Algebra 1

Introduction to Commutative Algebra

Lecture Notes, Summer 2019

Contents

Introduction

These are my lecture notes for the course *Algebra 1*, held by Dr. Thorsten Heidersdorf in the summer term 2019[1]. You can find the current version on my website (https://pankratius.gitlab.io/notes). There is also a version on the course hompage, but it might be outdated. If you find mistakes (there are still a lot) or have suggestions, please send me an e-mail to s6aawild@uni-bonn.de. I want to thank everyone who already pointed some of them out to me and apologize for the long time it took me to fix them.

The recomended literature for this course is [**AM94**], [**EE95**] and [**MR89**]. I also like to use [**Alu09**].

Dr. Heidersdorf introduced categories and (exact) functors in lecture 6. I decided to put this (and a bit more) in a seperate appendix, which will be added during the semester. For now, the reader is e.g. refered to [**Ste19**].

Future Aaron here: Me introducing categories and stuff in the appendix did not happen during the semester. Overall, the appendix is a *huge* mess. I hope I will be able to fix this during the summer, before the new semester starts. I also plan to add some more stuff which I found interesting (and not too far away from the lecture) as well as the missing proof of the last few lectures. I also want to include the results of the exercise sheets, but still have to figure out the right places. The last lecture (lecture 23) was a big black box, and I am still not sure up to what detail I will be able to fix this.

And one more thing – I hope I will be able to do the same next semester for *Algebraic Geometry 1*, so stay tuned... .

[1] Last change: `2019-07-10 10:31:42 +0200`; Current commit: `05ab381`

CHAPTER 1

Rings

Convention. In this lecture rings are assumed to be

i) commutative: for all $ab = ba$ holds for all $a, b \in R$,
ii) unital: there is an element $1 = 1_R \in R$ such that $1a = a$ for all $a \in R$.

Ring homomorphisms $f : R \to S$ always respect the unit, i.e. $f(1_R) = 1_S$ holds.

1.1. Ideals

Definition* 1.A. Let $I \subseteq R$ be an ideal. Then I is a *proper ideal* or *proper* if $I \neq R$.

Definition 1.1.

i) A proper ideal $\mathfrak{p} \subsetneq R$ is a *prime ideal* if for all $x, y \in R$ with $xy \in \mathfrak{p}$, already $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ holds.
ii) A proper ideal $\mathfrak{m} \subsetneq R$ is a *maximal ideal* if there is no ideal I with $\mathfrak{m} \subsetneq I \subsetneq R$.

Notation* 1.B. I try to follow Dr. Heidersdorf's way of naming ideals, with one typographical addition: ordinary ideals are denoted as I, J,..., prime ideals as $\mathfrak{p}$,... and maximal ideals as $\mathfrak{m}$,... .

Lemma 1.2. Let $I \subseteq R$ be an ideal.

i) The following are equivalent:
   a) I is a prime ideal.
   b) R/I is an integral domain.

ii) The following are equivalent:
   a) I is a maximal ideal.
   b) R/I is a field.

Proof. We denote the coset of an element $a \in R$ in R/I by $\overline{a}$.

i) Let I be a prime ideal, and let $\overline{x}, \overline{y} \in R/I$ such that $0 = \overline{x} \cdot \overline{y} = \overline{xy}$. This means that xy is in I. As I is prime, $x \in I$ or $y \in I$ follows, and hence $\overline{x} = 0$ or $\overline{y} = 0$.

   Now assume that R/I is an integral domain. Let $x, y \in R$ with $xy \in I$. Hence $0 = \overline{xy} = \overline{x} \cdot \overline{y}$, and as R/I is an integral domain, $\overline{x} = 0$ or $\overline{y} = 0$ follows. So $x \in I$ or $y \in I$.

ii) Let I be maximal, and $x \notin I$. Consider the ideal generated by x and I, $\langle I, x\rangle$. As I is maximal and $I \subseteq \langle I, x\rangle$, we have $\langle I, x\rangle = R = \langle 1\rangle$. So there are $z \in I$, $y \in R$ such that $1 = xy + z$. So in R/I, we have

$$1 = \overline{xy + z} = \overline{x} \cdot \overline{y} + \overline{z} = \overline{x} \cdot \overline{y},$$

which shows that $\overline{x}$ is a unit in R/I.

Now assume that R/I is a field and let J be an ideal with $I \subseteq J \subseteq R$. If there is an $x \in J$ such that $x \notin I$, then $\overline{x}$ is invertible in R/I. So there are $z \in I$, $y \in R$ such that $1 = xy + z$. As $z \in J$ and $x \in J$ this implies $1 \in J$, and hence $J = R$.

□

Corollary 1.3. Let I be an ideal. If I is maximal then I is prime.

The following is a consequence of Zorn's Lemma and the ideal correspondence:

Lemma 1.4. Let $R \neq 0$ be a ring.

i) R contains a maximal ideal.
ii) Every ideal of R is contained in some maximal ideal.

Corollary 1.5.

i) Every $x \notin R^\times$ is contained in some maximal ideal of R.
ii) The units of R are given by the complement of the union over all maximal ideals $\mathfrak{m}$:

$$R^\times = R \setminus \bigcup_{\mathfrak{m} \text{ maximal ideal}} \mathfrak{m}.$$

iii) Let $\mathfrak{m} \subseteq R$ be a maximal ideal in a local ring R and $x \in \mathfrak{m}$. Then $1 + x$ is a unit in R.

Proof.

i) Consider the ideal generated by x. As x is not a unit $\langle x\rangle \subsetneq \langle 1\rangle$ holds. So by Corollary 1.5, there is a maximal ideal containing $\langle x\rangle$, and in particular x.
ii) Let $x \notin \mathfrak{m}$ for all maximal ideals $\mathfrak{m}$. Then $\langle x\rangle \subsetneq \mathfrak{m}$ for all maximal ideals $\mathfrak{m}$, and hence $\langle x\rangle = \langle 1\rangle$.

□

Example 1.6. Consider the case $R = \mathbf{Z}$. Then the prime ideals are $\langle 0\rangle$ and $\langle p\rangle$, for every prime number p.

Lemma* 1.C. Let R be a ring, and consider the polynomial ring $R[X_1, \ldots, X_n]$ in n variables. Then for every $0 \leq m \leq n$ there is an isomorphism

$$R[X_1, \ldots, X_n]/\langle X_1, \ldots, X_m\rangle \cong R[X_{m+1}, \ldots, X_n].$$

Example 1.7. Let R be an integral domain. Consider the polynomial ring in n variables, $R[X_1, \ldots, X_n]$. Let $m \leq n$ and consider the ideal $\langle X_1, \ldots, X_m\rangle$. Then by Lemma* 1.C, we have $R[X_1, \ldots, X_n]/\langle X_1, \ldots X_m\rangle \cong R[X_{m+1}, \ldots, X_n]$. As R is an integral domain, $R[X_{m+1}, \ldots, X_n]$ is too. So by Lemma 1.2,

$\langle X_1, \ldots, X_m \rangle$ is a prime ideal. However, $\langle X_1, \ldots, X_m \rangle$ is not necessarily maximal:

Consider the case $m = 2$, $n = 2$: the quotient $R[X_1, X_2]/\langle X_1, X_2 \rangle$ is isomorphic to R. So, again by Lemma 1.2, $\langle X_1, X_2 \rangle$ is maximal if and only if R is a field.

1.2. The Spectrum of a Ring

Definition 1.8. Let R be a ring, $M \subseteq R$ a set. We define

$$Z(M) \coloneqq \left\{ \mathfrak{p} \subset R \;\middle|\; \begin{array}{l} \mathfrak{p} \text{ is a prime ideal of } R, \\ M \subseteq \mathfrak{p}. \end{array} \right\}.$$

Lemma 1.9. For every set $M \subseteq R$

$$Z(M) = Z(\langle M \rangle)$$

holds.

Example 1.10.

i) $Z(\langle 1 \rangle) = \emptyset$. $Z(\langle 0 \rangle)$ is the set of all prime ideals.
ii) Let $\mathfrak{m}$ be a maximal ideal. Then $Z(\mathfrak{m}) = \{\mathfrak{m}\}$. For prime ideals, the converse is also true: Let $\mathfrak{p}$ be a prime ideal with $Z(\mathfrak{p}) = \{\mathfrak{p}\}$. By Lemma 1.4, there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$. So $\{\mathfrak{p}, \mathfrak{m}\} \subseteq Z(\mathfrak{p})$, which implies $\mathfrak{p} = \mathfrak{m}$. Hence $\mathfrak{p}$ is maximal.
iii) Consider $\mathbf{Z}$, and let $n \in \mathbf{Z}$. Then $Z(\langle n \rangle) = \{p \mid p \text{ prime}, p \text{ divides } n\}$.

Definition 1.11. Let X be a set, and V a system of subsets of X. We say V defines a *topology* on X if the following holds:

i) arbitrary intersections of elements of V are again in V;
ii) finite unions of elements of V are again in V;
iii) X and $\emptyset$ are in V.

In this case, the elements of V are called *closed sets*.

Proposition 1.12. Let $I, J \subseteq R$ be ideals and $\{I_\lambda\}_{\lambda \in \Lambda}$ a collection of ideals of R.

i) If $I \subseteq J$ then $Z(I) \supseteq Z(J)$;
ii) $Z(IJ) = Z(I) \cup Z(J)$;
iii) $Z\left(\sum_{\lambda \in \Lambda} I_\lambda\right) = \bigcap_{\lambda \in \Lambda} Z(I_\lambda)$.

Proof.

i) Every prime ideal that contains J also contains I, hence $Z(J) \subseteq Z(I)$.
ii) IJ is a subset of both I and J. So by i), $Z(IJ) \supseteq Z(I)$ and $Z(IJ) \supseteq Z(J)$; hence $Z(IJ) \supseteq Z(I) \cup Z(J)$.

Let $\mathfrak{p}$ be a prime ideal with $IJ \subseteq \mathfrak{p}$. Assume $I \nsubseteq \mathfrak{p}$, and let $x \in I$ be an element with $x \notin \mathfrak{p}$. For all $y \in J$ the product xy is an element of $IJ \subseteq \mathfrak{p}$. As $\mathfrak{p}$ is a prime ideal, $y \in \mathfrak{p}$ follows, and hence $J \subseteq \mathfrak{p}$. This implies $Z(IJ) \subseteq Z(I) \cup Z(J)$.

iii) Let $\mathfrak{p}$ be a prime ideal that contains all of the I_λ. As ideals are closed under addition, $\mathfrak{p}$ also contains $\sum_{\lambda\in\Lambda} I_\lambda$. So $\bigcap_{\lambda\in\Lambda} Z(I_\lambda) \subseteq Z\left(\sum_{\lambda\in\Lambda} I_\lambda\right)$. On the other hand, every I_λ is a subset of $\sum_{\lambda\in\Lambda} I_\lambda$, so every prime ideal that contains $\sum_{\lambda\in\Lambda} I_\lambda$ in particular contains each I_λ, and hence $Z\left(\sum_{\lambda\in\Lambda} I_\lambda\right) \subseteq \bigcap_{\lambda\in\Lambda} Z(I_\lambda)$.

□

Corollary 1.13. The collection of the $Z(I)$ for all ideals I of R define a topology on the set of all prime ideals of R.

Definition 1.14. The *spectrum* $\operatorname{Spec} R$ of R is the set of all prime ideals of R with the topology from Corollary 1.13. This topology is called the *Zariski topology*.

Definition⋆ 1.D. The set of all maximal ideals of R is denoted by $\operatorname{MaxSpec} R$.

Definition 1.15. A set in $\operatorname{Spec} R$ is *open* if it is of the form $\operatorname{Spec} R \setminus Z(I)$, for an ideal I.

Recall the following fact about quotient rings:

Proposition 1.16. Let $I \subseteq R$ be an ideal and $\varphi : R \to R'$ a ring homomorphism such that $I \subseteq \ker\varphi$. Then there is a unique ring homomorphism $\varphi' : R/I \to R'$ such that the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ \downarrow & \nearrow_{\varphi'} & \\ R/I & & \end{array}$$

In the case $I = \ker\varphi$, φ' is a ring isomorphism

$$R/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi.$$

Lemma 1.17. Let $\varphi : R \to R'$ be a ring homomorphism and $\mathfrak{p} \subset R'$ a prime ideal. Then the preimage $\varphi^{-1}(\mathfrak{p}) \subset R$ is again a prime ideal.

Proof. Consider the composition

$$\tilde{\varphi} : R \xrightarrow{\varphi} R' \longrightarrow R'/\mathfrak{p}.$$

Then $\ker\tilde{\varphi} = \varphi^{-1}(\mathfrak{p})$. By Proposition 1.16, there exists a unique, injective ring homomorphism $\varphi' : R/\varphi^{-1}(\mathfrak{p}) \to R'/\mathfrak{p}$ such that the diagram

$$\begin{array}{ccccc} R & \xrightarrow{\varphi} & R' & \longrightarrow & R'/\mathfrak{p} \\ \downarrow & & & \nearrow_{\varphi'} & \\ R/\varphi^{-1}(\mathfrak{p}) & & & & \end{array}$$

commutes.

This identifies $R/\varphi^{-1}(\mathfrak{p})$ with a subring of $R'/\mathfrak{p}$. By applying Lemma 1.2 twice, we get that $\varphi^{-1}(\mathfrak{p})$ is indeed a prime ideal. □

Remark⋆ 1.E. This statement is in general not true for maximal ideals: Consider the embedding $\mathbf{Z} \hookrightarrow \mathbf{Q}$. Then the preimage of the maximal ideal $\langle 0\rangle \subseteq \mathbf{Q}$ is $\langle 0\rangle$, but $\langle 0\rangle$ is not maximal in $\mathbf{Z}$.

Proposition 1.18. Every ring homomorphism $\varphi : R \to R'$ induces a continous map

$$\begin{aligned} \varphi^{\#} : \operatorname{Spec} R' &\longrightarrow \operatorname{Spec} R \\ \mathfrak{p} &\longmapsto \varphi^{-1}(\mathfrak{p}). \end{aligned}$$

Proof. By Lemma 1.17, $\varphi^{\#}$ is well-defined.
Let $I \subseteq R$ be an ideal. Then

$$\begin{aligned} \left(\varphi^{\#}\right)^{-1}(Z(I)) &= \left\{\mathfrak{p} \in \operatorname{Spec} R' \;\middle|\; \varphi^{\#}(\mathfrak{p}) \in Z(I)\right\} \\ &= \left\{\mathfrak{p} \in \operatorname{Spec} R' \;\middle|\; I \subseteq \varphi^{-1}(\mathfrak{p})\right\} \\ &= \left\{\mathfrak{p} \in \operatorname{Spec} R' \;\middle|\; \varphi(I) \subseteq \mathfrak{p}\right\} \\ &= Z(\varphi(I)), \end{aligned}$$

so $\varphi^{\#}$ is continous, as preimages of closed sets are closed. □

Notation* 1.F. The map $\varphi^{\#}$ is also denoted as $\operatorname{Spec}\varphi$.

Corollary 1.19. The assignment of the spectrum to a ring can be intepreted as a functor

$$\operatorname{Spec} : \mathbf{CRing}^{\mathrm{op}} \longrightarrow \mathbf{Top}.$$

In particular: Isomorphic rings have homeomorphic spectra.

Remark 1.20.

i) Let R be an integral domain. This is equivalent to $\langle 0\rangle$ being a prime ideal. Now let $\mathfrak{p}$ be any prime ideal. Then $\langle 0\rangle$ is in every open subset containing $\mathfrak{p}$. So $\operatorname{Spec} R$ is not Hausdorff.

ii) For any prime ideal $\mathfrak{p} \in \operatorname{Spec} R$,

$$\overline{\{\mathfrak{p}\}} = \bigcap_{\substack{I \subseteq \mathfrak{p} \\ I \text{ ideal}}} Z(I) = Z(\mathfrak{p}).$$

So $\mathfrak{p}$ is maximal if and only if $\{\mathfrak{p}\}$ is closed in $\operatorname{Spec} R$ (by Example 1.10).

iii) Let R be an integral domain. Then $\langle 0\rangle \in \operatorname{Spec} R$ is a point with

$$\overline{\{\langle 0\rangle\}} = Z(\langle 0\rangle) = \operatorname{Spec} R.$$

Remark* 1.G. Let $I \subseteq R$ be an ideal. Then the projection $\pi : R \twoheadrightarrow R/I$ induces a homeomorphism

$$\begin{aligned} \pi^{\#} : Z(I) &\xrightarrow{\sim} \operatorname{Spec} R/I \\ \mathfrak{p} &\longmapsto \pi(\mathfrak{p}). \end{aligned}$$

Lemma 1.21. $\operatorname{Spec} R$ is *quasi-compact*: for every covering

$$\operatorname{Spec} R = \bigcup_{\lambda \in \Lambda} U_\lambda$$

where each of the U_λ is an open subset of $\operatorname{Spec} R$ and Λ an arbitrary index set, there are finitely many $U_{\lambda_1}, \dots, U_{\lambda_n}$ such that

$$\operatorname{Spec} R = \bigcup_{i=1}^{n} U_{\lambda_i}.$$

PROOF. This will be on the first exercise sheet. □

End of Lecture 1

1.3. Radicals

We now want to find an equivalent characterisation of $Z(I) = Z(J)$ for two ideals I, J of R.

Definition 1.22. Let $I \subseteq R$ be an ideal. The *radical* of I is

$$\sqrt{I} \coloneqq \{x \in R \mid \text{there exists an } n > 0 \text{ such that } x^n \in I\}.$$

Definition* 1.H. An element $x \in R$ is called *nilpotent* if there is an $n > 0$ such that $x^n = 0$.

Example* 1.I.

i) The zero element is always nilpotent.
ii) In an integral domain, there are no non-zero nilpotent elements.

Lemma 1.23.

i) $\sqrt{I}$ is an ideal of R.
ii) $I \subseteq \sqrt{I} = \sqrt{\sqrt{I}}$.
iii) $\sqrt{I} = R$ if and only if $I = R$.
iv) $R/\sqrt{I}$ has no non-zero nilpotent elements.

PROOF.

i) Let $x, y \in \sqrt{I}$ and $m, n > 0$ such that $x^m, y^n \in I$. Then

$$(x+y)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i}.$$

Now by assumption $x^i \in I$ for $i \geq m$ and $y^{m+n-1-i} \in I$ for $i < m$. So the whole sum is in I, and hence $x + y \in \sqrt{I}$. Furthermore, we have for any $r \in R$

$$(rx)^m = r^m x^m$$

which is in I.

ii) By setting $n = 1$, we get $I \subseteq \sqrt{I}$, and hence $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. For the reverse inclusion, let $x \in \sqrt{\sqrt{I}}$ and $n > 0$ such that $x^n \in I$. Then there is a $m > 0$ such that $x^{nm} = (x^n)^m \in I$.

iii) As $1^n = 1$ for all $n > 0$, $1 \in I$ if and only if $1 \in \sqrt{I}$.

iv) Let $\overline{z} \in R/\sqrt{I}$ with $\overline{z}^n = 0$. Then $z^n \in \sqrt{I}$, so $z \in \sqrt{\sqrt{I}} = \sqrt{I}$, which is equivalent to $\overline{z} = 0$.

□

Definition 1.24.
i) An ideal I is a *radical ideal* if $I = \sqrt{I}$ holds.
ii) $\operatorname{Nil} R \coloneqq \sqrt{\langle 0 \rangle}$ is the *nilradical* .
iii) If R has no non-zero nilpotent elements then R is *reduced* .

Example* 1.J. Let $I \subseteq R$ be an ideal and $\pi : R \to I$ the canonical projection. Then the nilradical of R/I is given by

$$\begin{aligned}\operatorname{Nil} R/I &= \{\overline{x} \in R/I \mid \overline{x}^n = 0 \text{ for a } n > 0\} \\ &= \{\pi(x) \mid x \in R, x^n \in I \text{ for a } n > 0\} \\ &= \pi\left(\sqrt{I}\right).\end{aligned}$$

Lemma 1.25. An ideal I is a radical ideal if and only if R/I is reduced.

Proof. We have the following equivalences:

$$\begin{aligned}I \text{ is a radical ideal} &\iff \text{for all } x \in R,\ n > 0 \text{ with } x^n \text{ it holds that } x \in I \\ &\iff \text{in } R/I:\ \overline{x}^n = 0 \text{ implies } \overline{x} = 0 \\ &\iff R/I \text{ is reduced.}\end{aligned}$$

□

Definition 1.26. We call $R_{\text{red}} \coloneqq R/\operatorname{Nil} R$ the *reduced ring associated to* R.

Example 1.27. Let $R = \mathbf{Z}$ and $I = \langle a \rangle$ for an $0 \neq a \in \mathbf{Z}$. How does $\sqrt{\langle a \rangle}$ look like? Consider the decomposition into prime factors

$$a = p_1^{m_1} \cdot \ldots \cdot p_l^{m_l}.$$

Then $\sqrt{\langle a \rangle} = \langle p_1 \ldots p_l \rangle$:

If $x \in \sqrt{\langle a \rangle}$, then there is a $n > 0$ such that $x^n \in \langle a \rangle$. So a divides x^n, and hence $p_1, \ldots p_l$ divide x, which implies $x \in \langle p_1 \ldots p_l \rangle$. Let now $x \in \langle p_1 \ldots p_l \rangle$. Choose $n \geq \max\{m_1, \ldots, m_l\}$. Then $x^n \in \langle p_1^n \ldots p_l^n \rangle \subseteq \langle p_1^{m_1} \ldots p_l^{m_l} \rangle = \langle a \rangle$ which implies $x \in \sqrt{\langle a \rangle}$.

Proposition 1.28. For any ideal I

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \text{ prime} \\ I \subseteq \mathfrak{p}}} \mathfrak{p}$$

holds.

Proof. Let $x \in \sqrt{I}$ and $n > 0$ such that $x^n \in I$. Let $\mathfrak{p}$ be a prime ideal with $I \subseteq \mathfrak{p}$. Then $x^n \in \mathfrak{p}$, and as $\mathfrak{p}$ is a prime ideal, this already implies $x \in \mathfrak{p}$.

For the converse, assume that x is in the intersection of all prime ideals that contain I and that $x \notin \sqrt{I}$. We now want to use Zorn's Lemma in a non-obvious way to arrive at a contradiction. For that, define

$$\Sigma \coloneqq \left\{ J \subset R \;\middle|\; \begin{array}{l} J \text{ is an ideal of } R, \\ \text{for all } n > 0\text{: } x^n \notin J. \end{array} \right\}.$$

First note that $I \in \Sigma$, as $x \notin \sqrt{I}$; so $\Sigma \neq \emptyset$. Furthermore, Σ is partially ordered by inclusion. Let $(J_t)_{t\in T}$ be a non-empty chain in Σ and consider

$$\tilde{J} \coloneqq \bigcup_{t\in T} J_t.$$

Then $\tilde{J}$ contains I, is an ideal[1] and does not contain x^n for any $n > 0$. So $\tilde{J}$ is an upper bound of $(J_t)_{t\in T}$. By Zorn's Lemma, this implies that Σ contains a maximal element $\tilde{\mathfrak{p}}$. We now show that $\tilde{\mathfrak{p}}$ is a prime ideal:

Let $a, b \in R \setminus \tilde{\mathfrak{p}}$. Then $\langle a\rangle + \tilde{\mathfrak{p}}, \langle b\rangle + \tilde{\mathfrak{p}}$ strictly contain $\tilde{p}$ and hence cannot be in Σ. By definition of Σ, there are now $m, n > 0$ such that $x^m \in \langle a\rangle + \tilde{\mathfrak{p}}$ and $y^n \in \langle b\rangle + \tilde{\mathfrak{p}}$. So there are $c, d \in R$ and $r, s \in \tilde{\mathfrak{p}}$ such that $x^m = ac + r$ and $x^n = bd + s$. Now

$$\begin{aligned} x^{m+n} &(ac + r) \cdot (bd + s) \\ &= \underbrace{abcd}_{\in\langle ab\rangle} + \underbrace{rbd + sac + rs}_{\in\tilde{\mathfrak{p}}}, \end{aligned}$$

so $x^{n+m} \in \langle ab\rangle + \tilde{\mathfrak{p}}$. If ab would be an element of $\tilde{\mathfrak{p}}$, then $\langle ab\rangle \subseteq \tilde{\mathfrak{p}}$, which would imply $x^{n+m} \in \tilde{\mathfrak{p}}$. Therefore ab cannot be an element of $\tilde{\mathfrak{p}}$, which is equivalent to $\tilde{\mathfrak{p}}$ being prime.

But by the original assumption, $x \in \bigcap_{I\subseteq\mathfrak{p}} \mathfrak{p}$, and hence $x \in \tilde{\mathfrak{p}}$. This is a contradiction as $\tilde{\mathfrak{p}}$ is an element of Σ. □

Corollary 1.29.

i) The nilradical of R is given the intersection of all prime ideals of R:

$$\operatorname{Nil} R = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}.$$

ii)* The canonical projection $\pi : R \to R/\operatorname{Nil} R$ induces a homeomorphism

$$\pi^{\#} : \operatorname{Spec} R \xrightarrow{\sim} \operatorname{Spec}(R/\operatorname{Nil} R).$$

Proof. The spectrum of the quotient by $\operatorname{Nil} R$ is given by

$$\begin{aligned} \operatorname{Spec} R/\operatorname{Nil} R &= \{\text{prime ideals of } R/\operatorname{Nil} R\} \\ &= \{\pi(\mathfrak{p}) \mid \mathfrak{p} \text{ prime},\ \operatorname{Nil} R \subseteq \mathfrak{p}\} \\ &= \{\pi(\mathfrak{p}) \mid \mathfrak{p} \text{ prime}\}. \end{aligned}$$

□

Example* 1.K. Consider $R \coloneqq \mathbf{Z}/a\mathbf{Z}$. Then the nilradical is given by

$$\operatorname{Nil} R = \bigcap_{\substack{p \text{ prime} \\ p|n}} \langle \overline{p}\rangle = \langle \overline{p_1 \dots p_m}\rangle,$$

[1] Note that in general, unions of ideals are not ideals.

where $a = p_1^{m_1} \cdot \ldots \cdot p_l^{m_l}$. Note that this recovers the results of Example* 1.J and Example 1.27.

In particular, this shows that the nilradical of a ring is not necessarily a prime ideal.

Corollary 1.30. For any ideal I of R, $Z(I) = Z\left(\sqrt{I}\right)$ holds.

Proof. As $I \subseteq \sqrt{I}$, $Z\left(\sqrt{I}\right) \subseteq Z(I)$ follows (c.f. Proposition 1.12). On the other hand, as

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \text{ prime} \\ I \subseteq \mathfrak{p}}} \mathfrak{p},$$

every prime ideal that contains I also contains $\sqrt{I}$. So $Z(I) = Z\left(\sqrt{I}\right)$. □

Corollary 1.31. For all ideals I, J the following holds:

i) $Z(J) \subseteq Z(I)$ if and only if $\sqrt{J} \supseteq \sqrt{I}$.
ii) $Z(I) = Z(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Proof. By symmetry, it suffices to prove i). If $\sqrt{I} \subseteq \sqrt{J}$, then by Proposition 1.12 $Z\left(\sqrt{I}\right) \supseteq Z\left(\sqrt{J}\right)$ holds. Corollary 1.30 now implies $Z(I) \supseteq Z(J)$.

For the other direction, assume $Z(J) \subseteq Z(I)$. Then every prime ideal that contains J also contains I. Now

$$\begin{aligned} \sqrt{I} &= \bigcap_{\substack{\mathfrak{p} \text{ prime} \\ I \subseteq \mathfrak{p}}} \mathfrak{p} \\ &\subseteq \bigcap_{\substack{\mathfrak{p} \text{ prime} \\ J \subseteq \mathfrak{p}}} \mathfrak{p} = \sqrt{J}. \end{aligned}$$

□

We now introduce a notion similar to the nilradical, but for maximal ideals:

Definition 1.32. The *Jacobson radical* $\operatorname{Jac} R$ is defined as the intersection of all maximal ideals of R:

$$\operatorname{Jac} R := \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}.$$

Proposition 1.33. The Jacobson radical of R is given by

$$\operatorname{Jac} R = \left\{ x \in R \;\middle|\; 1 - ax \in R^\times \text{ for all } a \in R \right\}.$$

Proof.

„$\subseteq$ “: Let $x \in \operatorname{Jac} R$ and $a \in R$. Assume $1 - ax$ is not a unit in R. Then by Corollary 1.5 there is a maximal ideal $\mathfrak{m}$ containing $1 - ax$. But then

$$1 = (1 - ax) + ax$$

As both summands are in $\mathfrak{m}$, $1 \in \mathfrak{m}$ would follow, which is a contradiction.

„$\supseteq$ “: Let $x \in R$ be an element such that $1 - ax$ is a unit for every $a \in R$, and let $\mathfrak{m}$ be a maximal ideal that does not contain x. Then $\langle x \rangle + \mathfrak{m} = \langle 1 \rangle$, so there is a $a \in R$ and $y \in \mathfrak{m}$ such that $1 = ax + y$. But then $y = 1 - ax$ would be a unit, which is not possible (as $y \in \mathfrak{m}$).

□

1.4. Local Rings and Rings of Fractions

Definition 1.34. A ring R is *local* if it contains exactly one maximal ideal.

Example⋆ 1.L.

i) Every field is a local ring, with maximal ideal $\langle 0 \rangle$.

ii) Let $\mathfrak{p} \subseteq R$ be a prime ideal, $S \coloneqq R \setminus \mathfrak{p}$ and the localization $R_\mathfrak{p} \coloneqq S^{-1}R$. Then $R_\mathfrak{p}$ is a local ring:
Consider the ideal

$$I \coloneqq \left\{ \frac{a}{s} \;\middle|\; a \in \mathfrak{p}, s \in S \right\}.$$

Let $b/t \notin I$. Hence $b \notin \mathfrak{p}$, which implies $b \in S$. So b/t is a unit in $R_\mathfrak{p}$. This shows that every ideal $J \subseteq R_\mathfrak{p}$ with $J \subsetneq I$ contains a unit.

Lemma 1.35. Let $I \subsetneq R$ be an ideal. Then the following are equivalent:

i) R is a local ring with maximal ideal I;

ii) $R \setminus I \subseteq R^\times$;

iii) $R \setminus I = R^\times$.

Proof. This follows from Corollary 1.5. □

End of Lecture 2

Lemma 1.36. Let $\mathfrak{m} \subset R$ be a maximal ideal. If $1 + x$ is a unit in R for every $x \in \mathfrak{m}$, then R is a local ring with maximal ideal $\mathfrak{m}$.

Proof. Let $b \in R \setminus \mathfrak{m}$. As $\mathfrak{m}$ is maximal, $\langle b \rangle + \mathfrak{m} = R$. So there are $a \in R, x \in \mathfrak{m}$ such that $ab + x = 1$. Hence $ab = 1 - x \in R^\times$, by assumption. But then $\langle b \rangle = 1$, and hence b is a unit in R. The claim follows now from Lemma 1.35. □

Lemma⋆ 1.M. Let R be a local ring, with maximal ideal $\mathfrak{m}$. Then $1 + x$ is a unit for every $x \in \mathfrak{m}$.

Proof. This follows direclty from Proposition 1.33. □

Lemma⋆ 1.N. Let $\varphi : R \to k$ be a surjective ring homomorphism, where k is a field. Then $\ker \varphi$ is a maximal ideal of R.

Proof. By Proposition 1.16, there is a unique isomorphism $R/\ker\varphi \cong k$. The claim now follows from Lemma 1.2. □

Example 1.37.

i) For every prime number p and every $n \geq 1$, $R \coloneqq \mathbf{Z}/p^n\mathbf{Z}$ is a local ring: The prime ideals in R are in one-to-one, order preserving correspondence with the prime ideals in $\mathbf{Z}$ that contain $\langle p^n \rangle$. But the only prime ideal that contains $\langle p^n \rangle$ is $\langle p \rangle$. So R has only one prime ideal, given by $\langle \overline{p} \rangle$, which has to be maximal.

Note that for all $n > 1$, $\mathbf{Z}/p^n\mathbf{Z}$ is a finite local ring, which is not an integral domain, so in particular not a field.

ii) Let R be a local ring with maximal ideal $\mathfrak{m}$, and consider the *ring of formal power series*

$$R[[t]] \coloneqq \left\{ \sum_{i=0}^{\infty} a_i t^i \;\middle|\; a_i \in R \right\}$$

(for more on this ring, see A.1.1).
There is a well-defined evaluation map

$$\begin{array}{rcl} \mathrm{ev} : R[[t]] & \longrightarrow & R/\mathfrak{m} \\ \displaystyle\sum_{i=0}^{\infty} a_i t^i & \longmapsto & \overline{a_0} \end{array}$$

with kernel $\ker(\mathrm{ev}) = \mathfrak{m} + \langle t \rangle$. As ev is surjective, Lemma* 1.N implies that $\ker(\mathrm{ev})$ is a maximal ideal of $R[[t]]$.

It is also the only maximal ideal: Let $f \in \ker \mathrm{ev}$, so

$$f = \sum_{i=0}^{\infty} a_i t^i$$

with $a_0 \in \mathfrak{m}$. Consider now $1 + f$. We construct an inverse g for $1 + f$, so that the claim follows from Lemma 1.36: Let $g \in R[[t]]$ be a polynomial of the form

$$g = \sum_{i=0}^{\infty} b_i t^i.$$

The condition $(1 + f)g = 1$ is equivalent to requiring $(1 + a_0)b_0 = 1$ and

$$(1 + a_0)\, b_n + a_1 b_{n-1} + \ldots + a_n b_0 = 0 \text{ for all } n > 0.$$

By Lemma* 1.M $1 + a_0$ is a unit in R, so such a b_0 exists. Assuming that $b_0, \ldots b_{n-1}$ are already constructed, the equation

$$(1 + a_0)\, b_n + a_1 b_{n-1} + \ldots + a_n b_0 = 0$$

can be re-written as

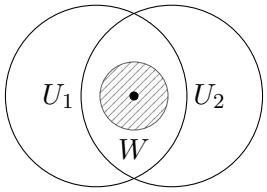
$$b_n \coloneqq -(1 + a_0)^{-1} \cdot (a_n b_0 + \ldots + a_1 b_{n-1}),$$

which is well-defined, as $(1 + a_0)$ is a unit. By induction, we obtain an inverse g for $1 + f$.

iii) Consider $\mathbf{R}^n$ with the standard topology, and let $X \subseteq \mathbf{R}^n$ be an open subset with $0 \in X$. We define an equivalence relation on the set of tuples

$$\left\{ (U, f) \;\middle|\; \begin{array}{l} U \subseteq X \text{ an open subset with } 0 \in U, \\ f : U \to \mathbf{R} \text{ continuous.} \end{array} \right\},$$

by setting $(U_1, f) \sim (U_2, g)$ if there is an open subset $W \subseteq X$ such that $0 \in W$, $W \subseteq U_1 \cap U_2$ and $f|_W = g|_W$. The equivalence class of (U, f) is denoted by $[U, f]$ and is called a *germ* at 0:



Consider now the set of all germs at 0

$$\mathcal{F}_0 \coloneqq \left\{ [U, f] \;\middle|\; \begin{array}{l} U \subseteq X \text{ an open subset with } 0 \in U, \\ f : U \to \mathbf{R} \text{ continuous.} \end{array} \right\},$$

which is called the *stalk* at 0. We can define a ring structure on $\mathcal{F}_0$ by setting

$$[U_1, f_1] + [U_2, f_2] \coloneqq [U_1 \cap U_2, f_1 + f_2]$$

and

$$[U_1, f_1] \cdot [U_2, f_2] \coloneqq [U_1 \cap U_2, f_1 \cdot f_2],$$

which is inherited from the pointwise ring structure on functions to $\mathbf{R}$. Note that this is well-defined: If $[U_1, f_1] = [U_1', f_1']$ such that $f_1|_{W_1} = f_1'|_{W_1}$ for an open subset $W_1 \subseteq U_1 \cap U_1'$ and $[U_2, f_2] = [U_2', f_2']$ such that $f_2|_{W_2} = f_2'|_{W_2}$, then $f_1 + g_1 = f_2 + g_2$ and $f_1 \cdot g_1 = f_2 \cdot g_2$ on $W_1 \cap W_2 \subseteq U_1 \cap U_2$.

