K[t^3, t^4, t^5]$ and the map $t \mapsto (t^3, t^4, t^5)$ is a parametrisation of the curve $V(I)$.

Lemma 7.12. *Let $|K| = \infty$ and $0 \neq f \in K[x_1, ..., x_n]$. Then:*

$$\exists\, a_1, ..., a_n \in K\backslash\{0\} : f(\underline{a}) \neq 0$$

Note. If $K = \mathbb{Z}/2\mathbb{Z}$ (i.e. finite), $f = (z-1)z \in K[z]$ vanishes everywhere.

Moreover, if f is homogenous, then we may assume that $a_n = 1$.

Proof. We do an induction on n

- $n = 1$: $|\{a \in K \,|\, f(a) = 0\}| \leq \deg(f) < \infty$. Since $|K| = \infty, \exists\, a \in K\backslash\{0\}$: $f(a) \neq 0$
- $n-1 \to n$: $f = \sum_{i=0}^k f_i x_n^i$ with $f_i \in K[x_1, ..., x_{n-1}]$ and $f_k \neq 0$. Then by induction there exist $a_1, ..., a_{n-1} \in K\backslash\{0\}$, such that $f_k(a_1, ..., a_{n-1}) \neq 0$.

$$\Longrightarrow 0 \neq f(a_1, ..., a_{n-1}, x_n) \in K[x_n]$$
$$\overset{n=1}{\Longrightarrow} \exists\, a_n \in K\backslash\{0\} : f(a_1, ..., a_n) \neq 0$$

Moreover, if f is homogenous of degree k, then

$$0 \neq f(\underline{a}) = a_n^k f(\frac{a_1}{a_n}, ..., \frac{a_n}{a_n} = 1)$$

□

Lemma 7.13. *Let $0 \neq f = f_0 + ... + f_k \in K[\underline{x}], f_i$ homogenous of degree i and $a_1, ..., a_{n-1} \in K$, such that $f_k(a_1, ...a_{n-1}, 1) = 1$. Now consider the map*

$$\psi_{\underline{a}} : K[\underline{x}] \to K[\underline{x}] : x_i \mapsto \begin{cases} x_n & , i = n \\ x_i + a_i x_n & , i < n \end{cases}$$

i.e. the coordinate change by $M = \begin{pmatrix} 1 & 0 & 0 & a_1 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & a_{n-1} \\ 0 & \dots & 0 & 1 \end{pmatrix}^t$. *Then:*

$$\psi_{\underline{a}}(f) = x_n^k + \sum_{i=0}^{k-1} c_i x_n^i, c_i \in K[x_1, ..., x_{n-1}]$$

is monic in x_n.

Proof.

Let

$$\begin{aligned}
\psi_{\underline{a}}(f_k) &= \sum_{|\alpha|=0}^{k} b_\alpha x_1^{\alpha_1} \cdot ... \cdot x_{n-1}^{\alpha_{n-1}} \cdot x_n^{k-|\alpha|}, \alpha = (\alpha_1, ..., \alpha_{n-1}) \\
\Longrightarrow f_k &= \sum_{|\alpha|=0}^{k} b_\alpha (x_1 - a_1 x_n)^{\alpha_1} \cdot ... \cdot (x_{n-1} - a_{n-1} x_n)^{\alpha_{n-1}} \cdot x_n^{|\alpha|-k} \\
\Longrightarrow b_{(0,...,0)} &= f_k(a_1, ..., a_{n-1}, 1) = 1 \\
\Longrightarrow \psi_{\underline{a}}(f_k) &= x_n^k + \sum_{|\alpha|=1}^{k} b_\alpha x_1^{\alpha_1} \cdot ... \cdot x_{n-1}^{\alpha_{n-1}} \cdot \underbrace{x_n^{k-|\alpha|}}_{k-|\alpha|<k\,!} \\
\Longrightarrow \psi_{\underline{a}}(f) &= \psi_{\underline{a}}(f_k) + ... + \underbrace{\psi_{\underline{a}}(f_0)}_{\deg<k} = x_n^k + \sum_{i=0}^{k-1} c_i x_n^i, c_i \in K[x_1, ..., x_{n-1}]
\end{aligned}$$

□

Proof 7.14 (of 7.9)**.**

We do the proof by induction on n, where $R = K[\alpha_1, \dots, \alpha_n]$.

If $n = 1$ we set $M = (1)$ and $\beta_1 = \alpha_1$. If α_1 is trancendental over K we are done with $d = 1$. Otherwise, there is a monic polynomial $0 \neq p \in K[x_1]$ such that $p(\alpha_1) = 0$, so that indeed α_1 is integral over K. Thus we are done with $d = 0$.

Let now $n > 1$. If $\alpha_1, \dots, \alpha_n$ are algebraically independent, we are done with $M = I_{n\times n}$ and $d = n$. Otherwise there exists an $f = f_0 + ... + f_k \in K[x_1, ..., x_n]$ with $f_k \neq 0$, f_i homogenous of degree i , such that

$$f(\alpha_1, ..., \alpha_n) = 0.$$

Applying 7.12 to f_k yields:

$$\exists\, a_1, ..., a_{k-1} \in K\setminus\{0\} : \xi := f_k(a_1, ..., a_{k-1}, 1) \neq 0$$

Dividing f_k by ξ, we may assume that $f_k(a_1, ..., a_{k-1}, 1) = 1$.

Applying 7.13 yields that $p = \psi_{\underline{a}}(f) = x_n^k + \sum_{j=0}^{k-1} c_j x_n^j \in K[\underline{x}]$ satisfies

$$p(\beta_1', ..., \beta_n') = f(\alpha_1, ..., \alpha_n) = 0$$

where

$$\underline{\beta'} = \underbrace{\begin{pmatrix} & & -a_1 \\ & I_{n-1} & \vdots \\ & & -a_{n-1} \\ & 0 & 1 \end{pmatrix}}_{=:M'} \underline{\alpha}$$

Thus $\beta_n' = \alpha_n$ is integral over $K[\beta_1', ..., \beta_{n-1}']$.

Applying induction to $K[\beta_1', \ldots, \beta_{n-1}']$ there exists an $M'' \in \mathrm{Mat}(n-1 \times n-1, K)$ as in 7.9, such that

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix} = M'' \begin{pmatrix} \beta_1' \\ \vdots \\ \beta_{n-1}' \end{pmatrix}$$

satisfies $\beta_1, ..., \beta_d$ algebraically indep.$_{/K}$ and β_i is integral over $K[\beta_1, ..., \beta_{i-1}] \, \forall \, i > d$.

Set $M := \begin{pmatrix} M'' & 0 \\ 0 & 1 \end{pmatrix} \cdot M' \in \mathrm{Mat}(n \times n, K)$, which is of suitable form and then

$$M\underline{\alpha} = \begin{pmatrix} M'' & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \beta_1' \\ \vdots \\ \beta_n' \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n = \beta_n' = \alpha_n \end{pmatrix}$$

Note. M is a product of matrices where just one column is *not* the unit vector and these entries satisfy a polynomial relation of the form $f(a) \neq 0$. Thus the entries of a non-suitable matrix form a Zariski-closed subset!

□

Proof of Remark 7.10 d. We want to show that we may choose $\beta_1, \ldots, \beta_d$ such that $\mathrm{Quot}(R)$ is separable over $K(\beta_1, \ldots, \beta_d)$, if K is algebraically closed.

Since in characteristic zero every field extension is separable we may assume that $\mathrm{char}(K) = p > 0$.

In the proof of Theorem 7.9 we can assume that the polynomial f is irreducible since otherwise we can replace it by some irreducible factor vanishing at $(\alpha_1, \ldots, \alpha_n)$. Suppose now that f is separable in some variable, w.l.o.g. in x_n, then $\mathrm{Quot}(R) = K(\beta_1, \ldots, \beta_n)$ is separable over $K(\beta_1, \ldots, \beta_{n-1})$ and continuing inductively as above we find that $\mathrm{Quot}(R)$ is separable over $K(\beta_1, \ldots, \beta_d)$ as a tower of separable extensions.

It thus remains to show that f cannot be inseparable in all variables. For this we recall that f is inseparable in x_i if and only if $f \in K[x_1, \ldots, x_i^p, \ldots, x_n]$. Thus f is inseparable in all variables if and only if there is some polynomial $g = \sum_\gamma c_\gamma \cdot \underline{x}^\gamma \in K[x_1, \ldots, x_n]$ such that

$$f = g\big(x_1^p, \ldots, x_n^p\big).$$

We now choose a p-th root $\sqrt[p]{c_\gamma} \in K$ in the algebraically closed field K for each coefficient c_γ of g and set

$$h = \sum_\gamma \sqrt[p]{c_\gamma} \cdot \underline{x}^\gamma \in K[x_1, \ldots, x_n],$$

then

$$h^p = g\big(x_1^p, \ldots, x_n^p\big) = f,$$

since in characteristic p we have $(a+b)^p = a^p + b^p$. However, this contradicts the irreducibility of f. $\square$

Lemma 7.15. *Let R be an ID and let $K[\underline{y}] \hookrightarrow R$ be integral. Suppose moreover that $Q, \tilde{Q} \in \operatorname{Spec}(R)$ s.t. $Q \subsetneq \tilde{Q}$ and there is no $Q' \in \operatorname{Spec}(R)$ s.t. $Q \subsetneq Q' \subsetneq \tilde{Q}$. Then $Q^c \subsetneq \tilde{Q}^c$ and there is no $P \in \operatorname{Spec}(K[\underline{y}])$ s.t. $Q^c \subsetneq P \subsetneq \tilde{Q}^c$.*

Proof. Since R is integral over $K[\underline{y}]$ we deduce from Corollary 6.13 that $Q^c \subsetneq \tilde{Q}^c$, which proves the first part.

Suppose now there is a prime ideal P in $K[\underline{y}]$ strictly between Q^c and $\tilde{Q}^c$. By Proposition 6.8 we know that the extension

$$K[\underline{y}]/Q^c \hookrightarrow R/Q \tag{7.1}$$

is integral again. Applying Noether Normalisation 7.9 to the K-algebra $K[\underline{y}]/Q^c$ we get a finite extension

$$K[\underline{z}] \hookrightarrow K[\underline{y}]/Q^c, \tag{7.2}$$

and Corollary 6.13 implies the strict inclusion of prime ideals

$$0 = Q^c/Q^c \cap K[\underline{z}] \subsetneq P/Q^c \cap K[\underline{z}] \subsetneq \tilde{Q}^c/Q^c \cap K[\underline{z}]. \tag{7.3}$$

Combining the integral extensions in (B)) and (7.2) we get an integral extension

$$K[\underline{z}] \hookrightarrow R/Q$$

and the last prime ideal in (7.3) coincides with the contraction $\tilde{Q}/Q \cap K[\underline{z}]$ under this extension. Applying Going-Down 6.19 we therefore find a prime ideal Q'/Q in R/Q with

$$Q'/Q \subsetneq Q/Q$$

and $Q'/Q \cap K[\underline{z}] = P/Q^c \cap K[\underline{z}] \neq 0$, which then implies

$$Q \subsetneq Q' \subsetneq \tilde{Q},$$

in contradiction to our assumption. $\square$

Definition 7.16. A ring R is called *catenarian* $:\Longleftrightarrow$ between any two given prime ideals $Q \subseteq Q'$ all maximal chains of primes ideals have the same finite length.

