MAS439/MAS6320
COMMUTATIVE ALGEBRA AND ALGEBRAIC GEOMETRY II

EVGENY SHINDER

1. Modules

Fields often make their properties known to us via vector spaces: we care so much about $\mathbb{R}$ at least partly because our universe looks like a three-dimensional vector space over it.

Modules offer a generalisation for commutative rings of what vector spaces do for fields. The definition is very similar to the definition of a vector space.

We define modules, submodules, homomorphisms of modules and quotient modules, and prove three Isomorphism Theorems.

1.1. Modules and submodules.

Definition 1.1. *Let R be a commutative ring. An R-*module *consists of an abelian group M together with a map*

$$R \times M \longrightarrow M,$$

written as $(r, m) \mapsto rm$, satisfying the following axioms:

- *for all $m \in M$, we have $1m = m$;*
- *for all $r, s \in R$ and $m \in M$, we have $(rs)m = r(sm)$;*
- *for all $r, s \in R$ and $m \in M$, we have $(r + s)m = rm + sm$;*
- *for all $r \in R$ and $m, n \in M$, we have $r(m + n) = rm + rn$.*

So we can add and subtract elements of M, and multiply them by elements of R. The reader might wonder why there are no axioms explaining that zeroes and subtraction behave nicely. It turns out they're not necessary:

Proposition 1.2. *Let R be a commutative ring and M an R-module. Then for all $m \in M$ we have $0m = 0$ and $(-1)m = -m$.*

Proof. Firstly, we have

$$1m + 0m = (1 + 0)m = 1m,$$

and so cancelling the $1m$ from both sides, we have $0m = 0$.

Secondly, we have

$$0 = 0m = (1 + (-1))m = 1m + (-1)m = m + (-1)m.$$

By taking the m to the other side, we get that $(-1)m = -m$. □

In case our ring is a field, we get nothing different:

Example 1.3. *If K is a field, then a K-module is exactly the same thing as a vector space over K.*

There is one other ring whose modules are a deeply familiar concept:

Date: February 2, 2018.

Proposition 1.4. *A $\mathbb{Z}$-module is the same thing as an abelian group.*

Proof. A $\mathbb{Z}$-module consists of an abelian group A, plus a multiplication map $\mathbb{Z} \times A \to A$ satisfying the module axioms. But these are uniquely determined by the abelian group structure.

For example,

$$5a = (1+1+1+1+1)a = 1a + 1a + 1a + 1a + 1a = a + a + a + a + a,$$

and

$$-3a = ((-1) + (-1) + (-1))a = (-1)a + (-1)a + (-1)a = -a - a - a.$$

Hence the scalar multiplication adds nothing new. □

However, we can often describe a module in terms of linear algebra concepts that we know about already:

Example 1.5. *A $\mathbb{C}[T]$-module consists of a complex vector space V equipped with a map $T : V \to V$.*

Indeed, adding and scalar multiplying by constant polynomials give us a $\mathbb{C}$-module, and multiplying by T gives the linear map.

Remark 1.6. *One nice thing about vector spaces is that they all have a basis: any K-vector space looks like K^n for some (possibly infinite) n. That's absolutely not true for modules over a general ring, as the example above shows: not every abelian group is of the form $\mathbb{Z}^n$.*

One occasionally needs to talk about subsets of modules which are modules. The definition is what you might expect:

Definition 1.7. *Let R be a commutative ring. A* submodule *of an R-module M consists of a subset of M which contains the zero element and is closed under addition and under multiplication by elements of R.*

Perhaps the most striking use of this is to rephrase something you know about already in this new language:

Proposition 1.8. *Let R be a commutative ring. Then addition and multiplication makes R into an R-module, and a submodule of R is exactly the same thing as an ideal of R.*

Proof. All the axioms of a module (in Definition 1.1) are well-known formulae for multiplication in a commutative ring, so R has the structure of an R-module.

A submodule of R is a subset closed under scalar multiplication by elements of R, and under addition and subtraction. That's exactly the same thing as an ideal of R. □

Here's a boring example of a module:

Example 1.9. *Let R be a commutative ring. Then the* trivial *module is given by the singleton set $\{0\}$, with the only possible addition and scalar multiplication.*

You can think of that as corresponding to the zero ideal, if you like.

Here's another general way of constructing modules.

Example 1.10. *Let R and S be a commutative rings, and let $f : R \to S$ be a ring homomorphism. Also, let M be an S-module. Then the formula $rm = f(r)m$ makes M into an R-module.*

1.2. **Homomorphisms of modules.**

Example 1.11. *By the above, as S is a module over itself, a ring homomorphism $f : R \to S$ makes S into an R-module, with the multiplication given by $rs = f(r)s$.*

Conceptually, I sometimes like to think of a ring homomorphism $f : R \to S$ as being a way of making S into an R-module, together with a way of multiplying all the elements of S with each other.

We can take Cartesian products of modules, though we usually choose to give it another name:

Definition 1.12. *Let R be a commutative ring, and let M and N be R-modules. We define a new R-module $M \oplus N$, the* direct sum *of M and N to consist of the abelian group $M \times N$ together with the following definition of multiplication:*

$$r(m, n) = (rm, rn) \quad \textit{(for } r \in R,\ m \in M \textit{ and } n \in N\textit{)}.$$

If we keep doing this on M, forming $M \oplus \cdots \oplus M$, we get something that deserves to be called M^n for some n (sometimes written $M^{\oplus n}$ to remind you what the operation you're repeating is called). A element of M^n can be thought of as an n-tuple $(m_1, \ldots, m_n)$ of elements of M.

This construction happens particularly frequently when M is R itself (regarded as a module over itself): we say that the resulting module R^n is a *(finitely generated) free* module over R.

There is an infinite version of these ideas, where we direct sum together infinitely many modules, but we won't need it.

The last thing I ought to talk about is the notion of a homomorphism of R-modules. I hope you can guess what this is:

Definition 1.13. *Let R be a commutative ring and let M and N be R-modules. A* homomorphism *$f : M \to N$ consists of a homomorphism of abelian groups from M to N with the property that $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$.*

Example 1.14. *If M is an R-module and M' a submodule, then the inclusion map $M' \to M$ is a module homomorphism.*

Example 1.15. *If R is a field, then a R-module homomorphism is exactly the same thing as a vector space homomorphism.*

Example 1.16. *If $R = \mathbb{Z}$, then a $\mathbb{Z}$-module homomorphism is exactly the same thing as a homomorphism of abelian groups.*

1.3. **Finitely generated modules.**

Definition 1.17. *Let R be a commutative ring and let M be an R-module. We say that elements $m_1, \ldots, m_k \in M$* generate *M if, for all $m \in M$ there are $r_1, \ldots, r_k \in R$ such that*

$$r_1 m_1 + \cdots + r_k m_k = m.$$

If there are elements $m_1, \ldots, m_k$ which generate M, we say that it is finitely generated*.*

Example 1.18. *The finitely generated free module R^n is indeed finitely generated (as we'd expect).*

In fact we can take the generators to be

$$\begin{aligned} r_1 &= (1, 0, 0, \ldots, 0, 0) \\ r_2 &= (0, 1, 0, \ldots, 0, 0) \\ &\vdots \\ r_n &= (0, 0, 0, \ldots, 0, 1) \end{aligned}$$

and then the element $r = (r_1, \dots, r_n)$ *can be written as*

$$r = r_1 m_1 + \cdots + r_n m_n.$$

Not every module is finitely generated. Here's an example:

Example 1.19. *Recall that a* $\mathbb{Z}$*-module is the same thing as an abelian group. The* $\mathbb{Z}$*-module given by* $\mathbb{R}$ *under addition is not finitely generated. To see that let* $m_1, \dots, m_k \in \mathbb{R}$ *be a finite list of real numbers. Then the set*

$$\{r_1 m_1 + \cdots + r_k m_k \mid r_1, \dots, r_k \in \mathbb{Z}\}$$

is countable. So it cannot be all of $\mathbb{R}$*, as* $\mathbb{R}$ *is uncountable. This shows that* $\mathbb{R}$ *does not admit a finite number of generators.*

Exercise 1.20. *Is* $\mathbb{Q}$ *a finitely generated* $\mathbb{Z}$*-module?*

Proposition 1.21. *An* R*-module* M *is finitely generated if and only if there exists a surjective homomorphism of* R*-modules*

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

for some finite n*.*

Proof. If M is finitely generated, say generated by $m_1, \dots, m_n \in M$, then we may define an R-module homomorphism

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

via

$$\phi(a_1, \dots, a_n) = a_1 m_1 + \cdots + a_n m_n.$$

It see to see that ϕ is a homomorphism:

$$\phi(ra_1, \dots, ra_n) = ra_1 m_1 + \cdots + ra_n m_n = r\phi(a_1, \dots, a_n)$$
$$\phi(a_1 + b_1, \dots, a_n + b_n) = (a_1 + b_1)m_1 + \cdots + (a_n + b_n)m_n = \phi(a_1, \dots, a_n) + \phi(b_1, \dots, b_n).$$

Since $m_1, \dots, m_n$ are generators, ϕ is surjective.

Conversely, if a surjective homomorphism $\phi : R^n \to M$ exists, it is immediate that images $m_1 = \phi(e_1), \dots, m_n = \phi(e_n)$ generate M, so that M is finitely generated. □

1.4. **Quotient modules.** Imitating the definitions of quotient abelian groups and quotient vector spaces, we can define quotient modules.

In order to do so, let's first recall definitions and notation for quotients of abelian groups. Given an abelian group A and a subgroup B, we put an equivalence relation on A to define the quotient, setting $a \approx a'$ if there is $b \in B$ such that $a' \approx a + b$.

We write A/B for the quotient abelian group, which is the set of equivalence classes under this relation. We write $a + B$ for the equivalence class containing a if we're being formal, or simply call it a if we're being informal.

That gives us what we need to define quotient modules.

Definition 1.22. *Let* R *be a commutative ring, let* M *be an* R*-module and let* N *be a submodule of* M*. The* quotient module M/N *has objects consisting of the quotient abelian group* M/N*, with multiplication defined by the multiplication structure on* M*.*

Note that the multiplication is well-defined: if we have $m \approx m'$ in M, then $m' = m+n$ for some $n \in N$. Then

$$rm' = r(m+n) = rm + rn,$$

and $rn \in N$ since N is a submodule of M, so $rm' \approx rm$.

The standard examples are that if R is a field, then quotient modules are simply quotient vector spaces, while if R is $\mathbb{Z}$, then quotient modules are simply quotient abelian groups.

The following are the standard results explaining the good behaviour of quotient modules:

Theorem 1.23 (First isomorphism theorem)**.** *Let R be a commutative ring. Let M and N be R-modules, and let $\phi : M \to N$ be a homomorphism between them. Then:*

(1) *the kernel* $\mathrm{Ker}(\phi)$ *is a submodule of* M*,*
(2) *the image* $\mathrm{Im}(\phi)$ *is a submodule of* N*, and*
(3) *there is an isomorphism* $\mathrm{Im}(\phi) \simeq M/\mathrm{Ker}(\phi)$*.*

Proof. The kernel is a subgroup of M because ϕ is an abelian group homomorphism. It's closed under multiplication by R since if $f(m) = 0$, then $\phi(rm) = r\phi(m) = r0 = 0$ for all r, and is hence a submodule.

Similarly, the image is a subgroup of M because ϕ is an abelian group homomorphism. It's also closed under multiplication by R since $r\phi(m) = \phi(rm)$.

The isomorphism between $\mathrm{Im}(\phi)$ and $M/\mathrm{Ker}(\phi)$ is defined as follows. Given an element $n \in \mathrm{Im}(\phi)$, associate to it an element $m \in M$ such that $\phi(m) = n$ (which is possible as n is in the image). There may be several possible choices of such m. But given any two such choices m and m', we have $\phi(m-m') = \phi(m) - \phi(m') = n - n = 0$, and hence $m - m' \in \mathrm{Ker}(\phi)$, and hence equal in $M/ker(\phi)$.

Conversely to any element $m + \mathrm{Ker}(\phi)$ in $M/\mathrm{Ker}(\phi)$ we associate the element $\phi(m) \in \mathrm{Im}(\phi)$, and this is well-defined since $\mathrm{Ker}(\phi)$ is sent to zero by definition. These two can easily be seen to define inverse module maps making an isomorphism. □

Theorem 1.24 (Second isomorphism theorem)**.** *Let R be a commutative ring. Let M be an R-module, and let S and T be submodules of M. Then:*

(1) *the set*

$$S + T = \{s + t \mid s \in S, t \in T\}$$

is a submodule of M containing S and T as submodules,
(2) *the intersection $S \cap T$ is a submodule of S, and*
(3) *there is an isomorphism $(S+T)/T \simeq S/(S \cap T)$.*

Proof. The set $S + T$ is a subgroup of M (as proved in the isomorphism theorems for groups, for example). It is closed under multiplication by R as, if $s \in S$ and $t \in T$ then $r(s+t) = rs+rt \in S+T$. Hence it is indeed a submodule of M, and it contains S (as elements of the form $s + 0$) and T (as elements of the form $0 + t$).

The set $S \cap T$ is clearly a subgroup of S, and it is closed under multiplication by R (as if $x \in S$ and $x \in T$, then $rx \in S$ and $rx \in T$ as S and T are submodules of M), and hence $rx \in S \cap T$.

To define an isomorphism between $(S+T)/T$ and $S/(S \cap T)$ we must define mutually inverse maps in each direction.

The map from $(S+T)/T$ to $S/(S \cap T)$ sends an element $(s+t)+T$ to $s + (S \cap T)$. This is well-defined. Indeed, suppose we have another way of writing the same element:

$$(s+t) + T = (s' + t') + T.$$

Then $(s+t)-(s'-t') \in T$. But this is equal to $(s-s')+(t-t')$. The latter bracket is clearly in T, so we have $s-s' \in T$. But $s-s'$ is also in S, so it's in $S \cap T$, and hence $s+(S\cap T)$ and $s'+(S\cap T)$ are the same element of $S/(S\cap T)$. It can now readily be checked to be a module homomorphism.

The map from $S/(S\cap T)$ to $(S+T)/T$ sends an element $s+(S\cap T)$ to $(s+0)+T$. To show that this is well-defined, suppose that we chose another representation $s'+(S\cap T)$. Then $s-s' \in S\cap T$, so in particular $(s+0)-(s'+0) \in T$, so their images are the same. This can also be checked to be a module homomorphism.

It's easy to see that these maps are indeed mutually inverse. If we start with $s+(S\cap T) \in S/(S\cap T)$, we get $(s+0)+T \in (S+T)/T$ and then recover $s+(S\cap T) \in S/(S\cap T)$.

Conversely if we start with $(s+t)+T \in (S+T)/T$, we get $s+S\cap T \in S/(S\cap T)$ and then $(s+0)+T \in (S+T)/T$. This differs from $(s+t)+T$ by $t \in T$, and is hence equal as an element of $(S+T)/T$. □

Theorem 1.25 (Third isomorphism theorem)**.** *Let R be a commutative ring. Let M be an R-module. Let N be a submodule of M, and P a submodule of N. Then:*

(i) *the quotient N/P is a submodule of the quotient M/P, and*
(ii) *there is an isomorphism $(M/P)/(N/P) \simeq M/N$.*

Proof. The first part is reasonably clear: the elements $n+P \in N/P$, where $n \in N$, are a subset of those elements $m+P \in M/P$, where $m \in M$, since N is a submodule of P.

For the second part, we define a pair of mutually inverse homomorphisms between $(M/P)/(N/P)$ and M/N.

An element of the $(M/P)/(N/P)$ is of the form $(m+P)+(N/P)$; given such an element we associate to it the element $m+N \in M/N$. We must show that this is well-defined. Suppose $(m+P)+(N/P)$ and $(m'+P)+(N/P)$ give the same element in $(M/P)/(N/P)$; then $m+P$ and $m'+P$ differ by an element of N/P; in other words $m-m' \in N$. But this says exactly that m and m' are sent to the same coset of N in M, so that this construction is well-defined.

Conversely, suppose given an element $m+N \in M/N$. We associate to it the element $(m+P)+(N/P)$. Again, it is not clear that it is well-defined. So suppose we have two different representations $m+N$ and $m'+N$ for the same element, so that $m-m' \in N$. Then $(m+P)-(m'+P) \in N/P$, so we get a well-defined element of $(M/P)/(N/P)$.

As in the above cases, it's easy to check that these constructions are module homomorphisms, and it's obvious that they're mutually inverse. □

2. Noetherian and Artinian modules

2.1. **Chain conditions.** There are a lot of unpleasant rings out there, and a lot of nasty unpleasant modules over them. It's good to have notions of "nice", particularly if we want to do algebraic geometry.

Here are some straightforward ones, which come up repeatedly:

Definition 2.1. *Let R be a commutative ring, and let M be an R-module.*

- *We say that M satisfies the* ascending chain condition*, or that M is* Noetherian *if any ascending chain of submodules of M stabilises. That is, if we have R-modules*

$$N_1 \subset N_2 \subset N_3 \subset \cdots \subset M,$$

then there is some n such that $N_n = N_{n+1} = N_{n+2} = \cdots$.

- *We say that M satisfies the* descending chain condition*, or that M is* Artinian *if any descending chain of submodules of M stabilises. That is, if we have R-modules*

$$M \supset N_1 \supset N_2 \supset N_3 \supset \cdots,$$

then there is some n such that $N_n = N_{n+1} = N_{n+2} = \cdots$.

