Commutative algebra

komalg1u0um17em

Lecturer: Péter Frenkel*

2022/2023/2

1 First lecture

1.1 Motivation

We study commutative rings, so during the course every ring is commutative, with identity, unless otherwise specified. Three main motivators are algebraic number theory, i.e. the study of $\mathbb{Z}$: introduces quotients e.g. $\mathbb{Z}_m$ for Diophantine equations, and extensions of $\mathbb{Z}$ are studied, e.g. $|K:\mathbb{Q}|<\infty$ a finite extension.

Definition 1.1. $\alpha \in K$ is an algebraic integer, if it satisfies a monic polinomial, i.e. $\alpha^n + \sum_0^{n-1} c_i \alpha^i = 0$. $\mathcal{O}_K$ denotes the ring of algebraic integers (proof later).

Specifically it contains $\mathbb{Z}$, and we study it's number theory, and this provides information about $\mathbb{Z}$ itself.

Example 1.2. $x^3+y^3=z^3$, we want to study this in $\mathbb{Z}[\omega]$, where ω is a primitive third root of unity (Eulerian integers). Here $K=\mathbb{Q}[\omega]$. Now we can write $x^3=z^3-y^3$, and we can factor this as $(z-y)(z-\omega y)(z-\omega^2 y)$.

Another motivator is invariant theory. X is "some sort of space", a set with some structure, a vector space, a topologial space, algebraic variety or similar, and we have a group G acting on X by symmetries. Consider a function $f: X \to R$, which are invariant under this group action, i.e. $f^g = f$, meaning $f(gx)=f(x)$ for all $g \in G$. We want to consider all invariant functions, which will again form a ring (under pointwise operations). If we have no structure on X, these are just functions defined on the orbits, not very interesting, but if we only allow structure preserving functions, this becomes rather nontrivial.

Example 1.3. Suppose we have a vector space over a field K, for example $X=K^n$ (suppose $|K|=\infty$), and take polynomial functions $X \to K$, denoted $K[x_1,\dots,x_n]$. Consider the group S_n acting by permutation of variables. We denote the invariant functions by $K[x_1,\dots,x_n]^{S_n} \leq K[x_1,\dots,x_n]$, these are polynomials invariant under a permutation of coordinates, i.e. symmteric polynomials. This will again be a polynomial ring generated by the elementary symmetric polynomials.

The third big motivator is algebraic geometry! It is the study of point-sets defined by polynomial equations. Take a field extension $L|K$, and look at the affine space L^n. We take a set of polynomials $\mathcal{F} \subset K[x_1,\dots,x_n]$, and define $V_L(\mathcal{F}) := \{\alpha \in L^n | f(\alpha)=0 \ \forall f \in \mathcal{F}\}$. Conversly,one can look at a subset $Y \subset L^n$, and consider $I_K(Y) := \{f \in K[x_1\dots,x_n] | \forall \alpha \in Y \ f(\alpha)=0\}$, this is clearly an ideal in $K[x_1\dots,x_n] =: A$. Clearly $A/I_K(Y) = \{f|_Y : f \in A\}$.
An important special case is when $L=K$, an algebraically closed field.

Proposition 1.4. *These sets $V_L(\mathcal{F})$ are the closed sets of a topology, the K-Zariski topology on L^n.*

Proof. Firstly we need that $\emptyset$ is closed, this is true, it is the zero locus of the constant 1 polynomial.
Secondly L^n is closed, as it is the zero set of the constant 0 polynomial, or the empty polynomial set.*
We need that arbitrary intersections of closed sets is closed as well. $\cap V_L(F_i) = V_L(\cup F_i)$ is clear, and we are done.
Finally, the union of two closed sets has to be closed. $V_L(F) \cup V_L(G) = V_L(FG)$, where $FG := \{fg : f \in F, g \in G\}$. The $\subset$ containment is easy, if F vanishes at some point, all products of the form fg also vanish, similarly for G The other direction is trickier. Assume $fg(\alpha) = 0$ forall $fg \in FG$, but there exists f and g which don't vanish at a point, but this contradicts our assumption, since the product of two nonzero numbers is nonzero, so it does not vanish in FG. □

Let's restrict ourselves to the algebraically closed case, and take an affine algebraic (i.e. Zariski closed) set $X \subset K^n$.

Definition 1.5. The coordinate ring of X is defined as before $A/I(X) =: \mathcal{A}_X$.

This is the K-algebra generated by the restrictions of the coordinate functions of K^n to X.
If we have $L|K$ an extension, and $F \subset A := K[x_1, \ldots, x_n]$, we see, that $V_L(F) = V_L((F)) = V_L(\sqrt{(F)})$.

Definition 1.6. The radical of an ideal $I \subset A$ is defined as $\sqrt{I} := \{\alpha \in A : \exists k : \alpha^k \in I\}$. The nilradical of A is defined as $N(A) := \sqrt{(0)}$, this is precisely the set of nilpotent elements.

Proposition 1.7. *The radical of an ideal is again an ideal.*

Remark 1.8. This is not true in noncommutative rings! The sum of two nilpotent matrices is not neccesarily nilpotent.

Proof. $0 \in \sqrt{I}$ is clear. If $a \in A, b \in \sqrt{I}$, then $ab \in \sqrt{I}$, since we have a k such that $b^k \in I$, thus $(ab)^k \in I$.
The only nontrivial bit, is that the radical is closed under addition. Suppose $a, b \in \sqrt{I}$ we have an exponent such that $a^k \in I, b^l \in I$, expand $(a+b)^{k+l-1} = \sum_{i+j=k+l-1} \binom{k+l-1}{i} a^i b^j$, and we see that each term is in I, since either $i \geq k$ or $j \geq l$. □

For the second equality, we only need, that if $f(\alpha)^k = 0$, then $f(\alpha) = 0$.

1.2 A more formal introduction

Definition 1.9. A subring always means a subring containing the identity. In particular the identity element of a ring, and its subring is always the same. Also ring homomorphisms should respect the identity element!

Example 1.10. In $\mathbb{Z}_6$ the subset $\{0, 3\}$ is not considered a subring

Definition 1.11. If A is a ring, and $a \in A$, we call a a zero-divizor iff there exists $0 \neq b \in A$ such that $ab = 0$. Inparticular we consider zero a zero divisor in any ring except the trivial.

Definition 1.12. A ring is a domanin iff it has precisely one zero divizor. In particular the trivial ring is not a domain.
A is a field, if $A \setminus \{0\}$ is a group w.r.t. multiplication.

*either one is fine

Fact 1.13. *Every field is a domain.*

Definition 1.14. $I \triangleleft A$, I is called maximal iff $I \neq (1)$ and $\nexists I \subsetneq J \subsetneq A$, with $J \triangleleft A$.

Proposition 1.15. *An ideal $I \triangleleft A$ is maximal iff A/I is a field.*

Proof. I being maximal is equivalent to having precisely two ideals in the interval $[I, A]$, this is again equivalent to the quotient A/I having exactly two ideals, which are clearly the fields. □

Maximal ideals are not functorial unfortunately.

Example 1.16. $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $\mathbb{Q}$ only has one maximal ideal, (0), but the preimage has more maximal ideals.

To correct this, we wish to consider ideals, the quotient of which are domains, since a subring of a domain is again a domain.

Definition 1.17. A is a ring with $P \triangleleft A$. P is called prime, iff $P \neq (1)$, and if $a, b \in A$, $ab \in P$ implies $a \in P$ or $b \in P$.

Example 1.18. $A = \mathbb{Z}$, the ideals are of the form (n). This ideal is prime if $n \neq 1$, and we need $n|ab$ to imply $n|a$ or $n|b$, i.e. $n = 0$ or a prime number.

Remark 1.19. (0) is prime iff A is a domain.

Proposition 1.20. *I is prime iff A/I is a domain.*

Proof. $I \neq (1)$ is equivalent to $|A/IW| \geq 2$. The other condition is equivalent to saying that A/I has no nonzero zero divizors, and this reproduces the definition of a domain. □

Corrolary 1.21. *Every maximal ideal is prime.*

Proposition 1.22. *$\phi : A \to B$ is a ring homomorphism, and $P \triangleleft B$ is a prime ideal, then $\phi^{-1}(B)$ is a prime ideal in A.*

Proof. The preimage of an ideal is always an ideal, trivial homework. Take the quitoent $A/\phi^{-1}(P) \leq B/P$, since $A \xrightarrow{\phi} B \xrightarrow{\nu} B/P$, and $ker\nu = P$, the kernel of the composition, denoted by ψ will be $\phi^{-1}(P)$, and this shows, that $A/\phi^{-1}(P) = im\psi$ is a subring of B/P, i.e. a domain. □

Sometimes we need to show, that many prime ideals exist, a tool for this is

Lemma 1.23 (Zorn)**.** *Let $(\Sigma, \leq)$ be a partially ordered set such that every chain* has an upper bound. Then Σ has a maximal element, i.e. $\exists m \in \Sigma$ such that $\nexists m' \in \Sigma$ such that $m < m'$.*

Proposition 1.24. *A is a ring with $I \triangleleft A$, $I \neq (1)$. Then $\exists M \triangleleft A$ a maximal ideal with $I \subset M$.*

Proof. Consider $\Sigma = \{J \triangleleft A : I \subset J,\ J \neq (1)\}$, this is a nonempty set (it contains I), endowed with the $\subset$ relation. Take a chain in this $\mathcal{C} \subset \Sigma$. If $\mathcal{C}$ is the emptyset, then I is an upper bound. If the chain is nonempty, then consider $\cup\mathcal{C}$, which is again an ideal containing I, and not containing 1, an upper bound! Now apply Zorn's lemma to get a maximal element of Σ, call it M. This will be our maximal ideal containing I □

Corrolary 1.25. *If A is a ring with at least two elements, then it has a maximal ideal.*

*totally ordered subset

Proposition 1.26. *Suppose that in a ring A, we have a multiplicatively closed subset S containing 1. Let $\Sigma := \{I \lhd A : I \cap S = \emptyset\}$, and let P be a maximal element of Σ. Then P is prime.*

Proof. $P \cap S = \emptyset$, so it does not containg 1. We need to prove, that if $a, b \notin P$, then $ab \notin P$. Look at $P + (a)$, this is a strictly bigger ideal, than P. This means, that it is not disjoint from S (i.e. not in Σ). So for some elements $p + ra = s$, and repeating the same argument $p' + r'b = s'$. Multiply these together,

$$S \ni ss' = (p + ra)(p' + r'b) = pp' + pr'b + rap' + rr'ab$$

We see that the first three terms are in P, this implies, that $rr'ab \notin P$. □

Theorem 1.27. *If A is a ring, then the nilradical*

$$N(A) = \bigcap_{P \text{ a prime ideal}} P.$$

Further if $I \lhd A$, then

$$\sqrt{I} = \bigcap_{I \subset P \text{ a prime ideal}} P$$

Proof. It enough to prove the second statement, the first is the second applied to (0). The inclusion $\subseteq$ is trivial, for if $a \in \sqrt{I}$, and $I \subset P$ is a prime ideal since $a^k \in P$, a itself will be in P by primality.
For $\supseteq$ we take $x \notin \sqrt{I}$, and want a prime ideal $I \subset P$ such that $x \notin P$. Take $S = \{x^k : k \in \mathbb{N}\}$, this is a multiplicative subset clearly. Take $\Sigma = \{J \lhd A : I \subset J, J \cap S = \emptyset\}$. I is such an ideal, so it is nonempty. We can apply Zorn's lemma for the same reason as before. Take $P \in \Sigma$ maximal, and by the previous proposition it is prime, and not containing x. □

Definition 1.28. A is reduced if $N(A) = \{0\}$.

Example 1.29. $\mathbb{Z}_{p^n}$ is non-reduced for $n > 1$, also $K[x]/(x^2)$ for geometers :)

Proposition 1.30. *If A is any ring, then $A/N(A)$ is reduced.*

Proof. Assume $r + N(A)$ is nilpotent in the factor. This means, that $\exists n \geq 1 : (r + N(A))^n = N(A)$, i.e. $r^n \in N(A)$, so it is nilpotent, there is a k such that $(r^n)^k = 0$, thus r is nilpotent, it is in $N(A)$. □

Definition 1.31. *Spec*(A) as a set is the collection of prime ideals of A. It is endowed with the appropriate notion of a Zariski topology, namely for any $I \lhd A$ we can take $V(I) := \{P \in Spec(A) : I \subset P\}$ to be the closed subsets.

We check that this is actually a topology.

Lemma 1.32. *This makes Spec(A) into a topological space.*

Proof. Finite unions enough to check two. $V(I) \cup V(J) = V(IJ)$. If $I \subset P$, then $IJ \subset P$, so $\subseteq$is clear. If $P \in V(IJ)$, then since P is prime $IJ \subset P$ implies $I \subset P$ or $J \subset P$ clearly by the definition (if $a \in I, \notin P$ and $b \in J, \notin P$, then $ab \in IJ, \notin P$, a contradiction to the primality of P).
Arbitrary intersections. Take $\bigcap V(I_\alpha)$, this will coincide with $V((\cup I_\alpha))$. To see this pick a P from the intersection. This means, that it contains every I_α, and this further implies, that it contains the ideal generated by all of them, i.e. $P \in V((\cup I_\alpha))$. □

Definition 1.33. $I, J \triangleleft A$, the product is defined as $IJ := \{\sum_1^k a_i b_i | a_i \in I, b_i \in J\}$.

Remark 1.34. As a topological space $Spec(A/N(A)) \simeq Spec(A)$.

Proof. Every prime ideal contains the nilradical, so $P \mapsto P/N(A)$ will be a prime ideal* in $A/N(A)$, and a good choice for a homeomorphism. Take $P \neq Q$ two prime ideals in A, then $P/N(A) \neq Q/N(A)$ obviously, take elements which distinguish them, then $a+N(A), b+N(A)$ distinguishes the two factors. It is surhective, take the preimage of an ideal in the factor, the second isomorphism theorem tells us that $A/\phi^{-1}(P) = A/N(A)/P$, which is a domain, i.e. the preimage is prime.
Why is it a homeomorphism? Take $\bar{I} \subset A/N(A)$, and $V(\bar{I}) \subset Spec(A/N(A))$. The preimage consists of prime ideals, which contain the preimage of $\bar{I}$ under the factor map, so it is also closed and the map is continous.
For the continuity of the inverse take† $I \triangleleft A$, $V(I) = \{P | I \subset P\} = \{P | I + N(A) \subset P\}$ since any prime ideal contains the nilradical. The image under ϕ will be a closed set, namely $V((I + N(A))/N(A))$. □

When is $Spec(A) = \{*\}$ for a reduced ring A. This means there is a single prime ideal, which has to be zero. There are always maximal ideals as well, so A is in fact a field.
Taking the spectrum is a contravariant functor. For a map $\phi : A \to B$ the induced map $\phi^* : Spec(B) \to Spec(A)$ is defined by taking the complete preimage.

Lemma 1.35. *$P \triangleleft B$ is prime, then $\phi^{-1}(P)$ is also prime.*

Proof. $A/\phi^{-1}(P) \hookrightarrow B/P$, and any subring of a domain is a domain, so the preimage is indeed a prime. □

Points should correspond to the images of the singleton sets. If $P \in Spec(A)$, then $A \to A/P \hookrightarrow K = Q(A/P)$ into the field of fractions, this gives the $\phi^* : Spec(K) = \{*\} \to Spec(A)$ that hits P.

Proposition 1.36. *$\phi^* : Spec(B) \to Spec(A)$ is continous.*

Proposition 1.37. *Take $I \triangleleft A$, the closed set $V(I) \subset Spec(A)$ has to have closed preimage. This preimage looks like $\{P \triangleleft B | \phi^{-1}(P) \supset I\}$, i.e. $P \subset \phi(I)$, and it is a closed set $V((\phi(I)))$*

2 Second lecture

Definition 2.1. Let A be a ring (commutative with 1 as always), the Jacobson radical of A is the intersection of all maximal ideals, $J(A) := \cap_{m-Spec(A)} M$.

