1. Auxiliary result for DF7.4.32: (part of DF7.4.30 and DF7.4.31a) Let I be an ideal of the commutative ring R. Define
$$\operatorname{rad} I = \left\{ r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+ \right\}$$
called the *radical* of I. If $\operatorname{rad} I = I$ we call I a *radical ideal*. Prove that $\operatorname{rad} I$ is an ideal containing I, and that every prime ideal of R is a radical ideal.

   Proof. We have that $0 \in \operatorname{rad} I$ since $0^1 = 0 \in I$, so $\operatorname{rad} I$ is a nonempty subset of R. Furthermore, observe that any element $q \in I$ is in $\operatorname{rad} I$ since $q^1 \in I$; it follows that $I \subseteq \operatorname{rad} I$.

   Then for $r, s \in \operatorname{rad} I$, there exist $n, m \in \mathbb{Z}^+$ such that $r^n, s^m \in I$. Observe that $-s \in \operatorname{rad} I$ since $(-s)^m = \pm s^m \in I$ (the sign depending on the parity of m). Then $r - s \in \operatorname{rad} I$ since $(r-s)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} r^k (-s)^{n+m-k}$, and we may split the sum into $\sum_{k=0}^{n-1} \binom{n+m}{k} r^k (-s)^{n+m-k} + \sum_{k=n}^{n+m} \binom{n+m}{k} r^k (-s)^{n+m-k}$, which is a sum of elements in I since I is an ideal and in each sum the exponent on either r or s is sufficiently large to guarantee that each term is in I.

   We have that $rs \in \operatorname{rad} I$ since $(rs)^n m = (r^n)^m (s^m)^n \in I$ since I is an ideal; for any $p \in R$, we have that $pr \in \operatorname{rad} I$ since $(pr)^n = p^n r^n \in I$ since I is an ideal. Hence $\operatorname{rad} I$ is an ideal of R containing the ideal I.

   Let P be a prime ideal of R, and we show that $\operatorname{rad} P = P$. We already know that $P \subseteq \operatorname{rad} P$, so it is sufficient to show the reverse inclusion. Suppose $p \in \operatorname{rad} P$, so that $p^n \in P$ for some $n \in \mathbb{Z}^+$. Then $p^n = pp^{n-1} \in P$, so that either p or p^{n-1} is in P since P is a prime ideal. If $p \in P$ then we are done. If not, then repeat the process with p^{n-1} in place of p^n and keep repeating until eventually we find that $p \in P$ since n is finite. Since $p \in \operatorname{rad} P$ was arbitrary, it follows that $\operatorname{rad} P \subseteq P$ and so $\operatorname{rad} P = P$ for a prime ideal P of R. □

2. (DF7.4.32) Let I be an ideal of the commutative ring R and define $\operatorname{Jac} I$ to be the intersection of all maximal ideals of R that contain I where the convention is that $\operatorname{Jac} R = R$. (If I is the zero ideal, $\operatorname{Jac} 0$ is called the *Jacobson radical* of the ring R, so $\operatorname{Jac} I$ is the preimage in R of the Jacobson radical of R/I.)

   (a) Prove that $\operatorname{Jac} I$ is an ideal of R containing I.

   Proof. Observe that $0 \in \operatorname{Jac} I$ since 0 is in every ideal of R, and in particular, will be in every maximal ideal of R containing I. Hence $\operatorname{Jac} I$ is a nonempty subset of R. Furthermore, observe that $I \subseteq \operatorname{Jac} I$ since any element of I is contained in every maximal ideal containing I, meaning such an element is in $\operatorname{Jac} I$.

   Let $a, b \in \operatorname{Jac} I$. Then for any maximal ideal M containing I we have that $a, b \in M$ so that $a - b \in M$. Since M was an arbitrary maximal ideal M containing I it follows that $a - b \in \operatorname{Jac} I$. Similarly, $ab \in M$ and $ra \in M$ for any $r \in R$ so $ab, ra \in \operatorname{Jac} I$. Hence $\operatorname{Jac} I$ is an ideal of R containing I. □

   (b) Prove that $\operatorname{rad} I \subseteq \operatorname{Jac} I$, where $\operatorname{rad} I$ is the radical of I defined in Exercise 30.

   Proof. Suppose that M is any maximal ideal of R containing I. We show that $\operatorname{rad} I \subseteq M$. Let $r \in \operatorname{rad} I$, so that $r^n \in I$ for some $n \in \mathbb{Z}^+$. Since $I \subseteq M$, it follows that $r^n \in M$. Since r was arbitrary, $\operatorname{rad} I \subseteq \operatorname{rad} M$, and since M is a maximal (hence prime) ideal, $\operatorname{rad} I \subseteq \operatorname{rad} M = M$.

Since M was any maximal ideal of R containing I, it follows that $\operatorname{rad} I \subseteq \operatorname{Jac} I$. □

(c) Let $n > 1$ be an integer. Describe $\operatorname{Jac} n\mathbb{Z}$ in terms of the prime factorization of n.

For primes dividing n we have that $\operatorname{Jac} n\mathbb{Z}$ is given by the ideal generated by the product of each unique (up to associates) prime factor dividing n.

