Homework Exercises

In the following, k denotes a field, and $X, Y, T, ...$ are commuting indeterminates. Assume k is algebraically closed whenever you think that will make life simpler.

1. Show that the ideal $J = (X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n)$ of $k[X,Y]$ cannot be generated by less than $n+1$ elements. What is the dimension of the ring $k[X,Y]/J$? (Hint: consider the vector space dimension of $J/J\mathfrak{m}$ where $\mathfrak{m} = (X,Y)$.)

2. Let J be the ideal of $R = k[X,Y]$ generated by $f = Y - X^2$. Find a k-vector space basis for a vector space complement to J in R, and hence show that there is a ring isomorphism $R/J \cong k[T]$.

3. Let J be the ideal of $R = k[X,Y]$ generated by $f = Y^2 - X^3$. Find a basis for a complement to J in R. Hence show that there is a k-algebra homomorphism $k[X,Y] \to k[T]$ with kernel J and image the subring $k[T^2, T^3]$ of $k[T]$. (Of course, $k[T^2, T^3]$ denotes the subalgebra generated by T^2 and T^3; what is a basis for this ring.)

4. Let $S = k[T^2, T^3]$. Suppose that k is algebraically closed. Let $\theta : S \to k$ be a k-algebra homomorphism. Establish a natural bijection between the points in k^2 lying on the curve $Y^2 - X^3 = 0$, and such θ. If p is a point on the curve, let I_p be the kernel of the corresponding θ. Show that $\dim_k(I_p/I_p^2)$ is one, except when $p = (0,0)$. (Sketch the curve over the real numbers and notice where the curve is not smooth.)

5. Let I be the ideal in $k[X,Y]$ generated by X, and let $R = k + I$. Show that R is a ring. Show that R is NOT noetherian. You should probably keep in mind a basis for R; you might then see an obvious candidate for an ideal of R which is NOT finitely generated. Is I finitely generated *as an ideal of* R?

6. Show that $k[x]$ is integrally closed in $k(x)$.

7. Find the integral closure of $k[x^2, x(x^2-1)]$ in $k(x)$.

8. (Noether normalization) Find a subring $k[y]$ of $k[x, x^{-1}]$ such that $k[x, x^{-1}]$ is a finitely generated $k[y]$-module.

9. Let $R = k[x,y]/(y^p - x^q)$ where p and q are relatively prime positive integers. The ring R is a domain, so has a field of fractions, F say. What is the integral closure of R in F? (Hint: look for an injective map $R \to k[t]$, and work inside $k[t]$, making use of question 1.)

10. (Harder) The ring $R = k[x,y]/(y^2 - x^3 - x^2)$ is a domain, so has a field of fractions. Find the integeral closure of R in its field of fractions.

11. Show that $\mathbb{Q}[x][x^{-1}, (x+1)^{-1}, (x+2)^{-1}, \ldots]$ is not a finitely generated $\mathbb{Q}$-algebra. Is it noetherian?

12. Recall that an ideal $\mathfrak{p}$ of R is *prime* if $R/\mathfrak{p}$ is a domain (i.e., has no zero-divisors). Let $\operatorname{Spec} R$, the spectrum of R, denote the set of prime ideals in R. Show that if $\varphi : R \to S$ is a ring homomorphism, then there is an induced map $\operatorname{Spec} S \to \operatorname{Spec} R$. Give an example to show that this map need not send maximal ideals to maximal ideals.

13. Let $R \subset S$ be rings. Suppose that S is a finitely generated R-module. Let $\mathfrak{m}$ be a maximal ideal of R. Prove that $S\mathfrak{m} \neq S$. (Hint: if $S = Rs_1 + \cdots + Rs_n$, and the result were false, then for each i we could write $s_i = \sum_j r_{ij} s_j$ with each $r_{ij} \in \mathfrak{m}$; it would then follow that $\det(\delta_{ij} - r_{ij}) = 0$, whence $1 \in \mathfrak{m}$, a contradiction). Hence prove there is a maximal ideal $\mathfrak{n}$ of S such that $\mathfrak{m} = R \cap \mathfrak{n}$. Hence show that the map $\operatorname{Spec} S \to \operatorname{Spec} R$ induced by the inclusion of R in S is surjective on the maximal ideals. (What does this mean in the context of Noether normalization).

14. Let $R = k[u,v,w]/(u^2 - vw)$. Show that R embeds in the polynomial ring $S = k[x,y]$ by sending each of u, v, w to a homogenous degree two polynomial. Use the fact that S is integrally closed to show that the image of R under this embedding is integrally closed (in its field of fractions). (Hint: it would be helpful to talk about degree a lot.)

15. Are the following ideals of $k[x,y]$ prime or not:

    (a) $I_1 = (x-3)$,

    (b) $I_2 = (x^2 - y^2, x+y)$,

    (c) $I_3 = (1 + x^2 - y^2, x+y)$,

    (d) $I_4 = (x^3 + y^3, x^6 + y^6)$?

16. Show that the minimal primes of $k[x,y,z]$ containing

$$I = (x(y+z), x(y-z) - 2y)$$

    are (x,y), (y,z), $(x-1, y+z)$. Find a product of these primes contained in I.

17. Find the minimal primes over the ideals (xy, yz, zx) and $(x^2+y^2+z^2, xy+yz+xz)$ of $k[x,y,z]$.

18. What is the radical of the ideal $(xy, (x-y)z)$ in $k[x,y,z]$?

19. Show that the Zariski topology really is a topology.

20. Show that the subset $\operatorname{Max} R \subset \operatorname{Spec} R$ consists of closed points. Moreover, show that if if k is an algebraically closed field, and $R = k[X_1, \ldots, X_n]$, the bijection

$$\operatorname{Max} R \leftrightarrow \mathbb{A}^n$$

given by the Nullstellensatz is a homeomorphism when $\mathbb{A}^n$ is given the Zariski topology as defined in class, and $\operatorname{Max} R$ is given the induced topology by virtue of its being a subspace of $\operatorname{Spec} R$.

21. Let $f : R \to S$ be a ring homomorphism. Show that f induces a continuous function $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$, sending $\mathfrak{p} \in \operatorname{Spec} S$ to $f^{-1}(\mathfrak{p}) := \{r \in R \mid f(r) \in \mathfrak{p}\}$.

22. Consider question 21 with $S = R/I$ and f the quotient map. Show that $f^* : \operatorname{Spec} R/I \to \operatorname{Spec} R$ is the a homeomorphism onto the closed subspace $\mathcal{V}(I) \subset \operatorname{Spec} R$.

23. Suppose that R is a commutative domain. Let $\mathcal{S}$ be a subset of $R - \{0\}$ that is closed under multiplication. Show there is a ring $R_{\mathcal{S}}$ and a ring homomorphism $\alpha : R \to R_{\mathcal{S}}$ with the following properties:

    (a) if $s \in \mathcal{S}$, then $\alpha(s)$ is a unit in $R_{\mathcal{S}}$;

    (b) every element of $R_{\mathcal{S}}$ is of the form $\alpha(x)\alpha(s)^{-1}$ for some $x \in R$ and $s \in \mathcal{S}$;

    (c) α is injective;

    (d) if $\beta : R \to T$ is a ring homomorphism such that $\beta(s)$ is a unit for every $s \in \mathcal{S}$, there is a unique ring homomorphism $\theta : R_{\mathcal{S}} \to T$ such that $\beta = \theta\alpha$.

    We call $R_{\mathcal{S}}$ the localization of R at $\mathcal{S}$.

24. What should one do in the previous exercises if R is not a domain? One would certainly like to invert elements of S to the extent that it is possible.

25. Assume one is in the same situation as in Exercise 23. If I is an ideal of $R_{\mathcal{S}}$ show that $I = (I \cap R)R_{\mathcal{S}}$. Give an example to show that if J is an ideal of R, then $J \neq R \cap JR_{\mathcal{S}}$ in general.

26. Assume one is in the same situation as in Exercise 23. If $\mathfrak{p}$ is a prime ideal of R, show that $\mathfrak{p}R_{\mathcal{S}}$ is either equal to $R_{\mathcal{S}}$ or a prime ideal of $\mathfrak{p}R_{\mathcal{S}}$.

27. Assume one is in the same situation as in Exercise 23. Show that every prime ideal of $R_{\mathcal{S}}$ is of the form $\mathfrak{p}R_{\mathcal{S}}$ for some $\mathfrak{p} \in \operatorname{Spec} R$.

28. Assume one is in the same situation as in Exercise 23. Show that the ring homomorphism $\alpha : R \to R_{\mathcal{S}}$ induces a continuous map $\operatorname{Spec} R_{\mathcal{S}} \to \operatorname{Spec} R$ embedding $\operatorname{Spec} R_{\mathcal{S}}$ as an open subset. The complement of this open set is $V(I)$ for some ideal I. What is I?