Theorem 7.17 (strong form of 5.31)**.**

$$P \in \operatorname{Spec}(K[\underline{x}]) \implies {}^{K[\underline{x}]}\!/\!_{P} \textit{ is catenarian with } \dim(K[\underline{x}]/P) = n - \operatorname{codim}(P)$$

In particular, all maximal chains of prime ideals in $K[\underline{x}]/P$ have the same length.

Proof. It suffices to prove the "in particular" part and the dimesion statement, and for this we consider two cases:

- ($P = 0$): We do an induction on n (where $\underline{x} = (x_1, ..., x_n)$)
  - $n = 0$: ✓
  - $n - 1 \to n$: Since $\dim(K[\underline{x}]) = n$ by Corollary 7.7 each maximal chain of prime ideals in R is finite.

    So let $0 = P_0 \subsetneq ... \subsetneq P_m \lhd \cdot K[\underline{x}]$ be any maximal chain of prime ideals. Choose any $0 \neq f \in P_1$ irreducible. Since the chain is maximal, we necessarily must have $P_1 = \langle f \rangle$.

    $$\implies \overline{0} = {}^{P_1}\!/\!_{\langle f \rangle} \subsetneq ... \subsetneq {}^{P_m}\!/\!_{\langle f \rangle}$$

    is a maximal chain of prime ideals in ${}^{K[\underline{x}]}\!/\!_{\langle f \rangle}$. Applying 7.20 and 7.9 yields a NN

    $$R = K[y_1, ..., y_{n-1}] \overset{\text{finite}}{\hookrightarrow} {}^{K[\underline{x}]}\!/\!_{\langle f \rangle}$$

    By 7.15 we get, that

    $$R \cap {}^{P_1}\!/\!_{\langle f \rangle} \subsetneq ... \subsetneq R \cap {}^{P_m}\!/\!_{\langle f \rangle}$$

    is a maximal chain in R. By induction we derive

    $$m = \dim(R) + 1 = n$$

- ($P \neq 0$): Let $0 = \overline{P_0} \subsetneq ... \subsetneq \overline{P_m}$ be a maximal chain of prime ideals in ${}^{K[\underline{x}]}\!/\!_{P}$

  $$\implies \exists\, P_0 \subsetneq ... \subsetneq P_m, \text{ such that } \overline{P_i} = {}^{P_i}\!/\!_{P}$$
  $$\implies \exists \text{ chain } 0 = L_0 \subsetneq ... \subsetneq L_k = P = P_0 \subsetneq ... \subsetneq P_m$$

  which is a chain in R and where $k = \operatorname{codim}(P)$. By applying the first case we derive $m = n - k$.

$\square$

Corollary 7.18. *If R is a noetherian ring where all maximal chains of prime ideals have the same length and let $f \in R \setminus R^*$ a non-zero divisor, then*

$$\dim(R/\langle f\rangle) = \dim(R) - 1.$$

In particular, if $P \in \operatorname{Spec}(K[\underline{x}])$ and $f \in K[\underline{x}] \setminus K^*$ with $f \notin P$ then

$$\dim\big(K[\underline{x}]/\langle f, P\rangle\big) = \dim(K[\underline{x}]/P) - 1 = n - \operatorname{codim}(P) - 1.$$

Proof. Consider any chain of prime ideals $P_1 \subsetneq \ldots \subsetneq P_k$ in R where P_1 is minimal over f. By Corollary 5.28 the codimension of P_1 is one and thus there is a prime ideal P_0 strictly contained in P_1. By the one-to-one correspondence of prime ideals we see that $\dim(R/\langle f\rangle) \leq \dim(R) - 1$. If the left hand side is infinite the statement holds. Otherwise we may assume that the sequence $P_1 \subsetneq \ldots \subsetneq P_k$ cannot be prolonged, i.e. $\dim(R/\langle f\rangle) = k - 1$. Since $\operatorname{codim}(P_1) = 1$ also the sequence $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_k$ cannot be prolonged, and by the assumption on R this implies that $\dim(R) = k$ as claimed. The in particular part follows from Theorem 7.17. □

Corollary 7.19.

- $\operatorname{Spec}(K[x_1, ..., x_n]) = \dot{\bigcup}_{i=0}^{n} X_i$, *where*
$$X_i := \{P \in \operatorname{Spec}(K[\underline{x}]) \mid \operatorname{codim}(P) = i\}$$
- $X_n = \mathfrak{m} - \operatorname{Spec}(K[\underline{x}]) \overset{\text{if } K=\overline{K}}{=} \{\langle x_1 - a_1, ..., x_n - a_n\rangle\}$
- $X_1 = \{\langle f\rangle \mid f$ *is irreducible*$\}$
- $X_0 = \{\langle 0\rangle\}$

In particular:

$$\operatorname{Spec}(\mathbb{C}[x, y]) = \{\langle x - a, y - b\rangle\} \,\dot{\cup}\, \{\langle f\rangle \mid f \text{ irreducible}\} \,\dot{\cup}\, \{\langle 0\rangle\}$$

Note. In general $\operatorname{codim}(P) = 2 \not\Rightarrow \exists f, g : P = \langle f, g\rangle$

Remark 7.20.

(a) If $K \subseteq L \subseteq M$ are field extensions and M is algebraic over L, then

$$\operatorname{trdeg}_K(L) = \operatorname{trdeg}_K(M).$$

(b) If $I \trianglelefteq K[x_1, \ldots, x_n]$, then $\operatorname{trdeg}_K\big(K[x_1, \ldots, x_n]/I\big) \leq n$.

(c) $\operatorname{trdeg}_K(K[x_1, ..., x_n]) = \operatorname{trdeg}_K(K(x_1, ..., x_n)) = n$

(d) Let R be a finitely generated K-algebra which is an integral domain. Then:

$$\operatorname{trdeg}_K(R) = \operatorname{trdeg}_K\big(\operatorname{Quot}(R)\big).$$

Proof. Exercise □

Corollary 7.21. *If R is a finitely generated K-algebra, then*

$$\dim(R) = \operatorname{trdeg}_K(R).$$

Proof. By Theorem 7.9 we have $\beta_1, \ldots, \beta_d$ in R which are algebraically independent over K where $d = \dim(R)$, so that

$$\operatorname{trdeg}_K(R) \geq \dim(R).$$

It remains to show that $\dim(R) \geq \operatorname{trdeg}_K(R)$.

For that we may assume that $R = K[\underline{x}]/I$ for some ideal I. By Remark 7.20 we know that

$$m = \operatorname{trdeg}_K(R) \leq n < \infty.$$

We will do the proof in two steps:

1) Reduce to the case where I is a prime ideal.

2) Prove the claim when I is prime.

Let $\operatorname{Min}(I) = \{P_1, \ldots, P_k\}$ be the minimal associated prime ideals of I, then $\sqrt{I} = P_1 \cap \ldots \cap P_k$ is a minimal primary decomposition of the radical of I. Choose $a_1, \ldots, a_m \in K[\underline{x}]$ such that their residue classes in R are algebraically independent over K.

Suppose that for each $i = 1, \ldots, k$ the residue classes of the a_j in $K[\underline{x}]/P_i$ are algebraically dependent over K. Then there exist non-zero polynomials $f_i \in K[z_1, \ldots, z_m]$ such that

$$f_i(a_1, \ldots, a_m) \in P_i$$

and $0 \neq f = f_1 \cdots f_k \in K[z_1, \ldots, z_m]$ satisfies

$$f(a_1, \ldots, a_m) \in P_1 \cdots P_k \subseteq P_1 \cap \ldots \cap P_k = \sqrt{I}.$$

But then there is an integer $l \geq 1$ such that

$$f^l(a_1, \ldots, a_m) \in I,$$

in contradiction to the fact that the a_i are algebraically independent over K modulo I. Thus there is some i such that

$$\operatorname{trdeg}_K(R) = m \leq \operatorname{trdeg}_K(K[\underline{x}]/P_i)$$

and

$$\dim(K[\underline{x}]/P_i) \leq \dim(R).$$

It thus suffices to show $\operatorname{trdeg}_K(K[\underline{x}]/P_i) \leq \dim(K[\underline{x}]/P_i)$. In other words, we may assume that I is a prime ideal.

In that case R is an integral domain and by Theorem 7.9 we get a finite Noether normalisation

$$K[y_1,\ldots,y_d]\cong K[\beta_1,\ldots,\beta_d]\subseteq R,$$

where $d=\dim(R)$. This induces an inclusion of the quotient fields

$$K(y_1,\ldots,y_d)\cong K(\beta_1,\ldots,\beta_d)\subseteq \operatorname{Quot}(R),$$

and we claim that this inclusion is algebraic. Now, if $\frac{a}{b}\in\operatorname{Quot}(R)$ then it suffices to show that a and $\frac{1}{b}$ are algebraic over $K(\beta_1,\ldots,\beta_d)$ by Corollary 6.4 (e). Since a and b are elements of R, a and b are integral over $K[\beta_1,\ldots,\beta_d]$. Then a is also algebraic over $K(\beta_1,\ldots,\beta_d)$, and b satisfies a relation of the form

$$\sum_{j=0}^{m} c_j\cdot b^j=0$$

with $c_j\in K[\beta_1,\ldots,\beta_d]$. Multiplying this equation by $\frac{1}{b^m}$ we get

$$\sum_{j=0}^{m} c_{m-j}\cdot\left(\frac{1}{b}\right)^j=0,$$

which shows that $\frac{1}{b}$ is also algebraic over $K(\beta_1,\ldots,\beta_d)$.

