Nullstellensatz and Hauptidealsatz

Shrivathsa Pandelu

December 3, 2022

1 Integral Extensions

Let A be a subring of a ring B. An element $x \in B$ is said to be integral over A if it satisfies some monic polynomial with coefficients in A. What this means is that the ring $A[x]$ is a finitely generated module over A.

Lemma 1. *The following are equivalent:*

i) $x \in B$ *is integral over* A*;*
ii) $A[x]$ *is a finitely generated* A*-module;*
iii) $A[x]$ *is contained in a subring* C *of* B *which is a finitely generated* A*-module;*
iv) There exists a faithful $A[x]$*-module* M *which is finitely generated as an* A*-module.*

Proof. i) $\implies$ ii): Let x satisfy a monic polynomial $x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0 = 0$, so x^r is an A-linear combination of $1, x, \ldots, x^{r-1}$. Recursively, we see that all higher powers of x are linear combinations of $1, x, \ldots, x^{r-1}$, hence $A[x]$ is finitely generated as an A-module.
ii) $\implies$ iii): This is obvious.
iii) $\implies$ iv): Take $M = C$ which is faithful as an $A[x]$-module as if $yM = 0$ then $y = 0$ for $1 \in C$.
iv) $\implies$ i): Since M is an $A[x]$-module, we have the A-module homomorphism $m \mapsto xm, m \in M$. Since M is finitely generated as an A-module, there is a polynomial in x over A which annihilates M. Since M is faithful as an $A[x]$-module, such a polynomial should be 0 in $A[x]$, hence 0 in B. □

Corollary 1. *If* $x_1, \ldots, x_n \in B$*, are each integral over* A*, then* $A[x_1, \ldots, x_n]$ *is a finitely generated* A*-module.*

Proof. Induction on n, $A[x_1]$ is a finitely generated A-module. If $A_{n-1} = A[x_1, \ldots, x_{n-1}]$ is a finitely generated A-module, then $A[x_1, \ldots, x_n]$ is a finitely generated A_{n-1}-module. So $A[x_1, \ldots, x_n]$ is also a finitely generated A-module. □

Corollary 2. *The set* C *of elements of* B *which are integral over* A *form a subring of* B*.*

Definition 1. *The set of all elements* C *which are integral over* A *is called the integral closure of* A *in* B*. If* $C = A$*,* A *is said to be integrally closed in* B *and if* $C = B$*,* B *is said to be integral over* A*.*

Corollary 3. *If* $A \subseteq B \subseteq C$ *and if* C *is integral over* B *and* B *is integral over* A*, then* C *is integral over* A*.*

Proof. Let $x \in C$, satisfying an equation $x^n + b_1 x^{n-1} + \cdots + b_n = 0$ over B. The ring $B' = A[b_1, \ldots, b_n]$ is a finitely generated A-module and $B'[x]$ is a finitely generated B'-module. Hence $B'[x]$ is a finitely generated A-module, hence x is integral over A. □

Corollary 4. *Let* $A \subseteq B$ *and let* C *be the integral closure of* A *in* B*, then* C *is integrally closed in* B*.*

Theorem 1.1. *Let* $A \subseteq B$ *be rings,* B *integral over* A*.*

i) If $\mathfrak{b}$ *is an ideal of* B *and* $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b} \cap A$*, then* $B/\mathfrak{b}$ *is integral over* $A/\mathfrak{a}$*.*
ii) If S *is a multiplicatively closed subset of* A*, then* $S^{-1}B$ *is integral over* $S^{-1}A$*.*

Proof. i) Given $x \in B$, reduce the equation satisfied by x mod $\mathfrak{b}$ to get an equation over $A/\mathfrak{a}$. Note that $A/\mathfrak{a}$ is a subring of $B/\mathfrak{b}$.
ii) Let $x \in B$ satisfy $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, then, over $S^{-1}A$, $x/s \in S^{-1}B$ satisfies

$$(x/s)^n + (a_1/s)(x/s)^{n-1} + \cdots + a_n/s^n = 0.$$

□

1.1 Going up theorem

Theorem 1.2. *Let $A \subseteq B$ be integral domains, B integral over A. Then B is a field if and only if A is a field.*

Proof. Suppose A is a field, $y \in B, y \neq 0$. Let $y^n + a_1 y^{n-1} + \cdots + a_n = 0$ be a relation of smallest degree. Since B is a domain, $a_n \neq 0$, hence is a unit in A, hence in B. We then have $y(y^{n-1} + a_1 y^{n-2} + \cdots + a_1) = -a_n$, hence y is a unit in B.
Conversely, suppose B is a field and let $x \in A$ be nonzero. Then $x^{-1} \in B$ and satisfies some polynomial relation over A of some degree m. Multiplying such a relation by x^{m-1} gives x^{-1} as a polynomial in x over A, hence $x^{-1} \in A$. □

Corollary 5. *Let $A \subseteq B$ be rings, B integral over A; let $\mathfrak{q}$ be a prime ideal of B and let $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$ and both are integral domains. □

Corollary 6. *Let $A \subseteq B$ be rings, B integral over A; let $\mathfrak{q}$ be a prime ideal and $\mathfrak{q}'$ any ideal such that $\mathfrak{q} \subseteq \mathfrak{q}', \mathfrak{q}^c = \mathfrak{q}'^c = \mathfrak{p}$ say. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. We know that $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ and that $\mathfrak{m} = \mathfrak{p}^e$ is maximal in $A_\mathfrak{p}$. Let $\mathfrak{n}, \mathfrak{n}'$ be the extensions of $\mathfrak{q}, \mathfrak{q}'$ respectively in $B_\mathfrak{p}$, then both of these restrict to the maximal ideal $\mathfrak{m}$ and $\mathfrak{n} \subseteq \mathfrak{n}'$. It is easy to see that the extension of $\mathfrak{q}$ is a prime ideal in $B_\mathfrak{p}$, hence by the previous corollary, it is maximal. Therefore, $\mathfrak{n} = \mathfrak{n}'$, hence $\mathfrak{q} = \mathfrak{q}'$. □

Theorem 1.3. *Let $A \subseteq B$ be rings, B integral over A, and let $\mathfrak{p}$ be a prime ideal of A. Then there exists a prime ideal $\mathfrak{q}$ of B which restricts to $\mathfrak{p}$.*

Proof. Let $\mathfrak{n}$ be any maximal ideal in $B_\mathfrak{p}$, then it must restrict to the extension $\mathfrak{p}^e$ in $A_\mathfrak{p}$ by integrality. Take $\mathfrak{q} = \mathfrak{n}^c$, then $\mathfrak{q}$ must restrict to $\mathfrak{p}$. □

Theorem 1.4. *(Going up theorem) Let $A \subseteq B$ be rings, B integral over A; let $\mathfrak{p}_1 \subseteq \ldots \mathfrak{p}_n$ be a chain of prime ideals of A and $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m (m < n)$ a chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i, 1 \leq i \leq m$. Then the chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i, 1 \leq i \leq n$.*

Proof. By induction it suffices to prove for the case $m = 1, n = 2$. The idea is to use the previous theorem. To obtain prime ideals containing $\mathfrak{q}_1$, we simply go module $\mathfrak{q}_1$. So consider $\bar{A} = A/\mathfrak{p}_1, \bar{B} = \mathfrak{q}_1$, then $\bar{A} \subseteq \bar{B}$ and $\bar{B}$ is integral over $\bar{A}$. So, there is a prime ideal $\mathfrak{q}_2$ of $\bar{B}$ such that $\mathfrak{q}_2 \cap \bar{A} = \mathfrak{p}_2$ in $\bar{A}$. Lifting back $\mathfrak{q}_2$ to B gives $\mathfrak{q}$ as required. □

We look at the situation from a geometric perspective. If B is integral over A, then so are the corresponding polynomial rings. Intuitively an integral extension is like adding points to A in a sparse manner. Think of going from $\mathbb{Z}$ to $\mathbb{Z}[\sqrt{2}]$ as opposed to $\mathbb{Z}[1/2]$. This is because non integral but algebraic elements require us to invert the leading coefficient which then creates sequences "converging" to zero etc.
So, when adding points in a sparse manner, the theorem above says that a variety downstairs comes from removing points in a variety upstairs. The going up theorem relates, to an extent, the dimensions of varieties over the two things. Since we are adding points in a sparse manner, we shouldn't expect the dimension to change.

1.2 Going down theorem

Theorem 1.5. *Let $A \subseteq B$ be rings, C the integral closure of A in B. Let S be a multiplicatively closed subset of A. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. By an earlier result, $S^{-1}C$ is integral over $S^{-1}A$ because C is integral over A. Conversly, let $b/s \in S^{-1}B$ be integral over $S^{-1}A$ satisfying a polynomial $(b/s)^n + (a_1/s_1)(b/s)^{n-1} + \cdots + (a_n/s_n) = 0$. Clearing the denominators, we find that there is a $t \in S$ such that $bt \in C$, hence $b/s \in S^{-1}C$. □

Definition 2. *An integral domain is said to be integrally closed if it is integrally closed in its field of fractions.*

Remark. Some sources also refer to it as a normal ring. Seeing how the word "normal" is quite over used in mathematics, I shall use "integrally closed".