These are actually used more commonly as niceness conditions for rings rather than modules:

Definition 2.2. *Let R be a commutative ring.*

- *We say that R is a* Noetherian ring *if R is a Noetherian R-module. Since submodules of R are the same thing as ideals, this means that every increasing chain of ideals*

$$I_1 \subset I_2 \subset \cdots$$

stabilises.
- *We say that R is a* Artinian ring *if R is an Artinian R-module. Similarly, this means that every decreasing chain of ideals*

$$I_1 \supset I_2 \supset \cdots$$

stabilises.

Here are some examples of modules which are or are not Noetherian, and which are or are not Artinian.

Example 2.3. *Let $R = \mathbb{Z}$. Recall that R-modules are simply abelian groups.*

(1) *$\mathbb{Z}/m$ is Artinian and Noetherian as $\mathbb{Z}$-module. Indeed, since this module is a finite set, it only has finitely many submodules, and any chain stabilizes.*

(2) *$\mathbb{Z}$ is Noetherian but not Artinian $\mathbb{Z}$-module. Decoding the terminology a bit, this says that every ascending chain of ideals in $\mathbb{Z}$ stabilises, but not every descending chain.*

Since $\mathbb{Z}$ is a principal ideal domain, any ideal is generated by some single element, and containment is the same as divisibility. Hence an ascending chain of ideals

$$(n_1) \subseteq (n_2) \subseteq (n_3) \subseteq \cdots$$

gives us a chain of nonnegative integers, each a factor of the one before:

$$\cdots \mid n_3 \mid n_2 \mid n_1.$$

That means that $n_1 \geq n_2 \geq n_3 \geq \cdots \geq 0$, so certainly the chain stabilises, and hence $\mathbb{Z}$ is a Noetherian $\mathbb{Z}$-module.

However, it is not Artinian. Consider the following descending chain of ideals:

$$(1) \supseteq (2) \supseteq (4) \supseteq (8) \supseteq (16) \supseteq \cdots.$$

This does not stabilise.

(3) *The set $\mathbb{C}^\times$ of nonzero complex numbers is an abelian group, and hence a $\mathbb{Z}$-module. Let p be a prime, and consider the subset*

$$U = \left\{ x \in \mathbb{C}^\times \mid x^{p^n} = 1 \quad \text{for some } n \right\}.$$

That is a subgroup of $\mathbb{C}^\times$, and it is Artinian but not Noetherian as a $\mathbb{Z}$-module.

Let U_n be the subgroup consisting of all p^n-th roots of unity: that is, all $x \in \mathbb{C}^\times$ such that $x^{p^n} = 1$.

Then we have an ascending chain

$$U_1 \subsetneq U_2 \subsetneq U_3 \subsetneq \cdots$$

of submodules of U, which does not stabilise as they're all different. So U is not a Noetherian $\mathbb{Z}$-module.

However, it's not difficult to show (exercise!) that the U_i's are the only submodules of U. Hence any descending chain stabilises.

If we take modules which are "infinite-dimensional" in some appropriate sense, it's quite likely that they will be neither:

Example 2.4. *The set of complex polynomials $\mathbb{C}[x]$ is a complex vector space and hence a $\mathbb{C}$-module. In this example we show that it is neither Artinian nor Noetherian as a $\mathbb{C}$-module.*

Let U_n be the vector space of polynomials of degree at most n. Being a vector space, it is a submodule of $\mathbb{C}[x]$. Then the chain

$$U_1 \subsetneq U_2 \subsetneq U_3 \subsetneq \cdots$$

is an ascending chain which does not stabilise, showing that $\mathbb{C}[x]$ is not a Noetherian $\mathbb{C}$-module.

Similarly, let V_n be the space of polynomials which are a multiple of x^n (equivalently, those which have a root at 0 of order n). Then the chain

$$V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \cdots$$

is a descending chain which does not stabilise, showing that $\mathbb{C}[x]$ is not an Artinian $\mathbb{C}$-module.

The following may not quite be obvious, and you should let it sink in.

Example 2.5. *The reader may think that the argument in the previous example says that $\mathbb{C}[x]$ is neither a Noetherian nor an Artinian ring. This is false.*

The proof there gives an ascending chain of submodules of $\mathbb{C}[x]$ regarded only as a $\mathbb{C}$-module, not a $\mathbb{C}[x]$-module. *This means that it does not show that $\mathbb{C}[x]$ is not Noetherian. In fact,* $\mathbb{C}[x]$ is *Noetherian, by a theorem of Hilbert.*

On the other hand, the example there of a descending chain is in fact a descending chain of $\mathbb{C}[x]$-modules (they're all ideals in $\mathbb{C}[x]$). Hence $\mathbb{C}[x]$ is definitely not an Artinian ring.

The next Theorem shows why we may care about Noetherian modules a bit more than about Artinian modules.

Theorem 2.6. *Let M be an R-module. Then M is Noetherian if and only if every submodule $N \subset M$ is finitely generated.*

Proof. Let M have the property that every submodule is finitely generated. Let

$$N_0 \subset N_1 \subset$$

be an ascending chain of submodule of M. Let

$$N = \bigcup_{i=0}^{\infty} N_i.$$

It is essentially obvious that N is a submodule of M. Now since N is finitely generated we have

$$N = \langle n_1, \ldots, n_r \rangle$$

for some $n_j \in N$. Since every n_j lies in one of the submodules N_{i_j}, we may choose a submodule N_i, $i = \max(i_1, \ldots, i_r)$ which contains every n_j, and then we have

$$N_k = N = N_i, \text{ for } k \geq i$$

and the chain stabilizes.

To prove the converse implication, assume that N to be an infinitely generated submodule of M and define a chain of submodules in M inductively as:

$$N_1 = \langle n_1 \rangle$$
$$N_2 = \langle n_1, n_2 \rangle$$
$$N_3 = \langle n_1, n_2, n_3 \rangle$$
$$\dots$$

where each element n_{j+1} is taken from the complement $N \backslash N_j$ (the complement is never empty, since N is not finitely generated: $N \neq N_j$ for every j). □

Corollary 2.7. *Noetherian modules are finitely generated.*

Proof. Put $N = M$ in the Theorem. □

2.2. **Properties of Noetherian and Artinian modules.** We will see now that many of the properties of Noetherian and Artinian modules develop in the same way. To develop this theory we need to rely on quotient modules. So I start by explaining what are the **submodules of the quotient module**.

Proposition 2.8. *Let $N \subset M$ be an R-submodule, and let us consider the quotient module M/N. Then we have a natural bijection:*

$$\{\textit{Submodules } \overline{K} \subset M/N\} \leftrightarrow \{\textit{Intermediate submodules } N \subset K \subset M\} \tag{2.1}$$

Proof. If we have an intermediate submodule $N \subset K \subset M$, then we can define a submodule

$$\overline{K} := K/N \subset M/N.$$

as in the Third Isomorphism Theorem last week. In other words $\overline{K}$ consists of equivalence classes $k + N$, $k \in K$.

Conversely, given an arbitrary submodule $\overline{K} \subset M/N$ we can look at its preimage under the canonical quotient homomorphism $\phi : M \to M/N$:

$$K := \phi^{-1}(\overline{K}) = \{m \in N : m + N \in \overline{K}\}.$$

□

Example 2.9. *Let's illustrate the bijection (3.1) in the case $R = \mathbb{Z}$, $M = \mathbb{Z}$, $N = 12\mathbb{Z} \subset M$. Intermediate submodules*

$$12\mathbb{Z} \subset K \subset \mathbb{Z}$$

correspond to divisors of 12: for every divisor n we can define $K = n\mathbb{Z}$. The corresponding submodule of $\mathbb{Z}_{12} = \mathbb{Z}/12\mathbb{Z}$ is generated by $\overline{n}$.

Lemma 2.10. *Let $N \subset M$ be a R-submodule. Then M is Noetherian (resp. Artinian) if and only if both N and M/N are Noetherian (resp. Artinian).*

Proof. We do the proof of the Noetherian property. The Artinian property is proved in the same way.

There are two statements to prove now. Let first us assume that M is Noetherian, and show that N and M/N are also Noetherian. A chain of submodules in N is at the same time a chain of submodules in M. Since the latter chains stabilize, N is Noetherian. Now take a chain of

submodules in M/N. According to (3.1) this chain gives us a chain of submodules in M, and it must stablize, so must the original chain.

Now let us assume that both N and M/N are Noetherian. To show that M is Noetherian, consider a chain of submodules in M:

$$M_1 \subset M_2 \subset \cdots \subset M$$

and this gives rise to two other chains:

$$M_1 \cap N \subset M_2 \cap N \subset \cdots \subset N$$

and

$$(M_1 + N)/N \subset (M_2 + N)/N \subset \cdots \subset M/N.$$

Both of the new chains stabilize since N and M/N are Noetherian: for $i \geq n$ we have

$$M_i \cap N = M_{i+1} \cap N$$
$$(M_i + N)/N = (M_{i+1} + N)/N$$

Note that by from the Third Isomorphism Theorem we have a natural isomorphism

$$(M_i + N)/N \simeq M_i/(M_i \cap N).$$

Now comparing the two adjacent submodules M_i, M_{i+1} for $i \geq n$ we see that they have the same submodule

$$K := M_i \cap N = M_{i+1} \cap N$$

such that the quotient modules M_i/K, M_{i+1}/K are also the same as submodules in M/K. This forces $M_i = M_{i+1}$. □

Lemma 2.11. *If M and N are Noetherian (resp. Artinian) R-modules, then $M \oplus N$ is Noetherian (resp. Artinian) R-module.*

Proof. This follows very easily from Lemma 2.11. Consider an R-submodule

$$M = \{m, 0\} \subset M \oplus N.$$

Note the quotient is computed as

$$(M \oplus N)/M \simeq N$$

(for example, we can use First Isomorphism Theorem applied to the projection $M \oplus N \to N$).

The statement follows from Lemma 2.11. □

Theorem 2.12. *If R is a Noetherian (resp. Artinian) ring and M is a finitely generated R-module, then M is a Noetherian (resp. Artinian) R-module.*

Proof. Since M is finitely generated we know that M admits a surjective homomorphism

$$R^n \to M.$$

Using induction on Lemma 2.11 we see that R^n is Noetherian (resp. Artinian) R-module. The rest follows from Lemma 2.10. □

2.3. **Properties of Noetherian and Artinian rings.** In contrast to the case of modules, properties of Noetherian and Artinian rings are very different.

The following theorem and its corollary demonstrate that Noetherian rings appear naturally in Algebraic Geometry.

Theorem 2.13 (Hilbert's Basis Theorem)**.** *If R is Noetherian then $R[x]$ is Noetherian.*

Proof. See last semester's notes. □

Corollary 2.14. *Let R be a quotient ring of a polynomial ring: $R = k[x_1, \ldots, x_n]/I$, for some ideal I. Then R is a Noetherian ring.*

Proof. By the Hilbert Basis Theorem applied inductively we deduce that the ring $k[x_1, \ldots, x_n]$ is Noetherian. Now R is a finitely generated (actually, cyclic) $k[x_1, \ldots, x_n]$-module, hence Theorem 2.12 implies that R is Noetherian as $k[x_1, \ldots, x_n]$-module. Since ideals in R are the same as $k[x_1, \ldots, x_n]$ submodules this implies that R is Noetherian as a ring as well. □

Remark 2.15. *Of course $k[x_1, \ldots, x_n]$ is* **not Artinian** *ring, see Example 2.5.*

In fact Artinian rings are not at all as general as Noetherian rings, and their structure is much simpler.

Proposition 2.16. *An Artinian ring S which is an integral domain is a field.*

Proof. For every $0 \neq x \in S$ the following sequence of ideals in S:

$$\cdots \subset (x^{n+1}) \subset (x^n) \subset \cdots \subset (1) = S$$

stabilizes. This means that $yx^{n+1} = x^n$ for some $y \in S$. Since S is a domain we have

$$yx^{n+1} = x^n \implies yx = 1$$

so that x is invertible.

Since every nonzero element $x \in S$ is invertible, S is a field. □

Proposition 2.17. *If R is Artinian, then every prime ideal in R is maximal.*

Proof. Let $I \subset R$ be an ideal. Assume that I is prime so that the quotient ring $S = R/I$ is an integral domain. By Theorem 2.12 S is an Artinian ring and by the previous proposition S is a field. Thus I is a maximal ideal. □

Remark 2.18. *Surprisingly every Artinian ring is Noetherian (see Atiyah-MacDonald, Chapter 8) but we do not prove this fact.*

3. Localization

The concept of localization generalizes the fraction field construction, i.e. the process of forming $\mathbb{Q}$ from $\mathbb{Z}$. This applies equally well to rings and modules. Geometrically localization corresponds to considering small open neighbourhoods in algebraic sets, hence the name.

Denominators for localization must lie in a so-called multiplicative subset:

Definition 3.1. *A* multiplicative subset *U of a ring R is a subset $U \subset R$ such that:*

- *$1 \in U$, and*
- *if $a, b \in U$, then $ab \in U$.*

Example 3.2. *If $f \in R$ is an element, then*

$$\{1, f, f^2, f^3, \dots\}$$

is a multiplicative subset.

Example 3.3. *Let $U = R\backslash\{0\}$. Then U is a multiplicative subset if and only if R is an integral domain.*

Example 3.4. *Let $I \subset R$ be an ideal. Then $U = R\backslash I$ is a multiplicative subset if and only I is a prime ideal. This example generalizes the one before: R is an integral domain if and only if $\{0\}$ is a prime ideal.*

Now that we understand multiplicative subsets, we can use them to define rings of fractions. Given a multiplicative subset U of R, we define a new ring $U^{-1}R$ to have as elements symbols of the form $\frac{a}{b}$, where $a \in R$ and $b \in U$, subject to an equivalence relation.

The correct equivalence relation which we'll use might be thought a little surprising: we say that $\frac{a}{b} = \frac{c}{d}$ if there is $t \in U$ such that

$$t(ad - bc) = 0$$

or equivalently

$$tad = tbc.$$

We ought to make the following check:

Proposition 3.5. *The relation on fractions defined above is an equivalence relation.*

Proof. Reflexivity is easy: $\frac{a}{b} = \frac{a}{b}$ as we can take $t = 1$ and get $1ab = 1ab$. Symmetry is similarly clear: if $tad = tbc$ then $tbc = tad$.

To check transitivity suppose $\frac{a}{b} = \frac{c}{d}$ and $\frac{c}{d} = \frac{e}{f}$. This means that there is some $t \in U$ such that $tad = tbc$, and some $u \in U$ such that $ucf = ude$. We need to find $v \in U$ such that $vaf = vbe$. The obvious choice is $v = tud$ (which is in U, as all the factors are), and then

$$vaf = tuadf = tubcf = tubde = vbe$$

as required. □

Now we show that this structure is a ring:

Theorem 3.6. *The set $U^{-1}R$, under the equivalence relation above, equipped with the usual arithmetic operations for fractions, is a commutative ring.*

Proof. What we really need to show that the usual operations are *well-defined*: that is, equivalent inputs give equivalent outputs.

First we show that if $\frac{a}{b} = \frac{c}{d}$, then $\frac{a}{b} + \frac{e}{f} = \frac{c}{d} + \frac{e}{f}$, or in other words that $\frac{af+be}{bf} = \frac{cf+de}{df}$.

So we have $tad = tbc$ for some $t \in U$, and we need to show that for some $u \in U$ we have $u(af + be)df = u(cf + de)bf$. If we take $u = t$ we get

$$t(af + be)df = tadf^2 + tbdef = tbcf^2 + tbdef = t(cf + de)bf$$

as needed.

Secondly, we show that if $\frac{a}{b} = \frac{c}{d}$, then $\frac{a}{b}\frac{e}{f} = \frac{c}{d}\frac{e}{f}$, or in other words that $\frac{ae}{bf} = \frac{ce}{df}$. So, again we have $tad = tbc$ for some $t \in U$, and we need to show that for some $u \in U$ we have $uadef = ubcef$. Again this works with $u = t$.

This having been proved, the rest (the commutative ring axioms) depends simply on standard properties of fraction arithmetic. □

There is a ring homomorphism $L_U : R \to U^{-1}R$ sending $a \mapsto \frac{a}{1}$, generalising the map $Z \to \mathbb{Q}$. Note that under this homomorphism, everything in U becomes invertible in $U^{-1}R$, since $L_U(u) = \frac{u}{1}$ has inverse $\frac{1}{u}$.

This observation gives us a way of explaining this construction, which is less explicit but often more helpful:

Theorem 3.7. *Let $f : R \to S$ be a ring homomorphism which sends elements of U to invertible elements in S. There is a unique ring homomorphism $g : U^{-1}R \to S$ such that f is the composite gL_U.*

Proof. We must have $g(\frac{a}{1}) = f(a)$ for $a \in R$, and we must have $g(\frac{1}{b}) = f(b)^{-1}$ for $b \in U$. Therefore we must have

$$g\left(\frac{a}{b}\right) = g\left(\frac{a}{1}\frac{1}{b}\right) = g\left(\frac{a}{1}\right) g\left(\frac{1}{b}\right) = f(a)f(b)^{-1}.$$

As a result of this, we know what g must be: so there is at most one homomorphism; we merely need to show that this works.

It sends equal elements to equal elements: if $\frac{a}{b} = \frac{c}{d}$ then there is some $t \in U$ with $tad = tbc$. Under these circumstances, g sends $\frac{a}{b}$ to $f(a)f(b)^{-1}$ and $\frac{c}{d}$ to $f(c)f(d)^{-1}$.

