# SPRING 2023: MATH 791 EXAM 2 SOLUTIONS

For this exam, you may use your notes, the Daily Summary, and any homework you have done, but you may not consult any other sources, including, any algebra textbook, the internet, any fellow graduate students, or any professor except your Math 791 instructor. You may not cite without proof any facts not covered in class or the homework. Please upload a pdf copy of your solutions to Canvas no later than 5pm on Monday, March 27.

Each problem is worth 10 points. To receive full credit, all proofs must be complete and contain the appropriate amount of detail. All rings in this exam are **commutative rings**. Good luck on the exam!

1. Use the division algorithm to give a direct proof that if $F$ is a field, then $F[x]$ is a UFD, without first showing $F[x]$ is. PID.

Solution. For the existence of factorizations, we want to show every non-zero, non-constant polynomial is a product of irreducible polynomials. Suppose this fails. We let $T$ denote the set of non-constant polynomials that cannot be factored as a product of irreducible polynomials and let $X$ denote the set of degrees of the polynomials in $T$. If $T \neq \emptyset$, then $X \neq \emptyset$. By the Well ordering Principle, there exists a least element $n$ in $X$. Let $f(x) \in T$ have degree $n$. Then by definition, $f(x)$ is not irreducible, so $f(x) = a(x)b(x)$, for $a(x), b(x) \in F[x]$ each having degree less than $n$. Thus, neither $a(x)$ nor $b(x)$ belong to $T$, and hence each is a product of finitely many irreducible polynomials. Since $f(x) = a(x)b(x)$, the same applies to $f(x)$, which is a contradiction. Thus, $T = \emptyset$ and every non-zero, non-constant polynomial in $F[x]$ can be factored as a product of irreducible polynomials.

For uniqueness, by what we have done in class, it suffices to show any irreducible polynomial $q(x)$ is a prime element in $F[x]$. Suppose $q(x) \mid a(x)b(x)$ in $F[x]$, and $q(x) \nmid a(x)$. We claim there exist $c(x), d(x) \in F[x]$ such that $1 = c(x)a(x) + d(x)q(x)$. If so, then $b(x) = a(x)b(x)c(x) + b(x)d(x)q(x)$. Since $q(x)$ divides the right hand side of this equation, $q(x)$ divides $b(x)$, which is what we want.

We now prove the claim by induction on the degree of $a(x)$. If the $\deg(a(x)) = 1$, then we can write $q(x) = a(x)\cdot\lambda + \gamma$, where $\lambda, \gamma \in F$ are non-zero since $q(x)$ is irreducible and does not divide $a(x)$. Thus, $1 = -\frac{\lambda}{\gamma}\cdot a(x) + 1\cdot q(x)$. Now suppose $\deg(a(x)) > 1$. If $\deg(a(x)) \leq \deg(q(x))$, we can write $q(x) = h(x)a(x) + r(x)$, with $\deg(r(x)) < \deg(a(x))$. Note $r(x) \neq 0$, since $q(x)$ is irreducible. By induction, we have $1 = c(x)r(x) + d(x)q(x)$, for $c(x), d(x) \in F[x]$. Thus,

$$1 = c(x)(q(x) - h(x)a(x)) + d(x)q(x) = \{-c(x)h(x)\}a(x) + \{c(x) + d(x)\}q(x),$$

which gives what we want. If $\deg(q(x)) < \deg(a(x))$, we write $a(x) = q(x)l(x) + t(x)$, where $t(x)$ is not zero, since $q(x)$ does not divide $a(x)$. Since

$$\deg(t(x)) < \deg(q(x)) < \deg(a(x)),$$

by induction, we have $1 = c(x)t(x) + d(x)q(x)$, for $c(x), d(x) \in F[x]$. Setting $t(x) = a(x) - q(x)l(x)$ in this last equation, and rewriting, gives what we want.

2. Let $R$ be a UFD.

(i) Using the definition of greatest common divisor from Homework 17, show that any two non-zero, non-unit elements in $R$ have a greatest common divisor. Hint: How might this work in $\mathbb{Z}$ without using the division algorithm?

(ii) Give a definition of least common multiple analogous to the greatest common divisor definition from Homework 17, and then show that any two non-zero, non-unit elements in $R$ have a least common multiple (LCM).

(iii) Conclude that for $a, b$, non-zero, non-units in $R$: $\mathrm{GCD}(a, b)\cdot\mathrm{LCM}(a, b) = ab$.

Solution. For (i), 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 $q_i = u_ip_i$, 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.

