

### Math 566 - Homework 3

#### SOLUTIONS

Prof. Arturo Magidin

1. This problem generalizes the analysis given in class of the ring  $M_{2 \times 2}(\mathbb{R})$ . Let  $R$  be a ring with identity, and let  $S$  be the ring of all  $n \times n$  matrices with coefficients in  $R$ .

- (i) Prove that if  $J$  is an ideal of  $R$ , then  $M_{n \times n}(J)$ , the ring of all  $n \times n$  matrices with coefficients in  $J$ , is an ideal of  $S$ .

**Proof.** Since  $J$  is closed under sums and products, it follows that  $M_{n \times n}(J)$  is a subring of  $S$ .

To show it is an ideal, let  $B = (b_{ij})$  be an element of  $M_{n \times n}(J)$ , and let  $A = (a_{ij})$  be an element of  $S$ . We want to show that every entry of  $AB$  and of  $BA$  lies in  $J$ . The  $(i, j)$ th entry of  $AB$  is given by

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Since  $b_{rj} \in J$  for  $r = 1, \dots, n$  and  $J$  is an ideal, then  $a_{ir}b_{rj} \in J$  for each  $r$ , hence the sum is in  $J$ . Thus, the  $(i, j)$ th entry of  $AB$  is in  $J$ . This shows that  $M_{n \times n}(J)$  is a left ideal.

The  $(i, j)$ th entry of  $BA$  is

$$b_{i1}a_{1j} + \cdots + b_{in}a_{nj}.$$

Again, since  $J$  is an ideal, each  $b_{ir}a_{rj}$  lies in  $J$ , hence the product  $BA$  lies in  $M_{n \times n}(J)$ . Thus,  $M_{n \times n}(J)$  is a right ideal as well, and we are done.  $\square$

- (ii) Prove that if  $K$  is an ideal of  $S$ , then there exists an ideal  $J$  of  $R$  such that  $K = M_{n \times n}(J)$ . HINT: Given  $K$ , let  $J$  be the set of all elements of  $R$  that appear as an entry in some element of  $K$ . Then use matrices  $E_{ij}$  (with  $1_R$  in the  $(i, j)$  entry, 0 elsewhere) to show  $K = M_{n \times n}(J)$ .

**Proof.** As in the hint, let  $J$  be the set of all elements of  $R$  that appear as an entry in some element of  $K$ . We need to show that this is an ideal, and that  $K = M_{n \times n}(J)$ .

Let  $E_{rs}$  be the matrix that has a 1 in the  $(r, s)$ th entry and zeros elsewhere. Then given a matrix  $A = (a_{ij})$ , we have that  $C = E_{rs}A$  is the matrix that has the  $s$ th row of  $A$  in the  $r$ th row, and zeros elsewhere: the only nonzero entries are those that involve  $e_{rs}$ , which are the entries  $c_{rk}$  of  $C$ , and

$$c_{rk} = e_{r1}a_{1k} + \cdots + e_{rn}a_{nk} = a_{sk}.$$

Similarly, the matrix  $D = AE_{rs}$  is the matrix that has the  $r$ th column of  $A$  in the  $s$ th column, and zeros elsewhere. Hence,  $E_{ij}AE_{rs}$  is a matrix whose  $(i, s)$ th entry is  $a_{jr}$ , and has zeros elsewhere.

So given any  $A \in K$ ,  $E_{1i}AE_{j1} \in K$  has  $a_{ij}$  in the  $(1, 1)$  entry. That is, for every  $r \in J$ , there is a matrix  $A_r \in K$  that has  $r$  in the  $(1, 1)$  entry, and zeros elsewhere.

Now note that  $J$  is nonempty (it contains 0, since the zero matrix is in  $K$ ); that  $A_r - A_s = A_{r-s} \in K$ , so  $J$  is closed under differences; and that given any  $a \in R$ ,  $r \in J$ ,  $A_a A_r = A_{ar} \in K$ , so  $ar \in J$ ;  $A_r A_a = A_{ra}$ , so  $ra \in J$ . Thus,  $J$  is indeed an ideal of  $R$ .