Theorem 1.6. *Let $\phi : M \to N$ be an A-module homomorphism. Then the following are equivalent:*

i) ϕ is injective (surjective);
ii) $\phi_{\mathfrak{p}}$ is injective (surjective) for each prime ideal $\mathfrak{p}$;
iii) $\phi_{\mathfrak{m}}$ is injective (surjective), for each maximal ideal $\mathfrak{m}$.

Proof. Given a multiplicative set $S \subset A, S^{-1}$ is a functor on the category of A-modules and it is in fact an exact functor, i.e., if $M \to N \to P$ is exact, then so is $S^{-1}M \to S^{-1}N \to S^{-1}P$. Given the homomorphism above, we can always form the exact sequence

$$0 \to \ker(\phi) \to M \to N \to \operatorname{coker}(\phi) \to 0$$

and by the exactness of S^{-1}, we have i) $\implies$ ii), iii). We always have ii) $\implies$ iii), so we just need to prove iii) $\implies$ i).
Suppose $\phi_{\mathfrak{m}}$ is injective for every maximal ideal $\mathfrak{m}$. Suppose $a \in \ker(\phi)$ is nonzero, then its annihilator is a proper ideal contained in some maximal ideal $\mathfrak{m}$. But $\phi_{\mathfrak{m}}$ is injective, so there exists $t \notin \mathfrak{m}$ such that $ta = 0$, but this is a contradiction.
Similarly, suppose $\phi_{\mathfrak{m}}$ is surjective for every maximal ideal $\mathfrak{m}$, given $n \in N$ consider the quotient ideal $\{a \in A : an \in \phi(M)\}$. If this is a proper ideal, then it is contained in some maximal ideal $\mathfrak{m}$. There is some $m/s \in M_{\mathfrak{m}}$ such that $\phi(m)/s = n$, which would mean that there is some $t \notin \mathfrak{m}$ such that $tn \in \phi(M)$, but this is a contradiction. □

Corollary 7. *Let A be an integral domain. Then the following are equivalent:*

i) A is integrally closed;
ii) $A_{\mathfrak{p}}$ is integrally closed, for each prime ideal $\mathfrak{p}$;
iii) $A_{\mathfrak{m}}$ is integrally closed, for each maximal ideal $\mathfrak{m}$.

Proof. Let K be the fraction field of A, C its integral closure in K, and $f : A \to C$ the inclusion map. Now K is also the fraction fields of $A_{\mathfrak{p}}, A_{\mathfrak{m}}$ and by the lemma, $C_{\mathfrak{p}}, C_{\mathfrak{m}}$ are the integral closures of $A_{\mathfrak{p}}, A_{\mathfrak{m}}$ respectively. Now, $A, A_{\mathfrak{p}}, A_{\mathfrak{m}}$ are integrally closed iff $f, f_{\mathfrak{p}}, f_{\mathfrak{m}}$ are respectively surjective. □

Lemma 2. *Let C be the integral closure of A in B and let $\mathfrak{a}^e$ be the extension of an ideal $\mathfrak{a}$ of A in C. Then the integral closure of $\mathfrak{a}$ in B is the radical of $\mathfrak{a}^e$ in C.*

Proof. If $x \in B$ is integral over $\mathfrak{a}$, we have an equation of the form $x^n + a_1 x^{n-1} + \cdots + a_n = 0, a_i \in \mathfrak{a}$. Therefore, $x \in C$, hence $x^n \in \mathfrak{a}^e \implies x \in r(\mathfrak{a}^e)$. Conversely, suppose $x \in r(\mathfrak{a}^e)$, then $x^n = \sum a_i x_i$ for some $n \geq 1, a_i \in \mathfrak{a}, x_i \in C$.
Since each x_i is integral over $A, M = A[x_1, \ldots, x_m]$ is a finitely generated A-module and $x^n M \subseteq \mathfrak{a}M$. This means that the map of multiplication by x^n satisfies a monic polynomial over $\mathfrak{a}$, hence is integral over A. □

Theorem 1.7. *Let $A \subseteq B$ be integral domains, A integrally closed, and let $x \in B$ be integral over an ideal $\mathfrak{a}$ of A. Then x is algebraic over the field of fractions K of A, and if its minimal polynomial over K is $t^n + a_1 t^{n-1} + \cdots + a_n$, then $a_1, \ldots, a_n$ lie in $r(\mathfrak{a})$.*

Proof. Let F be the field of fractions of B, then there is an inclusion map $K \hookrightarrow F$ and the element $x \in F$ is algebraic over K. Let L be the extension of K containing all conjugates $x_1, \ldots, x_n$ of x (can be taken as a subfield of the algebraic closure). In L, each x_i satisfies the same equation over K, hence each x_i is integral over $\mathfrak{a}$.
Therefore, the coefficients (which are in A for A is integrally closed) of the minimal polynomial of x over K, which are polynomials in the x_i, are integral over $\mathfrak{a}$. Hence, by the lemma above, each a_i lies in the radical $r(\mathfrak{a})$. □

Lemma 3. *Let $f : A \to B$ be a ring homomorphism and $\mathfrak{p}$ a prime ideal of A. Then $\mathfrak{p}$ is a contraction of a prime if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.*

Proof. Suppose $\mathfrak{p} = \mathfrak{q}^c = f^{-1}(\mathfrak{q})$, then it is clear that extending and contracting $\mathfrak{p}$ gives back $\mathfrak{p}$. Conversely, suppose $\mathfrak{p}^{ec} = \mathfrak{p}$ (note that the extension need not be prime), and let $S = f(A \setminus \mathfrak{p})$. Clearly, S is multiplicatively closed and the extension $\mathfrak{p}^e$ doesn't meet S, because the contraction is $\mathfrak{p}$. Therefore, $\mathfrak{p}^e$ extends to a proper ideal in $S^{-1}B$, and let it be contained in a maximal ideal $\mathfrak{m}$. The contraction $\mathfrak{q}$ of $\mathfrak{m}$ to B is a prime ideal containing $\mathfrak{p}^e$ and furthermore, $\mathfrak{q} \cap S = \emptyset$. Therefore, $\mathfrak{q}^c = \mathfrak{p}$ and $\mathfrak{p}$ is a contraction of a prime. □

Theorem 1.8. *(Going-down theorem) Let $A \subseteq B$ be integral domains, A integrally closed, B integral over A. let $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ be a chain of prime ideals of A, and let $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m (m < n)$ be a chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i, 1 \leq i \leq m$. Then the chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i, 1 \leq i \leq n$.*

Proof. Again we reduce to the case $m = 1, n = 2$. To obtain a prime ideal contained in $\mathfrak{q}_1$, we localise at $\mathfrak{q}_1$. Since every ideal of $B_{\mathfrak{q}_1}$ is an extended ideal, by the lemma, it suffices to show that $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$. We have the extensions $A \subseteq B \subseteq B_{\mathfrak{q}_1}$.
Elements of $B_{\mathfrak{q}_1}\mathfrak{p}_2$ are of the form $y/s, y \in B\mathfrak{p}_2, s \notin \mathfrak{q}_1$. By an earlier lemma, y is integral over $\mathfrak{p}_2$ (for it is in the radical of $\mathfrak{p}_2^e$), and since A is integrally closed, over the fraction field K of A, it has a minimal polynomial

$$y^r + u_1 y^{r-1} + \cdots + u_r = 0$$

with $u_1, \ldots, u_r \in \mathfrak{p}_2$.
Now suppose $x = y/s \in B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$, then $s = yx^{-1}$ with $x^{-1} \in K$ (this is happening in the field of fractions of B), so the minimal polynomial of s is given by

$$s^r + v_1 s^{r-1} + \cdots + v_r = 0$$

with $v_i = u_i/x^i$.
Since s is integral over A, we know that $v_1, \ldots, v_r$ are also integral over A (as they are the coefficients of the minimal polynomial of s), hence elements of A (for A is integrally closed). But in A, we also have the equation $x^i v_i = u_i \in \mathfrak{p}_2$.
If $x \notin \mathfrak{p}_2$, then $v_i \in \mathfrak{p}_2$, hence $s^r \in B\mathfrak{p}_2 \subseteq \mathfrak{q}_1$ which is a contradiction. So, $x \in \mathfrak{p}_2$ and $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$. □

2 Another point of view

Consider the ring $\mathbb{Z}[\sqrt{5}]$. This is not integrally closed because the element $(1+\sqrt{5})/2$ from the fraction field is integral, it satisfies $x(x-1) = 1$. Rewriting, we get $(1+\sqrt{5})(-1+\sqrt{5}) = (2)(2)$. In a sense, not being integrally closed is close to not being a UFD. More precisely, if some a/b from the fraction field is integral, we can rearrange its equation to get b^n as a polynomial in a.
Intuitively, sticking to monic polynomials means that we aren't inverting "large" elements of A. Similarly being integrally closed means that the fraction field only adds "fractional parts". Above, the number $(-1+\sqrt{5})/2$ is between 1 and 2 and subtracting 1 makes it negative. So, there's a "gap" between 1 and 2 that is not filled by purely fractional parts. So, being integrally closed means that the only remaining elements are the "true" fractional parts. Note that this discussion heavily borrows from the properties of the real line.

