Modern Algebra II

A first course in commutative ring theory

(Version: January 14, 2025)

Acknowledgement

These are the lecture notes of "Modern Algebra II" that I teach in 2024 at the National Taiwan University. I would like to thank the teaching assistant Hajime Nakahashi, as well as all the students who attend the lectures. Special thanks to Jia-Lin Hsu, Yung-Chen Li, Jun-Ting Lin, Tzu-Yang Tsai, Shao-Wei Wang, and Yi-Teng Wu for helpful feedback.

All comments are very welcome.

Contents

Acknowledgement 2

Lecture 1. A brief introduction 5

1. Rings arising from number theory 5
2. Motivations from algebraic geometry 6

Lecture 2. Algebraic numbers and integrality 8

Lecture 3. The geometry of rings and ideals 11

4. The historical origin of ideals 11
5. Ideals and algebraic closed subsets 11
6. Affine schemes: a first definition 13

Lecture 4. Tensor products 19

7. Tensor products 19
8. Properties of tensor products 21
9. Tensor algebras 24

Lecture 5. Localizations 26

10. Localizations 26
11. Nakayama's lemma 33

Lecture 6. Maximal ideals and Hilbert's Nullstellensatz 36

12. 36

Lecture 7. Generators and relations 39

13. Finite generation and finite presentation 39
14. Locally free modules 41

Lecture 8. Krull dimension and chain conditions 44

15. Krull dimension of a ring 44
16. Chain conditions 46
17. Associated points of modules 49

Lecture 9. Dimension and integral morphisms 52

18. Finite and integral morphisms 52
19. Dimension of finitely generated **k**-algebras 54

Lecture 10. Codimension 57

20. Catenary spaces 57
21. Krull's principal ideal theorem (Hauptidealsatz) 58

Lecture 11. Valuation rings 61

22. Riemann surfaces and number fields 61
23. Unique factorization of ideals in a Dedekind domain 64
24. Weil divisors and Cartier divisors 66

Lecture 12. Differentials 69
25. 69
26. Dimension of the tangent cone 74

Lecture 13. Projective modules and flat modules 80
27. Extensions 80
28. Higher Ext-groups 82
29. Flat modules 86

Lecture 14. Completion 91
30. Examples and definition 91
31. Completion 92
32. Completion of Noetherian rings 93

Bibliography 95

LECTURE 1

A brief introduction

Throughout these notes, unless otherwise specified a ring A is always assumed to be

- commutative;
- unital (i.e. there exists an element $1 \in A$ such that $1 \cdot x = x \cdot 1 = x$ for any $x \in A$).

A morphism of rings $f : A \to B$ always maps 1 to 1. We also assume the axiom of choice together with its consequence (e.g. Zorn's lemma).

Modern Algebra II of this semester is mainly about the theory of commutative rings. Examples of rings are

$$\mathbf{Z},\ \mathbf{Q},\ \mathbf{Z}[e^{2\pi\imath/n}],\ \mathbf{C}[X],\ \mathbf{Z}[X,Y]/(Y^2 - X^3 - X),\ \mathbf{C}[X_1, X_2, \ldots],\ \ldots$$

There are two main sources which motivate the development of the theory of commutative rings: *algebraic number theory* and *algebraic geometry*.

1. Rings arising from number theory

1.1. Sums of two squares. When is a positive integer n equal to the sum of two squares, namely $n = a^2 + b^2$ with $a, b \in \mathbf{Z}$? If n is odd, then an obvious necessary condition is that $n \in 4\mathbf{Z} + 1$. A little experiment shows that

$$1 = 0^2 + 1^2,\ \ 5 = 1^2 + 2^2,\ \ 9 = 0^2 + 3^2,\ \ 13 = 2^2 + 3^2,\ \ 17 = 1^2 + 4^2,$$

$$21 \text{ is not a sum of two squares},\ \ 25 = 0^2 + 5^2,\ \ 29 = 2^2 + 5^2,$$

$$33 \text{ is not a sum of two squares},\quad 37 = 1^2 + 6^2, \ldots\ldots,$$

and one see that the converse does not hold in general. However:

Theorem 1.1 (Fermat). *Let p be an odd prime number. Then p is a sum of two squares if and only if $p \in 4\mathbf{Z} + 1$.*

1.2. Gauss integers and Gauss primes. The proof of Fermat's theorem we present here involves the ring of *Gauss integers*:

$$\mathbf{Z}[\imath] = \{\, a + b\imath \mid a, b \in \mathbf{Z} \,\}$$

where $\imath$ is a square root of -1. One can run the Euclidean division with respect to the multiplicative norm $N : \mathbf{Z}[\imath] \to \mathbf{Z}_{\geq 0}$ defined by

$$N(a + b\imath) = a^2 + b^2.$$

That $\mathbf{Z}[\imath]$ is a Euclidean domain implies that $\mathbf{Z}[\imath]$ is a unique factorization domain (UFD).

Exercise 1.2. Find the greatest common divisor of $8 + 10\imath$ and $2 + 6\imath$ by the Euclidean algorithm.

Exercise 1.3. What are the units of $\mathbf{Z}[\imath]$? Show that $z \in \mathbf{Z}[\imath]$ is a unit if and only if $N(z) = 1$.

The notions of prime elements and irreducible elements in $\mathbf{Z}[\imath]$ therefore coincide, and we call them *Gauss primes*. They relate the two statements in Fermat's theorem as follows.

Theorem 1.4. *Let $p \in \mathbf{Z}$ be an odd prime number. The following assertions are equivalent:*

(1) p is a sum of two squares.

(2) p is not a Gauss prime.

(3) $p \in 4\mathbf{Z} + 1$.

Proof. First we show that (2) implies (1). Suppose that $p = \alpha\beta$ with non-unit $\alpha, \beta \in \mathbf{Z}[\imath]$. Then

$$p^2 = N(p) = N(\alpha)N(\beta).$$

As $N(\alpha), N(\beta) \neq 1$ and p is a prime number, we have $p = N(\alpha)$, which is a sum of two squares.

It remains to show that (3) implies (2). Suppose that $p = 4k + 1$ with $k \in \mathbf{Z}_{>0}$. Modulo p, we have

$$-1 = (p-1)! = (2k)!^2,$$

where the first equality follows from Wilson's theorem. Thus if $n := (2k)!$, we have

$$p \mid (n + \imath)(n - \imath)$$

in $\mathbf{Z}$, and therefore in $\mathbf{Z}[\imath]$. As neither factor is divisible by p, it follows that p is not a Gauss prime. □

In the following exercise, we describe all the Gauss primes.

Exercise 1.5. Show that $z \in \mathbf{Z}[\imath]$ is a Gauss prime if and only if up to multiplying by a unit, z satisfies one of the following descriptions:

(1) $z = 1 + \imath$;
(2) $z = a + b\imath$ such that $N(z)$ a prime number with $N(z) \in 4\mathbf{Z} + 1$;
(3) z is a prime number with $z \in 4\mathbf{Z} + 3$.

(Hint: first show that $N(z) = p$ or p^2 for some prime number p.)

Theorem 1.4 and its proof provide an example showing that how rings such as $\mathbf{Z}[\imath]$ can be used to provide new perspectives, or to explain what lie behind some elementary statements in number theory. There are other examples, such as solving the Diophantine equation

$$X^2 - dY^2 = 1$$

with $X, Y \in \mathbf{Z}$ for a given square-free integer d is equivalent to finding units in the quadratic integer ring $\mathbf{Z}[\sqrt{d}]$. Historically, motivated by Fermat's last "theorem", the rings of cyclotomic integers $\mathbf{Z}[\zeta_n]$ where ζ_n is a primitive nth root of unity were also heavily studied in the 19th century (e.g. whether $\mathbf{Z}[\zeta_n]$ is a UFD).

Remark 1.6. See [**3**] for a one-line proof of Fermat's theorem and related discussions.

2. Motivations from algebraic geometry

Apart from algebraic number theory, we've mentionned that another source of the theory of commutative rings is algebraic geometry.

2.1. Manifolds. We have a contravariant fully faithful embedding[1]

$$\begin{aligned} \text{Smooth manifolds} &\to \text{Commutative } \mathbf{R}\text{-algebras} \\ M &\mapsto \mathscr{C}^\infty(M) \end{aligned} \tag{2.1}$$

So the study of smooth manifolds M (e.g. the de Rham cohomology, the embedding problem, etc.) is formally equivalent to the study of their rings of smooth functions $\mathscr{C}^\infty(M)$, together with the homomorphisms between them. See also [**4**, Exercise 1.26].

Let M be a manifold. We also have a faithful functor

$$\begin{aligned} \text{Smooth vector bundles on } M &\to \mathscr{C}^\infty(M)\text{-modules} \\ V &\mapsto \Gamma(X, V)\,, \end{aligned} \tag{2.2}$$

whose essential image is the subcategory of finitely generated projective $\mathscr{C}^\infty(M)$-modules; see [**11**, Chapter 12].

[1] See [**11**, Chapter 7] for more detail. In physical language, $\mathscr{C}^\infty(X)$ can be regarded as the algebra of observables, and the fully faithful embedding could be interpreted by the observability principle: namely things and differences exist if and only if we can observe them.

2.2. Affine space and its algebraic closed subsets. Instead of smooth manifolds, now consider the affine space $\mathbf{A}^d_{\mathbf{k}} := \mathbf{k}^d$ of dimension $d \in \mathbf{Z}_{\geq 0}$ over an algebraically closed field $\mathbf{k}$. The ring of polynomial functions on $\mathbf{A}^d_{\mathbf{k}}$ is the $\mathbf{k}$-algebra

$$\mathbf{k}[X_1, \ldots, X_d].$$

The first objects that we are interested in algebraic geometry are the subsets

$$Z = \{ P_i = 0 \mid \text{ for all } i \in J \} \subset \mathbf{A}^d_{\mathbf{k}}$$

of $\mathbf{A}^d_{\mathbf{k}}$ cut out by a collection of polynomial functions $\{P_i\}_{i \in J}$. Equivalently, Z is defined by the ideal

$$I = (P_i)_{i \in J} \subset \mathbf{k}[X_1, \ldots, X_d]$$

generated by $\{P_i\}_{i \in J}$:

$$Z = Z(I) := \left\{ x \in \mathbf{A}^d_{\mathbf{k}} \,\middle|\, f(x) = 0 \text{ for all } f \in I \right\}. \tag{2.3}$$

We call such a subset Z an *affine algebraic closed subset*. The study of Z in the context of algebraic geometry is contained in the study of the quotient

$$R = \mathbf{k}[X_1, \ldots, X_d]/I.$$

Modules over R are analogous to vector bundles over a manifold.

The local models in algebraic geometry are the so-called *affine schemes*, which form a category equivalent to the category of commutative rings. Therefore just as multivariable calculus is the local theory of differential geometry, the local study of algebraic geometry is equivalent to the study of commutative rings.

Commutative rings appear in various contexts, and different perspectives allow us to formulate and study concepts of commutative rings of different origins (geometric and topological ones such as differentials, cohomology; arithmetic ones such as factoriality).

LECTURE 2

Algebraic numbers and integrality

3.1. Number fields and their Z-structures. The goal of algebraic number theory is to study algebraic numbers, which, by definition, are the elements of the algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ in $\mathbf{C}$. Studying them consists of studying the finite field extensions K of $\mathbf{Q}$. These fields are called *number fields*.

It is a remarkable and fundamental fact that each number field K has a *canonical* **Z**-*structure*. This **Z**-structure provides a natural generalization of "integers" in a number field K and plays a central rôle in the theory of algebraic numbers.

Theorem-Definition 3.1. *There exists a unique maximal subring $\mathscr{O}_K$ of K which is a* **Z***-structure of the* **Q***-vector space K; in other words, there exists a* **Q***-linear isomorphism*

$$K \xrightarrow{\sim} \mathbf{Q}^d$$

mapping $\mathscr{O}_K$ onto $\mathbf{Z}^d \subset \mathbf{Q}^d$. We call $\mathscr{O}_K$ the ring of integers of *K.*

Note that if such a ring $\mathscr{O}_K$ exists, then $\mathscr{O}_K$ is a **Z**-module of finite type. We will then see that for every $\alpha \in \mathscr{O}_K$, we can find a monic polynomial $P \in \mathbf{Z}[X]$ (i.e. the leading coefficient of P is 1) such that $P(\alpha) = 0$. Elements satisfying the above properties are called *integral (over* **Z***)*, and eventually we will see that $\mathscr{O}_K$ consists of all integral elements of K. We shall first define and study integral elements in a more general context.

3.2. Integral elements. Let B be a ring and let $A \subset B$ be a subring. An element $b \in B$ is called *integral* over A if there exists a monic polynomial $P \in A[X]$ such that $P(b) = 0$.

Proposition 3.2. *Let $b \in B$. The following assertions are equivalent:*

(1) $b \in B$ is integral.

(2) The subring $A[b] \subset B$ generated by A and b is an A-module of finite type.

(3) $A[b]$ is contained in a subring $C \subset B$ of finite type as an A-module.

Proof. The implications (1) ⇒ (2) ⇒ (3) are clear. The implication (3) ⇒ (1) follows from the Cayley–Hamilton Theorem below, applied to the multiplication $\cdot b : C \circlearrowleft$. □

Theorem 3.3 (Cayley–Hamilton)**.** *Let R be a ring and let M be an R-module generated by n element. For every R-linear endomorphism $\phi : M \circlearrowleft$, there exists a monic polynomial $P \in R[X]$ of degree n such that*

$$P(\phi) = 0.$$

Moreover if $\phi(M) \subset IM$ for some ideal $I \subset R$, then we can choose

$$P = X^n + r_{n-1}X^{n-1} + \cdots + r_0 \in R[X]$$

with $r_{n-j} \in I^j$ for all j.

Proof. Let $v_1, \dots, v_n$ be generators of M and write

$$\phi(v_i) = \sum_{j=1}^{n} r_{ij} v_j$$

with $r_{ij} \in R$ (or $r_{ij} \in I$ for the second statement). Let δ_{ij} be the Kronecker delta and consider the matrix

$$A := (\delta_{ij}\phi - r_{ij})_{1 \le i,j \le n}$$

with coefficients in the subring $R' \subset \mathrm{End}_R(M)$ generated by ϕ and the multiplications $x \mapsto rx$ for all $r \in R$; we still use r to denote the image of $r \in R$ in $\mathrm{End}_R(M)$.

Note that R' is commutative, so if C denotes the transpose of the cofactor matrix of A, then

$$CA = \det(A) I_n \in M_n(R').$$

By definition, we have $Av = 0$, where v is the column matrix consisting of $v_1, \ldots, v_n$, so $\det(A) \in R'$ evaluating at v_i is zero for all i. It follows that $\det(A) = 0$, and we finish the proof by developing $\det(A)$. □

We prove by induction on n the following corollary.

Corollary 3.4. *Let $b_1, \ldots, b_n \in B$ be integral elements over A. Then $A[b_1, \ldots, b_n] \subset B$ is an A-module of finite type.*

3.3. Integral extensions and finite extensions. Let A be a ring. An A-algebra is a ring B together with a ring homomorphism $\phi : A \to B$. An A-algebra is naturally a A-module, with

$$a \cdot b := \phi(a)b$$

for any $a \in A$ and $b \in B$. That $\phi : A \to B$ is a ring homomorphism gives rise to several rules that $a \cdot b$ needs to satisfy.

There are two notions of finiteness of algebras that we can define.

- We say that B is a *finite A-algebra* (or that B is finite over A) if B regarded as an A-module is of finite type.
- We say that B is a *finitely generated A-algebra* (or an A-algebra of finite type) if there exists a finite number of elements $b_1, \ldots, b_n$ such that any element of B is a polynomial in $b_1, \ldots, b_n$ with coefficients in A. Equivalently, there exists a surjective morphism of A-algebras

$$A[X_1, \ldots, X_n] \to A$$

for some $n \in \mathbf{Z}_{\geq 0}$.

Here, a morphism between two A-algebras B and C is a ring homomorphism $f : B \to C$ which commutes with the structural morphisms:

$$\begin{tikzcd} B \arrow[rr, "f"] & & C \\ & A \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Exercise 3.5. Let $f : B \to C$ be a ring homomorphism between two A-algebras. Show that f is a morphism of A-modules if and only if f is a morphism of A-algebras.

Corollary 3.6. *Let B be a ring and let $A \subset B$ be a subring. Suppose that B is a finitely generated A-algebra. Then B is integral over A if and only if B is finite over A.*

Proof. The "if" part follows from Proposition 3.2 applied to $C = B$. The "only if" part follows from Corollary 3.4. □

Remark 3.7. The finite generation assumption in Corollary 3.6 is required: Consider for instance $\mathbf{Q} \hookrightarrow \overline{\mathbf{Q}}$.

3.4. Integral closure. Let A be a subring of a ring B be as before.

Corollary-Definition 3.8. *The subset $\overline{A} \subset B$ of integral elements over A is a subring. We call $\overline{A}$ the* integral closure of *A in B.*

Proof. Let x, y be two integral elements of B. Then both $x + y$ and xy are in $A[x, y]$, which is a finite type A-module by Corollary 3.4. We conclude by Proposition 3.2 with $C = A[x, y]$. □

If every $b \in B$ is integral over A, we say that B is an *integral extension* of A. On the other hand if $A = \overline{A}$, then we say that A is *integrally closed in* B. In general, we say that an integral domain A is an *integrally closed domain* (or a *normal domain*) if it is integrally closed in its field of fractions.

The transitivity of integral extensions is another immediate corollary of Proposition 3.2.

Corollary 3.9 (Transitivity of integral extensions)**.** *Let $A \subset B \subset C$ be inclusions of subrings. If B is an integral extension of A and C is an integral extension of B, then C is an integral extension of A.*

Proof. Let $x \in C$. Since x is integral over B, we have

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0 \tag{3.4}$$

for some $b_0, \ldots, b_{n-1} \in B$. These coefficients are integral over A, so $A' := A[b_0, \ldots, b_{n-1}] \subset C$ is an A-module of finite type. As $A'[x]$ is an A'-module of finite type by (3.4), it is an A-module of finite type by transitivity. We conclude by Proposition 3.2 with $C = A'[x]$ that x is integral over A. □

Exercise 3.10. Show that if a ring R is a UFD, then it is integrally closed in its field of fractions.

Exercise 3.11 (The Gauss lemma)**.** Let A be an integrally closed domain and let K be its field of fractions. Let $f \in A[t]$ be a monic. Suppose that $f = gh$ in $K[t]$ with $g, h \in K[t]$ monic. Show that $g, h \in A[t]$. (Hint: consider the splitting field L of f. Observe that the coefficients of g are in the ring generated by the roots of f in L, and they are integral over A.)

Exercise 3.12. A be an integrally closed domain. Show that $A[t]$ is also an integrally closed domain. (Hint: By Exercise 3.10, enough to show that $A[t]$ is integrally closed in $K[t]$ where K be the field of fraction of A. Show that if $f \in K[t]$ is integral over $A[t]$, then the constant coefficient of f is in A. Continue by induction on the degree of f.)

3.5. The geometry of numbers.

Proof of Theorem 3.1. Let $\mathcal{O}_K$ be the integral closure of $\mathbf{Z}$ in the number field K. By the primitive element theorem, there exists $\alpha \in \overline{\mathbf{Q}}$ such that $K = \mathbf{Q}[\alpha]$ in $\overline{\mathbf{Q}}$. We can assume that α is integral over $\mathbf{Z}$. Then $1, \alpha, \ldots, \alpha^{d-1}$ where $d := [K : \mathbf{Q}]$ are $\mathbf{Z}$-independent in $\mathcal{O}_K$. So the free $\mathbf{Z}$-module $\mathcal{O}_K$ has rank at least d.

Now let $x_1, \ldots, x_p$ be the real conjugates of α, and let $z_1, \overline{z_1}, \ldots, z_q, \overline{z_q}$ be the conjugates of α which are not real. For each index i, Let $\sigma_i : K \hookrightarrow \mathbf{R}$ (resp. $\tau_i : K \hookrightarrow \mathbf{C}$) be the embeddings of K sending α to x_i (resp. z_i), and let

$$\sigma = (\sigma_1, \ldots, \sigma_p, \tau_1, \ldots, \tau_q) : K \hookrightarrow \mathbf{R}^p \times \mathbf{C}^q =: V.$$

We claim that $\sigma(\mathcal{O}_K)$ is a discrete subgroup of V. Indeed, otherwise for all $\varepsilon > 0$, there exists nonzero $x \in \mathcal{O}_K$ such that $|\sigma_i(x)|, |\tau_j(x)| < \varepsilon$ for all i and j, but then e.g.

$$\sigma_1(x) \cdots \sigma_p(x)\tau_1(x)\overline{\tau_1(x)} \cdots \tau_q(x)\overline{\tau_q(x)},$$

which is the (nonzero) constant term in the minimal polynomial of x, cannot be an integer if ε is small. As $x \in \mathcal{O}_K$, its minimal polynomial has coefficients in $\mathbf{Z}$, which is a contradiction. Since $\dim_{\mathbf{R}} V = p + 2q = d$, the discreteness of $\sigma(\mathcal{O}_K)$ in $\sigma(K)$ implies that $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank at most d, and therefore equal to d. Hence $\mathcal{O}_K$ is a $\mathbf{Z}$-structure of K.

Finally, suppose that $\Lambda \subset K$ is another subring of K which is of finite type as a $\mathbf{Z}$-module. Then for any $x \in \Lambda$, the subring $\mathbf{Z}[x] \subset K$ is also a $\mathbf{Z}$-module of finite type. So x is integral over $\mathbf{Z}$ by Proposition 3.2, and thus $\Lambda \subset \mathcal{O}_K$, which proves that $\mathcal{O}_K$ is maximal. □

Problem 3.13. *What is the ring of integers of a cyclotomic field $\mathbf{Q}[\zeta_n]$?*

LECTURE 3

The geometry of rings and ideals

4. The historical origin of ideals

For a more complete treatment, see **[6]** and the references therein.

4.1. Failure of the uniqueness of factorizations. Some rings in Section 1 are not UFD. For instance in $\mathbf{Z}[\sqrt{-5}]$, we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Exercise 4.1. Show that 2 is irreducible in $\mathbf{Z}[\sqrt{-5}]$, and both $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are not divisible by 2. (Hint: consider the multiplicative norm $N(z) = |z|^2$.) When is 2 irreducible in $\mathbf{Z}[\zeta_n]$?

The ring of cyclotomic integers $\mathbf{Z}[\zeta_n]$ is a Principal Ideal Domain (PID) for $n \leq 22$, but not anymore for $n = 23$![1] For instance, the product

$$(1 + \zeta_{23}^2 + \zeta_{23}^4 + \zeta_{23}^5 + \zeta_{23}^6 + \zeta_{23}^{10} + \zeta_{23}^{11})(1 + \zeta_{23} + \zeta_{23}^5 + \zeta_{23}^6 + \zeta_{23}^7 + \zeta_{23}^9 + \zeta_{23}^{11})$$

is divisible by 2, but both factors are not. Again, since 2 is irreducible in $\mathbf{Z}[\zeta_{23}]$, the ring $\mathbf{Z}[\zeta_{23}]$ is even not a UFD.

4.2. Kummer's "ideal numbers". One of the key contributions of Kummer is the introduction of "ideal numbers" (nowadays called *ideals*), which generalize "numbers" in $\mathbf{Z}[\zeta_n]$. He also realized that contrary to numbers in $\mathbf{Z}[\zeta_n]$, any proper ideal of $\mathbf{Z}[\zeta_n]$ admits a unique factorization into prime ideals. Later, Dedekind generalized the statement to the ring of integers in any number field; we will come back to this, and viewed it as a corollary of the primary decomposition. Note that this generalization is interesting only when the ring R is not a PID.

5. Ideals and algebraic closed subsets

5.1. Zariski topology. Let $\mathbf{k}$ be an algebraically closed field. Recall that any ideal $I \subset \mathbf{k}[X_1, \ldots, X_d]$ cuts out an affine algebraic closed subset

$$Z = Z(I) := \left\{ x \in \mathbf{A}^d_{\mathbf{k}} \;\middle|\; f(x) = 0 \text{ for all } f \in I \right\}.$$

For instance, the maximal ideal

$$\mathfrak{m}_x := (X_1 - x_1, \ldots, X_d - x_d)$$

cuts out the point $x = (x_1, \ldots, x_d) \in \mathbf{A}^d_{\mathbf{k}}$, which is thus an affine algebraic closed subset.

Exercise 5.1. Prove the following statements.

(1) The empty set and $\mathbf{A}^d_{\mathbf{k}}$ are both algebraic closed subsets.

(2) For any collection of ideals $\{I_i\}_{i \in J}$ of $\mathbf{k}[X_1, \ldots, X_d]$, we have

$$Z\left(\bigcup_{i \in J} I_i\right) = \bigcap_{i \in J} Z(I_i).$$

(3) For any pair of ideals $I, J \subset \mathbf{k}[X_1, \ldots, X_d]$, we have $Z(I) \cup Z(J) = Z(IJ) = Z(I \cap J)$. Here we recall that the product $I_1 I_2$ of two ideals I_1, I_2 in a ring R is the ideal generated by $x_1 x_2$ for all $x_1 \in I_1$ and $x_2 \in I_1$.

[1] Historically, some unsuccessful attempt of proving Fermat's last theorem was based on the false belief that $\mathbf{Z}[\zeta_n]$ is always a PID.

Therefore the algebraic closed subsets of $\mathbf{A}^d_{\mathbf{k}}$ define the closed subsets of a topology on $\mathbf{A}^d_{\mathbf{k}}$, called the *Zariski topology*.

For any algebraic closed subset $Z \subset \mathbf{A}^d_{\mathbf{k}}$, the subset

$$I(Z) := \{\, f \in \mathbf{k}[X_1, \dots, X_d] \,\big|\, f(x) = 0 \text{ for all } x \in Z \,\}$$

of polynomial functions vanishing along Z form an ideal. We may then consider the quotient

$$\mathbf{k}[Z] := \mathbf{k}[X_1, \dots, X_d]/I(Z)$$

and call it *the ring of polynomial functions of* Z. This is the analogue of $\mathscr{C}^\infty(X)$ of a smooth manifold X.

Exercise 5.2. Let $Z_1, Z_2 \subset \mathbf{A}^d_{\mathbf{k}}$ be two algebraic closed subset. Show that

$$I(Z_1 \cup Z_2) = I(Z_1) \cap I(Z_2).$$

5.2. Radical. Suppose that $Z \subset \mathbf{A}^d_{\mathbf{k}}$ is the algebraic subset defined by the ideal I. Note that $I \subset I(Z)$. More generally, $I(Z)$ contains any polynomial function f such that $f^n \in I$ for some power $n \in \mathbf{Z}_{>0}$. This motivates the following definition:

Definition 5.3. Let R be a ring. For any ideal $I \subset R$, the *radical* of I is defined as

$$\sqrt{I} := \{\, f \in R \,\big|\, f^n \in I \text{ for some } n \in \mathbf{Z}_{>0} \,\}.$$

An ideal I is called *radical* if $I = \sqrt{I}$.

For instance, any prime ideal (in particular, maximal ideal) of R is radical.

Proposition 5.4. *The radical $\sqrt{I}$ of I is an ideal. More precisely, suppose that $I \neq R$. Then $\sqrt{I}$ is the intersection of the prime ideals containing I.*

Proof. Let $\mathfrak{p}$ be a prime ideal containing I. For every $f \in \sqrt{I}$, we have $f^n \in I \subset \mathfrak{p}$ for some integer $n > 0$. Since $\mathfrak{p}$ is a prime ideal, we have $f \in \mathfrak{p}$. Thus $\sqrt{I} \subset \mathfrak{p}$.

Conversely, let $f \notin \sqrt{I}$. Consider the set

$$\Sigma := \{\, J \subset R \text{ ideal } \,\big|\, I \subset J \text{ and } f^n \notin J \text{ for all integers } n > 0 \,\}.$$

ordered by inclusion. Since $\Sigma \neq \emptyset$ (because $I \in \Sigma$), by Zorn's lemma Σ has a maximal element $\mathfrak{p}$. Notice that $\mathfrak{p}$ is a prime ideal: indeed, for any $x, y \notin \mathfrak{p}$, as $\mathfrak{p}$ is maximal in Σ, we have

$$f^m \in (x) + \mathfrak{p}, \quad f^n \in (y) + \mathfrak{p}$$

for some integers $m, n > 0$. So $f^{m+n} \in (xy) + \mathfrak{p}$, showing that $xy \notin \mathfrak{p}$. Hence $\mathfrak{p}$ is a prime ideal such that $f \notin \mathfrak{p}$. □

Remark 5.5. Quite often, given a collection of ideals satisfying certain properties, the maximal ones are prime. See [**12**, Chapter 10.28] for more discussions.

Exercise 5.6. Give an elementary proof of the first statement of Proposition 5.4 without using Zorn's lemma.

Exercise 5.7. For any ideal $I \subset R$, show that $\sqrt{I} = R$ if and only if $I = R$.

5.3. Hilbert's Nullstellensatz: statement. We will see that in fact, $\sqrt{I}$ contains already all the polynomials vanishing along Z:

Theorem 5.8 (Hilbert's Nullstellensatz)**.** *We have $I(Z(I)) = \sqrt{I}$.*

As a consequence, $Z \mapsto I(Z)$ defines a one-to-one correspondence between the algebraic closed subsets $Z \subset \mathbf{A}^d_{\mathbf{k}}$ and the radical ideals of $\mathbf{k}[X_1, \dots, X_d]$.

Corollary 5.9. *Let $Z \subset \mathbf{A}^d_{\mathbf{k}}$ be an algebraic closed subset. The above correspondence induces a bijection between the points of Z and the maximal ideals of $\mathbf{k}[Z]$. Precisely, it maps $x \in Z$ to the image of $\mathfrak{m}_x$ in $\mathbf{k}[Z]$.*

Proof. We prove Corollary 5.9 for the case $Z = \mathbf{A}^d_{\mathbf{k}}$, and leave the general case as an exercise.

Let $\mathfrak{m} \subset \mathbf{k}[X_1, \ldots, X_d]$ be a maximal ideal. Since $\mathfrak{m} \neq \mathbf{k}[X_1, \ldots, X_d]$, we have $Z(\mathfrak{m}) \neq \emptyset$ by Hilbert's Nullstellensatz and Exercise 5.7. Let $x \in Z(\mathfrak{m})$. Then

$$\mathfrak{m} \subset I(Z(\mathfrak{m})) \subset I(\{x\}) \subset \mathfrak{m}_x$$

Since $\mathfrak{m}$ is maximal, necessarily $\mathfrak{m} = \mathfrak{m}_x$. Thus $\mathfrak{m} \mapsto Z(\mathfrak{m}) = \{x\}$ is the inverse of $I : x \mapsto I(\{x\}) = \mathfrak{m}_x$. □

5.4. Irreducible closed subsets and prime ideals.

Definition 5.10. An algebraic closed subset Z is called *irreducible* if Z is nonempty and

$$Z = Z_1 \cup Z_2 \quad \Rightarrow \quad (Z = Z_1 \text{ or } Z = Z_2)$$

for any algebraic closed subsets Z_1 and Z_2.

For instance, $Z(X_1X_2) = Z(X_1) \cup Z(X_2)$ is not irreducible.

Exercise 5.11. Show that the correspondence $Z \mapsto I(Z)$ induces a bijection between the irreducible algebraic closed subsets of $\mathbf{A}^d_{\mathbf{k}}$ and the prime ideals of $\mathbf{k}[X_1, \ldots, X_d]$. (Your proof should involve Hilbert's Nullstellensatz.)

We therefore have a dictionary

$$\begin{aligned} \text{Spaces} &\longleftrightarrow \text{Rings (of functions)} \\ \mathbf{A}^d_{\mathbf{k}} &\longleftrightarrow \mathbf{k}[X_1, \ldots, X_d] \\ Z &\longleftrightarrow \mathbf{k}[Z] \end{aligned}$$

as well as bijections

$$\begin{aligned} \text{In } \mathbf{A}^d_{\mathbf{k}} &\qquad \text{In } \mathbf{k}[X_1, \ldots, X_d] \\ \text{Algebraic closed subsets} &\longleftrightarrow \text{Radical ideals} \\ \text{Irreducible closed subsets} &\longleftrightarrow \text{Prime ideals} \\ \text{(Closed) points} &\longleftrightarrow \text{Maximal ideals} \end{aligned}$$

6. Affine schemes: a first definition

6.1. Spectrum.

Let R be a ring. The previous dictionary motivates the following definition.

Definition 6.1. As a set, the *spectrum* of R is defined as

$$\operatorname{Spec}(R) := \{\, \text{prime ideals of } R \,\}.$$

The *maximal spectrum* of R is defined as

$$\operatorname{Specm}(R) := \{\, \text{maximal ideals of } R \,\}.$$

Example 6.2. We still assume that $\mathbf{k}$ is algebraically closed. Let $Z \subset \mathbf{A}^d_{\mathbf{k}}$ be an algebraic closed subset. By Corollary 5.9 we have

$$\operatorname{Specm}(\mathbf{k}[Z]) = Z.$$

Example 6.3. The ideals of $\mathbf{Z}$ are

$$(0), (1), (2), \ldots$$

and

$$\operatorname{Spec}(\mathbf{Z}) = \{\, (p) \;\big|\; p \text{ prime number} \,\} \cup \{(0)\}.$$

Exercise 6.4. For $R = \mathbf{R}[X]$, show that

$$\operatorname{Spec}(\mathbf{R}[X]) = \operatorname{Specm}(\mathbf{R}[X]) \cup \{(0)\},$$

and construct a natural bijection

$$\mathrm{Specm}(\mathbf{R}[X]) = \mathbf{R} \sqcup \frac{\{z \in \mathbf{C}\backslash\mathbf{R}\}}{\text{complex conjugate}}.$$

6.2. Zariski closed subsets.

Exercise 6.5. In § 5, show that (2.3) can be rewritten as

$$Z(I) = \left\{ x \in \mathbf{k}^d \,\middle|\, I \subset \mathfrak{m}_x \right\}.$$

This motivates us to define for any ideal $I \subset R$, the subset

$$V(I) := \{ \mathfrak{p} \in \mathrm{Spec}(R) \mid I \subset \mathfrak{p} \} \subset \mathrm{Spec}(R).$$

Such subsets are called *Zariski closed subsets*. They define a topology on Spec(R) by the following exercise, called the *Zariski topology*.

As a first definition, an *affine scheme* is the data (Spec(R), R) associated to a ring R, where we regard Spec(R) as a topological space. To simplfy the notation, such data (Spec(R), R) is again denoted by Spec(R). The ring R could be interpreted as the "ring of (regular) functions" on Spec(R). For any $f \in R$ and $\mathfrak{p} \in \mathrm{Spec}(R)$, one could think of the relation $f \in \mathfrak{p}$ as "f vanishes at $\mathfrak{p}$" (or equivalently, f vanishes along $V(\mathfrak{p})$). We will explain how we "evaluate functions" after we introduce localization.

Exercise 6.6. Prove the analogous statements in Exercise 5.1 with $\mathbf{k}[X_1, \ldots, X_d]$ replaced by R and $\mathbf{A}^d_{\mathbf{k}}$ by Spec(R). Show that

$$V(I) = V(\sqrt{I})$$

for any ideal $I \subset R$.

The following statement could be regarded as the "Nullstellensatz for Spec", which always holds and is much easier then Hilbert's Nullstellensatz (for the maximal spectrum).

Exercise 6.7. Let $I \subset R$ be an ideal and let $f \in R$. Show that f vanishes at every $\mathfrak{p} \in V(I)$ if and only if $f \in \sqrt{I}$. Deduce that

$$V : \mathrm{Spec}(R) \to \{ \textit{Irreducible} \text{ Zariski closed subsets of } \mathrm{Spec}(R) \} \tag{6.1}$$

is a *bijection*.

6.3. Generic points, closed points. The following exercise shows that every irreducible Zariski closed subset of Spec(R) has a unique dense point.

Exercise 6.8. Show that the Zariski closure of $\mathfrak{p} \in \mathrm{Spec}(R)$ is $V(\mathfrak{p})$, and that $\mathfrak{p}$ is the only point of $V(\mathfrak{p})$ with this property.

We call $\mathfrak{p}$ the *generic point* of $V(\mathfrak{p})$.

Exercise 6.9. Show that a point $\mathfrak{p}$ is closed in Spec(R) if and only if $\mathfrak{p} \in \mathrm{Specm}(R)$.

Elements of Specm(R) are therefore called *closed points* of Spec(R).

Example 6.10. Let $\mathbf{k}$ be an algebraically closed field. As sets, we have

$$\mathrm{Spec}(\mathbf{k}[X_1, \ldots, X_d]) = \left\{ \text{Irreducible algebraic closed subsets of } \mathbf{A}^d_{\mathbf{k}} \right\}.$$

Let $\mathfrak{p} \in \mathrm{Spec}(\mathbf{k}[X_1, \ldots, X_d])$. Through the above description we have

$$\overline{\mathfrak{p}} = \{ \text{Irreducible algebraic closed subsets contained in } Z(\mathfrak{p}) \}$$

and

$$\overline{\mathfrak{p}} \cap \mathbf{A}^d_{\mathbf{k}} = Z(\mathfrak{p}).$$

Here is one way to draw Spec($\mathbf{k}[X, Y]$), taken from Mumford's red book **[9]**:

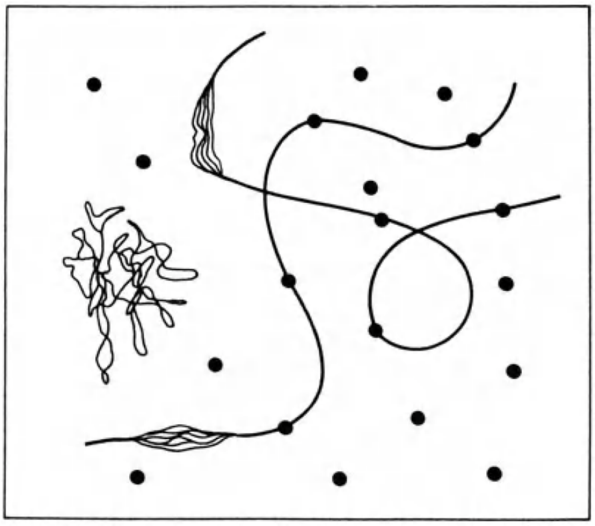

FIGURE 1. A picture of Spec$\mathbf{k}[X, Y]$ from [**9**]

In the picture, Zariski closed subsets have either dimension 0 (points), 1 (curves), or 2 (the whole plane). The "fuzzy" points represent the generic points of some irreducible Zariski closed subsets.

6.4. Spec($\mathbf{Z}$)**,** Spec$\mathbf{C}[X]$ **and** Spec$\mathbf{Z}[X]$**.**

There are two kinds of points in Spec$\mathbf{C}[X]$:

- Maximal ideals $(X - a)$, which correspond to $a \in \mathbf{C}$.
- The generic point (0) of Spec$\mathbf{C}[X]$, namely the point which is dense in Spec$\mathbf{C}[X]$.

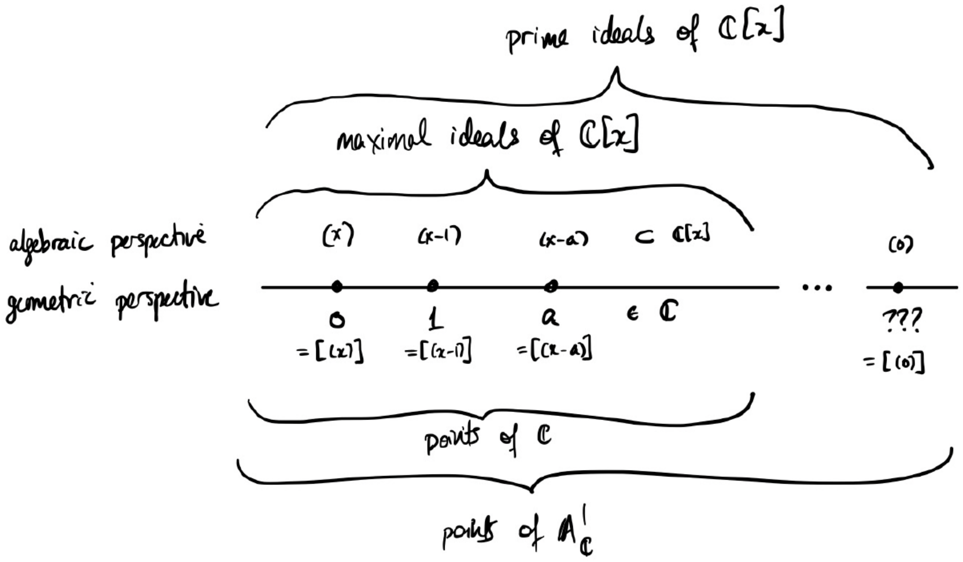

FIGURE 2. A picture of Spec$\mathbf{C}[X]$ from [**13**]

In Spec($\mathbf{Z}$), there are also two kinds of points:

- Maximal ideals (p), which corresponds to prime numbers $p \in \mathbf{Z}$.
- The generic point (0) of Spec($\mathbf{Z}$).

