

## H/wk 11, Solutions to selected problems

### Ch. 3.2, Problem 18

(a) Show that  $\mathbb{Q}(\sqrt{5}i) = \{r + s\sqrt{5}i \mid r, s \in \mathbb{Q}\}$  is a subfield of  $\mathbb{C}$ .

#### Solution.

First, we check that  $\mathbb{Q}(\sqrt{5}i)$  is a subring of  $\mathbb{C}$ .

Suppose  $z_1 = r_1 + s_1\sqrt{5}i, z_2 = r_2 + s_2\sqrt{5}i \in \mathbb{Q}(\sqrt{5}i)$  where  $r_1, s_1, r_2, s_2 \in \mathbb{Q}$  are arbitrary. Then  $z_1 + z_2 = (r_1 + r_2) + (s_1 + s_2)\sqrt{5}i \in \mathbb{Q}(\sqrt{5}i)$  and  $-z_1 = -r_1 - s_1\sqrt{5}i \in \mathbb{Q}(\sqrt{5}i)$  since  $r_1 + s_1, r_2 + s_2, -r_1, -s_2 \in \mathbb{Q}$ . We also have

$$z_1 z_2 = (r_1 + s_1\sqrt{5}i)(r_2 + s_2\sqrt{5}i) = r_1 r_2 - 5s_1 s_2 + (r_1 s_2 + r_2 s_1)\sqrt{5}i \in \mathbb{Q}(\sqrt{5}i).$$

so that  $\mathbb{Q}(\sqrt{5}i)$  is indeed a subring of  $\mathbb{C}$ . It remains to check that for every nonzero  $z \in \mathbb{Q}(\sqrt{5}i)$  we have  $\frac{1}{z} \in \mathbb{Q}(\sqrt{5}i)$ .

Let  $z = r + s\sqrt{5}i \neq 0$  be an arbitrary nonzero element of  $\mathbb{Q}(\sqrt{5}i)$ , so that  $r, s \in \mathbb{Q}$  are not both equal to zero.

Then in  $\mathbb{C}$  we have

$$\frac{1}{z} = \frac{1}{r + s\sqrt{5}i} = \frac{r - s\sqrt{5}i}{(r + s\sqrt{5}i)(r - s\sqrt{5}i)} = \frac{r - s\sqrt{5}i}{r^2 + 5s^2} = \frac{r}{r^2 + 5s^2} - \frac{s}{r^2 + 5s^2}\sqrt{5}i.$$

Thus  $\frac{1}{z} \in \mathbb{Q}(\sqrt{5}i)$  since  $\frac{r}{r^2 + 5s^2}, -\frac{s}{r^2 + 5s^2} \in \mathbb{Q}$ .

Therefore  $\mathbb{Q}(\sqrt{5}i)$  is a subfield of  $\mathbb{C}$ , as required.

(b) Show that  $\mathbb{Z}(\sqrt{5}i) = \{r + s\sqrt{5}i \mid r, s \in \mathbb{Z}\}$  is a subring of  $\mathbb{C}$  and find all the units in  $\mathbb{Z}(\sqrt{5}i)$ .

#### Solution.

Exactly the same argument as in (a) shows that  $\mathbb{Z}(\sqrt{5}i)$  is a subring of  $\mathbb{C}$ . Moreover, the argument in (a) actually gives a formula for  $z^{-1} = \frac{1}{z} \in \mathbb{Z}(\sqrt{5}i)$  in the case where  $z \in \mathbb{Z}(\sqrt{5}i)$  is a unit.

Thus we have to find out for which  $r, s \in \mathbb{Z}$  (not both zero) we have

$$\frac{1}{z} = \frac{r}{r^2 + 5s^2} - \frac{s}{r^2 + 5s^2}\sqrt{5}i \in \mathbb{Z}(\sqrt{5}i),$$

that is, for which  $r, s \in \mathbb{Z}$  (not both zero) the numbers  $\frac{r}{r^2 + 5s^2}, -\frac{s}{r^2 + 5s^2}$  are both integers.

