Spring 2024: Math 791 Exam 2 Solutions

For this exam, you may use your notes, the Daily Summary, and any homework problem (giving complete details), but you may not consult **any other sources**, including: any algebra textbook, the internet, classmates or other students not in this class, or any professor except your Math 791 instructor. You may not cite any ring theoretic facts not covered in class or the homework. To receive full credit, all proofs must be complete and contain the appropriate amount of detail. **Please return a copy of your solutions to my mailbox in Snow 405 no later than 5pm on Monday, March 25**.

Each problem below is worth 10 points. Good luck on the exam!

1. Ideals I, J contained in the commutative ring R are said to be *comaximal* if $I + J = R$. Prove that if I and J are comaximal, then $IJ = I \cap J$ and $R/(I \cap J)$ is isomorphic to $(R/I) \times (R/J)$. Conclude that if R is a PID and $a, b \in R$ have no common divisor, then for all $c, d \in R$, the system of equations $x \equiv c \bmod aR$ and $x \equiv d \bmod bR$ has a solution.

Solution. For the first statement, it follows immediately from the definition of IJ that $IJ \subseteq I \cap J$, for any ideals $I, J \subseteq R$. If $I + J = R$, then $i + j = 1$, for some $i \in I$ and $j \in J$. Therefore, if $a \in I \cap J$, then $a = ai + aj$. But $ai + aj \in IJ$, so $a \in IJ$.

For the second statement, we define $\phi : R \to (R/I) \times (R/J)$ by $\phi(a) = (a+I, a+J)$, for all $a \in R$. It is straightforward to check that ϕ is a ring homomorphism. Moreover, $a \in R$ is in the kernel of ϕ if and only if $a + I = i$ and $a + J = J$ if and only if $a \in I \cap J$. Thus, the kernel of ϕ is $I \cap J$. If we show that ϕ is surjective, then $R/(I \cap J)$ is isomorphic to $(R/I) \times (R/J)$, by the first isomorphism theorem for rings.

Let $(b + I, c + J)$ be an element of $(R/I) \times (R/J)$. Then for $i + j = 1$ as above, we have $b = bi + bj$, so that $b + I = bj + I$. Similarly, $c = ci + cj$, so that $c + J = ci + J$. Thus,

$$\phi(bj + ci) = (bj + ci + I, bj + ci + J) = (bj + I, ci + J) = (b + I, c + J),$$

showing that ϕ is surjective. □

For the final statement, if R is a PID and $a, b \in R$ have not common factor, then the ideals aR and bR are comaximal. Thus, the map $\phi : R \to (R/aR) \times (R/bR)$ is surjective. If $\phi(r) = (c+I, d+I)$, then $r \equiv c \bmod aR$ and $r \equiv d \bmod dR$, so that r is a solution to the given set of equations. □

2. Let R be a commutative ring. The *nilradical* of R is the set $\text{nilrad}(R) := \{a \in R \mid a^n = 0, \text{ for some } n \geq 1\}$. The elements of $\text{nilrad}(R)$ are the *nilpotent* elements of R. Prove:

(i) Show that $\text{nilrad}(R)$ is an ideal of R that is contained in every prime ideal of R. See Homework 20 for the definition of a prime ideal.

(ii) Suppose $c \in R$ is not nilpotent and consider the set $S := \{1, c, c^2, \dots, \}$. Use Zorn's lemma to show that there exists an ideal P maximal with respect to the property that $P \cap S = \emptyset$.

(iii) Show that P from part (ii) is a prime ideal. Hint: If $ab \in P$ and $a \notin P$ and $b \notin P$, consider the ideals $P + aR$ and $P + bR$.

(iv) Conclude that the nilradical of a commutative ring is the intersection of all prime ideals in R.

Solution. For (i), suppose a, b are nilpotent, say $a^n = 0 = b^m$. Then

$$(a + b)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n + m - 1 - i}{i} a^{n+m-1-i} b^i.$$

Here $\binom{n+m-1-i}{i}$ means 1_R added to itself $\binom{n+m-1-i}{i}$ times. In each term $a^{n+m-1-i}b^i$, either $n + m - 1 - i \geq n$ or $i \geq m$, and thus, each of these terms equals zero. Therefore $a + b$ is nilpotent. In addition, suppose $r \in R$. Then $(ra)^n = r^n a^n = 0$, so ra is nilpotent. Thus, the nilradical of R is an ideal. Moreover, if a is in the nilradical of R, and $P \subseteq R$ is a prime ideal then $a^n = 0 \in P$, for some $n \geq 1$. An easy induction shows that if $c^n \in P$, then $c \in P$. Thus, $a \in P$, so that the nilradical of R is contained in every prime ideal $P \subseteq R$.

