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?

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

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.

A different argument. We will show that the intersection of all maximal ideals of R is trivial. Since every maximal ideal is prime, this implies the result (even without using part a)). Suppose that a belongs to all maximal ideals. Then for every $k \geq 1$, a^k belongs to all maximal ideals of R. Recall now that if u is in all maximal ideals, then $1 - u$ does not belong to any maximal ideal, hence $1 - u$ is invertible. Thus $1 - a^k$ is invertible for every $k > 0$. Now there is $n > 1$ such that $a^n = a$. This means that $a(a^{n-1} - 1) = 0$. Since $a^{n-1} - 1$ is invertible, we see that $a = 0$.

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

a) Define the norm on the ring R and list its key properties.

b) Find all invertible elements in R.

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

d) 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?

Solution. a) For any $u = a + b\sqrt{-3}$ in R define $u^* = a - b\sqrt{-3}$. It is clear that $u^* \in R$ and $(u^*)^* = u$. Also, $u \mapsto u^*$ is an automorphism of the ring R. We define the norm $N(u) = uu^*$. Then $N(a + b\sqrt{-3}) = a^2 + 3b^2$, so the norm is always a non-negative integer. We have $N(uw) = N(u)N(w)$ for any $u, w \in R$ and $N(u) = 0$ if and only if $u = 0$.

b) If $x, y \in R$ and $xy = 1$ 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, both x and y are ± 1. In other words, the only invertible elements of R are 1 and -1.

Alternatively, we found in class all 6 invertible elements in S_{-3} and only ± 1 belong to R (any element invertible in R is also invertible in S_{-3}).

c) Note that each of the three elements has norm 4. Suppose that one of the elements factors as xy. Then $N(x)N(y) = N(xy) = 4$. Recall that $N(x), N(y)$ are positive integers. 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, if $a^2 + 3b^2 = 2$ for integers a, b then $b = 0$ (as otherwise $a^2 + 3b^2 \geq 3b^3 \geq 3 > 2$) and $a^2 = 2$, which is not possible. In other words, $N(x) = 2$ is not possible. Thus one of x, y must be invertible. This proves that each of the three elements is irreducible.

Since ± 1 are the only invertible elements, 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.

d) 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, $(1+\sqrt{-3})^2$, and $2(1+\sqrt{-3})$ Clearly 2^2 and $2(1+\sqrt{-3})$ are 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. Note that this implies that I is a proper ideal (as $2R \neq R$).

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 and $x \neq 0$, we conclude that $x = \pm 2$ and $I = 2R$, which is clearly false. This shows that I is not principal.

Another argument: 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).

Recall 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, and therefore it is the field $\mathbb{Z}/2\mathbb{Z}$.

Problem 3. a) State Eisenstein criterion.

b) 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 $R = \mathbb{Q}[x]$.

Solution. a) **Eisenstein Criterion**. *Let $f(x) = f_0 + f_1x + \ldots + f_nx^n$ be a polynomial in $R[x]$, where R is an integral domain. Suppose that there is a prime ideal P of R such that $f_n \notin P$, $f_0, f_1, \ldots, f_{n-1} \in P$ and $f_0 \notin P^2$. Then if $f = gh$ for some $g, h \in R[x]$, then one of g, h is constant.*

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 $R[y]$ (in UFD's irreducible elements are prime). We will use the Eisenstein criterion. 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 both $x^{2017}-1$ 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 (i.e. $\gcd(x^2, x^{2017}-1, x^2-1) = 1$ in R), this constant must be invertible in R. This proves that 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).

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

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 $b \in I^n = a^n R$ 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 (for every m there is a factorization of b with more than m irreducible factors).

Alternatively, note that $aw_{n+1} = w_n$. It follows that $w_1 R \subseteq w_2 R \subseteq w_3 R \ldots$. Since R is Noetherian (or has ACCP), we must have $w_{k+1}R = w_k R$ for some k, which implies that $aw_{k+1}R = w_{k+1}R$. It follows that a is invertible, a contradiction. This argument actually shows the result in a more general situation, when R is an integral domain with $ACCP$ 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 $a^{n+1}R = a^n R$ 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 ring which contains a left ideal I minimal among all non-zero left ideals. Suppose that $I^2 \neq 0$.

a) Prove that $Ra = I$ for all $a \in I$, $a \neq 0$.

b) Prove that if $a \in I$ then either $Ia = I$ or $Ia = \{0\}$.

c) Prove that there is $a \in I$ such that $Ia = I$. Prove that for any such a the map $I \longrightarrow I$ given by $x \mapsto xa$ is bijective.

d) Let a be as in c). Prove that there is an element $e \in I$ such that $e^2 = e$ and $ea = a$. Conclude that $I = Re$.

e) Show that $Re \cap R(1-e) = \{0\}$ and $R = Re + R(1-e)$.

