MATH 902 LECTURE NOTES, SPRING 2022

Contents

Lecture of January 19, 2022

In this class, all rings are assumed to be commutative, with associative multiplication and containing 1.

1. Finiteness conditions

1.1. **Finitely generated algebras.** We start by recalling a definition from last semester, specialized to the setting of commutative rings.

Definition 1.1 (Algebra)**.** Given a ring A, an *A-algebra* is a ring R equipped with a ring homomorphism $\phi : A \to R$. This defines an A-module structure on R given by restriction of scalars, that is, for $a \in A$ and $r \in R$, $ar := \phi(a)r$ that is compatible with the internal multiplication of R i.e.,

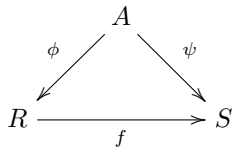
$$a(rs) = (ar)s = r(as) \text{ for all } a \in A, rs \in R.$$

We will call ϕ the *structure homomorphism* of the A-algebra R.

Example 1.2.
- If A is a ring and $x_1, \ldots, x_n$ are indeterminates, the inclusion map $A \hookrightarrow A[x_1, \ldots, x_n]$ makes the polynomial ring into an A-algebra.

- When $A \subseteq R$ the inclusion map makes R an A-algebra. In this case the A-module multiplication ar coincides with the internal (ring) multiplication on R.
- Any ring comes with a unique structure as a $\mathbb{Z}$-algebra.

The collection of A-algebras forms a category where the morphisms are ring homomorphisms $f : R \to S$ such that the following diagram commutes



for structural homomorphisms $\varphi : A \to R$ and $\psi : A \to S$.

Definition 1.3 (Algebra generation)**.** Let R be an A-algebra and let $\Lambda \subseteq R$ be a set. The *A-algebra generated by* a subset Λ of R, denoted $A[\Lambda]$, is the smallest (w.r.t containment) subring of R containing Λ and $\varphi(A)$.

A set of elements $\Lambda \subseteq R$ *generates* R as an A-algebra if $R = A[\Lambda]$.

Note that there are two different meanings for the notation $A[S]$ for a ring A and set S: one calls for a polynomial ring, and the other calls for a subring of something.

This can be unpackaged more concretely in a number of equivalent ways:

Lemma 1.4. *The following are equivalent*

(1) Λ *generates R as an A-algebra.*
(2) *Every element in R admits a polynomial expression in Λ with coefficients in $\phi(A)$, i.e.*

$$R = \left\{ \sum_{\text{finite}} \phi(a)\lambda_1^{i_1} \cdots \lambda_n^{i_n} \mid a \in A, \lambda_j \in \Lambda, i_j \in \mathbb{N} \right\}.$$

(3) *The A-algebra homomorphism $\psi : A[X] \to R$, where $A[X]$ is a polynomial ring on a set of indeterminates X in bijection with Λ and $\psi(x_i) = \lambda_i$, is surjective.*

Proof. Let $S = \left\{\sum_{\text{finite}} \phi(a)\lambda_1^{i_1} \cdots \lambda_n^{i_n} \mid a \in A, \lambda_j \in \Lambda, i_j \in \mathbb{N}\right\}$. For the equivalence between (2) and (3) we note that S is the image of ψ. In particular, S is a subring of R. It then follows from the definition that (1) implies (2). Conversely, any subring of R containing $\phi(A)$ and Λ certainly must contain S, so (2) implies (1). □

Example 1.5. We may have also seen these brackets used in $\mathbb{Z}[\sqrt{d}]$ for some $d \in \mathbb{Z}$ to describe the ring

$$\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

In fact, this is a special instance of generating: the $\mathbb{Z}$-algebra generated by $\sqrt{d}$ in the most natural place, the algebraic closure of $\mathbb{Q}$, is exactly the set above. The point is that for any power $(\sqrt{2})^n$, write $n = 2q + r$ with $r \in \{0, 1\}$, so $(\sqrt{2})^n = 2^d(\sqrt{2})^r$. Similarly, the ring $\mathbb{Z}[\sqrt[3]{d}]$ can be written as

$$\{a + b\sqrt[3]{d} + c\sqrt[3]{d^2} \mid a, b, c \in \mathbb{Z}\}.$$

Note that the homomorphism ψ in part (3) need not be injective.

- If the homomorphism ψ is injective (so an isomorphism) we say that A is a *free* algebra.
- the set $\ker(\psi)$ measures how far R is from being a free A-algebra and is called the set of *relations* on Λ.

Definition 1.6 (Algebra-finite)**.** We say that $\varphi : A \to R$ is *algebra-finite*, or R is a *finitely generated A-algebra*, if there exists a finite set of elements $f_1, \dots, f_d$ that generates R as an A-algebra. We write $R = A[f_1, \dots, f_d]$ to denote this.

The term *finite-type* is also used to mean this.

Remark 1.7. Note that, by the lemma on generating sets, an A-algebra is finitely generated if and only if it is isomorphic to a quotient of a polynomial ring over A in finitely many variables. The choice of an isomorphism with a quotient of a polynomial ring is equivalent to a choice of generating set.

Lecture of January 21, 2022

Example 1.8. Let K be a field, and $B = K[x, xy, xy^2, xy^3, \dots] \subseteq C = K[x, y]$, where x and y are indeterminates. Let A be a finitely generated subalgebra of B, and write $A = K[f_1, \dots, f_d]$. Since each f_i is a (finite) polynomial expression in the monomials $\{xy^i \mid i \in \mathbb{N}\}$, it involves only finitely many of these monomials. Thus, there is an m such that $\{f_1, \dots, f_d\} \subset K[x, xy, \dots, xy^m]$, and hence $A \subseteq K[x, xy, \dots, xy^m]$. But, every element of $K[x, xy, \dots, xy^m]$ is a K-linear combination of monomials with the property that the y exponent is no more than m times the x exponent, so this ring does not contain xy^{m+1}. Thus, B is not a finitely generated K-algebra.

Optional Exercise 1.9. Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be ring homomorphisms (so B is an A-algebra via ϕ, C is a B-algebra via ψ, and C is an A-algebra via $\psi \circ \phi$). Then

- If $A \xrightarrow{\phi} B$ and $B \xrightarrow{\psi} C$ are algebra-finite, then $A \xrightarrow{\psi\phi} C$ is algebra-finite. (Take the union of the generating sets.)
- If $A \xrightarrow{\psi\phi} C$ is algebra-finite, then $B \xrightarrow{\psi} C$ is algebra-finite. (Use the same generating set.)
- If $A \xrightarrow{\psi\phi} C$ is algebra-finite, then $A \xrightarrow{\phi} B$ may *not* be algebra-finite. (Use the previous example.)

Remark 1.10. Any surjective φ is algebra-finite: the target is generated by 1. Since any homomorphism $\phi : A \to R$ can be factored as $\phi = \psi \circ \varphi$ where φ is the surjection $\varphi : A \to A/\ker(\varphi)$ and ψ is the inclusion $\psi : A/\ker(\varphi) \hookrightarrow R$, to understand algebra-finiteness, it suffices to restrict our attention to injective homomorphisms by the last bullet point of the previous exercise.

There are many basic questions about algebra generators that are surprisingly difficult. Let $R = \mathbb{C}[x_1, \dots, x_n]$ and $f_1, \dots, f_n \in R$. When do $f_1, \dots, f_n$ generate R over $\mathbb{C}$? It is not too hard to show that the Jacobian determinant

$$\det \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$$

must be a nonzero constant. It is a big open question whether this is in fact a sufficient condition!

1.2. **Finitely generated modules.** We will also find it quite useful to consider a stronger finiteness property for maps.

Definition 1.11. (Module generation) Let M be an A-module and let $\Gamma \subseteq M$ be a set. The *A-submodule of M generated by* Γ, denoted $\sum_{\gamma \in \Gamma} A\gamma$, is the smallest (w.r.t containment) submodule of M containing Γ.

A set of elements $\Gamma \subseteq M$ *generates* M as an A-module if the submodule of M generated by Γ is M itself, i.e. $M = \sum_{\gamma \in \Gamma} A\gamma$.

This also has some equivalent realizations:

Lemma 1.12. *The following are equivalent:*

(1) Γ *generates* M *as an* A*-module.*
(2) *Every element of* M *admits a linear combination expression in the elements of* Γ *with coefficients in* A*.*
(3) *The homomorphism* $\theta : A^{\oplus Y} \to M$*, where* $A^{\oplus Y}$ *is a free* A*-module with basis* Y *in bijection with* Γ *via* $\theta(y_i) = \gamma_i$*, is surjective.*

Optional Exercise 1.13. Prove the previous lemma.

Definition 1.14 (Module-finite)**.** We say that a ring homomorphism $\varphi : A \to R$ is *module-finite* if R is a finitely-generated A-module, that is, there is a *finite* set $r_1, \dots, r_n \in R$ so that $R = \sum_{i=1}^{n} Ar_i$.

As with algebra-finiteness, surjective maps are always module-finite in a trivial way. The notion of module-finite is much stronger than algebra-finite, since a linear combination is a very special type of polynomial expression. To be specific:

Lemma 1.15 (Module-finite $\Rightarrow$ algebra-finite)**.** *If* $\varphi : A \to R$ *is module-finite then it is algebra-finite.*

The converse is not true.

Example 1.16.
(1) If $K \subseteq L$ are fields, L is module-finite over K just means that L is a finite field extension of K.
(2) The Gaussian integers $\mathbb{Z}[i]$ satisfy the well-known property (or definition, depending on your source) that any element $z \in \mathbb{Z}[i]$ admits a unique expression $z = a + bi$ with $a, b \in \mathbb{Z}$. That is, $\mathbb{Z}[i]$ is generated as a $\mathbb{Z}$-module by $\{1, i\}$; moreover, they form a free module basis!
(3) If R is a ring and x an indeterminate, $R \subseteq R[x]$ is not module-finite. Indeed, $R[x]$ is a free R-module on the basis $\{1, x, x^2, x^3, \dots\}$. It is however algebra-finite.
(4) Another map that is *not* module-finite is the inclusion of $K[x] \subseteq K[x, 1/x]$. Note that any element of $K[x, 1/x]$ can be written in the form $f(x)/x^n$ for some $f(x) \in K[x]$ and $n \in \mathbb{N}$. Then, any finitely generated $K[x]$-submodule M of $K[x, 1/x]$ is of the form $M = \sum_i \frac{f_i(x)}{x^{n_i}} \cdot K[x]$; taking $N = \max\{n_i \mid i\}$, we find that $M \subseteq 1/x^N \cdot K[x] \neq K[x, 1/x]$.

Optional Exercise 1.17. Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be ring homomorphisms. Then

- If $A \xrightarrow{\phi} B$ and $B \xrightarrow{\psi} C$ are module-finite, then $A \xrightarrow{\psi\phi} C$ is module-finite.
- If $A \xrightarrow{\psi\phi} C$ is module-finite, then $B \xrightarrow{\psi} C$ is module-finite.

We will see that $A \xrightarrow{\psi\phi} C$ is module-finite does not imply $A \xrightarrow{\phi} B$ is module-finite soon.

1.3. **Integral extensions.** In field theory, there is a close relationship between (vector space-)finite field extensions and algebraic equations. The situation for rings is similar.

Definition 1.18 (Integral element/extension)**.** Let $\phi : A \to R$ be a ring homomorphism (for which we will denote $\phi(a)$ by a) and $r \in R$. The element r is *integral* if there are elements $a_0, \dots, a_{n-1} \in A$ such that

$$r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0;$$

i.e., r satisfies a *equation of integral dependence* over A. The homomorphism ϕ is *integral* if every element of R is integral over A.

Example 1.19. Let $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. The element $t = \sqrt{2} \in A$ is integral over $\mathbb{Z}$, since $t^2 - 2 = 0$. Likewise, $s = 1 + \sqrt{2}$ is integral over $\mathbb{Z}$, as $s^2 = 3 + 2\sqrt{2}$, so $s^2 - 2s - 1 = 0$.

On the other hand, $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$: if

$$\left(\frac{1}{2}\right)^n + a_{n-1}\left(\frac{1}{2}\right)^{n-1} + \cdots + a_0 = 0$$

with $a_i \in \mathbb{Z}$, multiply through by 2^n to get $1 + 2a_{n-1} + 2^2 a_{n-2} + \cdots + 2^n a_0 = 0$, which is impossible.

Lecture of January 24, 2022

Proposition 1.20. *Let $A \subseteq R$ be rings.*

(1) *If $r \in R$ is integral over A then $A[r]$ is module-finite over A.*
(2) *If $r_1, \ldots, r_t \in R$ are integral over A then $A[r_1, \ldots, r_t]$ is module-finite over A.*

Proof. (1) Suppose r is integral over A, satisfying the equation $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$. Then $A[r] = \sum_{i=0}^{n-1} Ar^i$. Indeed, $s \in A[r]$ with a polynomial expression $s = p(r) = \sum c_j r^j$ of degree $m \geqslant n$, we can use the equation above to rewrite the leading term $a^m r^m$ as $-a_m r^{m-n}(a_{n-1}r^{n-1} + \cdots + a_1 r + a_0)$, and decrease the degree in r.