Proposition 2.2. *$J(A) \triangleleft A$, since it is the intersection of ideals.*
$N(A) \subset J(A)$, since $N(A) \subset \cap_{Pprime} P \subset \cap_{m-Spec} = J(A)$ since every maximal ideal is prime.
$J(A/J(A)) = 0$

Proof. We have the map $A \to A/J(A) \to 0$. The maximal ideals of the factor correspond to the maximal ideals of A, containing $J(A)$. We have to intersect all maximal ideals containing $J(A)$ in A, which is just $J(A)$, so it goes to zero in the factor. □

Example 2.3. $J(\mathbb{Z}) = 0$, since the maximal ideals are the ideals generated by prime numbers.

*second ismorphism theorem says that $(A/N(A))/(P/N(A)) = A/P$, which is a domain
†$I + J = (I, J)$

Proposition 2.4. $J(A) = \{x \in A : 1 - xy \in U(A)\ \forall y \in A\}$

Proof. Start with $\subseteq$: $x \in J(A)$ means, that it is contained in all maximal ideals. This implies, that $\forall y$ and max ideal M $xy \in M$, so $1 - xy \notin M$, implying that $(1 - xy) = (1)$.
Now $\supseteq$. Consider $x \notin J(A)$, so there is a maximal ideal M excluding it. There is a natural map $A \to A/M \to 0$, the fator is a field, $\bar{x}$ is nonzero, so it is invertible, thus it has an inverse $\bar{y}$ such that $\bar{x}\bar{y} = \bar{1}$, meaning $1 - xy \in M$, thus it is not a unit. □

And now for something completely different, ${}_AM$ modules. $(M, +)$ is an abelian group, with a multiplication by elements of A given, satisfying the standard axioms:

- $(a + b)m = am + bm$
- $a(m + n) = am + an$
- $(ab)m = a(bm)$
- $1m = m$

We can talk about submodules, a subset containing 0, closed under the addition operation, and the scalar multiplication. Given $U, V \leq M$, we can talk about $U + V = \{u + v\} =< U \cup V >\leq M$. Also for $I \triangleleft A$ we can have $IU = \{\sum a_i u_i : a_i \in I, u_i \in U\}$. Every ring is a module over itself, the submodules are precisely the ideals of A.
We can also talk about factor modules.

Definition 2.5. $U, V \leq M$, consider $(U : V) := \{a \in A : aV \leq U\} \triangleleft A$.

Remark 2.6. $(U : V)V \leq U$

Definition 2.7. $AnnV := (0 : V)$ (again obviously an ideal of A).

Definition 2.8. $N \leq M$ we can form M/N. For $m, m' \in M$ we say $m \equiv m' \mod N$ iff $m - m' \in N$, and consider the set of equivalence classes under this relation, consisting of N, and its translates. Take the quotient group as tha base group of the new module, and the ring action is inherited from M.* We also have the factor map, a homomorphism of modules.

Theorem 2.9 (Homomorphism theorem)**.** *$\phi : M \to N$ a homomorphism of A-modules, $im\phi = M/ker\phi$.*

Theorem 2.10 (First isomorphism theorem)**.** *$H, N \leq M$, $(H + N)/N = H/(H \cap N)$*

Theorem 2.11 (Second isomorphism theorem)**.** *$L \leq N \leq M$, then $M/N = (M/L)/(N/L)$.*

Remark 2.12. $U, V \leq M$, then $(U : V) = Ann((U + V)/U)$

Proof. $a \in A$, if $aV \leq U$, then $a(U + V) \leq U$ equivalently. This also means that $a((U + V)/U) = 0$, which was the statement. □

To study rings, we consider modules over that ring. This is motivated by the fact for example, that ideals are the submodules of ${}_AA$, and factors are also modules ${}_A(A/I)$.

*easy check

Definition 2.13. ${}_AM$ is finitely generated (M is finite over A), if there exists $m_1, \ldots, m_n$ such that $M =< m_1, \ldots, m_n >$.

Proposition 2.14. *${}_AM$, then M is finite over A iff $\exists n$ and a homomorphism such that the sequence $A^n \to M \to 0$ is exact.*

Proof. $A^n =< e_1, \ldots, e_n >$ obviously, if we have a surjective homomorphism, the images of these generate M. Conversely, if M is finite over A, take the finitely many generators $m_1, \ldots, m_n$, and obviously $e_i \mapsto m_i$ extends to a homomorphism. □

${}_AM$, we can look at $S(M) := \{N : N \leq M\}$. We can order the submodules w.r.t. inclusion, or reverse inclusion to get two posets.

Definition 2.15. Given a poset $(S, \leq)$, we say that S is Noetherian, if every ascending chain stabilises, i.e. for any chain $s_1 \leq s_2 \leq \ldots$ there exists an n, such that $s_n = s_{n+1} = \ldots$
We call S Artinian, if this holds for descending sequences $s_1 \geq s_2 \geq \ldots$.

Proposition 2.16. *$(S, \leq)$ a poset, the following are equivalent.*

1. *S is Noetherian*
2. *Every strictiy ascending chain is finite (there is no strictly increasing infinite squence)*
3. *Every nonempty subset has a maximal element*
4. *Downwards induction works in S, i.e. for a property P to hold for all elements of S it is sufficient, to satisfy the following: If $s \in S$, and Pt for all $t > s$, then Ps.*

Proof. Trivial. The first two are clearly equivalent. The three implies four, since $s \in S : \not Ps$, if this is nonempty, it has a maximal element s, and downwards induction fails.
Conversely four implies three. Consider $P =\notin X$, by contradiction, if X has no maximal element, then by induction P holds for all $s \in S$, i.e. $X = \emptyset$.
Clearly 3 implies 2, and conversely 2 implies three, if a set has no maximum we create an infinite chain by choosing greater and greater elements. □

Similarly

Proposition 2.17. *Artinian property has the same proposition with the relations reversed.*

Definition 2.18. Given ${}_AM$, we say that is is Noetherian iff $(S(M), \leq)$ is Noetherian, and Artinian iff $(S(M), \leq)$ is Artinian.

Example 2.19. Look at ${}_{\mathbb{Z}}\mathbb{Z}$. It is Noetherian, but not Artinian. We can have a decreasing infinite chain $(p) \supset (p^2) \supset \ldots$, but no ascending ones.
For a prime p we can consider $\mathbb{Z}_{p^\infty} := \{k/p^n : n, k \in \mathbb{N}\}$ with addition mod 1 as operation. This is an Abelian group, i.e. a $\mathbb{Z}$ module, which is Artinian, but not Noetherian. We see this by descibing all subgroups. There is the trivial one, then the denominator can be p, p^2 and so on, this gives an increasing sequence $0 < Z_p < Z_{p^2} < \ldots$.

Example 2.20. $A = K$ a field, then modules are vector spaces. Now clearly ${}_AM$ is Noetherian iff the dimension is finite, and this is also equivalent to M being Artinian.

Proposition 2.21. *A is a ring, and there are $M_1, \dots, M_n \in m - SpecA$ such that $\prod M_i = 0$, then for any ${}_AV$ V is Artinian iff it is Noetherian.*

Lemma 2.22. *$N \leq M$, then M is Noetherian iff $N, M/N$ are both Noetherian (and similarly for Artinian).*

Proof. For the if part, it is very easy, any submodule is also Noetherian, and we can pull back chain by the factor map, so they also have to stabilise. This is the same for both Noetherian andArtinian modules.
For the converse consider the map $S(M) \to S(N) \times S(M/N)$ where $H \mapsto (H \cap N, (H+N)/N)$. If $H \leq H'$, then $H \cap N \leq H' \cap N$ and $H + N \leq H' + N$ and thus$(H+N)/N \leq (H'+N)/N$, so this map is monotone. We want, that if $H \leq H' \leq M$ with $H \cap n = H' \cap N$ and $H + N = H' + N$, then this imples, that $H = H'$. Indeed, if $x \in H'$, then $x \in H' + N = H + N$, i.e. $x = h + n$.So $N \ni n = x - h \in H' - H \leq H'$, so $n \in H' \cap N = H \cap N$, thus $n \in H$ and $x = n + h \in H$.
This proes that the above map is not just monotone, but strictly so, and we are done. □

Corrolary 2.23. *For $M = M_0 \geq \cdots \geq M_n = 0$ M being Noetherian (Artinian) is equivalent to having M_{i-1}/M_i Noteherian (Artinian) for all i.*

Proof of proposition. Define $V_i = M_1 \cdot \cdots \cdot M_i V$ to get a chain just as above. Now V is Artinian iff $Q_I := V_{i-1}/V_i$ is, for all i. Observe that $M_i Q_i = 0$, so Q_i is a module A/M_i, which is a field, i.e. Q_i is q vector space, so it being Artinian is equivalent to being Noetherian, and we are done with the proposition. □

Remark 2.24. Technically we only needed, that $M_1 \cdot \cdots \cdot M_n V = 0$.

Remark 2.25. Consider a poset $(L, \leq)$. Define the length of S as $sup\{n : s_0 < s_1 < \cdots < s_n\}$.* This defines the length of a module ${}_AM$ as $l(M) = l(S(M))$. The above proof actually shows, that for $N \leq M$ we have $l(M) \leq l(N) + l(M/N)$.

Remark 2.26. $l(M) \geq l(N) + l(M/N)$ also holds pretty much trivially, having a chain in N, and another in M/N we can pull it back by the factor map to get a chain in M of length the sum of the two.

Theorem 2.27. *$l(M) = l(N) + l(M/N)$ for all $N \leq M$.*

Definition 2.28. We call a ring Noetherian (Artinian) if ${}_AA$ is Noetherian (Artinian).

Example 2.29. $\mathbb{Z}$ is Noetherian, but not Artinian.

Theorem 2.30 (Hopkins)**.** *If the ring A is Artinian, then A is Noetherian.*

Theorem 2.31 (Hilbert's basissatz)**.** *If R is Noetherian, then $R[x]$ is Noetherian.*

We'll see these later.

Corrolary 2.32. *If A is a ring, and $M_1 \cdot \cdots \cdot M_n = 0$ for $M_i \in m - Spec(A)$, then A is Artinian iff it is Noetherian.*

Proposition 2.33. *${}_AM$ is Noetherian iff all submodules are finitely generated.*

*the length of a chain is the number of steps

Proof. If M is Noetherian, if it is 0, the statement is clear. If not, choose a nonzero element. If it generates M, we are happy, if not choose another element not in the cyclicsubmodule generated by the first, if they generate we are happy, if not pick a new one and so on to get a strictly increasing sequence of submodules, and by the Noetherian proeprty we are done.
Suppose now, that we have an infinite increasing sequence $N_1 \leq N_2 \leq \ldots$, and take the union to get a new submodule $N \leq M$. We get by assumption, that N is finitely generated by $x_1, \ldots, x_n$ where $x_i \in N_{k_i}$, and taking the maximum of the k_i we see that the chain stabilises. □

Corrolary 2.34. *A ring A is Noetherian iff all ideals are finitely generated.*

A bit of notation, if $f(x) = \sum_0^n a_i x^i \in R(x)$ we call a_n the leading coefficient, and $a_n x^n$ the leading term.

Lemma 2.35. *$J, I \triangleleft R[x]$ such that $J \subset I$, and for all nonzero $f \in I$ there is a $g \in J$ such that the leading terms are equal,then $I = J$.*

Proof. Take a nonzero $f \in I$, find its friend in J, with the same leading term. $f - g$ is still in I, the degree is smaller and we are done by induction. □

Proof of the Basissatz. Take $I \triangleleft R[x]$, we wish to prove that it is fin. gen.. Define $I_n := \{a_n : \exists \sum_0^n a_i x^i \in I\} \triangleleft R$. Obviously $I_n \subset I_{n+1}$, since if $f \in I$, then $xf \in I$. We know that R is Noetherian, so this chain stabilises at say n $I_n = I_{n+1} = \ldots$. All of these ideals are finitely generated $I_0, I_1, \ldots, I_n$. This means the existance of finite subsets $\mathcal{F}_i \subset I$ all members are of degree i, and their leading coefficients generate I_i. Now take $\mathcal{F} := \mathcal{F}_0 \cup \cdots \cup \mathcal{F}_n$, and we claim, that this generates I. We only have to check, that for all nonzero elements of I there is an element in $(\mathcal{F})$ with the same leading term. This is prefectly clear, if $degf \leq n$ by construction there is $g \in (\mathcal{F}_i)$ with the same leading term. If the degree of our f is at least n, then its leading coefficient is in I_n,so there is a g of degree n with the same leading coefficient, and we can multiply up by some x^k. Now we are done by the lemma. □

Proposition 2.36. *If A is Noetherian, and $F \subset A$, then there exists a finite subset $G \subset F$ such that $(G) = (F)$.*

Proof. Trivial homework. □

3 Third lecture

We'll discuss decompositions of ideals. The story begins, with the fundamental theoremof arithmetic, i.e. $\mathbb{Z}$ is a UFD, also all principal ideal domains are UFD's, every element is the essentially unique product of irreducible elements. We wish to study algebraic extensions, i.e. $|K : \mathbb{Q}| < \infty$, and take the algebraic integers, $K \cap \Omega = \sigma_K$. But not all rings of algebraic integers are UFD's.

Example 3.1. $\mathbb{Q}[\sqrt{-5}]$ is not a UFD, since $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, and these decompositions are not the same up to unit factors. The units are only ± 1.

Kummer found out the way to fix this problem of non-uniqueness to take prime ideals, which he thought of as being ideal elements of a new ring. So $I \subset A$ will have to satisfy the natural axioms of an ideal, if we want to think about "which elements are divisble by I?". In the previous example $(2, 1 + \sqrt{-5}), (3, 1 + \sqrt{-5}), (2, 1 - \sqrt{-5}), (3, 1 - \sqrt{-5})$ are all prime ideals, and unique factorisation works with ideals, instead of elements, the

ideal (6) is precisely the product of the previous 4. Generally, nonzero ideals in the group of algebraic integers of a number field have unique prouct decompositions into prime ideals, these rings are called Dedekind rings.

Definition 3.2. If A is a ring (comm. with 1), the Krull dimension of A is defined as $sup\{n : P_0 \subset \cdots \subset P_n, P_i \in specA\}$.

Example 3.3. $dimA < 0$ iff $A = 0$, there are no prime ideals. $dimA \leq 0$ iff all prime ideals are maximal, for example if A is a field. A PID, which is not a field has $dimA = 1$, since all nonzero primes are maximal.* $dimK[x_1, \ldots, x_n] = n$, $\geq$ is easy, $(0) \subset (x_1) \subset \ldots, (x_1, \ldots, x_n)$, the other directionis hard, we'll see later. Also the dimension can be infinite, for example $K[x_1, \ldots]$ has an infinitely long chain. Connecting with the previous example, the ring σ_K has dimension 1.

In higher dimensional rings most ideals don't have prime decompositions, most elements are irreducible and the theory isn't really useful, so we wish to replace products by intersections. This still generalises the FTA since $(n) = \cap(p_i^{\alpha_i})$ where $n = \prod p_i^{\alpha_i}$, n is not only the product, but the least common multiple of these prime powers. What would correspond to prime power ideals in a general (Noetherian) ring?

Definition 3.4. $I \lhd A$ is irreducible iff $I \neq (1)$, and it does not decompose as an intersection, except in the trivial way, i.e. $I = J \cap J'$ iff $J = I$ or $I = J'$.

Proposition 3.5. *A Noetherian, $I \lhd A$, then $\exists n \in \mathbb{Z}_{\geq 0}$ and $I_1, \ldots, I_n \lhd A$ irreducible ideals with $I = \bigcap I_i$.*

Proof. Use downwards induction, assume that every ideal J strictly greater than I is a finite intersection of irreducibles. If $I = (1)$ we are done, it is the empty intersection. If I is irreducible we are done, and finally if it is not irreducible, it is the intersection of two strictly greater ideals, for which we already have the proposition by induction. □

Question: $\phi : A \to B$, and $I \lhd B$ is irreducible, then is $\phi^{-1}(I)$ irreducible?

This seems false, but we don't have a counterexample. To make this class functorial we need to enlarge it a bit.

Definition 3.6. $Q \lhd A$ is primary, if $Q \neq (1)$, and if $a, b \in A$ are such that $ab \in Q$, then either $a \in Q$ or $b \in \sqrt{Q}$.