Definition 3. *For a ring A, the dimension $dim(A)$ is defined as $\sup_n\{n | \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n; \mathfrak{p}_i \in Spec(A)\}$, i.e., it is the supremum of length of chains of primes in A. Similarly, the height $ht(\mathfrak{p})$ of a prime is defined as the supremum of lengths of chains of primes contained in (and terminating at) $\mathfrak{p}$.*

To each ring A (commutative, with 1), we have the associated topological space $\mathrm{Spec}(A)$ and there is a partial order induced by inclusion. The dimension of a ring is a property of this topological space. More precisely, there is a contravariant functor Spec from the category of rings to the

category of topological spaces and each ring homomorphism $f : A \to B$ induces a continuous map $f^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$.
From a partially ordered set (poset) X we can form another poset $C^u(X)$ consisting of all finite chains. Given two chains $\tilde{a} = a_0 < a_1 < \cdots < a_n, \tilde{b} = b_0 < b_1 < \cdots < b_m$, we can say that $\tilde{a} < \tilde{b}$ if $n \leq m$ and $a_i = b_i, 0 \leq i \leq n$. One can verifiy that this is indeed a partial order. There is another order that we can put on the same set, namely $\tilde{a} < \tilde{b}$ if $n \leq m$ and $a_{n-i} = b_{m-i}, 0 \leq i \leq n$, call this set $C^d(X)$.
When B is integral over A, then Corollary 6 tells us that the map $f^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is in fact order preserving. So, not only do we have a map between their spectra, but we also have the maps

$$f_u^* : C^u(\mathrm{Spec}(B)) \to C^u(\mathrm{Spec}(A),$$

$$f_d^* : C^d(\mathrm{Spec}(B)) \to C^d(\mathrm{Spec}(A)).$$

The going up (down) theorem says that if $\tilde{a} \in \mathrm{Im}(f_u^*)$ (likewise f_d^* when A is integrally closed), then anything larger than $\tilde{a}$ is also in the image.
Now, Theorem 1.3 tells us that f^* is surjective. Then, by the Cohen–Seidenberg theorems, i.e., going up and down, the mapsf_u^*, f_d^* are surjective as well (f_d^* requires A to be integrally closed).
From $C^u(\mathrm{Spec}(A))$, for example, we have the length function to $\mathbb{N}$. The dimension is the supremum of this image. It is clear that f_u^* preserves length. By Corollary 6 we know that f_u^* is injective and going up theorem tells that it is surjective. Therefore,

$$\dim(A) = \dim(B).$$

By similar arguments, when A is integrally closed, by the going down theorem, for $\mathfrak{q} \in \mathrm{Spec}(B)$,

$$\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(f^*(\mathfrak{q})).$$

3 Noether Normalization and Zariski's lemma

Theorem 3.1. *(Noether normalization) Let k be an infinite field and let $A \neq 0$ be a finitely generated k-algebra. Then there exist elements $y_1, \ldots, y_r \in A$ which are algebraically independent over k and such that A is integral over $k[y_1, \ldots, y_r]$.*

Proof. Let A be generated by $x_1, \ldots, x_n$ as a k-algebra. If there is no algebraic dependence among these generators, then A is algebraically independent over k and we can take $r = n, y_i = x_i, 1 \leq i \leq n$.
Else, there is some algebraic dependence among these generators, i.e., there is some polynomial over k in n variables satisfied by $x_1, \ldots, x_n$, say $p(x_1, \ldots, x_n) = 0$.
Write $p = p_d + p_{d-1} + \cdots + p_1 + p_0$ as a sum of its homogenous components, and suppose x_n appears in p_d. In order to obtain integrality, we tweak p so that the coefficient of the highest degree in x_n is a constant. The monomials in p_d are of the form $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ with $a_1 + \cdots + a_n = d$. Obviously, if there was a term x_n^d, then it is clear that x_n is integral over the others. In order to arrive at such a monic coefficient, we do a linear change of $x_i, i < n$.
Replace x_i with $x_i - \lambda_i x_n$, i.e., set $x_i' = x_i - \lambda_i x_n$, then $A = k[x_1', \ldots, x_{n-1}', x_n]$ and

$$p(x_1' + \lambda_1 x_n, \ldots, x_{n-1}' + \lambda_{n-1} x_n, x_n) = 0.$$

Upon a linear change of variables, each p_j is still homogenous in $x_1', \ldots, x_{n-1}', x_n$ and the leading term of this polynomial (in the new set of generators) starts with $p_d(\lambda_1, \ldots, \lambda_{n-1}, 1)x_n^d$.
Since k is an infinite field, we can choose $\lambda_1, \ldots, \lambda_{n-1}$ so that the leading coefficient is nonzero. This means that x_n is integral over $k[x_1', \ldots, x_{n-1}']$. Essentially, we replaced the set of generators with a new set $x_1', \ldots, x_{n-1}', x_n$ obtained by a linear transformation such that x_n is integral over $k[x_1', \ldots, x_{n-1}']$.
We can repeat the construction and in a finite number of steps (since the number of generators required strictly decreases) arrive at $y_1, \ldots, y_r \in A$ which are algebraically independent over k such that A is integral over $k[y_1, \ldots, y_r]$ (being integral is transitive). □

Let us look closely at what the theorem means. Since at each stage all we did was a linear transformation, there is an invertible matrix $M \in k^{n\times n}$ such that after acting M on the generators of A, we get $A = k[y_1,\dots,y_r,y_{r+1},\dots,y_n]$ where $y_1,\dots,y_r$ are algebraically independent over k and y_j are integral over $k[y_1,\dots,y_r]$ for $j \geq r+1$.
Assume that k is algebraically closed. Suppose that $X = Z(I)$ for some ideal $I \subset k[x_1,\dots,x_n]$ and $A = k[x_1,\dots,x_n]/I$. We can act M on X and x_i and take $A = k[y_1,\dots,y_n]/\tilde{I}$ where these y_i are all algebraically independent and $\tilde{I}$ is the modified I (i.e., replace each $g(\underset{\sim}{x})$ with $g(M\underset{\sim}{x})$).
Let $L = k^r$ and $\pi\colon X \to L$ be the projection onto the first r coordinates. We claim that π is surjective. Let $b = (b_1,\dots,b_r) \in L$ be arbitrary and $e_b\colon k[y_1,\dots,y_r] \to k$ be the evaluation at b.
Since A is algebraic over $k[y_1,\dots,y_r]$ and k is algebraically closed, there is an extension $\tilde{e_b}\colon A \to k$ of e_b. Let $a_i = \tilde{e_b}(y_i)$. Given $g \in \tilde{I}$ we know that $g(y_1,\dots,y_n) = 0$ (because we modified I) where these y_i are from A. Since the extension is a ring homomorphism, we have $g(a_1,\dots,a_n) = 0$. Since $g \in \tilde{I}$ is arbitrary, $(a_1,\dots,a_n) \in X$. By definition of $\tilde{e_b}$ we must have $a_i = b_i, 1 \leq i \leq r$, therefore $\pi(a_1,\dots,a_n) = b$ completing the proof.
In general, suppose we have an affine set $X \subseteq \mathbb{A}^n$. The coordinates on the affine plane give us a set of coordinates on X, but these coordinates are far from optimal. To capture a notion of dimension we would like these coordinates to be minimal in the sense of algebraic independence. Noether normalization gives us a bunch of independent coordinates on which the others depend algebraically and it also gives a linear transformation onto an r-dimensional subspace hinting at the dimension.

Theorem 3.2. *(Weak Nullstellensatz) Let X be an affine variety in k^n, k algebraically closed, given by the vanishing of some ideal I. If $I(X) \neq (1)$, then X is non empty. Moreover, the maximal ideals of $k[x_1,\dots,x_n]$ are all of the form $(x_1 - a_1,\dots,x_n - a_n)$ for some $a_1,\dots,a_n \in k$.*

Proof. Set $A = k[x_1,\dots,x_n]/I$. Noether normalization (as $A \neq 0$, is finitely generated) applies and we get a surjective mapping $\pi\colon X \to k^r$ for some $r \geq 0$. This implies X is non empty. Note also that if $I(X)$ denotes the vanishing ideal fo X, then when $X \neq \emptyset$, we must have $I(X) \neq 1$. Moreover, if $I(X) \neq 1$ then it is also necessary that X be non empty. So we conclude $I(X) \neq 1 \iff X \neq \emptyset$ and moreover, if $I \neq 1$ then $Z(I) \neq \emptyset$. It is also clear that $\mathfrak{a} \subseteq I(Z(\mathfrak{a}))$ for any ideal $\mathfrak{a}$.
Now let $\mathfrak{m}$ be a maximal ideal and let $p = (p_1,\dots,p_n) \in Z(\mathfrak{m})$ (we know this is non empty by the arguments above). We have $I(p) \supseteq (x_1 - p_1,\dots,x_n - p_n)$ and $I(p) \supseteq I(Z(\mathfrak{m})) \supseteq \mathfrak{m}$. Because $I(p) \neq 1$, by maximality of $\mathfrak{m}$ we conclude that $\mathfrak{m} = (x_1 - p_1,\dots,x_n - p_n)$ (it's clear that $(x_1 - p_1,\dots,x_n - p_n)$ is a maximal ideal). □