It is clear that  $|r| \leq r^2 + 5s^2$  and  $|s| \leq r^2 + 5s^2$  and hence  $\left| \frac{r}{r^2 + 5s^2} \right| \leq 1$ ,  $\left| \frac{s}{r^2 + 5s^2} \right| \leq 1$

Thus if  $\frac{r}{r^2 + 5s^2}, -\frac{s}{r^2 + 5s^2}$  are both integers then they belong to the set  $\{-1, 0, 1\}$ . If  $\frac{r}{r^2 + 5s^2} = 0$  then  $r = 0$  (and hence  $s \neq 0$  since by assumption at least one of  $r, s$  is not zero) and therefore  $\frac{s}{r^2 + 5s^2} = \frac{1}{5s} \notin \mathbb{Z}$  since  $s \in \mathbb{Z}$  is a nonzero integer.

Thus the case  $\frac{r}{r^2 + 5s^2} = 0$  is impossible and hence  $\left| \frac{r}{r^2 + 5s^2} \right| = 1$ . Therefore  $|r| = |r^2 + 5s^2|$ . If  $s \neq 0$  then for any integers  $r, s$  we have  $|r| < |r^2 + 5s^2|$ . Hence  $s = 0$  (and hence  $r \neq 0$ ) and the condition  $|r| = |r^2 + 5s^2|$  yields  $|r| = |r^2|$ . Since  $r$  is a nonzero integer, this implies  $r = \pm 1$ .

This gives us the possibilities:  $r = 1, s = 0$  and  $r = -1, s = 0$  for the values of  $r, s$ . Each of these two possibilities in fact does yield a unit in  $\mathbb{Z}(\sqrt{5}i)$ .

The case  $r = 1, s = 0$  gives  $z = r + s\sqrt{5}i = 1$  with  $\frac{1}{z} = \frac{1}{1} = 1 \in \mathbb{Z}(\sqrt{5}i)$ . The case  $r = -1, s = 0$  gives  $z = r + s\sqrt{5}i = -1$  with  $\frac{1}{z} = \frac{1}{-1} = -1 \in \mathbb{Z}(\sqrt{5}i)$ .

Thus  $\mathbb{Z}(\sqrt{5}i)$  has exactly two units, namely 1 and  $-1$ .

### Ch. 3.2, Problem 18

Let  $p, q$  be quaternions and let  $a, b \in \mathbb{R}$ . Show that:

- (a)  $(q^*)^* = q$ . [This is an immediate corollary of the definitions]
- (b)  $(ap + bq)^* = ap^* + bq^*$  [This is an easy corollary of the definitions]
- (c)  $N(q) = qq^* = q^*q$ .

#### Solution.

Recall that for  $q = x + yi + zj + wk$  (where  $x, y, z, w \in \mathbb{R}$  we have  $N(q) = x^2 + y^2 + z^2 + w^2$  and  $q^* = x - yi - zj - wk$ .

We have:

$$\begin{aligned} qq^* &= (x + yi + zj + wk)(x - yi - zj - wk) = \\ &x^2 - xyi - xzj - xwk + xyi - y^2i^2 - yzj - ywk + xzj - yzji - z^2j^2 - zwk + \\ &\quad xwk - wyki - zwkj - w^2k^2 = \\ &x^2 + y^2 - yzk + ywj + yzk + z^2 - zwi - wyj +zwi + w^2 = x^2 + y^2 + z^2 + w^2 = N(q). \end{aligned}$$

Thus we have verified that for every quaternion  $q$  we have  $N(q) = qq^*$ .

Put  $q_1 = q^*$ . Then by definition  $N(q) = N(q_1)$ . By the above line we have  $N(q_1) = q_1q_1^*$ , which yields  $N(q) = q^*(q^*)^* = q^*q$ . Thus  $N(q) = q^*q$ , as required.