For (ii), Let X denote the set of ideals J contained in R such that $J \cap S = \emptyset$. Note that X is non-empty since $\langle 0 \rangle \cap S = \emptyset$. If we partially order X by inclusion, we obtain a partially ordered set. Let $C = \{J_\alpha\}_{\alpha \in A}$ be a chain in X. We have seen in class that $J_0 = \bigcup_\alpha J_\alpha$ is an ideal of R. Moreover, $J_0 \cap S = \emptyset$, since $J_\alpha \cap S = \emptyset$, for any element in the chain. Thus $J_0 \in X$ and J_0 is clearly an upper bound for C. Thus, by Zorns Lemma, there exists an ideal $P \subseteq R$ maximal with respect to the property that $P \cap S = \emptyset$.

For (iii), suppose $\in P$, yet neither a nor b belongs to P. Then $P + \langle a \rangle$ and $P + \langle b \rangle$ both properly contain P. By the maximality of P, neither of these ideals belong to X. Thus, $(P + \langle a \rangle) \cap S \neq \emptyset$ and $(P + \langle b \rangle) \cap S \neq \emptyset$. We therefore have equations $c^r = p_1 + r_1 a$ and $c^t = p_2 + r_2 b$, for $c^r, c^t \notin P$ and $p_i \in P$ and $r_i \in R$. Therefore

$$c^r c^t = p_1 p_2 + ab(r_1 p_2 + r_2 p_1) + r_1 r_2 ab.$$

But the left hand side of this equation belongs to S and the right hand side belongs to P, contradiction. Therefore, either $a \in P$ or $b \in P$, and thus P is a prime ideal.

For (iv), part (iii) shows that if $c \in R$ is not nilpotent, then there exists a prime ideal $P \subseteq R$ not containing c. Thus the intersection of all prime ideals in R is contained in the nilradical, and hence by part (i), equals the nilradical of R. □

3. Let R be an integral domain. In what follows, $a, b, c, d \in R$ will be non-zero, non-unit elements. Given $a, b \in R$, $d \in R$ is said to be a *greatest common divisor*, or GCD, of a and b if the following conditions hold:

(i) $d \mid a$ and $d \mid b$
(ii) Whenever $e \mid a$ and $e \mid b$, then $e \mid d$.

Use this definition to prove the following statements. GCDs are assumed to exist for any pair of non-zero, non-units.

(i) GCDs are unique up to a unit multiple. Henceforth, we will refer to *the* GCD of a and b.
(ii) Show that dc is the GCD of ac and bc, for d the GCD of a and b. Use this to show that if d is the GCD of a and b, then 1 is the GCD of $\frac{a}{d}$ and $\frac{b}{d}$.
(iii) Prove that if the GCD of a and b is 1 and $a \mid bc$, then $a \mid c$.

Solution. For (i), if d and d' are GCDs of A and b, then $d \mid d'$ and $d' \mid d$, so d and d' are associates.

For the first statement in (ii), let $e = \mathrm{GCD}(ac, bc)$. Then $c \mid ac$ and $c \mid bc$, so $c \mid e$. Thus, $e = cd$, for some $d \in R$. Write $ac = eu$ and $bc = ev$. Then $ac = dcu$, so $a = du$. Similarly, $b = dv$. Thus, $d \mid a$ and $d \mid b$. Now suppose $f \mid a$ and $f \mid b$. Then $fc \mid ac$ and $fc \mid bc$, therefore, $fc \mid e$. Since $e = dc$, we have $f \mid d$. Thus, d is the GCD of a and b, which gives what we want.

For the second statement in (ii), we have

$$d = \mathrm{GCD}(a, b) = \mathrm{GCD}(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}) = d \cdot \mathrm{GCD}(\frac{a}{d}, \frac{b}{d}).$$

Dividing both sides of this last equation by d gives what we want.

For (iii), $c = c \cdot 1 = c \cdot \mathrm{GCD}(a, b) = \mathrm{GCD}(ac, bc)$. But $a \mid ac$ and $a \mid bc$, so $a \mid \mathrm{GCD}(ac, ab) = c$, which is what we want. □

4. Suppose R is a UFD. Show that the GCD of any two non-zero, non-unit elements exists.[1] Then define the concept of least common multiple and conclude that for non-zero, non-units $a, b \in R$, $\mathrm{GCD}(a, b) \cdot \mathrm{LCM}(a, b) = ab$.

