

## SOLVED PROBLEMS: SECTION 1.1

17. Show that in any ring  $R$  the commutative law for addition is redundant, in the sense that it follows from the other axioms for a ring.

*Solution:* The proof has to involve the distributive laws, because they provide the only connection between addition and multiplication in a ring. For any  $a, b \in R$ , we consider the product  $(1+a)(1+b)$  and expand it in two different ways.

$$\begin{aligned}(1+a)(1+b) &= (1+a) \cdot 1 + (1+a) \cdot b = (1 \cdot 1 + a \cdot 1) + (1 \cdot b + a \cdot b) \\ &= (1+a) + (b+ab) = 1 + ((a+b) + ab) \\ (1+a)(1+b) &= 1 \cdot (1+b) + a \cdot (1+b) = (1 \cdot 1 + 1 \cdot b) + (a \cdot 1 + a \cdot b) \\ &= (1+b) + (a+ab) = 1 + ((b+a) + ab)\end{aligned}$$

Since  $R$  is a group under addition, we can cancel 1 from the left, and then  $ab$  from the right, to obtain  $b+a = a+b$ .

*Alternate solution:* We can also use the two distributive laws to expand the product  $(a+b)(1+1)$  in two different ways. We can then cancel  $a$  from the left and  $b$  from the right to obtain  $b+a = a+b$ .

18. An element  $a \in R$  is said to be *nilpotent* if  $a^k = 0$  for some positive integer  $k$ . Determine the nilpotent elements of  $\mathbf{Z}_n$ .

*Solution:* Let  $[a]_n$  denote the congruence class modulo  $n$  of the integer  $a$ . By definition,  $([a]_n)^k = [0]$  iff  $n$  is a factor of  $a^k$ . It follows that  $([a]_n)^k = [0]$  for some exponent  $k$  iff each prime factor of  $n$  is a factor of  $a$ .

*Note:* If  $a \in R$  is nilpotent, then the smallest positive integer  $k$  with  $a^k = 0$  is called the *index of nilpotence* of  $a$ . In  $\mathbf{Z}_n$  the index of nilpotence of  $[a]_n$  can be found easily, provided the prime factorizations of  $n$  and  $a$  are known.

19. Show that for any ring  $R$  the diagonal elements  $\{(a, a) \mid a \in R\}$  form a subring of the direct sum  $R \oplus R$ .

*Solution:* The given subset is closed under addition and multiplication since  $(a, a) + (b, b) = (a+b, a+b)$  and  $(a, a) \cdot (b, b) = (ab, ab)$ . It certainly contains the identity elements  $(0, 0)$  and  $(1, 1)$ , and it is a subgroup since it contains the additive inverse  $(-a, -a)$  of each element  $(a, a)$ .

20. Let  $R$  be a ring, and let  $X$  be any subset of  $R$ . Show that the following subset is a subring of  $R$ :  $C(X) = \{r \in R \mid rx = xr \ \forall x \in X\}$ .

*Solution:* It is clear that  $1 \in C(X)$ , so the subset is nonempty. If  $a, b \in C(X)$ , then  $ax = xa$  and  $bx = xb$ , for all  $x \in X$ . It follows that  $(a+b)x = ax + bx = xa + xb = x(a+b)$ ,  $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$ , and  $(-a)x = (-1 \cdot a)x = x(-1 \cdot a) = x(-a)$ , and so  $C(X)$  is a subring of  $R$ .

21. Show that if  $\{R_\alpha\}_{\alpha \in I}$  is any collection of subrings of the ring  $S$ , then the intersection  $\bigcap_{\alpha \in I} R_\alpha$  is a subring of  $S$ .

*Solution:* Let  $\bigcap_{\alpha \in I} R_\alpha = R$ , and let  $a, b \in R$ . Then  $a, b \in R_\alpha$  for all  $\alpha$ , so  $a+b$ ,  $a-b$ , and  $ab$  belong to  $R_\alpha$  for all  $\alpha$ , since each  $R_\alpha$  is a subring. Finally, it is clear that  $1 \in \bigcap_{\alpha \in I} R_\alpha$  since  $1 \in R_\alpha$  for all  $\alpha$ .