Since every entry of every element of  $K$  lies in  $J$ , it follows that  $K \subseteq M_{n \times n}(J)$ . Conversely, let  $B \in M_{n \times n}(J)$ ; then  $A_{bij} \in K$  (since  $b_{ij} \in J$ ). And

$$B = \sum_{r=1}^n \sum_{s=1}^n E_{r1} A_{bij} E_{1s},$$

so  $B \in K$ . Thus,  $M_{n \times n}(J) \subseteq K$ , which proves equality.  $\square$

2. Given a function  $f: \mathbb{R} \rightarrow \mathbb{R}$ , the *support* of  $f$  is the set

$$\text{supp}(f) = \{r \in \mathbb{R} \mid f(r) \neq 0\}.$$

We say  $f$  has compact support if there exists  $N > 0$  such that  $\text{supp}(f) \subseteq [-N, N]$ . Let  $R$  be the ring of all continuous function  $f: \mathbb{R} \rightarrow \mathbb{R}$  that have compact support, with pointwise addition and multiplication. (You may take for granted that this is a ring). Show that  $R$  is a ring that does not have a unity but satisfies  $R^2 = R$ .

**Proof.** To show that  $R$  does not have a unity, we show that for every  $f \in R$  there exists  $g \in R$  such that  $g \neq 0$  and  $fg = 0$  (the zero function); since  $R$  is not the zero ring, this shows that  $R$  does not have a unity.

Let  $f \in R$ . Then there exists  $N > 0$  such that  $\text{supp}(f) \subseteq [-N, N]$ . Let  $g$  be the function

$$g(x) = \begin{cases} 0 & \text{if } x < -N - 2, \\ x + N + 2 & \text{if } -N - 2 \leq x \leq -N - 1 \\ -N - x & \text{if } -N - 1 \leq x \leq -N \\ 0 & \text{if } -N \leq x \leq N \\ x - N & \text{if } N \leq x \leq N + 1 \\ 2 - N - x & \text{if } N + 1 \leq x \leq N + 2 \\ 0 & \text{if } x \geq N + 2. \end{cases}$$

Then  $g$  is continuous,  $g \neq 0$ ,  $g$  has compact support (contained in  $[-N - 2, N + 2]$ ), but  $g(x) = 0$  for all  $x \in [-N, N]$ , so  $fg = 0$ . Thus,  $R$  does not have a unity.

However, given any  $f \in R$ , if the support of  $f$  is contained in  $[-N, N]$ , then let  $h$  be the function

$$h(x) = \begin{cases} 0 & \text{if } x < -N - 1 \\ x + N + 1 & \text{if } -N - 1 \leq x \leq -N \\ 1 & \text{if } -N \leq x \leq N \\ N + 1 - x & \text{if } N \leq x \leq N + 1 \\ 0 & \text{if } N + 1 \leq x \end{cases}$$

Then  $h$  is continuous of compact support (contained in  $[-N - 1, N + 1]$ ), and since  $h(x) = 1$  for all  $x \in [-N, N]$ , and  $f(x) = 0$  for all  $x \notin [-N, N]$ , then  $fh = f$ ; so  $f \in R^2$ . Thus,  $R \subseteq R^2 \subseteq R$ , hence  $R = R^2$ , even though  $R$  does not have a unity.  $\square$

3. Let  $R = 2\mathbb{Z}$  be the ring of even integers. Show that  $M = 4\mathbb{Z}$  is a maximal ideal, but that it is not a prime ideal.

**Proof.** Since  $4\mathbb{Z} \subseteq 2\mathbb{Z}$ , and  $4\mathbb{Z}$  is an ideal of  $\mathbb{Z}$ , then it is an ideal of  $2\mathbb{Z}$ .

If  $M \subseteq N \subseteq 2\mathbb{Z}$  is an ideal of  $2\mathbb{Z}$ , then it must be a subgroup of  $2\mathbb{Z}$ , hence a subgroup of  $\mathbb{Z}$ ; this means that  $N = a\mathbb{Z}$  for some positive integer  $a$ . Since  $4\mathbb{Z} \subseteq a\mathbb{Z} \subseteq 2\mathbb{Z}$ , it follows that  $2|a$  and  $a|4$ . The only positive integers that can satisfy these two conditions are 2 and 4, so either  $N = M$  or  $N = 2\mathbb{Z}$ . Therefore,  $M$  is a maximal ideal of  $2\mathbb{Z}$ .

However,  $M$  is not a prime ideal of  $2\mathbb{Z}$ : for  $2\mathbb{Z}$  is an ideal of itself, and  $(2\mathbb{Z})(2\mathbb{Z}) = 4\mathbb{Z} = M$ ; but  $2\mathbb{Z} \not\subseteq 4\mathbb{Z}$ . Thus,  $M$  is not a prime ideal of  $2\mathbb{Z}$ .  $\square$

4. Let  $R$  and  $S$  be rings, and let  $f: R \rightarrow S$  be a ring homomorphism.

- (i) Show that if  $f$  is surjective and  $P$  is a prime ideal of  $R$  that contains  $\ker(f)$ , then  $f(P)$  is a prime ideal of  $S$ .

