Solutions to the Midterm, Math 525

Problem 1. Let R be a commutative ring such that for every $a \in R$ there is a natural number $n > 1$ such that $a^n = a$.

a) Prove that every prime ideal in R is maximal. Hint: What can you say when R is an integral domain? (6 points)

b) Prove that the intersection of all prime ideals of R is trivial. (2 points)

Solution. a) Let P be a prime ideal of R and let $\pi : R \longrightarrow R/P$ be the quotient homomorphism. Since P is prime, the ring R/P is a domain. Let $b \in R/P$. Since π is surjective, we have $b = \pi(a)$ for some $a \in R$. We know that $a^n = a$ for some $n > 1$. It follows that

$$b = \pi(a) = \pi(a^n) = \pi(a)^n = b^n.$$

Thus $b(b^{n-1} - 1) = 0$. Since R/P is a domain, we conclude that either $b = 0$ or $b^{n-1} = 1$. It follows that if $b \neq 0$ then $b^{n-1} = 1$, so b is invertible. In other words, every non-zero element of R/P is invertible, so R/P is a field. This means that P is a maximal ideal.

b) By problem 3 d) from Homework 1 we know that the intersection of all prime ideals in a commutative ring is equal to the nilradical. Let a belong to all prime ideals of R, so a is nilpotent: $a^m = 0$ for some $m > 0$. We also know that $a^n = a$ for some $n > 1$. It follows that $a^{n^k} = a$ for every $k > 0$. Take k such that $n^k > m$. Then $a = a^{n^k} = a^m a^{n^k - m} = 0$. Thus the only element in the intersection of all prime ideals is 0.

Problem 2. Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$ (so this ring is a subring of R_{-3}).

a) Find all invertible elements in R. (1 point)

b) Prove that 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ are irreducible in R. Conclude that R is not a UFD. (3 points)

c) Prove that the ideal $I = < 2, 1 + \sqrt{-3} >$ of R is not principal and that it is maximal. Prove that $I^2 = 2I$. Is there an n such that I^n is principal? (4 points)

Solution. a) Recall that we have the norm map $N : R \longrightarrow \mathbb{Z}$, $N(a + b\sqrt{-3}) = a^2 + 3b^2$ which has the property that $N(xy) = N(x)N(y)$ for any $x, y \in R$. If $xy = 1$ then $N(x)N(y) = N(1) = 1$ so $N(x) = N(y) = 1$ (since $N(x)$ is a non-negative integer for all $x \in R$). Now $a^2 + 3b^2 = 1$ for integers a, b if and only if $a = \pm 1$ and $b = 0$. Thus the only invertible elements of R are 1 and -1.

Alternatively, we found in class all 6 invertible elements in R_{-3} and only ± 1 belong to R.

b) Note that each of the three elements has norm 4. Suppose that one of the elements factors as xy. Then $N(x)N(y) = 4$. If $N(x) = 1$ then $x = \pm 1$ is invertible. Similarly for $N(y) = 1$. The only other possibility is that $N(x) = N(y) = 2$. However $a^2 + 3b^2 = 2$ is not possible for any integers a, b. Thus one of x, y must be invertible proving that each of the three elements is irreducible.

Note that no two of the elements 2, $1+\sqrt{-3}$, $1-\sqrt{-3}$ are associated and $4 = 2\cdot 2 = (1-\sqrt{-3})(1+\sqrt{-3})$. Thus 4 has two inequivalent factorizations into irreducible elements, hence R is not a UFD.

A different argument: $(1 - \sqrt{-3})(1 + \sqrt{-3}) \in 2R$ but neither $(1 - \sqrt{-3})$ nor $(1 + \sqrt{-3})$ is in $2R$. This means that $2R$ is not a prime ideal so 2 is irreducible but not prime. Hence R is not a UFD.

c) Let us start by proving that $I^2 = 2I$. Since $2 \in I$, clearly $2I \subseteq I^2$. Note that I^2 is generated by $2^2 = 4 \in 2I$, $2(1+\sqrt{-3}) \in 2I$ and

$$(1+\sqrt{-3})^2 = -2 + 2\sqrt{-3} = 2((1+\sqrt{-3}) - 2) \in 2I.$$

Thus all three generators belong to $2I$, so $I^2 \subseteq 2I$. Hence $I^2 = 2I$ as claimed.