Therefore we may also visualize Spec($\mathbf{Z}$) as a line, just like Spec$\mathbf{C}[X]$:

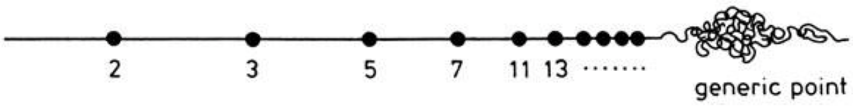

FIGURE 3. A picture of Spec($\mathbf{Z}$) from [**9**]

Exercise 6.11. Here is a picture of Spec$\mathbf{Z}[X]$, again from Mumford's red book. Explain why we draw Spec$\mathbf{Z}[X]$ this way.

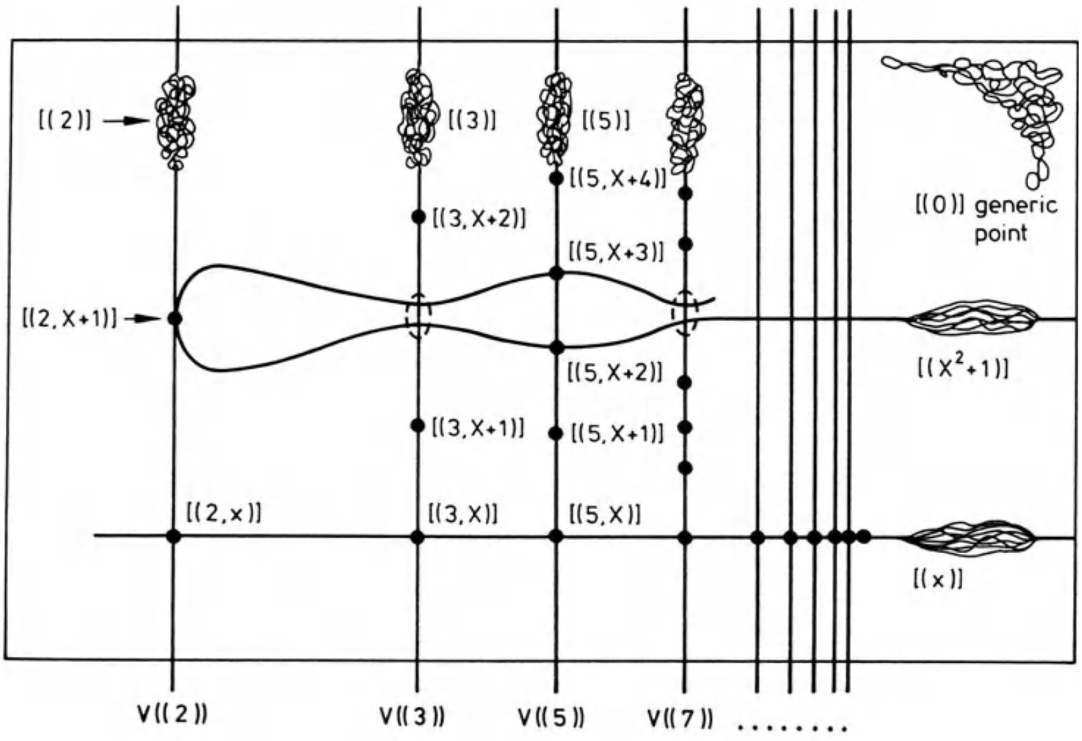

FIGURE 4. A picture of Spec$\mathbf{Z}[X]$ from [**9**]

6.5. Morphisms. Let $g = f^{\#} : A \to B$ be a ring homomorphism. Recall that the premimage $g^{-1}(I)$ of an ideal $I \subset B$ is again an ideal, and we have an induced injective ring homomorphism

$$A/g^{-1}(I) \to B/I.$$

If $I = \mathfrak{p}$ is a prime ideal, then $B/\mathfrak{p}$ is an integral domain, so $A/g^{-1}(\mathfrak{p})$ is an integral domain as well. This shows that $g^{-1}(\mathfrak{p})$ is a prime ideal of A, and we therefore have a map

$$f = g^{-1} : \text{Spec}(B) \to \text{Spec}(A).$$

Exercise 6.12. Show that f is continuous with respect to the Zariski topology.

Therefore, taking the spectrum defines a contravariant functor

$$\text{Spec} : \text{Rings} \to \text{Top}$$

from the category of rings to the category of topological spaces.

A morphism of affine schemes is the data $(f, f^{\#})$ as above. Most of the time it is simply denoted by f, but we shall keep in mind that $f^{\#}$ determines the continuous map between spectra, and not conversely.

Example 6.13. In algebraic geometry, we consider maps $\mathbf{A}^d_{\mathbf{k}} \to \mathbf{A}^n_{\mathbf{k}}$ between affine spaces defined by polynomials, i.e. of the form

$$\begin{aligned} f : \mathbf{A}^d_{\mathbf{k}} &\to \mathbf{A}^n_{\mathbf{k}} \\ x &\mapsto (P_1(x), \dots, P_n(x)). \end{aligned} \tag{6.2}$$

for some $P_1, \dots, P_n \in \mathbf{k}[X_1, \dots, X_d]$. It is induced by the homomorphism

$$\begin{aligned} f^\# : \mathbf{k}[X_1, \dots, X_n] &\to \mathbf{k}[X_1, \dots, X_d] \\ g &\mapsto g(P_1, \dots, P_n). \end{aligned} \tag{6.3}$$

Conversely, every $\mathbf{k}$-algebra morphism from $\mathbf{k}[X_1, \dots, X_n]$ to $\mathbf{k}[X_1, \dots, X_d]$ is of the form (6.3).

Exercise 6.14. Let R be a ring and let $I \subset R$ be an ideal. Show that

$$\operatorname{Spec}(R/I) \to \operatorname{Spec}(R)$$

induced by the quotient map $R \to R/I$ is homeomorphic onto $V(I)$.

Exercise 6.15. "Draw" the morphism

$$\operatorname{Spec} R[Y]/(Y^2 + 1) \to \operatorname{Spec}(R)$$

for $R = \mathbf{C}[X]$, and for $R = \mathbf{Z}$.

6.6. Reduced subscheme. The radical $\sqrt{0}$ of the zero ideal 0 of a ring R is called the *nilradical* of R, and is denoted by $\mathrm{Nil}(R)$. Elements of $\mathrm{Nil}(R)$ are called *nilpotent* elements. A ring R is called *reduced* if $\mathrm{Nil}(R) = 0$. Since $\mathrm{Nil}(R)$ is radical, the quotient

$$R_{\mathrm{red}} := R/\mathrm{Nil}(R)$$

is a reduced ring.

Exercise 6.16. Show that the morphism $\operatorname{Spec}(R_{\mathrm{red}}) \to \operatorname{Spec}(R)$ induced by the quotient $R \to R_{\mathrm{red}}$ is a homeomorphism. We call $\operatorname{Spec}(R_{\mathrm{red}})$ the *reduced subscheme* of $\operatorname{Spec}(R)$.

Remark 6.17. Although $\operatorname{Spec}(R_{\mathrm{red}})$ and $\operatorname{Spec}(R)$ are topologically indistinguishable, the scheme structure on $\operatorname{Spec}(R)$ is richer than that on $\operatorname{Spec}(R_{\mathrm{red}})$ (informally, because there are more functions over $\operatorname{Spec}(R)$ than over $\operatorname{Spec}(R_{\mathrm{red}})$). For instance, let $\mathbf{k}$ be a field. Then both $\operatorname{Spec}(\mathbf{k})$ and $\operatorname{Spec} \mathbf{k}[\varepsilon]/(\varepsilon^2)$ are topologically a point. Now assume that $\mathbf{k}$ is algebraically closed, and let $Z \subset \mathbf{A}^d_{\mathbf{k}}$ be an algebraic closed subset together with a closed point $x \in Z$. Then the evaluation map $\mathrm{ev}_x : \mathbf{k}[Z] \to \mathbf{k}$ at x is only $\mathbf{k}$-morphism such that the image of the induced morphism

$$\operatorname{Spec}(\mathbf{k}) \to \operatorname{Spec} \mathbf{k}[Z]$$

is x. On the other hand, there are in general many $\mathbf{k}$-morphisms $\mathbf{k}[Z] \to \mathbf{k}[\varepsilon]/(\varepsilon^2)$ having the same property. Later in this course or in the course of algebraic geometry, you will see that such morphisms

$$\operatorname{Spec} \mathbf{k}[\varepsilon]/(\varepsilon^2) \to \operatorname{Spec} \mathbf{k}[Z]$$

correspond to tangent vectors of Z at x (therefore contains more information then just $x \hookrightarrow Z$).

Remark 6.18. The functor $R \mapsto R_{\mathrm{red}}$ from the category of rings to the category of reduced rings is surjective on objects. It follows from the universal property of quotient rings that this functor is left adjoint to the inclusion functor.

6.7. Affine varieties. Let $\mathbf{k}$ be a field. An *affine* $\mathbf{k}$*-variety* is the spectrum $\operatorname{Spec}(R)$ of a finitely generated $\mathbf{k}$-algebra R such that R is reduced.

Exercise 6.19. Suppose that $\mathbf{k}$ is algebraically closed. Show that

$$\begin{aligned} \{\text{ Affine } \mathbf{k}\text{-varieties }\} &\xrightarrow{\sim} \left\{ \text{Affine algebraic closed subsets (in some } \mathbf{A}^n_{\mathbf{k}}) \right\} \\ \operatorname{Spec}(R) &\mapsto \operatorname{Specm}(R). \end{aligned}$$

is a bijection

We will see that affine **k**-varieties satisfy some non-trivial geometric properties that we expect to hold at an intuitive level (see *e.g.* Lecture 6, Sections 19 and 20).

6.8. Absolute versus relative. Any ring is naturally a **Z**-algebra. Precisely, the forgetful functor

$$\mathbf{Z}\text{-Alg} \to \text{Ring}$$

from the category of **Z**-algebras to the category of rings is an equivalence. So the study of rings is contained in the study of *R-algebras* with R varying among rings. Statements for R-algebras are therefore more precise and general than the same statements for rings.

Dually, the the study of schemes is contained in the study of schemes equipped with a morphism to some fixed schemes S. Such data are called *S-schemes*. We qualify statements concerning S-schemes as *relative*, and statements concerning schemes (or equivalently when $S = \text{Spec}(\mathbf{Z})$) as *absolute*.

LECTURE 4

Tensor products

7. Tensor products

Let's start with three facets of tensor products before we construct them.

7.1. First facet: extension of scalars. Let V be a vector space of dimension d over a field K. If we choose a basis $e_1, \dots, e_d$ of V, then every element of V is a linear combination of the e_i's with coefficients in K, which gives a K-linear isomorphism

$$V \simeq \oplus_{i=1}^{d} K \cdot e_i.$$

Now let L/K be a field extension. The tensor product

$$V_L := V \otimes_K L$$

that we will define can be understood as the extension of scalars. With the above chosen basis $e_1, \dots, e_d$, there exists a canonical isomorphism

$$V_L \simeq \oplus_{i=1}^{d} L \cdot e_i,$$

through which V_L can be described as an L-vector space having the same basis elements as V, but replacing the coefficient field with L. If we have a K-linear map $\phi : U \to V$ between K-vector spaces, it also extends to an L-linear map

$$\phi_L : U_L \to V_L$$

defined by the same matrix.

7.2. Universal property of extension of scalars. We also notice that if V is a K-vector space and W is an L-vector space, then any K-linear map $\psi : V \to W$ has a unique L-linear extension $\tilde{\psi} : V_L \to W$. This motivates us to define extension of scalars as follows.

Theorem-Definition 7.1 (Universal property of extension of scalars)**.** *Let A be a ring and let B be an A-algebra. Let M be an A-module. There exists a B-module $M \otimes_A B$, together with an A-linear map*

$$\phi : M \to M \otimes_A B,$$

satisfying the following universal property: for any A-linear map $\psi : M \to N$ to some B-module N, there exists a unique B-linear map $\tilde{\psi} : M \otimes_A B \to N$ such that

$$\begin{tikzcd} M \arrow[r, "\forall\, \psi"] \arrow[dr, "\phi"'] & N \\ & M \otimes_A B \arrow[u, "\exists!\, \tilde{\psi}"'] \end{tikzcd}$$

commutes. Moreover, the pair $(M \otimes_A B, \phi)$ is unique up to unique isomorphism. We call $M \otimes_A B$ the B-module obtained from M by extension of scalars.

7.3. Second facet: fiber product of affine schemes. Let R be a ring and let A be an R-algebra. This gives rise to a structural morphism of affine scheme

$$\mathrm{Spec}(A) \to \mathrm{Spec}(R)$$

making $\mathrm{Spec}(A)$ an *affine scheme over* $\mathrm{Spec}(R)$.

Through the functor Spec, showing that fiber products exist in the category of affine schemes over R is equivalent to showing that *fiber coproducts* exist in the category of R-algebras. Tensor products of R-algebras provide the answer.

Theorem-Definition 7.2 (Universal property of tensor products of algebras)**.** *Let A be a ring and let B, C be A-algebras. There exists an A-module $B \otimes_A C$, together with morphisms of A-algebras $\phi_B : B \to B \otimes_A C$ and $\phi_C : C \to B \otimes_A C$, which satisfy the following universal property: for any pair of morphisms of A-algebras ψ_1, ψ_2 as in the diagram, there exists a unique morphism of A-algebras $\psi : B \otimes_A C \to Z$ such that*

$$\begin{tikzcd}
 & & Z \\
B \arrow[r, "\phi_B"'] \arrow[urr, bend left, "\forall\psi_1"] & B \otimes_A C \arrow[ur, "\exists!\psi"'] & \\
A \arrow[u] \arrow[r] & C \arrow[u, "\phi_C"] \arrow[uur, bend right, "\forall\psi_2"'] &
\end{tikzcd}$$

commutes. Moreover, the triple $(B \otimes_A C; \phi_B, \phi_C)$ is unique up to unique isomorphism. We call $B \otimes_A C$ the tensor product of B and C over A.

Therefore if $\mathrm{Spec}(A)$ and $\mathrm{Spec}(B)$ are affine schemes over R, we can define the product as

$$\mathrm{Spec}(A) \times_{\mathrm{Spec}(R)} \mathrm{Spec}(B) = \mathrm{Spec}(A \otimes_R B).$$

7.4. Third facet: linearization of bilinear maps.

Theorem-Definition 7.3 (Universal property of tensor products of modules)**.** *Let M and N be two R-modules. There exists an R-module $M \otimes_R N$, together with an R-bilinear map*

$$\phi : M \times N \to M \otimes_R N,$$

satisfying the following universal property: for any R-bilinear map $\psi : M \times N \to L$ to some R-module L, there exists a unique R-linear map $\tilde{\psi} : M \otimes_R N \to L$ such that

$$\begin{tikzcd}
M \times N \arrow[r, "\forall\psi"] \arrow[dr, "\phi"'] & L \\
 & M \otimes_R N \arrow[u, "\exists!\tilde{\psi}"']
\end{tikzcd}$$

commutes. Moreover, the pair $(M \otimes_R N, \phi)$ is unique up to unique isomorphism. The R-module $M \otimes_R N$ is called the tensor product of M and N over R.

7.5. Construction of tensor products of modules. Now we start the constructions, and consider first Theorem 7.3. Since we want $\phi : M \times N \to M \otimes_R N$ to be R-bilinear, we just define the R-module $M \otimes_R N$ straightforwardly by generators and relations as follows:

- Generators: $m \otimes n$ for all $m \in M$ and $n \in N$.
- The R-submodule of relations $\mathscr{R}$ is generated by

$$(m + m') \otimes n = m \otimes n + m' \otimes n, \qquad m \otimes (n + n') = m \otimes n + m \otimes n',$$

$$(rm) \otimes n = m \otimes (rn) = r(m \otimes n),$$

for all $m, m' \in M$, $n, n' \in N$, and $r \in R$.

Namely,

$$M \otimes_R N := \left(\bigoplus_{m \in M, n \in N} R \cdot (m \otimes n) \right) \Big/ \mathscr{R}.$$

For every $m \in M$ and $n \in N$, we still use $m \otimes n$ to denote its image in $M \otimes_R N$. Elements in $M \otimes_R N$ of the form $m \otimes n$ are called *pure tensors*, or *simple tensors*.

Exercise 7.4. Prove Theorem 7.3.

Given a finite number of R-modules $M_1, \ldots, M_n$, we define the tensor product

$$M_1 \otimes_R \cdots \otimes_R M_n$$

in a similar way. It satisfies a similar universal property, replacing bilinear maps with multilinear maps.

Exercise 7.5. Let M, N, L be R-modules. Show that we have canonical isomorphisms

- $R \otimes_R M \xrightarrow{\sim} M$,
- $M \otimes_R N \xrightarrow{\sim} N \otimes_R M$,
- $(M \otimes_R N) \otimes_R L \xrightarrow{\sim} M \otimes_R (N \otimes_R L)$,
- $(M \oplus N) \otimes_R L \xrightarrow{\sim} (M \otimes_R L) \oplus (N \otimes_R L)$,

defined by $r \otimes m \mapsto rm$, $\quad m \otimes n \mapsto n \otimes m$, etc.

7.6. Constructions of other tensor products. Now we consider Theorems 7.1 and 7.2. In the setting of Theorem 7.1, the previous construction defines $M \otimes_A B$ as an A-module. We define the B-module structure on $M \otimes_A B$ by

$$b' \cdot (m \otimes b) := m \otimes (b'b)$$

for any pure tensor $m \otimes b$ and any $b' \in B$, then extend linearly.

Exercise 7.6. Show that the B-module structure on $M \otimes_A B$ is well-defined and satisfies the universal property in Theorem 7.1.

Likewise for Theorem 7.2, we define the ring structure (i.e. the product) on $B \otimes_A C$ by

$$(b \otimes c) \cdot (b' \otimes c') := (bb') \otimes (cc')$$

for pure tensors $b \otimes c$ and $b' \otimes c'$, then extend linearly. Define

$$\begin{aligned} s : A &\to B \otimes_A C \\ a &\mapsto a \cdot (1 \otimes 1). \end{aligned}$$

Exercise 7.7. Show that s defines an A-algebra structure on $B \otimes_A C$. Prove Theorem 7.2.

7.7. Tensor product of morphisms. Let M_1, M_2, N_1, N_2 be R-modules. For any R-linear morphisms $f : M_1 \to M_2$ and $g : N_1 \to N_2$, we have a well-defined R-linear map

$$f \otimes g : M_1 \otimes_R N_1 \to M_2 \otimes_R N_2$$

defined by $(f \otimes g)(m \otimes n) \to f(m) \otimes g(n)$ on pure tensors, then extend by linearity. In particular for any R-module, this defines an endofunctor

$$\bullet \otimes_R N : \mathrm{Mod}_R \to \mathrm{Mod}_R$$

on the category of R-modules, sending an R-module M to $M \otimes_R N$, and $f \in \mathrm{Hom}_R(M_1, M_2)$ to $f \otimes \mathrm{Id}_N$.

Similarly let A be a ring and let B be an A-algebra. Taking tensor product defines a functor

$$\bullet \otimes_A B : \mathrm{Mod}_A \to \mathrm{Mod}_B$$

from the category of A-modules to the category of B-modules.

8. Properties of tensor products

8.1. Restriction and extension of scalars. Let A be a ring and let $\phi : A \to B$ be an A-algebra. Any B-module M has an induced A-module structure, defined by

$$a \cdot m := \phi(a) \cdot m$$

for every $a \in A$ and $m \in M$. As a morphism of B-modules is naturally a morphism of A-modules, we thus have a functor

$$\mathrm{Mod}_B \to \mathrm{Mod}_A$$

from the category of B-modules to the category of A-modules, called the *restriction of scalars* (or the *forgetful functor*).

The restriction of scalars and the extension of scalars are related as follows.

Exercise 8.1. Show that the extension of scalars and the restriction of scalars form an adjoint pair: namely there exist natural (to be defined below) bijections

$$\mathrm{Hom}_B(M \otimes_A B, N) \simeq \mathrm{Hom}_A(M, N)$$

for any A-module M and B-module N. (Hint: use the universal property.)

In general, given a pair of functors $F : \mathscr{C} \to \mathscr{D}$ and $G : \mathscr{D} \to \mathscr{C}$, we say (F, G) forms an adjoint pair if for every object $X \in \mathscr{C}$ and $Y \in \mathscr{D}$, there exist bijections

$$\alpha_{X,Y} : \mathrm{Hom}_{\mathscr{D}}(F(X), Y) \xrightarrow{\sim} \mathrm{Hom}_{\mathscr{C}}(X, G(Y))$$

which are natural, in the sense that for any morphism $g : Y \to Y'$ in $\mathscr{D}$, the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathscr{D}}(F(X), Y) \arrow[r, "\alpha_{X,Y}"] \arrow[d, "g\circ"'] & \mathrm{Hom}_{\mathscr{C}}(X, G(Y)) \arrow[d, "G(g)\circ"] \\
\mathrm{Hom}_{\mathscr{D}}(F(X), Y') \arrow[r, "\alpha_{X,Y'}"] & \mathrm{Hom}_{\mathscr{C}}(X, G(Y'))
\end{tikzcd}$$

commutes, and same for the similar diagram defined for any morphism $f : X \to X'$ in $\mathscr{C}$. We also say that F is left-adjoint to G, and G is right-adjoint to F.

8.2. Aside 1: Un éventail infini de variétés. Consider an algebraic closed subset Z of $\mathbf{A}^n_{\mathbf{C}}$ defined by an ideal $I \subset \mathbf{Z}[X_1, \ldots, X_n]$ of polynomials with *integer* coefficients. For each prime number p, we may consider the same collection of defining polynomials, and consider their coefficients modulo p. This defines another algebraic closed subset Z_p of in the affine space $\mathbf{A}^n$ over $\overline{\mathbf{F}_p}$.

The theory of schemes provides a way to fit them together. Let's consider instead the affine scheme

$$X = \mathrm{Spec}\mathbf{Z}[X_1, \ldots, X_n]/I.$$

Since *any ring* R is naturally a $\mathbf{Z}$-algebra, we have cartesian squares

$$\begin{tikzcd}
X_R \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & X \arrow[d] \\
\mathrm{Spec}(R) \arrow[r] & \mathrm{Spec}(\mathbf{Z})
\end{tikzcd}$$

When $R = \mathbf{C}$, this turns X into a complex subscheme of $\mathbf{A}^n_{\mathbf{C}}$. When $R = \mathbf{F}_p$, we obtain the reduction modulo p of X.

In general, if $f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is a morphism of affine schemes and $I \subset A$ is an ideal, then the *fiber* of f over the closed subscheme $\mathrm{Spec}(A/I) \subset \mathrm{Spec}(A)$ is

$$\mathrm{Spec}(B \otimes_A (A/I)) = \mathrm{Spec}(B/IB) \subset \mathrm{Spec}(B).$$

8.3. Aside 2: restricted and induced representations. Let G be a group acting on a vector space V over a field $\mathbf{k}$. This defines a structure of left $\mathbf{k}[G]$-module on V, and we have an equivalence of categories

$$G\text{-Rep}/\mathbf{k} \simeq \mathrm{Mod}_{\mathbf{k}[G]}$$

between the category of G-representations over $\mathbf{k}$ and the category of right $\mathbf{k}[G]$-modules.

Extension and restriction of scalars can be defined for right modules over noncommutative rings. If we take a subgroup $H \leq G$, then the restriction of scalars to $\mathbf{k}[H]$ and the extension of scalars $\otimes_{\mathbf{k}[H]}\mathbf{k}[G]$ on the right hand side correspond on the left hand side to taking the restricted and the induced representations.

8.4. $\otimes$ and Hom**.** Tensor product of modules is related to the Hom-functor also by means of adjoint pair.

Let N be an R-module. For any R-module L, let $\mathrm{Hom}_R(N, L)$ be the space of R-linear maps from N to L. We regard $\mathrm{Hom}_R(N, L)$ as an R-module defined by $(r\phi)(x) := r\phi(x)$ for any $r \in R$, $\phi \in \mathrm{Hom}_R(N, L)$, and $x \in N$. We then have a covariant functor

$$\mathrm{Hom}_R(N, \bullet) : \mathrm{Mod}_R \to \mathrm{Mod}_R$$

sending L to $\mathrm{Hom}_R(N, L)$, and a morphism $\phi : L \to L'$ to

$$\phi\circ : \mathrm{Hom}_R(N, L) \to \mathrm{Hom}_R(N, L').$$

Likewise, we have a contravariant functor $\mathrm{Hom}_R(\bullet, N)$.

Exercise 8.2. Let M be an R-module. Show that $\bullet \otimes_R M$ is left adjoint to $\mathrm{Hom}_R(M, \bullet)$: namely there exist natural bijections

$$\mathrm{Hom}_R(L \otimes_R M, N) \simeq \mathrm{Hom}_R(L, \mathrm{Hom}_R(M, N))$$

for any R-modules L and N.

Note that $\mathrm{Hom}_R(L, \mathrm{Hom}_R(M, N))$ can also be identified as the R-modules of R-bilinear maps

$$L \times M \to N.$$

In particular when $N = R$, it follows that the space of R-bilinear form on $L\times M$ is isomorphic to $(L\otimes_R M)^\vee$. Here $M^\vee := \mathrm{Hom}_R(M, R)$ (called the *dual* of M) for any R-module M.

Exercise 8.3. Do we have natural bijections $\mathrm{Hom}_R(L, M \otimes_R N) \simeq \mathrm{Hom}_R(\mathrm{Hom}_R(L, M), N))$ for any R-modules L, M, N?

8.5. Tensor product is right-exact. Let R be a ring and let M be an R-module. What is $M \otimes_R (R/I)$ for an ideal $I \subset R$?

Let

$$\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \to \cdots$$

be a (finite or infinite) sequence of morphisms of R-modules. We say that the sequence is *exact* if

$$\mathrm{Im}(f_{i-1}) = \ker(f_i)$$

for all index i. For instance, saying that the sequence of R-modules

$$M'' \xrightarrow{f} M' \xrightarrow{g} M \to 0$$

is exact means that we can identify M as M' quotient by the relations $f(M'')$.

Proposition 8.4. *Let N be an R-module. For any exact sequence*

$$M'' \xrightarrow{f} M' \xrightarrow{g} M \to 0 \tag{8.1}$$

of R-modules the induced sequence

$$M'' \otimes_R N \xrightarrow{f\otimes\mathrm{Id}} M' \otimes_R N \xrightarrow{g\otimes\mathrm{Id}} M \otimes_R N \to 0$$

is also exact.

We may interpret Proposition 8.4 as follows: after tensoring N, the module $M' \otimes_R N$ still generated $M \otimes_R N$, and the relations are precisely those induced by the relations before tensoring N.

Proof. From the exactness of (8.1), it is clear that $g \otimes \mathrm{Id}$ is surjective. Now consider the R-linear map

$$\phi : M \otimes_R N \to \frac{M' \otimes_R N}{\mathrm{Im}(f \otimes \mathrm{Id})}$$

defined by $m \otimes n \mapsto m' \otimes n$ on pure tensors, where m' is any element of $g^{-1}(m)$. The exactness of (8.1) again implies that ϕ is well-defined. By construction, ϕ is the inverse of $g \otimes \mathrm{Id}$ on pure tensors, so $g \otimes \mathrm{Id} = \phi^{-1}$ by R-linearlity. Hence $\mathrm{Im}(f \otimes \mathrm{Id}) = \ker(g \otimes \mathrm{Id})$. □

Proposition 8.4 implies the following useful isomorphism.

Exercise 8.5. Let M be an R-module and let $I \subset R$ be an ideal. Show that

$$M \otimes_R (R/I) \simeq M/IM$$

as R/I-modules. Similarly, if A is an R-algebra, show that

$$A \otimes_R (R/I) \simeq A/IA$$

as A-algebras.

Remark 8.6. Left (resp. right) adjoint functors between abelian categories are always right-exact (resp. left-exact).

9. Tensor algebras

Let R be a ring and let M be an R-module.

9.1. Tensor algebras. For every $n \in \mathbf{Z}_{\geq 0}$, we define inductively

$$T^0(M) := R, \quad T^n(M) := T^{n-1}(M) \otimes_R M$$

and let

$$T(M) := \bigoplus_{n=0}^{\infty} T^n(M).$$

We define product on $T(M)$, first for pure tensors by

$$(x_1 \otimes \cdots \otimes x_i) \cdot (y_1 \otimes \cdots \otimes y_j) = (x_1 \otimes \cdots \otimes x_i \otimes y_1 \otimes \cdots \otimes y_j),$$

then extend by linearity. We can therefore consider $T(M)$ as a *noncommutative* graded R-algebra, and call it the tensor algebra associated to M.

9.2. Symmetric and exterior algebras.

Theorem-Definition 9.1 (Universal property of symmetric and exterior powers)**.** *Let M be an R-module. Let n be a positive integer. There exists an R-module N together with an R-multilinear symmetric (resp. alternating) map*

$$\phi : M^n \to N$$

which satisfies the following universal property: for any symmetric (resp. alternating) R-multilinear map $\psi : M^n \to L$ to some R-module L, there exists a unique R-linear map $\tilde{\psi} : N \to L$ such that

$$\begin{tikzcd} M^n \arrow[r, "\forall\psi"] \arrow[dr, "\phi"'] & L \\ & N \arrow[u, "\exists!\tilde{\psi}"'] \end{tikzcd}$$

commutes. Moreover, the pair (N, ϕ) is unique up to unique isomorphism. The R-module N is called the symmetric power *(resp. the* exterior power*) of M over R, and is denoted* $\mathrm{Sym}^n M$ *(resp. $\bigwedge^n M$).*

The symmetric algebra associated to an R-module M is defined as

$$\mathrm{Sym}(M) := \frac{T(M)}{<x \otimes y - y \otimes x \mid x, y \in M>},$$

where the denominator is the two-sided ideal generated by all the $x \otimes y - y \otimes x$.

Exercise 9.2. Show that the grading on $T(M)$ induces a grading $\oplus_i \mathrm{Sym}^i(M)$ on $\mathrm{Sym}(M)$, and that $\mathrm{Sym}(M)$ is a *commutative* graded R-algebra. Show that the composition

$$\phi : M^n \to T^n(M) \to \mathrm{Sym}^n(M)$$

satisfies the universal property in Theorem 9.1.

Exercise 9.3. Show that $\mathrm{Sym}(M)$ satisfies the following universal property. For any R-linear map $\psi : M \to L$ to some R-algebra L, there exists a unique R-linear map $\tilde{\psi} : \mathrm{Sym}(M) \to L$ such that

$$\begin{tikzcd} M \arrow[r, "\forall\psi"] \arrow[dr, "\phi"'] & L \\ & \mathrm{Sym}(M) \arrow[u, "\exists!\tilde{\psi}"'] \end{tikzcd}$$

commutes.

The image of a pure tensor $x_1 \otimes \cdots \otimes x_n$ in $\mathrm{Sym}^n(M)$ is denoted by

$$x_1 \cdots x_n.$$

When $n!$ is invertible in R, the quotient $q : T^n(M) \to \mathrm{Sym}^n(M)$ splits: the map defined by

$$x_1 \cdots x_n \mapsto \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}$$

extends to a morphism of R-modules $\imath : \mathrm{Sym}^n(M) \to T^n(M)$ such that $q \circ \imath$ is the identity.

Exercise 9.4. Let V be a vector space over a field $\mathbf{k}$ of finite dimension n. Show that there is an isomorphism

$$\mathrm{Sym}(V) \simeq \mathbf{k}[X_1, \ldots, X_n]$$

as graded $\mathbf{k}$-algebras.

The exterior algebra associated to an R-module M is defined as

$$\bigwedge M := \frac{T(M)}{<x \otimes x \mid x \in M>},$$

where the denominator is the two-sided ideal generated by all the $x \otimes x$.

Exercise 9.5. Likewise, show that the grading on $T(M)$ induces a grading $\oplus_i \bigwedge^i M$ on $\bigwedge M$, and that $\bigwedge M$ is a *graded-commutative* graded R-algebra: namely, for every $a \in \bigwedge^i M$ and $b \in \bigwedge^j M$, we have

$$b \wedge a = (-1)^{ij} a \wedge b,$$

where $\wedge$ is the product on $\bigwedge M$. Show that the composition

$$\phi : M^n \to T^n(M) \to \bigwedge^n M$$

satisfies the universal property in Theorem 9.1.

The image of a pure tensor $x_1 \otimes \cdots \otimes x_n$ in $\bigwedge^n(M)$ is denoted by

$$x_1 \wedge \cdots \wedge x_n.$$

When $n!$ is invertible in R, the map defined by

$$x_1 \wedge \cdots \wedge x_n \mapsto \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}$$

extends to a morphism of R-modules $\bigwedge^n M \to T^n(M)$ and defines a splitting of the quotient $q : T^n(M) \to \bigwedge^n M$.

Exercise 9.6. Let K be a field and let V be a K-vector space. Construct a natural K-linear identification between $\mathrm{Sym}^n(V^\vee)$ (resp. $\bigwedge^n V^\vee$) and the space of symmetric (resp. alternating) multilinear forms on V.

LECTURE 5

Localizations

10. Localizations

Let R be a ring.

10.1. Some guiding principle. A subset $S \subset R$ is called *multiplicative* if

- $1 \in S$;
- $a, b \in S$ implies $ab \in S$.

Given such a subset $S \subset R$, we want to define a ring of fractions $S^{-1}R$ where elements of S are formally inverted, namely elements of $S^{-1}R$ are of the form r/s with $r \in R$ and $s \in S$. When R is an integral domain and $S = R - \{0\}$, we want $S^{-1}R = \mathrm{Frac}(R)$.

When R is an integral domain, naturally we want two fractions r/s and r'/s' to be equal in $S^{-1}R$ if and only if they satisfy their "cross-multiplications" are equal, namely $rs' - r's = 0$. In general, it may happen that some $s \in S$ is annihilated by some nonzero $r \in R$, and we want

$$\frac{r}{1} = \frac{0}{s} = 0 = \frac{0}{s'} \in S^{-1}R.$$

for any other $s' \in S$ (for instance $s' = 1$). In general we don't have $r \cdot s' - 0 \cdot 1 = 0$, but rather

$$r \cdot s' - 0 \cdot 1 = \frac{0}{s}.$$

Therefore when R is an arbitrary ring (which might contain zero divisors), it is more natural to consider the condition

$$r/s = r'/s' \Leftrightarrow rs' - r's = \frac{0}{t} \quad \text{for some } t \in S,$$

namely $rs' - r's$ equals to some representative of zero.

Finally, the addition and multiplication of fractions should follow the usual rules.

10.2. Localization of rings and modules. As a set, the *localization* of R by a multiplicative subset $S \subset R$ is

$$S^{-1}R = (R \times S)/\sim,$$

where $\sim$ is the equivalence relation defined as

$$(r, s) \sim (r', s') \Leftrightarrow t(s'r - sr') = 0 \text{ for some } t \in S.$$

The image of (r, s) in $S^{-1}R$ is also commonly denoted by r/s. Given $r/s, r'/s' \in S^{-1}R$, we define

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

Exercise 10.1. Verify that $\sim$ is indeed an equivalence relation, and that $(S^{-1}R, +, \cdot)$ is a ring. Show that the localization map $R \to S^{-1}R$ sending r to $r/1$ defines an R-algebra structure on $S^{-1}R$.

Let M be an R-module and let $S \subset R$ be a multiplicative subset. The localization $S^{-1}M$ of M is an $S^{-1}R$-module defined similarly, with R replaced by M everywhere in the above definition, except that

$$\frac{r}{s} \cdot \frac{m}{s'} = \frac{rm}{ss'}$$

is for every $r/s \in S^{-1}R$ and every $m/s' \in S^{-1}M$. Likewise, the localization map $M \to S^{-1}M$ sending m to $m/1$ is a morphism of R-modules. By construction,

$$\ker(M \to S^{-1}M) = \{\, m \in M \mid sm = 0 \text{ for some } s \in S \,\}.$$

Exercise 10.2. Show that $S^{-1}R = 0$ if and only if $0 \in S$.

Exercise 10.3. Show that the an R-module N is in the image of the forgetful functor

$$\mathrm{Mod}_{S^{-1}R} \to \mathrm{Mod}_R$$

if and only if the multiplication $s : N \circlearrowleft$ by any $s \in S$ is an automorphism.

10.3. The universal property. Let $S \subset R$ be a multiplicative subset.

Proposition 10.4 (Universal property of localizations of rings)**.** *For every ring homomorphism $\psi : R \to A$ from R such that $\psi(s)$ is invertible for all $s \in S$, there exists a unique ring homomorphism $\tilde{\psi} : S^{-1}R \to A$ such that*

$$\begin{tikzcd}
R \arrow[r, "\forall\psi"] \arrow[dr, "localization"'] & A \\
& S^{-1}R \arrow[u, "\exists!\tilde{\psi}"']
\end{tikzcd}$$

commutes.

As a consequence, if $R \to A$ is an R-algebra, then the universal property provides a natural $S^{-1}R$-algebra structure on $S^{-1}A$.

Proposition 10.5 (Universal property of localizations of modules)**.** *Let M be an R-module. For every $S^{-1}R$-module N and every morphism of R-modules $\psi : M \to N$, there exists a unique morphism of $S^{-1}R$-modules $\tilde{\psi} : S^{-1}M \to N$ such that*

$$\begin{tikzcd}
M \arrow[r, "\forall\psi"] \arrow[dr, "localization"'] & N \\
& S^{-1}M \arrow[u, "\exists!\tilde{\psi}"']
\end{tikzcd}$$

commutes.

Exercise 10.6. Prove the above universal properties.

For any morphism of R-modules $f : M \to N$, the universal property yields a morphism of $S^{-1}R$-modules $S^{-1}f : S^{-1}M \to S^{-1}N$ such that

$$\begin{tikzcd}
S^{-1}M \arrow[r, "S^{-1}f"] & S^{-1}N \\
M \arrow[u] \arrow[r, "f"] & N \arrow[u]
\end{tikzcd}$$

commutes; explicitly,

$$(S^{-1}f)(m/s) = f(m)/s.$$

Thus the localization defines a functor

$$S^{-1} : \mathrm{Mod}_R \to \mathrm{Mod}_{S^{-1}R}$$

from the category of R-modules to itself. If $f : A \to B$ is a morphism of R-algebra, then the localization $S^{-1}f : S^{-1}A \to S^{-1}B$ is also a morphism of $S^{-1}R$-algebra.

Exercise 10.7. Let $S \subset T \subset R$ be multiplicative subsets. Show that the localization

$$T^{-1}M \xrightarrow{\sim} T^{-1}(S^{-1}M)$$

of the localization map $M \to S^{-1}M$ by T is is an isomorphism of $T^{-1}R$-modules.

10.4. Localization as extension of scalars.

Exercise 10.8. For any R-module M and any multiplicative subset $S \subset R$, show that

$$M \otimes_R S^{-1}R \xrightarrow{\sim} S^{-1}M$$

sending $m \otimes (r/s)$ to rm/s is well defined and is an isomorphism of $S^{-1}R$-modules. (Hint: compare the universal properties of both sides and use Exercise 10.3.)

In particular, the localization functor $S^{-1} : \mathrm{Mod}_R \to \mathrm{Mod}_{S^{-1}R}$ is left adjoint to the forgetful functor.

Exercise 10.9. Show that

$$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \xrightarrow{\sim} S^{-1}(M \otimes_R N)$$

sending $(m/r) \otimes (n/s)$ to $(m \otimes n)/rs$ is an isomorphism of $S^{-1}R$-modules.

10.5. Exacteness of localizations.

Proposition 10.10. *Let*

$$L \xrightarrow{f} M \xrightarrow{g} N$$

be an exact sequence of R-modules. The induced sequence

$$S^{-1}L \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}N$$

is exact as well.

Proof. Since S^{-1} is a functor, we have $(S^{-1}g) \circ (S^{-1}f) = 0$. Now suppose that $(S^{-1}g)(n/s) = g(n)/s = 0$, then $g(tn) = tg(n) = 0$ for some $t \in S$. So $tn = f(m)$ for some $m \in M$. Thus $n/s = f(m)/ts = (S^{-1}f)(m/ts)$. □

In particular, the localization of a submodule is still a submodule, and localization commutes with taking quotient.

Exercise 10.11. Let $I \subset R$ be an ideal. Show that we have a ring isomorphism

$$S^{-1}(R/I) \xrightarrow{\sim} (S^{-1}R)/IS^{-1}R$$

which identifies $S^{-1}R \to S^{-1}(R/I)$ and the quotient map $S^{-1}R \to (S^{-1}R)/IS^{-1}R$.

Exercise 10.12. Let M be an R-module. The map

$$S^{-1} : \{\text{ submodules of } M \} \to \left\{ \text{submodules of } S^{-1}M \right\}$$

is surjective. More precisely, for any submodule $N \subset S^{-1}M$, if $\phi : M \to S^{-1}M$ is the localization map, then

$$S^{-1}(\phi^{-1}(N)) = N.$$

In particular,

$$\left\{ \text{ideals of } S^{-1}R \right\} = \left\{ I \cdot S^{-1}R \;\middle|\; I \text{ ideal of } R \right\}.$$

Proposition 10.13. *The localization map $\phi : R \to S^{-1}R$ induces a homeomorphism*

$$\mathrm{Spec}(S^{-1}R) \xrightarrow{\sim} \{\, \mathfrak{p} \in \mathrm{Spec}(R) \;\big|\; \mathfrak{p} \cap S = \emptyset \,\}$$

where the target is endowed with the topology induced from Spec(R).