First, let $a, b \in R$ be non-zero non-units. Factoring each of these elements into a product of primes, we may write $a = up_1^{e_1} \cdots p_r^{e_r}$ and $b = vp_1^{f_1} \cdots p_r^{f_r}$, where each p_j is prime, u and v are units, and $e_i, f_i \geq 0$. Thus for example, if $p_c \nmid a$, then $e_c = 0$. Set $d := p_1^{\min\{e_1, f_1\}} \cdots p_r^{\min\{e_r, f_r\}}$, so that $d \mid a$ and $d \mid b$. Note, if each $\min\{e_i, f_i\} = 0$, then we take $d = 1$. We now show that d is a GCD of a and b. For this, we have to show that if c divides both a and b, then c divides d. Suppose c is such an element. We can write $a = ch$ and $b = ck$, for $k, h \in R$. Let $\tilde{u} q_1^{g_1} \cdots q_t^{g_t}$ be a prime factorization of c, where $\tilde{u}$ is a unit. Then, $up_1^{e_1} \cdots p_r^{e_r} = \tilde{u} q_1^{g_1} \cdots q_t^{g_t} \cdot h$. By uniqueness of factorization, each q_j must be a unit multiple of some p_i and $g_j \leq e_i$. By reindexing the q_j's we may assume $q_i = u_i p_i$, for $1 \leq i \leq t$, and thus $g_i \leq e_i$, for $1 \leq i \leq t$. Since $c \mid b$, each $g_i \leq f_i$. It follows that each $g_i \leq \min\{e_i, f_i\}$, and thus $c \mid d$, which is what we want.

To define the LCM of a and b in a way that is analogous to the definition of GCD in Homework 17, we say that h is an LCM of a, b if: (i) $a \mid h$ and $b \mid h$ and (ii) If $a \mid k$ and $b \mid k$, then $h \mid k$. Essentially the same proof in the paragraph above shows that $h := p_1^{\max\{e_1, f_1\}} \cdots p_r^{\max\{e_r, f_r\}}$ is an LCM of a and b. Part (iii) now follows from (i) and (ii) since $p_i^{\min\{e_i, f_i\} + \max\{e_i, f_i\}} = p_i^{e_i + f_i}$, for all i. □

5. Let R be a commutative ring. Describe with proof the two-sided ideals in $S := \mathrm{M}_n(R)$. Hint: Consider the matrices E_{ij} that have 1 in the (i, j)-entry and zeros elsewhere.

Solution. We show that J is a two-sided ideal of R if and only if there is an ideal $I \subseteq S$ such that $J = \mathrm{M}_n(I)$. If $J = \mathrm{M}_n(I)$ for some two-sided ideal $I \subseteq S$, then clearly J is a two-sided ideal of R, since for any $A \in R$ and $B, C \in J$, the entries of AB, BA and $B + C$ belong to I. For the converse, suppose $J \subseteq R$ is a two-sided ideal. Let I denote

[1] Interesting example: Let A denote the set of all polynomials in $\mathbb{Q}[x]$ whose constant term is in $\mathbb{Z}$. Then any two non-zero, non-units in A have a GCD, but A is *not* a UFD.

the set of elements $a \in R$ such that a is an entry of a matrix belonging to J. We need to show that I is a two-sided ideal of R and $\mathrm{M}_n(I) = J$.

We first make some observations. We let E_{ij} be the matrix with 1 in the (i,j) entry and zeros elsewhere. It is easy to check that $E_{ij} \cdot E_{kt} = 0$, if $j \neq k$ and $E_{ij} \cdot E_{kt} = E_{it}$ when $j = k$. Now, for any $A \in R$, $E_{ij}A$ is the matrix whose ith row is the jth row of A, and all other rows are zero. In other words, $E_{ij}A = a_{j1}E_{i1} + \cdots + a_{jn} \cdot E_{in}$. Thus, $E_{ij}AE_{kt} = a_{jk} \cdot E_{it}$, which belongs to J, if $A \in J$.

Suppose $a \in I$. Then a is the (i,j)th entry of a matrix A in J, and thus, $a_{ij}E_{ij} = E_{ii}AE_{jj}$ belongs to J. Thus, for any $r \in S$, $rE_{ii} \cdot aE_{ij} = raE_{ij}$ and $aE_{ij} \cdot rE_{jj} = arE_{ij}$ belong to J, and therefore $ra \in I$ and $ar \in I$.