Example 3.7 (Primary ideals in $\mathbb{Z}$). (n) will be primary iff $n = 0$ or a prime power. This is true, since if $p^\alpha | ab$, than either $p^\alpha | a$ or $p | b$, and if $n = uv$ with $(u, v) = 1$, then $n \nmid u$ and $n \nmid v^k$ for any k.†

In general primary ideals are not powers of prime ideals, this implication is false in either direction.

Proposition 3.8. *$\phi : A \to B$ ring hom, and $Q \lhd B$ primary, then $\phi^{-1}(Q)$ is primary in A.*

Proof. $\phi(1) = 1 \notin Q$, so the preimage is not the unit ideal. if $ab \in \phi^b - 1(Q)$, then $\phi ab \in Q$, so $\phi a \in Q$ or $\phi b \in \sqrt{Q}$ and so either $a \in \phi^{-1}Q$ or $b \in \sqrt{\phi^{-1}Q}$. □

Proposition 3.9. *$Q \lhd A$ is primary iff $A/Q \neq 0$ and all zero divisors are nilpotent in this factor.*

*homework sheet 2

†this is the same as the ideal being irreducible in $\mathbb{Z}$, but maybe not elswhere

Proof. A/Q is nontrivial, since $Q \neq (1)$. If $\bar{a}\bar{b} = 0$ in the quotient with $\bar{a} \neq 0$, then $\bar{b} \in N(A/Q)$, since this means, that $ab \in Q$ with $a \notin Q$, so $b \in \sqrt{Q}$, which means precisely that $\bar{b}$ is nilpotent in A/Q. □

Proposition 3.10. *If Q is primary, than $\sqrt{Q}$ is prime.*

Proof. Q is not the unit ideal, so its radical is not the unit ideal either. If $ab \in \sqrt{Q}$, then $ab^n \in Q$ for some power n. This means that $a^n \in Q$ or $b^n \in \sqrt{Q}$, so $a \in \sqrt{Q}$ or $b \in \sqrt{q}$, this is the prime tulajdonság. □

Remark 3.11. $P \in specA$, then $\sqrt{P^n} = P$ for all n.*

Proof. $P^n \subseteq P$, and $\sqrt{P^n} \subseteq \sqrt{P} = P \subseteq \sqrt{P^n}$. □

Example 3.12. $A = k[x, y, z]/(xy - z^2)$, and $P = (\bar{x}, \bar{z})$. This ideal is prime, since $A/P = k[y]$. $P^2 = (\bar{x}^2, \bar{z}^2, \bar{x}\bar{z})$, and we claim, that this is not primary. Consider $A/P^2 = k[x, y, z]/(x^2, xz, z^2, xy)$, and in this ring $\bar{\bar{y}}$ is a zero divisor, which is not nilpotent. The image of x is a zero divisor pair, and $y^n \notin P^2$ for any n.

This means the reverse implication of 3.10 is not true.

Definition 3.13. $Q \triangleleft A$, and $P \in specA$, we call Q P-primary iff Q is primary and $\sqrt{Q} = P$.

Proposition 3.14. *Q, Q' is P-primary, then $Q \cap Q'$ is P-primary.*

Lemma 3.15. *$I, J \triangleleft A$, then $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*

Proof. $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$ is clear. Now suppose $x \in \sqrt{I} \cap \sqrt{J}$, so $x^n \in I$ and $x^m \in J$, and taking the maximum $x^{\max} \in \sqrt{I \cap J}$. □

Proof of proposition. $\sqrt{Q \cap Q'} = P \cap P = P$ by the lemma, but we need also, that $Q \cap Q'$ is primary, so take $ab \in Q \cap Q'$. If $b \notin P$, then $a \in Q, Q'$ and so it is also in the intersection. □

Proposition 3.16. *If Q is an ideal of A, with $\sqrt{Q} \in m - specA$, then Q is primary.*

Proof. Obviously $\sqrt{Q} \neq (1)$. If we have a product in Q ab, with $b \notin \sqrt{Q}$, then since the radical is maximal, b has an inverse mod $\sqrt{Q}$, $(1 + bc)^n \in Q$, and this has the form $1 + bx$ for some x, now multiply by a to get $a + abx \in Q$, but $abx \in Q$, so $a \in Q$ and we are done. □

Example 3.17. $k[x_1, \ldots, x_n]$ with k a field. $Q = (S)$, where S is a set of monomials s.t. $1 \notin S$, and for all i $\exists s : x_i^s \in S$, then obviously $\sqrt{Q} = (x_1, \ldots, x_n)$, so these ideals are primary.
A concrete example would be $(x^2, xy) \triangleleft k[x, y]$. To decompose this take $(x) \cap (x, y)^2 = (x) \cap (x^2, y)$, these are both primary decompositions of our ideal†
Notice, that $(x, y)^2 = (x^2, y) \cap (x, y^2)$.

Fact 3.18. *$I \triangleleft A$ is irreducible iff $A/I \neq 0$ and $\forall 0 \neq a, b \in A/I : \exists x, y \in A/I : xa = yb \neq 0$.*

First I being irreducible isequivalent to having (0) irreducible in $A/I =: B$. Firstly it is clear, that $(0) \neq (1)$. If (0) is irreducible then for $a, b \neq 0$, then $(a), (b), \neq (0)$ we also have $(a) \cap (b) \neq (0)$ by irreducibility. Conversely if J, J' are nonzero ideals, and a, b are in the respective ideals, then the assumption of having a nonzero common multiple gives a nonzero element in the intersection, i.e. zero is irreducible.

*remember, $P^n = (\prod_1^n p_i | p_i \in P)$ with n fixed
†all prime ideals are primary!+proposition

Lemma 3.19 (E. Noether)**.** *If A is a Noteherian ring, then every irreducible ideal is primary.*

Proof. It is sufficient to show, that if (0) is irreducible, then it is primary,since otherwise we can pass to the factor.
We have to prove, that if every nonzero pair of elements have a nonzero common multiple, then every zero divisor is nilpotent. Let $uv = 0$ with $v \neq 0$, we want u nilpotent. Take $(0) \subset Ann(u) \subset Ann(u^2) \subset \dots$ since this sequence is increasing, and A is Noetherian this stabilises, i.e. $Ann(u^n) = Ann(u^{n+1})$.
It is enough to show, that v and u^n have no nonzero common multiple. $xv = yu^n$, then it should follow that $xv = yu^n = 0$. $0 = xuv = yu^{n+1}$, this means that $y \in Ann(u^{n+1}) = Ann(u^n)$,and we are done. □

Theorem 3.20 (Lasker-Noether)**.** *If A is Noetherian, I is an ideal, then there exists an n, such that $I = \bigcap Q_i$ for some primary ideals Q_i.*

Proof. Returning to the previous example, the decompositions are not the same, but the radicals are. Suppose $I = \bigcap Q_i$ for some primary ideals Q_i, with $P_i = \sqrt{Q_i}$. Take $x \in A$ and consider $(I : x) = \{a : ax \in I\}$. The ideal $\sqrt{(I : x)} = \bigcap_{x \notin Q_i} P_i$.
Now $(I : x) = \bigcap (Q_i : x)$, so $\sqrt{(I : x)} = \bigcap \sqrt{(Q_i : x)}$ and we need a lemma.

Lemma 3.21. *Q os P-primary, then $(Q : x)$ can be either (1) if $x \in Q$, in this case $\sqrt{Q} = (1)$ as well. On the other hand if $x \notin Q$, then the radical $\sqrt{(Q : x)}$ is P.*

Proof. m i s s i n g □

□

Definition 3.22. If $I \triangleleft A$ and $P \in specA$, then P belongs to I iff there is an $x \in A$ such that $\sqrt{(I : x)} = P$.

Proposition 3.23. *If P belongs to I, and $I = \bigcap Q_i$, with Q_i P_i primary, then $P \in \{P_i\}$.*

Proof. $P = \sqrt{(I : x)} = \bigcap_{x \notin Q_i} P_i \supset \prod_{x \notin Q_i} P_i$, so there exists an i with $P_i \subseteq P$ where $x \notin Q_i$, but P is also bigger than every ideal P_i. □

4 Fourth Lecture

missing

Theorem 4.1 (first uniqueness theorem of primary decomposition)**.** *$I = Q_1 \cap \dots \cap Q_n$ is a shortest primary decomposition, then $\{\sqrt{Q_i} : P \in specA,\ P \text{ belongs to } I\}$. This means, that n is unique.*

Example 4.2. $k[x, y]$, and take $(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$. these are two shortest decompositions of the same ideal, but notice (x) is in both of them!

If $I \triangleleft A$, suppose it has a primary decomposition $I = \bigcap_1^n Q_i$, and the primes belonging to I denoted by $\{P_i = \sqrt{Q_i}\}$. Assume that for all $i \leq k$ and $j > k$ $P_i \not\supseteq P_j$, i.e. $\{P_1, \dots, P_k\}$ is downwards closed as a poset in $(\{P_i\}, \subset)$.

Theorem 4.3 (second uniqueness theorem)**.** *Then $Q_1 \cap \dots \cap Q_k$ is unique*

Example 4.4. If P_1 is minimal, then Q_1 is unique.

Proof. $x \in A$, when is $x \in \bigcap_1^k Q_i$ true? we want to give an answer independent of the decomposition. Firstly this is equivalent to having $\{i \in [n] : x \notin Q_i\} \subset [k+1, \ldots, n]$, and furthermore this equivalent to saying $\bigcap_{x \notin Q_i} P_i \supseteq P_{k+1} \cap \cdots \cap P_n$. One direction is clear, for the other, if there exists an index $i \leq k$ with $x \notin Q_i$, then $P_i \supseteq \bigcap_{k+1}^n P_i \supseteq P_{k+1} \cdot \cdots \cdot P_n$, a contradiction by the downwards closed property, no $P_{>k}$ is contained in P_i. Finally this is equivalent to having $\sqrt{(I : x)} \supseteq \bigcap_{k+1}^n P_i$, and this description does not use the decomposition, as we wanted. □

Theorem 4.5. *A is Artinian iff A is Noetherian with $dim A = 0$.*

Lemma 4.6. *$I \triangleleft A$ with A Noetherian, then $\exists k : \sqrt{I}^k \subseteq I$.*

Proof. $\sqrt{I}$ is finitely generated $(a_1, \ldots, a_r)$, and here exists exponents for each of these generators where $a_i^{k_i} \in I$. Take $k = 1 + \sum(k_i - 1)$, and any k-fold product in $\sqrt{I}$ will have at least one generator to the k_i power, and we are done. □

Definition 4.7. A is Artinian iff there is no decreasing sequence of ideals.

Example 4.8. If $|A| < \infty$, e.g. $\mathbb{Z}_n$. If the number of ideals is finite, then also clearly we get artinian rings, if A is a PID, then $R/(m)$ is artinian for any nonzero element m. A finite dimensional algebra over a field is also artinian.

Fact 4.9. *An Artinian domain is a field.*

Proof. $0 \neq x$ and consider the ideals (x^i), this is a descending sequence, so $\exists m : (x^m) = (x^{m+1})$, i.e. $x^{n+1}y = x^m$, i.e. $xy = 1$ since we are in a domain. □

Corrolary 4.10. *If A is Artinian, then $dim A = 0$.*

Proof. Choose a prime P, A/P is an Artinian domain, i.e. a field, i.e. every P is maximal, so the krull dimension is zero. □

Lemma 4.11. *If A is Artinian, then there are only finitely many prime ideals.*

Proof. Suppose there are infinitely many prime ideals $P_1, \ldots$. Take $I_n = \bigcap_1^n P_i$, this gives a descending sequence, and strictly so, because $P_{n+1} \not\supset P_1 \cap \cdots \cap P_n \supset P_1 \cdot \cdots \cdot P_n$, and it does not contain any of these by primality since all primes are maximal, and these are distinct ideals. □

Definition 4.12. $I \triangleleft A$, then I is called nilpotent iff $\exists k : I^k = 0$.

Theorem 4.13. *If A is Artinian, then $J(A)$ is nilpotent.*

Proof. Consider the powers of the Jacobson radical $J(A) \supset J(A)^2 \supset \ldots$, let it stabilise at the n-step, and call the stable ideal J. Clearly $J^2 = J$, we want it to be zero. Assume it nonzero and look for a contradiction.* Take the set of ideals which are contained in J, and $IJ \neq 0$ holds, this is a nonempty set of ideals. Take a minimal element I by the artinian property, and we find an element $a \in I$ with $aJ \neq 0$, since it was minimal we have to have $aJ = I$, thus $aJJ \neq 0$, and there is a $y \in J$ such that $ay = a$, and since J is a part of the Jacobsonradical $1 - y$ is invertible, so $a = 0$, a contradiction. □

*this implies $A \neq 0$, and $J \neq (1)$

Corrolary 4.14. *If A is Artinian, then there are $P_1, \ldots, P_n \in SpecA$ such that $\prod P_i = 0$.*

Proof. J(A)=$\cap_{Spec(A)} P \supseteq \prod_{specA} P$, the spectrum is finite, and $J(A)$ is nilpotent, we are done. □

Corrolary 4.15. *If A is Artinian, then A is Noteherian.*

This shows one direction of the big theorem, now we want to show that a dimension 0 Noetherian ring is Artinian. In a Noetherian ring the ideals have primary decompositions, e.g. $(0) = \bigcap_1^n Q_i$ where Q_i is P_i primary. We know that $Q_i \supseteq P_i^{k_i}$ for some numbers k_i. By the assumption on the dimension we get that the 0 ideal is the product of maximal ideals, and in this case we already know that Noetherian implies Artinian. We have a structure theorem as well, Artinian rings are sums of local Artinian rings.

Definition 4.16. A is local, if there is a unique maximal ideal.

Remark 4.17. $\{I\} = m - specA$ iff $I \neq (1)$, and $A \setminus I = U(A)$.

Example 4.18. $\mathbb{Z}_{p^k}$ for some prime power are local.

Why are these "local"? $X \subseteq K^n$ an affine algebraic subset over an algebraically closed field K. $\mathcal{A}_X$ its coordinate ring, we can define the local ring of X at p consisting of functions only defined on an open subset containing p, and such that the function is represented by a rational function, with nonzero denominator at p. Two functions are equal in the local ring iff they agree on an open neighborhood. The maximal ideal will be the functions vanishing at p, the factor is K, so it is maximal, and everybody outside is invertible.

Lemma 4.19. *I_1, I_2, J are ideals in A, and $I_1 + J = (1), I_2 + J = (1)$, then we claim that $I_1 I_2 + J = (1)$.*

Proof. $1 + a_1 + b = a_2 + b$, and $1 = 1 * 1 = (a_1 + b)(a_2 + b) \in a_1 a_2 + J$. □

Lemma 4.20. *If I, J are coprime, then $IJ = I \cap J$*

Proof. one direction is trivial, take $x \in I \cap J$. write $1 = a + b$, $x = 1x = xa + xb$, and both terms here are inside IJ. □

Corrolary 4.21. *If we are given $I_1, \ldots, I_n$, pairwise coprime,then again the product is the same as the intersection.*

Proof. We can use the previous two lemmas to do induction, to replace I_1, I_2 by $I_1 I_2$, and everything stays intact. □

Theorem 4.22 (Chinese remainder theorem)**.** *Let $I_1, \ldots, I_n$ be pairwise coprime ideals. Take $\phi : A \to \oplus A/I_i$. We claim that ϕ is surjective, $ker\phi = \prod I_i$, and $A/\prod I_i = \oplus A/I_i$.*

Proof. the kernel is obvious, using the fact that the intersection is the same is the product. The third claim follows from the first by the homomorphism theorem, so we focus on the first. ϕ is an A-module homomorphism. The image is an A-submodule, so we only need to find $(0, .., 1, ..., 0)$ in the image. this is clear, since$I_i + \cap I_j = (1)$, thus we can find $a + x = 1$, so we get an element which is 1 mod I_i and 0 mod I_j for all other j's, and we are done. □

5 Fifth lecture

beginning missing again

Proposition 5.1. *A local, e an idempotent, then $e = 0$ or 1.*

Proposition 5.2. *M a maximal ideal in A, $k \geq 1$, then A/M^k is local.*

Finishing the proof of the structure theorem of Artinian rings, and now for something completely different. Last time we had the ring of local functions of a variety at a point, we wish to generalise this. Suppose A is a ring, and consider $S \subseteq A$, with $1 \in S$, and $SS \subset S$, we wish to allow these elements as denominators. Consider ordered pairs $\{[a, s] : a \in A, s \in S\}$, and we introduce an equivalence, $[a, s] \sim [b, t]$ precisely when $\exists u \in S : u(ta - sb) = 0$.