Proof. We only show that the map is bijective.

To show that the map is well defined and injective, it suffices by Exercise 10.12 to show that for any prime ideal $\mathfrak{p}'$ of $S^{-1}R$, we have $\phi^{-1}(\mathfrak{p}') \cap S = \emptyset$. Suppose that $s \in \phi^{-1}(\mathfrak{p}') \cap S$, then $\phi(s) \in \mathfrak{p}'$ is a unit of $S^{-1}R$, which is impossible.

Let $\mathfrak{p}$ be a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$. Let $a/s, b/t \in S^{-1}R$ such that $ab/st \in \mathfrak{p} \cdot S^{-1}R$. Then $ab \in \mathfrak{p} \cdot S^{-1}R$, so $uab \in \mathfrak{p}$ for some $u \in S$. Since $u \notin \mathfrak{p}$ by assumption, necessarily $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, thus $a/s \in \mathfrak{p} \cdot S^{-1}R$ or $b/t \in \mathfrak{p} \cdot S^{-1}R$. Hence $\mathfrak{p} \cdot S^{-1}R$ is a prime ideal.

Finally, we need to show that $\phi^{-1}(\mathfrak{p} \cdot S^{-1}R) = \mathfrak{p}$. Clearly $\phi^{-1}(\mathfrak{p} \cdot S^{-1}R) \supset \mathfrak{p}$. Conversely, if $r \in R$ such that $r/1 \in \mathfrak{p} \cdot S^{-1}R$, then $ur \in \mathfrak{p}$ for some $u \in S$. Again since $\mathfrak{p} \cap S = \emptyset$, we have $r \in \mathfrak{p}$. □

Exercise 10.14. Finish the proof, by showing that the bijection is a homeomorphism.

10.6. Localization and Hom.

Proposition 10.15. *Let M and N be R-modules and let $S \subset R$ be a multiplicative subset. Suppose that M is* finitely presented *(see § 13.3). Then we have an isomorphism of $S^{-1}R$-modules*

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

Proof. Let

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

be a finite presentation of M. Tensoring with $S := S^{-1}R$ yields an exact sequence

$$S^m \to S^n \to S \otimes_R M \to 0.$$

Applying Hom to the above exact sequences yields exact sequences

$$0 \to \mathrm{Hom}_R(M, N) \to N^m \to N^n \tag{10.1}$$

and

$$0 \to \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N) \to (S \otimes_R N)^m \to (S \otimes_R N)^n. \tag{10.2}$$

Since localization is exact, applying S^{-1} to (10.1) gives

$$0 \to S^{-1}\mathrm{Hom}_R(M, N) \to (S \otimes_R N)^m \to (S \otimes_R N)^n. \tag{10.3}$$

As the morphisms $(S \otimes_R N)^m \to (S \otimes_R N)^n$ in (10.2) and in (10.3) are the same, we have $\mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \simeq S^{-1}\mathrm{Hom}_R(M, N)$. □

Exercise 10.16. Write down the natural isomorphism $\mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \xrightarrow{\sim} S^{-1}\mathrm{Hom}_R(M, N)$.

Remark 10.17. Proposition 10.15 is false if we don't assume that M is finitely presented, even if we assume M finitely generated; see **[2]** for a counterexample.

10.7. First examples: the standard opens $D(f)$. Let $\mathbf{k}$ be an algebraically closed field and let $f \in \mathbf{k}[X_1, \ldots, X_d]$ be an irreducible polynomial. On the Zariski open $\mathbf{A}^d_{\mathbf{k}} - Z(f)$, the functions of the form

$$\frac{h}{g} \quad \text{with } g(z) = 0 \text{ implies } z \in Z(f)$$

is well defined. As a consequence of Nullstellensatz, the condition on g is equivalent to $g = c \cdot f^n$ for some $n \in \mathbf{Z}_{\geq 0}$ and some unit $c \in \mathbf{k}^\times$. Therefore the ring of such functions is exactly the localization of $\mathbf{k}[X_1, \ldots, X_d]$ by the multiplicative subset

$$\{\, f^n \;\big|\; n \in \mathbf{Z}_{\geq 0} \,\}.$$

More generally for any ring R and any $f \in R$, we consider

$$R_f := \text{localization of } R \text{ by } \{\, f^n \;\big|\; n \in \mathbf{Z}_{\geq 0} \,\}.$$

By Proposition 10.13, the map $R \to R_f$ induces a homeomorphism

$$\mathrm{Spec}(R_f) \xrightarrow{\sim} \{\, \mathfrak{p} \in \mathrm{Spec}(R) \;\big|\; f \notin \mathfrak{p} \,\} = \mathrm{Spec}(R) - V(f). \tag{10.4}$$

Through this homeomorphism, we can therefore endow the Zariski open $\mathrm{Spec}(R) - V(f)$ with an affine scheme structure, so regard R_f as the ring of functions on $\mathrm{Spec}(R) - V(f)$. We call $D(f) := \mathrm{Spec}(R_f)$ a *standard Zariski open subset*.

Exercise 10.18. Show that the standard open subsets $D(f)$ form a basis of topology of $\mathrm{Spec}(R)$. In other words, show that any Zariski open $U \subset \mathrm{Spec}(R)$ is a union of standard open subsets.

When $R = \mathbf{k}[X_1, \dots, X_d]$, then for every $f \in R$, the homeomorphism (10.4) restricts to a bijection

$$\mathrm{Specm}(R_f) \simeq \mathbf{A}^d_{\mathbf{k}} - Z(f).$$

The same statement holds more generally if $\mathbf{A}^d_{\mathbf{k}}$ and R are replaced with an affine algebraic closed subset $Z \subset \mathbf{A}^d_{\mathbf{k}}$ and its coordinate ring.

Exercise 10.19.

(1) Show that $R_f \simeq R[X]/(1 - Xf)$.
(2) Let $f, g \in R$. Show that $R_{fg} = (R_f)_g = (R_g)_f$.

For an R-module M, the localization of M by $\{ f^n \mid n \in \mathbf{Z}_{\geq 0} \}$ is denoted similarly by M_f.

10.8. Prime avoidance. We've mentioned that the standard open subsets $D(f)$ form a basis of topology of $\mathrm{Spec}(R)$. We have the following more precise statement.

Proposition 10.20. *Let $\Sigma \in \mathrm{Spec}(R)$ be a finite subset. Suppose that $\Sigma \in \mathrm{Spec}(R) - V(I)$ for some ideal $I \subset R$, then there exists $f \in I$ such that $\Sigma \subset D(f)$ $(\subset \mathrm{Spec}(R) - V(I))$.*

Proposition 10.20 is equivalent to the following algebraic reformulation, which we prove instead.

Proposition 10.21 (Prime avoidance). *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset R$ be prime ideals and let $I \subset R$ be an ideal. If $I \subset \bigcup_{i=1}^n \mathfrak{p}_i$, then $I \subset \mathfrak{p}_i$ for some i.*

Proof. We prove by induction on n the following equivalent statement: if $I \not\subset \mathfrak{p}_i$ for every i, then there exists $x \in I$ such that $x \notin \mathfrak{p}_i$ for all i. The case $n = 1$ is clear. Suppose that the statement is proven for $n - 1$. Then there exists $r \in I$ such that $y \notin \mathfrak{p}_i$ for every $i = 1, \dots, n-1$. Assume that $y \in \mathfrak{p}_n$ (otherwise $x = y$ works). We can assume that $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ whenever $i \neq j$, so $I \not\subset \mathfrak{p}_n$ implies that $I\mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} \not\subset \mathfrak{p}_n$ by the Exercise below. Choose $z \in I\mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}$ such that $z \notin \mathfrak{p}_n$. Then $x = y + z$ works. □

Exercise 10.22. Let $\mathfrak{p} \subset R$ be a prime ideal. Show that for every pair of ideals $I, J \subset R$, if $IJ \subset \mathfrak{p}$ then $I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$.

Remark 10.23. The same conclusion of Proposition 10.20 still holds if we only assume that all but two ideals among $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are prime [**12**, 00DS].

10.9. Germs of smooth functions. Let M be a manifold and let $p \in M$ be a point. Recall the a germ of smooth functions (U, f) at p is a smooth function $f : U \to \mathbf{R}$ defined on a neighborhood of $U \subset M$ of p. Two germs (U, f) and (V, g) are identified if and only if $f = g$ on a smaller neighborhood of p. If we have a basis of topology $\mathscr{C}$ on M, every germs of smooth function is represented by (U, f) for some $U \in \mathscr{C}$.

The germ of smooth functions at p from a ring $\mathscr{C}^\infty_{M,p}$. Note that $(U, f) \in \mathscr{C}^\infty_{M,p}$ is invertible if and only if $f(p) \neq 0$. It follows that the kernel

$$\mathfrak{m} := \ker(\mathscr{C}^\infty_{M,p} \to \mathbf{R})$$

of the evaluation map at p is the *unique* maximal ideal of $\mathscr{C}^\infty_{M,p}$.

Similarly, given a smooth vector bundle E over M of rank r, the germs of local sections of E at p are defined in the same way as the germs of smooth functions. They form a free $\mathscr{C}^\infty_{M,p}$-module $\mathscr{E}_p$ of rank r.

10.10. Second examples: rings of germs. Now let R be a ring and let $\mathfrak{p} \in \mathrm{Spec}(R)$.

We've mentioned in Exercise 10.18 that the standard open subsets form a basis of Zariski topology, so we copy the above definition, and define a germ of regular functions as a pair $(D(f), g \in R_f)$ with $\mathfrak{p} \in D(f)$, and identify $(D(f_1), g_1 \in R_{f_1})$ with $(D(f_2), g_2 \in R_{f_2})$ whenever "$g_1 = g_2$ on $D(f_1) \cap D(f_2)$", or precisely $g_1 = g_2$ in $R_{f_1 f_2}$.

Exercise 10.24. Show that the germs of regular functions at $\mathfrak{p}$ form a ring, isomorphic to

$$R_{\mathfrak{p}} := \text{ localization of } R \text{ by } R - \mathfrak{p}.$$

(Note that $R - \mathfrak{p}$ is multiplicative because $\mathfrak{p}$ is a prime ideal.)

We call $R_{\mathfrak{p}}$ the localization of R at the prime ideal $\mathfrak{p}$. The reason we call the functor $R \mapsto S^{-1}R$ localization is due to the above examples and the local nature of rings of germs. The following exercise provides another indication.

Exercise 10.25. Show that

$$\operatorname{Spec}(R_{\mathfrak{p}}) = \bigcap_{U \ni \mathfrak{p}} U,$$

where $\operatorname{Spec}(R_{\mathfrak{p}})$ is viewed as a subset of $\operatorname{Spec}(R)$ by Proposition 10.13, and U runs through all Zariski open of $\operatorname{Spec}(R)$ containing $\mathfrak{p}$.

Exercise 10.26. Let $f \in R$ and $\mathfrak{p} \in D(f)$. Show that $(R_f)_{\mathfrak{p}} = R_{\mathfrak{p}}$.

When R is an integral domain, its localization at the generic point is $R_{(0)} = \operatorname{Frac}(R)$. We call $\operatorname{Frac}(R)$ the *function field* of $\operatorname{Spec}(R)$.

10.11. Local rings. Let R be a ring and let $\mathfrak{p} \in \operatorname{Spec}(R)$. The following corollary of Proposition 10.13 is analogous to the case of rings of germs of smooth functions.

Corollary 10.27. *$\mathfrak{p}R_{\mathfrak{p}}$ is the unique maximal ideal of $R_{\mathfrak{p}}$.*

In general, a ring R with a unique maximal ideal is called a *local ring*. Equivalently, $\operatorname{Spec}(R)$ has a unique closed point, whence the name "local ring". Sometimes a local ring is denoted more precisely by $(R, \mathfrak{m})$, where $\mathfrak{m}$ is the unique maximal ideal of R. The field $R/\mathfrak{m}$ is called the *residue field*.

Exercise 10.28. Let R be a ring and $\mathfrak{m} \subset R$ an ideal. Prove the equivalence of the following assertions.

(1) $(R, \mathfrak{m})$ is a local ring.
(2) The non-unit elements of R form an ideal, equal to $\mathfrak{m}$.
(3) $R \neq 0$ and for every $x \in R$, either x or $1 + x$ is a unit.

Let R be any ring and let $\mathfrak{p} \in \operatorname{Spec}(R)$. The residue field of the local ring $R_{\mathfrak{p}}$ is also called the *residue field of* $\mathfrak{p}$, sometimes denoted by $\kappa(\mathfrak{p})$.

Exercise 10.29. Using the exactness of localization, show that $\kappa(\mathfrak{p}) \simeq \operatorname{Frac}(R_{\mathfrak{p}})$.

10.12. Scheme-theoretic fibers. Let $f : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ be a morphism of affine schemes induced by the ring homomorphism $\phi : A \to B$. Let $\mathfrak{p} \in \operatorname{Spec}(A)$. A natural scheme structure on the fiber $f^{-1}(\mathfrak{p})$ is defined as follows.

Consider the cartesian square of affine schemes

(10.5)
$$\begin{tikzcd}
\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p})) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & \operatorname{Spec}(B) \arrow[d] \\
\operatorname{Spec}(\kappa(\mathfrak{p})) \arrow[r] & \operatorname{Spec}(A)
\end{tikzcd}$$

where the horizontal arrow at the bottom is induced by the composition $A \to A_{\mathfrak{p}} \to A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. This is also a cartesian square of topological spaces by the following lemma.

Lemma 10.30. *Let*

$$\eta : B \to B_{\mathfrak{p}} \to B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \simeq B \otimes_A \kappa(\mathfrak{p})$$

be the composition of the localization and the quotient maps. The map

(10.6)
$$\begin{aligned} \operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p})) &\to f^{-1}(\mathfrak{p}) \\ \mathfrak{q} &\mapsto \eta^{-1}(\mathfrak{q}). \end{aligned}$$

is an order-preserving bijection.

Proof. The prime ideals of $B \otimes_A \kappa(\mathfrak{p})$ are in bijection with the prime ideals $\mathfrak{q} \subset B$ with $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$ by Proposition 10.13 (for "$\subset$") and Exercise 12.1 (for "$\supset$"), and they are exactly the preimages of $\mathfrak{p}$ under f. □

As topological spaces, $\mathrm{Spec}(\kappa(\mathfrak{p})) \to \mathrm{Spec}(A)$ is the inclusion of $\mathfrak{p}$ into $\mathrm{Spec}(A)$. We therefore regard $\mathrm{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ as the *scheme-theoretic fiber* of $\mathfrak{p} \in \mathrm{Spec}(A)$.

10.13. Local properties. Informally, a property (P) is called *local* if it holds whenever it holds for each germ. For instance for smooth functions on a manifold, "being identically zero" is a local property.

Here we present some local properties of rings, modules, etc.

Proposition 10.31. *Let M be an R-module and let $m \in M$. The following assertions are equivalent.*

(1) $m = 0$;
(2) $m = 0$ in $M_\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$;
(3) $m = 0$ in $M_\mathfrak{m}$ for all maximal ideal $\mathfrak{m} \subset R$.

Proof. It is clear that (1) $\Rightarrow$ (2) $\Rightarrow$ (3). Now assume that $m \neq 0$ in M. Then $1 \notin \mathrm{Ann}(m)$, so the ideal $\mathrm{Ann}(m)$ is contained in some maximal ideal $\mathfrak{m}$. Since no element of $R - \mathfrak{m}$ annihilates m, we have $m \neq 0$ in $M_\mathfrak{m}$. □

Corollary 10.32. *Let M be an R-module. The following assertions are equivalent.*

(1) $M = 0$;
(2) $M_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$;
(3) $M_\mathfrak{m} = 0$ for all maximal ideal $\mathfrak{m} \subset R$.

Corollary 10.33. *Let $f : M \to N$ be a morphism of R-modules. The following assertions are equivalent.*

(1) f is injective (resp. surjective);
(2) $f_\mathfrak{p}$ is injective (resp. surjective) for all $\mathfrak{p} \in \mathrm{Spec}(R)$;
(3) $f_\mathfrak{m}$ is injective (resp. surjective) for all maximal ideal $\mathfrak{m} \subset R$.

Here, $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is the localization of f by $R - \mathfrak{p}$.

Proof. Since localization is exact, (1) implies (2). Clearly (2) implies (3). Now assume (3). Again since localization is exact, we have $\ker(f)_\mathfrak{m} = \ker(f_\mathfrak{m}) = 0$ for all maximal ideal $\mathfrak{m} \subset R$. Hence $\ker(f) = 0$ by Corollary 10.32. The proof for the surjectivity is similar. □

10.14. Support. Let f be a smooth function on a manifold M. The support of f is defined as

$$\mathrm{Supp}(f) = \overline{\{\, p \in M \mid f(p) \neq 0 \,\}} = \left\{ p \in M \;\middle|\; f \neq 0 \in \mathscr{C}^\infty_{M,p} \right\}.$$

For an element m of an R-module M, the *support of m* is defined similarly:

$$\mathrm{Supp}(m) = \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid m \neq 0 \in M_\mathfrak{p} \,\}.$$

We also define

$$\mathrm{Supp}(M) := \{\, \mathfrak{p} \in \mathrm{Spec}(R) \mid M_\mathfrak{p} \neq 0 \,\},$$

and call it the *support of M*.

Proposition 10.34. *Let M be an R-module. We have*

$$\mathrm{Supp}(m) = V(\mathrm{Ann}(m)) \subset \mathrm{Spec}(R).$$

Proof. Let $\mathfrak{p} \in \mathrm{Spec}(R)$. We have $\mathfrak{p} \in \mathrm{Supp}(m)$ if and only if $m \neq 0$ in $M_\mathfrak{p}$, which is equivalent to $\mathrm{Ann}(m) \subset \mathfrak{p}$. □

Corollary 10.35. *Suppose that M is generated by finitely many elements $m_1, \dots, m_k$ over R. We have*

$$\mathrm{Supp}(M) = \bigcup_{i=1}^{k} \mathrm{Supp}(m_i) = V(\mathrm{Ann}(M)) \subset \mathrm{Spec}(R).$$

In particular, both $\mathrm{Supp}(m)$ *and* $\mathrm{Supp}(M)$ *are closed in* $\mathrm{Spec}(R)$.

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $m_1, \ldots, m_k$ also generated $M_\mathfrak{p}$ over $R_\mathfrak{p}$ by Corollary 10.33. So $\mathfrak{p} \in \operatorname{Supp}(M)$ if and only if $m_i \neq 0$ in $M_\mathfrak{p}$ for some i, namely $\mathfrak{p} \in \operatorname{Supp}(m_i)$. Hence

$$\operatorname{Supp}(M) = \bigcup_i \operatorname{Supp}(m_i) = \bigcup_i V(\operatorname{Ann}(m_i)) = V(\operatorname{Ann}(M)).$$

□

Exercise 10.36. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of R-modules. Show that

$$\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'').$$

10.15. Localization and integral extensions. Localization commutes with taking integral closure.

Proposition 10.37. *Let B be a ring and $A \subset B$ a subring. Let S be a multiplicative subset of A. If C is the integral closure of A in B, then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. Let $c/s \in S^{-1}C$ with $c \in C$. Since c is integral over A, we have

$$c^n + \sum_{i=0}^{n-1} a_i c^i = 0$$

for some integer $n \geq 1$ and $a_i \in A$, so

$$(c/s)^n + \sum_{i=0}^{n-1} (a_i/s^{n-i})(c/s)^i = 0,$$

which shows that c/s is integral over $S^{-1}A$.

Conversely, let $b/s \in S^{-1}B$ be an element integral over $S^{-1}A$. Then

$$(b/s)^m + \sum_{i=0}^{m-1} (a'_i/s_i)(b/s)^i = 0$$

for some integer $m \geq 1$ and some $a'_i \in A$. Up to replacing b and s by $b\sigma$ and $s\sigma$ with $\sigma := s_0 \cdots s_{m-1}$, we have

$$(b/s)^m + \sum_{i=0}^{m-1} (a''_i/s^{m-i})(b/s)^i = 0$$

for some $a''_i \in A$. Multiplying the above equality by s^m shows that b is integral over A, namely $b \in C$. □

Corollary 10.38. *Let R be an integral domain. The following assertions are equivalent.*

(1) *R is integrally closed;*
(2) *$R_\mathfrak{p}$ is integrally closed for all $\mathfrak{p} \in \operatorname{Spec}(R)$;*
(3) *$R_\mathfrak{m}$ is is integrally closed for all maximal ideal $\mathfrak{m} \subset R$.*

Proof. Let C be the integral closure of A in $\operatorname{Frac}(A)$ and let $f : A \hookrightarrow C$ be the inclusion. For every $\mathfrak{p} \in \operatorname{Spec}(R)$, by Proposition 10.37 the localization $f_\mathfrak{p} : A_\mathfrak{p} \hookrightarrow C_\mathfrak{p}$ is the inclusion of $A_\mathfrak{p}$ into its integral closure. We conclude by Corollary 10.33. □

11. Nakayama's lemma

11.1. Germs and fibers. Let M be a smooth manifold and let E be a smooth vector bundle over M of rank r. Let $p \in M$ and let $\mathfrak{m}_p$ be the maximal ideal of $\mathscr{C}^\infty_{M,p}$. Since $\mathfrak{m}_p$ is the kernel of the evaluation map at p, the residue field $\mathscr{C}^\infty_{M,p}/\mathfrak{m}_p$ is isomorphic to $\mathbf{R}$. We have

$$\mathscr{E}|_p := \mathscr{E}_p \otimes_{\mathscr{C}^\infty_{M,p}} (\mathscr{C}^\infty_{M,p}/\mathfrak{m}_p) \simeq \mathscr{E}_p/\mathfrak{m}_p\mathscr{E}_p \simeq E_p \simeq \mathbf{R}^r$$

as $\mathbf{R}$-vector spaces, where E_p is the fiber of the vector bundle E.

Now let M be a module over a ring R. If we consider M as an object over $\operatorname{Spec}(R)$, one could regard it as an analogue of modules of sections of a vector bundle. For every $\mathfrak{p} \in \operatorname{Spec}(R)$, elements of the localization $M_{\mathfrak{p}}$ are called *germs of the module* M at $\mathfrak{p}$. The tensor product

$$M|_{\mathfrak{p}} := M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} \kappa(\mathfrak{p})$$

is called the *fiber* of M at $\mathfrak{p}$, or the *restriction* of M to $\mathfrak{p}$. It is a $\kappa(\mathfrak{p})$-vector space.

Exercise 11.1 (The local nature of fibers above closed points)**.** Let $\mathfrak{m} \subset R$ be a maximal ideal. Show that

$$R/\mathfrak{m} \simeq R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}.$$

More generally, show that for every R-module M, we have

$$M|_{\mathfrak{m}} \simeq (M_{\mathfrak{m}})|_{\mathfrak{m}R_{\mathfrak{m}}}.$$

Elements of M can be regarded as *global sections*. For any $\sigma \in M$, the *value* of σ at $\mathfrak{p}$ is defined as the image $\sigma|_{\mathfrak{p}} \in M|_{\mathfrak{p}}$ of σ in the fiber over $\mathfrak{p} \in \operatorname{Spec}(R)$. In particular, the value $f_{|\mathfrak{p}}$ of a regular function $f \in R$ at $\mathfrak{p}$ is an element of the residue field $\kappa(\mathfrak{p})$. Note that a section $\sigma \in M$ takes values in different vector spaces $M|_{\mathfrak{p}}$, depending on $\mathfrak{p}$.

Example 11.2. Let $\mathbf{k}$ be an algebraically closed field and let $R = \mathbf{k}[X, Y]$. Consider e.g.

$$f := \frac{X - Y}{X(Y + X)} \in \mathbf{k}(X, Y).$$

We can regard f as an element of $R_{X(Y+X)}$, i.e. as a regular function on the standard open $D(X(Y + X))$. Take a closed point $\mathfrak{m} \in D(X(Y + X))$, e.g. the maximal ideal corresponding to the point $(2, 3)$. Then through the $\mathbf{k}$-linear isomorphism $\kappa(\mathfrak{m}) \simeq R_{X(Y+X)}/\mathfrak{m} \xrightarrow{\sim} \mathbf{k}$, we have

$$f|_{\mathfrak{m}} = \frac{2 - 3}{2(3 + 2)} = -\frac{1}{10},$$

which is exactly the evaluation of f at $(2, 3)$.

Now consider $\mathfrak{p} = (Y)$, the generic point of the X-axis. Under the natural isomorphism $\kappa(\mathfrak{p}) \simeq \mathbf{k}(X)$, we have

$$f|_{\mathfrak{p}} = \frac{X}{X^2} = \frac{1}{X},$$

namely we evaluate f by setting $Y = 0$.

Exercise 11.3. What is the value of $\frac{7}{13}$ at $(5) \in \operatorname{Spec}(\mathbf{Z})$?

11.2. Spreading out generators from fibers to germs, and the Nakayama lemma. Again, consider a smooth vector bundle E of rank r over a smooth manifold M. Let $p \in M$. Then any $v \in E|_p$ extends to a germ of smooth sections $\tilde{v} \in \mathscr{E}_p$. Moreover, if $v_1, \ldots, v_N$ are generators of $E|_p$ over $\mathbf{R}$, then any extensions $\widetilde{v_1}, \ldots, \widetilde{v_N}$ of them to $\mathscr{E}_p$ again generate $\mathscr{E}_p$ over $\mathscr{C}^\infty_{M,p}$.

Here is the analogue statement for finitely generated modules, which we will prove as a corollary of the Nakayama lemma.

Corollary 11.4. *Let $(R, \mathfrak{m}, \mathbf{k})$ be a local ring and let M be a finitely generated R-module. Let $v_1, \ldots, v_d$ be a basis of the $\mathbf{k}$-vector space $M|_{\mathfrak{m}}$. Then any liftings $\widetilde{v_1}, \ldots, \widetilde{v_d} \in M$ of $v_1, \ldots, v_d$ generate M.*

In this lecture, we call the following result the *Nakayama lemma*. The statement is the case $d = 0$ of Corollary 11.4.

Theorem 11.5. *Let $(R, \mathfrak{m})$ be a local ring and let M be a* finitely generated *R-module. If $\mathfrak{m}M = M$ (*i.e. *$M|_{\mathfrak{m}} = 0$), then $M = 0$.*

Proof. Applying the Cayley–Hamilton theorem (Theorem 3.3) to the identity on M shows that $(1 + r)M = 0$ for some $r \in \mathfrak{m}$. Since $(R, \mathfrak{m})$ is a local ring, $1 + r$ is a unit. Hence $M = 0$. □

Corollary 11.6. *Let R be any ring and let M be a finitely generated R-module. Then $M|_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m} \subset R$ if and only if $M = 0$.*

Proof. This is a direct consequence of Theorem 11.5 and Corollary 10.32. □

Proof of Corollary 11.4. First of all, since M is finitely over R, so is the quotient $M|_{\mathfrak{m}} = M/\mathfrak{m}M$. Thus $M|_{\mathfrak{m}}$ is indeed finite dimension over $\mathbf{k}$. By assumption, we have

$$M = \mathfrak{m}M + \sum_{i=1}^{d} R\widetilde{v_i}.$$

Applying Theorem 11.5 to $M/\sum_{i=1}^{d} R\widetilde{v_i}$ (which is finite over R because so is M) shows that $M = \sum_{i=1}^{d} R\widetilde{v_i}$. □

LECTURE 6

Maximal ideals and Hilbert's Nullstellensatz

12.

12.1. Maps between maximal spectra? In general, a ring homomorphism $f : A \to B$ does *not* induce a map between their maximal spectra; consider e.g. $f : \mathbf{Z} \hookrightarrow \mathbf{Q}$.

Exercise 12.1. Let $f : A \to B$ be a *surjective* ring homomorphism. Let $I := \ker f$. Consider

$$f^{-1} : \{\text{ Ideals of } B\ \} \to \{\text{ Ideals of } A \text{ containing } I\ \}$$

(1) Show that f^{-1} is a bijection which preserves inclusions. More precisely, show that $J \mapsto f(J)$ is the inverse of f^{-1}.
(2) Show that f^{-1} sends maximal ideals to maximal ideals.

The following statement singles out another important class of homomorphisms $f : A \to B$ containing Example 6.13, for which this property holds.

Proposition 12.2. *Let* $\mathbf{k}$ *be a field and let* A *and* B *be finitely generated* $\mathbf{k}$*-algebras. Any morphism* $f : A \to B$ *of* $\mathbf{k}$*-algebras induces*

$$f^{-1} : \mathrm{Specm}(B) \to \mathrm{Specm}(A).$$

Proof. By Exercise 12.1, up to replacing A by $f(A)$, we can assume that f is injective. Let $\mathfrak{m} \subset B$ be a maximal ideal. Then f induces an injective homomorphism

$$A/f^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m}$$

of $\mathbf{k}$-algebras.

If we know that $B/\mathfrak{m}$ is a finite field extension of $\mathbf{k}$, then the $\mathbf{k}$-algebra $A/f^{-1}(\mathfrak{m})$ is a field, and thus $f^{-1}(\mathfrak{m})$ is a maximal ideal of A. This is indeed the case by Zariski's lemma stated below. □

12.2. Zariski's lemma.

Proposition 12.3 (Zariski's lemma)**.** *Let* $L/\mathbf{k}$ *be a field extension. Suppose that* L *is finitely generated as a* $\mathbf{k}$*-algebra. Then* $L/\mathbf{k}$ *is a finite extension.*

Proof. By assumption, there exist $x_1, \dots x_n \in L$ such that $L = \mathbf{k}[x_1, \dots, x_n]$. We prove the proposition by induction on $n \geq 0$. The case $n = 0$ is trivial. Suppose that $n = k \in \mathbf{Z}_{>0}$ and that the proposition is proven for $n = k - 1$. Then L is a finite extension over $\mathbf{k}(x_n)$. So there exists $0 \neq f \in \mathbf{k}[x_n]$ such that $f \cdot x_i$ is integral over $\mathbf{k}[x_n]$ for every $i = 1, \dots, n-1$. As $\mathbf{k}(x_n) \subset L = \mathbf{k}[x_n][x_1, \dots, x_{n-1}]$ and integral elements form a subring, it follows that for every $F \in \mathbf{k}(x_n)$, there exists an integer $N \geq 0$ such that $f^N F \in \mathbf{k}(x_n)$ is integral over $\mathbf{k}[x_n]$.

Suppose that $\mathbf{k}(x_n)$ is not a finite extension $\mathbf{k}$, then the morphism $\mathbf{k}(X) \to \mathbf{k}(x_n)$ of $\mathbf{k}$-algebras sending X to x_n is an isomorphism (see Exercise). Since $\mathbf{k}[x_n]$ is integrally closed, we have $f^N F \in \mathbf{k}[x_n]$. But this is impossible if we take $F = 1/P$ for some $P \in \mathbf{k}[x_n]$ which does not divide f (such an element P exists since there are infinitely many irreducible monic polynomials in $\mathbf{k}[X]$). Thus $\mathbf{k}(x_n)/\mathbf{k}$ is a finite extension. As $L/\mathbf{k}(x_n)$ is also a finite extension by the induction hypothesis, the proposition follows. □

We will also use Zariski's lemma later to prove Hilbert's Nullstellensatz. The following corollary gives a first hint how they are related.

Corollary 12.4. *Let $\mathfrak{m} \subset \mathbf{k}[X_1, \ldots, X_n]$ be a maximal ideal.*

(1) The residue field $\mathbf{k}[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite extension of $\mathbf{k}$.

(2) As a consequence, if $\mathbf{k}$ is algebraically closed then there exsit $a_1, \ldots, a_n$ such that

$$\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n).$$

Proof. The first assertion follows directly from Zariski's lemma. For the second statement, since $\mathbf{k}$ is algebraically closed, we have an isomorphism

$$\mathbf{k}[X_1, \ldots, X_n]/\mathfrak{m} \simeq \mathbf{k}.$$

For each $i = 1, \ldots, n$, let $a_i \in \mathbf{k}$ denote the image of X_i. Then

$$(X_1 - a_1, \ldots, X_n - a_n) \subset \mathfrak{m}.$$

As $(X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal, the above inclusion is an equality. □

Remark 12.5. Corollary 12.4.(2) should remind us *Hadamard's lemma* for smooth functions.

12.3. Nullstellensatz.

Let $\mathbf{k}$ be a field.

For every subset $S \subset \mathbf{k}[X_1, \ldots, X_n]$, let $Z(S) \subset \mathbf{A}^n_{\overline{\mathbf{k}}}$ be the algebraic subset in the affine space *over the algebraic closure $\overline{k}$* cut out by S.

Proposition 12.6 (Weak Nullstellensatz). *Let $S \subset \mathbf{k}[X_1, \ldots, X_n]$ be a subset such that $Z(S) = \emptyset$. Then the ideal generated by S is $\mathbf{k}[X_1, \ldots, X_n]$.*

In other words if $Z(S) = \emptyset$, then we have the "partition of unity" of the form

$$1 = \sum f_i g_i$$

with $f_i \in S$ and $g_i \in \mathbf{k}[X_1, \ldots, X_n]$.

Proof. Assume to the contrary that the ideal I generated by S is not $\mathbf{k}[X_1, \ldots, X_n]$. Then I is contained in a maximal ideal $\mathfrak{m}$. By Corollary 12.4, we have a $\mathbf{k}$-linear inclusion

$$\mathbf{k}[X_1, \ldots, X_n]/\mathfrak{m} \subset \overline{\mathbf{k}}$$

of fields. For every $i = 1, \ldots, n$, if $a_i \in \overline{\mathbf{k}}$ denote the image of X_i, then $f(a_1, \ldots, a_n) = 0$ for all $f \in \mathfrak{m}$. Thus $Z(S) \neq \emptyset$. □

For every algebraic subset $Z \subset \mathbf{A}^n_{\overline{\mathbf{k}}}$, let

$$I(Z) := \{ f \in \mathbf{k}[X_1, \ldots, X_n] \mid f(p) = 0 \text{ for all } p \in Z \},$$

which is an ideal of $\mathbf{k}[X_1, \ldots, X_n]$.

Theorem 12.7 (Nullstellensatz). *For every ideal $I \subset \mathbf{k}[X_1, \ldots, X_n]$, we have*

$$I(Z(I)) = \sqrt{I}.$$

Proof. (Rabinowitch's trick, conceptualized by localization.)

It is clear that $\sqrt{I} \subset I(Z(I))$.

Let $f \in I(Z(I))$. Since $f \in \sqrt{I}$ if and only if f is nilpotent in $R := \mathbf{k}[X_1, \ldots, X_n]/I$, it suffices to show that $R_f = 0$. We have

$$R_f \simeq \frac{R[X]}{(1 - Xf)} = \frac{\mathbf{k}[X_1, \ldots, X_n, X]}{I + (1 - Xf)}$$

by Exercise 10.19. Regarding I as an ideal in $\mathbf{k}[X_1, \ldots, X_n, X]$, we have

$$Z(I + (1 - Xf)) = Z(I) \cap Z(1 - Xf) = \emptyset \subset \mathbf{A}^{n+1}_{\overline{k}},$$

so $I + (1 - Xf) = \mathbf{k}[X_1, \ldots, X_n, X]$ by weak Nullstellensatz. Hence $R_f = 0$. □

12.4. Density of closed points. Here is a consequence of Hilbert's Nullstellensatz.

Corollary 12.8. *Let* $\mathbf{k}$ *be a field and let* A *be a finitely generated* $\mathbf{k}$*-algebra. The closed points of* $\operatorname{Spec}(A)$ *form a dense subset.*

Proof. If $I \subset A$ is an ideal such that $Z(I)$ contains all the maximal ideals of A, then I is contained in the *Jacobson radical* of A, defined as

$$\operatorname{rad}(A) := \bigcap_{\mathfrak{m}\in\operatorname{Specm}(A)} \mathfrak{m}.$$

So it suffices to show that

$$\operatorname{rad}(A) = \operatorname{Nil}(A).$$

We have the following more general statement.

Lemma 12.9. *For every ideal* $I \subset A$*, we have*

$$\sqrt{I} = \bigcap_{I\subset\mathfrak{m}\in\operatorname{Specm}(A)} \mathfrak{m}$$

Proof. It is clear that $\sqrt{I} \subset \bigcap_{I\subset\mathfrak{m}\in\operatorname{Specm}(A)} \mathfrak{m}$.

Choose a surjective ring homomorphism

$$f : R := \mathbf{k}[X_1, \dots, X_d] \to A.$$

By Exercise 12.1, up to replacing I by $f^{-1}(I)$, it suffices to prove the statement for $A = R$ and $I \subset R$.

Let $f \in R$ such that $f \in \mathfrak{m}$ for all maximal ideal $\mathfrak{m} \subset R$ containing I. Let $p \in Z(I) \subset \mathbf{A}^n_{\overline{\mathbf{k}}}$ and let

$$\overline{\mathfrak{m}} \subset \overline{R} := \overline{\mathbf{k}}[X_1, \dots, X_d]$$

be the corresponding maximal ideal. Then $I \subset \overline{\mathfrak{m}}$, where we identify I as a subset of $\overline{R}$ through $R \subset \overline{R}$. Let $\mathfrak{m} := R \cap \overline{\mathfrak{m}}$. We have $\mathfrak{m} \subsetneq R$ (because $1 \notin \mathfrak{m}$). Though we don't need this, actually $\mathfrak{m}$ is a maximal ideal of R: the natural map

$$R/\mathfrak{m} \hookrightarrow \overline{R}/\overline{\mathfrak{m}} \simeq \overline{\mathbf{k}}$$

is an injective homomorphism of $\mathbf{k}$-algebras, so $R/\mathfrak{m}$ is a field. As $I \subset R \cap \overline{\mathfrak{m}} = \mathfrak{m}$, we have $f \in \mathfrak{m} \subset \overline{\mathfrak{m}}$, and thus $f(p) = 0$. Hence

$$\bigcap_{I\subset\mathfrak{m}\in\operatorname{Specm}(A)} \mathfrak{m} \subset I(Z(I)),$$

and we conclude by the Nullstellensatz $I(Z(I)) = \sqrt{I}$. □

□

LECTURE 7

Generators and relations

13. Finite generation and finite presentation

Let R be a ring and let M be an R-module.

13.1. Free modules. An R-module M is called *free* if it is isomorphic to $\bigoplus_{i\in I} R$ for some set I. For instance, when $\mathbf{k}$ is a field, every $\mathbf{k}$-module is free (by the axiom of choice). When I is finite, we call $\#I$ the *rank* of M. It is well-defined by the following proposition.

Proposition 13.1. *Let $m, n \in \mathbf{Z}_{\geq 0}$. If there exists an injective morphism $f : R^m \to R^n$ of R-modules, then $m \leq n$. In particular, $R^m \simeq R^n$ if and only if $m = n$.*

Proof. Suppose that $m > n$. Consider the composition

$$\phi : R^m \xrightarrow{f} R^n \hookrightarrow R^m$$

of f with the inclusion identifying R^n with $R^n \times 0 \subset R^m$. By Cayley-Hamilton, we have

$$\phi^k + r_{k-1}\phi^{k-1} + \cdots + r_0 = 0$$

for some $k \in \mathbf{Z}_{>0}$ and $r_0, \dots, r_{k-1} \in R$; we can assume that k is minimal. The last component of the image of $(0, \dots, 0, 1) \in R^m$ in R^m under $\phi^k + r_{k-1}\phi^{k-1} + \cdots + r_0$ is r_0, so $r_0 = 0$. As ϕ is injective, we have $\phi^{k-1} + r_{k-1}\phi^{k-2} + \cdots + r_1 = 0$, which contradicts the minimality of k. □

Remark 13.2. Infinite products $\prod_{i\in I} R$ of a ring are *not* free in general. For instance, $\mathbf{Z}^{\mathbf{Z}}$ is not free (first proven by Baer); see [**1**] for an interesting proof and related discussion. The group $\mathbf{Z}^{\mathbf{Z}}$ is also called the Baer–Specker group (Specker shows that any *countable* subgroup of $\mathbf{Z}^{\mathbf{Z}}$ is free).

13.2. Generators. Given a subset $\{ e_i \mid i \in I \}$ of elements of M. We call $\{ e_i \mid i \in I \}$ a *set of generators* of M if every $m \in M$ is an R-linear combination of $\{ e_i \mid i \in I \}$; in other words the morphism

$$p : \bigoplus_{i\in I} R \to M$$

of R-modules sending $(r_i)_{i\in I}$ to $\sum_{i\in I} r_i e_i$ is surjective.

We've already mentioned that if M has a finite set of generators, then we call M an *R-module of finite type* (or a finitely generated R-module, or simply a *finite R-module*). Every finite R-module is a quotient of a free module of finite rank, and *vice versa*.

Exercise 13.3. Show that every finitely generated free R-module has finite rank.

Lemma 13.4. *Let*

$$0 \to K \to M \to N \to 0$$

be an exact sequence of R-modules.

1. *Suppose that K and N are finitely generated. Then M is also finitely generated.*
2. *Suppose that M is finitely generated. Then N is finitely generated.*

Proof. Exercise. □

Remark 13.5. In the above lemma, in general M is finitely generated does not imply that K is finitely generated (see Exercise 13.7). We will see next that if we assume N to be *finitely presented*, then K is finitely generated.