Since $\operatorname{Quot}(R)$ is algebraic over $K(\beta_1,\ldots,\beta_d)$ we have

$$\begin{aligned}\operatorname{trdeg}_K(R)\overset{7.20c.}{=}\operatorname{trdeg}_K(\operatorname{Quot}(R))\overset{7.20d.}{=}\operatorname{trdeg}_K\big(K(\beta_1,\ldots,\beta_d)\big)&=\\ \operatorname{trdeg}_K\big(K(y_1,\ldots,y_d)\big)&\overset{7.20a.}{=}d=\dim(R).\end{aligned}$$

$\square$

Corollary 7.22. *In particular, if $P\in\operatorname{Spec}(K[\underline{x}])$ is a prime ideal and $R=K[\underline{x}]/P$, then*

$$\dim(R)=\operatorname{trdeg}_K\big(\operatorname{Quot}(R)\big).$$

Proof. This follows right away from Corollary 7.21 and Remark 7.20 b.. $\square$

8. Valuation Rings and Dedekind Domains

A). Valuation Rings

Definition 8.1.

(a) Let $(G,+)$ be an abelian group, $\leq$ a total ordering on G. We call $(G,+,\leq)$ a *totally ordered group*

$$:\iff (g \leq g', h \in G \implies g+h \leq g'+h)$$

(b) Let K be a field, $(G,+,\leq)$ a totally ordered group. A *valuation* of K in G is a group homomorphism $\nu : (K^*, \cdot) \to (G,+)$, such that

$$\nu(a+b) \geq \min\{\nu(a), \nu(b)\} \;\forall\, a,b \in K^* \text{ with } a+b \neq 0$$

Notation:

$$R_\nu := \{a \in K^* \mid \nu(a) \geq 0\} \cup \{0\} \leq K$$

is a subring of K and called the *valuation ring* (VR) of K with respect to ν.
Note.

- We have to prove, that R_ν is indeed a subring:
  - $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1) \implies \nu(1) = 0 \implies 1 \in R_\nu$
  - $\nu(1) = \nu(-1) + \nu(-1) = 2\nu(-1) \implies \nu(-1) = 0$
  - $\nu(-a) = \nu((-1) \cdot a) = \nu(-1) + \nu(a) = \nu(a) \geq 0 \implies -a \in R_\nu$
- In G, no element $g \neq e$ can have finite order, since otherwise

$$e \lneq g \lneq \dots \lneq kg = e \;\lightning$$

or

$$e \gneq g \gneq \dots \gneq kg = e \;\lightning$$

- $K = \operatorname{Quot}(R_\nu)$

Proof.

"$\supseteq$": ✓

"$\subseteq$": Let $a \in K \backslash R_\nu$

$$\implies \nu\left(\frac{1}{a}\right) = -\underbrace{\nu(a)}_{<0} > 0$$

Thus $\frac{1}{a} \in R_\nu \implies a = \frac{1}{\frac{1}{a}} \in \mathrm{Quot}(R_\nu)$

$\square$

- $a \in K^* \implies a \in R_\nu$ or $\frac{1}{a} \in R_\nu$

If $(G, +, \leq) = (\mathbb{Z}, +, \leq)$ and ν is surjective, then we call ν a *discrete valuation* and R_ν the *discrete valuation ring* (DVR) of ν.

(c) An ID R is called a valuation ring (VR) $:\iff \forall\, 0 \neq a \in \mathrm{Quot}(R) : a \in R$ or $\frac{1}{a} \in R$.

A VR R is called discrete (DVR) $:\iff$ R is noetherian, but not a field.

Example 8.2.

(a) $(\mathbb{R}, +, \leq)$ is a totally ordered group with respect to the usual ordering and so is every subgroup

(b) Every field is a VR

(c) R ID, $K = \mathrm{Quot}(R), (G, +, \leq)$ a tot. ordered group and $\upsilon : R\backslash\{0\} \to G$ a map, such that $\upsilon(ab) = \upsilon(a) + \upsilon(b)$ and $\upsilon(a + b) \geq \min\{\upsilon(a), \upsilon(b)\}$ if $a, b, a + b \neq 0$. Then

$$\nu : K^* \to G : \frac{a}{b} \mapsto \upsilon(a) - \upsilon(b)$$

is a valuation of K.

Proof.

$$\begin{aligned} \frac{a}{b} = \frac{a'}{b'} &\implies ab' = a'b \\ &\implies \upsilon(a) + \upsilon(b') = \upsilon(a') + \upsilon(b) \end{aligned}$$

Hence ν is welldefined. Moreover,

$$\begin{aligned} \nu(\frac{a}{b} \cdot \frac{a'}{b'}) &= \upsilon(aa') - \upsilon(bb') \\ &= \upsilon(a) + \upsilon(a') - \upsilon(b) - \upsilon(b') \\ &= \nu(\frac{a}{b}) + \nu(\frac{a'}{b'}) \end{aligned}$$

and

$$\begin{aligned}\nu(\frac{a}{b}+\frac{a'}{b'}) &= \nu(\frac{ab'+a'b}{bb'})\\ &= \upsilon(ab'+a'b)-\upsilon(bb')\\ &\geq \min\{\upsilon(ab'),\upsilon(a'b)\}-\upsilon(bb')\\ &= \min\{\upsilon(a)+\upsilon(b')-\upsilon(b)-\upsilon(b'),\upsilon(a')+\upsilon(b)-\upsilon(b)-\upsilon(b')\}\\ &= \min\{\nu(\frac{a}{b}),\nu(\frac{a'}{b'})\}\end{aligned}$$

□

(d) R UFD, $K = \mathrm{Quot}(R), p \in R$ prime. Let

$$\upsilon : R\backslash\{0\} \to \mathbb{Z} : a \mapsto n_a, \text{where } a = b \cdot p^{n_a}, p \nmid b$$

Then

$$\begin{aligned}\upsilon(a \cdot a') &= \upsilon(bp^{n_a}, b'p^{n_{a'}})\\ &= \upsilon(bb'p^{n_a n_{a'}})\\ &= n_a + n_{a'} = \upsilon(a)+\upsilon(a')\\ \upsilon(a+a') &= \upsilon(bp^{n_a}+b'p^{n_{a'}})\\ &= \upsilon((b+b'p^{n_a-n_{a'}})p^{n_{a'}})(\text{wlog } n_a \geq n_{a'})\\ &\geq n_{a'} = \min\{\upsilon(a),\upsilon(a')\}\end{aligned}$$

Hence, by applying (c) we know that

$$\nu : K^* \to \mathbb{Z}, \frac{a}{b} \mapsto n_a - n_b$$

is a discrete valuation on K and

$$R_\nu = \{\frac{a}{b} \mid n_a \geq n_b\} = \{\frac{a}{b} \mid p \nmid b\} = R_{\langle p\rangle}$$

is its DVR. Examples for this are:

(1) $R = \mathbb{Z}, K = \mathbb{Q}, p$ prime number $\implies R_\nu = \mathbb{Z}_{\langle p\rangle}$

(2) $R = k[\underline{x}], K = k(\underline{x}), p \in R$ irreducible. Then $R_\nu = k[\underline{x}]_{\langle p\rangle}$ is a DVR.

Note. $\frac{1}{a} \in K \implies \begin{cases} p \mid a & \implies a = (\frac{1}{a})^{-1} \in R_\nu \\ p \nmid a & \implies \frac{1}{a} \in R_\nu \end{cases}$

Proposition 8.3.

An ID R is a VR $\iff R = R_\nu$ for some valuation ν

Proof.

- "$\Longleftarrow$": $R_\nu \subseteq K = \mathrm{Quot}(R_\nu)$. Let $0 \neq a \in K$. Then, as we noticed in the definition: $a \in R_\nu$ or $\frac{1}{a} \in R_\nu$. Hence R is a VR.
- "$\Longrightarrow$": Let $K := \mathrm{Quot}(R)$. Then

$$G = {K^*}\!\big/_{R^*}$$

is an abelian group. Define

$$\overline{a} \geq \overline{b} :\Longleftrightarrow \frac{a}{b} \in R$$

This is well-defined: If $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$ there exist $g, h \in R^*$, such that $a' = ga, b' = hb$ Thus

$$\frac{a}{b} = \frac{a'}{b'} \cdot \underbrace{\frac{g}{h}}_{\in R^*} \Longrightarrow \frac{a}{b} \in R \Longleftrightarrow \frac{a'}{b'} \in R$$

Since R is a VR we know that either $\frac{a}{b} \in R$ or $\frac{b}{a} \in R$, hence "$\geq$" is a total ordering and $\overline{a} \cdot \overline{c} \geq \overline{b} \cdot \overline{c}$ for $\overline{a} \geq \overline{b}, \overline{c} \in G$. Hence $(G, \cdot, \geq)$ is a totally ordered group.

We define

$$\nu : K^* \to G : a \mapsto \overline{a}$$

Then ν is obviously a group homomorphism. Moreover:

$$\begin{aligned} \overline{a} \geq \overline{b} &\Longrightarrow \frac{a}{b} \in R \\ &\Longrightarrow 1 + \frac{a}{b} = \frac{a+b}{b} \in R \\ &\Longrightarrow \nu(a+b) = \overline{a+b} \geq \overline{b} = \min\{\nu(a), \nu(b)\} \end{aligned}$$

Hence ν is a valuation!

$$\begin{aligned} \Longrightarrow R_\nu &= \{a \in K^* \mid \nu(a) \geq e_G = \overline{1} = \nu(1)\} \cup \{0\} \\ &= \{a \in K^* \mid \overline{a} \geq \overline{1}\} \cup \{0\} \\ &= \{a \in K^* \mid a = \frac{a}{1} \in R\} \cup \{0\} \\ &= R \end{aligned}$$

$\square$

Proposition 8.4 (First property of VR's)**.** *Let R be a VR. Then:*

(a) R is local with $\mathfrak{m}_R = \{a \in \mathrm{Quot}(R) \backslash \{0\} \mid \frac{1}{a} \notin R\} \cup \{0\} \lhd \cdot R$

(b) If $R \subsetneq R' \leq \mathrm{Quot}(R)$*, then*

- R' *is a VR*
- $\mathfrak{m}_{R'} \subsetneq \mathfrak{m}_R$
- $R' = R_{\mathfrak{m}_{R'}}$

In particular: $\dim(R) > \dim(R')$

(c) R *is normal, i.e.* $\mathrm{Int}_{\mathrm{Quot}(R)}(R) = R$

(d) $\{I \mid I \trianglelefteq R\}$ *is totally ordered with respect to inclusion, i.e.*

$$I, J \trianglelefteq R \implies I \subseteq J \text{ or } J \subseteq I$$

(e) $I = \langle a_1, ..., a_r \rangle_R \trianglelefteq R \implies \exists\, i : I = \langle a_i \rangle_R$*. In particular, if* R *is a DVR, then* R *is a PID and* $\dim R = 1$*.*

Proof.