For (ii), to define the LCM of $a$ and $b$ in a way that is analogous to the definition of GCD in Homework 14, 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 $i$. □

3. 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. □

4. Let $R$ denote the set of polynomials in $\mathbb{Q}[x]$ with constant term in $\mathbb{Z}$. Show that $R$ is an integral domain having the property that any two non-zero, non-unit elements have a GCD, but $R$ is not a UFD. Hint: Use the previous problem to show $R$ is not a UFD, and then use the fact that $\mathbb{Q}[x]$ is a UFD.

Solution. It is easy to check that $R$ is a ring, since it is contained in $\mathbb{Q}[x]$ and is closed under addition and multiplication. Moreover, $R$ is an integral domain, because $\mathbb{Q}[x]$ is an integral domain. We first note that $R$ does not satisfy the ascending chain condition on principal ideals, so $R$ cannot be a UFD, by the previous problem. This follows since $\langle x\rangle \subsetneq \langle \frac{x}{2}\rangle \subsetneq \langle \frac{x}{4}\rangle \subsetneq \cdots$ is an ascending chain of principal ideals in $R$ that does not terminate (since 2 is not a unit in $R$). Indeed, if $\langle \frac{x}{2^n}\rangle = \langle \frac{x}{2^{n+1}}\rangle$ for some $n$, then there exists $f \in R$ such that $\frac{x}{2^{n+1}} = f \cdot \frac{x}{2^n}$. But then, $1 = 2 \cdot f$, which is a contradiction.

To see that GCDs exist in $R$, let $f, g \in R$ be non-zero, non-unit elements. We will use the fact the $f$ and $g$ have a GCD in $B := \mathbb{Q}[X]$ and that GCDs in $B$ are unique only up to units. First write $f = nf_0$ and $g = mg_0$, where $n, m \in \mathbb{Z}$ are such that both $f_0$ and $g_0$ have constant terms equal to 1. Let $d_0 \in B$ be the GCD of $f_0$ and $g_0$ so that $d_0$ also has constant term equal to 1. In $B$ we have equations $f_0 = d_0 \cdot u$ and $g_0 = d_0 \cdot v$. But then, $u$ and $v$ must have constant terms equal to 1, and hence belong to $R$. In other words, $d_0$ is a common divisor of $f_0$ and $g_0$ in $R$. Suppose that $h|f_0$ and $h|g_0$ for some $h \in R$. Since the constant term of $h$ is an integer, it must be $\pm 1$. Since $h$ is also a common divisor of $f_0$ and $g_0$ in $B$, $h$ divides $d_0$ in $B$, say $d_0 = h \cdot q$, for $q \in B$. Since the constant term of $h$ is $\pm 1$, it follows that the constant term of $q$ is $\pm 1$, so $q \in R$. In other words, $d_0$ is a GCD of $f_0$ and $g_0$ in $R$. Now if $\delta \in \mathbb{Z}$ is the GCD of $n$ and $m$, then it is straightforward to check that $\delta \cdot d_0 \in R$ is a GCD of $f$ and $g$.

5. $I \subseteq R$ be an ideal. Show that there is a one-to-one correspondence between the ideals of $R/I$ and the ideals of $R/I$. Show that under this correspondence prime ideals (respectively, maximal ideals) of $R$ containing $I$ correspond to prime ideals (respectively, maximal ideals) in $R/I$.

Solution. Because $R$ is an abelian group under addition, and any ideal of $R$ is a subgroup of $R$, by the correspondence theorem for groups, we know that if $K \subseteq R/I$ is an ideal, then as a subgroup, $K = H/I$, for an additive subgroup $H \subseteq R$. Suppose $r \in R$ and $h \in H$. Then $(r+I)\cdot(h+I) \in K = H/I$, since $K$ is an ideal of $R/I$. Thus, $(rh+I) \in H/I$, so that $rh - h_0 \in I$, for some $h_0 \in H$. Since $I \subseteq H$, we have $rh - h_0 \in H$ and thus, $rh \in H$, showing $H$ is an ideal of $R$. Since $J/I$ is clearly an ideal of $R/I$ for any ideal $J \subseteq R$ containing $I$, we have a 1-1 correspondence between the ideals of $R$ containing $I$ and the ideals of $R/I$.