Now suppose $a, b \in I$. Then by what we have previously shown, aE_{uv} and bE_{st} belong to J, for some u, v, s, t. Thus, $bE_{st} \cdot E_{tv} = bE_{sv} \in J$. Therefore $E_{us} \cdot bE_{sv} = bE_{uv}$ belongs to J, and thus $(a+b)E_{uv}$ is in J. Therefore $a + b \in I$, so I is a two-sided ideal of R.

To finish the proof, we first note that by definition $J \subseteq \mathrm{M}_n(I)$. For the converse, suppose $B = (b_{ij}) \in \mathrm{M}_n(I)$. Then, for each (i,j) there exists a matrix A_{ij} with b_{ij} as an entry, say, the (u,v)th entry. Then $E_{iu}AE_{vj} = b_{ij}E_{ij} \in J$. It follows that $B = \Sigma_{i,j} b_{ij}E_{ij} \in J$. Thus, $J = \mathrm{M}_n(I)$, which completes the proof. □

6. Show that any UFD satisfies the ascending chain condition on principal ideals.

Solution. Suppose $a, b \in R$ are non-zero, non-units and $\langle a \rangle \subsetneq \langle b \rangle$. Write $a = up_1^{e_1} \cdots p_r^{e_r}$, with each p_i prime, $e_i \geq 1$ and u a unit. Then we have $a = bc$, with c not a unit. It follows that we may assume $b = vp_1^{f_1} \cdots p_r^{f_r}$, with each $f_i \leq e_i$ and strict inequality for at least one i, and v a unit. It follows that there cannot be a chain of principal ideals above $\langle a \rangle$ with more than $e_1 + \cdots + e_r$ strict containments. This implies that R satisfies the ascending chain condition on principal ideals. □

7. Consider the sequence of polynomial rings $\mathbb{Q}[x] \subseteq \mathbb{Q}[x^{\frac{1}{2}}] \subseteq \mathbb{Q}[x^{\frac{1}{4}}] \subseteq \cdots$ and set $R := \bigcup_{n \geq 1} \mathbb{Q}[x^{\frac{1}{2^n}}]$. Prove that if $f \in R$ and the constant term of f is 0, then f is not an irreducible element in the integral domain R. Conclude that no element in R with zero constant term can be written as a product of irreducible elements.

Solution. If for each $n \geq 0$, we set $R_n := \mathbb{Q}[x^{\frac{1}{2^n}}]$, then we have $R_0 \subseteq R_1 \subseteq \cdots$ and $R = \bigcup_{n \geq 0} R_n$. We first note that the reason the conclusion works is that even $x = x^{\frac{1}{2}} \cdot x^{\frac{1}{2}}$ is not irreducible. But then the same applies to all powers $x^{\frac{1}{2^n}}$ of x.

Now, take $f \in R$. Then $f \in R_n$, for some n, so we may write f as a polynomial in $x^{\frac{1}{2^n}}$ with coefficients in $\mathbb{Q}$. If f has zero constant term, then $f = a_r x^{\frac{r}{2^n}} + a_{r-1} x^{\frac{r-1}{2^n}} + \cdots + a_1 x^{\frac{1}{2^n}}$, with each $a_j \in \mathbb{Q}$. Now, for $1 \leq t \leq r$, $x^{\frac{t}{2^n}} = x^{\frac{1}{2^{n+1}}} \cdot x^{\frac{2t-1}{2^{n+1}}}$. Thus, we may factor $x^{\frac{1}{2^{n+1}}}$ from each term and write $f = x^{\frac{1}{2^{n+1}}} \cdot g$ for some $g \in R_{n+1} \subseteq R$ with zero constant term. Note that g is not a unit in R, else there exists $h \in R$ such that $gh = 1$. However, $h \in R_s$, for some $s \geq 1$, so that if $q \geq \max(s, n+1)$, then $g, h \in R_q$ and $1 = hg$ in R_q. But R_q is a polynomial ring in the variable $x^{\frac{1}{2^q}}$, so the only units in R_q are constants. Thus g is not a unit in R, so that no $f \in R$ with constant term 0 is irreducible.

The second statement now follows immediately from the first, since the only possible irreducible elements in R have non-zero constant term, and the product of elements in R with non-zero constant term has non-zero constant term. □

8. This problem is a generalization of problem 1 on Homework 16. Here we create a ring of fractions when the ring we start with is not necessarily an integral domain. Let R be a commutative ring and $S \subseteq R$ a multiplicatively closed set, i.e., $1 \in S$, $0 \notin S$ and $s_1 s_2 \in S$, whenever $s_1, s_2 \in S$. Let Q denote the set of ordered pairs $(a, s) \in R \times S$. Define $(a, s) \sim (a', s')$ if and only of there exists $s_0 \in S$ such that $s_0(as' - a's) = 0$.