If I was principal, we would have $I = xR$ for some $x \in R$, and therefore $x^2R = (2x)R$. This means that x^2 and $2x$ are associated, i.e. $x^2 = \pm 2x$. Since R is a domain, we conclude that $x = \pm 2$ and $I = 2R$, which is clearly false. This shows that I is not principal (so, in particular, it is proper).

Alternatively, note first that I is a proper ideal. Indeed, elements of I are of the form $2(a+b\sqrt{-3}) + (1+\sqrt{-3})(c+d\sqrt{-3}) = (2a+c-3d) + (2b+c+d)\sqrt{-3}$. Note that the integers $2a+c-3d$ and $2b+c+d$ have the same parity so $2a+c-3d = 1$ and $2b+c+d = 0$ is not possible. Thus $1 \notin I$. Yet another argument: since we already know that $I^2 = 2I$, I must be proper as $R^2 = R \neq 2R$.

Now if $I = xR$ was principal then x would divide 2. But 2 is irreducible, so 2 and x would be associated and consequently $I = 2R$, which is false.

Note that a straightforward induction shows that $I^n = 2^{n-1}I$ for all n. Since I is not principal, I^n is not principal for all $n > 0$ (a simple exercise: if R is a domain, $a \neq 0$ and I is an ideal such that aI is principal then I is principal).

Note that the additive group of R is $\mathbb{Z} \oplus \mathbb{Z}$. Thus $R/2R$ has 4 elements. Since I strictly contains $2R$, R/I has 2 elements. Thus R/I must be the field $\mathbb{Z}/2\mathbb{Z}$, so I is maximal.

Alternatively, note that $1 + I = \sqrt{-3} + I$, so $(a+b\sqrt{-3}) + I = (a+b) + I$ which is I if $a+b$ is even and $1+I$ if $a+b$ is odd. Thus R/I has 2 elements.

Problem 3. Prove that the polynomial $f = x^2y^{2017} + x^{2017}y + x^2 - y - 1$ is a prime element in the ring $\mathbb{Q}[x,y]$. Hint: Consider f as a polynomial in $R[y]$, where $R = \mathbb{Q}[x]$. A homework problem may be useful. (8 points)

Solution. We have $f = x^2y^{2017} + (x^{2017}-1)y + (x^2-1) \in R[y]$. Not that $R = Q[x]$ is a PID, hence a UFD. It follows that $R[y]$ is a UFD, so it suffices to show that f is irreducible in $R[y]$. We will use the Eisenstein criterion (see Problem 2b) of Homework 3). Note that $P = (1-x)R$ is a prime ideal of R as $1 - x \in R$ is irreducible in R (hence prime). Note that $x^2 \notin P$, all the other coefficients of f are in P (as $1-x$ divides $x^{2017}-1$ and x^2-1) and x^2-1 is not in P^2 (as $(x-1)^2$ does not divide x^2-1). By Eisenstein criterion, if $f = gh$ for some $g,h \in R[y]$ then one of g,h is in R (i.e. is constant as a polynomial in y). Since f is primitive (as $\gcd(x^2, x^{2017}-1, x^2-1) = 1$ in R), this constant must be invertible in R, hence f is irreducible.

Problem 4. Let R be a PID and let I, J be proper ideals of R.

a) Prove that the intersection of all the ideals I^n, $n = 1, 2, \ldots$, is trivial (this is true, but much harder to prove, for any Noetherian integral domain and any ideal I). (2 points)

b) Prove that if $J \neq \{0\}$ then $\bigcap_{n=1}^{\infty}(J + I^n) = J + I^k$ for some k. (6 points)

Solution. a) Since R is a PID, $I = aR$ is principal. We may assume $a \neq 0$ (otherwise the result is clear). Let $b \in \bigcap_{n=1}^{\infty} I^n$ so $b \in I^n = a^nR$ for every n. This means that $b = a^n w_n$ for some $w_n \in R$. Suppose that $b \neq 0$. Then $w_n \neq 0$ for all n. Since R is a UFD, a is a product of k irreducible elements for some $k \geq 1$. Thus $b = a^n w_n$ is a product of at least nk irreducible elements. Since n is arbitrary, b has many factorizations into irreducible elements, a contradiction.

