SOME ALGEBRAIC DEFINITIONS AND CONSTRUCTIONS

Definition 1. A *monoid* is a set M with an element e and an associative multiplication $M \times M \longrightarrow M$ for which e is a two-sided identity element: $em = m = me$ for all $m \in M$. A *group* is a monoid in which each element m has an inverse element m^{-1}, so that $mm^{-1} = e = m^{-1}m$.

A *homomorphism $f : M \longrightarrow N$ of monoids* is a function f such that $f(mn) = f(m)f(n)$ and $f(e_M) = e_N$. A "homomorphism" of any kind of algebraic structure is a function that preserves all of the structure that goes into the definition.

When M is commutative, $mn = nm$ for all $m, n \in M$, we often write the product as $+$, the identity element as 0, and the inverse of m as $-m$. As a convention, it is convenient to say that a commutative monoid is "Abelian" when we choose to think of its product as "addition", but to use the word "commutative" when we choose to think of its product as "multiplication"; in the latter case, we write the identity element as 1.

Definition 2. The *Grothendieck construction* on an Abelian monoid is an Abelian group $G(M)$ together with a homomorphism of Abelian monoids $i : M \longrightarrow G(M)$ such that, for any Abelian group A and homomorphism of Abelian monoids $f : M \longrightarrow A$, there exists a unique homomorphism of Abelian groups $\tilde{f} : G(M) \longrightarrow A$ such that $\tilde{f} \circ i = f$.

We construct $G(M)$ explicitly by taking equivalence classes of ordered pairs (m, n) of elements of M, thought of as "$m - n$", under the equivalence relation generated by $(m, n) \simeq (m', n')$ if $m + n' = n + m'$. The "addition" on $G(M)$ is specified by passing to equivalence classes from $(m, n) + (p, q) = (m + p, n + q)$. The homomorphism i sends m to the equivalence class of $(m, 0)$, and the additive inverse $-i(m)$ is the equivalence class of $(0, m)$.

Once the construction is completed, it is usual to be sloppy and write m for $i(m)$ and $m - n$ for $i(m) - i(n)$, which is the equivalence class of (m, n), just as we do when constructing the integers from the non-negative integers. However, as we saw by example, this is an abuse of notation since i can send two elements of M to the same element of $G(M)$.

Definition 3. A *semiring* T is a set T which is both an Abelian monoid (addition $+$ and identity element 0) and a monoid (multiplication $\cdot$ and identity element 1) and that satisfies the distributive laws: $(s + s')t = st + s't$ and $s(t + t') = st + st'$. A ring is a semi-ring R which is an Abelian group under its addition. A ring or semi-ring is commutative if its multiplication is commutative.

A *homomorphism $f : S \longrightarrow T$ of semi-rings* is a function f such that $f(s+s') = f(s) + f(s')$, $f(0) = 0$ (which is implied if R is a ring), $f(ss') = f(s)f(s')$, and $f(1) = 1$; the last is not implied, but we insist that it be true: we are only interested in rings and semi-rings with unit. The kernel of f is the set elements $s \in S$ such that $f(s) = 0$. The image of f is the set of elements of the form $f(s)$ in T.

Exercise 4. If every element of a ring R satisfies $x^2 = x$, then the ring is commutative. The same is true if every element satisfies $x^4 = x$.

Definition 5. The *Grothendieck construction* on a commutative semi-ring T is a commutative ring $G(T)$ together with a homomorphism of commutative semi-rings $i : T \longrightarrow G(T)$ such that, for any commutative ring R and homomorphism of semi-rings $f : T \longrightarrow R$, there exists a unique homomorphism of rings $\tilde{f} : G(T) \longrightarrow R$ such that $\tilde{f} \circ i = f$.

We construct $G(T)$ explicitly by applying our previous construction to T regarded just as an Abelian monoid under addition. We then give $G(T)$ a multiplication by passing to equivalence classes from the rule $(m, n)(p, q) = (mp+nq, mq-np)$, checking that this is indeed well-defined. With our abuse of notation, this becomes $(m - n)(p - q) = mp + nq - mq - np$.

Example 6. Let G be a finite group. Consider finite sets S with actions by G, that is products $G \times S \longrightarrow S$ such that $g(g's) = (gg')s$ and $es = s$. For example, for $H \subset G$, the orbit set $G/H = \{kH | k \in G\}$ is a G-set with $g(kH) = (gk)H$. Let $T(G)$ be the set of equivalence classes of finite G-sets, where two finite G-sets are equivalent if there is a bijection $\alpha : S \cong S'$ that preserves the action by G, $\alpha(gs) = g\alpha(s)$. Then $T(G)$ is a commutative semi-ring with "addition" given by disjoint union of finite G-sets, $S \coprod S'$, and "multiplication" given by Cartesian product, $S \times S'$, with $g(s, s') = (gs, gs')$. The Grothendieck ring of $T(G)$ is denoted $A(G)$ and called the *Burnside ring* of G.

Exercise 7. Show that, as an Abelian group, $A(G)$ is free Abelian with basis elements the equivalence classes $[G/H]$ of orbits G/H. Letting $G = \pi_p$ be the cyclic group of prime order p, determine the multiplication table for $A(\pi_p)$.

