Solutions to odd-numbered exercises
Peter J. Cameron, *Introduction to Algebra*, Chapter 2

2.1 The answers are (a) No; (b) No; (c) Yes; (d) Yes; (e) No; (f) Yes; (g) Yes; (h) No; (i) Yes; (j) No.

(a) No: The inverse law for addition (A3) fails. There is no natural number b such that $1+b=0$.

(In fact, if your convention is that zero is not a natural number, it doesn't satisfy (A2) either.)

(b) We adopted the convention that the zero polynomial doesn't have a degree, in which case this set is not a ring since (A2) fails.

If, however, you decide that 0 has degree -1 (or some such), then the set is still not a ring for $n>0$: the closure law for multiplication (M0) fails (if $n>0$). The polynomials x^n and x^n both belong to our set, but their product x^{2n} does not. [If $n=0$, then we have just the constant polynomials, in other words, the real numbers, which do indeed form a ring.]

(c) Yes: Rather than laboriously check all the axioms, let us take it for granted that real polynomials form a ring, and apply the subring test. Certainly $\mathbb{Z}[x]$ is non-empty. If $f(x)$ and $g(x)$ are polynomials in $\mathbb{Z}[x]$ (i.e. with integer coefficients), then so are $f(x)-g(x)$ and $f(x)g(x)$. So $\mathbb{Z}[x]$ passes the Second Subring Test.

Alternatively, using the theorem that the polynomials over a ring form a ring, it is clear that $\mathbb{Z}[x]$ is a ring.

(d) Yes: This set is a non-empty subset of $\mathbb{Z}[x]$, which we have just shown to be a ring; so we can apply the Subring Test again. If $f(x)$ and $g(x)$ are polynomials with integer coefficients having constant term 0, then so are $f(x)-g(x)$ and $f(x)g(x)$.

(e) No: x^2 and x^3 both belong to this set, but their product x^5 does not.

(f) Yes: Apply the Subring Test. If $f(2)=g(2)=0$, then $(f-g)(2)=f(2)-g(2)=0$ and $(fg)(2)=f(2)g(2)=0$. [We are using here the fact that, if we subtract or multiply polynomials and then make a substitution, we get the same answer as if we make the substitution and then subtract or multiply. Why is this?]

(g) Yes: If m and n are divisible by 3, then so are $m-n$ and mn.

(h) No: the matrices $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$ are both non-singular (they have determinant 1), but their sum is $\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$, which is singular. So (A0) fails.

(i) Yes: Apply the subring test (since $\mathbb{C}$ is a ring).

(j) No: This set contains $x+1$ and $x-1$ but not x^2-1, so (M0) fails.

2.3 In all cases we can apply the Subring Test since all are contained in $M_2(\mathbb{R})$.

(a) Not a ring. For $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix}$, that is, the product of symmetric matrices need not be symmetric.

(b) Not a ring. For $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, that is, the product of skew-symmetric matrices need not be skew-symmetric.

(c) This set is a ring. For, if $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $B = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$ are upper triangular, then $A - B = \begin{pmatrix} a-d & b-e \\ 0 & c-f \end{pmatrix}$ and $AB = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}$ are both upper triangular.

- This ring is not commutative, as we saw in the solution to Exercise 1.49.
- There is an identity, namely $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ which is upper triangular.
- It is not a division ring since the non-zero matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ has no inverse.

(d) This set is also a ring. The argument is similar to that in (c). This time, $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; in other words, we have a *zero ring* (all products are zero. So

- the multiplication is commutative;
- there is no identity;
- it is not a division ring.

(e) Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$. Then

$$A - B = \begin{pmatrix} a-c & b-d \\ -(b-d) & a-c \end{pmatrix} \text{ and } AB = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}.$$

Both are of the correct form to belong to the set R we are considering. So it passes the subring test. Calculation shows that the multiplication is commutative; the identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ belongs to the set; and, if a and b are not both zero, then the inverse of $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ turns out (with a little calculation) to be

$$\begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix}.$$

[Multiply it out and see!] So R is a commutative division ring, that is, a field.

Remark The ring R in part (e) is isomorphic to the field of complex numbers. Check that the rules for addition and multiplication for complex numbers $a+b\mathrm{i}$ and for matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ work in exactly the same way.

2.5 (a) We can argue informally: $m \cdot x$ is the sum of m terms equal to x. So, if we add $m \cdot x$ to $n \cdot x$, we add m xs to n xs, giving $m+n$ altogether; and if we add up $n \cdot x$ m times, the effect is to add mn xs. So the results hold.

More formally, we can use induction. We can define $n \cdot x$ by the rules:

- $1 \cdot x = x$;
- for $n \geq 1$, $(n+1) \cdot x = n \cdot x + x$.

Now let us prove the first identity by induction on n.