29. Decompose $\mathcal{V}(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3)$ into its irreducible components.

30. Although $f = y^2 + x^2(x-1)^2 \in \mathbb{R}[x,y]$ is irreducible and therefore generates a prime ideal, $\mathcal{V}(f) \subset \mathbb{A}^2_{\mathbb{R}}$ is NOT irreducible. Explain this.

31. Let $X \subset Y$ be algebraic sets. Show that every irreducible component of X is contained in some irreducible component of Y. Give both an algebraic and a topological proof.

32. Do the points in $\mathbb{R}^2$ with polar coordinates (r, θ) such that $r = \sin\theta$ form an algebraic set?

33. Let $0 \neq f \in k[x,y]$ and suppose that the degree of f is n. Let $C = \mathcal{V}(f)$. Let L be a line in k^2 such that $L \not\subset C$. Show that $L \cap C$ has at most n points. Is there a line meeting C at exactly n points? (Hint: Let g be the defining equation of L, and think about the image of f in $k[x,y]/(g)$.)

34. Show that $\mathbb{A}^2_k$ is irreducible if k is infinite. What if k is finite?

35. (Vijay's example.) Let I be the ideal in $k[X,Y,Z]$ generated by $X^2 - Y^3$ and $Y^2 - Z^3$. Write x, y, z for the images of X, Y, Z in $R = k[X,Y,Z]/I$. Observe that there is a map $\theta : R \to k[t]$ defined by $x \mapsto t^9$, $y \mapsto t^6$, and $z \mapsto t^4$.

    Show that $R = k[z] \oplus xk[z] \oplus yk[z] \oplus xyk[z]$ (probably best to do this by using the usual basis in $k[X,Y,Z]$ and looking at a complement of I). Thus R is a free $k[z]$-module of rank 4.

    By viewing $k[t]$ as a free $k[t^4]$-module, show that θ is injective, and hence that I is a prime ideal.

36. Let $C \subset \mathbb{R}^2$ be the curve defined by the equation $y^3 = x^3 - x^4$. For each $t \in \mathbb{R}$, let L_t be the line $y = xt$. Show that $L_t \cap C = \{(0,0), p_t\}$ for a unique $p_t \in C$. Hence define a map $f : \mathbb{A}^1 \to C$ by $f(t) = p_t$. Show that f is a regular map.

37. Show that the number of maximal ideals in a finite dimensional k-algebra is finite. (Hint: first mod out by the ideal of elements which annihilate all simple modules, and observe that this quotient ring is semisimple. There are other alternatives.)

38. Prove the long theorem concerning the interplay of properties of a regular map $f : X \to Y$ and the corresponding ring homomorphism $\varphi : \mathcal{O}(Y) \to \mathcal{O}(X)$ between the rings of regular functions.

39. Let R be a domain, X a new variable, and f a non-zero element of R. Let $R[f^{-1}]$ be the subring of Fract R generated by R and f^{-1}.

    (a) Show that $R[f^{-1}] = \{rf^{-n} \mid r \in R, n \geq 0\}$.

    (b) Show that $R[f^{-1}] \cong R[X]/(Xf - 1)$. Hint: show that the kernel of the ring homomorphism $\phi : R[X] \to R[f^{-1}]$ defined by $\Phi(r) = r$ for $r \in R$ and $\Phi(X) = f^{-1}$ is exactly the ideal $(fX - 1)$.

40. (You should compare this with the sneaky trick in the proof of the strong Nullstellensatz.)

    Let I be a prime ideal in $k[X_1, \ldots, X_n]$, and let $Z = \mathcal{V}(I) \subset \mathbb{A}^n$ be its zero locus. Prove the following:

    (a) If $0 \neq f \in \mathcal{O}(Z)$, then

    $$\mathcal{O}(Z)[f^{-1}] \cong k[X_1, \ldots, X_n, X_{n+1}]/(X_{n+1}f - 1, I).$$

    Thus there is an algebraic set $W \subset \mathbb{A}^{n+1}$ such that $\mathcal{O}(Z)[f^{-1}] \cong \mathcal{O}(W)$.

    (b) If $Z_f = \{p \in Z \mid f(p) \neq 0\}$, then there is a bijection between points of Z_f and points of W given by

    $$p = (\alpha_1, \ldots, \alpha_n) \leftrightarrow (\alpha_1, \ldots, \alpha_n, f(p)^{-1}).$$

    (c) The bijection between Z_f and W is a homeomorphism when W has the Zariski topology and Z_f has the subspace topology induced by the fact that it is a subspace of Z with the Zariski topology.

41. Discuss the example $k[t - t^{-1}] \subset k[t, t^{-1}]$ in the context of Exercise ?? above. Discuss both the geometric and algebraic aspects of this example.

    Let K denote a commutative ring, and let M and N be K-modules. If P is another K-module a *K-bilinear map*

    $$f : M \times N \to P$$

    is a map such that both $f(m, -) : N \to P$ and $f(-, n) : N \to P$ are K-module maps for all $m \in M$ and $n \in N$. The *tensor product* of M and N is a pair $(M \otimes N, \lambda)$ consisting of a K-module $M \otimes N$ and a K-bilinear map

    $$\lambda : M \times N \to M \otimes N$$

    that is universal with respect to such bilinear maps in the following sense: if $\theta : M \times N \to P$ is a K-bilinear map, then there is a unique K-module homomorphism $\rho : M \otimes N \to P$ such that $\theta = \rho\lambda$.

    Although the definite article "the" is used in the above definition, we have not yet shown the uniqueness of the tensor product. Indeed, we haven't even shown that a tensor product exists.

42. (Existence) Show that $(M \otimes N, \lambda)$ exists in the following way. Let F be the free K-module with basis the elements of $M \times N$, and let $\mu : M \times N \to F$ be the map sending each (m, n) to the corresponding basis element. Let E be the K-submodule of F generated by the elements

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n), \quad (m, n_1 + n_2) - (m, n_1) - (m, n_2),$$

and

$$(rm, n) - r(m, n), \quad (m, rn) - r(m, n),$$

where $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $r \in K$. Now define $\lambda : M \times N \to F/E$ to be the composition of μ with the quotient module map. Show that λ is bilinear, and that $(F/E, \lambda)$ has the required universal property.

Notation. The image of (m, n) in $M \otimes N$ is denoted $m \otimes n$. Thus, in $M \otimes N$, we have

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \quad m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2,$$

and

$$r.(m \otimes n) = (rm) \otimes n = m \otimes (rn).$$

Basic Properties of $\otimes$.

(i). $(L \oplus M) \otimes N \cong (L \otimes N) \oplus (M \otimes N)$

(ii). $(L \otimes M) \otimes N \cong L \otimes (M \otimes N)$

(iii). $\mathrm{Hom}_K(L, \mathrm{Hom}_K(M, N)) \cong \mathrm{Hom}_K(L \otimes M, N)$

(iv). $M \otimes K^n \cong M^n$, where L^n denotes the direct sum of n copies of L.

43. (Uniqueness) Show that if (T, λ') has the appropriate universal property, then there is a K-module isomorphism $\varphi : F/E \to T$ such that $\varphi\lambda = \lambda'$.

44. Show that if M and N are free K-modules of rank m and n respectively, then $M \otimes N$ is free of rank mn.

45. Let $K = \mathbb{Z}$, and let $M = \mathbb{Z}/(a)$ and $N = \mathbb{Z}/(b)$, where $ab \neq 0$. Show that $M \otimes N \cong \mathbb{Z}/(d)$ where $d = (a, b)$.

46. Let $\{p_1, \ldots, p_n\}$ be n distinct points on the affine line, and let X denote their complement.

(a) Show that X can be given the structure of a variety, and determine $\mathcal{O}(X)$.

(b) Show that as the set of n points changes, so might the isomorphism class of X.

(c) Find the smallest m such that X is isomorphic to an algebraic subset of $\mathbb{A}^m$.

47. Let X be the affine curve defined by the equation $y^2 = x^2(x+1)$. Consider the rational function $f = y/x \in k(X)$. Describe the domains of definition of f and f^2.

48. Do NOT assume k is algebraically closed. Let $f, g \in k[x, y]$ be irreducibles and suppose that neither is a (scalar) multiple of the other. Prove that $\mathcal{V}(f, g)$ is finite, thus proving that two distinct curves meet at a finite number of points. Prove this using the following method: Write $K = k(x)$, and prove that f and g have no common factors in $K[y]$. Deduce that there exist $a, b \in K[y]$ such that $af + bg = 1$. By clearing denominators show that there exist $0 \neq h, p, q \in k[x]$ such that $h = pf + qg$. Hence conclude that there are only finitely many possible values for the x-coordinates of the points in $\mathcal{V}(f, g)$. Do a similar thing for the y-coordinates, and hence get the result.