13.3. Finite presentation. An R-module M is called *finitely presented* if there exists an exact sequence

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

for some integers m and n. In plain words, a finitely presented module is a module having not only finitely many generators, but also the module of relations among are generated by finitely many relations.

Lemma 13.6. *Let*

$$0 \to K \to M \to N \to 0$$

be an exact sequence of R-modules.

(1) Suppose that K and N are finitely presented. Then M is also finitely presented.
(2) Suppose that M is finitely generated and N is finitely presented. Then K is finitely generated.
(3) Suppose that M is finitely presented and K is finitely generated. Then N is finitely presented.

Proof. Exercise. □

Exercise 13.7. Construct a finitely presented R-module M such that

(1) M admits a submodule which is not finite over R.
(2) M admits a quotient which is not finitely presented.

(Hint: consider e.g. $R = M = \mathbf{Z}[X_1, X_2, \ldots]$.)

Exercise 13.8. Let M be a finitely generated (resp. finitely presented) R-module and let $R \to A$ be a ring homomorphism. Show that the base change $M \otimes_R A$ is finitely generated (resp. finitely presented) over A. In particular, the localization $S^{-1}M$ of M by a multiplicative subset $S \subset R$ is finitely generated (resp. finitely presented) over $S^{-1}R$.

13.4. Openness of surjectivity and the isomorphism property. Let $f : M \to N$ be a morphism of R-modules and let $\mathfrak{p} \in \mathrm{Spec}(R)$.

Proposition 13.9. *Suppose that N is* finitely generated *over R. If $f_\mathfrak{p}$ is surjective, then there exists a standard open subset $D(g) \subset$* Spec(R) *containing $\mathfrak{p}$ such that the localization $M_g \to N_g$ is surjective.*

Proof. As localization is an exact functor, we have

$$\mathrm{coker}(f)_\mathfrak{p} = \mathrm{coker}(f_\mathfrak{p}) = 0.$$

In particular the support Σ of coker(f) is strictly contained in Spec(R). Since N is finite over R, so is coker(f) by Lemma 13.4, so Spec(R) − Σ is a Zariski open neighborhood of $\mathfrak{p} \in \mathrm{Spec}(R)$ by Exercise 10.35. As the standard open subsets form a basis of Zariski topology, there exists $g \in R$ such that $\mathfrak{p} \in D(g) \subset \mathrm{Spec}(R) - \Sigma$. Since $\mathrm{coker}(f_\mathfrak{q}) = \mathrm{coker}(f)_\mathfrak{q} = 0$ for every $\mathfrak{q} \in D(g)$, the localization $M_g \to N_g$ is surjective by Corollary 10.33. □

Proposition 13.10. *Suppose that M is* finitely generated *and N is* finitely presented *over R. If $f_\mathfrak{p}$ is an isomorphism, then there exists a standard open subset $D(h) \subset$* Spec(R) *containing $\mathfrak{p}$ such that the localization $M_h \to N_h$ is an isomorphism.*

Proof. By Proposition 13.9, there exists a standard open $D(g) \subset \mathrm{Spec}(R)$ containing $\mathfrak{p}$ such that $f_g : M_g \to N_g$ is surjective. Let $K := \ker(f_g)$. Since M_g is finitely generated and N_g is finitely presented, K is finitely generated. So $\mathrm{Supp}(K) \subset D(g)$ is a Zariski closed subset. As

$$K_\mathfrak{p} = \ker(f_g)_\mathfrak{p} = \ker((f_g)_\mathfrak{p}) = \ker(f_\mathfrak{p}) = 0,$$

we have $\mathfrak{p} \notin \mathrm{Supp}(K)$, So there exists $h \in R$ such that $\mathfrak{p} \in D(h) \subset D(g) - \mathrm{Supp}(K)$, and therefore

$$\ker(f_\mathfrak{q}) = \ker((f_g)_\mathfrak{q}) = \ker(f_g)_\mathfrak{q} = K_\mathfrak{q} = 0$$

for every $\mathfrak{q} \in D(h)$. Thus $f_\mathfrak{q}$ is an isomorphism for every $\mathfrak{q} \in D(h)$. We conclude by Corollary 10.33 that $M_h \to N_h$ is an isomorphism. □

13.5. Upper semicountinuity of the number of generators.

Corollary 13.11. *Let M be a finite R-module. For every $k \in \mathbf{Z}_{\geq 0}$, the set*

$$\{ \mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \text{ is generated by } k \text{ elements over } R_{\mathfrak{p}} \}$$

is open in $\operatorname{Spec}(R)$. *Moreover, for every point $\mathfrak{p}$ in the above set, there exists a standard open subset $D(h) \subset \operatorname{Spec}(R)$ containing $\mathfrak{p}$ such that there exists a surjective morphism of R_h-modules*

$$R_h^k \twoheadrightarrow M_h.$$

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $M_{\mathfrak{p}}$ is generated k elements; we can assume that these elements are of the form $m_1/1, \ldots, m_k/1$ with $m_i \in M$ for all i. Consider the morphism of R-modules

$$\begin{aligned} f : R^k &\to M \\ (r_1, \ldots, r_k) &\mapsto r_1 m_1 + \cdots r_k m_k. \end{aligned} \tag{13.1}$$

Then $f_{\mathfrak{p}}$ is surjective. Since M is finite over R, we conclude by Proposition 13.9. □

13.6. Openness of being free.

Corollary 13.12. *Let M be a finitely presented R-module. The set*

$$\{ \mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \text{ is free over } R_{\mathfrak{p}} \}$$

is open in $\operatorname{Spec}(R)$. *Moreover, for every point $\mathfrak{p}$ in the above set, there exists a standard open subset $D(h) \subset \operatorname{Spec}(R)$ containing $\mathfrak{p}$ such that*

$$M_h \simeq R_h^k$$

as R_h-modules, with $k = \operatorname{rank}_{R_{\mathfrak{p}}} M_{\mathfrak{p}}$.

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $M_{\mathfrak{p}}$ is free over $R_{\mathfrak{p}}$. Since M is finitely generated over R, so is $M_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$, so there exist $m_1, \ldots, m_k \in M$ whose images in $M_{\mathfrak{p}}$ form a basis of the free $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$. Consider the morphism of R-modules

$$\begin{aligned} f :&R^k \to M \\ (r_1, \ldots, r_k) &\mapsto r_1 m_1 + \cdots r_k m_k, \end{aligned} \tag{13.2}$$

Since $f_{\mathfrak{p}}$ is an isomorphism and M is finitely presented, we conclude by Proposition 13.10. □

13.7. Finite generation/presentation are Zariski local properties. Suppose that $(f_1, \ldots f_k) = R$.

Proposition 13.13. *Let M be an R-module.*

(1) If M_{f_i} is finitely generated over R_{f_i} for each i, then M is finitely generated over R.
(2) If M_{f_i} is finitely presented over R_{f_i} for each i, then M is finitely presented over R.

Proof. Let $\Sigma_i \subset M_{f_i}$ be a finite subset which generate M_{f_i}; we can assume that Σ_i is the image of some finite subset $\Sigma_i' \subset M$ under the localization map $M \to M_{f_i}$. Let $\Sigma := \cup_{i=1}^k \Sigma_i'$, and consider the map $g : R^{\Sigma} \to M$ sending $(r_s)_{s \in \Sigma}$ to $\sum_{s \in \Sigma} r_s \cdot s$. For every prime ideal $\mathfrak{p} \subset R$, we have $f_i \notin \mathfrak{p}$ for some i. So $g_{\mathfrak{p}} : R_{\mathfrak{p}}^{\Sigma} \to M_{\mathfrak{p}}$ is the localization of $R_{f_i}^{\Sigma} \to M_{f_i}$, which is surjective. Hence g is surjective.

We leave (2) as an exercise. □

14. Locally free modules

Let R be a ring.

14.1. Definition.

Definition 14.1. An R-module M is called *locally free* if for every $\mathfrak{p} \in \operatorname{Spec}(R)$, there exists a standard open $D(h) \subset \operatorname{Spec}(R)$ containing $\mathfrak{p}$ such that M_h is a free R_h-module.

We could regard locally free modules over R as vector bundles on $\mathrm{Spec}(R)$. Note that by Proposition 13.13, every finitely generated locally free module is finitely presented. Assume that M is a finitely presented R-module. Then by Corollary 13.12 and the exactness of localization, an R-module M is locally free if and only if $M_{\mathfrak{p}}$ is free over $R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$.

Exercise 14.2. Let M be a finitely presented R-module. Show that $\mathrm{rank}_{R_{\mathfrak{p}}} M_{\mathfrak{p}}$ is finite for every $\mathfrak{p} \in \mathrm{Spec}(R)$, and that $\mathfrak{p} \mapsto \mathrm{rank}_{R_{\mathfrak{p}}} M_{\mathfrak{p}}$ is locally constant. When $\mathrm{rank}_{R_{\mathfrak{p}}} M_{\mathfrak{p}}$ is constant, we call it the *rank* of M.

Exercise 14.3. Let M and N be locally free modules over R of rank m and n respectively.

- Show that $M \otimes_R N$ is locally free of rank mn
- Show that
$$M^\vee := \mathrm{Hom}_R(M, R)$$
is also locally free of rank m.

We will see that there exist locally free modules which are not free.

Exercise 14.4. Show that locally free modules are torsion free.

14.2. Picard group of a ring. Locally free modules of rank 1 are called *invertible modules* because of the following property.

Exercise 14.5. Let M be a locally free R-module of rank 1. Show that
$$M \otimes_R M^\vee \simeq R$$
as R-modules.

Together with Exercise 14.3, we see that
$$\mathrm{Pic}(R) := \{\text{ Invertible } R\text{-modules }\} / \simeq$$
endowed with the binary operation $\otimes_R$ is a group. We call $\mathrm{Pic}(R)$ the *Picard group* of R.

14.3. First examples: fractional principal ideals. Suppose that R is an integral domain. Then for every nonzero $r \in R$, the principal ideal (r) is isomorphic to R as an R-module, so (r) is an invertible R-module. More generally, let $K = \mathrm{Frac}(R)$, and define *fractional principal ideals* as R-submodules of K of the form $(\alpha) := \alpha \cdot R$ for some $\alpha \in K$. They are also invertible R-modules. We have $(a)(b) = (ab)$ and $(a)(a^{-1}) = (1)$ for every $a, b \in K^\times$. So the fractional principal ideals form a group, denoted by $\mathrm{Prin}(R)$.

Exercise 14.6. Show that $\mathrm{Prin}(R) \simeq K^\times / R^\times$.

Note that since every fractional principal ideal is isomorphic to R, it is zero in $\mathrm{Pic}(R)$. Finally, we note that $R_f = \cup_{i \in \mathbf{Z}} (f^i)$ for every nonzero $f \in R$.

14.4. Invertible modules and fractional ideals. Let M be an invertible R-module. Then there exists $h \in R$ together with an isomorphism $\phi : M_h \xrightarrow{\sim} R_h$ of R_h-modules. Suppose that R is an integral domain and let $K := \mathrm{Frac}(R)$. Since M is torsion free, the localization $M \hookrightarrow M_h$ is injective. We consider the composition of injective morphisms of R-modules
$$M \hookrightarrow M_h \xrightarrow{\phi} R_h \hookrightarrow K,$$
and let $I \subset K$ be the image. Since M is finite over R, necessarily $I \subset (h^k)$ for some $k \in \mathbf{Z}$.

Still assuming that R is an integral domain. In general, a nonzero R-submodule $I \subset K$ of a fractional principal ideal is called a *fractional ideal*. We just saw that invertible modules are fractional ideals. If a fractional ideal I is isomorphic (as an R-module) to some invertible module, then we call I an *invertible fractional ideal*.

Note that every ideal of R is a fractional ideal. The product IJ of two fractional ideals $I, J \subset K$, defined as the R-submodule of K generated by all $ij \in K$ with $i \in I$ and $j \in J$, is still a fractional ideal.

14.5. Fractional ideals over a local integral domain.

Proposition 14.7. *Let $(R, \mathfrak{m})$ be a local integral domain and let $K := \mathrm{Frac}(R)$. Let $I \subset K$ be a fractional ideal. The following assertions are equivalent.*

(1) I is invertible.

(2) I is principal.

(3) $I^{-1}I = (1)$, where $I^{-1} := \{ x \in K \mid xI \subset R \}$.

Proof. We've already seen that (2) implies (1). Assume that I is invertible. Since R is already local, we have an isomorphism $\phi : R \xrightarrow{\sim} I$ as R-modules. So I is equal to the fractional ideal $(\phi(1)) \subset K$. Thus (1) implies (2).

Suppose that $I = (h)$ is principal. Then $h^{-1} \in I^{-1}$, so $1 \in I^{-1}I$. Thus (2) implies (3). Finally we assume (3), and write $1 = \sum_{i=1}^{n} a_i b_i$ with $a_i \in I$ and $b_i \in I^{-1}$. Since $1 \notin \mathfrak{m}$, we have $u := a_i b_i \in R - \mathfrak{m}$ for some i. As R is local, u is invertible. Thus for any $x \in I$, we have

$$x = xu^{-1}b_i a_i \in (a_i),$$

namely $I \subset (a_i)$. Hence $I = (a_i)$, which proves (2). □

14.6. Characterizations of invertible fractional ideals. Again, let R be an integral domain and let $K := \mathrm{Frac}(R)$. For every fractional ideal $I \subset K$, define

$$I^{-1} := \{ x \in K \mid xI \subset R \}.$$

This is a natural generalization of the inverse of a fractional principal ideal, which already appears in Proposition 14.7.

We only have $I^{-1}I \subset R$, and in general the inclusion is strict. The property $I^{-1}I = R$ actually characterizes invertible fractional ideals.

Corollary 14.8. *Let R be an integral domain and let I be a fractional ideal of R. The following assertions are equivalent.*

(1) I is invertible.

(2) We have $I^{-1}I = (1)$.

Proof. Since both (1) and (2) are local properties, Corollary 14.8 is a consequence of Proposition 14.7. □

Exercise 14.9. Let $\mathbf{k}$ be a field. Show that the ideal I of $\mathbf{k}[t^2, t^3]$ generated by t^2 and t^3 is not invertible.

Invertible fractional ideals form a group, denoted by $\mathscr{I}(R)$, which contains $\mathrm{Prin}(R)$ as a subgroup.

Exercise 14.10. Show that $\mathscr{I}(R)/\mathrm{Prin}(R) \simeq \mathrm{Pic}(R)$. In other words, we have an exact sequence

$$0 \to R^\times \to K^\times \to \mathscr{I}(R) \to \mathrm{Pic}(R) \to 0.$$

Exercise 14.11. Let R be a UFD. Then every invertible fractional ideal of R is principal.

By Exercise 14.11, the Picard group $\mathrm{Pic}(R)$ is therefore an obstruction for an integral domain R to be a UFD. When R is a ring of integer, $\mathrm{Pic}(R)$ is always finite, and the cardinal of $\mathrm{Pic}(R)$ is called the *class number* of R. This is an important invariant of rings of integers, and we refer to lectures of algebraic number theory for further properties.

LECTURE 8

Krull dimension and chain conditions

15. Krull dimension of a ring

15.1. Krull dimension. Let X be a topological space. In these lectures we will only be interested in the situation where X is an affine scheme endowed with the Zariski topology. The Zariski topology is quite coarse (if we compare with e.g. the Euclidean topology). It is then reasonable to first consider the following definition of dimension; later we will see that when X is e.g. an affine algebraic closed subset over a field, it has good properties and is indeed a suitable definition.

Definition 15.1. The *(Krull) dimension* of X, denoted $\dim X$, is defined as the supremum of the length d of the chains of irreducible closed subsets

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_d$$

of X. If X is empty, we set $\dim X = -\infty$.

Here, a closed subset $Z \subset X$ is called *irreducible* if

- $Z \neq \emptyset$;
- for any closed subsets $Z_1, Z_2 \subset X$, we have $Z = Z_1 \cup Z_2$ implies $Z = Z_1$ or $Z = Z_2$.

A closed subset which is not irreducible is called *reducible*.

Remark 15.2. In algebraic geometry, the emptyset $\emptyset$ is *not* connected by convention. In these lectures we adopt such a convention.

Exercise 15.3. Show that an irreducible topological space is connected.

Exercise 15.4. Let $Y \subset X$, endowed with the topology induced from X. Show that

$$\begin{aligned} \{\, \text{Irreducible closed subsets of } Y \,\} &\to \{\, \text{Irreducible closed subsets } Z \subset X \text{ with } Z \cap Y \neq \emptyset \,\}. \\ W &\mapsto \text{the closure of } W \text{ in } X \end{aligned} \tag{15.1}$$

is well defined, injective, and preserves inclusions. Deduce that $\dim Y \leq \dim X$.

The following exercise shows that dimension is a *local* notion.

Exercise 15.5. For every $x \in X$, set

$$\dim_x X := \min \{\, \dim U \;\big|\; U \subset X \text{ is an open neighborhood of } x \,\}$$

and call it the dimension of X at x. Show that

$$\dim X = \sup_{x \in X} \dim_x X.$$

Deduce that $x \mapsto \dim_x X$ is upper semi-continuous.

15.2. Codimension. Let X be a topological space.

Definition 15.6. Let $Z \subset X$ be an *irreducible closed subset*. The *codimension* of Z in X, denoted $\operatorname{codim}_X Z$, is defined as the supremum of the length c of the chains of irreducible closed subsets

$$Z = Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_c$$

of X containing Z.

Remark 15.7. We always have

$$\operatorname{codim}_X Z + \dim Z \leq \dim X.$$

In general we do not have equality.

Exercise 15.8. Let $U \subset X$ be an open subset. Show that (15.1) is *bijective* for $Y = U$. Deduce that

$$\operatorname{codim}_U Z \cap U = \operatorname{codim}_X Z$$

whenever $Z \cap U \neq \emptyset$. For U nonempty, do we have $\dim U = \dim X$?

15.3. More on irreducible closed subsets. Let X be a topological space. An *irreducible component of* X is a maximal irreducible closed subset of X.

Proposition 15.9. *Any topological space X is the union of its irreducible components. In particular, any nonempty space X has an irreducible component.*

Proof. We can assume that $X \neq \emptyset$. Let $x \in X$ and let $(\Sigma, \subset)$ be the partially ordered set of irreducible closed subsets of X containing x. By Exercise 15.4, the closure of any point of X is irreducible, so Σ is nonempty. For any chain $Z_1 \subset Z_2 \subset \cdots$ of elements of Σ, the union $Z := \cup_i Z_i$ contains x and is still irreducible. Indeed, suppose that $Z = Z' \cup Z''$ for some closed subsets $Z', Z'' \subset X$. Since each Z_i is irreducible, there exists an infinite subsequence $\{Z_{i_j}\}$ such that $Z' \cap Z_{i_j} = Z_{i_j}$ for all j or $Z'' \cap Z_{i_j} = Z_{i_j}$ for all j. Thus $Z' = Z$ or $Z'' = Z$. Hence by Zorn's lemma, Σ contains a maximal element, which is thus an irreducible component of X containing x. □

15.4. Dimension and codimension of an affine scheme. Let R be a ring. The Krull dimension $\dim R$ of R is defined as the Krull dimension of $\operatorname{Spec}(R)$. Since there is a one-to-one order-reversing correspondence between the irreducible subsets of R and the prime ideals of R, the dimension of R is also equal to the supremum of the length d of the chains of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d$$

of R.

The following two lemmas are both consequences of Proposition 10.13.

Lemma 15.10. *We have*

$$\dim R = \sup_{\mathfrak{p} \in \operatorname{Spec}(R)} \dim R_{\mathfrak{p}}.$$

Proof. Every chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d =: \mathfrak{p}$ of prime ideals of R localizes to $\mathfrak{p}_0 R_{\mathfrak{p}} \subsetneq \mathfrak{p}_1 R_{\mathfrak{p}} \subsetneq \cdots \subsetneq \mathfrak{p}_d R_{\mathfrak{p}}$ by Proposition 10.13. So $\dim R \leq \sup_{\mathfrak{p} \in \operatorname{Spec}(R)} \dim R_{\mathfrak{p}}$ We use Proposition 10.13 again to show that $\dim R \geq \dim R_{\mathfrak{p}}$ for any $\mathfrak{p} \in \operatorname{Spec}(R)$. □

Exercise 15.11. Show that $\dim R_{\mathfrak{p}} \leq \dim_{\mathfrak{p}} \operatorname{Spec}(R)$, and that the inequality is strict in general.

Lemma 15.12. *Let $\mathfrak{p} \in \operatorname{Spec}(R) =: X$ and let $Y = \overline{\mathfrak{p}} \subset X$. We have*

$$\operatorname{codim}_X Y = \dim R_{\mathfrak{p}}.$$

Proof. This is because we have a one-to-one order-preserving correspondence between the prime ideals of $R_{\mathfrak{p}}$ and the prime ideals of R containing $\mathfrak{p}$, by Proposition 10.13. □

Exercise 15.13. Let $\mathbf{k}$ be an algebraically closed field and let $R = \mathbf{k}[X, Y, Z]/(XZ, YZ)$. Compute $\dim R$ and $\dim R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$.

Example 15.14. We have $\dim \mathbf{k}[X_1, \ldots, X_d] \geq d$, because

$$(X_1, \ldots, X_d) \supsetneq (X_1, \ldots, X_{d-1}) \supsetneq \cdots \supsetneq (X_1) \supsetneq (0).$$

Later we will see that it is actually an equality.

16. Chain conditions

16.1. Chain conditions on partially ordered sets. Let $(\Sigma, \leq)$ be a partially ordered set. We say that Σ satisfies the *ascending chain condition* (a.c.c.) if any increasing sequence

$$s_1 \leq s_2 \leq \cdots$$

in Σ is stationary after finitely many terms.

Lemma 16.1. *The following assertions are equivalent.*

(1) Σ satisfies a.c.c.

(2) Any nonempty subset of Σ has a maximal element.

Proof. Assume (2). Then any increasing sequence $s_1 \leq s_2 \leq \cdots$ has a maximal s_n. Hence the sequence is stationary after s_n. Assume that (2) does not hold. Then there exists $S \subset \Sigma$ without maximal element. We can therefore construct inductively an infinite strictly increasing sequence in S by the axiom of choice. □

Likewise, we say that Σ satisfies the *descending chain condition* (d.c.c.) if any decreasing sequence in Σ is stationary after finitely many terms.

16.2. Noetherian topological space. Here is an application of Lemma 16.1. A topological space X is called *Noetherian* if the set of closed subsets of X ordered by inclusion satisfies d.c.c. This implies $\dim X < \infty$, but not conversely (e.g. $\mathbf{R}$ with the usual topology).

Proposition 16.2. *Any closed subset of a Noetherian space X is a finite union of irreducible closed subsets.*

Proof. Suppose that the set S of closed subsets $Z \subset X$ which does not satisfy the conclusion of the proposition is nonempty. Then S has a minimal element Z by Lemma 16.1, which is necessarily reducible. So $Z = Z_1 \cup Z_2$, with Z_1, Z_2 closed subsets in X and $Z_1, Z_2 \subsetneq Z$. The minimality of Z implies that both Z_1 and Z_2 are finite unions of irreducible closed subsets, and therefore so is Z, which is a contradiction. □

Exercise 16.3. Show that a Noetherian topological space X has only finitely many irreducible components. (Hint: show that if $X = X_1 \cup \cdots \cup X_n$ where each X_i is an irreducible closed subset, and $X_i \not\subset X_j$ whenever $i \neq j$, then $X_1, \ldots, X_n$ are exactly the irreducible components of X.)

16.3. Noetherian rings. A ring R is called *Noetherian* if the set of ideals of R ordered by inclusion satisfies a.c.c.

Exercise 16.4. Let R be a Noetherian ring. Show that $\mathrm{Spec}(R)$ is Noetherian.

The converse of Exercise 16.4 does not hold in general, for instance for $R = \mathbf{k}[X_1, X_2, \ldots]/(X_1^2, X_2^2, \ldots)$ (Exercise: $(X_1, X_2, \ldots)$ is the only prime ideal of R). The spectrum $\mathrm{Spec} R$ of a ring R is Noetherian if and only if the set of *radical ideals* of R satisfies a.c.c.

The same ring $R = \mathbf{k}[X_1, X_2, \ldots]/(X_1^2, X_2^2, \ldots)$ also shows that in general, $\dim \mathrm{Spec}(R) < \infty$ does not imply that R is Noetherian. Actually the converse does not hold neither: see e.g. [**12**, 02JC] for examples of Noetherian rings having infinite dimension. We will see, however, that Noetherian *local* ring is always finite dimensional in Corollary 21.5.

Exercise 16.5. Let R be a Noetherian ring. Show that any $f \in R$ is a product of finitely many irreducible elements.

Exercise 16.6. Let R be a Noetherian ring. For every ideal $I \subset R$, show that $(\sqrt{I})^n \subset I$ for some integer $n > 0$. (Hint: $\sqrt{I}$ is finitely generated.)

Exercise 16.7. Show that any surjective endomorphism $f : R \to R$ of a Noetherian ring is an isomorphism. (Hint: consider $\ker(f) \subset \ker(f \circ f) \subset \cdots$.)

16.4. Hilbert's basis theorem.

Theorem 16.8 (Hilbert's basis theorem)**.** *Let R be a ring. If R is Noetherian, then $R[X]$ is also Noetherian.*

Proof. Let $I_0 \subset I_1 \subset \cdots$ be an ascending chain of ideals of $R[X]$. For every pair of nonnegative integers n and d, define the ideal

$$J_{n,d} := \{ \text{Leading coefficient of } P \mid P \in I_n \text{ with } \deg P = d \} \cup \{0\} \subset R.$$

We have $J_{n,d} \subset J_{n',d'}$ if $n \leq n'$ and $d \leq d'$. As R is Noetherian, there exists $n_0 \in \mathbf{Z}_{\geq 0}$ such that $J_{n,d} = J_{n_0,d}$ for all $n \geq n_0$ and all $d \in \mathbf{Z}_{\geq 0}$.

Now let $n \geq n_0$ and let $f = \sum_{i=0}^{d} a_i X^i \in I_n$ with $a_i \in R$. Then $a_d \in J_{n,d} = J_{n_0,d}$, so a_d is also the leading coefficient of some $g \in I_{n_0}$ with $\deg g = d$. It follows that $f - g \in I_n$ with $\deg(f-g) \leq d-1$, and we argue by induction on d that $f \in I_{n_0}$. □

Corollary 16.9. *Let R be a Noetherian ring (e.g. a field). Any finitely generated R-algebra is Noetherian.*

Remark 16.10. Let R be a Noetherian integral domain. The integral closure of R in $\mathrm{Frac}(R)$ is not necessarily Noetherian (see e.g. [**10**, Appendix, Example 5]).

16.5. Noetherian modules. Let R be a ring. More generally, we say that an R-module M is *Noetherian* if the set of submodules of M satisfies a.c.c. The following lemma shows that non Noetherian R-modules M are exactly the R-modules which contain non finitely generated submodules. This characterization is useful.

Lemma 16.11. *Let R be a ring and let M be and R-module. The following assertions are equivalent.*

(1) M is Noetherian.
(2) Every submodule of M is finitely generated.

Proof. Suppose that $N \subset M$ is a submodule which is not finitely generated. Consider

$$S = \{ \text{finitely generated submodules of } N \}.$$

Then S has no maximal element (by the axiom of choice). Hence M is not Noetherian.

Now assume (2). Let $N_1 \subset N_2 \subset \cdots$ be a sequence of submodules of M. Then $N := \cup_i N_i$ is also a submodule of M. By assumption, N is generated over R by finitely many elements $n_1, \ldots, n_k$, and there exists some N_m which contains them. Hence $N = N_m$. □

Corollary 16.12. *Every principal ideal domain is a Noetherian ring.*

Exercise 16.13. Let $\mathbf{k}$ be a field. Then $\mathbf{k}[X,Y]$ is Noetherian by Hilbert's basis theorem. Show that the subring of $\mathbf{k}[X,Y]$ generated by XY^i for $i \in \mathbf{Z}_{\geq 0}$ is not Noetherian.

Exercise 16.14. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of R-modules. Show that M is Noetherian if and only if both M' and M'' are Noetherian.

Lemma 16.15. *Let R be a Noetherian ring and let M be an R-module. The following assertions are equivalent.*

(1) M is finitely generated.
(2) M is finitely presented.
(3) M is Noetherian.

Proof. It is clear that (2) implies (1). Both (1) ⇒ (3) and (3) ⇒ (2) follow from Exercise 16.14. □

Lemma 16.16. *Let M be an R-module. If M is Noetherian, then $R/\mathrm{Ann}(M)$ is Noetherian.*

Proof. Up to replacing R by $R/\mathrm{Ann}(M)$, we can assume that $\mathrm{Ann}(M) = 0$. Since M is Noetherian, by Lemma 16.11 it is generated by finitely many elements $m_1, \ldots, m_k \in M$. Since $\mathrm{Ann}(M) = 0$, the morphism

$$\begin{aligned} R &\to M^k \\ r &\mapsto (rm_1, \ldots, rm_k) \end{aligned}$$

of R-modules is injective. Since M^k is Noetherian by Exercise 16.14, so is R by Lemma 16.11. □

Exercise 16.17. Let R be a Noetherian ring and let $S \subset R$ be a multiplicative subset. Show that $S^{-1}R$ is also Noetherian.

Exercise 16.18. Let M be a Noetherian R-module and let N be a finitely generated R-module. Show that $M \otimes_R N$ is Noetherian.

16.6. Artinian rings and modules. A ring R (resp. an R-module M) is called Artinian if the set of ideals of R (resp. submodules of M) ordered by inclusion satisfies d.c.c.

Exercise 16.19. Let V be a vector space over a field $\mathbf{k}$. Show that the following assertions are equivalent.

(1) V has finite dimension.
(2) V is Noetherian.
(3) V is Artinian.

Although the Noetherian and the Artinian conditions look alike, Noetherian rings and modules are much more important (mostly due to Lemma 16.11). As the following theorem indicates, Artinian rings are very specific.

Theorem 16.20. *Let R be a ring. The following assertions are equivalent.*

(1) R is an Artinian ring.
(2) R is Noetherian with $\dim R = 0$.
(3) R is Noetherian, and $\operatorname{Spec}(R)$ *is discrete and finite.*

Proof. First we show (3) ⇒ (1). The assertion (3) implies that R has only finitely many prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, and they are all maximal. By Exercise 16.6, we have $\operatorname{Nil}(R)^n = 0$ for some integer $n > 0$. Since

$$\operatorname{Nil}(R) = \bigcap_{i=1}^{n} \mathfrak{p}_i \supset \prod_{i=1}^{n} \mathfrak{p}_i,$$

there exists a finite sequence of maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_k \subset R$ such that $\mathfrak{m}_1 \cdots \mathfrak{m}_k = 0$. Let $J_0 := R$ and $J_i := \mathfrak{m}_1 \cdots \mathfrak{m}_i$. Consider the exact sequences of R-modules

$$0 \to J_{i+1} \to J_i \to J_i/J_{i+1} \to 0.$$

By induction starting from $i = 0$, all the terms in the exact sequence are Noetherian by Exercise 16.14.

Since J_i/J_{i+1} is a module over the field $R/\mathfrak{m}_{i+1}$, by Exercise 16.19 it is also an Artinian $(R/\mathfrak{m}_{i+1})$-module. As $\mathfrak{m}_{i+1} \cdot (J_i/J_{i+1}) = 0$, the quotient J_i/J_{i+1} regarded as an R-module is also Artinian. Hence by a backward induction starting from J_k and the following exercise, R is Artinian.

Exercise 16.21. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of R-modules. Show that M is Artinian if and only if both M' and M'' are Artinian.

We show (1) ⇒ (2). Suppose that R is Artinian. First we prove that $\dim R = 0$, namely every prime ideal $\mathfrak{p} \subset R$ is maximal. Let $x \in R/\mathfrak{p}$ be a nonzero element. As $A := R/\mathfrak{p}$ also satisfies d.c.c., we have $(x^n) = (x^{n+1})$ for some integer $n > 0$. So $x^n = x^{n+1}y$ for some $y \in A$. Since A is an integral domain, we have $xy = 1$. Hence x is invertible, so $\mathfrak{p}$ is a maximal ideal.

Lemma 16.22. *Let R be an Artinian ring. There exists $n \in \mathbf{Z}_{>0}$ such that* $\operatorname{Nil}(R)^n = 0$.

Proof. Since R is Artinian, there exits $n \in \mathbf{Z}_{>0}$ such that $\operatorname{Nil}(R)^n = \operatorname{Nil}(R)^{n+1} =: I$. Assume that $I \neq 0$. Consider

$$S := \{ \text{Ideals } J \subset R \mid JI \neq 0 \}.$$

Since $I \in S \neq \emptyset$, by Lemma 16.1, the set S contains a minimal element J. As $JI \neq 0$, there exists $x \in J$ such that $xI \neq 0$. So $J = (x)$ by minimality. Since $(xI)I = JI^2 = JI \neq 0$, again by minimality we have $(x) = xI$. So $xy = x$ for some $y \in I$. Since $1 - y$ is unit (because y is contained in every maximal ideal of R), necessarily $x = 0$, which is impossible. Hence $\operatorname{Nil}(R)^n = I = 0$. □

Since R is Artinian, we have

$$\mathrm{Nil}(R) = \bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p} = \bigcap_{i=1}^{n} \mathfrak{p}_i \supset \prod_{i=1}^{n} \mathfrak{p}_i$$

for some prime, and therefore maximal, ideals $\mathfrak{p}_i$. So there exists a finite sequence of maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_k \subset R$ such that $\mathfrak{m}_1 \cdots \mathfrak{m}_k = 0$. Set $J_0 := R$ and $J_i := \mathfrak{m}_1 \cdots \mathfrak{m}_i$, and consider again the exact sequences of R-modules

$$0 \to J_{i+1} \to J_i \to J_i/J_{i+1} \to 0.$$

The same argument as before, exchanging Noetherian with Artinian, shows that R is Noetherian.

Now we show (2) ⇒ (3). Since $\dim R = 0$, every point of $\mathrm{Spec}(R)$ is a closed point, and each closed point is a maximal irreducible closed subset of $\mathrm{Spec}(R)$. If follows from Exercise 16.3 that $\mathrm{Spec}(R)$ is finite, hence also discrete because every point of $\mathrm{Spec}(R)$ is a closed. □

Exercise 16.23. Let p be a prime number. Show that the $\mathbf{Z}$-module $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ is Artinian but not Noetherian.

16.7. Length, composition series, Jordan–Hölder property. Let R be a ring and let M be an R-module. The module M is called *simple* if the only submodules of M are itself and 0.

Exercise 16.24. Show that an R-module M is simple if and only if $M \simeq R/\mathfrak{m}$ as R-modules for some maximal ideal $\mathfrak{m} \subset R$.

A *composition series* of an R-module M is a finite filtration

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$$

of R-submodules such that each graded piece M_i/M_{i+1} is a nonzero simple R-module.

Exercise 16.25. Show that the following assertions are equivalent:

(1) M has a composition series.
(2) M is both Noetherian and Artinian.

Exercise 16.26. Suppose that M has a composition series (M_i) of length n. Prove the following statements.

(1) Any strictly decreasing sequence of submodules can be completed to a composition series.
(2) Any composition series of M has length n.
(3) (Jordan-Hölder property) Moreover, if (M'_i) is another composition series, then up to a permutation of indices, we have $M_i/M_{i+1} \simeq M'_i/M'_{i+1}$ as R-modules for all i.

The length $\mathrm{lg}(M)$ of an R-module M is defined as the length of any of its composition series if they exist, otherwise $\mathrm{lg}(M) := \infty$.

Exercise 16.27. Let

$$0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$$

be an exact sequence of R-modules. Show that $\sum_{i=1}^{n}(-1)^i \mathrm{lg}(M_i) = 0$.

For the details, (i.e. the solutions of the exercises), we refer to [**4**, Chapter 6].

17. Associated points of modules

Let R be a ring and let M be an R-module. Throughout §17, we assume that R is *Noetherian*.

17.1. Associated points.

Definition 17.1. An *associated point* of M is the generic point $\mathfrak{p} \subset \mathrm{Spec}(R)$ of an irreducible component of $\mathrm{Supp}(m) = V(\mathrm{Ann}(m))$ (by Proposition 10.34) for some $m \in M$. They form a subset of $\mathrm{Spec}(R)$, denoted by $\mathrm{Ass}(M)$.

Exercise 17.2. Let $\mathbf{k}$ be a field. Find the associated points and the embedded points of $R = \mathbf{k}[X, Y]/(Y^2, XY)$. Draw a picture.

Exercise 17.3. Let R be an integral domain and let $I \subset R$ be a nonzero ideal (e.g. $I = R$). Show that (0) is the only associated point of I. Let $\mathfrak{p} \subset R$ be a prime ideal. Viewing $R/\mathfrak{p}$ as an R-module, show that $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

The above exercise implies in particular that every element in a minimal prime ideal $\mathfrak{p}$ of R is a zero divisor. This is true in general (without assuming R Noetherian)

Lemma 17.4. *Let R be a (not necessarily) ring and let $\mathfrak{p} \subset R$ be a minimal prime ideal. Every $z \in \mathfrak{p}$ is a zero divisor.*

Proof. Since $\mathfrak{p}$ is a minimal prime, $\mathfrak{p}A_{\mathfrak{p}}$ is the unique prime ideal of $A_{\mathfrak{p}}$. So z is nilpotent in $A_{\mathfrak{p}}$. It follows that $z^n t = 0$ for some integer $n \geq 1$ and $t \in A - \mathfrak{p}$. □

Exercise 17.5. Let $S \subset R$ be a multiplicative subset. Show that

$$\operatorname{Ass}(S^{-1}M) = \operatorname{Ass}(M) \cap \operatorname{Spec}(S^{-1}R).$$

Lemma 17.6. *We have $M = 0$ if and only if* $\operatorname{Ass}(M) = \emptyset$.

Proof. It is clear that if $M = 0$, then $\operatorname{Ass}(M) = \emptyset$. Suppose that there exists a nonzero element $m \in M$. Then $\operatorname{Ann}(m) \neq R$, so $V(\operatorname{Ann}(m)) \neq \emptyset$. Hence the generic point of an irreducible component of $V(\operatorname{Ann}(m))$ (which exists by Proposition 15.9) is an associated point of M. □

Proposition 17.7. *Let $\mathfrak{p} \in \operatorname{Spec}(R)$. The following assertions are equivalent.*

(1) $\mathfrak{p} \in \operatorname{Ass}(M)$.

(2) $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}(M_{\mathfrak{p}})$.

(3) *There exists $m \in M_{\mathfrak{p}}$ such that* $\sqrt{\operatorname{Ann}(m)} = \mathfrak{p}R_{\mathfrak{p}}$.

Proof. The equivalence (1) ⇔ (2) follows from Exercise 17.5. It is clear that (3) ⇒ (2). Now assume (2). Then there exists $m \in M_{\mathfrak{p}}$ such that $V(\mathfrak{p}R_{\mathfrak{p}})$ is an irreducible component of $V(\operatorname{Ann}(m))$. So $\mathfrak{p}R_{\mathfrak{p}}$ is a minimal prime ideal of $R_{\mathfrak{p}}$ which contains $\operatorname{Ann}(m)$. Since any prime ideal of $R_{\mathfrak{p}}$ is contained in $\mathfrak{p}R_{\mathfrak{p}}$, necessarily $\sqrt{\operatorname{Ann}(m)} = \mathfrak{p}R_{\mathfrak{p}}$. □

Exercise 17.8. (Compare Exercise 10.36.) Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of R-modules. Show that

- $\operatorname{Ass}(M') \subset \operatorname{Ass}(M)$;
- $\operatorname{Ass}(M) \subset \operatorname{Ass}(M') \cup \operatorname{Ass}(M'')$.

(Hint: use Proposition 17.7.)

17.2. Embedded points.

Proposition-Definition 17.9. *Assume that M is a finite R-module.*

(1) *We have* $\operatorname{Ass}(M) \subset \operatorname{Supp}(M)$.

(2) *The generic points of the irreducible components of* $\operatorname{Supp}(M)$ *belong to* $\operatorname{Ass}(M)$. *The other elements of* $\operatorname{Ass}(M)$ *are called the* embedded points *of M.*

Proof. The first assertion is clear. Suppose that M is generated by $m_1, \ldots, m_k$. Then $\operatorname{Supp}(M) = \bigcup_{i=1}^k \operatorname{Supp}(m_i)$ by Corollary 10.35. Since the union is finite and each $\operatorname{Supp}(m_i)$ is closed, an irreducible component Z of $\operatorname{Supp}(M)$ is necessarily an irreducible component of some $\operatorname{Supp}(m_i)$. □

Example 17.10. If $R = \mathbf{k}[X, Y]/(Y^2, XY)$, then (X, Y) is an embedded point of $\operatorname{Spec}(R)$.

Exercise 17.11. Let $R = \mathbf{Z}$ and $M = \mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$ where $n \geq 1$ is an integer. Compute $\operatorname{Ass}(M)$ and find all the embedded points of M.