These are, however, equal:

$$\begin{aligned} f(a)f(b)^{-1} &= f(a)f(d)f(d)^{-1}f(t)f(t)^{-1}f(b)^{-1} \\ &= f(tad)\left(f(d)f(t)f(b)\right)^{-1} \\ &= f(tbc)\left(f(d)f(t)f(b)\right)^{-1} \\ &= f(c)f(b)f(b)^{-1}f(t)f(t)^{-1}f(d)^{-1} \\ &= f(c)f(d)^{-1}. \end{aligned}$$

Now we know that it is well-defined, it is easy to check that g is a homomorphism. □

We like to say that $U^{-1}R$ is the *universal* commutative ring with a homomorphism from R which sends elements of U to invertible elements.

As opposed to the familiar case $\mathbb{Z} \to \mathbb{Q}$ the localization homomorphism L_U is not always injective:

Lemma 3.8. *The kernel of L_U has the form:*

$$\mathrm{Ker}(L_U) = \{r \in R : t \cdot r = 0, \text{ for some } t \in U\}.$$

Proof. The proof is straightforward:

$$r \in \mathrm{Ker}(L_U) \iff \frac{r}{1} = \frac{0}{1} \in U^{-1}R \iff t \cdot r = 0, \text{ for some } t \in U.$$

□

Corollary 3.9. *If R is an integral domain, and $U \subset R$ a multiplicative system in R, then the homomorphism $L_U : R \to U^{-1}R$ is injective. So we'll simply write $R \subset U^{-1}R$ in this case.*

With all these preliminaries in place, we can define the central thing of interest:

Definition 3.10. *Let R be a commutative ring, and let P be a prime ideal in R. The* localization of R at P*, written R_P, is the commutative ring $(R \backslash P)^{-1}R$.*

Unpacking this definition, we can consider R_P to be a ring of fractions $\frac{a}{b}$, where $a, b \in R$ and $b \notin P$.

Example 3.11 (Localization in Number Theory)**.** *Take $R = \mathbb{Z}$ and $P = (p)$ where p is a prime. For the sake of explicitness, let's take $p = 7$.*

The localization $\mathbb{Z}_{(7)}$ is the set of fractions $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $7 \nmid b$. It's a subring of $\mathbb{Q}$: we can add, subtract, and multiply, and we can divide by any prime except 7. The effect of this is to make a ring where 7 is the only prime: all other primes have become units.

Number theorists use these rings (for values of p which may or may not be 7) a lot to focus on one prime at a time. They call them the p-local integers*.*

Example 3.12 (Geometric meaning of localization)**.** *In the world of Algebraic Geometry the ring $\mathbb{C}[z]$ represents the ring of functions on the complex line $\mathbb{A}^1_{\mathbb{C}} = \mathbb{C}$.*

The field of rational functions

$$\mathbb{C}(z) = (\mathbb{C}[z]\backslash\{0\})^{-1}\mathbb{C}[z] = \Big\{\frac{f(z)}{g(z)} : f, g \in \mathbb{C}[z]\Big\}$$

represents meromorphic functions, i.e. functions which admit poles: one for every root of $g(z)$.

Now let us take a prime ideal $P = (z - a)$ and see what localization at P does to $\mathbb{C}[z]$:

$$\mathbb{C}[z]_P = \Big\{\frac{f(z)}{g(z)} : f \in \mathbb{C}[z], g \in \mathbb{C}[z]\backslash(z-a)\Big\} = \Big\{\frac{f(z)}{g(z)} : f, g \in \mathbb{C}[z], g(a) \neq 0\Big\}$$

This is precisely the ring of meromorphic functions with no poles at $z = a$, i.e. functions regular at a. In other words when considering localization ring $\mathbb{C}[z]_P$ we restrict our attention to a small open neighbourhood around $z = a$.

The following theorem explains that localization of rings is a useful tool for similar reasons to why quotient rings are useful: these constructions make rings simpler, in particular there are fewer prime ideals in the localized ring than in the original ring (think of the $\mathbb{Z}_{(7)}$ example above!).

Theorem 3.13. *Let $U \subset R$ be a multiplicative subset. Then we have an inclusion-preserving bijection:*

$$\{\text{Prime ideals } P' \subset U^{-1}R\} \leftrightarrow \{\text{Prime ideals } P \subset R \text{ such that } P \cap U = \emptyset\} \tag{3.1}$$

Under this bijection maximal ideals correspond to maximal ideals.

Proof. The map from the set of ideals on the left to the set of ideals on the right is $P' \mapsto L_U^{-1}(P')$. Note that the preimage of a prime ideal under any ring homomorphism is a prime ideal. The ideal $L_U^{-1}(P')$ does not intersect U, otherwise P' would contain an image of an element of U, which is impossible as elements of U become units in $U^{-1}R$.

It is also clear that this map preserves inclusions: $P_1' \subset P_2' \implies L_U^{-1}P_1 \subset L_U^{-1}P_2$.

The map in other direction attaches to an ideal P the ideal

$$U^{-1}P = \Big\{\frac{a}{s} : a \in P, s \in U\Big\}.$$

One easily checks that this is indeed an ideal. To see that $U^{-1}P$ is prime consider a product

$$\frac{a}{s} \cdot \frac{a'}{s'} \in U^{-1}P,$$

so that

$$\frac{aa'}{ss'} = \frac{a}{s} \cdot \frac{a'}{s'} = \frac{b}{u}$$

with $b \in P$. This yields

$$t(uaa' - ss'b) = 0 \implies (tu)aa' = tss'b \in P,$$

and since P is prime one of the elements tu, a or a' is in P. But since $P \cap U = \emptyset$, we deduce that $tu \notin P$, so that either a or a' belongs to P, which means that one of the original fractions

$$\frac{a}{s}, \frac{a'}{s'}$$

belongs to P.

It is clear that the assignment $P \mapsto U^{-1}P$ preserves inclusions:

$$P_1 \subset P_2 \implies U^{-1}P_1 \subset U^{-1}P_2.$$

It remains to check that the two maps just defined are inverses of each other: this will establish the desired bijection.

We first take a prime ideal $P \subset R$, $P \cap R = \emptyset$ and consider

$$\begin{aligned} L_U^{-1}(U^{-1}P) &= L_U^{-1}\left(\left\{\frac{a}{s} : a \in P\right\}\right) = \\ &= \left\{b \in R : L_U(b) = \frac{a}{s}, \text{ for some } a \in P,\, s \in U\right\} = \\ &= \left\{b \in R : \frac{b}{1} = \frac{a}{s}, \text{ for some } a \in P,\, s \in U\right\} = \\ &= \{b \in R : t(bs - a) = 0, \text{ for some } a \in P,\, t, s \in U\} = \\ &= \{b \in R : ub \in P, \text{ for some } u \in U\} = P. \end{aligned}$$

Now we take a prime ideal $P' \subset U^{-1}R$ and consider

$$\begin{aligned} U^{-1}L_U^{-1}(P') &= U^{-1}\left\{a \in R : \frac{a}{1} \in P'\right\} = \\ &= \left\{\frac{a}{u} \in R : \frac{a}{1} \in P', u \in U\right\} = P' \end{aligned}$$

□

Corollary 3.14. *If $P \subset R$ is a prime ideal, then the ring R_P has the unique maximal ideal*

$$m_P = \{\frac{p}{t} : p \in P, t \notin P\} \subset R_P,$$

and prime ideals of R_P are in bijection with prime ideals of R contained in P.

Proof. The previous Theorem tells us that prime ideals in R_P are in inclusion-preserving bijection with ideals in R which do not intersect with $R \backslash P$, i.e. are contained in P.

Among these the maximal ideal is P, and it corresponds to $m_P = U^{-1}P$. □

Definition 3.15. *A ring R with a unique maximal ideal is called a local ring.*

Thus the previous Corollary tells us that localized rings R_P are local. Examples are rings $\mathbb{Z}_{(7)}$ and $\mathbb{C}[x]_{(x-a)}$ considered earlier.

3.1. **Localization of modules.** Given a ring R, a multiplicative subset U and a R-module M, we can use fractions to form a $U^{-1}R$-module $U^{-1}M$: objects are fractions $\frac{a}{b}$ with $a \in M$ and $b \in U$, subject to the equivalence relation that $\frac{a}{b} = \frac{c}{d}$ if there is $t \in U$ such that $tad = tbc$.

Addition is defined by the usual formula:

$$\frac{a}{b} + \frac{c}{d} = \frac{da + bc}{bd},$$

(note that this does make sense: we're never multiplying two elements of M together), and scalar multiplication by elements of $U^{-1}R$ is defined by the usual formula

$$\frac{r}{s} \cdot \frac{a}{b} = \frac{ra}{sb}.$$

It is not hard to check that these definitions work.

It's also easy to show that we have

$$U^{-1}(M \oplus N) = U^{-1}M \oplus U^{-1}N. \tag{3.2}$$

Example 3.16. *Let U be the multiplicative subset $\mathbb{Z}\backslash\{0\} \subset \mathbb{Z}$. Then we have $\mathbb{Q} = U^{-1}\mathbb{Z}$.*

Now suppose we have an abelian group A, and regard it as a $\mathbb{Z}$-module. Hence $U^{-1}A$ is supposed to be a $\mathbb{Q}$-module: a rational vector space. We can explain how this works in the case where A is finitely generated. In this case, $A = \mathbb{Z}^n \oplus A'$, where A' is finite.

For any finite abelian group A', we have $U^{-1}A' = 0$, the trivial vector space! Indeed, any element $x \in A'$ has $kx = 0$ for some nonzero $k \in \mathbb{Z}$, and then

$$\frac{x}{1} = \frac{0}{1} \qquad \text{since } kx1 = k01.$$

On the other hand, considering the free $\mathbb{Z}$-module $\mathbb{Z}$, we have $U^{-1}\mathbb{Z} = \mathbb{Q}$. Indeed, the definition is the same as the standard definition of $\mathbb{Q}$ as the fraction field of $\mathbb{Z}$.

Hence, for this particular choice of U, we have

$$U^{-1}A = U^{-1}(\mathbb{Z}^n \oplus A') = \mathbb{Q}^n;$$

the rule is "throw away the torsion and turn the $\mathbb{Z}$s into $\mathbb{Q}$'s".

One extra feature, which is frequently important, is this:

Proposition 3.17. *Let R be a commutative ring, U a multiplicative subset, and M and N both R-modules, and let $\phi : M \to N$ be an R-module homomorphism. Then there is a $U^{-1}R$-module homomorphism $U^{-1}\phi : U^{-1}M \to U^{-1}N$.*

Proof. Define

$$U^{-1}\phi\left(\frac{a}{b}\right) = \frac{\phi(a)}{b};$$

it is immediate to check that this works. □

We call this behaviour *functoriality*: the phenomenon that many constructions that can be done to objects can also be done to their homomorphisms. Formally this means that localization is a *functor*

$$U^{-1} : R - mod \to (U^{-1}R) - mod \tag{3.3}$$

between the category of R-modules and the category of $U^{-1}R$-modules.

Lemma 3.18. *Let M be a finitely generated R-module. Then $U^{-1}M = 0$ if and only U intersects* $\mathrm{Ann}(M)$.

Recall that annihilator $\mathrm{Ann}(M) \subset R$ is the ideal $\{r \in R : rm = 0 \text{ for all } m \in M\}$.

Proof. Let $m_1, \ldots, m_n$ be a set of generators for M. We have a chain of equivalences:

$$\begin{aligned} U^{-1}M = 0 &\iff \frac{m}{u} = \frac{0}{1} \text{ for all } m \in M, u \in U \iff \\ &\iff tum = 0 \text{ for all } m \in M,\ u \in U, \text{ for some } t \in U \iff \\ &\iff \text{there exist } t_1, \ldots, t_n \in U \text{ such that } t_i m_i = 0 \iff \\ &\iff \text{there exist } t \in U \text{ such that } tm = 0 \text{ for all } m \in M \iff \\ &\iff \mathrm{Ann}(M) \cap U \neq \emptyset. \end{aligned}$$

□

Definition 3.19. *Let R be a ring, P a prime ideal of R and M an R-module. We define the* localization *M_P of M to be the R_P-module $(R \backslash P)^{-1}M$.*

It is not hard to imagine that this should be an important tool: if localization lets us look at a commutative ring R "one prime ideal at a time", then localising modules allows us to look at the effects of each prime ideal of R on their modules, too.

By the above, localization of modules is functorial: if we have R a commutative ring, P a prime ideal, and $M \to N$ a homomorphism of R-modules, then we get a homomorphism of P-modules $M_P \to N_P$.

We now investigate properties of the localization functor (3.3). From (3.2) we know that it preserves direct sums. We check that it also preserves kernels and quotients.

Proposition 3.20. *Let $U \subset R$ be a multiplicative subset and $N \subset M$ a submodule of R-module. Then we have a natural isomorphism*

$$U^{-1}(M/N) \simeq (U^{-1}M)/(U^{-1}N).$$

Digression on cokernels. Did it ever occur to you that definitions of injective and surjective as usually given are not exactly analogous? Here is a way to make the definitions of injective and surjective match up.

Let $f : M \to N$ be a homomorphism of R-modules. Then we define cokernel of f as the quotient:

$$\mathrm{Coker}(f) = N/\mathrm{I}m(f).$$

Now we have:

$$\begin{aligned} f \text{ injective} &\iff \mathrm{Ker}(f) = 0 \\ f \text{ surjective} &\iff \mathrm{Coker}(f) = 0 \end{aligned}$$

Proposition 3.21. *Localization functor (3.3) preserves kernels, images and cokernels, that is if $f : M \to N$ is a homomorphism of R-modules, then there are natural isomorphisms*

$$\begin{aligned} U^{-1}\,\mathrm{Ker}(f) &\simeq \mathrm{Ker}(U^{-1}f) \\ U^{-1}\mathrm{I}m(f) &\simeq \mathrm{I}m(U^{-1}f) \\ U^{-1}\,\mathrm{Coker}(f) &\simeq \mathrm{Coker}(U^{-1}f) \end{aligned}$$

where $U^{-1}f : U^{-1}M \to U^{-1}N$.

Proof. For the kernel we calculate:

$$\begin{aligned}\mathrm{Ker}(U^{-1}f) &= \left\{\frac{m}{u} : U^{-1}f\left(\frac{m}{u}\right) = \frac{0}{1}\right\} = \\ &= \left\{\frac{m}{u} : \frac{f(m)}{u} = \frac{0}{1}\right\} = \\ &= \left\{\frac{m}{u} : tf(m) = 0, \text{ for some } t \in U\right\} = \\ &= \left\{\frac{m}{u} : f(m) = 0\right\} = U^{-1}Ker(f)\end{aligned}$$

and now for the image:

$$\mathrm{I}m(U^{-1}f) = \left\{\frac{f(m)}{u} : m \in M, u \in U\right\} = U^{-1}\mathrm{I}m(f).$$

Finally for the cokernel the statement follows from the one about the image and Proposition 3.20. □

4. Nakayama's Lemma

4.1. **Nilradical and Jacobson Radical.** Let R be a ring. The Nilradical of R is defined as intersection of all prime ideals:

$$Nil(R) = \bigcap_{P \subset R} P.$$

Note that $Nil(R)$ is an intersection of ideals, hence an ideal.

Proposition 4.1. *Nilradical coincides with the ideal consisting of all nilpotent elements:*

$$a \in Nil(R) \iff a^n = 0 \text{ for some } n > 0.$$

Proof. If $a^n = 0$, then since $0 \in P$ for every prime ideal, we have $a \in P$ (because P is prime). This proves one direction.

Conversely, let a be not nilpotent. We need to show that there is a prime ideal not containing P. Consider the multiplicative subset

$$U = \{a^n : n \in \mathbb{N}\} \subset R.$$

Consider the localized ring $U^{-1}R$ and take any prime ideal

$$P' \subset U^{-1}R.$$

By our basic correspondence between prime ideals in R and prime ideals in $U^{-1}R$ we see that there is a prime ideal $P \subset R$ not intersecting U. That's exactly what we were looking for! □

The Jacobson radical is defined as intersection of all maximal ideals in R:

$$J(R) = \bigcap_{m \subset R} m.$$

$J(R)$ is an ideal in R. Since every maximal ideal is prime, so that the intersection in defining $J(R)$ goes over larger set than in $Nil(R)$, we have an inclusion $Nil(R) \subset J(R)$.

Example 4.2. *If R is a local ring, then $J(R)$ is its unique maximal ideal.*

Here's an alternative characterisation:

Proposition 4.3. *Let R be a commutative ring. Then for an element $x \in R$, we have $x \in J(R)$ if and only if $1 - xy$ is a unit in R for all $y \in R$.*

Proof. We'll show firstly that if $x \in J(R)$, then $1 - xy$ is a unit. Indeed, suppose it isn't. Then let $I = (1 - xy)$, a proper ideal of R. The ideal I is contained in a maximal ideal M. Since $x \in J(R)$, we have $x \in M$, so $xy \in M$. Also $1 - xy \in M$ since $1 - xy \in I$. Hence $1 \in M$, which is a contradiction.