49. (Do NOT use the Nullstellensatz in this exercise.) Let k be an infinite field. Let $0 \neq f \in k[x_1, \ldots, x_n]$. Prove that $\mathcal{V}(f) \neq \mathbb{A}^n$. Hint: Suppose that x_n appears in the expression for f, and write f as a polynomial in x_n with coefficients in $k[x_1, \ldots, x_{n-1}]$, then use induction on n, making use of the previous problem. Give an example to show this fails if k is finite.

50. Think of six interesting questions about the fields $\mathbb{F}_p$ and $\mathbb{Q}(\sqrt{d})$.

51. The field of rational functions in one variable, denoted $k(x)$, consists of all ratios p/q where p and q are polynomials in x having coefficients in k, and $q \neq 0$. We add and multiply these in the obvious way. The inverse of a non-zero element p/q is q/p. This is the field of rational functions on the affine line over k. Likewise, the field $k(x, y)$ of rational functions on the affine plane over k consists of all ratios p/q where p and q are polynomials in the variables x and y, and $q \neq 0$. Are the fields $k(x)$ and $k(x, y)$ isomorphic? What does the word "isomorphic" mean in this context?

52. Let X be a set, and R the set of all functions $f : X \to k$. If f and g belong to R, how do you suggest we define the sum $f + g$, and the product fg? List what you think are the important properties of the sum and product? Is there an element of R that deserves the name *zero*? Is there an element of R that deserves the name *one*? If so, say what that element is, and what its properties are that warrant it being given that name?

53. Write $C(X)$ instead of R for the set of all k-valued functions on X. For each subset Z of X, define

$$I(Z) := \{f \in C(X) \mid f(x) = 0 \text{ for all } x \in Z\}.$$

State all the properties of I that you think are important. For example, how does it behave with respect to the sum and product in R? Is there a special name for subsets of R having these properties?

54. Let Z be a subset of X. Define $\psi : C(X) \to C(Z)$ by

$$\psi(f) = f|_Z.$$

That is, if $f : X \to k$, $\psi(f)$ is the restriction of f to Z. What are the properties of ψ with respect to the addition and multiplication operations in $C(X)$ and $C(Z)$? How do the elements you labelled *one* and *zero* behave under ψ?

55. Let R be *any* ring of functions $X \to k$. Associate to each subset Z of X the subset

$$I(Z) := \{f \in R \mid f|_Z = 0\}.$$

If $Z' \subset Z$, what is the relation between $I(Z)$ and $I(Z')$? How are $I(Z \cap Z')$ and $I(Z \cup Z')$ related to $I(Z)$ and $I(Z')$?

56. Let R be any ring of functions $X \to k$. Associate to each ideal I in R the subset

$$Z(I) = \{z \in X \mid f(z) = 0 \text{ for all } f \in I\}.$$

What is the relation between the notions of inclusion, sum and product of ideals, and the notions of inclusion, intersection, and union of subsets of X?

57. Let R be any ring of functions $X \to k$. The previous exercises give functions $I(-)$ and $Z(-)$ between subsets of X and ideals of R. What can you say about the compositions $I \circ Z$ and $Z \circ I$?

58. Let X and Y be two sets, and let $\alpha : Y \to X$ be any function. Define $\psi : C(X) \to C(Y)$ by

$$\psi(f) = f \circ \alpha;$$

that is, if $y \in Y$, then $\psi(f)(y) = f(\alpha(y))$. What are the properties of ψ with respect to the operations of addition and multiplication in $C(X)$ and $C(Y)$? How do the elements you labelled *one* and *zero* behave under ψ?

59. Let $\beta : Z \to Y$ and $\alpha : Y \to X$ be maps between sets. Let $C(\beta) : C(Y) \to C(Z)$ and $C(\alpha) : C(X) \to C(Y)$ be the induced maps, namely $C(\beta)(g) = g \circ \beta$ and $C(\alpha)(f) = f \circ \alpha$. Show that $C(\alpha\beta) = C(\beta) \circ C(\alpha)$. Show that if α is the identity map, then $C(\alpha)$ is also the identity map.

60. State four interesting questions about $\mathbb{C}[x, y, z]/(f)$.

61. State four interesting questions about $\mathbb{C}[x, y, z]/(f, g)$.

62. Show that every non-constant homogeneous polynomial in $\mathbb{C}[x, y]$ factors as a product of linear polynomials. Hence show that the zero locus of a non-constant homogeneous polynomial in $\mathbb{C}[x, y]$ is a union of 1-dimensional subspaces of $\mathbb{C}^2$; that is, a union of complex lines through the origin.

63. Suppose that $f_1, \ldots, f_r$ are homogeneous polynomials in $\mathbb{C}[x_1, \ldots, x_n]$. Show that their common zero locus,

$$V(f_1, \ldots, f_r) := \{p \in \mathbb{C}^n \mid f_1(p) = \cdots = f_r(p) = 0\},$$

is a union of lines (i.e., complex lines through the origin).

64. If U is a vector space that is the direct sum of various subspaces U_d, $d \geq 0$, and V is a subspace such that $V = \oplus_{d=0}^{\infty}(V \cap U_d)$, show that

$$U/V \cong \bigoplus_{d=0}^{\infty} \frac{U_d}{V \cap U_d},$$

and hence that

$$U/V = \bigoplus_{d=0}^{\infty} \frac{U_d + V}{V}.$$

65. Let I be an ideal of $k[x_1, \ldots, x_n]$ that is generated by homogeneous elements. Show that

$$I = \bigoplus_{d=0}^{\infty} I \cap k[x_1, \ldots, x_n]_d.$$

66. Show that $\mathbb{Z}[x]$ is not a principal ideal domain.

67. Show that $k[x, y]$ is not a principal ideal domain.

68. Characterize the irreducible polynomials of degree two in $k[x]$ when $\operatorname{char} k \neq 2$. What about when $\operatorname{char} k = 2$?

69. Use the Euclidean algorithm to find the greatest common divisor in $\mathbb{Q}[x]$ of $nx^{n+1} - (n+1)x^n + 1$ and $x^n - nx + n - 1$. Express the greatest common divisor in the form $af + bg$ where f and g are the two given polynomials and a and b are suitable elements of $\mathbb{Q}[x]$.

70. Let C be the curve in $\mathbb{R}^2$ cut out by the equation $y^2 - x^3 = 0$. Consider $R = \mathbb{R}[x, y]/(x^3 - y^2)$ as a ring of functions $C \to \mathbb{R}$. Show that R is isomorphic to the subring of the polynomial ring $k[t]$ consisting of those polynomials of the form

$$\alpha_0 + \alpha_2 t^2 + \cdots + \alpha_n t^n.$$

71. Continue the previous question. For each point $p \in C$, let $\mathfrak{m}_p$ denote the ideal of R consisting of those functions that vanish at p. Show that $\dim_{\mathbb{R}} \mathfrak{m}_p/\mathfrak{m}_p^2 = 1$ if $p \neq (0, 0)$, and that $\dim_{\mathbb{R}} \mathfrak{m}_q/\mathfrak{m}_q^2 = 2$ when $q = (0, 0)$.

72. Continue the previous question. Decide exactly which ideals $\mathfrak{m}_p$ are principal.

73. Show that $1 + x_1^2 + \cdots + x_n^2$ is an irreducible polynomial in $\mathbb{C}[x_1, \ldots, x_n]$ for all $n \geq 2$.

74. Let I be a two-sided ideal in a ring R. Prove there is a bijection between the set of two-sided ideals in R that contain I and the set of ideals in R/I. Under the bijection an ideal J in R corresponds to J/I.

    Show that
    $$R/J \cong \frac{R/I}{J/I}.$$

    How do the sum and product of ideals correspond under this bijection?

75. Show that a finite domain is a field.

76. Let R be a commutative domain containing a field k. Show that R is a field if $\dim_k R < \infty$.

77. Let R and S be rings. Their product $R \times S$ is their cartesian product with component-wise addition and multiplication. This is a ring.

    If I and J are ideals in a ring R such that $I + J = R$, show that $R/I \cap J \cong R/I \times R/J$.

78. In a PID show that $\gcd(f, g)$ generates the ideal (f, g).

79. Let R be a commutative ring. An ideal $\mathfrak{p}$ in R is prime if $R/\mathfrak{p}$ is a domain. This is equivalent to the condition that a product xy can belong to $\mathfrak{p}$ only if either x or y does. The spectrum of R, denoted $\operatorname{Spec} R$, is the set of all prime ideals. Notice that every maximal ideal is prime so $\operatorname{Spec} R$ contains $\operatorname{Max} R$, the set of maximal ideals.

    We make $\operatorname{Spec} R$ a topological space by defining the closed sets to be
    $$V(I) := \{\mathfrak{p} \mid \mathfrak{p} \supset I\},$$
    where I runs over all two-sided ideals of R. Show this really does make $\operatorname{Spec} R$ a topological space. This is called the Zariski topology.