Exercise 8. Show that there is a unique homomorphism of rings $\chi_H : A(G) \longrightarrow \mathbf{Z}$ that sends the equivalence class of a finite G-set S to the cardinality of the fixed point set $S^H = \{s | hs = s \text{ for all } h \in H\}$. We say that H' is conjugate to H if $gHg^{-1} = H'$ for some $g \in G$ and we write (H) for the conjugacy class of H. Choosing one H from each conjugacy class, we obtain a homomorphism of rings $\chi : A(G) \longrightarrow C(G)$, where $C(G)$ denotes the Cartesian product of one copy of Z for each conjugacy class (H) and χ has coordinate homomorphisms the χ_H. It is always true that χ is one-to-one. Prove this when $G = \pi_p$. Is χ surjective?

Definition 9. A commutative ring R is an *integral domain* if it has no zero divisors: $xy = 0$ implies $x = 0$ or $y = 0$. A commutative ring R is a *field* if every non-zero element x has an inverse element x^{-1}.

An element of R with an inverse is a *unit*, the set of units of R form a group under multiplication, and this group is $R - \{0\}$ if and only if R is a field. A field is an integral domain.

Exercise 10. Show that a finite integral domain is a field.

Definition 11. An *ideal* I in a commutative ring R is an Abelian subgroup under addition such that $ra \in I$ if $r \in R$ and $a \in I$. An ideal P is *prime* if $ab \in I$ implies $a \in I$ or $b \in I$. An ideal M is *maximal* if the only proper ideal of R that contains M is M itself.

Proposition 12. *R is an integral domain if and only if 0 is a prime ideal. R is a field if and only if 0 is a maximal ideal.*

For an ideal I, the quotient ring R/I is the set of equivalence classes of elements of R, where x is equivalent to y if $x - y$ is in I. It inherits an addition and multiplication from R that makes it a commutative ring such that the quotient map $R \longrightarrow R/I$ is a homomorphism of rings.

Proposition 13. *If $f : R \longrightarrow S$ is any homomorphism of rings, then its kernel is an ideal I and its image is isomorphic to R/I.*

Proposition 14. *R/I is an integral domain if and only if I is prime. R/I is a field if and only if I is maximal. A maximal ideal is prime, but not conversely.*

Exercise 15. Let $f : R \longrightarrow S$ be a homomorphism of rings and let $J \subset S$ be an ideal. Let $I = f^{-1}(J) = \{a | f(a) \in J\} \subset R$. Show that I is an ideal and that I is prime if J is prime. Show by example that I need not be maximal when J is maximal.

Exercise 16. Find all of the prime and maximal ideals of $\mathbf{Z} \times \mathbf{Z}$. Then find all of the prime and maximal ideals of $A(\pi_p)$.

Exercise 17. Let R be the ring of continuous functions from the closed interval $[0, 1]$ to the real numbers under pointwise addition and multiplication. This means that $(f + g)(t) = f(t) + g(t)$ and $(fg)(t) = f(t)g(t)$. Let M be a maximal ideal of R. Show that there is an element $t \in [0, 1]$ such that $M = \{f | f(t) = 0\}$.

Observe that the set of maximal ideals in this example has a topology, since it can be identified with the topological space $[0, 1]$. We shall come back to this idea.

Definition 18. Let R be an integral domain. The field of fractions of R is a field K together with a homomorphism of integral domains $i : R \longrightarrow K$ such that, for any homomorphism of integral domains $f : R \longrightarrow L$, where L is a field, there is a unique homomorphism of fields $\tilde{f} : K \longrightarrow L$ such that $\tilde{f} \circ i = f$.

The explicit construction is familiar: the elements of K are fractions x/y, where $x, y \in R$ and $y \neq 0$. The addition and multiplication are given by the evident formulas. The following is a special case of a more general definition.

Definition 19. Let R be a commutative ring and let $R \subset A$ where A is a ring. We say that A is an R-algebra if $ra = ar$ for $r \in R$ and $a \in A$.

Thus A is automatically an R-algebra if A is commutative. The polynomial algebra $R[x_1, \ldots, x_n]$ can be defined inductively as $R[x_1, \ldots, x_{n-1}][x_n]$. Yet again, there is a universal property here: for any commutative R-algebra A and any function $f \colon \{x_1, \ldots, x_n\} \longrightarrow A$, there is a unique homomorphism of R-algebras $\tilde{f} \colon R[x_1, \ldots, x_n] \longrightarrow A$ such the $\tilde{f} \circ i = f$. The point is that, by definition, a homomorphism of R-algebras must restrict to the identity function on R, and then $\tilde{f}$ is entirely determined by the $f(x_i)$.

Polynomials $f \in R[x_1, \ldots, x_n]$ have degrees in each variable, and a total degree. In $R[x]$, we have $\deg(fg) = \deg(f) + \deg(g)$ and $\deg(f + g) \leq \max(\deg(f), \deg(g))$. Proofs of results about polynomials often proceed by inductive arguments in which one lowers degrees of polynomials by taking appropriate linear combinations. The new proof of the Nullstellensatz carries that simple idea to extreme lengths.

Proposition 20. *If R is an integral domain, then $R[x_1, \ldots, x_n]$ is an integral domain.*

Indeed, by induction on n, it suffices to show this for $n = 1$. Here $fg = 0$ implies $\deg(fg) = 0$, and the conclusion follows.

An element p of an integral domain R is *irreducible* if it is not zero and not a unit, and if $p = ab$ implies that either a or b is a unit. This is one possible generalization of the notion of a prime number in $\mathbb{Z}$. Here is another. An element p is *prime* if the *principal ideal* $(p) = \{rp | r \in R\}$ is a prime ideal. Every prime element is irreducible (prove this), but not conversely.

Exercise 21. In the quadratic ring $\mathbf{Z}[\sqrt{-5}]$, the element 3 is irreducible but is not prime.