It follows immediately from the paragraph above that $K \subseteq R/I$ is a maximal ideal if and only if $K = M/I$ for a maximal ideal $M \subseteq R$. Now suppose $P$ is a prime ideal of $R$. If $(a + I) \cdot (b + I) \in P/I$, then $(ab + I) \in P/I$. Thus, $ab - p \in I$, for some $p \in P$. Since $I \subseteq P$, $ab - p \in P$, so $ab \in P$. Since $P$ is prime, $a \in P$ or $b \in P$, say, $a \in P$. Thus, $(a + I) \in P/I$, showing $P/I$ is prime. The converse is similar.

6. Let $M \subseteq R$ be a maximal ideal and $R[x]$ denote the polynomial ring in $x$ over $R$.

(i) Prove that there exist infinitely many maximal ideals $\mathcal{M} \subseteq R[x]$ such that $\mathcal{M} \cap R = M$. Hint: You will need to show that a polynomial ring with coefficients in a field has infinitely many irreducible polynomials. (5 points)

(ii) Show that there do not exist proper prime ideals $M[x] \subsetneq P \subsetneq Q \subseteq R[x]$. (5 points)

Solution. For part (i), we use the fact from Homework 19 that $R[x]/M[x] \cong (R/M)[x]$. Since $R/M$ is a field, $R[x]/M[x]$ has infinitely many irreducible polynomials, each one generating a maximal ideal in $R[x]/M[x]$ (since an irreducible elements generates an ideal maximal among principal ideals, and $R[x]/M[x]$ is a PID). By the previous problem, there are infinitely many maximal ideals in $R[x]$ containing $M[x]$. The proof that $F[x]$ has infinitely many irreducible polynomials, when $F$ is a field, is similar to Euclid's proof that there are infinitely many prime numbers: Suppose, by way of contradiction, $q_1, \ldots, q_r$ are the only irreducible polynomials. Then, no $q_i$ divides $f := q_1 \cdots q_r + 1$, and $f$ is not a unit in $F[x]$. Since $F[x]$ is a UFD, $f$ is either irreducible or divisible by an irreducible polynomial that is not any of the $q_i$, which is a contradiction.[1] Thus, $F[x]$ contains infinitely many irreducible polynomials.

(ii) By the previous problem, the prime ideals in $R[x]$ containing $M[x]$ correspond to the prime ideals in $R[x]/M[x]$ which is a PID, by part (i). In a PID, (0) is a prime ideal and the non-zero prime ideals are also maximal ideals, so that one cannot have a chain of primes $(0) \subsetneq P' \subsetneq Q'$ in a PID, and hence not in $R[x]/M[x]$, which gives what we want.

7. Let $R$ be an integral domain, and $P = \langle p \rangle$, where $p \in R$ is a prime element. Set $I := \bigcap_{n=1}^{\infty} P^n$, where $P^n = \langle p^n \rangle$.
   (i) Prove that if $Q$ is a prime ideal *properly contained* in $P$, then $Q \subseteq I$. (3 points)
   (ii) Show that $I = pI$. (2 points)
   (iii) Show that $I$ is a prime ideal. (2 points)
   (iv) Prove that if $R$ is a UFD, then $I = 0$. (3 points)

Solution. For (i), suppose $q \in Q$. Write $q = r_1 p$. Since $Q$ is properly contained in $P$, $p \notin Q$. Thus, $r_1 \in Q$, since $Q$ is a prime ideal. We may therefore write $r_1 = r_2 p$. Thus, $q = r_1 p = r_2 p^2$. Continuing inductively, there exist $r_n \in R$ such that $q = r_n p^n$, showing $Q \subseteq I$.

For (ii), it suffices to show that $I \subseteq pI$. Take $x \in I$, and write $x = pr$. Then, for all $n$, $x = pr \in \langle p^{n+1} \rangle$, so that $r \in \langle p^n \rangle$, for all $n$, showing $r \in I$. Therefore, $I \subseteq pI$, which is what we want.

For (iii), suppose $I$ is not a prime ideal. Then for some $a, b \in R$, we have $ab \in I$ and neither $a$ nor $b$ belong to $I$. We can then write $a = cp^n$ and $b = dp^m$, with $p \nmid c$ and $p \nmid d$. Then $cdp^{n+m} = ab \in I$, thus, $cdp^{n+m} = ep^{n+m+1}$, for some $e \in R$. Therefore, $cd = ep$. Thus, $p \mid cd$, so $p \mid c$ or $p \mid d$, which is a contradiction. Thus, $I$ is a prime ideal.

There are several ways to see (iv). Here is one way: Suppose $0 \neq x \in I$. Then we can write $x = q_1 \cdots q_r$ as a product of prime elements, since $R$ is a UFD. On the other hand, $x \in \langle p^{r+1} \rangle$, so $x = cp^{r+1}$, a product of at least $r+1$ primes. This contradicts the unique factorization property.