80. Let R be a PID. Show that $\operatorname{Spec} R = \operatorname{Max} R \cup \{0\}$. Describe the closed subsets of $\operatorname{Spec} R$. In particular, if k is an algebraically closed field, what is $\operatorname{Spec} k[t]$ and what is the topology on it? Think of the example of $k = \mathbb{C}$ and compare this to the usual topology.

81. If $\psi : R \to S$ is a homomorphism between commutative rings show that there is an induced map
    $$\psi^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R,$$
    and that this map is continuous. Is this true if we replace $\operatorname{Spec} R$ and $\operatorname{Spec} S$ by $\operatorname{Max} R$ and $\operatorname{Max} S$?

You have just shown that the rule $R \mapsto \operatorname{Spec} R$ and $\psi \mapsto \psi^\sharp$ is a contravariant functor from the category of commutative rings to the category of topological spaces (contravariant because the arrows change direction). Actually you also need to show that $\mathrm{id}_R^\sharp = \mathrm{id}_{\operatorname{Spec} R}$ and $(\psi\phi)^\sharp = \phi^\sharp\psi^\sharp$.

82. View $R = k[x_1, \ldots, x_n]$ as functions $k^n \to k$. Show that there is a natural iinjective map $k^n \to \operatorname{Max} R \to \operatorname{Spec} R$, so the Zariski topology induces a topology on k^n. What are the closed subsets of k^n? Show that every polynomial function $f : k^n \to k$, i.e. every $f \in R$, is a continuous map when k^n and k are both given the Zariski topologies. (The Zariski topology on k is obtained from the inclusions $k \to \operatorname{Max} k[t] \to \operatorname{Spec} k[t]$).

83. A boolean ring is a commutative ring in which $x^2 = x$ for every element. If R is boolean show that $\operatorname{Max} R = \operatorname{Spec} R$.

84. Let R be a commutative domain and suppose that every non-zero non-unit is a product of irreducibles. Show R is a UFD if and only if (x) is a prime ideal for all irreducibles in R.

    In particular, since $R = k[x_1, \ldots, x_n]$ is a UFD, this shows that $R/(f)$ is a domain if and only if f is irreducible.

85. A commutative ring is local if it has a unique maximal ideal. Let $p \in \mathbb{Z}$ be prime. Show that the subring

$$S := \{a/b \mid a, b \in \mathbb{Z},\ p \text{ does not divide } b\}$$

    of $\mathbb{Q}$ is local.

86. Let p be an irreducible element in a PID R. Show that the ring

$$S := \{a/b \mid a, b \in R,\ p \text{ does not divide } b\}$$

    is local.

87. Let J and K be ideals in $k[x_1, \ldots, x_n]$. Define

$$K : J := \{x \in k[x_1, \ldots, x_n] \mid xJ \subset K\}.$$

    Suppose K is a radical ideal. Show that $V(K : J) = \overline{V(K) \backslash V(J)}$.

88. Good notation can have lots of wonderful consequences. The notation (I:J) *is supposed to remind you of ratios. Now we all know that* $\frac{a}{b}.\frac{b}{c} = \frac{a}{c}$ *so the notation suggests* there might be some rel K). Can you find such a relation? Does the rule for adding fractions suggest some statement you can make about $(I : J) + (K : L)$? Can you say anything about $((I : K) : (J : K))$?

89. In $\mathbb{Z}[x]$ factor into irreducibles $x^n - 1$ for $3 \leq n \leq 10$.

90. Are any two of the following rings isomorphic:

$$\mathbb{Z}/(4),\ \mathbb{F}_2[x]/(x^2),\ \mathbb{F}_2[t]/(t^2-1),\ \mathbb{F}_2[y]/(y^2+y+1)?$$

Explain. You can sometimes show two rings are not isomorphic by showing that their (lattices of) ideals are different.

91. What is the integral closure of $R = k[x,y]/(y^2 - x^2(x-1))$ in its field of fractions. Hint: find a subring of $k[t]$ that is isomorphic to R.

92. Let R be a domain with field of fractions F. Let $\mathcal{S}$ be a subset of R consisting of non-zero elements and suppose that $st \in \mathcal{S}$ whenever s and t belong to $\mathcal{S}$. Let $S = R[\mathcal{S}^{-1}]$ be the subring of F generated by R and the inverses of the elements in $\mathcal{S}$. Every element in S can therefore be written in the form xy^{-1} where $x \in R$ and $y \in \mathcal{S}$. Show there is a natural 1-1 correspondence between the prime ideals of S and the prime ideals $\mathfrak{p}$ of R such that $\mathfrak{p} \cap \mathcal{S} = \phi$.

93. Continue with the notation of the previous exercise. A previous week's homework exercise showed that the inclusion map $\psi : R \to R[\mathcal{S}^{-1}]$ induces a continuous map

$$\psi^\sharp : \operatorname{Spec} R[\mathcal{S}^{-1}] \to \operatorname{Spec} R$$

when the two spectra are given the Zariski topology. Show that this map is a homeomorphism onto the subset of $\operatorname{Spec} R$ that is the complement of the set

$$Z := \{\mathfrak{q} \in \operatorname{Spec} R \mid \mathfrak{q} \cap \mathcal{S} \neq \phi\}.$$

Remarks and hints: Let's write U for the complement to Z. The topology on U is induced from that on $\operatorname{Spec} R$—the closed sets of U are exactly the subsets of the form $Y \cap U$ where Y is a closed subset of $\operatorname{Spec} R$. If J is an ideal of $R[\mathcal{S}^{-1}]$, then $J = (J \cap R)R[\mathcal{S}^{-1}]$, i.e., as an ideal of $R[\mathcal{S}^{-1}]$, J is generated by its intersection with R. If I is an ideal in R, then $IR[\mathcal{S}^{-1}] = \{as^{-1} \mid a \in I, s \in \mathcal{S}\}$. You can use these remarks without proof.

In general Z will not be a closed subset of $\operatorname{Spec} R$. When R is the ring of integers and $\mathcal{S}$ consists of all non-zero integers, then $Z \subset \operatorname{Spec} \mathbb{Z}$ consists of all non-zero ideals in $\mathbb{Z}$, and this subset of $\operatorname{Spec} \mathbb{Z}$ is not equal to $V(I)$ for any ideal I in $\mathbb{Z}$. Remember the zero ideal belongs to $\operatorname{Spec} \mathbb{Z}$. In this case $R[\mathcal{S}^{-1}] = \mathbb{Q}$, and the map $\operatorname{Spec} \mathbb{Q} \to \operatorname{Spec} \mathbb{Z}$ sends the unique point in $\operatorname{Spec} \mathbb{Q}$ to the zero prime ideal in $\operatorname{Spec} \mathbb{Z}$.

However, if $\mathcal{S}$ is finitely generated (meaning there are elements $s_1, \ldots s_n \in \mathcal{S}$ such that $\mathcal{S} = \{s_1^{i_1} \cdots s_n^{i_n} \mid (i_1, \ldots, i_n) \in \mathbb{N}^n\}$) Z is closed.

94. Let L be a submodule of a left R-module N. Show that there is a bijection between the submodules of N that contain L and the submodules of N/L.

Under the bijection a submodule M lying between L and N corresponds to the submodule M/L of N/L. Show that

$$N/M \cong \frac{N/L}{M/L}.$$

95. Let M be a left R-module. If I is an ideal of R we write

$$IM := \{\sum_{i=1}^{n} a_i m_i \mid n \geq 0,\ a_i \in I,\ m_i \in M\}.$$

Show that IM is a submodule of M. Show that if $IM = 0$, there is a natural way to make M a left R/I-module.

96. Let S be any subring of $R = k[x]$ that is strictly larger than k. Show that R is a finitely generated R-module. What minimal information about S would allow you to obtain an upper bound on the number of elements needed to generate R as an S-module?

97. Hilbert showed that every ideal in a polynomial ring $k[x_1, \ldots, x_n]$ is finitely generated. Find explicit generators for the ideal

$$I := \{f \in \mathbb{R}[x, y, z] \mid f(a, b, c) = 0 \text{ for all } (a, b, c) \in S^2\}.$$

where S^2 is the sphere

$$S^2 := \{(a, b, c) \in \mathbb{R}^3 \mid a^2 + b^2 + c^2 = 1\}.$$

98. Show that $k[x]$ has infinitely many irreducible elements, and use that to show that $k(x)$ is not a finitely generated $k[x]$-module.

99. Let R be a subring of the commutative ring S. Suppose that S is a finitely generated R-module. Show that if $\mathfrak{m}$ is a maximal ideal of R, then $S\mathfrak{m} \neq S$ (Hint: suppose to the contrary that $S = S\mathfrak{m}$ and write $S = \sum_i Rs_i$ and $s_i = \sum_j r_{ij} s_j$ with $r_{ij} \in \mathfrak{m}$; then prove that the determinant of the matrix $(r_{ij} - \delta_{ij})$ is zero, and conclude that $1 \in \mathfrak{m}$.)