- (c)  $(pq)^* = q^*p^*$ .

#### Solution.

A direct check easily shows that  $(iq)^* = -q^*i$ ,  $(jq)^* = -q^*j$ ,  $(kq)^* = -q^*k$ . Thus for  $q = x + yi + zj + wk$  we have  $iq = xi + yi^2 + zij + wik = -y + xi - wj + zk$  and  $(iq)^* = -y - xi + wj - zk$ . On the other hand  $-q^*i = (-x + yi + zj + wk)i = -xi + yi^2 + zji + wki = -y - xi + wj - zk$ . Thus indeed  $(iq)^* = -q^*i = q^*i^*$ . The other equalities above are checked similarly.

Now let  $p$  and  $q$  be arbitrary quaternions and write  $p$  as  $p = a + bi + cj + dk$ , where  $a, b, c, d \in \mathbb{R}$ . Using (b) and the above formulas, we have:

$$\begin{aligned} (pq)^* &= ((a + bi + cj + dk)q)^* = aq^* + b(iq)^* + c(jq)^* + d(kq)^* = \\ &aq^* - bq^*i - cq^*j - dq^*k = q^*(a - bi - cj - dk) = q^*p^* \end{aligned}$$

as required.

- (c)  $N(pq) = N(p)N(q)$ .

#### Solution.

We have

$$\begin{aligned} N(pq) &= pq(pq)^* = pqq^*p^* = pN(q)p^* = && \text{since } N(q) \in \mathbb{R} \\ &pp^*N(q) = N(p)N(q), \end{aligned}$$

as required.

### Ch. 3.3, Problem 5

(a) If  $A$  is an ideal in  $R$  and  $B$  is an ideal in  $S$ , show that  $A \times B$  is an ideal in  $R \times S$ .

**Solution.**

Let  $(a_1, b_1) \in A \times B$  and  $(a_2, b_2) \in A \times B$  be arbitrary. Thus  $a_1, a_2 \in A$ ,  $b_1, b_2 \in B$ . We have  $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \in A \times B$  since  $a_1 + a_2 \in A$  and  $b_1 + b_2 \in B$  because  $A$  and  $B$  are ideals and are closed under addition. Similarly,  $-(a_1, b_1) = (-a_1, -b_1) \in A \times B$  since  $-a_1 \in A$  and  $-b_1 \in B$ .

Now let  $(a, b) \in A \times B$  and  $(r, s) \in R \times S$  be arbitrary. Thus  $a \in A$ ,  $b \in B$ . We have  $(r, s)(a, b) = (ra, sb)$ . Since  $A$  is an ideal in  $R$  and  $a \in A$ , we have  $ra \in A$ . Similarly, since  $B$  is an ideal in  $S$  and  $b \in B$ , we have  $sb \in B$ . Therefore  $(r, s)(a, b) = (ra, sb) \in A \times B$ . A similar argument shows that  $(a, b)(r, s) = (ar, bs) \in A \times B$ .

Thus  $A \times B$  is an ideal in  $R \times S$ , as claimed.

(b) Show that every ideal  $\mathcal{A}$  of  $R \times S$  has the form  $\mathcal{A} = A \times B$  where  $A$  is an ideal in  $R$  and  $B$  is an ideal in  $S$ .

**Solution.**

Put  $A = \{a \in R : (a, 0) \in \mathcal{A}\}$  and put  $B = \{b \in S : (0, b) \in \mathcal{A}\}$ . We claim that  $A$  is an ideal in  $R$  and  $B$  is an ideal in  $S$ .