Theorem 3.3. *(Zariski's lemma) Let k be a field and B a finitely generated k algebra. If B is a field then it is a finite algebraic extension of k.*

Direct proof. Let B be generated by $x_1,\dots,x_n$. We induct on n. If $n = 1$, then x_1^{-1} is a polynomial in x_1, hence x_1 is algebraic over k and B is a finite algebraic extension. Assume the result for $n-1$ generators. Let $A = k[x_1]$ and K be the fraction field of A. Then $k \subset K \subset B$ and B is generated by $x_2,\dots,x_n$ over K, hence is a finite algebraic extension of K.
Each $x_i, i \geq 2$ satisfies a polynomial over K with coefficients of the form $a/b, a, b \in A$. Let $f \in A$ be the common denominator over all these polynomials so that each x_i is integral over A_f. Since B is generated over A by $x_2,\dots,x_n$ and B contains K, we conclude that B, K are integral over A_f.
If x_1 is transcendental over k, then A is integrally closed, hence A_f is integrally closed. This forces $A_f = K$ which is absurd because then $f+1$ is invertible over A_f giving us some $g \in A, n \geq 1$ such that $g(f+1) = f^n$. But A is a UFD forcing $f+1$ to be a unit in A which is possible only if f is constant. But in the case when f is constant, $K = A_f = A$ is a contradiction (for x_1 was assumed transcendental). Therefore, x_1 is algebraic over k, hence A is algebraic over k. This means that f is invertible over A, hence $A_f = A$ and K is integral over A. By transitivity of integrality, B is algebraic over k and a finite algebraic extension of k. □

Proof via Noether normalization. Alternatively, we may use Noether normalization to obtain some $y_1,\dots,y_r \in B$ which are algebraically independent over A such that B is integral over $k[y_1,\dots,y_r]$. However, B is a field, so we know that $k[y_1,\dots,y_r]$ is a field which forces some algebraic dependence among the y_i unless $r = 0$ and B is algebraic over k. □

We can deduce the Weak Nullstellensatz from the Zariski lemma as follows: let $\mathfrak{m}$ be a maximal ideal of $k[x_1,\dots,x_m]$, then $B = k[x_1,\dots,x_n]/\mathfrak{m}$ is a finitely generated algebra over k which is also a field, hence it is integral over k. So, each x_i satisfies some polynomial $p_i(t)$ which, k being algebraically closed, splits into linear factors over k. In B, this same polynomial evaluated at x_i is zero, and being a field, some $(x_i - a_i)$, a factor of $p_i(x_i)$, is forced to be zero. Therefore, $(x_i - a_i) \in \mathfrak{m}$ for some $a_i \in k$ and we conclude that $\mathfrak{m} = (x_1 - a_1,\dots,x_n - a_n)$ as required.
Conversely, assume the Weak Nullstellensatz. Given B as in the theorem, there is a ring and k-algebra surjective homomorphism $k[x_1,\dots,x_n] \to B$. If $\mathfrak{m}$ denotes the kernel, then the quotient $B = k[x_1,\dots,x_n]/\mathfrak{m}$ is a field. We know that $\mathfrak{m} = (x_1 - a_1,\dots,x_n - a_n)$ so we see that the generators of B over k are integral over k (satisfying linear polynomials. Therefore, B is integral over k.

Theorem 3.4. *(Extension of Noether Normalization) Let A be a subring of an integral domain B such that B is finitely generated over A. Then there is an $A \ni s \neq 0$ and $y_1,\dots,y_n \in B$ algebraically independent over A such that B_s is integral over B'_s where $B' = A[y_1,\dots,y_n]$.*

One idea is to proceed as in the proof of normalization above with linear change of variables, i.e., choosing a different set of generators by a linear change. The point of this change is to make the "relations" polynomial monic (or at least start with an x_n^N where $B = A[x_1,\dots,x_n]$). In this case, if A was infinite, then by looking at the leading coefficient polynomial ($p(\lambda_1,\dots,\lambda_{n-1},1)$ in the proof above) over the fraction field, we can find some $\lambda_i \in A$ such that the leading coefficient is nonzero. Then the idea would be to localise at that coefficient and proceed by an induction.
In order to generalize, we need a different kind of change of variables. The main idea is to reduce the number of generators and induct.

Proof. Let $B = A[x_1,\dots,x_n]$ as an A-algebra. If the $x_1,\dots,x_n$ are algebraically independent, then we can take $s = 1, y_i = x_i$ and we're done. So, suppose they satisfy some polynomial relation, $p(x_1,\dots,x_n) = 0$.
Relabeling if necessary, we may assume that x_n is involved in some term. Let N be an integer larger than all the degrees of x_is appearing in p and consider the change of variables $x_i = x'_i + x_n^{N^i}, i < N$ and $x_n = x_n$. This is an automorphism of $A[x_1,\dots,x_n]$.
Then we have

$$p(x'_1 + x_n^N, x'_2 + x_n^{N_2},\dots,x'_{n-1} + x_n^{N^{n-1}}, x_n) = 0.$$

The terms $c_{a_1,\dots,a_n} x_1^{a_1}\dots x_n^{a_n}$ is replaced by $c_{a_1,\dots,a_n}(x'_1 + x_n^N)^{a_1}\dots(x'_{n-1} + x_n^{N^{n-1}})^{a_{n-1}} x_n^{a_n}$. Expanding this gives us a term

$$c_{a_1,\dots,a_n} x_n^{a_n + a_1 N + a_2 N^2 + \cdots + a_{n-1}N^{n-1}}.$$

In the final polynomial, these powers of x_n add up. However, observe that by the choice of N and the uniqueness of base N expansion of integers, none of these terms cancel out because they are all different powers of x_n. There is one caveat though, which is when $x_n^a = x_n^b$ for some a, b because B is an algebra over A. In this case, we see that x_n is some root of unity (B is an integral domain), which would directly tell us that B is integral over $A[x_1,\dots,x_{n-1}]$ thus reducing one step in the induction. So, assuming that all of these distinct powers of x_n don't interfere with each other, we have some maximal power of x_n appearing in this polynomial with some nonzero coefficient, c. Therefore, B_c (we can localise B freely because we can push the denominator to the coefficients when necessary; the point of localisation is so that we have containment of rings) is integral over $C = A_c[x'_1,\dots,x'_{n-1}]$ which is a finitely generated algebra over the integral domain A_c. By induction, obtain some $b_1,\dots,b_r \in C$ algebraically independent over A_c and a $A_c \ni d \neq 0$ such that C_d is integral over $(A_c)_d[b_1,\dots,b_r]$.
Since c is a unit in A_c, we may assume $d \in A$. Observe that $(A_c)_d = A_{cd}$, therefore, B_{cd} is integral over $A_{cd}[b_1,\dots,b_r]$. We may also assume that $b_i \in B$ just by scaling because the algebraic independence doesn't change (since the denominators are all powers of c to start with). Furthermore, observe that algebraic dependence of the b_is over A is equivalent to that over A_s because algebraic independence doesn't need monic polynomials, so we may freely scale our coefficients. □

Remark. This also proves Noether normalization for arbitrary fields.

4 Jacobson rings

Theorem 4.1. *Let A be a ring, the following are equivalent:*

i) Every prime ideal in A is an intersection of maximal ideals.
ii) In every homomorphic image of A the nilradical is equal to the Jacobson radical.
iii) Every prime ideal in A which is not maximal is equal to the intersection of prime ideals which contain it strictly.

Proof. • i)$\Leftrightarrow$ ii): Any homomorphic image of A is isomorphic to $A/\mathfrak{a}$ for some $\mathfrak{a}$. The nilradical of $A/\mathfrak{a}$ is the intersection of all prime ideals containing $\mathfrak{a}$ and similarly the Jacobson radical is obtained by the intersection of maximal ideals containing $\mathfrak{a}$. Assuming i), ii) follows.
Conversely, assuming ii), the nilradical of $A/\mathfrak{p}$ is equal to its Jacobson radical, hence the intersection of maximal ideals containing $\mathfrak{p}$ is equal to $\mathfrak{p}$.
- ii)$\Rightarrow$ iii): Let $\mathfrak{p}$ be a prime ideal which is not maximal, then the nilradical of $A/\mathfrak{p}$, which is zero, is the intersection of all maximal ideals containing $\mathfrak{p}$. These maximal ideals are prime ideals which strictly contain $\mathfrak{p}$ for $\mathfrak{p}$ is not maximal. It follows that $\mathfrak{p}$ is the intersection of prime ideals strictly containing $\mathfrak{p}$ (because a subfamily of such primes intersect to $\mathfrak{p}$).
- iii)$\Rightarrow$ i): Suppose i) is not true, then there is a prime ideal $\mathfrak{p}$ which is not an intersection of maximal ideals. Passing to the quotient, we may assume that A is an integral domain and that the Jacobson radical is nonzero. In this case, choose a nonzero $f \in \mathrm{J}(A)$ and consider the ring A_f. This is nonzero as f is notnilpotent, and let $\mathfrak{m}$ be the pullback of a maximal ideal. Then $\mathfrak{m}$ is a prime ideal in A and maximal in not containing f. This means that $\mathfrak{m}$ is itself not maximal for f is in the Jacobson radical and that $\mathfrak{m}$ cannot be written as an intersection of strictly larger prime ideals for they all should contain f, thus contradicting iii).