Hence show that there is a maximal ideal $\mathfrak{n}$ of S such that $\mathfrak{n} \cap R = \mathfrak{m}$. What does this say in terms of the map $\operatorname{Spec} S \to \operatorname{Spec} R$ induced by the inclusion $R \to S$?

100. Let p be a non-zero element in the commutative ring R. Show that (p) is a prime ideal if and only if p is a prime element of R.

101. Are the following ideals of $k[x, y]$ prime or not? Give reasons, and say whether your answer depends on the characteristic of k.

(a) $(x^3 - y^2)$

(b) $(1 + x^3 - y^3)$

(c) $(x^2 - y^2, x + y)$

(d) $(1 + x^2 - y^2, x + y)$

(e) $(x^2 + y^2, x + y)$

102. If I is an ideal in a commutative ring R, a prime ideal $\mathfrak{p}$ containing I is called a minimal prime over I if there are no prime ideals $\mathfrak{q}$ such that $I \subset \mathfrak{q} \subset \mathfrak{p}$ other than $\mathfrak{q} = \mathfrak{p}$.

What are the minimal primes over the following ideals:

(a) $(1 + x^2 - y^2, x + y)$ in $k[x, y]$;

(b) (xy, yz, zx) in $k[x, y, z]$;

(c) $(x^2 + y^2 + z^2, xy + yz + xz)$ in $k[x, y, z]$.

103. Find the radical of the ideal $(xy, z(x - y))$ in $k[x, y, z]$.

104. What are the closed points in Spec R?

105. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct prime ideals, what is the radical of $\mathfrak{p}_1^{i_1} \cdots \mathfrak{p}_n^{i_n}$?

106. Give an example to show that a sum of radical ideals need not be radical.

107. Describe the subvariety

$$x(y + z) = x(y - z) - 2y = 0$$

of $\mathbb{C}^3$ by describing its irreducible components and their intersections.

108. What are the irreducible components of the subvariety of $\mathbb{C}^2$ given by

$$x^4 - y^4 = y^4 - x^2y^2 + xy^2 - x^3 = 0?$$

109. Is $(x^2 - y^3, y^2 - z^3)$ a prime ideal of $k[x, y, z]$?

110. Let $C \subset \mathbb{R}^2$ be the curve $y^3 = x^3 - x^4$. Let L_t, $t \in \mathbb{R}$, be the line $y = tx$. Show that L_t meets C at $\{(0, 0), p_t\}$ where p_t is a unique point of C. Define the map $f : \mathbb{R} \to C$ by $f(t) = p_t$. Is f a morphism? Is it bijective? Sketch C.

111. If f is an irreducible polynomial in $k[x_1, \ldots, x_n]$, is $V(f)$ irreducible? Explain. What if $f = y^2 + x^2(x - 1)^2 \in \mathbb{R}[x, y]$?

112. Let $I = (x^2 + y^2, x^2 - y^2) \subset \mathbb{C}[x, y]$. Find $V(I)$ and $\dim_{\mathbb{C}} \mathbb{C}[x, y]/I$.

113. If $X \subset Y$ are closed subvarieties of $\mathbb{A}^n$, show that every irreducible component of X is contained in some irreducible component of Y.

Math 504, Homework 8, November 30, 2001

Do all problems. In the exercises below k, K, L, and F, denote fields. We write $\mathbb{F}_q$ for the field with $q = p^n$ elements—you can assume there is a unique field of this cardinality when p is a positive prime. You may use Eisenstein's criterion.

1. Let K be a degree two extension of k. If $\operatorname{char} k \neq 2$, show that $K = k(\alpha)$ for some $\alpha \in K$ such that $\alpha^2 \in k$. If $\operatorname{char} k = 2$, show that $K = k(\alpha)$ and either α^2 or $\alpha^2 + \alpha$ is in k. If k is finite that only the second alternative occurs.

2. Is $x^2 + 5$ irreducible over $\mathbb{F}_{169}$?

3. Let α be a complex number such that $\alpha^3 + \alpha + 1 = 0$. Does $\mathbb{Q}(\alpha)$ contain $i = \sqrt{-1}$. Does $\mathbb{Q}(\sqrt[4]{-2})$ contain i?

4. Let K be an extension of k, and $\alpha \in K$. We write $k[\alpha]$ for the smallest subring of K containing k and α and $k(\alpha)$ for the smallest subfield of K containing k and α. Show that $k[\alpha] = k(\alpha)$ if and only if α is algebraic over k.

5. Let K and F be extension fields of k and $\alpha \in K$ and $\beta \in F$. Show that $k(\alpha) \cong k(\beta)$ if and only if α and β have the same minimal polynomial.

6. Find the minimal polynomial of $\sqrt{5}+\sqrt{7}$ over each of the fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{14})$, and $\mathbb{Q}(\sqrt{5}-\sqrt{7})$.

7. Let α be a complex root of the polynomial $x^3 - 3x + 5$. Find the inverse of $\alpha^2 + 2\alpha - 1$ in $\mathbb{Q}(\alpha)$ in the form $a + b\alpha + c\alpha^2$ where $a, b, c \in \mathbb{Q}$.

8. Let $\zeta_n = e^{2\pi i/n}$. Find the minimal polynomial of ζ_n over $\mathbb{Q}$ for $3 \leq n \leq 12$.

9. Find the minimal polynomial of ζ_{12} over $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\zeta_6)$, and $\mathbb{Q}(\zeta_4)$.

10. Find the minimal polynomial of $\zeta_5^2 + \zeta_5^3$ over $\mathbb{Q}$.

11. Let α be the real 35^{th} root of 2. What is the degree of the minimal polynomial of $1 + \alpha^2$ over $\mathbb{Q}$?

Some Solutions

1. First, $k[X,Y]$ has a k-vector space basis $\{X^iY^j \mid i,j \geq 0\}$ and the maximal ideal $\mathfrak{m} = (X,Y)$ has basis $\{X^iY^j \mid i+j \geq 1\}$. It follows that $\mathfrak{m}^n$ has basis $\{X^iY^j \mid i+j \geq n\}$ and that $\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = n+1$. Therefore

$$\dim_k \frac{k[X,Y]}{\mathfrak{m}^n} = |\{(i,j) \in \mathbb{N}^2 \mid i+j \leq n\} == 1+2+\cdots+n = \frac{1}{2}n(n+1).$$

The ideal J in the question is $\mathfrak{m}^n$, so $\dim_k k[X,Y]/J = n(n+1)/2$.

Let R be any k-algebra, $\mathfrak{m}$ a maximal ideal of R such that $R/\mathfrak{m} \cong k$, and $I = a_1R + \cdots + a_tR$ an ideal. Then $I/I\mathfrak{m}$ is an $R/\mathfrak{m}$-module generated by the images of $a_1,\ldots,a_t$ so is a k-vector space of dimension $\leq t$. Hence the minimal number of generators for the ideal I is $\geq \dim_k I/I\mathfrak{m}$.

In this problem we see that $J/\mathfrak{m}J$ has dimension $n+1$, so J needs at least $n+1$ generators.

4. The kernel of the map $\psi : k[X,Y] \to k[T]$ defined by $\psi(X) = T^2$ and $\psi(Y) = T^3$ contains $J = (X^3 - Y^2)$. There is a vector space decomposition

$$k[X,Y] = k[X] \oplus Yk[X] \oplus J.$$

To see this first observe that each X^iY^j belongs to the sum on the right: this is clear if $j = 0$ or $j = 1$ and, if $j \geq 2$, $X^iY^j = X^iY^{j-2}(Y^2 - X^3) + X^{i+3}Y^{j-2}$ so we may then argue by induction on j. The sum is direct because there is a direct sum $k[T^2] \oplus T^3k[T^2]$ in $k[T]$. This also makes it clear that $\ker\psi = J$.

Thus $k[X,Y]/(X^3 - Y^2) \cong S = k[T^2,T^3] \subset k[T]$. There is an obvious bijection between k-algebra homomorphisms $\theta : S \to k$ and k-algebra homomorphisms $\theta : k[X,Y] \to k$ that vanish on J. A k-algebra homomorphism $\theta : k[X,Y] \to k$ is completely determined by $\alpha = \theta(X)$ and $\beta = \theta(Y)$, and $J \subset \ker\theta$ if and only if $\alpha^3 = \beta^2$, i.e., if and only if $(\alpha,\beta) \in C$ where C is the curve $X^3 = Y^2$. So the k-algebra homomorphisms $\theta : k[T^2,T^3] \to k$ are in bijection with the points on C.