(i) Show that $\sim$ is an equivalence relation. Denote the equivalence class of (a, s) by a/s.
(ii) Define $a/b + c/d := (ad + bc)/bd$ and $a/b \cdot c/d := ac/bd$. Prove that these operations are well-defined, and then show that R_S, the set of equivalence classes, forms a commutative ring. R_S is often called R *localized at* S.
(iii) Show that the natural map $\phi : R \to R_S$ given by $\phi(r) = r/1$ is a ring homomorphism, and then describe the kernel of ϕ.
(iv) Give an example such that the map $\phi : R \to R_S$ in part (iii) has non-zero kernel.
(v) What are the units in R_S?

Solution. For (i), the relation is clearly reflexive and symmetric. Suppose $(a, s) \sim (a_1, s_1) \sim (a_2, s_2)$. Then there exists $s', s'' \in S$ such that $s'(as_1 - a_1 s) = 0$ and $s''(a_1 s_2 - a_2 s_1) = 0$. Multiplying the first equation by $s''s_2$ and the second equation by $s's$ and adding gives: $s''s_1 s'(as_2 - a_2 s) = 0$, showing $(a, s) \sim (a_2, s_2)$.

For (ii) we just show addition is well defined. The proof that multiplication is well defined is similar, and that we have a commutative. ring follows easily from the fact that R is a commutative ring. Suppose $a/b = a'/b'$ and $c/d = c'/d'$. Then there exist $s, s' \in S$ such that $s(ab' - a'b) = 0$ and $s'(cd' - c'd) = 0$. Multiplying the first equation by $s'dd'$ and the second equation by sbb', and adding gives $ss'\{(dd'ab' + cd'bb') - (dd'a'b + c'dbb')\} = 0$, which shows that $(ad + bc)/bd = (a'd' + b'c')b'd'$, which is what we want.

For (iii),that ϕ is a ring homomorphism follows easily from the definitions. Now $r \in R$ belongs to the kernel of ϕ if and only if $r/1 = 0/1$ in R_S if and only if $s(r \cdot 1 - 0 \cdot 1) = 0$ for some $s \in R$ if and only if $sr = 0$, for some $s \in S$.

For (iv) consider $R = \mathbb{Z}/6\mathbb{Z}$ and $S = \{0, \overline{1}, \overline{2}, \overline{2^2}, ...\} = \{\overline{1}, \overline{2}\}$. Then $\overline{2} \cdot \overline{3} = \overline{0}$ in R, showing that $\overline{3}$ is in the kernel of ϕ, for ϕ as in (iii).

For (v), we note that $a/s \in R_S$ is a unit if and only if $a/1$ is a unit. Thus, we determine when $a/1$ is a unit. We claim $a/1$ is a unit in R_S if and only if there exist $b \in R$ and $s \in S$ such that $sba \in S$. To see this, suppose $a/1 \in R_S$ is a unit. Then there exists $b/s_1 \in R_S$ such that $(a/1) \cdot (b/s_1) = 1/1$. Thus there exists $s \in S$ such that $s(ab - s_1) = 0$. It follows that there exists $s \in S$ and $b \in R$ such that $sba \in S$. The converse is similar. □

9. Let R be a UFD with quotient field K. Suppose $S \subseteq R$ is multiplicatively closed. Show that R_S is a UFD.

Solution. We first note that since R is an integral domain, $a/s = b/s'$ in R_S if and only if $s'a = sb$ in R. Now note that since any element in R is a product of prime elements, and any element in R_S is a unit times $a/1$, for $a \in R$, it suffices to show that if $p \in R$ is a prime element, and p does not divide any element in S, then $p/1$ is a prime element in R_S. (Note: If $p \mid s$, for $s \in S$, then s is a unit in R_S, and therefore, p is a unit in R_S). For this, suppose $p/1$ divides $(a/s) \cdot (b/s')$ in R_S. Then $(p/1) \cdot (c/s_1) = (a/s) \cdot (b/s')$ in R_S. Thus, in R, $pcss' = abs_1$, so that p divides abs_1s_2. Since $s_1s_2 \in S$, $p \nmid s_1s_2$ so $p \mid a$ or $p \mid b$, say $a = pc$, for $c \in R$. Then $a/s = (p/1) \cdot (c/s)$ showing that $p/1$ divides a/s in R_S, so $p/1$ is a prime element. □

10. Let k be a field and set $R := k[[x]]$, the formal power series ring in x over k. Using the definition given in Homework 18, show that R is a discrete valuation ring with quotient field K, where K can be identified with the set of all formal expressions, $\sum_{n=-n_0}^{\infty} \alpha_n x^n$, where $n_0 \geq 0$ and each $\alpha_n \in k$. Such an expression is called a *Laurent power series*. Hint: Show that $f(x) \in R$ is a unit if and only if its constant term is non-zero.