**Proof.** Since  $P \neq R$  and contains  $\ker(f)$ , the Lattice Isomorphism Theorem guarantees that  $f(P) \neq S$ .

Let  $A$  and  $B$  be ideals of  $S$  such that  $AB \subseteq f(P)$ . We need to show that  $A \subseteq f(P)$  or  $B \subseteq f(P)$ . We know that  $f^{-1}(A)$ ,  $f^{-1}(B)$  are ideals of  $R$ . Now note that  $f^{-1}(A)f^{-1}(B) \subseteq f^{-1}(AB)$ : indeed, if  $x_1, \dots, x_n \in f^{-1}(A)$  and  $y_1, \dots, y_n \in f^{-1}(B)$ , then  $f(x_i) \in A$  and  $f(y_j) \in B$  for all  $i, j$ . Hence

$$f(x_1y_1 + \dots + x_ny_n) = f(x_1)f(y_1) + \dots + f(x_n)f(y_n) \in AB,$$

hence  $x_1y_1 + \cdots + x_ny_n \in f^{-1}(AB)$ .

Now, since  $AB \subseteq f(P)$ , then  $f^{-1}(AB) \subseteq f^{-1}(f(P)) = P$  (since  $P$  contains  $\ker(f)$ ). Thus,  $f^{-1}(A)f^{-1}(B) \subseteq f^{-1}(AB) \subseteq P$ . Since  $P$  is prime by assumption, it follows that  $f^{-1}(A) \subseteq P$  or  $f^{-1}(B) \subseteq P$ , and since  $f$  is onto, this implies that  $A \subseteq f(P)$  or  $B \subseteq f(P)$ . Thus,  $f(P)$  is a prime ideal of  $S$ .  $\square$

- (ii) Show that if  $Q$  is a completely prime ideal of  $S$  that does not contain  $f(R)$ , then  $f^{-1}(Q)$  is a completely prime ideal of  $R$  that contains  $\ker(f)$ .

**Proof.** Since  $Q$  does not contain  $f(R)$ , then  $f^{-1}(Q) \neq R$ . Being the inverse image of an ideal of  $S$ , we know that  $f^{-1}(Q)$  is an ideal of  $R$ . Now let  $a, b \in R$  be such that  $ab \in f^{-1}(Q)$ . Then  $f(ab) = f(a)f(b) \in Q$ . Since  $Q$  is completely prime, either  $f(a) \in Q$  or  $f(b) \in Q$ . If  $f(a) \in Q$ , then  $a \in f^{-1}(Q)$ ; if  $f(b) \in Q$ , then  $b \in f^{-1}(Q)$ . Thus,  $ab \in f^{-1}(Q)$  implies  $a \in f^{-1}(Q)$  or  $b \in f^{-1}(Q)$ , showing  $f^{-1}(Q)$  is completely prime, as claimed.  $\square$

5. Let  $R$  be a principal ideal ring, and let  $f: R \rightarrow S$  be a surjective ring homomorphism. Show that  $S$  is a principal ideal ring. Conclude that if  $R$  is a principal ideal ring, and  $I$  is an ideal of  $R$ , then  $R/I$  is a principal ideal ring.

**Proof.** Let  $K$  be an ideal of  $S$ . Then  $f^{-1}(K)$  is an ideal of  $R$ , hence  $f^{-1}(K) = (a)$  for some  $a \in R$ . We claim that  $K = (f(a))$ . Indeed, let  $s \in K$ . Since  $f$  is surjective, there exists  $x \in R$  such that  $f(x) = s$ . And since  $f(x) \in K$ , then  $x \in f^{-1}(K) = (a)$ . Therefore,  $x = ra + at + na + \sum r_i at_i$  for some  $r, t, r_i, t_i \in R, n \in \mathbb{Z}$ . Thus,

$$\begin{aligned} s &= f(x) = f\left(ra + at + na + \sum r_i at_i\right) \\ &= f(r)f(a) + f(a)f(t) + nf(a) + \sum f(r_i)f(a)f(t_i) \in (f(a)). \end{aligned}$$

Thus,  $K \subseteq (f(a))$ . Conversely, since  $a \in (a) = f^{-1}(K)$ , then  $f(a) \in K$ , so  $(f(a)) \subseteq K$ . This gives equality. Thus, every ideal of  $S$  is principal, so  $S$  is a principal ideal ring.