Now suppose that $1 - xy$ is a unit for all y, and suppose there is a maximal ideal M with $x \notin M$. Then the ideal sum $M + (x)$ (which, you'll remember, is defined to be $\{i + j \mid i \in M, j \in (x)\}$) is a bigger ideal than M and is hence the whole of R (as M is maximal). Hence $1 \in M + (x)$, so $1 = u + xy$ for some $u \in M$ and some $y \in R$. Hence $1 - xy \in M$. But if $1 - xy$ is a unit, then $M = R$, a contradiction. □

4.2. **Matrices over rings.** Every square matrix with entries in a commutative ring has a determinant, and your favourite technique for computing the determinant will work fine.

However, not every matrix has an inverse: of course, for a general commutative ring, not even every 1×1 matrix has an inverse! We can form the adjugate matrix, however. (The *adjugate* matrix is the matrix you have immediately before you divide by the determinant to obtain the inverse: it's the transpose of the matrix of cofactors).

The same proof as usual shows that, for any square matrix A over any commutative ring whatsoever, we have

$$A \operatorname{adj}(A) = \operatorname{adj}(A) A = \det(A) \cdot I$$

where I is the identity matrix and $\operatorname{adj}(A)$ is the adjugate of A.

For example, if we have a two-by-two matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then its adjugate is given by

$$\operatorname{adj}(A) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

and we have

$$\begin{aligned} A \operatorname{adj}(A) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} \\ &= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \operatorname{adj}(A) A, \end{aligned}$$

and so both are equal to the determinant $\det(A) = ad - bc$ times the identity matrix. In particular, whenever we have a matrix with invertible determinant, it is invertible.

Matrices are useful with modules for the same reason that they're useful with vector spaces: they define homomorphisms of finitely generated free modules.

We'll also be needing this construction a lot:

Definition 4.4. *Let R be a commutative ring, I an ideal in R, and M an R-module. We write IM for the set*

$$IM = \{i_1 m_1 + \cdots + i_k m_k \mid i_i \in I, m_i \in M\}.$$

This is a submodule of M, since it's a subset of M and is evidently closed under addition and scalar multiplication.

Theorem 4.5 (Cayley-Hamilton)**.** *Let R be a commutative ring, and I an ideal in R. Let M be a finitely generated R-module and $\phi : M \to M$ a R-module homomorphism.*

Suppose that $\mathrm{Im}(\phi) \subset IM$. Then we can produce an equation for ϕ of the form $\phi^n + i_{n-1}\phi^{n-1} + \cdots + i_1\phi + i_0 = 0$, where all the elements i_k are in I.

For the proof of the Theorem, we need modules over polynomial rings $R[t]$. As I already mentioned in the very first lecture $R[t]$-modules are same things as R-modules together with an R-module homomorphism $\phi : R \to R$. Indeed, if we have an $R[t]$-module, then t-action determines a map $\phi : M \to M$ by the rule $\phi(m) = tm$, and from the properties of modules it follows that ϕ is an R-module homomorphism.

Conversely, given an R-module M with a homomorphism $\phi : M \to M$ we may define $R[t]$-module structure on M via

$$p(t) \cdot m := p(\phi)(m).$$

This means that $p(t) = \sum_{k=0}^{n} a_k t^k$ acts as

$$p(t) \cdot m := \sum_{k=0}^{n} a_k \phi^k(m).$$

It is easily seen that M is an $R[t]$-module homomorphism.

Lemma 4.6. *Let M, N be R-modules and let $R[t]$-module structure be specified on M by an R-module homomorphism ϕ and on N by an R-module homomorphism π. Let $\psi : M \to N$ be an R-module homomorphism. Then ψ is an $R[t]$-module homomorphism if and only if is the following diagram is commutative:*

$$\begin{array}{ccc} M & \xrightarrow{\phi} & M \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi} \\ N & \xrightarrow{\pi} & N \end{array}$$

Proof. The proof is left as homework assignment. □

Proof of the Cayley-Hamilton Theorem. The idea is to consider the characteristic equation $p(t) \in R[t]$ for ϕ and to prove that $p(\phi) = 0$.

Case 1: M is a free finitely generated module $M = R^n$. Let $e_1, \ldots, e_n$ be a basis for M. Let us consider the action of ϕ on this basis:

$$\phi(m_i) = \sum a_{ij} m_j$$

and since $\mathrm{Im}(\phi) \subset IM$ we will have $a_{ij} \in I$. Thus we have a matrix $A = (a_{ij}) \in M_n(I)$ of the map ϕ as in the usual linear algebra setup. Now let us consider the matrix

$$B = t \cdot Id_n - A \in M_n(I[t]) = M_n(I)[t].$$

and its determinant

$$p(t) = \det(B) = t^n + i_{n-1}t^{n-1} + \cdots + i_1 t + i_0 \in R[t].$$

All the coefficients i_j belong to A because the matrix coefficients a_{ij} are in I.

We may regard R^n not as an R-module but as $R[t]$-modules with t acting by A. The matrix $B \in M_n(t)[t]$ will act on R^n, and actually it will act trivially:

$$B(v) = tv - Av = Av - Av = 0, \text{ for all } v \in R^n.$$

Thus the determinant $p(t) \in R[t]$ of B also acts by zero:

$$p(t)v = p(A)v = 0, \text{ for all } v \in R^n.$$

so $p(A) = 0$ as a matrix.

Case 2: M is an arbitrary finitely generated module. Choose a set of generators $m_1, \ldots, m_n$ for M and let $\psi : R^n \to M$ be the corresponding surjective homomorphism. We may choose a matrix A for M by considering where the generators m_i are sent, and this way we obtain a commutative diagram

$$\begin{array}{ccc} R^n & \xrightarrow{A} & R^n \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi} \\ M & \xrightarrow{\phi} & M \end{array}$$

Now if we consider M as an $R[t]$-module with t acting by ϕ, the commutative diagram above simply tells us that $\psi : R^n \to M$ is an $R[t]$-module homomorphism.

Now the key point: from Case 1 we already know that there is a polynomial $p(t)$ with the properties we need such that $p(t)$ acts trivially on R^n. But since ψ is a surjective $R[t]$-module homomorphism, it follows that $p(t)$ acts trivially on M as well. Thus $p(\phi) = 0$. □

Corollary 4.7. (a) *If M is a finitely generated R-module and $\alpha : M \to M$ is a surjective homomorphism, then α is an isomorphism.*

(b) *If $M = R^n$, the free R-module of rank n, then any set of n generators is linearly independent*

(c) *The rank is well-defined, that is if $R^m \simeq R^n$, then $n = m$*

Proof. (a) We regard M as an $R[t]$-module where t acts by α. Now we apply the Cayley-Hamilton Theorem to M, $\phi = id : M \to M$ and $I = (t) \subset R[t]$. M is finitely-generated as an R module, so is obviously finitely generated as an $R[t]$-module as well. Since α is surjective, $IM = tM = \alpha M = M$. All the assumptions of the Cayley-Hamilton Theorem are satisfied and we obtain that

$$(id + i_{n-1} + \cdots + i_0)(m) = 0 \text{ for all } m \in M.$$

Since the i_j's belong to $I = (t)R[t]$, it follows that there exists a polynomial $p(t)$ such that

$$1 - tq(t) \in R[t]$$

acts by zero on M. This means that $1 - \alpha q(\alpha) = 0$, and we get that $q(\alpha)$ is the inverse of α.

(b) The set of n generators $m_1, \ldots, m_n$ define a surjective map

$$\beta : R^n \to M = R^n.$$

By part (a), β must be an isomorphism which is equivalent to the set $m_1, \ldots, m_n$ being R-linear independent.

(c) Assume $m \leq n$, call the isomorphism $\phi : R^m \to R^n$ and consider the images of $e_1, \ldots, e_m \in R^m$

$$v_1 = \phi(e_1), \ldots, v_m = \phi(e_m) \in R^n.$$

Since ϕ is an isomorphism, these m elements generate R^n. Even though this is quite peculiar, there is no contradiction so far!

Now add $m - n$ zero elements to make the generating set to have size n:

$$v_1, \ldots, v_m, 0, \ldots, 0.$$

By assumption these generate R^n, but are not linearly independent unless $m = n$. □

Remark 4.8. *Of course, we could ask whether ϕ being injective implies that it's bijective, but that's not true. For example, the homomorphism $f : \mathbb{Z} \to \mathbb{Z}$ of $\mathbb{Z}$-modules defined by $f(x) = 2x$ is an injection but not a surjection of finitely generated modules.*

4.3. **Nakayama's Lemma.** Nakayama's Lemma is a series of results saying that finitely-generated modules are not so very different to finite-dimensional vector spaces.

We need some preparatory work based on the Cayley-Hamilton Theorem.

Lemma 4.9. *Let R be a commutative ring, and let M be a finitely generated R-module. Let I be an ideal of R such that $IM = M$. Then there exists $r \in I$ such that $(1 - r)M = 0$.*

Proof. Take ϕ to be the identity in Theorem 4.5 above.

This gives us an identity of the form

$$(1 + i_{n-1} + \cdots + i_1 + i_0)m = 0,$$

valid for all $m \in M$ where the coefficients lie in I. We obtain what we need by putting $r = -i_{n-1} - \cdots - i_1 - i_0$. □

Theorem 4.10 (Nakayama's Lemma)**.** *Let R be a commutative ring, I be an ideal contained in the Jacobson radical of R and M a finitely-generated R-module.*

(a) *If $IM = M$, then $M = 0$.*
(b) *If $N \subset M$ is a submodule such that $IM + N = M$, then $N = M$*
(c) *If $m_1, \ldots, m_n \in M$ have images in M/IM that generate it as an R-module, then $m_1, \ldots, m_n$ generate M as an R-module*

Proof. (a) We wish to use Lemma 4.9 above. This gives us that $(1-r)M = 0$ for some $r \in I \subset J(R)$. By Proposition 4.3, $1 - r$ is a unit in R, and hence $(1 - r)M = M$, and so $M = 0$.

(b), (c) This is left for the homework assignment.

□

Example 4.11. *For a possibly useful example, consider $R = \mathbb{Z}_{(7)}$. This ring has Jacobson radical equal to its unique maximal ideal (7). This says then that if $(7)M = M$ for any finitely-generated module M, then $M = 0$.*

Note that $(7)M = 7M$, the multiples of 7. So this tells us that multiplying by 7 cannot be surjective on any nontrivial finitely-generated $\mathbb{Z}_{(7)}$-module.

Example 4.12. *Let R be a local Noetherian ring with maximal ideal $m \subset R$. Consider a descending chain*

$$\cdots \subset m^{n+1} \subset m^n \subset \ldots$$

of ideals in R. Recall that by definition m^n is generated by products $a_1 \cdots a_n$ of elements $a_i \in m$. Informally, we would think of m^n as functions vanishing up to order n at a given point.

Now if if R is an integral domain and not a field, then all $m^n \neq 0$. Indeed, since R is not a field, we have $m \neq 0$, and since R is an integral domain for every $0 \neq x \in m$, we have $0 \neq x^n \in m^n$, so all $m^n \neq 0$.

Now let us apply Nakayama's Lemma to show that the chain of inclusions above is strictly descending. Consider m^n as an R-module. Since R is Noetherian, m^n is finitely generated. Thus by Nakayma's Lemma if for some n we had an equality

$$m^{n+1} = m \cdot m^n = m^n \implies m^n = 0,$$

which we know is not the case. Thus the chain of ideals m^n is strictly descending.

In particular, we have a non-zero module m/m^2. This module will be important later on when we study tangent spaces and dimensions of rings and algebraic sets.

5. Integral Extensions

5.1. **Integral Elements and Integral Extensions.** Let R be a commutative ring. Recall from last semester that an *R-algebra* is a commutative ring S together with a homomorphism $f : R \to S$. In this section we'll talk about some nice classes of R-algebras. Recall that when we have an R-algebra S, then S is also an R-module.

Suppose we have a chain of homomorphisms of commutative rings

$$R \xrightarrow{f} S \xrightarrow{g} T.$$

Then f makes S into an R-algebra, g makes T into an S-algebra, and gf makes T into an R-algebra.

Proposition 5.1. *Suppose given a chain of homomorphisms as above. If S is a finitely-generated R-module, and T is a finitely-generated S-module, then T is also a finitely-generated R-module.*

Proof. If S is a finitely-generated R-module, then there are elements $s_1, \ldots, s_m \in S$ such that any element $a \in S$ can be expressed as a sum

$$a = \sum_{1 \le i \le m} a_i s_i.$$

If T is a finitely-generated S-module, then there elements $t_1, \ldots, t_n \in T$ such that any element $b \in T$ can be expressed as a sum

$$b = \sum_{1 \le j \le n}^{n} b_j t_j.$$

Now, we will show that the elements $s_i t_j$ (for $1 \le i \le m$ and $1 \le j \le n$) generate T as an R-module.

Indeed, let b be any element of T. We can write

$$b = \sum_{1 \le j \le n} b_j t_j = \sum_{1 \le j \le n} \sum_{1 \le i \le m} (a_{ij} s_i) t_j = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{ij} (s_i t_j),$$

for some elements $b_j \in S$ and $a_{ij} \in R$, exactly as needed. □

Now we introduce a definition, extremely useful in Algebraic Number Theory and Algebraic Geometry alike:

Definition 5.2. *Let S be an R-algebra. An element $x \in S$ is said to be* integral over R *if it satisfies a monic polynomial equation*

$$x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0,$$

where $a_{n-1}, \ldots, a_0 \in R$.

Formally, what we really mean by that, of course, is that there are elements $a_{n-1}, \ldots, a_0$ of R such that

$$x^n + f(a_{n-1}) x^{n-1} + \cdots + f(a_0) = 0,$$

where $f : R \to S$ is the structure map of the S-algebra R. But it's commonplace to not mention the structure map, and I'll usually avoid doing so from now on.

Here are some examples and nonexamples.

Example 5.3. *Given a commutative ring homomorphism $f : R \to S$, any element $r \in R$ is integral over R, because it is a root of the equation $x - r = 0$.*

Exercise 5.4. *The element $1/2 \in \mathbb{Q}$ is not integral over $\mathbb{Z}$.*

Example 5.5. *The element $\sqrt{17} \in \mathbb{R}$ is integral over $\mathbb{Z}$, for example, because it satisfies $x^2 - 17 = 0$.*

Example 5.6. *The golden ratio $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$, because it satisfies $x^2 - x - 1 = 0$.*

Example 5.7. *Any element of $\mathbb{C}$ is integral over $\mathbb{R}$. Indeed, if $x = a + ib$, then $(x - a)^2 = -b^2$ and hence $x^2 - 2ax + a^2 + b^2 = 0$.*

Now we'll see what this has to do with things we were talking about earlier:

Theorem 5.8. *Let S be an R-algebra. The following are equivalent:*

(i) *S is a finitely-generated R-module;*
(ii) *S is generated as an R-algebra by integral elements $x_1, \ldots, x_n$;*
(iii) *S is a finitely-generated R-algebra, and every element of S is integral over R.*

Proof. The implication (iii) $\Rightarrow$ (ii) is obvious. We'll prove (ii) $\Rightarrow$ (i) and then (i) $\Rightarrow$ (iii).

In order to prove (ii) $\Rightarrow$ (i), suppose that S is generated as an R-algebra by $x_1, \ldots, x_n$ which are roots of monic polynomials of degrees $d_1, \ldots, d_n$ respectively.

Then S is generated as an R-module by the monomials $x_1^{a_1} \cdots x_n^{a_n}$. But in fact we don't need the monomials where $a_i \geq d_i$ for any i, since we can use integrality to rewrite these. This means we have a finite set of generators.

Now we must prove (i) $\Rightarrow$ (iii). Note firstly that if S is a finitely-generated R-module then it's certainly a finitely-generated R-algebra: the module generators generate it as an algebra.

Let $x_1, \ldots, x_n$ generate S as an R-module, and let s be any element of S; we must show s is a root of a monic polynomial with coefficients in R.

We now employ the Cayley-Hamilton Theorem from last week, taking $I = R$, $M = S$ (note that $IM = M$), and $\phi\colon S \to S$ to be $m \mapsto sm$. This gives us the monic polynomial we want, with coefficients in R. □

Definition 5.9. *We say that an R-algebra satisfying the conditions of Theorem 5.8 is an* integral extension*.*

Typically this will applied to to a subring $R \subset S$ (or more generally an injective homomorphism $R \to S$), and this explains using the word "extension".

Corollary 5.10. *Let $f\colon R \to S$ be a ring homomorphism. Then sums and products of elements in S which are integral over R are integral over R. Furthermore then the set of integral elements forms a subalgebra of S.*

Proof. Suppose given two elements $x, y \in S$ which are integral over R. Then consider the subalgebra $T \subset S$ generated as an R-algebra by x and y.

Since it's generated by integral elements x and y, by Theorem 5.8 all its elements are integral over R, but this includes $x + y$ and xy.

The "furthermore" claim follows from what we have shown and from the fact that every element of $f(R)$ is integral over R. □

We now investigate how integral extensions behave with respect to taking quotient rings. Let $R \xrightarrow{f} S$ be an algebra, and $I \subset R$ be an ideal. In this case the image of $f(I)$ does not have to be an ideal: $f(I) \subset S$ is an abelian subgroup but there is no reason for $f(I)$ to be closed under S-multiplication. For example, if we consider the inclusion homomorphism $\mathbb{Z} \to \mathbb{Q}$, then the image of the ideal (2), that is the set of all even integers, is not an ideal in $\mathbb{Q}$.