Remark 17.12. Our definition of associated points also makes sense without assuming R to be Noetherian, and they are called *weakly associated points* in [**12**, Tag 0546]. For a module M over an arbitrary ring R, the associated points of M are the points $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $\mathfrak{p} = \mathrm{Ann}(m)$ for some $m \in M$. It is clear that associated points are weakly associated points. Our definition of associated points when the ring R is Noetherian is justified by the following result.

Lemma 17.13. *Let M be a module over a Noetherian ring R. Then weakly associated points of M coincide with associated points of M.*

Proof. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ be a weakly associated point of M. As R is Noetherian, we have $\mathfrak{p} = (f_1, \dots, f_k)$. By Proposition 17.7, there exists $m \in M$ and $f \in R - \mathfrak{p}$ such that $\sqrt{\mathrm{Ann}(m/f)} = \mathfrak{p}R_{\mathfrak{p}}$. In particular, for all index i, we have $f_i^{e_i} m/f = 0$ in $M_{\mathfrak{p}}$. So up to replacing m by $f_1^{n_1} \cdots f_1^{n_k} m/f$ for some suitable integers $n_1, \dots, n_k$, and noting that it only increases $\sqrt{\mathrm{Ann}(m/f)}$ but $\sqrt{\mathrm{Ann}(m/f)} = \mathfrak{p}R_{\mathfrak{p}}$ is already maximal, we can assume that $f_i m/f = 0$ for all i but still $m/f \neq 0$. Hence $\mathfrak{p}R_{\mathfrak{p}} = \mathrm{Ann}(m/f)$. It follows that $\mathfrak{p} \subset \mathrm{Ann}(m)$. Since $\mathfrak{p}R_{\mathfrak{p}}$ is the maximal ideal of the local ring $R_{\mathfrak{p}}$, necessarily $\mathfrak{p} = \mathrm{Ann}(m)$. □

Exercise 17.14. Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module. Show that $\mathfrak{m} \in \mathrm{Ass}(M)$ if and only if every element of $\mathfrak{m}$ is a zero divisor of M.

17.3. A filtration on finite modules over a Noetherian ring.

Proposition 17.15. *Let R be a Noetherian ring and let M be a finite R-module. There exists a finite filtration*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

such that for every index i, we have $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ as R-modules for some prime ideal $\mathfrak{p}_i \subset R$.

Recall that if each $\mathfrak{p}_i$ is maximal, then such a filtration is a composition series of M, which is a rather special situation.

Proof. Suppose that $M \neq 0$. Then there exists $\mathfrak{p}_1 \in \mathrm{Ass}(M)$ by Lemma 17.6. So there exists $m \in M$ such that $\mathrm{Ann}(m) = \mathfrak{p}_1$ by Lemma 17.13. It follows that $M_1 := R \cdot m \subset M$ is isomorphic to $R/\mathfrak{p}_1$. Replacing M by M/M_1 and repeating the same procedure give rise to an ascending chain

$$0 = M_0 \subset M_1 \subset \cdots$$

such that each graded piece satisfies $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i \subset R$. We conclude by the ascending chain condition of M. □

Exercise 17.16. Let R be a Noetherian ring and let M be a finite R-module. Show that $\mathrm{Supp}(M)$ is a finite set of closed points if and only if M has finite length.

Corollary 17.17. *Let R be a Noetherian ring and let M be a finite R-module. Then* $\mathrm{Ass}(M)$ *is finite.*

Proof. Since for any prime ideal $\mathfrak{p} \subset R$, the R-module $R/\mathfrak{p}$ satisfies $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$, Corollary 17.17 follows from Proposition 17.15 and Exercise 17.8. □

LECTURE 9

Dimension and integral morphisms

18. Finite and integral morphisms

A ring homomorphism $A \to B$ is called *finite* if the induced *A-module* structure on B is finitely generated. A morphism of affine schemes $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is called finite if it is defined by a finite ring homomorphism $A \to B$.

Example 18.1. Let $\mathbf{k}$ be a field. If A is a finite $\mathbf{k}$-algebra, then A is Artinian. In particular, the underlying topological space of $\mathrm{Spec}(A)$ is finite and discrete by Theorem 16.20.

Exercise 18.2.

(1) Show that the composition of two finite morphisms is finite.

(2) Let

$$\begin{tikzcd} \mathrm{Spec}(B \otimes_A C) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & \mathrm{Spec}(B) \arrow[d] \\ \mathrm{Spec}(C) \arrow[r] & \mathrm{Spec}(A) \end{tikzcd}$$

be a cartesian square of affine schemes. Suppose that $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is finite. Show that the base change $\mathrm{Spec}(B \otimes_A C) \to \mathrm{Spec}(C)$ is also finite.

Proposition 18.3. *Every finite morphism $\pi : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ has finite fibers.*

Proof. Let $\mathfrak{p} \in \mathrm{Spec}(A)$. It suffices to show that $\mathrm{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ is finite, since it is the scheme-theoretic fiber of $\mathfrak{p}$ (see § 10.12). Since $A \to B$ is finite, so is the base change $\kappa(\mathfrak{p}) \to B \otimes_A \kappa(\mathfrak{p})$, and we've seen in Example 18.1 that $\mathrm{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ is finite. □

18.1. Noether normalization. Let $\mathbf{k}$ be a field and let A be a nonzero *finitely generated* $\mathbf{k}$-algebra. The following theorem asserts that there always exists a finite $\mathbf{k}$-morphism from $\mathrm{Spec}(A)$ onto an affine space.

Theorem 18.4 (Noether normalization lemma)**.** *There exists an injective finite morphism of $\mathbf{k}$-algebras*

$$\mathbf{k}[X_1, \dots, X_n] \hookrightarrow A$$

for some integer $n \geq 0$.

When $\mathbf{k}$ is an infinite field, one strategy of proving Theorem 18.4 is the following. By assumption, we have a surjective morphism $\mathbf{k}[Y_1, \dots, Y_m] \twoheadrightarrow A$ of $\mathbf{k}$-algebra, and therefore an embedding $\mathrm{Specm}(A) \subset \mathbf{A}^m_{\mathbf{k}}$. If $\mathbf{k}$ is an infinite field, then one can find some linear projection $\mathbf{A}^m_{\mathbf{k}} \to \mathbf{A}^{m-1}_{\mathbf{k}}$ whose restriction to $\mathrm{Specm}(A)$ is finite. We continue until $\mathrm{Specm}(A)$ projects finitely onto some $\mathbf{A}^n_{\mathbf{k}}$.

Proof of Theorem 18.4. We have

$$A \simeq \mathbf{k}[Y_1, \dots, Y_m]/I$$

as $\mathbf{k}$-algebras, where $m \in \mathbf{Z}_{\geq 0}$ and $I \subset \mathbf{k}[Y_1, \dots, Y_m]$ is an ideal which is not (1). We prove Theorem 18.4 by induction on m.

For $m = 0$, the structural morphism $\mathbf{k} \to A$ does the job. Suppose that Theorem 18.4 is proven for $m - 1$. If $I = (0)$, then we already have $\mathbf{k}[Y_1, \dots, Y_m] \simeq A$, so we assume $I \neq (0)$. It suffices to find $y_1, \dots, y_{m-1} \in \mathbf{k}[Y_1, \dots, Y_m]$ such that $\mathbf{k}[y_1, \dots, y_{m-1}] \to A$ is finite: A is then finite over the $\mathbf{k}$-subalgebra

$A' \subset A$ generated by $y_1, \ldots, y_{m-1}$, and by the induction hypothesis, we have a finite injective morphism $\mathbf{k}[X_1, \ldots, X_n] \hookrightarrow A'$ of $\mathbf{k}$-algebras. Hence the composition $\mathbf{k}[X_1, \ldots, X_n] \hookrightarrow A' \hookrightarrow A$ is also finite.

We can assume that $I = (f)$ for some $f \neq 0 \in \mathbf{k}[Y_1, \ldots, Y_m]$. For $i = 1, \ldots, m-1$, set $y_i = Y_i - Y_m^{e_{m-1}} \in \mathbf{k}[Y_1, \ldots, Y_m]$. It suffices to show that the image of Y_m in A is integral over $\mathbf{k}[y_1, \ldots, y_{m-1}]$, and we conclude by Corollary 3.8 and Proposition 3.2. This follows from the following exercise.

Exercise 18.5. Show that there exist positive integers $e_1 \gg e_2 \gg \cdots \gg e_{m-1}$ such that

$$f(y_1 + Y_m^{e_1}, \ldots, y_{m-1} + Y_m^{e_{m-1}}, Y_m) = aY_m^d + (\text{lower degree terms in } Y_m)$$

for some $a \neq 0 \in \mathbf{k}$. (If $\mathbf{k}$ is infinite, the construction is simpler: show that there exist $\lambda_1, \ldots, \lambda_{m-1} \in \mathbf{k}$ such that

$$f(y_1 + \lambda_1 Y_m, \ldots, y_{m-1} + \lambda_{m-1} Y_m, Y_m) = aY_m^d + (\text{lower degree terms in } Y_m)$$

for some $a \neq 0 \in \mathbf{k}$.)

□

18.2. Lying-over property. A ring homomorphism $\phi : A \to B$ is called *integral* if $\phi(A) \subset B$ is an integral extension. By Proposition 3.2, any finite ring homomorphism is integral.

Exercise 18.6. Show that the composition of integral morphisms is integral, and that integral morphisms are preserved under base change. Namely, prove the statements in Exercise 18.2, replacing "finite" by "integral.

Exercise 18.7. Let $\mathbf{k}$ be a field and let $\mathbf{k} \hookrightarrow A$ be an integral extension. Show that $\dim A = 0$, namely every prime ideal of A is maximal. (Hint: integral domain + finite over $\mathbf{k} \Rightarrow$ field.)

Proposition 18.8 (Lying-over property). *Let $\phi : A \to B$ be an injective ring homomorphism. If ϕ is integral, then the induced morphism* Spec(B) $\to$ Spec(A) *of affine schemes is surjective.*

Proof. We have to show that for every $\mathfrak{p} \in \operatorname{Spec}(A)$, its scheme-theoretic fiber $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ is nonempty; in other words, $\mathfrak{p}B_{\mathfrak{p}} \subsetneq B_{\mathfrak{p}}$.

Assume to the contrary that $\mathfrak{p}B_{\mathfrak{p}} = B_{\mathfrak{p}}$. Then $1 = \sum_{i=1}^n f_i b_i$ with $f_i \in \mathfrak{p}$ and $b_i \in B_{\mathfrak{p}}$. Since $A \hookrightarrow B$ is integral, so is $A_{\mathfrak{p}} \hookrightarrow B_{\mathfrak{p}}$ by Proposition 10.37. So if $M \subset B_{\mathfrak{p}}$ is the $A_{\mathfrak{p}}$-subalgebra generated by $b_1, \ldots, b_n$, then M is finite as an $A_{\mathfrak{p}}$-module by Corollary 3.6. As $1 = \sum_{i=1}^n f_i b_i$ implies $(\mathfrak{p}A_{\mathfrak{p}})M = M$, we conclude by Nakayama's lemma that $M = 0$, which is impossible. □

Exercise 18.9. Show that an integral morphism Spec(B) $\to$ Spec(A) of affine schemes is closed.

18.3. Dimension and integral extensions.

Corollary 18.10 (Going-up property). *Let $A \to B$ be an integral ring homomorphism and let f :* Spec(B) $\to$ Spec(A) *be the induced morphism of affine schemes. Let $\mathfrak{p} \subset \mathfrak{p}' \subset A$ be prime ideals of A. If there exists $\mathfrak{q} \in f^{-1}(\mathfrak{p})$, then there exists $\mathfrak{q}' \in f^{-1}(\mathfrak{p}')$ such that $\mathfrak{q} \subset \mathfrak{q}'$.*

Proof. The homomorphism $A \to B$ induces an injective integral ring homomorphism $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$. So there exists $\overline{\mathfrak{q}'} \in \operatorname{Spec}(B/\mathfrak{q})$ lying over $\mathfrak{p}'/\mathfrak{p} \in \operatorname{Spec}(A/\mathfrak{p})$ by Proposition 18.8. A preimage $\mathfrak{q}' \in \operatorname{Spec}(B)$ of $\overline{\mathfrak{q}'}$ satisfies the conclusion of the corollary. □

Proposition 18.11. *Let $A \to B$ be an integral ring homomorphism and let f :* Spec(B) $\to$ Spec(A) *be the induced morphism of affine schemes. Let $\mathfrak{p} \in$* Spec(A) *and let $\mathfrak{q}, \mathfrak{q}' \in f^{-1}(\mathfrak{p})$. Then neither $\mathfrak{q} \subset \mathfrak{q}'$ nor $\mathfrak{q}' \subset \mathfrak{q}$. In other words, all the (scheme-theoretic) fibers of f have dimension* 0.

Proof. Since $A \to B$ is integral, so is $\kappa(\mathfrak{p}) \to B \otimes_A \kappa(\mathfrak{p})$ by Exercise 18.6. So by Exercise 18.7, every prime ideal of $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ is maximal. Since the bijection $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p})) \xrightarrow{\sim} f^{-1}(\mathfrak{p})$ is order-preserving, the first statement of Proposition 18.11 follows. The last statement follows from Lemma 10.30. □

The following proposition shows that integral extensions preserve dimension.

Corollary 18.12. *Let $\phi : A \to B$ be an integral ring homomorphism. Then* $\dim A \geq \dim B$. *If moreover ϕ is injective, then* $\dim A = \dim B$.

Proof. The first statement follows from Proposition 18.11. The second statement follows from the lying-over property and the going-up property. □

18.4. Galois actions. Let K be a field and let $A \subset K$ be subring. Let L/K be a field extension and let $B \subset L$ be the integral closure of A in L. As the $\mathrm{Aut}(L/K)$-action on L fixes A, the subring $B \subset L$ is stable under $\mathrm{Aut}(L/K)$-action. Also for every prime ideal $\mathfrak{p} \subset A$, the automorphism group $\mathrm{Aut}(L/K)$ acts on the set of prime ideals of B lying over $\mathfrak{p}$.

The following proposition could be regarded as a generalization of the transitivity of the Galois action on the conjugate elements for normal field extensions.

Proposition 18.13. *Let A be an integrally closed domain and let $K = \mathrm{Frac}(A)$. Let L/K be a normal extension and let B be the integral closure of A in L. For every prime ideal $\mathfrak{p} \subset A$, the Galois group $\mathrm{Aut}(L/K)$ acts transitively on the set of prime ideals of B lying over $\mathfrak{p}$.*

Proof, assuming that L/K is finite. We only proof Proposition 18.13 in the case where L/K is finite, and refer to [7, Proof of Theorem 9.3.(iii)] for the general case. Then $\mathrm{Aut}(L/K) = \{ \sigma_1, \ldots, \sigma_d \}$ is finite. Let $\mathfrak{q}, \mathfrak{q}' \subset B$ be two prime ideals lying over $\mathfrak{p}$, and suppose that $\mathfrak{q}' \neq \sigma_j(\mathfrak{q})$ for all j. Then $\mathfrak{q}' \not\subset \sigma_j(\mathfrak{q})$ by Proposition 18.11. So by prime avoidance, there exists $x \in \mathfrak{q}'$ such that $x \notin \sigma_j(\mathfrak{q})$ for all j. Since $\sigma_j(x) \notin \mathfrak{q}$ for all j, we also have $\mathrm{Nm}_{L/K}(x) = \left(\prod_{j=1}^{n} \sigma_j(x)\right)^{[L:K(x)]} \notin \mathfrak{q}$ by Exercise 18.14. As $\mathrm{Nm}_{L/K}(x) \in B \cap K$ and A is integrally closed, we have $\mathrm{Nm}_{L/K}(x) \in A$. Since x divides $\mathrm{Nm}_{L/K}(x)$ in B, we also have $\mathrm{Nm}_{L/K}(x) \in \mathfrak{q}'$. But then $\mathrm{Nm}_{L/K}(x) \in \mathfrak{q}' \cap A = \mathfrak{p} \subset \mathfrak{q}$, which is a contradiction. □

Exercise 18.14. Let L/K be a normal field extension. Let $\alpha \in L$. Let $P_\alpha \in K[X]$ be the minimal polynomial of α and let $c_\alpha \in K[X]$ be the characteristic polynomial of the K-linear map

$$\begin{aligned} \mu_\alpha : L &\to L \\ x &\mapsto \alpha x. \end{aligned}$$

Show that

$$c_\alpha = P_\alpha^{[L:K(\alpha)]}.$$

Deduce that

$$\mathrm{Nm}_{L/K}(\alpha) := \det \mu_\alpha = \left(\prod_{\sigma \in \mathrm{Aut}(L/K)} \sigma(\alpha) \right)^{[L:K(\alpha)]}.$$

We call $\mathrm{Nm}_{L/K} : L \to K$ the *norm* map.

19. Dimension of finitely generated k-algebras

Krull dimension and codimension have better behavior for finitely generated algebras over a field **k**. For instance, we will see that the inequality in Remark 15.7 is always an equality.

19.1. Transcendence bases. Let $K/\mathbf{k}$ be a field extension. A collection of elements $\{x_i \in K\}_{i \in I}$ is called *algebraically independent* if the morphism of **k**-algebras

$$\mathbf{k}[X_i; i \in I] \to K$$

sending X_i to x_i is injective. We say that $K/\mathbf{k}$ is a *purely transcendental extension* if

$$K \simeq \mathbf{k}(X_i; i \in I)$$

as **k**-algebras.

Lemma-Definition 19.1. *There exist algebraically independent elements $\{x_i \in K\}_{i \in I}$ such that the subfield F they generate is purely transcendental over* **k**, *and K/F is algebraic. We call $\{x_i \in K\}_{i \in I}$ a transcendence basis of $K/\mathbf{k}$.*

Proof. Consider

$$\Sigma := \{\, S \subset K \;\big|\; S \text{ algebraically independent over } \mathbf{k} \,\}$$

ordered by inclusion. We have $\Sigma \neq \emptyset$ (because $\emptyset \in \Sigma$), and every chain $S_1 \subset S_2 \subset \cdots$ is contained in $\cup_i S_i$, which is also in Σ. Thus by Zorn's lemma, Σ has a maximal element B. By construction, K is algebraic over $F = \mathbf{k}(B)$. □

Exercise 19.2. By adapting the above argument, show that any subset $G \subset K$ such that $\mathbf{k}(G) = K$ contains a transcendence basis.

Example 19.3. Let A be a finitely generated $\mathbf{k}$-algebra which is an integral domain, and let $K = \mathrm{Frac}(A)$. The Noether normalization lemma asserts that we even have a finite extension $\mathbf{k}[X_1, \dots, X_n] \hookrightarrow A$ of $\mathbf{k}$-algebras. Taking the fractional fields yields a transcendence basis of $K/\mathbf{k}$.

Lemma-Definition 19.4. *Either all the transcendence bases of $K/\mathbf{k}$ are finite and have the same cardinality, or all the transcendence bases of $K/\mathbf{k}$ are infinite. The* transcendental degree *of K over $\mathbf{k}$ is defined as the cardinal (resp. ∞) in the first (resp. second) case. It is denoted* $\mathrm{trdeg}_{\mathbf{k}} K \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$.

Proof. Let B and B' be two transcendence bases of $K/\mathbf{k}$. Suppose that $|B| \geq |B'|$. We can assume that $B' = \{\, \beta_1, \dots, \beta_n \,\}$ is finite. For any $\alpha_1 \in B$, since B' is a transcendence basis, there exists a polynomial $f \in \mathbf{k}[X, Y_1, \dots, Y_n]$ involving X such that

$$f(\alpha_1, \beta_1, \dots, \beta_n) = 0. \tag{19.1}$$

The polynomial f also involves one of Y_i, which we can assume to be Y_1.

We claim that $B'' := \{\, \alpha_1, \beta_2, \dots, \beta_n \,\}$ is a transcendence basis of $K/\mathbf{k}$. That f involves Y_1, implies that β_1 is algebraic over B'', so the extensions $K/\mathbf{k}(B'', \beta_1)/\mathbf{k}(B'')$ are algebraic. Assume to the contrary that B'' is not algebraically independent over $\mathbf{k}$. Since $\{\, \beta_2, \dots, \beta_n \,\}$ is algebraically independent, α_1 is then algebraic over $\mathbf{k}(\beta_2, \dots, \beta_n)$. But then β_1 is algebraic over $\mathbf{k}(\beta_2, \dots, \beta_n)$ by (19.1), which contradicts the assumption that B' is algebraically independent.

After finitely many substitutions as above, we obtain a subset $\{\, \alpha_1, \dots, \alpha_n \,\} \subset B$ of cardinal n which is a transcendence basis of $K/\mathbf{k}$, so necessarily $B = \{\, \alpha_1, \dots, \alpha_n \,\}$. □

Exercise 19.5. Let $K/L/\mathbf{k}$ be field extensions. Show that

$$\mathrm{trdeg}_{\mathbf{k}} K = \mathrm{trdeg}_{\mathbf{k}} L + \mathrm{trdeg}_L K.$$

Exercise 19.6. Let $f \in \mathbf{k}[X_1, \dots, X_d]$ be an irreducible element and let K be the field of fractions of $\mathbf{k}[X_1, \dots, X_d]/(f)$. Show that

$$\mathrm{trdeg}_{\mathbf{k}} K = d - 1.$$

19.2. Dimension and transcendental degree. Let $\mathbf{k}$ be a field and let A be a nonzero finitely generated $\mathbf{k}$-algebra.

Theorem 19.7. *Any injective finite morphism of $\mathbf{k}$-algebras*

$$R := \mathbf{k}[X_1, \dots, X_n] \hookrightarrow A$$

satisfies $n = \dim A$.

Proof. Since finite morphisms are integral, we have $\dim A = \dim R$ by Corollary 18.12. Therefore it suffices to prove Theorem 19.7 assuming that A is an *integral domain*; we now prove this by induction on $n \geq 0$.

If $n = 0$, then A is a finite $\mathbf{k}$-algebra. It follows that A is Artinian, so $\dim A = 0$ by Theorem 16.20. Now suppose that the statement is proven up to $n - 1$. We only need to show that $\dim R = n$. We've already seen that $\dim R \geq n$. Let $0 = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ be a chain of prime ideals of R. Up to replacing $\mathfrak{p}_1$ by (f) where $f \in \mathfrak{p}_1$ is an irreducible element of R, we can assume that $\mathfrak{p}_1 = (f)$. By the Noether normalization lemma, there exists an injective finite morphism of $\mathbf{k}$-algebras

$$\mathbf{k}[Y_1, \dots, Y_l] \hookrightarrow R/(f),$$

which induces a field extension

$$\mathbf{k}(Y_1, \ldots, Y_l) \hookrightarrow \mathrm{Frac}(R/(f)) =: K.$$

Since the images of $X_1, \ldots, X_n$ in K generate K without being algebraically independent, we have $\mathrm{trdeg}_{\mathbf{k}}\mathrm{Frac}(R/(f)) \leq n-1$ by Exercise 19.2. It follows from Exercise 19.5 that $l \leq n-1$, so $\dim R/(f) = l \leq n-1$ by the induction hypothesis. Since $(0) \subset \mathfrak{p}_2/\mathfrak{p}_1 \cdots \subset \mathfrak{p}_m/\mathfrak{p}_1$ is a sequence of prime ideals of $R/(f)$, we have $m \leq n$. Hence $\dim R \leq n$. □

Corollary 19.8. *Let A be a finitely generated* $\mathbf{k}$*-algebra which is an integral domain. Let $K := \mathrm{Frac}(A)$. We have*

$$\dim A = \mathrm{trdeg}_{\mathbf{k}} K.$$

Proof. We can assume that A is nonzero. Then this follows from the Noether normalization lemma and Theorem 19.7. □

LECTURE 10

Codimension

20. Catenary spaces

Let X be a topological space. We call X *catenary* if for every pair of irreducible closed subsets $Y, Y' \subset X$ with $Y \subset Y'$, we have $\operatorname{codim}_{Y'} Y < \infty$ and that all maximal chains of irreducible closed subsets between Y and Y' have the same length.

For an irreducible catenary space, the following exercise implies that the inequality in Remark 15.7 is always an equality.

Exercise 20.1. Show that the following statements are equivalent.

(1) X is catenary.

(2) For every triplet of nested irreducible closed subsets $Y_1 \subset Y_2 \subset Y_3$, we have $\operatorname{codim}_{Y_2} Y_1 < \infty$ and

$$\operatorname{codim}_{Y_3} Y_1 = \operatorname{codim}_{Y_3} Y_2 + \operatorname{codim}_{Y_2} Y_1.$$

20.1. Catenary rings. Let R be a ring. We call R *catenary* if $\operatorname{Spec}(R)$ is catenary.

Exercise 20.2. Suppose that for every pair of strictly nested prime ideals $\mathfrak{p} \subsetneq \mathfrak{p}'$ of R such that $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{p}'$ implies $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{q} = \mathfrak{p}'$ for every prime ideal $\mathfrak{q}$ of R, we have

$$\dim R/\mathfrak{p} = 1 + \dim R/\mathfrak{p}'.$$

Show that R is catenary.

Let $\mathbf{k}$ be a field. Irreducible affine $\mathbf{k}$-varieties are catenary.

Theorem 20.3. *Let $\mathbf{k}$ be a field and let A be a finitely generated $\mathbf{k}$-algebra. Suppose that $X := \operatorname{Spec}(A)$ is irreducible. Then A is catenary. In particular, for every $\mathfrak{p} \in \operatorname{Spec}(A)$, we have*

$$\dim X = \dim Y + \dim A_{\mathfrak{p}}$$

where $Y := \overline{\{\mathfrak{p}\}} \subset X$.

The proof of Theorem 20.3 that we will present rely on the going-down property of some integral extension that we shall prove first.

20.2. Going down.

Proposition 20.4 (Going-down property)**.** *Let A be an integrally closed domain and let $A \subset B$ be an integral extension with B an integral domain. Let $f : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ be the induced morphism of affine schemes Let $\mathfrak{p} \subset \mathfrak{p}' \subset A$ be a pair of nested prime ideals of A. If there exists $\mathfrak{q}' \in f^{-1}(\mathfrak{p}')$, then there exists $\mathfrak{q} \in f^{-1}(\mathfrak{p})$ such that $\mathfrak{q} \subset \mathfrak{q}'$.*

Proof. Let $K = \operatorname{Frac}(A)$ and let L/K be a normal closure of $\operatorname{Frac}(B)/K$. Let $C \subset L$ be the integral closure of A in L. By Proposition 18.8, there exist prime ideal $\widetilde{\mathfrak{q}'}, \widetilde{\mathfrak{q}_1} \subset C$ lying over $\mathfrak{q}' \subset B$ and $\mathfrak{p} \subset A$, respectively. By the going-up property, there exists a prime ideal $\widetilde{\mathfrak{q}_1'} \subset C$ such that $\widetilde{\mathfrak{q}_1} \subset \widetilde{\mathfrak{q}_1'}$ and $\widetilde{\mathfrak{q}_1'} \cap A = \mathfrak{p}'$. Since both $\widetilde{\mathfrak{q}'}, \widetilde{\mathfrak{q}_1'} \subset C$ lie over $\mathfrak{p}' \subset A$, by Proposition 18.13 there exists $\sigma \in \operatorname{Aut}(L/K)$ such that $\sigma(\widetilde{\mathfrak{q}_1'}) = \widetilde{\mathfrak{q}'}$. Then $\mathfrak{q} := B \cap \sigma(\widetilde{\mathfrak{q}_1})$ satisfies the conclusion of Proposition 29.15. □

Corollary 20.5. *Let* $\mathbf{k}$ *be a field and let* A *be a finitely generated reduced* $\mathbf{k}$*-algebra such that* $X := \operatorname{Spec}(A)$ *is irreducible. For every minimal nonzero prime ideal* $\mathfrak{p} \in \operatorname{Spec}(A)$*, we have*

$$\dim X = \dim Y + 1$$

where $Y := \overline{\{\mathfrak{p}\}} \subset X$*.*

Proof. First we assume that $A = \mathbf{k}[X_1, \ldots, X_d]$. Since $\mathfrak{p}$ is minimal, we have $\mathfrak{p} = (f)$ for some nonzero irreducible element $f \in A$. We conclude by Exercise 19.6 and Corollary 19.8 that $\dim Y = \dim X - 1$.

Now we prove Corollary 20.5 for the general case. Let $d := \dim X$. Since $Y \subsetneq X$ and both Y and X are irreducible, we have

$$\dim Y \leq d - 1.$$

By the Noether normalization lemma, we have a finite injective morphism of $\mathbf{k}$-algebras

$$\phi : R := \mathbf{k}[X_1, \ldots, X_d] \hookrightarrow A.$$

The induced morphism

$$R/(\mathfrak{p} \cap R) \hookrightarrow A/\mathfrak{p}$$

is also injective and finite, so

$$\dim Y = \dim \pi(Y)$$

by Corollary 18.12, where $\pi : X \to \operatorname{Spec}(R)$ is the projection induced by ϕ.

Assume that $\dim \pi(Y) \leq d - 2$. Since π is finite, $\pi(Y)$ is Zariski closed in $\operatorname{Spec}(R)$. As Y is irreducible, so is $\pi(Y)$. Therefore by the case $A = \mathbf{k}[X_1, \ldots, X_d]$ above, we have $\pi(Y) \subsetneq Z \subsetneq \operatorname{Spec}(R)$ for some irreducible closed subset Z of $\operatorname{Spec}(R)$. As π satisfies the going-down property by Proposition 29.15, we have $Y \subsetneq Z' \subsetneq X$ for some irreducible closed subset Z' of X, which contradicts the assumption that the prime ideal $\mathfrak{p}$ is minimal. Hence $\dim \pi(Y) = d - 1$. □

Proof of Theorem 20.3. Theorem 20.3 now follows from Corollary 20.5 and Exercise 20.2. □

21. Krull's principal ideal theorem (Hauptidealsatz)

Throughout this section, let R be a *Noetherian* ring.

21.1. Statement. Krull's principal ideal theorem asserts that the Zariski closed subset cut out by a function, if not empty, has codimension at most 1.

Theorem 21.1 (Krull's principal ideal theorem)**.** *Let* $f \in R$*.*

(1) The irreducible components of $V(f)$ *has codimension* 0 *or* 1*.*
(2) If f *is not a zero divisor, then all the irreducible components of* $V(f)$ *have codimension* 1*.*

Proof of (2) assuming (1). Suppose that not all irreducible components of $V(f)$ have codimension 1. Then by (1), f is contained in some minimal prime ideal $\mathfrak{p}$. By Lemma 17.4, f is a zero divisor. □

We prove Theorem 21.1.(1) in a series of exercises.

Exercise 21.2.

(1) Show that we can assume that R is a local ring, whose maximal ideal $\mathfrak{p}$ is the minimal prime ideal of R containing f. Thus we need to show that for any prime ideal $\mathfrak{q} \subset R$ such that $f \notin \mathfrak{q}$, we have $\dim A_{\mathfrak{q}} = 0$.
(2) Consider the *symbolic power* of $\mathfrak{q}$:

$$\mathfrak{q}^{(n)} := \{\, r \in R \mid \text{the localization of } r \text{ in } R_{\mathfrak{q}} \text{ lies in } (\mathfrak{q}R_{\mathfrak{q}})^n \,\}.$$

Show that there exists an integer $n > 0$ such that

$$\mathfrak{q}^{(n)} + (f) = \mathfrak{q}^{(n+1)} + (f)$$

in R, by showing that $R/(f)$ is Artinian.

(3) Show that $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary: namely for any $x, y \in R$ such that $xy \in \mathfrak{q}^{(n)}$, we have $x \notin \mathfrak{q} \Rightarrow y \in \mathfrak{q}^{(n)}$. Deduce that
$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + (f)\mathfrak{q}^{(n)}$$
and conclude by Nakayama's lemma that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$.

(4) Deduce from $\mathfrak{q}^n A_\mathfrak{q} \subset \mathfrak{q}^{(n)} A_\mathfrak{q} \subset \mathfrak{q}^{(n+1)} A_\mathfrak{q}$ that
$$\mathfrak{q}^n A_\mathfrak{q} = \mathfrak{q}^{n+1} A_\mathfrak{q},$$
then $\mathfrak{q}^n A_\mathfrak{q} = 0$, again by Nakayama's lemma.

(5) Conclude that $\dim A_\mathfrak{q} = 0$.

21.2. Krull's height theorem.

Corollary 21.3 (Krull's height theorem). *Let $f_1, \dots, f_k \in R$. Then every irreducible component of $V(f_1, \dots, f_k)$ has codimension at most k.*

Remark 21.4. The *height* of a prime ideal $\mathfrak{p} \subset R$ is defined as the codimension of the irreducible closed subset of associated to $\mathfrak{p}$ in $\operatorname{Spec}(R)$.

Proof. Let $\mathfrak{p} \subset \operatorname{Spec}(R)$ be the prime ideal associated to an irreducible component of $V(f_1, \dots, f_k)$. Up to replacing R by $R_\mathfrak{p}$, we can assume that R is a local ring, and the maximal ideal $\mathfrak{p}$ of R is the minimal prime ideal containing $f_1, \dots, f_k$.

We prove Corollary 21.3 in this setting by induction on $k \geq 1$. The case $k = 1$ is Krull's principal ideal theorem. Suppose that $\mathfrak{q} \subsetneq \mathfrak{p}$ is a maximal prime ideal of R which is strictly contained in $\mathfrak{p}$. We will show that $\mathfrak{q}$ is a minimal prime ideal of R containing some $g_1, \dots, g_{k-1}$; Corollary 21.3 then follows from the induction hypothesis.

Since $\mathfrak{q} \subsetneq \mathfrak{p}$, by the minimality of $\mathfrak{p}$ we have $(f_1, \dots, f_k) \not\subset \mathfrak{q}$; we can assume that $f_k \notin \mathfrak{q}$. By the maximality of $\mathfrak{q}$ and $\mathfrak{p}$, we have $V(\mathfrak{q}, f_k) = \{\mathfrak{p}\}$. So for every $i = 1, \dots, k-1$, we have $f_i^{n_i} = g_i + a_i f_k$ for some $g_i \in \mathfrak{q}$ and $a_i \in R$. Since
$$V(g_1, \dots, g_{k-1}, f_k) = V(f_1^{n_1}, \dots, f_{k-1}^{n_{k-1}}, f_k) = V(f_1, \dots, f_k) = \{\mathfrak{p}\},$$
the ideal $\mathfrak{p}/(g_1, \dots, g_{k-1})$ has codimension at most 1 in $R/(g_1, \dots, g_{k-1})$ by the principal ideal theorem. Since $\mathfrak{q} \subsetneq \mathfrak{p}$, necessarily the prime ideal $\mathfrak{q}/(g_1, \dots, g_{k-1})$ has codimension 0. Hence $\mathfrak{q}$ is a minimal prime ideal of R containing $g_1, \dots, g_{k-1}$. □

21.3. System of parameters of Noetherian local rings.

Corollary 21.5. *Any Noetherian local ring has finite dimension.*

Proof. Let $(R, \mathfrak{m})$ be a Noetherian local ring. We have $\mathfrak{m} = (f_1, \dots, f_k)$, so $V(f_1, \dots, f_k) = \{\mathfrak{m}\}$ since $\mathfrak{m}$ is a maximal ideal. We conclude by Krull's height theorem that $\dim R \leq k$. □

Exercise 21.6. Let $(R, \mathfrak{m})$ be a Noetherian local ring such that $\dim R = d$. Show that there exists $f_1, \dots, f_d$ such that
$$V(f_1, \dots, f_d) = \{\mathfrak{m}\}.$$
We call $f_1, \dots, f_d$ a *system of parameters* of $(R, \mathfrak{m})$.

21.4. Invertible ideals define subschemes of codimension 1. Let R be a Noetherian integral domain.

Corollary 21.7. *Let $I \subset R$ be an ideal. Suppose that I is invertible, then every irreducible component of $V(I)$ has codimension* 1.

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(R)$ be a minimal prime ideal containing I. Then $\mathfrak{p}R_\mathfrak{p}$ be the unique prime ideal of $R_\mathfrak{p}$ containing $I_\mathfrak{p}$. Since $I_\mathfrak{p}$ is principal and nonzero by Proposition 14.7, and since $R_\mathfrak{p}$ is an integral domain, it follows from Theorem 21.1 that $\mathfrak{p}R_\mathfrak{p}$ has height 1 in $R_\mathfrak{p}$. Thus $\mathfrak{p}$ has height 1 in R. □

Remark 21.8. The converse of Corollary 21.7 is not true: see Exercise 14.9.

21.5. Characterization of UFDs. Here is another consequence of the principal ideal theorem.

Theorem 21.9. *Let R be an integral domain. The following assertions are equivalent.*

(1) R is a UFD.

(2) Every prime ideal of height one is principal.

Proof. We start with the easy direction (1) ⇒ (2). Suppose that R is a UFD. Let $\mathfrak{p} \subset R$ be a prime ideal of height 1. Let $f \in \mathfrak{p}$. Since f is not a unit and $\mathfrak{p}$ is prime, that R is a UFD implies taht f has a prime factor p which belongs to $\mathfrak{p}$. Since (p) is a prime ideal and $\mathfrak{p}$ has height 1, we have $(p) = \mathfrak{p}$.

Now assume (2). Since R is Noetherian, it suffices to show that every irreducible element f of R is prime. Let $\mathfrak{p} \subset R$ be a minimal prime ideal of R containing f. By the principal ideal theorem, $\mathfrak{p}$ has height 1, so $\mathfrak{p} = (r)$ for some $r \in R \backslash R^\times$ by assumption. Thus $f = cr$ for some $c \in R$, and since f is irreducible, c is a unit. Hence $(f) = (r) = \mathfrak{p}$. □

LECTURE 11

Valuation rings

22. Riemann surfaces and number fields

22.1. Reconstruction of a Riemann surface from its function field. Let X be a connected Riemann surface. For any nonzero meromorphic function f on X and any point $p \in X$, we have

$$f(z) = \sum_{n \geq \mathrm{ord}_p f} a_n z^n$$

for some local holomoprhic coordinate z of X around p, and some integer N with $a_N \neq 0$. The integer N is called the order of f of p, denoted by $\mathrm{ord}_p f$. The function ord_p is a discrete valuation of $\mathscr{M}(X)$, defined as follows.

Definition 22.1. Let K be a field. A *discrete valuation* of K is a surjective map

$$v : K^\times \twoheadrightarrow \mathbf{Z}$$

with $v(0) := \infty$, such that for every $f, g \in K$, we have

- $v(f+g) \geq \min\{\, v(f), v(g)\,\}$;
- $v(fg) = v(f) + v(g)$.

We have the following fundamental result in the theory of Riemann surfaces.

Theorem 22.2 (Dedekind, Weber). *Let X be a connected compact Riemann surface. The map*

$$\begin{aligned} X &\to \{\, \text{Discrete valuations on } \mathscr{M}(X) \,\} \\ p &\mapsto \mathrm{ord}_p \end{aligned}$$

is bijective.

Remark 22.3. The above result also holds for non-compact Riemann surfaces, which was proven by Hironaka, under the pseudonym "Iss'sa".

Exercise 22.4. Let X be the Riemann sphere. Show that $\mathrm{ord}_\infty f = -\deg f$ for every $f \in \mathscr{M}(X) = \mathbf{C}(z)$.

Finally, note that $\mathrm{ord}_p(f)$ only depends on the local behavior of f at p. For instance, if f is holomorphic at p, then $\mathrm{ord}_p(f)$ only depends on $f \in \mathscr{O}_{X,p}$ regarded as a germ of holomorphic function at p.

22.2. p-adic valuation. For every prime number p, the *p-adic valuation* of a nonzero rational number r is the integer $v_p(r)$ defined by the unique factorization

$$|r| = \prod_{p \text{ prime number}} p^{v_p(r)}.$$

This is also an example of discrete valuation.

22.3. Valuations and absolute values (or places). Let K be a field. An *absolute value* of K is a function

$$|\bullet| : K \to \mathbf{R}_{\geq 0}$$

satisfying the following properties: for every $x, y \in K$, we have

(1) $|x| = 0$ if and only if $x = 0$;
(2) $|xy| = |x||y|$ (multiplicativity);
(3) $|x+y| \leq |x| + |y|$ (triangle inequality).

We call $| \bullet |$ *non-Archimedean* if moreover

(3′) $|x + y| \leq \max(|x|, |y|)$ for every $x, y \in K$ (ultrametric triangle inequality).

Otherwise, we call $| \bullet |$ *Archimedean*. Note that (2) implies that $|1| = 1$ and that (3′) is stronger than (3).

The name *Archimedean* is justified by the following characterization of Archimedean absolute values.

Proposition 22.5. *Let $| \bullet |$ be an absolute value of K. The following assertions are equivalent.*

(1) $| \bullet |$ is Archimedean.

(2) The set $\{ |n| \mid n \in \mathbf{Z} \}$ is unbounded

(3) $| \bullet |$ satisfies the Archimedean property: for every pair of non zero elements $x, y \in K$, there exists $n \in \mathbf{Z}$ such that $|nx| > |y|$.

Proof. We prove (1) ⇒ (2), and leave the other implications as exercises.