Proof. Let n have prime factorization $p_1^{e_1} \cdots p_s^{e_s}$. Observe that maximal ideals in $\mathbb{Z}$ are the prime ideals (p) for prime numbers p, and that $(n) \subseteq (p)$ if and only if $p \mid n$. It follows that the maximal ideals of $\mathbb{Z}$ containing (n) are the ideals (p_i) for $1 \leq i \leq s$. Hence $\operatorname{Jac} n\mathbb{Z}$ is the intersection of all such (p_i). But because the prime factors p_i of n are pairwise coprime (that is, for $i \neq j$ we have p_i, p_j coprime, and this implies that the set of primes p_i is coprime), it follows that $\operatorname{Jac} n\mathbb{Z} = \bigcap_{i=1}^{n} (p_i) = (p_1 \cdots p_n)$.

To see the last equality, take any two coprime elements $p, q \in \mathbb{Z}$ and we compute the intersection $(p) \cap (q)$ directly via basic number theory: an element $r \in R$ is in (p) if $p \mid r$, and is in (q) if $q \mid r$. So the coprime numbers p, q simultaneously divide r so that pq divides r. Hence $r \in (pq)$. Similarly, if $r \in (pq)$ then $pq \mid r$ and by transitivity of divisibility we have that $p \mid r$ and $q \mid r$. The last equality is the (finitely) repeated application of this fact. □

3. (DF9.1.3) If R is a commutative ring and $x_1, x_2, \ldots, x_n$ are independent variables over R, prove that $R[x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}]$ is isomorphic to $R[x_1, x_2, \ldots, x_n]$ for any permutation π of $\{1, 2, \ldots, n\}$.

Proof. Nonzero polynomials in $x_1, x_2, \ldots, x_n$ with coefficients in R are finite sums of nonzero monomial terms; that is, an element $p \in R[x_1, x_2, \ldots, x_n]$ is given by

$$p(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{N} a_i x_1^{d_{1i}} x_2^{d_{2i}} \cdots x_n^{d_{ni}}$$

where N depends on p, $a_i \in R$, and d_{ji} are nonnegative integers.

Consider the map ϕ from $R[x_1, x_2, \ldots, x_n]$ to $R[x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}]$ which permutes the indeterminates via π:

$$p(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{N} a_i x_1^{d_{1i}} x_2^{d_{2i}} \cdots x_n^{d_{ni}} \mapsto \sum_{i=1}^{N} a_i x_{\pi(1)}^{d_{1i}} x_{\pi(2)}^{d_{2i}} \cdots x_{\pi(n)}^{d_{ni}} = p(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}),$$

where $p(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$ is viewed as an element of $R[x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}]$

It is clear that for polynomials $p, q \in R[x_1, x_2, \ldots, x_n]$ that $\phi(p + q) = \phi(p) + \phi(q)$ and $\phi(pq) = \phi(p)\phi(q)$ since the operations of addition and multiplication are defined the same way, so that it did not matter when we relabeled the variables. Furthermore, the constant polynomial 1 is mapped to 1 since there was nothing to relabel. It follows that ϕ is a ring homomorphism.

We show that the kernel of this homomorphism is trivial: Suppose by way of contradiction that a nonzero polynomial p defined in the same way as above is sent to the zero polynomial under ϕ; that is, $\phi(p) = \sum_{i=1}^{N} a_i x_{\pi(1)}^{d_{1i}} x_{\pi(2)}^{d_{2i}} \cdots x_{\pi(n)}^{d_{ni}} = 0$. Since the d_{ji} are nonnegative integers, it follows that each a_i must all be zero, which is not possible since we chose p to be a nonzero polynomial. Hence ϕ has trivial kernel, meaning it is injective.

Take any polynomial $q \in R[x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}]$ given by $q(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)})$, and observe that q' given by $q'(x_1, x_2, \dots, x_n) = q(x_1, x_2, \dots, x_n)$ (so just viewing q as an element of $R[x_1, x_2, \dots, x_n]$), that $\phi(q') = q$ (by definition of ϕ, as $q(x_1, x_2, \dots, x_n) \mapsto q(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)})$). Hence ϕ is surjective since we can reverse the relabeling (since π is a permutation) and find preimages for every polynomial in $R[x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}]$ under ϕ.

It follows that ϕ is an isomorphism of rings, which yields the fact that $R[x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}]$ is isomorphic to $R[x_1, x_2, \dots, x_n]$ (for an arbitrary permutation π of $\{1, 2, \dots, n\}$). □

4. (DF9.1.5) Prove that (x, y) and $(2, x, y)$ are prime ideals in $\mathbb{Z}[x, y]$ but only the latter ideal is a maximal ideal.

Proof. An ideal I of R is prime if and only if R/I is an integral domain, and if R/I is a field it follows that I is a maximal ideal.