(a) Since obviously $\mathfrak{m}_R = R \backslash R^*$, we only have to show that $\mathfrak{m}_R \trianglelefteq R$. So let $a, b \in \mathfrak{m}_R, r \in R$:

Suppose that $ra \notin \mathfrak{m}_R \implies ra \in R^* \implies \frac{1}{a} = r\frac{1}{ra} \in R$ ↯.

Now suppose that $a + b \notin \mathfrak{m}_R \implies a, b \neq 0$. W.l.o.g we can assume that $\frac{b}{a} \in R$, since R is a VR. Then $a + b = (1 + \frac{b}{a})a \in \mathfrak{m}_R$ ↯

(b) $R \subsetneq R' \subseteq \mathrm{Quot}(R) =: K$ Then $K = \mathrm{Quot}(R')$. By definition R' is a VR (if $a \in K$ with $\frac{1}{a} \notin R'$, then $\frac{1}{a} \notin R$ and thus $a \in R \subseteq R'$). Hence, by (a), R' is local and obviously

$$\mathfrak{m}_{R'} = \{a \in K \mid \frac{1}{a} \notin R'\} \subseteq \{a \in K \mid \frac{1}{a} \notin R\} = \mathfrak{m}_R$$

Since $R \subsetneq R'$ there exists an $a \in R' \backslash R$ and since R is a VR we must have $\frac{1}{a} \in R$. Hence $\frac{1}{a} \in \mathfrak{m}_R$ and $\frac{1}{a} \notin \mathfrak{m}_{R'}$, so we have a strict inclusion.

Since $R \backslash \mathfrak{m}_{R'} \subseteq R' \backslash \mathfrak{m}_{R'} = (R')^*$ we know that $R'' := R_{\mathfrak{m}_{R'}} \subseteq R'$ is a VR by (a) and $\mathfrak{m}_{R''} = \mathfrak{m}_{R'}$:

"$\supseteq$": ✓

"$\subseteq$": Let $a = \frac{b}{c} \in \mathfrak{m}_{R''}$ where $b, c \in R, b \in \mathfrak{m}_{R'}, c \notin \mathfrak{m}_{R'}$. Then $c \in (R')^*$ and hence $a \in \mathfrak{m}_{R'}$

Thus we must have $R'' = R'$, because otherwise, as we proved above, we would have $\mathfrak{m}_{R'} \subsetneq \mathfrak{m}_{R''}$ ↯

(c) Suppose that $a \in \mathrm{Quot}(R) \backslash R$ and $f = x^n + \sum_{i=0}^{n-1} a_i x^i \in R[x]$ such that $f(a) = 0$. Then by dividing by a^{n-1}

$$a = -\sum_{i=0}^{n-1} \underbrace{a_i}_{\in R} (\underbrace{\frac{1}{a}}_{\in R})^{n-i-1} \in R \lightning$$

(d) Exerc. 49

(e) By (d) there exists an i, such that $\langle a_j \rangle \subseteq \langle a_i \rangle \; \forall j = 1..r$. Thus $I = \langle a_i \rangle_R$. Furthermore, every DVR is noetherian, so every ideal is finitely generated, hence principal. So R is a PID and since it is not a field, by 4.17 it has dimension 1.

□

Corollary 8.5.

An ID R is a DVR $\iff$ $R = R_\nu$ for some discrete valuation ν

Proof.

- "$\Longrightarrow$": Since R is a DVR, by 8.4 it is a PID and local. Hence

$$\mathfrak{m}_R = \langle t \rangle_R \Longrightarrow R = R_{\langle t \rangle_R} \overset{8.2(d)}{=} R_\nu$$

  for some discrete valuation ν.

- "$\Longleftarrow$": Let $0 \neq I \trianglelefteq R$. Choose $0 \neq f \in I$ with $\nu(f)$ minimal. We show that $I = \langle f \rangle$:

  "$\supseteq$": ✓

  "$\subseteq$": Let $0 \neq g \in I$

$$\begin{aligned} &\Longrightarrow \nu(g) \geq \nu(f) \\ &\Longrightarrow \nu(\frac{g}{f}) \geq 0 \\ &\Longrightarrow \frac{g}{f} \in R_\nu \\ &\Longrightarrow g = \underbrace{\frac{g}{f}}_{\in R} \cdot f \in \langle f \rangle_R \end{aligned}$$

  Thus R is a PID, hence noetherian and since by 8.3 it already is a VR, it is a DVR.

□

Corollary 8.6. *Let R be a VR, k a field, such that*

$$k \subseteq R \subseteq \mathrm{Quot}(R) =: K, \mathrm{trdeg}_k(K) < \infty$$

Then:

$$\dim R \leq \mathrm{trdeg}_k(K) - \mathrm{trdeg}_k(R/\mathfrak{m}_R)$$

Proof. Skipped □

Example 8.7.

(a) Let $f \in k[\underline{x}]$ be irreducible. Then

- $k \subseteq k[\underline{x}]_{\langle f \rangle} =: R \subseteq \mathrm{Quot}(R) = k(\underline{x}) =: K$
- R is a DVR by 8.2(d), 8.5
- $\implies \dim(R) = 1$
- $\mathrm{trdeg}_k(K) \overset{7.20}{=} n :=$ 'number of variables'
- $R/\mathfrak{m}_R = k[\underline{x}]_{\langle f \rangle}/\langle f \rangle = (k[\underline{x}]/\langle f \rangle)_{\langle \overline{0} \rangle} = \mathrm{Quot}(k[\underline{x}]/\langle f \rangle)$

Hence

$$\begin{aligned} \mathrm{trdeg}_k(R/\mathfrak{m}_R) &= \mathrm{trdeg}_k(\mathrm{Quot}(k[\underline{x}]/\langle f \rangle)) \\ &= \mathrm{trdeg}_k(k[\underline{x}]/\langle f \rangle) \\ &\overset{7.2}{=} \dim(k[\underline{x}]/\langle f \rangle) \\ &\overset{7.7}{=} n-1 \end{aligned}$$

Thus $\dim(R) = 1 = \mathrm{trdeg}_k(K) - \mathrm{trdeg}_k(R/\mathfrak{m}_R)$

(b) Let $K\{\{t\}\} = \{\sum_{n=0}^{\infty} a_n t^{\alpha_n} \,|\, \mathbb{R} \ni \alpha_n \nearrow \infty, a_n \in K\}$ the field of *puiseux series* over K, where

$$\mathrm{ord} : K\{\{t\}\} \setminus \{0\} \to \mathbb{R} : f \mapsto \min\{\alpha_n \,|\, a_n \neq 0\}$$

is a valuation. Then:

- $R_{\mathrm{ord}} = \{f \in K\{\{t\}\} \,|\, \mathrm{ord}(f) \geq 0\}$ is the VR
- $\dim(R_{\mathrm{ord}}) = 1$, but R_{ord} is not noetherian, hence it is *not* a DVR.
- If $\alpha_1, ..., \alpha_n$ are algebraicaly independent$_{/\mathbb{Q}}$, then $t^{\alpha_1}, ..., t^{\alpha_n}$ are algebraically independent over $K = \{a \cdot t^0 \,|\, a \in K\}$
- Hence $\mathrm{trdeg}_K(K\{\{t\}\}) = \infty$ (cf. Exerc. 50)

(c) Let $\alpha_1, ..., \alpha_n \in \mathbb{R}$ be algebraically indep.$_{/\mathbb{Q}}$. Then for $\varphi_{\underline{\alpha}} : K(x_1, ..., x_n) \hookrightarrow K\{\{t\}\}, x_i \mapsto t^{\alpha_i}$ we get a valuation

$$\nu : \mathrm{ord} \circ \varphi_{\underline{\alpha}} : K(\underline{x}) \to \mathbb{R}$$

on $K(\underline{x})$ and

- $\dim R_\nu = 1$
- $\mathrm{trdeg}_K(K(\underline{x})) = n$
- $R_\nu / \mathfrak{m}_{R_\nu} \cong K$
- Hence for $n \geq 2 \dim R = 1 < n = \mathrm{trdeg}_K(K(\underline{x})) - \mathrm{trdeg}_K(R/\mathfrak{m}_R)$

Theorem 8.8. *Let R be an ID, $I \trianglelefteq R, I \subsetneq R$. Then:*

$$\exists\, R \subseteq R' \subseteq \mathrm{Quot}(R) : R' \textit{ is a VR and } I \cdot R' \subseteq \mathfrak{m}_{R'}$$

Proof. Consider

$$M := \{R' \leq \mathrm{Quot}(R) \mid R \subseteq R' \text{ and } I \cdot R' \neq R'\}$$

Then $M \neq \emptyset$, since $R \in M$ and M is partially ordered with respect to inclusion. Now let $\mathcal{R}$ be any totally ordered subset of M and $R' = \bigcup_{R'' \in \mathcal{R}} R'' \leq \mathrm{Quot}(R)$. Then $R \subseteq R' \subseteq \mathrm{Quot}(R)$ and $I \cdot R' \neq R'$, since: Suppose $1 \in I \cdot R'$:

$$\begin{aligned} &\Longrightarrow 1 = \sum_{i=1}^{n} a_i b_i, a_i \in R', b_i \in I \\ &\Longrightarrow \exists\, R'' \in \mathcal{R} : a_1, ..., a_n \in R'' \\ &\Longrightarrow 1 \in I \cdot R'' \ \lightning \end{aligned}$$

Hence $R' \in M$ and it is an upper bound for the chain above. Hence we can apply Zorn's lemma and there exists an $R' \in M$ maximal with respect to inclusion. It remains to show that R' is a VR:

Suppose $x \in \mathrm{Quot}(R') = \mathrm{Quot}(R)$, such that $x \notin R'$ and $\frac{1}{x} \notin R'$

$$\Longrightarrow R' \subsetneq R'[x], R' \subsetneq R'\left[\frac{1}{x}\right]$$

$$\Longrightarrow R'[x], R'\left[\frac{1}{x}\right] \notin M, \text{ since } R' \text{ is maximal}$$

$$\Longrightarrow I \cdot R'[x] = \underbrace{R'[x]}_{\ni 1}, I \cdot R'\left[\frac{1}{x}\right] = \underbrace{R'\left[\frac{1}{x}\right]}_{\ni 1}$$

$$\Longrightarrow \exists\, a_i, b_j \in I \cdot R' : 1 = \sum_{i=0}^{n} a_i x^i = \sum_{j=0}^{m} b_j \frac{1}{x^j}; n, m \text{ minimal}$$

$$\Longrightarrow (\text{wlog } n \geq m)\ 1 - b_0 = (1 - b_0) \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} (1 - b_0) a_i x^i \text{ and}$$

$$(1 - b_0) a_n x^n = a_n x^n \sum_{j=\mathbf{1}}^{m} b_j \frac{1}{x^j} = \sum_{j=1}^{m} b_j a_n x^{n-j}$$

$$\Longrightarrow 1 = (1 - b_0) + b_0 = \sum_{i=0}^{n-1} \underbrace{(1 - b_0) a_i}_{\in I \cdot R'} x^i + \sum_{j=1}^{m} \underbrace{a_n b_j}_{\in I \cdot R'} x^{n-j} + \underbrace{b_0}_{\in I \cdot R'} \lightning$$

which is a contradiction, since n was minimal. ☐

Corollary 8.9. *If R is an ID, then:*

$$\mathrm{Int}_{\mathrm{Quot}(R)}(R) = \bigcap_{R \subseteq R' \subseteq \mathrm{Quot}(R), R' \ VR} R'$$

is the normalisation of R.