If  $I$  is an ideal of  $R$ , then  $\pi: R \rightarrow R/I$  is a surjective ring homomorphism ( $\pi$  is the canonical projection); by the previous paragraph, this means that if  $R$  is a principal ideal ring, then its surjective image  $R/I$  is also a principal ideal ring.  $\square$

6. Find all prime and maximal ideals of the ring  $\mathbb{Z}_{15}$  (integers modulo 15; i.e.,  $\mathbb{Z}/15\mathbb{Z}$ ), the ring  $\mathbb{Z}_{19}$ , and the ring  $\mathbb{Z}_8$ .

**Answer.** Since  $\mathbb{Z}_{15} = \mathbb{Z}/15\mathbb{Z}$ , the Lattice Isomorphism Theorem tells us that the ideals of  $\mathbb{Z}_{15}$  are precisely the ideal of  $\mathbb{Z}$  that contain  $15\mathbb{Z}$ . This also tells us that the maximal ideals of  $\mathbb{Z}_{15}$  correspond to the maximal ideals of  $\mathbb{Z}$  that contain  $15\mathbb{Z}$ ; and Problem 4 tells us that the prime ideals of  $\mathbb{Z}_{15}$  correspond to the prime ideals of  $\mathbb{Z}$  that contain  $15\mathbb{Z}$ .

If  $15\mathbb{Z} \subseteq a\mathbb{Z}$ , then 15 must be a multiple of  $a$ ; so the only possibilities are  $a = 1, a = 3, a = 5,$  and  $a = 15$ . The prime and maximal ideals are then  $(3 + 15\mathbb{Z})$  and  $(5 + 15\mathbb{Z})$ .

Proceeding as above, the ideals of  $\mathbb{Z}_{19}$  correspond to ideals of  $\mathbb{Z}$  that contain  $19\mathbb{Z}$ . The only possibilities are  $19\mathbb{Z}$  and  $\mathbb{Z}$  itself. So the only ideals of  $\mathbb{Z}_{19}$  are  $(0 + 19\mathbb{Z})$  and  $(1 + 19\mathbb{Z})$ . The former is maximal and prime.

Finally, the ideals of  $\mathbb{Z}_8$  correspond to ideals of  $\mathbb{Z}$  that contain  $(8)$ . These are  $(1), (2), (4),$  and  $(8)$ . Only  $(2)$  is maximal; so  $(2 + 8\mathbb{Z})$  is maximal and prime in  $\mathbb{Z}_8$ . None of the other ideals are completely prime, hence neither are their images.  $\square$

7. If  $m > 1$ , find all prime and maximal ideals of the ring  $\mathbb{Z}_m$  in terms of the prime factorization of  $m$ .

**Answer.** Write a prime factorization of  $m$ ,

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

with  $1 < p_1 < \dots < p_r$  primes, and  $\alpha_i > 0$  for all  $i$ .

The ideals of  $\mathbb{Z}_m$  correspond to ideals of  $\mathbb{Z}$  that contain  $m\mathbb{Z}$ , which in turn correspond to positive integer  $a$  such that  $a$  divides  $m$ . Thanks to Problem 4, we know that the image of  $a\mathbb{Z}$  in  $\mathbb{Z}_m$  is prime if and only if  $a\mathbb{Z}$  is prime, if and only if  $a = 0$  or  $a$  is prime (and since  $a > 0$ , the former cannot happen); and by the Lattice Isomorphism Theorem we know that the image is maximal if and only if  $a$  is a prime integer.

Since the only primes that divide  $m$  are the  $p_i$ , we conclude that the prime and maximal ideals of  $\mathbb{Z}_m$  are precisely the ideals  $(p_i + m\mathbb{Z})$ ,  $i = 1, \dots, r$ . This agrees with our answers in the previous problem.  $\square$

8. Let  $R$  be a ring, not necessarily commutative, and let  $P$  be a two sided ideal of  $R$  that is different from  $R$ . Prove that the following are equivalent:

- (i)  $P$  is a prime ideal of  $R$ .
- (ii) If  $r, s \in R$  are such that  $rRs = \{ras \mid a \in R\} \subseteq P$ , then  $r \in P$  or  $s \in P$ . HINT: If  $rRs \subseteq P$ , then  $(RrR)(RsR) \subseteq P$ ; and  $(a)^3 \subseteq RaR$  for all  $a \in R$ .
- (iii) If  $(r)$  and  $(s)$  are principal ideals of  $R$  such that  $(r)(s) \subseteq P$ , then  $r \in P$  or  $s \in P$ .
- (iv) If  $U$  and  $V$  are right ideals of  $R$  such that  $UV \subseteq P$ , then  $U \subseteq P$  or  $V \subseteq P$ .
- (v) If  $U$  and  $V$  are left ideals of  $P$  such that  $UV \subseteq P$ , then  $U \subseteq P$  or  $V \subseteq P$ .

