1 Chapter 1

1.1 Rings, Ideals, Radicals

1. Exercise 1. Show that if x is nilpotent and u is a unit, $x + u$ is a unit.

   Exercise 1 solution. Suppose $x^m = 0$. First consider $u = 1$. We have $(1 + x)(1 - x + x^2 - \cdots + (-x)^{m-1}) = 1 + (-1)^{m-1}x^m = 1$. Thus $1 + x$ is a unit. Now for arbitrary u, we have $u + x = u(1 + u^{-1}x)$, and since $u^{-1}x$ is clearly nilpotent and the unit group is closed under products, $u + x$ must be a unit as well.

2. Exercise 2. Let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Prove that

   (a) f is a unit of $A[x]$ if and only if all the coefficients but the constant term are nilpotents of A and the constant term is a unit of A.

   Exercise 2a solution. One direction is easy: if a_0 is a unit and $a_1, \dots, a_n$ are nilpotents, then $a_1x+\cdots+a_nx^n$ is in the nilradical of $A[x]$, and then the previous problem shows that $f = a_0 + (a_1x + \cdots + a_nx^n)$ is a unit.

   In the other direction, let f be a unit; suppose $fg = 1$. Looking at the constant terms, it is clear that a_0 is a unit. Now for the higher-degree terms, it is enough to show a_n is nilpotent, for if it is, then $f' = f - a_nx^n$ is a unit by Exercise 1. Then by the same argument it will be true that a_{n-1}, the lead coefficient of f', is nilpotent, and so on down the line.

   Suppose $g = b_0+b_1x+\cdots+b_mx^m$. Then $a_nb_m = 0$. Furthermore, $a_{n-1}b_m+a_nb_{m-1} = 0$; multiplying by a_n, we find $a_na_{n-1}b_m + a_n^2b_{m-1} = 0$. But the first term is zero since a_nb_m is zero. So $a_n^2b_{m-1} = 0$ too. Continuing inductively: the coefficient of the term x^k in the product is $\sum_{i+j=k} a_ib_j$ (where $i, j \geq 0$), and this is zero if $k \geq 1$ because $fg = 1$. If $k \geq n$, writing $k = m + n - r$ (so $r \leq m$), we can rewrite this sum as

   $$\sum_{i=0}^{r} a_{n-r+i}b_{m-i} = 0$$

   provided we define $a_{n-r+i} = 0$ if $n - r + i < 0$ (which will happen if $r > n$). This equation is true for all r satisfying $r \leq m$, since this implies $n + m - r \geq n > 0$. (There is nothing to prove when $n = 0$.) We have shown $a_nb_m = 0$, and we contend $a_n^rb_{m-r}$ is zero for all $r \leq m$. We prove it by induction on r, with the case $r = 0$ the one just handled. (In fact, we handled $r = 1$ as an intimation of the induction step.) Multiply the above equation by a_n^r:

   $$\sum_{i=0}^{r} a_n^r a_{n-r+i}b_{m-i} = 0$$

For all the terms with $i < r$, the induction hypothesis tells us $a^r b_{m-i} = a^{r-i-1}a^{i+1}b_{m-i} = 0$. Thus the equation simplifies to

$$a_n^r a_{n-r+r} b_{m-r} = a_n^{r+1} b_{m-r}$$

and we have proven the inductive claim. (This follows Atiyah-MacDonald's hint.)

This holds in particular when $r = m$, so $a_n^{m+1} b_0 = 0$. But b_0 is a unit, as we mentioned at the beginning; so a_n is nilpotent. This completes the argument that if f is a unit, then a_0 is a unit, and $a_1, \dots, a_n$ are nilpotent (the converse already having been established).

(b) f is nilpotent if and only if all the coefficients are nilpotent.

Exercise 2b solution. Since nilpotents form an ideal, if all the coefficients are nilpotent then they are in the nilradical of $A[x]$, and then f is in the nilradical of $A[x]$. In the other direction, suppose f is nilpotent. Let $\mathfrak{N}$ be the nilradical of A. Consider the mod $\mathfrak{N}$ reduction of f, in the ring $A/\mathfrak{N}[x]$. Now $A/\mathfrak{N}$ has no nilpotents. Thus if $f \mod \mathfrak{N}$ is nonzero, then by considering its leading term, no power of $f \mod \mathfrak{N}$ is zero in $A/\mathfrak{N}[x]$. In particular, f is not nilpotent. It follows that since f is nilpotent by assumption, $f \mod \mathfrak{N}$ is zero. But then all of f's coefficients are in $\mathfrak{N}$, i.e. nilpotent.

(c) f is a zero-divisor if and only if f is annihilated by a nonzero element of A.

Exercise 2c solution. Certainly if $af = 0, a \in A$, then f is a zero-divisor, by definition. In the other direction, suppose $gf = 0$, $g \in A[x]$. Suppose $f = a_0 + a_1 x + \dots + a_n x^n$ and $g = b_0 + b_1 x + \dots + b_m x^m$. Let g be chosen to have minimal degree among polynomials that annihilate f. Our basic goal is to show that g is degree zero. Now $a_n b_m = 0$ by considering the leading term of the product fg. Therefore $a_n g$ has lower degree than g. It obviously annihilates f since g does. By the minimality of g, then, $a_n g = 0$. In particular, $a_n b_k = 0$, $\forall 0 \leq k \leq m$. Thus since $a_{n-1}b_m + a_n b_{m-1} = 0$ we can deduce that $a_{n-1}b_m = 0$ as well. Then again $a_{n-1}g$ has lower degree than g and annihilates f, so is zero, so a_{n-1} annihilates g. Continuing in like manner, by induction we find that $a_k g = 0$, $\forall 0 \leq k \leq n$. This tells us that the coefficients from f all annihilate g; thus they annihilate its coefficients term-by-term. *Any* coefficient from g therefore annihilates f. It follows by the minimality assumption on g that actually it only has a constant term (otherwise its coefficients would violate its own minimality).

(d) f is *primitive* if its coefficients generate the unit ideal. Prove that a product is primitive if and only if its coefficients are primitive.

(Note: if the ring A is a unique factorization domain, the word "primitive" has a slightly different meaning: in that context it means the coefficients do not have a nonunit common factor. The two meanings coincide if the ring is a principal ideal domain.)