An integral domain is a *principal ideal domain* (PID) if every ideal I is principal. This is true of $\mathbb{Z}$ and of $F[x]$ for a field F, and in this case every irreducible element is prime: the two notions coincide. Moreover, in this case, p is irreducible if and only if (p) is not just prime but maximal: if $(p) \subset (q)$, then $p = rq$, and if p is irreducible then r must be a unit and $(p) = (q)$.

Definition 22. An integral domain R is a *unique factorization domain* (UFD) if every non-zero element a that is not a unit can be written in as a finite product of irreducibles, uniquely up to multiplication by units. That is, if $a = p_1 \cdots p_m$ and $a = q_1 \dots q_n$, then $m = n$ and, after reordering, $q_i = u_i p_i$ for a unit u_i.

Theorem 23. *Every principal ideal domain is a unique factorization domain.*

Theorem 24. *If R is a unique factorization domain, then so is $R[x]$.*

Corollary 25. *If R is a unique factorization domain, then so is $R[x_1, \dots, x_n]$.*

Of course, this would be false if UFD were replaced by PID, since x_1 would be an irreducible element such that (x_1) is not maximal.

In $\mathbf{R}[x]$, $x^2 + 1$ is irreducible, and the field $\mathbb{R}[x]/(x^2 + 1)$ is a copy of the complex numbers $\mathbb{C}$: we have adjoined $i = \sqrt{-1}$.

Theorem 26 (Fundamental theorem of algebra)**.** *Every $f \in \mathbf{C}[x]$ has a root $a \in \mathbf{C}$. Thus, if f is monic, it splits completely as a product of linear polynomials $x - a_i$.*

This means that the only maximal ideals in $\mathbf{C}[x]$ are the principal ideals $(x - a)$. A field K with the property of the conclusion is said to be *algebraically closed*. The Nullstellensatz says that this property propagates to polynomials in many variables.

Theorem 27 (Nullstellensatz)**.** *Let K be an algebraically closed field. Then an ideal M in $K[x_1, \dots, x_n]$ is maximal if and only if there are elements $a_i \in K$ such that M is the ideal generated by the elements $x_i - a_i$. That is,*

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

With $K = \mathbf{C}$, the set of maximal ideals can be identified with $\mathbf{C^n}$ and thus given a topology. Again, we shall return to this idea.

The new proof of the Nullstellensatz is a direct consequence of the following theorem, which a priori has nothing to do with algebraically closed fields.

Theorem 28 (Munshi)**.** *Let R be an integral domain with the property that the intersection of the non-zero prime ideals in R is zero. If M is a maximal ideal in $R[x_1, \dots, x_n]$, then $M \cap R \neq 0$.*

Proof of the Nullstellensatz. Let M be a maximal ideal in $K[x_1, \ldots, x_n]$, where $n \geq 2$. Regard this ring as $K[x_1][x_2, \ldots, x_n]$. The ring $K[x_1]$ satisfies the hypothesis on R in Munshi's theorem, as we show shortly, hence there is a non-zero element $f \in M \cap K[x_1]$. Since K is algebraically closed, f splits into a product of linear factors. Since f is in M, at least one of those linear factors, say $x_1 - a_1$, is in M. The same argument gives an element $x_i - a_i$ in M for each i, $1 \leq i \leq n$. Then

$$(x_1 - a_1, \ldots, x_n - a_n) \subset M.$$

Since $(x_1 - a_1, \ldots, x_n - a_n)$ is maximal, equality holds and we are done. □

We have used a special case of a result of Kaplansky, and we will also need Kaplansky's result in the proof of Munshi's theorem.

Theorem 29 (Kaplansky)**.** *Let R be an integral domain. Then the intersection I of the non-zero prime ideals in $R[x]$ is zero.*

Let K be the field of fractions of R. We need a definition and some lemmas.

Definition 30. R is of finite type if K is finitely generated as an R-algebra.

Lemma 31. *If K is generated by elements k_1, …, k_n, where $k_i = a_i/b_i$, then it is generated by the single element $c = b_1 \cdots b_n$, so that $K = R[1/c]$.*

Lemma 32. *The following conditions on a non-zero $c \in R$ are equivalent.*

(i) $c \in I$.
(ii) *Any non-zero ideal J of R contains some power of c.*
(iii) $K = R[1/c]$.

Proof. (i) $\Longrightarrow$ (ii). Assume that no power of c is in J and let P be an ideal maximal among those that contain J but do not contain any power of c. Then P is prime. Indeed if $ab \in P$ and neither a nor b is in P, then (P, a) and (P, b) each properly contain P and therefore contain some power of c, say $p + ra = c^m$ and $q + sb = c^n$ for some $p, q \in P$ and $r, s \in R$. The product of these two elements is a power of c that is in P, which is a contradiction. But then P is a prime ideal that does not contain c, contradicting (i). Therefore some power of c must be in J.
(ii) $\Longrightarrow$ (iii) For any non-zero $b \in R$, some power c^n of c is in the ideal (b), say $rb = c^n$. Then, in K, $1/b = r/c^n$. This implies (iii).
(iii) $\Longrightarrow$ (i) Let P be any non-zero prime ideal of R, let b be a non-zero element of P, and write $1/b = r/c^n$. Then $br = c^n$ is in P, hence $c \in P$. Therefore $c \in I$. □

Lemma 33. *If R is a PID, then R is of finite type if and only if it has only finitely many prime elements p_i (up to units).*

Proof. If $0 \neq c \in R$, then, up to a unit, c is a product of finitely many prime elements p_i. If $K = R[1/c]$, then these must be the only prime elements in R. □