Now let $\mathfrak{m}$ be a maximal ideal of S. Write x and y for the images of X and Y in $k[X,Y]/J$ and $\mathfrak{m} = (x-\alpha, y-\beta)$ where $(\alpha,\beta) \in C$. Then $\mathfrak{m}$ is the image of the maximal ideal $\mathfrak{n} = (X-\alpha, Y-\beta)$ in $k[X,Y]$ so $\mathfrak{m}/\mathfrak{m}^2$ is a quotient of $\mathfrak{n}/\mathfrak{n}^2$ and $\dim_k \mathfrak{m}/\mathfrak{m}^2 \leq \dim_k \mathfrak{n}/\mathfrak{n}^2 = 2$. I showed in class (Lemma 5.7) that $\mathfrak{m} \neq \mathfrak{m}^2$.

If $\mathfrak{m} = (x,y) = kT^2 + kT^3 + \cdots$ (i.e., if $(\alpha,\beta) = (0,0)$) then $\mathfrak{m}^2 = kT^4 + kT^5 + \cdots$, so $\dim(\mathfrak{m}/\mathfrak{m}^2) = 2$.

We will now show that if $\mathfrak{m} \neq (x,y)$, then $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$. So assume $(0,0) \neq (\alpha,\beta) \in C$. It suffices to show that $x-\alpha$ and $y-\beta$ are linearly dependent modulo $\mathfrak{m}^2$. Certainly $\mathfrak{m}^2$ contains

$$(y-\beta)^2 = y^2 - 2\beta y + \beta^2 = x^3 - 2\beta y + \beta^2$$

and $(x-\alpha)^2 = x^2 - 2\alpha x + \alpha^2$, so contains $x^3 - 2\alpha x^2 + \alpha^2 x$ and $x^3 - 2\alpha(2\alpha x -$

$\alpha^2) + \alpha^2 x = x^3 - 3\alpha^2 x + 2\alpha^3$. Hence $\mathfrak{m}^2$ contains

$$\begin{aligned}\left(x^3 - 2\beta y + \beta^2\right) - \left(x^3 - 3\alpha^2 x + 2\alpha^3\right) &= -2\beta y + \beta^2 + 3\alpha^2 x - 2\alpha^3 \\ &= -2\beta y + 3\alpha^2 x - \alpha^3 \\ &= 3\alpha^2(x-\alpha) - 2\beta(y-\beta).\end{aligned}$$

Hence $x - \alpha$ and $y - \beta$ are linearly dependent modulo $\mathfrak{m}^2$ and $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$.

14. Let $\phi : T = k[u,v,w] \to R = k[x,y]$ be the k-algebra homomorphism defined by $\phi(u) = xy$, $\phi(v) = x^2$, and $\phi(w) = y^2$. The image of ϕ is the subring of $k[x,y]$ consisting of all polynomials having no odd degree terms; i.e., $\mathrm{im}(\phi)$ is spanned by all $x^i y^j$ such that $i + j$ is even.

The kernel of ϕ contains $f = u^2 - vw$ and hence contains the ideal fT. It is trickier to show this is exactly the kernel.

Here is one such argument based on the fact that R and T are *graded* k-algebras, i.e, there is a nice notion of "degree".

Define T_n to be the linear span of all $u^p v^q w^r$ such that $p+q+r = n$. Define R_n to be the linear span of all $x^i y^j$ such that $i + j = n$. Then $T = \oplus_{n\geq 0} T_n$ and $R = \oplus_{n\geq 0} R_n$ and $T_i T_j \subset T_{i+j}$ and $R_i R_j \subset R_{i+j}$ for all i and j.

Since $\phi : T \to R$ maps T_n surjectively onto R_{2n},

$$\ker\phi = \bigoplus_{n\geq 0} \left(T_n \cap \ker\phi\right).$$

Thus, to show that $\ker\phi = fT$ it suffices to show that $T_n \cap \ker\phi = fT_{n-2}$ for all n. Because $T_n \to R_{2n}$ is surjective we know that

$$\dim_k\left(T_n \cap \ker\phi\right) = \dim T_n - \dim R_{2n}.$$

But $\dim R_i = i + 1$ and $\dim T_i = \binom{i+2}{2}$, so

$$\dim_k\left(T_n \cap \ker\phi\right) = \frac{1}{2}n(n+1) - (2n+1) = \frac{1}{2}(n-1)(n-2) = \dim T_{n-2} = \dim fT_{n-2}.$$

Hence $T_n \cap \ker\phi = fT_{n-2}$ and $\ker\phi = (u^2 - vw)T$.

Write S for $\phi(T) \subset R$ and write $S_i = S \cap R_i$. Thus $S_i = 0$ if i is odd and $S_i = R_i$ if i is even. Now we show that S is integrally closed in its field of fractions $\mathrm{Fract}\, S$. There are injections

$$\begin{array}{ccc} S & \longrightarrow & R \\ \downarrow & & \downarrow \\ \mathrm{Fract}\, S & \longrightarrow & \mathrm{Fract}\, R. \end{array}$$

Suppose that $\xi \in \mathrm{Fract}\, S$ is integral over S. Then $\xi \in \mathrm{Fract}\, R$ is integral over R and hence is in R because $k[x,y]$ in integrally closed, so it remains to show that $R \cap \mathrm{Fract}\, S = S$.

If $R \cap \operatorname{Fract} S$ is strictly larger than S we can find an $r \in R$ of minimal degree (i.e., $r \in R_0 \oplus R_1 \oplus \cdots \oplus R_n$ with n minimal) such that $r = a/b$ for some $a, b \in S$ with $b \neq 0$. Then $rb = a$. Write

$$\begin{aligned} r &= r_n + \text{lower degree terms}, \\ a &= a_m + \text{lower degree terms}, \\ b &= b_p + \text{lower degree terms}, \end{aligned}$$

where $a_i, b_i, r_i \in R_i$. Looking at the highest degree term $r_n b_p = a_m$; but $a, b \in S$, so p and m are even. Hence n is also even and $r_n \in S$. Thus $r - r_n = ab^{-1} - r_n \in R \cap \operatorname{Fract} S$; but $\deg(r - r_n) < \deg r$, so $r - r_n \in S$. Hence $r \in S$.

15. The ideal $(x-3)$ is prime in $k[x,y]$ because $k[x,y]/(x-3) \cong k[y]$ which is a domain. To be precise, $(x-3)$ is the kernel of the surjective k-algebra homomorphism $\phi : k[x,y] \to k[y]$ defined by $\phi(x) = 3$ and $\phi(y) = y$.

The ideal $I = (x^2 - y^2, x + y)$ is equal to $(x + y)$, and this is a prime ideal in $k[x,y]$ because $k[x,y]/(x+y) \cong k[y]$.

The ideal $J = (1 + x^2 - y^2, x + y)$ is equal to $(1, x + y)$ which equals the ring itself. But the ring itself is *not* considered to be a prime ideal.

The ideal $K = (x^3 + y^3, x^6 + y^6)$ is not prime because it contains the product $(x + y)(x^2 - xy + y^2)$ and neither of these elements is in K because $K \subset \sum_{i+j \geq 3} k x^i y^j$.

16. To show that the minimal primes over $I = (x(y+z), x(y-z)-2y)$ are $\mathfrak{p}_1 = (x,y)$, $\mathfrak{p}_2 = (y,z)$, and $\mathfrak{p}_3 = (x-1, y+z)$ it suffices to show that I is contained in each of these and that I contains some product involving all three of them, but not a product involving only two of them—it is obvious that each $\mathfrak{p}_i$ is prime because $k[x,y,z]/\mathfrak{p}_i \cong k[t]$, the polynomial ring in one variable, and $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ if $i \neq j$.

One sees at a glance that $I \subset \mathfrak{p}_1 \cap \mathfrak{p}_2$ and, since $x(y-z)-2y = (x-1)(y-z)-(y+z)$, $I \subset \mathfrak{p}_3$. Hence $I \subset \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3$ and $V(I) \supset V(\mathfrak{p}_1) \cup V(\mathfrak{p}_2) \cup V(\mathfrak{p}_3) = V(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)$.

We will now show that $V(I) \subset V(\mathfrak{p}_1) \cup V(\mathfrak{p}_2) \cup V(\mathfrak{p}_3)$ from which it will follow that $V(I) = V(\mathfrak{p}_1) \cup V(\mathfrak{p}_2) \cup V(\mathfrak{p}_3)$, whence $\sqrt{I} = \sqrt{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3$. Let $(a,b,c) \in V(I)$. Suppose first that $b = 0$; then $ac = 0$ so $(a,b,c) \in V(\mathfrak{p}_1) \cup V(\mathfrak{p}_2)$. Now suppose that $b \neq 0$. Then $0 = a(b+c) = (a-2)b - ac = (a-2)b + ab = (a-1)b$, so $a = 1$ and $b + c = 0$, whence $(a,b,c) \in V(\mathfrak{p}_3)$. Hence $\sqrt{I} = \sqrt{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}$ and $(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^n \subset I$ for some n.