(2) Write $A_0 := A \subseteq A_1 := A[r_1] \subseteq A_2 := A[r_1, r_2] \subseteq \cdots \subseteq A_t := A[r_1, \ldots, r_t]$. Note that r_i is integral over A_{i-1}: use the same monic equation of r_i over A. Then, the inclusion $A \subseteq A[r_1, \ldots, r_t]$ is a composition of module-finite maps, hence is module-finite. □

We recall that the *classical adjoint* of an $n \times n$ matrix A is the $n \times n$ matrix whose (i, j)-entry is $(-1)^{i+j}$ times the determimant of the matrix obtained from A by removing the ith column and the jth row.

Lemma 1.21 (Determinantal trick)**.** *Let R be a ring, $B \in M_{n\times n}(R)$, $v \in R^{\oplus n}$, and $r \in R$.*

(1) $\mathrm{adj}(B)B = \det(B)I_{n\times n}$.
(2) *If $Bv = rv$, then* $\det(rI_{n\times n} - B)v = 0$.

Proof. (1) When R is a field, this is a basic linear algebra fact. We deduce the case of a general ring from the field case.

The ring R is a $\mathbb{Z}$-algebra, so we can write R as a quotient of some polynomial ring $\mathbb{Z}[X]$. Let $\psi : \mathbb{Z}[X] \twoheadrightarrow R$ be a surjection, $a_{ij} \in \mathbb{Z}[X]$ be such that $\psi(a_{ij}) = b_{ij}$, and let $A = [a_{ij}]$. Note that

$$\psi(\mathrm{adj}(A)_{ij}) = \mathrm{adj}(B)_{ij} \quad \text{and} \quad \psi((\mathrm{adj}(A)A)_{ij}) = (\mathrm{adj}(B)B)_{ij},$$

since ψ is a homomorphism, and the entries are the same polynomial functions of the entries of the matrices A and B, respectively. Thus, it suffices to establish

$$\mathrm{adj}(B)B = \det(B)I_{n\times n}$$

in the case when $R = \mathbb{Z}[X]$, and we can do this entry by entry. Now, $R = \mathbb{Z}[X]$ is an integral domain, hence a subring of a field (its fraction field). Since both sides of the equation

$$(\mathrm{adj}(B)B)_{ij} = (\det(B)I_{n\times n})_{ij}$$

live in R and are equal in the fraction field (by linear algebra) they are equal in R. This holds for all i, j, and thus 1) holds.

(2) We have $(rI_{n\times n} - B)v = 0$, so by part 1)

$$\det(rI_{n\times n} - B)v = \mathrm{adj}(rI_{n\times n} - B)(rI_{n\times n} - B)v = 0.$$ □

Theorem 1.22. *Let $A \subseteq R$ be module-finite. Then R is integral over A.*

Proof. Given $r \in R$, we want to show that r is integral over A. The idea is to show that multiplication by r, realized as a linear transformation over A, satisfies the characteristic polynomial of that linear transformation.

Write $R = Ar_1 + \cdots + Ar_t$. We may assume that $r_1 = 1$, perhaps by adding module generators. By assumption, we can find $a_{ij} \in A$ such that

$$rr_i = \sum_{j=1}^{t} a_{ij} r_j$$

for each i. Let $C = [a_{ij}]$, and v be the column vector $(r_1, \ldots, r_t)$. We have $rv = Cv$, so by the determinant trick, $\det(rI_{n\times n} - C)v = 0$. Since we chose one of the entries of v to be 1, we have in particular that $\det(rI_{n\times n} - C) = 0$. Expanding this determinant as a polynomial in r, this is a monic equation with coefficients in A. □

Collecting the previous results, we now have a useful characterization of module-finite extensions:

Corollary 1.23 (Characterization of module-finite extensions)**.** *Let $A \subseteq R$ be rings. R is module-finite over A if and only if R is integral and algebra-finite over A.*

Proof. ($\Rightarrow$): A generating set for R as an A-module serves as a generating set as an A-algebra. The remainder of this direction comes from the previous theorem. ($\Leftarrow$): If $R = A[r_1, \ldots, r_t]$ is integral over A, so that each r_i is integral over A, then R is module-finite over A by Proposition 1.20. □

Corollary 1.24. *If R is generated over A by integral elements, then R is integral. Thus, if $A \subseteq S$, the set of elements of S that are integral over A form a subring of S.*

Proof. Let $R = A[\Lambda]$, with λ integral over A for all $\lambda \in \Lambda$. Given $r \in R$, there is a finite subset $L \subseteq \Lambda$ such that $r \in A[L]$. By the theorem, $A[L]$ is module-finite over A, and $r \in A[L]$ is integral over A.

For the latter statement, the first statement implies that

$$\{\text{integral elements}\} \subseteq A[\{\text{integral elements}\}] \subseteq \{\text{integral elements}\},$$

so equality holds throughout, and {integral elements} is a ring. □

Example 1.25.

(1) Not all integral extensions are module-finite. Let $K = \overline{K}$, and consider the ring

$$R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots] \subseteq \overline{K(x)}.$$

Clearly R is generated by integral elements over $K[x]$, hence integral, but is not algebra-finite over $K[x]$.

(2) Let x, y, z be indeterminates. Set $R = \mathbb{C}[x, y]$ to be a polynomial ring, and $S = \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$ to be a quotient of a polynomial ring. We claim that we can realize R as a subring of S; i.e., the $\mathbb{C}$-algebra homomorphism from R to S that sends x to x and y to y is injective. Indeed, the kernel is the set of polynomials in x, y that are multiples of $z^2 + x^2 + y^2$, but, thinking of $\mathbb{C}[x, y, z]$ as $R[z]$, any nonzero multiple of $z^2 + x^2 + y^2$ must have z-degree at least 2, so none only involve x, y. Thus, we have an inclusion $R \subseteq S$.

The ring S is module-finite over R: indeed, S is generated over R as an algebra by one element z that is integral over R.

Lecture of January 26, 2022

Definition 1.26. If $A \subseteq R$, the *integral closure of A in R* is the set of elements of R that are integral over A. If R is a domain, the *integral closure* of R is its integral closure in its fraction field.

Example 1.27. $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$: this follows from essentially the same argument we used to show that $\frac{1}{2}$ is not integral over $\mathbb{Q}$.

Optional Exercise 1.28. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ is $\begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4. \end{cases}$

Optional Exercise 1.29. Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be ring homomorphisms. Then $A \xrightarrow{\phi} B$ and $B \xrightarrow{\psi} C$ are integral if and only if $A \xrightarrow{\psi\phi} C$ is integral.

Here is a useful fact about integral extensions that we will use multiple times; it also gives a flavor for the power of the integrality condition on a map.

Proposition 1.30. *Let R and S be domains and $R \subseteq S$ be integral. Then R is a field if and only if S is a field.*

Proof. ($\Rightarrow$) Say $R = K$ is a field and let $s \in S$ be nonzero. The ring $K[s]$ is integral over K and algebra-finite, hence module finite; i.e., a finite dimensional vector space. Then multiplication by s on $K[s]$ is an injective K-linear map, since $K[s] \subseteq S$ is a domain, and hence surjective. This means that s has an inverse, and hence S is a field.

($\Leftarrow$) Say $S = L$ is a field and let $r \in R$. Then $r^{-1} \in L$ and is hence integral over R. Take an integral equation

$$(r^{-1})^n + a_1(r^{-1})^{n-1} + \cdots + a_n = 0$$

with $a_i \in R$, and multiply through by r^{n-1} to get

$$r^{-1} + a_1 + a_2 r + \cdots + a_n r^{n-1} = 0,$$

so $r^{-1} \in R$. □

1.4. **Commutative Noetherian rings and modules.** We recall that a ring R is *Noetherian* if the following equivalent conditions hold:

(1) The set of ideals of R has ACC (every ascending chain has a maximal element)
(2) Every nonempty collection of ideals of R has a maximal element (i.e., an ideal not contained in any other; not necessarily a maximal ideal though)
(3) Every ideal of R is finitely generated.

Similarly, a module M is *Noetherian* if the following equivalent conditions hold:

(1) The set of submodules of M has ACC (every ascending chain has a maximal element)
(2) Every nonempty collection of sumbodules of M has a maximal element
(3) Every submodule of M is finitely generated.

When R is Noetherian, a module is finitely generated if and only if it is Noetherian, and hence every submodule of a finitely generated module is finitely generated.

Example 1.31.
(1) If K is a field, the only ideals in K are (0) and (1) = K, so K is a Noetherian ring.
(2) $\mathbb{Z}$ is a Noetherian ring. More generally, if R is a PID, then R is Noetherian. Indeed, every ideal is finitely generated!

(3) As a special case of the previous example, consider the ring of germs of complex analytic functions near 0,

$$\mathbb{C}\{z\} := \{f(z) \in \mathbb{C}[\![z]\!] \mid f \text{ is analytic on a neighborhood of } z = 0\}.$$

This ring is a PID: every ideal is of the form (z^n), since any $f \in \mathbb{C}\{z\}$ can be written as $z^n g(z)$ for some $g(z) \neq 0$, and any such $g(z)$ is a unit in $\mathbb{C}\{z\}$.

(4) A ring that is *not* Noetherian is a polynomial ring in infinitely many variables over a field k, $R = k[x_1, x_2, \ldots]$: the ascending chain of ideals

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$$

does *not* stabilize.

(5) The ring $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots]$ is also *not* Noetherian. A nice ascending chain of ideals is

$$(x) \subsetneqq (x^{1/2}) \subsetneqq (x^{1/3}) \subsetneqq (x^{1/4}) \subsetneqq \cdots.$$

(6) The ring of continuous real-valued functions $\mathcal{C}(\mathbb{R}, \mathbb{R})$ is *not* Noetherian: the chain of ideals

$$I_n = \{f(x) \mid f|_{[-1/n, 1/n]} \equiv 0\}$$

is increasing and proper. The same construction shows that the ring of infinitely differentiable real functions $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ is not Noetherian: properness of the chain follows from, e.g., Urysohn's lemma (though it's not too hard to find functions distinguishing the ideals in the chain). Note that if we asked for analytic functions instead of infinitely-differentiable functions, every element of the chain would be the zero ideal!

Remark 1.32. If R is Noetherian and $I \subseteq R$, then R/I is Noetherian as well, since there is an order-preserving bijection

$$\{\text{ideals of } R \text{ that contain } I\} \leftrightarrow \{\text{ideals of } R/I\}.$$

Definition 1.33. If R is a commutative ring and x is an indeterminate the set

$$R[\![x]\!] = \left\{ \sum_{i \geqslant 0} r_i x^i \mid r_i \in R \right\}$$

with the obvious addition and multiplication is called the *power series ring* in the variable x with coefficients in R. If $x_1, \ldots, x_d$ are distinct indeterminates the *power series ring* in all of these variables is defined inductively as

$$R[\![x_1, \ldots, x_n]\!] = (R[\![x_1, \ldots, x_{d-1}]\!])\,[\![x_d]\!].$$

We will now give a huge family of Noetherian rings.

Theorem 1.34 (Hilbert's Basis Theorem)**.** *Let R be a Noetherian ring. Then the rings $R[x_1, \ldots, x_d]$ and $R[\![x_1, \ldots, x_d]\!]$ are Noetherian.*

Proof. We give the proof for polynomial rings, and indicate the difference in the power series argument. By induction on d, we can reduce to the case $d = 1$. Given $I \subseteq R[x]$, let

$$J = \{a \in R \mid \text{there is some } ax^n + \text{lower order terms (wrt } x) \in I\}.$$

So $J \subseteq R$ consists of all the leading coefficients of polynomials in I. We can check (exercise) that this is an ideal of R. By our hypothesis, J is finitely generated, so let $J = (a_1, \ldots, a_t)$. Pick $f_1, \ldots, f_t \in R[x]$ such that the leading coefficient of f_i is a_i, and set $N = \max_i \{\deg f_i\}$.

Given any $f \in I$ of degree greater than N, we can cancel off the leading term of f by subtracting a suitable combination of the f_i, so any $f \in I$ can be written as $f = g + h$ where $h \in (f_1, \dots, f_t)$ and $g \in I$ has degree at most N, so $g \in I \cap (R + Rx + \cdots + Rx^N)$. Note that since $I \cap (R + Rx + \cdots + Rx^N)$ is a submodule of the finitely generated free R-module $R + Rx + \cdots + Rx^N$, it is also finitely generated as an R-module. Given such a generating set, say $I \cap (R + Rx + \cdots + Rx^N) = (f_{t+1}, \dots, f_s)$, we can write any such $f \in I$ as an $R[x]$-linear combination of these generators and the f_i's. Therefore, $I = (f_1, \dots, f_t, f_{t+1}, \dots, f_s)$ is finitely generated, and $R[x]$ is a Noetherian ring.

In the power series case, take J to be the coefficients of *lowest degree* terms. □

Corollary 1.35. *If R is Noetherian, then any finitely generated R-algebra is Noetherian as well.*

Proof. A finitely generated R-algebra is a quotient ring of a polynomial ring in finitely many variables over R. □

Note that the converse to this is false, e.g., a power series ring over a field is Noetherian, but is not a finitely generated algebra.