Exercise 2d solution. One direction is trivial: if either f or g is not primitive, its coefficients are contained in some maximal ideal $\mathfrak{m} \triangleleft A$, and then so are the coefficients of fg. Thus if fg is primitive then so are f and g. In the other direction, suppose fg is not primitive; let $\mathfrak{m}$ be a maximal ideal of A containing its coefficients. Let $\bar{f}, \bar{g}$ be the residues of f, g in $(A/\mathfrak{m})[x]$. If f, g were primitive, $\bar{f}, \bar{g}$ would both be nonzero; but this is a contradiction, because $\bar{f}\bar{g} = 0$ by construction, and $A/\mathfrak{m}$ is a field since $\mathfrak{m}$ is maximal, so $(A/\mathfrak{m})[x]$ is an integral domain. So at least one of f, g is not primitive. We deduce that if f, g are individually primitive, so is fg.

3. Exercise 4. Show that in $A[x]$, the Jacobson radical and nilradical are equal.

   Exercise 4 solution. Since the nilradical is always contained in the Jacobson radical, we just need to show that it is the whole thing, i.e. that any element of $A[x]$ that fails to be nilpotent also fails to be in the Jacobson radical.

   From exercise 2b we know that if $f \in A[x]$ is not nilpotent, it has some coefficient that's not nilpotent. Then xf has a nonconstant coefficient that is not nilpotent. From exercise 2a we know this means $1 + xf$ is not a unit. By Proposition 1.9 of Atiyah-MacDonald, this means that f is not in the Jacobson radical.

4. Exercise 6. A ring A has the property that every ideal not in the nilradical contains a nonzero idempotent (i.e. an element x such that $x^2 = x$). Prove that the nilradical and Jacobson radical of A coincide.

   Exercise 6 solution. Again, the task is to prove that anything non-nilpotent is not in the Jacobson radical.

   Suppose x is not nilpotent. Then the principal ideal generated by x is not contained in the nilradical, so by the assumption about A it contains a nonzero idempotent, i.e. there exists y such that xy is a nonzero idempotent. Then I claim $1 - xy$ is not a unit. Indeed, it is an idempotent. (In general, if e is an idempotent, then $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$, so $1 - e$ is an idempotent as well.) It is not 1 because xy is not zero. An idempotent not equal to 1 can never be a unit: if $e^2 = e$ and e is a unit, cancellation gives $e = 1$. Thus $1 - xy$ is not a unit, and Proposition 1.9 again shows that x is not in the Jacobson radical.

5. Exercise 7. Let A be a ring in which all $x \in A$ satisfy $x^n = x$ for some $n > 1$ (depending on x). Show that every prime ideal of A is maximal.

Exercise 7 solution. Let $\mathfrak{p}$ be a prime ideal of A. Then $A/\mathfrak{p}$ is a domain in which all x satisfy $x^n = x$ for some $n > 1$; i.e. $x(x^{n-1} - 1) = 0$. Since it is a domain, if x is nonzero this means x satisfies $x^{n-1} - 1 = 0$, so that x^{n-2} is a multiplicative inverse for x. (Since $n \geq 2$, this is defined.) This means that $A/\mathfrak{p}$ is a field, so $\mathfrak{p}$ is maximal.

6. Exercise 8. Let A be a nonzero ring. Show that the set of all prime ideals has elements that are minimal with respect to inclusion.

   Exercise 8 solution. First note that a decreasing family of prime ideals $\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \dots$ has prime intersection. Proof: let $ab \in \bigcap \mathfrak{p}_i$. Suppose $a \notin \bigcap \mathfrak{p}_i$. Then there is some $\mathfrak{p}_{i^*}$ that a is not in. For all $j > i^*$, this implies (by the containments) that $a \notin \mathfrak{p}_j$. But then (by primality) $b \in \mathfrak{p}_j$, $\forall j > i^*$, and this implies (again by the containments) that $b \in \mathfrak{p}_j, \forall j$; thus $b \in \bigcap \mathfrak{p}_i$, so the latter is prime.

   Order the set of prime ideals by reverse inclusion. We have just shown that every chain has an upper bound on this order. Since there is at least one prime ideal (take any maximal ideal), the set of prime ideals is nonempty, and Zorn's lemma applies. The maximal elements are the minimal prime ideals.

7. Exercise 10. Let A be a ring, $\mathfrak{N}$ its nilradical. Show the following are equivalent: (i) A has just one prime ideal; (ii) every element of A is either a unit or nilpotent; (iii) $A/\mathfrak{N}$ is a field.

   Exercise 10 solution.

   (i)$\Rightarrow$(iii). Suppose A has just one prime ideal $\mathfrak{p}$. Then $\mathfrak{N}$, since it is the intersection of the prime ideals, $= \mathfrak{p}$. $\mathfrak{N}$ is contained in some maximal ideal $\mathfrak{m}$, which is also prime, thus $\mathfrak{N} = \mathfrak{m}$ as well, and $A/\mathfrak{N} = A/\mathfrak{m}$ is a field.

   (iii)$\Rightarrow$(ii). If $A/\mathfrak{N}$ is a field, then for every element $x \notin \mathfrak{N}$ (i.e. every x not nilpotent), there is a y such that $\bar{x}\bar{y} = 1$ in $A/\mathfrak{N}$; i.e. $xy = 1 + z$ for some $z \in \mathfrak{N}$. By Exercise 1, $1 + z$ is a unit. Then clearly x is a unit. Thus everything that is not nilpotent is a unit.

   (ii)$\Rightarrow$(i). On the assumption that everything in A that is not nilpotent is a unit, we immediately get that $\mathfrak{N}$ is maximal and is therefore prime. Since it is also the intersection of all prime ideals, it is beneath every other prime ideal in the lattice of prime ideals, ordered by inclusion; but since it is a maximal ideal it is also maximal in this lattice. This can only happen if the lattice contains a unique prime ideal $\mathfrak{N}$. We are done.

8. Exercise 11. A ring A is *boolean* if $\forall x \in A$, $x^2 = x$. In a boolean ring, show that

   (a) $2x = 0$.

   Exercise 11a solution. We have $(x+x)^2 = x + x$ but also $(x+x)^2 = x^2 + 2x^2 + x^2 =$

$x+2x+x$. So $x+2x+x = x+x$, and $2x = 0$. (More succintly, $4x = 4x^2 = (2x)^2 = 2x$, so $2x = 0$.)

(b) Every prime ideal $\mathfrak{p}$ is maximal, and $A/\mathfrak{p} = \mathbb{F}_2$.

Exercise 11b solution. The first claim follows from the second. Let $\mathfrak{p}$ be a prime ideal. Then $A/\mathfrak{p}$ is a domain, in which $x^2 = x$ still obtains, for all x in the domain. Now being a domain, $A/\mathfrak{p}$ is embedded in a field, which means the polynomial $x^2 - x$ can't have more than two roots. Since every element of $A/\mathfrak{p}$ is a root of this equation, actually it has at most two elements. Since a prime ideal is proper, it has at least two. Thus it has exactly two, and is $\mathbb{F}_2$. We are done.