**Proof.** We first prove that (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) $\implies$ (i). Then we prove (iii) $\implies$ (v) $\implies$ (i).

(i) $\implies$ (ii) Assume that  $P$  is a prime ideal of  $R$ , and that  $r, s \in R$  are such that  $rRs \subseteq P$ . We need to show that  $r \in P$  or  $s \in P$ . Now, for  $x \in R$ , we let  $RxR$  be the set of all finite sums of elements of the form  $axb$  with  $a, b \in R$ ; this is a two-sided ideal of  $R$  (it need not contain  $x$ , if  $R$  does not have a unity).

Since  $rRs \subseteq P$ , and  $RR \subseteq R$ , then  $(RrR)(RsR) = R(rRRs)R \subseteq R(rRs)R \subseteq RPR \subseteq P$ ; since  $P$  is a prime ideal and  $RrR$  and  $RsR$  are ideals, it follows that  $RrR \subseteq P$  or  $RsR \subseteq P$ .

Following the hint, next note that  $(a)^3 \subseteq RaR$  for all  $a \in R$ ; indeed, elements of  $(a)^3$  are finite sums of elements of the form

$$\left( ra + as + na + \sum r_i a s_i \right) \left( ta + au + ma + \sum t_j a u_j \right) \left( wa + az + ka + \sum w_\ell a z_\ell \right).$$

Expanding these we obtain sums in which each term is of the form  $xay$  for some  $x$  and  $y$  in  $R$ ; note that  $x$  and  $y$  may themselves contain  $a$ . For instance, the term obtained by multiplying  $ra$ ,  $ta$ , and  $wa$  is  $ratawa$ , which can be written as  $(r)a(tawa)$ , so setting  $x = r$  and  $y = tawa$  shows that it lies in  $RaR$ . The same is true for all summands, so  $(a)^3 \subseteq RaR$ , as claimed.

Thus, if  $RrR \subseteq P$ , then  $(r)^3 \subseteq P$ ; since  $P$  is prime, this implies that  $(r) \subseteq P$  (either  $(r)$  or  $(r)^2$  are contained in  $P$ ; and if  $(r)^2 = (r)(r) \subseteq P$ , then we must have  $(r) \subseteq P$ ). So  $r \in (r) \subseteq P$ , as desired. Symmetrically, if  $RsR \subseteq P$ , then  $(s)^3 \subseteq P$ , hence  $s \in (s) \subseteq P$ . In conclusion, if  $rRs \subseteq P$ , then either  $r \in P$  or  $s \in P$ , as (ii) claims.

(ii) $\implies$ (iii) Assume that  $P$  is an ideal such for all  $a, b \in R$ , if  $aRb \subseteq P$  then either  $a \in P$  or  $b \in P$ . Let  $r$  and  $s$  be elements of  $R$  such that  $(r)(s) \subseteq P$ . We want to show that either  $r \in P$  or  $s \in P$ .

Note that every element of  $rRs$  lies in  $(r)(s)$ , since for every  $x \in R$ ,  $r \in (r)$  and  $xs \in (s)$ , hence  $rxs \in (r)(s)$ . Thus,  $rRs \subseteq (r)(s) \subseteq P$ . By (ii), this implies that  $r \in P$  or  $s \in P$ , as desired.

(iii) $\implies$ (iv) Assume that for all  $r$  and  $s$ , if  $(r)(s) \subseteq P$ , then  $r \in P$  or  $s \in P$ . Let  $U$  and  $V$  be right ideals of  $R$  such that  $UV \subseteq P$ . We want to show that  $U \subseteq P$  or  $V \subseteq P$ .