The stalk $\mathcal{F}_0$ is a local ring: Consider the the ring homomorphism

$$\begin{array}{rcl} \varphi : \mathcal{F}_0 & \longrightarrow & \mathbf{R} \\ [U, f] & \longmapsto & f(0). \end{array}$$

This is well-defined, as all functions in the germ $[U, f]$ agree on 0. As $\varphi([X, f = c]) = c$ for all $c \in \mathbf{R}$, we see that φ is surjective and hence $\ker \varphi$ is a maximal ideal (Lemma* 1.N).

Let now $[U, f] \in \ker \varphi$. As f is continuous, there is an open neighbourhood W of 0 such that $1 + f(x) \neq 0$ for all $x \in W$. Hence $[W, 1/(1+f)]$ is the unit element of $\mathcal{F}_0$. The claim now follows from Lemma 1.36.

Remark* 1.O. Germs and stalks can be defined in the more general context of *(pre-)sheaves*. The example we considered is for the *sheaf of continous functions* $\mathbf{R}^n \to \mathbf{R}$. For more, the reader is refered to [Vak18, Chapter 2].

Remark* 1.P. Here are some more facts on $R[[t]]$ for a general ring R:

i) As R-modules the map

$$R[[t]] \to \prod_{\mathbf{N}} R, \qquad \sum_{i=0}^{\infty} a_i t^i \mapsto (a_i)_{i\in\mathbf{N}}$$

is a well-defined isomorphism. It is a classical (non-trivial) result that the infinite product $\prod_{\mathbf{N}} \mathbf{Z}$ is not a free.

ii) The units in $R[[t]]$ are of the form $a_0 + \ldots$, where a_0 is a unit in R. This similar to the case where R is local.

iii) So we can still describe the maximal ideals $\operatorname{MaxSpec} R[[t]]$: by ii), every maximal ideal necessarily contains t and hence corresponds to a maximal ideal of $R[[t]]/\langle t\rangle \cong R$. So we have

$$\operatorname{MaxSpec} R[[t]] = \{\mathfrak{m} + \langle t\rangle \mid \mathfrak{m} \in \operatorname{MaxSpec} R\}.$$

Since for any ideal $I \subseteq R$ the maximal ideals over $I + \langle t\rangle$ are precisley of the form $\mathfrak{m} + \langle t\rangle$ for the maximal ideals $\mathfrak{m}$ over $I \subseteq \mathfrak{m}$ the assignment

$$\begin{array}{rcl} \operatorname{MaxSpec} R[[t]] & \longleftrightarrow & \operatorname{MaxSpec} R \\ \mathfrak{m} & \longmapsto & \mathfrak{m} \cap R \\ \mathfrak{m} + \langle t\rangle & \longleftarrow\!\shortmid & \mathfrak{m} \end{array}$$

is a homeomorphism (where we equip $\operatorname{MaxSpec} R[[t]]$ and $\operatorname{MaxSpec} R$ with the subspace topology).

The following is a recollection of basic facts about rings of fractions. More details can be found in [Sch19, 5.17].

Definition 1.38. A subset $S \subseteq R$ is called *multiplicative* if

i) $1 \in S$;

ii) for all $a, b \in S$ it holds that $ab \in S$.

Remark/Definition 1.39. Let $S \subseteq R$ be a multiplicative set. We can define an equivalence relation on $S \times R$ by

$$(s, a) \sim (t, b) \text{ if there is a } u \in S \text{ such that } u\,(ta - sb) = 0.$$

Denote by $S^{-1}R$ the set of equivalence classes of $\sim$, and by a/s or $\frac{a}{s}$ the equivalence class $[(s, a)]$.

We can define a ring structure on $S^{-1}R$ by setting

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}$$

and

$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

To show that this is well-defined requires S to be multiplicative and some work, so we will not do this here.

The ring $S^{-1}R$ is called the *ring of fractions with respect to* S. Mostly, S will be left implicit, so that we refer to $S^{-1}R$ only as *the ring of fractions*.

Lemma 1.40.

i) The map

$$\begin{array}{rcl} \eta : R & \longrightarrow & S^{-1}R \\ a & \longmapsto & \dfrac{a}{1} \end{array}$$

is a ring homomorphism. The elements of S are invertible in $S^{-1}R$: $\eta(S) \subseteq \left(S^{-1}R\right)^{\times}$.

ii) If R has no zero-divisors, then $S^{-1}R$ has no zero-divisors too.

iii) If S has no zero-divisors, then η is injective.

PROOF. Ommited. □

Proposition 1.41. Let $S \subseteq R$ be a multiplicative subset and $g : R \to R'$ a ring homomorphism such that $g(S) \subseteq (R')^{\times}$. Then g factors over the ring of fractions: there is a unique ring homomorphism $g' : S^{-1}R \to R'$ such that

$$\begin{array}{ccc} R & \xrightarrow{\ g\ } & R' \\ {\scriptstyle \eta}\downarrow & \nearrow_{g'} & \\ S^{-1}R & & \end{array}$$

commutes.

PROOF. Ommited. □

Example 1.42.

i) Let $S = \{1\}$. Then $S^{-1}R \cong R$.

ii) Let $0 \neq a \in R$ be an element and

$$S \coloneqq \{a^n \mid n > 0\}.$$

Then $R_a \coloneqq S^{-1}R$ is called the *localization at* a.

iii) Let $\mathfrak{p}$ be a prime ideal and $S \coloneqq R \setminus \mathfrak{p}$. Then S is a multiplicative subset. Then $R_{\mathfrak{p}} \coloneqq S^{-1}R$ is the *localization at* $\mathfrak{p}$.

Example 1.43. Consider the case $R = \mathbf{Z}$. Then for any prime number p, the localization at p is given by

$$\mathbf{Z}_p = \left\{ \frac{a}{p^n} \;\middle|\; a \in \mathbf{Z}, n \geq 0 \right\}.$$

The localization at a prime ideal $\mathfrak{p} = \langle p \rangle$ however is given by

$$\mathbf{Z}_{\mathfrak{p}} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbf{Z},\ p \text{ does not divide } b \right\}.$$

Note that $\mathbf{Z}_p$ and $\mathbf{Z}_{\mathfrak{p}}$ are different from each other; both are extremly different from $\mathbf{Z}/p\mathbf{Z}$!

Lemma* 1.Q. For an element $x \in R$, the following are equivalent:

i) $x = 0$,

ii) $\eta(x) = 0$ for all prime ideals $\mathfrak{p} \in \operatorname{Spec} R$,

iii) $\eta(x) = 0$ for all maximal ideals $\mathfrak{m} \in \operatorname{MaxSpec} R$.

PROOF. Ommited. □

Definition 1.44. Let $\varphi : R \to R'$ be a ring homomorphism.

i) Let $J \subseteq R'$ be an ideal. We denote by

$$J \cap R \coloneqq \varphi^{-1}(J) \subseteq R$$

the *contraction* of J by φ.

ii) Let $I \subseteq R$ be an ideal. We denote by

$$IR' \coloneqq \langle \varphi(I) \rangle \subseteq R'$$

the *extension* of I by φ.

In both cases, the map φ is often left implicit.

Lemma 1.45. Let $\varphi : R \to R'$ be a ring homomorphism.

i) Extensions and contractions of ideals by φ are again ideals.

ii) For all ideals $I \subseteq R$ and $J \subseteq R'$, $I \subseteq (IR') \cap R = I$ and $J \supseteq (J \cap R) R' = J$ holds.

Theorem 1.46. *Let $S \subseteq R$ be a multiplicative subset.*

i) *If $I \subseteq R$ is an ideal, then*

$$I\left(S^{-1}R\right) = \left\{ \frac{a}{s} \;\middle|\; a \in I, s \in S \right\}.$$

ii) *If $I \subseteq R$ is an ideal, then*

$$I\left(S^{-1}R\right) \cap R = \{a \in R \mid \text{there is a } n \in S \text{ such that } na \in I\}.$$

iii) *If $J \subseteq S^{-1}R$ is an ideal, then*

$$(J \cap R) S^{-1}R = J.$$

iv) *If $\mathfrak{p}$ is a prime ideal in R with $\mathfrak{p} \cap S = \emptyset$, then $\mathfrak{p}\left(S^{-1}R\right)$ is a prime ideal in $S^{-1}R$.*

v) *The maps*

$$\begin{array}{rcl} \operatorname{Spec} S^{-1}R & \longleftrightarrow & \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \emptyset\} \\ \mathfrak{q} & \longmapsto & \mathfrak{q} \cap R \\ \mathfrak{p}\left(S^{-1}R\right) & \longmapsfrom & \mathfrak{p} \end{array}$$

are mutually inverse and preseve inclusions.

Remark* 1.R. The statement in v) is actually stronger: If we consider the set

$$\{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \emptyset\}$$

with the subspace topology in $\operatorname{Spec} R$, then the map $\mathfrak{q} \mapsto \mathfrak{q} \cap R$ is actually a homeomorphism.

Proof. Ommited. □

Remark* 1.S. In Theorem 1.46, all statements about contractions and extensions of ideals are with respect to the canonical inclusion $\eta : R \to S^{-1}R$.

Proof of Theorem 1.46.

i) Let $a/s \in S^{-1}R$ with $a \in I$ and $s \in S$. Then
$$\begin{aligned}\frac{a}{s} &= \frac{a}{1} \cdot \frac{1}{s} \\ &= \eta(a) \cdot \frac{1}{s},\end{aligned}$$
which is in $I\left(S^{-1}R\right)$, as $\eta(a)$ is.

Let now $x \in I\left(S^{-1}R\right)$, so there are $a_i \in I, b_i \in R$ and $s_i \in S$ such that
$$x = \sum_i \frac{b_i}{s_i} \cdot \frac{a_i}{1}.$$
Set
$$s \coloneqq \prod_i s_i \text{ and } a \coloneqq \sum_i b_i \left(\prod_{i \neq j} s_j a_j\right).$$
Then $s \in S$, as S is a multiplicative set, and $a \in I$, as I is an ideal. As $x = a/s$, the claim follows.

ii) Let $a \in \left(IS^{-1}R\right) \cap R$. Then $a/1 \in I\left(S^{-1}R\right)$. We now have the following chain of equivalences $a \in I\left(S^{-1}R\right)$ if and only if
$$\begin{aligned}&\text{there are } b \in I, t \in S, \text{ such that } \frac{a}{1} = \frac{b}{t} \\ \iff\ &\text{there are } b \in I \text{ and } s, t \in S \text{ with } s(ta - b) = 0 \\ \iff\ &\text{there is a } n \in S \text{ such that } na \in I,\end{aligned}$$
where the first equivalence follows from i), the second from the definition of the localization and the third from the following argument:

If there are such b, t and s, then $(st)a = sb$. But $n \coloneqq st$ is in S (as s and t are) and sb is in I, as b is. On the other hand, if there is a $n \in S$ such that $b \coloneqq na \in I$, then for $t \coloneqq n$ and $s \coloneqq 1$ we have $1 \cdot (na - na) = 0$.

iii) $(J \cap R) S^{-1}R \subseteq J$ is always true (Lemma 1.45). For the other inclusion, let $x = a/s \in J$. Then
$$\frac{a}{1} = \frac{s}{1} \cdot \frac{a}{s}$$
and hence $a \in J \cap R$. So $a/s \in (J \cap R) S^{-1}R$, by i).

iv) Let $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal with $\mathfrak{p} \cap S = \emptyset$, and let $a/s, b/t \in S^{-1}R \backslash \mathfrak{p}\left(S^{-1}R\right)$. If $(ab)/(st) \in S^{-1}R \setminus \mathfrak{p}\left(S^{-1}R\right)$. Then there are $c \in p, u \in S$ such that $(ab)/(st) = c/u$ (by i). By the definition of the localization, there is now a $v \in S$ such that
$$v\,(uab - stc) = 0.$$
So $(vu)\,ab = (vst)c \in \mathfrak{p}$, as $\mathfrak{p}$ is an ideal. But since $ab \notin \mathfrak{p}$ this implies $vu \in \mathfrak{p} \cap S$, contradicting $\mathfrak{p} \cap S = \emptyset$.

□

Corollary 1.47. Let $\mathfrak{p} \subseteq R$ be a prime ideal.

i) There is a bijection
$$\operatorname{Spec} R_{\mathfrak{p}} \longrightarrow \{\mathfrak{p}' \in \operatorname{Spec} R \mid \mathfrak{p}' \cap (R \setminus \mathfrak{p}) = \emptyset\} = \{\mathfrak{p}' \in \operatorname{Spec} R \mid \mathfrak{p}' \subseteq \mathfrak{p}\}.$$

ii) $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.

Corollary 1.48. The map

$$\operatorname{Spec}\eta : \operatorname{Spec} S^{-1}R \longrightarrow \operatorname{Spec} R$$

is injective, with image

$$\{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \emptyset\}.$$

Definition 1.49. In the special case $S = \{a^n \mid n \geq 0\}$ the image of $\operatorname{Spec}\eta$ is $D(a) \coloneqq \operatorname{Spec} R \setminus Z(\langle a \rangle)$, which is called a *principal open subset*.

Remark* 1.T. The principal open subsets form a *basis* for the Zariski topology: for every open subset $U \subseteq \operatorname{Spec} R$ and a point $x \in U$ there is a principal open subset $D(a)$ such that $x \in D(a) \subseteq U$.

End of Lecture 3

CHAPTER 2

Modules and Integral Extensions

2.1. Modules - Basics

Definition 2.1. An *R-module* M $(M, +, \cdot)$ is an abelian group $(M, +)$ together with a map

$$\begin{aligned} \cdot : R \times M &\longrightarrow M \\ a, x &\longmapsto ax \end{aligned}$$

such that

i) $(a+b)x = ax + bx$,
ii) $a(x+y) = ax + ay$,
iii) $a(bx) = (ab)x$,
iv) $1_R x = x$

for all $x, y \in M$ and $a, b \in R$.

Example 2.2.

i) Let k be a field. Then k-modules are precisely k-vector spaces.
ii) Let $I \subseteq R$ be an ideal. Then I can be regarded as an R-module, since it is closed under addition and multiplication by elements in R.
iii) Consider $R = \mathbf{Z}$. Let G be an abelian group. Then G is a $\mathbf{Z}$-module, by setting
$$nx \coloneqq \underbrace{x + \ldots + x}_{n \text{ times}}$$
and $(-1)x \coloneqq -x$.
iv) Let $\varphi : R \to R'$ be a ring homomorphism and let M be an R'-module. Then M can be regarded as an R-module, by setting
$$ay \coloneqq \varphi(a)y$$
for all $a \in R$. This is called *restriction of scalars*.

Definition 2.3. Let M, M' be R-modules and $f : M \to M'$ a map. We say f is an *R-linear map* if

i) $f(x + x') = f(x) + f(x')$,
ii) $f(ax) = af(x)$

for all $a \in R$ and $x, x' \in M$.

Remark 2.4.

i) Composition of R-linear maps are again R-linear: If $f : M \to N$ and $g : N \to O$ are R-linear maps, then their composition $g \circ f : M \to O$ is R-linear too.

ii) For all R-modules M, the identity map $\mathrm{id} : M \to M,\ x \mapsto x$ is R-linear.
iii) Let $f : M \to N$ be a bijective R-linear map. Then the inverse $f^{-1} : N \to M$ is R-linear too. In this case, we say f is an *isomorphism* of R-modules.

So we can construct a category R-**Mod**, where objects are R-modules and morphisms are R-linear maps.

iv) For two R-modules M, N, the set of R-linear maps
$$\hom_R(M,N) \coloneqq \left\{ f : M \to M' \;\middle|\; f \text{ is } R\text{-linear} \right\}$$
is an R-module, by setting $f+g : x \mapsto f(x)+g(x)$ and $af : x \mapsto f(ax)$ for all $f, g \in \hom_R(M,N)$ and $a \in R$. In the notation, the ring R is sometimes ommited and we just write $\hom(M,N)$ for $\hom_R(M,N)$. So R-**Mod** is an abelian and a pre-R-linear category.
v) For an R-module M, the set of R-linear maps $\mathrm{End}_R(M) \coloneqq \hom_R(M,M)$ has also *non-commutative* ring structure, by setting $fg : x \mapsto (f \circ g)(x)$ for all $f, g \in \mathrm{End}_R(M)$. We call $\mathrm{End}_R(M)$ the set of *R-linear endomorphism*, and f an *(R-linear) endomorphism.*

Remark* 2.A. Using the restriction of scalars from Example 2.2, we obtain a functor $F_\varphi : R'$-**Mod** $\to R$-**Mod** for all rings R, R' and ring homomorphisms $\varphi : R \to R'$. This functor is *faithful*: for all R'-modules M, N, the induced map $\hom_{R'}(M,N) \to \hom_R(M,N)$ is injective.

Example 2.5. Let M be a R-module. The map
$$\begin{aligned} M &\longrightarrow \hom_R(R,M) \\ x &\longmapsto [a \mapsto ax] \end{aligned}$$
is an isomorphism of R-modules, with inverse
$$\begin{aligned} \hom_R(R,M) &\longrightarrow M \\ f &\longmapsto f(1). \end{aligned}$$

Example 2.6. Let R be a ring. Then an $R[t]$-module is „the same“ as an R-module M, together with an endomorphism $f : M \to M$.

If M is an R-module, we can define the an $R[t]$-structure on M by setting $tm \coloneqq f(m)$ for all $m \in M$ and extending linearly:
$$\left(\sum_{i=0}^{n} a_i t^i \right)(m) \coloneqq \sum_{i=0}^{n} a_i f^{(i)}(m).$$

If, on the other hand, M is an $R[X]$-module, we can regard M as an R-module, by restriction of scalars for the embedding $R \hookrightarrow R[t]$. We also get an endomorphism $f : M \to M$, defined by $m \mapsto tm$.

Definition 2.7. Let M be an R-module. A subset $M' \subseteq M$ is an *R-submodule* if
i) M' is a subgroup of $(M, +)$ and
ii) for all $a \in R$ and $x \in M'$, it holds that $ax \in M'$.

If the ring R is clear, we will often refer to M' just as a *submodule.*

Example⋆ 2.B.

i) Let k be a field. Then k-submodules of k-modules are precisely k-subspaces.
ii) Let $I \subseteq R$ be an ideal. Then I is an R-submodule of R.
iii) Let $H \subseteq G$ be a subgroup of an abelian group G. Then H is a $\mathbf{Z}$-submodule.

Proposition 2.8. Let $M' \subseteq M$ be a submodule. Then the quotient group M/M' becomes an R-module, by setting

$$\begin{aligned} \cdot : R \times R/M' &\longrightarrow M/M' \\ r, x + M' &\longrightarrow (rx) + M'. \end{aligned}$$

The quotient map $M \to M/M'$ is R-linear.

Proof. Ommited. □

Definition 2.9. Let $f : M \to N$ be an R-linear map.

i) The *kernel* of f is defined as

$$\ker f \coloneqq \{x \in M \mid f(x) = 0\}.$$

ii) The *image* of f is defined as

$$\operatorname{im} f \coloneqq \{f(x) \mid x \in M\}.$$

Proposition 2.10. Let $f : M \to N$ be an R-linear map. The kernel of f is a submodule of M, the image of f is a submodule of N.

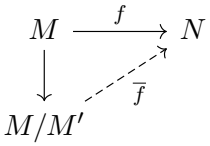
Definition 2.11. Let $f : M \to N$ be an R-linear map. The *cokernel* of f is defined as $\operatorname{coker} f \coloneqq N/\operatorname{im} f$.

Lemma⋆ 2.C. Let $f : M \to N$ be an R-linear map.

i) The kernel of f is trivial if and only if f is injective.
ii) The cokernel of f is trivial if and only if f is surjective.

Proposition 2.12. Let $f : M \to N$ be an R-linear map.

i) Let $M' \subseteq M$ be a submodule such that $M' \subseteq \ker f$. Then there is a unique R-linear map $\overline{f} : M/M' \to N$ such that the following diagram commutes:



ii) There is a unique isomorphism $\tilde{f} : M/\ker f \xrightarrow{\sim} \operatorname{im} f$ such that the following diagram commutes:

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ \downarrow & & \uparrow \\ M/\ker f & \xrightarrow[\tilde{f}]{\sim} & \operatorname{im} f \end{array}$$

PROOF. Ommited. □

End of Lecture 4

2.2. Free and Finitely Generated Modules

Lemma 2.13. Let M be an R-module, (M_i) a family of submodules of M. Then the intersection $\bigcap_i M_i$ and the sum

$$\sum_i M_i \coloneqq \left\{ \sum_i m_i \;\middle|\; \begin{array}{l} m_i \in M_i, \\ m_i \neq 0 \text{ for only finitely many } i. \end{array} \right\}$$

are submodules of M.

PROOF. Ommited. □

Definition 2.14.

i) Let $M_1, M_2 \subseteq M$ be submodules of an R-module M. If $M_1 \cap M_2 = \{0\}$ and $M_1 + M_2 = M$, we write $M_1 \oplus_{\text{int}} M_2 = M$. This construction is called the *(internal) direct sum* of M_1 and M_2.

ii) Let (M_i) be a family of R-modules. Then the *product* of the $\{M_i\}$ is defined as the cartesian product $\prod_i M_i$, with component-wise addition and scalar multiplication.

iii) Let (M_i) be a family of R-modules. Then the *direct sum* (or *coproduct*) $\{M_i\}$ is defined as the submodule

$$\bigoplus_i M_i \coloneqq \left\{ (m_i) \;\middle|\; \begin{array}{l} (m_i) \in \prod_i M_i, \\ m_i \neq 0 \text{ for only finitely many } i. \end{array} \right\} \subseteq \prod_i M_i.$$

Remark⋆ 2.D.

i) If we regard two submodules $M_1, M_2 \subseteq M$ of an R-module M with $M_1 \oplus_{\text{int}} M_2 = M$ as R-modules, then $M_1 \oplus M_2 \cong M = M_1 \oplus_{\text{int}} M_2$. So we will not distinguish further between the two notions.

ii) If (M_i) is a finite family of R-modules, then the product and direct sum of the M_i are equal.

iii) The product of a family (M_i) is indeed a product in the category R-**Mod**. The coproduct of a family (M_i) is indeed a coprodcut in the category R-**Mod**.

Definition 2.15. Let $\{x_i\}$ be a family of elements in an R-module M.

i) We say $\{x_i\}$ is a *generating system* of M, if every $x \in M$ can be written as a finite linear combination of x_i.
ii) We define the subspace $\operatorname{Lin}\{x_i\}$ *generated by* $\{x_i\}$ as

$$\operatorname{Lin}\{x_i\} \coloneqq \left\{ \sum a_i x_i \;\middle|\; \begin{array}{l} a_i \in I, \\ a_i \neq 0 \text{ for only finitely many } i. \end{array} \right\}.$$

iii) We say $\{x_i\}$ is *linearly independent* if for all tuples $(x_1, \ldots, x_n)$ of elements from $\{x_i\}$ there are no $a_i \in R$ such that

$$a_1 x_1 + \ldots + a_n x_n = 0.$$

iv) We say $\{x_i\}$ is a *basis* if it is a linearly independent generating system.
v) M is a *free R-module* if there is an index set I such that $M \cong \bigoplus_{i \in I} R$.
vi) M is a *finite-free R-module* if there is a finite index set I such that $M \cong \bigoplus_{i \in I} R$.
vii) M is a *finitely generated R-module* if M has a finite generating system.

Definition* 2.E. Let M be an R-module. We say M is *finitely presented* or that M is an *R-module of finite presentation* if there are integers n, m and an exact sequence of the form

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

Example* 2.F.
i) If M is finitely presented then M is already finitely generated.
ii) The converse is in general not true: The sequence $R^m \to R^n \to M$ being exact is equivalent to saying that $R^m \to R^n$ is a kernel for the projection $R^n \to M$. Consider now any non-noetherian ring and $I \subseteq R$ an ideal which is not finitely generated. Then R/I is not finitely presented. As a concrete example, there is no presentation for $k[t_1, \ldots]/\langle t_1, \ldots \rangle$.

Lemma* 2.G. Let M be an R-module.
i) M is free if and only if M has a basis.
ii) M is finite-free if and only if it is finitely generated and free.

Remark* 2.H. The alternative characterizations of a basis, as known from linear algebra for vector spaces, does not hold for general modules: Consider $R = \mathbf{Z}$ and $M = \mathbf{Z}$. Then $\mathbf{Z}$ has a basis given by $\{1\}$. However, the subset $\{2, 3\}$ is also linear independet, and the subset $\{2\}$ does not generate all of $\mathbf{Z}$.

Remark 2.16. Let M be a free R-module with basis $\{x_i\}_{i\in I}$. Let M' be another R-module and $\{y_i\}_{i\in I}$ a subset of M'. Then there is a unique R-linear map $f : M \to M'$ such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{\exists! f} & M' \\ \uparrow & \nearrow_{\overline{f}} & \\ \{x_i\}_{i\in I} & & \end{array}$$

commutes. Here, the map of sets $\overline{f} : \{x_i\}_{i\in I}$ is given by $\overline{f}(x_i) \coloneqq y_i$ for all $i \in I$. This is called the *universal property of a free module*.

If M' is a finitely generated R-module, then in particular there is a surjective map $R^n \to M'$.

Example 2.17.

i) For $R = \mathbf{Z}$ and $M = \mathbf{Z}/p\mathbf{Z}$, M is not a free $\mathbf{Z}$-module, as every element has torsion.

ii) For $R = \mathbf{Z}$ and $M = \mathbf{Q}$, M is not finitely generated as $\mathbf{Z}$-module.

Definition 2.18. Let M be an R-module and $I \subseteq R$ an ideal. We define the submodule IM as

$$IM \coloneqq \operatorname{Lin}\{am \mid a \in I, m \in M\}.$$

Lemma* 2.I. Let M be an R-module and $I \subseteq R$ an ideal. Then R/IM has the structure of an R/I-module.

Lemma 2.19. Let M be an R-module such that

$$R^n \cong M \cong R^m$$

for $n, m \in \mathbf{N}$. Then $m = n$ follows.

Proof. Let $\mathfrak{m} \subseteq R$ be a maximal ideal, so $R/\mathfrak{m}$ is a field. Then

$$\begin{aligned} \dim_{R/\mathfrak{m}R} M/\mathfrak{m}M &= \dim_{R/\mathfrak{m}R} R^n/\mathfrak{m}R^n \\ &= \dim_{R/\mathfrak{m}R} (R/\mathfrak{m}R)^n \\ &= n, \end{aligned}$$

so n is uniquely determined. □

Remark 2.20 (Linear Algebra for Modules)**.** For $n, m \in \mathbf{N}$, we can identify $\hom_R(R^n, R^m)$ with the set $\operatorname{Mat}(n \times m, R)$ of $n \times m$-matrices with entries in R. For an endomorphism $f : R^n \to R^n$, we have that f is an isomorphism if and only if its associated matrix is invertible.

Using the Leibniz formula, we define the *determinant* of a $n \times n$ matrix $A = (a_{i,j}) \in \operatorname{Mat}(n \times n, R)$ as

$$\det A \coloneqq \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \dots a_{n,\sigma(n)}.$$

Using the determinant, we associate to every matrix $A = (a_{i,j}) \in \operatorname{Mat}(n\times n, R)$ the *adjugate matrix* $\operatorname{adju} M$, which is defined as

$$\Big((\operatorname{adju} A)_{i,j}\Big) \coloneqq (-1)^{i+j} \det A_{j,i}$$

where the matrix $A_{j,i} \in \mathrm{Mat}\left((n-1)\times(n-1), R\right)$ is obtained from A by removing the j-th row and the i-th column. It then holds that

$$A \operatorname{adju} A = (\operatorname{adju} A)\, A = \det A \cdot E_n$$

where E_n denotes the $n \times n$ unit matrix. As the determinant stays multiplicative for matrices with entries in an arbitrary ring, we have that a matrix with entries in R is invertible if and only if its determinant is a unit in R.

Proposition 2.21 (Cayley-Hamilton for Modules)**.** Let M be a finitely generated R-module, $I \subseteq R$ an ideal and $f : M \to M$ an endomorphism, such that $f(M) \subseteq IM$. Then there is a monic polynomial $p = \sum_{i=0}^{n} a_i t^i \in R[t]$ such that $a_i \in I$ for $i \neq n$ and $p(f) = 0$ holds.

Proof. Let $\{m_1, \ldots, m_n\}$ be a generating set for M. Then $f(m_i) \in IM$ for all $1 \leq i \leq n$, and so there are $a_{ij} \in I$ for $1 \leq i, j \leq n$ such that

$$(*) \qquad f(m_j) = \sum_{i=1}^{n} a_{ij} m_i.$$

By Example 2.6, we can regard M as an $R[t]$-module, with the action $tx \coloneqq f(x)$ for all $x \in M$. The condition $(*)$ then reads as

$$\sum_{i=0}^{n} (t\delta_{ij} - a_{ij})\, m_j = 0 \quad \text{for all } 1 \leq j \leq n.$$

Consider now the matrices $A \coloneqq \left((t\delta_{ij} - a_{ij})_{i,j}\right)$ and $B \coloneqq \operatorname{adju} A$. Then $BA = \det A \cdot E_n$, and hence

$$\det\left((t\delta_{ij} - a_{ij})_{i,j}\right)(m_j) = 0.$$

The claim follows for the polynomial $p \coloneqq \det\left((t\delta_{ij} - a_{ij})_{i,j}\right)$. (That p is monic and the non-leading coefficients are in I follows from the Leibniz-formula.) □

Lemma 2.22. Let M be a finitely generated R-module and $f : M \to M$ a surjective R-linear map. Then f is already an isomorphism.

Proof. As in Example 2.6, we consider M as an $R[t_1]$ module. Consider the ideal $I \coloneqq \langle t_1 \rangle \subseteq R[t_1]$. As f is surjective, $IM = M$ follows. By Proposition 2.21 (for the endomorphism $\mathrm{id} : M \to M$), there is a polynomial $p = t_2^n + a_{n-1}t_2^{n-1} + \ldots + a_0 \in R[t_1][t_2]$ such that $p(\mathrm{id}) = 0$. So there is a polynomial $q \in R[t_1]$ with

$$\mathrm{id} = t_1 q(t_1).$$

Evaluating at f gives the invese. □

We will now state and prove two version of *Nakayama's Lemma*:

Lemma 2.23 (Nakayama - „the general one“)**.** Let M be a finitely generated R-module and $I \subseteq R$ an ideal with $IM = M$.

i) There is an $a \in I$ such that $am = m$ for all $m \in M$.
ii) There is a $x \in R$ such that $1 - x \in I$ and $xM = 0$.

Proof.

i) Apply Proposition 2.21 to $\mathrm{id} : M \to M$. Then there are $a_0, \ldots, a_{n-1} \in I$ such that
$$\mathrm{id} = (-(a_{n-1} + \ldots + a_0))\,\mathrm{id}\,.$$
As I is an ideal, $-(a_{n-1} + \ldots + a_0) \in I$.
ii) For $x \coloneqq 1 + a_{n-1} + \ldots + a_0$, where the $a_0, \ldots, a_{n-1}$ are choosen as in the proof of i), the claim follows.

□

Lemma 2.24 (Nakayama - „the classical one“)**.** Let M be a finitely generated R-module, and $I \subseteq \operatorname{Jac} R$ an ideal. Then $IM = M$ if and only if $M = 0$.

Proof. If $M = 0$, then $IM = 0$. If $IM = M$, then by Lemma 2.23 there is an $x \in R$ such that $1 - x \in \operatorname{Jac} R$. Now by Proposition 1.33, $x = 1 - (1 - x) \in R^\times$. But this implies $1m = 0$ for all $m \in M$. So $M = 0$. □

Lemma⋆ 2.J. Let M be a finitely generated R-module, and M' a submodule. Then M/M' is again finitely generated.

Proof. By Remark 2.16, there is a surjective map $R^n \to M$. Extend this to a surjective map $R^n \to M \to M/M'$. □

Remark⋆ 2.K. It is in general not true that submodules of finitely generated modules are again finitely generated: Let
$$I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq R$$
be a strictly increasing chain of ideals in a ring R. Then the ideal
$$I \coloneqq \bigcup_{i=1}^{\infty} I_i$$
is not finitely generated as an R-module.

Proof. I is an ideal, since it is the union over a chain of ideals. Furthermore, $I \neq R$, since there is no ideal I_i with $1 \in I_i$. If there were $f_1, \ldots, f_n$ such that $I = \langle f_1, \ldots, f_n \rangle$ then there would be a m such that $f_1, \ldots, f_n \in I_m$. But then $I \subseteq I_m \subsetneq I_{m+1} \subsetneq I$, which is not possible. So I is not a finitely generated R-module. □

So consider now the polynomial ring in infintely many variables over a ring $R \neq 0$, $R' \coloneqq R[t_1, t_2, \ldots]$. Then the chain of ideals
$$\langle t_1 \rangle \subsetneq \langle t_1, t_2 \rangle \subsetneq \ldots \subsetneq R'$$
is strictly increasing, so the submodule $\langle t_1, t_2, \ldots \rangle$ is not finitely generated as an R-module.

This observation leads to the following definition: A ring R is *noetherian* if it satisfies one of the following equivalent conditions:

i) All ideals $I \subseteq R$ are finitely generated as R-modules.
ii) There is no strictly increasing chain of ideals.
iii) Every non-empty set $\mathfrak{M}$ of ideals of R has an inclusion-maximal element.

We have already encountered noetherian rings: A field is noetherian, since there are no proper ideals other than $\langle 0 \rangle$. We showed (without using the name) last semester that PIDs are noetherian (in the proof that PIDs are factorial, [Sch19, Satz 5.30]).

In the same vein, we call an R-module M *noetherian* if it satisfies one of the following equivalent conditions:

i) Every submodule $N \subseteq M$ is finitely generated.
ii) There is no strictly increasing chain of submodules.
iii) Every non-empty set $\mathfrak{M}$ of submodules of M has an inclusion-maximal element.

It can be shown that an R-module M is noetherian if and only if it is finitely generated and $R/\operatorname{Ann}_R(M)$ is a noetherian ring (a proof can be found in [Fra17, 1.3, Prop. 5].)

Corollary 2.25. Let M be a finitely generated R-module, $N \subseteq M$ a submodule and $I \subseteq \operatorname{Jac} R$ such that

$$M = IM + N.$$

Then $M = N$ holds.

Proof. We have

$$\begin{aligned} I(M/N) &= (IM + N)/N \\ &= M/N. \end{aligned}$$

Then by Lemma* 2.J and Lemma 2.24, $M/N = 0$ follows, which implies $M = N$. □

End of Lecture 5

Lemma 2.26. Let M be a finitely-generated R-module, $m_1, \dots, m_n \in M$ and $I \subseteq \operatorname{Jac} R$ an ideal. Then the following are equivalent:

i) The set $\{m_i\}_i$ generates M as an R-module.
ii) The set $\{\overline{m_i}\}_i$ generates M/IM as an R/I-module.