(c) Every finitely generated ideal in A is principal.

Exercise 11c solution. Consider a finitely generated ideal $(x_1, \dots, x_m)$. I claim this ideal is generated by the single element $1 - (1 - x_1) \dots (1 - x_m)$.

To prove this, I need to show that any linear combination of $x_1, \dots, x_m$ is actually a multiple of $1 - (1 - x_1) \dots (1 - x_m)$. Consider

$$\sum_{i=1}^{m} a_i x_i$$

where each $a_i \in A$. Then consider

$$\left(\sum_{i=1}^{m} a_i x_i\right)(1 - (1 - x_1) \dots (1 - x_m))$$

The result of this multiplication is

$$\sum_{i=1}^{m} a_i x_i - \sum_{i=1}^{m} a_i x_i (1 - x_i) \prod_{j \neq i} (1 - x_j)$$

But $x_i(1 - x_i) = x_i - x_i^2 = 0$, so all the summands under the second sum vanish. Letting $\chi = \sum_{i=1}^{m} a_i x_i$ be an arbitrary linear combination of the x_i's (i.e. an arbitrary element of $(x_1, \dots, x_m)$), and $\nu = 1 - (1 - x_1) \dots (1 - x_m)$, we have just shown that $\chi\nu = \chi$. So anything in $(x_1, \dots, x_m)$ is actually in (ν). The reverse inclusion is clear since $\nu \in (x_1, \dots, x_m)$. Thus $(x_1, \dots, x_m) = (\nu)$.

9. Exercise 12. Prove that a local ring contains no idempotent $\neq 0, 1$.

Exercise 12 solution. In a local ring, there is a unique maximal ideal $\mathfrak{m}$ and everything outside of it is a unit. (If anything outside it were not a unit, it would be contained in a different maximal ideal, but there's only one.) No unit not equal to 1 can be idempotent, as we showed in Exercise 6; so we cannot find an idempotent $\neq 1$ outside

$\mathfrak{m}$. It remains to show that there is not a an idempotent $\neq 0$ inside $\mathfrak{m}$. So suppose $x^2 = x$ and $x \in \mathfrak{m}$. Then $x - x^2 = x(1-x) = 0$. I claim $1-x$ is a unit. If not, then $1-x \in \mathfrak{m}$, but then $1 = x + (1-x) \in \mathfrak{m}$, absurd. But if $1-x$ is a unit, then $x(1-x) = 0$ implies (by cancellation of the unit) that $x = 0$. We are done.

1.2 Prime Spectrum

This and the next section set up fundamental tools of algebraic geometry. We gain insight into the geometric objects under study (curves, surfaces, etc.) by looking at the ring of polynomial functions on those objects. We also reverse the process and start with a ring and construct an underlying geometric object of which it can be seen as the "ring of functions." This underlying geometric object is called its *prime spectrum*. The following exercises define the prime spectrum. See the comments below on exercise 16c, and also exercises 26-28, for more context. Also, Exercises 23-24 in Chapter 3 are aimed at fleshing out the way in which it makes sense to think about the ring elements as "functions" on the prime spectrum.

1. Exercise 15. Let A be a ring and let $X = \operatorname{Spec} A$ be the set of prime ideals of A. For arbitrary $E \subset A$, define $V(E)$ to be the set of all prime ideals containing E. Check that

   (a) If $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$.

   Exercise 15a solution. Any ideal containing E also contains $\mathfrak{a}$ by definition of the latter, so $V(E) = V(\mathfrak{a})$. $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$ because $\sqrt{\mathfrak{a}}$ is precisely the intersection of the prime ideals containing $\mathfrak{a}$, so any prime ideal containing $\mathfrak{a}$ contains $\sqrt{\mathfrak{a}}$.

   (b) $V(0) = X$ and $V(1) = \varnothing$.

   Exercise 15b solution. Every prime ideal contains 0, so $V(0) = X$, and no prime ideal can contain 1, so $V(1) = \varnothing$.

   (c) If $(E_i)_{i \in I}$ is a family of subsets of A, then

   $$V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i)$$

   Exercise 15c solution. The left side is the set of prime ideals containing the union of the E_i's, while the left side is the set of prime ideals that contain E_i for each $i \in I$.

   (d) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

Exercise 15d solution. Let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{ab}$. I aim to show it contains either all of $\mathfrak{a}$ or all of $\mathfrak{b}$. This will show that $V(\mathfrak{ab}) \subset V(\mathfrak{a}) \cup V(\mathfrak{b})$. Since $V(\mathfrak{ab}) \supset V(\mathfrak{a} \cap \mathfrak{b}) \supset V(\mathfrak{a}) \cup V(\mathfrak{b})$ trivially, this will complete the problem.

Suppose $\mathfrak{p}$ contains the product $\mathfrak{ab}$, and suppose there is some $a \in \mathfrak{a}$ that $\mathfrak{p}$ does not contain. For *all* $b \in \mathfrak{b}$, $ab \in \mathfrak{ab} \subset \mathfrak{p}$, and by primality of $\mathfrak{p}$ this means $b \in \mathfrak{p}$ $\forall b \in \mathfrak{b}$, i.e. $\mathfrak{b} \subset \mathfrak{p}$.

These results show that sets of the form $V(E)$ are closed under arbitrary intersection and finite union and contain $X, \varnothing$; thus they obey the axioms for the closed sets of a topology; it is called the Zariski topology on $X = \operatorname{Spec} A$.

2. Exercise 16. Describe $\operatorname{Spec} A$ for $A =$

(a) $\mathbb{Z}$.

Exercise 16a solution. Because $\mathbb{Z}$ is a principal ideal domain, the nonzero prime ideals are exactly the ideals generated by irreducible elements; i.e. $\operatorname{Spec} A$ is the set of ideals generated by integer primes, and zero. The proper closed subsets of $\operatorname{Spec} A$ are the finite sets of integer primes, since for any element of $\mathbb{Z}$, there are only finitely many prime ideals containing it (namely those generated by the primes that divide it); thus $V(E)$ is finite for a singleton E; and making E bigger can only make $V(E)$ smaller.

(b) $\mathbb{R}$.

Exercise 16b solution. This is a field, so zero is the only prime ideal.

(c) $\mathbb{C}[x]$.

Exercise 16c solution. Like $\mathbb{Z}$, $\mathbb{C}[x]$ is a principal ideal domain. Therefore all the nonzero prime ideals are generated by irreducible elements. Since $\mathbb{C}$ is algebraically closed, the irreducible elements have the form $x - \alpha$ for $\alpha \in \mathbb{C}$. Therefore the prime ideals are $(x - \alpha)$ for $\alpha \in \mathbb{C}$, and zero. The closed sets are finite collections of the nonzero primes, just as in the case of $\mathbb{Z}$ and for the same reason.