It is kinda tedious to show, but $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \subset I$!

If $\mathfrak{p}_1^i\mathfrak{p}_2^j \subset I$, then $V(I) \subset V(\mathfrak{p}_1\mathfrak{p}_2) = V(\mathfrak{p}_1) \cup V(\mathfrak{p}_2)$. But this ain't the case because $(1,1,-1) \in V(I)$ but is not in $V(\mathfrak{p}_1)$ or $V(\mathfrak{p}_2)$. Similarly, $(2,0,0) \in V(I)$ but is not in $V(\mathfrak{p}_1) \cup V(\mathfrak{p}_3)$, so $\mathfrak{p}_1^i\mathfrak{p}_3^j \not\subset I$. Finally, $(0,0,1) \in V(J)$ but is not in $V(\mathfrak{p}_2) \cup V(\mathfrak{p}_3)$ so $\mathfrak{p}_2^i\mathfrak{p}_3^j \not\subset I$.

17. Before doing this exercise notice that lines and planes in $\mathbb{A}^n$ are irreducible because their coordinate rings are domains—the coordinate ring of a line (resp., a plane) is a polynomial ring in one (resp., two) variable(s). If we are working in $\mathbb{A}^3$ with coordinate functions x, y, z, let's write P_x for the plane $x = 0$, L_{xy} for the line $x = y = 0$, et cetera.

The minimal primes over $J = (xy, xz, yz)$ are in bijection with the irreducible components of $V(J)$ so we first find those. Then

$$\begin{aligned} V(J) &= V(xy) \cap V(xz) \cap V(yz) \\ &= (P_x \cup P_y) \cap (P_x \cup P_z) \cap (P_y \cup P_z) \\ &= L_{xy} \cup L_{xz} \cup L_{yz}. \end{aligned}$$

Hence the minimal primes over J are

$$(x,y),\ (x,z),\ (y,z)$$

and

$$\sqrt{J} = (x,y) \cap (x,z) \cap (y,z) = (xz, yz, xy).$$

Notice that $(xz, yz, xy)^2 \subset J$.

18. The radical of the ideal $I = (xy, (x-y)z)$ in $k[x,y,z]$ is the intersection of the minimal primes over I. Those minimal primes are in bijection with the

irreducible components of $V(I)$ so we first find those. Then

$$\begin{aligned} V(I) &= V(xy) \cap V((x-y)z) \\ &= (P_x \cup P_y) \cap (P_{x-y} \cup P_z) \\ &= (P_x \cap P_{x-y}) \cup (P_x \cap P_z) \cup (P_y \cap P_{x-y}) \cup (P_y \cap P_z) \\ &= L_{xy} \cup L_{xz} \cup L_{xy} \cup L_{yz}. \end{aligned}$$

Hence the minimal primes over I are

$$(x,y),\ (x,z),\ (y,z)$$

and

$$\sqrt{I} = (x,y) \cap (x,z) \cap (y,z) = (xz, yz, xy).$$

Notice that $(xz, yz, xy)^2 \subset I$.

29. Really 23...I have a numbering problemo. Let $I = (y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3)$. Decomposing $V(I) \subset \mathbb{A}^2$ into its irreducible components is equivalent to finding the minimal primes over I. Since $(y^2 - x)(y^2 + x) = y^4 - x^2 \in I$, $I = I_1 \cap I_2$ and $V(I) = V(I_1) \cup V(I_2)$ where

$$I_1 = (y^2 - x, y^4 - x^2y^2 + xy^2 - x^3) = (y^2 - x, y^4 - y^6 + y^4 - y^6) = (y^2 - x, 2(y^4 - y^6))$$

and

$$I_2 = (y^2 + x, y^4 - x^2y^2 + xy^2 - x^3) = (y^2 + x, y^4 - y^6 - y^4 + y^6) = (y^2 + x).$$

Now $k[x,y]/I_1 \cong k[y]/(2y^4(1-y)(1+y))$ so

$$V(I_1) = \begin{cases} \{(0,0), (1,1), (-1,1)\} & \text{if } \operatorname{char} k \neq 2 \\ \text{the parabola } x = y^2 & \text{if } \operatorname{char} k = 2. \end{cases}$$

Also $k[x,y]/I_2 \cong k[y]$, so $V(I_2)$ is the parabola $x + y^2 = 0$. Thus

$$V(I) = \begin{cases} \{\text{the parabola } x = -y^2\} \cup \{(1,1)\} & \text{if } \operatorname{char} k \neq 2 \\ \text{the parabola } x = y^2 & \text{if } \operatorname{char} k = 2. \end{cases}$$

39. Should be 34!

Lemma. *Let f be a non-zero element in a domain R and $R[f^{-1}]$ the subring of* Fract R *generated by R and f^{-1}. Then $R[X]/(Xf-1) \cong R[f^{-1}]$.*

Proof: It is clear that $R[f^{-1}]$ is the image of the map $\phi : R[X] \to \operatorname{Fract} R$ defined by $\phi(r) = r$ for $r \in R$ and $\phi(X) = f^{-1}$.

It is clear that $\ker\phi \supset (Xf-1)$. To prove the reverse inclusion, suppose that $a = \sum_{i=0}^{n} a_i X^i$ is in the kernel of f. We will argue by induction on $n = \deg a$. Multiplying $\phi(a)$ by f^n, we see that

$$0 = \sum_{i=0}^{n} a_i f^{n-i} = a_0 f^n + a_1 f^{n-1} + \cdots + a_{n-1} f + a_n,$$

whence f divides a_n. Write $a_n = fb$. Now

$$a = bX^{n-1}(Xf-1) + (a_{n-1}+b)X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1 X + a_0.$$

The first term of the sum on the right-hand side belongs to $\ker\phi$, so the sum of the other terms is also in $\ker\phi$; but that sum has degree $\leq n-1$ so, by the induction hypothesis, belongs to $(Xf-1)$. Hence $a \in (Xf-1)$. $\square$

It is clear that there is a bijection $p = (\alpha_1, \ldots, \alpha_n) \leftrightarrow (\alpha_1, \ldots, \alpha_n, f(p)^{-1})$ between the points of $Z_f := \{p \in Z \mid f(p) \neq 0\}$ and points of $W = V(I, X_{n+1}f - 1)$.

(c) The projection map $\pi : \mathbb{A}^{n+1} = \mathbb{A}^n \times \mathbb{A}^1 \to \mathbb{A}^n$, $(p,q) \mapsto p$, is a morphism, so continuous with respect to the Zariski topologies. Hence the restriction of π to $W = V(I, X_{n+1}f - 1)$ is a continuous map $\pi : W \to Z_f$. This is a bijection, so its inverse is also continuous. Thus W is homeomorphic to Z_f.

87. Should be 81!

By definition, $(K : J)J \subset K$, so

$$V(K) \subset V((K:J)J) = V(K:J) \cup V(J),$$

whence $V(K) - V(J) \subset V(K:J)$ and, because $V(K:J)$ is closed,

$$\overline{V(K) - V(J)} \subset V(K:J).$$

To prove the reverse inclusion we need to assume that K is radical, so assume that. This implies $(K:J)$ is radical too: if $a^2 \in (K:J)$ then $a^2 J \subset K$ so $(aJ)^2 \subset K$, whence $aJ \subset K$.

Let $f \in I(V(K) - V(J))$ and $g \in J$. Let $p \in V(K)$. If $p \notin V(J)$, then $f(p) = 0$; if $p \in V(J)$, then $g(p) = 0$; in either case, $(fg)(p) = 0$. Hence $fg \in I(V(K)) = K$. But this is true for all $g \in J$, so $fJ \subset K$ and $f \in (K:J)$, so

$$I(V(K) - V(J)) \subset (K:J).$$

Now, using the fact established in class that $I(V(S)) = \overline{S}$ for any subset $S \subset \mathbb{A}^n$, we get

$$\overline{V(K) - V(J)} = V(I(V(K) - V(J))) \supset V(K:J).$$

92. Should be 85! We consider the map $f : \operatorname{Spec} S \to \operatorname{Spec} R$, $f(\mathfrak{p}) := R \cap \mathfrak{p}$. Write $U := \{\mathfrak{q} \in \operatorname{Spec} R \mid \mathfrak{q} \cap \mathcal{S} = \phi\}$. The image of f is contained in U because if $f(\mathfrak{p})$ were not in U then $R \cap \mathfrak{p}$ would contain some $s \in \mathcal{S}$. But then $\mathfrak{p}$ contains s and hence $s^{-1}s = 1$, contradicting the fact that $\mathfrak{p}$ is prime (so not equal to S!).