Lemma 34. *If $R \subset S \subset K$ and R is of finite type, then S is of finite type.*

Proof. K is also the field of fractions of S. If $K = R[c^{-1}]$, then $K = S[c^{-1}]$. □

Lemma 35. *$K[x]$ has infinitely many prime ideals.*

Proof. $K[x]$ is a PID, and it has infinitely many monic irreducible polynomials, which are prime elements. Indeed, Euclid's proof that there are infinitely many prime numbers applies. if p_1, …, p_n are all of the irreducible monic polynomials and $q = 1 + p_1 \cdots p_n$, then q is a monic polynomial divisible by none of the p_i. □

Proof of Kaplansky's theorem. Suppose that $c \in I$ is non-zero. If F is the field of fractions of $R[x]$, then $R[x] \subset K[x] \subset F$ and $F = R[x][c^{-1}] = K[x][c^{-1}]$. Lemma 33 gives that $K[x]$ has finitely many prime elements, but Lemma 35 gives that $K[x]$ has infinitely many prime elements. The contradiction proves the result. □

Proof of Munshi's theorem. . We first prove the case $n = 1$, then the case $n = 2$. It will be immediately apparent that the same argument applies to prove the general case, at the price of just a little added notational complexity.

Let $n = 1$, write $x = x_1$, and assume for a contradiction that $M \cap R = 0$. Let

$$f(x) = a_0x^k + a_1x^{k-1} + \cdots + a_k$$

be a polynomial of minimal degree in M, where $a_i \in R$ and $a_k \neq 0$. Then our assumption is that $k \geq 1$. By hypothesis, there is a non-zero prime ideal P such that $a_0 \notin P$. Let $p \in P$ be non-zero. Since $p \in R$, $p \notin M$. Thus $(M, p) = R[x]$. Let $S = R - P$. For each $s \in S$, we can choose an element $g_s(x) \in R[x]$ such that $pg_s(x) + s \in M$. Since $s \notin P$, $s \notin (p)$ and $pg_s(x) + s \neq 0$. Note that $g_s(x)$ and $g_s(x) + s$ have the same degree. Here $g_s(x)$ need not be unique, and we agree to choose $g_s(x)$ to be of minimal degree among all possible choices. Since $pg_s(x) + s \in M$, its degree is at least k.

Further, we choose s_0 to be an element of S such that $g_{s_0}(x)$ has minimal degree among all $g_s(x)$. Write

$$g_{s_0}(x) = b_0x^j + b_1x^{j-1} + \cdots + b_j$$

with $b_0 \neq 0$. Then $j \geq k$. Since P is prime and both $a_0 \in S$ and $s_0 \in S$, $t = a_0s_0 \in S$. We have the element

$$a_0(pg_{s_0}(x) + s_0) - b_0px^{j-k}f(x) \in M.$$

Its degree is at most $j-1$, since the coefficient of x^j is zero. Clearly, we may rewrite this polynomial as an expression of the form

$$g_t(x) + t \in M.$$

Since $g_t(x)$ has degree at most $j - 1$, this contradicts the choice of s_0. Thus our original assumption that $k \geq 1$ is incorrect and $M \cap P \neq 0$.

Now let $n = 2$ and again assume for a contradiction that $M \cap R = 0$. Write $x = x_1$ and $y = x_2$ to simplify notation. Since Kaplansky's theorem shows that $R[x]$ and $R[y]$ satisfy the hypothesis of Munshi's theorem, the case $n = 1$ gives that $M \cap R[x] \neq 0$ and $M \cap R[y] \neq 0$. Choose polynomials $d(x) \in M \cap R[x]$ and $e(y) \in M \cap R[y]$ of minimal degrees m and n among all such polynomials.

Let N be the non-negative integers and give $N \times N$ the reverse lexicographic order: $(i, j) < (i', j')$ if $j < j'$ or if $j = j'$ and $i < i'$. Define the bidegree of a non-zero polynomial $h = \sum a_{ij}x^iy^j$ to be the maximal (i, j) such that $a_{ij} \neq 0$; we call a_{ij} the leading coefficient of h. It is convenient pictorially to think of the points of $N \times N$ as a lattice in the plane, with arrows drawn left and downwards to indicate adjacent inequalities.

The polynomials $y^jd(x)$ and $x^ie(y)$ in M have bidegrees (m, j) and (i, n), respectively. Since $M \cap R = 0$, $m > 0$ and $n > 0$, so that

$$(0, 0) < (m, 0) < (0, n).$$

Let B and ∂B denote the lower left box

$$B = \{(i, j) \mid i \leq m \text{ and } j \leq n\}$$

and its partial boundary

$$\partial B = \{(i,j) \mid i = m \text{ or } j = n\} \subset B.$$

We have an element of M of bidegree (i,j) for each $(i,j) \in \partial B$.

A *flow* F from (a_q, b_q) to $(0,0)$ is a finite sequence of adjacent lattice points

$$(0,0) < (a_1, b_1) < \cdots < (a_q, b_q),$$

so that, for $0 \leq i < q$, either

(i) $a_i = a_{i+1} - 1$ and $b_i = b_{i+1}$ or
(ii) $a_i = a_{i+1}$ and $b_i = b_{i+1} - 1$.

We say that $(a_i, b_i) \in F$ is a point on the flow F. Observe that

(iii) Any flow from a point outside B to $(0,0)$ must intersect ∂B.
(iv) Any flow from a point in B to $(0,0)$ is part of a flow from (m,n) to $(0,0)$.