Aside: this is a key motivating example in algebraic geometry. Because the nonzero primes of $\mathbb{C}[x]$ correspond bijectively with the elements of $\mathbb{C}$, we see $\operatorname{Spec} \mathbb{C}[x]$, the topological space, as basically "being" the complex plane. (Although in AG we tend to think of it as a "line" because it is one-dimensional over the base field $\mathbb{C}$.) The zero ideal is included for technical reasons we will get into later; we think of it as representing a "generic point" of the complex plane. The elements of $\mathbb{C}[x]$ are naturally interpreted as functions on $\mathbb{C}$; thus in this case, the elements of the ring are naturally thought of as functions on the prime spectrum of the ring. We will take this as a cue and, even where it is a less natural interpretation, we will tend to think of elements of a ring as "functions" on the ring's prime spectrum.

(d) $\mathbb{R}[x]$.

Exercise 16d solution. Now we additionally have maximal ideals generated by quadratic polynomials of the form $(x-\beta)(x-\bar{\beta})$ for $\beta \in \mathbb{C} \smallsetminus \mathbb{R}$. Again, all nonzero primes are maximal, because the ring is a principal ideal domain. (In a p.i.d., suppose that $\mathfrak{p} = (p)$ is a prime ideal, and $a \notin (p)$, $(a)+(p) = (b)$. Then $b \mid p$ and $b \mid a$, so $bc = p$ for some c. Because (p) is prime, b or c is a unit. If c is a unit, $b \mid a$ implies $p \mid a$. So if $p \nmid a$, i.e. $a \notin (p)$, then it must be b that is a unit. This is to say, (p) is maximal.) Closed sets are thus finite collections of real points and pairs of complex conjugate points.

(e) $\mathbb{Z}[x]$.

Exercise 16e solution. Aside: I found it necessary, in proving the classification below of the prime ideals of $\mathbb{Z}[x]$, to refer to Gauss' Lemma, which is not discussed in Atiyah-MacDonald. It is covered in any standard introductory text on abstract algebra such as Artin, *Algebra*.

The prime ideals are (p) for $p \in \mathbb{Z}$ prime; $(f) \in \mathbb{Z}[x]$ primitive and irreducible over $\mathbb{Q}$; and (p, f) for f such that its mod p reduction is irreducible over $\mathbb{F}_p$. All the prime ideals have this form. Proof:

Let $\mathfrak{p} \lhd \mathbb{Z}[x]$ be a nonzero prime ideal. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$; either it is 0 or else generated by p for some prime p in $\mathbb{Z}$.

Case 1: It is 0. Then let f be a nonconstant polynomial in $\mathfrak{p}$ of minimal degree. If f is not primitive (in the sense that its coefficients have a nontrivial common factor), then $f = af'$ with $a \in \mathbb{Z}$ and f' primitive; since $\mathfrak{p}$ is prime and $a \notin \mathfrak{p}$ (since $\mathfrak{p} \cap \mathbb{Z} = 0$), this means $f' \in \mathfrak{p}$; thus we may take f to be primitive. If f is not irreducible over $\mathbb{Q}$ then it is not irreducible over $\mathbb{Z}$ by Gauss' lemma, and then a factorization $f = gh$ into nonconstant factors, together with an application of $\mathfrak{p}$'s primeness, contradicts f's degree minimality. Thus f is irreducible over $\mathbb{Q}$. I claim that in this case, $\mathfrak{p} = (f)$. Indeed, if $g \in \mathfrak{p}$, then divide g by f in $\mathbb{Q}[x]$, obtaining an equation $g = qf + r$, with $q, r \in \mathbb{Q}[x]$ and $\deg r < \deg f$. Then clear denominators, to yield $mg = mqf + mr$, with $m \in \mathbb{Z}$ and $mq, mr \in \mathbb{Z}[x]$. But then $mr = mg - mqf$ is in $\mathfrak{p}$, and we conclude since f was of minimal degree in $\mathfrak{p}$ among nonzero polynomials, and $\deg mr = \deg r < \deg f$, that $mr = 0$. But then $r = 0$, so f divides g in $\mathbb{Q}[x]$; and by Gauss' Lemma, this implies f divides g in $\mathbb{Z}[x]$. Thus $\mathfrak{p} = (f)$.

Case 2: It is (p) for some prime $p \in \mathbb{Z}$. Then $\mathfrak{p}$ is the pullback (i.e. contraction, in Atiyah-MacDonald's language) of a prime ideal of $\mathbb{Z}[x]/(p) = \mathbb{F}_p[x]$ under the canonical homomorphism. Since $\mathbb{F}_p[x]$ is a univariate polynomial ring over a field, as in Exercises 16c and 16d, its prime ideals are the zero ideal and the ideals generated by irreducible polynomials. In the former case, the inverse image in $\mathbb{Z}[x]$ is (p), while in the latter, it is (p, f) where f is some polynomial whose mod p reduction is irreducible over $\mathbb{F}_p$.

This completes the classification of prime ideals of $\mathbb{Z}[x]$; thus the description of $\operatorname{Spec}\mathbb{Z}[x]$.

What are the closed sets? Finite collections of these, with the restriction that if a given prime ideal is in a closed set, then every ideal containing it is as well, e.g. if (f) is in $V(E)$, then so is (f,p) for all p.

3. Exercise 17. If $f \in A$, let X_f be the complement of $V(f)$ in $X = \operatorname{Spec} A$. (In the geometric picture based on $A = k[x_1, \dots, x_n]$, X_f is the complement of a hypersurface...) Prove the following:

   (a) The X_f form a basis for the Zariski topology.

   Exercise 17a solution. We have to show that every open set is a union of these; i.e. that every closed set is an intersection of $V(f)$'s. This is clear from Exercise 15c. Any $E \subset A$ is a union of singletons $\{f\}_{f\in E}$; so $V(E) = \bigcap_{f\in E} V(f)$.

   (b) $X_f \cap X_g = X_{fg}$.

   Exercise 17b solution. The left side is the set of prime ideals not containing f and not containing g, i.e. containing neither f nor g. If a prime ideal fails to contain both f and g, it can't contain fg, by its primality. Thus $X_f \cap X_g \subset X_{fg}$. In the other direction, if it doesn't contain fg then it certainly can't contain either f or g, just by idealhood, so $X_f \cap X_g \supset X_{fg}$.