Alternatively, note that $aw_{n+1} = w_n$. It follows that $w_1R \subseteq w_2R \subseteq w_3R \ldots$. Since R is Noetherian (or has PACC), we must have $w_kR = w_{k+1}R$ for some k, which implies that a is invertible, a contradiction. This argument actually shows the result in a more general situation, when R is an integral domain with $PACC$ and I is principal.

Yet another argument is based on the following observation we proved in class: if R is a PID and K is a non-zero ideal of R then R has only finitely many ideals containing K. Note that $I^{n+1} \subsetneq I^n$ for every n (as $a^{n+1}R = a^nR$ would imply that $a^n = a^{n+1}r$, i.e. $1 = ar$, so a would be invertible). So if the intersection $K = \bigcap_{n=1}^{\infty} I^n$ was nontrivial we would have infinitely many different ideals I^n, $n = 1, 2, \ldots$ all containing K, a contradiction.

b) We proved in class that if R is a PID and J is a non-zero ideal of R then R has only finitely many ideals containing J. Note that $J + I \supseteq J + I^2 \supseteq J + I^3 \supseteq \ldots \supseteq J$ is a descending chain of ideals containing J. The finiteness of the set of ideals containing J implies that $J + I^k = J + I^{k+1} = J + I^{k+2} = \ldots$ for some k and therefore $\bigcap_{n=1}^{\infty}(J + I^n) = J + I^k$.

Another way is to show first that in a UFD, given any two non-zero elements a, b there is k such that $\gcd(b, a^k) = \gcd(b, a^{k+1}) = \gcd(b, a^{k+2}) \ldots$. In a PID, when $I = aR$ and $J = bR$, we have $J + I^n = \gcd(b, a^n)R$, so the result follows.

Problem 5. Let R be a commutative ring and $I =< a, b >$ be an ideal of R generated by two elements a, b and such that $I^2 = I$.

a) Show that every element of I is of the form $ia + jb$ for some $i, j \in I$ (2 points).

b) Suppose that $p, q, s, t \in R$ are such that $pa + qb = 0$ and $sa + tb = 0$. Show that $(pt - sq)a = 0 = (pt - sq)b$ (one way to approach it is by using 2×2 matrices). (2 points)

c) Use a) and b) to show that there is $e \in I$ such that $(1 - e)a = 0 = (1 - e)b$ (3 points).

d) Show that $e^2 = e$ and $I = Re$ (hint: what is $(1 - e)I$?). Conclude that I is a unital ring and $J = R(1 - e)$ is also a unital ring and $R = I \oplus J$. (3 points)

e) (Optional for extra credit) Prove c) when you only know that I is finitely generated.

Solution. a) We will show first that if $I =< a_1, \ldots, a_k >$ is a finitely generated ideal and J is any ideal then every element of IJ is of the form $a_1j_1 + \ldots + a_kj_k$ for some $j_1, \ldots, j_k \in J$. In fact, every element x of IJ is of the form $x = i_1t_1 + i_2t_2 + \ldots + i_mt_m$ for some $i_1, \ldots, i_m \in I$ and $t_1, \ldots, t_m \in J$. Now $i_n = r_{n,1}a_1 + r_{n,2}a_2 + \ldots + r_{n,k}a_k$ for some $r_{n,1}, \ldots, r_{n,k} \in R$. Thus

$$x = \sum_{n=1}^{m}(\sum_{l=1}^{k} r_{n,l}a_l)t_n = \sum_{l=1}^{k} a_l \sum_{n=1}^{m} r_{n,l}t_n$$

and $j_l = \sum_{n=1}^{m} r_{n,l}t_n \in J$ for $l = 1, 2, \ldots, k$. This proves our claim.