8. Let $R$ be a commutative ring. The *Jacobson radical* of $R$ is defined to be the intersection of all maximal ideals of $R$. Show that an element $a \in R$ belongs to the Jacobson radical if and only if $1 + ra$ is a unit for all $r \in R$. You may use the fact that any proper ideal in a commutative ring is contained in a maximal ideal.

Solution. Suppose $x \in R$ belongs to the Jacobson radical. Then for any $r \in R$ and maximal ideal $M \subseteq R$, $rx \in M$, and therefore $1 + rx \notin M$. Thus, $\langle 1 + rx \rangle$ is not a proper ideal, since every proper ideal is contained in a maximal ideal. Thus $1 \in \langle 1 + rx \rangle$, showing that $1 + rx$ is a unit.

Conversely, suppose $x \in R$ has the property that $1 + rx$ is a unit for every $r \in R$. By way of contradiction, suppose there exists a maximal ideal $M$ with $x \notin M$. Then $M + \langle x \rangle$ properly contains $M$, and thus $M + \langle x \rangle = R$. We may therefore write $1 = m + sx$, for some $m \in M$ and $s \in R$. But then $m = 1 + (-s)x$, which is a unit, and therefore a contradiction, since $M$ does not contain a unit. Thus, $x$ must belong to every maximal ideal, which gives what we want. □

9. Let $R$ be a commutative ring and $S \subseteq R$ *multiplicatively closed set*, i.e., $0 \notin S$ and $S$ is closed under multiplication. 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 $a/s$. (1 point)
   (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* $S$. (4 points)
   (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 $\phi$. (2 points)
   (iv) Give an example of a commutative ring $R$ and multiplicatively closed set $S \subseteq R$ such that the map $\phi$ in part (iii) has non-zero kernel. (2 points)
   (v) What are the units in $R_S$? (1 point)

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 $(a, s) \sim (a_2, s_2)$.

[1] There are UFDs with finitely many primes, e.g., a DVR. However, if $q_1, \ldots, q_r$ are the only primes (irreducibles) in a UFD, then $f := q_1 \cdots q_r + 1$ is a unit.

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 $\phi$ is a ring homomorphism follows easily from the definitions. Now $r \in R$ belongs to the kernel of $\phi$ 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 $\phi$, for $\phi$ 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, since $1/s$ is a unit in $R_S$. 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.

10. Let $S \subseteq R$ be a multiplicatively closed set. Suppose $J, P \subseteq R$ are ideals of $R$ with $P$ prime and $P \cap S = \emptyset$.
   (i) Show that $J_S$ is an ideal of $R_S$ and $P_S$ is a prime ideal of $R_S$. (2 points)
   (ii) Show that if $K$ is an ideal of $R_S$, there exists an ideal $J$ of $R$ such that $K = J_S$. Show that if $K$ is prime, then the there exists a prime ideal $P \subseteq R$, disjoint from $S$, such that such that $P_S = K$. (2 points)
   (iii) For $J \subseteq R$ a proper ideals, when is $J_S$ a proper ideal of $R_S$? (2 points)
   (iv) Show that there is a one-to-one correspondence between the prime ideals of $R_S$ and the prime ideals of $R$ disjoint from $S$. (3 points)
   (v) Let $R = \mathbb{Z}$ and $S = \{2, 4, 8, 16, 32, \ldots\}$. Set $I := \langle 6 \rangle$ and $J = \langle 3 \rangle$. Prove that $S$ is a multiplicatively closed set disjoint from $I$ and $J$ and that $J_S = I_S$ in $R_S$, showing that there need not be a 1-1 correspondence between the ideals of $R$ disjoint from $S$ and the ideals of $R_S$. (2 points)

Solution. For (i), it is straightforward to check that $J_S$ is an ideal. Since $P \cap S = \emptyset$, $P_S$ is a proper ideal of $R_S$. Suppose $(a/s_1) \cdot (b/s_2) \in P_S$. Then $(a/s_1) \cdot (b/s_2) = p/s_3$, for some $p \in P$ and $s_1, s_2, s_3 \in R$. Then, in $R$, we have $s'(s_3ab - s_1s_2p) = 0$. Thus, $s's_3ab \in P$. Since $P$ is prime and $s', s_3 \notin P$, $ab \in P$, and thus $a \in P$ or $b \in P$. Say $a \in P$. Then $a/s_1 \in P_S$, which shows that $P_S$ is prime.