   (c) $X_f = \varnothing \Leftrightarrow f$ is nilpotent.

   Exercise 17c solution. This is another statement of the fact that the nilradical is the intersection of the prime ideals. $X_f = \varnothing$ means all prime ideals contain f; therefore it is in the nilradical. In the other direction, if f is in the nilradical then all prime ideals contain it, so $X_f = \varnothing$.

   (d) $X_f = X \Leftrightarrow f$ is a unit.

   Exercise 17d solution. The claim to be proven is equivalent to the statement that the units of A are exactly the elements not contained in any prime ideal. This is because any proper ideal is in some maximal ideal, which is prime. So while obviously a unit is not in any prime ideal, also anything not in a prime ideal must have the principal ideal it generates be everything, thus it is a unit.

   (e) $X_f = X_g$ if and only if (f) and (g) have the same radical.

Exercise 17e solution. $X_f = X_g$ if and only if $V(f) = V(g)$. Now $V(f) = V(\sqrt{(f)})$ and $V(g) = V(\sqrt{(g)})$ by Exercise 15a. Therefore if (f) and (g) have the same radical, $X_f = X_g$. Conversely, if $X_f = X_g$ then f and g are contained in the same prime ideals. But the radical of (f) is exactly the intersection of the prime ideals containing f, and similarly for (g), so this condition implies $\sqrt{(f)} = \sqrt{(g)}$.

(f) X is quasicompact. (Aside: in algebraic geometry, the word "compact", meaning, as usual, that every open cover has a finite subcover, tends to be replaced with the word "quasicompact", because this property is possessed by most of the spaces under study, even if they are not what we are used to thinking of as compact. Fore example, $\operatorname{Spec} \mathbb{C}[x]$, the algebraic-geometric model of the topological space $\mathbb{C}$, is quasicompact, even though it is not compact in the Euclidean topology. There are other more advanced concepts that do a better job of substituting for the usual notion of compactness.)

Exercise 17f solution. Open sets of X are unions of X_f's. Thus an open covering is a union of X_f's. If there is a finite subcover of X_f's then there is also a finite subcover of the original cover, consisting of the original open sets containing the selected X_f's. So it is sufficient to show that if a family $\{X_f\}_{f\in E}$ covers X, a finite subfamily does too.

To say that $\{X_f\}_{f\in E}$ covers X is to say that $\bigcap_{f\in E} V(f) = \varnothing$. I.e. there is no prime ideal of A containing all the f's in E. Let $\mathfrak{a}$ be the ideal generated by all the f's in E. Since it is not contained in a prime ideal it must be (1). Then there is an equation

$$1 = \sum_{i=1}^{m} a_i f_i$$

occurring in A. The finite set $\{f_i\}_1^m$ already generates (1), so it is not contained in any prime ideal; so the X_{f_i} cover X.

(g) More generally, each X_f is quasicompact.

Exercise 17g solution. Suppose we have a family of X_g covering X_f. This means that the $V(g)$s' intersection lies inside $V(f)$. I.e. that every prime ideal containing all the g's also contains f. Then f is in every prime ideal containing the ideal generated by the g's; in other words, it is in the radical of the ideal generated by the g's. Then some power of f is in this ideal, so a finite number of g's generate a power of f. The intersection of the corresponding $V(g)$'s is the set of prime ideals containing each of the g's, and since any of these prime ideals therefore contains the generated power of f, since they are prime they all contain f and so are in $V(f)$. Then the associated X_g's cover X_f.

(h) An open subset of X is quasicompact if and only if it is a finite union of X_f's.

Exercise 17h solution. If it is open, it is a union of X_f's, as we showed in (a), so if it is not a finite union, then clearly it is not compact: the X_f's of which it is a union form an open cover with no finite subcover. Conversely, if it *is* a finite union, we use our above result, and the following basic lemma: a finite union of quasicompact sets is quasicompact. Proof: let $X_1, \dots, X_m$ be quasicompact subsets of X. An open cover for $\bigcup_{i=1}^m X_i$ is individually an open cover for each X_i, which has a finite subcover, and they can be amalgamated to give an open cover for the union.

4. Exercise 18. Let $x \in \operatorname{Spec} A$ be a point of $\operatorname{Spec} A$ the topological space, and let $\mathfrak{p}_x$ be the same element of $\operatorname{Spec} A$ except stressing that it is a prime ideal of A.

(a) Show $\{x\} \subset \operatorname{Spec} A$ is closed if and only if $\mathfrak{p}_x$ is maximal.

Exercise 18a solution. If a closed set contains a given prime ideal, it must also contain every prime ideal containing this one; in particular, every maximal ideal containing it. So if $\mathfrak{p}_x$ is not maximal, then any closed set containing x must also contain any $\mathfrak{m} \supset \mathfrak{p}_x$.

(b) Show the closure of $\{x\}$ is $V(\mathfrak{p}_x)$.

Exercise 18b solution. This is basically just the definition, plus the observation in the solution of Exercise 18a. $V(\mathfrak{p}_x)$ contains $\{x\}$ and the points corresponding to the prime ideals containing $\mathfrak{p}_x$. We observed in the solution of Exercise 18a that any closed set containing $\{x\}$ must contain all of these points. Thus $V(\mathfrak{p}_x)$ is a closed set containing $\{x\}$ and contained in any closed set containing $\{x\}$. I.e. it is the closure of $\{x\}$.

(c) $y \in \overline{\{x\}} \Leftrightarrow \mathfrak{p}_y \supset \mathfrak{p}_x$.

Exercise 18c solution. This is the same observation. y is in x's closure means that $\mathfrak{p}_y$ lies above $\mathfrak{p}_x$, so it is forced into any closed set containing x.

(d) X is a T_0 space, i.e. any two points are separated by an open set containing one and not the other.

Exercise 18d solution. Equivalently, there is a closed set containing one and not the other. (Take its complement to find the desired open set.) If $x \neq y$ and $\mathfrak{p}_y$ does not contain $\mathfrak{p}_x$, then $V(\mathfrak{p}_x)$ is the desired closed set: $\mathfrak{p}_y$ is not among the prime ideals containing $\mathfrak{p}_x$ literally means $y \notin V(\mathfrak{p}_x)$. If $\mathfrak{p}_y$ *does* contain $\mathfrak{p}_x$, switch x and y to find what we seek.

5. Exercise 21. Let $\phi : A \to B$ be a ring homomorphism. Let $X = \operatorname{Spec} A, Y = \operatorname{Spec} B$. If $\mathfrak{q} \in Y$, then $\phi^{-1}(\mathfrak{q})$ is a prime ideal of A, i.e. a point of X. So ϕ induces a mapping

$\phi^*: Y \to X$. (This map is called the *pullback* of ϕ.) Show that

(a) If $f \in A$ then $\phi^{*-1}(X_f) = Y_{\phi(f)}$, and thus that ϕ^* is continuous.