The right thing to do is to consider the ideal generated by $f(I)$ in S: $IS = f(I)S$. This consists of sums of elements of the form $i \cdot s$, $i \in I$, $s \in S$. In other words, IS is the smallest ideal in S which contains $f(I)$.

In this setting we can pass to the quotient rings R/I and S/IS and obtain a homomorphism between them as follows. The homomorphism $R \to S$ defines a composition $R \to S \to S/IS$ which factors to give a ring homomorphism $\overline{f} : R/I \to S/IS$ via the rule:

$$\overline{f}(r + I) = f(r) + IS,$$

and this is well-defined since $f(i) = i \cdot 1 \in IS$.

Lemma 5.11. *If $R \xrightarrow{f} S$ is an integral extension, and $I \subset R$ is an ideal, then the extension $R/I \xrightarrow{\overline{f}} S/IS$ is integral.*

Proof. To check that the extension $R/I \to S/IS$ is integral we need to show that S/IS is finitely generated as R/I-module. But this is clear: if $s_1, \dots, s_r \in S$ generate S as R-module, then the images $s_1 + IS, \dots, s_r + IS$ generate S/IS, as R-module as well as an R/I-module. □

5.2. **Finite maps of algebraic sets.**

Definition 5.12. *We call a polynomial map of algebraic sets $X \to Y$ finite if the ring homomorphism $k[Y] \to k[X]$ is an integral extension.*

Recall that integral extension simply means that $k[X]$ is a finitely generated $k[Y]$-module. In practice to check that a map is finite we rely on Theorem 5.8: it is sufficient to verify that the $k[Y]$-algebra $k[X]$ is generated by integral elements.

Example 5.13. *Let $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ be a polynomial map defined by $\phi(t) = t^2$. We check that ϕ is a finite map by considering the coordinate rings. Both coordinate rings are $k[t]$, but it will be less confusing if denote the coordinate on the source $\mathbb{A}^1$ by t, and on the target $\mathbb{A}^1$ by u. Then the the map of coordinate rings is:*

$$f : k[u] \to k[t]$$
$$p(u) \mapsto p(\phi(t)) = p(t^2).$$

By considering the top degree term of p we see that f is injective. The image of f consists of polynomials in t^2:

$$\mathrm{Im}(f) = k[t^2] \subset k[t].$$

Hence we are talking about an extension $k[t^2] \subset k[t]$. The key point is that the generator t is integral as it satisfies a monic equation

$$x^2 - t^2 = 0$$

with coefficients in $k[t^2]$. By Theorem 5.8 the above extension is integral, hence the map of algebraic sets ϕ is finite.

Theorem 5.14. *Every finite map $\phi : X \to Y$ has finite fibers, that is for every $y \in Y$ the set $\phi^{-1}(y) = \{x \in X : \phi(x) = y\} \subset X$ is finite.*

Proof. The proof consists of three steps.

Step 1: In this step we identify the fibers algebraically. For every y we construct a ring R^y such that points in $\phi^{-1}(y)$ correspond to maximal ideals in R^y.

For every point $y \in Y$ denote by $m_y \subset k[Y]$ the maximal ideal of functions which vanish at y. Note that by the First Isomorphism Theorem we have $k[Y]/m_y \simeq k$. Similarly, if $x \in X$ we have the corresponding ideal $m_x \subset k[X]$.

We need to translate the condition $\phi(y) = x$ into algebraic language:

Lemma 5.15. *Let $\phi : X \to Y$ be a polynomial map of algebraic sets, let $x \in X$, $y \in Y$ be points, and let $m_x \subset k[X]$, $m_y \subset k[Y]$ the corresponding maximal ideals. Let $f : k[Y] \to k[X]$ be the k-algebra homomorphism corresponding to ϕ. Then we have*

$$\phi(x) = y \iff m_x \supset m_y k[X].$$

Recall that the ideal $m_y k[X]$ is the same thing as $f(m_y)k[X]$: the smallest ideal of $k[X]$ which contains $f(m_y)$.

Proof of the Lemma. Recall how $f : k[Y] \to k[X]$ is constructed from $\phi : X \to Y$: if $h \in k[Y]$ is a polynomial function, then $f(h) = h \circ \phi \in k[X]$, that is $f(h)(x) = h(\phi(x))$.

If $\phi(x) = y$, then for every $h \in k[X]$ if $h \in m_y$, then $f(h) = h \circ \phi \in m_x$, since $f(h)(x) = h(\phi(x)) = h(y) = 0$. This shows that $f(m_y) \subset m_x$, and since m_x is an ideal, this implies that $f(m_y)k[Y] \subset m_x$.

Now if $\phi(x) = y' \neq y$, then we can find a function $h \in k[Y]$ such that $h(y) = 0$, $h(y') \neq 0$. In this case $f(h) \notin m_x$ since $f(h)(x) = h(\phi(x)) = h(y') \neq 0$. Thus $f(m_y)k[X] \not\subset m_x$. □

We continue proving the Theorem. From the Lemma it follows that points in $\phi^{-1}(y)$ are in bijection with maximal ideals in the ring $R^y := k[X]/(m_y k[Y])$.

Step 2: In this step we show that R^y is an Artinian ring for every $y \in Y$. Since the extension $k[Y] \to k[X]$ is integral, by Lemma 5.11, for every $y \in Y$ the extension

$$k[Y]/m_y \to k[X]/(m_y k[X]) = R^y.$$

is integral. On the other hand $k[Y]/m_y$ is isomorphic to k, thus R^y is an integral extension of k, i.e. a finite-dimensional as k-vector space. We deduce that R^y is an Artinian k-module, hence an Artinian ring.

Step 3: In this final step we show that fibers of ϕ are finite. Assume that there are infinitely many points $x_1, x_2, \ldots$ in X contained in a fiber $\phi^{-1}(y)$. For every n consider an ideal $I_n = I(\{x_1, x_2, \ldots, x_n\}) \subset k[X]$ of functions vanishing at the n points. This is a strictly decreasing chain:

$$I_1 \supset I_2 \supset \ldots$$

Since by assumption all the points x_j are contained in the fiber $\phi^{-1}(y)$, every one of the ideals I_n contains the ideal $m_y k[X]$ (like in Step 1). This yields an infinite strictly descending chain of ideals in $k[X]/(m_y k[X]) = R^y$:

$$\overline{I_1} \supset \overline{I_2} \supset \ldots$$

contradicting to the fact that R^y is Artinian. This shows that all fibers are in fact finite. □

Example 5.16. *Let us compute the fibers of the finite polynomial map $\phi(t) = t^2$ from Example 5.13. For every $a \in \mathbb{A}^1$ the fiber is*

$$\phi^{-1}(a) = \begin{cases} \{\pm\sqrt{a}\}, & a \neq 0 \\ \{0\}, & a = 0 \end{cases}$$

which are evidently finite sets. To demonstrate the proof of Theorem 5.14 we consider the rings R^a, $a \in \mathbb{A}^1$*:*

$$R^a = k[X]/(m_y k[X]) = k[t]/(t-a) = k[u]/(t^2-a).$$

Maximal ideals in $k[t]/(u^2-a)$ *correspond to maximal ideals in* $k[t]$ *that contain* t^2-a*, i.e. divisors of the polynomial* $t^2-a = (t-\sqrt{a})(t+\sqrt{a})$*.*

If $a = 0$*, then we have* $k[t]/(t^2)$*, which is a local ring with the maximal ideal* $(\bar{t})$ *corresponding to* $0 \in \phi^{-1}(0)$*. If* $a \neq 0$*, then there are two maximal ideals* $(\bar{t}-\sqrt{a}), (\bar{t}+\sqrt{a}) \subset k[t]/(t^2-a)$*, corresponding to the two elements* $\pm\sqrt{a} \in \phi^{-1}(a)$*.*

Remark 5.17. *If we consider finite and surjective maps, these are analogous to finite coverings in topology.*

6. Noether Normalization

6.1. **Noether Normalization.**

Theorem 6.1 (Noether Normalization, geometric form)**.** *Let* k *be an algebraically closed field, and let* X *be an algebraic set. Then there exists an* $n \geq 0$ *and a finite surjective polynomial map* $\phi : X \to \mathbb{A}^n$*.*

Remark 6.2. *Recall that a finite polynomial map has finite fibers, so it's reasonable to expect that in the setup of Noether Normalization* X *will be "n-dimensional". We'll see that this is the case as soon as we define what dimension of an algebraic set is.*

As usual in Algebraic Geometry to prove Noether Normalization we need to translate the geometric statement into the language of algebra. Since Noether Normalization deals with finite maps $X \to \mathbb{A}^n$, the algebraic side will deal with integral extensions $k[x_1, \ldots, x_n] \to k[X]$.

Definition 6.3. *Let* k *be a field and let* S *be an* k*-algebra. (Note that this is the same thing as an embedding of rings* $k \subset S$*). We say that elements* $s_1, \ldots, s_n$ *of* S *are* algebraically independent over k *if the* k*-algebra homomorphism*

$$k[x_1, \ldots, x_n] \to S$$

sending x_i *to* s_i *for each* i*, is an injective homomorphism.*

Equivalently, $s_1, \ldots, s_n$ are algebraically independent if there are no nonzero n-variable polynomials with coefficients in k which vanish at $(s_1, \ldots, s_n)$.

Example 6.4. *Let* $R = k[x, y]$ *be the polynomial ring. Then* x, y *are algebraically independent over* k*.*

Example 6.5. *Let* $R = k[x, y]/(y^2 - x^3)$*. The elements* x, y *are algebraically dependent over* k*, as they satisfy an equation* $y^2 - x^3 = 0$*.*

The next Theorem describes the structure of finitely generated algebras.

Theorem 6.6 (Noether Normalization Theorem, algebraic form)**.** *Let* k *be an infinite field, and* R *a finitely-generated* k*-algebra. Then* R *is an integral extension of a polynomial ring over* k*.*

More precisely, there are algebraically independent elements $s_1, \ldots, s_n$ *of* S *such that* S *is an integral extension of the subring* $k[s_1, \ldots, s_n]$*:*

$$k \subset k[s_1, \ldots, s_n] \subset R.$$

Proof. Let $s_1, \dots, s_n$ generate S as k-algebra. We do induction on n. When $n = 0$, $S = k$ and there is nothing to prove.

If $s_1, \dots, s_n$ are algebraically independent, then the homomorphism $k[x_1, \dots, x_n]$ sending x_i to s_i is an isomorphism, and again there is nothing to prove.

So assume that $n > 0$ and that the generators $s_1, \dots, s_n$ are algebraically dependent, and let $f(s_1, \dots, s_n) = 0$ be a relation between them. Here $f \in k[x_1, \dots, x_n]$ is a polynomial.

Consider first the case when the polynomial f has the form

$$f(x_1, \dots, x_n) = x_n^d + a_{n-1}(x_1, \dots, x_{n-1})x_n^{d-1} + \dots + a_1(x_1, \dots, x_{n-1})x_n + a_0(x_1, \dots, x_{n-1}) \tag{6.1}$$

that is it's monic considered as a polynomial in x_n. In this case since $f(s_1, \dots, s_n) = s_n^d + \dots = 0$, we see that s_n is integral over the subalgebra S' generated by $s_1, \dots, s_{n-1}$ and we apply the induction hypothesis to S': S' will be integral over a polynomial ring, and since being integral is a transitive relation, same applies to S.

It remains to show that after a change of coordinates we will have (6.1). Let $\deg(f) = d$ and let f_d be the sum of degree d monomials of f so that

$$f(x_1, \dots, x_n) = f_d(x_1, \dots, x_n) + \text{ lower degree monomials.}$$

Now assume that x_n is one of the variables which enters f_d nontrivially, otherwise renumber the variables.

Now apply the change of coordinates $x_i' = x_i - a_i x_n$, for $i < n$ and see how the polynomial f changes. We write the new polynomial as a polynomial in x_n:

$$\begin{aligned} f(x_1 + a_1x_n, \dots, x_{n-1} + a_{n-1}x_n, x_n) &= f_d(x_1 + a_1x_n, \dots, x_{n-1} + a_{n-1}x_n, x_n) + \text{ lower degree monomials} \\ &= f_d(a_1, \dots, a_{n-1}, 1)x_n^d + \text{ lower degree terms in } x_n. \end{aligned}$$

Thus if we pick general $a_1, \dots, a_{n-1} \in k$, then the coefficient $f_d(a_1, \dots, a_{n-1}, 1) \in k$ is nonzero (here we use that k is infinite), and after dividing by this coefficient the equation will take the form (6.1). □

Proof of the geometric form of Noether Normalization. We apply the algebraic form of Noether Normalization to finitely generated k-algebra $S = k[X]$. Then the k-algebra embedding $k[x_1, \dots, x_n] \subset S$ translates into a polynomial map $\phi : X \to \mathbb{A}^n$. This polynomial map is finite since the corresponding extension of k-algebras is integral.

Proving that ϕ is surjective requires a bit more technology, and I omit the proof of this step (see Atiyah-Macdonald, Theorem 5.10). □

7. Proving the Nullstellensatz

In this chapter k is an algebraically closed field, e.g. $k = \mathbb{C}$.

7.1. **Recollection: Nullstellensatz and its Corollaries.** Recall that if $J \subset R$ is an ideal then its radical is $\sqrt{J} = \{r \in R : r^n \in J, \text{ for some } n \geq 1\}$.

The following Theorem was stated (but not proved) in Tom's notes for Semester 1 as Theorem 14.5.

Theorem 7.1 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field, and let J be an ideal in the polynomial algebra $k[x_1, \dots, x_n]$. Then the ideal of elements of $k[x_1, \dots, x_n]$ which vanish on the zeroes of J is equal to the radical of J:*

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

Corollary 7.2. *The assignments $J \mapsto V(J)$ and $V \mapsto I(V)$ define mutually inverse inclusion-reversing bijections:*

$$V : \{\text{Radical ideals } J \subset k[x_1, \ldots, x_n]\} \leftrightarrow \{\text{Algebraic subsets } V \subset \mathbb{A}^n\} : I$$

Proof. It follows easily from definitions that the assignments I, V are inclusion-reversing: $J \subset J' \implies V(J) \supset V(J')$ and $X \subset X' \implies I(X') \supset I(X)$.

If J is a radical ideal, then by the Hilbert Nullstellensatz $I(V(J)) = \sqrt{J} = J$. It remains to show that if X is an algebraic set, then $V(I(X)) = X$. This is surprisingly a very formal, hence simple, step: since X is an algebraic set we have an ideal J such that $X = V(J)$. Now

$$V(I(X)) = V(I(V(J)) = V(\sqrt{J}) = V(J) = X.$$

□

Corollary 7.3. *There is a bijection between the set of points of $\mathbb{A}^n$ and the set of maximal ideals of $k[x_1, \ldots, x_n]$:*

$$k^n \leftrightarrow \mathrm{Specm}(k[x_1, \ldots, x_n])$$
$$a \in k^n \mapsto m_a = (x_1 - a_1, \ldots, x_n - a_n)$$

Proof. Since the bijections I and V of Corollary 7.2 are order reversing, maximal elements among the radical ideals correspond to minimal elements among the algebraic subsets.

We need to be a bit careful here as strictly speaking the only maximal element in the set of radical ideals is the ideal (1) which corresponds to $\emptyset = V(1)$, the empty algebraic set, which is indeed a minimal algebraic subset of $\mathbb{A}^n$.

After dismissing these trivial cases we obtain a bijection between maximal ideals among $J \neq (1)$, that is maximal ideals of $k[x_1, \ldots, x_n]$ and minimal non-empty algebraic subsets of $\mathbb{A}^n$, that is points.

If $a \in \mathbb{A}^n$ is a point, then $I(a) = (x_1 - a_1, \ldots, x_n - a_n)$. Indeed the ideal in the LHS is contained in $I(a)$, and since it is maximal and $I(a) \neq (1)$, the two ideals must be equal. □

We have more general versions of the above corollaries with the k-algebra $R = k[x_1, \ldots, x_n]$ replaced by $R = k[X] = k[x_1, \ldots, x_n]/I(X)$, the coordinate ring of an algebraic set $X \subset \mathbb{A}^n$.

Corollary 7.4. *The assignments $J \mapsto V(J)$ and $V \mapsto I(V)$ define mutually inverse bijections:*

$$V : \{\text{Radical ideals } J \subset k[X]\} \leftrightarrow \{\text{Algebraic subsets } V \subset X\} : I$$

Proof. Consider the bijection of Corollary 7.2 applied to the set of radical ideals $J \subset k[x_1, \ldots, x_n]$ such that $J \supset I(X)$. Since the $I - V$ bijections are order-reversing we have:

$$J \supset I(X) \iff V(J) \subset V(I(X)) = X,$$

which yields a bijection

$$V : \{\text{Radical ideals } I(X) \subset J \subset k[x_1, \ldots, x_n]\} \leftrightarrow \{\text{Algebraic subsets } V \subset X\} : I$$

Now ideals $\overline{J} \subset k[X]$ are in bijection with ideals $I(X) \subset J \subset k[x_1, \ldots, x_n]$, and radical ideals correspond to radical ideals (why?). This finishes the proof. □

Corollary 7.5. *There is a bijection between the set of points of X and the set of maximal ideals of $k[X]$:*

$$X \leftrightarrow \mathrm{Specm}(k[X])$$
$$a \in k^n \mapsto m_a = (x_1 - a_1, \ldots, x_n - a_n)$$

Proof. This can be deduced either from Corollary 7.3 or from Corollary 7.4. □

7.2. **Proving the Nullstellensatz.** There are many proofs of the Nullstellensatz, and all of them are kind of complicated. Our method of proof will do it in several steps: hopefully these steps may be of independent interest. The proof will use most of the techniques studied so far: quotient rings, localization, integral extensions and Noether Normalization. Before proving the general form of Hilbert Nullstellensatz we establish the bijection between maximal ideals and points of Corollary 7.3.