- Starting the induction for $n = 1$: the left-hand side is $(m+1) \cdot x$ and the right is $m \cdot x + x$, which are equal according to our definition.
- The inductive step. Suppose that $(m+n) \cdot x = m \cdot x + n \cdot x$. Then

$$\begin{aligned} (m+n+1) \cdot x &= (m+n) \cdot x + x \text{ (by definition)} \\ &= (m \cdot x + n \cdot x) + x \text{ (by the induction hypothesis)} \\ &= m \cdot x + (n \cdot x + x) \text{ (by the associative law)} \\ &= m \cdot x + (n+1) \cdot x \text{ (by definition).} \end{aligned}$$

So the result holds with $n+1$ replacing n, and is true for all n by induction.

The proof by induction of the second equation is for you to try!

(b) We have

$$\begin{aligned} n \cdot x &= x + \cdots + x \text{ (n terms)} \\ &= (1 + \cdots + 1)x \text{ (by the distributive law)} \\ &= (n \cdot 1)x \\ &= 0x \text{ (by assumption)} \\ &= 0. \end{aligned}$$

2.7 (a) Since $-x$ is the unique additive inverse of x, it is enough to show that $(-1)x$ is also an inverse of x, that is, that $x + (-1)x = 0$. This holds because

$$x + (-1)x = 1x + (-1)x = (1 + (-1))x = 0x = 0.$$

(b) Again, it suffices to show that $-y-x$ is an inverse of $x+y$:

$$(x+y) + (-y-x) = x + (y-y) - x = x + 0 - x = x - x = 0.$$

(c) Suppose that all the axioms hold except possibly the commutative law for addition. Check that the properties of inverses, and in particular the results of (a) and (b) above, both hold. (There is a bit more to be done here: for example, in (a), as well as showing that $x+(-1)x=0$, we have also to show that $(-1)x+x=0$; but the argument is quite similar.) Now we have

$$-x-y=(-1)(x+y)=-(x+y)=-y-x.$$

So addition of $-x$ and $-y$ is commutative, for any x and y. Since any element has an inverse, this actually shows that addition of arbitrary elements is commutative.

2.9. To show that $R\times S$ is a ring, it is necessary to check the ring axioms. Everything is very straightforward, since if we evaluate anything in $R\times S$, we just get the corresponding expressions in the two coordinates. For a simple case, consider (A4):

$$(r_1,s_1)+(r_2,s_2)=(r_1+r_2,s_1+s_2)=(r_2+r_1,s_2+s_1)=(r_2,s_2)+(r_1,s_1).$$

One point should be noted. When we write (r_1+r_2,s_1+s_2) or (r_1r_2,s_1s_2), the addition and multiplication in the first coordinate are those of the ring R, while those in the second coordinate are those of S. So, for example, the zero element of the ring $R\times S$ is $(0_R,0_S)$, where 0_R is the zero of R and 0_S is the zero of S. If you just write $(0,0)$, you must make clear that 0 means two different things in the two positions.

The proof of the commutative law for $R\times S$, assuming the commutative law for R and for S, is much like the proofs of the other axioms. To prove the converse (the 'only if' part), argue by contradiction. If $r_1r_2\neq r_2r_1$, then $(r_1,0)(r_2,0)\neq(r_2,0)(r_1,0)$. So, if R is not commutative, then $R\times S$ is not commutative. Similarly for S. So, if $R\times S$ is commutative, then both R and S are commutative.

The argument for the identity is similar. If 1_R and 1_S are identities in R and S respectively, then $(1_R,1_S)$ is the identity of $R\times S$. Conversely, if (u,v) is an identity of $R\times S$, then u and v are identities in R and S respectively.

The answer to the last part is: *$R\times S$ is a field if and only if one of R and S consists of just one element (namely, 0), and the other is a field.* For the forward implication, argue by contradiction. Suppose that both R and S have more than one element. Let r and s be non-zero elements of R and S respectively. Then $(r,0_S)$ and $(0_R,s)$ are non-zero elements of $R\times S$; but their product is zero, so $R\times S$ has divisors of zero, and cannot be a field. If, say, R is zero, then $R\times S$ is isomorphic to S (by means of the mapping θ defined by $(0_R,s)\theta=s$); so $R\times S$ is a field if and only if S is a field.

2.11. This exercise requires the verification of a whole list of axioms.

The displayed identity is easily checked:

$$\begin{aligned}&(a\cdot 1+b\mathrm{i}+c\mathrm{j}+d\mathrm{k})(a\cdot 1-b\mathrm{i}-c\mathrm{j}-d\mathrm{k})\\ &\quad=(a^2+b^2+c^2+d^2)\cdot 1+(ab-ba+cd-dc)\mathrm{i}\\ &\qquad+(ac-ca-bd+db)\mathrm{j}+(ad-da+bc-cb)\mathrm{k}.\end{aligned}$$

Now, letting $N=a^2+b^2+c^2+d^2$, we have

$$(a\cdot 1+b\mathrm{i}+c\mathrm{j}+d\mathrm{k})\left((a/N)\cdot 1-(b/N)\mathrm{i}-(c/N)\mathrm{j}-(d/N)\mathrm{k}\right)=1$$

if $N\neq 0$; so non-zero elements have multiplicative inverses.