Exercise 21a solution. What is $\phi^{*-1}(X_f)$? X_f is every prime ideal of A not containing f. So $\phi^{*-1}(X_f)$ is the set of prime ideals $\mathfrak{q}$ of B such that $\phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q})$ does not contain f. But $\phi^{-1}(\mathfrak{q})$ doesn't contain f if and only if $\mathfrak{q}$ doesn't contain $\phi(f)$. So $\phi^{*-1}(X_f)$ is the set of prime ideals $\mathfrak{q}$ of B that fail to contain $\phi(f)$. This is $Y_{\phi(f)}$.

It follows that ϕ^* is continuous because we have just shown that the inverse image of a basic open set is open.

(b) If $\mathfrak{a}$ is an ideal of A, then $\phi^{*-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$.

Exercise 21b solution. What is $\phi^{*-1}(V(\mathfrak{a}))$? This is the set of all prime ideals of B (i.e. elements of Y) such that when they are pulled back along ϕ to A, they contain $\mathfrak{a}$. Thus they have to contain $\mathfrak{a}$'s image under ϕ, and this means they have to contain the smallest ideal containing $\phi(\mathfrak{a})$, which is $\mathfrak{a}^e$. Conversely, anything that contains $\mathfrak{a}^e$ pulls back to something containing $\mathfrak{a}$, so it is in $\phi^{*-1}(V(\mathfrak{a}))$. Thus $\phi^{*-1}(V(\mathfrak{a}))$ is equal to the set of prime ideals of B containing $\mathfrak{a}^e$, which is $V(\mathfrak{a})^e$.

(c) If $\mathfrak{b} \lhd B$, then $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{b}^c)$.

Exercise 21c solution. $\phi^*(V(\mathfrak{b}))$ is the set of preimages of the prime ideals of B containing $\mathfrak{b}$. Every such preimage contains $\mathfrak{b}^c$. Thus it is a subset of $V(\mathfrak{b}^c)$; this is a closed set containing it. Therefore $V(\mathfrak{b}^c) \supset \overline{\phi^*(V(\mathfrak{b}))}$. We still need to show that $V(\mathfrak{b}^c)$ is the *smallest* closed set containing $\phi^*(V(\mathfrak{b}))$; i.e. that any closed set containing $\phi^*(V(\mathfrak{b}))$ contains $V(\mathfrak{b}^c)$.

All closed sets have the form $V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of A. Since, as a generality, the intersection of the prime ideals containing $\mathfrak{a}$ is $\sqrt{\mathfrak{a}}$ (Proposition 1.14), $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$, and $V(\mathfrak{a})$ contains $V(\mathfrak{b}^c)$ if and only if $\sqrt{a} \subset \sqrt{\mathfrak{b}^c}$. Thus we must show that if $V(\mathfrak{a})$ contains $\phi^*(V(\mathfrak{b}))$, then $\sqrt{a} \subset \sqrt{\mathfrak{b}^c}$.

If $V(\mathfrak{a})$ contains $\phi^*(V(\mathfrak{b}))$, then each preimage of each prime ideal containing $\mathfrak{b}$ contains $\mathfrak{a}$. Thus their intersection does as well. Because intersections commute with contractions, $\bigcap_{\mathfrak{p}\supset\mathfrak{b}} \mathfrak{p}^c = \left(\bigcap_{\mathfrak{p}\supset\mathfrak{b}} \mathfrak{p}\right)^c = \left(\sqrt{b}\right)^c$, so we have just shown that $\mathfrak{a} \subset \left(\sqrt{\mathfrak{b}}\right)^c$. It is straightforward to check that radicals commute with contractions, so we have $\mathfrak{a} \subset \sqrt{\mathfrak{b}^c}$. Taking radicals on both sides completes the proof that $\sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{b}^c}$, establishing what was needed.

(d) If ϕ is surjective, then ϕ^* is a homeomorphism of Y onto the closed subset $V(\ker\phi)$ of X. (In particular, $\operatorname{Spec} A$ and $\operatorname{Spec} A/\mathfrak{N}$ are naturally homeomorphic.)

Exercise 21d solution. If ϕ is surjective, then ϕ^* is a one-to-one correspondence of prime ideals of A containing $\ker\phi$ (i.e. of $V(\ker\phi)$) with prime ideals of B, by the correspondence theorem. This correspondence respects both primeness and all ideal containments, so it preserves the definition of closed sets and is thus a homeomorphism.

Since all prime ideals of A contain $\mathfrak{N}$, $V(\mathfrak{N}) = \operatorname{Spec} A$, so this is a homeomorphism of $\operatorname{Spec} A$ to $\operatorname{Spec} A/\mathfrak{N}$, where ϕ is the canonical homeomorphism.

(e) If ϕ is injective, then $\phi^*(Y)$ is dense in X. More generally, $\phi^*(Y)$ is dense in $X \Leftrightarrow \ker\phi \subset \mathfrak{N}$.

Exercise 21e solution. We aim at the more general result. Let $\phi : A \to B$ be a ring homomorphism such that $\mathfrak{N} \supset \ker\phi$. Let V be a closed subset of $X = \operatorname{Spec} A$, and let $Y = \operatorname{Spec} B$. I aim to show that if V is proper, it doesn't contain $\phi^*(Y)$, implying that $\phi^*(Y)$ is dense in X. Let V be a proper closed subset of X. It has the form $V(\mathfrak{a})$ for some (radical) ideal $\mathfrak{a} \lhd A$. Furthermore, $\mathfrak{a}$ is not contained in $\mathfrak{N}$; it contains some a that is not nilpotent. Then $\phi(a)$ is not nilpotent either (because $\mathfrak{N} \supset \ker\phi$); so there exists a prime ideal of B, say $\mathfrak{q}$, that does not contain it. Then $\mathfrak{q}^c = \phi^{-1}(\mathfrak{q}) = \phi^*(\mathfrak{q})$ does not contain a. It is therefore a prime ideal i.e. point of $\phi^*(Y)$ that does not contain a and therefore is not an element of $V(\mathfrak{a})$. Thus $V(\mathfrak{a})$ does not contain $\phi^*(Y)$.