Proof.

"$\subseteq$": Let $x \in \mathrm{Int}_{\mathrm{Quot}(R)}(R) \Longrightarrow x$ integral$_{/R}$, hence integral$_{/R'}$ for all $R' \leq \mathrm{Quot}(R)$ VR with $R \subseteq R'$. By 8.4(c) we must have $x \in R'$.

"$\supseteq$": Suppose $x \notin \mathrm{Int}_{\mathrm{Quot}(R)}(R)$

$$\begin{aligned}
&\Longrightarrow x \notin R\left[\frac{1}{x}\right] \\
&\quad \text{(since otherwise } x = a_n\frac{1}{x^n} + a_{n-1}\frac{1}{x^{n-1}} + ... + a_0, \text{hence} \\
&\quad x^{n+1} = a_n + a_{n-1}x + ... + a_0x^n \lightning) \\
&\Longrightarrow \frac{1}{x} \notin (R\left[\frac{1}{x}\right])^* \\
&\Longrightarrow \exists\, \mathfrak{m} \lhd \cdot R\left[\frac{1}{x}\right] : \frac{1}{x} \in \mathfrak{m} \\
&\overset{8.8}{\Longrightarrow} \exists\, R\left[\frac{1}{x}\right] \subseteq R' \text{ VR } \subseteq \mathrm{Quot}(R\left[\frac{1}{x}\right]) = \mathrm{Quot}(R'), \underbrace{\mathfrak{m}}_{\ni\frac{1}{x}} \cdot R' \neq R' \\
&\Longrightarrow \frac{1}{x} \notin (R')^* \\
&\Longrightarrow x \notin R', \text{ hence } x \notin \bigcap R'
\end{aligned}$$

$\square$

Proposition 8.10. *Let $(R, \mathfrak{m})$ be a local, noetherian ID of dimension $\dim(R) = 1$. Then the following are equivalent:*

(a) R is a DVR

(b) R is a PID

(c) $\mathfrak{m}$ is principal

(d) $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$, i.e. $(R, \mathfrak{m})$ is regular.

(e) $0 \neq I \trianglelefteq R \Longrightarrow \exists\, n \geq 0 : I = \mathfrak{m}^n$

(f) $\exists\, t \in R : \forall\, 0 \neq I \trianglelefteq R : \exists\, n \geq 0 : I = \langle t^n \rangle$

(g) R is normal

(h) $\dim_{R/\mathfrak{m}}(\mathfrak{m}^k/\mathfrak{m}^{k+1}) = 1$ for all $k \geq 0$.

Note that condition (h) actually implies that $\dim(R) = 1$.

Proof.

- "(a) $\Longrightarrow$ (b)": 8.4(e)
- "(b) $\Longrightarrow$ (c)": ✓
- "(c) $\Longrightarrow$ (d)":

"$\leq$": ✓

"$\geq$": Assume that $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 0$ Then $\mathfrak{m} = \mathfrak{m}^2$, hence by NAK $\mathfrak{m} = 0 \lightning_{\dim R=1}$

- "(d) $\implies$ (c)": 2.12
- "(c) $\implies$ (e)": Let $0 \neq I \trianglelefteq R$

$$\begin{aligned}
&\implies \sqrt{I} = \bigcap_{P \text{ prime}, I \subseteq P} P \overset{\dim(R)=1}{=} \mathfrak{m} \\
&\overset{5.4}{\implies} I \text{ is } \mathfrak{m}\text{-primary} \\
&\overset{5.6}{\implies} \exists\, n : \langle t^n \rangle = \mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}^{n-1} = \langle t^{n-1} \rangle \\
&\implies 1 = \dim_{R/\mathfrak{m}}(\mathfrak{m}^{n-1}/\mathfrak{m}^n) \geq \dim_{R/\mathfrak{m}}(I/\mathfrak{m}^n) \\
&\implies I = \mathfrak{m}^{n-1} \text{ or } I = \mathfrak{m}^n
\end{aligned}$$

- "(e) $\implies$ (f)": $\dim(R) = 1$ and NAK

$$\begin{aligned}
&\implies \exists\, t \in \mathfrak{m} \backslash \mathfrak{m}^2 \\
&\overset{(e)}{\implies} \exists\, n : \langle t \rangle = \mathfrak{m}^n \\
&\overset{t \notin \mathfrak{m}^2}{\implies} n = 1 \\
&\implies \langle t \rangle = \mathfrak{m} \\
&\implies \mathfrak{m}^k = \langle t \rangle^k = \langle t^k \rangle
\end{aligned}$$

- "(f) $\implies$ (a)": Since R is a PID and $\mathfrak{m} = \langle t \rangle$

$$\begin{aligned}
&\implies R = R_{\langle t \rangle} \overset{8.2(d)}{=} R_\nu \text{with respect to some valuation } \nu \\
&\overset{8.3}{\implies} R \text{ is a DVR}
\end{aligned}$$

- "(a) $\implies$ (g)": 8.4(b)
- "(g) $\implies$ (c)": Let $0 \neq a \in \mathfrak{m}$ and set $I = \langle a \rangle$.

  With the same argument as in "(c) $\implies$ (e)" we get

$$\begin{aligned}
&\exists\, n : \mathfrak{m}^n \subseteq I \subsetneq \mathfrak{m}^{n-1} \\
\implies &\exists\, b \in \mathfrak{m}^{n-1} \backslash \langle a \rangle
\end{aligned}$$

  We want to show: $\mathfrak{m} = \langle t \rangle_R$, where $t = \frac{a}{b} \in \mathrm{Quot}(R)$.
  Note. $b\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq \langle a \rangle$, hence $\frac{1}{t}\mathfrak{m} = \frac{b}{a}\mathfrak{m} \subseteq R$

Now suppose that $\frac{1}{t} \cdot \mathfrak{m} \subseteq \mathfrak{m}$ and consider the R-linear map

$$\phi : \mathfrak{m} \to \mathfrak{m}, x \mapsto \frac{1}{t} \cdot x$$

$$\begin{aligned} &\overset{2.6}{\Longrightarrow} \chi_\phi\left(\frac{1}{t}\right) = 0 \\ &\Longrightarrow \frac{1}{t} \text{ integral}_{/R} \\ &\overset{R \text{ normal}}{\Longrightarrow} \frac{1}{t} \in R \\ &\Longrightarrow b = \frac{1}{t} \cdot a \in \langle a \rangle_R \ \lightning \end{aligned}$$

Hence $\frac{1}{t} \cdot \mathfrak{m} = R$ and thus

$$\mathfrak{m} = t \cdot \frac{1}{t} \cdot \mathfrak{m} = tR = \langle t \rangle_R$$

- "(h) $\Longrightarrow$ (d)": This is clear with $k = 1$.
- "(f) $\Longrightarrow$ (h)": By (f) we know that the quotient $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is generated by the residue class of t^k and thus the dimension is at most 1. If the dimension was zero, then by Nakayama's Lemma we would have $\mathfrak{m}^k = 0$ and R would be artinian in contradiction to $\dim(R) = 1$.

It only remains to show that condition (h) implies that the dimension of R is one. If $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$, then by Nakayama's Lemma $\mathfrak{m}$ is generated by one element and by Krull's Principle Ideal Theorem $\dim(R) = \operatorname{codim}(\mathfrak{m}) \leq 1$. Moreover, if the dimension was zero, R would be artinian and some power of $\mathfrak{m}^k$ would be zero, in contradiction to the assumption (h). $\square$

Example 8.11. $K\llbracket x \rrbracket, \mathbb{R}\{x\}, \mathbb{C}\{x\}, K[x]_{\langle x \rangle}$ are DVR's.

B). Dedekind Domains

Definition 8.12. A ring R is a *Dedekind domain* (DD) $:\Longleftrightarrow$

- R is an ID
- R is noetherian
- $\dim(R) = 1$
- $0 \neq Q \trianglelefteq R, Q \subsetneq R$ primary

$$\Longrightarrow \exists\, n \geq 1, P \in \mathfrak{m} - \operatorname{Spec}(R) : Q = P^n$$

(The idea is to use DDs as generalisation of UFDs for ideals)

Proposition 8.13. *Let R be a noeth. ID with $\dim(R) = 1, 0 \neq I \trianglelefteq R, I \subsetneq R$. Then:*

$$\exists_1 \, Q_1, ..., Q_r \trianglelefteq R \text{ primary} : I = Q_1 \cdot ... \cdot Q_r, \sqrt{Q_i} \neq \sqrt{Q_j} \, \forall i \neq j$$

In particular: Every nonzero ideal in a DD factorises uniquely as a product of prime powers.

Proof. Exerc. 33 □

Definition 8.14. Let R be a DD, $I, J \trianglelefteq R, P \in \operatorname{Spec}(R)$

(a) $n_P(I) := \sup\{n \geq 0 \,|\, I \subseteq P^n\}$ is the *order* of P as prime factor of I.

(b) I *divides* $J :\iff I \mid J :\iff \exists Q \trianglelefteq R : J = I \cdot Q$

Proposition 8.15. *Let R be a DD, $0 \neq I, J \trianglelefteq R$. Then:*

(a) $I = \prod_{P \lhd \cdot R} P^{n_P(I)} = \prod_{P \in \operatorname{Ass}(I)} P^{n_P(I)}$ *and* $n_P(I) = 0 \iff P \notin \operatorname{Ass}(I)$

(b) $I \mid J \iff J \subseteq I \iff n_P(I) \leq n_P(J) \, \forall \, P \lhd \cdot R$

(c) $I \cdot J = \prod_{P \lhd \cdot R} P^{n_P(I) + n_P(J)}$

- $\gcd(I, J) := I + J = \prod_{P \lhd \cdot R} P^{\min\{n_P(I), n_P(J)\}}$
- $\operatorname{lcm}(I, J) := I \cap J = \prod_{P \lhd \cdot R} P^{\max\{n_P(I), n_P(J)\}}$

Hence $I \cdot J = (I + J) \cdot (I \cap J)$

Proof.