Indeed, let  $r \in R$  and  $a \in A$  be arbitrary. Then  $(r, 0)(a, 0) = (ra, 0) \in \mathcal{A}$  since  $(a, 0) \in \mathcal{A}$ . Hence by definition of  $A$  we have  $ra \in A$ . Similarly,  $(a, 0)(r, 0) = (ar, 0) \in \mathcal{A}$  and hence  $ar \in A$ . Also, if  $a \in A$  then  $(a, 0) \in \mathcal{A}$  and hence  $-(a, 0) = (-a, 0) \in \mathcal{A}$  since  $\mathcal{A}$  is an ideal. Therefore by definition of  $A$  we see that  $-a \in A$ . If  $a_1, a_2 \in A$  then  $(a_1, 0), (a_2, 0) \in \mathcal{A}$  and  $(a_1, 0) + (a_2, 0) = (a_1 + a_2, 0) \in \mathcal{A}$  since  $\mathcal{A}$  is an ideal. Hence  $a_1 + a_2 \in A$  by definition of  $A$ . Thus we have verified that  $A$  is an ideal in  $R$ . A similar argument shows that  $B$  is an ideal in  $S$ .

We now claim that  $\mathcal{A} = A \times B$ . First, if  $a \in A, b \in B$  then  $(a, 0), (0, b) \in \mathcal{A}$  and hence  $(a, b) = (a, 0) + (0, b) \in \mathcal{A}$ . This shows that  $A \times B \subseteq \mathcal{A}$ .

Suppose now that  $(a, b) \in \mathcal{A}$ . Then  $(1, 0)(a, b) = (a, 0) \in \mathcal{A}$  since  $\mathcal{A}$  is an ideal. Hence  $a \in A$  by definition of  $A$ . Similarly, since  $\mathcal{A}$  is an ideal, we have  $(0, 1)(a, b) = (0, b) \in \mathcal{A}$  and hence  $b \in B$  by definition of  $B$ . Thus  $(a, b) \in A \times B$ . This shows that  $\mathcal{A} \subseteq A \times B$ . Since we have already shown that  $A \times B \subseteq \mathcal{A}$ , it follows that  $\mathcal{A} = A \times B$ .

(c) Show that the maximal ideals of  $R \times S$  are either of the form  $A \times S$  where  $A$  is a maximal ideal in  $R$  or of the form  $R \times B$  where  $B$  is a maximal ideal in  $S$ .

**Solution.**

First, we need to show that if  $A$  is a maximal ideal in  $R$  and  $B$  is a maximal ideal in  $S$  then  $A \times S$  and  $R \times B$  are maximal ideals in  $R \times S$ . Indeed, suppose that  $A \times S$  is not maximal in  $R \times S$ . Then there exists an ideal  $\mathcal{A}'$  in  $R \times S$  such that  $A \times S \subsetneq \mathcal{A}' \subsetneq R \times S$ . By part (a) we know that  $\mathcal{A}' = A' \times B'$  where  $A'$  is an ideal in  $R$  and  $B'$  is an ideal in  $S$ . Since  $A \times S \subsetneq A' \times B'$ , it follows that  $B' = S$  and  $A \subsetneq A'$ . Moreover, since  $A \times S \subsetneq A' \times S \subsetneq R \times S$ , it follows that  $A \subsetneq A' \subsetneq R$ . This contradicts the assumption that  $A$  is a maximal ideal in  $R$ . Thus indeed  $A \times S$  is a maximal ideal in  $R \times S$ . A similar argument shows that  $R \times B$  is a maximal ideal in  $R \times S$ .

Let  $\mathcal{A}$  be a maximal ideal in  $R \times S$ . By (b) we know that  $\mathcal{A} = A \times B$  where  $A$  is an ideal in  $R$  and  $B$  is an ideal in  $S$ .

First we claim that either  $A = R$  or  $B = S$ . Suppose not, that is  $A \neq R$  and  $B \neq S$ . Then  $\mathcal{A} = A \times B \subsetneq R \times B \subsetneq R \times S$ . Since  $R \times B$  is an ideal in  $R \times S$ , this contradicts maximality of  $\mathcal{A}$  in  $R \times S$ .