Applying our observation to $I =< a, b >$ and $J = I$, we see that every element of I^2 is of the form $ia + jb$ for some $i, j \in I$. Part a) follows now from the assumption that $I = I^2$.

b) Let $A = \begin{bmatrix} p & q \\ s & t \end{bmatrix}$ and $v = \begin{bmatrix} a \\ b \end{bmatrix}$. Then our assumption is $Av = 0$. Now take $B = \begin{bmatrix} t & -q \\ -s & p \end{bmatrix}$. Then $BA = \begin{bmatrix} pt - sq & 0 \\ 0 & pt - sq \end{bmatrix}$. Now $(BA)v = B(Av) = B0 = 0$, i.e. $\begin{bmatrix} pt - sq & 0 \\ 0 & pt - sq \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, which is exactly what we are asked to prove.

A more direct argument (which is not that useful for answering part e)) is to note that $0 = t(pa+qb) - q(sa+tb) = (pt-sq)a$ and $0 = p(sa+tb) - s(pa+qb) = (pt-sq)b$.

c) By a we can write $a = i_1a + j_1b$ and $b = i_2a + j_2b$ for some $i_1, i_2, j_1, j_2 \in I$. In other words, $(i_1-1)a + j_1b = 0 = i_2a + (j_2-1)b$. Note that $(i_1-1)(j_2-1) - j_1i_2 = 1 - (j_2 + 1_1 + j_1i_2 - j_2i_1) = 1 - e$, where $e = j_2 + 1_1 + j_1i_2 - j_2i_1 \in I$. By part b) we have $(1-e)a = 0 = (1-e)b$.

d) Since every element x in I is of the form $r_1a + r_2b$ for some $r_1, r_2 \in R$, we see from c) that $(1-e)x = 0$. In other words $x = ex = xe$ for all $x \in I$. Thus $I \subseteq Re$. Since $e \in I$, we have $e = e^2$ and $Re \subseteq I$. It follows that $I = Re$ and $e \in I$ serves as identity for multiplication in I. Thus I is a unital ring (the only thing potentially missing for an ideal to be a unital ring is the identity for multiplication). Note that $(1-e)(1-e) = 1-e$ so $1-e$ is the identity for multiplication within the ideal $J = R(1-e)$. Now $x = xe + x(1-e)$ for all $x \in R$ so $R = I + J$. Finally, if $u \in I \cap J$ then $eu = u$ and $u = (1-e)u = u - eu = 0$, so $I \cap J = \{0\}$. This shows that $R = I \oplus J$.

e) We are assuming that I is a finitely generated ideal such that $I^2 = I$ and we want to prove that $(1-e)I = 0$ for some $e \in I$. Let $I =< a_1, \ldots a_n >$. Using part a), we see that

$$a_k = i_{k,1}a_1 + i_{k,2}a_2 + \ldots + i_{k,n}a_n$$

for some $i_{s,t} \in I$, $1 \leq s \leq n$, $1 \leq t \leq n$. Let A be the $n \times n$ matrix whose (s,t)-entry is $i_{s,t}$. Then $(I_n - A)v = 0$, where v is the column vector $(a_1, \ldots, a_n)$ and I_n is the $n \times n$ identity matrix.

We need now some facts about determinants. The determinant of a matrix is a polynomial expression in the entries of the matrix and it makes sense over any commutative ring. If $f : R \longrightarrow S$ is a ring homomorphism then $\det(f(D)) = f(\det(D))$ for any square matrix D, where $f(D)$ is obtained from D by applying f to every entry of D. Moreover for every matrix A there is a matrix B (with entries in R) such that $BA = AB = \det(A)I_n$ (the s,t-entry of B is $(-1)^{s+t}$ times the determinant of the matrix obtained from A by removing its t-th row and s-th column). The matrix B is usually denoted by A^D and called the adjoint matrix of A.