Going downstream in the flow corresponds to going down in the order. Let $\mathscr{F}$ denote the (finite) set of all flows from (m,n) to $(0,0)$.

Now we mimic the proof in the case $n = 1$.

For a flow F from (m,n) to $(0,0)$, let M_F be the set of non-zero polynomials in M with bidegree on F. Then M_F is non empty since there are non-zero polynomials of bidegree (m,n) in M. Choose a polynomial $f_F \in M_F$ of minimal bidegree. Since $M \cap R = 0$, the bidegree of f_F is not $(0,0)$; let a_F be its leading coefficient. Let $a \in R$ be the product of the a_F. There is a non-zero prime ideal $P \subset R$ such that $a \notin P$. Let $p \in P$ be non-zero. Since $p \in R$, $p \notin M$. Thus $(M, p) = R[x,y]$. Let $S = R - P$. Since $a \in S$, $a_F \in S$ for all $F \in \mathscr{F}$. For each $s \in S$, we can choose an element $g_s(x,y) \in R[x,y]$ such that $pg_s(x,y) + s \in M$. Since $s \notin P$, $s \notin (p)$ and $pg_s(x) + s \neq 0$. Here $g_s(x,y)$ need not be unique, and we agree to choose $g_s(x,y)$ to be of minimal bidegree among all possible choices.

Further, we choose s_0 to be an element of S such that $g_{s_0}(x,y)$ has minimal bidegree among all $g_s(x,y)$. Let b be the leading coefficient of $g_{s_0}(x,y)$. Consider any flow from the bidegree of $g_{s_0}(x,y)$ to $(0,0)$. By (iii) and (iv), this flow must coincide with a flow F from (m,n) to $(0,0)$ from some point onwards. Clearly the bidegree of f_F lies downstream to, or coincides with, the bidegree of $g_{s_0}(x,y)$. Let (u,v) be the difference of the bidegrees of these two polynomials. Then $x^u y^v f_F$ and $pg_{s_0}(x,y) + s_0$ are elements of M of the same bidegree. Multiplying by bp and a_F, we obtain elements of M with the same leading term. Since P is prime and both $a_F \in S$ and $s_0 \in S$, $t = a_F s_0 \in S$. The element

$$a_F(pg_{s_0}(x,y) + s_0) - bpx^u y^v f_F \in M$$

can be rewritten in the form

$$pg_t(x,y) + t \in M,$$

where the bidegree of $g_t(x,y)$ is less than the bidegree of $g_{s_0}(x,y)$. This is a contradiction, hence our original assumption $M \cap R = 0$ must be false.

As said at the start, the generalization to n variables works the same way. □

The name "Nullstellensatz", or "zero place theorem", comes from the following consequence.

Corollary 36. *If I is a proper ideal of $F[x_1, \ldots, x_n]$, then there is an element $a = (a_1, \ldots, a_n) \in F^n$ such that $f(a) = 0$ for all $f \in I$.*

Proof. I must be contained in some maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$. □

The result we have called the Nullstellensatz is actually the "weak form". For completeness, and because it is the real starting point of algebraic geometry, we go on to show just how little more is required to derive the strong form. The argument is standard. We do need the Hilbert basis theorem. A commutative ring is *Noetherian* if every ideal is finitely generated. We need only consider integral domains, but the general case of the following result is no more difficult.

Theorem 37 (Hilbert basis theorem)**.** *If R is a commutative Noetherian ring, then so is $R[x]$. Therefore $R[x_1, \ldots, x_n]$ is Noetherian for all n.*

An ideal I is a *radical ideal* if $a^n \in I$ implies $a \in I$. The *radical of an ideal I*, denoted $\sqrt{I}$, is the set of all elements a some power of which is in I. It is not hard to see that it is in fact an ideal containing I.

Now focus on $F[x_1, \cdots, x_n]$ for a field F and a fixed n. Write $\mathbb{A}^n = \mathbb{A}^n[F]$ for F^n regarded just as a set, and call it *affine space*. One point is to ignore its linear structure as a vector space over F. The zeroes $\mathscr{Z}(I)$ of an ideal $I \subset F[x_1, \cdots, x_n]$ are the points $a \in \mathbb{A}^n$ such that $f(a) = 0$ for all $f \in I$. The *affine algebraic sets* are the subsets V of $\mathbb{A}^n$ that are the zeroes of a set of polynomials $\{f_i\}$. The ideal $\mathscr{I}(V)$ is then defined to be the set of all polynomials f such that $f(v) = 0$ for all $v \in V$. This is an ideal, and it is clearly a radical ideal: if $(f^n)(v) = f(v)^n = 0$, then $f(v) = 0$.

Thus an algebraic set V gives rise to a radical ideal $\mathscr{I}(V)$, and an ideal I gives rise to an algebraic set $\mathscr{Z}(I)$. Because we start with sets V that are the zeroes of a set of polynomials, it is immediate that $V = \mathscr{Z}(\mathscr{I}(V))$. On the other hand, for an ideal I, it is immediate that $I \subset \mathscr{I}(\mathscr{Z}(I))$. Equality cannot be expected in general since $\mathscr{I}(\mathscr{Z}(I))$ must be a radical ideal. However, even if we start with a radical ideal, equality need not hold. The point is that not all radical ideals are of the form $\mathscr{I}(V)$ for some V. For example, any prime ideal is a radical ideal, and the prime ideal $(x^2 + 1) \in \mathbb{R}[x]$ has no zeroes in $\mathbb{R}$. The strong form of the Nullstellensatz says that these conclusions do hold for algebraically closed fields.