Proposition 5.3. *$\sim$ is an equivalence relation.*

Proof. $[a, s] \sim [a, s]$:$1(sa - sa) = 0$, so this is easy.
Symmetry is also completely obvious $u(ta - sb) = 0$, then $u(sb - ta) = 0$.
Transitivity is the harder bit. $[a, s] \sim [b, t]$ and $[b, t] \sim [c, r]$. $u(ta - sb) = 0$, and $v(rb - tc) = 0$ by definition. $tuv(ra - sc) = 0$, firtsly $uv \in S$, since it is closed under multiplication. $uta = usb$ and $vrb = vtc$ by the first equations, and simple calculation shows the sought identity. □

We denote the class $[a, s]/\sim = \frac{a}{s}$
Introduce $S^{-1}A = \{\frac{a}{s} : a \in A, s \in S\}$, we introduce operations. $\frac{a}{s} + \frac{b}{t} := \frac{ta+sb}{st}$ and $\frac{a}{s}\frac{b}{t} := \frac{ab}{st}$.

Proposition 5.4. *$S^{-1}A$ is a ring with these operations.*

Proof. Take $\frac{a}{s} = \frac{a'}{s'}$, we need to show, that $\frac{ta+sb}{st} = \frac{ta'+s'b}{s't}$. There is a u s.t. $u(s'a - sa') = 0$. It is a simple check, that $u(s't(ta + sb) - st(ta' + s'b)) = 0$, thus addition is well defined.
Under the same assumption we need multiplication makes sense. $\frac{ab}{st} = \frac{a'b}{s't}$? By definition $u(s'tab - sta'b) = 0$, so multiplication is also well defined.
Addition is clearly commutative, associativity is also quite clear from the well-definedness and associativity of the operations of A.
$\frac{0}{1}$ is a zero element clearly, additive inverses behave the expected way as well, $-\frac{a}{s} = \frac{-a}{s}$.*
Multiplication is again commutative associative, distributivity is not completely clear, but is a simple computation $\frac{c}{r}(\frac{a}{b} + \frac{b}{t}) = \frac{c}{r}\frac{a}{b} + \frac{c}{r}\frac{b}{t}$, expanding both sides by definition we only have to check that $\frac{r}{r} = \frac{1}{1} = 1$, which is clear, $1(ras - rsa) = 0$. □

There is a canonical homomorphism $\phi : A \to S^{-1}A$, which sends $\phi : a \mapsto \frac{a}{1}$. Observe that for $s \in S$, $\phi(s) \in U(S^{-1}A)$. This ϕ has a universal property!† Suppose $A \xrightarrow{\phi} S^{-1}A$, and $A \xrightarrow{\psi} B$ such that $\forall s \in S : \psi(s) \in U(B)$. In this case there is a unique homomorphism $\eta : S^{-1}A \to B$ such that this triangle commutes.

Proof. We need apriori that $\eta(\frac{a}{1}) = \psi(a)$ for the diagram to commute. $\frac{s}{1}\frac{a}{s} = \frac{a}{1}$ apply eta to this to get $\psi(s)\eta(\frac{a}{s}) = \psi(a)$, and we are assuming that the elements of the image of S is invertible, thus $\eta(\frac{a}{s}) = \frac{\psi(a)}{\psi(s)}$, there are no choices. This shows uniqueness, we need to check that this is an actual homomorphism.

*here we use, that actually $\frac{0}{s} = \frac{0}{1}$ for any s since 1 is the multiplicative identity.
†its the freeest possible ring with the property that the elements of S are invertible

Well defined, since $u(s'a - sa') = 0$, and applying ψ gives what we wanted. Why is it a ring homomorphism? Trivial calculation applying the definition of addition in $S^{-1}A$, and using that ψ is a homomorphism. Multiplicativity is even easier, it respects 1 as well, since ψ is a homomorphism. □

Example 5.5. $P \in SpecA$, and choose $S = A \setminus P$. We denote $S^{-1}A =: A_P$, called the localisation of A at P. Another basic example is when $A = \mathcal{A}_X$ for an affine variety over an algebraically closed field. P will be the maimal ideal of a point.

Moreover, take a module ${}_AM$, and $S \subseteq A$ containing 1 and $SS \subseteq S$. We can consider $\{[m, s] : m \in M, s \in S\}$ with the same equivalence relation.

Proposition 5.6. *It is actually an equivalence relation on $M \times S$.*

Proof. Trivial homework. □

Definition 5.7. $S^{-1}M := (M \times S)/\sim$, called a module of fractions.

Proposition 5.8. *$S^{-1}M$ is a module over $S^{-1}A$.*

Proof. The action of the ring of fractions is the obvious one*, the calculations are trivial homework. □

S^{-1} actually gives a functor $A - mod \to S^{-1}A - mod$. We wish to create from $M \xrightarrow{f} N$ another morphism $S^{-1}f : S^{-1}M \to S^{-1}N$. The map is again the obvious one, $\frac{m}{s} \mapsto \frac{f(m)}{s}$. It is well defined for the same reasons as before $u(ms' - sm') = 0$, and so $u(s'f(m) - sf(m')) = 0$ since f is a module homomorphism. $S^{-1}f$ will also be a module homomorphism clearly, following from f being a module hom. It's clear that compositions are also respected, making S^{-1} a functor as stated.

Definition 5.9. $M \xrightarrow{f} N \xrightarrow{g} Q$ is exact at N, if $imf = kerg$.

Proposition 5.10. *S^{-1} is an exact functor, i.e. if $M \xrightarrow{f} N \xrightarrow{g} Q$ is exact, then $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}Q$ is also exact.*

Proof. We need $imS^{-1}f = kerS^{-1}g$. One inclusion is trivial, since $S^{-1}(g \circ f) = S^{-1}0 = 0$ since the original sequence was exact.
Assume now, that $S^{-1}g(\frac{n}{s}) = 0$, we need, that it is in $imS^{-1}f$. We know, that $\frac{g(n)}{s} = \frac{0}{0}$, ergo $\exists t \in S : tg(n) = g(tn) = 0$, so $tn \in kerg$, thus we get that $tn = f(m)$ for some $m \in M$. Now $\frac{n}{s} = S^{-1}f(\frac{m}{st})$ clearly, thus the new sequence is exact. □

Recall the definition of a short exact sequence:

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

with the above sequence exact at M', M, M''. Clearly f is injective, g is surjective and $imf = kerg$. Basically $M' \leq M$, and $M/M' = M''$.
From the previous proposition its clear that for every short exact sequence of A modules we get a SES of $S^{-1}A$ modules. Every ideal is a submodule, the factor is also a module, so we get another SES, namely $S^{-1}(A/U) = S^{-1}A/S^{-1}I$, and clearly $S^{-1}I \lhd S^{-1}A$, and these factors are not only isomorphic as modules,

* $\frac{a}{u}\frac{m}{s} := \frac{am}{us}$

but as rings as well. The LHS consists of elements $\frac{\bar{a}}{s}$, the RHS are $\overline{\frac{a}{s}}$, and we can easily check, that this identification respects products, and 1 as well.
Generally given a ring homomorphism $\phi : A \to B$ if we have an ideal $I \lhd A$, we can extend it $I^e = \phi(I)B$. Similarly for $J \lhd B$ we can take $J^c := \phi^{-1}(J) \lhd A$. These operations are clearly monotone. What happens if we take I^{ec}? This ideal clearly *contains* I. If we take J^{ce} we get some ideal which is *contained in* J. Furthermore $I^{ece} = I^e$ by the previous two remarks, similarly $J^{cec} = J^c$.

Definition 5.11. $I \lhd A$, we call I a contractive ideal (w.r.t. ϕ) if there is $J \lhd B : I = J^c$, or $I^{ec} = I$, and similarly J is an extended ideal iff there is $I \lhd A : I^e = J$ or $J^{ce} = J$.

Restricted to contracted and extended ideals we see that e, c are bijections between these sets.
Now back to $\phi : A \to S^{-1}A$

Proposition 5.12. *Every ideal of $S^{-1}A$ is extended.*

Proof. Look at $J^c = \{a \in a : \frac{a}{1} \in J\}$. Now extend it J^{ce}. Take $\frac{a}{s} \in J$, and clearly $\frac{s}{1}\frac{a}{s} = \frac{a}{1} \in J$, thus $a \in J^c$, thus $\frac{a}{s} = a/s\phi(a) \in J^{ce}$, the other containment always holds and we are done. □

Proposition 5.13. *I is contracted iff ($s \in S, a \in A, sa \in I$ implies that $a \in I$)*.*

Proof. We want $I^{ec} = I$, one inclusion is always true, only need $I^{ec} \subseteq I$. $I^e = \phi(I)S^{-1}A = \{\sum a_i/1 \cdot b_i/s_i : a_i \in I, b_i \in A, s_i \in S\} = \{a/s : a \in A, s \in S\} = S^{-1}I$. for $a \in A$ $a/1 \in I^e$ iff $\exists s \in S : sa \in I$, so the two sets coincide precisely when I is S saturated. □

Corrolary 5.14. *The ideals of $S^{-1}A$ are in bijection with the S-saturated ideals of A.*

6 Sixth lecture

We started studying rings and modules of fractions. We saw that the S-saturated ideals of A correspond bijectively to ideals of $S^{-1}A$. Sums and products of ideals behave as expected $S^{-1}I + S^{-1}J = S^{-1}(I+J)$ and $(S^{-1}I)(S^{-1})J = S^{-1}(IJ)$. We also discussed localisation at a prime ideal P, $S = A \setminus P$ is a multiplicatively closed set and the construction specializes to this case. What are S-saturated ideals in this case?

Remark 6.1. If I is S-saturated, then $I = (1)$ or $I \subseteq P$.

Proof. If $1 \notin I$, then $\forall a \in I$ $a = 1 \cdot a$. By saturatedness $a \notin S$, thus $a \in P$. □

Corrolary 6.2. *$Q \in SpecA$ another prime ideal is S-saturated iff $Q \subseteq P$.*

Proof. If Q is saturated, by the previous proposition we are done, conversely if $Q \subseteq P$, then take $a \notin Q$, and $s \in S$, so $s \notin P$, thus $s \notin Q$ so $sa \notin Q$, and Q is saturated. □

What is $SpecA_P$? As a set it will be $\{J \lhd A_p\} = \{I_P : I \lhd A \text{ S saturated}\}$. The ideal $I_P = \{a/b : a \in I, b \notin P\}$, and by saturatedness (and $I \neq (1)$) $I \subseteq P$. When will an ideal of this form prime? Clearly iff I is a prime ideal. So $SpecA_P = \{Q_P : Q \text{ prime in } A, Q \subseteq P\} \leftrightarrow \{Q \in SpecA : Q \subseteq P\}$.

Corrolary 6.3. *If P is a prime ideal in A, then A_P is a local ring, with maximal ideal P_P. Further $dim A_P = htP = sup\{n : P = P_0 \supset \cdots \supset P_n, P_i \in SpecA\}$.*

*We say that I is S-saturated

Example 6.4. $M \in m - SpecA$, then $A/M = k$ is a field (residue field of M). Now A_M is local, and $A_M/M_M = (A/M)_M = k_M = k$. One step further, consider M_M/M_M^2, this is a module over A_M, isomorphic to $(M/M^2)_M$, this is a module over $A/M = k$, since M annihilates all elements of this, so it is a k-vector space, and localisation does nothing, it is isomorphic (as a vector space) to just M/M^2.

Consider $k = \bar{k}$, $X \subseteq k^n$ an affine algebraic set, $A = \mathcal{A}_X$ and $p \in X$, $M = m_p$ its maximal ideal. Now $A/M = k$. The tangent space of X at p is $T_pX = \{v \in k^n : \forall F \in I(X) : dF(v) = 0\}$, i.e. the vectors which get annihilated by the differentials of the defining equations of X (we evaluate the differential at p, and apply it to v). This is clearly a linear subspace of k^n. Now take the cotangent space $T_p^*X = Hom_k(T_pX, k)$.

Proposition 6.5. *We claim, that this cotangent space is isomorphic to the previously discussed vector space M/M^2.*

Proof. M is the set of polynomial functions on X that vanish at p. To such an f we want to assign its differential at p, which is an element of T_p^*X. since f is in the coordinate ring, we have to prove that this assignment makes sense modulo $I(X)$, i.e. $F \in I(X)$ has to imply that $d_pFv = 0$, but this is precisely the definition of the tangent space, so $\phi : f \mapsto d_pf$ is a well defined map $M \to T_p^*X$. We claim that $ker\phi = M^2$. Firstly if $f, g \in M$, represent them by polynomials F, G with $F|_X = f$, and $G|_X = g$. They both vanish at p, taking $d_p(FG) = F(p)d_pG + G(P) + d_p(F) = 0$. For the converse inclusion let $d_pf \equiv 0$ on T_pX for some $f \in M$. Represent it by a polynomial F. The lift of the ideal of p onto the whole k^n is $\tilde{M} = (x_1 - a_1, \ldots, x_n - a_n)$ if $p = (a_1 \ldots, a_n)$. Since $F(p) = 0$, we can write $F = \sum c_i(x_i - a_i) + \tilde{M}^2$, and see that $d_pF = (c_1, \ldots, c_n)$. By assumption this vector is in the span of $d_pG : G \in I(X)$, so we find a $G \in I(X)$ such that $d_pG = d_pF$, and this $d_p(F - G) = 0$ and $(F - G)(p) = 0$, thus $F \in \tilde{M}^2 + I(X)$ as stated.
Finally we need ϕ to be surjective. $\forall \xi \in T_p^*X$ we take a lift $\tilde{\xi} : k^n \to k$. We can take $\tilde{\xi}(x_1 - a_1, \ldots, x_n - a_n)|_X$ which will be adequate to show surhectivity. □

The upshot is that $T_p^* = M/M^2 = M_M/M_M^2$, where $A_M = \mathcal{O}_{X,p}$ with M_M being the maximal ideal of A_M. The local ring tells you every local information about the point p.

Lemma 6.6. *${}_AM$ a finitely generated module, $\phi \in EndM$, suppose $I \triangleleft A$ such that $im\phi \leq IM$. We claim, that $\exists n \exists a_0, \ldots, a_{n-1} \in I : \phi^n + a_{n-1}\phi^{n-1} + \cdots + a_0 \cdot id = 0$.*

Proof. $M =< m_1, \ldots, m_n >, \forall i : \phi(m_i) = \sum c_{ij}m_j$ with $c_{ij} \in I$. We see, that the product $\phi \cdot 1_n(m_1, \ldots, m_n)^T = C(m_1, \ldots, m_n)$ for some $C \in M_n(I)$ where 1_n is the $n \times n$ identity matrix. We get $(\phi 1_n - C)m = 0$ in $M_n(A[\phi])$. Take now the matrix of signed cofactors of $\phi 1_n - C$ transposed, as you do, call it B and multiply on both sides. As is usual we get $det(\phi 1_n - C)1_n m = 0$, and since the elements of m generate, the element $det(\phi 1_n - C) = 0 \in EndM$. Expanding the determinant, we get the statement. □

Corrolary 6.7 (Nakayama's lemma)**.** *M a finitely generated module with $J(A)M = M$, then $M = 0$.*

Proof. Apply the lemma to $\phi = id$ and $I = J(A)$. We get that $(1 + a)id = 0$ for some $a \in J(A)$, and $1 + a \in U(A)$, thus $id = 0$ and we are done. □

Corrolary 6.8. *M is a finitely generated module, $N \leq M$ and $N + J(A)M = M$, then $N = M$.*

Proof. M/N is again finitely generated, and by the property required $J(A)M/N = M/N$, thus $M/N = 0$ and we are done. □

Corrolary 6.9. *If A is local with maximal ideal m, and we are given a finite module M over A, then if $mM = M$, then $M = 0$.*

Corrolary 6.10. *Suppose A Noetherian local, with maximal ideal m, and $f_1, \ldots, f_n \in m$ such that $\bar{f}_i$ span the vectorspace m/m^2. In this case we claim, that $(f_1, \ldots, f_n) = m$.*

Proof. Its clear that $(f_1, \ldots, f_n) + m^2 = m$ by assumption. Take $N = (f_i : i = 1, \ldots, n)$ and $M = m$. Clearly $m^2 = J(A)M$, and we are done.* □

Corrolary 6.11. *$k = \bar{k}$, $X \subseteq k^n$ affine algebraic set with $p \in X$. Consider the local ring $\mathcal{O}_{X,p}$ of X at p with maximal ideal m. Suppose $f_1, \ldots, f_r \in M = \{f \in \mathcal{A}_X : f(p) = 0\}$ such that $< d_p f_i : i = 1, \ldots, r >= T_p^* X$. We claim, that $m = (f_i : i = 1, \ldots, r)$.*

Proof. Apply the previous corrolary. $\mathcal{O}_{X,p}$ is Noetherian, since it is a localisation of a factor of a Noetherian ring, and $d_p f_i = \bar{f}_i \in m/m^2$, and we are done. □

A ring extension $B \geq A$ is finite if B is a finitely generated module over A.