Solution. Suppose $f(x) = \sum_{n=0}^{\infty} a_n x^n$ in R is a unit. Then there exists $g = \sum_{n=0}^{\infty} b_n x^n$ such that $fg = 1$. In particular, $a_0b_0 = 1$, so $a_0 \neq 0$. Now suppose $a_0 \neq 0$. We seek $g = \sum_{n=0}^{\infty} b_n x^n$ such that $fg = 1$. Such an element exists, if and only if we can solve the following infinite system of equations over k, thinking of the b_i as elements to be determined.

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ &\vdots \\ a_0b_n + \cdots + a_nb_0 &= 0 \\ &\vdots \end{aligned}$$

Since a_0 is not zero, we can solve the first equation for b_0, i.e., we can take $b_0 = a_0^{-1}$, since k is a field. Since $b_0 = a_0^{-1}$, if we use this in the second equation, we see that we can solve for b_1, as an element in k. Assume by induction, that we have determined $b_0, \ldots, b_{n-1}$ from the first n equations. Then from $a_0b_n + \cdots + a_nb_0 = 0$, we can solve for b_n. Thus, the system of equations above has a solution in k, so that f has an inverse in R.

We next note that for $f \in R$, $x \mid f$ if and only if the constant term of f is zero, which by what we have just shown, happens if and only if f is not a unit. So, if $x \mid fg$, for $f, g \in R$, one of f or g is not a unit, and thus has zero constant term, and thus $x \mid f$ or $x \mid g$. Therefore x is a prime element. Moreover, if $f \in R$ and $f = \sum_{n=1}^{\infty} a_n x^n$, let n_0 be the least non-negative integer such that $a_{n_0} \neq 0$. Therefore, we can write $f = ux^{n_0}$, with $u \in R$ a unit (since the constant term of u is a_{n_0}). This shows that, up to a unit multiple, x is the only prime element in R. Moreover, if $I \subseteq R$ is a non-zero proper ideal, then, every element in I has the form vx^n, for a unit $v \in R$ and $n \geq 1$. If we take g such that n is least among the elements of I, then $\langle g \rangle = I$, showing that R is a PID and therefore a DVR.

Now, suppose $a/b \in K$, with $a, b \in R$. Then $a = ux^r$ abd $b = vx^s$, with $u, v \in R$ units, and $r, s \geq 0$. Then $a/b = uv^{-1}x^{r-s}$. Write $uv^{-1} = h(x) = \sum_{n=0}^{\infty} h_n x^n$ as an element of R, so that

$$a/b = x^{r-s} \cdot h(x) = \sum_{n=0}^{\infty} h_n x^{n+r-s} = \sum_{n=r-s}^{\infty} h'_n x^n,$$

where each $h'_n = h_{n-(r-s)}$. Thus, every element in K is a Laurent power series. Conversely, any Laurent series $f = \sum_{n=-n_0}^{\infty} \alpha_n x^n$, where $n_0 \geq 0$ can be written as $f = x^{-n_0}u$, where $u \in R$ is a unit (and we assume a_{-n_0} is the first non-zero coefficient of f). Thus, $f \in K$, so that K is the set of Laurent power series. □

Bonus Problems. Five points each. Bonus problems must be almost completely correct to receive any bonus points.

BP1. Suppose R is an integral domain and $S \subseteq R$ is a multiplicatively closed set such that each element in S is a finite product of primes. Let T denote the set of prime factors of the elements of S and assume further that no element of R is divisible by infinitely many elements in T. Prove that R is a UFD if R_S is a UFD.