22. Let  $\alpha$  be an algebraic integer that is a root of  $p(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$  in  $\mathbf{Z}[x]$ . Show that  $\mathbf{Z}[\alpha] = \{c_{n-1}\alpha^{n-1} + c_{n-2}\alpha^{n-2} + \cdots + c_1\alpha + c_0 \mid c_i \in \mathbf{Z}\}$  is a subring of  $\mathbf{C}$ .

*Solution:* It is easy to check that  $\mathbf{Z}[\alpha]$  is a subgroup under addition, and 1 can certainly be written in the required form. Since  $\alpha$  is a root of  $p(x)$ , we have  $p(\alpha) = 0$ , which gives us the identity  $\alpha^n = -b_{n-1}\alpha^{n-1} - \cdots - b_1\alpha - b_0$ . Multiplying this identity by  $\alpha$  and substituting for  $\alpha^n$  gives us an identity expressing  $\alpha^{n+1}$  in terms of  $\alpha^{n-1}, \alpha^{n-2}, \dots, \alpha, 1$ . We can find similar identities for  $\alpha^{n+2}, \dots, \alpha^{2n-2}$ . In multiplying two elements of  $\mathbf{Z}[\alpha]$ , the highest power of  $\alpha$  that we obtain is  $\alpha^{2n-2}$ , and so the various identities can be used to reduce any product of two elements of  $\mathbf{Z}[\alpha]$  to an expression of the required form. It follows that  $\mathbf{Z}[\alpha]$  is closed under multiplication, and thus it is a subring of the field of complex numbers.

23. Let  $R$  be a ring, let  $S$  be a subring of  $R$ , and let  $I$  be an ideal of  $R$ . Show that the following subset is a subring of  $R$ :  $S + I = \{s + a \mid s \in S, a \in I\}$ .

*Solution:* Since  $S$  is a subring of  $R$  and  $I$  is an ideal of  $R$ , each is a subgroup of  $R$  (under addition). It follows from elementary group theory that  $S + I$  is a subgroup of  $R$ . The multiplicative identity 1 belongs to  $S + I$  since it can be written in the form  $1 + 0$ , with  $1 \in S$  and  $0 \in I$ . Finally, the set is closed under multiplication since if  $s, t \in S$  and  $a, b \in I$ , then  $(s + a)(t + b) = st + (at + (s + a)b)$ . We have  $st \in S$  since  $S$  is a subring, and the elements  $at$  and  $(s + a)b$  belong to  $I$  since it is an ideal, and  $a, b \in I$ , while  $t$  and  $s + a$  belong to  $R$ .

24. Let  $a, b$  be elements of the ring  $R$ . Show that  $1 - ab$  is a unit if and only if  $1 - ba$  is a unit. If this is the case, find  $(1 - ab)^{-1}$ .

*Solution:* First assume that  $1 - ab$  is invertible, and let  $x = (1 - ab)^{-1}$ . Then  $x(1 - ab) = 1$ , so  $bx(1 - ab)a = ba$ , and therefore  $(1 - ba) + bx(1 - ab)a = 1$ . Now  $1 = (1 - ba) + bx(a - aba) = (1 - ba) + bxa(1 - ba) = (1 + bxa)(1 - ba)$ . It can be checked easily that  $(1 - ba)(1 + bxa) = 1$ , so  $(1 - ba)^{-1} = (1 + bxa)$ . A similar argument shows that if  $1 - ba$  is invertible, then so is  $1 - ab$ .

25. Prove that the ring  $R$  is commutative if  $x^2 - x \in \mathbf{Z}(R)$ , for all  $x \in R$ .

*Solution:* Let  $a, b \in R$ , and consider  $x = a + b$ . We have  $x^2 - x = (a + b)^2 - (a + b) = (a^2 - a) + (b^2 - b) + (ab + ba)$  in  $\mathbf{Z}(R)$ , along with  $a^2 - a$  and  $b^2 - b$ , so it follows that  $ab + ba \in \mathbf{Z}(R)$ . But then  $a^2b + aba = a(ab + ba) = (ab + ba)a = aba + ba^2$ , which implies that  $a^2b = ba^2$ . Since this holds for all  $b \in R$ , we have  $a^2 \in \mathbf{Z}(R)$ . Finally,  $a = a^2 - (a^2 - a) \in \mathbf{Z}(R)$ , for all  $a \in R$ .