Suppose that there exists $M > 0$ such that $|n| \leq M$ for all $n \in \mathbf{Z}$. Let $x, y \in K$. For every positive integer n, we have

$$|x + y|^n \leq \sum_{i=0}^{n} \left| \binom{n}{i} \right| |x|^i |y|^{n-i} \leq N(n+1) \max(|x|^n, |y|^n).$$

Taking $\sqrt[n]{}$ and letting $n \to \infty$ yield $|x + y| \leq \max(|x|, |y|)$. □

Corollary 22.6. *If K has positive characteristic, then any absolute value on K is non-Archimedean.*

Fix a real number $e > 1$. A discrete valuation v of a field K gives rise to a non-Archimedean absolute value

$$|x|_v := e^{-v(x)} \qquad (x \in K).$$

Note that the topology on K defines by the metric $| \bullet |_v$ does not depend on the choice of $e > 0$, and we call it the v-adic topology on K.

An (topological) equivalence class of absolute values of K is called a *place* of K. The following statement is an analogue of Theorem 22.2; we refer to [**8**, Theorem 7.12] for a proof.

Theorem 22.7 (Ostrowski)**.**

$$\begin{aligned} \{ \textit{Prime numbers} \} \cup \{\infty\} &\to \{ \textit{Places on } \mathbf{Q} \} \\ p &\mapsto | \bullet |_p \end{aligned} \tag{22.1}$$

where $| \bullet |_p = | \bullet |_{v_p}$ and $| \bullet |_\infty$ is the restriction of the usual absolute value on $\mathbf{R}$ to $\mathbf{Q}$, is bijective. Moreover, $| \bullet |$ is Archimedean if and only if $| \bullet | = | \bullet |_\infty$.

22.4. Discrete valuation rings.

Theorem-Definition 22.8. *Let $(R, \mathfrak{m})$ be a Noetherian local integral domain and let $K := \mathrm{Frac}(R)$. The following assertions are equivalent.*

(1) $\mathfrak{m}$ is principal.

(2) R is a PID, and every nonzero ideal of R is of the form $\mathfrak{m}^k$ for some integer $k \geq 0$.

(3) There exists a discrete valuation v on K such that

$$R = \{ x \in K \mid v(x) \geq 0 \}.$$

Note that this implies

$$\mathfrak{m} = \{ x \in K \mid v(x) \geq 1 \}.$$

(4) R is integrally closed, with Krull dimension 1.

If $(R, \mathfrak{m})$ satisfies the above properties, we call R a discrete valuation ring *(or DVR for short). An element $x \in R$ which generates $\mathfrak{m}$ is called a* uniformizing parameter *(or uniformizer).*

Proof. Assume (1), namely $\mathfrak{m} = (x)$ for some $x \in R$. By the principal ideal theorem, we have $\dim R = 1$. Let $I \subset R$ be a non zero ideal. Then $\dim R/I = 0$. Since R is Noetherian, R/I is Artinian. It follows from Lemma 16.22 that $\mathfrak{m}^N \subset I$ for large $N \in \mathbf{Z}$. Note that $(x)^{k+1} \subsetneq (x)^k$: otherwise $x^k = rx^{k+1}$ for some $r \in R$, so $rx = 1$ because R is an integral domain, which contradicts $x \in \mathfrak{m}$. So there exists some integer $k \geq 0$ such that $I \subset \mathfrak{m}^k$ and $I \not\subset \mathfrak{m}^{k+1}$, namely there exists $y \in I$ such that $y \in (x^k)$ but $y \notin (x^{k+1})$. Write $y = ax^k$ for some $a \in R$. Then $a \notin (x) = \mathfrak{m}$, so a is invertible. It follows that $x^k \in I$ so $\mathfrak{m}^k = (x^k) \subset I \subset \mathfrak{m}^k$. Hence (1) implies (2).

Exercise 22.9. Assume (2) and that $\mathfrak{m} = (x)$. For every integer k, let $(x^k) \subset K$ be the principal fractional ideal associated to x^k. Show that

$$\begin{aligned} \nu : K^\times &\to \mathbf{Z} \\ f &\mapsto \max\left\{ k \in \mathbf{Z} \,\middle|\, f \in (x^k) \right\} \end{aligned}$$

is a discrete valuation and $R = \{ x \in K \mid \nu(x) \geq 0 \}$.

Assume (3). Let $x \in K$ be an integral element over R. Then

$$x^n = \sum_{i=0}^{n-1} r_i x^i$$

for some integer n and some $r_0, \ldots, r_{n-1} \in R$. Suppose that $x \notin R$. Then $\nu(x) < 0$, so $\nu(1/x) > 0$, which implies $1/x \in R$. Thus $x = \sum_{i=0}^{n-1} r_i x^{i-n+1} \in R$, which is a contradiction. So R is integrally closed.

To show that $\dim R = 1$, we need to show that $\mathfrak{m}$ is the unique nonzero prime ideal of R. As ν is surjective, there exists $x \in R$ such that $\nu(x) = 1$. Note that $\mathfrak{m} = (x)$: we have $(x) \subset \mathfrak{m}$ by (3), and if $y \in \mathfrak{m}$, then $y = x(y/x)$ and $y/x \in R$ because $\nu(y/x) \geq 0$. Let $\mathfrak{p} \subset R$ be a nonzero prime ideal and let $f \in \mathfrak{p}$ be a nonzero element. Since $k := \nu(f) \geq 1$ (because f is not a unit in R), the quotient $a := f/x^k$ is a unit in R. Since $f = ax^k \in \mathfrak{p}$ and $a \notin \mathfrak{p}$, we have $x \in \mathfrak{p}$. This proves (4).

Finally we assume (4). By Proposition 14.7, it suffices to show that $\mathfrak{m}$ is invertible, namely $\mathfrak{m}^{-1}\mathfrak{m} = R$ Since $\dim R = 1$, we have $\mathfrak{m} \neq 0$, so there exists $x \in \mathfrak{m} - \mathfrak{m}^2$ by the Nakayama lemma. As (x) is not (0) nor R, regarded $R/(x)$ as an R-module we have $\mathrm{Ass}(R/(x)) = \{\mathfrak{m}\}$. So there exists $y \in R$ such that

$$\{ z \in R \mid yz \in (x) \} = \mathfrak{m}.$$

It follows that if $a := y/x$, then $a \in \mathfrak{m}^{-1}$ and $a \notin R$.

Suppose that $\mathfrak{m}^{-1}\mathfrak{m} \subsetneq R$. Then $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m}$. So $a \cdot \mathfrak{m} \subset \mathfrak{m}$, which implies by Cayley–Hamilton that $P(\alpha) \cdot \mathfrak{m} = 0$ for some

$$P = X^n + r_{n-1}X^{n-1} + \cdots + r_0 \in R[X]$$

So $P(\alpha) = 0$. Because R is integrally closed, this contradicts with $a \notin R$. Hence $\mathfrak{m}$ is invertible, which proves (1). □

Exercise 22.10. Let $(R, \mathfrak{m})$ be a DVR. Show that every fractional ideal of R is of the form $\mathfrak{m}^k$ for some integer k. Show that for all integers k, ℓ, we have $\mathfrak{m}^k = \mathfrak{m}^\ell \subset K$ if and only if $k = \ell$.

22.5. Henselian trait. Let R be a DVR. Let $K := \mathrm{Frac}(R)$ and let k be the residue field of R. As a topological space, $S = \mathrm{Spec}(R)$ consists of two points: the generic point $\eta = \mathrm{Spec}(K)$ and the special point $s = \mathrm{Spec}(k)$. The generic point is dense, and the special point is closed. The spectrum of a DVR R is often pictured as a (one-dimensional smooth) trait centered at s. They are among the simplest schemes of positive dimension, and are ubiquitous in algebraic geometry.

22.6. Dedekind domain. The following statement is a direct consequence of Theorem 22.8.

Corollary-Definition 22.11. *Let R be a Noetherien integral domain. The following assertions are equivalent.*

(1) R is integrally closed with $\dim R = 1$.

(2) $R_\mathfrak{m}$ is a DVR for every maximal ideal $\mathfrak{m} \subset R$.

If R satisfies the above properties, we call R a Dedekind domain.

Exercise 22.12. Show that the ring of integers of a number field is a Dedekind domain.

Here is the generalization of Ostrowski's theorem to algebraic number fields; we refer to [**8**, Theorem 7.14] for the details.

Theorem 22.13. *Let K be a number field and let $\mathscr{O}_K$ be its ring of integer.*

(1) The map

$$\begin{aligned} \{\,\text{Real or complex embeddings } \sigma : K \hookrightarrow \mathbf{R} \text{ or } \mathbf{C}\,\} &\to \{\,\text{Archimedean places on } K\,\} \\ \sigma &\mapsto |x|_\sigma := |\sigma(x)| \end{aligned} \tag{22.2}$$

is bijective.

(2) The map

$$\begin{aligned} \operatorname{Spec}(\mathscr{O}_K) &\to \{\,\text{Non-Archimedean places on } K\,\} \\ \mathfrak{p} &\mapsto |x|_\mathfrak{p} := \#\,(\mathscr{O}_K/\mathfrak{p})^{-v_\mathfrak{p}(x)}\,. \end{aligned} \tag{22.3}$$

is bijective.

(3) If we call the above absolute values $|\bullet|_\mathfrak{p}$ and $|\bullet|_\sigma$ normalized places, then for every $x \in K^\times$, we have

$$\prod_{v \text{ normalized places}} |x|_v = 1.$$

Exercise 22.14. In the above statement, show that $\mathscr{O}_K/\mathfrak{p}$ is finite.

23. Unique factorization of ideals in a Dedekind domain

Let R be a ring.

23.1. Chinese Remainder Theorem. Let $I, J \subset R$ be ideals of R. We say that I and J are *coprime* if $I + J = R$.

Example 23.1. Let $m, n \in \mathbf{Z}$. Then (m) and (n) are coprime if and only if $\gcd(m, n) = 1$.

Example 23.2. In any ring, distinct maximal ideals $\mathfrak{p}, \mathfrak{q}$ of R are coprime.

Exercise 23.3. Let $I, J \subset R$ be ideals of R. Suppose that I and J are coprime. Show that I^m and J^n are also coprime for all positive integers m and n.

Proposition 23.4 (Chinese Remainder Theorem). *Let $I_1, \dots, I_n \subset R$ be ideals of R which are pairwise coprime. Then*

$$I := I_1 \cdots I_n = \bigcap_{i=1}^n I_i$$

and the sequence

$$0 \to I \to R \xrightarrow{q} \prod_{i=1}^n R/I_i \to 0$$

defined by the inclusion and the quotients is exact.

Proof. It is clear that $\ker q = \bigcap_{i=1}^n I_i$. We prove Proposition 23.4 by induction on $n \geq 2$. For $n = 2$, since I_1 and I_2 are coprime, we have $a_1 + a_2 = 1$ for some $a_1 \in I_1$ and $a_2 \in I_2$. So for any $x_1, x_2 \in R$, we have the equalities in R/I_1

$$x := a_1x_2 + a_2x_1 = (a_1 + a_2)x_1 = x_1,$$

and similarly $x = x_2$ in R/I_2. Hence $R \to (R/I_1) \times (R/I_2)$ is surjective. It is clear that the kernel is of the above map is $I_1 \cap I_2$. We always have $I_1I_2 \subset I_1 \cap I_2$. Now if $r \in I_1 \cap I_2$, then $r = a_1r + a_2r \in I_1I_2$.

We next prove Proposition 23.4 for $n > 2$ bases on the inductive hypothesis. Since I_1 is coprime to I_i for each index $i > 1$, we have $a_i + b_i = 1$ for some $a_i \in I_1$ and $b_i \in I_i$. So

$$1 = (a_2 + b_2) \cdots (a_n + b_n) \in I_1 + (I_2 \cdots I_n),$$

namely I_1 and $J := \prod_{i=2}^n I_i$ are coprime. By the induction hypothesis and, we have

$$R \xrightarrow{q} \prod_{i=1}^n R/I_i \xrightarrow{\sim} (R/I_1) \times (R/J)$$

and the composition is the product of the quotient map, which is surjective with kernel equal to $I_1 J = I_1 \cdots I_n$ by the case $n = 2$. □

23.2. Unique factorization.

Lemma 23.5. *Let R be a Noetherian integral domain with $\dim R = 1$. Let $I \subset R$ be a nonzero ideal. Suppose that for every maximal ideal $\mathfrak{m} \in \operatorname{Specm}(R)$, we have $I_\mathfrak{m} = \mathfrak{m}^{e_\mathfrak{m}} R_\mathfrak{m}$ for some integer $e_\mathfrak{m} \geq 0$. Then $e_\mathfrak{m} = 0$ for all but finitely many $\mathfrak{m}$, and*

$$I = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_k^{e_k},$$

where $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ are the maximal ideals for which $e_i := e_{\mathfrak{m}_i} > 0$.

Proof. Since R is Noetherian, R/I has finitely many associated points $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$. As $\dim R = 1$ and R is an integral domain, all prime ideals of R are maximal, except for (0). As $(0) \notin \operatorname{Ass}(R/I)$ (because $I \neq (0)$), these prime ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ are therefore maximal. Thus $\operatorname{Supp}(R/I) = \{ \mathfrak{m}_1, \ldots, \mathfrak{m}_k \}$. It follows that $e_\mathfrak{m} > 0$ if and only if $\mathfrak{m}$ is one of $\mathfrak{m}_i$, hence the number of $\mathfrak{m}$ for which $e_\mathfrak{m} > 0$ is finite.

Next we show that $I \subset \mathfrak{m}^{e_\mathfrak{m}}$ for each $\mathfrak{m} \in \operatorname{Specm}(R)$. Let $r \in I$. Since $I_\mathfrak{m} = \mathfrak{m}^{e_\mathfrak{m}} R_\mathfrak{m}$, we have $sr \in \mathfrak{m}^{e_\mathfrak{m}}$ for some $s \in R - \mathfrak{m}$. Since $\mathfrak{m}$ is a maximal ideal, we have $\operatorname{Spec}(R/\mathfrak{m}^{e_\mathfrak{m}}) = \{ \mathfrak{m}/\mathfrak{m}^{e_\mathfrak{m}} \}$, so $(R/\mathfrak{m}^{e_\mathfrak{m}}, \mathfrak{m}/\mathfrak{m}^{e_\mathfrak{m}})$ is a local ring. It follows that s is invertible in $R/\mathfrak{m}^{e_\mathfrak{m}}$, hence $r \in \mathfrak{m}^{e_\mathfrak{m}}$, showing that $I \subset \mathfrak{m}^{e_\mathfrak{m}}$.

It follows that

$$I \subset \bigcap_{\mathfrak{m} \in \operatorname{Specm}(R)} \mathfrak{m}^{e_\mathfrak{m}} = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_k^{e_k},$$

where the equality follows from Proposition 23.4 and Exercise 23.3. Since $(\mathfrak{m}_i^{e_i})_\mathfrak{m} = R_\mathfrak{m}$ whenever $\mathfrak{m}$ is a maximal ideal different from $\mathfrak{m}_i$, we have

$$(\mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_k^{e_k})_\mathfrak{m} = \mathfrak{m}^{e_\mathfrak{m}} R_\mathfrak{m}.$$

Since $I_\mathfrak{m} = \mathfrak{m}^{e_\mathfrak{m}} R_\mathfrak{m}$ for all $\mathfrak{m} \in \operatorname{Specm}(R)$, it follows from Corollary 10.33 that $I = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_k^{e_k}$. □

Theorem 23.6. *Let R be a Dedekind domain. Every nonzero ideal $I \subset R$ is a product*

$$I = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_k^{e_k}$$

of maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ of R. Moreover, the maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ and the exponents $e_1, \ldots, e_k$ are unique (up to permutations).

Proof. Since $R_\mathfrak{m}$ is a DVR, Theorem 22.8 implies that $I_\mathfrak{m} = \mathfrak{m}^{e_\mathfrak{m}} R_\mathfrak{m}$ for some $e_\mathfrak{m} \in \mathbf{Z}_{\geq 0}$. Thus the existence of factorization follows from Lemma 23.5. As

$$(\mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_k^{e_k})_\mathfrak{m} = \begin{cases} \mathfrak{m}_i^{e_i} R_{\mathfrak{m}_i} & \text{if } \mathfrak{m} = \mathfrak{m}_i \\ R_\mathfrak{m} & \text{if } \mathfrak{m} \text{ is different from all } \mathfrak{m}_i, \end{cases}$$

the uniqueness follows from Exercise 22.10. □

Exercise 23.7.

(1) Show that $\mathbf{Z}[\sqrt{-5}]$ is a Dedekind domain.
(2) In $\mathbf{Z}[\sqrt{-5}]$, we have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. What is the factorization of the ideal (6)?

23.3. Valuation rings. A *totally ordered abelian group* is an abelian group Γ endowed with a total order $\geq$ satisfying the following property: for all $\gamma, \gamma_1, \gamma_2 \in \Gamma$,

$$\gamma_1 \geq \gamma_2 \quad \Rightarrow \quad \gamma + \gamma_1 \geq \gamma + \gamma_2.$$

Definition 23.8. Let K be a field. A *valuation* of K is a map

$$v : K^\times \to \Gamma$$

to some totally ordered abelian group $(\Gamma, \geq)$ with $\nu(0) := \infty$, such that for every $f, g \in K$, we have

- $\nu(f+g) \geq \min\{\, \nu(f), \nu(g) \,\}$;
- $\nu(fg) = \nu(f) + \nu(g)$.

(Here, we set $\infty + x = \infty$ and $\infty \geq x$ for all $x \in \Gamma \cup \{\infty\}$.)

Let ν be a valuation on K. The ring

$$R_\nu := \{\, x \in K \mid \nu(x) \geq 0 \,\}$$

is called the *valuation ring* of ν.

Exercise 23.9. Show that R_ν is a local ring, with maximal ideal

$$\mathfrak{m}_\nu := \{\, x \in K \mid \nu(x) > 0 \,\}.$$

If a ring R is the valuation ring of some valuation ν, then we call R a *valuation ring*.

Exercise 23.10. Let R be an integral domain. Show that the following assertions are equivalent:

(1) R is a valuation ring.
(2) For every nonzero $x \in K = \mathrm{Frac}(R)$, either $x \in R$ or $x^{-1} \in R$.

(Hint for (2) ⇒ (1): First show that for every $a, b \in K^\times$, we have either $(a) \subset (b)$ or $(b) \subset (a)$. Show that $\nu : K^\times \to \mathrm{Prin}(R)$ is a valuation.)

Exercise 23.11. Show that a valuation ring is integrally closed.

23.4. Zariski–Riemann space. You may skip this paragraph if you have not learnt algebraic geometry.

Let X be an irreducible $\mathbf{k}$-variety. Let $\mathbf{k}(X)$ be a function field of X. For any valuation ν on $\mathbf{k}(X)$, the set

$$Z = \{\, x \in X \;\big|\; \mathscr{O}_{X,x} \subset R_\nu \,\}$$

is either empty or an irreducible closed subset. In the latter case, the generic point of Z is called the *center* of ν.

Example 23.12. Let $\widetilde{X} \to \mathrm{Spec}\,\mathbf{k}[X,Y]$ be the blowup at the origin o and let $E \subset \widetilde{X}$ be the exceptional divisor. Then

$$f \mapsto \mathrm{ord}_E(f)$$

defines a discrete valuation on $\mathbf{k}(X,Y)$, whose center on $\mathrm{Spec}\,\mathbf{k}[X,Y]$ is o.

Assume that X is proper, then Z is always nonempty by the valuative criterion of properness. The following theorem, due to Zariski, is a higher dimensional generalization of Dedekind–Weber's theorem.

Theorem 23.13 (Zariski). *Let X be a proper irreducible $\mathbf{k}$-variety. The map*

$$\begin{aligned} \{\ \textit{Valuations on } \mathbf{k}(X),\ \textit{trivial on } \mathbf{k}\,\} &\to \varprojlim_{X' \to X} X' \\ \nu &\mapsto \textit{center of } \nu \textit{ on } X', \end{aligned} \tag{23.1}$$

where $X' \to X$ runs through every proper birational morphism, is bijective.

24. Weil divisors and Cartier divisors

Let R be an integral domain and let $X := \mathrm{Spec}(R)$.

24.1. Weil divisors. Let $X^{(1)}$ denote the set of points of X of height 1. Define

$$Z^1(X) := \bigoplus_{\mathfrak{p} \in X^{(1)}} \mathbf{Z} \cdot [\mathfrak{p}] \simeq \bigoplus_{\substack{D \subset \mathrm{Spec}(R) \\ \text{irreducible reduced closed subset} \\ \mathrm{codim} D = 1}} \mathbf{Z} \cdot D$$

as the free abelian group generated by the prime ideals of R of height 1. Elements of $Z^1(X)$ are called *Weil divisors* of X.

24.2. Weil divisors and fractional ideals. Assume that R is *regular in codimension* 1, namely $R_\mathfrak{p}$ is a DVR for every prime ideal $\mathfrak{p} \subset R$ of height 1; this is the case when e.g. R is a Noetherian integrally closed domain. Then for every fractional ideal $I \subset K := \mathrm{Frac}(R)$, by Exercise 22.10 the localization $I_\mathfrak{p} \simeq IR_\mathfrak{p} \subset K$ at $\mathfrak{p} \in X^{(1)}$ is of the form $(\mathfrak{p}R_\mathfrak{p})^{e_\mathfrak{p}}$ for some integer $e_\mathfrak{p}$.

Lemma 24.1. *Suppose that R is Noetherian. Then $e_\mathfrak{p} = 0$ for all but finitely many $\mathfrak{p} \in X^{(1)}$.*

Proof. We have $(f) \subset I \subset (1/g) \subset K$ for some nonzero $f, g \in R$. By Krull's principal ideal theorem, all the irreducible components of $V(f)$ and $V(g)$ have codimension 1. Since R is Noetherian, there exist only finitely many $\mathfrak{p} \in X^{(1)}$ such that $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$. Let $\mathfrak{p} \in X^{(1)}$ such that $f, g \notin \mathfrak{p}$. As localization is exact, we have $I_\mathfrak{p} = R_\mathfrak{p}$. □

Thus if R is a Noetherian integral domain which is regular in codimension 1, then for every fractional ideal I, we can define

$$\mathrm{div}(I) := \sum_{\mathfrak{p} \in X^{(1)}} e_\mathfrak{p}[\mathfrak{p}] \in Z^1(X).$$

Exercise 24.2. Let $I, J \subset K$ be two fractional ideals. Show that

$$\mathrm{div}(IJ) = \mathrm{div}(I) + \mathrm{div}(J).$$

Exercise 24.3. Let $f \in K^\times$. Show that

$$\mathrm{div}(f) := \mathrm{div}(\text{fractional ideal generated by } f) = \sum_{\mathfrak{p} \in X^{(1)}} \nu_\mathfrak{p}(f)[\mathfrak{p}],$$

where $\nu_\mathfrak{p}$ is the valuation of the DVR $R_\mathfrak{p}$.

The Weil divisors of the form $\mathrm{div}(f)$ are called *principal Weil divisors*. The quotient

$$\mathrm{Cl}(R) := Z^1(X)/\{\, \text{Principal Weil divisors} \,\}$$

is called the *class group* of R.

24.3. Algebraic Hartogs' lemma.

Theorem 24.4 (Algebraic Hartogs' lemma). *Let R be a Noetherian integrally closed domain. Then in $K := \mathrm{Frac}(R)$ we have*

$$R = \bigcap_{\mathfrak{p} \in X^{(1)}} R_\mathfrak{p}.$$

Proof. Let $x \in \bigcap_{\mathfrak{p} \in X^{(1)}} R_\mathfrak{p}$ and let

$$I := \{\, r \in R \mid rx \in R \,\}$$

be the "ideal of denominators of x". Suppose that $x \notin R$, then I is a proper ideal of R. Let $\mathfrak{q}$ be the minimal prime ideal of R containing I. Then $x \notin R_\mathfrak{q}$. By the exactness of localization, we have

$$I_\mathfrak{q} = \{\, r \in R_\mathfrak{q} \,\big|\, rx \in R_\mathfrak{q} \,\}$$

As $\mathfrak{q}R_\mathfrak{q}$ is the only prime ideal of $R_\mathfrak{q}$ containing $I_\mathfrak{q}$ and $R_\mathfrak{q}$ is Noethrian, the quotient $R_\mathfrak{q}/I_\mathfrak{q}$ is Artinian. So there exists an integer $k \geq 0$ such that $(\mathfrak{q}R_\mathfrak{q})^{k+1} \subset I_\mathfrak{q} \subsetneq (\mathfrak{q}R_\mathfrak{q})^k$. Let $c \in (\mathfrak{q}R_\mathfrak{q})^k \backslash I_\mathfrak{q}$ and $z := cx$. We have $z \notin R_\mathfrak{q}$ but $z \cdot \mathfrak{q} \subset I_\mathfrak{q} \subset \mathfrak{q}R_\mathfrak{q}$. It follows from Cayley–Hamilton that z is integral over $R_\mathfrak{q}$, so $z \in R_\mathfrak{q}$, which is a contradiction. □

Corollary 24.5. *Let R be a Noetherian integrally closed domain. Let $\mathfrak{p} \in X^{(1)}$. The following assertions are equivalent.*

(1) $\mathfrak{p}$ is a principal ideal.

(2) $[\mathfrak{p}]$ is a principal Weil divisor.

Proof. The easy direction (1) ⇒ (2) is left as an exercise.

Suppose that $[\mathfrak{p}] = \mathrm{div}(f)$ for some $f \in K^\times$. Then $f \in R_\mathfrak{p}$ for all $\mathfrak{p} \in X^{(1)}$, so $f \in R$ by algebraic Hartogs' lemma. Let $g \in \mathfrak{p}$. Then $\nu_\mathfrak{p}(g) \geq \nu_\mathfrak{p}(f)$ for all $\mathfrak{p} \in X^{(1)}$. So $g/f \in R$, again by algebraic Hartogs' lemma. Hence $\mathfrak{p} = (f)$. □

Algebraic Hartogs' lemma combined with the characterization of UFDs (Theorem 21.9) also shows that the class group is the obstruction for an integrally closed domain to be a UFD.

Corollary 24.6. *Let R be an integral domain. The following assertions are equivalent.*

(1) R is a UFD.

(2) R is integrally closed and $\mathrm{Cl}(R) = 0$.

Exercise 24.7.

(1) Show that $(2, 1 + \sqrt{-5})$ is a prime ideal of $\mathbf{Z}[\sqrt{-5}]$ which is not principal.

(2) What is the class group of $\mathbf{Z}[\sqrt{-5}]$?

24.4. Cartier divisors.

Corollary 24.8. *Let R be a Noetherian integrally closed domain. Then*

$$\begin{aligned} \mathrm{div} : \mathscr{I}(R) &\to Z^1(X) \\ I &\mapsto \sum_{\mathfrak{p} \in X^{(1)}} e_\mathfrak{p}[\mathfrak{p}]. \end{aligned} \tag{24.1}$$

is an injective group homomorphism.

Elements in $\mathrm{CDiv}(X) := \mathrm{div}(\mathscr{I}(R))$ are called *Cartier divisors*.

Proof. That div is a group homomorphism follows from Exercise 24.2.

Suppose that $I \in \mathscr{I}(R)$ is mapped to 0. Then $I, I^{-1} \subset R$ are ideals of R by algebraic Hartogs' lemma. Since $I^{-1}I = R$, necessarily $I = R$. □

Not all Weil divisors are Cartier:

Exercise 24.9. Let $R = \mathbf{C}[x, y, z]/(xy - z^2)$ (so $X = \mathrm{Spec}(R)$ is the quadric cone). Show that the $(x, y) \subset R$ (which defines the ruling of X) is Weil but not Cartier. Show that $\mathrm{div}(x) = 2\mathrm{div}(x, y)$ (which is thus Cartier).

24.5. Bonus: Jia-Lin Hsu's criterion of UFD.

Theorem 24.10 (Jia-Lin Hsu). *Let R be a Noetherian integrally closed domain and let $K = \mathrm{Frac}(R)$. The following assertions are equivalent.*

(1) R is a UFD.

(2) Every $x \in K^\times$ can be written as f/g for some $f, g \in R$ such that every irreducible component of $V(f) \cap V(g)$ has codimension at least 2 in X.

Proof. (1) $\Longrightarrow$ (2) is easy.

Assume that R is not UFD, then there exists a prime ideal $\mathfrak{p} \subset R$ of height 1 which is not principal. Since R is Noetherian, there exists an irreducible element $p \in \mathfrak{p}$. As $\mathfrak{p}$ is not principal, there exists $q \in \mathfrak{p}$ such that $p \nmid q$. Again since R is Noetherian, q has an irreducible factor; up to replacing q by this irreducible factor we can assume that q is irreducible. As p is also irreducible and $p \nmid q$, we have $q \nmid p$.

Suppose that $p/q = f/g$. For every Weil divisor D, write $D = D_+ - D_-$ with both D_+ and D_- effective without common component. Then

$$\mathrm{Div}(f) = \mathrm{Div}(f/g)_+ = \mathrm{Div}(p/q)_+ \leq \mathrm{Div}(p).$$

So $f | p$ by Hartogs' lemma. Note that f is not unit: otherwise $g/f = q/p \in R$, contradicting $p \nmid q$. So $p = uf$ for some unit $u \in R$. Thus $q = ug$, showing that $f, g \in \mathfrak{p}$, contradicting the assumption on $V(f) \cap V(g)$. □

LECTURE 12

Differentials

25.

25.1. Tangent vectors and derivations on smooth manifolds. Let M be a manifold. Recall that a *derivation* at a point $p \in M$ is an $\mathbf{R}$-linear map

$$\begin{aligned}\mathscr{C}^{\infty}_{M,p} &\to \mathbf{R}\\ f &\mapsto f'(p)\end{aligned}$$

satisfying the Leibniz rule

$$(fg)'(p) = f'(p)g(p) + f(p)g'(p).$$

Derivations at p form an $\mathbf{R}$-vector space, canonically isomorphic to the tangent space $T_{M,p}$ of M at p.

Note that the Leibniz rule together with the $\mathbf{R}$-linearity implies that $f'(p) = 0$ if f is constant. So a derivation is determined by its restriction

$$\mathfrak{m} \to \mathbf{R}$$

to the maximal ideal $\mathfrak{m}$ of $\mathscr{C}^{\infty}_{M,p}$. Also, note that if $f, g \in \mathfrak{m}$, then $(fg)' = 0$ by the Leibniz rule. Thus the derivation descends to an $\mathbf{R}$-linear map

$$\mathfrak{m}/\mathfrak{m}^2 \to \mathbf{R}.$$

Exercise 25.1. Show that the above construction defines an isomorphism of $\mathbf{R}$-linear spaces.

$$T_{M,p} \simeq (\mathfrak{m}/\mathfrak{m}^2)^{\vee}.$$

25.2. Affine cones. Let $\mathbf{k}$ be an algebraically closed field. Then $\mathbf{k}^{\times}$ acts on $\mathbf{k}^d$ by scalar multiplication. If $Z \subset \mathbf{k}^d$ is an algebraic closed subset which is stable under the $\mathbf{k}^{\times}$-action, we call Z an affine cone.

Exercise 25.2. Show that an algebraic closed subset $Z \subset \mathbf{k}^d$ is an affine cone if and only if $I(Z)$ is a homogeneous ideal, defined in the following exercise.

Exercise 25.3. Let $R_\bullet$ be a $\mathbf{Z}_{\geq 0}$-graded ring and let $I \subset R_\bullet$ be an ideal.

(1) Show that the following assertions are equivalent.
   (a) I is generated by homogeneous elements (namely elements of R_d for some d).
   (b) $I = \bigoplus_{d \geq 0} I_d$ where $I_d = R_d \cap I$.

   A *homogeneous ideal* is an ideal $I \subset R_\bullet$ satisfying the above properties.
(2) Let $I \subset R_\bullet$ be an homogeneous ideal. Show that the graded ring structure on $R_\bullet$ induces a graded ring structure on the direct sum $\bigoplus_{d=0}^{\infty} R_d/I_d$ of abelian groups, and that the natural map

$$\bigoplus_{d=0}^{\infty} R_d/I_d \to R_\bullet/I$$

   is a ring isomorphism. Thus defines a graded ring structure on $R_\bullet/I$.

25.3. Tangent cone of an affine variety. Let $f \in \mathbf{C}[X_1, \dots, X_n]$ and let

$$X = \{\, x \in \mathbf{C}^n \mid f(x) = 0 \,\}.$$

Suppose that X contains the origin $o \in \mathbf{C}^n$ and that we want to take a photo of X centered at o. If we zoom in on o, which corresponds to the coordinate change $x' = x/\varepsilon$ for some small $\varepsilon > 0$, then the shape we see is approximately a *cone*. Indeed, suppose that k is the lowest degree monomial appearing in f, and write

$$f = \sum_{\ell \geq k} f_\ell$$

where f_ℓ is the sum of all the monomials of degree ℓ of f, then

$$\left\{ x' \in \mathbf{C}^n \;\middle|\; f(\varepsilon \cdot x') = \sum_{\ell \geq k} \varepsilon^\ell f_\ell(x') = 0 \right\}$$

is approximately

$$\{ x' \in \mathbf{C}^n \mid f_k(x') = 0 \}$$

when $\varepsilon \to 0$. We call it the tangent cone of X at o.

More generally, let $\mathbf{k}$ be a field and let $I \subset R := \mathbf{k}[X_1, \ldots, X_d]$ be an ideal. Suppose that $V(I)$ contains the origin $o \in \mathbf{A}^d_{\mathbf{k}}$. Then the tangent cone of $\operatorname{Spec}(R/I)$ at o is naturally defines as the scheme $\operatorname{Spec}(R/I^\#)$ where

$$I^\# = \{ g \in R \mid g \text{ is the lowest degree homogeneous component of some } f \in I \}.$$

The tangent cone of $\operatorname{Spec}(R/I)$ at any closed point $z \in V(I)$ is the tangent cone of $\operatorname{Spec}(R/J)$ at the origin, where $J = \{ f(x-z) \mid f \in I \}$ is the translation of I by z.

25.4. Tangent cone of (the spectrum of) a local ring. Let $(R, \mathfrak{m})$ be a local ring. The tangent cone of $X := \operatorname{Spec}(R)$ at the closed point $p \in X$ is defined as

$$C_{X,p} := \operatorname{Spec}\left(\bigoplus_{k=0}^{\infty} \mathfrak{m}^k/\mathfrak{m}^{k+1} \right).$$

Example 25.4. Suppose that R is the localization of $\mathbf{k}[X_1, \ldots, X_d]$ at the origin $o \in \mathbf{A}^d_{\mathbf{k}}$. Then $\bigoplus_{k=0}^{\infty} \mathfrak{m}^k/\mathfrak{m}^{k+1}$ is isomorphic to $\mathbf{k}[X_1, \ldots, X_d]$ as graded rings.

Example 25.5. More generally, let I be an ideal of $R := \mathbf{k}[X_1, \ldots, X_d]$. Then the tangent cone of the affine scheme $\operatorname{Spec}(R/I)$ at some closed point p is the tangent cone of the localization of R/I at p.

Indeed, suppose that p is the origin. Let $\widetilde{\mathfrak{m}} := (X_1, \ldots, X_d)$ and let $\mathfrak{m}$ be the maximal ideal of the localization of R/I at $\widetilde{\mathfrak{m}}/I$. Then

$$\frac{\mathfrak{m}^d}{\mathfrak{m}^{d+1}} \simeq (\mathfrak{m}^d)|_{\mathfrak{m}} \simeq \left(\frac{\widetilde{\mathfrak{m}}^d}{\widetilde{\mathfrak{m}}^d \cap I} \right)|_{\widetilde{\mathfrak{m}} \bmod I} \simeq \frac{\widetilde{\mathfrak{m}}^d}{(I \cap \widetilde{\mathfrak{m}}^d) + \widetilde{\mathfrak{m}}^{d+1}}$$

by Exercise 11.1. Note that

$$(I \cap \widetilde{\mathfrak{m}}^d) + \widetilde{\mathfrak{m}}^{d+1} = I^\#_d + \widetilde{\mathfrak{m}}^{d+1},$$

so we have ring isomorphisms

$$R/I^\# \simeq \bigoplus_{d=0}^{\infty} \frac{\widetilde{\mathfrak{m}}^d}{I^\#_d + \widetilde{\mathfrak{m}}^{d+1}} \simeq \bigoplus_{d=0}^{\infty} \frac{\mathfrak{m}^d}{\mathfrak{m}^{d+1}}.$$

Exercise 25.6. Suppose that I is the vanishing ideal of a linear subspace $X \subset \mathbf{A}^d_{\mathbf{k}}$. With the same notations as in the previous example, show that we have ring isomorphisms

$$R/I \simeq \operatorname{Sym}^\bullet(\mathfrak{m}/\mathfrak{m}^2) \simeq \bigoplus_{k=0}^{\infty} \mathfrak{m}^k/\mathfrak{m}^{k+1}.$$

25.5. Tangent space. Let $\mathbf{k}$ be an algebraically closed field and let $Z \subset \mathbf{k}^d$ be an affine variety containing the origin o. We define the tangent space $T_{Z,o}$ of Z at o to be the linear hull of the tangent cone $C_{Z,o}$: namely, the smallest linear subsapce of $\mathbf{k}^d$ containing $C_{Z,o}$ as a *scheme*.

Exercise 25.7. Show that $T_{Z,o}$ is defined by the linear terms of the elements of $I(Z)$. Deduce that if Z is defined by the polynomials $f_1, \ldots, f_m \in \mathbf{k}[X_1, \ldots, X_d]$, then $T_{Z,o}$ is defined by the linear equations

$$\sum_{i=1}^{d} X_i \partial_{X_i} f_1 = \cdots = \sum_{i=1}^{d} X_i \partial_{X_i} f_m = 0.$$

Exercise 25.8. Let $\mathbf{k}$ be an algebraically closed field. Let X and Y denote the coordinates of $\mathbf{k}^2$. Describe the tangent cones and the tangent spaces of the three affine curves $C \subset \mathbf{k}^2$ at the origin defined respectively by the following equations.

(1) $Y^2 = X$.
(2) $Y^2 = X^3 + X^2$.
(3) $X^2 = Y^3$.

More generally, for any local ring $(R, \mathfrak{m})$, the tangent space of $X := \operatorname{Spec}(R)$ at the closed point $p \in X$ is defined as

$$T_{X,p} := \operatorname{Spec}(\operatorname{Sym}^\bullet(\mathfrak{m}/\mathfrak{m}^2)).$$

We have an embedding $C_{X,p} \subset T_{X,p}$ induced by the projection

$$\operatorname{Sym}^\bullet(\mathfrak{m}/\mathfrak{m}^2) \twoheadrightarrow \bigoplus_{k=0}^{\infty} \mathfrak{m}^k/\mathfrak{m}^{k+1}.$$

The closed points of $T_{X,p}$ form a vector space over $\mathbf{k} := R/\mathfrak{m}$, canonically isomorphic to $(\mathfrak{m}/\mathfrak{m}^2)^\vee = \operatorname{Hom}_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2, \mathbf{k})$. By Exercise 25.6, this generalizes the previous definition of the tangent space of an affine variety.

25.6. Cotangent space and the module of differentials. The study of an affine scheme $\operatorname{Spec}(R)$ consists of the study of R, namely the ring of regular functions on $\operatorname{Spec}(R)$. From the algebraic perspective, instead of studying the "tangent vectors" of $\operatorname{Spec}(R)$, it would be more natural to consider "differential forms". This is already hinted when we mention that closed points of the tangent space of an affine variety at a closed point $\mathfrak{m}$ is canonically identified with the vector space $(\mathfrak{m}/\mathfrak{m}^2)^\vee$. We thus define the *cotangent space* of (the spectrum of) a local ring $(R, \mathfrak{m})$ at the closed point $\mathfrak{m}$ to be $\mathfrak{m}/\mathfrak{m}^2$.

In addition to cotangent space, we also define *cotangent module* $\Omega_{A/R}$ of an R-algebra A; this is the analog of the cotangent bundle over a manifold. We will see in Proposition 25.18 that over a rational point p, the fiber $(\Omega_{A/R})|_p$ coincides with the cotangent space $\mathfrak{m}_p/\mathfrak{m}_p^2$.

Definition 25.9. Let $R \to A$ be an R-algebra. The *module of (relative) differentials* $\Omega_{A/R}$ of A over R is the quotient of the free A-module generated by the symbols df for all $f \in A$, quotient by the A-submodule generated by the relations

(1) $dr = 0$ for all $r \in R$ (i.e. the functions pulled back from Spec$R$ have vanishing differentials);
(2) $d(f + g) = df + dg$;
(3) (Leibniz' rule) $d(fg) = f \cdot dg + g \cdot df$.

We also call $\Omega_{A/R}$ the module of Kähler differentials.

Exercise 25.10. Let R be a ring and let $A = R[X_1, \dots, X_n]/(f_1, \dots, f_m)$. Show that $\Omega_{A/R}$ is the quotient of the free A-module generated by $dX_1, \dots, dX_n$, quotient by the relations $df_1 = \cdots df_m$, or precisely

$$\sum_{i=1}^{d} (\partial_{X_i} f_1) dX_i = \cdots = \sum_{i=1}^{d} (\partial_{X_i} f_m) dX_i = 0.$$

Exercise 25.11. Show that if $R \to A$ is a finitely generated (resp. finitely presented) A-algebra, then $\Omega_{A/R}$ is a finitely generated (resp. finitely presented) A-module. Here, an R-algebra A is called finitely presented if A is the quotient of $R[X_1, \dots, X_n]$ by a finitely generated ideal.