Proof. If the set $\{\overline{m_i}\}_i$ generates M/IM as an R/I-module, then it also generates R/I as an R-module, since the canonical map $R \to R/I$ is surjective. So

$$\langle m_1, \dots, m_n \rangle + IM = M$$

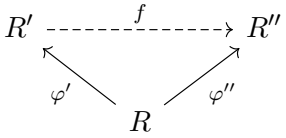
and by Corollary 2.25, $\langle m_1, \dots, m_n \rangle = M$ follows. □

2.3. Algebras

Definition 2.27. Let R be a ring.

i) A *R-algebra* consists of a tuple (R', φ), where R' is a ring and $\varphi : R \to R'$ is a ring homomorphism.

ii) Let $(R', \varphi'), (R'', \phi'')$ be R-algebras. A ring homomorphism $f : R' \to R''$ is an *R-algebra homomorphism* if the following diagram commutes:



iii) Let R' be an R-algebra. We say R' is *finitely generated as R-algebra* if there is a $n \geq 0$ and $b_1, \ldots, b_n \in R'$ such that the evaluation map

$$\begin{aligned} \mathrm{ev}_{b_1,\ldots,b_n} : R[t_1, \ldots, t_n] &\longrightarrow R' \\ t_i &\longmapsto b_i \end{aligned}$$

is surjective. In this case, we will also sometimes say that R' is *an R-algebra of finite type*.

Remark* 2.L. The morphism φ in the definition of an R-algebra is often left implicit.

Warning 2.28. Being finitely generated as R-module implies being finitely generated as an R-algebra. The converse is in general *not true*: For example, the polynomial ring $R[t_1, \ldots, t_n]$ is not a finitely generated R-module.

2.4. Localization of Modules

Remark/Definition 2.29. Let M be an R-module and $S \subseteq R$ be a multiplicative set. We can define an equivalence relation on $S \times M$ by

$$(s, x) \sim (t, y) \text{ if there is a } u \in S \text{ such that } u\,(tx - sy) = 0.$$

Denote by $S^{-1}M$ the set of equivalence classes of $\sim$, and by x/s or $\frac{x}{s}$ the equivalence class $[(s, x)]$.

We can define a $S^{-1}R$-module structure on $S^{-1}M$ by setting

$$\frac{x}{s} + \frac{y}{t} \coloneqq \frac{tx + sy}{st}$$

and

$$\frac{a}{s} \cdot \frac{y}{t} \coloneqq \frac{ay}{st}.$$

To show that this is well-defined requires S to be multiplicative and is analogous to the localization of rings.

The module $S^{-1}M$ is called the *localization of M by S*.

Further remkarks on the localization of modules can be found in C.3.

Proposition 2.30. Localization is functorial: Given a ring R and a multiplicative subset S, we can define a functor

$$\begin{aligned} S^{-1}(-) : R\text{-}\mathbf{Mod} &\longrightarrow S^{-1}R\text{-}\mathbf{Mod} \\ M &\longmapsto S^{-1}M \end{aligned}$$

which sends an R-linear map $f : M \to N$ to the induced $S^{-1}R$-linear map

$$\begin{aligned} S^{-1}f : S^{-1}M &\longrightarrow S^{-1}N \\ \frac{x}{s} &\longmapsto \frac{f(x)}{s}. \end{aligned}$$

PROOF. We need to show that $S^{-1}f$ is always a well-defined $S^{-1}R$-linear map. We only show well-definedness: Let $x/s = y/t$ in $S^{-1}M$. So there exists a $u \in S$ such that $u(tx - sy) = 0$. As f is R-linear, this implies $u\,(tf(x) - sf(y)) = 0$ and hence $f(x)/s = f(y)/t$. □

Definition 2.31.

i) A sequence of the form

$$\ldots \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow M_{i+1} \longrightarrow \ldots\,,$$

where the M_i are R-modules and the f_i are R-linear maps is called *exact at* i if $\operatorname{im} f_i = \ker f_{i+1}$. We say this sequence is *exact* if it is exact at every i.

ii) An exact sequence of the form

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

is a *short-exact sequence*.

Lemma 2.32.

i) The sequence $0 \longrightarrow M' \xrightarrow{f} M$ is exact if and only if f is injective.

ii) The sequence $M \xrightarrow{g} N \longrightarrow 0$ is exact if and only if g is surjective.

iii) The sequence $0 \longrightarrow M' \xrightarrow{h} M \longrightarrow 0$ is exact if and only if h is an isomorphism.

iv) Let $M' \subseteq M$ be a submodule. Then the sequence

$$0 \longrightarrow M' \hookrightarrow M \twoheadrightarrow M/M' \longrightarrow 0$$

is short-exact.

Lemma* 2.M. Let

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

be a short-exact sequence of R-modules. Then: M is finitely generated if and only if both M' and M'' are.

PROOF. This is on Exercise Sheet 3. □

Lemma 2.33. Let $S \subseteq R$ be a multiplicative set. Then the localization-functor $F : R\text{-}\mathbf{Mod} \to S^{-1}R\text{-}\mathbf{Mod}$ is exact.

PROOF. F is additive: Let $f, f' : M \to N$ be two R-linear maps. Then

$$\begin{aligned} F\left(f + f'\right)(x/s) &= \frac{(f + f')(x)}{s} \\ &= \frac{f(x) + f'(x)}{s} \\ &= \frac{f(x)}{s} + \frac{f'(x)}{s} \\ &= F(f)(x/s) + F\left(f'\right)(x/s)\,. \end{aligned}$$

Let now $y/t \in \ker F(g)$, so $g(y)/t = 0$. Now by the definition of the localization there is a $u \in S$ such that $ug(y) = 0$, and hence $uy \in \ker g$. As

the original sequence is short exact, there is a $x \in M$ such that $f(x) = uy$. Then $F(f)\,(x/(ut)) = (uy)/(ut) = y/t$, so y/t is in the image of $F(f)$. □

Corollary 2.34. Let $N \subseteq M$ be a submodule of an R-module M. Then $S^{-1}\,(M/N) \cong \left(S^{-1}M\right) / \left(S^{-1}N\right)$.

Proof. Consider the short-exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0\ .$$

Since localization is an exact functor, the sequence

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

is exact too. Hence $S^{-1}M/S^{-1}N \cong S^{-1}\,(M/N)$. □

End of Lecture 6

2.5. Integral Extensions

Convention. In this and the remaining sections of this chapter, we will consider R-algebras R', induced by ring homomorphisms $\varphi : R \to R'$. In the notation, φ will be ommited, i.e. for $a \in R$ and $b \in R'$, $ab \coloneqq \varphi(a)b$. If φ is injective, we will show this pictorial by a hooked arrow $\hookrightarrow$. In this case we further identify R with a subset of R'. So for an element $a \in R$ and $\varphi : R \hookrightarrow R'$, $a \in R'$ means $\varphi(a) \in R'$.

Definition 2.35. Let R' be an R-algebra.

i) An element $a \in R'$ is *integral over* R if there is a monic polynomial $p \in R[t]$ such that $p(a) = 0$, i.e. there are $c_{n-1}, \ldots, c_0 \in R$ such that
$$a^n + c_{n-1}a^{n-1} + \ldots + c_0 = 0.$$
ii) The ring R' is *integral over* R if all $a \in R'$ are integral over R.
iii) The set
$$\overline{R} \coloneqq \left\{a \in R' \;\middle|\; a \text{ integral over } R\right\}$$
is the *integral closure* of R in R'.
iv) The ring R is *integraly closed in* R' if $\overline{R} = \operatorname{im}(\varphi : R \to R')$.
v) The ring R' is *finite over* R if R' is finitely generated as R-module.

Example 2.36. Consider the inclusion $\mathbf{Z} \hookrightarrow \mathbf{Q}$: Let $a \in \mathbf{Q}$ be integral over $\mathbf{Z}$. Then there is a monic polynomial $p \in \mathbf{Z}[t]$ such that $p(a) = 0$, i.e. there are $c_{n-1}, \ldots, c_0 \in \mathbf{Z}$ such that

$$0 = a^n + c_{n-1}a^{n-1} + \ldots + c_0.$$

Let now $a = r/s$ where $r, s \in \mathbf{Z}$ are coprime. Then

$$r^n = -s\left(c_{n-1}r^{n-1} + \ldots + c_0 s^n\right)$$

and hence s divides r. So $s \in^{\times} Z = \{\pm 1\}$, which implies $a \in \mathbf{Z}$ and thus $\overline{\mathbf{Z}} = \mathbf{Z}$.

This argument still holds if we replace $\mathbf{Z}$ by a general factorial ring R and $\mathbf{Q}$ by $\operatorname{Quot} R$.

Warning 2.37. Unlike in the special case of fields, the condition that a polynomial p is monic is necessary, as it is in general not possible to invert the leading coefficient. For example, $a = 1/2 \in \mathbf{Q}$ is a root of $2t - 1 \in \mathbf{Z}[t]$, but still not integral over $\mathbf{Z}$.

Remark/Definition 2.38. Let R' be an R-algebra and $b_1, \ldots, b_n \in R'$. We denote by

$$R[b_1, \ldots, b_n] \coloneqq \left\{ \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} b^{i_1} \ldots b^{i_n} \;\middle|\; a_{i_1,\ldots,i_n} \in R \right\} \subseteq R'$$

the smallest R-subalgebra of R' which contains all of the $b_1, \ldots, b_n$.

Lemma 2.39. Let R' be an R-algebra, $b \in R'$. Then the following are equivalent:

i) b is integral over R.
ii) The R-subalgebra $R[b]$ is a finitely generated R-module.
iii) There is a R-subalgebra $\tilde{R} \subseteq R'$ such that $R[b] \subseteq \tilde{R} \subseteq R'$, $\tilde{R}$ is a finitely generated R-module and $b \in \tilde{R}$.

Proof. i) $\implies$ ii): Let $p = t^n + c_{n-1}t^{n-1} + \ldots + c_0 \in R[t]$ be a polynomial such that $p(b) = 0$. Then the set $\{1, b, \ldots, b^{n-1}\}$ generates $R[b]$ as R-module.

ii) $\implies$ iii): We can simply choose $\tilde{R} \coloneqq R[b]$.

iii) $\implies$ i): If we regard $\tilde{R}$ as an R-module, left-multiplication with b (i.e. the map $f_b : R' \to R'$, $m \mapsto b \cdot m$) is an R-linear endomorphism of R'.

As $\tilde{R}$ is finitely generated as an R-module, Cayley-Hamilton (Proposition 2.21) implies that there is a monic polynomial $p \in R[t]$ such that $p(f_b) = 0$. So in particular we have $0 = p(f_b)(1) = p(b)$. □

Lemma 2.40. Let $\varphi : R \to R'$ and $\varphi' : R' \to R''$ be ring homomorphisms, and consider R' as an R-algebra and R'' as an R'-algebra.

i) If R' is finite over R and R'' is finite over R', then R'' is finite over R.
ii) If R' is integral over R and R'' is integral over R', then R'' is integral over R.

Proof. Ommited. □

Corollary 2.41. Let R' be an R-algebra. Then the following are equivalent:

i) R' is finite over R.
ii) There are elements $b_1, \ldots, b_n \in R'$ which are integral over R such that $R' = R[b_1, \ldots, b_n]$.
iii) R' is an R-algebra of finite type and integral over R.

Corollary 2.42. Let R' be an R-algebra. Then the integral closure $\overline{R} \subseteq R'$ is an R-subalgebra.

Remark⋆ 2.N. Let $\varphi : R \to R'$ be a ring homomorphism and let $S \subseteq R$ be a multiplicative set. Then the localization of R' by S as an R-module and the localization of R' by $f(S)$ as a ring are isomorphic as R-algebras.

Lemma⋆ 2.O. Let R' be an R-algebra via the ring homomorphism $\varphi : R \to R'$ and $S \subseteq R$ a multiplicative set. Then the localization $S^{-1}R'$ is still a ring and the induced map of $S^{-1}R$-modules

$$\begin{aligned} S^{-1}(\varphi) : S^{-1}R &\longrightarrow S^{-1}R' \\ \frac{a}{s} &\longmapsto \frac{\varphi(a)}{s} \end{aligned}$$

is also a ring homomorphism.

Lemma 2.43. Let R' be an R-algebra and R' integral over R.

i) Let $I \subseteq R'$ be an ideal and $J \coloneqq R \cap I$. Then R'/I is integral over R/J.

ii) Let $S \subseteq R$ be a multiplicative set. We can regard the localized $S^{-1}R$-module $S^{-1}R'$ as an $S^{-1}R$ module via the induced map from Lemma⋆ 2.O. Then $S^{-1}R'$ is integral over $S^{-1}R$.

Proof. Ommited. □

2.6. Going Up and Going Down

Definition⋆ 2.P. Let R' be an R-algebra via the ring homomorphism $\varphi : R \to R'$. If φ is injective and R' integral over R, we say that R' is an *integral extension of* R.

Lemma 2.44. Let R and R' be integral domains and R' an integral extension of R. Then R' is a field if and only if R is a field.

Proof. Assume that R' is a field and let $a \in R \setminus \{0\}$. We want to show that the inverse b of a, which exists in R', is an element of R. As b is integral over R, there are $c_0, \dots, c_{n-1} \in R$ such that $b^n = \sum c_i b^i$. Since $b = a^{n-1}b^n$, we have

$$b = \sum_{i=0}^{n-1} c_i a^{n-1-i}$$

so $b \in R$. Note that we did not need that R or R' is an integral domain for this direction.

Let now $a \in R' \setminus \{0\}$. As a is integral over R, $R[a]$ is a finite dimensional R-vector space (R is assumed to be a field). Consider now the map

$$\begin{aligned} f_a : R[a] &\longrightarrow R[a] \\ m &\longmapsto am. \end{aligned}$$

This is R-linear and injective, as R' is an integral domain, and hence bijective. So there is a $b \in R'$ such that $ab = 1$. □

Lemma 2.45. Let R' be an R-algebra which is integral over R and $\mathfrak{q} \subseteq R'$ a prime ideal. Set $\mathfrak{p} \coloneqq \mathfrak{q} \cap R$. Then $R/\mathfrak{p} \to R'/\mathfrak{q}$ is an integral extension.

PROOF. By Lemma 2.43 we have that $R'/\mathfrak{q}$ is integral over $R/\mathfrak{p}$. Let $\varphi : R \to R'$ be the ring homomorphism that induces the R-algebra structure on R'. Then for the composition

$$\overline{\varphi} : R \xrightarrow{\varphi} R' \longrightarrow R'/\mathfrak{q}$$

we have $\mathfrak{p} = R \cap \mathfrak{q} = \ker \overline{\varphi}$. So we get a factorisation of the form

$$\begin{array}{ccccc} R & \xrightarrow{\varphi} & R' & \longrightarrow & R'/\mathfrak{q} \\ \downarrow & & & \nearrow_{\overline{\varphi}'} & \\ R/\mathfrak{p} & & & & \end{array}$$

and $\overline{\varphi}'$ is injective. So $R'/\mathfrak{q}$ is an integral extension of $R/\mathfrak{p}$. □

Remark⋆ 2.Q. In the lecture, the claim of Lemma 2.45 was only made for injective ring homomorphisms $\varphi : R \hookrightarrow R'$. But this is not necessary, since the induced map $\overline{\varphi}'$ is injective, even if φ was not (this is also the version stated in [**Fra18b**, Prop. 6.8]).

Corollary 2.46. Let R' be an R-algebra which is interal over R and $\mathfrak{q} \subseteq R'$ a prime ideal. Set $\mathfrak{p} \coloneqq \mathfrak{q} \cap R$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.

PROOF. By Lemma 2.45, $R/\mathfrak{p} \hookrightarrow R'/\mathfrak{q}$ is an integral extension. The claim now follwos from Lemma 2.44 and Lemma 1.2 □

Lemma 2.47 (3am-Lemma)**.** Let R' be an integral extension of R and $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \in \operatorname{Spec} R'$ prime ideals with $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R$. Then already $\mathfrak{q}_1 = \mathfrak{q}_2$ holds.

PROOF. Let $\mathfrak{p} \coloneqq \mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R$ and consider $R'_{\mathfrak{p}}$ as the localized R-module or equivalently the localization by $\varphi(\mathfrak{p})$. (We have $R'_{\mathfrak{p}} \neq 0$ as φ is injective.) We then have the following commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi,\ \text{integral}} & R' \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta'} \\ R_{\mathfrak{p}} & \xrightarrow[\varphi',\ \text{integral}]{} & R'_{\mathfrak{p}} \end{array}$$

with maps

$$\eta' : R' \to R'_{\mathfrak{p}},\ a \mapsto \frac{a}{1}$$

and

$$\begin{array}{rcl} \varphi' : R_{\mathfrak{p}} & \longrightarrow & R'_{\mathfrak{p}} \\ \dfrac{a}{s} & \longmapsto & \dfrac{\varphi(a)}{\varphi(s)} = \dfrac{\varphi(a)}{s} \end{array}$$

where we identify $s \in R$ and $\varphi(s) \in R'$.

We now have that $\mathfrak{q}'_i \coloneqq \mathfrak{q}_i R'_{\mathfrak{p}}$ is a prime ideal in $R'_{\mathfrak{p}}$ for $i = 1, 2$, as $\mathfrak{q}_i \cap (\varphi(R \setminus \mathfrak{p})) = \emptyset$.

By the commutativity of the above diagram we get

$$\begin{aligned} \left(\mathfrak{q}'_i \cap R_{\mathfrak{p}}\right) \cap R &= \left(\mathfrak{q}'_i \cap R'\right) \cap R \\ &= \left(\left(\mathfrak{q}_i R'_{\mathfrak{p}}\right) \cap R'\right) \cap R. \end{aligned}$$

As $\mathfrak{p}$ is prime in R, we can use Theorem 1.46, v) to get $\left(\mathfrak{q}_i R'_{\mathfrak{p}}\right) \cap R' = \mathfrak{q}_i$ and hence

$$\begin{aligned}\left(\mathfrak{q}'_i \cap R_{\mathfrak{p}}\right) \cap R &= \mathfrak{q}_i \cap R \\ &= \mathfrak{p}.\end{aligned}$$

So, by Theorem 1.46, iii), we have that

$$\begin{aligned}\mathfrak{p}R_{\mathfrak{p}} &= \left(\left(\mathfrak{q}'_i \cap R_{\mathfrak{p}}\right) \cap R\right) R_{\mathfrak{p}} \\ &= \mathfrak{q}'_i \cap R_{\mathfrak{p}}.\end{aligned}$$

Now by Corollary 1.47, ii) we have that $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$, so by Corollary 2.46 we have that both $\mathfrak{q}'_1$ and $\mathfrak{q}_2$ are maximal in $R'_{\mathfrak{p}}$. But since we assumed $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ this implies $\mathfrak{q}'_1 = \mathfrak{q}'_2$.

Using Theorem 1.46 one last time, we get

$$\begin{aligned}\mathfrak{q}_1 &= \left(\mathfrak{q}_1 \cdot R'_{\mathfrak{p}}\right) \cap R' \\ &= \mathfrak{q}'_1 \cap R' \\ &= \mathfrak{q}'_2 \cap R' \\ &= \mathfrak{q}_2,\end{aligned}$$

which finishes the proof. □

Remark⋆ 2.R. The nickname "3am-Lemma" comes from a characterization of its proof Dr. Heidersdorf gave in the lecture. A more suitable description is that for the induced map $\varphi^{\#} : \operatorname{Spec} R' \to \operatorname{Spec} R$ there is no proper inclusion in thefibres.

Remark⋆ 2.S. The 3am-lemma should also be true if $\varphi : R \to R'$ is not assumed to be injective, c.f. [Sta19, 00GT]. One way of seeing this should be the following :

Let $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq R'$ be the prime ideals in question, and assume only that R' is integral over R. By Lemma 2.45, we get that $\overline{\varphi} : R/\mathfrak{p} \to R'/\mathfrak{q}_1$ is an integral extension. Denote by $\pi' : R' \to R'/\mathfrak{q}_1$ the canonical projection. We now can apply our version of the 3am-lemma (Lemma 2.47) to φ to get that $\pi'(\mathfrak{q}_1) = \pi'(\mathfrak{q}_2)$. So by Remark⋆ 1.G, we get $\mathfrak{q}_1 = \mathfrak{q}_2$.

End of Lecture 7

Lemma 2.48 (Lying Over)**.** Let $\varphi : R \hookrightarrow R'$ be an integral extension of R. Then for all prime ideals $\mathfrak{p} \in \operatorname{Spec} R$ there is a prime ideal $\mathfrak{q} \in \operatorname{Spec} R'$ such that $\mathfrak{q} \cap R = \mathfrak{p}$, i.e. the induced morphism $\operatorname{Spec} \varphi : \operatorname{Spec} R' \to \operatorname{Spec} R$ is surjective.

Proof. Let $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal. Consider the commutative diagram

$$\begin{array}{ccc} R & \xhookrightarrow{\varphi,\ \text{integral}} & R' \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta'} \\ R_{\mathfrak{p}} & \xhookrightarrow{\varphi',\ \text{integral}} & R'_{\mathfrak{p}} \end{array}$$

We have that φ' is injective, as localization is exact (Lemma 2.33). So in particular, $R'_{\mathfrak{p}} \neq 0$ and there is a maximal ideal $\mathfrak{n} \subseteq R'_{\mathfrak{p}}$. Since φ' is an integral extension $\mathfrak{n} \cap R_{\mathfrak{p}}$ is again maximal (Corollary 2.46).

By Corollary 1.47, $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ and thus $\mathfrak{n} \cap R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$. Set $\mathfrak{q} \coloneqq \mathfrak{n} \cap R' \subseteq R'$. Then:

$$\begin{aligned} \mathfrak{q} \cap R &= \left(\mathfrak{n} \cap R'\right) \cap R \\ &= (\mathfrak{n} \cap R_{\mathfrak{p}}) \cap R \\ &= (\mathfrak{p}R_{\mathfrak{p}}) \cap R \\ &= \mathfrak{p}. \end{aligned}$$

□

Definition 2.49. Let $\varphi : R \to R'$ be an algebra.

i) We say that φ satisfies *going up* if given a chain of prime ideals

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \ldots \subseteq \mathfrak{p}_n$$

in R and a chain of prime ideals

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \ldots \mathfrak{q}_m$$

in R' with $m \leq n$ and $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for all $1 \leq i \leq m$ there are prime ideals $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ such that the following holds:
- $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for all $m+1 \leq i \leq n$; and
- the ideals $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ fit into the chain

$$\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_{m+1} \subseteq \ldots \subseteq \mathfrak{q}_n.$$

ii) We say that φ satisfies *going down* if given a chain of prime ideals

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \ldots \supseteq \mathfrak{p}_n$$

in R and a chain of prime ideals

$$\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \ldots \mathfrak{q}_m$$

with $m \leq n$ and $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for all $1 \leq i \leq m$ there are prime ideals $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ such that the following holds:
- $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for all $m+1 \leq i \leq n$; and
- the ideals $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ fit into the chain

$$\mathfrak{q}_1 \supseteq \ldots \supseteq \mathfrak{q}_{m+1} \supseteq \ldots \supseteq \mathfrak{q}_n.$$

Lemma 2.50. Let $\varphi : R \to R'$ be a ring homomorphism.

i) The following are equivalent:
   a) φ satisfies going down.
   b) For all prime ideals $\mathfrak{q} \in \operatorname{Spec} R'$ and $\mathfrak{p} \coloneqq \mathfrak{q} \cap R$, the induced map $\operatorname{Spec} R'_{\mathfrak{q}} \to \operatorname{Spec} R_{\mathfrak{p}}$ is surjective.

ii) The following are equivalent:
   a) φ satisfies going up.
   b) For all prime ideals $\mathfrak{q} \in \operatorname{Spec} R'$ and $\mathfrak{p} \coloneqq \mathfrak{q} \cap R$, the induced map $\operatorname{Spec}(R/\mathfrak{p}) \to \operatorname{Spec}(R'/\mathfrak{q})$ is surjective.

c) The induced map $\varphi^{\#} : \operatorname{Spec} R' \to \operatorname{Spec} R$ is closed: images of closed sets in $\operatorname{Spec} R'$ under $\varphi^{\#}$ are closed in $\operatorname{Spec} R$.

PROOF. This will be on the 5th exercise sheet. □

Theorem 2.51 (Going Up for Integral Extensions)**.** *Let $\varphi : R \hookrightarrow R'$ be an integral extension. Then φ satisfies going up.*

PROOF. Let $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} R$ and $\mathfrak{q}_1 \in \operatorname{Spec} R'$ be prime ideals such that $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ and $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. We now have the following commutative diagram

$$\begin{array}{ccc} R & \xhookrightarrow{\varphi,\ \text{integral}} & R' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ R/\mathfrak{p}_1 & \xhookrightarrow[\varphi',\ \text{integral}]{} & R'/\mathfrak{q}_1 \end{array}$$

where φ' is an integral extension by Lemma 2.43 and Lemma 2.45. The ideal $\mathfrak{p}_2/\mathfrak{p}_1$ is prime in $R/\mathfrak{p}_1$ (Remark* 1.G) and hence Lying Over (Lemma 2.48) implies that there is a prime ideal $\mathfrak{q}_2' \in \operatorname{Spec} R'/\mathfrak{q}_1$ such that $\mathfrak{q}_2' \cap R/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$.

Consider now the prime ideal $\mathfrak{q}_2 \coloneqq \mathfrak{q}_2' \cap R'$. Then $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and

$$\begin{aligned} \mathfrak{q}_2 \cap R &= \left(\mathfrak{q}_2' \cap R'\right) \cap R \\ &= (\mathfrak{p}_2/\mathfrak{p}_1) \cap R \\ &= \mathfrak{p}_2. \end{aligned}$$

□

Remark* 2.T. There are also extension that are not integral but still satisfy going up: A trivial example is the embedding $\mathbf{Q} \hookrightarrow \mathbf{R}$ or more generaly any field extension that is not algebraic.

As another example, consider the embedding $\mathbf{Z} \hookrightarrow \mathbf{Z}[t]$. This is not integral (because by Corollary 2.41 this would imply that $\mathbf{Z}[t]$ is a finite $\mathbf{Z}$-module). However, for every prime ideal $\mathfrak{q} \in \mathbf{Z}$ the image $\mathfrak{p}\mathbf{Z}[t]$ is prime too.

Going Down for Integral over Normal.

Definition 2.52. Let $\varphi : R \to R'$ be an algebra and $I \subseteq R$ an ideal.

i) An element $b \in R'$ is *integral over I* if there is a monic polynomial $p \in R[t]$ such that $p(b) = 0$ and the non-leading coefficients of p are in I.

ii) The set

$$\overline{I} \coloneqq \left\{ b \in R' \;\middle|\; b \text{ is integral over } I \right\}.$$

is the *integral closure of I in R*.

Lemma* 2.U. Let $\varphi : R \to R'$ be an algebra and $I \subseteq R$ an ideal. Then an element $b \in R'$ is integral over I if and only if there is a $n > 0$ such that b^n is integral over I.

Lemma 2.53. Let $\varphi : R \to R'$ be an algebra and $I \subseteq R$ an ideal. Consider the ideal $I\overline{R} \subseteq \overline{R}$. Then $\overline{I} = \sqrt{I\overline{R}} \subseteq \overline{R}$.

PROOF. If $b \in \overline{I} \subseteq \overline{R}$ then there are $a_0, \dots, a_{n-1} \in I$ such that

$$b^n = a_{n-1}b^{n-1} + \dots + a_0,$$

so $b^n \in I\overline{R}$ and hence $b \in \sqrt{I\overline{R}}$.

Let now $b \in I\overline{R}$ (this suffices, by Lemma* 2.U), so there are $a_i, \dots, a_n \in I$ and $\overline{c}_1, \dots, \overline{c}_n \in \overline{R}$ such that $b = a_1c_1 + \dots + a_nc_n$. Since the c_i are integral over R, the module $M \coloneqq R[c_1, \dots, c_n]$ is finitely generated (by Lemma 2.39). Consider now the R-linear map

$$\begin{aligned} f_b : M &\longrightarrow M \\ x &\longmapsto xb^n. \end{aligned}$$

Then $\operatorname{im} f_b \subseteq IM$, and hence by Cayley-Hamilton (Proposition 2.21) there is a monic polynomial $p \in R[t]$ with non-leading coefficients in I such that $p(f_b) = 0$. So in particular, $p(b^n) = 0$, hence b is integral over I (again by Lemma* 2.U). □

Definition 2.54. Let R be an integral domain. We say R is *normal* if R is integrally closed in its quotient field.

Example 2.55. Every factorial ring is normal.

Lemma* 2.V. Being normal is a local property: For an integral domain, the following are equivalent:

i) R is normal.
ii) $R_\mathfrak{p}$ is normal for all $\mathfrak{p} \in \operatorname{Spec} R$.
iii) $R_\mathfrak{m}$ is normal for all $\mathfrak{m} \in \operatorname{MaxSpec} R$.

Lemma* 2.W. Let $\varphi : R \hookrightarrow R'$ be an injective map, with R, R' integral domains.

i) This induces a field extension $\operatorname{Quot} R \hookrightarrow \operatorname{Quot} R'$.
ii) If $R \hookrightarrow R'$ is integral, then $\operatorname{Quot} R \hookrightarrow \operatorname{Quot} R'$ is too,
iii) If $R \hookrightarrow R'$ is finite, then $\operatorname{Quot} R \hookrightarrow \operatorname{Quot} R'$ is too.

PROOF.

i) Since φ is injective, every non-zero element in R gets mapped to a unit in $\operatorname{Quot} R'$. So by the univesal property of the localization, we get an induced map

$$\begin{array}{ccc} R & \xhookrightarrow{\varphi} & R' \\ \downarrow & & \downarrow \\ \operatorname{Quot} R & \dashrightarrow & \operatorname{Quot} R' \end{array}$$

ii) Localizing R, R' (as modules) at $S \coloneqq R \setminus \{0\}$ gives an intgegral extension (Lemma 2.43) $\operatorname{Quot} R = S^{-1}R \hookrightarrow S^{-1}R'$. By Lemma 2.44, we get that $S^{-1}R'$ is a field, and hence $S^{-1}R' = \operatorname{Quot} R'$. So $\operatorname{Quot} R \hookrightarrow \operatorname{Quot} R'$ is algebraic.
iii) Localizing once again at $S \coloneqq R \setminus \{0\}$ gives a finite (localizing is exact) extension $\operatorname{Quot} R = S^{-1}R \hookrightarrow S^{-1}R'$. Arguing as in ii),

$\operatorname{Quot} R' = S^{-1}R'$ follows, so $S^{-1}R'$ is a finite $\operatorname{Quot} R$-vector space.

□

Lemma 2.56. Let $\varphi : R \hookrightarrow R'$ be an integral extension, with R, R' integral domains and R normal. Let $b \in R'$ be integral over some ideal $I \subseteq R$. Then $b/1$ is algebraic over $\operatorname{Quot} R$ and the non-leading coefficients of its minimal polynomial are already in $\sqrt{I}$.

PROOF. By Lemma* 2.W, there is indeed a minimal polynomial for b.

Set $K \coloneqq \operatorname{Quot} R$, and consider the intermediate field $K \subseteq K[b] \subseteq \operatorname{Quot} R'$. Let L be a field extension of $K[b]$ such that the minimal polynomial p of b is a product of linear factors in L (e.g. the algebraic closure of $K[b]$). So p has the form

$$p = (t - x_1) \dots (t - x_n),$$

where the $x_1, \dots, x_n$ are elements of L.

As b is integral over R, there is a monic polynomial $f \in R[t] \subseteq K[t]$ with $f(b) = 0$. By the minimal property of the minimal polynomial, $p \mid f$ follows and hence all roots of p are also roots of f which shows that the $x_1, \dots, x_n$ are integral over I. Since the non-leading coefficients of p are in $K[x_1, \dots, x_n]$ we get that they are integral over I too (Lemma* 2.U).

Since we assumed that R is normal, we get that the a_i are already in R. By applying Lemma* 2.U to $R' = K$, we get $\overline{I} = \sqrt{I}$, so $a_i \in \sqrt{I}$. □

Lemma 2.57. Let $\varphi : R \to R'$ be a ring homomorphism and $\mathfrak{p} \in \operatorname{Spec} R$ a prime ideal. Then the following are equivalent:

i) There is a prime ideal $\mathfrak{q} \in \operatorname{Spec} R'$ such that $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$.
ii) It holds that $\varphi^{-1}\left(\varphi(\mathfrak{p})R'\right) = \mathfrak{p}$.

PROOF. This will be on the 5th exercise sheet. □

Theorem 2.58 (Going Down)**.** *Let $\varphi : R \to R'$ be an integral extension. Assume that R, R' are integral domains and that R is normal. Then φ satisfies going down.*

End of Lecture 8

PROOF. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq R$ and $\mathfrak{q}_2 \subseteq R'$ be prime ideals such that $\mathfrak{p}_2 = \mathfrak{q}_2 \cap R$. We want to find a prime ideal $\mathfrak{q}_1 \in R'$ such that $\mathfrak{p}_1 = \mathfrak{q}_1 \cap R$ and $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$:

$$\begin{array}{ccccc} R' & \exists \mathfrak{q}_1 & \subseteq & \mathfrak{q}_2 \\ {\scriptstyle\varphi}\uparrow & \vdots & & \downarrow \\ R & \mathfrak{p}_1 & \subseteq & \mathfrak{p}_2 \end{array}$$

Consider now the map

$$\varphi' : R \xhookrightarrow{\varphi} R' \xhookrightarrow{\eta} R'_{\mathfrak{q}_2} .$$

We are going to show that under φ',

$$(*) \qquad \left(\mathfrak{p}_1 R'_{\mathfrak{q}_2}\right) \cap R = \mathfrak{p}_1$$

holds. Assume for now that this is the case. Then Lemma 2.57 implies that there is a prime ideal $\mathfrak{q}_1' \subseteq R'_{\mathfrak{q}_2}$ such that $\mathfrak{q}_1' \cap R = \mathfrak{p}_1$. For $\mathfrak{q}_1 \coloneqq \mathfrak{q}_1' \cap R'$ we have that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$, and $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ (by Corollary 1.47, i)), which shows that φ satisfies going down.

We now prove $(*)$: Note first that $\mathfrak{p}_1 \subseteq \left(\mathfrak{p}_1 R'_{\mathfrak{q}_2}\right) \cap R$ is always true. So it suffices to show $\left(\mathfrak{p}_1 R'_{\mathfrak{q}_2}\right) \cap R \subseteq \mathfrak{p}_1$. We will do this by contradiction:

Let $x \in \left(\mathfrak{p}_1 R'_{\mathfrak{q}_2}\right) \cap R$ be any element and consider $\varphi'(x) \in \mathfrak{p}_1 R'_{\mathfrak{q}_2}$, which we will identify with x. As $\mathfrak{p}_1 R'_{\mathfrak{q}_2} = \left(\mathfrak{p}_1 R'\right) R'_{\mathfrak{q}_2}$ there are $y \in \mathfrak{p}_1 R'$ and $s \in R' \setminus \mathfrak{q}_2$ such that $x = y/s$ (Theorem 1.46, i)). Now by Lemma* 2.U, y is integral over $\mathfrak{p}_1$ (we have $y \in \mathfrak{p}_1 R' \subseteq \sqrt{\mathfrak{p}_1 R'} = \sqrt{\mathfrak{p}_1 \overline{R}}$, since R' is integral over R.). Let $p_y \in (\operatorname{Quot}(R))[t]$ be the minimal polynomial of y over $K \coloneqq \operatorname{Quot}(R)$ (c.f. Lemma* 2.W). By Lemma 2.56, the non-leading coefficients of p_y, say $a_0, \ldots, a_{n-1}$, are in $\sqrt{\mathfrak{p}_1} = \mathfrak{p}_1$ (since $\mathfrak{p}_1$ is a prime ideal).