Theorem 38 (Strong form of the Nullstellensatz)**.** *Let F be an algebraically closed field. Then, for any ideal $I \subset F[x_1, \cdots, x_n]$, $\mathscr{I}(\mathscr{Z}(I)) = \sqrt{I}$. Therefore the correspondences $\mathscr{Z}$ and $\mathscr{I}$ between algebraic sets and radical ideals are inverse bijections.*

Proof. We must prove that $\mathscr{I}(\mathscr{Z}(I)) \subset \sqrt{I}$. By the Hilbert basis theorem, I is generated by a finite set $\{f_1, \ldots, f_q\}$ of polynomials. Let $g \in \mathscr{I}(\mathscr{Z}(I))$. We must prove that some power of g is in I. Introduce a new variable y and let $J \subset F[x_1, \cdots, x_n, y]$ be the ideal generated by the f_i and $yg - 1$. Clearly g and the f_i depend only on the x_i, and g vanishes on any point $a \in \mathbb{A}^n$ on which each f_i vanishes. Therefore, if $a \in \mathbb{A}^{n+1}$ and $f_i(a) = 0$ for all i, then $a_{n+1}g(a) - 1 = -1$. Thus $\mathscr{Z}(J)$ is empty and J cannot be a proper ideal, so that $J = F[x_1, \cdots, x_n, y]$. We may write

$$1 = h_1 f_1 + \cdots + h_q f_q + h_{q+1}(yg - 1)$$

for some $h_i \in F[x_1, \cdots, x_n, y]$. Working in the field of fractions, say, we may set $z = y^{-1}$ and think of the h_i as polynomials in the x_i and z^{-1}, and we may think of the last summand as $z^{-1}h_{q+1}(g - z)$. Multiplying by z^N for N large enough to

clear denominators, we obtain

$$z^N = j_1 f_1 + \cdots j_q f_q + j_{q+1}(g - z)$$

for some $j_i \in F[x_1, \cdots, x_n, z]$. We may set $z = g$ in this polynomial equation, and this shows that $g^N \in I$. □

It is convenient to let radical ideals I correspond to their quotient F-algebras $F[x_1, \cdots, x_n]/I$. If $I = \mathscr{I}(V)$, this is called the *coordinate ring* of V and denoted $F[V]$. It is to be thought of as the ring of polynomial functions on V, since two polynomials f and g define the same element of $F[V]$ if and only if their restrictions to V are the same; that is their difference is identically zero on V and therefore in the ideal I. The passage back and forth between algebraic sets and their coordinate rings is an algebraization of the geometry of solutions to polynomial equations, the starting point of algebraic geometry.

The geometry has an underlying topology, and we want to understand that algebraically. Working more generally now, let R be any commutative ring. Let $\mathrm{Spec}(R)$ denote the set of all prime ideals of R. We define a topology on $\mathrm{Spec}(R)$ by letting the closed sets be the sets

$$V(I) = \{P \,|\, I \subset P\}$$

where I ranges over all ideals of R. This is called the *Zariski topology*.

To say that the set of sets $V(I)$ is a topology is to say that the empty set and the entire set are closed, and that finite unions and arbitrary intersections of closed sets are closed. The empty set is $V(R)$: no prime ideal contains R. The whole set is $V(0)$: every prime ideal contains the ideal $0 = \{0\}$. If J is the product of a finite set of ideals $\{I_q\}$, denoted $J = \prod I_q$, then J is the ideal of linear combinations of products of one element from each I_q, and a prime ideal P contains J if and only if it contains one of the I_q. This means that $V(J)$ is the union of the $V(I_q)$. If J is the sum of an arbitrary set of ideals $\{I_q\}$, denoted $J = \sum I_q$, then J is the ideal of finite R-linear combinations of elements of the I_q, and a prime ideal P contains J if and only if it contains each of the I_q. This means that $V(J)$ is the intersection of the $V(I_q)$.

Moreover, the space $\mathrm{Spec}(R)$ is compact. One way of specifying compactness is to say that if an intersection of a set of closed subsets is empty, then the intersection of some finite subset of the given set is empty. If $\{I_q\}$ is a set of ideals such that $\cap_q \mathscr{V}(I_q) = \emptyset$, then no prime ideal contains all of the I_q, so that the sum $J = \sum I_q$ must be all of R. Then we can write 1 as a finite linear combination of elements $a_r \in I_r$ for some finite subset $\{I_r\}$ of the original set. No prime ideal can contain all of the I_r, since it would then contain 1.

For an element $r \in R$, let $D(r)$ denote the set of prime ideals such that $r \notin P$. As the complement of the closed set $V((r))$, $D(r)$ is open. These open sets form a basis for the topology. For each prime ideal P, there is at least one $r \notin P$, so that $P \in D(r)$. If $P \in D(r) \cap D(s)$, then $P \in D(rs) \subset D(r) \cap D(s)$. That is, if $r \notin P$ and $s \notin P$, then $rs \notin P$, and if $rs \notin Q$, then $r \notin Q$ and $s \notin Q$.

We define $\mathrm{Max}(R) \subset \mathrm{Spec}(R)$ to be the subspace whose points are the maximal ideals of R. This is still compact, by the same proof. A basis for its topology is given by the sets $E(r) = D(r) \cap \mathrm{Max}(R)$.