□

A ring satisfying the conditions above is called a *Jacobson ring*. Geometrically, if $A = k[x_1, \ldots, x_n]/I$ is a Jacobson ring, then the prime ideals of A describe the irreducible components of $Z(I)$ and the maximal ideals correspond to the minimal irreducible components. The Weak Nullstellensatz says that the minimal irreducible components are points and A being Jacobson says that the irreducible components are the union of minimal irreducible components. There is no indication as to whether the union is finite or not.

Lemma 4. *If A is a Jacobson integral domain and $0 \neq a \in A$, then A_a is also a Jacobson ring.*

Proof. Recall that prime (maximal) ideals of A_a are prime (maximal) ideals of A not containing a and this is a bijective correspondence. Let $\mathfrak{p} \in \mathrm{Spec}(A)$ not contain a. We claim that

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \in \mathrm{Max}(A) \\ a \notin \mathfrak{m} \supseteq \mathfrak{p}}} \mathfrak{m}.$$

Clearly $\mathfrak{p}$ is contained in the intersection. Suppose b is an element in the intersection, then $ab \in \mathfrak{m}$ for every maximal ideal that contains $\mathfrak{p}$ or a. The intersection of such maximal ideals is contained in the intersection of all maximal ideals containing $\mathfrak{p}$, hence $ab \in \mathfrak{p} \implies b \in \mathfrak{p}$. □

Theorem 4.2. *(General Nullstellensatz) Let A be a Jacobson ring and B an A-algebra. If B is either integral over A or finitely generated as an A-algebra, then B is a Jacobson ring. In particular, every finitely generated ring, and every finitely generated algebra over a field is a Jacobson ring.*

Proof. First suppose B is integral, then recall that every prime in A has a prime over it in B and one is maximal iff the other is. So, given a prime $\mathfrak{q} \in \mathrm{Spec}(B)$, let it contract to $\mathfrak{p}$. By integrality, there is a one to one correspondence between the primes containing $\mathfrak{q}$ and those containing $\mathfrak{p}$. Since A is Jacobson, $\mathfrak{p}$ is the intersection of the maximal ideals containing it which means that the intersection of maximal ideals containing $\mathfrak{q}$ is an ideal $\mathfrak{a} \supseteq \mathfrak{q}$ which contracts to $\mathfrak{p}$. By Corollary 6 we conclude that $\mathfrak{a} = \mathfrak{q}$ is an intersection of maximal ideals.

Next, suppose B is finitely generated as an A-algebra. Let $\mathfrak{q} \in \mathrm{Spec}(B)$ and let it contract to $\mathfrak{p} \in \mathrm{Spec}(A)$. We need to show that the Jacobson radical of $B/\mathfrak{q}$ is zero. Observe that $B/\mathfrak{q}$ is a finitely generated $A/\mathfrak{p}$-algebra (using the "same" generators). So we reduce to the case where A, B are domains, A is still a Jacobson ring. By the extended Noether normalization, we know that there is some nonzero $s \in A$ and $y_1, \ldots, y_r \in B$ algebraically independent over A such that B_s is integral over $A_s[y_1, \ldots, y_r]$. Because of the correspondence between ideals, if the Jacobson radical of B_s is zero, then so is that of B. Moreover, by the first part, if $A_s[y_1, \ldots, y_r]$ is Jacobson, then so is B_s. Note that A_s is still a Jacobson ring.
So we are reduced to the case where A is a domain and $B = A[x_1, \ldots, x_n]$ is a polynomial ring. What we want to show is that the Jacobson radical is zero, i.e., given a nonzero polynomial f we want to find a maximal ideal not containing f. But this is obvious because $A[x_1, \ldots, x_n]$ is an integral domain, so we can localise at f, find a maximal ideal (every nonzero ring has a maximal ideal by Zorn's lemma) and pull it back. □

We digress a bit here to discuss what this looks like from a topological point of view. Let A denote a ring. A point x of $\mathrm{Spec}(A)$ is closed iff it corresponds to a maximal idea: indeed, if x corresponds to $\mathfrak{m} \in \mathrm{Max}(A)$ then $x = Z(\mathfrak{m})$. Conversely, if $x = Z(\mathfrak{a})$ for some ideal $\mathfrak{a}$, then because every ideal is contained in a maximal ideal, x must be a maximal ideal containing $\mathfrak{a}$.
Next, suppose $S \subseteq \mathrm{Max}(A)$, then $\overline{S} = Z(\cap_{x \in S} x)$. By definition of closure, we have $\subseteq$ inclusion. Conversely, suppose $\mathfrak{p} \in Z(\cap_{x \in S} x)$ and let D_f be a basic neighbourhood of $\mathfrak{p}$ (this is the set of all primes not containing $f \in A$). If f was in every maximal ideal in S, then f is in the intersection of those maximal ideals, which would imply $f \in \mathfrak{p}$, therefore, $D_f \cap S \neq \emptyset$ which gives us the required equality.
Now, suppose A is Jacobson, then given a closed set $Z = Z(\mathfrak{a})$, because the nilradical of $A/\mathfrak{a}$ is the same as its Jacobson radical and from the observation above, we see that $Z = \overline{Z \cap \mathrm{Max}(A)}$. In other words, Z is given as the closure of the closed points in Z. The converse is also clear.

Definition 4. *A topological space X is called Jacobson if every closed subset Z is the closure of the closed points contained in Z.*

Corollary 8. *A ring A is Jacobson iff Spec(A) is Jacobson.*

5 Artin-Tate lemma

Theorem 5.1. *(Artin-Tate lemma) Let $A \subseteq B \subseteq C$ be rings. Suppose A is Noetherian, C is finitely generated as an A-algebra and either finitely generated as a B-module or integral over B. Then B is finitely generated as an A-algebra.*

Proof. Let $C = A[x_1, \ldots, x_m]$ then $x_1, \ldots, x_m$ generate C as a B-algebra and if each is integral over B, then C is a finitely generated B-module. Conversely, if C is a finitely generated B-module, then C is integral over B.
Let $y_1, \ldots, y_n$ generate C as a B-module, then we have

$$x_i = \sum_j b_{ij} y_j \quad (b_{ij} \in B)$$

$$y_i y_j = \sum_k b_{ijk} y_k \quad (b_{ijk} \in B)$$

Let B_0 be the algebra generate over A by b_{ij}, b_{ijk}. By Hilbert's basis theorem (and the fact that quotients of Noetherian rings is Noetherian), B_0 is Noetherian and $A \subseteq B_0 \subseteq B$.
Now, elements of C are polynomials in x_i with coefficients in A. Using the expressions above, we can write elements in C as a linear combination of y_i with coefficients in B_0. This means C is a finitely generated B_0 module. Since B_0 is Noetherian and B is a B_0-submodule of C, B is a finitely generated B_0-module. Since B_0 is a finitely generated A-algebra, B is also a finitely generated A-algebra (taking the generators to be the generators of B_0 over A together with those of B over B_0). □

The Noetherian hypothesis is necessary and an example is found in [8].

Theorem 5.2. *(Zariski's lemma via Artin-Tate) Let k be a field, E a finitely generated k-algebra. If E is a field then it is a finite algebraic extension of k.*

Proof. Let $E = k[x_1,\dots,x_n]$. If E is not algebraic, then we may renumber the x_i so that $x_1,\dots,x_r$ are algebraically independent over $k, r \geq 1$ and each $x_j, j > r$ is algebraic over $F = k(x_1,\dots,x_r)$. Now we have $k \subseteq F \subseteq E$ and E is of finite type over k and finite over F, hence by Artin-Tate lemma, F is of finite type over k, i.e., F is a finitely generated k-algebra.
Now, suppose the generators are $y_1,\dots,y_s$ where each y_i is of the form f_i/g_i for polynomials $f_i, g_i \in k[x_1,\dots,x_r]$. However, the element $h = (g_1 g_2 \dots g_s + 1)^{-1}$ (if this is undefined, then the g_1 are constants, hence we can just look at $1/x_1$, for example) cannot be written as a polynomial in y_i over k, which is a contradiction. Therefore, E is algebraic over k, and therefore finite algebraic. □

Corollary 9. *(Weak Nullstellensatz) Let k be a field, A a finitely generated k-algebra. Let $\mathfrak{m}$ be a maximal ideal of A. Then $A/\mathfrak{m}$ is a finite algebraic extension of k. In particular, if k is algebraically closed then $A/\mathfrak{m} \cong k$.*