(a) Since R is a DD, by 8.13 we know that $I = \prod_{P \in \operatorname{Ass}(I)} P^{m_P}$ with $m_P \geq 1$. Now suppose that $Q \lhd \cdot R$ and $I \subseteq Q$. Then $\prod P^{m_P} \subseteq Q$ and since Q is prime there exists a $P \in \operatorname{Ass}(I) : P \subseteq Q$. As both ideals are maximal, we have $P = Q \in \operatorname{Ass}(I)$. Hence:

$$n_P(I) \neq 0 \iff P \in \operatorname{Ass}(I)$$

It remains to show that $(P \in \operatorname{Ass}(I) \implies m_P = n_P(I))$:

"$\leq$": $I \subseteq P^{m_P} \implies n_P(I) \geq m_P$

"$\geq$": $(P_P)^{m_P} = I_P \subseteq (P_P)^{n_P(I)} \implies m_P \geq n_P(I)$

(b)
- $I \mid J \implies \exists Q : J = I \cdot Q \implies J = I \cdot Q \subseteq I$
- $J \subseteq I \implies \prod_{P \lhd \cdot R} P^{n_P(J)} = J \subseteq I = \prod_{P \lhd \cdot R} P^{n_P(I)}$ Localising at a fixed P yields

$$n_P(J) \geq n_P(I)$$

- $n_P(I) \leq n_P(J) \, \forall P \lhd\cdot R \implies J = I \cdot \prod P^{n_P(I)-n_P(J)}$. Hence $I \mid J$.

(c)
- $I \cdot J = \prod_{P \lhd\cdot R} P^{n_P(I)+n_P(J)}$ is clear
- $I + J = \prod_{P \lhd\cdot R} P^{\min\{n_P(I),n_P(J)\}}$:

$$\begin{aligned} I, J \subseteq I + J &\overset{(b)}{\implies} n_P(I), n_P(J) \geq n_P(I+J) \\ &\implies n_P(I+J) \leq \min\{n_P(I), n_P(J)\} \leq n_P(I), n_P(J) \\ &\implies I + J \overset{(b)}{\supseteq} \prod_{P \lhd\cdot R} P^{\min\{n_P(I),n_P(J)\}} \overset{(b)}{\supseteq} I, J \\ &\implies I + J = \prod_{P \lhd\cdot R} P^{\min\{n_P(I),n_P(J)\}} \end{aligned}$$

since $I + J$ is the smallest ideal containing I and J.

- $I \cap J = \prod_{P \lhd\cdot R} P^{\max\{n_P(I),n_P(J)\}}$:

$$\begin{aligned} I \cap J \subseteq I, J &\overset{(b)}{\implies} n_P(I \cap J) \geq n_P(I), n_P(J) \\ &\implies n_P(I \cap J) \geq \max\{n_P(I), n_P(J)\} \geq n_P(I), n_P(J) \\ &\overset{(b)}{\implies} I \cap J \subseteq \prod_{P \lhd\cdot R} P^{\max\{n_P(I),n_P(J)\}} \overset{(b)}{\subseteq} I, J \\ &\implies \prod_{P \lhd\cdot R} P^{\max\{n_P(I),n_P(J)\}} \subseteq I \cap J \end{aligned}$$

$\implies$ Equality

$\square$

Theorem 8.16. *Let R be a DD, $I \trianglelefteq R, 0 \neq a \in I$. Then:*

$$\exists\, b \in I : \langle a, b \rangle_R = I$$

In particular: Every ideal in a DD can be generated by two elements.

Proof. For $P \in \mathrm{Ass}(I)$ choose

$$b_P \in \left(P^{n_P(I)} \cdot \left(\prod_{P \neq Q \in \mathrm{Ass}(\langle a \rangle)} Q^{n_Q(I)+1} \right) \right) \setminus \left(\prod_{Q \in \mathrm{Ass}(\langle a \rangle)} Q^{n_Q(I)+1} \right) =: J_P$$

Suppose $b_P \in P^{n_P(I)+1}$. Then

$$b_P \in P^{n_P(I)+1} \cap J_P \overset{8.15}{=} \prod_{Q \in \mathrm{Ass}(\langle a \rangle)} Q^{n_Q(I)+1} \lightning$$

Hence

$$\Longrightarrow b := \sum_{P \in \mathrm{Ass}(\langle a \rangle)} b_P \quad \notin Q^{n_Q(I)+1}\, \forall Q \in \mathrm{Ass}(\langle a \rangle)$$

$$\begin{aligned}
&\Longrightarrow n_Q(I) \overset{\langle a,b\rangle \subseteq I}{\leq} n_Q(\langle a,b\rangle) \overset{\langle a,b\rangle \nsubseteq Q^{n_Q(I)+1}}{\leq} n_Q(I)\\
&\Longrightarrow n_Q(I) = n_Q(\langle a,b\rangle)\, \forall\, Q \in \mathrm{Ass}(\langle a \rangle)
\end{aligned}$$

And for all $Q \in \mathfrak{m} - \mathrm{Spec}(R) \backslash \mathrm{Ass}(\langle a \rangle)$

$$\begin{aligned}
&\Longrightarrow n_Q(\langle a,b\rangle) \leq n_Q(\langle a \rangle) \overset{Q \notin \mathrm{Ass}(I)}{=} 0 \text{ and}\\
&\quad\ n_Q(\langle a \rangle) \geq n_Q(I)\\
&\Longrightarrow n_Q(I) = n_Q(\langle a \rangle) = n_Q(\langle a,b\rangle) = 0
\end{aligned}$$

Hence

$$n_Q(I) = n_Q(\langle a,b\rangle)\, \forall\, Q \lhd \cdot R$$

and by 8.15 $I = \langle a,b\rangle$ $\square$

Theorem 8.17. *Let R be a noetherian ID of dimension* $\dim(R) = 1$. *Then the following are equivalent:*

(a) R is a DD.

(b) R is normal.

(c) $\forall\, 0 \neq P \in \mathrm{Spec}(R) : R_P$ is a DVR.

Proof.

- "(a) $\Longrightarrow$ (c)": Let $0 \neq I \trianglelefteq R_P, I \subsetneq R_P$

$$\begin{aligned}
&\Longrightarrow \sqrt{I} = \bigcap_{I \subseteq Q \lhd \cdot R_P} Q \quad = P^e \lhd \cdot R_P\\
&\Longrightarrow I \text{ is } P^e\text{-primary}\\
&\Longrightarrow I^c \text{ is } P^{ec} = P\text{-primary}\\
&\overset{R\ \mathrm{DD}}{\Longrightarrow} I^c = P^n \text{ for some } n\\
&\Longrightarrow I \overset{3.2}{=} I^{ce} = (P^e)^n\\
&\overset{8.10}{\Longrightarrow} R_P \text{ is a DVR}
\end{aligned}$$

- "(c) $\implies$ (a)": Let $0 \neq Q \trianglelefteq R, Q \subsetneq R$ be P-primary and $n = \max\{k \mid Q \subseteq P^k\} \geq 1$

$$\begin{aligned}
&\implies P_P^{n+1} \not\supseteq Q_P \subseteq P_P^n \\
&\overset{R_P \text{ DVR}}{\implies} Q_P = P_P^n \\
&\implies Q \subseteq P^n \subseteq (P^n)^{ec} = (Q_P)^c = Q^{ec} \overset{5.4}{=} Q \\
&\implies Q = P^n
\end{aligned}$$

- "(b) $\iff$ (c)":

$$\begin{aligned}
R \text{ normal} &\overset{6.9}{\iff} \forall\, \mathfrak{m} \lhd \cdot R : R_{\mathfrak{m}} \text{ normal} \\
&\overset{8.10}{\iff} \forall\, \mathfrak{m} \lhd \cdot R : R_{\mathfrak{m}} \text{ is a DVR}
\end{aligned}$$

$\square$

Remark 8.18. *Let $\mathfrak{X} \subseteq \mathbb{A}_K^n$ be an affine curve, $K = \overline{K}$ and let*

$$R = K[\mathfrak{X}] = K[x_1, ..., x_n] / I(\mathfrak{X})$$

Then

$$\begin{aligned}
&\mathfrak{X} \textit{ is } \text{smooth} \\
\iff &\forall\, p \in \mathfrak{X} : 1 = \dim_p(\mathfrak{X}) = \dim_p(T_p(\mathfrak{X})) = \dim_{R_p/\mathfrak{m}_p^2}(\mathfrak{m}_p/\mathfrak{m}_p^2) = \dim_K(\mathfrak{m}_p/\mathfrak{m}_p^2) \\
\iff &R_{\mathfrak{m}_P} \textit{ is a DVR } (\forall\, p \in \mathfrak{X} \overset{HNS}{\iff} \forall\, \mathfrak{m} \lhd \cdot R \iff \forall\, 0 \neq P \in \operatorname{Spec}(R)) \\
\overset{8.7}{\iff} &K[\mathfrak{X}] \textit{ normal} \\
\overset{8.17}{\iff} &K[\mathfrak{X}] \textit{ is a DD} \\
\iff &\mathfrak{X} \textit{ is } \text{normal}
\end{aligned}$$

Note. In higher dimensions only (smooth $\implies$ normal) holds! In terms of algebraic geometry one can see DD's as the equivalent to smooth curves. For example:

- $\mathfrak{X} = V(y - x^2) \implies K[\mathfrak{X}] = K[x, y] / \langle y - x^2 \rangle \cong K[z]$ is a DD
- $\mathfrak{X} = \{(t, t^2, t^3) \in \mathbb{A}_K^3 \mid t \in K\}$. Then

  $$K[\mathfrak{X}] = K[x, y, z] / \langle z - x^3, y - x^2, xz - y^2 \rangle \cong K[t]$$

  is a DD.

Example 8.19. If R is a PID but not a field, then R is a DD. In particular $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[t]$, $K[\![t]\!]$, $\mathbb{R}\{x\}$,$\mathbb{C}\{x\}$ are DD's.

Definition 8.20. A finite algebraic field extension K of $\mathbb{Q}$ is called an *algebraic number field* and $\mathrm{Int}_K(\mathbb{Z})$ is called its *ring of integers*.