25.7. Cotangent exact sequence. Recall that if $\pi : M \to N$ is a submersion of manifolds, then we have a short exact sequence of vector bundles

$$0 \to T_{M/N} \to T_M \to \pi^* T_N \to 0,$$

defining the relative tangent bundle $T_{M/N}$. The following the is analogous statement for cotangent modules, which also explains why $\Omega_{A/R}$ is called module of relative differentials.

Proposition 25.12. *Let $R \to A \to B$ be ring homomorphisms. We have an exact sequence of B-modules*

$$B \otimes_A \Omega_{A/R} \xrightarrow{b\otimes(da)\mapsto b\cdot da} \Omega_{B/R} \xrightarrow{db\mapsto db} \Omega_{B/A} \to 0.$$

Proof. It is clear that $\Omega_{B/R} \to \Omega_{B/A}$ is surjective. The composition of the two maps in the sequence is zero, because $da = 0$ in $\Omega_{B/A}$ for every $a \in A$. Finally, it follows from the defining relations of the modules of differentials that the kernel of $\Omega_{B/R} \to \Omega_{B/A}$ is the B-submodule generated by da for all $a \in A$, and this is exactly the image of $B \otimes_A \Omega_{A/R} \to \Omega_{B/R}$. □

Exercise 25.13. Let L/K be a field extension with finite transcendental degree.

(1) Compute $\Omega_{L/K}$ when L/K is purely transcendental.
(2) Show that $\Omega_{L/K} = 0$ if and only if L/K is an algebraic separable extension.

25.8. Conormal modules. Recall that if $Z \subset M$ is a closed submanifold of a manifold M, then we have a short exact sequence of vector bundles

$$0 \to T_Z \to T_{M|Z} \to N_{Z/M} \to 0,$$

defining the normal bundle $N_{Z/M}$ of Z in M.

Here is the analogous statement for cotangent modules.

Proposition 25.14. *Let R be a ring and let $A \to B$ be a surjective morphism of R-algebras. Let $I := \ker(A \to B)$. We have an exact sequence of B-modules*

$$I/I^2 \xrightarrow{i\mapsto 1\otimes(di)} B \otimes_A \Omega_{A/R} \xrightarrow{b\otimes(da)\mapsto b\cdot da} \Omega_{B/R} \to 0.$$

In the above statement, we call I/I^2 the *conormal module* of Spec(B) in Spec(A).

Proof. First we note that since $B = A/I$, the map $I/I^2 \to B \otimes_A \Omega_{A/R}$ is well defined by the Leibniz rule.

Since $A \to B$ is surjective, we have $\Omega_{B/A} = 0$, so $B \otimes_A \Omega_{A/R} \to \Omega_{B/R}$ is surjective by Proposition 25.12. It is clear that the composition of the two maps in the sequence is zero. Finally, the first map is isomorphic to $B \otimes_A I \to B \otimes_A \Omega_{A/R}$ defined by $b \otimes i \mapsto b \otimes di$, so its cokernel Q is generated as a B-module by $1 \otimes db$ for all $b \in B$. We verify that the defining relations $\Omega_{B/R}$ can also be lifted to the defining relations of Q, hence $Q \simeq \Omega_{B/R}$. □

25.9. Derivation and universal property. Let R be a ring and let A be an R-algebra. Let M be an A-module. An R-derivation from A to M is a map $D : A \to M$ satisfying the following properties.

(1) $Dr = 0$ for all $r \in R$;
(2) $D(f + g) = Df + Dg$ for all $f, g \in A$;
(3) (Leibniz' rule) $D(fg) = f \cdot Dg + g \cdot Df$ for all $f, g \in A$.

Equivalently and more concisely, an R-derivation is an R-linear morphism $D : A \to M$ which satisfies Leibniz' rule as above. The R-derivations from A to M form an A-module, denoted by $\mathrm{Der}_R(A, M)$.

For instance, the map $d : A \to \Omega_{A/R}$ is an R-derivation; this is the universal one.

Proposition 25.15 (Universal property of modules of differentials)**.** *For any A-module M, the map*

$$\begin{aligned} \mathrm{Hom}_A(\Omega_{A/R}, M) &\to \mathrm{Der}_R(A, M). \\ \phi &\mapsto \phi \circ d \end{aligned} \tag{25.1}$$

is an isomorphism of A-modules.

Exercise 25.16. Prove Proposition 25.15.

As a consequence, if $D : A \to N$ is an R-derivation such that the universal property stated in Proposition 25.15 holds for D instead of $d : A \to \Omega_{A/R}$, then there is a unique isomorphism $\phi : N \xrightarrow{\sim} \Omega_{A/R}$ of A-modules such that $\phi \circ D = d$.

Exercise 25.17. Let $\mathbf{k}$ be a field and let R be a $\mathbf{k}$-algebra. Let $\mathfrak{m} \subset \mathrm{Specm}(R)$ be a closed point such that $R/\mathfrak{m} \simeq \mathbf{k}$ (as $\mathbf{k}$-algebras); such a point is called a $\mathbf{k}$*-point*, or a *rational point* of $\mathrm{Spec}(R)$. Show that the map

$$\mathrm{Der}_{\mathbf{k}}(R, \mathbf{k}) \to \mathrm{Hom}_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2, \mathbf{k})$$

sending D to its restriction to $\mathfrak{m}$ is well defined and is a $\mathbf{k}$-linear isomorphism. (The argument should be similar to that of Exercise 25.1.)

25.10. Cotangent space at a rational point. Let $\mathbf{k}$ be a field and let R be a finitely generated $\mathbf{k}$-algebra.

Proposition 25.18. *For every* $\mathbf{k}$*-point* $x \in \mathrm{Spec}(R)$ *which corresponds to the maximal ideal* $\mathfrak{m} \in R$*, the map*

$$\mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\sim} (\Omega_{R/\mathbf{k}})|_x$$

defined by $f \mapsto (df)|_x$ *is a* $\mathbf{k}$*-linear isomorphism.*

Proof. That $\mathfrak{m}/\mathfrak{m}^2 \to (\Omega_{A/\mathbf{k}})|_x$ is well defined follows from the Leibniz rule. We will instead show that the dual of $\mathfrak{m}/\mathfrak{m}^2 \to (\Omega_{A/\mathbf{k}})|_x$ is an isomorphism.

We have canonical isomorphisms of $\mathbf{k}$-vector spaces

$$\mathrm{Hom}_{\mathbf{k}}(\Omega_{R/\mathbf{k}} \otimes_R \mathbf{k}, \mathbf{k}) \simeq \mathrm{Hom}_R(\Omega_{R/\mathbf{k}}, \mathbf{k}) \simeq \mathrm{Der}_{\mathbf{k}}(R, \mathbf{k}) \simeq \mathrm{Hom}_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2, \mathbf{k}),$$

where the first isomorphism is the adjunction of extension-restriction of scalars, the second isomorphism is the universal property of modules of differentials, and the third isomorphism is the one in Exercise 25.17. We verify that the dual of the composition of the above isomporhisms is $f \mapsto (df)|_x$. □

Exercise 25.19. Let $x \in \mathrm{Spec}(R)$ be a $\mathbf{k}$-point and let $\phi : R \to \mathbf{k}$ be the induced quotient map. Show that

$$\begin{aligned} \mathrm{Hom}_R(\Omega_{R/\mathbf{k}}, \mathbf{k}) &\to \left\{ \mathbf{k}\text{-algebra factorizations } R \xrightarrow{\widetilde{\phi}} \mathbf{k}[\varepsilon]/(\varepsilon^2) \to \mathbf{k} \text{ of } \phi \right\}. \\ \psi &\mapsto (\widetilde{\phi} : f \mapsto \phi(f) + \varepsilon\psi(f)) \end{aligned} \tag{25.2}$$

is a bijection. Thus morphisms of schemes $\mathrm{Spec}(\mathbf{k}[\varepsilon]/(\varepsilon^2)) \to \mathrm{Spec}(R)$ over $\mathbf{k}$ can be regarded as tangent vectors on $\mathrm{Spec}(R)$.

25.11. Pullback and localization. Let

$$\begin{tikzcd} A \arrow[r] & A' \\ R \arrow[u] \arrow[r, "f"] & R' \arrow[u] \end{tikzcd} \tag{25.3}$$

be a commutative diagram of ring homomorphisms. It induces an morphism of A'-modules

$$\phi : A' \otimes_A \Omega_{A/R} \to \Omega_{A'/R'}$$

sending $a' \otimes da$ to $a' \cdot da$.

Exercise 25.20.

(1) Show that the morphism $\phi : A' \otimes_A \Omega_{A/R} \to \Omega_{A'/R'}$ introduced above is well defined, and is the image of the R-derivation $A \to A' \to \Omega_{A'/R'}$ under

$$\mathrm{Der}_R(A, \Omega_{A'/R'}) \simeq \mathrm{Hom}_A(\Omega_{A/R}, \Omega_{A'/R'}) \simeq \mathrm{Hom}_{A'}(A' \otimes_A \Omega_{A/R}, \Omega_{A'/R'}),$$

where the first isomorphism is the universal property of modules of differentials, and the second isomorphism is the adjunction of extension-restriction of scalars.

(2) Suppose that (25.3) is a co-cartesian square (namely $A' \simeq A \otimes_R R'$), show that

$$\phi : A' \otimes_A \Omega_{A/R} \xrightarrow{\sim} \Omega_{A'/R'}$$

is an isomrophism.

Exercise 25.21. Let $f : R \to A$ be a ring homomorphism. Let $S \subset R$ and $T \subset A$ be multiplicative subsets such that $f(S) \subset T$. Show that

$$T^{-1}\Omega_{A/R} \simeq \Omega_{T^{-1}A/S^{-1}R}.$$

25.12. The cotangent module is the conormal module of the diagonal. Let R be a ring and let A be an R-algebra. Let

$$X := \operatorname{Spec}(A) \times_{\operatorname{Spec}(R)} \operatorname{Spec}(A) \simeq \operatorname{Spec}(A \otimes_R A)$$

The *diagonal* of X is the subscheme $\Delta \subset X$ defined by the ideal $I_\Delta \subset A \otimes_R A$ generated by

$$a := a \otimes 1 - 1 \otimes a \quad : \quad a \in A.$$

Exercise 25.22. Show that I_Δ is the kernel of $A \otimes_R A \to A$ defined by $a \otimes a' \mapsto aa'$. Hint: observe that if $\sum_i a_i a_i' = 0$, then

$$\sum_i a_i \otimes a_i' = \sum_i (1 \otimes a_i')(a_i \otimes 1 - 1 \otimes a_i).$$

Exercise 25.23. Show that

$$\begin{aligned} \delta : A &\to I_\Delta / I_\Delta^2. \\ A &\mapsto a \otimes 1 - 1 \otimes a \mod I_\Delta^2 \end{aligned} \tag{25.4}$$

is an R-derivation.

We thus have a factorization

$$\delta : A \xrightarrow{d} \Omega_{A/R} \xrightarrow{\phi} I_\Delta / I_\Delta^2$$

of δ, by the universal property of $\Omega_{A/R}$. Note that since da for all $a \in A$ generate the A-module $\Omega_{A/R}$, the morphism ϕ of A-modules is surjective.

Exercise 25.24. Show that $\psi : I_\Delta / I_\Delta^2 \to \Omega_{A/R}$ defined by $a \otimes b \mapsto a \cdot db$ is well-defined, and $\psi \circ \phi = \mathrm{Id}$.

The above statements lead to the following:

Proposition 25.25. *The map $\phi : \Omega_{A/R} \to I_\Delta / I_\Delta^2$ is an isomorphism of A-modules.*

26. Dimension of the tangent cone

Let $(R, \mathfrak{m})$ be a Noetherian local ring.

Theorem 26.1. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Let $\mathbf{k} = R/\mathfrak{m}$. The function*

$$H_{R,\mathfrak{m}} : i \mapsto: \dim_{\mathbf{k}} \mathfrak{m}^i / \mathfrak{m}^{i+1}$$

is polynomial for $i \gg 0$, and the degree is equal to $\dim R - 1$. As a consequence,

$$\dim R = \dim C_{R,\mathfrak{m}}.$$

26.1. Hilbert–Samuel function. We will derive Theorem 26.1 as a consequence of a more general statement (Theorem 26.17) that we will prove by induction. For this reason, we consider the following functions which generalize $H_{R,\mathfrak{m}}$.

Let M be a finitely generated R-module. An ideal $I \subset R$ is called a *parameter ideal of M* if $\operatorname{Supp}(M/IM) = \{\mathfrak{m}\}$. This generalizes the notion of parameter ideal of a local ring. If I is a parameter ideal of M, then for all $n \in \mathbf{Z}_{\geq 0}$, by Exercise 17.16 the R-module $I^n M / I^{n+1} M$ has finite length. The *Hilbert–Samuel function* is defined as

$$H_{M,I} : n \mapsto \lg_R(I^n M / I^{n+1} M).$$

26.2. Associated graded ring and module. Let $I \subset R$ be an ideal. We define The *associated graded ring* of R and *associated graded module* of M by

$$\operatorname{gr}_I R := \bigoplus_{n=0}^{\infty} I^n / I^{n+1}, \quad \operatorname{gr}_I M := \bigoplus_{n=0}^{\infty} I^n M / I^{n+1} M.$$

We regard $\mathrm{gr}_I M$ as a graded $\mathrm{gr}_I R$-module as follows: for any $r \in I^\ell/I^{\ell+1}$ and $m \in I^n M/I^{n+1}M$, we first lift them to $\tilde{r} \in I^\ell$ and $\tilde{m} \in I^n M$, then $\tilde{r}\tilde{m} \in I^{\ell+n}M$ modulo $I^{\ell+n+1}M$ is independent of the liftings.

Lemma 26.2. *If M is finitely generated over R, then $\mathrm{gr}_I M$ is finitely generated over $\mathrm{gr}_I R$.*

Proof. Since M/IM is finitely generated over R and $I^n M/I^{n+1}M = (I^n/I^{n+1}) \cdot (M/IM)$, Lemma 26.2 follows. □

Lemma 26.3. *If R is Noetherian, then $\mathrm{gr}_I R$ is also Noetherian.*

Proof. Since I is a finitely generated ideal, by construction $\mathrm{gr}_I R$ is a finitely generated R/I-algebra. As R/I is Noetherian, it follows that $\mathrm{gr}_I R$ is also Noetherian. □

26.3. Hilbert functions. Let $R = \bigoplus_{d=0}^\infty R_d$ be a graded ring and let $M = \bigoplus_{d \in \mathbf{Z}} M_d$ be a graded R-module; in these lectures, a graded ring is always $\mathbf{Z}_{\geq 0}$ but a graded module is $\mathbf{Z}$-graded. Each M_d is thus an R_0-module. Suppose that each M_d is an R_0-module of finite length, the function

$$H_M : i \mapsto \lg_{R_0} M_d$$

is called the *Hilbert function* of the graded R-module M.

Exercise 26.4. Let $I \subset R$ be a parameter ideal of the R-module M. Show that

$$H_{M,I} = H_{\mathrm{gr}_I M}$$

where $\mathrm{gr}_I M$ is regarded as a graded module over $\mathrm{gr}_I R$.

26.4. Polynomiality of Hilbert functions. Let R be a graded ring. We say that R is *finitely generated in degree* 1 if there exist $r_1, \ldots, r_n \in R_1$ which generate R as an R_0-algebra.

Theorem 26.5. *Let R be a graded ring. Suppose that R is generated in degree 1 by k elements. Let M be a finitely generated R-module such that each R_0-module M_d has finite length (this is the case when e.g. R_0 is Artinian). Then there exist an integer $n_0 \geq 0$ and a polynomial $P_M \in \mathbf{Q}[x]$ with $\deg P < k$ such that*

$$H_M(n) = P_M(n)$$

for all $n \geq n_0$.

The polynomial P_M is called the *Hilbert polynomial* of the graded R-module M.

Proof. We prove Theorem 26.5 by induction on k. Suppose that $k = 0$. Then $R = R_0$. Since M is finitely generated over R, we have $M_d = 0$ for d sufficiently large. Hence $P = 0$ works.

Suppose that R is generated by $x_1, \ldots, x_k \in R_1$ as an R_0-algebra. Consider the exact sequence

$$0 \to K \to M \xrightarrow{\times x_1} M(1) \to Q \to 0$$

where $M(d)$ is the graded module defined by $M(d)_i := M_{d+i}$, and K and Q are the kernel and the cokernel of $M \xrightarrow{\times x_1} M(1)$. Since $M \xrightarrow{\times x_1} M(1)$ preserves the grading, both K and Q are graded R-modules. Since the length function is additive, we have $H_M(n+1) - H_M(n) = H_Q(n) - H_K(n)$. Note that x_1 annihilates both K and Q, we can regard them as modules over $R/(x_1)$. So by the induction hypothesis, $n \mapsto H_Q(n) - H_K(n)$ is a rational polynomial function when $n \gg 0$. We conclude by Lemma 26.8 below. □

Corollary 26.6. *Let R be a local ring and let M be a finitely generated R-module. Let $I \subset R$ be a parameter ideal of M. Then there exists a polynomial $P_{M,I} \in \mathbf{Q}[x]$ such that $H_{M,I}(n) = P_{M,I}(n)$ for $n \gg 0$. Moreover, if I is generated by k elements, then $\deg P_{M,I} < k$.*

Proof. It suffices to show that $\deg P_{M,I} = \deg P_{M,\mathfrak{m}}$. Up to replacing R by $R/\mathrm{Ann}(M)$, we can assume that $\mathrm{Supp}(M) = \mathrm{Spec}(R)$. Then $\mathrm{Ann}(M/IM) = I$, and thus $V(I) = \mathrm{Supp}(M/IM) = \{\mathfrak{m}\}$. So $\dim R/I = 0$. Since R is Noetherian, R/I is thus Artinian, and we conclude by Theorem 26.5 and Exercise 26.4. □

26.5. Polynomial differences. For any $k \in \mathbf{Z}_{\geq 0}$, define the polynomial

$$x \mapsto \binom{x}{k} := \frac{x(x-1)\cdots(x-k+1)}{k!}$$

Exercise 26.7. For any $k, n \in \mathbf{Z}_{\geq 0}$, show that

$$\binom{n}{k} = \sum_{m=0}^{n-1} \binom{m}{k-1}$$

Lemma 26.8. *Let $H : \mathbf{Z} \to \mathbf{Z}$ be a function. Suppose that there exist $n_0 \geq 0$ and a polynomial $Q \in \mathbf{Q}[x]$ such that*

$$H(n+1) - H(n) = Q(n)$$

for all $n \geq n_0$, then there exists a polynomial $P \in \mathbf{Q}[x]$ such that

$$H(n) = P(n)$$

for all $n \geq n_0$. Moreover $\deg P = \deg Q + 1$.

Proof. By translation, we can assume that $n_0 = 0$. For every $n \geq 0$, we have

$$H(n) = H(0) + \sum_{i=0}^{n-1} Q(i).$$

Since Q is a $\mathbf{Q}$-linear combination of the polynomials $x \mapsto \binom{x}{k}$ follows from Exercise 26.7. □

26.6. A variant of the Hilbert–Samuel function. We also consider the following variant of the Hilbert–Samuel function:

$$\widetilde{H}_{M,I} : n \mapsto \lg_R(M/I^n M).$$

We have

$$H_{M,I}(n) = \widetilde{H}_{M,I}(n+1) - \widetilde{H}_{M,I}(n).$$

So there exists a polynomial $\widetilde{P}_{M,I} \in \mathbf{Q}[x]$ such that $\widetilde{H}_{M,I}(n) = \widetilde{P}_{M,I}(n)$ for $n \gg 0$ and $\deg \widetilde{P}_{M,I} = 1 + \deg P_{M,I}$.

26.7. Upper bound of the degree of the Hilbert polynomial. Let R be a local ring and let M be an R-module.

Lemma 26.9. *The degree of the Hilbert–Samuel polynomial $P_{M,I}$ does not depend on the parameter ideal I.*

Proof. It suffices to show that $\deg P_{M,I} = \deg P_{M,\mathfrak{m}}$. As we did in the proof of Corollary 26.6, up to replacing R by $R/\mathrm{Ann}(M)$, we can assume that $\mathrm{Supp}(M) = \mathrm{Spec}(R)$. This implies that R/I is Artinian, so there exists some integer $d > 0$ such that

$$\mathfrak{m}^d \subset I \subset \mathfrak{m}.$$

Since

$$\widetilde{H}_{M,\mathfrak{m}}(n) \leq \widetilde{H}_{M,I}(n) \leq \widetilde{H}_{M,\mathfrak{m}^d}(n),$$

we have

$$\widetilde{P}_{M,\mathfrak{m}}(n) \leq \widetilde{P}_{M,I}(n) \leq \widetilde{P}_{M,\mathfrak{m}}(dn)$$

for $n \gg 0$. Hence $\deg \widetilde{P}_{M,I} = \deg \widetilde{P}_{M,\mathfrak{m}}$, which finishes the proof. □

Corollary 26.10. *We have* $\deg P_{M,I} \leq \dim \mathrm{Supp}(M) - 1$.

Proof. Up to replacing R by $R/\mathrm{Ann}(M)$, we can assume that $\mathrm{Supp}(M) = \mathrm{Spec}(R)$. By Exercise 21.6, some parameter ideal I is generated by $\dim R$ elements. It follows from Theorem 26.5 and Lemma 26.9 that $\deg P_{M,I} \leq \dim R - 1 = \dim \mathrm{Supp}(M) - 1$. □

26.8. Blowup algebra. Let R be a ring and let $I \subset R$ be an ideal. The *blowup algebra* (or the *Rees algebra*) of I is R is the graded R-algebra

$$\mathrm{Bl}_I R := \bigoplus_{d=0}^{\infty} I^d.$$

Remark 26.11. In this remark we assume some background in algebraic geometry. Suppose that I is finitely generated. Then the morphism The blowup Proj ${}_R\mathrm{Bl}_I R \to \mathrm{Spec}(R)$ defined by the R-algebra structure of $\mathrm{Bl}_I R$ is the blowup of $\mathrm{Spec}(R)$ along I, which is why $\mathrm{Bl}_I R$ is called the blowup algebra. Note that we have a surjective morphism

$$\mathrm{Bl}_I R \twoheadrightarrow C_{R,I} := \bigoplus_{d=0}^{\infty} I^d/I^{d+1},$$

and the kernel is the ideal $I \cdot \mathrm{Bl}_I R = I \oplus I^2 \oplus \cdots$. The the ideal $I \cdot \mathrm{Bl}_I R$ cuts out a Cartier divisor E in Proj ${}_R\mathrm{Bl}_I R$, called the *exceptional divisor*. The divisor E is isomorphic to the projectivized normal cone Proj $C_{R,I}$ of I in R.

Let M be an R-module. A filtration

$$\mathscr{I} : M = M_0 \supset M_1 \supset \cdots$$

is called an *I-filtration* if $IM_d \subset M_{d+1}$ for all index d. Let

$$\mathrm{Bl}_{\mathscr{I}} M := \bigoplus_{d=0}^{\infty} M_d,$$

regarded as a $\mathrm{Bl}_I R$-module in a natural way.

Proposition 26.12. *Let $\mathscr{I} : M = M_0 \supset M_1 \supset \cdots$ be an I-filtration of M such that each M_d is finitely generated over R. The following assertions are equivalent.*

(1) $\mathrm{Bl}_{\mathscr{I}} M$ is finitely generated over $\mathrm{Bl}_I R$.

(2) There exists an integer n_0 such that $M_{n+1} = IM_n$ for every $n \geq n_0$.

If the filtration $\mathscr{I}$ satisfies (2) in Proposition 26.12, we call $\mathscr{I}$ an *I-stable* filtration.

Proof. It is clear that (2) implies (1). Suppose that $\mathrm{Bl}_{\mathscr{I}} M$ is finitely generated over $\mathrm{Bl}_I R$: we can assume that $\mathrm{Bl}_{\mathscr{I}} M$ is generated by homogeneous elements of degree $\leq n_0$. Then for every $i \in \mathbf{Z}_{\geq 0}$ and every $m \in M_{n_0+i}$ we have

$$m = \sum_{j=0}^{n_0} \sum_{\ell=0}^{s_j} r^{(\ell)}_{n_0+i-j} m^{(\ell)}_j$$

for some $r^{(\ell)}_{n_0+i-j} \in R_{n_0+i-j}$ and $m^{(\ell)}_j \in M_j$. Hence

$$M_{n_0+i} \subset \sum_{j=0}^{n_0} I^{n_0+i-j} M_j \subset I^i M_{n_0}.$$

So $M_{n_0+i} = I^i M_{n_0}$, which shows that $M_{n+1} = IM_n$ for every $n \geq n_0$. □

Corollary 26.13 (Artin–Rees lemma). *Let R be a Noetherian ring and let M be a finitely generated R-module with an I-filtration*

$$\mathscr{I} : M = M_0 \supset M_1 \supset \cdots .$$

Let $M' \subset M$ be a R-submodule. If $\mathscr{I}$ is I-stable, then the I-filtration

$$\mathscr{I}' = M' \cap \mathscr{I} : \ (M' \cap M_0) \supset (M' \cap M_1) \supset \cdots$$

is also I-stable.

Proof. Since R is Noetherian and $\mathrm{Bl}_I R$ is a finitely generated R-algebra, $\mathrm{Bl}_I R$ is also Noetherian. By Proposition 26.12, $\mathrm{Bl}_{\mathscr{I}} M$ is finitely generated over $\mathrm{Bl}_I R$, so $\mathrm{Bl}_{\mathscr{I}'} M'$ is also finitely generated over $\mathrm{Bl}_I R$. Hence $\mathscr{I}'$ is I-stable by Proposition 26.12. □

Corollary 26.14 (Krull's intersection theorem). *Let $(R, \mathfrak{m})$ be a Noetherian local integral domain. We have*

$$\bigcap_{n \geq 0} \mathfrak{m}^n = 0.$$

Proof. Let $I \subset R$ be an ideal. Applying the Artin–Rees lemma to I endowed with the $\mathfrak{m}$-filtration

$$I \supset (\mathfrak{m} \cap I) \supset (\mathfrak{m}^2 \cap I) \supset \cdots$$

shows that for $n \gg 0$, we have

$$\mathfrak{m}^{n+1} \cap I = \mathfrak{m}(\mathfrak{m}^n \cap I).$$

For $I = \bigcap_{n \geq 0} \mathfrak{m}^n$, we thus have $I = \mathfrak{m}I$, hence I by the Nakayama lemma. □

Remark 26.15. Note the the conclusion of Krull's intersection theorem does not hold for the local ring $(\mathscr{C}^\infty_{0,\mathbf{R}}, \mathfrak{m})$, because $\mathfrak{m}^d$ is the ideal of germs of smooth functions f with $f(0) = f'(0) = \cdots = f^{(d-1)}(0) = 0$, but $x \mapsto \exp(-1/x^2)$ has vanishing derivatives at 0 of all orders.

26.9. An additivity result of the Hilbert–Samuel function.

Lemma 26.16. *Let R be a local ring and let*

$$0 \to M' \to M \to M'' \to 0$$

be a short exact sequence of R-modules. Let I be a parameter ideal of both M and M'. *Then there exists $Q \in \mathbf{Q}[x]$ with positive leading coefficient and* $\deg Q \leq \deg \widetilde{P}_{M',I} - 1$ *such that*

$$\widetilde{P}_{M,I}(n) = \widetilde{P}_{M',I}(n) + \widetilde{P}_{M'',I}(n) - Q(n),$$

for $n \gg 0$.

Proof. We have an exact sequence

$$0 \to \frac{M' \cap I^n M}{I^n M'} \to \frac{M'}{I^n M'} \to \frac{M}{I^n M} \to \frac{M''}{I^n M''} \to 0,$$

which yields

$$\widetilde{P}_{M,I}(n) = \widetilde{P}_{M',I}(n) + \widetilde{P}_{M'',I}(n) - Q(n),$$

where Q is a polynomial such that

$$Q(n) := \lg_R \left(\frac{M' \cap I^n M}{I^n M'} \right)$$

for $n \gg 0$.

By Artin–Rees, there exsits an integer n_0 such that for all positive integer $i > 0$, we have

$$M' \cap I^{n_0+i} M = I^i (M' \cap I^{n_0} M') \subset I^i M'.$$

So

$$Q(n) \leq \widetilde{H}_{M',I}(n) - \widetilde{H}_{M',I}(n - n_0),$$

for $n \gg 0$, showing that the polynomial Q satisfies $\deg Q \leq \deg \widetilde{P}_{M',I} - 1$. □

26.10. Lower bound of the degree of the Hilbert polynomial.

Theorem 26.17. *Let $(R, \mathfrak{m})$ be a local ring and let M be a finitely generated R-module. We have*

$$\deg \widetilde{P}_{M,\mathfrak{m}} = \dim \operatorname{Supp}(M).$$

Proof. By Corollary 26.10, it remains to show that $\deg \widetilde{P}_{M,\mathfrak{m}} \geq \dim \operatorname{Supp}(M)$.

We can assume that $M \neq 0$. We prove Theorem 26.17 by induction on $\dim \operatorname{Supp}(M) \geq 0$. Suppose that $\dim \operatorname{Supp}(M) = 0$. Then $\widetilde{P}_{M,\mathfrak{m}} \neq 0$ (otherwise, $M = \mathfrak{m}M$, which is impossible by Nakayama's lemma). So we always have $\deg \widetilde{P}_{M,\mathfrak{m}} \geq 0$.

Let $\mathfrak{p} \in \operatorname{Spec}(R)$ be the generic point of an irreducible component of $\operatorname{Supp}(M)$ of maximal dimension. In particular $\mathfrak{p} \in \operatorname{Ass}_R(M)$, so $\mathfrak{p} = \operatorname{Ann}(m)$ for some $m \in M$, and therefor M contains an R-submodule isomorphic to $R/\mathfrak{p}$. Since $\widetilde{P}_{R/\mathfrak{p},\mathfrak{m}}(n) \leq \widetilde{P}_{M,\mathfrak{m}}(n)$ for $n \gg 0$, we can assume that $M = R/\mathfrak{p}$. Furthermore, since

$$\lg_R \frac{R}{\mathfrak{p} + \mathfrak{m}^n} = \lg_{R/\mathfrak{p}} \frac{R/\mathfrak{p}}{\mathfrak{m}^n/\mathfrak{p}},$$

we can assume that $M = R$ and that R is a local integral domain.

Let $x \in R$ be a nonzero element. Applying Lemma 26.16 to the short exact sequence

$$0 \to R \xrightarrow{\times x} R \to R/(x) \to 0$$

yields

$$\deg \widetilde{P}_{R,\mathfrak{m}} \geq 1 + \deg \widetilde{P}_{R/(x),\mathfrak{m}},$$

so $\deg \widetilde{P}_{R,\mathfrak{m}} \geq 1 + \dim R/(x)$ by the induction hypothesis. Since $x \neq 0$ and R is an integral domain, we have $\dim R = 1 + \dim R/(x)$ by the principal ideal theorem, which finishes the proof. □

26.11. Regular local rings.

Definition 26.18. A Noetherian local ring $(R, \mathfrak{m})$ is called *regular* if at the closed point $\mathfrak{m}$, the tangent cone is equal to the tangent space.

Exercise 26.19. Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension d. Let $\mathbf{k} = R/\mathfrak{m}$ Show that the following assertions are equivalent.

(1) R is regular.
(2) $\mathfrak{m}$ is generated by exactly d elements.
(3) $\dim_{\mathbf{k}} \mathfrak{m}/\mathfrak{m}^2 = d$.

Exercise 26.20. Let $(R, \mathfrak{m})$ be a Noetherian local ring.

(1) Suppose that $\dim R = 0$. Show that R is regular if and only if R is a field.
(2) Suppose that $\dim R = 1$. Show that R is regular if and only if R is a DVR.

LECTURE 13

Projective modules and flat modules

Let R be a ring.

27. Extensions

27.1. The set of extensions. Let M and N be R-modules. We can always produce a new R-module from them by considering $M \oplus N$. It sits in the middle of a short exact sequence of the form

$$0 \to N \to E \to M \to 0 \tag{27.1}$$

but not all R-module E fitting in (27.1) is isomorphic to $M \oplus N$, for instance we have the exact sequence

$$0 \to \mathbf{Z} \xrightarrow{\times 2} \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0.$$

This is the main reason why R-modules are much more complicated then vector spaces over a field.

A short exact sequence (27.1) is called an *extension of M by N*. We let

$$\mathrm{Ext}_R(M, N) := \{ \text{ extensions of } M \text{ by } N \} / \text{equivalence},$$

where two extensions $N \to E \to M$ and $N \to E' \to M$ are equivalent if there exists an isomorphism $\phi : E \xrightarrow{\sim} E'$ of R-modules such that the diagram

$$\begin{tikzcd} N \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d, "\phi", "\wr"'] & M \arrow[d, equal] \\ N \arrow[r] & E' \arrow[r] & M \end{tikzcd}$$

commutes.

Exercise 27.1. Let $d > 0$ be an integer. What is the cardinal of $\mathrm{Ext}_{\mathbf{Z}}(\mathbf{Z}/d, \mathbf{Z})$?

The above exercise imply in particular that equality in $\mathrm{Ext}_R(M, N)$ doesn't imply that the middle terms are isomorphic.

27.2. Pullback and pushout. Let $f : L \to M$ and $g : L \to N$ be morphisms of R-modules. Define

$$M \coprod_L N := \mathrm{coker}\Big(L \xrightarrow{x \mapsto (f(x), -g(x))} M \oplus N\Big).$$

Exercise 27.2. Show that $M \coprod_L N$ satisfies the universal property of the fiber coproduct of M and N over L.

Let $f : M \to L$ and $g : N \to L$ be morphisms of R-modules. Define

$$M \times_L N := \ker\Big(M \oplus N \xrightarrow{(m,n) \mapsto f(m) - g(n)} L\Big).$$

Exercise 27.3. Show that $M \times_L N$ satisfies the universal property of the fiber product of M and N over L.

27.3. Functoriality of $\mathrm{Ext}_R(M, N)$. Let M and N be R-modules. Every morphism of R-modules $f : N \to N'$ defines a natural map

$$\mathrm{Ext}_R(M, N) \to \mathrm{Ext}_R(M, N')$$

sending $N \to E \to M$ to the second line of the natural commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, "f"] & E \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N' \arrow[r] & E \coprod_N N' \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

Likewise, every morphism of R-modules $g : M \to M'$ defines a natural map

$$\mathrm{Ext}_R(M', N) \to \mathrm{Ext}_R(M, N)$$

sending $N \to E \to M'$ to the first line of the natural commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E \times_{M'} M \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, "g"] & 0 \\
0 \arrow[r] & N \arrow[r] & E' \arrow[r] & M' \arrow[r] & 0
\end{tikzcd}$$

Exercise 27.4. Verify that

$$\mathrm{Ext}_R(\bullet, \bullet) : (\mathrm{Mod}_R)^{\mathrm{op}} \times \mathrm{Mod}_R \to \mathrm{Set}$$

is a bifunctor.

27.4. The Baer sum. Let $E_1, E_2 \in \mathrm{Ext}_R(M, N)$. We have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & N \oplus N \arrow[r] \arrow[d, "(n,n') \mapsto n+n'"'] & E_1 \oplus E_2 \arrow[r] \arrow[d] & M \oplus M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E' \arrow[r] & M \oplus M \arrow[r] & 0 \\
0 \arrow[r] & N \arrow[r] & E_1 + E_2 \arrow[r] \arrow[u] & M \arrow[r] \arrow[u, "m \mapsto (m,m)"'] & 0
\end{tikzcd}$$

where E' is the R-module such that upper-left square is co-cartesian and $E_1 + E_2$ is the R-module such that lower-right square is cartesian; the horizontal arrows are the natural ones

Exercise 27.5. Prove the following statements.

(1) The horizontal sequences are exact.

(2) $\mathrm{Ext}_R(M, N)$ endowed with the addition defined by $(E_1, E_2) \mapsto E_1 + E_2$ is an abelian group.

27.5. The R-module structure on $\mathrm{Ext}_R(M, N)$. The extension group $\mathrm{Ext}_R(M, N)$ has a natural R-module structure defined as follows. For every $r \in R$ and every extension $e \in \mathrm{Ext}_R(M, N)$ which corresponds to the exact sequence

$$0 \to N \xrightarrow{\phi} E \xrightarrow{\psi} M \to 0,$$

the product $r \cdot e \in \mathrm{Ext}_R(M, N)$ is defined by the pushout construction

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, "\times r"] & E \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \arrow[r] & E \coprod_N N \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

Exercise 27.6. Show that $r \cdot e \in \mathrm{Ext}_R(M, N)$ is also represented by the extension obtained by the pullback construction

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E \times_N N \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, "\times r"] & 0 \\
0 \arrow[r] & N \arrow[r] & E \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

Exercise 27.7. Given morphisms of R-modules $M \to M'$ and $N \to N'$, show that the maps $\mathrm{Ext}_R(M, N) \to \mathrm{Ext}_R(M, N')$ and $\mathrm{Ext}_R(M', N) \to \mathrm{Ext}_R(M, N)$ are morphisms of R-modules.

27.6. The Yoneda product between Hom **and** Ext**.** Let M, N, N' be R-modules. Consider the map

$$\mu : \mathrm{Hom}_R(M, N) \times \mathrm{Ext}_R(N, N') \to \mathrm{Ext}_R(M, N')$$

sending a morphism $g : M \to N$ and an extension $e \in \mathrm{Ext}_R(M, N')$ to the image of e under the homomorphism $\mathrm{Ext}_R(N, N') \to \mathrm{Ext}_R(M, N')$ induced by g.

Exercise 27.8. Show that μ is R-bilinear.

27.7. Extending the exact sequence. Let M be an R-module. We know that the functors $\mathrm{Hom}_R(M, \bullet)$ and $\mathrm{Hom}_R(\bullet, M)$ are left-exact, but not necessarily right exact. However, we can extend the induced exact sequence from the right by a few terms involving Ext.

Exercise 27.9. Let N be an R-module and let

$$0 \to M' \to M \to M'' \to 0$$

be a short exact sequence of R-modules. Show that we have exact sequences

$$0 \to \mathrm{Hom}_R(N, M') \to \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, M'') \to \mathrm{Ext}_R(N, M') \to \mathrm{Ext}_R(N, M) \to \mathrm{Ext}_R(N, M'')$$

and

$$0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N) \to \mathrm{Ext}_R(M'', N) \to \mathrm{Ext}_R(M, N) \to \mathrm{Ext}_R(M', N),$$

where the maps between Hom and Ext are defined by the Yoneda product.

27.8. Computing Hom**.** Let M and N be R-modules. Every R-module M is defined by generators and relations, and this is how $\mathrm{Hom}_R(M, N)$ is usually computed. Precisely, we have an exact sequence

$$R^{\oplus J} \to R^{\oplus I} \to M \to 0,$$

which induces a short exact sequence

$$0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(R^{\oplus I}, N) \to \mathrm{Hom}_R(R^{\oplus J}, N).$$

Note that we have $\mathrm{Hom}_R(R^{\oplus I}, N) \simeq \prod_I N$.

27.9. Computing Ext**.** Next we compute $\mathrm{Ext}_R(M, N)$ Start with an exact sequence

$$0 \to K \to F_0 \to M \to 0$$

where F_0 is a free R-module (of generators of M, so K is the submodule of relations).

Exercise 27.10. Let F be a free module. Show that $\mathrm{Ext}_R(F, N) = 0$.

By Exercise 27.9, we have a short exact sequence

$$\mathrm{Hom}_R(F_0, N) \to \mathrm{Hom}_R(K, N) \to \mathrm{Ext}_R(M, N) \to 0.$$

We can compute $\mathrm{Hom}_R(F_0, N) \to \mathrm{Hom}_R(K, N)$, again using generators and relations of K. Precisely, start with an exact sequence

$$F_2 \to F_1 \to K \to 0$$

or equivalently, an exact sequence

$$F_2 \to F_1 \to F_0 \to M \to 0$$

where F_1 and F_2 are free R-modules, we then have

$$\mathrm{Ext}_R(M, N) \simeq \mathrm{coker}(\mathrm{Hom}_R(F_0, N) \to \mathrm{Hom}_R(K, N)) \simeq \frac{\ker(\mathrm{Hom}_R(F_1, N) \to \mathrm{Hom}_R(F_2, N))}{\mathrm{Im}(\mathrm{Hom}_R(F_0, N) \to \mathrm{Hom}_R(F_1, N))}.$$

28. Higher Ext-groups

28.1. Free resolutions and higher Ext. Any R-module M has a *free resolution*, namely an exact sequence of R-modules

$$\cdots \to F_1 \to F_0 \to M \to 0$$

where F_i are free R-modules; the sequence can be unbounded from the left. The previous discussion motivates us to consider free resolutions of R-modules, and use them to define higher Ext-groups $\mathrm{Ext}^i_R(M,N)$ and further extend the exact sequences in Exercise 27.9.

We will see that the key property in the construction of $\mathrm{Ext}^i_R(M,N)$, is that the functor $\mathrm{Hom}(F_i,\bullet)$ is exact. An R-module P such that $\mathrm{Hom}(P,\bullet)$ is (right-)exact is called a *projective module*, and it is thus more natural to consider more generally *projective resolutions* of M: these are exact sequences of R-modules

$$\cdots \xrightarrow{d} P_1 \xrightarrow{d} P_0 \to M \to 0 \qquad (\mathscr{R})$$

such that each P_i is a projective module.