Now let $R = \mathbb{C}[x_1, \cdots, x_n]$. The maximal ideals in R are in bijective correspondence with points $a = (a_1, \ldots, a_n) \in \mathbb{A}^n(\mathbb{C})$; the correspondence sends a to

$M_a = (x_1 - a_1, \ldots, x_n - a_n)$. For $f \in R$, $f \notin M_a$ means that $f(a) \neq 0$. That is, $E(f)$ is the set of points of $\mathbb{C}^n = \mathbb{A}^n(\mathbb{C})$ that do not satisfy the polynomial f. These sets are open in the standard metric topology on $\mathbb{C}^n$. Thus the latter topology is finer (has more open sets) than the Zariski topology. Said another way the identity function from $\mathbb{C}^n$ to $\mathbb{A}^n[\mathbb{C}]$ is continuous, but its inverse is not. This is strikingly illustrated by the compactness of $\mathbb{A}^n[\mathbb{C}]$ and non-compactness of $\mathbb{C}^n$.

Rather than pursue inadequately the direction of algebraic geometry, we give some idea of the information in the topology on $\mathrm{Spec}(R)$ by describing in algebraic terms what the components of $\mathrm{Spec}(R)$ mean.

A space X is connected if it is not the disjoint union of two open subsets; equivalently, it is not the disjoint union of two closed subsets. We say that x and y are in the same component of X, and we write $x \sim y$, if there is a connected subspace of X that contains both x and y. The equivalence classes of points are called the components of X. Equivalently, they are the maximal connected subsets of X. They are connected disjoint subspaces whose union is X, and any connected subset of X intersects only one of them. Components are closed, but they need not be open unless there are only finitely many of them. They must not be confused with path components, with which they coincide when X is locally path connected. That fails for Spec(R). We let πX denote the set of components of X.

An element $e \in R$ is *idempotent* if $e^2 = e$, and we say that two idempotents are orthogonal if their product is zero. If $R = R_1 \times R_2$, then $e_1 = (1, 0)$ and $e_2 = (0, 1)$ are orthogonal idempotents of R such that $e_1 + e_2 = 1$. Thus any prime ideal of R must contain e_1 or e_2, but not both. We conclude that the prime ideals of R are the ideals of the form $P_1 \times R_2$ or $R_1 \times P_2$, where P_i is a prime ideal of R_i. Moreover, these two collections of primes are each closed subsets, namely $V(R_2)$ and $V(R_1)$, where $R_1 = R_1 \times 0 \subset R$ and similarly for R_2. Therefore these two closed sets are also open, and they separate $\mathrm{Spec}(R)$ into two components. This behavior generalizes.

Proposition 39. *Let R be a commutative Noetherian ring. The decompositions of 1 as a sum $1 = e_1 + \cdots e_n$ of n non-zero orthogonal idempotents are in bijective correspondence with the decompositions of R as the direct sum of n ideals and with the decompositions of Spec(R) as disjoint unions of n open and closed subsets. Thus Spec(R) is connected if and only if 0 and 1 are the only idempotents of R.*

Proof. The ideal and component corresponding to e_i are (e_i) and $U_i = V((1 - e_i))$. Clearly $(e_i) \cap (e_j) = 0$, $U_i \cap U_j = \emptyset$ for $i \neq j$ and each prime is in one of the U_i. □

An idempotent is indecomposable if it is non-zero and is not the sum of two non-zero idempotents; the summands must be orthogonal if $2r = 0$ implies $r = 0$. The proposition is most interesting when each idempotent is indecomposable.

Now let us return to the Burnside ring $A(G)$ of a finite group G. Recall that fixed point cardinality homomorphisms give a ring homomorphism $\chi : A(G) \longrightarrow C(G)$, where $C(G)$ is the product over conjugacy classes (H) of copies of $\mathbb{Z}$. A subgroup of G is *perfect* if it is equal to its commutator subgroup. A subgroup is *solvable* if it has a composition series (each term is a maximal normal subgroup of the previous one) whose factors are cyclic of prime order. Each $H \subset G$ has a smallest normal subgroup H_s such that H/H_s is solvable; $(H_s)_s = H_s$, and H is perfect if and only if $H = H_s$. There is a composition series

$$H_s = H_k \lhd H_{k-1} \lhd \cdots \lhd H_1 = H \tag{40}$$

such that each H_j/H_{j+1} is cyclic of order p_j for some primes p_j. Thus G is solvable if and only $G_s = e$. Let $P(G)$ be the set of conjugacy classes of perfect subgroups of G. We can identify $P(G)$ with the set of equivalence classes of conjugacy classes (H), where (H) is equivalent to (H') if $(H_s) = (H'_s)$.

We shall sketch two ways to prove the following result.

Theorem 41. *The indecomposable idempotents of $A(G)$ are in bijective correspondence with the elements of $P(G)$. Therefore G is solvable if and only if the only idempotent elements of $A(G)$ are 0 and 1, that is, Spec$(A(G))$ is connected.*

Thus the Feit-Thompson theorem says that Spec$(A(G))$ is connected if G has odd order. We briefly explain the idea. We mentioned the follow result before.