Assume now that $x \notin \mathfrak{p}_1$, so in particular $x \neq 0$ and hence s has the form $y/x \in \operatorname{Quot} R'$, and $1/x \in K$. This implies that the minimal polynomial p_s of s over k has the form

$$t^n + \frac{a_{n-1}}{t} t^{n-1} + \ldots + \frac{a_0}{x^n}.$$

Set $\tilde{a}_i \coloneqq a_i / x^{n-i}$ for $(i = 0, \ldots, n-1)$. Since $s \in R'$ is integral over R (by assumption on φ), we have by Lemma 2.56 that the $\tilde{a}_i$ are already in R.

Now in R, we have $\tilde{a}_i x^{n-1} = a_i \in \mathfrak{p}_1$, and since we assumed $x \notin \mathfrak{p}_1$, this implies $\tilde{a}_i \in \mathfrak{p}_1$ for all $i = 0, \ldots, n-1$. But then

$$s^n = -\left(\tilde{a}_{n-1} s^{n-1} + \ldots + \tilde{a}_0\right) \in \mathfrak{p}_1 R \subseteq \mathfrak{p}_2 R' \mathfrak{q}_2,$$

contradicting $s \notin \mathfrak{q}_2$. □

More Examples of Going Down. The proofs for the following propositions will (hopefully) be added in the future.

Theorem* 2.X. *Let $\varphi : R \to R'$ be flat, i.e. R' is flat as an R-module. Then φ satisfies going down.*

Theorem* 2.Y. *Let $\varphi : R \to R'$ be a ring homomorphism such that $\operatorname{Spec}\varphi : \operatorname{Spec} R' \to \operatorname{Spec} R$ is open (i.e. maps open sets to open sets.). Then φ satisfies going down.*

2.7. Noether Normalization Lemma

Theorem 2.59 (Noether Normalization Lemma (NNL))**.** *Let k be a field, and A a finitely generated k-algebra. Let*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_m \subsetneq A$$

be a chain of ideals in A. Then there is a $n \geq 0$, $a_1, \ldots, a_n \in A$ and $0 \leq h_1 \leq \ldots \leq h_m \leq n$ such that:

i) *the elements $a_1, \ldots, a_n$ are algebraically independent over k;*
ii) *$k[a_1, \ldots, a_n] \subseteq A$ is a finite ring extension; and*
iii) *$I_l \cap k[a_1, \ldots, a_n] = (a_1, \ldots, a_{h_l})$.*

We will only prove i) and ii). The proof of iii) can be found in [Fra18b].

Lemma 2.60. Let k be a field, and $0 \neq f \in k[t_1, \ldots, t_n]$ a non-zero polynomial. Then there are $r_1, \ldots, r_{n-1} \in \mathbf{N}$ such that after the substitution $t_i \coloneqq Y_i + t_n^{r_i}$ $(1 \leq i \leq n-1)$, the polynomial f has the form

$$f = ct_n^m + h_1 t_n^{m-1} + \ldots + h_m \in k[Y_1, \ldots, Y_{n-1}, t_n],$$

for a $m > 0$, $c \in k^\times$ and $h_1, \ldots, h_m \in k[Y_1, \ldots, Y_{n-1}]$.

Proof. Assume f has the form

$$f = \sum_{\sigma \in \mathbf{N}^n} b_\sigma t_1^{\sigma_1} \ldots t_n^{\sigma_n}.$$

After substituting $t_i \coloneqq Y_i + t_n^{r_i}$ for (yet to be determined) $r_i \geq 0$, this becomes

$$f = \sum_{\sigma \in \mathbf{N}^n} b_\sigma \left(Y_1 + t_n^{r_1}\right)^{\sigma_1} \ldots \left(Y_{n-1} + t_n^{r_{n-1}}\right)^{\sigma_{n-1}} t_n^{\sigma_n}.$$

Let now $\tau \in \mathbf{N}^n$ be a specific multi-index. Define

$$e(\tau) \coloneqq \tau_1 r_1 + \ldots + \tau_{n-1} r_{n-1} + \tau_n$$

With this notation, we obtain a factorisation of the τ-summand of f which reads as follows:

$$b_\tau t_n^{\tau_n} \prod_{i=1}^{n-1} \left(Y_i + t_n^{r_i}\right)^{\tau_i} = b_\tau t_n^{e(\tau)} + \\ (\text{terms where } t_n \text{ has stricly lower degrees}).$$

Claim 1. The r_i can be choosen in such a way that for each different pair of multi-indices $\sigma, \tau \in \mathbf{N}^n$, the associated exponents $e(\sigma), e(\tau)$ are different too:

By definition, there is a $M > 0$ such that $b_\sigma = 0$ for all multi-indices $\sigma \in \mathbf{N}^n \backslash \{0, \ldots, M-1\}$. Set now $r_1 \coloneqq M$, $r_2 \coloneqq M^2$, $\ldots, r_{n-1} \coloneqq M^{n-1}$, and let $\sigma \in \mathbf{N}^n$ be a multi-index with $b_\sigma \neq 0$. Then the value of

$$e(\sigma) = \sigma_n + \sum_{i=1}^{n-1} \sigma_i r_i = \sigma_n + \sigma_1 M + \ldots + \sigma_{n-1} M^{n-1}$$

is uniquely determined by the values of the $\sigma_1, \ldots, \sigma_n$ (since the M-adic expansion of a natural number is unique, and M was chosen in such a way that $\sigma_i < M$ for all $1 \leq i \leq n$).

Now for such a choice of r_i, there is a unique multi-index $\sigma \in \mathbf{N}^n$ such that the corresponding exponent $e(\sigma)$ is maximal and $b_\sigma \neq 0$. After re-grouping the expansion of f in decreasing order of powers of t_n, the claim follows with $m \coloneqq e(\sigma)$ and $c \coloneqq b_\sigma$. □

Proof of NNL (Theorem 2.59). Denote by $x_1, \ldots, x_m \in A$ a set of generators of A. We want to show that there are algebraically independent $a_1, \ldots, a_n$ such that the ring homomorphism $k[a_1, \ldots, a_n] \to A$ is injective and A is a finitely-generated $k[a_1, \ldots, a_n]$-module. We will do this by induction on the number m of generators:

The case $m = 0$ is trivial. So assume NNL holds for $m - 1$ generatos. If the $x_1, \ldots, x_m$ are algebraically independent then the canonical map $k[x_1, \ldots, x_m] \to A$ is indeed injective, and A is a finitely generated $k[x_1, \ldots, x_m]$-module.

If, however, the x_i are not algebraically independent, then there is a polynomial $0 \neq f \in k[t_1, \ldots, t_m]$ such that $f(x_1, \ldots, x_m) = 0$. Set $y_i := x_i - x_m^{r_i}$ for $1 \leq i \leq 0$ and (yet to be determined) r_i. We then have

$$0 = f\left(y_1 + x_m^{r_1}, \ldots, y_{m-1} + x_{m-1}^{r_{m-1}}\right).$$

But by Lemma 2.60, there is a set of exponents r_i such that

$$0 = f(y_1 + x_m^{r_1}, \ldots, y_{m-1} + x_{m-1}^{r_{m-1}}) = cx_m^d + h_1 x_m^{d-1} + \ldots + h_d$$

with $h_1, \ldots, h_d \in k[y_1, \ldots, y_{m-1}]$ and $c \in k^\times$. So x_m is integral over $k[y_1, \ldots, y_{m-1}]$ and $k[y_1, \ldots, y_{m-1}][x_m]$ is a finite $k[y_1, \ldots, y_{m-1}]$-module (Corollary 2.41). By induction hypothesis, there are algebraically independent $a_1, \ldots, a_n$ such that $k[a_1, \ldots, a_n] \hookrightarrow k[y_1, \ldots, y_{m-1}]$ is finite. Hence

$$k[a_1, \ldots, a_n] \hookrightarrow k[y_1, \ldots, y_{m-1}] \hookrightarrow k[y_1, \ldots, y_{m-1}][x_m] = A$$

is finite (Lemma 2.40), which proves the claim. □

End of Lecture 9

Notation. Let $s \in R$ and consider the multiplicative set $S := \{1, s, s^2, \ldots\}$. Then the localization of an R-module M at S is denoted by

$$M[s^{-1}] := S^{-1}M.$$

Lemma* 2.Z. Let R' be an R-algebra of finite type, and $S \subseteq R$ a multiplicative subset. Then the localization $S^{-1}R'$ of R' (as R-algebra) is an $S^{-1}R$-algebra of finite type.

Proof. Since R' is of finite type, there is surjective ring homomorphism $R[t_1, \ldots, t_n] \twoheadrightarrow R'$. Since localization is exact, we get an induced epimorphism

$$\left(S^{-1}R\right)[t_1, \ldots, t_n] \xrightarrow{\sim} S^{-1}\left(R[t_1, \ldots, t_n]\right) \twoheadrightarrow S^{-1}R'.$$

□

The following is a generalization of NNL to integral domains:

Proposition 2.61. Let R be an integral domain and R' an R-algebra of finite type.

i) There exists an element $s \in R \setminus \{0\}$ and elements $b_1, \ldots, b_n \in R'$ such that
   - the elements $b_1, \ldots, b_n$ are algebraically independent over the fraction field $\operatorname{Quot} R$; and
   - the ring extension
   $$R[s^{-1}][b_1, \ldots, b_n] \hookrightarrow R'[s^{-1}]$$
   is finite.

ii) For all prime ideals $\mathfrak{p} \subseteq R[s^{-1}]$ there is a prime ideal $\mathfrak{q} \subseteq R'[s^{-1}]$ such that $\mathfrak{q} \cap R[s^{-1}] = \mathfrak{p}$.

iii) For all prime ideals $\mathfrak{p} \in \operatorname{Spec} R[s^{-1}]$ and the prime ideal $\mathfrak{q}$ which was constructed in ii), it holds that

$$\begin{aligned}\operatorname{Quot}\left(R/(\mathfrak{p} \cap R)\right) = \operatorname{Quot}\left(R[s^{-1}]/\mathfrak{p}\right) &\subseteq \operatorname{Quot}\left(R'[s^{-1}]/\mathfrak{q}\right) \\ &= \operatorname{Quot}\left(R'/(\mathfrak{q} \cap R')\right),\end{aligned}$$

and the extension is a finite field extension.

PROOF.

i) Set $S := R \setminus \{0\}$. Then the induced extension

$$k := \operatorname{Quot} R = S^{-1}R \hookrightarrow S^{-1}R'$$

is of finite type (Lemma* 2.Z) and we can apply Noethers Normalization Lemma (Theorem 2.59) to get algebraically independent elements $b'_1, \ldots, b'_n \in S^{-1}R'$ such that $k[b'_1, \ldots, b'_n] \hookrightarrow S^{-1}R'$ is a finite ring extension. Choose now representatives $b_i \in R'$ and $s_i \in S$ such that $b'_i = b_i/s_i$. Then the b_i are already algebraically independent over k and $k[b_1, \ldots, b_n] = k[b'_1, \ldots, b'_n]$ (since $1/s_i$ is in k for all i).

As R' is an R-algebra of finite type, there are $c_1, \ldots, c_m \in R'$ (not necessarily algebraically independent) such that $R[c_1, \ldots, c_m] = R'$. As $S^{-1}R'$ is finite over $k[b_1, \ldots, b_n]$ it is in particular integral over $k[b_1, \ldots, b_n]$ (Corollary 2.41) and hence there are monic polynomials $f_i \in k[b_1, \ldots, b_n][t]$ such that $f_i(c_i/1) = 0$ in $S^{-1}R'$ (for $1 \leq i \leq m$). We can now choose a $u \in S$ such that the coefficients of all of the f_i are already in the image of the morphism

$$R[u^{-1}][b_1, \ldots, b_n] \longrightarrow k[b_1, \ldots, b_n]$$

which is induced by the embedding $R[u^{-1}] \hookrightarrow k$. Then there are monic polynomials $g_i \in R[u^{-1}][b_1, \ldots, b_n][t]$ such that g_i gets mapped to f_i for all $1 \leq i \leq m$. Since $b_i, c_i \in R'$ we have $g_i \in R'[u^{-1}]$. So $g_i \in \ker\left(R'[u^{-1}] \to S^{-1}R'\right)$, as $g(c_i)$ gets mapped to $f(c_i/1) = 0$ (by construction of the f_i). Hence there are $v_i \in R\setminus\{0\}$ such that $v_i g_i(c_i) = 0$ in $R'[u^{-1}]$. Define now $v := v_1 \ldots v_m$ and $s := vu$.

By the universal property of the localization at u and the fact that $R[u^{-1}][b_1, \ldots, b_n]$ we get a morphism

$$\psi : R[u^{-1}][b_1, \ldots, b_n] \longrightarrow R[s^{-1}][b_1, \ldots, b_n],$$

which also induces a morphism between the corresponding polynomial rings. Set $h_i := \psi(g_i) \in R[s{-}1][b_1, \ldots, b_n][t]$. Then the h_i are monic, since ψ is a ring homomorphism, and $h_i(c_i)0$. So the c_i are integral over $R[s^{-1}][b_1, \ldots, b_n]$, and thus $R[s^{-1}][b_1, \ldots, b_n] \hookrightarrow R'[s^{-1}]$ is finite (note $R'[s^{-1}] = R[s^{-1}][c_1, \ldots, c_m]$ and then apply Corollary 2.41).

ii) Let $\mathfrak{p} \in \operatorname{Spec} R[s^{-1}]$ be a prime ideal. Define

$$\mathfrak{p}' := \mathfrak{p}R[s^{-1}][b_1, \ldots, b_n] + \langle b_1, \ldots, b_n \rangle.$$

Then $\mathfrak{p}' \cap R[s^{-1}] = \mathfrak{p}$ the map

$$\begin{array}{rcl} R[s^{-1}][b_1, \ldots, b_n] & \longrightarrow & R[s^{-1}]/\mathfrak{p} \\ 1 & \longmapsto & \overline{1} \\ b_i & \longmapsto & 0 \end{array}$$

induces an isomorphism

$$R[s^{-1}][b_1, \dots, b_n]/\mathfrak{p}' \quad \xrightarrow{\sim} \quad R[s^{-1}]/\mathfrak{p}.$$

(Note that this is well-defined, since the b_i are algebraically independent). As $\mathfrak{p}$ is a prime ideal, we get that $\mathfrak{p}'$ is too.

Using Lying Over (Lemma 2.48) for the finite integral extension (by i))

$$R[s^{-1}][b_1, \dots, b_n] \longhookrightarrow R'[s^{-1}]$$

we get that there is a prime ideal $\mathfrak{q} \sin \operatorname{Spec} R'[s^{-1}]$ such that $\mathfrak{q} \cap R[s^{-1}][b_1, \dots, b_n] = \mathfrak{p}'$. Thus

$$\big(\mathfrak{q} \cap R[s^{-1}][b_1, \dots, b_n]\big) \cap R[s^{-1}] = \mathfrak{p}.$$

iii) Consider the following commutative diagram

$$\begin{array}{ccc} R[s^{-1}][b_1, \dots, b_n] & \xhookrightarrow[\text{integral}]{\text{finite}} & R'[s^{-1}] \\ \downarrow & & \downarrow \\ R[s^{-1}][b_1, \dots, b_n]/\mathfrak{p}' & \longhookrightarrow & R'[s^{-1}]/\mathfrak{q} \end{array}$$

Then

$$R[s^{-1}]/\mathfrak{p} \longhookrightarrow R'[s^{-1}]/\mathfrak{q}$$

is an integral extension too (Lemma 2.45) and finite, since

$$R[s^{-1}][b_1, \dots, b_n] \longhookrightarrow R'[s^{-1}]$$

is.

We also have that

$$\operatorname{Quot} R[s^{-1}]/\mathfrak{p} \hookrightarrow \operatorname{Quot} R'[s^{-1}]/\mathfrak{q}$$

is finite, by Lemma* 2.W.

As $s \notin \mathfrak{p} \cap R$, we have

$$\big(R[s^{-1}]\big)_{\mathfrak{p}} \Big/ \Big(\mathfrak{p} \cdot \big(R[s^{-1}]\big)_{\mathfrak{p}}\Big) \cong R_{\mathfrak{p} \cap R}/(R_{\mathfrak{p} \cap R}) \,,$$

which implies

$$\operatorname{Quot} R[s^{-1}]/\mathfrak{p} \cong \operatorname{Quot} R/\mathfrak{p} \cap R,$$

as for any ring A and $\mathfrak{b} \in \operatorname{Spec} A$ it holds that $\operatorname{Quot} A/\mathfrak{b} \cong A_{\mathfrak{b}}/\left(\mathfrak{b} \cdot A_{\mathfrak{b}}\right)$.

□

CHAPTER 3

Hilbert's Nullstellensatz and some Algebraic Geometry

3.1. Jacobson Rings

Definition 3.1. A ring R is a *Jacobson ring* if for all prime ideals $\mathfrak{p} \subseteq R$ it holds that

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{p} \subseteq \mathfrak{m} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}.$$

Lemma 3.2. For a ring R, the following are equivalent:

i) R is a Jacobson ring.

ii) For all prime ideals $\mathfrak{p} \subseteq R$ and $a \in R \setminus \mathfrak{p}$, there is a maximal ideal $\mathfrak{m}$ such that $\mathfrak{p} \subseteq \mathfrak{m}$ and $a \notin \mathfrak{m}$.

iii) For all ideals $I \subseteq R$ it holds that

$$\sqrt{I} = \bigcap_{\substack{I \subseteq \mathfrak{m} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}.$$

Proof. i) $\iff$ iii) follows from Proposition 1.28. □

Example 3.3.

i) Fields are Jacobson rings.

ii) If R is a local ring, which has only one prime ideal, the R is a Jacobson ring.

Example* 3.A.

i) If R be a noetherian domain such that every non-zero prime ideal is maximal and R has infinitely many maximal ideals, then R is Jacobson: Since every non-zero ideal is maximal, it suffices to show $\langle 0 \rangle = \operatorname{Jac} R$. For that, it suffices that every non-zero $x \in R$ is only contained in finitely many prime ideals, i.e. that $Z(x)$ is finite. But $Z(x)$ is isomorphic to $\operatorname{Spec} R/\langle x \rangle$. Now $R/\langle x \rangle$ is noetherian and every prime ideal is minimal. It is a general fact that noetherian rings have only finitely many minimal prime ideals so the claim follows.

ii) Claim i) implies that all factorial rings with infinitly many prime ideals are Jacobson (like $\mathbf{Z}$). Note that for a factorial ring the condition $\operatorname{Jac} R = 0$ suffices for being jacobson.

iii) Let on the other hand R be a domain which has only finitely many prime ideals. Then R cannot be Jacobson: We have

$$0 \neq \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n,$$

for the maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$.

Lemma 3.4. Let $\varphi : R \hookrightarrow R'$ be an integral extension. Assume R is a Jacobson ring. Then R' is too.

PROOF. Let $\mathfrak{q} \in \operatorname{Spec} R'$ be a prime ideal and set

$$J := \bigcap_{\substack{\mathfrak{q} \subseteq \mathfrak{m} \\ \mathfrak{m} \in \operatorname{MaxSpec} R}} \mathfrak{m}.$$

We first show that $J \cap R = \mathfrak{q} \cap R := \mathfrak{p}$:

Since R is a Jacobson ring $\mathfrak{p}$ is the intersection of all maximal ideals containing it. Now for any maximal ideal $\mathfrak{m} \in \operatorname{MaxSpec} R$ with $\mathfrak{p} \subseteq \mathfrak{m}$, going up (Theorem 2.51) implies that there is a prime ideal $\mathfrak{n} \in \operatorname{Spec} R'$ with $\mathfrak{n} \cap R = \mathfrak{m}$ and $\mathfrak{q} \subseteq \mathfrak{n}$. By Lemma 2.44 we get that $\mathfrak{n}$ is maximal too, and $J \cap R = \mathfrak{p}$ follows.

We are now in the following situation:

$$\begin{array}{ccc} R & \xrightarrow{\text{integral}} & R' \\ \downarrow & & \downarrow \\ R_{\mathfrak{p}} & \xrightarrow[\text{integral}]{} & R' \end{array} \qquad \begin{array}{ccc} \mathfrak{p} = R \cap \mathfrak{q} & \longrightarrow & \mathfrak{q} \\ & & \downarrow \\ & & \mathfrak{q}R'_{\mathfrak{p}}. \end{array}$$

Since $\mathfrak{q} \cap R = \mathfrak{p}$, we have $\varphi(R \setminus \mathfrak{p}) \cap \mathfrak{q} = \emptyset$, so $\mathfrak{q}R'_{\mathfrak{q}}$ is prime in $R'_{\mathfrak{p}}$. Furthermore, we have $\mathfrak{q}R'_{\mathfrak{p}} \cap R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$. Since $\mathfrak{p}R_{\mathfrak{p}}$ is a maximal ideal (Corollary 1.47), Lemma 2.44 implies that $\mathfrak{q}R'_{\mathfrak{p}}$ is a maximal ideal.

As $\mathfrak{q} \subseteq J$ we have $\mathfrak{q}R'_{\mathfrak{p}} \subseteq JR'_{\mathfrak{p}}$. Since $(R \cap J) \cap (R \setminus \mathfrak{p}) = \emptyset$ we have that $JR'_{\mathfrak{p}}$ is a proper ideal, so $\mathfrak{q}R'_{\mathfrak{p}} = JR'_{\mathfrak{q}}$ follows. But now

$$\begin{aligned} J \subseteq \left(JR'_{\mathfrak{p}}\right) \cap R' &= \mathfrak{q}R'_{\mathfrak{q}} \cap R' \\ &= \mathfrak{q}, \end{aligned}$$

so $J = \mathfrak{q}$ follows. □

3.2. Hilbert's Nullstellensatz

Theorem 3.5 (Generalized Hilbert's Nullstellensatz, GHNS)**.** *Let R be a Jacobson ring and R' an R-algebra of finite type. Then*

i) *R' is a Jacobson ring too.*

ii) *For all maximal ideals $\mathfrak{n} \subseteq R'$ it holds that:*
- *The ideal $\mathfrak{m} := \mathfrak{n} \cap R$ is a maximal ideal.*
- *For this $\mathfrak{m}$, $R/\mathfrak{m} \hookrightarrow R'/\mathfrak{n}$ is a finite field extension.*

PROOF.

i) Let $\mathfrak{q} \in \operatorname{Spec} R'$ be a prime ideal and $b \in R' \setminus \mathfrak{q}$. By Lemma 3.2, we want to show that there is a maximal ideal $\mathfrak{n} \in \operatorname{MaxSpec} R'$ such that $\mathfrak{q} \subseteq \mathfrak{n}$ and $b \notin \mathfrak{n}$.

Consider the ring extension:

$$\tilde{R} \coloneqq R/\left(\mathfrak{q} \cap R\right) \hookrightarrow R'/\mathfrak{q} \hookrightarrow \left(R'/\mathfrak{q}\right)\left[b^{-1}\right] =: \tilde{R}'.$$

Now $\tilde{R}$ is an integral domain and $\tilde{R} \hookrightarrow \tilde{R}'$ is an $\tilde{R}'$-algebra of finite type. So by Proposition 2.61, there is a $\tilde{s} \in \tilde{R} \setminus \{0\}$ such that:

$$(*) \qquad \begin{cases} \text{For all } \tilde{\mathfrak{p}} \in \operatorname{Spec} \tilde{R} \text{ with } \tilde{s} \notin \mathfrak{p} \text{ there is a} \\ \tilde{\mathfrak{q}} \in \operatorname{Spec} \tilde{R}' \text{ such that } \tilde{\mathfrak{q}} \cap \tilde{R} = \tilde{\mathfrak{p}} \text{ and} \\ \text{the extension } \operatorname{Quot}\left(\tilde{R}/\tilde{\mathfrak{p}}\right) \hookrightarrow \operatorname{Quot}\left(\tilde{R}'/\tilde{\mathfrak{q}}\right) \text{ is finite} \end{cases}$$

Let $s \in R$ be a preimage of $\tilde{s}$ under $R \twoheadrightarrow \tilde{R}$, so $s \notin \mathfrak{q} \cap R$. Since R is jacobson, there is a maximal ideal $\mathfrak{m} \in \operatorname{MaxSpec} R$ such that

$$\mathfrak{q} \cap R \subseteq \mathfrak{m} \text{ and } s \notin \mathfrak{m}.$$

Hence $\tilde{s}$ is not contained in the maximal ideal $\mathfrak{m}\tilde{R} \in \operatorname{MaxSpec} \tilde{R}$. By applying $(*)$ to $\tilde{\mathfrak{m}} \coloneqq \mathfrak{m}\tilde{R}$ we get a prime ideal $\tilde{\mathfrak{n}} \in \operatorname{Spec} \tilde{R}'$ such that $\tilde{\mathfrak{n}} \cap \tilde{R} = \tilde{\mathfrak{m}}$.

Consider now the finite field extension $\operatorname{Quot} \tilde{R} \hookrightarrow \operatorname{Quot} \tilde{R}'$. We now have $\operatorname{Quot} \tilde{R}/\tilde{\mathfrak{m}} = \tilde{R}/\mathfrak{m}$ as $\tilde{\mathfrak{m}}$ is maximal. We also have $\tilde{R}/\tilde{\mathfrak{m}} = R/\mathfrak{m}$ and $\tilde{R}'/\tilde{\mathfrak{n}} = R'/\mathfrak{n}$ (where $\mathfrak{n} \coloneqq \tilde{\mathfrak{n}} \cap R'$). So now we arrive at the following commutative diagram:

$$\begin{array}{ccc} R & \xhookrightarrow{\text{finite}} & R' \\ \downarrow & & \downarrow \\ R/\mathfrak{m} & \hookrightarrow & R'/\mathfrak{n} \\ \| & & \downarrow \\ \operatorname{Quot} \tilde{R}/\tilde{\mathfrak{m}} & \xhookrightarrow{\text{finite}} & \operatorname{Quot} \tilde{R}'/\tilde{\mathfrak{n}} \end{array}$$

So $R/\mathfrak{m} \hookrightarrow R'/\mathfrak{n}$ is integral, and hence $\mathfrak{n}$ is a maximal ideal (Lemma 2.44).

Since $\mathfrak{n}$ is the preimage of a prime ideal in quotient $R'/\mathfrak{q}$, it folows that $\mathfrak{q} \subseteq \mathfrak{n}$.

By the description of prime ideals in the localization (Theorem 1.46) we get a bijection:

$$\begin{array}{ccc} \operatorname{Spec}\left(R'/\mathfrak{q}\right)\left[b^{-1}\right] & \xrightarrow{\sim} & \left\{\mathfrak{q}' \in \operatorname{Spec} R' \;\middle|\; \mathfrak{q} \subseteq \mathfrak{q}',\ b \notin \mathfrak{q}'\right\} \\ \tilde{\mathfrak{q}} & \longmapsto & \tilde{\mathfrak{q}} \cap R' \end{array}$$

So $b \notin \mathfrak{n}$, which concludes the proof.

ii) Let $\mathfrak{q} \in \operatorname{MaxSpec} R'$ be a maximal ideal. By applying the construction for $b = 1$, we get a maximal ideal $\mathfrak{m} \in \operatorname{MaxSpec} R$ with $\mathfrak{q} \cap R \subseteq \mathfrak{m}$ and a maximal ideal $\mathfrak{n} \in \operatorname{MaxSpec} R'$ with $\mathfrak{n} \cap R = \mathfrak{m}$ and $\mathfrak{q} \subseteq \mathfrak{n}$. Since $\mathfrak{q}$ is a maximal ideal, $\mathfrak{q} = \mathfrak{n}$ follows. So $\mathfrak{n} \cap R = \mathfrak{q} \cap R = \mathfrak{m}$, which is maximal.

We also have that $\operatorname{Quot} \tilde{R}/\tilde{m} \hookrightarrow \operatorname{Quot} \tilde{R}'/\tilde{\mathfrak{n}}$ is finite. Since $\operatorname{Quot} \tilde{R}/\tilde{\mathfrak{m}} = R/\tilde{\mathfrak{m}}$ and $\operatorname{Quot} \tilde{B}/\tilde{\mathfrak{n}} = B/\mathfrak{q}$, the claim follows.

□

End of Lecture 10

Corollary 3.6. Let k be a field and A a k-algebra of finite type. Then

i) A is a Jacobson ring.
ii) For all maximal ideals $\mathfrak{m} \in \operatorname{MaxSpec} A$ the map $k \to A \to A/\mathfrak{m}$ is a finite field extension.
iii) The maximal ideals of A are given by
$$\operatorname{MaxSpec} A = \{\mathfrak{p} \in \operatorname{Spec} A \mid k \to \operatorname{Quot} A/\mathfrak{p} \text{ is finite}\}.$$
iv) Let $f : A \to B$ be a homomorphism of k-algebras of finite type and $\mathfrak{m} \in \operatorname{MaxSpec} B$ a maximal ideal. Then $\mathfrak{m} \cap A$ is maximal too.

Proof.

i) This is just i) of GHNS (Theorem 3.5).
ii) By ii) of GHNS, $\mathfrak{m} \cap k$ is a maximal ideal in k. But since k is a field, this implies that $\mathfrak{m} \cap k = \langle 0 \rangle$. So by the second part of ii), $k \hookrightarrow A/\mathfrak{m}$ is a finite field extension.
iii) The inclusion „$\subseteq$“ is just ii). For the other direction let $\mathfrak{p} \subseteq A$ be a prime ideal and assume that in
$$k \hookrightarrow A/\mathfrak{p} \hookrightarrow \operatorname{Quot} A/\mathfrak{p}$$
the composition $k \hookrightarrow \operatorname{Quot} A/\mathfrak{p}$ is a finite field extension. Then $A/\mathfrak{p} \hookrightarrow \operatorname{Quot} A/\mathfrak{p}$ is necessarily finite, and so in particular integral. Now by Lemma 2.44, this implies that $A/\mathfrak{p}$ is a field, and hence $\mathfrak{p}$ is a maximal ideal.
iv) Since B is of finite type, it is in particular an A-algebra of finite type. By applying ii) of GHNS to $A \to B$, the claim follows.

□

Corollary 3.7. Denote by k-$\mathbf{Alg}^{\text{f.t.}}$ the category whose objects are k-algebras of finite type and whose morphisms are k-algebra homomorphisms maps. Then $\operatorname{MaxSpec}(-)$ induces a contravariant functor
$$\begin{aligned} \operatorname{MaxSpec}(-) : k\text{-}\mathbf{Alg}^{\text{f.t.}} &\longrightarrow \mathbf{Top} \\ A &\longmapsto \operatorname{MaxSpec} A \end{aligned}$$
which maps k-algebra homomorphisms $\varphi : A \to B$ to the restriction of $\varphi^{\#}$ to $\operatorname{MaxSpec} B$.

Proof. We only show that the restriction of $\varphi^{\#}$ is well-defined, i.e. that we indeed get a map $\varphi^{\#} : \operatorname{MaxSpec} B \to \operatorname{MaxSpec} A$. But this is just iv) of Corollary 3.6. □

Theorem 3.8 (Weak Nullstellensatz)**.** *Let k be an algebraically closed field. For a tupel $x = (x_1, \dots, x_n) \in k^n$, denote by $\mathfrak{m}_x$ the ideal*
$$\mathfrak{m}_x := \langle t_1 - x_1, t_2 - x_2, \dots, t_n - x_n \rangle \subseteq k[t_1, \dots, t_n].$$
Then $\mathfrak{m}_x$ is a maximal ideal and the assignment
$$\begin{aligned} k^n &\longrightarrow \operatorname{MaxSpec} k[t_1, \dots, t_n] \\ x &\longmapsto \mathfrak{m}_x \end{aligned}$$

is a bijection.

PROOF. As $k[t_1, \ldots, t_n]/\mathfrak{m}_x \cong k$ we find that $\mathfrak{m}_x$ is indeed a maximal ideal. We also have $\mathfrak{m}_x \neq \mathfrak{m}_y$ for $x, y \in k^n$ with $x \neq y$.

It remains to show the surjectivity: Let $\mathfrak{m} \in \operatorname{MaxSpec} k[t_1, \ldots, t_n]$ be a maximal ideal. Then by Corollary 3.6, we have that $k \hookrightarrow A/\mathfrak{m}$ is a finite field extension. As k is algebraically closed, there are no non-trivial algebraic field extensions of k, so in particular there are no finite extensions. So we have $k \cong a/\mathfrak{m}$.

Denote by π the map $\pi : A \twoheadrightarrow A/\mathfrak{m} \xrightarrow{\sim} k$ and set $x_i \coloneqq \pi(t_i)$. Then $t_i - x_i \in \ker \pi$, and so $\mathfrak{m}_x = \langle t_1 - x_1, \ldots, t_n - x_n \rangle \subseteq \ker \pi = \mathfrak{m}$. But as $\mathfrak{m}_x$ is maximal and $\mathfrak{m} \neq A$, it follows that $\mathfrak{m}_x = \mathfrak{m}$. □

Remark* 3.B. That a field satiesfies the Weak Nullstellensatz is equivalent to k being algebraically closed, since it implies that every irreducible polynomial in $k[t]$ is of the form $t - a$ for a $a \in k$.

3.3. The Dimension of a Ring

Definition 3.9. Let R be a ring.

i) The *dimension of* R is defined as

$$\dim R \coloneqq \sup \left\{ l \in \mathbf{N} \;\middle|\; \begin{array}{l} \text{there is an ascending chain of prime ideals} \\ \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_l \end{array} \right\}$$

if it exists and $\dim R \coloneqq \infty$ otherwise.

ii) Let $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal. Then the *height* is defined as

$$\operatorname{ht} \mathfrak{p} \coloneqq \sup \left\{ l \in \mathbf{N} \;\middle|\; \begin{array}{l} \text{there is an ascending chain of prime ideals} \\ \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_l \subseteq \mathfrak{p} \end{array} \right\}$$

if it exists and $\operatorname{ht} \mathfrak{p} \coloneqq \infty$ otherwise.

Example 3.10.

i) Let k be a field. Then $\dim k = 0$, as every prime ideal is maximal.

ii) Let R be a prinicipal ideal domain which is not a field. Then every ascending chain of prime ideals in R is of the form $\langle 0 \rangle \subsetneq \langle p \rangle$, for a prime element $p \in R$. So $\dim R = 1$.

iii) Consider the polynomial ring in n variables over a field k. Then

$$0 \subsetneq \langle t_1 \rangle \subsetneq \langle t_1, t_2 \rangle \subsetneq \ldots \subsetneq \langle t_1, \ldots, t_n \rangle$$

is stricly ascending, so $\dim k[t_1, \ldots, t_n] \geq n$.

Lemma 3.11. Let $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal.

i) It holds that $\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}}$.

ii) It holds that $\dim R \geq \dim R/\mathfrak{p} + \operatorname{ht} \mathfrak{p}$.

iii) The dimension of R is local in the following sense:

$$\begin{aligned} \dim R &= \sup \{ \dim R_{\mathfrak{m}} \mid \mathfrak{m} \in \operatorname{MaxSpec} R \} \\ &= \sup \{ \operatorname{ht} \mathfrak{m} \mid \mathfrak{m} \in \operatorname{MaxSpec} R \} . \end{aligned}$$

PROOF.

i) By the classification of prime ideals in $R_\mathfrak{p}$ (Corollary 1.47), there is a order-preserving bijection

$$\operatorname{Spec} R_\mathfrak{p} \xleftrightarrow{\sim} \{\mathfrak{p}' \in \operatorname{Spec} R \mid \mathfrak{p}' \subseteq \mathfrak{p}\}.$$

Now the statement is now just the definition of height and dimension.

ii) This follows from the classification of prime ideals of $R/\mathfrak{p}$ (Remark* 1.G) and the definition of height and dimension.

iii) After localising at a maximal ideal, the image of an ascending chain is still an ascending chain. Vice versa, every ascending chain in the localization at a maximal ideal can be lifted to an ascending chain in R. This shows the first equality. The second equality follows from i).