If  $V \subseteq P$ , we are done. Otherwise, let  $s \in V$  be such that  $s \notin P$ . We want to show that  $U \subseteq V$ . To that end, let  $r \in U$ . We claim that  $(r)(s) \subseteq P$ . Indeed, an element of  $(r)(s)$  is a sum of products of the form

$$\left( ar + rb + nr + \sum a_i r b_i \right) \left( xs + sy + ms + \sum x_j s y_j \right);$$

each of the terms lies in  $P$ :

- $arxs = a((rx)s)$ . Since  $r \in U$ ,  $s \in V$ , and both  $U$  and  $V$  are right ideals,  $rx \in U$ ,  $rxs \in UV \subseteq P$ , and so  $arxs \in P$ .
- Similarly,  $arsy = a((rs)y) \in P$ .
- $(ar)(ms) = a(m(rs))$ ; since  $rs \in UV$ , then  $m(rs) \in UV \subseteq P$ ; hence  $(ar)(ms) \in P$ .
- $ar \sum x_j sy_j = a \sum (rx_j)(sy_j)$ ; each  $rx_j$  is in  $U$ ; each  $sy_j$  is in  $V$ , so  $\sum rx_j sy_j \in UV \subseteq P$ , hence  $a \sum rx_j sy_j \in P$ .
- $(rb)(xs) = (rbx)s \in UV \subseteq P$ .
- $(rb)(sy) = (rb)(sy) \in UV \subseteq P$ .
- $(rb)(ms) \in UV \subseteq P$ .
- $(rb) \sum x_j sy_j = \sum (rbx_j)(sy_j) \in UV \subseteq P$ .
- $(nr)(xs) = n(rx)s \in UV \subseteq P$ .
- $(nr)(sy) \in UV \subseteq P$ .
- $(nr)(ms) = nm(rs) \in UV \subseteq P$ .
- $(nr) \sum x_j sy_j = \sum (nrx_j)(sy_j) \in UV \subseteq P$ .
- $(a_i rb_i)(xs) = a_i((rb_i x)s)$ . Then  $rb_i x \in U$ ,  $s \in V$ , so  $rb_i xs \in UV \subseteq P$ , and since  $P$  is an ideal, multiplying on the left by  $a_i$  will yield an element of  $P$ .
- $(a_i rb_i)(sy) = a_i((rb_i)(sy))$ . Since  $rb_i \in U$ , and  $sy \in V$ , then  $rb_i sy \in UV \subseteq P$ ; thus, multiplying on the left by  $a_i$  yields an element of  $P$ .
- $(a_i rb_i)(ms) = a_i((rb_i)(ms))$ ; as above, this lies in  $P$  because  $rb_i \in U$ ,  $ms \in V$ , and  $UV \subseteq P$ .
- $(a_i rb_i)(x_j sy_j) = a_i((rb_i x_j)(sy_j))$ ; again,  $rb_i x_j \in U$  because  $r \in U$  and  $U$  is a right ideal; and  $sy_j \in V$ . So  $rb_i x_j sy_j \in UV \subseteq P$ , hence  $a_i rb_i x_j sy_j \in P$ .

Thus, every term is in  $P$ , so their sum is in  $P$ , as claimed.

Thus,  $(r)(s) \subseteq P$ , so by (iii) it follows that  $r \in P$  or  $s \in P$ . But  $s \notin P$ , hence  $r \in P$ .

We therefore have: for all  $r \in U$ ,  $r \in P$ . That is,  $U \subseteq P$ . This is what we wanted to prove.

(iv) $\implies$ (i) Assume that for every right ideals  $U$  and  $V$ , if  $UV \subseteq P$  then  $U \subseteq P$  or  $V \subseteq P$ . If  $A$  and  $B$  are ideals, then in particular they are right ideals, so  $AB \subseteq P$  implies  $A \subseteq P$  or  $B \subseteq P$ ; thus,  $P$  is prime.

(iii) $\implies$ (v) The argument is very similar to the one proving that (iii) implies (iv). Let  $U$  and  $V$  be left ideals such that  $UV \subseteq P$ . If  $U \subseteq P$  we are done; otherwise, let  $r \in U$  be an element such that  $r \notin P$ . We want to show that  $V \subseteq P$ . Let  $s \in V$ .

Then  $(r)(s) \subseteq P$ , arguing as in (iii) $\implies$ (iv) term by term. Hence, by (iii),  $r \in P$  or  $s \in P$ ; since  $r \notin P$  by choice of  $r$ , it follows that  $s \in P$ . Thus,  $V \subseteq P$ , as desired.

(v) $\implies$ (i) If  $A$  and  $B$  are ideals such that  $AB \subseteq P$ , then  $A$  and  $B$  are also left ideals, so by (v) it follows that  $A \subseteq P$  or  $B \subseteq P$ . Thus,  $P$  is a prime ideal, as claimed.  $\square$