In the other direction, if $\mathfrak{N} \not\supset \ker\phi$, then there exists non-nilpotent a such that $\phi(a) = 0$. Then $V(a)$ is a closed subset of X containing the entire image $\phi^*(Y)$, because $\phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q})$ contains $a \in \phi^{-1}(0)$ for every prime ideal $\mathfrak{q} \in Y$. Meanwhile, because a is not nilpotent, there exists a prime ideal not containing it, so $V(a)$ is a proper closed subset of X, and $\phi^*(Y)$ is therefore not dense in X.

(f) Let $\psi : B \to C$ be another ring homomorphism. Then $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.

Exercise 21f solution. We just evaluate the two sides on the same element $\mathfrak{p}$ of $\operatorname{Spec} C$:

$$(\psi \circ \phi)^*(\mathfrak{p}) = (\psi \circ \phi)^{-1}(\mathfrak{p}) = \phi^{-1}(\psi^{-1}(\mathfrak{p})) = \phi^* \circ \psi^*(\mathfrak{p})$$

(g) Let A be an integral domain with just one non-zero prime ideal $\mathfrak{p}$, and let K be A's field of fractions. Let $B = A/\mathfrak{p} \times K$. Define $\phi : A \to B$ by $\phi(x) = (\bar{x}, x)$, where $\bar{x}$ is the image of x in $A/\mathfrak{p}$. Show that ϕ^* is bijective but not a homeomorphism.

Exercise 21g solution. Both $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$ have two elements: $\operatorname{Spec} A = \{\mathfrak{p}, (0)\}$ since the zero ideal is prime because A is an integral domain. Meanwhile, $A/\mathfrak{p}$ is a field, since $\mathfrak{p}$ must be maximal (since it must have a maximal ideal which is prime, and $\mathfrak{p}$ is the only nonzero prime); and K is of course a field; so B is a product of two fields and thus its only prime ideals are $\{0\} \times K$ and $A/\mathfrak{p} \times \{0\}$. (It is generally true that the only ideals of a product of fields $k \times k'$ are the whole thing, zero, and $k \times \{0\}$ and $\{0\} \times k$, and the latter are the only primes.)

Now $\phi^*(\{0\} \times K) = \mathfrak{p}$ since $\phi(x) = (0, x)$ for any $x \in \mathfrak{p}$, and $\phi^*(A/\mathfrak{p} \times \{0\}) = (0)$, because $\phi(x) = (\bar{x}, x) \in A/\mathfrak{p} \times \{0\}$ implies $x = 0$. Therefore ϕ^* is a bijection. However, the Zariski topology on $\operatorname{Spec} B$ is discrete, since neither prime ideal is contained in the other, whereas the Zariski topology on $\operatorname{Spec} A$ is not, because $\mathfrak{p} \supset (0)$ and thus any closed set containing (0) also contains $\mathfrak{p}$.

1.3 Affine Varieties

1. Exercise 26. Here Atiyah and MacDonald define MaxSpec (the set of maximal ideals), noting that in general it does not have the nice functorial properties of Spec, because maximal ideals don't always pull back to maximal ideals. But in some cases it is useful because the elements of MaxSpec can be identified with the points of a topological space.

   Let X be a compact hausdorff topological space and let $C(X)$ be the ring of continuous real-valued functions on X. For $x \in X$, let $\mathfrak{m}_x$ be the ideal of functions vanishing at x. It is maximal because it is the kernel of the homomorphism $C(X) \to \mathbb{R}$ that maps $f \mapsto f(x)$, and this homomorphism is surjective with image the field $\mathbb{R}$. So $x \mapsto \mathfrak{m}_x$ is a mapping μ of X into $\tilde{X} = \operatorname{MaxSpec} C(X)$. The problem aims to show μ is a homeomorphism.

   (a) Show that μ is surjective: in other words, every maximal ideal of $C(X)$ has the form $\mathfrak{m}_x$.

   Exercise 26a solution. Let $\mathfrak{m}$ be a maximal ideal of $C(X)$. Suppose that the functions $f \in \mathfrak{m}$ had no common zero. By continuity, the set X_f on which a given function f is nonzero is open. If the functions f of $\mathfrak{m}$ have no common zero, then the nonzero sets cover X. Thus $\{X_f\}_{f \in \mathfrak{m}}$ is an open cover for X, and by compactness it has a finite subcover $\{X_{f_1}, \dots, X_{f_n}\}$. Then the functions $f_1, \dots, f_n$ have no common zero. Then the function $f = f_1^2 + \cdots + f_n^2 \in \mathfrak{m}$ is nonvanishing, and thus invertible in $C(X)$. It is thus a unit, and $\mathfrak{m}$ is the unit ideal, a contradiction. So the functions of $\mathfrak{m}$ have some common zero, say x. Then $\mathfrak{m} \subset \mathfrak{m}_x$, with equality because the former is maximal.

   (b) By Urysohn's lemma, the continuous functions separate the points of x. Thus show μ is injective.

Exercise 26b solution. This is because if $x \neq y$, then there is a continuous function zero at x and nonzero at y and conversely. Thus $\mathfrak{m}_x \neq \mathfrak{m}_y$.

(c) Let $f \in C(X)$. Let $U_f = \{x \in X : f(x) \neq 0\}$. (I feel Atiyah and MacDonald could have called this X_f to stress the connection with the notation in Exercises 17 and 21.) Let $\tilde{U}_f = \{\mathfrak{m} \in \tilde{X} : f \notin \mathfrak{m}\}$. Show that $\mu(U_f) = \tilde{U}_f$. Show that the open sets U_f, resp. $\tilde{U}_f$, form a basis for the topology of X, resp. $\tilde{X}$, and thus μ is a homeomorphism. (This is a motivating example for algebraic geometry because it shows that the geometric structure of X can be recovered from the ring $C(X)$.)

Exercise 26c solution. $f(x) \neq 0$ if and only if $f \notin \mathfrak{m}_x$; therefore $\mu(U_f) = \tilde{U}_f$.

It is clear why $\tilde{U}_f$ are a basis for the topology of $\tilde{X}$; they are just the intersections with $\operatorname{MaxSpec} C(X)$ of a basis for the topology of $\operatorname{Spec} C(X)$; see problem 17.

As for why U_f form a basis for the topology of X, this is due to Urysohn's lemma (which applies because every compact hausdorff space is normal i.e. T_4). Given an arbitrary open set V, pick a point $x \in V$. The sets $\{x\}$ and $X \setminus V$ are both closed and disjoint; thus by Urysohn's lemma, there is a continuous function f with $f(x) = 1$ and $f|_{X \setminus V} = 0$. Then U_f is contained in V and contains x. Since this construction can be performed for any $x \in V$, it can be used to express V as a union of the U_f's. This shows the U_f's form a basis for the topology.

Thus X can be reconstructed as a topological space from $C(X)$.