□

Definition* 3.C. Let $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ be an ascending chain in R. We say that this chain is *maximal* if there is no prime ideal $\mathfrak{p} \in \operatorname{Spec} R$ with $\mathfrak{p} \subsetneq \mathfrak{p}_0$ or $\mathfrak{p}_i \subsetneq \mathfrak{p} \subsetneq \mathfrak{p}_{i+1}$ (for $0 \leq i \leq n-1$) or $\mathfrak{p}_n \subsetneq \mathfrak{p}$.

Lemma 3.12. Let R be a ring with $\dim R < \infty$. Assume all maximal chains in R have the same length. Let $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal.

i) All maximal chains in $R/\mathfrak{p}$ have the same length.

ii) It holds that $\dim R = \dim R/\mathfrak{p} + \operatorname{ht} \mathfrak{p}$.

iii) It holds that $\dim R_\mathfrak{p} = \dim R$ if $\mathfrak{p}$ is a maximal ideal.

PROOF. Let $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_r$ be a maximal chain in $R/\mathfrak{p}$. We can lift this to a chain in R and complete it to a maximal chain of the form

$$\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_m = \mathfrak{p} = \mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_r.$$

Now $\operatorname{ht} \mathfrak{p} \geq m$ and $\dim R/\mathfrak{p} \geq r$. By the assumption that every maximal chain in R has the same length, it follows that $m+r = \dim R$. By Lemma 3.11 ii), we have

$$\dim R \geq \dim R/\mathfrak{p} + \operatorname{ht} p = m + r = \dim R.$$

So $\operatorname{ht} \mathfrak{p} = m$ and $\dim R/\mathfrak{p} = r$ follows. This shows ii). For i), note that the completion of the lift of the ideal chain in R is independend from r, so r has to be necessarily the same for all prime chains in $R/\mathfrak{p}$. Claim iii) now follows from ii), since for a maximal ideal, we have $\dim R/\mathfrak{p} = 0$. □

Proposition 3.13. Let $\varphi : R \hookrightarrow R'$ be an integral ring extension.

i) It holds that $\dim R = \dim R'$.

ii) For all $\mathfrak{q} \in \operatorname{Spec} R'$ it holds that $\dim R_{\mathfrak{q} \cap R} \geq \dim R'_\mathfrak{q}$.

iii) If φ satisfies going down then $\dim R_{\mathfrak{q} \cap R} = \dim R'_\mathfrak{q}$.

PROOF.

i) Let $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_l$ be an ascending chain in R'. Then $\mathfrak{q}_0 \cap R \subsetneq \ldots \subsetneq \mathfrak{q}_l \cap R$ is an ascending chain in R (That the inclusions are strict follows from Lemma 2.47). This shows $\dim R \geq \dim R'$.

Let $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_d$ be an ascending chain in R. Then by Lying Over (Lemma 2.48) there is a prime ideal $\mathfrak{q}_0 \in \operatorname{Spec} R'$ with $\mathfrak{q}_0 \cap R = \mathfrak{p}$. Now by Theorem 2.51 there is a chain $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_d$ in R' such that the following diagram is commutative:

$$\begin{array}{ccccccc} \mathfrak{q}_0 & \subsetneq & \mathfrak{q}_1 & \subsetneq & \cdots & \subsetneq & \mathfrak{q}_d \\ | & & | & & & & | \\ \mathfrak{p}_0 & \subsetneq & \mathfrak{p}_1 & \subsetneq & \cdots & \subsetneq & \mathfrak{p}_d \end{array}$$

That the inclusions are strict follows from Lemma 2.47.

ii) Let $\mathfrak{q}_0 \subsetneq \ldots \mathfrak{q}_l = \mathfrak{q}$ be a chain in R'. This gives a chain of the form $\mathfrak{q}_0 \cap R \subsetneq \ldots \subsetneq \mathfrak{q}_l \cap R$ in R. By applying Lemma 3.11 twice, the claim follows.

iii) Let $\mathfrak{p}_0 \subsetneq \ldots \mathfrak{p}_l = \mathfrak{q} \cap R$ be a chain in R. By applying going up, we can lift this to a chain of the form

$$\begin{array}{ccccccc} \mathfrak{q}_0 & \supsetneq & \mathfrak{q}_{l-1} & \supsetneq & \cdots & \supsetneq & \mathfrak{q}_0 \\ | & & | & & & & | \\ \mathfrak{q} \cap R & \supsetneq & \mathfrak{p}_{l-1} & \supsetneq & \cdots & \supsetneq & \mathfrak{p}_0 \end{array}$$

So $\dim R'_{\mathfrak{q}} \geq \dim R_{\mathfrak{q} \cap R}$. The claim now follows from ii).

□

Lemma* 3.D (Going Between)**.** Let k be a field and R a k-algebra of finite type. Let $R \hookrightarrow R'$ be an integral ring extension. Let $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \mathfrak{p}_3$ be prime ideals in k and $\mathfrak{q}_1 \subsetneq \mathfrak{q}_3$ prime ideals in R'. Assume that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$ and $\mathfrak{q}_3 \cap R = \mathfrak{p}_3$. Then there is a prime ideal $\mathfrak{q}_2 \in \operatorname{Spec} R'$ satisfying $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \mathfrak{q}_3$.

Proof. This is on the sixth exercise sheet. □

Remark* 3.E. Note that in the setting of going between, it does not necessarily hold that $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$. A counterexample can also be found in the solutions to sheet 6.

Theorem 3.14. *Let k be a field.*

i) *It holds that $\dim k[t_1, \ldots, t_n] = n$.*

ii) *All maximal chains in $k[t_1, \ldots, t_n] = n$ have the same length.*

Proof. We will do this by induction on n. In the case $n = 1$, $k[t]$ is an integral domain, and hence has dimension 1. In particular, maximal chains have necessarily the same length.

In the general case, consider a chain of prime ideals $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_m$ in $k[t_1, \ldots, t_n]$. Without loss of generality, we can assume that this chain is maximal. This implies that $\mathfrak{p} = \langle 0 \rangle$ (since $k[t_1, \ldots, t_n]$ is an integral domain), $\mathfrak{p}_m$ is a maximal ideal and $\mathfrak{p}_1 = \langle f \rangle$, where f is an irreducible polynomial (since $k[t_1, \ldots, t_n]$ is factorial). Using Lemma 2.60, we can assume that f is a monic polynomial in t_n, with non-leading coefficients in $k[t_1, \ldots, t_{n-1}]$.

So we get an integral extension $k[t_1,\dots,t_{n-1}] \hookrightarrow k[t_1,\dots,t_n]/\langle f\rangle$. Consider now the images of the original chain under the following maps:

$$\begin{aligned} \pi^{\#} : \operatorname{Spec} k[t_1,\dots,t_n] &\longrightarrow \operatorname{Spec} k[t_1,\dots,t_n]/\mathfrak{p}_1 \\ \mathfrak{p}_i &\longmapsto \mathfrak{p}_i/\mathfrak{p}_1 \\ \varphi^{\#} : \operatorname{Spec} k[t_1,\dots,t_n]/\mathfrak{p}_1 &\longrightarrow \operatorname{Spec} \varphi^k[t_1,\dots,t_{n-1}] \\ \mathfrak{q} &\longmapsto \mathfrak{q} \cap k[t_1,\dots,t_{n-1}], \end{aligned}$$

for all prime ideals $\mathfrak{p}_i$ in the chain we started with. Then both maps preserve prime ideals (the image of a prime ideal under $\pi^{\#}$ is again prime, since π maps into a quotient), strict inclusions of prime ideals ($\varphi^{\#}$ by Lemma 2.47). Furthermore, maximal chains are mapped to maximal chains:

In the chain

$$0 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \cap k[t_1,\dots,t_{n-1}] \subsetneq \dots \subsetneq \mathfrak{p}_m/\mathfrak{p}_1 \cap k[t_1,\dots,t_{n-1}]$$

the ideal $\mathfrak{p}_2/\mathfrak{p}_1 \cap k[t_1,\dots,t_{n-1}]$ is again maximal, by Corollary 3.6 iii). Now by Going Between (Lemma* 3.D), the chain is indeed maximal. But by the induction hypothesis, the length of a maximal chain in $k[t_1,\dots,t_{n-1}]$ is exactly $n-1$, for all maximal chains. Using the prime ideal correspondence for the quotient, the claim follows. □

Let k be a field and A a k-algebra of finite type. Then by the Noether Normalization Lemma (Theorem 2.59), there are algebraically independet elements $e_1,\dots,e_n$ such that A is integral over $k[e_1,\dots,e_n]$.

Corollary 3.15. In this case, $n = \dim A$ holds.

Proof. By Proposition 3.13, we have $\dim A = \dim k[e_1,\dots,e_n]$ and $\dim k[e_1,\dots,e_n] = n$ by Theorem 3.14. □

Corollary 3.16. Let A be a k-algebra of finite type and assume that A is an integral domain. Then all maximal chains in A have the same length.

Proof. Let $\varphi : k[t_1,\dots,t_n] \twoheadrightarrow A$, then $A \cong k[t_1,\dots,t_n]/\ker\varphi$. Since A is an integral domain it follows that $\ker\varphi$ is a prime ideal. Since by Theorem 3.14 all chains in $k[t_1,\dots,t_n]$ have the same length and $\ker\varphi$ is prime, the same is true for $k[t_1,\dots,t_n]/\ker\varphi$ (by Lemma 3.12). □

Corollary* 3.F. Let A be a k-algebra of finite type and integral domain. Then for every maximal ideal $\mathfrak{m} \in \operatorname{MaxSpec} A$, we have $\dim A_{\mathfrak{m}} = \dim A$.

Proof. This now follows from the more general result Lemma 3.12. □

End of Lecture 11

3.4. Zero Sets and Varieties

Definition 3.17.

i) Let k be a field and $n \geq 1$ an integer. We denote by $\mathbb{A}^n_k := k^n$ the *affine space*.

ii) Let $S \subseteq k[t_1,\dots,t_n]$ be a subset. We denote by

$$V(S) := \{a \in \mathbb{A}^n_k \mid f(a) = 0 \text{ for all } f \in S\},$$

the *vanishing set of* S. Here, $f(a) = f((a_1, \ldots, a_n))$ is a short-hand notation for the image of f under the evaluation morphism $X_i \mapsto a_i$.

iii) Subsets of $\mathbb{A}_k^n$, which are of the form $V(T)$ for a subset $T \subseteq k[t_1, \ldots, t_n]$, are called *varieties* or *algebraic subsets*.

Example 3.18. These are some examples of varieties:

i) $V(x^2 + y^2 - 1) = \left\{(a, b) \in k^2 \;\middle|\; a^2 + b^2 = 1\right\}$.
ii) $V(x \cdot y) = \left\{(a, b) \in k^2 \;\middle|\; a = 0 \text{ or } b = 0\right\}$.
iii) $V(\{x - a, y - b\}) = \{(a, b)\}$.

Lemma 3.19.

i) Let $S_1 \subseteq S_2 \subseteq k[t_1, \ldots, t_n]$. Then $V(S_1) \supseteq V(S_2)$.
ii) Let $S \subseteq k[t_1, \ldots, t_n]$. Then $V(S) = V(\langle S \rangle)$.

Proof. Ommited. □

Example 3.20. We want to describe the varieties in $\mathbb{A}_k^1$ for k algebraically closed. Let $I \subseteq k[t]$ be an ideal. Since $k[t]$ is a prinicipal ideal domain, there is a $f \in k[t]$ such that $I = \langle f \rangle$. Then, using Lemma 3.19 we get

$$\begin{aligned} V(I) &= V(\{f\}) \\ &= \{x \in k \mid f(x) = 0\} \\ &= \{x \in k \mid (t - a_1) \cdot \ldots \cdot (t - a_n) = 0\} \\ &= \{a_1, \ldots, a_n\}. \end{aligned}$$

Note that it was crucial that k is algebraically closed, since otherwise we would have not obtained a factorisation of f.

Definition 3.21.

i) Let $X \subseteq \mathbb{A}_k^n$ be a subset. Define

$$\mathrm{I}(X) \coloneqq \{f \in k[t_1, \ldots, t_n] \mid f(x) = 0 \text{ for all } x \in X\}.$$

ii) Let $X \subseteq \mathbb{A}_k^n$ be a subset. Define $A(X) \coloneqq k[t_1, \ldots, t_n]/\mathrm{I}(X)$ as the *ring of polynomial functions on* X or the *coordinate ring at* X.

Note that $A(X)$ is a finitely-generated k-algebra.

Proof. $\mathrm{I}(X)$ is indeed an ideal, so this is well-defined. □

Remark⋆ 3.G. Note that $A(\mathbb{A}_k^n) = k[t_1, \ldots, t_n]$.

Example 3.22. Let $a \coloneqq (a_1, \ldots, a_n) \in \mathbb{A}_k^n$. Then

$$\mathrm{I}(a) = m_a = (t_1 - a_1, \ldots, t_n - a_n).$$

Definition 3.23. Let $Y \subseteq X \subseteq \mathbb{A}_k^n$ and $S \subseteq A(X)$.

i) The set $V_X(S) \coloneqq \{x \in X \mid f(x) = 0 \text{ for all } f \in S\}$ is a *subvariety of* X.
ii) We define $\mathrm{I}_X(Y) \coloneqq \{f \in A(X) \mid f(y) = 0 \text{ for all } y \in Y\}$.

Lemma 3.24. Let $X \subseteq \mathbb{A}_k^n$ be a variety, $Y, Y' \subseteq X$ and $S, S' \subseteq A(X)$.

i) If $Y \subseteq Y'$, then $\mathrm{I}_X(Y) \supseteq \mathrm{I}_X(Y')$. If $S \subset S'$, then $V_X(S) \supseteq V_X(S')$.
ii) It holds that $Y \subseteq V_X(\mathrm{I}_X(Y))$ and $S \subseteq \mathrm{I}_X(V_X(S))$.
iii) If Y is a subvariety of X, then $Y = V_X(\mathrm{I}_X(Y))$.
iv) If Y is a subvariety of X, then $A(X)/\mathrm{I}_X(Y) = A(Y)$.
v) It holds that $\mathrm{I}_X(Y_1 \cup Y_2) = \mathrm{I}_X(Y_1) \cap \mathrm{I}(Y_2)$.

PROOF. i), ii) and v) are clear from the definition. For iii), note that we only need to show $V_X(\mathrm{I}_X(Y)) \subseteq Y$, since the other inclusion follows from ii). But since Y is a subvariety of X, there is a $S \subseteq A(X)$ such that $Y = V_X(S)$. Then, using i) and ii), we get

$$S \overset{\text{ii)}}{\subseteq} \mathrm{I}_X(V_X(S)) = I(Y) \overset{\text{i)}}{\Longrightarrow} V_X(\mathrm{I}_X(Y)) \subseteq V_X(S) = Y.$$

For iv), note that the restricion map

$$\begin{array}{ccc} A(X) & \longrightarrow & A(Y) \\ f & \longmapsto & f|_Y \end{array}$$

is well-defined and surjective, with kernel $\mathrm{I}_X(Y)$. □

Notation 3.25. In the following, if the subset X is clear, we will ommit it in the notation for I and V.

Remark 3.26. In light of Lemma 3.24 it seems reasonable to ask if $\mathrm{I}(V(J)) \subseteq J$ holds for a general ideal. But in general, this is far from being true:

i) For the ideal
$$J \coloneqq \langle (t-a_1)^{k_1} \cdot \ldots \cdot (t-a_n)^{k_n} \rangle \subseteq \mathbf{C}[t]$$
with $k_i \geq 0$ and $a_i \in \mathbf{C}$, we have $V(J) = \{a_1, \ldots, a_n\}$. So $\mathrm{I}(V(J))$ consists of all polynomials which have each of the factors $t - a_i$ at least once. So if one of the k_i is greater than 1 J is a proper subset of $\mathrm{I}(V(J))$.
ii) Consider
$$J \coloneqq \langle t^2 + 1 \rangle \subseteq \mathbf{R}[t].$$
Then $\mathrm{I}(J) = \emptyset$, so $\mathrm{I}(V(J)) = \mathrm{I}(\emptyset) = \mathbf{R}[t]$.

End of Lecture 12

Lemma 3.27. Let $Y \subseteq \mathbb{A}^n_k$ be a subset. Then $V(\mathrm{I}(Y)) = \overline{Y}$.

PROOF. now that $Y \subseteq V(\mathrm{I}(Y))$, by Lemma 3.24. Since $V(\mathrm{I}(Y))$ is closed, we get $\overline{Y} \subseteq V(\mathrm{I}(Y))$.

On the other hand, $\overline{Y}$ is closed. So by definition, there is an ideal $J \subseteq k[t_1, \ldots, t_n]$ such that $\overline{Y} = V(J)$. Since $J \subseteq \mathrm{I}(Y)$, we have

$$\overline{Y} = V(J) \subseteq V(\mathrm{I}(Y)).$$

□

We now prove yet another Hilbert's Nullstellensatz:

Theorem 3.28 (Hilbert's Nullstellensatz)**.** *Let $J \subseteq k[t_1, \dots, t_n]$ be an ideal. Then $\mathrm{I}(V(J)) = \sqrt{J}$ holds.*

PROOF. We have

$$\begin{aligned} V(J) &= \{a \in \mathbb{A}_k^n \mid f(a) = 0 \text{ for all } f \in J\} \\ &= \{a \in \mathbb{A}_k^n \mid J \subseteq \mathfrak{m}_a \coloneqq \ker(\mathrm{ev}_a : k[t_1, \dots, t_n] \to k)\} \end{aligned}$$

and

$$\mathrm{I}(V(J)) = \{f \in k[t_1, \dots, t_n] \mid f(a) = 0 \text{ for all } a \in V(J)\}.$$

Hence $f \in \mathrm{I}(V(J))$ if and only if for all $a \in \mathbb{A}_k^n$ with $J \subseteq \mathfrak{m}_a$ it holds that $J \in \mathfrak{m}_a$, so

$$\mathrm{I}(V(J)) = \bigcap_{\substack{a \in \mathbb{A}_k^n \\ J \subseteq \mathfrak{m}_a}} \mathfrak{m}_a.$$

By the Weak Nullstellensatz (Theorem 3.8) we have

$$\operatorname{MaxSpec} k[t_1, \dots, t_n] = \{\mathfrak{m}_a \mid a \in \mathbb{A}_k^n\},$$

and hence

$$\begin{aligned} \mathrm{I}(V(J)) &= \bigcap_{\substack{\mathfrak{m} \in \operatorname{MaxSpec} k[t_1, \dots, t_n] \\ J \subseteq \mathfrak{m}}} \mathfrak{m} \\ &= \sqrt{J}, \end{aligned}$$

as $k[t_1, \dots, t_n]$ is a Jacobson ring (Corollary 3.6, and then Lemma 3.2). □

3.5. The Zariski-Topology on $\mathbb{A}_k^n$

Convention. In the following, k always denote an algebraically closed field.

Lemma 3.29. Let I, J be ideals in $k[t_1, \dots, t_n]$ and $\{I_l\}_{l \in L}$ a family of ideals in $k[t_1, \dots, t_n]$.

i) It holds that $V\left(\sum_l I_l\right) = \bigcap_l V(I_l)$.
ii) It holds that $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.

PROOF.

i) We have $V\left(\sum_l I_l\right) \subseteq V(I_l)$ for all $l \in L$, by Lemma 3.19. So $V\left(\sum_l I_l\right) \subseteq \bigcap_l V(I_l)$.
   Let now $x \in \bigcap_l V(I_l)$. Then for any polynomial $f \in \sum_l I_l$, $f(x) = 0$, so $x \in V\left(\sum_l I_l\right)$.
ii) We have $V(J) \supseteq V(I \cap J) \supseteq V(I) \cup V(J)$. Let $x \in V(IJ)$, with $x \notin V(I)$. Then there is a $f \in I$ such that $f(x) \neq 0$. Now for any $g \in J$, we have $fg \in IJ$ and hence $(fg)(x) = 0$. So $g(x) = 0$ and thus $x \in V(J)$.

□

Proposition 3.30. By the above lemma, the subsets of the form $V(I) \subseteq \mathbb{A}_k^n$ satisfy the axioms of closed sets of a topology on $\mathbb{A}_k^n$. This topology is the *Zariski-Topology on* $\mathbb{A}_k^n$

Remark 3.31. The Zariski-Topology on $\mathbb{A}_k^n$ is quite weird:

i) Let $X := \left\{x \in \mathbb{A}^1_{\mathbf{C}} \;\middle|\; |x| \leq 1\right\}$ be the unit disk in $\mathbf{C}$. As closed subsets of $\mathbb{A}^1_{\mathbf{C}}$ are finite sets (Example 3.20), we get $\overline{X} = \mathbb{A}^1_{\mathbf{C}}$.

ii) Let $\varphi : \mathbb{A}^1_{\mathbf{C}} \to \mathbb{A}^1_{\mathbf{C}}$ be bijective. Then preimages of finite sets are finite. So φ is already continous.

Lemma* 3.H (Prime Avoidance)**.** Let $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_m \in \operatorname{Spec} R$ be prime ideals and $I, I_1, \ldots, I_n \subseteq R$ ideals.

i) If $I \subseteq \bigcap_{i=1}^m \mathfrak{p}_i$, then there exists an $1 \leq i \leq m$ such that $I \subseteq \mathfrak{p}_i$.

ii) If $\bigcap_{i=1}^n I_i \subseteq \mathfrak{p}$, then there is a $1 \leq i \leq n$ such that $I_i \subseteq \mathfrak{p}$.

iii) If $\bigcap_{i=1}^n I_i = \mathfrak{p}$, then there is a $1 \leq i \leq n$ such that $I_i = \mathfrak{p}$.

iv) Parts ii) also holds if one of the ideals is not prime.

Proof. This is on the seventh exercise sheet. (Part iv) actually not). □

Definition* 3.I. Let $I \subseteq R$ be an ideal. We say I is a r*adical ideal* if $\sqrt{I} = I$ holds.

Definition* 3.J. A topological space X is called *irreducible* if every decomposition $X = X_1 \cup X_2$ in closed subsets X_1, X_2 implies that X_1 or X_2 equals X.

Theorem 3.32.

i) *The maps*

$$\begin{array}{rcl} \{\textit{varieties in } \mathbb{A}_k^n\} & \longleftrightarrow & \{\textit{radical ideals in } k[t_1, \ldots, t_n]\} \\ Y & \longmapsto & \mathrm{I}(Y) \\ V(J) & \longmapsfrom & J \end{array}$$

are mutually inverse bijections.

ii) *The bijection from i) restricts to a bijection*

$$\{\textit{closed, irreducible subsets of } \mathbb{A}_k^n\} \longleftrightarrow \operatorname{Spec} k[t_1, \ldots, t_n].$$

iii) *The bijection from i) restricts to a bijection*

$$\{\{x\} \subseteq \mathbb{A}_k^n\} \longleftrightarrow \operatorname{MaxSpec} k[t_1, \ldots, t_n].$$

Proof.

i) Since k is an integral domain, we have $\sqrt{\mathrm{I}(X)} = \mathrm{I}(X)$ for all $X \subseteq \mathbb{A}_k^n$. If $X \subseteq \mathbb{A}_k^n$ is a variety then by Lemma 3.27, we have $V(\mathrm{I}(X)) = \overline{X}$. Since the closed sets in $\mathbb{A}_k^n$ are precisley the varieties, we get $V(\mathrm{I}(X)) = X$.

Let $J \subseteq k[t_1, \ldots, t_n]$ be a radical ideal. By the Nullstellensatz (Theorem 3.28), we have $\mathrm{I}(V(J)) = \sqrt{J} = J$.

ii) Let $Y \subseteq \mathbb{A}_k^n$ be closed and irreducible. We want to show that $\mathrm{I}(Y)$ is a prime ideal. We do this by contradiction:

Assume there are polynomials $f, g \in k[t_1, \ldots, t_n] \setminus \mathrm{I}(Y)$ such that $fg \in \mathrm{I}(Y)$. Now $V\left(\mathrm{I}(Y) + \langle f \rangle\right), V\left(\mathrm{I}(Y) + \langle g \rangle\right) \subseteq Y$ are proper

subsets of Y, because if $V(\mathrm{I}(Y) + \langle f \rangle) = Y$, then $f(y) = 0$ would hold for every $y \in Y$ which would mean $f \in \mathrm{I}(Y)$.

As Y is irreducible it holds that

$$V(\mathrm{I}(Y) + \langle f \rangle) \cup V(\mathrm{I}(Y) + \langle g \rangle) \subsetneq Y$$

By Lemma 3.24, we have

$$V(\mathrm{I}(Y) + \langle f \rangle) \cup V(\mathrm{I}(Y) + \langle g \rangle) = V((\mathrm{I}(Y) + \langle f \rangle) \cdot (\mathrm{I}(Y) + \langle g \rangle))$$

We also have

$$\begin{aligned}(\mathrm{I}(Y) + \langle f \rangle) \cdot (\mathrm{I}(Y) + \langle g \rangle) &\subseteq \mathrm{I}(Y) + \langle fg \rangle \\ &= \mathrm{I}(Y),\end{aligned}$$

as we assume $fg \in \mathrm{I}(Y)$. Putting all of this together, we get

$$\begin{aligned}Y &= V(\mathrm{I}(Y)) \\ &= V(\mathrm{I}(Y) + \langle fg \rangle) \\ &\subseteq V(\mathrm{I}(Y) + \langle f \rangle) \cap V(\mathrm{I}(Y) + \langle g \rangle) \\ &\subsetneq Y,\end{aligned}$$

which is not possible. This shows that the $\mathrm{I}(Y)$ is indeed a prime ideal.

For the other map, let $\mathfrak{p} \in \operatorname{Spec} k[t_1, \ldots, t_n]$ be a prime ideal and assume there is a decomposition $V(\mathfrak{p}) = V(I_1) \cap V(I_2) = V(I_1 I_2)$ for some ideals $I_1, I_2 \subseteq k[t_1, \ldots, t_n]$. Using part i), we get

$$\mathfrak{p} = \sqrt{\mathfrak{p}} = \sqrt{I_1 I_2} \supseteq I_1 \cap I_2,$$

which implies $I_1 \subseteq \mathfrak{p}$ or $I_2 \subseteq \mathfrak{p}$ (by Prime Avoidance, Lemma* 3.H, ii)). Thus $V(\mathfrak{p}) \subseteq V(I_1)$ or $V(\mathfrak{p}) \subseteq V(I_2)$ and so $V(\mathfrak{p})$ is indeed irreducible.

iii) Let $\mathfrak{m} \in \operatorname{MaxSpec} k[t_1, \ldots, t_n]$ be a maximal ideal. Then by the Weak Nullstellensatz (Theorem 3.8) it is of the form $\mathfrak{m} = \mathfrak{m}_a$ for an $a \in \mathbb{A}^n_k$. We now have $V(\mathfrak{m}_a) = \{a\}$.

For the other direction, let $a \in \mathbb{A}^n_k$ be a point. We then have

$$\mathrm{I}(\{a\}) = \{f \in k[t_1, \ldots, t_n] \mid f(a) = 0\} = \mathfrak{m}_a.$$

□

Corollary 3.33. Let $X \subseteq \mathbb{A}^n_k$ be a variety.

i) The maps

$$\begin{array}{rcl}\{\text{closed subsets of } X\} & \longleftrightarrow & \{\text{radical ideals in } A(X)\} \\ Y & \longmapsto & \mathrm{I}_X(Y) \\ V_X(J) & \longmapsfrom & J\end{array}$$

are mutually inverse bijections.

ii) The bijection from i) restricts to a bijection

$$\{\text{closed, irreducible subsets of } X\} \quad \longleftrightarrow \quad \operatorname{Spec} A(X).$$

iii) The bijection from i) restricts to a bijection

$$\{\{x\} \subseteq X\} \quad \longleftrightarrow \quad \operatorname{MaxSpec} A(X).$$

Definition 3.34. Let X be a topological space. A closed, irreducible subset $C \subseteq X$ is an *irreducible component* if for all closed subsets $Z \subseteq X$ with $C \subseteq Z$ already $C = Z$ follows.

Corollary 3.35. Let $X \subseteq \mathbb{A}_k^n$ be a variety. Then the maps

$$\begin{array}{rcl} \{\text{irreducible components of } X\} & \longleftrightarrow & \{\text{minimal prime ideals in } A(X)\} \\ Y & \longmapsto & \mathrm{I}_X(Y) \\ V_X(J) & \longmapsfrom & J \end{array}$$

are mutually inverse bijections.

End of Lecture 13

3.6. Morphisms of Varieties

Definition 3.36. Let $X \subseteq \mathbb{A}_k^n$ be a variety and $A(X)$ the coordinate ring.

i) We say a function $\varphi : X \to k$ is *regular* if there is a polynomial $f \in k[t_1, \ldots, t_n]$ such that $\varphi(a) = f(a)$ for all $a \in X$. We denote the set of regular functions $X \to k$ is denoted by $\mathcal{O}(X)$.

ii) Let X, X' be varieties, with $X \subseteq \mathbb{A}_k^n$ and $X' \subseteq \mathbb{A}_k^m$. We say a function $(\varphi_1, \ldots, \varphi_m) = \varphi : X \to X'$ is *regular* or *a morphism of affine varieties* if all components are regular. We denote the set of regular functions $X \to X'$ by $\operatorname{Hom}(X, X')$.

Remark* 3.K. The set $\mathcal{O}(X)$ has a natural ring structure, which is given by $(f+g)(x) \coloneqq f(x)+g(x)$ and $(f \cdot g)(x) \coloneqq f(x)g(x)$. That's why it is also called the *ring of regular functions on* X.

Lemma 3.37. The ring $\mathcal{O}(X)$ of regular functions and the coordinate ring $A(X)$ are isomorphic.

Proof. Consider the ring homomorphism

$$\begin{array}{rcl} k[t_1, \ldots, t_n] & \longrightarrow & \mathcal{O}(X) \\ f & \longmapsto & (x \mapsto f(x)) \,. \end{array}$$

Then by definition of $\mathcal{O}(X)$ this map is surjective. The kernel is given precisley by $\mathrm{I}(X)$, so $A(X) = k[t_1, \ldots, t_n]/\mathrm{I}(X) \cong \mathcal{O}(X)$. □

Theorem 3.38. *Let $X \subseteq \mathbb{A}_k^n$, $X' \subseteq \mathbb{A}_k^m$ be varieties. Then there is a bijection*

$$\operatorname{Hom}(X, X') \quad \xrightarrow{\sim} \quad \hom(\mathcal{O}(X'), \mathcal{O}(X)).$$

PROOF. Let $\varphi : X \to X'$ be a morphism of affine varieties, then φ induces a ring homomorphism

$$\begin{array}{rcl} \varphi^* : \mathcal{O}(X') & \longrightarrow & \mathcal{O}(X) \\ \left(X' \xrightarrow{\psi} k\right) & \longmapsto & \left(X \xrightarrow{\varphi} X' \xrightarrow{\psi} k\right). \end{array}$$

We show that the assignment

$$\begin{array}{rcl} (-)^* : \mathrm{Hom}(X, X') & \longrightarrow & \hom(\mathcal{O}(X'), \mathcal{O}(X)) \\ \varphi & \longmapsto & \varphi^* \end{array}$$

is a bijection:

For that, note that φ is uniquely determined by φ^*: Consider the coordinate function

$$\begin{array}{rcl} y_i : X' & \longrightarrow & k \\ (y_1, \ldots, y_m) & \longmapsto & y_i. \end{array}$$

Then $\varphi^*(y_i) = \varphi_i$ for all $1 \leq i \leq m$. So in particular, φ^* is injective.

For the surjectivity of $(-)^*$, let $\beta : \mathcal{O}(X') \to \mathcal{O}(X)$ be a ring homomorphism. Define a map

$$\varphi = (\varphi_1, \ldots, \varphi_m) : X \to \mathbb{A}_k^m$$

by $\varphi_i := \beta(y_i)$. Then $\varphi^* = \beta$. It remains to show that $\operatorname{im}\varphi \subseteq X'$. For that, let $a \in X$. Since X' is a variety, it suffices to show $\varphi(a) \in V(\mathrm{I}(X'))$. Using the isomorphism from Lemma 3.37, we can associate to g an element $\overline{g} \in A(X') \cong \mathcal{O}(X')$, and as $g \in \mathrm{I}(X')$ we have $\overline{g} = 0$. Hence $\varphi^*(\overline{g}) = 0$ and thus $g(\varphi(a)) = 0$ for all $a \in X$. □

3.7. Some examples

This part of the lecture will be added at some point in the future.

CHAPTER 4

Noetherian Rings and Modules

Definition 4.1. Let R be a ring and M be an R-module.

i) We say M is *noetherian* if every ascending chain $M_0 \subseteq M_1 \subseteq \ldots$ of submodules of M terminates after finitely many steps, i.e. there is a $n \in \mathbf{N}$ such that $M_k = M_n$ for all $k \geq n$.

ii) We say M is *artinian* if every descending chain $M_0 \supseteq M_1 \supseteq \ldots$ of submodules of M terminates after finitely many steps, i.e. there is a $n \in \mathbf{N}$ such that $M_k = M_n$ for all $k \geq n$.

iii) We say R is *noetherian/artinian* if it is noetherian/artinian as an R-module.

Example 4.2.

i) Every field is noetherian and artinian.

ii) Let V be a vector space. Then V is noetherian if and only if it is artinian if and only if it is finite dimensional.

iii) The ring of integers $\mathbf{Z}$ is noetherian: For every chain of ideals $I_0 \subseteq I_1 \subseteq \ldots$, the ideal I_1 is generated by a single element $a \in \mathbf{Z}$. Since $\mathbf{Z}/a\mathbf{Z}$ is finite, there are only finitely many ideals lying over I_1.

However, $\mathbf{Z}$ is not artinian: The chain $\mathbf{Z} \supsetneq 2\mathbf{Z} \supsetneq 4\mathbf{Z} \supsetneq \ldots$ is stricly descending but does not terminate.

iv) The polynomial in infinitely many variables over a field $k[t_1, \ldots]$ is neither noetherian nor artinian: The chain $\langle t_1 \rangle \subsetneq \langle t_1, t_2 \rangle \subsetneq \ldots$ is stricly increasing but does not terminate; the chain $\langle t_1 \rangle \supsetneq \langle t_1^2 \rangle \supsetneq \ldots$ is stricly decreasing but does not terminate.

Remark* 4.A. There are noetherian rings with $\dim R = \infty$. An example can be found in [**EE95**, Exercise 9.6].

End of Lecture 14

Lemma 4.3. Let M be an R-module.

i) The following are equivalent:
   a) M is noetherian.
   b) Every non-empty family of submodules of M has an inclusion-maximal element.
   c) Every submodule of M is finitely generated.

ii) M is artinian if and only if every non-empty family of M has an inclusion-minimal element.

PROOF.

i) For a) $\implies$ b), let $(N_i)_i$ be a family of submodules of M. Then (N_i) is partially ordered by inclusion, and since M is noetherian, every chain of elements from (N_i) has an upper bound (namely the subspace that terminates the chain). So by Zorn's Lemma, there is an inclusion-maximal subspace of (N_i).