Claim: If I is an ideal of $S = R[\mathcal{S}^{-1}]$, then $I = (R \cap I)S$. Proof: Certainly, $(R \cap I)S \subset I$ because I is an ideal of S. On the other hand, every element of I is of the form xs^{-1} for some $x \in R$ and $s \in \mathcal{S}$ and since $x = xs^{-1}s$, $x \in R \cap I$; therefore $x \in (R \cap I)S$. $\Diamond$

It follows that f is injective.

Now let $\mathfrak{q} \in \operatorname{Spec} R$ be such that $\mathfrak{q} \cap \mathcal{S} = \phi$. We will show that $f : \operatorname{Spec} S \to U$ is surjective by showing that $\mathfrak{q}S$ is prime and $\mathfrak{q} = f(\mathfrak{q}S)$.

In order to show that $\mathfrak{q}S$ is prime, suppose $as^{-1}, bt^{-1} \in S$ are such that $as^{-1}bt^{-1} = cu^{-1} \in \mathfrak{q}S$. We can assume $a, b, c \in R$, $c \in \mathfrak{q}$, and $s, t, u \in \mathcal{S}$. Then $abu = cst \in \mathfrak{q}$. But $\mathfrak{q}$ is prime so at least one of a, b, u belongs to $\mathfrak{q}$. But $\mathcal{S} \cap \mathfrak{q} = \phi$ so either a or b is in $\mathfrak{q}$, and therefore either as^{-1} or bt^{-1} in in $\mathfrak{q}S$. This shows that $\mathfrak{q}S$ is prime.

Now we show that $f(\mathfrak{q}S) = \mathfrak{q}$. Certainly, $\mathfrak{q} \subset R \cap \mathfrak{q}S$. Suppose that $r \in R \cap \mathfrak{q}S$. Then $r = as^{-1}$ where $a \in \mathfrak{q}$ and $s \in S$. Therefore $sr \in \mathfrak{q}$; but $s \notin \mathfrak{q}$, so $r \in \mathfrak{q}$. Thus $\mathfrak{q} = R \cap \mathfrak{q}S = f(\mathfrak{q}S)$. So $f : \operatorname{Spec} S \to U$ is a surjective map. This completes the proof of the bijection

$$U \longleftrightarrow \operatorname{Spec} S.$$

Final Remark. If $\mathcal{S}$ is generated by $s_1, \ldots, s_n$, then U is open because it is the union of the open sets $\operatorname{Spec} R - V(s_i)$, where $V(s_i) = \{\mathfrak{q} \mid s_i \in \mathfrak{q}\}$.

93. Should be 86! To show that the map $f : \operatorname{Spec} S \to U$ in the previous exercise is a homeomorphism it remains to show it is continuous. But this is an immediate consequence of the fact that the map $f : \operatorname{Spec} S \to \operatorname{Spec} R$, $\mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p})$ is continuous for any ring homomorphism $\phi : R \to S$.

113. Should be 106! Write $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_n$ as a union of irreducible components. If Z is an irreducible component of $X \subset Y$, then $Z = (Z \cap Y_1) \cup \cdots \cup (Z \cap Y_n)$ expresses Z as a union of closed subsets so $Z = Z \cap Y_i$ for some i, whence $Z \subset Y_i$.

42. Should be 36! The best way to establish these isomorphisms is to use the universal property of $M \otimes_R N$.

This universal property of $M \otimes_R N$ (or, more accurately, of the pair $(M \otimes_R N, \lambda)$) can be stated as follows: there is an R-bilinear map $\lambda : M \times N \to M \otimes_R N$ such that for every R-module D the map

$$\begin{aligned} \operatorname{Hom}_R(M \otimes_R N, D) &\to \operatorname{Bilin}(M \times N, D) \\ \rho &\mapsto \rho \circ \lambda \end{aligned}$$

is bijective.

This property of $M \otimes_R N$ has the following consequence.

Lemma 0.1 *Suppose that D is a R-module and $\lambda' : M \times N \to D$ is an R-bilinear map with the property that for every R-module Q the map*

$$\begin{aligned} \mathrm{Hom}_R(D, Q) &\to \mathrm{Bilin}(M \times N, Q) \\ \nu &\mapsto \nu \circ \lambda' \end{aligned}$$

is bijective. Then there is a unique R-module homomorphism $\rho : M \otimes_R N \to D$ such that $\lambda' = \rho \circ \lambda$, and ρ is an isomorphism.

Proof. The existence of a R-module homomorphism $\rho : M \otimes_R N$ such that $\lambda' = \rho\lambda$ is guaranteed by the universal property for $(M \otimes_R N, \lambda)$.

Because of the universal property satisfied by (D, λ'), if we take $Q = M \otimes_R N$ there is a R-module homomorphism $\nu : D \to M \otimes_R N \to D$ such that $\lambda = \nu\lambda'$.

The R-module homomorphism $\nu\rho : M \otimes_R N \to M \otimes_R N$ has the property that $\nu\rho\lambda = \nu\lambda' = \lambda$. However, the identity map $\mathrm{id}_{M \otimes_R N}$ also has the property that $\mathrm{id}_{M \otimes_R N} \lambda = \lambda$ so, by the uniqueness clause in the universal property for $M \otimes_R N$ (applied with $D = M \otimes_R N$) $\nu\rho = \mathrm{id}\, M \otimes_R N$.

Repeating the argument in the previous paragraph for D in place of $M \otimes_R N$, we see that $\rho\nu = \mathrm{id}_D$. Hence ν is an isomorphism.

Finally, the uniqueness of the homomorphism ρ satisfying $\lambda' = \rho\lambda$ is ensured by the uniqeness clause in the universal property for $(M \otimes_R N, \lambda)$. □

It is pretty tedious establishing all the basic properties of $\otimes_R$ so I will only prove there is an isomorphism of R-modules

$$\Theta : \mathrm{Hom}_R(M \otimes_R N, D) \to \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, D))$$

given by

$$\Theta(f)(m)(n) = f(m \otimes n)$$

for $f \in \mathrm{Hom}_R(M \otimes_R N, D)$, $m \in M$, and $n \in N$. I really only care that Θ is an isomorphism of abelian groups, but it is no extra work to check that Θ is an R-module map.

First we define $\Psi : \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, D)) \to \mathrm{Bilin}(M \times N, D)$ by

$$\Psi(f)(m, n) = f(m)(n).$$

Since f is an R-module map $\Psi(f)(-, n) : M \to D$ is R-linear. Since $f(m)$ is an R-module map $\Psi(f)(m, -)$ is R-linear. It follows that $\Psi(f)$ is R-bilinear.

Define $\Phi : \mathrm{Bilin}(M \times N, D) \to \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, D))$ by

$$\Phi(\alpha)(m)(n) = \alpha(m, n).$$

Since $\alpha(m, -)$ is R-linear $\Phi(\alpha)(m)$ is an R-module map. Since $\alpha(-, n)$ is R-linear $\Phi(\alpha)$ is an R-module map. Hence $\Phi(\alpha) \in \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, D))$.

It is easy to check that Φ and Ψ are mutually inverse so

$$\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, D)) \cong \mathrm{Bilin}(M \times N, D) \cong \mathrm{Hom}_R(M \otimes_R N, D).$$

45. Should be 39! Let a and b be positive integers and $d = \gcd(a, b)$. To show that

$$\frac{\mathbb{Z}}{(a)} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{(b)} \cong \frac{\mathbb{Z}}{(d)}$$

we will show that the bilinear map

$$\lambda : \frac{\mathbb{Z}}{(a)} \times \frac{\mathbb{Z}}{(b)} \to \frac{\mathbb{Z}}{(d)}$$

defined by

$$\lambda(i, j) = \overline{ij}$$

has the appropriate universal property. Notice that λ is well-defined because d divides a and b. Let $\theta : \frac{\mathbb{Z}}{(a)} \times \frac{\mathbb{Z}}{(b)} \to M$ be a $\mathbb{Z}$-bilinear map. Define the R-module map

$$\rho : \frac{\mathbb{Z}}{(d)} \to M$$

by $\rho(1) = \theta(1, 1)$. To see that there really is an R-module map with this property we need only check that $d.\theta(1, 1) = 0$. This is true because there are integers u, v such that $d = au + bv$, whence

$$d.\theta(1, 1) = \theta(d, 1) = \theta(au + bv, 1) = \theta(bv, 1) = b\theta(v, 1) = \theta(v, b) = 0.$$

Now, using the bilinearity of θ twice,

$$\rho\lambda(i, j) = \rho(\overline{ij}) = ij\rho(1) = ij\theta(1, 1) = i\theta(1, j) = \theta(i, j)$$

whence $\rho\lambda = \theta$. Moreover ρ is the only R-module map such that $\rho\lambda = \theta$ because if $\rho'\lambda = \theta$ also then $\rho'(1) = \rho'\lambda(1, 1) = \theta(1, 1)$.

90. Should be 83!