Theorem 5.3. *(Strong Nullstellensatz) Let k be an algebraically closed field, let A denote the polynomial ring $k[t_1,\dots,t_n$ and let $\mathfrak{a}$ be an ideal of A. Then $I(Z(\mathfrak{a})) = r(\mathfrak{a})$ where $Z(\mathfrak{a})$ denotes the zero set of $\mathfrak{a}$ and $I(V)$ denotes the vanishing ideal of any $V \subseteq k^n$.*

Proof. It is clear that $r(\mathfrak{a}) \subseteq I(Z(\mathfrak{a}))$. Conversely, suppose $f \notin r(\mathfrak{a})$, then there is a prime $\mathfrak{p} \supseteq \mathfrak{a}$ not containing f. We move to the subset of $Z(I)$ determined by $\mathfrak{p}$. This has coordinate ring $B = A/\mathfrak{p}$. Let $\bar{f}$ denote the image of f in B and concider $C = B_{\bar{f}}$.
Intuitively, C is zoning in on a point where f doesn't vanish by giving us a ring of functions at such a point. Let $\mathfrak{m}$ be a maximal ideal of C. Since C is a finitely generated k-algebra and k is algebraically closed, $C/\mathfrak{m} = k$. Let x_i be the image of t_i through the compositions $A \to B \to C \to k$. So we have a point $x = (x_1,\dots,x_n) \in k^n$.
Because these are ring homomorphisms and $\mathfrak{a} \subseteq \mathfrak{p}$ and $f \notin \mathfrak{p}$ we see that $x \in Z(I)$ but $f(x) \neq 0$ as f is a unit in C. Therefore, $I(Z(\mathfrak{a})) = r(\mathfrak{a})$. □

6 Rabinowitsch trick

In the spirit of collecting all the proofs of the nullstellensatz that I have come across, here is a neat trick by George Yuri Rainich, [9]. Suppose f vanishes on the zero set of $f_1,\dots,f_m \in k[x_1,\dots,x_n]$. Then the ideal $(f_1,\dots,f_k, 1 - x_0 f) \subseteq k[x_0,\dots,x_n]$ doesn't vanish anywhere. By the weak nullstellensatz, there exist polynomials $g_0,\dots,g_m$ such that

$$1 = g_0(1 - x_0 f) + \sum_{i \geq 1} g_i f_i.$$

Here g_i are polynomials in $x_0,\dots,x_n$. Since this holds as polynomials, we can substitute $1/f(x_1,\dots,x_n)$ for x_0 and after clearing out the denomintors, some power f^r of f is in the ideal $(f_1,\dots,f_m)$ thus proving the strong nullstellensatz.

7 AC/DC

Noetherian modules satisfy the ascending chain condition (acc) on submodules while Artinian rings satisfy the descending chain condition (dcc). It turns out that a ring is Artinian iff it is Noetherian with Krull dimension 0. This section contains selected results from [1] chapters 6 and 8.

Proposition 1. *Let A be a Noetherian ring with one prime ideal $\mathfrak{m}$, then $\mathfrak{m}^n = 0$ for some n.*

Proof. Since the radical of the zero ideal must be $\mathfrak{m}$ and $\mathfrak{m}$ is finitely generated, $\mathfrak{m}^n = 0$ for some sufficiently large n. □

By various correspondences, submodules, quotients and localisations of a module satisfying acc/dcc also satisfies the same. From this it follows that if $0 \to M' \to M \to M'' \to 0$ is an exact sequence of modules then M is Noetherian/Artinian iff M', M'' are. We next have

Proposition 2. *Suppose M is an R-module with a filtration $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$. Then M is Artinian (Noetherian) iff each quotient is Artinian (Noetherian).*

Proof. We prove for dcc, the exact same proof works for acc. First suppose M satisfies dcc, then each M_i is Artinian as well (being submodules) and each quotient is Artinian as well (by correspondence between submodules in the original module and submodules in the quotient).
Conversely, suppose each quotient is Artinian, this means in particular that M_{n-1} is Artinian. Quotient throughout by M_{n-1} to get a shorter filtration with each quotient being Artinian. By induction (the cases $n = 1, 2$ are clear), we conclude that $M_{n-1}, M/M_{n-1}$ are Artinian, hence M is Artinian. □

Now we make a few observations. A vector space over a field k is finite dimensional iff it is a Artinian iff it is a Noetherian k-module. Given a maximal ideal $\mathfrak{m}$ of a ring A, we always have the $\mathfrak{m}$-adic filtration $A \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \ldots$. Using Nakayama's lemma, $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ iff $\mathfrak{m}^n = 0$.
Each quotient is an $A/\mathfrak{m} = k$-vector space and if $\mathfrak{m}$ is finitely generated, then each quotient is finitely generated.
More generally, we have the following in [1]

Corollary 10 (Corollary 6.11 of [1])**.** *Let A be a ring in which the zero ideal is a product $\mathfrak{m}_1 \ldots \mathfrak{m}_n$ of maximal ideals. Then A is Noetherian iff it is Artinian.*

The proof uses the filtration by successive product of maximal ideals and because each quotient is a vector space over some field, we know that acc and dcc are related to this being finite dimensional and let's us go from acc to dcc and vice versa.

Proposition 3. *All primes in an Artinian ring are maximal.*

Proof. Let $\mathfrak{p}$ be a prime in an Artinian ring A, then $A/\mathfrak{p}$ is an Artinian integral domain. By dcc, given $x \in A/\mathfrak{p}$ there is some n, y such that $x^{n+1}y = x^n$. We can cancel the x^n to obtain an inverse of x which means $A/\mathfrak{p}$ is a field. □

Proposition 4. *Artinian rings have finitely many maximal ideals.*

Proof. Consider the set of all finite intersections of maximal ideals. By dcc, this has a minimal element $\mathfrak{m}_1 \cap \ldots \mathfrak{m}_n$. If $\mathfrak{m}$ is any maximal ideal, then taking its intersection with this minimal element shows $\mathfrak{m} \supseteq \mathfrak{m}_1 \cap \ldots \mathfrak{m}_n$ and it follows that $\mathfrak{m} = \mathfrak{m}_i$ for some i. □

Proposition 5. *The nilradical of an Artinian ring is nilpotent.*

Proof. Let $\mathfrak{R}$ denote the nilradical. By dcc, there is an n such that $\mathfrak{R}^n = \mathfrak{R}^{n+1} = \cdots = \mathfrak{a}$. If $\mathfrak{a} \neq 0$, consider the set of ideals $\mathfrak{b}$ for which $\mathfrak{a}\mathfrak{b} \neq 0$ (the nilradical is one such ideal). There is a smallest such ideal $\mathfrak{c}$ and there is an $x \in \mathfrak{c}$ such that $x\mathfrak{a} \neq 0$. We also have $x\mathfrak{a}^2 = x\mathfrak{a}$, so by minimality, $\mathfrak{c} = (x) = x\mathfrak{a}$ which means that there is a $y \in \mathfrak{a}$ such that $x = xy = xy^2 = \ldots$. Since $\mathfrak{a} \subseteq \mathfrak{R}, y$ is nilpotent, hence $x = 0$. □

Now we have all the ingredients to conclude

Theorem 7.1. *A ring A is Artinian iff it is Noetherian of Krull dimension 0.*

Proof. Suppose A is Artinian, then it has dimension 0 and has finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. The nilradical is the intersection of these maximal ideals, so the product of kth powers of $\mathfrak{m}_i$s is contained in the kth power of the intersection, which is 0 for large k, hence the 0 ideal is a product of maximal ideals and we're done by a corollary above.
Conversely, if A is Noetherian of dimension 0, the primary decomposition (in a Noetherian ring we have decomposition into irreducible ideals which are primary) of the zero ideal tells us that A has finitely many minimal primes (a version of prime avoidance), and these have to be maximal as well. In a Noetherian ring, the nilradical is nilpotent, and in our case, the nilradical is an intersection of maximal ideals and we are reduced to the previous case. □

8 Hauptidealsatz

In this final section we provide a proof of Krull's Hauptidealsatz (Principal Ideal Theorem) and some of its implications.

Theorem 8.1. *Let A be a Noetherian ring and $I = (f)$ a principal ideal, then each minimal prime over I has height at most one. Moreover, if f is not a zero divisor, then such primes have height* 1.

Theorem 8.2. *Let A be a Noetherian ring and I an ideal generated by n elements, then each minimal prime over I has height at most n, and equal to n if the generators form a regular sequence.*

Definition 5. *A sequence $(a_1, \dots, a_n)$ is regular if the ideal isn't all of A and if a_i is not a zero divisor in $A/(a_1, \dots, a_{i-1})$.*

Note that the order matters: $x, y(1-x), z(1-x)$ is regular in $k[x,y,z]$ whereas $y(1-x), z(1-x), x$ is not. There are situations where permutations don't matter, see [11]. The idea is that at each stage you are removing one dimension. Observe that if $(a_1, \dots, a_n)$ is a regular sequence contained in a prime ideal $\mathfrak{p}$, then the sequence remains regular upon locailzation at $\mathfrak{p}$.
Before providing the proofs we discuss the idea of height and dimension. We have defined the Krull dimension and height earlier. For a general ideal I, it is tempting to define a height or dimension but such definitions don't make much geometric sense: $I = ((y-1)y, xy)$ has as its zero sets the x axis and the point $(0,1)$ and is not principal. We should instead restrict ourselves to irreducible algebraic sets, or those ideals that have prime ideals as their radicals. But this alone is not enough: consider $I = (x^2, xy)$ whose zero set is the x axis and the origin is a double point. This has prime radical but a direct extension of dimension isn't quite satisfactory because the algebra sees the multplicity, but the geometry doesn't. We restrict to primary ideals.
Secondly, if A is a finitely generated k-algebra, then by Noether normalization we can obtain $A \supseteq k[y_1, \dots, y_r] \supseteq k$ where the y_i are independent over k and A is algebraic over $k[y_1, \dots, y_r]$. In this case we can define the dimension of A over k to be the transcendental degree $\operatorname{trdeg}_k(A) = r$. Of course, the immediate question is whether this is unique and whether these definitions agree.