For b) $\implies$ c), let N be a submodule of M and let (N_i) be the family of finitely-generated submodules of N. Then (N_i) is non-empty, since $\{0\} \subseteq N$ is finitely-generated. So by b), there is an inclusion-maximal subspace $P \in (N_i)$. Assume that P is a proper submodule of N, and let P be generated by the elements $p_1, \ldots, p_k$. Then there is an element $p_{k+1} \in N \setminus P$. But now the subspace $\langle p_1, \ldots, p_{k+1} \rangle$ is a finitely-generated submodule of N that has P as a proper subset. This contradicts the maximality of P.

Finally, for c) $\implies$ a), let $M_0 \subsetneq M_1 \subsetneq \ldots$ be an ascending chain of submodules of M. Consider the subspace $\tilde{M} \coloneqq \cup M_i$. Then by assumption, $\tilde{M}$ is finitely generated. So there is a $i \geq 0$ such that the set of generators is in M_k for all $k \geq i$. So $M_k = M_i$ for all $k \geq i$ follows, and hence the chain terminates.

ii) That M being artinian implies that every non-empty family of subspaces has an inclusion-minimal element can be shown analogous to a) $\implies$ b) in i). For the other direction, note that every descending chain of submodules of M has an inclusion-minimal element which necessarily terminates the chain.

□

Corollary 4.4. Every principal ideal domain is a noetherian ring.

Remark 4.5. Let $I \subseteq R$ be an ideal and M an R-module. Then the quotient M/IM is both an R/I-module and an R-module. Using the definition of a noetherian module, we get that M/IM is noetherian as an R-module if and only if it is noetherian as an R/I-module (since statements about chains of submodules are independent from the ground ring, and R-submodules are precisley R/I-submodules).

Lemma 4.6. Let M be an R-module and

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

be a short-exact sequence of R-modules.

i) M is noetherian if and only if both N and N' are.

ii) M is artinian if and only if both N and N' are.

PROOF. By duality, it suffices to show i). Without loss of generality, we can assume that N is a submodule of M and that $N' = M/N$. Assume first that M is noetherian. Let $N_0 \subseteq N_1 \subseteq N_2 \subseteq \ldots$ be a chain of submodules of M. We can regard this as a chain in N and since M is noetherian, it terminates in M at a module N_n. So the original chain in N terminates in N_n too. Analogously, let $P_0 \subseteq P_1 \subseteq \ldots$ be a chain in M/N and denote by $q : M \twoheadrightarrow M/N$ the canonical projection to the quotient. Set $M_k \coloneqq q^{-1}(P_k)$

for all k. Then $M_0 \subseteq M_1 \subseteq \dots$ is an ascending chain in M, which terminates in a submodule M_n since M is noetherian. Then the original chain terminates in $P_n = q(M_n)$ (the equality holds since q is surjective.)

For the other direction, let $M_0 \subseteq M_1 \subseteq \dots$ be an ascending chain in M. Set $N_k \coloneqq M_k \cap N$ and $P_k \coloneqq (M_k + N)/N$. So we get ascending chains $N_0 \subseteq N_1 \subseteq \dots$ and $P_0 \subseteq P_1 \subseteq \dots$ in N and M/N respectivley. Since N and M/N are noetherian, there is a $n > 0$ such that $P_k = P_n$ and $N_k = N_n$ for all $k \geq n$. Then the original chain in M terminates in n too:

Denote by $i : N \hookrightarrow M$ the inclusion of N into M and let $x \in M_k$ for a $k \geq n$. Then there is a $x' \in M_n$ such that $q(x) = q(x')$ (as the chain terminates in the quotient and q is surjective). So $x - x' \in \ker q = \operatorname{im} i$ and hence there is a $y \in N$ such that $i(y) = x - x'$. This implies $y \in i^{-1}(M_k) = i^{-1}(M_n)$. Hence $x = i(y) + x'$, which implies $x \in M_n$, as $i(y)$ and x' are. □

Corollary 4.7. Let R be a noetherian ring.

i) Let M, N be R-modules. Then $M \oplus N$ is noetherian if and only if M, N are.
ii) Let M be a finitely-generated R-module. Then M is noetherian.

Proof.

i) This follows from the previous lemma, using the short-exact sequence $0 \to M \to M \oplus N \to N \to 0$.
ii) By i), R^n is noetherian for all $n > 0$. Since M is finitely-generated as R-module, it is isomorphic to a quotient of R^n for a $n > 0$. So by the previous lemma, M is noetherian.

□

Theorem 4.8 (Hilbert's Basissatz, HBS)**.** *Let R be a noetherian ring. Then the polynomial ring $R[t]$ is also a noetherian ring.*

Proof. We will do this by contradiction - assume $R[t]$ is not noetherian. So by Lemma 4.3 there is an ideal $I \subseteq R[t]$ which is not finitely generated. We can now inductivley choose elements $f_0, f_1, \dots \in I$ which have the following properties: The polynomial $f_0 \in I$ has minimal degree among all polynomials in I. We then choose f_{n+1} as a polynomial of minimal degree in $I \setminus \langle f_0, \dots, f_n \rangle$ for all $n > 0$.

In this way, we get an infinite sequence

$$f_0, f_1, \dots \in I \text{ such that } f_{n+1} \notin \langle f_0, \dots, f_n \rangle.$$

Set $d_n \coloneqq \deg f_n$. Then, by construction, we have $d_{n+1} \geq d_n$. Let now a_k be the leading coefficient of $f_k = a_k X^{d_k} + (\text{lower order terms in } X)$. This yields the ascending chain $\langle a_0 \rangle \subseteq \langle a_0, a_1 \rangle \subseteq \dots$ in R. Now since R is noetherian, this terminates for a n and hence the leading coefficient of f_{n+1}, i.e. a_{n+1}, is of the form

$$a_{n+1} = c_0 a_0 + \dots + c_n a_n,$$

for some $c_0, \dots, c_n \in R$.

Consider now the polynomial

$$f'_{n+1} \coloneqq f_{n+1} - \sum_{k=0}^{n} c_k t^{d_{n+1}-d_k} f_k.$$

Then the coefficient of $t^{d_{n+1}}$ is

$$a_{n+1} - \sum_{k=0}^{n} c_k a_k = 0,$$

by the above observation. So f'_{n+1} is a polynomial with $\deg f'_{n+1} < \deg f_{n+1}$ and $f'_{n+1} \notin \langle f_0, \dots, f_n \rangle$ (as otherwise $f_n = f'_{n+1} + \sum_{k=0}^{n} c_k t^{d_{n+1}-d_k} f_k$ would also be in $\langle f_0, \dots, f_n \rangle$). But this is a contradiction to the minimality of f_{n+1}. □

Corollary 4.9. Let R be a noetherian ring and A an R-algebra of finite type. Then A is a noetherian ring.

Proof. This is on exercise sheet 8. □

Remark 4.10.

i) Let $X \subseteq \mathbb{A}^n_k$ be a variety. Then $A(X)$ is noetherian and hence every ideal $I \subseteq A(X)$ is finitely generated. So every subvariety of X is already determined by finitely many polynomial equations.

ii) By the ascending chain condition for $A(X)$, we get that every chain of subvarities $X_0 \supseteq X_1 \supseteq \dots$ terminates.

iii) Assume X has infinitely many points $a_1, a_2, \dots \in X \subseteq \mathbb{A}^n_k$. This gives an ascending chain of closed subsets, by setting $X_n \coloneqq \bigcup_{k \leq n} \{a_k\}$. Then this chain corresponds to a descending chain of ideals in $A(X)$ which does not become stationary. So $A(X)$ cannot be artinian.

Proposition 4.11.

i) If R is an artinian ring, then R has only finitely many maximal ideals and all prime ideals are maximal.

ii) For a ring R the following are equivalent
   a) R is artinian.
   b) R is noetherian and every prime ideal is maximal.

Proof. This is on exercise sheet 8. □

Proposition 4.12. Let R be a ring and A an R-algebra of finite type which is integral over R. Then for $p \in \operatorname{Spec} R$, there are only finitely many prime ideals in A which lie over p. This means that the induced map $\operatorname{Spec} A \to \operatorname{Spec} R$ has finite fibre.

Proof. This in on exercise sheet 8. □

End of Lecture 15

4.1. Dimension Theory of Noetherian Rings

Definition 4.13. Let $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal and $n \in \mathbf{N}$. We define $\mathfrak{p}^{(n)} \coloneqq (\mathfrak{p}^n R_\mathfrak{p}) \cap R$ which is called the *n-th symbolic power of* $\mathfrak{p}$.

Lemma 4.14. Let $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal.

i) It holds that
$$\mathfrak{p}^{(n)} = \{a \in R \mid \text{there is a } s \in R \setminus \mathfrak{p} \text{ such that } sa \in \mathfrak{p}^n\}.$$
ii) The chain $\mathfrak{p}^{(0)} \supseteq \mathfrak{p}^{(1)} \supseteq \dots$ is descending and $\mathfrak{p}^{(0)} = R$, $\mathfrak{p}^{(1)} = \mathfrak{p}$.
iii) It holds that $\mathfrak{p}^n \subseteq \mathfrak{p}^{(n)}$ for all $n \in \mathbf{N}$.
iv) It holds that
$$\mathfrak{p}^{(n)} R_\mathfrak{p} = \mathfrak{p}^n R_\mathfrak{p} = (\mathfrak{p} R_\mathfrak{p})^n.$$

Proof.

i) For the inclusion "$\supseteq$", let $a \in R$ and assume that there is a $s \in R \setminus \mathfrak{p}$ such that $sa \in \mathfrak{p}^n$. Then in $R_\mathfrak{p}$ we have that $a/1 = sa/s \in \mathfrak{p}^n R_\mathfrak{p}$ and hence $a \in (\mathfrak{p}^n R_\mathfrak{p}) \cap R$.

   For the reverse inclusion, let $a \in (\mathfrak{p}^n R_\mathfrak{p}) \cap R$. Then $a/1 \in \mathfrak{p}^n R_\mathfrak{p}$ and so there is a $b \in \mathfrak{p}^n$ and a $t \in R \setminus \mathfrak{p}$ such that $a/1 = b/t$. Hence there exists a $u \in R \setminus \mathfrak{p}$ such that $uta = ub \in \mathfrak{p}^n$. So $s \coloneqq ut \notin \mathfrak{p}$ (since $\mathfrak{p}$ is prime) and $sa = ub \in \mathfrak{p}^n$.
ii) This is clear.
iii) This follows from i).
iv) The first equality is just Lemma 1.45 applied to $\mathfrak{p}$. For the second equality and the direction "$\subseteq$", let $b \in \mathfrak{p}^n$. Then there are $b_{ij} \in \mathfrak{p}$ such that $b = \sum_i b_{i,1} \dots b_{i,n}$. For $s \in R \setminus \mathfrak{p}$ we have
$$\frac{b}{s} = \sum_i \frac{b_{i,1}}{s} \cdot \frac{b_{i,2}}{1} \dots \frac{b_{i,n}}{1} \in (\mathfrak{p} R_\mathfrak{p})^n$$

   For the inclusion „$\supseteq$", let $c \in (\mathfrak{p} R_\mathfrak{p})^n$. Then there are $b_{i,j} \in \mathfrak{p}$ and $s_{i,j} \in R \setminus \mathfrak{p}$ such that
$$c = \sum_i \frac{b_{i,1}}{s_{i,1}} \dots \frac{b_{i,n}}{s_{i,n}}.$$
   Set
$$s \coloneqq \prod_{i,j} s_{i,j} \text{ and } b \coloneqq \sum_i \left(\left(\prod_{\substack{1 \le j \le n \\ j \neq i}} s_{ij} \right) \left(\prod_{j=1}^n b_{i,j} \right) \right).$$
   Then $b \in R \setminus \mathfrak{p}$ and $b \in \mathfrak{p}^{(n)}$ and thus $c = b/s \in \mathfrak{p}^n R_\mathfrak{p}$.

□

Definition* 4.B. Let $a \in R$ and $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal. We say that $\mathfrak{p}$ *is minimal over* a if $a \in \mathfrak{p}$ holds and there is no prime ideal $\mathfrak{q} \in \operatorname{Spec} R$ such that $\langle a \rangle \subseteq \mathfrak{q} \subsetneq \mathfrak{p}$ holds.

Theorem 4.15 (Krull's Principal Ideal Theorem)**.** *Let R be a noetherian ring and $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal. If there is an element $a \in R$ such that $\mathfrak{p}$ is minimal over a then $\dim R_{\mathfrak{p}} \leq 1$ holds.*

Proof. Let $\mathfrak{q}' \subseteq \mathfrak{q} \subsetneq \mathfrak{p}$ be a chain of prime ideals. We want to show $\mathfrak{q} = \mathfrak{q}'$. For that, consider the following simplifications

$$R \rightsquigarrow R/\mathfrak{q}' \rightsquigarrow \left(R/\mathfrak{q}'\right)_{\mathfrak{p}}.$$

Then $(R/\mathfrak{q}')_{\mathfrak{p}}$ is a local noetherian integral domain and by various prime ideal coefficients, it suffices to show $\mathfrak{q}\,(R/\mathfrak{q}')_{\mathfrak{p}} = 0$. So we show the following: *Let $(R, \mathfrak{p})$ be a local noetherian integral domain such that the unique maximal ideal $\mathfrak{p}$ is minimal over an element $a \in R$. Then all other prime ideals $\mathfrak{q} \in \operatorname{Spec} R \setminus \operatorname{MaxSpec} R$ are zero.*

Claim 1. Let $\mathfrak{q} \in \operatorname{Spec} R$ be a prime ideal. Then $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + \langle a \rangle$.

The quotient $R/\langle a \rangle$ is a noetherian ring and since there are no prime ideals between $\langle a \rangle$ and $\mathfrak{m}$, we have $\dim R/\langle a \rangle = 0$. So $R/\langle a \rangle$ is artinian (Proposition 4.11, ii)). Consider now the prime ideal chain

$$\left(\mathfrak{q}^{(0)} + \langle a \rangle\right)/\langle a \rangle \supseteq \left(\mathfrak{q}^{(1)} + \langle a \rangle\right)/\langle a \rangle \supseteq \dots$$

in $R/\langle a \rangle$. Then this terminates (as $R/\langle a \rangle$ is artinian) and so there is a $n \geq 0$ such that $\mathfrak{q}^{(n)} + \langle a \rangle \subseteq \mathfrak{q}^{(n+1)} + \langle a \rangle$, and in particular $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + \langle a \rangle$.

Claim 2. In the above situation, it holds that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + \mathfrak{p}\mathfrak{q}^{(n)}$.

The inclusion $\supseteq$ is clear since $\mathfrak{q}^{(n+1)} \subseteq \mathfrak{q}^{(n)}$ (Lemma 4.14). For the other inclusion let $b \in \mathfrak{q}^{(n)}$. Then by the above claim we have $b = c + ar$ with $c \in \mathfrak{q}^{(n+1)}$ and $r \in R$. So $ar = b - c \in \mathfrak{q}^{(n)}$. By Lemma 4.14 i), there is a $s \in R \setminus \mathfrak{q}$ such that $s \cdot ar \in \mathfrak{q}^n$. As $\mathfrak{p}$ is minimal over a, we have $a \notin \mathfrak{q}$ and thus $sa \cdot r \in \mathfrak{q}^n$ implies $r \in \mathfrak{q}^{(n)}$ (again by Lemma 4.14,i)). Now this gives $b = c + ar$, with $c \in \mathfrak{q}^{(n+1)}$, $r \in \mathfrak{q}^{(n)}$ and $a \in \mathfrak{p}$ and thus $b \in \mathfrak{q}^{(n+1)} + \mathfrak{p}\mathfrak{q}^{(n)}$.

We now apply the Nakayama Corollary 2.25 to $M := \mathfrak{q}^{(n)}$, $N := \mathfrak{q}^{(n+1)}$ and $I = \mathfrak{p}$ (Note that $I = \operatorname{Jac} R$, since R is a local ring). Then as $M = N + IM$ we get $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$.

Consider now the localization $R_{\mathfrak{q}}$. By applying Lemma 4.14 iv) twice we have

$$\begin{aligned}(\mathfrak{q}R_{\mathfrak{q}})^n &= \mathfrak{q}^{(n)}R_{\mathfrak{q}} \\ &= \mathfrak{q}^{(n+1)}R_{\mathfrak{q}} \\ &= (\mathfrak{q}R_{\mathfrak{q}})^{n+1}.\end{aligned}$$

NoWe now apply the classical Nakayama Lemma (Lemma 2.24) to $M = (\mathfrak{q}R_{\mathfrak{q}})^n$, $I = \mathfrak{q}R_{\mathfrak{q}} = \operatorname{Jac} R_{\mathfrak{q}}$, and since

$$M = (\mathfrak{q}R_{\mathfrak{q}})^n = (\mathfrak{q}R_{\mathfrak{q}})^{n+1} = IM$$

this yields $M = 0$. As $R_{\mathfrak{q}} \neq 0$, this implies $\mathfrak{q}^n = 0$ and as R is a domain, this ultimately shows $\mathfrak{q} = 0$. □

Lemma 4.16. Let R be an artinian ring. Then the Jacobson ideal $\operatorname{Jac} R$ is nilpotent, i.e. there is a $k \geq 1$ such that $(\operatorname{Jac} R)^k 0$.

Proof. As R is an artinian ring, Proposition 4.11 ii) implies that $\mathcal{N} \coloneqq \operatorname{Nil} R = \operatorname{Jac} R$. The chain $\mathcal{N} \supseteq \mathcal{N}^2 \supseteq \dots$ is decreasing and hence terminates (as R is artinian). So there is $k \geq 1$ such that $\mathcal{N}^k = \mathcal{N}^{k+1} =: \mathfrak{a}$. Assume $\mathfrak{a} \neq 0$. Then the set

$$\Sigma \coloneqq \left\{ \mathfrak{b} \subseteq R \;\middle|\; \begin{array}{l} \mathfrak{b} \text{ is an ideal} \\ \mathfrak{b} \cdot \mathfrak{a} \neq 0 \end{array} \right\}$$

is not empty as $\mathfrak{a} \in \Sigma$. Now Σ is partially ordered by inclusion and R being artinian implies that Σ has an inclusion-minimal element $\mathfrak{c}$ (by Lemma 4.3).

Now by the minimality condition $\mathfrak{c} = \langle x \rangle$ for an element $x \in R$ (as there is an $x \in \mathfrak{c}$ with $x\mathfrak{a} \neq 0$). We also have $x\mathfrak{a} \subseteq \langle x \rangle$, as $(x\mathfrak{a})\,\mathfrak{a} = x\mathfrak{a}^2 = x\mathfrak{a} \neq 0$ and hence $x\mathfrak{a} \subseteq \langle x \rangle$.

So there is a $y \in \mathfrak{a}$ wit $x = xy$. Hence $x = xy^k = 0$, contradicting $x \neq 0$. □

Lemma 4.17. Let $(R, \mathfrak{m})$ be a local noetherian ring with unique maximal ideal $\mathfrak{m}$ and $I \subsetneq R$ a proper ideal. Then the following are equivalent:

i) There is a $n \geq 1$ such that $\mathfrak{m}^n \subseteq I$.
ii) For all prime ideals $\mathfrak{q} \in \operatorname{Spec} R$ with $I \subseteq \mathfrak{p}$ it already holds that $\mathfrak{p} = \mathfrak{m}$.
iii) It holds that $\dim R/I = 0$.
iv) The ring R/I is artinian.

An ideal satisfying any of the above conditions is called an *ideal of definition*.

Proof of Lemma 4.17.

Claim 1. *Let $(R, \mathfrak{m})$ be a local ring such that there is a $k \geq 1$ with $\mathfrak{m}^k = 0$. Then* $\operatorname{Spec} R = \{\mathfrak{m}\}$.

For all $\mathfrak{p} \in \operatorname{Spec} R$ prime we have $\mathfrak{p} \subseteq \mathfrak{m}$. Now let $b \in \mathfrak{m}$. Then $b^k = 0 \in \mathfrak{p}$ and so $b \in \mathfrak{p}$.

Applying this to R/I proves i) $\implies$ ii). Now ii) $\implies$ iii) is just the definition of $\dim R/I$.

iii) $\implies$ iv): R/I is still a noetherian ring and $\dim R/I = 0$ is equivalent to all prime ideals of R/I being already maximal. The claim now follows from Proposition 4.11.

iv) $\implies$ i): By Lemma 4.16 we have that $\operatorname{Jac} R/I$ is nilpotent. But since $\operatorname{Jac} R/I = \overline{\mathfrak{m}}$, this just means that there is a $n \geq 1$ with $\mathfrak{m}^n \subseteq I$. □

Theorem 4.18. *Let $(R, \mathfrak{m})$ be a local noetherian ring.*

i) *If $I = \langle a_1, \dots, a_l \rangle$ is an ideal of definition, then* $\dim R \leq l$.
ii) *Assume* $\dim R = d$. *Then there is an ideal of definition which is generated by d elements.*

Corollary 4.19. Let R be a noetherian ring, $a_1, \dots, a_l \in R$ and $\mathfrak{p} \in \operatorname{Spec} R$ be a minimal prime ideal of $\langle a_1, \dots, a_l \rangle$. Then $\dim R_{\mathfrak{p}} \leq l$.

PROOF. After localising at $\mathfrak{p}$ the ring $R_{\mathfrak{p}}$ is a noetherian local ring. Now the ideal $\langle a_1, \dots, a_l \rangle$ is an ideal of definition, by Lemma 4.17 ii). □

Corollary 4.20. Let A be a k-algebra of finite type and a domain. For an element $0 \neq x \in A$, let $\mathfrak{p}$ be a minimal prime ideal of x. Then $\dim A/\mathfrak{p} = \dim A - 1$.

PROOF. By Corollary 4.19 we have $\dim A_{\mathfrak{p}} \leq 1$. Now in the case $\dim A_{\mathfrak{p}} = 0$ this means that $\mathfrak{p}$ is a minimal prime ideal of A and hence $\mathfrak{p} = \langle 0 \rangle$ (as A is an integral domain). But then $x = 0$, contradicting the assumption $x \neq 0$.

So $\dim A_{\mathfrak{p}} = 1$. Now by Lemma 3.12 and Corollary 3.16 we have $\dim A = \dim A/\mathfrak{p} + \dim A_{\mathfrak{p}}$ and hence

$$\dim A/\mathfrak{p} = \dim A - \dim A_{\mathfrak{p}} = \dim A - 1.$$

□

End of Lecture 16

Lemma 4.21. Let R be a noetherian ring and $I \subseteq R$ an ideal. Then there are only finitely many prime ideals $\mathfrak{q} \in \operatorname{Spec} R$ which are minimal over I.

PROOF. This will be on Exercise Sheet 10. □

PROOF OF THEOREM 4.18. We prove both claims by induction, on l and d respectivley.

i) The case $l = 0$ is trivial, and the case $l = 1$ is precisley Theorem 4.15 (Note that $\mathfrak{m}$ is minimal over $\langle a \rangle$ and that $\dim R = \operatorname{ht} \mathfrak{m}$ holds for a local ring, Lemma 3.11). So assume the claim holds for ideals of definition in local rings which are generated by $l - 1$ elements.

Let $\mathfrak{q} \in \operatorname{Spec} R$ be a prime ideal such that $\mathfrak{q} \subsetneq \mathfrak{m}$ and that there is no prime ideal between $\mathfrak{q}$ and $\mathfrak{m}$. So $I \not\subseteq \mathfrak{q}$ (since $\mathfrak{m}$ is minimal over I) and hence we can assume $a_1 \notin \mathfrak{q}$.

Consider now the ideal $\langle a_1 \rangle + \mathfrak{q}$. Then this is an ideal of definition, by the maximality of $\mathfrak{q}$. By Lemma 4.17 there is a $n \geq 1$ such that $\mathfrak{m}^n \subseteq \langle a_1 \rangle + \mathfrak{q}$ and in particular $g_2, \dots, g_l \in \mathfrak{q}$, $c_2, \dots, c_l \in R$ such that $a_i^n = c_i a_1 + g_i$ for all $i \geq 2$.

Claim 1. The ideal $\langle g_2, \dots, g_l, a_1 \rangle$ is an ideal of definition.

Set $r \coloneqq ln$. Then $I^r \subseteq \langle a_1, g_2, \dots, g_l \rangle$: An element $x \in I^r$ is of the form $x = \sum_\nu c_\nu a_{i_1,\nu} \dots a_{i_r,\nu}$. Now in each of the summands, each of the a_i appears with a power $\geq n$, and so the claim follows from the above observation.

Now since I is an ideal of definition, there is an $s > 0$ such that $\mathfrak{m}^s \subseteq I$ and so in total $m^{rs} \subseteq I^r \subseteq \langle a_1, g_2, \dots, g_l \rangle$ follows, which implies that $\langle a_1, g_2, \dots, g_l \rangle$ is an ideal of definition.

Consider now the quotient $R/\langle g_2, \dots, g_l \rangle$, in which $\overline{\mathfrak{q}} \coloneqq \mathfrak{q}/\langle g_2, \dots, g_l \rangle$ and $\overline{\mathfrak{m}} \coloneqq \mathfrak{m}/\langle g_2, \dots, g_l \rangle$ are prime ideals. By Claim 1 we ge get that

$\overline{a_1} \notin \overline{\mathfrak{q}}$ and hence that $\overline{\mathfrak{m}}$ is minimal over $\overline{a_1}$. Theorem 4.15 now implies that $\dim (R/\langle g_2, \dots, g_l\rangle)_{\mathfrak{m}} \leq 1$.

We now have

$$\dim (R/\langle g_2, \dots, g_l\rangle)_{\mathfrak{m}} = \dim R_{\mathfrak{m}}/\langle g_2, \dots, g_l\rangle \text{ and}$$
$$\dim (R/\langle g_2, \dots, g_l\rangle)_{\mathfrak{q}} = \dim R_{\mathfrak{q}}/\langle g_2, \dots, g_l\rangle,$$

and since $\mathfrak{q} \subsetneq \mathfrak{m}$ this implies $\dim R_{\mathfrak{q}}/\langle g_2, \dots, g_l\rangle = 0$. So by Lemma 4.17, $\langle g_2, \dots, g_l\rangle$ is an ideal of definition in $R_{\mathfrak{q}}$. By the induction hypothesis, we get $\dim R_{\mathfrak{q}} \leq l - 1$.

Let now $\mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_d$ be a chain in R such that $\mathfrak{m} = \mathfrak{p}_d$ and that there is no prime ideal between $\mathfrak{p}_{d-1}$ and $\mathfrak{m}$. We then have $\dim R_{\mathfrak{p}_{d-1}} \geq d - 1$ and by the above reasoning $\dim R_{\mathfrak{p}_{d-1}} \leq l - 1$. So $d \leq l$, which proves i).

ii) Let $\mathfrak{q} \in \operatorname{Spec} R$ be prime with $\operatorname{ht} \mathfrak{q} = d - 1$. Then by the induction hypothesis, there are $b_1, \dots, b_{d-1} \in R_{\mathfrak{q}}$ such that $\langle b_1, \dots, b_{d-1}\rangle$ is an ideal of definition in $R_{\mathfrak{q}}$. Now $b_i = a_i/s_i$ for some $a_i \in R$ and $s_i \in R \setminus \mathfrak{q}$ and so $\langle b_1, \dots, b_{d-1}\rangle = \langle a_1/1, \dots, a_{d-1}/1\rangle$. Hence in R, $\mathfrak{q}$ is minimal over $I \coloneqq \langle a_1, \dots, a_{d-1}\rangle$. By Lemma 4.21, there are only finitely many prime ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ which are minimal over $\langle a_1, \dots, a_{d-1}\rangle$.

Claim 2. *We have* $\mathfrak{m} \not\subseteq \mathfrak{q}_1 \cup \dots \cup \mathfrak{q}_r$.

If $\mathfrak{m} \subseteq \mathfrak{q}_1 \cup \dots \cup \mathfrak{q}_r$ then by prime avoidance (Lemma* 3.H) there is an i such that $\mathfrak{m} \subseteq \mathfrak{q}_i$ and hence $\mathfrak{m} = \mathfrak{q}_i$. So $\mathfrak{m}$ is a minimal prime ideal of $\langle a_1, \dots, a_{d-1}\rangle$ and by i), this would imply $\dim R \leq d - 1$.

Let now $a_d \in \mathfrak{m} \setminus (\mathfrak{q}_1 \cup \dots \cup \mathfrak{q}_r)$. Then $\langle a_1, \dots, a_{d-1}, a_d\rangle$ is an ideal of definition of R, since otherwise, there would be a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$ with $\langle a_1, \dots, a_d\rangle \subseteq \mathfrak{p} \subsetneq \mathfrak{m}$. But this would give a chain $\mathfrak{q}_1 \subsetneq \mathfrak{p}\mathfrak{m}$ for an $1 \leq i \leq r$, contradicting $\operatorname{ht} \mathfrak{q}_i \leq d - 1$.

□

4.2. Primary Decomposition in Noetherian Rings

Definition 4.22. Let R be a ring and $I \subsetneq R$ a proper ideal. We say I is a *primary ideal* if for all $a, b \in R$ with $ab \in I$ it already holds that $a \in I$ or $b^n \in I$, for a $n > 0$.

Example 4.23.

i) Prime ideals are in particular primary ideals.

ii) Let R be a principal ideal domain. Then an ideal I is primary if and only if $I = \mathfrak{p}^n$ holds, for a $n > 0$ and a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$.

Lemma 4.24. Let I be a primary ideal. Then $\sqrt{I}$ is a prime ideal.

Proof. Let $ab \in \sqrt{I}$. Then there is a $n > 0$ such that $(ab)^n \in I$. So since I is primary, $a^n \in I$ or $b^{nm} \in I$ follows, and hence $a \in \sqrt{I}$ or $b \in \sqrt{I}$. So $\sqrt{I}$ is indeed a prime ideal. □

Remark 4.25. Since

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p}\in\operatorname{Spec} R\\ I\subseteq\mathfrak{p}}} \mathfrak{p},$$

we have that $\mathfrak{p} \coloneqq \sqrt{I}$ is the smallest prime ideal which contains I. For this $\mathfrak{p}$, we say that I is $\mathfrak{p}$-*primary*.

Lemma 4.26. $I \subsetneq R$ be a proper ideal. Then I is a primary ideal if and only if every zero-divisor of R/I is nilpotent.

Proof. Let $\overline{a}\overline{b} = 0$. Then $ab \in I$ and hence $a \in I$ or $b^n \in I$, which implies $\overline{a} = 0$ or $\overline{b}^n = 0$. This works in the other direction as well. □

Lemma 4.27. Let $J \subseteq I \subsetneq R$ be ideals. Then I is primary if and only if I/J is primary in R/J.

Lemma 4.28. Let R be a ring. Then the following are equivalent:

i) R has only one prime ideal.
ii) Every element in R is either a unit or nilpotent.
iii) $\sqrt{\langle 0\rangle}$ is a maximal ideal.

Proof. This is on Exercise Sheet 10. □

Lemma 4.29. Let $\mathfrak{m}$ be a maximal ideal and $I \subsetneq R$ an ideal such that

i) $\sqrt{I} = \mathfrak{m}$; or
ii) $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ holds for a $n > 0$.

Then I is $\mathfrak{m}$-primary.

Proof.

i) In R/I, the ideal $\sqrt{\langle 0\rangle}$ is maximal. So the claim follow from Lemma 4.28.
ii) The square root is monotonical increasing, hence $\mathfrak{p} = \sqrt{\mathfrak{p}^n} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$, so $\sqrt{I} = \mathfrak{p}$ follows. Now this is just i).

□

Definition 4.30. Let $I \subsetneq R$ be an ideal. A *primary decomposition* of I is a finite set of primary ideal $I_1, \ldots, I_r$ such that $I = I_1 \cap \ldots \cap I_r$ holds.

Theorem 4.31. *Let R be a noetherian ring. Then every proper ideal $I \subsetneq R$ has a primary decomposition.*

Proof. Assume there are some ideals that do not have a primary decomposition. Since R is noetherian, there is an ideal I which is maximal with this property. Then in the ring $R' \coloneqq R/I$, the zero ideal $\langle 0\rangle$ is the only ideal which does not have a primary decomposition (Lemma 4.26).

Assume that $\langle 0\rangle$ is not primary in R'. Then there are $a, b \in R'$ such that $ab = 0$, but $a \neq 0$ and $b^n \neq 0$ for all $n \geq 1$. Consider now the ascending chain

$$\operatorname{Ann} b \subseteq \operatorname{Ann} b^2 \subseteq \operatorname{Ann} b^3 \subseteq \ldots,$$

which terminates, since R/I is noetherian. So there is a $n \geq 1$ such that $\operatorname{Ann} b^n = \operatorname{Ann} b^{n+1}$.

Claim 1. For this n, $\langle a\rangle \cap \langle b^n\rangle = 0$ holds.

Let $x \in \langle a\rangle \cap \langle b^n\rangle$. Then $x = ca = db^n$ for some $c, d \in R'$ holds. Now by assumption on a, b, we have $0 = cab = db^{n+1}$, and hence $d \in \operatorname{Ann} b^{n+1} = \operatorname{Ann} b^n$. So $x = db^n = 0$ follows.

Since $\langle a\rangle, \langle b^n\rangle \neq 0$, both of them have a primary decomposition, and hence $\langle a\rangle \cap \langle b^n\rangle$ has too. But this contradicts Claim 1.

So $\langle 0\rangle$ is primary. But this contradicts the original assumption that $\langle 0\rangle$ does not have a primary decomposition. □

Remark 4.32.

i) Let $A(X)$ be the coordinate ring of an affine variety X. Let $I \subsetneq A(X)$ be an ideal and $I = I_1 \cap \ldots \cap I_r$ a primary decomposition. Then

$$\begin{aligned} V(I) &= V(I_1) \cup \ldots \cup V(I_r) \\ &= V\left(\sqrt{I_1}\right) \cup \ldots \cup V\left(\sqrt{I_r}\right). \end{aligned}$$

So the primary decomposition of I induces a decomposition of $V(I)$ into irreducible components.

ii) Let $I = \langle (x-a_1)^{k_1} \ldots (x-a_n)^{k_n}\rangle$. Then $V(I) = \{a_1, \ldots, a_n\}$ and a primary decomposition of I is given by

$$(x-a_1)^{k_1} \cap \ldots \cap (x-a_n)^{k_n}.$$

End of Lecture 17

Lemma 4.33. Let $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal and $I_1, I_2 \subseteq R$ two $\mathfrak{p}$-primary ideals. Then the intersection $I_1 \cap I_2$ is $\mathfrak{p}$-primary too.

Proof. It holds that $\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2} = \mathfrak{p}$.

Furthermore, $I_1 \cap I_2$ is a primary ideal: Let $ab \in I_1 \cap I_2$. Then $a \in I_1$ or $b \in \mathfrak{p}$ and $a \in I_2$ or $b \in \mathfrak{p}$. So $a \in I_1 \cap I_2$ or $b \in \mathfrak{p}$, showing that $I_1 \cap I_2$ is indeed primary. □

Definition 4.34. Let $I = I_1 \cap \ldots \cap I_r$ be a primary decomposition, with $\mathfrak{p}_i := \sqrt{I_i}$. We say this decomposition is *minimal* if the following two conditions are satisfied:

i) none of the I_i is redundant: for all $1 \leq i \leq r$ it holds that

$$\bigcap_{i \neq j} I_j \not\subseteq I_i.$$

ii) The $\mathfrak{p}_i$ are pairwise different: $\mathfrak{p}_i \neq \mathfrak{p}_j$ holds for $i \neq j$.