Proposition 6.12. *$B \geq C \geq A$, and B is finite over C and C is finite over A, then B is finite over A.*

Proof. Actually the statement is if and only if. There are $b_1, \ldots b_n$ $B = \sum Cb_i$ and $C = \sum Ac_j$, thus $B = \sum \sum Ac_j b_i$. □

Definition 6.13. $B \geq A$ a ring extension, $b \in B$ is integral over A iff $\exists n \exists a_0, \ldots, a_{n-1} \in A$ such that $b^n + \cdots + a_0 = 0$, i.e. it satisfies some monic polynomial with coefficients from A.

Remark 6.14. $b \in A$, then b is integral over A, since $b + (-b) = 0$.

Proposition 6.15. *$B \geq A$, and $b \in B$, then TFAE:*

1. *b integral over A*
2. *$A[b]$ is a finite extension of A*
3. *$\exists A \leq C \leq B$ with $b \in C$ and C finite over A*
4. *$\exists_{A[b]} M$ which is finite over A, and $A[b]$ acts faithfully†*

Proof. $1 \to 2 \to 3 \to 4$ is clear, the only hard thing is $4 \to 1$. Use the lemma with $I = A \triangleleft A$, and $\phi : m \mapsto bm$, we get the minimal polynomial of b by the lemma □

7 Seventh lecture

Proposition 7.1. *L a field, $A \leq L$ a subring, A is integrally closed, $\alpha \in L$. Then α is integral over A is equivalent to having α algebraic over $FracA = K$, and $m_\alpha \in A[x]$ (the monic minimal polynomial of α over K).*

*Noetherien property guarantees that m is finitely generated as a module or as an ideal

†$f \in A[b]$ with $fM = 0$, then $f = 0$

Proof. Right to left is clear. If α is algebraic over K, we are done, call M the splitting field of $m_\alpha|L$, here m_α splits into linear factors $\alpha = \alpha_1, \dots, \alpha_n$ are the roots. Adjoin $K(\alpha_1, \dots, \alpha_n)$. There is an element of $Gal(K(...)|K)$ which sends α to α_i for any i, since they are roots of the same irreducible polynomial, thus α_i are integral over A. $m_\alpha(x) = x^n - \sigma_1 x^{n-1} \pm \dots \pm \sigma_n$, and since the α_i's are integral over A, these symmetric polynomials are also integral over A, they are elements of K by definition, and since A is integrally closed, they are in A, which is what we wanted. □

Definition 7.2. $B \geq A \triangleright I$, $b \in B$ we call b integrally closed over I iff there is an n, and $a_0, \dots, a_{n-1} \in I$ with $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$.

Proposition 7.3. *$B \geq A \triangleright I$, $b \in B$ tfae*

1. *b integral over I*
2. *$A[b]$ is finite over A and $b \in \sqrt{IA[b]}$*
3. *there exists $C \leq B$ with $C \geq A$, which is finite over A, and $b \in C$ with $b \in \sqrt{IC}$*
4. *there exists a faithful $A[b]$ module M which is finite over A, and there is an n with $b^n M \leq IM$.*

Proof. $1 \to 2$ is trivial, $2 \to 3$ is trivial, choose $C = A[b]$, $3 \to 4$ is trivial, choose $M = C$. Interesting case is $4 \to 1$, here we do the same as before. Consider the map $\phi : m \mapsto bm$, we constructed a matrix $X \in M_n(A)$ with $p_X(\phi) = 0$ for its characteristic polynomial, and from this we deduce $p_X(b) = 0$.

Lemma 7.4. *If b^n is integral over I, then b is integral over I.*

Proof. There is a k such that $b^{nk} \in \sum_j Ib^{nj} \subseteq \sum_j Ib^j$ and we are done. □

So we may assume that $n = 1$, and we get that $X \in M_n(I)$, and so $p_X(t)$ will have coefficients from I (except the leading 1). □

Corrolary 7.5. *Suppose $B \geq A$ is integral, $I \triangleleft A$ and $b \in B$. We claim that b is integral over I iff $b \in \sqrt{IB}$.*

Proof. Left to right we have $b \in \sqrt{IA[b]} \subseteq \sqrt{IB}$ by the previous statement. For the converse $b^n = a_1b_1 + \dots + a_kb_k$ with $a_i \in I, b_i \in B$. Take $C = A[b_1, \dots]$, a finite extension of A. Clearly $b^n \in IC$, by the third condition we get that b^n is integral over I, thus b is integral over I. □

Proposition 7.6. *$B \geq A$ integral, $P \in specA$, then $PB \cap A = P$*

Proof. $\supseteq$ is trivial. for the other one take $a \in PB \cap A$, and the corollary tells us that a is integrap over P, thus $a \in \sqrt{P} = P$. □

Proposition 7.7. *$B \geq A$ some ring extension, $P \in specA$ with $PB \cap A = P$. Then there is a prime ideal $Q \in specB$ with $Q \cap A = P$.*

Example 7.8. $\mathbb{Z}[i] > \mathbb{Z}$, take $(5) \in spec\mathbb{Z}$, if we extend and contract we just get back (5) as expected, but $5\mathbb{Z}[i]$ is not a prime ideal! There is a prime extesion however, e.g. $(2+i)\mathbb{Z}[i]$.

Proof. Take $S = A \setminus P$, now $PB \cap S = \emptyset$. By Zorn's lemma we see that there is a maximal ideal Q in B with $PB \subset Q$ and $Q \cap S = \emptyset$, and maximal ideals are prime. Now its clear that $Q \cap A \supseteq PB \cap A = P$, and $Q \cap A \subset P$, since it is disjoint from the complement of P. □

Corrolary 7.9. *$B \geq A$ integral and $P \in specA$, then there is a $Q \in specB$ with $Q \cap A = P$.*

Corrolary 7.10 (Going-up theorem (Cohen-Seidenberg))**.** *$B \geq A$ integral extension, and $P_0 \subset P_1 \subset \cdots \subset P_n$ with $P_i \in specA$. Suppose further that we have a partial lift of this chain, $Q_0 \subseteq Q_1 \subseteq \ldots, \subseteq Q_{m-1}$ with $0 \leq m \leq n$ and $Q_i \cap A = P_i$. We claim that there exist $Q_m, \ldots, Q_n$ finishing the job.*

Proof. Assume $m = n$, we extend one step at a time. We can also assume that $m = 1$, if it is 0, we only have to lift a prime, which we already did. So $P_0 \subseteq P_1$, take B/Q_0, which is integral over A/P_0 (every element of B satisfied some relation over A, we just look at the same relation modulo Q_0). By the previous proposition we get a prime $Q \in specB/Q_0$ which lifts P_1/P_0 and we are done. □

Theorem 7.11 (Going down theorem (Cohen-Seidenberg))**.** *$B \geq A$ domains, A integrally closed, B integral over A. Given a chain of prime ideals $P_0 \supseteq P_1 \supseteq \cdots \supseteq P_n$ ($P_i \in specA$) which is partially lifted to $Q_0 \supseteq Q_1 \supseteq \cdots \supseteq Q_{m-1}$ with $Q_i \in specB$ with $Q_i \cap A = P_i$, then the claim is that there is a $Q_m, \ldots, Q_n$ which completes the lift.*

Proof. We may assume $n = m = 1$ as before. Now instead of factoring we have to localise, we are interested in primes contined in Q_0. In general B_{Q_0} will not be integral over A_{P_0} :($P_1 A_{P_0}$ is a prime in the localised ring, we want to see that $P_1 A_{P_0} B_{Q_0} \cap A_{P_0} = P_1 A_{P_0}$, if we know this we get a $Q \in specB_{Q_0}$ which lifts $P_1 A_{P_0}$. We pull this Q back, and calculate. $Q \cap A = Q \cap A_{P_0} \cap A = P_1 A_{P_0} \cap A = P_1$, so it really is a lift. The other thing we whish to see, is $Q_0 \supseteq Q_1$. $Q_1 = Q \cap B \subseteq (Q_0)_{Q_0} \cap B = Q_0 B_{Q_0} \cap B = Q_0$.
For $P_1 A_{P_0} B_{Q_0} \cap A_{P_0} = P_1 A_{P_0}$ the $\supseteq$ part is clear. The LHS consists of elements of the form a/s with $s \in A \setminus P_0$, and there is a $b \in B \setminus Q_0$ such that $ba/s \in P_1 A_{P_0}$. We get that b is not integral over P_0, since $P_0 B \subseteq Q_0$. Now all we need is

Lemma 7.12. *$B \geq A$ domains A integrally closed, $P \in specA$, $b \in B, a \in A, a \notin P$. If ab is integral over P, then b is integral over P.*

Proof. Consider m_b and m_{ab} in $L|K$, with $L = fracB, K = fracA$. The relation we see is $a^n m_b(x) = m_{ab}(ax)$. We need to go deeper

Lemma 7.13. *L a field, A is an integrally closed subring, $K = fracA$, $\alpha \in L$ and $I \triangleleft A$ then α is integral over I iff α is algebraic over K and m_α has all non-leading coefficients in $\sqrt{I}$.*

Proof. Homework. □

□

□

8 Eight lecture

Lemma 8.1. *A integrally closed domain, I an ideal of A, $K = fracA$, and $L|K$: $\alpha \in L$ integral over I is equivalent to having α algebraic over K, with the monic polynomial having coefficients in $\sqrt{I}$.*

Proof. $m_\alpha(\alpha) = 0$, $\alpha^n = -\sum a_i \alpha^i$, so $\alpha^N \in \sum I\alpha^i$ and we are done.
Conversely $m_\alpha(x) = \prod(x - \alpha_i) = x^n + \sum a_i x^i$, where $a_i \in K$ and integral over I, because it is integrally closed and a_i is integral over A as well, they are in A. □

Lemma 8.2. *$B \geq A$ integral extension, B domain, $Q \lhd B$, with $Q \cap A = 0$, then $Q = 0$.*

Proof. $q \in Q$ is integral over A by assumption. $q^n + \sum a_i q^i = 0$ with $a_i \in A$ and n minimal. Reordering $-a_0 = q(q^{n-1} + \sum a_i q^{i-1})$ shows that it is in both A and Q, thus $-a_0 = 0$, and since $q^{n-1} + \ldots$ cannot be zero since n is minimal, we get that $q = 0$. □

Corrolary 8.3. *$B \geq A$ integral extension, $Q_0, Q \lhd B$ such that $Q_0 \in SpecB$. Assume also that $Q_0 \cap A = Q \cap A$, then we conclude that $Q_0 = Q$.*

Proof. $B/Q_0 \geq A/A \cap Q_0$ is integral, the bigger ring will be a domain since Q_0 is prime, and it also satisfies $Q/Q_0 \cap A/Q_0 \cap A = 0$, and we are done. □

Theorem 8.4. *$B \geq A$ integral, then $dimB = dimA$.*

Proof. $\geq$ is just the going up theorem. For $\leq$ we use the previous corollary, intersect a strictly increasing chain with A to get another strictly increasing chain. □

Proposition 8.5. *$B \geq C \geq A$ then $B \geq A$ is integral iff $B \geq C$ and $C \geq A$ are.*

Proof. $\rightarrow$ is trivial since $A \subset C$.
for $b \in B$ we get $b^n = \sum c_i b^i$ with $c_i \in C$, extend to $C_0 = A[c_i]$, which is a finite integral extension of A, B is integral over C_0 as well, so $C_0[b]|C_0$ is finite, thus $C_0[b]|A$ is also finite and we are done with the converse. □

Corrolary 8.6. *$B \geq A$, then $cl_B cl_B A = cl_B A$.*[*]

Proof. $\supset$ is trivial, for $\subset$ $cl_B cl_B A$ is ingegral over $cl_B A$ and also $cl_B A|A$ is integral, thus $cl_B cl_B A|A$ is integral. □

Proposition 8.7. *$B \geq A \supset S$ a multiplicative subset in the smaller ring. We get $S^{-1}B \geq S^{-1}A$, take $\alpha \in S^{-1}B$, it is integral over $S^{-1}A$ iff $\exists s \in S : s\alpha$ is integral over $\bar{A} = \{a/1\} \leq S^{-1}B$.*

Proof. $\leftarrow$: $s\alpha$ is integral over $S^{-1}A$ as well, since $\bar{A}$ is a subring of ot, also $1/s \in S^{-1}A$ and $\alpha = \frac{1}{s} s\alpha$, the product of two integral elements are integral as well.
$\rightarrow$: $\alpha^n = \sum \frac{a_i}{s} \alpha^i$ since we can choose a common denominator. Thus $(s\alpha)^n = \sum a_i s^{n-1-i} (s\alpha)^i$ shows that $s\alpha$ is really integral over $\bar{A}$. □

Example 8.8. $B = \mathbb{C}, A = \mathbb{Z}, S = \mathbb{Z} \setminus \{0\}$, so that $S^{-1}A = \mathbb{Q}$ and $S^{-1}B = \mathbb{C}$. Now if $\alpha \in \mathbb{C}$ α is an algebraic number iff there exists a nonzero number for which $n\alpha$ is an algebraic integer.

Definition 8.9. A a UFD, take $K = fracA$, $p \in A$ irreducible, then we can define the p-adic valuation $v_p : K \rightarrow \mathbb{Z} \cup \infty$. $v_p(0) = \infty$, and $v_p(p^n \frac{a}{b}) = n$ where $a, b \in A$ and $p \not| a, b$, and $n \in \mathbb{Z}$.

From now on $(\Gamma, +, \leq)$ will denote an ordered Abelian group.[†]

Definition 8.10. A Γ-valuation of a field K is: $v : K \rightarrow \Gamma \cup \{\infty\}$ with

- $v(x) = \infty$ iff $x = 0$
- $v(xy) = v(x) + v(y)$

[*] integral closure
[†] $\leq$ is a total order, $\gamma \leq \gamma'$ implies $\gamma + \delta \leq \gamma' + \delta$

- $v(x+y) \geq min(v(x), v(y))$

We call a surjective $\mathbb{Z}$ valuation *discrete valuation.*

Definition 8.11. $v : K \to T \cup \infty$ a valuation, then the valuation ring of K given by v is $A_v = \{x \in K : v(x) \geq 0\}$

Proposition 8.12. *A_v is a subring.*

Proof. $0 \in A_v$ is clear, also $v(1) = 0$ by the multiplicative axiom, thus $1 \in A_v$, and by the properties we get that it is closed under operations, and $2v(-1) = v(1) = 0$, and you cannot have a nonzero element of finite order in an ordered abelian group. □

Proposition 8.13. *K a field, $A \leq K$ when is there a valuation such that $A_v = A$? Iff $\forall 0 \neq x \in K$ $x \in A$ or $x^{-1} \in A$*

Proof. $\to$: is clear since $v(x) + v(x^{-1}) = 0$
$\leftarrow$: Take $\Gamma = U(K)/U(A)$, we order it: $x \leq y$ iff $y/x \in A$. This is a total order by the assumption, and antisymmtery comes from the factorisation. We get our ordered abelian group, the valuation we get trivially by sending 0 to infinity, and every other element to its class. Its clear tha $A_v = A$, and the first two valuation axioms as well, what about addition? $(x + y) \geq xU(A)$ or $yU(A)$. We can assume x, y nonzero, otherwise its trivial. We need that either $x + y/x$ or $(x + y)/y \in A$, which is clear since $1 + x/y$ or $1 + y/x$ is in A $(1 \in A)$. □

Theorem 8.14. *K a field, $A \leq K$, then $cl_K A = \cap\{A_v : A \leq A_v\}$ for all valuation rings, i.e. $\{x \in K : \forall v v|_A \geq 0 \to v(x) \geq 0\}$.*

Proof. If x is integral over A, $x^n + \sum a_i x^i = 0$ and a valuation is given. Apply v to the relation to see $nv(x) \geq min\{v(a_i) + iv(x) \geq iv(x)\}$, so there is an $i < n$ such that $(n - i)v(x) \geq 0$.
For the other inclusion $x \in K$ not integral over A, we want a Valuation ring containing A and excluding x.