Thus indeed either  $A = R$  or  $B = S$ . Suppose that  $A = R$ , as the other case is similar. Thus  $\mathcal{A} = R \times B$  for some ideal  $B$  in  $S$ . We claim that  $B$  is maximal in  $S$ . Indeed, if not and if there exists an ideal  $B'$  in  $S$  such that  $B \subsetneq B' \subsetneq S$  then  $\mathcal{A} = R \times B \subsetneq R \times B' \subsetneq R \times S$ . This contradicts maximality of  $\mathcal{A}$  since  $R \times B'$  is an ideal in  $R \times S$ . Thus indeed  $B$  is a maximal ideal in  $S$  and  $\mathcal{A} = R \times B$  has the required form.

If  $B = S$  then a similar argument shows that  $\mathcal{A} = A \times S$  where  $A$  is a maximal ideal in  $R$ .

**Ch. 3.3, Problem 9** Let  $R = \mathbb{Z}(i)$ . In each case find the number of elements in the factor ring  $R/A$  and describe the cosets of  $A$ .

(a)  $A = Ri$ .

**Solution.**

Note that  $i \in A = Ri$  and hence  $(-i)i = 1 \in Ri$ . Since  $1 \in Ri$ , for every  $z \in R$  we have  $z \cdot 1 = z \in Ri$ , which shows that  $A = Ri = R$ . Thus  $R/A = R/R = \{0 + R\}$  has a single element  $0 + R$ .

(b)  $A = R(1 - i)$ . We have  $1 - i \in A$  and hence  $1 + A = i + A$ . Therefore for every  $m, n \in \mathbb{Z}$  we have  $m + ni + A = m + n + A$ . Therefore  $R/A = \{p + A : p \in \mathbb{Z}\}$ .

Also, since  $1 - i \in A$ , we have  $(1 + i)(1 - i) = 1^2 - i^2 = 2 \in A$ , so that  $2 + A = 0 + A$ . Hence if  $p, q \in \mathbb{Z}$  and  $p \equiv q \pmod{2}$  then  $p + A = q + A$ . Therefore we have

$$R/A = \{p + A : p \in \mathbb{Z}\} = \{0 + A, 1 + A\}.$$

We claim that  $0 + A \neq 1 + A$ . Indeed, if  $0 + A = 1 + A$  then  $1 \in A = R(1 - i)$  and there exist integers  $m, n$  such that  $(m + ni)(1 - i) = 1$ . Then  $1 = (m + n) + (n - m)i$  and therefore  $m - n = 0, m + n = 1$ , so that  $2m = 1$ , yielding a contradiction with the fact that  $m \in \mathbb{Z}$ . Thus  $|R/A| = 2$  and  $R/A = \{0 + A, 1 + A\}$ .

(c)  $A = R(1 + 2i)$ .

**Solution.**

We have  $3 + i = (1 - i)(1 + 2i) \in R(1 + 2i) = A$  and hence  $i + A = -3 + A$ . This implies that for any  $m, n \in \mathbb{Z}$  we have  $m + ni + A = m - 3n + A$  and therefore  $R/A = \{p + A | p \in \mathbb{Z}\}$ .

We also have  $(1 - 2i)(1 + 2i) = 5 \in R(1 + 2i) = A$ . Therefore for any integers  $p, q$  with  $p \equiv q \pmod{5}$  we have  $p + A = q + A$ . It follows that