Solution. This problem is a converse to Problem 9. The difficulty in reversing the direction of the argument in Problem 9 above is the following. If $q \in R$ is such that $q/1$ is a prime element in R_S, then q need not be a prime element in R. For example, if $R = \mathbb{Z}$ and $S := \{1, 2, 2^2, 2^3, \ldots\}$, then 6 is a prime element in R_S, but it is not prime in R. The point is, that given such a q, we need to factor out all of the elements from S (or prime factors of elements of S) that are factors of q and this requires some sort of finiteness condition. So, assume that no element in R is divisible by infinitely many p in T. Let $q \in R$ be such that $q/1$ is a prime element in R_S. Choose the principal ideal $\langle p \rangle$ so that p is not divisible by any $p_i \in T$ and $\langle q/1 \rangle = \langle p/1 \rangle$ in R_S. This is possible once we divide out from q the finitely many $p_i \in T$ that might be factors of q. We now note that p is a prime element in R. Suppose $p|ab$, for $a, b \in R$. Then since $p/1$ is a unit multiple of $q/1$ in R_S and $q/1$ is a prime element, $p/1$ is a prime element in R_S. Thus, $p/1$ divides $a/1$ (say). Thus, in R, we have an equation $sa = pr$, for $r \in R$ and $s \in S$. Now, let p_i be a prime factor of s. If p_i divides p, then p_i divides q, which is not the case, since we have removed all such p_i to obtain p. Thus, p_i divides r. Similarly, every prime element in T that divides s divides r, so s divides r. Cancelling s from the equation $sa = pr$, we get $a = pr'$, for some $r' \in R$, which shows that p divides a. Thus, p is a prime element of R. Now, suppose $a \in R$ is a non-zero, non-unit element. By hypothesis, a is divisible by at most finitely many primes in T, say $a = a_0 b$, where a_0 is a product of primes from T and no prime in T divides b. In R_S, we can write $b/1$ as $uq_1/1 \cdots q_h/1$, where $u \in R_S$ is a unit and each $q_i/1$ is a prime in R_S. From the preceding, we may write each $q_i/1 = t_i \cdot (p_i/1)$, where $p_i \in R$ is prime, and $t_i \in R_S$ is a unit. Thus, gathering units, we have $b/1 = v \cdot (p_1/1) \cdots (p_h/1)$ in R_S, where $v \in R_S$ is a unit. Thus, $v = s/s'$, with $s, s' \in T$. Therefore, in R, $s'b = sp_1 \cdots p_h$. Since no prime factor of s' divides any p_i, all of the prime factors of s' divide s. Thus, we may cancel s' from both sides of this last equation to obtain $b = s''p_1 \cdots p_h$, showing that b is a product of primes. It follows that a is a product of primes, and therefore, R is a UFD. □

BP2. Let k be a field and R the polynomial ring in countably many variables over k. Prove that R is a UFD.

Solution. Set $R_0 := K$ and $R_n = K[x_1, \ldots, x_n]$, for all $n \geq 1$. By induction on n, and the theorem from class, each R_n is a UFD, since $R_{n+1} = R_n[x_{n+1}]$. We also have $R = \bigcup_{n \geq 1} R_n$. We make the following claim. If $p \in R_n$ is a prime (equivalently, irreducible) element, then p is a prime element in R. Assuming this holds, let $f \in R$ be a non-zero, non-unit element. Then $f \in R_n$ for some n. Thus, in R_n, $f = p_1 \cdots p_r$, a product of prime elements in R_n. By the claim, each p_i remains prime in R. Therefore, f is a product of primes in R, showing that R is a UFD.

Suppose $p \in R_n$ is prime and $p \mid ab$, for $a, b \in R$. Thus, $ab = pc$, for $c \in R$. We may choose m sufficiently larger than n so that $p, a, b, c \in R_m$. By a theorem from class, p is prime in $R_n[x_{n+1}]$. Iterating this, p is prime in $R_n[x_{n+1}, x_{n+2}]$. Inductively, we have that p is prime in $R_n[x_{n+1}, \ldots, x_m] = R_m$. In R_m we have $ab = pc$, so $p \mid a$ or $p \mid b$ in R_m, say $p \mid a$. But then clearly, $p \mid a$ in R, showing p is prime in R, which completes the proof. □

BP3. Let R be a commutative ring and $f(x) \in R[x]$. Show that $f(x)$ is a unit in $R[x]$ if and only if its constant term is a unit and all other coefficients of $f(x)$ are nilpotent. Hint: In any commutative ring, what sort of element is $n + u$, if n is nilpotent and u is a unit?