Proposition 4.35. If an ideal $I \subseteq R$ in an (arbitrary) ring R has a primary decomposition, then I has also a minmal primary decomposition.

Proof. Part i) is clear, and part ii) follows from Lemma 4.33. □

Notation 4.36. Let $N \subseteq M$ be a submodule and $m \in M$. We write

$$N : m \coloneqq \{a \in R \mid am \in N\}.$$

Lemma 4.37. In the above case, $N : m$ is an ideal of R.

PROOF. This is immediate. □

Lemma 4.38. Let I be a $\mathfrak{p}$-primary ideal. Then for all $a \in R$ it holds that $\sqrt{I : a} = R$ if $a \in R$ and $\sqrt{I : a} = \mathfrak{p}$ if $a \notin I$.

PROOF. If $a \in I$, then $I : a = R$ and hence $\sqrt{I : a} = \sqrt{R} = R$.

In the other case, let $b \in I : a$. Since I is primary, $b \in \mathfrak{p}$ follows. Now $I \subseteq I : a \subseteq \mathfrak{p}$ and hence

$$\mathfrak{p} = \sqrt{I} \subseteq \sqrt{I : a} \subseteq \sqrt{\mathfrak{p}},$$

since the square root is monotonical. □

Definition 4.39. Let $I \subseteq R$ be an ideal.

i) A prime ideal $\mathfrak{p} \in \operatorname{Spec} R$ is *associated to* I if there is an $a \in R$ such that $\mathfrak{p} = \sqrt{I : a}$. The set of prime ideals associated to I is denoted by $\operatorname{Ass}(I)$.

ii) The inclusion-minimal prime ideals in $\operatorname{Ass}(I)$ are called *isolated prime ideals of* I, all others *embedded prime ideals of* I.

Proposition 4.40. Let $I = I_1 \cap \ldots \cap I_r$ be a minimal primary decomposition of I, with $\mathfrak{p}_i \coloneqq \sqrt{I_i}$. Then $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\} = \operatorname{Ass}(I)$. So in particular, the number of primary ideals in the decomposition does not depend on the decomposition.

PROOF. We first show $\mathfrak{p}_i \in \operatorname{Ass}(I)$: Since the primary decomposition is minmal, there is an $a \in R$ such that $a \in \bigcap_{i \neq j} I_j$ and $a \notin I_i$ for an $1 \leq i \leq r$. Now $I : a = (I_1 : a) \cap \ldots \cap (I_r : a)$ and hence

$$\begin{aligned}
\sqrt{I : a} &= \sqrt{(I_1 : a) \cap \ldots \cap (I_r : a)} \\
&= \sqrt{I_1 : a} \cap \ldots \sqrt{I_r : a} \\
&\overset{4.38}{=} R \cap \ldots \cap R \cap \sqrt{I_i : a} \cap R \cap \ldots \cap R \\
&\overset{4.38}{=} \sqrt{I_i : a} = \mathfrak{p}_i,
\end{aligned}$$

where we used Lemma 4.38 in the marked equalities. So the inclusion „$\subseteq$“ follows.

For the other direction, let $\mathfrak{p} \in \operatorname{Ass}(I)$, so there is an $a \in R$ with $\sqrt{I : a}$. Now

$$\begin{aligned}
\mathfrak{p} &= \sqrt{I : a} \\
&= \sqrt{I_1 : a} \cap \ldots \cap \sqrt{I_r : a}.
\end{aligned}$$

Now by prime avoidance (Lemma* 3.H) we get $\mathfrak{p} = \sqrt{I_i : a}$ for an $1 \leq i \leq r$, and hence (again by Lemma 4.33) $\mathfrak{p} = \mathfrak{p}_i$ (since $\mathfrak{p} = R$ is not possible.) □

Proposition 4.41. Let R be a noetherian ring and $I \subseteq R$ an ideal.

i) The isolated prime ideal of I are precisley the minimal prime ideals over I.

ii) There are only finitely many minimal prime ideals over I.

PROOF. This is on Exercise Sheet 10. □

Lemma 4.42. Let $S \subseteq R$ be multiplicative closed and I a $\mathfrak{p}$-primary ideal. Denote by $\varphi : R \to S^{-1}R$ the canonical map into the localization.

i) If $S \cap \mathfrak{p} \neq \emptyset$, then $IS^{-1}R = S^{-1}R$.
ii) If $S \cap \mathfrak{p} = \emptyset$, then $(IS^{-1}R) \cap R = I$ and $IS^{-1}R$ is $\mathfrak{p}S^{-1}R$-primary.

PROOF. If $S \cap \mathfrak{p} \neq \emptyset$, then there is a $s \in S$ with $s \in \mathfrak{p} = \sqrt{I}$. So $s^n \in I$ for a $n \geq 1$. Now

$$\frac{1}{1} = \frac{s^n}{s^n} \in IS^{-1}R$$

and hence $(IS^{-1}R) \cap R = R$.

Assume now $S \cap \mathfrak{p} = \emptyset$ and let $a \in (S^{-1}R) \cap R$. Then $a/1 \in IS^{-1}R$ and hence there are $q \in I, s, n \in S$ such that $n(q - as) = 0$. Now $ans = nq \in I$. Since I is $\mathfrak{p}$-primary, this implies $a \in I$ or $ns \in \mathfrak{p}$, which in this case means $a \in I$. □

Proposition 4.43. Let $I = I_1 \cap \ldots \cap I_r$ be a minimal primary decomposition of I, with $\mathfrak{p}_i := \sqrt{I_i}$. If $\mathfrak{p}_i$ is minimal over I, then $(IR_{\mathfrak{p}_i}) \cap R = I_i$. In particular, the corresponding I_i do not depend on the decomposition.

PROOF. Let $S \subseteq R$ be a multiplicative set, then

$$(I_1 \cap \ldots \cap I_r)S^{-1}R = \left(I_1 S^{-1}R\right) \cap \ldots \cap \left(I_r S^{-1}R\right),$$

and hence

$$\left(IS^{-1}R\right) = \bigcap_{i=1}^{r} \left(I_i S^{-1}R\right).$$

Set now $S := R \setminus \mathfrak{p}_i$, such that $\mathfrak{p}_i$ is minimal over I. Then $S \cap \mathfrak{p}_i = \emptyset$ and $S \cap \mathfrak{p}_j \neq \emptyset$ for $i \neq j$, since $\mathfrak{p}_j \not\subseteq \mathfrak{p}_i$. Hence by Lemma 4.42 we get

$$(IR_{\mathfrak{p}_i}) \cap R = (I_i R_{\mathfrak{p}_i}) \cap R.$$

□

Remark 4.44. It is possible to defined primary decomposition in the more general context of modules:

i) Let M be an R-module and $\mathfrak{p} \in \operatorname{Spec} R$. We say that $\mathfrak{p}$ is associated to M if there is an $m \in M$ such that $\mathfrak{p} = \operatorname{Ann} m$ (Note that this does not coincide with the definition of an associated prime ideal for an ideal $I \subseteq R$, regarded as an R-module).
ii) We say that a submodule $N \subseteq M$ is primary if it has an associated primary ideal. It can be shown that every proper submodule N has a decomposition $N = N_1 \cap \ldots \cap N_r$ into primary submodules (if R is noetherian).
iii) The uniqueness results are similar to the ones for ideals. (ToDo: do this in more detail).

CHAPTER 5

Regular Rings

Remark⋆ 5.A. Let $(R, \mathfrak{m})$ be a regular noetherian ring. Then R has finite Krull-dimension.

PROOF. The maximal ideal $\mathfrak{m}$ is an ideal of definition. Since R is noetherian, $\mathfrak{m}$ is finitely generated, and hence $\dim R \leq$ number of generators of $\mathfrak{m}$, by Theorem 4.18. □

Notation. Let $(R, \mathfrak{m})$ be a local ring. If not otherwise mentioned, we denote by $k \coloneqq R/\mathfrak{m}$ the fraction field of $\mathfrak{m}$.

Lemma 5.1. Let $(R, \mathfrak{m})$ be a local noetherian ring with $d = \dim R$.

i) It holds that $d \leq \dim_k \mathfrak{m}/\mathfrak{m}$.
ii) We have $d = \dim_k \mathfrak{m}/\mathfrak{m}^2$ if and only if $\mathfrak{m}$ is generated by d elements.

PROOF. This is on exercise sheet 9 (Hint: Use Nakayama.). □

Definition 5.2.

i) Let $(R, \mathfrak{m})$ be a local noetherian ring. We say R is *regular* if $d = \dim_k \mathfrak{m}/\mathfrak{m}^2$ holds.
ii) We say a noetherian ring R is regular if all localization $R_\mathfrak{p}$ with $\mathfrak{p} \in \operatorname{Spec} R$ are regular in the sense of i).
iii) Let X be a variety. We say a point $a \in X$ is regular if $A(X)_{I(a)}$ is a regular local ring.

Remark⋆ 5.B.

i) Note that regular rings are *by definition* noetherian.
ii) It is not clear that the definitions of regular rings are consistent (i.e. that for a regular local ring (in the sense of i)) the dimension equality is satisfied for all localizations at prime ideals). But this seems to be the case ([Sta19, 00NN]) or [Fra18a, Page 33, Cor. 1]

End of Lecture 18

Lemma⋆ 5.C. Let $(R, \mathfrak{m})$ be a local noetherian ring. Then R is a field if and only if $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 0$.

PROOF. The one direction is clear. If, on the other hand, $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 0$, then this is equivalent to $\mathfrak{m} = \mathfrak{m}^2$. By Nakayama (Lemma 2.24), $\mathfrak{m} = 0$ follows and hence R is a field. □

Lemma* 5.D. Let $(R, \mathfrak{m})$ be a local noetherian ring and $f \in \mathfrak{m}$. Then $\dim R/\langle f\rangle \leq \dim R - 1$. If f is not contained in any of the minimal prime ideals of R then equality holds.

Proof. Let $\overline{x_1}, \dots, \overline{x_d}$ be elements in $R/\langle f\rangle$ such that $\langle \overline{x_1}, \dots, \overline{x_d}\rangle$ is an ideal of definition and $d = \dim R/\langle f\rangle$ (These exist, by Theorem 4.18, ii)). Then $\langle f, x_1 \dots, x_d\rangle$ is an ideal of definition of R, and hence $\dim R \leq \dim R/\langle f\rangle + 1$ (by Theorem 4.18, i)).

If f is not contained in any minimal prime ideal of R, then every chain in $R/\langle f\rangle$ can be lifted to chain of prime ideals which is at least one prime ideal away from being maximal, and hence equality follows. □

Lemma* 5.E. Let $(R, \mathfrak{m})$ be a regular local ring and $f \in \mathfrak{m} \setminus \langle 0\rangle$.

i) Set $\overline{R} \coloneqq R/\langle f\rangle$, $\overline{\mathfrak{m}} \coloneqq \mathfrak{m}/\langle f\rangle$ and $\overline{k} \coloneqq \overline{R}/\overline{\mathfrak{m}}$. Then
$$\dim_{\overline{k}} \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 = \begin{cases} \dim R, & \text{if } f \in \mathfrak{m}^2 \\ \dim R - 1, & \text{if } f \notin \mathfrak{m}^2 \end{cases}.$$
ii) Assume that $\dim \overline{R} = \dim R - 1$. Then $\overline{R}$ is regular if and only if $f \notin \mathfrak{m}^2$.
iii) If $f \notin \mathfrak{m}^2$, then $\dim \overline{R} = \dim R - 1$ and $\overline{R}$ is regular.

Proof. The canonical short-exact sequence
$$0 \longrightarrow \langle f\rangle \hookrightarrow \mathfrak{m} \twoheadrightarrow \overline{\mathfrak{m}} \longrightarrow 0,$$
where $\overline{\mathfrak{m}} \coloneqq \mathfrak{m}/\langle f\rangle$, now induces the following big commutative square:
$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \langle f\rangle \cap \mathfrak{m}^2 & \longrightarrow & \mathfrak{m}^2 & \longrightarrow & \overline{\mathfrak{m}}^2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \langle f\rangle & \longrightarrow & \mathfrak{m} & \longrightarrow & \overline{\mathfrak{m}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \langle f\rangle/\left(\langle f\rangle \cap \mathfrak{m}^2\right) & \longrightarrow & \mathfrak{m}/\mathfrak{m}^2 & \longrightarrow & \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$
Now all three columns and the two upper rows are exact, and hence the lower one is too (by the 9-lemma). So it is in particular exact as sequence of k-vector spaces and hence
$$\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim_k \langle f\rangle/\left(\langle f\rangle \cap \mathfrak{m}^2\right) + \dim_{\overline{k}} \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$$
holds (Note that $\mathfrak{m}/\mathfrak{m}^2$ is finite-dimensional, since R is noetherian. Furthermore, $\overline{R}/\overline{\mathfrak{m}} \cong R/\mathfrak{m}$, by the third isomorphism theorem.).

Since R is regular, we have $\dim R = \dim_k \mathfrak{m}/\mathfrak{m}^2$ and hence
$$\begin{aligned} \dim_{\overline{k}} \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 &= \dim_k \mathfrak{m}/\mathfrak{m}^2 - \dim_k \langle f\rangle/\left(\langle f\rangle \cap \mathfrak{m}^2\right) \\ &= \dim R - \dim_k \langle f\rangle/\left(\langle f\rangle \cap \mathfrak{m}^2\right). \end{aligned}$$
As $\dim_k \langle f\rangle/\left(\langle f\rangle \cap \mathfrak{m}^2\right) \leq 1$ and $\dim_k \langle f\rangle/\left(\langle f\rangle \cap \mathfrak{m}^2\right) = 0$ if and only if $f \in \mathfrak{m}^2$, then $\dim \overline{R} = \dim R - 1$ implies that $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$ is regular if and only if $f \notin \mathfrak{m}^2$. This shows i) and ii).

For iii), note that $\dim \overline{R} \leq \dim_{\overline{k}} \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 = \dim R - 1$, by i) and Lemma 5.1. Furthermore, by Lemma* 5.D, we have $\dim \overline{R} \geq \dim R - 1$. Hence equality follows, and $\overline{R}$ is regular by ii). □

Corollary* 5.F. Let $(R, \mathfrak{m})$ be a local noetherian integral domain and $f \in \mathfrak{m} \setminus \langle 0 \rangle$. Then $(R/\langle f \rangle, \mathfrak{m})$ is a regular local ring if and only if $f \notin \mathfrak{m}^2$.

Proof. By Lemma* 5.D, $\dim R/\langle f \rangle = \dim R - 1$ holds (since $f \neq 0$ and $\operatorname{MinSpec} R = \{\langle 0 \rangle\}$). The claim now follows directly from Lemma* 5.D. □

Proposition 5.3. Every regular local ring is an integral domain.

Proof. We will do this by induction on $n := \dim R$. The case $n = 0$ is Lemma* 5.C, which applies since R is regular.

In the general case $n > 0$, we will show that $\langle 0 \rangle$ is prime: Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ the minmal prime ideals over $\langle 0 \rangle$.

Claim 1. *We have* $\mathfrak{m} \not\subseteq \mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$.

If $\mathfrak{m} \subseteq \mathfrak{m}^2 \cup \ldots \cup \mathfrak{p}_r$, then by Prime Avoidance (Lemma* 3.H), we have $\mathfrak{m} \subseteq \mathfrak{m}^2$ or $\mathfrak{m} \subseteq \mathfrak{p}_i$ for an $1 \leq i \leq r$. If $\mathfrak{m}^2 = \mathfrak{m}$, then $\dim R = 0$ follows, since R is regular.

So assume $\mathfrak{m} = \mathfrak{p}_i$. Then already $\mathfrak{m} = \mathfrak{p}_j$ for all $1 \leq j \leq r$ follows, and hence $\operatorname{MinSpec} R = \operatorname{MaxSpec} R = \mathfrak{m}$ follows and hence $\dim R = 0$.

So there is a $a \in \mathfrak{m}$ with $a \notin \mathfrak{m}^2, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$. By Lemma* 5.E iii), we have that $\overline{R} := R/\langle a \rangle$ is regular with $\dim \overline{R} = \dim R - 1$. The induction hypothesis now implies that $\langle a \rangle$ is prime and hence there is an $1 \leq i \leq r$ such that $\mathfrak{p}_i \subseteq \langle a \rangle$. As $a \notin \mathfrak{p}_i$ and $a \in \mathfrak{m}$, we have $\mathfrak{m}\mathfrak{p}_i = \mathfrak{p}_i$, which implies $\mathfrak{p}_i = \langle 0 \rangle$ (by Nakayama, Lemma 2.24). □

5.1. Valuation Rings

Lemma 5.4. Let $(R, \mathfrak{m})$ be a 1-dimensional regular local ring. Then:

i) The maximal ideal $\mathfrak{m}$ is a primary ideal.
ii) For every non-zero $a \in R$ there is a unique $n \geq 1$ such that $\langle a \rangle = \mathfrak{m}^n$.

Proof.

i) Since $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$, $\mathfrak{m}$ is generated by one element (Lemma 5.1,ii)).
ii) Since R is an integral domain (Proposition 5.3), $\langle 0 \rangle$ is the only minimal prime ideal and R being 1-dimensional implies $\operatorname{Spec} R = \{\langle 0 \rangle, \mathfrak{m}\}$. So for every non-zero $a \in R$, $\langle a \rangle$ is an ideal of definition, and hence there is a minimal $n \geq 1$ such that $\mathfrak{m}^n \subseteq \langle a \rangle$ (Lemma 4.17). By i), $\mathfrak{m} = \langle t \rangle$ for a $t \in R$ and hence there is a $b \in R$ such that $t^n = ba$. If $b \in \mathfrak{m}$, then there is a b' such that $b = b't$ and hence $t^n = b'ta$ which would imply $t^{n-1} = b'a$, contradicting the minimality of n. So b is a unit, and hence $\mathfrak{m}^n = \langle a \rangle$.

□

Definition 5.5.

i) A *totally ordered group* is an abelian group $(G,+)$ with a total order $\leq$ such that for all pairs $m \leq n$ and $k \in G$ already $m+k \leq n+k$ follows.
ii) Let G be a totally ordered group. We extend the ordering and group strucutre on G to the set $G \cup \{\infty\}$ by $a \leq \infty$ and $a+\infty := \infty+a := \infty$ for all $a \in G$.
iii) Let K be a field and G a totally ordered group. A *valution on* K is a group homomorphism $\nu : K^\times \to G$ such that $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$ if $a+b \neq 0$. We extend ν to K be setting $\nu(0) := \infty$.
iv) Let $\nu : K^\times \to G$ be a valuation on K. Then $R_\nu := \{a \in K \mid \nu(a) \geq 0\}$ is called the *valuation ring of* ν.
v) The subgroup $\nu(K^\times) \subseteq G$ is called the *valuation subgroup of* ν.

PROOF. The valuation ring R_ν is indeed a ring: We have $\nu(0) = \infty \geq 0$ (by definition), $\nu(1) = 0$ (since ν is a group homomorphism) and for all $a, b \in K^\times$ it holds that $\nu(a+b) \geq \min\{0,0\} = 0$ and $\nu(ab) = 0+0 = 0$. □

Notation. More generally, we say that a ring R is a valuation ring if there is a valuation $\nu : K \to G$ such that $R = R_\nu$.

Example 5.6.
i) On every field, there is the trivial valuation $K^\times \to \{0\}$.
ii) Let R be a factorial ring, set $K := \operatorname{Quot} R$ and let p be a prime element of R. Now for every element $b \in R$, there is a unique maximal $m \geq 0$ such that $b = ap^m$. So every element $b' \in k$ has a unique decomposition of the form $b' = a'p^n$ with $n \in \mathbf{Z}$, such that a' is quotient of two elements from R that are both not divisible by p. Define a map $\nu : K^\times \to \mathbf{Z}$, $ap^n \mapsto n$. Then this is a valuation. The valuation ring is given by
$$R_\nu = \left\{ap^n \;\middle|\; a \in^\times K,\ n \geq 0,\ p \not| a\right\} \cup \{0\} = R_{\langle p \rangle},$$
and the value group is given by $\mathbf{Z}$.
iii) Let K be a field and consider the field
$$L := \left\{ \sum_{n \in \mathbf{Z}} a_n t^n \;\middle|\; a_n \in K,\ \{n \in \mathbf{Z} \mid a_n \neq 0\} \text{ has a lower bound} \right\}.$$
Then
$$\begin{array}{rcl} L^\times & \longrightarrow & \mathbf{Z} \\ \sum a_n t^n & \longmapsto & \min\{n \in \mathbf{Z} \mid a_n \neq 0\} \end{array}$$
is a valuation on L, with valuation ring $K[[t]]$. Note that this is a special case of ii), with $R = K[[t]]$.

End of Lecture 19

Lemma 5.7. Let $R = R_\nu$ be a valuation ring.
i) The ring R is an integral domain.
ii) For all $a \in K^\times$ it holds that $a \in R$ or $a^{-1} \in R$.

iii) For all $a, b \in R$ it holds that $\nu(a) \leq \nu(b)$ if and only if $b \in \langle a \rangle$.
iv) The group of units of R is given by $R^\times = \ker \nu$.
v) It holds that R is a local ring, with unique maximal ideal

$$\mathfrak{m} = \{a \in R \mid \nu(a) > 0\}.$$

vi) The ring R is normal.

Proof.
i) Since R is a subring of a field, it is an integral domain.
ii) Since ν is a group homomorphism, we have

$$\nu(a) + \nu(a^{-1}) = \nu(1) = 0.$$

So $\nu(a) \geq 0$ or $\nu(a^{-1}) \geq 0$.
iii) Assume that $a = 0$. Then $\nu(b) \geq \infty$ if and only if $\nu(b) = \infty$ if and only if $b = 0$ if and only if $b \in \langle 0 \rangle$, since R is an integral domain.
So assume $a \neq 0$. Then $\nu(a) \leq \nu(b)$ if and only if $\nu(b/a) \geq 0$ if and only if $b/a \in R$ if and only if $b \in \langle a \rangle$.
iv) Let $a \in R \setminus \{0\}$. Then $a \in R^\times$ if and only if $a^{-1} \in R$ if and only if $\nu(a^{-1}) = -\nu(a) \geq 0$ if and only if $\nu(a) = 0$.
v) Since ν is a group homomorphism, $\mathfrak{m}$ is an ideal. Let now $I \subseteq R$ be an ideal such that $I \not\subseteq \mathfrak{m}$. Then I contains an element $a \in R$ such that $\nu(a) = 0$, and hence $I = \langle 1 \rangle$, by iv).
vi) The fraction field of R is given by K. Let now $a \in K^\times$ be integral over R. So there are $c_{n-1}, \ldots, c_0$ such that

$$a^n + c_{n-1}a^{n-1} + \ldots + c_0 = 0.$$

Assume $a \notin R$. Then $a^{-1} \in R$ by ii). Hence

$$a = -\left(c_{n-1} + c_{n-2}a^{-1} + \ldots + a^{n-1}c_0\right),$$

and all summands are in R. But this is a contradiction.

□

Proposition 5.8. For a ring R, the following are equivalent:
i) R is a valuation ring.
ii) R is an integral domain such that for all $a \in (\operatorname{Quot} R)^\times$ it holds that $a \in R$ or $a^{-1} \in R$.

Proof. The direction i) $\implies$ ii) follows from Lemma 5.7. For the other direction, set $K := \operatorname{Quot} R$, $G := K^\times / R^\times$ (as quotient of abelian groups) and denote by $\overline{a}$ the image of $a \in K^\times$ in G. We make G into a totally ordered abelian group by setting:

$$\overline{a} \leq \overline{b} \text{ if and only if } b/a \in R.$$

Then this is well-defined, since for units $c_1, c_2 \in R^\times$, we have $a/b \in R$ if and only if $c_1/c_2 \cdot a/b \in R$. It is antisymmetric, since $a/b \in R$ and $b/a \in R$ implies that there is a unit $c \in R^\times$ such that $a/b = c$, transitive and by assumption $\overline{a} \leq \overline{b}$ or $\overline{b} \leq \overline{a}$ always holds. The relation is also compatible with the group structure on G, since $b/a \in R$ implies $bc/ac \in R$ for all $c \in K^\times$.

Denote by $\nu : K^\times \to G$ the quotient map. Then $\nu(a) \leq \nu(b)$ if and only if $b/a \in R$. Then ν is indeed a valuation on $K^\times$: By construction, ν is a group homomorphism, and if $a/b \in R$ then $(a+b)/b = a/b + 1 \in R$, and hence $\nu(a+b) \geq \nu(b)$ follows. □

Remark 5.9. Let $R_\nu \subseteq K$ be a valuation ring for the valuation $\nu : K^\times \to G$. Then this already determines ν in the following sense: It holds that $K = \operatorname{Quot} R$, $\nu(K^\times) = K^\times/R^\times$ and $\nu(a) \leq \nu(b)$ if and only if $\nu(b/a) \leq 0$ if and only $b/a \in R$.

5.2. Discrete Valuation Rings

Proposition 5.10. Let R be a valuation ring with maximal ideal $\mathfrak{m}$. Then the following are equivalent:

i) R is noetherian but not a field.
ii) R is a principal ideal domain but not a field.
iii) The valuation group of R is given by $\mathbf{Z}$.

Definition 5.11. In this case, we say that R is a *discrete valuation ring*

Proof. This will be added in the near future. □

Proposition 5.12. Let R be a local noetherian ring. Then the following are equivalent:

i) R is a discrete valuation ring.
ii) R is a prinicipal ideal domain.
iii) R is a one-dimensional factorial ring.
iv) R is a one-dimensional normal integral domain.
v) R is a one-dimensional regular local ring.

Proof. This will be added in the near future. □

End of Lecture 20

5.3. Dedekind Rings

Definition 5.13. Let R be a one-dimensional noetherian integral domain such that all localizations at prime ideals $R_\mathfrak{p}$ are discrete valuation rings. Then we say that R is a *Dedekind domain*.

Remark⋆ 5.G. By Proposition 5.12, this is well-defined.

Remark 5.14. A one-dimensional noetherian integral domain is a Dedekind domain if and onyl if it is normal.

Proof. By Lemma⋆ 2.V, being normal is a local property. By Proposition 5.12, a localization $R_\mathfrak{p}$ of R is a discrete valuation ring if and only if it is normal. □

Example 5.15.

i) The ring of integers $\mathbf{Z}$, and more generally, every principal ideal domain is a Dedekind domain.

ii) Let X be a smooth curve. Then the coordinate ring $A(X)$ is a Dedekind domain.

Definition* 5.H. Let $\mathbf{Q} \hookrightarrow K$ be a finite field extension. Then the integral closure of $\mathbf{Z}$ in K is the *ring of integers* and denoted by $\mathcal{O}_K$.

Theorem 5.16. *Let $\mathbf{Q} \hookrightarrow K$ be a finite field extension. Then the ring of integers $\mathcal{O}_K$ is a Dedekind domain.*

Proof. Since $\mathcal{O}_K$ is a subring of $\mathbf{Q}$, it is an integral domain. By definition of $\mathcal{O}_K$, the extension $\mathbf{Z} \hookrightarrow \mathcal{O}_K$ is integral and since $\dim \mathbf{Z} = 1$ it follows that $\dim \mathcal{O}_K = 1$ (by Proposition 3.13). Furthermore, every element $a \in \operatorname{Quot} \mathcal{O}_K$ is integral over $\mathbf{Z}$ and so by definition already in $\mathcal{O}_K$. The difficult part is to show that $\mathcal{O}_K$ is noetherian – we first need two more claims:

Claim 1. Let $m \in \mathbf{Z}$ be an integer. Then $\mathcal{O}_K/m\mathcal{O}_K$ has only finitely many elements.

Consider first the case $m = p$ for a prime number p. Now R/pR is a $\mathbf{F}_p$-vector space, since $\mathcal{O}_K$ is a $\mathbf{Z}$-module. So it suffices to show $\dim_{\mathbf{F}_p} \mathcal{O}_K/p\mathcal{O}_K \leq \dim_{\mathbf{Q}} K$: Let $\overline{b_1}, \ldots, \overline{b_n} \in \mathcal{O}_K/p\mathcal{O}_K$ be linearly independent. If there are $\lambda_1, \ldots, \lambda_n \in \mathbf{Q}$ such that

$$\lambda_1 b_1 + \ldots + \lambda_n b_n = 0,$$

then (by factoring out the common denominator) we can assume that $\lambda_1, \ldots, \lambda_n \in \mathbf{Z}$ and that not all λ_i are divisible by p. But then in $\mathcal{O}_K$, we get

$$\overline{\lambda_1 b_1} + \ldots + \overline{\lambda_n b_n} = 0,$$

contradicting that $\overline{b_1}, \ldots, \overline{b_n}$ are linearly independent. So each linearly independet subsest of $\mathcal{O}_K/m\mathcal{O}_K$ lifts to a linearly independet subset of $\mathcal{O}_K \subseteq K$ and hence $\dim_{\mathbf{F}_p} \mathcal{O}_K/m\mathcal{O}_K \leq \dim_{\mathbf{Q}} \mathcal{O}_K \leq \dim_{\mathbf{Q}} K$.

In the general case, note first that for any ring R a short-exact sequence of R-modules

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

the module M is finite if and only if both M' and M'' are finite. Furthermore, for a $\mathbf{Z}$-module M and all $m_1, m_2 \in \mathbf{Z}$ the sequence

$$0 \longrightarrow M/m_1 \longrightarrow M/(m_1 m_2)M \longrightarrow M/m_2 M \longrightarrow 0$$

is short-exact.

So if $m = p_1^{k_1}, \ldots, p_n^{k_n}$ for prime number $p_1, \ldots, p_n \in \mathbf{Z}$ then the above observations show that for each prime number, $\mathcal{O}_K/p_i^{k_i}$ is finite and hence $\mathcal{O}_K/(p_1^{n_1} \ldots p_n^{k_n})\mathcal{O}_K$ is finite too.

Claim 2. Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal. Then there is a non-zero $m \in \mathbf{Z}$ such that $m \in I$.

Assume to the contrary that there is no such m, i.e. $I \cap \mathbf{Z} = \{0\}$. Now the morphism $\mathbf{Z}/I \cap \mathbf{Z} \hookrightarrow \mathcal{O}_K/I$ is integral which implies

$$\dim \mathcal{O}_K/I = \dim \mathbf{Z}/(I \cap \mathbf{Z}) = \dim \mathbf{Z} = 1.$$

But since $\mathcal{O}_K$ is an integral domain and $I \neq 0$, $\dim \mathcal{O}_K/I < \dim \mathcal{O}_K$ holds. This is a contradiction (we noted earlier that $\dim \mathcal{O}_K = \dim \mathbf{Z} = 1$).

We now show that $\mathcal{O}_K$ is noetherian by showing that every ideal $I \subseteq \mathcal{O}_K$ is finitely generated: Let $I \subseteq \mathcal{O}_K$ be an ideal. By Claim 2, there is a $m \in I \cap \mathbf{Z}$. Now $I/\langle m \rangle$ is a submodule of $\mathcal{O}_K/\langle m \rangle$, and by Claim 1 $I/\langle m \rangle$ is finite, so in particular finitely generated. By Lemma* 2.M, this already implies that I is finitely generated. □

Theorem 5.17. *Let R be a Dedekind domain.*

i) *Let $\mathfrak{p} \in \operatorname{MaxSpec} R$ be a maximal ideal and $I \subseteq R$ an ideal. Then I is $\mathfrak{p}$-primary if and only if $I = \mathfrak{p}^k$ for a unique $k \geq 0$.*

ii) *Every ideal I has a decomposition of the form*

$$I = \mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_n^{k_n}$$

where $k_1, \ldots, k_n \geq 1$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n = \operatorname{Ass}(I)$. This decomposition is unique up to permutation.

Proof.

i) The direction " $\Longleftarrow$ " is true in any ring. For the other direction, we note that $IR_\mathfrak{p} \neq 0$ and that (by definition) $R_\mathfrak{p}$ is a discrete valuation ring. So by Proposition 5.12 and Lemma 5.4 there is a unique $k \geq 0$ such that $IR_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^k = \mathfrak{p}^k R_\mathfrak{p}$. Now by Lemma 4.42 $I = \mathfrak{p}^k$ follows.

ii) Since R is noetherian, there is a minimal primary decomposition of I such that $I = I_1 \cap \ldots I_n$ and $\operatorname{Ass}(I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. By part i), there are $k_i \geq 1$ such that $I_i = \mathfrak{p}_i^{k_1}$. Since the $\mathfrak{p}_i$ are maximal and coprime, we get

$$\mathfrak{p}_1^{k_1} \cap \ldots \cap \mathfrak{p}_n^{k_n} = \mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_n^{k_n}.$$

□

Lemma 5.18. Let R be a Dedekind domain.

i) For all collections $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of maximal ideals and natural numbers $k_1, \ldots, k_n, l_1, \ldots, l_n$ it holds that

$$\mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_n^{k_n} \subseteq \mathfrak{p}_1^{l_1} \cdot \ldots \cdot \mathfrak{p}_n^{l_n} \text{ if and only if } l_i \leq k_i \text{ for all } i.$$

ii) Let $a \in R$ be non-zero. Then there is a decomposition of the form

$$\langle a \rangle = \mathfrak{p}_1^{\nu_1(a)} \cdot \ldots \cdot \mathfrak{p}_n^{\nu_n(a)}$$

where $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \operatorname{Ass}(\langle a \rangle)$ and $\nu_i : R_{\mathfrak{p}_i} \to \operatorname{Quot}(R_{\mathfrak{p}_i})$ is the valuation on the localization.

Proof.

i) We first need the following basic facts about localizations

Fact 1. Let R be any ring (note necessarily noetherian, ...).
a) Let $I, J \subseteq R$ be ideals in an arbitrary ring R. Then $I \subseteq J$ if and only if $IR_{\mathfrak{m}} \subseteq JR_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$.
b) Let $R \to R'$ be a ring homomorphism. Then

$$(IJ)R' = (IR')(JR').$$

Now

$$\mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_n^{k_n} \subseteq \mathfrak{p}_1^{l_1} \cdot \ldots \cdot \mathfrak{p}_n^{l_n}$$

if and only if $(\mathfrak{p}_i R_{\mathfrak{p}_i})^{k_i} \subseteq (\mathfrak{p}_i R_{\mathfrak{p}_i})^{l_i}$ if and only if $k_i \leq l_i$ (since $R_{\mathfrak{p}_i}$ is a discrete valuation ring). The result now follows from Fact 1 a) and b) (and the fact that $\mathfrak{p}_i R_{\mathfrak{p}_k} = R_{\mathfrak{p}}$ for $i \neq j$).

ii) Let

$$\langle a \rangle = \mathfrak{p}_1^{\nu_1(a)} \cdot \ldots \cdot \mathfrak{p}_n^{\nu_n(a)}$$

with $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \operatorname{Ass}(\langle a \rangle)$. Then

$$\langle a \rangle R_{\mathfrak{p}_1} = (\mathfrak{p}_i R_{\mathfrak{p}_i})^{k_i},$$

which is exactly $\nu_i(a)$.

□

5.4. The Class Group

Definition 5.19. Let R be an integral domain and set $K \coloneqq \operatorname{Quot} R$.

i) A *fractional ideal* is an R-submodule of K such that there is a non-zero $a \in R$ with $aI \subseteq R$.

ii) Let $a_1, \ldots, a_n \in K$. We denote by

$$\langle a_1, \ldots, a_n \rangle \coloneqq Ra_1 + \ldots + Ra_n$$

the fractional ideal which is generated by $a_1, \ldots, a_n$. We say a fractional ideal I is *finitely generated* if there are $a_1, \ldots, a_n$ such that $I = \langle a_1, \ldots, a_n \rangle$. We say I is a *principal fractional ideal* if there is a $a \in K$ such that $I = \langle a \rangle$.