We start by gaining a little more understanding of finiteness:

Proposition 7.6. *Let $R \subset S$ be an integral extension and assume that R and S are integral domains. Then R is a field if and only if S is a field.*

Note that this gives us (for example) that $\mathbb{Q}$ is not a finitely-generated $\mathbb{Z}$-module, and that $\mathbb{C}(x)$ (the fraction field of $\mathbb{C}[x]$) is not a finitely-generated $\mathbb{C}[x]$-module.

Proof. Will be done in the homework assignment. □

This enables us to prove the following:

Theorem 7.7 (Zariski's Lemma)**.** *Let $k \subset L$ are fields and L is a finitely generated k-algebra, then L is an integral extension of k. Furthermore if k is algebraically closed, then $L = k$.*

Recall that an "integral extension" is a stronger condition than "finitely generated". Zariski's Lemma tells us that for fields the two concepts coincide.

Proof. The Noether Normalization Theorem states that L is an integral extension of some polynomial k-algebra $k[x_1, \dots, x_n]$.

Our aim is to show that $n = 0$. So, in order to get a contradiction, suppose that $n \geq 1$. But then we have that L has is integral over the subring $k[x_1, \dots, x_n]$, and Proposition 7.6 then tells us that $k[x_1, \dots, x_n]$ is a field. That's absurd: for example, x_1 is not invertible.

Assume now that k is algebraically closed. Take any element $x \in L$, it must satisfy a monic equation $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ with coefficients in k. But this polynomial splits as a product of roots (since k is algebraically closed):

$$(x - r_1) \cdots (x - r_n) = 0.$$

However, L is a field, so $x - r_i = 0$ for some i, so $x = r_i$ for some i. Hence any element $x \in L$ is in fact an element of k so that $L = k$. □

We now know enough to classify maximal ideals over polynomial rings over an algebraically closed field.

Theorem 7.8. *Let k be an algebraically closed field. Then the maximal ideals in $k[x_1, \dots, x_n]$ are exactly the ideals of the form*

$$m_a = (x_1 - a_1, \dots, x_n - a_n)$$

for elements $a_1, \dots, a_n \in k$.

Note this says that maximal ideals in $k[x_1, \dots, x_n]$ correspond to points in k^n. This is same as Corollary 7.3, but note that we do not yet have the Hilbert Nullstellensatz, but are in the process of proving it!

Proof. We should show that an ideal of this form is indeed maximal.

So consider the ideal

$$(x_1 - a_1, \dots, x_n - a_n).$$

By changing coordinates, writing y_i for $x_i - a_i$ we can consider the special case of $(y_1, \dots, y_n)$ as an ideal in $k[y_1, \dots, y_n]$. This ideal consists of all polynomials with zero constant term; the quotient is hence evidently k. Since this is a field, the ideal is maximal.

On the other hand, suppose we have a maximal ideal m of $k[x_1, \dots, x_n]$. Consider the field $L = k[x_1, \dots, x_n]/m$. This is generated over k by $\overline{x_1}, \dots, \overline{x_n}$, and so Zariski Lemma (Theorem 7.7) says that L is isomorphic to k as k-algebra:

$$k \subset L \simeq k$$

Now, let a_i be the image of $\overline{x_i}$ under this isomorphism. Now the element $x_i - a_i$ of $k[x_1, \dots, x_n]$ is sent to 0 in $k[x_1, \dots, x_n]/m$, and so $x_i - a_i \in m$.

Hence $(x_1 - a_1, \dots, x_n - a_n) \subset m$. But since the left-hand side is maximal, this must be m. □

Now (at last!) we can do the Nullstellensatz itself.

Proof of Hilbert Nullstellensatz (Theorem 7.1). The inclusion $I(V(J)) \supset J$ is easy: if $h \in J \subset k[x_1, \dots, x_n]$, then h is tautologically zero on $V(J)$, so $h \in I(V(J))$. Now since $I(V(J))$ is a radical ideal we also have $I(V(J)) \supset \sqrt{J}$. We need to show the opposite inclusion.

Assume that $f \notin \sqrt{J}$. We'll prove that $f(a) \neq 0$ for some $a \in V(J)$.

Lemma 7.9. *Let $J \subset R$ be any ideal. Then the radical of J is the intersection of all prime ideals containing J: $\sqrt{J} = \bigcap_{P \supset J} P$.*

Proof of Lemma. Will be done in the homework assignment. □

We continue proving Hilbert Nullstellensatz. Since $\sqrt{J} = \bigcap_{P \supset J} P$, and $f \notin \sqrt{J}$, we have $f \notin P$ for some prime ideal $P \supset J$. We now find a maximal ideal $m \supset P \supset J$ such that $f \notin m$.

For that consider the quotient R/P, and its localization $U^{-1}(R/P)$ with $U = \{1, \overline{f}, \overline{f}^2, \dots\}$. Since the result of localization is inverting f, we will write $R/P[\overline{f}^{-1}]$ for $U^{-1}(R/P)$.

We have a composition of homomorphisms

$$R \to R/P \to R/P[\overline{f}^{-1}].$$

of finitely generated k-algebras.

We get maps on the level of Specm (maximal spectrum):

$$\mathrm{Specm}(R/P[\overline{f}^{-1}]) \to \mathrm{Specm}(R/P) \to \mathrm{Specm}(R).$$

From the standard facts on how ideals behave with respect to taking quotients and localization we deduce that these maps are injective (compare to HW 5, Question 1):

$$\mathrm{Specm}(R/P[\overline{f}^{-1}]) \subset \mathrm{Specm}(R/P) \subset \mathrm{Specm}(R)$$

and in fact the image of $\mathrm{Specm}(R/P[\overline{f}^{-1}])$ in $\mathrm{Specm}(R)$ is

$$\{m \subset R : P \subset m, f \notin m\}.$$

We are done: since $\mathrm{Specm}(R/P[\overline{f}^{-1}]) \neq \emptyset$ (every ring has a maximal ideal) we get a maximal ideal $m \supset P \supset J$ in R such that $f \notin m$. By Theorem 7.8 we have $m = m_a$ for some $a \in k^n$, and we see that $a \in V(I)$, but $f(a) \neq 0$. □

8. Dimension Theory

Among the basic concepts associated to geometric objects there is a notion of dimension. One spends a lot of time introducing dimension in linear algebra, which then is generalized in differential geometry or complex geometry. There is even dimension of fractals: not an integer, but rather a real number in general!

For an algebraic set X we define its dimension, also called Krull dimension in terms of chains of irreducible algebraic subsets

$$X_0 \subset X_1 \subset \cdots \subset X,$$

thus generalizing the dimension defined for vector spaces.

When developing the geometric concept in algebraic geometry we usually start on the level of commutative algebra. This is also the case with the Krull dimension.

8.1. Heights of ideals and Krull dimension of rings.

Definition 8.1. *Let R be a commutative ring. The* **height** *of a prime ideal $P \subset R$, denoted* $\operatorname{ht} P$*, is the length h of the longest chain of prime ideals*

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_h = P.$$

(Note that by the length here we mean the number of inclusions, that is the number of prime ideals plus one.) If there are arbitrarily long such chains we set $\operatorname{ht} P = \infty$*.*

Remark 8.2. *In Noetherian rings, ideals have finite height.*

Example 8.3. *Let $R = \mathbb{C}[x]$. Maximal ideals correspond to linear polynomials $x - a$, and 0 is non-maximal prime ideal, thus we have chains of the type $0 \subset (x-a)$, and no other chains. We see that*

$$\operatorname{ht}(0) = 0$$
$$\operatorname{ht}(x-a) = 1.$$

Example 8.4. *Let $R = \mathbb{C}[x, y]$. Maximal ideals correspond to points $(a_1, a_2) \in \mathbb{C}^2$ and we have chains*

$$(0) \subset (x - a_1) \subset (x - a_1, y - a_2).$$

We see that $\operatorname{ht}(m_a) \geq 2$*. We'll see later that in fact* $\operatorname{ht}(m_a) = 2$*, but this is harder to prove, since we need to bound all possible chains.*

Definition 8.5. *The (Krull) dimension* $\dim(R)$ *of a ring R in general is the maximum of the lengths of all chains of primes, and infinity if the lengths are unbounded.*

Example 8.6. *The ring $\mathbb{C}$ has only one prime ideal (0) so that* $\dim(\mathbb{C}) = 0$*. The Krull dimension should not be confused with the dimension of a vector space!*

Example 8.7. *The study of heights in Example 8.3 implies that* $\dim(\mathbb{C}[x]) = 1$*.*

Remark 8.8. *Dimensions of Noetherian rings may be infinite! The simplest example is a bit complicated: it is a certain localization of a polynomial ring in infinitely many variables, where for every n there will be an ideal I_n of height* $\operatorname{ht}(I_n) \geq n$*.*

Lemma 8.9. *Let R be a ring and consider $\overline{R} = R/Nil(R)$, the quotient by the Nilradical. Then* $\dim(R) = \dim(\overline{R})$*.*

Proof. Every prime ideal in R contains $Nil(R)$: indeed one of the characterizations of $Nil(R)$ was the intersection of all prime ideals. Thus we have a bijection $\mathrm{Spec}(R) = \mathrm{Spec}(\overline{R})$, which is obviously order-preserving, hence $\dim(R) = \dim(\overline{R})$. □

Example 8.10. *Let $R = \mathbb{C}[x]/(x^n)$. We have $Nil(R) = (x)$. Using the previous Lemma we have*

$$\dim(R) = \dim(\overline{R}) = \dim(\mathbb{C}) = 0.$$

Furthermore in the homework assignment you will prove that every Artinian ring has dimension zero. This is one reason why I refer to Artinian rings as "small".

Lemma 8.11. *Let R be a local ring with maximal ideal m. Then*

$$\dim(R) = \mathrm{ht}(m).$$

Proof. We can put m on top of any chain of prime ideals, so that every maximal chain of prime ideals will end with m. □

Lemma 8.12. *Let $P \subset R$ be an ideal, and let R_P denote the localization at P (as usual). Recall that R_P is a local ring with maximal ideal m_P. Then*

$$\mathrm{ht}(P) = \mathrm{ht}(m_P) = \dim(R_P).$$

Proof. There is an order-preserving bijection between prime ideals in R_P and prime ideals in R which are contained in P. This gives a bijection on chains, which leads to the equality of heights. □

Example 8.13. *Let $R = \mathbb{Z}$. Maximal ideals are (p) for primes p, and the only non-maximal prime ideal is (0). We have chains $(0) \subset (p)$ and no other chains. This shows that $\mathrm{ht}(0) = 0$ and that $\mathrm{ht}(p) = 1$.*

Now we may consider localizations:

- *$P = (0)$, then $R_P = \mathbb{Q}$ (we invert all non-zero elements), and $\dim(\mathbb{Q}) = 0 = \mathrm{ht}(0)$*
- *$P = (p)$, then $R_P = \mathbb{Z}_{(p)}$ (we invert all primes other than p), and $\dim(\mathbb{Z}_{(p)}) = 1 = \mathrm{ht}(p)$.*

Example 8.14. *Consider the localization $R = \mathbb{C}[x]_{(x-a)}$, $a \in \mathbb{C}$. When defining localization I explained that its geometric meaning is to encapture information about a neighbourhood of a point. For dimension we have:*

$$\dim \mathbb{C}[x]_{(x-a)} = \mathrm{ht}_{\mathbb{C}[x]}(x-a) = 1,$$

thus the ring $R = \mathbb{C}[x]_{(x-a)}$ "knows" that it is a localization of one-dimensional object $\mathbb{A}^1$.

8.2. **The dimension of algebraic sets.**

Definition 8.15. *The* **dimension** *of an algebraic set $X \subseteq \mathbb{A}^n$ is the dimension of its coordinate ring $k[X]$.*

Theorem 8.16. *Let $X \subseteq \mathbb{A}^n$ be an algebraic set, let $I = I(X) \subseteq k[x_1, \ldots, x_n]$.*

The following numbers are equal:

(a) *The dimension of X*
(b) *The maximal length of a chain of prime ideals in $k[x_1, \ldots, x_n]$ containing I*
(c) *The maximal length of a chain of irreducible algebraic sets contained in X*

Proof. One uses bijections between the following sets coming from the Hilbert Nullstellensatz:

$$\{\text{Prime ideals in } k[X]\},$$
$$\{\text{Prime ideals in } k[x_1,\dots,x_n] \text{ which contain } I(X)\},$$
$$\{\text{Irreducible algebraic subsets } Z \subset X\}.$$

□

Lemma 8.17. *If $X \subseteq Y$ are algebraic sets with Y irreducible, and $\dim(X) = \dim(Y)$, then $X = Y$.*

Proof. If $X \neq Y$, then any chain of irreducible subsets of X can be extended by adding Y at the end (since Y is irreducible!), in which case maximal chains in X and Y can never have same length. □

Example 8.18. *If Y is reducible the Lemma above does not apply: let $X = V(xy) \subset \mathbb{A}^1$, and $Y = V(x) \subset \mathbb{A}^1$. Then X consists of two irreducible components $Y = V(x)$ and $Y' = V(y)$, and $\dim(X) = \dim(Y) = 1$.*

Proposition 8.19. *Let X be algebraic set with irreducible components $Z_1,\dots,Z_n$. Then*

$$\dim(X) = \max(\dim(Z_1),\dots,\dim(Z_n)).$$

Proof. Let us use the description of dimension as a maximal length of a chain of irreducible algebraic sets contained in X:

$$X_0 \subsetneq \cdots \subsetneq X_h \subset X.$$

It is obvious that $\dim(Z_j) \leq \dim(X)$ (every chain in Z_j is also a chain in X) so that $\max(\dim(Z_1),\dots,\dim(Z_n)) \leq \dim(X)$. By definition irreducible components of X are maximal irreducible subsets in X, hence $X_h = Z_j$ for some j, this means that in fact $\dim(X) = \dim(Z_j)$, and we are done. □

Example 8.20. *Let $X = V(zx, zy) \subset k^3$. When solving the system of equations $zx = 0, zy = 0$ we get two cases: either $z = 0$ or $x = y = 0$. This means that we have*

$$X = V(z) \cup V(x, y),$$

a union of plane isomorphic to $\mathbb{A}^2$ and a line isomorphic to $\mathbb{A}^1$. According to the Proposition, $\dim(X) = 2$ (assuming that $\dim(\mathbb{A}^2) = 2$, see Theorem 8.25 below).

8.3. **Finite polynomial maps and dimension.**

Theorem 8.21. *Let $\phi : X \to Y$ be a finite surjective polynomial map of algebraic sets. Then $\dim(X) = \dim(Y)$.*

Note that we do not require k to be algebraically closed. The theorem follows from a more general result when one takes $R = k[Y]$ and $S = k[X]$:

Theorem 8.22. *Let $R \subset S$ be a integral extension. Then $\dim(R) = \dim(S)$.*

Now this theorem relies on the following algebraic result which relates primes in integral extensions.

Theorem 8.23 (Going up Theorem)**.** *Let $R \subset S$ be an integral extension.*

(a) *For any prime $P \subset R$ there exists a prime $Q \subset S$ with $P = Q \cap R$.*
(b) *If $Q \subseteq Q' \subset S$ are primes with $Q \cap R = Q' \cap R$, then $Q = Q'$.*

(c) *For any chain of primes $P_0 \subset \cdots \subset P_n$ of R and prime $Q_0 \subset S$ such that $Q_0 \cap R = P_0$ there exist primes $Q_0 \subset Q_1 \subset \cdots \subset Q_n$ in S with $P_i = Q_i \cap R$.*

Proof of Theorem 8.22. To show that $\dim(Y) \geq \dim(X)$ we take a finite strict chain of primes $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_h$ in R and use Going Up (c) to lift this to a chain $Q_0 \subset Q_1 \subset \cdots \subset Q_h$ of primes in S. This new chain is obviously strict (otherwise, if $Q_i = Q_{i+1}$, then $P_i = P_{i+1}$), and this shows $\dim(Y) \geq \dim(X)$.

To show the converse inequality $\dim(X) \geq \dim(Y)$ we take a strict chain of primes $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_h$ in S and intersect these primes with R giving a chain $P_0 \subset Q_1 \subset \cdots \subset P_h$ of primes in R; now this chain is also strict by Going Up (b) and this shows $\dim(X) \geq \dim(Y)$. □

Proof of the Going Up Theorem. Proof of part (a):

- Consider $U = R \setminus P$, and replace R and S by localizations $R_P = U^{-1}R$ and $U^{-1}S$ respectively. Then $R_P \to U^{-1}S$ is injective (localization is exact!) and integral, because every element in $U^{-1}S$ has the form $\frac{s}{u} = s \cdot \frac{1}{u}$ with $s \in S$ integral and $\frac{1}{u} \in R_P$ is unit, so $\frac{s}{u}$ is integral.
- Thus we may assume that R is local with maximal ideal P
- Now any prime ideal $Q \subset S$ which contains PS will satisfy $Q \cap R = P$ because $Q \cap R \supset P$ and P is maximal.
- Thus we only need to show that PS is a proper ideal, that is $PS \neq S$.
- We use Nakayama's Lemma applied to finitely generated R-module S (S is a integral over R, hence it is a finitely generated R-module): $PS = S \implies S = 0$, which is impossible

Proof of part (b):

- We may replace R and S with R/P and S/Q. Indeed note $R/P \to S/Q$ is still injective, so that we have a ring extension $R/P \subset S/Q$ and it is obviously integral. We thus may assume that R, S are domains and that $P = 0$, $Q = 0$ and $0 \subseteq Q' \subset S$.
- Let us show that $Q' \cap R = 0$ is impossible unless $Q' = 0$
- Take an element $s \in Q'$ and write its equation as $s^d + r_{d-1}s^{d-1} + \cdots + r_0 = 0$.
- We may assume $r_0 \neq 0$, otherwise divide the equation by s (we are in a domain!)
- Hence we may rewrite the equation $r_0 = s \cdot (\dots) \in Q' \cap R = 0$, a contradiction!