Lemma 8.15. *x not integral over A, then x is not integral over $A[x^{-1}]$.*

Proof. If it were $x^n \in \sum_0^{n-1} A[x^{-1}]x^i \subset \sum_{-N}^{N} Ax^i$, thus $x^{n+N} \in \sum_0^{n+N-1} Ax^i$ a contradiction. □

Let $\Sigma = \{K \geq B \geq A[x^{-1}] : x \text{ not integral} | B\}$ Zorns lemma says that we get a maximal such B. We want to prove that for all $y \in K$ either y or y^{-1} is in B. Observe that B is integrally closed in K, if the integral closure were bigger, it would contradict its maximality, since x is not integral over A. If $y \notin B$ we want that $y^{-1} \in B$, and its sufficient to show that y^{-1} is integral over B. x is integral over $B[y]$ by maximality, thus $x^n \in \sum B[y]x^i$, i.e. $1 \in \sum B[y]x^{i-n} = \sum_1^n B[y]x^{-j}$.
x^{-1} is actually in the jacobson radical of B. $1 + x^{-1}b$ is nonzero at least, since $x \notin B$, we need that $B[\frac{1}{1+x^{-1}b}] = B$. x is not integral over B, so $x + b$ is also not integral over B, so its not integral over $B[\frac{1}{x+b}]$, and $B[\frac{b}{x+b}]$ is a subring of this, so its not integral over this either, and $\frac{1}{1+x^{-1}b} = 1 - \frac{b}{x+b}$, so x is not integral over $B[\frac{1}{1+x^{-1}b}]$, and by maximality this has to be equal to B.
Continuing on $1 = \sum_0^N y^k b_k$, where $b_k \in J(B)$, so $y^{-N} = \sum y^{k-N} b_k$, i.e. $y^- N(1 - b_0) \in \sum_1^N y^{k-N} b_k$, where $1 - b_0$ is invertible, since $b_0 \in J(B)$ and thus y^{-1} is integral over B. □

Proposition 8.16. *A is a domain, $dimA = 1$ and Noetherian. Take an ideal I of A, we claim that $\exists Q_1, \dots, Q_n$ primary ideals such that $I = \prod Q_i$, moreover the radicals of the Q_i are distinct, and such a decomposition is unique up to order.*

Proof. By the Lasker-Noether theorem we write $I = \cap Q_i$ where Q_i is P_i primary, and the P_i are distinct, Q_i nonzero, and they are pairwise coprime, so the intersection is the same as the product. We can't have inclusion between nonzero prime ideals, so the primary decmposition is unique. The converse direction is clear as well, we only have to check that the decomposition we get is really a shortest primary decomposition, but that is clear since by taking radicals we see, that no Q_i can contain the intersection of the others. □

Definition 8.17. Dedekind domain is an integrally closed Noetherian domain with dimension 1. We abbreviate it as *DD*.

Fact 8.18. *If A is a DD, and Q a primary ideal, then $Q = P^n$ for some $P \in specA$ and $n \in \mathbb{N}$.*

Fact 8.19. *$|K : \mathbb{Q}| \leq \infty$ then $o_K = K \cap \Omega$ is DD.*
Most of this is simple enough, o_k is clearly integrally closed in K, and so in its field of fractions as well, domain and dimension one is also clear, since it is an integral extension of $\mathbb{Z}$ its dimension is equal to $dim\mathbb{Z} = 1$, the Noetherian property is unclear.

Definition 8.20. A a domain, A is a discrete valuation domain if there is a v on $fracA$ discrete valuation such that $A = A_v$.

Example 8.21. $\mathbb{Z}_{(p)}$ is a DVD of the p-adic valuation.

9 Ninth lecture

Let K be an algebraic number field, i.e. $|K : \mathbb{Q}| < \infty$. Consider the trace function $tr : K \to \mathbb{Q}$, where $\alpha \mapsto tr(\beta \mapsto \alpha\beta)$, we consider the multiplication as a linear map on the finite dimensional $\mathbb{Q}$ vector space K. $tr1 = |K : \mathbb{Q}|$ clearly. We also have the bilinear form $K \times K \to \mathbb{Q}$ defined as $\alpha, \alpha' \mapsto tr(\alpha\alpha')$. It is clearly $\mathbb{Q}$ bilinear and nondegenerate, since if $0 \neq \alpha$, then $tr(\alpha\frac{1}{\alpha}) \neq 0$. If $\alpha \in \mathcal{O}_K = K \cap \Omega$, then the trace will be an integer, since $f(\alpha) = 0$ for some $f \in \mathbb{Z}[x]$, and the map of multiplication by α also satisfies this polynomial, thus all eigenvalues are integers.
Take $\alpha_1, \dots, \alpha_{|K:\mathbb{Q}|} \in \mathcal{O}_k$ a basis of K as a rational vector space. We can do this by choosing some basis, and multiplying the elements by some number so they become algebraic integers. Take the dual basis $\alpha^1, \dots \in K$ so that $tr(\alpha_i\alpha^j) = \delta_i^j$. $\mathcal{O}_K \leq \sum \mathbb{Z}\alpha^i$ is a finite module over $\mathbb{Z}$, so $\mathcal{O}_K$ is also a finite submodule, so he is a Noetherian $\mathbb{Z}$ module, and thus a Noetherian ring. All this implies that the algebraic integers of K are a Dedekind Domain.
The other basic example is if we take $K = \bar{K}$ a field and $C \subset K^n$ an irreducible smooth curve. In this context smooth means, that $\forall p \in C\ dimT_pC = dimC = 1$. If all this is satisfied, then $\mathcal{A}_C$ is also a Dedekind Domain, we will not prove this.
If A is a domain, $K = frac\ A$. We want to think of submodules $M \leq_A K$. We can multiply $M, N \leq_A K$ in the usual way, MN is also an A-submodule, we get a semigroup, the identity is A. We want to think of the invertible elements in this semigroup. If M is invertible, then it is finite over A, since if $MN = A$, then $\sum m_i n_i = 1$, then $m = m \cdot 1 = \sum mn_i m_i$, and $mn_i \in MN = A$, so $M = \sum Am_i$.

Definition 9.1. If $M \leq_A K$ we call M a fractional ideal iff $\exists 0 \neq a \in A : aM \leq A$.

Observe that if M is finite over A, then it is a fractional ideal, the finitely many generators have a common denominator, which multiplies it into A. The converse is true if A is Noetherian, since multiplication by a nonzero a is amodule isomorphism, and aM isa submodule, i.e. an ideal of A, and in a Noetherian ring all ideals are finitely generated.
If $MN = A$, then obviously $N = (A : M) = \{x \in K : xM \subset A\}$, since neccesarily $M(A : M) \subseteq A$, and we can only include elements of $(A : M)$ into N. We get that M is invertible iff $M(A : M) = A$. This is the case iff M is finite over A and for all maximal ideals $m \lhd A$ we get $M_m(A_m : M_m) = A_m$, so the above property has to hold locally.

Lemma 9.2. *${}_AM$ and two submodules given $P, N \leq M$, and S a multiplicative subset of A. Consider $S^{-1}(P : N)$ and we want to compare it to $(S^{-1}P : S^{-1}N)$. $\subseteq$ is clear*, and the other inclusion is also true if N is finite over A.*

Proof. Take the generators of N, some element multiplying $S^{-1}P$ into $S^{-1}N$, then it multiplies the generators as well, then we can multiply by the common denomintator from S since we only have finitely many, and we are done. □

For the statement we can assume M finite over A by the previous calculation. We want to consider $M_m(A_m : M_m) = M_m(A : M)_m$ by the lemma and since M is finite. This is equal to $(M(A : M))_m$, and the statement that this is equal to A_m for all m is equivalent to saying $M(A : M) = A$. One implication is clear,since we just localise back. For the converse the $M(A : M) \subseteq A$ is trivial, for the other one $M(A : M)$ is an ideal of A, and the assumption says that $M(A : M)$ is not contained in any maximal ideal, i.e. it is the unit ideal.

Proposition 9.3. *Suppose A is a domain, we claim that some properties being true is equivalent to them being true locally for all maximal ideals m.*

- *Noetherian*
- *$dim = 1$*
- *integrally closed*
- *primary ideal is a power of a prime ideal*
- *Noetherian and every nonzero fractional ideal is invertible*

Proof. First one. One implication is clear, ideals of A_m correspond monotonically to ideals of A. If we have an infinite sequence in A,the union is also an ideal contained in some maximal ideal, localisation at that ideals shows the converse.
The last one is also clear by the previous statement, $M_m(A_m : M_m)$ is equivalent to having M_m invertible. Observe that if M is a fractional ideal, then M_m is as well. It is enough to check the statement for integral ideals actually, since the principal fractional ideal $a^{-1}A$ inverts.
For dimension $dim\ A = sup\ ht\ m = sup\ dim\ A_m = 1$ in one direction, and if the dimension of A is 1, then any local ring has precisely two prime ideals.

*

Every primary ideal is a power of a prime: Ideals of A_m correspond to ideals contained in m, and primes and primary ideals correspond to each other, so if the statement if true in A, then is will be true in A_m. Conversely take a Q primary, it is contained in some m, localise at that ideal, there it is a prime power, and then contract so $Q = A \cap Q_m = P_m^n \cap A = P^n$.
Integrally closed: Let K be the field of fractions of A, clearly $frac\ A_m = K = frac\ A$. If A is integrally closed, take $\alpha \in K$ which is integral over A_m. We want to prove that $\alpha \in A_m$. For α there is an $s \in A \setminus m$ such that $s\alpha$ is integral over A, so it is contained in A, so $\alpha \in A_m$ clearly. For the converse take $\alpha \in K$ which is integral over A, we need to see that it is contained in A. α is integral over each A_m as well, thus $\alpha \in A_m$ for all m,if we take $\{a \in A : a\alpha \in A\}$ is an ideal of A, which is not contained in any maximal ideal,i.e. it is the unit ideal. □

This means, that from now on we work with only local Dedekind Domains, which turn out to be precisely discrete valuation rings.

Theorem 9.4. *For a domain the following are equivalent*

1. *DVD*
2. *Local DD*
3. *Noetherian local domain such that the unique maximal ideal $m \neq 0$ but is principal*
4. *Noetherian local domain with dim $m/m^2 = 1$*
5. *local, not a field and every nonzero fractional ideal is invertible*
6. *Noetherian local and the maximal ideal is invertible*
7. *Noetherian not a field and there exists an ideal m such that all nonzero ideals are a power of m*
8. *Noetherian local, $dim = 1$ and every primary ideal is a prime power*
9. *not a field, there is an element x such that every nonzero ideal is principal, generated by some powr of x*
10. *PID and there exists a unique nonzero prime ideal*
11. *local PID, not a field*
12. *PID, there exists a "unique"* irreducible element*
13. *UFD and there is a "unique" irreducible element*

Proof. $13 \to 1$ is clear, take the discrete valuation corresponding to the unique irreducible element, every element is of the form $p^n u$ for $n \in \mathbb{Z}$, this is every element of the field of fractions.
$12 \to 13$ is also trivial, every PID is a UFD.
$10 \to 12$ is also clear, that prime ideals are generated by irreducible elements.
$10 \leftrightarrow 11$ is also trivial, locality ensures that we only have a single prime, and thus maximal ideal.
$9 \to 10$ the ideal (x) will be the unique prime. x cannot be a unit since it would be a field.

*up to unit factor

$3 \leftrightarrow 4$ is also clear. Nakayamas lemma guarantees that the dimension is not 0, and the ideal being principal says that we can generate the vectorspace with one vector.
$7 \leftrightarrow 8$ is also easy. The increasing direction we see that m is the unique maximal ideal, so it will be local. Only (0) and m are primes so the dimension is 1, and every primeary is a prime power, since everyone is a prime power. The other direction there is a unique maximal ideal m, why is everyone a power of it? In a 1-dimensional Noetherian domainevery ideal is a product of primaries as seen last time, and every primeary is a prime power and we only have one nonzero prime, namely m, so everyone is a powerof m.
$3, 7 \to 9$ is basically tautological, the element generating m willsuffice for x-
$3 \to 6$ is trivial,...
$6 \to 7$ is mostly clear, we only need that every ideal is a power of m. We use downwards induction (we can do this since it is Noetherian). Consider $0 \neq I \lhd A$ and write $m^{-1}I$ by the hypothesis. We claim that this strictly contains I. $m^{-1} = (A : m) \ni 1$ by assumption, so $I \subseteq m^{-1}I$, but why is it strict? Suppose its equal, then $I = mI$, and by Nakayama's lemma (we are noetherian local) we get that $I = 0$, a contradiction. Now the downwards induction, $m^{-1}I = m^r$, thus $I = m^{r+1}$.
$7 \to 3$ it will be local, since m is the unique biggest ideal, m is nonzero since it is not a field. m is principal since $m \supset m^2$ strictly by Nakayama, choose $t \in m \setminus m^2$. Now $(t) = m^r$, it is contained in m, but not in m^2,thus it generates m, and it is principal.
$5 \to 6$ is also easy, it is Noetherian since all frac ideals are invertible, and so in particular m is, since every integral ideal is also a fractional ideal.
$1 \to 5$ take the discrete valuation, $A = \{x \in K : v(x) \geq 0\}$. $x|y$ is equivalent to having $v(y) \geq v(x)$, both say that $y/s \in A$ or $x = y = 0$. Take the smallest valuation of elements of an ideal, any one with smallest valuation will generate the whole ideal, the same is true for fractional ideals, i.e. the nonzero fractional ideals are precisely $\{v \geq c\}$ for some $c \in \mathbb{Z}$. We have to have a lower bound on our fractional ideals to be able to multiply it into A, and these are all infact ideals, and $\{v \geq c\}\{v \geq -c\} = A$, so they are all invertible, and finally $\{v \geq 1\}$ is clearly a unique maximal ideal of A.
$1 \to 2$ is clear, we see dimension 1 and Noetherian property already. We saw that $A \subseteq cl_K\ A = \cap A_v \subseteq A$ since A itself is a valuation ring.
$2 \to 3$ is the only hard thing. Noetherian and local is already assumed by saying local DD, and m is nonzero since the dimension is 1, we only need that it is principal. Take a nonzero element $a \in A$. *Spec* $A = \{0, m\}$, so *Spec* $A/(a) = \{m/(a)\}$, thus $A/(a)$ is Artinian, and in an artinian local ring $(m/(a))^N = 0$, thus $m^N \subseteq (a)$. Do this with $a \in m$, there is a highest power with $m^n \not\subseteq (a), m^{n+1} \subseteq (a)$. We can find $b \in m^n$ with $a \not| b$. This means that $\frac{b}{a} \notin A$, so $\frac{b}{a}$ is not integral over A either (since it is a DD, integrally closed), and $\frac{b}{a}m \not\subseteq m$, but $\frac{b}{a}m \subseteq A$, further it is an ideal, which is not contained in m (it is true since $bm \subseteq m^n m \subseteq (a)$), so in fact $\frac{b}{a}m = A$, thus $m = \frac{a}{b}A$, and it is principal. □

Theorem 9.5. *A Noetherian domain TFAE*

1. *DD*
2. *for every maximal ideal* m, A_m *is a DVD*
3. $dim A = 1$ *every primary is a prime power*
4. *not a field and every nonzero fractional ideal is invertible*

Proof. $2 \leftrightarrow 3$ these are local properties, and we can read off from the last theorem.
$2 \leftrightarrow 4$ locality we know, if we have the properties for A, then we have the properties locally and the other desciption from above gives us what we want.
$1 \leftrightarrow 2$ local DD is the same as DVD as we just saw. □

Corrolary 9.6. *If A is a DD, any nonzero ideal decomposes uniquely as a product of primes up to order.*

Proof. $P^r = P^2$, then $r = s$, and P^n is P-primary. □

For nonzero fractional ideals $I = P_1^{k_1} \dots I_r^{k_r}$ for some $k_i \in \mathbb{Z}$ and unique again up to order.