Returning to our problem, note that $\det(I_n - A) = 1 - e$ for some $e \in I$. Indeed, the natural homomorphism $R \longrightarrow R/I$ takes $I_n - A$ to the identity matrix, so it takes $\det(I_n - A)$ to 1. This means that $\det(I_n - A) = 1 - e$ for some $e \in I$. Now $0 = (I_n - A)^D((I_n - A)v) = ((I_n - A)^D(I_n - A))v = \det(I_n - A)v = (1-e)v$. This means that $(1-e)a_i = 0$ for $i = 1, \ldots, n$, i.e. $(1-e)I = 0$. Now we can repeat part d) to conclude that $e^2 = e$ and $I = Re$.

Problem 6. Let R be a commutative ring.

a) Let $a \in R$ and let M be an ideal of R. Show that the set $J = \{r \in R : ra \in M\}$ is an ideal containing M. (2 points)

b) Let $\mathcal{F}$ be the set of all ideals of R which are not finitely generated. Suppose that $\mathcal{F}$ is not empty. Prove that it contains maximal elements (with respect to inclusion). (3 points)

c) Let M be a maximal element of $\mathcal{F}$ and let $a \notin M$. Show that $M = N + Ja$ for some finitely generated ideal N contained in M, where J is the ideal from part a). Hint: what can you say about the ideal $M + Ra$? Conclude that $J = M$. Conclude that M is a prime ideal. (5 points)

Solution. a) If $s, t \in J$. Then $sa \in M$ and $ta \in M$, so $sa + ta = (s+t)a \in M$ and $s + t \in J$. Thus J is closed under addition. Clearly $0 \in J$ as $0 \cdot a = 0 \in M$. Finally, since $sa \in M$, for any $r \in R$ we have $r(sa) \in M$, i.e. $(rs)a \in M$, so $rs \in M$. This is all we need to verify that J is an ideal. Clearly if $m \in M$ then $am = ma \in M$ so $m \in J$. Thus M is contained in J.

b) We will use Zorn's Lemma. If $\mathcal{N}$ is a subset of $\mathcal{F}$ which is a chain then consider the union K of all the ideals in $\mathcal{N}$. We know that K is an ideal. We need to check that K is in $\mathcal{F}$. Then K will be an upper bound for our chain. Well, if K was not in $\mathcal{F}$, then K would be finitely generated: $K =< a_1, \ldots, a_m >$. As K is the union of our chain, there are ideals $M_i \in \mathcal{N}$ such that $a_i \in M_i$. Since these ideals are in a chain, one of them contains all the others. Thus, for some j we have $a_1, \ldots, a_m \in M_j$. It follows that $K =< a_1, \ldots, a_m >\subseteq M_j \subseteq K$, i.e. $K = M_j$ is finitely generated, a contradiction. Thus K is in $\mathcal{F}$, i.e. every chain in $\mathcal{F}$ has an upper bound in $\mathcal{F}$. By Zorn's Lemma, $\mathcal{F}$ contains maximal elements.

c) Since $a \notin M$, the ideal $M + Ra$ strictly contains M. Since M is maximal in $\mathcal{F}$, the ideal $M + Ra$ is not in $\mathcal{F}$. Thus $M + Ra$ is finitely generated. Let $m_1 + t_1a, m_2 + t_2a, \ldots, m_k + t_ka$ be generators of $M + Ra$, where $m_1, \ldots, m_k \in M$ and $t_1, \ldots, t_k \in R$. Let N be the ideal generated by $m_1, \ldots, m_k$, so $N \subseteq M$ and N is finitely generated. Note that $t_ia = (m_i + t_ia) - m_i \in M$, so $t_i \in J$. Thus $M \subseteq N + Ja$. On the other hand, both N and Ja are contained in M, so $N + Ja \subseteq M$. Hence $M = N + Ja$. We know from a) that J contains M. If J was strictly larger than M then J would not be in $\mathcal{F}$, i.e. J would be finitely generated: $J =< j_1, \ldots, j_n >$. But then the elements $m_s + j_ta$ with $1 \leq s \leq k$ and $1 \leq t \leq n$ would generate $N + Ja = M$, contrary to the fact that M is not finitely generated. This shows that $J = M$. Thus if $ba \in M$ then $b \in M$. Since a was an arbitrary element not in M, we see that M is a prime ideal.