Lecture of January 28, 2022

We now give a subtle connection between the finiteness conditions discussed.

Theorem 1.36 (Artin-Tate Lemma)**.** *Let $A \subseteq B \subseteq C$ be rings. Assume that*

- *A is Noetherian,*
- *C is module-finite over B, and*
- *C is algebra-finite over A.*

Then, B is algebra-finite over A.

Proof. Let $C = A[f_1, \dots, f_r]$ and $C = Bg_1 + \cdots + Bg_s$. Then,

$$f_i = \sum_j b_{ij} g_j \quad \text{and} \quad g_i g_j = \sum_k b_{ijk} g_k$$

for some $b_{ij}, b_{ijk} \in B$. Let $B_0 = A[\{b_{ij}, b_{ijk}\}] \subseteq B$. Since A is Noetherian, so is B_0.

We claim that $C = B_0\, g_1 + \cdots + B_0 g_s$. Given an element $c \in C$, write c as a polynomial expression in $f_1, \dots, f_r$, and since the f_i are linear combinations of the g_i, we can rewrite $c \in A[\{b_{ij}\}][g_1, \dots, g_s]$. Then using the equations for $g_i g_j$ we can write c in the form required.

Now, since B_0 is Noetherian, C is a finitely generated B_0-module, and $B \subseteq C$, then B is a finitely generated B_0-module, too. In particular, $B_0 \subseteq B$ is algebra-finite. We conclude that $A \subseteq B$ is algebra-finite, as required. □

1.5. **Application: Finite generation of rings of invariants.** Historically, commutative algebra has roots in classical questions of algebraic and geometric flavors, including the following natural question:

Question 1. *Given a (finite) set of symmetries, consider the collection of polynomial functions that are fixed by all of those symmetries. Can we describe all the fixed polynomials in terms of finitely many of them?*

To make this precise, let G be a group acting on a ring R, or just as well, a group of automorphisms of R. The main case we have in mind is when $R = K[x_1, \dots, x_d]$ is a polynomial ring and K is a field. We are interested in the set of elements that are *invariant* under the action,

$$R^G := \{r \in R \mid g(r) = r \text{ for all } g \in G\}.$$

Note that R^G is a subring of R. Indeed, given $r, s \in R^G$, then

$$r - s = g \cdot r - g \cdot s = g \cdot (r - s) \quad \text{and} \quad rs = (g \cdot r)(g \cdot s) = g \cdot (rs) \qquad \text{for all } g \in G,$$

since each g is a homomorphism. Note also that if $G = \langle g_1, \ldots, g_t \rangle$, then $r \in R^G$ if and only if $g_i(r) = r$ for $i = 1, \ldots, t$. The question above can now be rephrased as follows:

Question 2. *Given a finite group G acting on $R = K[x_1, \ldots, x_d]$, is R^G a finitely generated K-algebra?*

Observe that, in this setting, R^G is a K-subalgebra of R, which is a finitely generated K-algebra, but this does not guarantee a priori that R^G is a finitely generated K-algebra.

Example 1.37 (Negative variables)**.** Let $G = \{e, g\}$ act on $R = K[x]$ by negating the variable: $g \cdot x = -x$ for all i, so $g \cdot f(x) = f(-x)$. Suppose that the characteristic of K is not 2, so $-1 \neq 1$. Write $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. We have $g \cdot x^i = (-x)^i = (-1)^i x^i$, so

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

which differs from f unless for each odd i, $a_i = 0$. That is,

$$R^G = \{f \in R \mid \text{every term of } f \text{ has even degree}\}.$$

Any such f is a polynomial in x^2, so we have

$$R^G = K[x^2].$$

Optional Exercise 1.38. Generalize the last example as follows: let K be a filed with a primitive dth root of unity ζ, and let $G = \langle g \rangle \cong C_d$ act on $K[x_1, \ldots, x_n]$ via $g \cdot x_i = \zeta x_i$ for all i. Then

$$R^G = \{f \in R \mid \text{every term of } f \text{ has degree a multiple of } d\} = K[\{\text{monomials of degree d}\}].$$

Example 1.39 (Standard representation of the symmetric group)**.** Let S_n be the symmetric group on n letters acting on $R = K[x_1, \ldots, x_n]$ via $\sigma(x_i) = x_{\sigma(i)}$.

For example, if $n = 3$, then $f = x_1^2 + x_2^2 + x_3^2$ is invariant, while $g = x_1^2 + x_1 x_2 + x_2^2 + x_3^2$ is not, since swapping 1 with 3 gives a different polynomial.

You may recall the Fundamental Theorem of Symmetric Polynomials says that every element of R^{S_n} can be written as polynomial expression in the elementary symmetric polynomials

$$\begin{aligned} e_1 &= x_1 + \cdots + x_n \\ e_2 &= \sum x_i x_j \\ &\vdots \\ e_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

E.g, f above is $e_1^2 - 2e_2$. (Moreover, any symmetric polynomial can be written like so in a *unique* way, so R^{S_n} is a free K-algebra.) So even though we have infinitely many invariant polynomials, we can understand them in terms of only finitely many of them, which are *fundamental* invariants.

Proposition 1.40. *Let K be a field, R be a finitely-generated K-algebra, and G a finite group of automorphisms of R that fix K. Then $R^G \subseteq R$ is module-finite.*

Proof. Since integral implies module-finite, we will show that R is algebra-finite and integral over R^G.

First, since R is generated by a finite set as a K-algebra, and $K \subseteq R^G$, it is generated by the same finite set as an R^G-algebra as well. Extend the action of G on R to $R[t]$ with G fixing t. Now, for $r \in R$, consider the polynomial $F_r(t) = \prod_{g\in G}(t - g(r)) \in R[t]$. Then G fixes $F_r(t)$, since for each $h \in G$,

$$h(F_r(t)) = h\prod_{g\in G}(t - g\cdot r)) = \prod_{g\in G}(h\cdot t - hg\cdot r) = F_r(t)$$

Thus, $F_r(t) \in (R[t])^G$. Notice that $(R[t])^G = R^G[t]$, since

$$g\cdot(a_nt^n + \cdots + a_0) = a_nt^n + \cdots + a_0 \implies (g\cdot a_n)t^n + \cdots + (g\cdot a_0) = a_nt^n + \cdots + a_0.$$

Therefore, $F_r(t) \in R^G[t]$. The leading term (with respect to t) of $F_r(t)$ is $t^{|G|}$, so $F_r(t)$ is monic, and r is integral over R^G. Therefore, R is integral over R^G. □

Theorem 1.41 (Noether's finiteness theorem for invariants of finite groups)**.** *Let K be a field, R be a polynomial ring over K, and G be a finite group acting K-linearly on R. Then R^G is a finitely generated K-algebra.*

Proof. Observe that $K \subseteq R^G \subseteq R$, that K is Noetherian, $K \subseteq R$ is algebra-finite, and $R^G \subseteq R$ is module-finite. Thus, by the Artin-Tate Lemma, we are done! □

Lecture of January 31, 2022

2. Graded rings

2.1. **Basics of graded rings.** When we think of a polynomial ring R, we often think of R with its graded structure, in terms of degrees of elements. Other rings we have seen also have a graded structure, and this structure is actually very powerful.

Definition 2.1. An $\mathbb{N}$-*graded ring* is a ring R equipped with a direct sum decomposition as additive groups

$$R = \bigoplus_{a\geqslant 0} R_a,$$

such that $R_aR_b \subseteq R_{a+b}$ for every $a, b \in \mathbb{N}$, meaning that for any $r \in R_a$ and $s \in R_b$, we have $rs \in R_{a+b}$.

We say R is a *positively graded A-algebra* if R is $\mathbb{N}$-graded with $R_0 = A$.

More generally, for a semigroup T, a T-*graded* ring is a ring R with a direct sum decomposition of R as an additive group indexed by T:

$$R = \bigoplus_{a\in T} R_a$$

satisfying $R_aR_b \subseteq R_{a+b}$. We will assume for convenience that any grading semigroup is cancellative.

An element that lies in one of the summands R_a is said to be *homogeneous* of *degree* a; we write $|r|$ or $\deg(r)$ to denote the degree of a homogeneous element r.

By definition, an element in a graded ring is uniquely a sum of homogeneous elements, which we call its *homogeneous components* or *graded components*; we may write $[f]_d$ for the dth homogeneous component of f. One nice thing about graded rings is that many properties can usually be sufficiently checked on homogeneous elements, and these are often easier to deal with.

Lemma 2.2. *Let R be a T-graded ring.*

(1) *1 is homogeneous of degree $0 \in T$ (the identity of T).*
(2) *R_0 is a subring of R.*

(3) *Each R_a is a R_0-module.*

Proof. (1) Write $1 = \sum_a r_a$ with r_a homogeneous of degree a. Then $r_0 = r_0(\sum_a r_a) = \sum_a r_0 r_a$ implies $r_0 r_a = 0$ for $a \neq 0$. Similarly, taking the R_a component of $r_a = r_a(\sum_b r_b)$ yields $r_a = r_a r_0$ (here is where we use the cancellative assumption). Thus $r_a = 0$ for $a \neq 0$, so $1 \in R_0$.

(2) R_0 is a subgroup under addition, and $r, s \in R_0$ implies $rs \in R_0$. We also just showed $1 \in R_0$.

(3) R_a is a subgroup under addition, and $r \in R_0$, $s \in R_a$ implies $rs \in R_a$.

□

Remark 2.3. Note that whenever R is a graded ring, the multiplicative identity 1 must be a homogeneous element whose degree is the identity in T. In particular, if R is $\mathbb{N}$ or $\mathbb{Z}$-graded, then $1 \in R_0$ and R_0 is a subring of R.

Example 2.4. Let K be a field, and $R = K[x_1, \ldots, x_n]$ be a polynomial ring.

(1) There is an $\mathbb{N}$-grading on R called the *standard grading* where

$$R_d = K \cdot \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \sum_i \alpha_i = d\}.$$

Of course, this is the notion of degree familiar from grade school. So $x_1^2 + x_2 x_3$ is homogeneous in the standard grading, while $x_1^2 + x_2$ is not.

(2) We can give different $\mathbb{N}$-gradings on R by fixing some tuple $(\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ and letting x_i be a homogeneous element of degree β_i; we call this a grading with *weights* $(\beta_1, \ldots, \beta_n)$. Concretely,

$$R_d = K \cdot \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \sum_i \beta_i \alpha_i = d\}.$$

For example, in $K[x_1, x_2]$, $x_1^2 + x_2^3$ is not homogeneous in the standard grading, but it is homogeneous of degree 6 under the $\mathbb{N}$-grading with weights $(3, 2)$.

(3) A polynomial ring $R = K[x_1, \ldots, x_n]$ also admits a natural $\mathbb{N}^n$-grading, with

$$R_{(d_1, \ldots, d_n)} = K \cdot x_1^{d_1} \cdots x_n^{d_n}.$$

This is called the *fine grading*.

Definition 2.5. An ideal I in a graded ring R is called *homogeneous* if it can be generated by homogeneous elements.

Lemma 2.6. *Let I be an ideal in a graded ring R. The following are equivalent:*

(1) *I is homogeneous.*

(2) *For any element $f \in R$ we have $f \in I$ if and only if every homogeneous component of f lies in I.*

(3) *$I = \bigoplus_{a \in T} I_a$, where $I_a = I \cap R_a$.*

Proof. (1) $\Rightarrow$ (2): If I is homogeneous and $f \in I$, write f as a combination of the (homogeneous) generators of I, say $f_1, \ldots, f_n$:

$$f = r_1 f_1 + \cdots + r_n f_n.$$

Write each r_i as a sum of its components, say $r_i = [r_i]_{d_{i,1}} + \cdots + [r_i]_{d_{i,m_i}}$. Then, after substituting and collecting,

$$f = \sum_d ([r_1]_{d - |f_1|} f_1 + \cdots + [r_n]_{d - |f_n|} f_n)$$

expresses f as a sum of homogeneous elements of different degrees, so

$$f_d = [r_1]_{d-|f_1|}f_1 + \cdots + [r_n]_{d-|f_n|}f_n \in I.$$

(2) $\Rightarrow$ (1): Any element of I is a sum of its homogeneous components. Thus, in this case, the set of homogeneous elements in I is a generating set for I.

(2) $\Rightarrow$ (3): As above, I is generated by the collection of additive subgroups $\{I_a\}$ in this case; the sum is direct as there is no nontrivial $\mathbb{Z}$-linear combination of elements of different degrees.

(3) $\Rightarrow$ (2): Clear. □

Example 2.7. Given an $\mathbb{N}$-graded ring R, then $R_+ = \bigoplus_{d>0} R_d$ is a homogeneous ideal.