$$R/A = \{p + A : p \in \mathbb{Z}\} = \{0 + A, 1 + A, 2 + A, 3 + A, 4 + A\}.$$

We claim that the elements  $0 + A, 1 + A, 2 + A, 3 + A, 4 + A$  of  $R/A$  are distinct. Indeed, suppose not and for some integers  $0 \leq p < q \leq 4$  we have  $p + A = q + A$ , so that  $q - p \in A$ . The possible values of  $q - p$  are  $1, 2, 3, 4$ . Since  $q - p \in A = R(1 + 2i)$ , for some  $m, n \in \mathbb{Z}$  we have  $p - q = (m + ni)(1 + 2i)$ . Therefore  $|q - p|^2 = |m + ni|^2 |1 + 2i|^2 = (m^2 + n^2) \cdot 5$ , so that  $|q - p|^2$  is divisible by 5. Since the possible values of  $q - p$  are  $1, 2, 3, 4$ , the possible values of  $|q - p|^2$  are  $1, 4, 9, 16$ , none of which are divisible by 5. This gives us a contradiction. Hence all five elements  $0 + A, 1 + A, 2 + A, 3 + A, 4 + A$  of  $R/A$  are distinct,  $|R/A| = 5$  and  $R/A = \{0 + A, 1 + A, 2 + A, 3 + A, 4 + A\}$ .

(d)  $A = R(1 + 3i)$ .

**Solution.**

Since  $1 + 3i \in A$ , we have  $1 + A = -3i + A$ . Therefore for any integers  $n, m$  we have  $n + mi + A = (-3n + m)i + A$ . It follows that  $R/A = \{pi + A | p \in \mathbb{Z}\}$ .

We also have  $(1 + 3i)(1 - 3i) = 10 \in A$  and therefore  $pi + A = qi + A$  whenever  $p, q \in \mathbb{Z}$  are such that  $p \equiv q \pmod{10}$ . This implies that

$$R/A = \{0 + A, i + A, 2i + A, 3i + A, \dots, 9i + A\}.$$

We claim that the above ten elements of  $R/A$  are all distinct. Indeed, suppose not. Then there exist integers  $q, p$  such that  $0 \leq p < q \leq 9$  and such that  $p + A = q + A$ . Hence  $p - q \in A = R(1 + 3i)$  and there exist  $n, m \in \mathbb{Z}$  such that  $q - p = (m + ni)(1 + 3i)$ . This implies that  $|q - p|^2 = |m + ni|^2 |1 + 3i|^2 = 10(m + 2 + n^2)$ , so that  $(q - p)^2$  is divisible by 10. However,  $0 \leq p < q \leq 9$ , and therefore the possible values for  $(q - p)^2$  are  $1^2, 2^2, 3^2, \dots, 9^2$ . None of these numbers are divisible by 10, yielding a contradiction.

Thus indeed  $|R/A| = 10$ , and  $R/A = \{0 + A, i + A, 2i + A, 3i + A, \dots, 9i + A\}$ .

**Ch. 3.3, Problem 25**

Let  $R$  be a commutative ring. Write  $a|b$  if  $b = ra$  for some  $r \in R$ .

(a) Show that  $Rab \subseteq Ra \cap Rb$  for all  $a, b \in R$ .

(b) If  $Ra + Rb = R$ , show that  $Rab = Ra \cap Rb$ .

**Solution.**

By part (a) we already know that  $Rab \subseteq Ra \cap Rb$ . Suppose now that  $x \in Ra \cap Rb$ . Thus  $x = r_1a = r_2b$  for some  $r_1, r_2 \in R$ . Since  $Ra + Rb = R$ , we have  $1 \in Ra + Rb$  and hence  $1 = sa + tb$  for some  $s, t \in R$ . Multiplying this equation by  $x$  we get  $x = xsa + xtb$ . We then have  $x = xsa + xsb = r_2bsa + r_1atb = (r_2s + r_1t)ab \in Rab$ . Thus  $Ra \cap Rb \subseteq Rab$ . Since we already know that  $Rab \subseteq Ra \cap Rb$ , it follows that  $Rab = Ra \cap Rb$ .

(c) Show that  $u \in R$  is a unit if and only if  $Ru = R$ .

**Solution.**

Suppose that  $Ru = R$ . Then  $1 \in Ru$  and hence  $1 = ru$  for some  $r \in R$ . Since  $R$  is commutative, we have  $1 = ru = ur$ , so that  $u$  is a unit.