Consider the map sending a polynomial $p(x, y)$ to $p(0, 0)$ (evaluation at zero map from the polynomial ring to the integers). This is a homomorphism since $(p+q)(x, y) = p(x, y) + q(x, y)$ and $(pq)(x, y) = p(x, y)q(x, y)$ by definition, and it is surjective since we can put the constant term of some polynomial to be any any integer and so its image is the arbitrary integer. It follows that the kernel of this homomorphism is the ideal containing all polynomials in x, y which have 0 as the constant (degree zero) term. Hence the kernel is equal to $(x, y) = \{xp(x, y) + yq(x, y) \mid p, q \in \mathbb{Z}[x, y]\}$. We have that $\mathbb{Z}[x, y]/(x, y)$ is the set of all constant term (degree zero) polynomials in x and y, since in any polynomial in $\mathbb{Z}[x, y]$, any terms which contain powers of x or y are contained in the ideal (x, y). By the first isomorphism theorem the quotient ring is isomorphic to $\mathbb{Z}$, which is an integral domain, but not a field.

Similarly, consider the composition of the surjective homomorphism from the integers to $\mathbb{Z}/2\mathbb{Z}$ given by reduction modulo 2 with the evaluation at zero map from earlier; i.e., consider the (surjective) homomorphism from the polynomial ring to the integers modulo 2. The kernel of this composite map is the set of all polynomials whose constant term is a multiple of 2; the kernel is the ideal $(2, x, y)$ given by
$\{2r(x, y) + xp(x, y) + yq(x, y)) \mid r, p, q \in \mathbb{Z}[x, y]\}$. Hence $\mathbb{Z}[x, y]/(2, x, y)$ is the set of all degree zero terms with coefficents taken modulo 2; by the first isomorphism theorem this quotient ring is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is an integral domain but more importantly, a field.

It follows that (x, y) and $(2, x, y)$ are prime ideals in $\mathbb{Z}[x, y]$, but only $(2, x, y)$ is a maximal ideal. □

5. (DF9.1.17) An ideal I in $R[x_1, x_2, \dots, x_n]$ is called a *homogeneous ideal* if whenever $p \in I$ then each homogeneous component of p is also in I. Prove that an ideal is a homogeneous ideal if and only if it may be generated by homogeneous polynomials. [Use induction on degrees to show the "if" implication.]

Proof. Suppose that I is a homogeneous ideal, so that whenever $p \in I$ then each homogeneous component of p is also in I. For any element f of I with (arbitrary) degree d, we can write f uniquely as the sum of homogeneous components $f_0 + f_1 + \cdots + f_d$ (where f_k for $1 \leq k \leq d$ is the homogeneous component of degree k and some f_k may be zero). It follows from I being a homogeneous ideal that each of f_k are in I. Since f was an arbitrary polynomial in I, it follows that any polynomial in I may be written as the sum of homogeneous polynomials, which yields the fact that the ideal I is generated by homogeneous polynomials: We could give a generating set A to be the set of the homogeneous components of every polynomial in I, and so I would be contained in (A), and (A) is clearly contained in I since I is an ideal.

Conversely, suppose that an ideal I may be generated by homogeneous polynomials; that is, there is a generating set A (of homogeneous polynomials) such that $I = (A)$ and for any element $f \in I$ we may write f as a sum of elements in (A). We show that each homogeneous component of f is contained in I by induction.

Let $f = \sum_{i=1}^{N} p_i a_i$ for $a_i \in A$ and $p_i \in R[x_1, x_2, \ldots, x_n]$; each a_i is a homogeneous polynomial. We can expand each p_i uniquely into their sum of homogeneous components, so $p_i = p_{i0} + p_{i1} + \cdots + p_{i \deg p_i}$ where $\deg p_i$ is the degree of p_i, p_{ik} is the homogeneous component of p_i of degree k, and some of these terms may be zero. Then the summation for f becomes

$$f = \sum_{i=1}^{N} (p_{i0} + p_{i1} + \cdots + p_{i \deg p_i}) a_i = \sum_{i=1}^{N} (p_{i0} a_i + p_{i1} a_i + \cdots + p_{i \deg p_i} a_i),$$

and observe that every $p_{ik} a_i$ is a homogeneous polynomial of degree $k + \deg a_i$.

Since the sum is a finite sum, we can find the following: Let m be the minimal degree of the terms $p_{ik} a_i$ found in the sum. Then we can collect all such (homogeneous) polynomials $p_{ik} a_i$ of degree m in a summation A_m and it follows by the uniqueness of decomposition into homogeneous components that A_m is the homogeneous component of f (which may be zero). But A_m is given by a sum of elements of the form $p_{ik} a_i$, so that A_m is in $(A) = I$. It follows that the m-th degree homogeneous component of f is contained in I.

Suppose by induction that the j-th degree homogeneous component of f, given by A_j defined in a similar manner as to A_m, is in I. Then we argue that the $j+1$-th degree homogeneous component of f is contained in I in exactly the same manner. Collect the elements in the form $p_{ik} a_i$ of degree $j + 1$ and sum them up, call this sum A_{j+1}. It is clear that A_{j+1} is in $(A) = I$ so that by uniqueness of the homogeneous polynomial decomposition the $j + 1$-th homogeneous component of f is A_{j+1} and is contained in I. Hence by induction each of the homogeneous components of f are contained in I, and since f was arbitrary, I is a homogeneous ideal. □