Proposition 42. *The homomorphism $\chi : A(G) \longrightarrow C(G)$ is a monomorphism.*

Proof. Suppose $x \neq 0$ but $\chi(x) = 0$. Write $x = \sum a_H[G/H]$ in terms of our basis $\{[G/H]\}$. Partial order the basis elements by $[G/H] < [G/K]$ if H is subconjugate to K, which means that $gHg^{-1} \subset K$ for some $g \in G$. Let $[G/H]$ be maximal such that $a_H \neq 0$. If $K \subset G$ and $(G/K)^H$ is nonempty, then H must be subconjugate to G: $hgK = gK$ for all $h \in H$ implies $g^{-1}Hg \subset K$. When $K = H$, g must be in the normalizer NH of H in G, and we see that $(G/H)^H$ can be identified with the group $WH = NH/H$. Therefore

$$\chi_H(x) = a_H\chi(G/H) = a_H|WH| \neq 0,$$

contradicting our assumption that $\chi(x) = 0$. □

From here, there are two routes. If $e \in A(G)$ is an idempotent, then $\chi(e) \in C(G)$ is an idempotent, but we know all of the idempotents in a product of copies of $\mathbb{Z}$. So the question is: which idempotents of $C(G)$ can be in the image of χ? The answer is: precisely those idempotents $f \in C(G)$ whose coordinates $f(H)$ satisfy $f(H) = f(H_s)$. The $f(H)$ must all be 0 or 1. There are certain congruences which characterize those elements $f \in C(G)$ which are in the image of ϕ. Namely, for each $H \subset G$,

$$\sum [NH : NH \cap NK]\mu(K/H)f(K) \equiv 0 \bmod |WH|$$

where the sum runs over the H-conjugacy classes of groups $H \subset K \subset NH$ such that H is normal in K and K/H is cyclic; $\mu(K/H)$ is the number of generators of K/H. The proof is not very hard, but it does depend on some knowledge of the representation theory of finite groups. In principle, if Theorem 41 is true, then one can check it by using the congruences to prove that, for an idempotent f, f is in the image of ϕ if and only if $f(H_s) = f(H)$ for all H.

There is a trick that makes this easy, illustrates ideas, and allows us to minimize use of these horrid congruences. Suppose that H is normal in G with quotient group $G/H \cong \pi_p$, a cyclic group of order p. Then there are no groups K properly contained between H and G, so the sum has just two terms and reduces to

$$f(H) + (p-1)f(G) \equiv 0 \bmod p.$$

Equivalently, this is

$$f(H) \equiv f(G) \bmod p,$$

which is something that we can easily prove must hold. Indeed, if S is a finite G-set, then $S^G = (S^H)^{G/H}$. For a π_p-set T, it is clear that the elements of T that are not fixed by π_p break up into orbits of p elements each. Therefore $|T| - |T^{\pi_p}|$

is divisible by p. This implies the last congruence. If we know that $f(H)$ and $f(G)$ are each 0 or 1, then this forces $f(H) = f(G)$.

Now we go back to general principles. For an inclusion $i : H \subset G$, we obtain a ring homomorphism $i^*\colon A(G) \longrightarrow A(H)$ by use of the defining universal property of $A(G)$. We may regard a finite G-set S as a finite H-set i^*S, and i^* clearly sends disjoint unions to disjoint unions and Cartesian products to Cartesian products. Moreover, for $J \subset H$, $\chi_J \circ i^* = \chi_J$ since the J-fixed point set of S is the same whether S is considered as a G-set or as an H-set. That is, we can study the χ_J by restricting to $A(H)$ for any convenient subgroup H such that $J \subset H \subset G$.

Returning to our question of idempotents, to prove that $f(H_s) = f(H)$ for f in the image of χ, it suffices to show that if $H \subset K \subset G$ with H normal in K and $K/H \cong \pi_p$ for some prime p, then $f(K) \equiv f(H)$ mod$p$. But this is now clear: we may restrict down to $A(K)$ and apply our trick. Conversely, if f satisfies these equalities, then we can check directly that the congruences hold.

A more conceptual proof (which generalizes to compact Lie groups G) makes use of Proposition 39 and avoids use of the general congruences altogether. We can study the prime ideals of $A(G)$ by comparing them with the prime ideals of $C(G)$, which we understand completely. We have prime ideals

$$q(H,p) = \{x \,|\, \chi_H(x) \equiv 0 \text{ mod} p\}$$

where p is zero or a prime. These are the inverse images in $A(G)$ of prime ideals of $C(G)$ and therefore are prime ideals. Clearly $q(H,0) \subset q(H,p)$ for all non-zero p, and the ideals $q(h,p)$ for varying p are in the same component of $\mathrm{Spec}(A(G))$.

One can check that the $q(H,p)$ are all of the prime ideals of $A(G)$. However, there are redundancies. The minimal prime ideals $q(H,0)$ are distinct, in the sense that there is one for each conjugacy class (H). However, many H can give the same maximal ideal $q(H,p)$. Let us say that $H \sim_p K$ if $q(H,p) = q(K,p)$. If $H \lhd K$ and $K/H \cong \pi_p$, then $H \sim_p K$ since, for a finite K set S, $|S^H| - |S^K|$ is divisible by p. It is plausible and not hard to show that these relations and conjugacy generate the equivalence relation $\sim_p$. It can be deduced from this that $H \sim_p K$ implies $(H_s) = (K_s)$. Define

$$\beta : P(G) \longrightarrow \pi Spec(A(G))$$

by $\beta(L) = [q(L,0)]$, the component of $q(L,0)$. Define

$$\gamma : \pi Spec(A(G)) \longrightarrow P(G)$$

by $\gamma(q(H,p)) = (H_s)$. Before passing to components, one can use a slick argument to check that γ is continuous and deduce that γ is well-defined, but it is perhaps more convincing to check algebraically that if $q(H,p)$ and $q(H',p')$ are in the same component, then H_s is conjugate to H'_s. It is immediate that $\gamma\beta = \mathrm{id}$ on $P(G)$, and $\beta\gamma = \mathrm{id}$ since use of (40) and our description of $\sim_p$ imply that $q(H,p)$ and $q(H_s,0)$ are in the same component.