Proof of part (c):

- Using induction on n we can reduce to the case $n = 1$.
- S/Q_0 is integral extension of R/P_0
- Going Up (a) shows that there exists a prime Q_1/Q_0 of S/Q_0 lying over P_1/P_0.

□

Example 8.24. *To illustrate the power of Theorem 8.22 we look at the following familiar examples of integral extensions:*

(1) $\dim \mathbb{R} = \dim \mathbb{C} = 0$
(2) $\dim k[x]/(x^2) = \dim k = 0$
(3) $\dim \mathbb{Z}[\sqrt{2}] = \dim \mathbb{Z} = 1$
(4) $\dim k[x, y]/(y^2 - x^3) = \dim k[x] = 1$*; this tells us that $y^2 - x^3 = 0$ is a curve!*
(5) $\dim k[x, y]/(z^2 - xy) = \dim k[x, y] = 2$*; this tells us that $z^2 - xy = 0$ is a surface!*

We are ready to fulfill our expectation about dimension of the affine space.

Theorem 8.25. $\dim(\mathbb{A}^n) = n$.

Proof. We do a proof by induction on n. The cases $n = 0, 1$ already have been considered earlier.

A chain

$$0 \subsetneq \mathbb{A}^1 \subsetneq \cdots \subsetneq \mathbb{A}^n$$

of irreducible algebraic subsets has length n, so $\dim(\mathbb{A}^n) \geq n$.

We need to show that there is no chain of greater length. Consider a maximal chain of irreducible algebraic subsets:

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_{h-1} \subsetneq Z_h = \mathbb{A}^n.$$

Let $P = I(Z_{h-1}) \subset k[x_1, \ldots, x_n]$ be the ideal. Since Z_{h-1} is irreducible P is prime. Let $f \in P$ be an arbitrary non-zero element. Since P is prime, we may assume f to be irreducible (since one of the factors always will be in P). This translates to a chain

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_{h-1} \subset V(f) \subset Z_h = \mathbb{A}^n.$$

Since the original chain was assumed to be maximal, one of the new inclusions is not proper. If we had $V(f) = \mathbb{A}^n$, this would mean that $f \in I(V(f)) = I(\mathbb{A}^n) = 0$, which contradicts to our assumption $f \neq 0$. Thus we have $V(f) = Z_{h-1}$.

Let us show that $\dim(V(f)) \leq n - 1$, this will imply that $h - 1 \leq n - 1$ and $h \leq n$, so we will be able to bound the original chain.

Now to bound $\dim(V(f))$ we use Noether Normalization: there is a finite surjective polynomial map $\phi : V(f) \to \mathbb{A}^k$ and from the proof of Noether normalization it follows[1] that $k = n - 1$.

By induction hypothesis we have $\dim \mathbb{A}^{n-1} = n - 1$, so by Theorem 8.21 $\dim(V(f)) = n - 1$ as well. This means that chains of irreducible subsets of $\dim(V(f))$ have lengths bounded by $n - 1$ so that $h \leq n$, and we are done. □

9. Tensor products

Given a ring R and two R-modules M and N we will define their tensor product $M \otimes_R N$ and investigate its properties. We then discuss the geometric meaning of the construction: if $R = k$ is a field, $M = k[X]$ and $N = k[Y]$ are coordinate rings of algebraic sets X and Y, then $k[X] \otimes_k k[Y]$ is a k-algebra isomorphic to the coordinate ring of $X \times Y$.

9.1. **Tensor products of modules.**

Definition 9.1. *Let M, N, K be R-modules. A map $f : M \times N \to K$ is called R-bilinear if f is an homomorphism of R-modules in both variables, that is if*

$$f(rm_1 + m_2, n) = rf(m_1, n) + f(m_2, n), \text{ for all } r \in R,\ m_1, m_2 \in M,\ n \in N$$

and

$$f(m, rn_1 + n_2) = rf(m, n_1) + f(m, n_2), \text{ for all } r \in R,\ n_1, n_2 \in N,\ m \in M.$$

Let M, N be two R-modules. Let $F(M, N)$ be the free R-module with basis given by symbols $m \otimes n$ for $m \in M$, $n \in N$:

$$F(M, N) = \bigoplus_{m \in M, n \in N} R \cdot m \otimes n.$$

The R-module is very large, e.g. if M or N is uncountable as a set, then $F(M, N)$ has an uncountable basis.

[1]Indeeed, $k[V(f)] = k[x_1, \ldots, x_n]/(f)$ is generated by $x_1, \ldots, x_n$, and since $x_1, \ldots, x_n$ are algebraically dependent the first step of the inductive proof of Noether normalization will present $k[V(f)]$ as an integral extension of a polynomial ring $k[y_1, \ldots, y_{n-1}]$.

Definition 9.2. *The tensor product $M \otimes_R N$ is the R-module defined as a quotient*

$$F(M,N)/B(M,N)$$

with $B(M,N)$ submodule generated by relations:

$$\begin{aligned}(m_1 + rm_2) \otimes n - m_1 \otimes n - rm_2 \otimes n,\\ m \otimes (n_1 + rn_2) - m \otimes n_1 - rm \otimes n_2.\end{aligned} \tag{9.1}$$

Thus elements of $M \otimes_R N$ have the form

$$\sum_{i=1}^{k} m_i \otimes n_i$$

for $m_i \in M$, $n_i \in N$, and there are relations

$$\begin{aligned}(m_1 + rm_2) \otimes n = m_1 \otimes n + rm_2 \otimes n,\\ m \otimes (n_1 + rn_2) = m \otimes n_1 + rm \otimes n_2,\end{aligned} \tag{9.2}$$

for example

$$(2m) \otimes n = m \otimes n + m \otimes n = m \otimes (2n).$$

Elements of the kind $m \otimes n$ are called decomposable tensors. By construction decomposable tensors generate $M \otimes_R N$. In general there is no simple way to tell whether two elements of a tensor product are equal.

If the base ring R is fixed, we simply write $M \otimes N$ for $M \otimes_R N$. The definition of a tensor product $M \otimes_R N$ reminds the definition of a bilinear map $M \times N \to K$. The following Theorem tells that in fact the tensor product is "the smallest" R-module which receives an R-bilinear map from $M \times N$.

Theorem 9.3. *There is an R-bilinear map $\epsilon : M \times N \to M \otimes_R N$ defined as $\epsilon(m,n) = m \otimes n$. Furthermore, for any R-bilinear map $\alpha : M \times N \to K$ there is a unique R-module homomorphism $\overline{\alpha} : M \otimes_R N$ satisfying $\overline{\alpha} \circ \epsilon = \alpha$:*

$$\begin{array}{ccc} M \times N & \xrightarrow{\epsilon} & M \otimes_R N \\ {\scriptstyle\alpha}\downarrow & \swarrow_{\overline{\alpha}} & \\ K & & \end{array}$$

Thus maybe we can't really say what elements of $M \otimes_R N$ are, but the Theorem gives us a way to construct R-module homomorphisms $M \otimes_R N \to K$ for any R-module K.

Proof. It follows from relations defining the tensor product $M \otimes_R N$ that ϵ is bilinear.

Given a bilinear map $\alpha : M \times N \to K$ we first define an R-module homomorphism

$$\widetilde{\alpha} : F(M \times N) \to K$$

Since $F(M \times N)$ is a free R-module we may send basis elements anywhere we want, so we define $\widetilde{\alpha}(m \otimes n) = \alpha(m,n)$.

Now because α is bilinear, the submodule (9.1) of relations $B(M,N) \subset F(M,N)$ is annihilated by $\widetilde{\alpha}$:

$$\widetilde{\alpha}\left((m_1 + rm_2) \otimes n - m_1 \otimes n + rm_2 \otimes n\right) = \alpha(m_1 + rm_2, n) - \alpha(m_1, n) - r\alpha(m_2, n) = 0$$
$$\widetilde{\alpha}\left(m \otimes (n_1 + rn_2) - m \otimes n_1 + rm \otimes n_2\right) = \alpha(m, n_1 + rn_2) - \alpha(m, n_1) - r\alpha(m, n_2) = 0.$$

It follows that $\widetilde{\alpha}$ descends to give a R-homomorphism $\overline{\alpha} : M \otimes_R N \to K$ defined as

$$\overline{\alpha}(\sum_{i=1}^{k} m_i \otimes n_i) = \sum_{i=1}^{k} \alpha(m_i, n_i).$$

We see that $\overline{\alpha} \circ \epsilon = \alpha$.

Uniqueness of $\overline{\alpha}$ follows the fact that its values on decomposable tensors $m \otimes n$ is determined by α, and decomposable tensors span $M \otimes_R N$. □

Proposition 9.4. *If $R = k$, a field, and V and W are k-vector spaces with bases $V = \langle e_i \rangle_{i \in I}$, $W = \langle f_j \rangle_{j \in J}$, then $V \otimes_k W$ is a k-vector space with basis $e_i \otimes f_j$, $i \in I$, $j \in J$.*

We see that for vector spaces $\dim_k(V \otimes W) = \dim_k(V) \cdot \dim_k(W)$ in the case dimensions of V and W are finite.

Proof. By construction the elements $e_i \otimes f_j$ generate the k-vector space $V \otimes W$. We need to show that these elements are linearly independent.

For every $i \in I$, $j \in J$ consider k-bilinear maps

$$\pi_{i,j} : V \times W \to k$$
$$\left(\sum_i a_i e_i, \sum_j b_j f_j\right) \mapsto a_i b_j.$$

Using Theorem 9.3 these k-bilinear maps induce k-module homomorphisms $\overline{\pi}_{i,j}$ satisfying:

$$\overline{\pi}_{i,j}\left((\sum_i a_i e_i) \otimes (\sum_j b_j f_j)\right) = a_i b_j \in k, \tag{9.3}$$

and

$$\overline{\pi}_{i,j}\left(\sum_{i,j} a_{i,j} e_i \otimes f_j\right) = a_{ij} \in k.$$

Existence of such coordinate homomorphisms implies linear independence of the spanning set:

$$\sum_{i,j} a_{ij} e_i \otimes f_j = 0 \implies a_{ij} = \overline{\pi}_{i,j}(\sum_{i,j} a_{ij} e_i \otimes f_j) = 0 \text{ for all } i, j.$$

□

Example 9.5. *Let $R = k$, a field, and let $M = k[x]$, $N = k[y]$, polynomial rings in one variable considered as k-vector spaces. Applying the Proposition above to the bases $k[x] = \langle 1, x, x^2, \dots \rangle$, and $k[y] = \langle 1, y, y^2, \dots \rangle$ we obtain a k-basis for $k[x] \otimes_k k[y]$:*

$$x^i \otimes y^j,\ i \geq 0, j \geq 0.$$

Thus as k-vector space $k[x] \otimes_k k[y]$ is isomorphic to $k[x, y]$. We'll see later that this is in fact an isomorphisms of k-algebras (at the moment tensor product does not have an algebra structure).

Example 9.6. *Note how tensor product of modules depends on the base ring: $k[x] \otimes_k k[x] \simeq k[x_1, x_2]$ but $k[x] \otimes_{k[x]} k[x] \simeq k[x]$, see (1) in Proposition 9.7 below. Tensoring over bigger ring $k[x]$ rather than over k gives more relations among the tensors, and yields a smaller module. For instance $x \otimes 1$ and $1 \otimes x$ are distinct elements in $k[x] \otimes_k k[x]$, but coincide in $k[x] \otimes_{k[x]} k[x]$.*

Proposition 9.7. *We have the following natural isomorphisms of R-modules:*

(1) $R \otimes_R M \simeq M$
(2) $M \otimes_R N \simeq N \otimes_R M$
(3) $(M_1 \otimes_R M_2) \otimes_R M_3 \simeq M_1 \otimes_R (M_2 \otimes_R M_3)$
(4) $(M_1 \oplus M_2) \otimes_R N \simeq (M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$.

Proof. All these properties are proved in the same way: one constructs R-module homomorphisms in both directions using Theorem 9.3 and then checks that both compositions are identities. Since decomposable tensors generate tensor products it suffices to check whether compositions are identities on decomposable tensors.

I prove (1) while (2), (3) and (4) are done similarly. Let us construct R-module homomorphisms

$$\phi : R \otimes_R M \to M$$
$$\psi : M \to R \otimes_R M.$$

The first one is defined by the rule $\phi(r \otimes m) = rm$, this is well-defined by Theorem 9.3, since the RHS is bilinear in the two arguments. The second homomorphism is defined by $\psi(m) = 1 \otimes m$. This is well-defined since the RHS is linear in m.

We compute the two compositions:

$$\phi\psi(m) = \phi(1 \otimes m) = m$$
$$\psi\phi(r \otimes m) = \psi(rm) = 1 \otimes rm = r \otimes m,$$

these are identities, and we are done. □

Proposition 9.8. *If $f_1 : M_1 \to N_1$, $f_2 : M_2 \to N_2$ are R-module homomorphisms, then there is an R-module homomorphism $f_1 \otimes f_2 : M_1 \otimes M_2 \to N_1 \otimes N_2$ defined via $(f_1 \otimes f_2)(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$.*

In particular for every $f : M \to N$ and K there is an R-module homomorphism $f \otimes id : M \otimes K \to N \otimes K$.

Proof. One of the problems in the Homework assignment. □

9.2. **Extension of scalars and tensor products of algebras.**

Proposition 9.9. *Let R be a ring, M an R-module and S an R-algebra. Then the R-module $S \otimes_R M$ has a structure of S-module defined by*

$$t \cdot (\sum_{i=1}^{k} s_i \otimes m_i) := \sum_{i=1}^{k} (ts_i) \otimes m_i.$$

This construction is called extension of scalars: we make R-module M into an S-module in the most efficient way.

Proof. For every t we define a map m_t:

$$m_t : S \otimes_R M \to S \otimes_R M$$
$$s \otimes m \mapsto ts \otimes m$$

Because the RHS is bilinear in s and m this map gives a well-defined homomorphism of R-modules by Theorem 9.3. The axioms for $S \otimes_R M$ to be an S-module are encoded as:

$$m_1 = id$$
$$m_{t_1 t_2} = m_{t_1} \circ m_{t_2}$$
$$m_{t_1 + t_2} = m_{t_1} + m_{t_2},$$

and these follow immediately from the construction of m_t. □

Example 9.10. *We take $R = \mathbb{R}$, $M = \mathbb{R}[x]$, considered as $\mathbb{R}$-module, and $S = \mathbb{C}$, considered as $\mathbb{R}$-algebra. Let us consider the $\mathbb{C}$-algebra $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[x]$. As an $\mathbb{R}$-vector space $\mathbb{C}$ has a basis $1, i$, and $\mathbb{R}[x]$ has a basis $1, x, x^2, \dots$. Thus using Proposition 9.4 we find an $\mathbb{R}$-basis:*

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[x] = \langle 1 \otimes 1, i \otimes 1, 1 \otimes x, i \otimes x, 1 \otimes x^2, i \otimes x^2, \dots \rangle.$$

In other words elements of this module can be identified with

$$f(x) + ig(x),\ f(x), g(x) \in \mathbb{R}[x].$$

One checks that the $\mathbb{C}$-action is what it should be giving an isomorphism of $\mathbb{C}$-vector spaces

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[x] \simeq \mathbb{C}[x].$$

Proposition 9.11. *Let R be a ring and S and T be R-algebras. Then the R-module $S \otimes T$ has a structure of R-algebra with multiplication defined as*

$$\left(\sum_{i=1}^{k} s_i \otimes t_i\right) \cdot \left(\sum_{j=1}^{l} s'_j \otimes t'_j\right) = \sum_{i,j} s_i s'_j \otimes t_i t'_j.$$

Proof. The proof is similar to that of Proposition 9.9 but a bit more involved. □

Example 9.12. *Consider $S = k[x]$ and $T = k[y]$ as k-algebras. Let us consider $k[x] \otimes_k k[y]$ as a k-algebra. In Example 9.5 we constructed a k-module isomorphism*

$$k[x] \otimes_k k[y] \simeq k[x, y]$$
$$x^i \otimes x^j \mapsto x^i y^j$$

We check that this map is actually an isomorphism of k-algebras. For that we need to check that multiplication of the basis elements on both sides is respected by the map. This follows from how the ring structure is defined on the tensor product in Proposition 9.11:

$$(x^{i_1} \otimes y^{j_1}) \cdot (x^{i_2} \otimes y^{j_2}) = x^{i_1+i_2} \otimes y^{j_1+j_2}.$$

9.3. **Products of algebraic sets.**

Lemma 9.13. *Let $X \subset \mathbb{A}^n$ be algebraic subset with ideal $I(X) \subset k[x_1, \dots, x_n]$. Then $X \times \mathbb{A}^1 \subset \mathbb{A}^{n+1}$ is an algebraic subset with ideal $I(X)[y] \subset k[x_1, \dots, x_n, y]$, that is the ideal generated by $I(X)$ in $k[x_1, \dots, x_n, y]$.*

Proof. We start by noticing that the vanishing locus of $I(X)$ considered as a subset of $k[x_1, \dots, x_n, y]$ is $X \times \mathbb{A}^1$, as the there are no restrictions in the y direction. To find the ideal of $X \times \mathbb{A}^1$ we consider a polynomial

$$h(x_1, \dots, x_n, y) = \sum_{i=0}^{k} a_i(x_1, \dots, x_n) y^i \in k[x_1, \dots, x_n, y]$$

and notice that h vanishes at $X \times \mathbb{A}^n$ if and only if for all $(x_1, \dots, x_n) \in X$ the polynomial

$$h(x_1, \dots, x_n, y) \in k[y]$$

vanishes on $\mathbb{A}^1$, that is its coefficients $a_i(x_1, \dots, x_n)$ are all zero. It follows that $h \in I(X \times \mathbb{A}^1)$ if and only if $h \in I(X)[y]$. □

Theorem 9.14. *Let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ be algebraic sets with ideals $I(X) \subset k[\mathbb{A}^n]$, $I(Y) \subset k[\mathbb{A}^m]$. Then $X \times Y \subset \mathbb{A}^{n+m}$ is an algebraic set and $I(X \times Y) = I(X)k[\mathbb{A}^{n+m}] + I(Y)k[\mathbb{A}^{n+m}]$.*

Proof. Denote the coordinates on $\mathbb{A}^{n+m} = \mathbb{A}^n \times \mathbb{A}^m$ be $x_1, \ldots, x_n, y_1, \ldots, y_m$.