Suppose that  $u$  is a unit. Then  $u^{-1}u = 1 \in Ru$ . Hence for every  $r \in R$  we have  $r = r \cdot 1 \in Ru$  since  $1 \in Ru$ . Therefore  $R = Ru$ .

(d) Show that  $Rp$  is a prime ideal if and only if  $p|ab$  implies  $p|a$  or  $p|b$ .

**Solution.**

Suppose that  $Rp$  is a prime ideal and suppose that  $p|ab$  for some  $A, B \in R$ . We have  $ab = xp \in Rp$ . Therefore, since  $Rp$  is prime, either  $a \in Rp$  or  $b \in Rp$ , that is either  $p|a$  or  $p|b$ .

Suppose now that  $p|ab$  implies  $p|a$  or  $p|b$ . Let  $a, b \in R$  be such that  $ab \in Rp$ . Hence  $ab = rp$  for some  $r \in R$ , that is  $p|ab$ . By assumption this implies that  $p|a$  or  $p|b$  and hence  $a \in Rp$  or  $b \in Rp$ . We have shown that if  $ab \in Rp$  then  $a \in Rp$  or  $b \in Rp$  and therefore  $rp$  is a prime ideal, as required.

(e) Show that if  $R$  is an integral domain, then  $Ra = Rb$  if and only if  $a = ub$  for some unit  $u \in R$ .

**Solution.**

Suppose that  $Ra = Rb$ . We need to show that  $a = ub$  for some unit  $u \in R$ . Assume that  $a \neq 0, b \neq 0$  since the case where  $a = 0$  or  $b = 0$  is easy. Then  $a \in Rb$  and  $b \in Ra$  so that  $a = rb, b = sa$  for some  $r, s \in R$ . Hence  $a = rb = rsa$  and  $a(1 - rs) = 0$ . Since  $a \neq 0$  and  $R$  is an integral domain, it follows that  $1 = rs$ . Also, since  $R$  is commutative, we have  $1 = rs = sr$ , so that  $r, s$  are units. Thus  $a = rb$ , where  $r$  is a unit, as required.

Suppose now that  $a = ub$  for some unit  $u \in R$ . Then for every  $r \in R$  we have  $ra = rub \in Rb$  and hence  $Ra \subseteq Rb$ . Similarly, since  $b = u^{-1}a$ , for every  $r \in R$  we have  $rb = ru^{-1}a \in Ra$  and hence  $Rb \subseteq Ra$ . Thus  $Ra = Rb$ , as required.

### Ch. 3.3, Problem 26

Let  $A, B, C$  be ideals in  $R$  and define

$$AB := \{a_1b_1 + \dots + a_nb_n \mid a_i \in A, b_i \in B, n \geq 1\}$$

(a) Show that  $AB$  is an ideal in  $R$  and that  $AB \subseteq A \cap B$ .

#### Solution.

Suppose that  $x, y \in AB$ . Thus  $x = a_1b_1 + \dots + a_nb_n$  and  $y = a'_1b'_1 + \dots + a'_mb'_m$  where  $a_i, a'_i \in A, b_j, b'_j \in B$ . Then  $x + y = a_1b_1 + \dots + a_nb_n + a'_1b'_1 + \dots + a'_mb'_m \in AB$  by definition of  $AB$ . Also,  $-x = (-a_1)b_1 + \dots + (-a_n)b_n \in AB$  since  $-a_i \in A, b_i \in B$ . Also, for any  $r \in R$  we have

$$rx = (ra_1)b_1 + \dots + (ra_n)b_n \in AB$$

since  $A$  is an ideal in  $R$  and  $ra_i \in A$ . Similarly,  $rx = a_1(b_1r) + \dots + a_n(b_nr) \in AB$  since  $b_i r \in B$ . Thus indeed  $AB$  is an ideal in  $R$ .