Theorem 8.21. *The ring of integers of a finite algebraic number field is a DD.*

Proof. Let $\mathbb{Q} \subseteq K$ be a field extension, $d = \dim_{\mathbb{Q}} K$ and $R := \mathrm{Int}_K(\mathbb{Z})$. First we show that R is noetherian. By Exercise 30 it suffices to show:

$$\forall\, 0 \neq I \trianglelefteq R \implies I \cap \mathbb{Z} \neq \{0\}$$

Suppose $I \neq 0$, but $I \cap \mathbb{Z} = \{0\}$. Then

$$\mathbb{Z} = \mathbb{Z}/_{I \cap \mathbb{Z}} \hookrightarrow R/_I$$

is integral by 6.8 and by 6.17 we know that

$$\dim(\mathbb{Z}) = \dim(R/_I) < \dim(R) \overset{6.17, R = \mathrm{Int}_K(\mathbb{Z})}{=} \dim(\mathbb{Z}) \lightning$$

Now we show $\dim(R) = 1$ and that R is a normal ID: Since $\mathbb{Z} \hookrightarrow R$ is integral, by 6.17 $\dim(R) = \dim(\mathbb{Z}) = 1$ and since $\mathrm{Quot}(R) \subseteq K$

$$\begin{aligned} R \subseteq \mathrm{Int}_{\mathrm{Quot}(R)}(R) &\subseteq \mathrm{Int}_K(R) \\ &= \mathrm{Int}_K(\mathrm{Int}_K(\mathbb{Z})) \\ &\overset{6.7}{=} \mathrm{Int}_K(\mathbb{Z}) = R \end{aligned}$$

Hence $\mathrm{Int}_{\mathrm{Quot}(R)}(R) = R$. Hence R is normal (and of course an ID). By 8.17 it is a DD. ☐

Example 8.22. If $d < 0$ is squarefree, then

$$\mathrm{Int}_{\mathbb{Q}[\sqrt{d}]}(\mathbb{Z}) = \mathbb{Z}[\omega_d],\ \omega_d = \begin{cases} \sqrt{d} & , d \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2} & , d \equiv 1 \mod 4 \end{cases}$$

Proof. Exercise 42 ☐

Example 8.23.

(a) $R = \mathbb{Z}, I = \langle 6 \rangle \implies I = \langle 2 \rangle \langle 3 \rangle$ In this case prime factorisation of ideals corresponds to prime factorisation of elements.

(b) $R = \mathbb{Z}[\sqrt{-5}] = \mathrm{Int}_{Q[\sqrt{-5}]}(\mathbb{Z})$ is a DD, but not factorial: Let $I = \langle 6 \rangle$. Claim:

$$I = P^2 \cdot Q \cdot Q'$$

for $P = \left\langle 2, 1 + \sqrt{-5} \right\rangle, Q = \left\langle 3, 1 + \sqrt{-5} \right\rangle, Q' = \left\langle 3, 1 - \sqrt{-5} \right\rangle$ is the unique prime factorisation of I in R. but $\langle 2 \rangle = P^2, \langle 3 \rangle = Q \cdot Q'$ are *not* prime.

Proof. Exercise 34 ☐

C). Fractional Ideals, Invertible Ideals, Ideal Class Group

Definition 8.24. Let R be an ID, $K = \mathrm{Quot}(R), 0 \neq I \subseteq K$ an R- submodule of K.

(a) I is called a *fractional ideal* of R

$$:\Longleftrightarrow \exists\, 0 \neq x \in R : x \cdot I \subseteq R$$
$$\Longleftrightarrow \exists\, 0 \neq x \in R, I' \trianglelefteq R : I = \frac{1}{x} \cdot I'$$

A fractional ideal I is called *integral*

$$:\Longleftrightarrow I \subseteq R \Longleftrightarrow I \trianglelefteq R$$

A fractional ideal I is called *principal*

$$:\Longleftrightarrow \exists\, y \in K : I = \langle y \rangle_R = yR$$

Notation: $R :_K I := \{x \in K \mid x \cdot I \subseteq R\}$ is an R-submodule of K.

(b) I is called an *invertible ideal* of R (or *Cartier divisor* of R)

$$:\Longleftrightarrow \exists\, I' \leq K \text{ an } R\text{-submodule} : \langle ab \mid a \in I, b \in I' \rangle_R =: I \cdot I' = R$$
$$\Longleftrightarrow I \cdot (R :_K I) = R$$

Note. We have to prove the equivalence:

Proof. "$\Longleftarrow$" is clear and "$\Longrightarrow$" holds since

$$I' \subseteq (R :_K I) \implies R = I \cdot I' \subseteq I \cdot (R :_K I) \subseteq R$$

□

Notation:

$$\mathrm{Div}(R) := \{I \leq K \mid I \text{ is an invertible ideal}\}$$

is called the *ideal group* (or the *group of cartier divisors*) of R.
Note. Let $I, I' \in \mathrm{Div}(R)$

- $I \cdot I' \cdot (R :_K I') \cdot (R :_K I) = I \cdot R \cdot (R :_K I) = I \cdot (R :_K I) = R$. Hence $\mathrm{Div}(R)$ is closed with respect to "$\cdot$".
- $I \cdot R = I \;\forall\, I \in \mathrm{Div}(R)$
- $(I \cdot I') \cdot I'' = I \cdot (I' \cdot I'') \forall I, I'.I'' \in \mathrm{Div}(R)$ obviously
- $I \cdot (R :_K I) = R \implies (R :_K I) \in \mathrm{Div}(R)$ is the inverse of I.

In particular $I' = (R :_K I)$ in the definition, since the inverse is unique.

Example 8.25. Let R be an ID, $K = \mathrm{Quot}(R), I \leq K$ an R-submodule

(a) $I = \left\langle \frac{a_1}{b_1}, ..., \frac{a_n}{b_n} \right\rangle$ finitely generated, then I is fractional with $x = b_1 \cdot ... \cdot b_n$.

(b) R noetherian, I fractional, then I is finitely generated, since there exists an $x \in R, I' \trianglelefteq R : I = \frac{1}{x} I'$. As R is noetherian, $I' = \langle a_1, ..., a_n \rangle$, hence $I = \left\langle \frac{a_1}{x}, ..., \frac{a_n}{x} \right\rangle_R$.

(c) I invertible $\implies I$ fin. gen. $\overset{(a)}{\implies} I$ fractional, since:

$$\begin{aligned} & 1 \in R = I \cdot (R :_K I) \\ \implies & 1 = \sum_{i=1}^{n} a_i b_i, a_i \in I, b_i \in (R :_K I) \\ \implies & \forall\, c \in I : c = 1 \cdot c = \sum_{i=1}^{n} a_i \underbrace{(b_i \cdot c)}_{\in R} \in \langle a_1, ..., a_n \rangle_R \end{aligned}$$

(d) $I = \langle x \rangle$ principal, $0 \neq x \in K \implies I$ is invertible

(e) $R = \mathbb{Z}, K = \mathbb{Q}$, then

$$I \text{ fractional} \iff I = q \cdot \mathbb{Z} \text{ for some } 0 \neq q \in \mathbb{Q}$$
$$I \text{ integral} \iff I = q \cdot \mathbb{Z} \text{ for some } 0 \neq q \in \mathbb{Z}$$

Thus: fractional $\implies$ principal $\implies$ invertible

Proposition 8.26. *Let $(R, \mathfrak{m})$ be a local ID, $0 \neq I \leq \mathrm{Quot}(R) =: K$ an R-submodule. Then:*

$$I \textit{ is an invertible ideal} \iff I = \langle a \rangle \textit{ is principal, } a \neq 0$$

Proof.

- "$\Longleftarrow$": 8.25 (d)
- "$\Longrightarrow$": Since $I \cdot (R :_K I) = R$

$$\begin{aligned} \implies & \exists\, a \in \underbrace{I}_{\subseteq K}, b \in \underbrace{R :_K I}_{\subseteq K} : u := ab \notin \mathfrak{m} \\ \implies & u \in R^*, \text{ since } R \text{ is local} \end{aligned}$$

Let $c \in I$.

$$\begin{aligned} \implies & c \cdot b \in R \\ \implies & c = (c \cdot b) \cdot u^{-1} \cdot \frac{u}{b} = \underbrace{(c \cdot b) \cdot u^{-1}}_{\in R} \cdot a \in \langle a \rangle_R \end{aligned}$$

$$\implies I = \langle a \rangle$$

□

Proposition 8.27 (Invertibility is a local property). *Let R be an ID, $0 \neq I \subseteq K$ a fractional ideal. Then the following are equivalent:*

- *I is invertible over R.*
- *I is fin. gen. and I_P is invertible over $R_P \, \forall \, P \in \operatorname{Spec}(R)$*
- *I is fin. gen. and $I_{\mathfrak{m}}$ is invertible over $R_{\mathfrak{m}} \forall \mathfrak{m} \in \mathfrak{m} - \operatorname{Spec}(R)$*

In particular: For fin. gen. R-submodules of K invertibility is a local property.

Proof.

- "(a) $\implies$ (b)": By 8.25(c) I is finitely generated and
$$I \cdot I' = R \implies I_P \cdot I'_P = (I \cdot I')_P = R_P$$
Hence I_P is invertible
- "(b) $\implies$ (c)": ✓
- "(c) $\implies$ (a)": We have to show that
$$S^{-1}(R :_K I) = (S^{-1}R :_K S^{-1}I) \text{ for } S = R \backslash \mathfrak{m}$$
"$\subseteq$": Let $b \in (R :_K I), s \in S$
$$\implies \frac{b}{s} \cdot S^{-1}I \subseteq S^{-1}R \implies \frac{b}{s} \in S^{-1}R :_K S^{-1}I$$
"$\supseteq$": Since I is finitely generated we have $I = \langle a_1, ..., a_k \rangle$. Now let
$$\begin{aligned} &\frac{b}{t} \in S^{-1}R :_K S^{-1}I \\ \implies & b \cdot a_i = \frac{b}{t}(\underbrace{t \cdot a_i}_{\in S^{-1}I}) \in S^{-1}R \\ \implies & \exists \, s_i \in S : b \cdot a_i \cdot s_i \in R \\ \implies & \text{ For } s = s_1 \cdot ... \cdot s_n \; b \cdot a_i \cdot s \in R \\ \implies & b \cdot s \in R :_K I \\ \implies & \frac{b}{t} = \frac{bs}{ts} \in S^{-1}(R :_K I) \end{aligned}$$
Thus
$$\begin{aligned} (I \cdot (R :_K I))_{\mathfrak{m}} &= I_{\mathfrak{m}} \cdot (R :_K I)_{\mathfrak{m}} \\ &= I_{\mathfrak{m}} \cdot (R_{\mathfrak{m}} :_K I_{\mathfrak{m}}) = R_{\mathfrak{m}} \forall \, \mathfrak{m} \lhd \cdot R \\ \implies & I \cdot (R :_K I) \not\subseteq \mathfrak{m} \forall \, \mathfrak{m} \\ \implies & I \cdot (R :_K I) = R \end{aligned}$$

□

Corollary 8.28. *Let* $(R, \mathfrak{m})$ *be a local ID and not a field,* $K := \mathrm{Quot}(R)$*. Then*

$$R \text{ is a DVR} \iff \mathrm{Div}(R) = \{I \mid I \text{ fractional ideal of } R\}$$

(i.e. I *fractional* $\iff$ I *invertible)*

Proof.