Proposition 28.1. *Let P be an R-module. The following assertions are equivalent.*

(1) P is projective.

(2) $\mathrm{Ext}_R(P,N)=0$ *for every R-module N.*

(3) P is a direct summand of a free module.

Proof. Assume (1). Then for any extension $e\in\mathrm{Ext}_R(P,N)$ represented by the exact sequence

$$0\to N\to E\xrightarrow{\psi} P\to 0,$$

the morphism ψ has a section, showing that e is equivalent to the trivial extension $N\oplus P$.

Assume (2). Choose any surjective morphism $\phi : F \twoheadrightarrow P$ of R-modules from a free R-module F. Then (2) implies that the extension $\ker(\phi)\to F\to P$ is trivial, so P is a direct summand of F.

Finally assume that (3). Then the identity $\mathrm{Id}: P\to P$ has a factorization $P\hookrightarrow F\twoheadrightarrow P$ through a free R-module F. This induces for any R-module N, a factorization

$$\mathrm{Hom}_R(P,N)\to\mathrm{Hom}_R(F,N)\to\mathrm{Hom}_R(P,N)$$

of the identity map. Therefore if $N\twoheadrightarrow N'$ is a surjective morphism of R-modules, since $\mathrm{Hom}_R(F,N)\to\mathrm{Hom}_R(F,N')$ is surjective (because F is free), necessarily the induces map $\mathrm{Hom}_R(P,N)\to\mathrm{Hom}_R(P,N')$ is surjective. □

Given such a projective resolution $\mathscr{R}$ of M, define for each $i\in\mathbf{Z}$ the R-module

$$\mathrm{Ext}^i_R(M,N)_{\mathscr{R}} := H^i(\mathrm{Hom}_R(P_\bullet,N));$$

we set $P_i=0$ if $i<0$. Here, for any complex of R-modules $C^\bullet$, namely a sequence of morphisms of R-modules

$$\cdots\to C^{i-1}\xrightarrow{d^{i-1}} C^i\xrightarrow{d^i} C^{i+1}\to\cdots$$

such that $d^i\circ d^{i-1}=0$), the ith cohomology of $C^\bullet$ is defined as

$$H^i(C^\bullet) := \frac{\ker d^i}{\mathrm{Im} d^{i-1}}.$$

28.2. Functoriality and independence of the projective resolutions. Let M' be another R-module and let

$$\cdots\xrightarrow{d} P'_1\xrightarrow{d} P'_0\to M'\to 0 \qquad (\mathscr{R}')$$

be a projective resolution of M'. For any morphism $f: M\to M'$ of R-modules, since each P_i is projective, we can lift f to a morphism $F: P_\bullet\to P'_\bullet$ of complexes, namely a commutative diagram of R-modules

$$\begin{tikzcd}
\cdots \arrow[r] & P_2 \arrow[r] \arrow[d, "F_2"] & P_1 \arrow[r] \arrow[d, "F_1"] & P_0 \arrow[r] \arrow[d, "F_0"] & M \arrow[d, "f"] \\
\cdots \arrow[r] & P'_2 \arrow[r] & P'_1 \arrow[r] & P'_0 \arrow[r] & M'.
\end{tikzcd}$$

It induces a morphism of R-modules

$$\mathrm{Ext}^i_R(M',N)_{\mathscr{R}'}\to\mathrm{Ext}^i_R(M,N)_{\mathscr{R}}.$$

Exercise 28.2. Two morphisms of complexes $F, G : P_\bullet \to P'_\bullet$ are called *homotopic* if there exists for each index i a morphism of R-modules $h_i : P_i \to P'_{i+1}$ such that

$$F_i - G_i = dh_i + h_{i-1}d.$$

Show that if $F, G : P_\bullet \to P'_\bullet$ are homotopic, then the morphism $\mathrm{Ext}^i_R(M', N)_{\mathscr{R}'} \to \mathrm{Ext}^i_R(M, N)_{\mathscr{R}}$ they induce are the *same*.

Exercise 28.3. Let

$$\cdots \xrightarrow{d} P'_1 \xrightarrow{d} P'_0 \to M \to 0 \qquad (\mathscr{R}')$$

be another projective resolution of M. Show that all lifts $P_\bullet \to P'_\bullet$ of the identity $\mathrm{Id} : M \to M$ are homotopic. This provides a *canonical isomorphism*

$$\mathrm{Ext}^i_R(M, N)_{\mathscr{R}'} \simeq \mathrm{Ext}^i_R(M, N)_{\mathscr{R}}$$

Thanks to the previous exercise, we can set by a slight abuse of notation

$$\mathrm{Ext}^i_R(M, N) := \mathrm{Ext}^i_R(M, N)_{\mathscr{R}}.$$

28.3. Induced long exact sequence. Let N be an R-module. A short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of R-modules induces a long exact sequence of R-modules

$$\begin{aligned}
&0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N)\\
&\to \mathrm{Ext}^1_R(M'', N) \to \mathrm{Ext}^1_R(M, N) \to \mathrm{Ext}^1_R(M', N)\\
&\to \mathrm{Ext}^2_R(M'', N) \to \mathrm{Ext}^2_R(M, N) \to \mathrm{Ext}^2_R(M', N)\\
&\to \cdots
\end{aligned} \tag{28.1}$$

constructed as follows. First we choose any projective resolutions $P'_\bullet \to M'$ and $P''_\bullet \to M''$.

Exercise 28.4 (Horseshoe lemma). Show that there exists a resolution $P_\bullet \to M$ of M together with an exact sequence

$$0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$$

of complexes such that

$$\begin{tikzcd}
P'_0 \arrow[r] \arrow[d, "\varepsilon'"'] & P_0 \arrow[r] \arrow[d, "\varepsilon"'] & P''_0 \arrow[d, "\varepsilon''"'] \\
M' \arrow[r] & M \arrow[r] & M''
\end{tikzcd}$$

commutes. (Hint: Let $P_0 = P'_0 \oplus P''_0$ and let $P_0 \to M$ be the sum of ε' and a lifting $P''_0 \to M$ of ε''. The snake lemma shows that $0 \to \ker \varepsilon' \to \ker \varepsilon \to \ker \varepsilon'' \to 0$ is exact and let ε is surjective. Continue by induction.)

For every i, the maps $P'_\bullet \to P_\bullet \to P''_\bullet$ thus induce morphisms

$$\mathrm{Ext}^i_R(M'', N) \to \mathrm{Ext}^i_R(M, N) \to \mathrm{Ext}^i_R(M', N).$$

The map $\delta : \mathrm{Ext}^i_R(M', N) \to \mathrm{Ext}^{i+1}_R(M'', N)$ in (29.1) is constructed as follows. Let $\alpha \in \mathrm{Ext}^i_R(M', N)$ and let $\alpha' \in \mathrm{Hom}_R(P'_i, N)$ be a representative of α. Since P''_i is projective, by Proposition 28.1 and Exercise 27.9 applied to the short exact sequence

$$0 \to P'_i \to P_i \to P''_i \to 0$$

show that α' can be lifted to $\beta \in \mathrm{Hom}_R(P_i, N)$. Since α' maps to 0 in $\mathrm{Hom}_R(P'_{i+1}, N)$, the image $\gamma \in \mathrm{Hom}_R(P_{i+1}, N)$ of β maps to 0 in $\mathrm{Hom}_R(P'_{i+1}, N)$. Therefore γ is the image of some element $\gamma' \in \mathrm{Hom}_R(P''_{i+1}, N)$, and γ' maps to 0 in $\mathrm{Hom}_R(P''_{i+2}, N)$. We define $\delta(\alpha)$ to be the class of γ' in $\mathrm{Ext}^{i+1}_R(M'', N)$.

Exercise 28.5. Show that the morphisms in (29.1) are well-defined (namely, independent of all choices of we made in the constructions) and that (29.1) is an exact sequence.

Exercise 28.6. Show that the second exact sequence in Exercise 27.9 is isomorphic to the first six terms of (29.1).

28.4. Injective modules and injective resolutions. An R-module I is called *injective* if $\mathrm{Hom}(\bullet, I)$ is (right-)exact. An *injective resolution* of an R-module N is an exact sequence of R-modules

$$0 \to N \to I^0 \xrightarrow{d} I^1 \xrightarrow{d} I^2 \to \cdots \qquad (\mathscr{I})$$

where each I_j is an injective module.

Given such an injective resolution $\mathscr{I}$ of N, for every R-module M and every $i \in \mathbf{Z}$, we define the R-module

$$\mathrm{Ext}^i_R(M, N)_{\mathscr{I}} := H^i(\mathrm{Hom}_R(M, I^\bullet));$$

we set $I^i = 0$ if $i < 0$.

28.5. Comparison of Ext-groups.

Proposition 28.7. *Let M and N be R-modules. Let $(\mathscr{R})$ be a projective resolution of M and let $(\mathscr{I})$ be an injective resolution of N. For each i, we have a canonical isomorphism*

$$\mathrm{Ext}^i_R(M, N)_{\mathscr{R}} \simeq \mathrm{Ext}^i_R(M, N)_{\mathscr{I}}.$$

Proof. Let $K^{\bullet,\bullet}$ be the double complex defined by $K^{p,q} := \mathrm{Hom}_R(P_p, I^q)$. It follows from the exercise below that we have canonical isomorphisms

$$H^i(\mathrm{Hom}_R(P_\bullet, N)) \simeq H^i(\mathrm{Tot}(K^{\bullet,\bullet})) \simeq H^i(\mathrm{Hom}_R(M, I^\bullet)).$$

□

Exercise 28.8. Let $K^{\bullet,\bullet}$ be a double complex of R-modules, namely a collection of R-modules $K^{p,q}$ indexed by $(p, q) \in \mathbf{Z}^2$ together with morphisms of R-modules

$$d' : K^{p,q} \to K^{p+1,q}, \;\; d'' : K^{p,q} \to K^{p,q+1}$$

for each $p, q \in \mathbf{Z}$ such that

$$d'^2 = d''^2 = 0, \;\; d'd'' = d''d'.$$

The total complex $\mathrm{Tot}(K^{\bullet,\bullet})$ associated to $K^{\bullet,\bullet}$ is the complex $K^\bullet$ defined by

$$K^n := \oplus_{p+q=n} K^{p,q}$$

and $d : K^n \to K^{n+1}$ is defined by

$$dx = d'x + (-1)^p d''x$$

for all $x \in K^{p,q}$.

Suppose that $K^{p,q} = 0$ whenever $p < 0$ or $q < 0$. Let

$$X^\bullet := \ker(d : K^{\bullet,0} \to K^{\bullet,1}), \;\; Y^\bullet := \ker(d : K^{0,\bullet} \to K^{1,\bullet}).$$

Show that for each i, we have canonical isomorphisms

$$H^i(X^\bullet) \simeq H^i(\mathrm{Tot}(K^{\bullet,\bullet})) \simeq H^i(Y^\bullet).$$

28.6. Ideal-theoretic criteria for injectivity.

Proposition 28.9. *Let N be an R-module. The following assertions are equivalent.*

(1) *N is injective.*

(2) *For every ideal $I \subset R$, we have $\mathrm{Ext}^1_R(R/I, N) = 0$.*

(3) *For every ideal $I \subset R$, every R-linear morphism $I \subset N$ extends to an R-linear morphism $R \to N$.*

Proof. It is clear that (1) implies (3). Applying $\mathrm{Hom}_R(\bullet, N)$ to the short exact sequence

$$0 \to I \to R \to R/I \to 0$$

and note that $\mathrm{Ext}^1_R(R, N) = 0$, we obtain an exact sequence

$$\mathrm{Hom}_R(R, N) \to \mathrm{Hom}_R(I, N) \to \mathrm{Ext}^1_R(R/I, N) \to 0,$$

showing that (2) and (3) are equivalent.

The proof of (3) ⇒ (1) uses Zorn's lemma; see [**12**, 0AVF]. □

Exercise 28.10. Let M be a $\mathbf{Z}$-module (i.e. an abelian group). Show that M is injective if and only if M is divisible: namely for any $m \in M$ and any nonzero integer n, there exists $m' \in M$ such that we have $m = n \cdot m'$.

We admit the following proposition.

Proposition 28.11. *Any R-module N has an injective resolution. Namely, there exists an exact sequence of R-modules*

$$0 \to N \to I^0 \xrightarrow{d} I^1 \xrightarrow{d} I^2 \to \cdots \qquad (\mathscr{I})$$

where each I_j is an injective module.

Proof. See [**12**, Section 01D8]. □

As a consequence, we can always compute $\mathrm{Ext}^i_R(M, N)$ using injective resolutions of N. Exactly the "dual" argument of § 28.3 show that for every R-module M, a short exact sequence

$$0 \to N' \to N \to N'' \to 0$$

of R-modules induces a long exact sequence of R-modules

$$\begin{aligned}
&0 \to \mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'') \\
&\quad \to \mathrm{Ext}^1_R(M, N') \to \mathrm{Ext}^1_R(M, N) \to \mathrm{Ext}^1_R(M, N'') \\
&\quad \to \mathrm{Ext}^2_R(M, N') \to \mathrm{Ext}^2_R(M, N) \to \mathrm{Ext}^2_R(M, N'') \\
&\quad \to \cdots
\end{aligned} \tag{28.2}$$

28.7. Aside: the Eilenberg–Mazur swindle. The following argument

$$0 = (1-1) + (1-1) + \cdots = 1 + (-1+1) + (-1+1) + \cdots = 1$$

showing that $0 = 1$ is obviously incorrect. But the similar idea sometimes works in other contexts. Here is an example.

Proposition 28.12. *For every projective R-module P, there exists a free module F such that*

$$P \oplus F \simeq F.$$

Proof. Take an R-module Q such that $P \oplus Q$ is free. Then

$$F := (P \oplus Q) \oplus (P \oplus Q) \oplus \cdots = P \oplus (Q \oplus P) \oplus (Q \oplus P) \oplus \cdots \simeq P \oplus F.$$

□

29. Flat modules

Definition 29.1. An R-module M is called *flat* if $M \otimes_R \bullet$ is left-exact.

Lemma 29.2. *Let M be an R-module. If M is projective, then M is flat.*

Proof. Since M is projective, there exists an R-module Q such that $M \oplus Q =: F$ is free. For every injective morphism of R-modules $N \to N'$, we have the commutative diagram

$$\begin{tikzcd}
M \otimes_R N \arrow[r] \arrow[d] & M \otimes_R N' \arrow[d] \\
F \otimes_R N \arrow[r] & F \otimes_R N'
\end{tikzcd}$$

Since F is free, $F \otimes_R N \to F \otimes_R N'$ is injective. As M is a direct summand of F, the map $M \otimes_R N \to F \otimes_R N$ is also injective. Hence $M \otimes_R N \to M \otimes_R N'$ is injective. □

29.1. Tor functor. A *flat resolution* of an R-module M: is an exact sequence of R-modules

$$\cdots \xrightarrow{d} P_1 \xrightarrow{d} P_0 \to M \to 0 \qquad (\mathscr{R})$$

such that each P_i is a flat module. Given such a resolution $\mathscr{R}$ and another R-module N, define

$$\mathrm{Tor}_i^R(M,N)_{\mathscr{R}} := H_i(P_\bullet \otimes N);$$

here, for any complex of R-modules

$$\cdots \to C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \to \cdots,$$

the ith homology of $C_\bullet$ is defined as

$$H_i(C_\bullet) := \frac{\ker d_i}{\mathrm{Im} d_{i+1}}.$$

By the same argument and construction as in § 28.2, $\mathrm{Tor}_i^R(M,N)_{\mathscr{R}}$ is also functorial in M and in N, and we have a canonical isomorphism $\mathrm{Tor}_i^R(M,N)_{\mathscr{R}} \simeq \mathrm{Tor}_i^R(M,N)_{\mathscr{R}'}$ if $(\mathscr{R}')$ is another flat resolution of M. By a slight abuse of notation we set

$$\mathrm{Tor}_i^R(M,N) := \mathrm{Tor}_i^R(M,N)_{\mathscr{R}}.$$

Exactly as in § 28.5, we can also compute $\mathrm{Tor}_i^R(M,N)$ using flat resolutions of N.

Finally, the same argument as in § 28.3 shows that every short exact sequence

$$0 \to N' \to N \to N'' \to 0$$

of R-modules induces a long exact sequence of R-modules

$$\begin{aligned}
&\cdots \to \mathrm{Tor}_2^R(M,N') \to \mathrm{Tor}_2^R(M,N) \to \mathrm{Tor}_2^R(M,N'') \\
&\to \mathrm{Tor}_1^R(M,N') \to \mathrm{Tor}_1^R(M,N) \to \mathrm{Tor}_1^R(M,N'') \qquad (29.1)\\
&\to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0.
\end{aligned}$$

Exercise 29.3. Show that we have isomorphisms

$$\mathrm{Tor}_i^R(M,N) \simeq \mathrm{Tor}_i^R(N,M)$$

which are natural in M and in N.

Example 29.4. Let $r \in R$ which is not a zero-divisor. For every R-module M, using the projective resolution

$$0 \to R \xrightarrow{r} R \to R/(r) \to 0$$

of $R/(r)$, we obtain

$$\mathrm{Tor}_i^R(M, R/(r)) \simeq \begin{cases} M/rM & \text{if } i = 0 \\ \{\, m \in M \mid rm = 0 \,\} & \text{if } i = 1 \\ 0 & \text{if } i \geq 2. \end{cases} \qquad (29.2)$$

29.2. Basic facts of flat modules.

Exercise 29.5 (Base change preserves flatness)**.** Let M be an R-module and let $\phi : R \to A$ be a ring homomorphism. Show that the A-module $M \otimes_R A$ is flat.

Let $\phi : R \to A$ be a ring homomorphism, which defines an R-module structure on A. We say that ϕ *is flat*, or A *is flat over* R, if this R-module A is flat.

Exercise 29.6 (Transitivity of flatness)**.** Let $R \to A$ be a ring homomorphism and let M be an A-module. Suppose that M is flat over A and that A is flat over R. Show that M is flat over R.

Exercise 29.7. Let $S \subset R$ be a multiplicative subset. Show that the localization $R \to S^{-1}R$ is flat.

Exercise 29.8. Let $f : R \to A$ be a flat ring homomorphism. Let $\mathfrak{p} \in \operatorname{Spec}(A)$ and let $\mathfrak{q} = f^{-1}(\mathfrak{p}) \in \operatorname{Spec}(R)$. Show that the induced morphism $R_\mathfrak{q} \to A_\mathfrak{p}$ is also flat.

29.3. Flatness is a local property.

Proposition 29.9. *Let M be an R-module. The following assertions are equivalent.*

(1) M is flat over R.
(2) $M_\mathfrak{p}$ is flat over $R_\mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset R$.
(3) $M_\mathfrak{m}$ is flat over $R_\mathfrak{m}$ for every maximal ideal $\mathfrak{m} \subset R$.

Proof. By Exercise 29.7, it remains to prove (3) ⇒ (1). Let $f : N \to N'$ be an injective morphism of R-modules. Then for every maximal ideal $\mathfrak{m} \subset R$,

$$(f \otimes \mathrm{Id}_M)_\mathfrak{m} : (N \otimes_R M)_\mathfrak{m} \simeq N_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m} \xrightarrow{f_\mathfrak{m} \otimes \mathrm{Id}_{M_\mathfrak{m}}} N'_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m} \simeq (N' \otimes_R M)_\mathfrak{m}$$

is injective; here the isomorphisms are the ones defined in Exercise 10.9. Hence $f \otimes \mathrm{Id}_M$ is injective. □

Exercise 29.10. Show that locally free R-modules are flat.

29.4. Ideal-theoretic criteria for flatness.

Proposition 29.11. *Let M be an R-module. The following assertions are equivalent.*

(1) M is flat over R.
(2) For every finitely generated ideal $I \subset R$, the natural map $I \otimes_R M \to M$ is injective; therefore we have $I \otimes_R M \simeq IM$.
(3) For every finitely generated ideal $I \subset R$, we have $\operatorname{Tor}_1^R(M, R/I) = 0$.

Proof. It is clear that (1) ⇒ (3) ⇒ (2).

Assume (2). First we note that $I \otimes_R M \to M$ is injective for every ideal. Indeed, suppose that $\sum_{j=1}^k r_j \otimes m_j \mapsto 0$. Let $I' := (r_1, \dots, r_k)$. Then the composition

$$I' \otimes_R M \to I \otimes_R M \to M$$

is the natural map, which is injective. Hence $\sum_{j=1}^k r_j \otimes m_j = 0$ in $I \otimes_R M$. Therefore applying $\bullet \otimes_R M$ to

$$0 \to I \to R \to R/I \to 0$$

together with $\operatorname{Tor}_1^R(R, M) = 0$ shows that

$$\operatorname{Tor}_1^R(M, R/I) = 0.$$

We need to show that for every injective morphism of R-module $f : N \hookrightarrow N'$, the map $g := f \otimes \mathrm{Id}_M$ is also injective. Note that it suffices to prove the case where N'/N is finitely generated. Indeed, if $g(\sum_{j=1}^k n_j \otimes m_j) = 0$, then $\sum_{j=1}^k (f(n_j), m_j)$ is some element in the module of relations defining the tensor product $N' \otimes_R M$, which involves only finitely many $n'_1, \dots, n'_\ell \in N'$. Thus $\sum_{j=1}^k n_j \otimes m_j = 0$ in $N \otimes_R M$ follows from the injectivity of

$$N \otimes_R M \to \left(N + \sum_{i=1}^{\ell} R \cdot n'_i \right) \otimes_R M.$$

By induction on the number of generators of $Q := N'/N$, it suffices to show that $g : N \otimes_R M \to N' \otimes_R M$ is injective in the case where Q is generated by one element. In this case, we have $Q \simeq R/\mathrm{Ann}(Q)$. Applying $\bullet \otimes_R M$ to the short exact sequence

$$0 \to N \to N' \to R/\mathrm{Ann}(Q) \to 0$$

together with $\mathrm{Tor}_1^R(M, R/\mathrm{Ann}(Q)) = 0$ shows that $g : N \otimes_R M \to N' \otimes_R M$ is injective. □

29.5. Flatness and torsion-freeness. An R-module M is called *torsion free* if for every $r \in R$ and $m \in M$, $rm = 0$ implies that either $m = 0$ or r is a zero-divisor in R. The name "Tor" is partly due to the following result.

Proposition 29.12. *Flat modules are torsion free.*

Proof. Let M be a flat R-module. Let $r \in R$ which is not a zero-divisor. Then $R \xrightarrow{\times r} R$ is injective, so by flatness of M, its tensorization $M \xrightarrow{\times r} M$ with M is also injective. □

Exercise 29.13. Suppose that R is a PID. Show that an R-module M is flat if and only if M is torsion free.

29.6. Finite projective modules.

Proposition 29.14. *Let M be a finitely presented R-module. The following assertions are equivalent.*

(1) *M is locally free.*
(2) *M is projective.*
(3) *M is flat.*

Proof. By Exercise 29.10, we have (2) ⇒ (3).

Assume (3). Let $\mathfrak{p} \subset R$ be a prime ideal. Let $d := \dim_{\kappa(\mathfrak{p})} M|_{\mathfrak{p}}$ By the Nakayama lemma, there exists a surjective morphism $f : R_{\mathfrak{p}}^d \twoheadrightarrow M_{\mathfrak{p}}$ such that $f|_{\mathfrak{p}} : R^d|_{\mathfrak{p}} \xrightarrow{\sim} M|_{\mathfrak{p}}$. Since $M_{\mathfrak{p}}$ is flat over $R_{\mathfrak{p}}$, we have $\mathrm{Tor}_1^{R_{\mathfrak{p}}}(\bullet, M_{\mathfrak{p}}) = 0$, so tensoring $\kappa(\mathfrak{p})$ to the exact sequence

$$0 \to \ker(f) \to R_{\mathfrak{p}}^d \to M_{\mathfrak{p}} \to 0$$

shows that $\ker(f)|_{\mathfrak{p}} = 0$. Since $M_{\mathfrak{p}}$ is finitely presented, $\ker(f)$ is finitely generated. Thus $\ker(f)_{\mathfrak{p}} = 0$ by the Nakayama lemma, which shows that $M_{\mathfrak{p}}$ is free. Again since M is finitely presented, M is thus locally free.

Finally we show (1) ⇒ (2). Let $\phi : N \to N'$ be an surjective morphism of R-modules. We show that the induced morphism $\phi_M : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N')$ is surjective. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ be a prime ideal By Proposition 10.15, the localization $(\phi_M)_{\mathfrak{p}}$ is isomorphic to the morphism

$$\mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}}) \to \mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N'_{\mathfrak{p}})$$

induced by $\phi_{\mathfrak{p}} : N_{\mathfrak{p}} \to N'_{\mathfrak{p}}$. Since $M_{\mathfrak{p}}$ is free, $(\phi_M)_{\mathfrak{p}}$ is thus surjective. Hence ϕ_M is surjective. □

29.7. Going-down for flat morphisms. As a geometric consequence of flatness, we have the following statement.

Proposition 29.15 (Going-down property for flat morphisms). *Let $R \to A$ be a flat morphism of rings. Let $f : \mathrm{Spec}(A) \to \mathrm{Spec}(R)$ be the induced morphism of affine schemes. Let $\mathfrak{p} \subset \mathfrak{p}' \subset R$ be a pair of nested prime ideals of R. If there exists $\mathfrak{q}' \in f^{-1}(\mathfrak{p}')$, then there exists $\mathfrak{q} \in f^{-1}(\mathfrak{p})$ such that $\mathfrak{q} \subset \mathfrak{q}'$.*

We will prove Proposition 29.15 after we introduce and discuss about the notion of faithfully flat modules.

29.8. Faithfully flat modules. An R-module M is called *faithfully flat* if for any morphism of R-modules $f : N \to N'$,

$$N \xrightarrow{f} N' \text{ is injective} \quad \Leftrightarrow \quad N \otimes M \xrightarrow{f \otimes \mathrm{Id}_M} N' \otimes M \text{ is injective.}$$

Exercise 29.16. Let M be a flat R-module. Show that the following statements are equivalent.

(1) M is faithfully flat.

(2) $M \otimes_R N = 0$ implies $N = 0$ for any R-module N.

Exercise 29.17. Let M be an R-module. Show that the following statements are equivalent.

(1) M is faithfully flat.

(2) For any sequence of morphisms of R-modules $N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3$,

$$N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3 \text{ is exact} \quad \Leftrightarrow \quad N_1 \otimes M \xrightarrow{f\otimes \mathrm{Id}_M} N_2 \otimes M \xrightarrow{g\otimes \mathrm{Id}_M} N_3 \otimes M \text{ is exact.}$$

The following statement shows that a flat module M is faithfully flat if and only if

Proposition 29.18. *Let M be a flat R-module. The following assertions are equivalent.*

(1) M is faithfully flat.

(2) $M|_{\mathfrak{p}} \neq 0$ for any prime ideal $\mathfrak{p} \subset R$.

(3) $M|_{\mathfrak{m}} \neq 0$ for any maximal ideal $\mathfrak{m} \subset R$.

Proof. By Exercise 29.16 we have (1) $\implies$ (2). (2) $\implies$ (3) is clear. Now assume (3). Let N be any nonzero R-module. By Exercise 29.16, it suffices to show that $M \otimes_R N \neq 0$. Let $x \in N$ which is nonzero. Since M is flat, the morphism $(R \cdot x) \otimes_R M \to M \otimes_R N$ is injective. Since $x \neq 0$, $\mathrm{Ann}(x)$ is a proper ideal of R, so contained in a maximal ideal $\mathfrak{m}$. As $R \cdot x \simeq R/\mathrm{Ann}(x) \twoheadrightarrow R/\mathfrak{m}$, we have a surjective morphism $(R \cdot x) \otimes_R M \twoheadrightarrow M|_{\mathfrak{m}}$. Since $M|_{\mathfrak{m}} \neq 0$ by assumption, we conclude that $M \otimes_R N \neq 0$. □

29.9. Faithfully flat morphisms. Let $f : R \to A$ be a ring homomorphism, which defines an R-module structure on A. We say that *f is faithfully flat*, or *A is faithfully flat over R*, if this R-module A is faithfully flat.

Exercise 29.19. Let $f : R \to A$ be a ring homomorphism. Show that the following statements are equivalent.

(1) f is faithfully flat.

(2) f is flat and $\mathrm{Spec}(A) \to \mathrm{Spec}(R)$ is surjective.

(3) f is flat and every closed point of $\mathrm{Spec}(R)$ is in the image of $\mathrm{Spec}(A) \to \mathrm{Spec}(R)$.

(Hint: Lemma 10.30.)

Proof of Proposition 29.15. By Exercise 29.8, the morphism $f' : R_{\mathfrak{p}'} \to A_{\mathfrak{q}'}$ induced by f is flat. Since f'^{-1} takes the maximal ideal $\mathfrak{q}'A_{\mathfrak{q}'}$ to the maximal ideal $\mathfrak{p}'R_{\mathfrak{p}'}$, it follows from Exercise 29.19 that $\mathrm{Spec}(A_{\mathfrak{q}'}) \to \mathrm{Spec}(R_{\mathfrak{q}'})$ induced by f' is surjective. In particular, $\mathfrak{p}R_{\mathfrak{p}'}$ has a pre-image $\overline{\mathfrak{q}} \in \mathrm{Spec}(A_{\mathfrak{q}'})$. Hence the pre-image $\mathfrak{q} \subset A$ of $\overline{\mathfrak{q}}$ satisfies $\mathfrak{q} \subset \mathfrak{q}'$ and $f^{-1}(\mathfrak{q}) = \mathfrak{p}$. □

LECTURE 14

Completion

The final lecture of Modern Algebra II is devoted to completion. Due to time limit, some proofs are omitted. Reading the relevant details in the literature, such as [**5**, Chapter 7] or the Stack Project, is strongly recommended.

30. Examples and definition

Let p be a prime number.

30.1. p-adic integers. We've seen that $\mathbf{C}[X]$ and $\mathbf{Z}$ share some similarities. At every point $p \in \mathbf{C}$, every polynomial function $f \in \mathbf{C}[X]$ has a unique expansion

$$f(X) = a_0 + a_1(X - p) + \cdots + a_n(X - p)^n$$

with $a_i \in \mathbf{C}$. Likewise, for any prime number p, any positive number N can be written in a unique way in base p:

$$N = a_0 + a_1 \cdot p + \cdots + a_n \cdot p^n$$

with $a_n \in \{0, \ldots, p - 1\}$. According to this dictionary, the analogue of formal power series are p-adic integers:

$$\mathbf{Z}_p := \left\{ \text{formal infinite series } \sum_{i=0}^{\infty} a_i \cdot p^i \;\middle|\; a_i = 0, \ldots, p - 1 \right\}$$

Formal power series appear when we develop at a point p a rational function f which doesn't have a pole at p. Likewise, p-adic integers already when we try to develop fractions f such that the denominator of its reduced form is not divisible by p (i.e. $f \in \mathbf{Z}_{(p)}$). Infinite sum appears already when we develop negative integers, e.g.

$$-1 = \sum_{i=0}^{\infty} (p - 1) \cdot p^i.$$

The development of $f \in \mathbf{Z}_{(p)}$, is based on the isomorphism $\mathbf{Z}/p^n\mathbf{Z} \simeq \mathbf{Z}_{(p)}/p^n\mathbf{Z}_{(p)}$: the corresponding p-adic expansion

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

is a p-adic integer satisfying

$$f = \sum_{i=0}^{n} a_i \cdot p^i \mod p^{n+1}$$

for all n.

30.2. p-adic numbers. The analogue of formal Laurent series are p-adic numbers:

$$\mathbf{Q}_p := \left\{ \text{formal infinite series } \sum_{i \geq i_0} a_i \cdot p^i \;\middle|\; i_0 \in \mathbf{Z}; a_i = 0, \ldots, p - 1 \right\}.$$

Just as we can develop a rational function into a formal Laurent series, we can develop a rational number f into a p-adic number as follows. First we write

$$f = g \cdot p^m$$

with $g \in \mathbf{Z}_{(p)}$. If $\sum_{i=0}^{\infty} a_i \cdot p^i$ is the p-adic expansion of g, then the p-adic expansion of f is

$$\sum_{i=m}^{\infty} a_{i-m} \cdot p^i$$

30.3. The implicit function theorem, Newton's method, and Hensel's lemma.

Theorem 30.1 (Formal implicit function theorem). *Let $f(x,y) \in \mathbf{C}[[x,y]]$. If $f(0,0) = 0$ and $\partial_y f(0,0) \neq 0$, then there exists $y(x) \in \mathbf{C}[[x]]$ such that*

$$f(x, y(x)) = 0.$$

For instance, if $f(x,y) = (y-1)^2 - x - 1$, then

$$y = 1 + \text{power series expansion of } \sqrt{x+1} \text{ at } 0$$

works. Theorem 30.1 can be proven using Newton's method.

Hensel's lemma is the analogue of the implicit function theorem for $\mathbf{Z}_p$.

Theorem 30.2 (Hensel's lemma). *Let $f \in \mathbf{Z}_p[x]$ and let $\overline{f} \in \mathbf{F}_p[x]$ be its reduction modulo p. Suppose that $b \in \mathbf{F}_p$ is a root of $\overline{f}$ and*

$$\overline{f}'(b) \neq 0.$$

Then there exists a unique lift $a \in \mathbf{Z}_p$ of b to a root of f, namely

$$f(a) = 0 \quad \text{and} \quad a = b \mod p.$$

Exercise 30.3. Is 7 a square in $\mathbf{Z}_3$?

30.4. $\mathbf{Q}_p$ as a topological completion. Recall $\mathbf{R}$ is the completion of $\mathbf{Q}$ with respect to the usual absolute value.

Theorem 30.4. *$\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ with respect to the p-adic absolute value.*

31. Completion

31.1. Definition and basic properties. Let R be a ring and let I be an ideal. The I-adic completion of R is defined as

$$\hat{R} := \varprojlim R/I^n = \left\{ (a_n) \in \prod_{n=0}^{\infty} R/I^n \;\middle|\; a_n = a_{n+1} \mod I^n \right\}.$$

It is an R-subalgebra of $\prod_{n=0}^{\infty} R/I^n$.

Exercise 31.1. Show that

(1) $R[[X]] \simeq \widehat{R[X]}_{(X)}$

(2) $\mathbf{Z}_p \simeq \widehat{\mathbf{Z}_{(p)}}$,

where the completions are defined with respect to the maximal ideals. Show that $\mathbf{Z}_p$ is a DVR.

Exercise 31.2. Let $\mathfrak{m} \subset R$ be a maximal ideal. Show that the $\mathfrak{m}$-adic completion of R is a local ring, with maximal ideal $\mathfrak{m} \cdot \hat{R}$.

Similarly, if M is an R-module, its I-adic completion is defined as

$$\hat{M} := \varprojlim M/I^n M = \left\{ (m_n) \in \prod_{n=0}^{\infty} M/I^n M \;\middle|\; m_n = m_{n+1} \mod I^n M \right\}.$$

Exercise 31.3. Show that the $(\prod_{n=0}^{\infty} R/I^n)$-structure on $\prod_{n=0}^{\infty} M/I^n M$ induces an $\hat{R}$-module structure on $\hat{M}$.

For any morphism of R-modules $f : M \to N$, the completion naturally induces a morphism of $\hat{R}$-modules $\hat{f} : \hat{M} \to \hat{N}$. Therefore the I-adic completion defines a functor from the category of R-modules to itself.

Lemma 31.4. *Let $f : M \to N$ be a morphism of R-modules. If $f : M/IM \to N/IN$ is surjective (e.g. if f is surjective), then $\hat{f} : \hat{M} \to \hat{N}$ is also surjective.*

Lemma 31.5. *Let*

$$0 \to K \to M \to N \to 0$$

be an exact sequence. If N is flat, then the completion

$$0 \to \hat{K} \to \hat{M} \to \hat{N} \to 0$$

is also exact.

Remark 31.6. In general, Completion is not an exact functor. It is not even right-exact.

Exercise 31.7. Show that the natural map $M \otimes_R \hat{R} \to \hat{M}$ is surjective.

If the canonical morphism $M \to \hat{M}$ is an isomorphism, then we say that M is *I-adically complete*.

Lemma 31.8. *$\hat{M}$ is I-adically complete.*

31.2. Complete local rings are Henselian. Let $(R, \mathfrak{m})$ be a local ring with residue field κ. We call $(R, \mathfrak{m})$ a *Henselian ring* if the following property holds: for any monic polynomial $f \in R[X]$ and any root $a_0 \in \kappa$ of its reduction $\overline{f} \in \kappa[X]$ modulo $\mathfrak{m}$ such that

$$\overline{f}'(a_0) \neq 0,$$

there exists $a \in R$ such that

$$a = a_0 \mod \mathfrak{m} \qquad \text{and} \qquad f(a) = 0.$$

Theorem 31.9. *A complete local ring is henselian.*

Proof. Let $f \in R[X]$ be a monic and let $a_0 \in \kappa$ be a root of $\overline{f} \in \kappa[X]$ such that $\overline{f}'(a_0) \neq 0$. We prove by induction that a lifts to a root $a_n \in R/\mathfrak{m}^{n+1}$ of

$$f_n := f \mod \mathfrak{m}^{n+1} \in (R/\mathfrak{m}^{n+1})[X]$$

using Newton's method.

Suppose that $a_n \in R/\mathfrak{m}^{n+1}$ is constructed. Let $b \in R/\mathfrak{m}^{n+2}$ be any lift of a_n. Then $f_{n+1}(b) \in \mathfrak{m}^{n+1}/\mathfrak{m}^{n+2}$. As $\mathfrak{m}$ is the maximal ideal of the local ring R, only units of $R/\mathfrak{m}^{n+2}$ can map to units of $R/\mathfrak{m}$. Thus $f'_{n+1}(b)$ is invertible in $R/\mathfrak{m}^{n+2}$. Now set

$$a_{n+1} := b - \frac{f_{n+1}(b)}{f'_{n+1}(b)}.$$

□

32. Completion of Noetherian rings

In this section, we assume that the ring R is *Noetherian*. Let I be an ideal.

32.1. Basic properties.

Proposition 32.1. *The I-adic completion $\hat{R}$ of R is also Noetherian.*

In particular, $R[[X]]$ is also Noetherian.

Proposition 32.2. *Completion of finite R-modules is an exact functor.*

Proposition 32.3. *The ring morphism $R \to \hat{R}$ is flat. If $(R, \mathfrak{m})$ is a local ring and $I \subset \mathfrak{m}$, then $R \to \hat{R}$ is faithfully flat.*

32.2. Tangent cone of the completion. Let $(R, \mathfrak{m})$ be a Noetherian local ring, and let $\hat{R}$ be the $\mathfrak{m}$-adic completion.

Proposition 32.4. *We have a graded ring isomorphism*

$$\mathrm{gr}_{\hat{\mathfrak{m}}}\hat{R} \simeq \mathrm{gr}_{\mathfrak{m}}R.$$

32.3. Formal neighborhood. Let $\mathbf{k}$ be an algebraically closed field. The polynomial

$$y^2 - x^2(x+1)$$

is irreducible in $\mathbf{k}[x,y]_{(x,y)}$, but not in $\mathbf{k}[[x,y]]$ (because $x+1$ has a square root). The tangent cone at $(0,0)$ of the curve defined by $y^2 - x^2(x+1)$ also has two branches.

Bibliography

[1] The baer-specker group. https://wildtopology.com/2014/07/02/the-baer-specker-group/.

[2] Does localisation commute with hom for finitely-generated modules? https://math.stackexchange.com/questions/75812/does-localisation-commute-with-hom-for-finitely-generated-modules.

[3] Zagier's one-sentence proof of a theorem of fermat. https://mathoverflow.net/questions/31113/zagiers-one-sentence-proof-of-a-theorem-of-fermat.

[4] Michael F. Atiyah and I. G. Macdonald. Introduction to commutative algebra. Reading, Mass.-Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company (1969)., 1969.

[5] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[6] Franz Lemmermeyer. Jacobi and Kummer's ideal numbers. *Abh. Math. Semin. Univ. Hamb.*, 79(2):165–187, 2009.

[7] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[8] J. S. Milne. Algebraic number theory. https://www.jmilne.org/math/CourseNotes/ant.html.

[9] David Mumford. *The red book of varieties and schemes. Includes the Michigan lectures (1974) on "Curves and their Jacobians".*, volume 1358 of *Lect. Notes Math.* Berlin: Springer, 2nd, expanded ed. with contributions by Enrico Arbarello edition, 1999.

[10] Masayoshi Nagata. *Local rings*, volume 13 of *Intersci. Tracts Pure Appl. Math.* Interscience Publishers, New York, NY, 1962.

[11] Jet Nestruev. *Smooth manifolds and observables*, volume 220 of *Grad. Texts Math.* Cham: Springer, 2nd revised and expanded edition edition, 2020.

[12] The Stacks Project Authors. *Stacks Project*. http://stacks.math.columbia.edu, 2018.

[13] Ravi Vakil. The rising sea: foundations of algebraic geometry. https://math.stanford.edu/~vakil/216blog/.