Lemma 5. *With notation as above $r = dim(A)$.*

Proof. Since A is integral over $k[y_1, \dots, y_r]$ and $k[y_1, \dots, y_r]$ is integrally closed because it's a UFD by (one of many) Gauss' lemma, they have the same Krull dimensions, so we are left to find the dimension of polynomial rings. Using $0 \subset (y_1) \subset \cdots \subset (y_1, \dots, y_r)$ we see that the dimension is at least r. When $r = 1$, then because k is algebraically closed, it has Krull dimension 1. Assume this result for $k[y_1, \dots, y_n]$ for any $n < r$.
Let $0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m$ be a chain of prime ideals and let $u \in \mathfrak{p}_1$. Suppose, without loss of generality, $u \in k[y_2, \dots, y_r][y_1]$ is a non constant polynomial in y_1. Then $S = k[y_1, \dots, y_r]$ is integral over $T = k[u, y_2, \dots, y_r]$ (T need not be integrally closed because y_1 may be in its fraction field). Now, go modulo (u) so as to have a chain $0 \subset \overline{\mathfrak{p}_1} \subsetneq \cdots \subsetneq \overline{\mathfrak{p}_m}$ of primes in $S/(u)$ which is integral over $T/(u) = k[y_2, \dots, y_r]$. By incomparability (Corollary 6) the chain in $S/(u)$ descends to a chain in $T/(u)$ of length $m-1$ or m depending on whether $\mathfrak{p}_1 = (u)$ or not respectively. Thus we conclude that $m \leq r$ as required. As a corollary, r is well defined. □

8.1 Some thoughts on the symbolic power

Here, briefly, I want to think about symbolic powers and their geometric meaning. The setup is as follows. We have ideals on one hand and algebraic sets on the other. Irreducibility is important from the topological point of view, but doesn't translate quite directly to the algebraic side. We can define an ideal to be irreducible when it is not the intersection of two larger ideals, but this isn't quite satisfactory.
Consider $(x^2, xy, y^2) = (x^2, y) \cap (x, y^2)$. This describes the origin, with multiplicity 2 (here, multiplicity is just a vague intuitive term), but is not an irreducible ideal. The multiplicity has, in some sense, been artifically separated. We also don't have a uniqueness of decomposition as we have on the topological side.

Ideally, we want our decomposition of the ideals into ideals that describe the irreducible components of the corresponding algebraic set. Since irreducible components correspond to ideals having *prime* radicals, we group irreducible ideals with same radicals resulting in *a* primary decomposition. Algebraically, we define primary ideals to mimic the properties of prime powers of integers, we say $\mathfrak{q}$ is primary if whenever $xy \in \mathfrak{q}, x \in \mathfrak{q}$ or $y \in r(\mathfrak{q})$. But primary ideals need not be prime powers, nor are prime powers primary ideals.
How badly can a prime power fail to be primary? Well, take a prime $\mathfrak{p}$ and consider $\mathfrak{p}^n$. Now this always has a primary decomposition, and the associated primes (associated in the sense that they are obtained as radicals (which are determined uniquely) of the primary ideals involved in this decomposition; there is a more general sense of associated primes which turns out to be equivalent) all contain $\mathfrak{p}$. Of particular interest is the $\mathfrak{p}$-primary component, $\mathfrak{p}^{(n)}$ of $\mathfrak{p}^n$ and this is called the **symbolic power**.
In some vague sense, the symbolic power contains extra elements that are almost elements of $\mathfrak{p}^n$ but don't end up in that set because of some embedded perturbations coming from the embedded primes. As we'll see soon, to get the symbolic powers we will have to localize the ideal and contract it, which in some sense adds the "thick" points of higher multiplicities by "ignoring" the embedded primes.
Hold that thought. Going to the algebro-geometric correspondences, the elements of $\mathfrak{p}$ are functions (think of $\mathfrak{p}$ as an ideal in some polynomial algebra) that vanish on its affine variety, X. Pulling ideas from differential geometry/real analysis, we ask about the order of vanishing of functions. One could define that $f \in \mathfrak{p}$ has order at least 2 at some $x \in X$ if $f \in \mathfrak{m}_x^2$ where $\mathfrak{m}_x$ is the ideal of the point x. And a function in $\cap_{x \in X} \mathfrak{m}_x^n$ vanishes with order at least n on the whole of X.
Now, in this algebraic geometry setting, define the **differential power** $\mathfrak{p}^{<n>}$ of $\mathfrak{p}$ to be those functions with order at least n on all of X. The theorem of Zariski-Nagata says that the $\mathfrak{p}^{(n)} = \mathfrak{p}^{<n>}$. A good survey on symbolic powers can be found in [4]. The question of different containments of the symbolic and usual powers of an ideal is an interesting one, [10].
Next we figure out exactly what the nth symbolic power of a prime $\mathfrak{q}$ is. In a Noetherian ring we always have a primary decomposition and because we are looking at $\mathfrak{q}^n$ all the primes *belonging* to $\mathfrak{q}^n$ contain $\mathfrak{q}$ and furthermore, $\mathfrak{q}$ is the unique minimal/isolated prime belonging to $\mathfrak{q}^n$. We use Proposition 4.9 of [1] which gives us a tool to figure out the $\mathfrak{q}$-primary component, i.e., the nth symbolic power.
Specifically, we have to localize at $\mathfrak{q}$, extend the nth power and contract it back. In other words

$$\mathfrak{q}^{(n)} = \{r \in A : rs \in \mathfrak{q}^n \text{ for some } s \in A \setminus \mathfrak{q}\}.$$

The fact that this is a $\mathfrak{q}$-primary ideal is an exercise for the reader. There are some more properties of the symbolic power in exercises of [1], chapter 4.
We can define the symbolic powers for arbitrary ideals as

$$\mathfrak{a}^{(n)} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}_A(\mathfrak{a})} \phi_{\mathfrak{p}}^{-1}(\mathfrak{a}^n A_{\mathfrak{p}})$$

where $\mathrm{Ass}_A(\mathfrak{a})$ are the primes associated to $\mathfrak{a}$, i.e., those that appear as annihilators of elements of $A/\mathfrak{a}$. It is clear that successive symbolic powers form a descending chain.

8.2 Proofs

These proofs are more or less borrowed from [3].

Proof of Theorem 8.1. Let $\mathfrak{p}$ be a minimal prime over $I = (f)$. Since we want the height of $\mathfrak{p}$, we don't really care about things happening outside $\mathfrak{p}$, so we localize at $\mathfrak{p}$ and move to $A_{\mathfrak{p}}$. The heights don't change because of the correspondence between ideals of A and ideals of $A_{\mathfrak{p}}$. Therefore, we may assume that $\mathfrak{p}$ is the maximal ideal. Suppose $\mathfrak{q}$ is a prime contained in $\mathfrak{p}$. We first want to show that $A_{\mathfrak{q}}$ has dimension 0: this would mean that there can't be any prime below $\mathfrak{q}$ or between $\mathfrak{p}, \mathfrak{q}$.