Note. By 8.25 $\mathrm{Div}(R) \subseteq \{I \mid I \text{ fractional}\}$

- "$\Longrightarrow$": Let I be a fractional ideal of R

$$\Longrightarrow \exists\, I' \trianglelefteq R, I' \overset{R \text{ DVR}}{=} \langle y \rangle_R, 0 \neq x \in R : I = \frac{1}{x} \cdot I' = \left\langle \frac{y}{x} \right\rangle_R$$

$$\Longrightarrow I \text{ is principal}$$

$$\overset{8.25}{\Longrightarrow} I \text{ is invertible}$$

- "$\Longleftarrow$": Let $0 \neq I \trianglelefteq R$. Then I is a fractional ideal of R and by assumption invertible. By 8.26 it is principal, hence R is a PID and not a field. Thus by 8.10, R is a DVR.

□

Theorem 8.29. *Let* R *be an ID,* R *not a field. Then*

$$R \text{ is a DD} \iff \mathrm{Div}(R) = \{I \mid I \text{ fractional}\}$$

(i.e. I *fractional* $\iff$ I *invertible)*

Proof.

- "$\Longrightarrow$": Since R is a DD, R is noetherian and $R_\mathfrak{m}$ is a DVR $\forall \mathfrak{m} \triangleleft \cdot R$ by 8.17. Now let I be a fractional ideal of R.

$$\overset{8.25}{\Longrightarrow} I \text{ fin. gen. and } I_\mathfrak{m} \text{ fractional}$$

$$\Longrightarrow I = \frac{1}{x} I', I' \trianglelefteq R$$

$$\Longrightarrow I_\mathfrak{m} = \frac{1}{x} I'_\mathfrak{m}$$

$$\overset{R \text{ DVR}}{\Longrightarrow} I_\mathfrak{m} \text{ is invertible and } I \text{ is fin. gen}$$

$$\overset{8.27}{\Longrightarrow} I \text{ is invertible}$$

- "$\Longleftarrow$": Since every ideal $0 \neq I \trianglelefteq R$ is fractional, hence invertible, hence finitely generated, R is noetherian. Now we need to show that $R_\mathfrak{m}$ is a DVR $\forall \mathfrak{m} \lhd \cdot R$:

  Let I be a fractional ideal of $R_\mathfrak{m}$

$$\begin{aligned}
&\Longrightarrow I = \frac{1}{x} J, J \trianglelefteq R_\mathfrak{m} \\
&\Longrightarrow J^c \trianglelefteq R, \text{ in particular fractional} \\
&\overset{\text{By ass.}}{\Longrightarrow} J^c \text{ is invertible and fin. gen., as } R \text{ is noeth.} \\
&\overset{8.26}{\Longrightarrow} J = \langle y \rangle_R \text{ principal, as } R_\mathfrak{m} \text{ is local} \\
&\overset{8.28}{\Longrightarrow} R_\mathfrak{m} \text{ is a DVR} \\
&\Longrightarrow \dim(R_\mathfrak{m}) = 1
\end{aligned}$$

  Hence $\dim(R) = \sup_{\mathfrak{m} \lhd \cdot R} \{\underbrace{\dim(R_\mathfrak{m})}_{=1}\} = 1$ and thus R is a DD b 8.17.

$\square$

Corollary 8.30. *If R is a DD, then*

$$\mathrm{Div}(R) \overset{8.29}{=} \{I \mid I \text{ fractional}\} \cong \bigoplus_{P \lhd \cdot R} \mathbb{Z} \cdot P$$

is a free abelian group with free generators $\mathfrak{m} - \mathrm{Spec}(R)$ *by*

$$P_1^{a_1} \cdot \ldots \cdot P_n^{a_n} \mapsto a_1 \cdot P_1 + \ldots + a_n P_n$$

Remark 8.31. *The following is an exact sequence of abelian groups:*

$$\{1\} \longrightarrow R^* \longrightarrow K^* \xrightarrow{\phi: x \mapsto \langle x \rangle} \mathrm{Div}(R) \longrightarrow \mathrm{Coker}(\phi) \longrightarrow \{0\}$$

where

$$\mathrm{Coker}(\phi) = {}^{\mathrm{Div}(R)}\!/\!_{\{\langle x \rangle \mid x \in K^*\}} =: \mathrm{Pic}(R)$$

is the Picard group *of R or the* ideal class group *of R.*

If R is the ring of integers of an algebraic number field, then $|\mathrm{Pic}(R)| < \infty$ (this is hard to prove!) and it is called the class number *of $K = \mathrm{Quot}(R)$.*

Corollary 8.32. *For a DD R, the following are equivalent:*

(a) $|\mathrm{Pic}(R)| = 1$

(b) $\mathrm{Div}(R) = {}^{K^*}\!/\!_{R^*}$

(c) R is a P.I.D.

(d) R is a U.F.D.

Proof.

- "(a) $\iff$ (b)" by 8.31
- "(c) $\iff$ (d)" by Exercise 36
- "(a) $\implies$ (c)": Let $0 \neq I \trianglelefteq R$

$$\begin{aligned}&\implies I \text{ fractional}\\&\implies I \text{ invertible, i.e. } I \in \operatorname{Div}(R), \text{as } R \text{ is a DD}\\&\implies I \text{ principal, as } |\operatorname{Pic}(R)| = 1\end{aligned}$$

- "(c) $\implies$ (a)": Let I be any fractional ideal

$$\begin{aligned}&\implies I = \frac{1}{x} I', I' \trianglelefteq R, x \in R\\&\implies I' = \langle y \rangle\,, \text{ as } R \text{ is a PID}\\&\implies I = \left\langle \frac{y}{x} \right\rangle\end{aligned}$$

□

Corollary 8.33. *Let R be a DD and $h := |\operatorname{Pic}(R)|$ the class number of R. Then*

$$\forall\, I \trianglelefteq R : I^h \text{ is principal}$$

i.e. the class number measures, 'how far away' the ideals are from being principal.

Proof.

$$\begin{aligned}&0 \neq I \trianglelefteq R\\&\implies I \text{ fractional}\\&\implies I \text{ invertible, i.e. } I \in \operatorname{Div}(R)\\&\implies \overline{I^h} = \overline{I}^h = \overline{R} \in \operatorname{Pic}(R)\\&\implies I^h \in \{\langle x \rangle\,, x \in K^*\}\\&\implies I^h \text{ is principal}\end{aligned}$$

□

Remark 8.34 (cf. Bruns, §15). *Let*

$$R = \mathbb{Z}[\omega_d] = \mathrm{Int}_{\mathbb{Q}[\sqrt{d}]}(\mathbb{Z}), d \leq 1 \textit{ squarefree}$$

in the notation of 8.22. How can we determine the class number of $\mathbb{Q}[\sqrt{d}]$*? The idea is the following:*

First, find all maximal ideals $P \lhd \cdot R$*, such that*

$$\left|{}^{R}\!/_{P}\right| \leq \frac{2}{\pi}\sqrt{|\omega_d - \overline{\omega_d}|^2} = \frac{2}{\pi}\,|\omega_d - \overline{\omega_d}|$$

where

$$|\omega_d - \overline{\omega_d}|^2 = \begin{cases} |d| & , d \equiv 1(4) \\ |4d| & , d \equiv 2,3(4) \end{cases}$$

There are only finitely many of these ideals and their classes generate $\mathrm{Pic}(R)$*. Check then, how many different products can be built of these.*

Example 8.35.

(a) $(d = -1)$: $R = \mathbb{Z}[i]$ is a PID, so by 8.32 $|\mathrm{Pic}(R)| = 1$.

(b) $(d = -19)$: $R = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID by 1.41 (cf. Appendix), so again $|\mathrm{Pic}(R)| = 1$. An alternative approach would be to consider

$$\frac{2}{\pi}\sqrt{|\omega_d - \overline{\omega_d}|^2} = \frac{2\sqrt{19}}{\pi} < 3$$

Then show that there exists no $P \lhd \cdot R$ with $\left|{}^{R}\!/_{P}\right| = 2$. Hence follows that $|\mathrm{Pic}(R)| = 1$ and from this, that R is a PID

(c) $(d = -5)$: $R = \mathbb{Z}[\sqrt{-5}]$

$$P = \langle 2, 1 + \sqrt{-5} \rangle \lhd \cdot R$$

is not principal, since ${}^{R}\!/_{P} = \{\overline{0}, \overline{1}\} \cong \mathbb{Z}_2$ is a field. Hence $|\mathrm{Pic}(R)| \neq 1$.

Now consider

$$\frac{2}{\pi}\sqrt{|\omega_d - \overline{\omega_d}|^2} = \frac{4}{\pi}\sqrt{5} < 3$$

If $Q \lhd \cdot R$ with $\left|{}^{R}\!/_{Q}\right| = 2$, then $Q = P$, since:

$$\begin{aligned} & 1 \notin Q, \left|{}^{R}\!/_{Q}\right| = 2 \\ \Longrightarrow\ & 2 \in Q, \text{ since } \overline{1} + \overline{1} = \overline{2} = \overline{0} \\ \Longrightarrow\ & P^2 = \langle 2 \rangle \subseteq Q \\ \Longrightarrow\ & P \subseteq Q, \text{ as } Q \text{ is prime} \\ \Longrightarrow\ & P = Q, \text{ as both are maximal} \end{aligned}$$

Since $P^2 = \langle 2 \rangle$ is principal

$$\begin{aligned} &\Longrightarrow \overline{P}^2 = \overline{R} \in \operatorname{Pic}(R) \\ &\Longrightarrow \operatorname{Pic}(R) = \{\overline{R}, \overline{P}\} \\ &\Longrightarrow |\operatorname{Pic}(R)| = 2 \end{aligned}$$

(d) ($d \leq -1$, without proof):

$$\mathbb{Z}[\omega_d] \text{ UFD } \iff d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$$

Index