We now observe the following:

Lemma 2.8. *Let R be an T-graded ring, and I be a homogeneous ideal. Then R/I has a natural T-graded structure induced by the T-graded structure on R.*

Proof. The ideal I decomposes as the direct sum of its graded components, so we can write

$$R/I = \frac{\oplus R_a}{\oplus I_a} \cong \oplus \frac{R_a}{I_a}.$$ □

Example 2.9.
(1) The ideal $I = (w^2x + wyz + z^3, x^2 + 3xy + 5xz + 7yz + 11z^2)$ in $R = K[w, x, y, z]$ is homogeneous with respect to the standard grading on R, and thus the ring R/I admits an $\mathbb{N}$-grading with $|w| = |x| = |y| = |z| = 1$.
(2) In contrast, the ring $R = k[x, y, z]/(x^2 + y^3 + z^5)$ does not admit a grading with $|x| = |y| = |z| = 1$, but does admit a grading with $|x| = 15, |y| = 10, |z| = 6$.

Definition 2.10. Let R be a T-graded ring. A graded R-module is an R-module with a direct sum decomposition as additive groups indexed by T:

$$M = \bigoplus_{a\in T} M_a \text{ such that } R_aM_b \subseteq M_{a+b}$$

for all $a, b \in T$.

The notions of homogeneous element of a module and degree of a homogeneous element of a module take the obvious meanings. A notable abuse of notation: we will often talk about $\mathbb{Z}$-graded modules over $\mathbb{N}$-graded rings, and likewise.

We can also talk about graded homomorphisms.

Definition 2.11. Let R and S be T-graded rings with the same grading monoid T. A ring homomorphism $\phi : R \to S$ is *graded* or *degree-preserving* if $\phi(R_a) \subseteq S_a$ for all $a \in T$.

Note that our definition of ring homomorphism requires $1_R \mapsto 1_S$, and thus it does not make sense to talk about graded ring homomorphisms that shift degrees. But we can have graded module homomorphisms of any degree.

Definition 2.12. Let M and N be $\mathbb{Z}$-graded modules over the $\mathbb{N}$-graded ring R. A homomorphism of R-modules $\varphi : R \to S$ is *graded* if $\varphi(M_a) \subseteq N_{a+d}$ for all $a \in \mathbb{Z}$ and some fixed $d \in \mathbb{Z}$, called the *degree* of φ. A graded homomorphism of degree 0 is also called *degree-preserving*.

Example 2.13. Let K be a field, and let $R = K[x_1, \dots, x_n]$ be a polynomial ring with the standard grading. Given $c \in K = R_0$, the homomorphism of R-modules $R \to R$ given by $f \mapsto cf$ is degree preserving. However, if instead we take $g \in K = R_d$ for some $d > 0$, then the map

$$\begin{aligned} R &\longrightarrow R \\ f &\longmapsto gf \end{aligned}$$

is not degree preserving, although it is a graded map of degree d. We can make this a degree-preserving map if we shift the grading on R by defining $R(-d)$ to be the R-module R but with the $\mathbb{Z}$-grading given by $R(-d)_t = R_{t-d}$. With this grading, the component of degree d of $R(-d)$ is $R(-d)_d = R_0 = K$. Now the map

$$\begin{aligned} R(-d) &\longrightarrow R \\ f &\longmapsto gf \end{aligned}$$

is degree preserving.

Lecture of February 2, 2022

We observed earlier an important relationship between algebra-finiteness and Noetherianity that followed from the Hilbert basis theorem: if R is Noetherian, then any algebra-finite extension of R is also Noetherian. There isn't a converse to this in general: there are lots of algebras over fields K that are Noetherian but not algebra-finite over K. However, for graded rings, this converse relation holds.

Proposition 2.14. *Let R be an $\mathbb{N}$-graded ring, and consider homogeneous elements $f_1, \dots, f_n \in R$ of positive degree. Then $f_1, \dots, f_n$ generate the ideal $R_+ := \bigoplus_{d>0} R_d$ if and only if $f_1, \dots, f_n$ generate R as an R_0-algebra.*

Therefore, an $\mathbb{N}$-graded ring R is Noetherian if and only if R_0 is Noetherian and R is algebra-finite over R_0.

Proof. If $R = R_0[f_1, \dots, f_n]$, then any element $r \in R_+$ can be written as a polynomial expression $r = P(f_1, \dots, f_n)$ for some $P \in R_0[\underline{x}]$ with no constant term. Each monomial of P is a multiple of some x_i, and thus $r \in (f_1, \dots, f_n)$.

To show that $R_+ = (f_1, \dots, f_n)$ implies $R = R_0[f_1, \dots, f_n]$, it suffices to show that any homogeneous element $r \in R$ can be written as a polynomial expression in the f's with coefficients in R_0. We induce on the degree of r, with degree 0 as a trivial base case. For r homogeneous of positive degree, we must have $r \in R_+$, so by assumption we can write $r = a_1 f_1 + \cdots + a_n f_n$; moreover, since r and $f_1, \dots, f_n$ are all homogeneous, we can choose each coefficient a_i to be homogeneous of degree $|r| - |f_i|$. By the induction hypothesis, each a_i is a polynomial expression in the f's, so we are done.

For the final statement, if R_0 is Noetherian and R algebra-finite over R_0, then R is Noetherian by the Hilbert Basis Theorem. If R is Noetherian, then $R_0 \cong R/R_+$ is Noetherian. Moreover, R is algebra-finite over R_0 since R_+ is generated as an ideal by finitely many homogeneous elements by Noetherianity, so by the first statement, we get a finite algebra generating set for R over R_0. □

2.2. **Application: Finite generation rings of invariants.** If R is a graded ring, and G is a group acting on R by degree-preserving automorphisms, then R^G is a graded subring of R, meaning R^G is graded with respect to the same grading monoid.

Using this perspective, we can now give a different proof of the finite generation of invariant rings that works under different hypotheses. The proof we will discuss now is essentially Hilbert's proof. To do that, we need another notion that is very useful in commutative algebra.

Definition 2.15. Let S be an R-algebra corresponding to the ring homomorphism $\phi : R \to S$. We say that R is a *direct summand* of S if the map ϕ admits a left inverse as a map of R-modules.

Since the condition forces ϕ to be injective, we can assume it is an inclusion map (after renaming elements). Note that given any R-linear map $\pi : S \to R$, if $\pi(1) = 1$ then π is a splitting: indeed, $\pi(R) = \pi(r \cdot 1) = r\pi(1) = r$ for all $r \in R$.

Being a direct summand is really nice, since many good properties of S pass onto its direct summands.

Definition 2.16. Let $\phi : R \to S$ be a ring homomorphism.

- Given an ideal J in S, the preimage of J under ϕ is the *contraction* of J, denoted $\phi^{-1}(J)$ or $J \cap R$, even if ϕ is not an inclusion map.
- Given an ideal I in R, the *expansion* of I in S is the ideal of S generated by $\phi(I)$; we naturally denote this by IS .

Lemma 2.17. *Let R be a direct summand of S. Then, for any ideal $I \subseteq R$, we have $IS \cap R = I$.*

Proof. Let π be the corresponding splitting. Clearly, $I \subseteq IS \cap R$. Conversely, if $r \in IS \cap R$, we can write $r = s_1 f_1 + \cdots + s_t f_t$ for some $f_i \in I$, $s_i \in S$. Applying π, we have

$$r = \pi(r) = \pi\left(\sum_{i=1}^{t} s_i f_i\right) = \sum_{i=1}^{t} \pi\left(s_i f_i\right) = \sum_{i=1}^{t} \pi\left(s_i\right) f_i \in I. \qquad \square$$

Proposition 2.18. *Let R be a direct summand of S. If S is Noetherian, then so is R.*

Proof. Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

be a chain of ideals in R. The chain of ideals in S

$$I_1 S \subseteq I_2 S \subseteq I_3 S \subseteq \cdots$$

stabilizes, so there exist J, N such that $I_n R = J$ for $n \geqslant N$. Contracting to R, we get that $I_n = I_n S \cap R = J \cap R$ for $n \geqslant N$, so the original chain also stabilizes. $\square$

Proposition 2.19. *Let K be a field, and R be a polynomial ring over K. Let G be a finite group acting by degree preserving K-algebra automorphisms on R. Assume that the characteristic of K does not divide $|G|$. Then R^G is a direct summand of R.*

Proof. We consider the map $\rho : R \to R^G$ given by

$$\rho(r) = \frac{1}{|G|} \sum_{g \in G} g \cdot r.$$

First, note that the image of this map lies in R^G, since acting by g just permutes the elements in the sum, so the sum itself remains the same. We claim that this map ρ is a splitting for the inclusion $R^G \subseteq R$. To see that, let $s \in R^G$ and $r \in R$. We have

$$\rho(sr) = \frac{1}{|G|} \sum_{g \in G} g \cdot (sr) = \frac{1}{|G|} \sum_{g \in G} (g \cdot s)(g \cdot r) = \frac{1}{|G|} \sum_{g \in G} s(g \cdot r) = s \frac{1}{|G|} \sum_{g \in G} (g \cdot r) = s\rho(r),$$

so ρ is R^G-linear, and for $s \in R^G$,

$$\rho(s) = \frac{1}{|G|} \sum_{g \in G} g \cdot s = s. \qquad \square$$

Theorem 2.20 (Hilbert's finiteness theorem for invariants)**.** *Let K be a field, and R be a polynomial ring over K. Let G be a group acting by degree preserving K-algebra automorphisms on R. Assume that G is finite and $|G|$ does not divide the characteristic of K, or more generally, that R^G is a direct summand of R. Then R^G is a finitely generated K-algebra.*

Proof. Since G acts by degree preserving K-algebra automorphisms, R^G is an $\mathbb{N}$-graded subring of R with $R_0 = K$. Since R^G is a direct summand of R, R^G is Noetherian by Proposition 2.18. By our characterization of Noetherian graded rings, R^G is finitely generated over $R_0 = K$. $\square$

Remark 2.21. One important thing about this proof is that it applies to many infinite groups. In particular, for any *linearly reductive group*, including $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{SL}_n(\mathbb{C})$, and $(\mathbb{C}^\times)^n$, we can construct a splitting map ρ.

Lecture of February 4, 2022

3. Affine varieties

3.1. **Definition and examples of affine varieties.** Our next goal is to study solution sets of polynomial equations. Such solutions sets have a fancy name.

Definition 3.1. Let K be a field. We define *affine n-space* over K, denoted $\mathbb{A}^n_K$, to be the set of n-tuples over K:

$$\mathbb{A}^n_K = \{(a_1, \ldots, a_n) \mid a_i \in K\}.$$

Observe that any $f \in K[x_1, \ldots, x_n]$ can be considered as a function on $\mathbb{A}^n_K$, where $f(a_1, \ldots, a_n)$ is result of specializing x_i to a_i for each i.

Definition 3.2. For any subset $S \subseteq K[x_1, \ldots, x_n]$, we set

$$\mathcal{Z}(S) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n_K \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}.$$

We call $\mathcal{Z}(S)$ the *zero set* of S. A *subvariety* of $\mathbb{A}^n_K$ is a set of the form $\mathcal{Z}(S)$. An *affine variety*, or just a *variety*, is a subvariety of $\mathbb{A}^n_K$ for some n.

Remark 3.3. Note that if $L \supseteq K$ is a larger field, any polynomial $f \in K[x_1, \ldots, x_n]$ is also an element of $L[x_1, \ldots, x_n]$, and we can evaluate it at any point in $\mathbb{A}^n_L$. Thus, we may write $\mathcal{Z}_K(S)$ or $\mathcal{Z}_L(S)$ the distinguish between the zero sets over different fields.

Example 3.4.

(1) For $K = \mathbb{R}$ and $n = 2$, $\mathcal{Z}(y^2 - x^2(x+1))$ is a "nodal curve" in $\mathbb{A}^2_{\mathbb{R}}$, the real plane. Note that we've written x for x_1 and y for x_2 here.
(2) For $K = \mathbb{R}$ and $n = 3$, $\mathcal{Z}(z - x^2 - y^2)$ is a paraboloid in $\mathbb{A}^3_{\mathbb{R}}$, real three space.
(3) For $K = \mathbb{R}$ and $n = 3$, $\mathcal{Z}(z - x^2 - y^2, 3x - 2y + 7z - 7)$ is a circle in $\mathbb{A}^3_{\mathbb{R}}$.
(4) For $K = \mathbb{R}$ and $n = 3$, $\mathcal{Z}(xy, xz)$ is a line and a plane that cross transversely.
(5) Over an arbitrary field K, a linear subspace of $\mathbb{A}^n_K = K^n$ is a subvariety: such a subset is defined by some linear equations.
(6) For $K = \mathbb{R}$, $\mathcal{Z}_{\mathbb{R}}(x^2 + y^2 + 1) = \varnothing$. Note that $\mathcal{Z}_{\mathbb{C}}(x^2 + y^2 + 1) \neq \varnothing$, since it contains $(i, 0)$.
(7) For $K = \mathbb{R}$, $\mathcal{Z}_{\mathbb{R}}(x^2 + y^2) = \{(0, 0)\}$. On the other hand, $\mathcal{Z}_{\mathbb{C}}(x^2 + y^2)$ is a union of two "lines" in $\mathbb{C}^2$ (or two planes, in the "real" sense), given by the equations $x + iy = 0$ and $x - iy = 0$.

(8) The subset $\mathbb{A}^2_K \backslash \{(0,0)\}$ is not an algebraic subset of $\mathbb{A}^2_K$ if K is infinite. Why?

(9) The graph of the sine function is not an algebraic subset of $\mathbb{A}^2_{\mathbb{R}}$. Why not?