Observe that $A/(f)$ is an Artinian ring because there's only one prime ideal $\mathfrak{p}$ because it is minimal and the only maximal ideal. In this ring we have the descending chain

$$\mathfrak{q}^{(1)} + (f) \supseteq \mathfrak{q}^{(2)} + (f) \supseteq \dots$$

which should stabilize giving $\mathfrak{q}^{(n)} + (f) = \mathfrak{q}^{(n+1)} + (f)$ for some $n \geq 1$. Because $f \notin \mathfrak{q}$ (and using the definition of symbolic power above) we can see that this equality gives

$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + (f)\mathfrak{q}^{(n)}.$$

Now by a version of Nakayama's lemma (go modulo $n+1$th symbolic power) because f is in the maximal ideal $\mathfrak{p}$ we must have $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$.
Move to $A_\mathfrak{q}$. Here we have $\mathfrak{q}^{(n)}A_\mathfrak{q} = \mathfrak{q}^{(n+1)}A_\mathfrak{q}$. We know that $\mathfrak{q}^n A_\mathfrak{q} \subseteq \mathfrak{q}^{(n)}A_\mathfrak{q}$. Given $r \in \mathfrak{q}^n A_\mathfrak{q}$ there is some invertible s (from $A \setminus \mathfrak{q}$) such that $rs \in \mathfrak{q}^{n+1}A_\mathfrak{q}$ which implies that $\mathfrak{q}^n A_\mathfrak{q} \subseteq \mathfrak{q}^{n+}A_\mathfrak{q}$. We always have the reverse inclusion, so by Nakayama's lemma (because $\mathfrak{q}$ is maximal in $A_\mathfrak{q}$), we conclude

$$\mathfrak{q}^n A_\mathfrak{q} = 0.$$

Finally, a local ring $(R, \mathfrak{m})$ with $\mathfrak{m}^n = 0$ has only one prime, hence has dimension 0 which means that $A_\mathfrak{q}$ has dimension 0, therefore $\mathfrak{p}$ has height 1.
For the second part, if $\mathfrak{p}$ had height 0, $A_\mathfrak{p}$ has only one prime, hence f is nilpotent in $A_\mathfrak{p}$ because the nilradical is the intersection of all primes. Which tells us that f is a zero divisor in A. This doesn't really require A to be Noetherian, although if A were Noetherian, then we could conclude that not only is f a zero divisor, but it is in fact a nilpotent element in A. □

Proof of Theorem 8.2. We prove this by induction, let $I = (a_1, \dots, a_n), n \geq 2$ and let $\mathfrak{p}$ be minimal over I. Again, we may localize at $\mathfrak{p}$ and assume that it is maximal. Because A is Noetherian, the set of all primes strictly contained in $\mathfrak{p}$ has a maximal element $\mathfrak{q}$ (if this set were empty, then $\operatorname{ht}(\mathfrak{p}) = 0$ and elements of I are zero divisors: the argument in the proof of 8.1 showed that elements in height 0 primes are zero divisors).
Since $\mathfrak{p}$ is minimal, we know that $I \not\subseteq \mathfrak{q}$, say $a_j \notin \mathfrak{q}$. Now observe that $\mathfrak{p}$ is the only prime over $(a_1, \dots, a_n)$ and $(\mathfrak{q}, a_j)$, hence these two ideals have the same radicals, which means we may write

$$a_i^{n_i} = q_i + b_i a_j, 1 \leq i \leq n$$

for $q_i \in \mathfrak{q}, b_i \in A$ with $q_j = 0, b_j = 1, n_j = 1$ (there may be other equalities, but we pick this one for a_j.
The proof has two parts now, the first is to show that $\mathfrak{q}$ is minimal over $(q_1, \dots, q_n)$ (keep in mind that $q_j = 0$, so there are $n-1$ generators) and the second part is that when $(a_1, \dots, a_n)$ is a regular sequence, so is $(q_1, \dots, q_n)$ (having a zero in between is somewhat of an edgecase scenario, but doesn't really matter with the proof). We do the second part first.
Suppose we have a regular sequence to begin with. If some aq_t was a linear combination of $q_i, i < t$ then by rearranging the equations above, we see that $aa_t^{n_t}$ is a linear combination of $a_i, i < t, a_j$. If $j < t$, then a_t is a zero divisor (a_t appears only once, so the coefficients don't cancel out) modulo $(a_1, \dots, a_{t-1})$ and if $j > t$, then a_j is a zero divisor modulo $(a_1, \dots, a_{j-1})$ or the coefficients of a_j cancel out, making a_t a zero divisor modulo $(a_1, \dots, a_{t-1})$. Therefore, we have a regular sequence.
Finally, to prove that $\mathfrak{q}$ is minimal over $(q_1, \dots, q_n)$, look at $A/(q_1, \dots, q_n)$. In this ring, $\mathfrak{p}$ is minimal over the element (a_j), which means, by 8.1, it has height at most 1. In fact it has height exactly 1 because $a_j \in \mathfrak{p} \supsetneq \mathfrak{q} \supseteq (q_1, \dots, q_n)$. Therefore, $\mathfrak{q}$ is minimal over $(q_1, \dots, q_n)$, hence $\operatorname{ht}(\mathfrak{q}) \leq n-1$ and equality holds in the case of regular sequences.
Since this is true for every $\mathfrak{q}$ "just below" $\mathfrak{p}$, we conclude that $\operatorname{ht}(\mathfrak{p}) \leq n$ and equality holds when we have regular sequences. In fact, we can say that $\operatorname{ht}(\mathfrak{p}) = n-1$ or n because the induction steps add 1 to the height at every stage except in the final step where we have to use 8.1 for the last time. □

Theorem 8.3. *Suppose A is Noetherian and $\mathfrak{p}$ is a prime of height n, then it is a minimal prime over an ideal generated by n elements.*

Proof. If $n = 0$ then the result is clear, so assume$n \geq 1$. We inductively find elements $x_1, \ldots, x_i \in \mathfrak{p}$ such that minimal primes over $(x_1, \ldots, x_i)$ have height i. Suppose $x_1, \ldots, x_{i-1}$ have been found, set $I_{i-1} = (x_1, \ldots, x_{i-1}), i > 1$ and 0 of $i = 1$. By the Noetherian condition, there are finitely many minimal primes over I_{i-1} and each of these have heights $i - 1$. By prime avoidance lemma, $\mathfrak{p}$ is not contained in their union (when $i < n = \mathrm{ht}(\mathfrak{p})$), say x_i is one such element. Set $I_i = (x_1, \ldots, x_i)$.
By choice of x_i a $\mathfrak{q}$ minimal over I_i is not minimal over I_{i-1}, hence strictly contains a minimal one, making $\mathrm{ht}(\mathfrak{q}) \geq i$. By Hauptidealsatz, $\mathrm{ht}(\mathfrak{q}) = i$. The process terminates when we have n elements. □

If we define the height of any ideal as the infimum of heights of all minimal primes over it, then the theorem above holds for any ideal.

Corollary 11. *Let A be a Noetherian integral domain. Then A is a UFD iff all height 1 primes are principal.*

Proof. Suppose A is a UFD, $\mathfrak{p}$ a prime of height 1. Then $\mathfrak{p}$ is minimal over some principal ideal (f). Using a factorization of f, some irreducible element f_0 is in $\mathfrak{p}$. Then $0 \subsetneq (f_0) \subseteq \mathfrak{p}$ is a chain of primes, which means $\mathfrak{p} = (f_0)$ is principal.
By the Noetherian hypothesis, all elements have a factorization into irreducibles. Uniqueness follows if we prove that irreducible elements are prime. Suppose x is irreducible, $\mathfrak{p}$ minimal over x. Since A is an integral domain, $\mathrm{ht}(\mathfrak{p}) = 1$ which means it is principal, say $\mathfrak{p} = (a)$. Then $x = ab$ for some b and by irreducibility, b is a unit, hence $(x) = \mathfrak{p}$ is a prime ideal thus concluding the proof. □

9 Concluding section

The initial goal was to compile a bunch of proofs of the Nullstellensatz. Progress was slow due to procrastination and/or getting busy with other things. At some point I decided to include the Hauptidealsatz as well, primarily because both have a "satz" in their name, which is German for proof, but also because both are very important results that bridge geometry and algebra.
There are many other proofs of the Nullstellensatz and with varying degrees of generality. One particularly interesting proof is that of Munshi, [5] which uses a technique which doesn't appear above. Wikipedia's entry [7] and the MathOverflow thread, [6], are good places to look for the various forms of the Nullstellensatz.
The Hauptidealsatz leads to Dimension theory, where we try to look at different kinds of dimensions one can put on a ring and depending on how "nice" we want our rings to be, we get different classes of rings: catenary rings, universaly catenary rings, regular local rings, Cohen-Macaulay rings etc. It's a beautiful sequence of ideas, which I haven't learnt enough to write about nor would I write about it here for this is already too long. Then there are strong connections between algebra and geometry as in the last corollary. The one big result is Serre's criterion ([12]) which relates algebraic properties such as normality or being Cohen-Macaulay with geoemtric properties like depth (a notion not defined in this article). Matsumura's Commutative Algebra, [2], is a good place to learn about these results.

References

[1] *Introduction to Commutative Algebra*, Atiyah and MacDonald

[2] *Commutative Algebra*, Matsumura

[3] Ravi Vakil's textbook The Rising Sea, Foundations of Agebraic Geometry[link]

[4] Dao, Hailong, et al. "Symbolic powers of ideals." Singularities and foliations. geometry, topology and applications. Springer, Cham, 2015. 387-432.[link]

[5] May, J. Peter. "Munshi's Proof of the Nullstellensatz." The American Mathematical Monthly, vol. 110, no. 2, 2003, pp. 133–40. JSTOR, https://doi.org/10.2307/3647772. Online version[link]

[6] mathoverflow.net/questions/15226/elementary-interesting-proofs-of-the-nullstellensatz
A list of proofs of the Nullstellensatz[link]

[7] Wikipedia article on Hilbert's Nullstellensatz[link]

[8] Wikipedia article on Artin-Tate lemma[link]

[9] Wikipedia article on Rabinowitsch trick[link]

[10] Wikipedia article on Symbolic powers[link]

[11] Wikipedia article on regular sequences[link]

[12] Wikipedia article on Serre's criterion[link]