2. Exercise 27. Let k be an algebraically closed field and let

$$f_\alpha(t_1, \dots, t_n) = 0$$

be a set of polynomial equations (indexed by α) in n variables, with coefficients in k. The set X of all points $x = (x_1, \dots, x_n) \in k^n$ which satisfy these equations is an *affine algebraic variety.*

Consider the set of all polynomials $g \in k[t_1, \dots, t_n]$ with the property that $g(x) = 0$ for all $x \in X$. Check that this set is an ideal $I(X)$ in the polynomial ring. It is called the *ideal of the variety* X. The quotient ring

$$k[X] = k[t_1, \dots, t_n]/I(X)$$

is the ring of polynomial functions on X, because two polynomials g, h define the same function on X if and only if $g - h$ vanishes at every point of X, that is, if and only if $g - h \in I(X)$.

Let ξ_i be the image of t_i in $k[X]$. The ξ_i (for $1 \leq i \leq n$) are the *coordinate functions* on X: if $x \in X$, then $\xi_i(x)$ is the ith coordinate of x. $k[X]$ is generated as a k-algebra by the coordinate functions, so is called the *coordinate ring* (or affine algebra) of X.

As in Exercise 26, for each $x \in X$ let $\mathfrak{m}_x$ be the ideal of all $f \in k[X]$ such that $f(x) = 0$; check that it is a maximal ideal of $k[X]$. Hence, if $\tilde{X} = \mathrm{MaxSpec}(k[X])$, we have defined a mapping $\mu : X \to \tilde{X}$, namely $x \mapsto \mathfrak{m}_x$.

It is easy to show that μ is injective: if $x \neq y$, we must have $x_i \neq y_i$ for some i $(1 \leq i \leq n)$, and hence $\xi_i - x_i$ is in $\mathfrak{m}_x$ but not in $\mathfrak{m}_y$, so that $\mathfrak{m}_x \neq \mathfrak{m}_y$. What is less obvious (but still true) is that μ is *surjective*. This is one form of Hilbert's Nullstellensatz (see chapter 7).

Exercise 27 solution. Clearly $I(X)$ is closed under addition since if f, g both vanish on all of X, so does $f + g$. Furthermore, if a is any function at all (in particular any element of $k[t_1, \dots, t_n]$), then af also vanishes on all of X. Thus $I(X)$ is an ideal.

As in Exercise 26, $\mathfrak{m}_x$ is maximal because it is the kernel of the surjective homomorphism from $k[t_1, \dots, t_n]$ to k defined by mapping $f \mapsto f(x)$, and the image is a field.

Commentary: this discussion shows that, as in Exercise 26, the MaxSpec of the ring $k[X]$ is in bijection with the points of X. If we take a subset of X to be closed if it is defined by the vanishing of some polynomials, we get a topology on X called the Zariski topology, and this bijection also identifies this topology with the topology of $\mathrm{MaxSpec}\, k[X]$. Thus again we get a way to go back and forth between a topological space, X, and a ring of functions $k[X]$ on this topological space. The next exercise shows how algebraic maps between two affine varieties X and Y can be turned into corresponding ring homomorphisms between their respective rings of functions. This is the complement (in the concrete situation of affine varieties) of the process described in Exercise 21, which shows (in the more general context of an arbitrary ring) how to take a ring homomorphism and turn it into a continuous map between topological spaces.

3. Exercise 28. Let $f_1, \dots, f_m$ be elements of $k[t_1, \dots, t_n]$. They determine a *polynomial mapping* $\phi : k^n \to k^m$: if $x \in k^n$, the coordinates of $\phi(x)$ are $f_1(x), \dots, f_m(x)$.

   Let X, Y be affine algebraic varieties in k^n, k^m respectively. A mapping $\phi : X \to Y$ is said to be *regular* if ϕ is the restriction to X of a polynomial mapping from k^n to k^m.

   If η is a polynomial function on Y, then $\eta \circ \phi$ is a polynomial function on X. Hence ϕ induces a k-algebra homomorphism $k[Y] \to k[X]$, namely $\eta \mapsto \eta \circ \phi$. Show that in this way we obtain a one-to-one correspondence between regular mappings $X \to Y$ and k-algebra homomorphisms $k[Y] \to k[X]$.

   Exercise 28 solution. We have been given a map π from $\mathrm{Mor}(X, Y)$, the set of polynomial maps from X to Y, to $\mathrm{Hom}(k[Y], k[X])$, the set of k-algebra homomorphisms from $k[Y]$ to $k[X]$. As in the problem statement, π is defined by $\pi(\phi) = (\eta \mapsto \eta \circ \phi)$. We need to show it is a bijection.

First, distinct polynomial maps lead to distinct k-algebra homomorphisms, because the coordinate functions separate points. In more detail, if $\phi : X \to Y$ and $\phi' : X \to Y$ are distinct polynomial maps from X to Y, then there is some $x \in X$ such that $\phi(x) \neq \phi'(x)$. This means $\phi(x)$ and $\phi'(x)$ differ in at least one coordinate, say the ith. Let ξ_i be the ith coordinate function on Y (see Exercise 27 for the definition of the coordinate functions). Then $\xi_i(\phi(x)) \neq \xi_i(\phi'(x))$, and therefore $\xi_i \circ \phi \neq \xi_i \circ \phi'$. Thus the k-algebra homomorphisms $\pi(\phi) = (\eta \mapsto \eta \circ \phi)$ and $\pi(\phi') = (\eta \mapsto \eta \circ \phi')$ are distinct, since they differ at ξ_i. Thus π is injective.

To show that π is surjective, we need to show that any k-algebra homomorphism $f : k[Y] \to k[X]$ has the form $\pi(\phi) = (\eta \mapsto \eta \circ \phi)$ for some polynomial map ϕ from X to Y. So let f be an arbitrary such k-algebra homomorphism. Let $\xi_1, \dots, \xi_m$ be the coordinate functions on Y. Then $\xi_1, \dots, \xi_m$ generate $k[Y]$, so f is completely characterized by its action on the ξ's, and each $f(\xi_i)$ is an element of $k[X]$, i.e. a polynomial function on X. The desired polynomial map $\phi : X \to Y$ is given by $x \mapsto (f(\xi_1)(x), \dots, f(\xi_m)(x))$, because then $\xi_i \circ \phi(x) = f(\xi_i)(x)$. Thus, $\xi_i \circ \phi = f(\xi_i)$ for each i, and since a k-algebra homomorphism $k[Y] \to k[X]$ is determined by its action on the coordinate functions ξ_i, this means that $f = (\eta \mapsto \eta \circ \phi) = \pi(\phi)$ as desired. Thus π is surjective.