(10) For $K = \mathbb{R}$ or $\mathbb{C}$, the set

$$X = \{(t, t^2, t^3) \mid t \in K\}$$

is an algebraic variety, though it isn't clear from this description. In fact, $X = \mathcal{Z}(y - x^2, z - x^3)$. To see the containment "$\subseteq$", for $(t, t^2, t^3) \in X$, we have $t^2 - t^2 = 0$ and $t^3 - t^3 = 0$. For the containment "$\supseteq$", let $(a, b, c) \in \mathcal{Z}(y - x^2, z - x^3)$, so $b = a^2$ and $c = a^3$. Setting $t = a$, we get that $(a, b, c) = (t, t^2, t^3) \in X$. The same argument works over $\mathbb{C}$.

(11) For $K = \mathbb{R}$ or $\mathbb{C}$, the set

$$X = \{(t^3, t^4, t^5) \mid t \in \mathbb{R}\}$$

is an algebraic variety, though again it needs justification. Consider $Y = \mathcal{Z}(y^3 - x^4, z^3 - x^5)$; clearly $X \subseteq Y$. Over $\mathbb{R}$, for $(a, b, c) \in Y$, take $t = \sqrt[3]{a}$; then $a = t^3$, $b^3 = a^4$ means $b = \sqrt[3]{a^4}$, so $b = t^4$, and similarly $c = t^5$, so $X = Y$. We were using uniqueness of cube roots in this argument though, so we need to reconsider over $\mathbb{C}$. Indeed, if ω is a cube root of unity, then $(1, 1, \omega) \in Y \smallsetminus X$, so we need to do better. Let's try $Z = \mathcal{Z}(y^3 - x^4, z^3 - x^5, z^4 - y^5)$. Again, $X \subseteq Z$. Say that $(a, b, c) \in \mathbb{A}^3_{\mathbb{C}}$ are in Z, and let s be a cube root of a. Then $b^3 = a^4 = (s^4)^3$ implies that $b = \omega s^4$ for some cube root of unity ω' (maybe 1, maybe not). Similarly $c^3 = a^4 = (s^5)^3$ implies that $c = \omega'' s^5$ for some cube root of unity ω'' (maybe 1, maybe ω', maybe not). So at least $(a, b, c) = (s^3, \omega' s^4, \omega'' s^5)$. Let $t = \omega' s$. Then $(s^3, \omega' s^4, \omega'' s^5) = (t^3, t^4, \omega s^5)$, where $\omega = (\omega')^2 \omega''$ is again some cube root of unity. The equation $b^5 = c^4$ shows that $t^2 0 = \omega^5 t^2 0$. If $t \neq 0$, this shows $\omega = 1$, so $(a, b, c) = (t^3, t^4, t^5)$; if $t = 0$, then $(a, b, c) = (0, 0, 0) = (0^3, 0^4, 0^5)$. Thus, $X = Z$.

(12) For any field K and elements $a_1, \ldots, a_d \in K$, we have

$$\mathcal{Z}(x_1 - a_1, \ldots, x_d - a_d) = \{(a_1, \ldots, a_d)\}.$$

So, all one element subsets of $\mathbb{A}^d_K$ are algebraic subsets.

(13) Here is an example from linear algebra. Fix a field K and consider the set of pairs (A, v) of 2×2 matrices and 2×1 vectors over K. We can again identify this with $\mathbb{A}^6_K$; let's call our variables $x_{11}, x_{12}, x_{21}, x_{22}, y_1, y_2$, where we are thinking of $A = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$ and $v = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$. The set X of pairs (A, v) such that $Av = 0$ is a subvariety of $\mathbb{A}^6_K$:

$$X = \mathcal{Z}(x_{11} y_1 + x_{12} y_2, x_{21} y_1 + x_{22} y_2).$$

(14) Let's take another linear algebra example. We can identify the set of 2×3 matrices over a field K with $\mathbb{A}^6_K$. To make this line up a little more naturally, let's label our variables as $x_{11}, x_{12}, x_{13}, x_{21}, x_{22}, x_{23}$. I claim that the set X of matrices of rank < 2 is a subvariety of $\mathbb{A}^6_K$. To see this, we need to find equations. For a 2×3 matrix A to have rank < 2, it is necessary and sufficient that each 2×2 submatrix have rank < 2, which is equivalent to each of the 2×2 minors (subdeterminants) of the matrix to be zero. Thus,

$$X = \mathcal{Z}(x_{11} x_{22} - x_{12} x_{21}, x_{11} x_{23} - x_{13} x_{21}, x_{12} x_{23} - x_{13} x_{22}).$$

Proposition 3.5. *Let K be a field and $R = K[x_1, \ldots, x_n]$. Let $S, S_\lambda, T \subseteq R$ be arbitrary subsets, and $I, I_\lambda, J \subseteq R$ be ideals.*

(0) *$\mathcal{Z}(1) = \varnothing$ and $\mathcal{Z}(0) = \mathbb{A}^n_K$.*

(1) *If* $S \subseteq T$*, then* $\mathcal{Z}(S) \supseteq \mathcal{Z}(T)$.
(2) *If* $I = (S)$ *is the ideal generated by* S*, then* $\mathcal{Z}(S) = \mathcal{Z}(I)$.
(3) $\mathcal{Z}(\bigcup_{\lambda\in\Lambda} S_\lambda) = \bigcap_{\lambda\in\Lambda} \mathcal{Z}(S_\lambda)$.
(3') $\mathcal{Z}(\sum_{\lambda\in\Lambda} I_\lambda) = \bigcap_{\lambda\in\Lambda} \mathcal{Z}(I_\lambda)$.
(4) $\mathcal{Z}(\{fg \mid f \in S, g \in T\}) = \mathcal{Z}(S) \cup \mathcal{Z}(T)$.
(4') $\mathcal{Z}(I \cap J) = \mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$.

Proof. (0) is clear, since 1 is never equal to zero and 0 is always zero. (1) is also clear, since imposing more equations cannot enlarge the solution set.

For (2), we have $\mathcal{Z}(I) \subseteq \mathcal{Z}(S)$ by (1). On the other hand, if $f_1, \dots, f_m \in S$ and $r_1, \dots, r_m \in R$, and $(a_1, \dots, a_n) \in \mathcal{Z}(S)$, then $f_i(a_1, \dots, a_n) = 0$ for all i, so

$$(\sum_i r_i f_i)(a_1, \dots, a_n) = \sum_i r_i(a_1, \dots, a_n) f_i(a_1, \dots, a_n) = 0,$$

so $(a_1, \dots, a_n) \in \mathcal{Z}(\sum_i r_i f_i)$. Thus, $(a_1, \dots, a_n) \in \mathcal{Z}(I)$. That is, $\mathcal{Z}(S) \subseteq \mathcal{Z}(I)$. Similarly...

(3) is clear: for a point to satisfy be a solution to all of the equations in each set S_λ, it is equivalent to be a solution of each set of equations S_λ. For (3'), using (2) and (3), since $\sum_{\lambda\in\Lambda} I_\lambda$ is the ideal generated by $\bigcup_{\lambda\in\Lambda} I_\lambda$, we have

$$\mathcal{Z}(\sum_{\lambda\in\Lambda} I_\lambda) = \mathcal{Z}(\bigcup_{\lambda\in\Lambda} I_\lambda) = \bigcap_{\lambda\in\Lambda} \mathcal{Z}(I_\lambda).$$

For (4), it is clear that

$$\mathcal{Z}(S) \cup \mathcal{Z}(T) \subseteq \mathcal{Z}(\{fg \mid f \in S, g \in T\}),$$

since $f(a_1, \dots, a_n) = 0$ for all $f \in S$ implies $f(a_1, \dots, a_n)g(a_1, \dots, a_n) = 0$ for all $f \in S$ and all $g \in T$. On the other hand, if $(a_1, \dots, a_n) \notin \mathcal{Z}(S) \cup \mathcal{Z}(T)$, then there is some $f \in S$ and some $g \in T$ with $f(a_1, \dots, a_n) \neq 0$ and $g(a_1, \dots, a_n) \neq 0$, so $f(a_1, \dots, a_n)g(a_1, \dots, a_n) \neq 0$.

For (4'), since $IJ \subseteq I \cap J \subseteq I$ and $I \cap J \subseteq J$), by (1) we get

$$\mathcal{Z}(I) \cup \mathcal{Z}(J) \subseteq \mathcal{Z}(I \cap J) \subseteq \mathcal{Z}(IJ).$$

On the other hand, by (2) and (4) we get

$$\mathcal{Z}(IJ) \subseteq \mathcal{Z}(\{fg \mid f \in I, g \in J\}) = \mathcal{Z}(I) \cup \mathcal{Z}(J),$$

so the equalities hold throughout. □

Lecture of February 7, 2022

Remark 3.6. A basic corollary of (2) above and the Hilbert basis theorem says that every system of polynomial equations is equivalent to a finite one! Indeed, for any set S, $\mathcal{Z}(S) = \mathcal{Z}(I)$ for $I = (S)$, and since $K[x_1, \dots, x_n]$ is Noetherian, $S = (f_1, \dots, f_m)$ for some m, so $\mathcal{Z}(S) = \mathcal{Z}(f_1, \dots, f_m)$.

Definition 3.7. Let K be a field, and $X \subseteq \mathbb{A}^n_K$ be a subset. We define

$$\mathcal{I}(X) := \{f \in K[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in X\}$$

One evident relation between the two notions: for a subset $X \subseteq \mathbb{A}^n_K$ and a subset $S \subseteq K[x_1, \dots, x_n]$, we have

$$X \subseteq \mathcal{Z}(S) \iff \text{each } s \in S \text{ vanishes at each } x \in X \iff S \subseteq \mathcal{I}(X).$$

Definition 3.8. The *radical* of an ideal I in a ring R is the ideal

$$\sqrt{I} := \{f \in R \mid f^n \in I \text{ for some } n\}.$$

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

To see that $\sqrt{I}$ is an ideal, note that if $f^m, g^n \in I$, then

$$\begin{aligned}(f+g)^{m+n-1} &= \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} f^i g^{m+n-1-i} \\ &= f^m \left(f^{n-1} + \binom{m+n-1}{1} f^{n-2} g + \cdots + \binom{m+n-1}{n-1} g^{n-1} \right) \\ &+ g^n \left(\binom{m+n-1}{n} f^{m-1} + \binom{m+n-1}{n+1} f^{m-2} g + \cdots + g^{m-1} \right) \in I,\end{aligned}$$

and $(rf)^m = r^m f^m \in I$.

Note that $I \subset R$ is radical if and only if R/I has a nonzero nilpotent elements; i.e., R/I is *reduced*.

Proposition 3.9. *Let K be a field, and X, X_λ, Y be subsets of $\mathbb{A}^n_K$.*

(0) *$\mathcal{I}(\varnothing) = R$ and, if K is infinite, $\mathcal{I}(\mathbb{A}^n_K) = 0$.*
(1) *If $X \subseteq Y$, then $\mathcal{I}(X) \supseteq \mathcal{I}(Y)$.*
(2) *$\mathcal{I}(X)$ is a radical ideal.*

Proof. For (0), it is clear that $\mathcal{I}(\varnothing) = R$. Assume K is infinite. We show by induction on n that a nonzero polynomial in $K[x_1, \ldots, x_n]$ is nonzero at some point in $\mathbb{A}^n_K$. The case $n = 1$ is standard: a polynomial in $K[x]$ of degree d can have at most d roots. Now, let $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ be a nonzero polynomial. If f is a nonzero constant, it is nonzero at any point. Otherwise, we can assume that f nontrivally involves some variable, say x_n. Write

$$f(x_1, \ldots, x_n) = f_d(x_1, \ldots, x_{n-1}) x_n^d + \cdots + f_0(x_1, \ldots, x_{n-1}).$$

If f is identically zero, then for every $(a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}_K$,

$$f_d(a_1, \ldots, a_{n-1}) x_n^d + \cdots + f_0(a_1, \ldots, a_{n-1})$$

is a polynomial in one variable that is identically zero, so is the zero polynomial, so each $f_i(a_1, \ldots, a_{n-1})$ is identically zero. By the induction hypothesis, these are the zero polynomial, so $f(x_1, \ldots, x_n)$ is the zero polynomial, as required.

(1) is clear.

For (2), note that $f, g \in \mathcal{I}(X)$ and $r \in R$ implies $X \subseteq \mathcal{Z}(f, g)$ implies $X \subseteq \mathcal{Z}(rf + g)$ implies $rf + g \in \mathcal{I}(X)$, so $\mathcal{I}(X)$ is an ideal. If $f^t \in \mathcal{I}(X)$, then $f(a_1, \ldots, a_n)^t = 0$ for all $(a_1, \ldots, a_n) \in X$, so $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in X$, and $f \in \mathcal{I}(X)$. □

Determining $\mathcal{I}(X)$ can be very difficult; there was already some work involved in settling $\mathcal{I}(\mathbb{A}^n_K)$! We will explore the relationship between the associations $\mathcal{Z}$ and $\mathcal{I}$ more soon.

3.2. **Morphisms of varieties and coordinate rings.** The natural condition for a reasonable map between two varieties is that it should also be made from polynomials.