10 Tenth lecture

Definition 10.1. B an algebra over k, $\alpha_i \in B$ (k a field). Consider the map $\phi : k[x_1, \dots, x_n] \to B$ the substitution by $\underline{\alpha}$, the image is the subalgebra generated by the α_i. We call the α_i algebraically dependent if ϕ is not injective, independent if it is.

Remark 10.2. α is algebraically dependent iff α is algebraic over k, independent iff it is transcendental. If $\alpha_1, \dots, \alpha_n$ is independent, then $k[\alpha_1, \dots, \alpha_n] = k[x_1, \dots, x_n]$ as a k algebra.

Lemma 10.3 (Noether normalization)**.** *Suppose k a field, B is a finitely generated algebra over k, generated by n elements. Then $\exists d \leq n, \exists y_1, \dots, y_d \in B$ algebraically independent over k such that B is finite over $A = k[y_1, \dots, y_d]$.*

Proof. $B = k[x_1, \dots, x_n]$, if x_1 are algebraically independent, then we are done. Otherwise there is a nonzero polynomial such that $F(x_1, \dots, x_n) = 0$. Let $y_n = x_n, y_i = x_i - x_n^{r_i}$, where $r_i > 0$ will be chosen later. Now $x_i = y_i + y_n^{r_i}$, so the y_i still generate B. Plug in $F(y_1 + y_n^{r_1}, \dots, y_n) = 0$, we want to arrange this to be a monic relation for y_n. This will mean that y_n is integral over $k[y_1, \dots, y_{n-1}]$ and by induction we will be done. Substitute formal variables, so we can work with F as a polynomial $F(Y_1 + Y_n^{r_1}, \dots)$. Originally $F = \sum c_{\alpha_1,\dots,\alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$, after substitution we have to take the Y_n^* term from each component to get $c_{\alpha_1,\dots,\alpha_n} Y_n^{\alpha_1 r_1 + \dots + \alpha_n r_n}$,* we want that the exponent $\alpha_1 r_1 + \dots$ are distinct for all $(\alpha_1, \dots, \alpha_n)$, and this can be achieved easily, since we only have finitely many vectors, since we have a polynomial, we can just put $r_n = r, r_{n-1} = r, r_{n-2} = r^2, \dots$, with $r > max\alpha$, we get a top leading term, which appears only once, we divide by te coefficient and are done. □

Lemma 10.4 (Zariski)**.** *$L|k$ a field extension of finite type (L finitely generated as an algebra), then L is a finite dimensional vector space over k.*

Proof. L is finite of some subalgebra $k[X_1, \dots, D_d]$, if a field is integral over a ring, then the small ring is a field, this is true since every finite extension is integral, a polynomial ring is a field iff $d = 0$. □

Theorem 10.5 (Weak Nullstellensatz)**.** *k a field, consider $\mathcal{F} \subset k[X_1, \dots, X_n]$, assume $(\mathcal{F}) \neq (1)$, then $\exists L|k$ field extension which is finite ($|L : k| < \infty$) with $\alpha_1, \dots, \alpha_n \in L$ such that $\forall f \in \mathcal{F} : f(\alpha_1, \dots, \alpha_n) = 0$.*

*$r_n = 1$

Proof. $\exists M \in m - speck[X_1, \ldots, X_n]$ containing $\mathcal{F}$. Take $L = A/M$ with $A = k[X_1, \ldots, X_n]$. This is a field, the images of the X_i will suffice for the α_i. This is clearly finite since $L = k[\alpha_i]$ is of finite type, thus by Zariskis lemma we are done. □

Proof. If $k = \bar{k}$, then every finite extension is isomorphic to k, and $V(\mathcal{F}) = \emptyset$ iff $(\mathcal{F}) = (1)$. □

Theorem 10.6 (Hilbert's Nullstellensatz)**.** *1. Suppose k a field, $\mathcal{F} \subset k[X_1, \ldots, X_n] \ni g \notin \sqrt{(\mathcal{F})}$, then there is $L|k$ finite field extension and a point $\alpha \in L^n$ with $f(\alpha) = 0 \forall f \in \mathcal{F}$ and $g(\alpha) \neq 0$.*

2. Assume $k = \bar{k}$. $V(\mathcal{F}) \subset V(g)$ iff $g \in \sqrt{(\mathcal{F})}$.

3. $k = \bar{k}$, $I(V(\mathcal{F})) = \sqrt{(\mathcal{F})}$.

Proof. Rabinowitsch trick! Suppose for contradiction $\forall |L : k| < \infty$ $V_L(\mathcal{F}) \subset V_L(g)$, and want to prove that $g \in \sqrt{(\mathcal{F})}$. If we take $\mathcal{F} \cup \{1 - X_0 g\}$, where we extended our polynomialring with a new variable its variety will be empty. Applying the weak nullstellensatz $(\mathcal{F}, 1 - X_0 g) = (1)$. Now $1 = h_0(1 - X_0 g) + \sum_1^N h_i f_i$ with $f_i \in \mathcal{F}, h_i \in k[X_0, X_1, \ldots, X_n]$. First case $g = 0$, then we are done. If it is nonzero, substitute (factor) $X_0 = \frac{1}{g}$, and

$$1 = \sum_1^N h_i(\frac{1}{g}, X_1, \ldots, X_n) f_i(X_1, \ldots, X_n)$$

Now clear denominators by multiplying with g^m to get

$$g^m = \sum_1^N g^m h_i(\frac{1}{g}, X_1, \ldots, X_n) f_i(X_1, \ldots, X_n)$$

and the coefficients are polynomials for $m >> 0$, this represents an element of $g^m \in (\mathcal{F})$ and we are done. The other two follow trivially. □

Remark 10.7. If $k = \bar{k}$, then this theorem tells you that affine algebraic sets correspond bijectively to radical ideals, the correspondence being the I and V operators.

Dimension theory

Theorem 10.8 (Krull's Hauptidealsatz)**.** *A Noetherian, $x \in A$ and $P \in spec\ A$. Assume P is a minimal prime ideal containing x, then ht $P \leq 1$.*

Definition 10.9. *$Q \in spec\ A$, $n \in \mathbb{N}$, then the n-th symbolic power of Q, denoted $Q^{(n)} := \{a \in A : \exists s \in A \setminus Q : sa \in Q^n\}$.*

Remark 10.10. *$\phi : A \to A_Q$ the obvious map, then $\phi^{-1}(Q_Q^n) = Q^{(n)}$. In particular $Q^{(n)}$ is Q-primary.*

Proof. We may assume that A is local and $P = m$, we could pass to A_P, and P_P is a minimal ideal containing $\frac{x}{1}$, and $htP = htP_P$. Take $Q \in spec\ A$, with $Q \subset P$. We want to show that Q is a minimal prime. Clearly $x \notin Q$, moreover $Spec\ A/(x) = \{P/(x)\}$, and this quotient is Artinian (every prime is maximal). Because of this we know that $\exists n : Q^{(n)} \subseteq Q^{(n+1)} + (x)$. $\forall q \in Q^{(n)} \exists q' \in Q^{(n+1)} \exists a \in a : q = a' + xa$, thus $xa = q - q' \in Q^{(n)}$, and x is not contained in this symbolic power, so a is. We get something stronger: $Q^{(n)} = Q^{(n+1)} + xQ^{(n)}$ (the converse inclusion is trivial). By Nakayama's lemma since $x \in P$ and P is the Jacobson radical by locality we get also that $Q^{(n)} = Q^{(n+1)}$. Thus $\phi^{-1}(Q_Q^n) = \phi^{-1}(Q_Q^{n+1})$ implying that $Q_Q^n = Q_Q^{n+1}$ since every ideal of

a local ring is an extended ideal. A_Q is a local ring with maximal ideal Q_Q and by Nakayama we get $Q_Q^n = 0$ and A_Q is Artinian. Now $ht(Q) = ht(Q_Q) = 0$, since Q_Q is the only prime ideal of A_Q, thus Q is a minimal prime. □

Now generalize.

Theorem 10.11. *A Noetherian, $x_1, \ldots, x_c \in A$ and P a minimal prime ideal containing these elements. We claim that $htP \leq c$.*

Proof. If $c = 0, 1$ we are done. Now apply induction, let $c \geq 2$ and the statement is true for $c-1$. We may also assume A to be local with maximal ideal P. Consider $Q \subset P$, want to show that $htQ \leq c-1$. We may assume Q to be a maximal prime contained in P (this exists by the Noetherian property). Say $x_c \notin Q$ by minimality and reindexing if necessary. We want to show that $\exists y_1, \ldots, y_{c-1}$ such that Q is a minimal prime ideal containing them. Consider $A/(Q + (x_c))$, here $\bar{P}$ is a minimal prime, and $\bar{P}^n = 0$, since that ring is Artinian, thus $P^n \subseteq Q + (x_c)$. We can write $x_i^n = y_i + a_i x_c$. We want to check that Q is a minimal prime containing these y_i's. Consider *spec* $A \ni Q_0 \subseteq Q$ containing the y_i, we want to see that $Q_0 = Q$. Observe that $\sqrt{Q_0 + (x_c)} \ni x_i$ and P is a minimal prime containing $Q_0 + (x_c)$, so in A/Q_0 we see $ht\bar{P} \leq 1$ by the Hauptidealsatz, and there cannot be another ideal $Q_0 \subset Q \subset P$ since the second inclusion is strict. □

Theorem 10.12. *k a field, then $dim k[x_1, \ldots, x_d] = d$.*

Proof. $\geq$ is clear, we have $0 \subset (x_1) \subset (X_1, x_2), \ldots,$ a chain of length d.
$\leq$ it is sufficient to show that any maximal ideal $M \triangleleft k[x_1, \ldots, x_d] = A$ has $htM \leq$. There is an $|L : k| < \infty$ and $\alpha \in L^n$ with $f(\alpha) = 0 \forall f \in M$. Take $B = L[x_1, \ldots, x_d]$, then $B \geq A$ is an integral ring extension. If we have a chain $M = P_0 \supset P_1 \supset \cdots \supset P_n$ with $P_i \in$ *spec* A we can lift it by the going down theorem. Choose $Q_0 = (x_1 - \alpha_1, \ldots, x_d - \alpha_d)$, a maximal ideal of B. $P_0 \subset Q_0$ by the relation, thus $Q_0 \cap A = P_0$ and we can lift. We get that $htM \leq htQ_0 \leq d$ by the general Hauptidealsatz. □

Definition 10.13. $L|K$ field extension, the transcendece degree of this extension is defined as $sup\{n : \exists \alpha \in L^n :$ algebraically independent over $K\}$.

Theorem 10.14. *k a field, B a finitely generated algebra over k which is a domain also, and $L = fracB$. We claim that $dimB = tr.deg(L|k)$.*

Proof. Noether normalisation $A = k[x_1, \ldots, x_d] \leq B$ such that B finite over A. $dimB = dimA = d$ as we saw. Take $K = fracA = k(x_1, \ldots, x_d)$, now $tr.deg(K|k) = d$. One direction is clear, the other direction we need to think about later. $L|K$ is an algebraic extension since B is finite over A. It follows that $tr.deg(L|k) = tr.deg(K|k)$. One inequality is clear, for the other one we need to think through that algebraic extensions don't raise the transcendence degree. □

11 Eleventh lecture

Proposition 11.1. *$L|K$ field extension, $\alpha_1, \ldots, \alpha_n \in L$algebraically independent over K and $\beta \in L$, then α_i, β is algebraically dependent precisely when β is algebraic over $K(\alpha_1, \ldots, \alpha_n)$*

Proof. If the numbers are algebraically dependent, then there is $F \in K[x_1, \ldots, x_n, y]$ not identically zero, and vanishing at α_i, β. Group the polynomial according to y $F = \sum f_i(\underline{x})y^i$, and since the α_i's are algebraically independent, and since there is an f_i nonzero, we get that β is algebraic over the field extension.
Conversely if there is a polynomial $G \in K(\alpha_i)[x]$ vanishing at β. We can also assume that $G \in K[\alpha_i][y]$, since the field extension is the ring of fractions of this ring, we can clear denominators. $G = \sum f(\underline{\alpha})y^i$, at least one of the coefficients is nonzero again, we can replace the α's by abstract variables x_i, and we are done, the set α_i, β is algebraically dependent. □

Corrolary 11.2. *Suppose $L|K$ a field extension, $(\alpha_1, \ldots, \alpha_n) = S$ TFAE:*

1. *S is a maximal algebraically independent system*
2. *S is algebraically independent and $L|K(S)$ is an algebraic field extension*
3. *S is minimal such that $L|K(S)$ is algebraic*

Proof. $1 \to 2$ is just the previous proposition.
$2 \to 3 : \forall i$ α_i is transcendental over $K(\alpha_1, \ldots, \hat{\alpha_i}, \ldots, \alpha_n)$ clearly, so S is minimal as claimed.
$2 \to 1$ is the other direction of the proposition.
$3 \to 2$ We may assume $\alpha_1, \ldots, \alpha_i$ algebraically independent with $\alpha_1, \ldots, \alpha_i, \alpha_j$ algebraically dependent for all $j > i$. This means α_j is algebraic over $K(\alpha_1, \ldots, \alpha_i)$, so L itself is already algebraic over this field since algebraic extension of an algebraic extension is algebraic, contradicting the minimality of S. □

Definition 11.3. S is called a trnascendence basis, if it satisfies any (and all) of the previous three properties.

Theorem 11.4. *$L|K$ field extension, $\alpha_1, \ldots$ algebraically independent over K, and $\beta_1, \ldots, \beta_n$ are such that $L|K(\beta_1, \ldots, \beta_n)$ is algebraic.*
We claim, that $\forall i \in [k] \exists j \in [n] : \alpha_1 \ldots, \hat{\alpha_i} \ldots \alpha_k \beta_j$ is algebraically independent over K, and $k \leq n$.