We note that $X \times Y$ is the intersection of two "cylinders":

$$X \times Y = X \times \mathbb{A}^m \cap \mathbb{A}^n \times Y.$$

Using Lemma 9.13 and easy induction we see that both of the two cylinders above are algebraic, and hence their intersection is also algebraic. For the ideal of $X \times Y$ we have

$$\begin{aligned} I(X \times Y) &= I(X \times \mathbb{A}^m) + I(\mathbb{A}^n \times Y) = \\ &= I(X)[y_1, \ldots, y_m] + I(Y)[x_1, \ldots, x_m] = \\ &= I(X)k[\mathbb{A}^{n+m}] + I(Y)k[\mathbb{A}^{n+m}]. \end{aligned}$$

□

Theorem 9.15. *The coordinate algebra of $X \times Y$ is isomorphic to $k[X] \otimes_k k[Y]$.*

Proof. Let $X \subset \mathbb{A}^n$ with coordinates $x_1, \ldots, x_n$ and $Y \subset \mathbb{A}^m$ with coordinates $y_1, \ldots, y_m$. By Theorem 9.14 we have

$$k[X \times Y] = k[\mathbb{A}^{n+m}]/I(X \times Y) = k[\mathbb{A}^{n+m}]/(I(X)k[\mathbb{A}^{n+m}] + I(X)k[\mathbb{A}^{n+m}]).$$

The proof is finished using identification $k[\mathbb{A}^{n+m}] \simeq k[\mathbb{A}^n] \otimes k[\mathbb{A}^m]$ (Example 9.12) and Lemma 9.16 below:

$$\begin{aligned} k[\mathbb{A}^{n+m}]/(I(X)k[\mathbb{A}^{n+m}] + I(X)k[\mathbb{A}^{n+m}]) &\simeq (k[\mathbb{A}^n] \otimes k[\mathbb{A}^m])/(I(X) \otimes k[\mathbb{A}^m] + k[\mathbb{A}^n] \otimes I(Y)) \simeq \\ &\simeq k[\mathbb{A}^n]/I(X) \otimes k[\mathbb{A}^m]/I(Y) \\ &\simeq k[X] \otimes k[Y]. \end{aligned}$$

□

Lemma 9.16. *Let $I_1 \subset R_1$, $I_2 \subset R_2$ be ideals in k-algebras R_1, R_2. Then there is a natural isomorphism of k-algebras*

$$R_1/I_1 \otimes_k R_2/I_2 \simeq (R_1 \otimes_k R_2)/(I_1 \otimes R_2 + R_1 \otimes I_2).$$

Proof. We construct k-algebra homomorphisms

$$\begin{aligned} R_1/I_1 \otimes_k R_2/I_2 &\to (R_1 \otimes_k R_2)/(I_1 \otimes R_2 + R_1 \otimes I_2) \\ \overline{r_1} \otimes \overline{r_2} &\mapsto \overline{r_1 \otimes r_2} \end{aligned}$$

and

$$\begin{aligned} (R_1 \otimes_k R_2)/(I_1 \otimes R_2 + R_1 \otimes I_2) &\to R_1/I_1 \otimes_k R_2/I_2 \\ \overline{r_1 \otimes r_2} &\mapsto \overline{r_1} \otimes \overline{r_2}. \end{aligned}$$

It is easy to see that these are well-defined and mutually inverse. □

Proposition 9.17. *Dimension of $X \times Y$ is* $\dim(X) + \dim(Y)$.

Proof. We apply Noether Normalization to X and Y to get finite surjective polynomial maps $\phi : X \to \mathbb{A}^n$, $\psi : Y \to \mathbb{A}^m$. Consider the map on the product:

$$\begin{aligned} \phi \times \psi : X \times Y &\to \mathbb{A}^{n+m} \\ (x, y) &\mapsto (\phi(x), \psi(y)). \end{aligned}$$

It is not hard to check that this polynomial map is also finite and surjective, so that

$$\dim(X \times Y) = n + m = \dim(X) + \dim(Y).$$

□

Remark 9.18. *Zariski Cancellation Problem asks about the following: if X is affine n-dimensional variety such that $X \times \mathbb{A}^1$ is isomorphic to $\mathbb{A}^{n+1}$, is it true that X is isomorphic to $\mathbb{A}^n$? This is not known for $n \geq 3$, and known to be false if characteristic of the base field k is positive.*

10. Regular rings

A point $P \in X$ of an algebraic set X can be a singular or non-singular. For example for an algebraic curve $X = V(f)$, $f \in k[x, y]$ a point $P \in X$ is nonsingular if and only if the partial derivatives $\frac{\partial f}{\partial x}(P)$ and $\frac{\partial f}{\partial y}(P)$ are not both equal to zero.

To define the concept in general we first study the algebraic side - regular local rings. These are defined in terms of the tangent space to a ring: from the algebraic perspective a point is singular if the tangent space at this point has dimension bigger than the Krull dimension of the ring. We then relate the algebraic definition to non-vanishing of the Jacobian matrix of derivatives.

10.1. **Tangent spaces and regular local rings.** Let R be a ring, and and let $m \subset R$ be a maximal ideal with quotient field $k = R/m$. Consider an R-module $V = m/m^2$ with an obvious action $r \cdot \overline{x} = \overline{rx}$. Since m annihilates V, V is an R/m-module, i.e. a vector space over k.

Definition 10.1. *The k-vector space m/m^2 is called the cotangent space to R at m, and the dual k-vector space $T_{m,R} = (m/m^2)^* = \operatorname{Hom}(m/m^2, k)$ is called the tangent space to R at m.*

Theorem 10.2. *Let (R, m) be a local Noetherian ring. Then*

1. $\dim T_{m,R} =$ *minimal number of generators of* $m \subset R$
2. $\dim T_{m,R} \geq \dim R$

Proof. 1. Let $k = R/m$, $n = \dim T_{m,R} = \dim_k m/m^2$. Then clearly m can not be generated by less than n elements. We will now show that m can be generated by n elements.

We apply Theorem 4.9 (c) (Nakayama's Lemma) to R-module $M = m$ and ideal $I = m$: pick a k-basis $\overline{f_1}, \ldots, \overline{f_n}$ of m/m^2. These elements are also generators of m/m^2 as R-module. By Theorem 4.9 (c) their preimages $f_1, \ldots, f_n \in m$ generate m as R-module. (Here we used the assumption that R is Noetherian: Nakayama's Lemma is a statement about Noetherian rings.)

2. Let $n = \dim T_{m,R}$. Part (1) implies that m is generated by n elements $f_1, \ldots, f_n \in m$. Now by Krull's principal ideal theorem (Theorem 10.3 below) applied inductively we get

$$\dim R/(f_1, \ldots, f_j) \geq \dim R - j.$$

In particular, for $j = n$ we get

$$0 = \dim R/m \geq \dim R - n$$

so that $n = \dim T_{m,R} \geq \dim R$. □

Theorem 10.3 (Krull's principal ideal theorem, Algebraic form)**.** *Let R be an a Noetherian ring, and let $f \in R$. Then exactly one of the following conditions holds:*

1. $R/(f) = 0$ *and f is a unit in R*
2. $\dim(R/(f)) = \dim(R)$*, and f is a zero-divisor in R*
3. $\dim(R/(f)) = \dim(R) - 1$

Corollary 10.4 (Krull's principal ideal theorem, Geometric form)**.** *Let X be an algebraic set, $f \in k[X]$, and $Y = V(f) \subset X$, the zero locus of the function f. Then* $\dim(Y)$ *is equal to* $\dim(X) - 1$ *or* $\dim(X)$*, unless Y is an empty set.*

Example 10.5. *$X = V(xy) \subset \mathbb{A}^2$ has dimension one. The three possibilities of the Theorem are realized as follows:*

(1) $f = 1$, $V(f) = \emptyset$
(2) $f = x$, $V(f) = V(x) \subset V(xy)$ *have same dimension one*
(3) $f = x^2 - 4$, $V(f)$ *consists of two points* $(2, 0)$ *and* $(-2, 0)$ *and has dimension zero which is one less than dimension of* X

Definition 10.6. *A local ring* (R, m) *is called* **regular** *if* $\dim R = \dim T_{m,R}$.

Example 10.7. *We consider three local rings:* $\mathbb{Z}_{(7)}$, k *(a field) and* $k[x]/(x^2)$ *and investigate which ones among these are regular.*

ring R	m	$\dim(R)$	$\dim(T_{m,R})$	*regular?*
$\mathbb{Z}_{(7)}$	$(\frac{7}{1})$	1	1	*yes*
k	(0)	0	0	*yes*
$k[x]/(x^2)$	(x)	0	1	*no*

10.2. **Tangent spaces and regular rings in the non-local case.**

Definition 10.8. *A ring* R *is called* **regular** *if for every maximal* $m \subset R$ *the localization* R_m *is regular.*

For example $R = \mathbb{Z}$ is a regular ring, since all its localizations at maximal ideals $\mathbb{Z}_{(p)}$ are regular local rings.

Lemma 10.9. *Let* (R_m, m_m) *be localization of a ring* R *at a maximal ideal* $m \subset R$. *Then there are natural isomorphisms* $k = R_m/m_m \simeq R/m$ *as fields, and* $m_m/m_m^2 \simeq m/m^2$ *as* k*-vector spaces.*

Proof. We recall that in the Chapter on localization we have proved that for $U \subset R$ a multiplicative set and $N \subset M$ modules we have $U^{-1}(M/N) = U^{-1}M/U^{-1}N$ as $U^{-1}R$-modules. We apply this to $U = R\backslash m$ to obtain

$$R_m/m_m = (R/m)_m = k$$
$$m_m/m_m^2 = (m/m^2)_m = m/m^2.$$

The localization in the second step does not change the modules as these are $k = R/m$-modules, so the complement to m already acts by invertible elements. □

Proposition 10.10. *The polynomial ring* $R = k[x_1, \ldots, x_n]$ *is a regular ring.*

Proof. To simplify the argument we give a proof in the case when k is algebraically closed.

We know that $\dim(R) = n$. Using Theorem 10.2 it suffices to check that every maximal ideal is generated by n elements.

By a corollary from the Hilbert Nullstellensatz we know that maximal ideals in R have the form

$$m = m_a = (x_1 - a_1, \ldots, x_n - a_n),\ a \in k^n$$

and the result follows. □

Remark 10.11. *Let us investigate the tangent space to* $k[x_1, \ldots, x_n]$ *at* $m = m_a$, $a \in k^n$ *in some detail.*

Let $y_i = x_i - a_i$. *We have*

$$f \in m \iff f(y_1, \ldots, y_n) = \sum_{i=1}^{n} A_i y_i + \sum_{i,j=1}^{n} B_{ij} y_i y_j + \textit{higher order terms}$$

$$f \in m^2 \iff f(y_1, \ldots, y_n) = \sum_{i,j=1}^{n} B_{ij} y_i y_j + \textit{higher order terms.}$$

Hence m/m^2 consists of $A_1\overline{y_1}+\cdots+A_n\overline{y_n}$, $A_i \in k$, and has dimension n. We will write $dx_i = \overline{y_i}$, so that the dual space $(m/m^2)^*$ is spanned by "directional derivatives" $\frac{\partial}{\partial x_i}$.

The meaning of this notation can be explained as follows: elements of the tangent space k-linear maps from m/m^2 to k, and $\frac{\partial}{\partial x_i}$ correspond to maps:

$$f \in m/m^2 \mapsto \frac{\partial}{\partial x_i}(f) = \frac{\partial f}{\partial x_i}(a).$$

10.3. **Nonsingular algebraic sets.**

Definition 10.12. *An algebraic set X is called* nonsingular *at a point P if the local ring $k[X]_{m_P}$ is regular.*

Definition 10.13. *An algebraic set X is called* nonsingular *if it is nonsingular at every point $P \in X$, or equivalently, if the ring $k[X]$ is regular.*

To make sense of these definitions we start with explaining the geometric meaning of the tangent space.

Proposition 10.14. *Let $X \subset \mathbb{A}^n$ be an algebraic set with ideal $I(X) = \langle f_1, \dots, f_r\rangle$. The tangent space to X at $a \in X$ can be identified with the following vector subspace of k^n:*

$$\{(\alpha_1, \dots, \alpha_n) \in k^n \mid \frac{\partial f_i(a)}{\partial x_1}\alpha_1 + \cdots + \frac{\partial f_i(a)}{\partial x_n}\alpha_n = 0 \ \ \forall i = 1 \dots r\}.$$

Proof. We consider m/m^2, and then take the dual vector space.

We change the coordinates to $y_j = x_j - a_j$ and write Taylor expansions for every f_i:

$$f_i(y_1, \dots, y_n) = 0 + \frac{\partial f_i(a)}{\partial x_1}y_1 + \cdots + \frac{\partial f_i(a)}{\partial x_n}y_n + O(y^2).$$

Computing $\overline{m_a}/\overline{m_a}^2 = (y_1, \dots, y_n)/((y_iy_j)_{i,j=1}^n + I(X))$ yields a quotient k-vector space

$$\frac{kdy_1 \oplus \cdots \oplus kdy_n}{(\frac{\partial f_i(a)}{\partial x_1}dy_1 + \cdots + \frac{\partial f_i(a)}{\partial x_n}dy_n)_{i=1}^r} = V/L$$

and the dual space is the one we need:

$$(V/L)^* = L^\perp = \{(\alpha_1, \dots, \alpha_n) : \sum_{i=1}^n \frac{\partial f_j(a)}{\partial x_i}\alpha_i = 0 \text{ for all } j\} \subset V^* = k^n.$$

□

Example 10.15. *Let $X = V(f) \subset \mathbb{A}^n$, i.e. X is given by one equation*

$$f(x_1, \dots, x_n) = 0.$$

Assume that X is non-empty. The tangent space to X at $a \in X$ has the form

$$T_{a,X} = \{(\alpha_1, \dots, \alpha_n) \in k^n : \frac{\partial f(a)}{\partial x_1}\alpha_1 + \cdots + \frac{\partial f(a)}{\partial x_n}\alpha_n = 0\} \subset k^n.$$

Thus there are two cases: $T_{a,X} = k^n$ (when all partial derivatives of f are zero at a), or $T_{a,X}$ has dimension $n-1$ (when at least one of the partial derivatives of f is not zero at a).

By Krull's Principal Ideal Theorem (Theorem 10.3) we have $\dim X = \dim(R_X)_m = n-1$ for every maximal ideal $m \subset R_X$. It follows from the description of the tangent space $T_{a,X}$ given above that X is nonsingular if and only if for every $a \in X$ the derivatives $\partial f/\partial x_i(a)$ do not vanish simultaneously.

Example 10.16. *Computing the partial derivatives we see that $y = x^2$ is a nonsingular curve, and $y^2 = x^3$ is singular at $(0, 0)$.*

Proposition 10.17 (Jacobian criterion)**.** *Let $X = V(f_1, \ldots, f_r) \subset \mathbb{A}^n$ be an algebraic set. If the Jacobian matrix*

$$J = (\frac{\partial f_i}{\partial x_j}(a))_{i=1\ldots r, j=1\ldots n}$$

has rank r for every $a \in X$, then X is non-singular of dimension $n - r$.

Proof. Note that if $X \neq \emptyset$, then by Krull's principal ideal theorem we have $\dim(X) \geq n-r$. We've seen that the tangent space $T_{a,X}$ to X at a is given by the kernel of $J : k^n \to k^r$. Since J has rank r, the kernel has dimension $n - r$. Thus we have

$$\dim T_{a,X} = n - r \leq \dim X$$

and the converse inequality holds always. □