Example 5.20.

i) Every ideal of R is a fractional ideal in K.

ii) The fractional ideal generated by some elements $a_1, \ldots, a_n$ is indeed a fractional ideal.

Lemma 5.21. Let I be a fractional ideal such that $aI \subseteq R$ is finitely generated. Then I is finitely generated as fractional ideal.

Definition 5.22. Let $I, J \subseteq R$ be submodules of K.

i) Set

$$I \cdot J \coloneqq \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; n \geq 0, a \in I, b \in J \right\},$$

and

$$I :_K J := \{a \in K \mid aJ \subseteq I\}.$$

ii) We say an R-submodule $I \subseteq K$ is invertible if there is an R-submodule $J \subseteq K$ such that $I \cdot J = K$.

Lemma 5.23. Let $I, J \subseteq R$ be submodules of K.

i) Assume $I \cdot J = R$. Then $J = R :_K I$.
ii) If $I = \langle a \rangle$ with $a \neq 0$ is a principal fractional ideal then I is invertible.
iii) If I is invertible then I is a fractional ideal.

Proof.

i) Assume $R = IJ$. We now have

$$J \subseteq R :_K I = (R :_K I)(IJ) \subseteq RJ = J$$

and hence $R :_K I = J$.
ii) If $I = \langle a \rangle$ then $\langle a \rangle \cdot \langle 1/a \rangle = R$.
iii) Let I be invertible, i.e. $I \cdot (R :_K I) = R$, so there are $a_i \in I$ and $b_i \in R :_K I$ such that $\sum a_i b_i = 1$. Let now $b \in I$ then $b = \sum a_i (b_i b)$ with $b_i b \in R$. Let a be the product of the denominators of the a_i, then $ab \in R$ and hence $aI \subseteq R$. So I is a fractional ideal.

□

End of Lecture 21

Technical Remark. *The proofs of the statements of this lecture will be added (hopefully) int the beginnig of September.*

Proposition 5.24. Let R be a Dedekind domain. Then every fractional ideal is invertible.

Corollary 5.25. Let R be a Dedekind ring. Then the set of fractional ideals becomes an group with the multiplication of fractional ideals as binary operation and the ring R as unit. We denote this group by $\mathrm{Div}(R)$. Furthermore, $\mathrm{Div}(R)$ is abelian.

Lemma 5.26. The set $\mathrm{Prin}(R)$ principal fractional ideals are a subgroup of $\mathrm{Div}(R)$.

Definition 5.27. The quotient $\mathrm{Div}(R)/\mathrm{Prin}(R)$ is denoted by $\mathrm{Cl}(R)$ and called the *class group of* R.

Remark 5.28. Here are two fun facts about the class group, which we are not able to prove in this lecture:

i) For every abelian group G there is a Dedekind ring R such that $G \cong \mathrm{Cl}(R)$.
ii) If $\mathcal{O}_K$ is the ring of integers of a number field, then $\mathrm{Cl}(\mathcal{O}_K)$ is finite. The *class number* of K is defined as $|\mathrm{Cl}(\mathcal{O}_K)|$.

Proposition 5.29. Let I be an invertible ideal in a Dedekind ring R. Then

$$I = \mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_n^{k_n}$$

for distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and unique integers $k_1, \ldots, k_n \in \mathbf{Z}$. This representation is unique up to permutation of maximal ideals.

Corollary 5.30. If R is a Dedekind domain, then the group of fractional ideals is the free abelian group generated by the maximal ideals.

Theorem 5.31. *Let R be a Dedekind domain. Then the following are equivalent:*

i) *R is a prinicipal ideal domain.*
ii) *R is factorial.*
iii) *The class group $\mathrm{Cl}(R)$ is trivial.*

5.5. Modules over PIDs and Projective Modules

Lemma 5.32. Let R be a principal ideal domain and N a finitely generated free R-module. Then every submodule $M \subseteq N$ is free too and $\operatorname{rg} M \leq \operatorname{rg} N$.

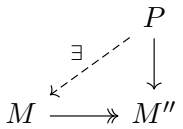
Remark* 5.I. The statement remains true even if N is not finitely generated, although a different proof is needed.

Lemma 5.33. Let R be a principal ideal domain and M a finitely-generated R-module. Then M is free if and only if it is torsion-free.

Lemma 5.34. Let $f : M \to N$ be a surjective R-linear map into a free R-module N. Then $M \cong \ker f \oplus N$.

Corollary 5.35. Let M be a finitely generated R-module. Then there is a decomposition $M \cong M' \oplus T(M)$ with M' free.

Definition 5.36. An R-module P is *projective* if for all R-linear maps $P \to M''$ and surjective R-linear maps $M \twoheadrightarrow M''$ there is an R-linear map $P \to M$ such that the diagram



commutes.

Example 5.37. If P is a free R-module, then P is projective.

Definition 5.38. Let

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

be a short-exact sequence of R-modules. A *split of g* is an R-linear map $\sigma : M'' \to M$ such that $g\sigma = \mathrm{id}_{M''}$. If there is a split of g, we say that g *splits* or that *the sequence is split-exact.*

Lemma 5.39. Let

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

be split-exact. Then there is a unique isomorphism $h : M \xrightarrow{\sim} M' \oplus M''$ such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \| & & \sim\downarrow & & \| & & \\ 0 & \longrightarrow & M' & \hookrightarrow & M & \twoheadrightarrow & M'' & \longrightarrow & 0 \end{array}$$

commutes.

End of Lecture 22

Technical Remark. *Dr. Heidersdorf said in the lecture that the content of the following is not relevant for the first exam. Moreover, he uses some pretty advanced facts about modules. I am not sure if I will be able to add their proofs in the future. The reader can find more on this topic in* [Sta19, 05E3].

Lemma 5.40. Let P be an R-module. Then the following are equivalent:

i) P is projective.
ii) For every surjective map $\pi : M \twoheadrightarrow M''$ the induced map
$$\pi_* : \hom(P, M) \to \hom(P, M'')$$
is surjective.
iii) For every surjective map $\pi : F \twoheadrightarrow M''$ with F free the induced map $\pi_* : \hom(P, M) \to \hom(P, M'')$ is surjective.
iv) P is a direct summand of a free R-module, i.e. there is an R-module Q and a free R-module F such that $F \cong P \oplus Q$.
v) For every surjective map $g : M \to P$ the induced sequence
$$0 \longrightarrow \ker g \hookrightarrow M \xrightarrow{g} P \longrightarrow 0$$
splits.

Definition 5.41. Let M be an R-module.

i) We say M is *locally finitely-generated* if for all prime ideals $\mathfrak{p} \in \operatorname{Spec} R$ there is an element $f \in R \setminus \mathfrak{p}$ such that M_f is a finitely-generated R_f-module.
ii) We say M is *locally finitely-presented* if for all prime ideals $\mathfrak{p} \in \operatorname{Spec} R$ there is an element $f \in R \setminus \mathfrak{p}$ such that M_f is a finitely-presented R_f-module. We say M is *locally free of finite rank* if for all prime ideals $\mathfrak{p} \in \operatorname{Spec} R$ there is an element $f \in R \setminus \mathfrak{p}$ such that M_f is a finitely-generated free R_f-module.
iii) We say M is *locally free of rank* n if for all prime ideals $\mathfrak{p} \in \operatorname{Spec} R$ there is an element $f \in R \setminus \mathfrak{p}$ such that M_f is isomorphic to R_f^n.

Theorem 5.42. *Let M be an R-module. Then the following are equivalent:*

i) *M is finitely-generated and projective.*
ii) *M is finitely-presented and $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m} \in \operatorname{MaxSpec} R$.*
iii) *M is locally-free of finite rank.*

Definition 5.43. Let M be an R-module. We say M is *invertible* if there is an R-module N such that $M \otimes_R N \cong R$.

Remark 5.44. If R is an integral domain, then the notions of invertible modules in the above sense and invertible R-modules in $\operatorname{Quot} R$ do not necessarily coincide.

Lemma 5.45. Let M be an R-module.

i) If M is invertible, then M is already finitely-generated.
ii) If R is a local ring and M is invertible, then M is free of rank 1.

Lemma 5.46. Let M be an R-module. The following are equivalent:

i) M is invertible.
ii) M is finitely generated and $M_{\mathfrak{m}} \cong R_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$.
iii) R is locally free of rank 1.

In this case, M is already finitely-presented and for every R-module N with $M \otimes_R N \cong R$ it already holds that $N \cong \hom(M, R)$.

Definition* 5.J. The R-module $\hom(M, R)$ is the *dual of* M and is also denoted by $M^\vee$.

Lemma* 5.K. If M is a finitely-presented R-module, N any R-module and $S \subseteq R$ a multiplicative subset then there is an isomorphism

$$S^{-1}\left(\hom_R(M, N)\right) \xrightarrow{\sim} \hom_{S^{-1}R}\left(S^{-1}M, S^{-1}N\right)$$

. So in particular, if M is a finitely-presented R-module, then

$$\left(\hom_R(M, R)\right)_{\mathfrak{m}} \cong \hom_{R_{\mathfrak{m}}}\left(M_{\mathfrak{m}}, R_{\mathfrak{m}}\right)$$

for all maximal ideals $\mathfrak{m} \in \operatorname{MaxSpec} R$.

Proof. This is [Wei94, 3.3.7]. □

Definition 5.47. Let R be an integral domain and $M \subseteq \operatorname{Quot} R$ a fractional ideal. Then M is a *local principal ideal* if $M_{\mathfrak{m}}$ is fractional principal ideal in $\operatorname{Quot} R_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$.

Lemma 5.48. Let R be an integral domain and $M, N \subseteq \operatorname{Quot} R$ fractional ideals.

i) There is a surjective linear map $\pi : M \otimes_R N \twoheadrightarrow M \cdot N$.
ii) If M is a local prinicipal ideal, then π is already an isomorphism.

Lemma 5.49. Let R be an integral domain and M an invertible fractional ideal. Then M is finitely generated.

Lemma 5.50. Let R be an integral domain and M a fractional ideal. Then M is invertible if and only if M is a non-zero fractional principal ideal.

Lemma 5.51. Let R be an integral domain and M a fractional ideal. Then the following are equivalent:

i) M is an invertible fractional ideal.
ii) M is finitely generated a locally principal ideal.

Theorem 5.52. *Let R be an intgral domain. Then the following are equivalent:*

i) *M is an invertible fractional ideal.*
ii) *M is an invertible module.*
iii) *M is projective.*

Definition 5.53. Let R be any ring. We define the *Picard group* $\mathrm{Pic}(R)$ of R as the set of isomorphism classes of invertible R-modules, where the multiplication is given by the tensor product.

Lemma 5.54. Let R be an integral domain. Then every invertible module is isomorphic to a fractional ideal.

Theorem 5.55. *If R is a Dedekind Domain, then $\mathrm{Pic}(R)$ is isomorphic to the class group $\mathrm{Cl}(R)$.*

End of Lecture 23

End of Algebra 1

APPENDIX A

Prerequisites - Rings

A.1. Basics

We recall some basic facts and definitions about rings which can be found in [Alu09, Chapter 3],[Str18, Sch19].

Proposition A.1 (Chinese Remainder Theorem)**.** Let $R \neq 0$ be a ring, and $I_1, \ldots, I_r \subseteq R$ ideals such that $I_i + I_j = R$ for all $i \neq j$. Then there is a surjective ring homomorphism

$$\begin{aligned} \varphi \colon R &\longrightarrow R/I_1 \times \ldots \times R/I_r \\ r &\longmapsto (\overline{r}, \ldots, \overline{r}), \end{aligned}$$

and $\ker \varphi = I_1 \cap \ldots \cap I_r$. In particular there is a ring isomorphism

$$R/\left(I_1 \cap \ldots \cap I_r\right) \xrightarrow{\sim} R/I_1 \times \ldots \times R/I_r.$$

A.1.1. Formal Power Series. Under construction.

APPENDIX B

Categories

This chapter is currently under construction. The reader can find the necessary (and much more!) material e.g. in [Ste19].

B.1. General Categories and Functors

B.1.1. Yoneda-Lemma.

Lemma B.1 (Yoneda-Lemma)**.**

i) Let $F : \mathcal{C} \to \mathbf{Set}$ be a functor and $A \in \mathcal{C}$ an object. Then for every element $u \in F(A)$, there is a natural transformation

$$\begin{aligned} \eta_u : \mathcal{C}(A, -) &\longrightarrow F \\ \eta_u(B) : \left(A \xrightarrow{f} B\right) &\longmapsto F(f)(u) \ \text{(for all } B \in \mathcal{C}). \end{aligned}$$

The maps

$$\begin{aligned} \{\text{natural transformations } \mathcal{C}(A, -) \to F\} &\longrightarrow F(A) \\ (\eta : \mathcal{C}(A, -) \to F) &\longmapsto \eta_A(\mathrm{id}_A) \\ (\eta_u : \mathcal{C}(A, -) \to F) &\longleftarrow u \end{aligned}$$

are mutually inverse and natural in F and A.

ii) Let $F : \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ be a functor and $A \in \mathcal{C}$ an object. Then for every element $u \in F(A)$, there is a natural transformation

$$\begin{aligned} \eta_u : \mathcal{C}(-, A) &\longrightarrow F \\ \eta_u(B) : \left(A \xrightarrow{f} B\right) &\longmapsto F(f)(u) \ \text{(for all } B \in \mathcal{C}). \end{aligned}$$

The maps

$$\begin{aligned} \{\text{natural transformations } \mathcal{C}(-, A) \to F\} &\longrightarrow F(A) \\ (\eta : \mathcal{C}(A, -) \to F) &\longmapsto \eta_A(\mathrm{id}_A) \\ (\eta_u : \mathcal{C}(A, -) \to F) &\longleftarrow u \end{aligned}$$

are mutually inverse and natural in F and A.

Lemma B.2 (Yoneda-Embedding)**.** Let $\mathcal{C}$ be a category.

i) The functor

$$\begin{aligned} \mathcal{C}^{\mathrm{op}} &\longrightarrow \mathbf{Fun}(\mathcal{C}, \mathbf{Set}) \\ X &\longmapsto \mathcal{C}(X, -) \end{aligned}$$

is fully faithful.

ii) The functor

$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathbf{Fun}\,(\mathcal{C}^{\mathrm{op}}, \mathbf{Set}) \\ Y & \longmapsto & \mathcal{C}(-, Y) \end{array}$$

is fully faithful.

Definition B.3. Let $F : \mathcal{C} \to \mathbf{Set}$ be a functor. An object $A \in \mathcal{C}$ is a *representing object of* F if there is a natural isomorphism

$$\mathcal{C}(A, -) \xrightarrow{\sim} F.$$

B.2. Additive and Abelian Categories

B.3. Some Homological Algebra

B.3.1. Some Diagram Lemmas.

Lemma B.4 (5-Lemma)**.** Let $\mathcal{A}$ be an abelian category. Let

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & X_1 & \longrightarrow & X_2 & \longrightarrow & X_3 & \longrightarrow & X_4 & \longrightarrow & X_5 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} & & \\ 0 & \longrightarrow & Y_1 & \longrightarrow & Y_2 & \longrightarrow & Y_3 & \longrightarrow & Y_4 & \longrightarrow & Y_5 & \longrightarrow & 0 \end{array}$$

be a commutative diagram in $\mathcal{A}$ with exact rows. Then

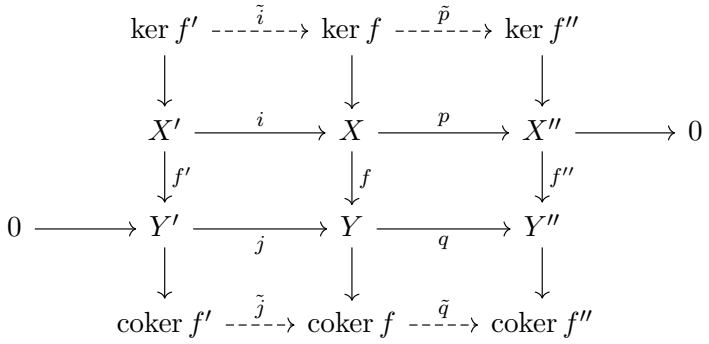
i) If f_2, f_4 are epimorphisms and f_5 is a monomorphism then f_3 is an epimorphisms too.
ii) If f_2, f_4 are monomorphism and f_1 is an epimorphisms then f_3 is a monomorphism.
iii) If f_2, f_4 are isomorphisms, f_1 an epimorphisms and f_5 a monomorphism then f_3 is an isomorphism.

Proof. Ommited. □

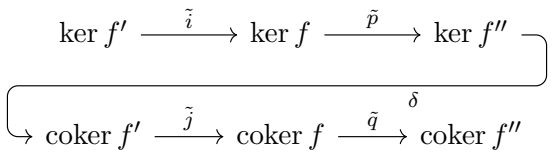
Lemma B.5 (Snake Lemma)**.** Let $\mathcal{A}$ be an abelian category. Let

$$\begin{array}{ccccccccc} & & X' & \xrightarrow{i} & X & \xrightarrow{p} & X'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & Y' & \xrightarrow[j]{} & Y & \xrightarrow[q]{} & Y'' & & \end{array}$$

be a commutative diaram in $\mathcal{A}$ with exact rows. Then there are induced morphisms such that the following diagram commutes



i) There is a morphism $\delta : \ker f'' \to \operatorname{coker} f'$ such that the sequence



is exact.

ii) If i is a monomorphism, then $\tilde{i}$ is a monomorphism too.

iii) If q is an epimorphisms, then $\tilde{q}$ is an epimorphisms too.

Proof. Ommited. □

APPENDIX C

Further Remarks - Modules

C.1. Projective Modules

Definition C.1. Let M be an R-module. We say M is a *projective R-module* if for all epimorphisms $f : X \to Y$ and morphisms $p : M \to Y$ there is a morphism $f' : M \to X$ such that the diagram

$$\begin{array}{ccccc} & & & & M \\ & & f' \swarrow & & \downarrow p \\ X & \longrightarrow & Y & \longrightarrow & 0 \end{array}$$

commutes.

Example C.2.

i) Let M be a free R-module. Then M is projective: Let (e_i) be a basis for M. For each epimorphisms $f : X \to Y$ and morphism $M \to Y$ we can choose for a basis element e_i a preimage under f, say x_i. Then the assignment $e_i \mapsto x_i$ can be extended to an R-linear map $M \to X$, by the universal property of the free module.

ii) The $\mathbf{Z}$-module $\mathbf{Z}/2\mathbf{Z}$ is not projective: Consider the projection $\mathbf{Z} \twoheadrightarrow \mathbf{Z}/2\mathbf{Z}$. Now any lift of the identity

$$\begin{array}{ccc} & & \mathbf{Z}/2\mathbf{Z} \\ & ? \swarrow & \| \\ \mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} \end{array}$$

would necessarily be the zero-morphism (a morphism $f : \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}$ has to satisfy $2f(1) = f(0) = 0$) but then the diagram is far from being commutative.

C.2. Tensor Products

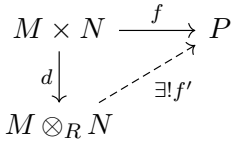
Definition C.3. Let M, N, P be R-modules and $f : M \times M' \to P$ a map. We say h is *R-bilinear* if for all $x \in M$, $y \in N$ the maps

$$\begin{aligned} f(x,-)\colon\ & N \to P, \quad y' \mapsto f(x,y') \\ f(-,y)\colon\ & M \to P, \quad x' \mapsto f(x',y) \end{aligned}$$

are R-linear.

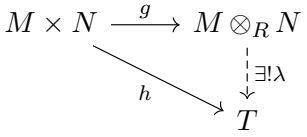
Proposition C.4 (Existence of Tensor Products 1)**.** Let M, N be R-modules.

i) Then there exists an R-module $M \otimes_R N$ and an R-bilinear map $g : M \times N \to M \otimes_R N$ such that for all other R-bilinear maps $f : M \times N \to P$ there is a unique R-linear map $f' : M \otimes_R N \to P$ such that the diagram



commutes.

ii) The tensor product is unique in the following sense: If there is another R-module T with an R-bilinear map $h : M \times N \to T$ and the property that every R-bilinear map $f : M \times N \to P$ factors uniquely over T, then there exists a unique isomorphism of R-modules $\lambda : M \otimes_R N \xrightarrow{\sim} T$ such that the diagram



commutes.

Proof. This is completely analogous to the proof for vector spaces, which can be found in [Sch18, 16.2]. A proof where „vector space“ is replaced with „module“ can be found in [Fra18b, Prop. 2.23]. □

There is another way of defining tensor products, c.f. [Bra16]:

Proposition C.5 (Existence of Tensor Products 2)**.** Let M, N be R-modules. Consider the bilinear-functor

$$\mathrm{bilin}_R(M, N; -) : R\text{-}\mathbf{Mod} \to \mathbf{Set}$$

which sends an R-module P to the set of R-bilinear maps $M \times N \to P$ and an R-linear map $f : P \to Q$ to the induced map

$$\begin{array}{ccc} \mathrm{bilin}_R(M, N; P) & \longrightarrow & \mathrm{bilin}_R(M, N; Q) \\ \left(M \times N \xrightarrow{h} P\right) & \longmapsto & \left(M \times N \xrightarrow{h} P \xrightarrow{f} Q\right). \end{array}$$

Then there exists a representing object $M \otimes_R N$ for $\mathrm{bilin}_R(M, N; -)$, i.e. a natural isomorphism $\mathrm{bilin}_R(M, N; -) \to \hom_R(M \times N, -)$.

The notions of a tensor product from Proposition C.4 and Proposition C.5 are the same. We call the R-module $M \otimes_R N$ the *tensor product of M and N over R*.

We will now use the Yoneda-Embedding (Lemma B.2) to show several properties of the tensor product:

Lemma C.6. Let M, N, M', N' be R-modules and let $f : M \to M'$, $g : N \to N'$ be R-linear maps. Then there is a unique R-linear map

$$\begin{array}{rcl} M \otimes_R N & \longrightarrow & M' \otimes_R N' \\ a \otimes b & \longmapsto & f(a) \otimes g(b). \end{array}$$

Proof. The maps f, g induce a natural transformation

$$\begin{array}{rcl} \eta : \mathrm{bilin}_R(M', N'; -) & \longrightarrow & \mathrm{bilin}_R(M, N; -) \\ \eta_P : \left(M' \times N' \xrightarrow{h} P\right) & \longmapsto & \left(M \times N \xrightarrow{(f,g)} M' \times N' \xrightarrow{h} P\right), \end{array}$$

where the map $(f, g) : M \times N \to M' \times N'$ is given by $(a, b) \mapsto (f(a), g(b))$. This is indeed natural as the diagram

$$\begin{array}{ccc} \mathrm{bilin}_R(M', N'; P) & \xrightarrow{\eta_P} & \mathrm{bilin}_R(M, N; P) \\ {\scriptstyle g\circ -}\downarrow & & \downarrow{\scriptstyle g\circ -} \\ \mathrm{bilin}_R(M', N'; P') & \xrightarrow[\eta_{P'}]{} & \mathrm{bilin}_R(M, N; P') \end{array}$$

commutes for all R-linear maps $P \xrightarrow{g} P'$.

By Proposition C.5 this corresponds to a natural transformation

$$\hom_R(M' \otimes_R N', -) \to \hom_R(M \otimes_R N, -).$$

Using the Yoneda embedding (Lemma B.2, i)), this corresponds to a unique R-linear map $M \otimes_R N \to M' \otimes_R N'$. □

Lemma C.7. Let M, N be R-modules. Then there is a R-linear isomorphism $M \otimes_R N \xrightarrow{\sim} N \otimes_R M$.

Proof. There is a natural isomorphism

$$\begin{array}{rcl} \eta : \mathrm{bilin}_R(M \times N, -) & \longrightarrow & \mathrm{bilin}_R(N \times M, -) \\ \eta_P : \left(M \times N \xrightarrow{(f,g)} P\right) & \longmapsto & \left(N \times M \xrightarrow{(g,f)} P\right). \end{array}$$

So by the Yoneda embedding, this corresponds to a R-linear isomorphism $M \otimes_R N \xrightarrow{\sim} N \otimes_R M$. □

Proposition C.8 (Tensor-Hom-Adjunction)**.** Let N be an R-module.

i) Consider the assignment

$$F : R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod},\ M \mapsto M \otimes_R N$$

which sends an R-linear map $f : M \to M'$ to the induced R-linear map $F(f) := f \otimes \mathrm{id}_N : M \otimes_R N \to M' \otimes_R N$ from Lemma C.6. Then this defines an additive functor $R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}$.

ii) Denote by G the covariant hom-functor

$$\begin{array}{rcl} G : R\text{-}\mathbf{Mod} & \longrightarrow & R\text{-}\mathbf{Mod} \\ P & \longmapsto & \hom_R(N, P) \\ \left(P \xrightarrow{h} P'\right) & \longmapsto & \left(\hom_R(N, P) \xrightarrow{h_*} \hom_R(N, P')\right). \end{array}$$

Then for all $M, P \in R$-**Mod**, there is well-defined map

$$\begin{array}{rcl} \phi : \hom_R(M \otimes_R N, P) & \longrightarrow & \hom_R(M, \hom_R(N, P)) \\ f & \longmapsto & (x \mapsto (y \mapsto f(x \otimes y))) . \end{array}$$

iii) The pair (F, G, ϕ) is an adjunction:
For all $M, P \in R$-**Mod**, the map ϕ from ii) is an isomorphism of R-modules, natural in M and P in the sense that the diagrams

$$\begin{array}{ccc} \hom_R(M' \otimes_R N, P) & \longrightarrow & \hom_R(M', \hom_R(N, P)) \\ {\scriptstyle (f \otimes \mathrm{id})^*}\downarrow & & \downarrow{\scriptstyle f^*} \\ \hom_R(M \otimes_R N, P) & \longrightarrow & \hom_R(M, \hom_R(N, P)) \end{array}$$

and

$$\begin{array}{ccc} \hom_R(M \otimes_R N, P) & \longrightarrow & \hom_R(M, \hom_R(N, P)) \\ {\scriptstyle g_*}\downarrow & & \downarrow{\scriptstyle (g_*)_*} \\ \hom_R(M \otimes_R N, P') & \longrightarrow & \hom_R(M, \hom_R(N, P')) \end{array}$$

commute for all R-linear maps $f : M \to M'$, $g : N \to N'$.

Proof. Consider the maps

$$\begin{array}{rcl} \mathrm{bilin}_R(M, N; P) & \longleftrightarrow & \hom_R(M, \hom_R(N, P)) \\ \left(M \times N \xrightarrow{f} P\right) & \longmapsto & (b \mapsto f(-, b)) \\ (a \times b \mapsto \psi(b)(a)) & \longleftarrow & \left(b \mapsto \left(M \xrightarrow{\psi} P\right)\right) . \end{array}$$

Then these are well-defined natural bijections. So we get for all $M, N, P \in R$-**Mod** a natural isomorphism

$$\mathrm{bilin}_R(M \times N, P) \cong \hom_R(M, \hom_R(N, P)) .$$

But since

$$\mathrm{bilin}_R(M \times N, P) \cong \hom_R(M \otimes_R N, P)$$

by the universal property of the tensor-product, the claim follows. □

Proposition C.9. Let N be an R-module and let

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

be a short-exact sequence of R-modules. Then the sequence

$$M' \xrightarrow{f \otimes \mathrm{id}} M \xrightarrow{g \otimes \mathrm{id}} M'' \longrightarrow 0$$

is again exact. So the tensor-product functor is right-exact.

Proof. This follows from the fact that the tensor product functor is left-adjoint. □

Corollary C.10. Let M be an R-module and $I \subseteq R$ an ideal. Then $R/I \otimes_R M \cong M/IM$ as R-modules.

PROOF. Consider the exact sequence

$$0 \longrightarrow I \hookrightarrow R \twoheadrightarrow R/IR \ .$$

Tensoring with M gives the exact sequence

$$I \otimes_R M \hookrightarrow R \otimes_R M \twoheadrightarrow R/IR \otimes_R M \ .$$

So $R/IR \otimes M \cong \operatorname{coker}(I \otimes M \to M,\ i \otimes \mapsto im)$, which is precisley M/IM. □

Example C.11. It is in general *not* true that the tensor product functor is left-exact: For that, consider the injective map $\mathbf{Z} \to \mathbf{Z},\ x \mapsto 2x$. Then tensoring with $\mathbf{Z}/2\mathbf{Z}$ gives an induced morphism

$$\begin{aligned} \mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/2\mathbf{Z} &\longrightarrow \mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z} \\ x \otimes 1 &\longmapsto 2x \otimes 1. \end{aligned}$$

But now we have $2x \otimes 1 = x \otimes 2 = 0$, so the induced homomorphism is the zero-morphism, and in particular not injective. (Note that we have $\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/2\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z}$).

C.2.1. Flat Modules. We saw in Example C.11 that the tensor product functor is in general not exact. This leads to the following definition:

Definition C.12. An R-module N is *flat* if the tensor-product functor $- \otimes_R N$ is exact.

Example C.13.

i) The ring R as a module is always flat, since $M \otimes_R R \cong N$ for all R-modules N.
ii) More generally, any projective R-module P is flat. If P is finitely presented, then the converse is also true.

C.2.2. Extension of Scalars. Let $\varphi : R \to R'$ be a ring homomorphism and M an R-module. Then φ induces the structure of an R-module on R' and hence we can form the tensor product $R' \otimes_R M$. Now this induces the structure of an R'-module on $R' \otimes_R M$ given by

$$r_1' \left(r_2' \otimes m\right) \coloneqq \left(r_1' r_2'\right) \otimes m,$$

which can be extended linearly. This is called *extensions of scalars* or *base change*.

Proposition C.14.

i) Extension of scalars is functorial: For every R-module homomorphism $f : M \to M'$ there is an induced R'-linear morphism $R' \otimes_R M \to R' \otimes_R M'$. Denote this functor by $F : R\text{-}\mathbf{Mod} \to R'\text{-}\mathbf{Mod}$.
ii) Recall that by Example 2.2, we can regard every R'-module as an R-module. This defines a functor $G : R'\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}$.
iii) The pair $F : R\text{-}\mathbf{Mod} \rightleftarrows R'\text{-}\mathbf{Mod} : G$ defines an adjunction.

PROOF.

i) For every R-linear map $f : M \to M'$, we get an R-bilinear map

$$\begin{aligned} R' \times M &\longrightarrow R' \times M' \\ r', m &\longmapsto r' \otimes f(m). \end{aligned}$$

This induces an R-linear map $R' \otimes_R M \to R' \otimes M'$, given on elementary tensors by $r' \otimes m \mapsto r' \otimes f(m)$. Cleary, this map is also R'-linear.

ii) An R'-linear map $M \to M'$ is in particular R-linear, since the action of R on M is given by $r.m \coloneqq \varphi(r)m$.

iii) The assignment

$$\begin{aligned} \hom_{R'}(M \otimes_R R', M') &\longrightarrow \hom_R(M, M') \\ M \otimes_R R' \xrightarrow{f} M' &\longmapsto (M \xrightarrow{f'} M',\ m \mapsto f(1 \otimes m)) \end{aligned}$$

is a natural bijection.

□

C.3. Localization of Modules

Proposition C.15. Let M be an R-module, $S \subseteq R$ a multiplicative set. Then the map

$$\begin{aligned} S^{-1}M &\xrightarrow{\sim} S^{-1}R \otimes_R M \\ \frac{x}{r} &\longmapsto \frac{1}{r} \otimes x \end{aligned}$$

is an isomorphism of $S^{-1}R$-modules.

C.4. Local-Global

For more, the reader is refered to [**Sta19**, 00EN].

Proposition C.16 (being zero is local)**.** Let M be an R-module. Then the following are equivalent:

i) $M = 0$.
ii) $M_\mathfrak{p} = 0$ for all prime ideals $\mathfrak{p} \subseteq R$.
iii) $M_\mathfrak{m} = 0$ for all maximal ideal $\mathfrak{m} \subseteq R$.

Proposition C.17 (being injective/surjective is local)**.** Let $f : M \to N$ be an R-linear map.

i) The following are equivalent:
   a) f is injective.
   b) $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective for all prime ideals $\mathfrak{p} \subseteq R$.
   c) $f_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ is injective for all maximal ideals $\mathfrak{m} \subseteq R$.

ii) The following are equivalent:
   a) f is surjective.
   b) $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is surjective for all prime ideals $\mathfrak{p} \subseteq R$.
   c) $f_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ is surjective for all maximal ideals $\mathfrak{m} \subseteq R$.

C.5. Structure Theorems for Modules

C.5.1. Modules over PIDs.

Definition C.18. Let R be a ring. We say R is a *principal ideal domain* if R is an integral domain and every ideal $I \subseteq R$ is of the form $\langle a \rangle$ for an $a \in R$.

The following facts about modules over PIDs are taken from [**Fra18b**, Chapter 4]

Proposition C.19. Let R be a PID and F a free R-module and $M \subseteq F$ a submodule. Then M is free.

Theorem C.20. *Let R be a PID and M a finitely generated R-module. Then there is a $r \geq 0$, an $r \geq 0$ and prime elements $p_1, \ldots, p_n \in R$ such that for all $1 \leq i \leq n$ there are $1 \leq s_{i_1} \leq \ldots \leq s_{i_{t_i}}$ with*

$$M \cong R^r \bigoplus \left(\bigoplus_{i=1}^{n} \bigoplus_{j=1}^{l_i} A/\left(p_i^{s_{i_j}}\right) \right)$$

Bibliography

[Alu09] Paolo Aluffi, *Algebra: chapter 0*, Vol. 104, American Mathematical Soc., 2009.

[AM94] M.F. Atiyah and I.G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley series in mathematics, Avalon Publishing, 1994.

[Bra16] M. Brandenburg, *Einführung in die kategorientheorie: Mit ausführlichen erklärungen und zahlreichen beispielen*, Springer Berlin Heidelberg, 2016.

[EE95] D. Eisenbud and P.D. Eisenbud, *Commutative algebra: With a view toward algebraic geometry*, Graduate Texts in Mathematics, Springer, 1995.

[Fra17] J. Franke, *Algebra 1 (lecture notes)* (2017), available at https://github.com/Nicholas42/AlgebraFranke/blob/master/AlgebraI/Alg1.pdf.

[Fra18a] ———, *Homological methods in commutative algebra (lecture notes)* (2018), available at https://github.com/Nicholas42/AlgebraFranke/raw/master/HomAlg/HomAlg.pdf.

[Fra18b] H. Franzen, *Algebra 1 (lecture notes)* (2018), available at https://github.com/lkempf/AlgebraStroppel.

[MR89] H. Matsumura and M. Reid, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1989.

[Sch18] J. Schröer, *Lineare algebra (lecture notes)* (2018).

[Sch19] ———, *Einführung in die algebra (lecture notes)* (2019).

[Sta19] The Stacks project authors, *The stacks project*, 2019.

[Ste19] J. Stelzner, *Foundations of representation theory (lecture notes)* (2019), available at https://github.com/cionx/foundations-in-representation-theory-notes-ws-18-19.

[Str18] C. Stroppel, *Einführung in die algebra (lecture notes)* (2018), available at https://github.com/lkempf/AlgebraStroppel.

[Vak18] R. Vakil, *MATH 216: Foundations of Algebraic Geometry* (2018), available at http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf.

[Wei94] C. Weibel, *An introduction to homological algebra*, Graduate Texts in Mathematics, Cambridge University Press, 1994.

Index