Definition 3.10. Suppose X is a subvariety of $\mathbb{A}^m_K$ and Y is a subvariety of $\mathbb{A}^n_K$. A *morphism of varieties* or *algebraic map* or *regular map* from X to Y is a function $\phi : X \to Y$ defined coordinatewise by polynomials

$g_1, \dots, g_n \in K[x_1, \dots, x_m]$, that is

$$\phi(a_1, \dots, a_m) = (g_1(a_1, \dots, a_m), \dots, g_n(a_1, \dots, a_m)) \text{ for all } \underline{a} \in X.$$

Not every choice of $g_1, \dots, g_n$ will give such a morphism, because the tuple $(g_1(\underline{a}), \dots, g_n(\underline{a}))$ has to satisfy the equations of Y. Furthermore, different choices of $g_1, \dots, g_n$ may yield the same morphism.

A morphism of varieties $\phi : X \to Y$ is an *isomorphism* if there is some $\phi : Y \to X$ such that $\phi \circ \psi = \mathrm{id}_Y$ and $\psi \circ \phi = \mathrm{id}_X$.

Example 3.11. (1) Let $X = \mathcal{Z}(xy - 1) \subseteq \mathbb{A}^2_K$ (i.e., X is a hyperbola) and define $\phi : X \to \mathbb{A}^1_K$ by $\phi(a, b) = a$. Then G is an algebraic map (indeed, it's given by a linear polynomial) and its image is $\mathbb{A}^1_K \backslash \{0\}$, which is *not* an algebraic subset of $\mathbb{A}^1_K$. So, the set-theoretic image of a morphism of varieties need not be a variety.

(2) Take an infinite field, and let Y be the classical cuspidal curve:

$$Y = \mathcal{Z}(y^2 - x^3) \subseteq \mathbb{A}^2_K.$$

Define

$$\phi : \mathbb{A}^1_K \to Y \quad \phi(t) = (t^2, t^3).$$

ϕ is an algebraic map from $\mathbb{A}^1_K$ to Y since the component functions are polynomial functions of t and $(t^3)^2 - (t^2)^3 = 0$ for all t.

Note that G is a bijection of sets. However, it is not an isomorphism. Indeed, if it were, we would have some map ψ such that $\psi \circ \phi = \mathrm{id}_{\mathbb{A}^1_K}$. This ψ would be given by a polynomial h in two variables such that $h(t^2, t^3) = t$. It is easy to see that no such h exists.

(3) Consider $\mathbb{A}^6_K$ as the space of 2×3 matrices over K with coordinates $x_{11}, \dots, x_{23}$, and consider $\mathbb{A}^5_K$ as the space of pairs of 2×1 and 1×3 matrices over K with coordinates y_1, y_2, z_1, z_2, z_3. The map of matrix multiplication from $\mathbb{A}^5_K$ to $\mathbb{A}^6_K$ is a regular map:

$$(y_1, y_2, z_1, z_2, z_3) \mapsto \begin{bmatrix} y_1 z_1 & y_1 z_2 & y_1 z_3 \\ y_2 z_1 & y_2 z_2 & y_2 z_3 \end{bmatrix}.$$

Definition 3.12. For an algebraic subset X of $\mathbb{A}^n_K$, the *coordinate (function) ring* or the *ring of regular functions* of X is the K-algebra

$$K[X] := K[x_1, \dots, x_n]/\mathcal{I}(X).$$

Recall that $\mathcal{I}(X)$ is a radical ideal, and so $K[X]$ is necessarily a reduced, finitely generated K-algebra. An algebra A is *reduced* if $a^n = 0$ implies $a = 0$ in A.

We call an *affine K-algebra* any ring of the form

$$K[x_1, \dots, x_n]/I \text{ for some ideal } I \subseteq K[x_1, \dots, x_n].$$

Remark 3.13. Let $Y = \mathbb{A}^1_K$ and let X be any algebraic subset of $\mathbb{A}^n_K$ for some n. Then an algebraic map $\phi : X \to \mathbb{A}^1_K$ is determined by a polynomial $f \in K[x_1, \dots, x_n]$. Two such polynomials f, g give the same map G if they agree on X, that is if $f - g \in \mathcal{I}(X)$. So, we have a bijection of sets

$$K[X] \cong \{\text{algebraic morphisms from } X \text{ to } \mathbb{A}^1_K\}.$$

In this way, $K[X]$ is analogous to the ring

$$\mathcal{C}_{\mathbb{R}}(T) := \{\text{the collection of continuous real valued functions on } T\}.$$

Definition 3.14. Let K be a field. Let $X \subseteq \mathbb{A}^m_K$ and $Y \subseteq \mathbb{A}^n_K$ be affine varieties. Let $\phi : X \to Y$ be a morphism given by $(g_1(x), \ldots, g_n(x))$, with $g_i \in K[x_1, \ldots, x_m]$. We define

$$\begin{array}{ccc} K[Y] & \xrightarrow{\phi^*} & K[X] \\ f(y_1, \ldots, y_n) & \longmapsto & f(g_1(x), \ldots, g_n(x)) \end{array}$$

Alternatively, thinking of $f \in K[Y]$ as a regular map from $Y \to A^1_K$, we have

$$\begin{array}{ccc} K[Y] & \xrightarrow{\phi^*} & K[X] \\ Y \xrightarrow{f} \mathbb{A}^1_K & \rightsquigarrow & X \xrightarrow{f\phi} \mathbb{A}^1_K \\ & & \| \\ & & X \xrightarrow{\phi} Y \xrightarrow{f} \mathbb{A}^1_K \end{array}$$

We may call this the *homomorphism induced by* ϕ or the *pullback* of ϕ.

Optional Exercise 3.15. Show that the rule ϕ^* is a well-defined ring homomorphism, and that the map $\phi \mapsto \phi^*$ is well-defined.

Optional Exercise 3.16. For any field K, there is a contravariant functor from affine varieties over K to affine K-algebras that

- on objects, maps a variety X to its coordinate ring $K[X]$,
- on morphisms, maps a morphism of varieties $X \xrightarrow{\phi} Y$ to its pullback $K[Y] \xrightarrow{\phi^*} K[X]$.

Proposition 3.17. *Let $X \subseteq \mathbb{A}^m_K$ and $Y \subseteq \mathbb{A}^n_K$ be affine varieties, and $\phi : X \to Y$ be a morphism. Then* $\ker(\phi^*) = \mathcal{I}(\operatorname{im}\phi)K[Y]$.

The proof is left as an exercise.

Lecture of February 9, 2022

3.3. The Zariski topology and irreducible varieties.

Definition 3.18. Let K be a field. The collection of subvarieties $X \subseteq \mathbb{A}^n_K$ is the collection of closed subsets in a topology on $\mathbb{A}^n_K$:

- $\varnothing = \mathcal{Z}(1)$ and $\mathbb{A}^n_K = \mathcal{Z}(0)$ are subvarieties,
- unions of two subvarieties are subvarieties (products of the equations), and
- arbitrary intersections of subvarieties are subvarieties (union of the equation sets).

This is called the *Zariski topology* on $\mathbb{A}^n_K$. Any subvariety of $\mathbb{A}^n_K$ obtains a *Zariski topology* as the subspace topology from $\mathbb{A}^n_K$.

This topology is not very similar to the Euclidean topology on a manifold; it is much coarser.

Example 3.19. Let K be an infinite field. The closed subsets in the Zariski topology on $\mathbb{A}^1_K$ are just the finite subsets, along with the whole space. Note that this topology is not Hausdorff; quite on the contrary, any two nonempty open sets have infinite intersection!

Here is a nice use of the topological structure.

Proposition 3.20. *Let $X \subseteq \mathbb{A}^n_K$ be a subset. Then $\mathcal{Z}(\mathcal{I}(X)) = \overline{X}$, the closure of X in the Zariski topology.*

Proof. Clearly $X \subseteq \mathcal{Z}(\mathcal{I}(X))$ and $\mathcal{Z}(\mathcal{I}(X))$ is closed, so $\overline{X} \subseteq \mathcal{Z}(\mathcal{I}(X))$. On the other hand, $\overline{X} = \bigcap_{\substack{W \supseteq X \\ W \text{ closed}}} W$. For $W \supseteq X$ closed, write $W = \mathcal{Z}(J)$; then $J \subseteq \mathcal{I}(W)$ and $W \supseteq X$ implies $\mathcal{I}(W) \subseteq \mathcal{I}(X)$, so $J \subseteq \mathcal{I}(X)$, hence $\mathcal{Z}(\mathcal{I}(X)) \subseteq \mathcal{Z}(J) = W$. It follows that $\mathcal{Z}(\mathcal{I}(X)) \subseteq \overline{X}$ as well. □

Remark 3.21. Note as a consequence that the function

$$\{\text{subvarieties of } \mathbb{A}^n_K\} \xrightarrow{\mathcal{I}} \{\text{ideals of } K[x_1, \dots, x_n]\}$$

is injective, since $\mathcal{Z}$ serves as a left inverse.

Recall that a topological space is connected if it cannot be written as the disjoint union of two closed subsets. Here is a much stronger notion of a similar flavor.

Definition 3.22. A topological space is *irreducible* if it cannot be written as a union of two proper closed subsets.

This is much stronger than connected, since there is no disjointness condition on the sets.

Optional Exercise 3.23.
(1) If $Y \subseteq X$ is irreducible, then so is $\overline{Y} \subseteq X$.
(2) If X is an irreducible topological space, and $f : X \to Y$ is continuous, then $f(X)$ is irreducible.
(3) Any nested union $\bigcup_{\lambda \in \Lambda} X_\lambda$ (for a totally ordered set Λ and $X_\mu \subseteq X_\nu$ for $\mu \leqslant \nu$) of irreducible spaces is irreducible.

Optional Exercise 3.24. A topological space is Hausdorff if and only if every irreducible subset is a point.

Proposition 3.25. *Let K be an infinite field. Affine space $\mathbb{A}^n_K$ is irreducible.*

Proof. Say that $\mathbb{A}^n_K = \mathcal{Z}(I) \cup \mathcal{Z}(J)$ for some ideals I, J. We need to show either $\mathcal{Z}(I) = \mathbb{A}^n_K$ or $\mathcal{Z}(J) = \mathbb{A}^n_K$. Note that $\mathbb{A}^n_K = \mathcal{Z}(IJ)$. We must have $IJ = 0$: if $f \in IJ \smallsetminus 0$, then $\mathcal{Z}(IJ) \subseteq \mathcal{Z}(f) \subsetneq \mathbb{A}^n_K$ since $\mathcal{I}(\mathbb{A}^n_K) = 0$. If I and J are both nonzero, take $f \in I \smallsetminus 0$, and $g \in J \smallsetminus 0$; we get $fg \in IJ \smallsetminus 0$, which is a contradiction. Thus, without loss of generality, $I = 0$, so $\mathcal{Z}(I) = \mathbb{A}^n_K$. □

Example 3.26. Affine space over a finite field is reducible: points are subvarieties, so finite unions of points are, and hence

$$\mathbb{A}^n_K = \{(0, \dots, 0)\} \cup \mathbb{A}^n_K \smallsetminus \{(0, \dots, 0)\}$$

is a decomposition into proper subvarieties.

Example 3.27. The variety $\mathcal{Z}_{\mathbb{R}}(xy, xz)$ is reducible: it is $\mathcal{Z}_{\mathbb{R}}(x) \cup \mathcal{Z}_{\mathbb{R}}(y, z)$, the union of a line and a plane, which are varieties.

Example 3.28. Let K be an infinite field. Think of $\mathbb{A}^6_K$ as the set of pairs of 2×2 matrices A (with coordinates x_{ij}) and 2×1 vectors v (with coordinates y_1, y_2), and let $X = \mathcal{Z}(x_{11}y_1 + x_{12}y_2, x_{21}y_1 + y_{22}y_2)$ be the variety of pairs such that $Av = 0$. If $Av = 0$ then either $v = 0$, or else v is a nonzero vector in the kernel of A, so $\det(A) = 0$. Thus, $X = X_1 \cup X_2$, where

$$X_1 = \mathcal{Z}(x_{11}y_1 + x_{12}y_2, x_{21}y_1 + y_{22}y_2, y_1, y_2) = \mathcal{Z}(y_1, y_2)$$

$$X_2 = \mathcal{Z}(x_{11}y_1 + x_{12}y_2, x_{21}y_1 + y_{22}y_2, x_{11}x_{22} - x_{12}x_{21}),$$

so X is reducible.

Lecture of February 11, 2022

Example 3.29. Let K be an infinite field. Think of $\mathbb{A}^6_K$ as the set of 2×3 matrices (with coordinates x_{ij}), and let X be the variety of matrices of rank at most 1. Any matrix $A \in X$ of rank at most one can be written as $A = BC$ for some 2×1 matrix B and some 1×3 matrix C, and conversely any such product has rank at most 1. It follows that X is the image of the morphism

$$\mathbb{A}^5 \longrightarrow \mathbb{A}^6$$

$$(y_1, y_2, z_1, z_2, z_3) \longmapsto \begin{pmatrix} y_1z_1 & y_1z_2 & y_1z_3 \\ y_2z_1 & y_2z_2 & y_2z_3 \end{pmatrix}$$

and hence is irreducible.