Solution. We first note that if A is a commutative ring and $n \in A$ is nilpotent and $u \in A$ is a unit, then $n+u$ is a unit. One way to see this is to note that if M is a maximal ideal, then M is a prime ideal, and thus by Problem 2, $n \in M$. If $n + u \in M$, then $u \in M$. But this is a contradiction, since no proper ideal contains a unit. Thus, $n + u$ is not contained in any maximal ideal, and therefore must be a unit. More computationally: First consider $n + 1$. Suppose $n^r = 0$. Without loss of generality, we may assume r is odd. Then $1 = 1 + n^r = (1 + n)(1 - n + n^2 - \cdots + n^{r-1})$, showing that $1 + n$ is a unit. To see that $u + n$ is a unit, note that $u^{-1}n$ is nilpotent and therefore, $1 + (u^{-1}n)$ is a unit. Therefore, $u \cdot (1 + (u^{-1}n)) = u + n$ is a unit.

Now, we write $f(x) = a_n x^n + \cdots + a_0$. Suppose a_0 is a unit and a_i is nilpotent for all remaining coefficients. Then for each $i \geq 1$, $a_i x^i$ is nilpotent, and therefore $a_n x^n + \cdots + a_1 x$ is nilpotent. By the paragraph above, $f(x)$ is a unit.

For the converse, we prove by induction on n that if $f(x)$ is a unit in R then a_0 is a unit and each a_i is nilpotent for $1 \leq i \leq n$. If $n = 0$, there is nothing to prove. Suppose $f(x)$ is a unit. Then there exists $g(x) = b_m x^m + \cdots + b_0$ such

that $f(x)g(x) = 1$. It follows that $a_0b_0 = 1$, so a_0 is a unit. We now look at the resulting system of equations:

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ &\vdots \\ a_nb_{m-2} + a_{n-1}b_{m-1} + a_{n-2}b_m &= 0 \\ a_nb_{m-1} + a_{n-1}b_m &= 0 \\ a_nb_m &= 0. \end{aligned}$$

If we multiply the second to last equation by a_n, we get $0 = a_n^2b_{m-1} + a_{n-1}a_nb_m = a_n^2b_{m-1}$. If we now multiply the third from last equation by a_n^2, we get

$$0 = a_n^3b_{m-2} + a_{n-1}a_n^2b_{m-1} + a_{n-1}a_n^2b_m = a_n^3b_{m-2}.$$

Thus, inductively we have $a^jb_{m-j+1} = 0$, for all j. It follows that $a_n^{m+1}b_0 = 0$. Since b_0 is a unit, a_n is nilpotent. Therefore $-a_nx^n$ is nilpotent. Since $f(x)$ is a unit, $f(x)+(-a_nx^n)$ is a unit. By induction, $a_1, \ldots, a_{n-1}$ are nilpotent, which is what we want.

Here's a more conceptual proof of this last fact. Suppose $f(x) \in R[x]$ is a unit. Clearly the constant term of $f(x)$ is a unit in R. Let $P \subseteq R$ be a prime ideal. From Homeworks 19 and 20, $R[x]/P[x]$ is isomorphic to $(R/P)[x]$, and hence an integral domain. Now, $\overline{f(x)}$, the image of $f(x)$ in $R[x]/P[x]$, is still a unit. But in an integral domain, a unit clearly has degree zero. Thus, all of the non-constant coefficients of $\overline{f(x)}$ are zero in R/P, and therefore, all of the non-constant coefficients of $f(x)$ belong to P. Since this holds for all prime ideals $P \subseteq R$, these coefficient are nilpotent, by Problem 2. □

BP4. Let R be the ring in problem 7 and $S \subseteq R$ be the multiplicatively closed set of polynomials with non-zero constant term. Prove that the ring R_S has no irreducible elements.

Solution. If $\frac{f}{s} \in R_S$ is non-zero and a non-unit, then $f \in R$ has constant term 0. Since s is a unit in R_S, $\frac{f}{s}$ is irreducible if and only if $\frac{f}{1}$ is irreducible. By Problem 7, f is not irreducible in R, in fact, $f = x^{\frac{1}{2^n}} \cdot g$, with $g \in R$ having constant term 0 and some $n \geq 1$. Thus, $\frac{f}{1} = \frac{x^{\frac{1}{2^n}}}{1} \cdot \frac{g}{1}$, showing that $\frac{f}{1}$ is not irreducible in R_S. □

Aside. In the literature, irreducible elements are sometimes called *atoms*, for obvious reasons. An integral domain in which each non-zero, non-unit be factored (not necessarily uniquely) as a product of a finite number of atoms (irreducible elements) is called an *atomic domain*. An integral domain without any atoms is then called an *anti-matter* integral domain. Thus, the ring R_S in BP4 is an anti-matter integral domain. This latter designation has absolutely nothing to do with physics, but was probably coined for the amusement of mathematicians who study such rings.