For (ii), if $K \subseteq R$ is an ideal, let $J := \{r \in R \mid r/s \in K\}$, for some $s \in S$ and $a, b \in J$, Since the elements of $S$ are units in $R_S$, $J = \{r \in R \mid r/1 \in K\}$. Suppose $a, b \in J$, then $a/1, b/1 \in K$ and thus, $a/1 + b/1 = (a + b)/1 \in K$, showing $a + b \in J$. Similarly, for any $r \in R$, $r/1 \cdot a/1 = ra/1 \in K$, so that $ab \in J$, showing $J$ is an ideal of $R$. By definition, $J_S = K$, as required.

For (iii), $J_S$ is not a proper ideal if and only if $1/1 \in J_S$ if and only if there is $j \in J$ such that $1/1 = j/1$ in $R_S$ if and only if there exists $s \in S$ such that $s(j - 1) = 0$ in $R$. This latter condition implies $sj \in S$, for some $j \in J$ and $s \in S$. Conversely, suppose $sj = s'$ for $s, s' \in S$ and $j \in J$. Then $1 \cdot (js - s') = 0$ in $R$, so that $j/s' = 1/s$ in $R_S$. Since $1/s$ is a unit in $R_S$, $J_S$ is not a proper ideal. Thus, $J_S$ is a proper ideal of $R_S$ if and only if for all $s \in S$ and $j \in J$, $sj \notin S$.

For (iv), if $P \subseteq R$ is a prime disjoint from $S$, then $P_S$ is a prime in $R_S$ and any prime in $R_S$ has this form. We must show that for $P' := \{r \in R \mid r/1 \in P_S\}$. $P = P'$. Clearly $P \subseteq P'$. Suppose $r \in P'$, i.e, $r/q \in P_S$. Then $r/1 = p/s$, for $p \in P$ and $s \in S$. Thus, $s'(rs - p) = 0$, for some $s' \in S$, and hence $ss'r \in P$. SInce $ss' \notin P$, $r \in P$, showing $P' \subseteq P$. Thus, $P = P'$ and we have the required one-to-one correspondence.

For (v), since $S = \{2^n \mid n \geq 1\}$, $S$ is multiplicatively closed, and it is disjoint from $I$ and $J$ since no element of $S$ is divisible by 3. Moreover, we have $\langle 6 \rangle \subseteq \langle 3 \rangle$, so in $R_S$, $I_S \subseteq J_S$. However, in $R_S$, 2 is a unit, and thus, $3/1 = (1/2) \cdot (6/1)$, showing $J_S \subseteq I_S$, which gives what we want.

**Bonus Problem.** Any part you work must be correct to receive bonus points. Let $R$ be an integral domain and suppose $S \subseteq R$ is a multiplicatively closed set such that every element of $S$ is a product of prime elements.
   (i) Show that $R_S$ is a UFD, if $R$ is a UFD. (5 points)
   (ii) Let $T$ denote the set of prime factors appearing among the elements of $S$ and assume that no element of $R$ is divisible by infinitely many primes in $T$. Prove that $R$ is a UFD, if $R_S$ is a UFD. (5 points)
   (iii) Use the foregoing to give a proof - different from the one given in class - that if $R$ is a UFD, then the polynomial rings $R[x]$ is a UFD. You may assume the result from class that a prime element in $R$ remains a prime element in $R[x]$. (5 points)

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 $R$. For part (i), we 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.

For part (ii), the difficulty in reversing the direction of the argument 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, see 10 (iv) above. 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 $p_i$ 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 $\mathcal{P}$ 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 $a = a_0b$, 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 $q_1/1 = t_1 \cdot (p_1/1)$, 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.

For part (iii), let $S$ be the non-zero, non-unit elements in $R$. Then every element of $S$ is a product of finitely many prime elements in $R$, since $R$ is a UFD. If $p$ is a prime element in $R$, then, by what we have shown in class, $p$ is a prime element in $R[x]$, thus $S$ is a multiplicatively closed set of elements in $R[x]$ whose elements are products of prime elements in $R[x]$. Suppose $p$ is a prime element in $R$, if $p \mid f(x)$ in $R[x]$, then $p$ divides every coefficient of $f(x)$ in $R$. It follows that every non-zero, non-unit in $R[x]$ is divisible by only finitely many primes appearing as factors of elements in $S$. Thus, by part (ii), $R[x]$ is a UFD, if $R[x]_S = R_S[x]$ is a UFD. But $R_S = K$, the quotient field of $R$. Thus, $R[x]_S = K[x]$ is a PID, and thus a UFD, which gives what we want.