Definition 3.30. Let X be a topological space. We say that X is a *Noetherian* topological space if the poset of open sets under containment has ACC, or equivalently that the poset of closed subsets has DCC.

Lemma 3.31. *Any affine variety X is a Noetherian topological space with the Zariski topology.*

Proof. It suffices to deal with $\mathbb{A}^n_K$, since subspaces of Noetherian spaces are Noetherian. If there was an infinite descending chain of closed subvarieties of $\mathbb{A}^n_K$, applying $\mathcal{I}$, we would obtain an infinite ascending chain of ideals in $K[x_1, \ldots, x_n]$, which contradicts Hilbert's Basis Theorem. □

Definition 3.32. Let X be a topological space. A maximal irreducible subspace of X is called an *irreducible component* of X.

Remark 3.33. An irreducible component of a space is closed, since the closure of an irreducible subset is closed.

Proposition 3.34. *Let X be a topological space.*

(1) *X is the union of its irreducible components.*
(2) *If $X = X_1 \cup \cdots \cup X_n$ with each X_i irreducible, and suppose that $X_i \nsubseteq \bigcup_{j \neq i} X_j$; i.e., the union $X = X_1 \cup \cdots \cup X_n$ is* irredundant*. Then $\{X_1, \ldots, X_n\}$ is the collection of irreducible components of X.*
(3) *If X is Noetherian, then X has finitely many irreducible components. Hence, if X is Noetherian, it can be written as an irredundant finite union of irreducible components in a unique way.*

Proof. (1) It suffices to show that any point is in an irreducible component. Let $x \in X$, and consider the collection of irreducible subsets of X that contain x. This is nonempty, since $\{x\}$ is in the collection. By the exercise above, the union of any chain under inclusion is again irreducible, so Zorn's lemma applies. Such a subset must be a maximal irreducible subset, since any larger subset also contains x.

(2) Let Y be an irreducible component of X. Then $Y = (X_1 \cap Y) \cup \cdots \cup (X_n \cap Y)$ implies that $X_i \cap Y = Y$, so $Y \subseteq X_i$ for some i. By maximality, we must have $Y = X_i$. This shows that every irreducible component is on the list.

Conversely, for some X_i, take $Y \supseteq X_i$ to be an irreducible component: we can do this by the same Zorn's Lemma argument as in the previous part. By what we just showed, $Y = X_j$ for some j. By irredundancy, we must have $i = j$, so X_i is an irreducible component.

(3) Consider the collection of closed subsets of X that are not finite unions of irreducibles. If this collection is nonempty (in particular, if X is not a finite union of irreducibles), it has a minimal element by DCC; call it Z. In particular, Z is reducible, so write $Z = Z' \cup Z''$ with Z', Z'' closed

proper subsets of Z. Since they are smaller than Z, they are finite unions of irreducibles. Putting them together expresses Z as a finite union of irreducibles. □

3.4. **Prime and maximal ideals.**

Theorem 3.35. *Let K be a field, and $X \subseteq \mathbb{A}^n_K$ be an affine variety.*

(1) *X is irreducible if and only if $\mathcal{I}(X)$ is a prime ideal.*
(2) *X is a point if and only if $\mathcal{I}(X)$ is a maximal ideal.*

Proof. (1) First we show that if $\mathcal{I}(X)$ is not prime, then X is reducible. Suppose that $f, g \notin \mathcal{I}(X)$ and $fg \in \mathcal{I}(X)$. Since $f \notin \mathcal{I}(X)$, f does not vanish at some point of X, so $X \not\subseteq \mathcal{Z}(f)$. Thus,

$$\mathcal{Z}(\mathcal{I}(X) + (f)) = \mathcal{Z}(\mathcal{I}(X)) \cap \mathcal{Z}(f) = X \cap \mathcal{Z}(f) \subsetneq X,$$

and likewise $\mathcal{Z}(\mathcal{I}(X) + (g)) \subsetneq X$. But

$$X \supseteq \mathcal{Z}(\mathcal{I}(X)+(f)) \cup \mathcal{Z}(\mathcal{I}(X)+(g)) = \mathcal{Z}((\mathcal{I}(X)+(f))(\mathcal{I}(X)+(g))) = \mathcal{Z}(\mathcal{I}(X)^2+(f,g)\mathcal{I}(X)+(fg)) \supseteq \mathcal{Z}(\mathcal{I}(X)) = X,$$

so $\mathcal{Z}(\mathcal{I}(X) + (f)) \cup \mathcal{Z}(\mathcal{I}(X) + (g)) = X$. This shows that X is reducible.

Now, we show that if X is reducible, then $\mathcal{I}(X)$ is not prime. Write $X = Y \cup Z$ with Y, Z closed and $Y, Z \subsetneq X$. We must that $\mathcal{I}(X) \subsetneq \mathcal{I}(Y), \mathcal{I}(Z)$, and $\mathcal{I}(Y) \neq \mathcal{I}(Z)$, since $Y \neq Z$. Take $f \in \mathcal{I}(Y) \smallsetminus \mathcal{I}(Z)$ and $g \in \mathcal{I}(Z) \smallsetminus \mathcal{I}(Y)$. Then $fg \in \mathcal{I}(Y) \cap \mathcal{I}(Z)$, so

$$\mathcal{Z}(fg) \supseteq \mathcal{Z}(\mathcal{I}(Y) \cap \mathcal{I}(Z)) = Y \cup Z = X.$$

Thus, $fg \in \mathcal{I}(X)$. This shows that $\mathcal{I}(X)$ is not prime.

(2) First, take $X = \{(a_1 \ldots, a_n)\}$. We have $x_i - a_i \in \mathcal{I}(X)$ for all i, so $\mathfrak{m} := (x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathcal{I}(X)$. The ideal $\mathfrak{m}$ is maximal, since the quotient $K[x_1, \ldots, x_n]/\mathfrak{m} \cong K$ is a field. Since the only larger ideal is the full ring itself, and $1 \notin \mathcal{I}(X)$, we must have $\mathcal{I}(X) = \mathfrak{m}$ is maximal.

On the other hand, if $X \supsetneq \{(a_1 \ldots, a_n)\}$, then $\mathcal{I}(X) \subsetneq \mathcal{I}(\{(a_1 \ldots, a_n)\})$, so $\mathcal{I}(X)$ is not maximal. □

Corollary 3.36. *Let K be a field.*

(1) *The maps $\mathcal{Z}$ and $\mathcal{I}$ induce a bijection*

$$\{\text{maximal ideals } \mathfrak{m} \text{ of } R = K[x_1, \ldots, x_n] \text{ such that } R/\mathfrak{m} \cong K\} \leftrightarrow \mathbb{A}^n_K$$

(2) *For any affine variety X, there is a bijection*

$$\{\text{maximal ideals } \mathfrak{m} \text{ of } K[X] \text{ such that } K[X]/\mathfrak{m} \cong K\} \leftrightarrow X$$

Lecture of February 14, 2022

Proof. For (1), we need to see that $\xrightarrow{\mathcal{Z}}$ and $\xleftarrow{\mathcal{I}}$ restrict to maps to/from the prescribed source and target. For $\mathcal{Z}$, let $\mathfrak{m}$ be a maximal ideal with residue field K, and consider $\pi : R \to R/\mathfrak{m} \cong K$. We then have that $\pi(x_i) = a_i$ for some $a_i \in K$, so $(x_1 - a_1, \ldots, x_n - a_n) \subseteq \ker(\pi) = \mathfrak{m}$, and this ideal is maximal, so equality holds. Then $\mathcal{Z}(\mathfrak{m}) = \{(a_1, \ldots, a_n)\}$, so $\mathcal{Z}$ gives a well-defined map from left to right. On the other hand, from the last theorem, we see that for any point, $\mathcal{I}$ yields an ideal of this form so $\mathcal{I}$ restricts to a well-defined map here. We know that $\mathcal{Z}(\mathcal{I}(x)) = x$ for a point x since a point is closed, and for an ideal $\mathfrak{m}$ as above, $\mathcal{I}(\mathcal{Z}(\mathfrak{m}))$ is a maximal ideal containing $\mathfrak{m}$, so must equal $\mathfrak{m}$.

For (2), we note that there is a bijection between maximal ideals of $K[X]$ and maximal ideals of $K[x_1, \dots, x_n]$ that contain $\mathcal{I}(X)$; moreover $\mathcal{I}(X) \subseteq \mathfrak{m}$ if and only if $\mathcal{Z}(\mathfrak{m}) \in \mathcal{Z}(\mathcal{I}(X)) = X$. Thus, the bijection from (1) induces a bijection between maximal ideals of $K[X]$ and points of X. □

To recap, over an any field K, the maps $\overset{\mathcal{Z}}{\leftarrow}$ and $\overset{\mathcal{I}}{\rightarrow}$ yield order-reversing maps between the collections below and satisfy $\mathcal{Z} \circ \mathcal{I} = \mathrm{id}$ in each case, so they induce bijections between the RHS and a subset of the LHS (the image of $\mathcal{I}$):

$$\begin{array}{cc} \underline{\text{in } K[x_1, \dots, x_n]} & \underline{\text{in } \mathbb{A}^n_K} \\ \{\text{radical ideals}\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} \{\text{varieties}\} \\ \{\text{prime ideals}\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} \{\text{irred vars}\} \\ \{\text{maximal ideals}\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} \{\text{points}\}. \end{array}$$

Likewise, for any variety X, we have order-reversing maps that induce bijections between the RHS and a subset of the LHS:

$$\begin{array}{cc} \underline{\text{in } K[X]} & \underline{\text{in } X} \\ \{\text{radical ideals}\} \leftrightarrows \{\text{subvarieties}\} \\ \{\text{prime ideals}\} \leftrightarrows \{\text{irred subvars}\} \\ \{\text{maximal ideals}\} \leftrightarrows \{\text{points}\}. \end{array}$$

In both cases, we identified the image of the last $\leftarrow$ as maximal ideals whose residue field was no bigger than the ground field.

Example 3.37. (1) The radical ideal $(0) \subseteq \mathbb{F}_p[x]$ is not in the image of $\mathcal{I}$ (i.e., is left of the the bijection above) over $K = \mathbb{F}_p$. Indeed, $\mathcal{I}(\mathcal{Z}(0)) = \mathcal{I}(\mathbb{A}^1_{\mathbb{F}_p}) = (x^p - x)$.

(2) The prime ideal $(x^2 + y^2 + z^2) \subseteq \mathbb{R}[x, y, z]$ is not in the image of $\mathcal{I}$ over $K = \mathbb{R}$: $\mathcal{I}(\mathcal{Z}(x^2 + y^2 + z^2)) = \mathcal{I}(\{(0, 0, 0\}) = (x, y, z)$.

(3) The maximal ideal $(x^2 + 1) \subseteq \mathbb{R}[x]$ is not in the image of $\mathcal{I}$ over $K = \mathbb{R}$: $\mathcal{I}(\mathcal{Z}(x^2 + 1)) = \mathcal{I}(\varnothing) = (1)$.

4. The Nullstellensatz and the prime spectrum

4.1. **Review of transcendence bases.**

Definition 4.1. Let $K \subseteq L$ be an extension of fields. A *transcendence basis* for L over K is a maximal algebraically independent subset of L.

Remark 4.2. (1) Every field extension has a transcendence basis. This is given by Zorn's Lemma once we see that a union of an increasing chain of algebraically independent sets is algebraically independent. Indeed if there were a nontrivial relation on some elements in the union, there would be a nontrivial relation on finitely many, and so a relation in one of the members in the chain.

(2) Every set of field generators for L/K contains a transcendence basis. This is also given by Zorn's lemma considering algebraically independent subsets of the given generating set.

(3) Observe that $\{x_\lambda\}_{\lambda \in \Lambda}$ is a transcendence basis for L over K, if an only if there is a factorization

$$K \subseteq K(\{x_\lambda\}_{\lambda \in \Lambda}) \subseteq L$$

where the first inclusion is *purely transcendental*, or isomorphic to a field of rational functions, and the second inclusion is algebraic (integral). If the latter were not algebraic, there would be an element of L transcendental over $K(\{x_\lambda\}_{\lambda\in\Lambda})$, and we could use that element to get a larger algebraically independent subset, contradicting the definition of transcendence basis. Conversely, if $K \subseteq K(\{x_\lambda\}_{\lambda\in\Lambda}) \subseteq L$ with the first inclusion purely transcendental and the second algebraic, $\{x_\lambda\}_{\lambda\in\Lambda}$ is a transcendence basis.

Lemma 4.3. *Let $\{x_1,\dots,x_m\}$ and $\{y_1,\dots,y_n\}$ be two transcendence bases for L over K. Then, there is some i such that $\{x_i, y_2,\dots,y_n\}$ is a transcendence basis.*

Proof. Since L is algebraic over $K(y_1,\dots,y_n)$, for each i there is some $p_i(t) \in K(y_1,\dots,y_n)[t]$ such that $p_i(x_i) = 0$. We can clear denominators to assume without loss of generality that $p_i(x_i) \in K[y_1,\dots,y_n][t]$.