Also, if  $x = a_1b_1 + \dots + a_nb_n \in AB$  as above, then  $a_i b_i \in A$  since  $A$  is an ideal and  $a_i b_i \in B$  since  $B$  is an ideal, so that  $a_i b_i \in A \cap B$ . Since  $A \cap B$  is an ideal and each  $a_i b_i \in A \cap B$ , it follows that  $x = a_1b_1 + \dots + a_nb_n \in A \cap B$ . Thus indeed  $AB \subseteq A \cap B$ .

(b) Show that  $A(B + C) = AB + AC$  and  $(B + C)A = BA + BC$ .

#### Solution.

We will verify that  $A(B + C) = AB + AC$  as the other equality is similar. Suppose that  $x \in A(B + C)$ . Then  $x = a_1y_1 + \dots + a_ny_n$  where  $a_i \in A$  and  $y_i \in B + C$ . Hence for every  $i$  we have  $y_i = b_i + c_i$  where  $b_i \in B, c_i \in C$ . Then

$$x = a_1(b_1 + c_1) + \dots + a_n(b_n + c_n) = (a_1b_1 + \dots + a_nb_n) + (a_1c_1 + \dots + a_nc_n) \in AB + AC$$

since  $a_1b_1 + \dots + a_nb_n \in AB$  and  $a_1c_1 + \dots + a_nc_n \in AC$ . Therefore  $A(B + C) \subseteq AB + AC$ .

Suppose now that  $x \in AB + AC$ . Then  $x = s + t$  where  $s \in AB$  and  $t \in AC$ . Therefore  $s = a_1b_1 + \dots + a_nb_n$  and  $t = a'_1c_1 + \dots + a'_m c_m$  where  $a_i, a'_i \in A, b_i \in B, c_i \in C$ . Note that  $b_i, c_j \in B + C$ . Therefore

$$x = a_1b_1 + \dots + a_nb_n + a'_1c_1 + \dots + a'_m c_m \in A(B + C)$$

by definition of  $A(B + C)$ . Thus  $AB + AC \subseteq A(B + C)$ . Since we already know that  $A(B + C) \subseteq AB + AC$ , it follows that  $A(B + C) = AB + AC$ , as required.

(c) Show that  $AR = A = RA$ .

#### Solution.

We will check that  $AR = A$  as the proof of  $RA = A$  is similar.

Suppose  $a \in A$ . Then  $a = a \cdot 1 \in AR$ . This shows that  $A \subseteq AR$ .

Suppose  $x \in AR$ . Then  $x = a_1r_1 + \dots + a_nr_n$  for some  $a_i \in A$ ,  $r_i \in R$ . Since  $A$  is an ideal in  $R$ , it follows that  $a_ir_i \in A$ . Again since  $A$  is an ideal, it is closed under addition and hence  $x = a_1r_1 + \dots + a_nr_n \in A$ . Thus  $AR \subseteq A$ . Since we already know that  $A \subseteq AR$ , it follows that  $AR = A$ .

(d) Show that  $A(BC) = (AB)C$ .

**Solution.**

Let  $x \in A(BC)$ . Then  $x = a_1y_1 + \dots + a_ny_n$  for some  $a_i \in A$ ,  $y_i \in BC$ . Since  $y_i \in BC$ , we have  $y_i = b_{1,i}c_{1,i} + \dots + b_{m_i,i}c_{m_i,i}$  for some  $b_{j,i} \in B$ ,  $c_{j,i} \in C$ ,  $m_i \geq 1$ .

Then

$$x = a_1y_1 + \dots + a_ny_n =$$

$$a_1b_{1,1}c_{1,1} + \dots + a_1b_{m_1,1}c_{m_1,1} + \dots + a_nb_{1,n}c_{1,n} + \dots + a_nb_{m_n,n}c_{m_n,n} \in (AB)C$$

since  $a_ib_{j,i} \in AB$ ,  $c_{j,i} \in C$ . Thus  $A(BC) \subseteq (AB)C$ . A similar argument shows that  $(AB)C \subseteq A(BC)$  and hence  $A(BC) = (AB)C$ .