We have established the following result:

Theorem. If R is a commutative ring in which every prime ideal is finitely generated then R is Noetherian.

Indeed, if R was not Noetherian, the set $\mathcal{F}$ would be non-empty but then it would contain a prime ideal, which would not be finitely generated.

****

Extra credit. This problem is optional.

Problem 7. Let $R = M_n(K)$ be the ring of all $n \times n$ matrices with entries in a field K, $n \geq 2$. Let $V = K^n$. We consider elements of V as $1 \times n$ matrices and define $v \cdot A$ to be matrix multiplication ($v \in V$ and $A \in R$).

a) Show that this multiplication makes V a right R-module. Prove that V is a simple R-module..

b) Find two different right ideals I, J of R such that V is isomorphic to each R/I and R/J (consult our discussion of simple modules in the last 8 minutes of lecture 13).

c) Show that if S is a commutative ring and I, J are ideals of S such that the R-modules R/I and R/J are isomorphic then $I = J$.

d) Prove that the right R-modules R and V^n are isomorphic.

e) Conclude that every simple R-module is isomorphic to V.

Solution. a) The fact that V is a right R-module is a straightforward consequence of properties of matrix multiplication. We leave the details to the reader.

Let $e_i \in V$ be the element $(0, \dots, 0, 1, 0 \dots, 0)$, where 1 is in the i-th place and 0 is everywhere else. Note that for any $v \in V$ there is $A \in R$ such that $e_1 A = v$. Indeed, take matrix A whose first row is v and all other rows consist of zeros. If $w \neq 0$ then there is $B \in R$ such that $wB = e_1$. Indeed, if the i-th coordinate t of v is non-zero then take B with i-th row $(1/t, 0, \dots, 0)$ and all other rows consisting of 0. This two observation together mean that for any two non-zero elements $u, w \in V$ there is $A \in R$ such that $uA = w$. It follows that if a submodule of V contains a non-zero element then it contains all V. This means that V is simple.

b) If W is a simple right R-module and $w \in W$ is any non-zero element then the function $f : R \longrightarrow W$, $f(r) = wr$ is a surjective homomorphism of R-modules and $W \equiv R/\ker f$. Let us apply this to $W = V$ and $w = e_i$. In this case $\ker f = J_i$ consists of all matrices whose i-th row is 0. Thus R/J_i are all isomorphic to V for $i = 1, \dots, n$.

c) For any right R-module M define $ann(R) = \{r \in R : mr = 0 \text{ for all } m \in M\}$. It is easy to see that $ann(R)$ is an ideal of R called the annihilator of M). Clearly, isomorphic R-modules have equal annihilators. When R is commutative and I is an ideal of R then the annihilator of R/I is I. Indeed, if if $r \in ann(I)$ then $I = (1 + I)r = r + I$, so $r \in I$. Conversely, if $r \in I$ and $a \in R$ then $(a + I)r = ar + I = ra + I = I$, so $r \in ann(I)$ (why doesn't it work for non-commutative rings?). Thus, if R/I and R/J are isomorphic then they have the same annihilators so $I = J$.

d) Consider the function $T : V^n \longrightarrow R$ which takes $(v_1, \dots, v_n)$ to the matrix whose i-th row is v_i, $i = 1, \dots, n$. It is straightforward to see that T is a bijection and it is a homomorphism of right R-modules (since the i-th row of the matrix BA is $b_i A$, where b_i is the i-th row of B). Thus R and V^n are indeed isomorphic as right R-modules.

d) Let W be any simple right R-module. Thus there is a surjective homomorphism from $R = V^n$ onto W. Restricting this homomorphism to at least one direct summand V of $R = V^n$ is non-trivial. Thus we get a non-zero homomorphism $V \longrightarrow W$. The image is a non-trivial submodule of W, so it is the whole W (as W is simple). The kernel is a proper submodule of V, hence it is trivial (as V is simple). Thus we have an isomorphism from V to W.