We claim that there is some i such that $p_i(t) \notin K[y_2,\dots,y_n][t]$. If not, so $p_i(t) \in K[y_2,\dots,y_n][t]$ for all i, note that each x_i is algebraic over $K(y_2,\dots,y_n)$. Thus, $K(x_1,\dots,x_m)$ is algebraic over $K(y_2,\dots,y_n)$, and since L is algebraic over $K(x_1,\dots,x_m)$, y is algebraic over $K(y_2,\dots,y_n)$, which contradicts that $\{y_1,\dots,y_n\}$ is a transcendence basis. This shows the claim.

Now, we claim that for such i, $\{x_i, y_2,\dots,y_n\}$ is a transcendence basis. Thinking of the equation $p_i(x_i) = 0$ as a polynomial expression in $K[x_i, y_2,\dots,y_n][y_1]$, y_1 is algebraic over $K(x_i, y_2,\dots,y_n)$, hence $K(y_1,\dots,y_n)$ is algebraic over $K(x_i, y_2,\dots,y_n)$, and L as well.

If $\{x_i, y_2,\dots,y_n\}$ were algebraically dependent, take a polynomial equation $p(x_i, y_2,\dots,y_n) = 0$. Note that this equation must involve x_i, since $y_2,\dots,y_n$ are algebraically independent. We would then have $K(x_i, y_2,\dots,y_n)$ is algebraic over $K(y_2,\dots,y_n)$. But since y_1 is algebraic over $K(x_i, y_2,\dots,y_n)$, we would have that $K(y_1,\dots,y_n)$ is algebraic over $K(y_2,\dots,y_n)$, which would contradict that $y_1,\dots,y_n$ is a transcendence basis. □

Proposition 4.4. *If $\{x_1,\dots,x_m\}$ and $\{y_1,\dots,y_n\}$ are two transcendence bases for L over K, then $m = n$.*

Proof. Say that $m \leqslant n$. If the intersection has $s < m$ elements, then without loss of generality $y_1 \notin \{x_1,\dots,x_m\}$. Then, for some i, $\{x_i, y_2\dots,y_n\}$ is a transcendence basis, and $\{x_1,\dots,x_m\} \cap \{x_i, y_2\dots,y_n\}$ has $s+1$ elements. Replacing $\{y_1,\dots,y_n\}$ with $\{x_i, y_2\dots,y_n\}$ and repeating this process, we obtain a transcendence basis with n elements such that $\{x_1,\dots,x_m\} \subseteq \{y_1,\dots,y_n\}$. But we must then have that these two transcendence bases are equal, so $m = n$. □

4.2. **Nullstellensatz.**

Theorem 4.5 (Zariski's Lemma)**.** *Let $K \subseteq L$ be fields. If L is a finitely generated K-algebra, then L is a finite dimensional K-vector space. In particular, if K is algebraically closed then $L = K$.*

Proof. Let $L = K[h_1,\dots,h_d]$. Since in particular $h_1,\dots,h_d$ generate L as a field over K, we can choose a transcendence basis for L/K from among the h's, and after reordering, we may assume that $h_1,\dots,h_c = x_1,\dots,x_c$ form a transcendence basis, and $h_{c+1},\dots,h_d$ are algebraic over $K' = K(x_1,\dots,x_c)$. Then L is integral and algebra-finite over K', hence module-finite. Thus, if $c = 0$, we are done. Suppose that $c \neq 0$; we will obtain a contradiction to complete the proof.

We can apply the Artin-Tate Lemma to $K \subseteq K' \subseteq L$ to see that K' is algebra-finite over K. In particular, there are f_i, g_i in the polynomial ring $K[x_1,\dots,x_c]$ such that $K' = K[\frac{f_1}{g_1},\dots,\frac{f_m}{g_m}]$. This implies that any element of K' can be written as a fraction with denominator $(g_1\cdots g_m)^n$ for some n. The element

$\frac{1}{g_1 \cdots g_m + 1} \in K'$ cannot be written this way; if so, we would have

$$\frac{v}{(g_1 \cdots g_m)^n} = \frac{1}{g_1 \cdots g_c + 1},$$

for some v with $g_1 \cdots g_m \nmid v$ (since the polynomial ring is a UFD). But, the equation $g_1 \cdots g_m v + v = (g_1 \cdots g_m)^n$ contradicts this.

Now if K is algebraically closed and $\ell \in L$, since L/K is finite then ℓ is algebraic over K, thus $\ell \in K$. □

Lecture of February 16, 2022

Theorem 4.6 (Hilbert's Nullstellensatz (Weak Form))**.** *Let K be an algebraically closed field and J be an ideal of $K[x_1, \dots x_n]$. We have*

$$\mathcal{Z}(J) = \varnothing \text{ if and only if } J = K[x_1, \dots, x_n].$$

Remark 4.7. One direction is clear. The nontrivial direction, in its most basic form, says the following: Suppose we are given a system of polynomial equations

$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0 \\ f_2(x_1, \dots, x_n) &= 0 \\ \vdots \qquad &= \vdots \\ f_m(x_1, \dots, x_n) &= 0 \end{aligned}$$

in n variables with coefficients in some algebraically closed field K. If the system has no solutions over K, then for some polynomials $g_1, \dots, g_m$ we have $\sum_i g_i f_i = 1$. One can think of $g_1, \dots, g_m$ as forming a "certificate" that there is no solution.

Proof. If $J = K[x_1, \dots, x_n]$, then $Z(J) = \varnothing$ since $1 = 0$ has no solutions.

We show that if $J \subset K[x_1, \dots, x_n]$ is a proper ideal, then $Z(J) \neq \varnothing$. Since J is proper, it is contained in some maximal ideal $\mathfrak{m}$. By Zariski's Lemma, $K[x_1, \dots, x_n]/\mathfrak{m} \cong K$, so we have $\mathcal{Z}(\mathfrak{m}) \neq \varnothing$. □

To attack the Strong Form of the Nullstellensatz, we will need an observation on inequations.

Remark 4.8 (Rabinowitz's trick). We write $\underline{x} = (x_1, \dots, x_n)$ and $\underline{a} = (a_1, \dots, a_n)$. Observe that, if $f(\underline{x})$ is a polynomial, $f(\underline{a}) \neq 0$ if and only if there is a solution $y = b \in K$ to $yf(\underline{a}) - 1 = 0$. In particular, a system of polynomial equations and inequations

$$f_1(\underline{x}) = 0, \dots, f_m(\underline{x}) = 0, g_1(\underline{x}) \neq 0, \dots, g_n(\underline{x}) \neq 0$$

has a solution $\underline{x} = \underline{a}$ if and only if the system

$$f_1(\underline{x}) = 0, \dots, f_m(\underline{x}) = 0, y_1 g_1(\underline{x}) - 1 = 0, \dots, y_n g_n(\underline{x}) - 1 = 0$$

has a solution $(\underline{x}, \underline{y}) = (\underline{a}, \underline{b})$. In fact, this is equivalent to a system in one extra variable:

$$f_1(\underline{x}) = 0, \dots, f_m(\underline{x}) = 0, y g_1(\underline{x}) \cdots g_n(\underline{x}) - 1 = 0.$$

Theorem 4.9 (Hilbert's Nullstellensatz (Strong Form))**.** *Let K be an algebraically closed field and let J be an ideal in the polynomial ring $R = K[x_1, \dots, x_n]$. Then, for $f \in R$, $\mathcal{Z}(f) \supseteq \mathcal{Z}(J)$ if and only if $f \in \sqrt{J}$.*

In particular, $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$.

Proof. The equations in $\sqrt{J}$ vanish on $\mathcal{Z}(J)$, so $\sqrt{J} \subseteq \mathcal{I}(\mathcal{Z}(J))$.

For the converse, suppose that $f(\underline{x})$ vanishes on $\mathcal{Z}(J)$. Write $J = (g_1, \ldots, g_m)$. Considering the system

$$g_1(\underline{x}) = 0, \ldots, g_m(\underline{x}) = 0, f(\underline{x}) \neq 0$$

we see that it has no solution since $f(\underline{x}) = 0$ is a consequence of the first m equations. By the remark above, this implies that $\mathcal{Z}(JS + (yf - 1)) = \varnothing$, where $JS + (yf - 1)$ is an ideal in the polynomial ring $S = K[x_1, \ldots, x_n, y]$. By the Weak Nullstellensatz, we see that $1 \in JS + (yf - 1)$. Write $J = (g_1(\underline{x}), \ldots, g_m(\underline{x}))$, and

$$1 = r_0(\underline{x}, y)(1 - yf(\underline{x})) + r_1(\underline{x}, y)g_1(\underline{x}) + \cdots + r_m(\underline{x}, y)g_m(\underline{x}).$$

We can apply an evaluation map $S \to \mathrm{Frac}(R)$ sending $y \mapsto 1/f$ to get

$$1 = r_1(\underline{x}, 1/f)g_1(\underline{x}) + \cdots + r_m(\underline{x}, 1/f)g_m(\underline{x}).$$

Since each r_i is polynomial, there is a largest negative power of f occurring; say that f^n serves as a common denominator. We can clear denominators multiplying by f^n to obtain (on the LHS) f^n as a polynomial combination of the g's (on the RHS). □

Corollary 4.10. *Let K be an algebraically closed field. The associations $\mathcal{Z}$ and $\mathcal{I}$ induce order-reversing bijections*

$$\begin{array}{ccc} \underline{\text{in } K[x_1, \ldots, x_n]} & & \underline{\text{in } \mathbb{A}^n_K} \\ \{\text{radical ideals}\} & \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} & \{\text{varieties}\} \\ \{\text{prime ideals}\} & \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} & \{\text{irred vars}\} \\ \{\text{maximal ideals}\} & \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} & \{\text{points}\}. \end{array}$$

In particular, given ideals I and J, we have $\mathcal{Z}(I) = \mathcal{Z}(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Likewise, for any variety X over an algebraically closed field, we have order-reversing bijections

$$\begin{array}{ccc} \underline{\text{in } K[X]} & & \underline{\text{in } X} \\ \{\text{radical ideals}\} & \leftrightarrows & \{\text{subvarieties}\} \\ \{\text{prime ideals}\} & \leftrightarrows & \{\text{irred subs}\} \\ \{\text{maximal ideals}\} & \leftrightarrows & \{\text{points}\}. \end{array}$$

Example 4.11. Recall that

$$X := \{(t^3, t^4, t^5) \mid t \in \mathbb{C}\} = \mathcal{Z}(I), \text{ where } I = (y^3 - x^4, z^3 - x^5, z^4 - y^5).$$

By the Nullstellensatz, $\mathcal{I}(X) = \sqrt{I}$. The ideal I is not radical: note that

$$x^9yz \equiv (x^4)(x^5)yz \equiv y^4z^4 \equiv y^9 \equiv x^{12} \equiv x^3y^3z^3 \qquad \mod I$$

and

$$x^6y^2z^2 \equiv x^2y^5z^2 \equiv x^2z^6 \equiv x^{12} \qquad \mod I$$

so

$$(x^3 - yz)^4 = x^{12} - 4x^9yz + 6x^6y^2z^2 - 4x^3y^3z^3 + y^4z^4 \equiv x^{12}(1 - 4 + 6 - 4 + 1) \equiv 0 \qquad \mod I.$$

One can show that $\sqrt{I} = (x^3 - yz, y^2 - xz, z^2 - x^2y)$.

4.3. **Spectrum of a ring.** As a consequence of the Nullstellensatz, for an algebraically closed field K and an algebra of the form $R = K[x_1, \ldots, x_n]/I$ that is reduced, we know that $I = \mathcal{I}(X)$ for some variety $X \subseteq \mathbb{A}^n_K$, and $R = K[X]$. We can recover X (as a set) from the ring R by taking the maximal ideals of R. Moreover, we can recover the Zariski topology on X: a subvariety of X corresponds to a (radical) ideal of R, so the closed subsets correspond to the sets of maximal ideals that contain a particular (radical) ideal of R. Moreover, we can reconstruct morphisms of varieties from the maps on their coordinate rings:

Optional Exercise 4.12. Let X, Y be affine varieties over an algebraically closed field with $R = K[X]$ and $S = K[Y]$. Let $\phi : X \to Y$ be an algebraic morphism, and $\phi^* : S \to R$ be the induced map on coordinate rings. Then the following diagram commutes:

$$\begin{array}{ccc} \operatorname{Max}(R) & \longrightarrow & \operatorname{Max}(S) \\ \downarrow & \mathfrak{m} \longmapsto (\phi^*)^{-1}(\mathfrak{m}) & \downarrow \\ X & \xrightarrow{\phi} & Y \end{array}$$

where the vertical maps send a maximal ideal of the form $(x_1 - a_1, \ldots, x_n - a_n)$ to the point $(a_1, \ldots, a_n)$; this is essentially the map $\mathcal{Z}$ on maximal ideals.

Remark 4.13. Loosely speaking, this exercise says that $\operatorname{Max}(-)$ can be thought of as a contravariant functor that, on the category of reduced finitely generated algebras over algebraically closed fields, is an inverse to the coordinate ring functor up to natural isomorphism. The precise statement is that functor yields an equivalence of categories.

Index