Solution. a) Since $a \in I$ and I is a left ideal, we have $Ra \subseteq I$. Since Ra is a left ideal and I is minimal, we have either $Ra = I$ or $Ra = \{0\}$. The latter is not possible, as $a \in Ra$ and $a \neq 0$. Thus $I = Ra$.

b) Note that if J is a left ideal in R and $b \in R$ then Jb is also a left ideal in R. Indeed, if ib, jb are elements of Jb $(i, j \in J)$ and $r \in R$, then $ib + jb = (i+j)b \in Jb$ (as $i + j \in J$) and $r(ib) = (ri)b \in Jb$ (as $ri \in J$).
We see that Ia is a left ideal contained in I so either $Ia = I$ or $Ia = \{0\}$.

c) If $Ia = \{0\}$ for all $a \in I$ (i.e. $xa = 0$ for any $x, a \in I$), then $I^2 = 0$ contrary to our assumption. Thus there is an a such that $Ia \neq \{0\}$, and then $Ia = I$ by part b).

Suppose that $Ia = I$. Consider the map $f : I \longrightarrow I$, $f(x) = xa$. This is a homomorphism of groups. Since $I = Ia$, this homomorphism is clearly surjective. Let K be the kernel of f. We claim that K is a left ideal. Indeed, K is a (additive) subgroup of I and if $u \in K$ and $r \in R$ then $ru \in I$ and $f(ru) = (ru)a = r(ua) = 0$, proving that $ru \in K$. Thus K is a left ideal containing in I, so $K = I$ or $K = \{0\}$. In the former case, $f = 0$ and therefore $I = 0$, which is false. Thus $K = \{0\}$. This means that f is injective. We showed that f is both injective and surjective, so it is a bijection.

d) Since f in part c) is bijective, we have $a = f(e) = ea$ for some $e \in I$. Now $e^2a = e(ea) = ea = a$ so $f(e) = f(e^2)$, hence $e = e^2$. Clearly $e \neq 0$ (as $a \neq 0$), so $I = Re$ by part a).

d) Suppose that $x \in Re \cap R(1-e)$. Then $x = re = s(1-e)$ for some $r, s \in R$. We see that $xe = (re)e = r(e^2) = re = x$. On the other hand, $xe = s(1-e)e = s(e-e^2) = 0$. This proves that $x = 0$. It follows that $Re \cap R(1-e) = \{0\}$.
For any $r \in R$ we have $r = re + r(1-e) \in Re + R(1-e)$. Thus $R = Re + R(1-e)$. This means that R is a direct sum $R = I \oplus J$ of left ideals, where $J = R(1-e)$.

Problem 6. 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 $i, j \in I$.

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).

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

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 $R = I \oplus J$.

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 $JI = IJ$ is of the form $j_1a_1 + \ldots + j_ka_k$ 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

$t_1,\dots,t_m\in J$. Now, for every n, $i_n=r_{n,1}a_1+r_{n,2}a_2+\ldots+r_{n,k}a_k$ for some $r_{n,1},\dots,r_{n,k}\in R$. Thus

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

where $j_l=\sum_{n=1}^{m}r_{n,l}t_n\in J$ for $l=1,2,\dots,k$. 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 part 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 $(i_1-1)(j_2-1)-j_1i_2=1-(j_2+i_1+j_1i_2-j_2i_1)=1-e$, where $e=j_2+i_1+j_1i_2-j_2i_1\in I$. 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 $(1-e)e=0$, i.e. $e=e^2$. Since I is an ideal and $e\in I$, we have $Re\subseteq I$. It follows that $I=Re$ and $e\in I$ serves as the identity for multiplication in I: if $i\in I$ then $i=re$ for some $r\in R$ and $ie=(re)e=re^2=re=i$. 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 $i_{s,t}\in I$, $1\le s\le n$, $1\le t\le n$. 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 $(a_1,\dots,a_n)$ 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 7. 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.

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).

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.

Solution. a) Let $s, t \in J$. 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 come from 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. We claim that $M + Ra = N + Ra$. Since $N \subseteq M$, the inclusion $N + Ra \subseteq M + Ra$ is clear. On the other hand, every generator $m_i + t_ia$ of $M + Ra$ belongs to $N + Ra$, so $M + Ra \subseteq N + Ra$.
In particular, $M \subseteq N + Ra$. Take $m \in M$, so $m = n + ta$ for some $n \in N$ and $t \in R$. Since $ta = m - n \in M$, we have $t \in J$, so $m \in N + Ja$. 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 $b \in M$.
We showed that for any element a not in M, if $ba \in M$ for some $b \in R$ then $b \in M$. This means 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.