Proof. Indirectly. $\forall j$ β_j would be algebraic over $K(\alpha_1, \ldots, \hat{\alpha}_i, \ldots)$, this means, that α_i is also algebraic over this field (since the β's generate), a contradiction. The second statement follows easily (?) □

Corrolary 11.5. *All transcendence bases of $L|K$ have the same cardinality, and is equal to $tr.deg(L|K)$.*

Corrolary 11.6 (of the Hauptidealsatz)**.** *A noetherian, $P \in specA$, then $htP < \infty$.*

Proof. $P(x_1, \ldots, x_c)$, then $htP \leq c$. □

Corrolary 11.7. *If A is Noetherian and local, then $dimA < \infty$.*

Proof. $dimA = htm$. □

Lemma 11.8 (prime avoidance)**.** *A is a ring, I is an ideal, also $P_1, \ldots, P_n$ are ideals with P_i prime with at most two exceptions ($3 \leq i \leq n$) if $I \subset \cup P_i$, then there is an i with $I \subseteq P_i$*

Proof. We may further assume that $\forall i : I \not\subseteq \cup_{j \neq i} P_i$ since otherwise we could use induction. So there is $x_i \in I \setminus \cup_{j \neq i} P_j \subset P_i$. Now take $x_1 \ldots x_{n-1} + x_n$. Clearly $x_n \in P_n$, and the latter product is not in P_n. If $n \geq 3$ we are done by primality, if $n = 2$ then there is only one term in the product, not in P_n. This element is clearly not in the union of the P_i's and we are done. □

Proposition 11.9. *In a Noetherian ring A every minimal prime ideal belongs to (0). There are finitely many minimal prime ideals. $x \in P$ with P prime and $htP = 0$, then x is a zero divisor.*

Lemma 11.10. *A Noetherian, I an ideal, then there is an n such that $I \supseteq \sqrt{I}^n$.*

Proof. $\sqrt{I} = (a_1, \ldots, a_n)$, take $1 + \sum r_i$ where $a_i^{r_i} \in I$. □

Proof of the proposition. Lasker Noether say that (0) has a primary decomposition Q_i. $Q_i \supseteq P_i^{n_i}$ by the lemma, now $\prod P_i^{n_i} = (0) \subset P$, so $P_i \subseteq P$ for some i, contradicting minimality. □

Theorem 11.11 (Converse of the Hauptidealsatz)**.** *A Noetherian, $P \in specA$. $htP \leq c$, then there exists $x_1, \ldots, x_n \in A$ such that P is a minimal prime containing these elements.*

Proof. If $x_1, \ldots, x_{i-1} \in P$ is already chosen such that $\forall Q \in specA$ with $x_1, \ldots, x_{i-1} \in Q$ and $htQ \geq i-1$, then we want to choose $x_i \in P$ so that the same property holds, any prime containing these i elements has height at least i. We have to assume that $htP \geq i$. The process starts, for $i = 1$ the statement is empty. After that $A/(x_1, \ldots, x_{i-1})$ is Noetherian, the image of P here is not a minimal prime by the Hauptidealsatz (a minimal prime containing $i-1$ elements has height at most $i-1$). By the prime avoidance lemma we can choose $\bar{x}_i \in \bar{P}$ which is not contained in any minimal prime (there are only finitely many minimal primes). Thus we are done, there is Q' containing Q which has height at least i. This process goes until we reach the height of P, as claimed. □

Corrolary 11.12. *A a Noetherian local ring, then $\dim A = htm = \min\{d : \sqrt{(x_1, \ldots, x_d)} = m\}$, i.e. the minimal number of elements needed to generate an m-primary ideal.*

Definition 11.13. A is a Noetherian local ring, $\dim A = d$. $x_1, \ldots, x_d$ is a sequence of parameters if $\sqrt{(x_1, \ldots, x_d)} = m$. We call such a sequence of parameters regular if $(x_1, \ldots, x_d) = m$.

Remark 11.14. There always exists a sequence of parameters.

Suppose we have an affine algebraic set, take the local ring at a point. A sequence of parameters are d local functions, and the variety germ of these functions is just the point we are considering.

Definition 11.15. A Noetherian local ring with a regular sequence of parameters is called a regular local ring.

Remark 11.16. If A is a Noetherian local ring, then $\dim_{A/m} m/m^2$ is precisely the minimalnumber of generators of m. This number is at least the dimension, as we just saw. Equality is achieved if and only if A is regular. Since this vectorspace is the cotangent space, the point will be smooth if and only if the ring is regular, a regular sequence of parameters locally paramterises the variety.

Theorem 11.17 (Auslander-Buchsban)**.** *Every regular local ring is a UFD.*

Proof. We only prove that it is a domain. A a Noetherian local ring, $x \in A$, look at $\dim A/(x)$. If $x \notin m$, then the factor is the 0 ring, and the dimension is < 0. Otherwise it is $\geq \dim A - 1$. $\dim A/(x) = htm/(x) = \min\{k : m/(x) \text{ is a minimal prime containing} \bar{x}_1, \ldots, \beta x_k\}$ this means, that m is a minimal prime containing $x, x_1, \ldots, x_k$. Observe that the dimension of the factor is $\leq \dim A - 1$ if $x \notin \cup_{htP=0} P$.
$\dim_{A/(x)/m/(x)} m/(x)/(m/(x))^2 = \dim_{A/m} m/(m^2+(x)) = \dim_{A/m} m/m^2/(m^2+(x))/m$, and this dimension is the same if $x \in m^2$, or one less if $x \notin m^2$. □

Corrolary 11.18. *If A is a regular local ring, and $x \in m \setminus (m^2 \cup_{htP=0} P)$, then* $\dim A/(x) = \dim A - 1$ *and $A/(x)$ is regular.*

Proposition 11.19. *A regular local ring is a domain.*

Proof. Induction on the Krull dimension. If $\dim A = 0$, then $m = (0)$, and A is a field. Assume $\dim A \geq 1$. Now $htm \geq 1$, so m is not a minimal prime, and $m \neq m^2$ (it would be zero otherwise by Nakayama). By prime avoidance there is an $x \in m \setminus (m^2 \cup_{htP=0} P)$. By the corollary $A/(x)$ is regular, the dimension is strictly less. By induction $A/(x)$ is a domain, so (x) is prime. By the assumptions on x, its principal ideal is not minimal, so we have a prime strictly contained in it, call it P. We want $P = 0$. $P = x(P : x) \subset mP$ and by Nakayama we are done. □

Definition 11.20. $k = \bar{k}$ with $X \subset k^n$ an affine algebraic set, $p \in X$. We call p a smooth/nonsingular point iff $\mathcal{O}_{X,p}$ is regular.

$L|K$ with $X \subset L^n$ a K-Zariski closed set, then X is a Noetherian topological space.

Proposition 11.21. *A Noetherian topological space can be written as a union of irreducible closed subspaces in an irredundant way. This decomposition is unique up to order.*

Proof. Induction, we may assume $\forall Y \subsetneq X$ is a unique union of irreducible closed sets, so X is as well. Irredundancy is also clear.
Take two decompositions $\cup X_i = \cup Y_j$. Now $X_i \subset \cup Y_j$, but it is irreducible, so $X_i \subset Y_j \subset X_{i'}$ if we make the argument once again, by irredundancy this can only happen if $i = i'$, and we are done. □

Back to the story. $X = X_1, \ldots, X_k$ is the decomposition into irreducible sets, $\mathcal{O}_{X,p} = \mathcal{O}_{X_p,p}$ where $X_p = \cup_{p \in X_i} X_i$, if p is smooth, then there is only one component, if there would be more, we could create zero divisors. If p is contained in only one component, then it is a smooth point of X iff it is a smooth point of its component.

Remark 11.22. If X is affine algebraic, $p \in X$ then p is smooth iff $\dim T_p X = \dim X_p$.

Proposition 11.23. *$k = \bar{k}$, X affine algebraic in k^n. $X \to \mathbb{Z}_{\geq 0}$ where $p \mapsto \dim T_p X$ is upper semicontinous, i.e. $\{p \in X : \dim T_p X < c\}$ is a Zariski open set in X.*

Proof. Let $I = I(X)$, $I = (f_1, \ldots, f_k)$ for some polynomials $f_i \in k[x_1, \ldots, x_n] = A$. $\dim T_p X = n - rk(J(f_1, \ldots, f_k)(p))$, the Jacobian has size $k \times n$. Now we only have to check, that the rank of the Jacobian is lowers semicontinous, i.e. $\{p \in X : r(J_p) < r\}$ is Zariski closed. This is clear, since this is equivalent to having all $r \times r$ minors of the matrix vanish, this gives additional polynomial equations and we are done. □

12 Twelfth lecture

Let Kbe an algebraically closed field, $X \subset K^n$ affine algebraic. We claim, that X is irreducible iff A_X is a domain.

Proof. If $Y, Z \subset K^n$ Zariski closed cover X we need, that Y or Z covers X by definition of being irreducible.* We switch to ideals by the nullstellensatz, X, Y, Z corresponds to radical ideals. In this language X being

*X is nonempty by assumption

irreducible means exactly that $I(X) \subset ab$, then a or b is contained in $I(X)$ for all radical ideals a, b. $I(X) \neq (1)$ since X is nonempty. We want to conclude, that this is equivalent to having $I(X)$ prime. Take an arbitrary ideal $a, b \not\subset I(X)$ with $ab \subset I(X)$, then it follows that $\sqrt{a}, \sqrt{b} \not\subset I(X)$, but their product will be contained in $\sqrt{I(X)} = I(X)$ since $\sqrt{ab} \subset \sqrt{a}\sqrt{b}$ and we are done. □

Proposition 12.1. *Let k be any field, consider $m \in m - specA$, where $A = k[x_1, \ldots, x_d]$. We claim $htm = d$.*

Proof. $htm \leq dimA = d$ is already checked. By the nullstellensatz there is a finite extension $L|k$ such that $\alpha \in L^d$. Consider $M = (x_1 - \alpha_1, \ldots) \in m - specB$ where $B = L[x_1, \ldots, x_n]$, and $m \subset M$. $M = M_0 \supset M_1 \supset ... \supset M_d$, where $M_i = (x_1 - \alpha_1, ..., x_{d-i} - \alpha_{d-i})$. Take $P_i = M_i \cap A$ to get another chain $P_0 \supset ....$ $P_0 = M \cap A \subset m$ so it is equal, since m is maximal. The primes will be distinct by a previous lemma, B is integral over A. □

Theorem 12.2. *k is a field, B is a k algebra of finite type which is a domain. $m \in m - specB$, then $htm = dimB =: d$.*

Proof. One inequality is clear, for the other direction we use Noether normalisation. B is finite over $A = k[x_1, \ldots, x_d]$. Consider $P = m \cap A \in m - specA$, it will be maximal by the going up theorem. We already know the statement in the polynomial ring case to get a chain $P_0 \supset P_1 \supset ... \supset P_d$ in A and by the going down theorem we can lift this to B and we are done. □

If we have an irreducible affine algebraic set X over an algebraically closed field k, then A_X will be a domain. Take $p \in X$, and localise at this point, we saw that the height of any maximal ideal is equal to the Krull dimension of B, which is the dimension of X. This means also, that p is a smooth point if and only if $dimT_pX = dimX$. An inequality is always true as seen last time, but does it occur actually?

Theorem 12.3. *$k = \bar{k}$ and $X \subset k^n$ is affine algebraic, irreducible, then the set os smooth points of X denoted X^{smooth} is a Zariski dense open set.*[*]

Proof. We only have to see, that it is nonempty. Let $d = dimX$, and $A = k[x_1, \ldots, x_n]$, denote the ideal of X by I. $B = A/I = A_X$, and $fracB = K_X$ (since B is a domain). Consider the field extension $K_X|k$. We know that $tr.dg(K_X|k) = d$, since it is the same as the Krull dimension of B. Denote the image of x_i restricted to our variety by $\bar{x}_i$. Clearly $K_X = k(\bar{x}_1, \ldots, \bar{x}_n)$, we extract a transcendence basis, so assume that $\bar{x}_1, \ldots, \bar{x}_d$ is such a basis over k. For all $i > d$ we get that there is a polynomial $F \in k[x_1, ..., x_d, x_i]$ which is nonzero, but $F(\bar{x}_1, \ldots, \bar{x}_d, \bar{x}_i) = 0$. Assume that $degF$ is minimal. This means in particular, that $F \in I$. Take the differential $dF = [\partial_j F]$. Minimality implies, that $deg\partial_i F < degF$, it must really depend on the last variable x_i. If this polynomial would be in I, then it would be zero, which it isn't by the previous remark (we use here that $chark = 0$, since otherwise the derivative behaves badly). We get, that for all $i > d$ there is an $F_i \in I$, such that $\partial_i F_i \notin I$. Take $\prod_{d+1}^{n} F_i$, this is still not in I, i.e. there is a point on X, where the product evaluates to a nonzero number. This means also that d_pF_i are linearly independent for $i = d+1, ..., n$. This means, that $dimT_pX \leq d$, since we found at least codimension many vectors orthogonally (the dF_i). □

And now for something completely different.

[*] char k=0

Tensor products of modules

Definition 12.4. Fix a ring A, M, N A-modules, and Z also. We want to study bihomomorphisms, i.e. $\phi : M \times N \to Z$ where: ϕ is linear in both arguments.

For fixed M, N we want to study *all* bihomomorphisms for fixed M, N, which we do by constructing a universal bihomomorphism denoted $\otimes$ to a ring denoted $M \otimes N$. If X is a set, then the A module freely generated by X is denoted $F_X := \oplus_X A$.* Take the free module $F_{M\times N}$ and mod out by a certain submodule to be constructed S. We have a map $M \times N \to F_{M\times N}$ where $(m, n) \to 1(m, n)$, and we want to mod out by a submodule, such that the composition becomes a bihomomorphism, with S as small as possible.

$$S =< (v_1 + v_2, w) - (v_1, w) - (v_2, w),\ (\lambda v, w) - \lambda(v, w),\ (v, w_1, w_2) - (v, w_1) - (v, w_2),\ (v, \lambda w) - \lambda(v, w) >$$

$(m, n) + S$ will be denoted $m \otimes n$. The composition of the injection into the free module, and the factor is called the tensor map, which is clearly the bihomomorphism by construction. Moreover this has a universal property: $M \times N \xrightarrow{\otimes} M \otimes N \xrightarrow{\exists!\psi} Z\ \forall \phi : M \times N \to Z$.

Lemma 12.5. $M \otimes N =< m \otimes n : m \in M, n \in N >$.

Proof. Completely trivial, since $F_{M\times N} =< (m, n) : ... >$, and we take a surjective image of this generating system. □

For the universal property uniqueness of ψ is trivial, since $\psi(m \otimes n) = \phi(m, n)$, it has to be. We can extend ϕ to $F_{M\times N}$, since it is free, $\eta : (m, n) \mapsto \phi(m, n)$, now we want to extend it to the tensor product module. For this one needs to check, that $S \subset ker\eta$. This is clear, since ϕ was a bihomomorphism, so η will also have the same identities and we are done (one only needs to check this on the generators).

Proposition 12.6. *If $M \times N \xrightarrow{\otimes'} M \otimes' N$ which also has the universal property, then there exists q unique isomorphism between $M \otimes N \to M \otimes' N$, which makes the triangle commute.*

Proof. Take $\phi = \otimes'$ and $Z = M \otimes' N$, there is a unique ψ with $\psi\otimes = \otimes'$, and in the other direction as well, there is a unique ψ' with $\otimes'\psi' = \otimes$. Consider the composition $\psi'\psi$ which makes a triangle commute, and the same triangle is commutative with $id_{M\otimes N}$, and similarly for $\otimes'$. □

Proposition 12.7. $A \otimes M = M$

Proof. Take the map $m \mapsto 1 \otimes m$, this map is surjective since $A \otimes M$ is generated by $a \otimes m = 1 \otimes am$. Why is it injective? Because it has an inverse, $a \otimes m \mapsto am$, and we are done† □

Proposition 12.8. *$M \otimes N = N \otimes M$, moreover there is a unique isomorphism with $m \otimes n \mapsto n \otimes m$.*

Clear by construction, or by the universal property. It is also associative up to isomorphism. $M \times N \times P \to (M \otimes N) \otimes P$ with $(m, n, p) \mapsto (m \otimes n) \otimes p$ is a trihomomorphism, moreover it is the universal one! One can look at the section functions $\phi_p : (m, n) \mapsto \phi(m, n, p)$ and use the universal property for the tensor product. This gives a map from $(M \otimes N) \times P \to Z$, we get a unique bihomomorphism, and then use the universal property again. If one takes the tensor products the other way around, we get another universal trihomomorphism, but it is an easy check, that the universal trihomomorphism is also unique up to unique isomorphism.

*direct sum, not product, so only finitely many coefficients are nonzero in any element

†all modules unital!

Example 12.9. $A = \mathbb{Z}$, take abelian groups and consider $\mathbb{Z} \otimes F_2 = F_2$. Note, that in the tensorial way of writing $2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0$. Take $2\mathbb{Z} \leq \mathbb{Z}$ and tensor it with F_2 again, here $2 \otimes 1$ is nonzero, since 2 is a generator of $2\mathbb{Z}$, which is isomorphic as a module to $\mathbb{Z}$. $2\mathbb{Z} \overset{\iota}{\hookrightarrow} \mathbb{Z}$ is injective, but the induced map $2\mathbb{Z} \otimes F_2 \to \mathbb{Z} \otimes F_2$ is not injective.
All types of other terrible behaviour arises as well, compared to vector spaces at least, for example $\mathbb{Q} \otimes \mathbb{Z}/(m) = 0$ for all nonzero m,$q \otimes r = q/m \otimes mr = q/m \otimes 0 = 0$.

A finitely generated algebra $k[S]$, we can ask how fast it generates, i.e. take products from S of length at most n, and consider the dimension of the generated subspace. This is a function $f(n)$ will be the Hilbert function, the degree.
At the exam there will be 2 topics, you choose one, and I choose one:D send the chosen topic 23 hours before the exam.