2.13. We use the First Isomorphism Theorem. We define a function θ from $R[x]$ to $(R/I)[x]$ by the rule that

$$(\sum a_n x^n)\theta = \sum \overline{a_n} x^n,$$

where $\overline{a} = I + a \in R/I$; that is, θ replaces each coefficient of a polynomial by its image under the canonical homomorphism from R to R/I. Now θ is a homomorphism: for example, if $f = \sum a_n x^n$ and $g = \sum b_n x^n$, then

$$(fg)\theta = \sum_n \overline{(\sum_k a_k b_{n-k})} x^n = \sum_n (\sum_k \overline{a_k}\,\overline{b_{n-k}}) x^n = (f\theta)(g\theta),$$

with a similar but easier calculation for addition. The kernel of θ consists of all polynomials $\sum a_n x^n \in R[x]$ for which $\overline{a_n} = 0$ (that is, $a_n \in I$) for all n; this is just $I[x]$.

So $I[x]$ is an ideal of $R[x]$ and $R[x]/I[x] \cong (R/I)[x]$.

2.15. (a) Recall that $m\mathbb{Z}$ is the set of all multiples of m. If $m\mathbb{Z}$ contains $n\mathbb{Z}$ then, in particular, $n \in m\mathbb{Z}$, so n is a multiple of m, or m divides n. Conversely, if m divides n, say $n = mk$, then $nx = m(kx)$ for all x; so every element of $n\mathbb{Z}$ is in $m\mathbb{Z}$, or $m\mathbb{Z}$ contains $n\mathbb{Z}$.

(b) The Second Isomorphism Theorem says that there is a bijection between ideals of $\mathbb{Z}/60\mathbb{Z}$ and ideals of $\mathbb{Z}$ containing $60\mathbb{Z}$. Since $\mathbb{Z}$ is a PID, every ideal has the form $m\mathbb{Z}$. By (a), $m\mathbb{Z}$ contains $60\mathbb{Z}$ if and only if m divides 60. So there are 12 ideals of $\mathbb{Z}/60\mathbb{Z}$, corresponding to the twelve divisors of 60, viz. $1,2,3,4,5,6,10,12,15,20,30,60$.

Again it follows from the Second Isomorphism Theorem that maximal ideals correspond. We proved in lectures that an ideal of a PID is maximal if and only if its generator is irreducible. So there are three maximal ideals of $\mathbb{Z}/60\mathbb{Z}$, corresponding to the prime divisors $2,3,5$.

(c) By exactly the same argument, the number of ideals of $\mathbb{Z}/n\mathbb{Z}$ is the number of divisors of n, and the number of maximal ideals is the number of prime divisors.

Any divisor of $n = p_1^{a_1} \cdots p_r^{a_r}$ has the form $p_1^{b_1} \cdots p_r^{b_r}$, where b_i lies between 0 and a_i inclusive. So there are $a_i + 1$ choices of b_i for each i. These choices are independent, so we multiply them together to get the number of divisors, which is

$$(a_1 + 1) \cdots (a_r + 1).$$

(For $n = 60 = 2^2 \cdot 3^1 \cdot 5^1$, this formula gives $(2+1)(1+1)(1+1) = 12$, in agreement with (b) above.)

The number of prime divisors is clearly r.

2.17. This question really asks us to prove that the formulae for addition and multiplication of polynomials work also when we think of a polynomial as a function on the ring R, so that, letting $f(u)$ denote the result of substituting u for x, we have $(f+g)(u) = f(u) + g(u)$ and $(fg)(u) = f(u)g(u)$. Both follow easily from the axioms (but note that the second equation does require (M4), the commutative law for multiplication!)

2.19. The homomorphism is given by

$$(mn\mathbb{Z} + x)\theta = n\mathbb{Z} + x.$$

It is not clear that it is well defined (independent of the choice of coset representative). To show this, suppose that $mn\mathbb{Z}+x = mn\mathbb{Z}+y$. Then $x-y$ is divisible by mn, and so certainly by n; thus $n\mathbb{Z}+x = n\mathbb{Z}+y$, as required.

Checking that θ is a homomorphism is straightforward. It is clearly onto.

2.21. We showed in Exercise 2.3(c) that R is a ring.

We are going to prove the whole thing in one blow, using the First Isomorphism Theorem. You can prove parts (a) and (b) directly without too much difficulty, but a direct proof of (c) is harder. A useful tip is that, if you are ever asked to prove that $R/I \cong S$, find a homomorphism $\theta : R \to S$ whose kernel is I and whose image is S. This is usually much easier than fiddling round with cosets; the only problem is in finding the homomorphism.

Define $\theta : R \to R$ by

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\theta = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}.$$

(This appears to be the only reasonable definition.) Now

$$\begin{aligned}
\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right)\theta &= \begin{pmatrix} a+d & b+e \\ 0 & c+f \end{pmatrix}\theta = \begin{pmatrix} a+d & 0 \\ 0 & c+f \end{pmatrix}, \\
\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\theta + \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\theta &= \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} + \begin{pmatrix} d & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} a+d & 0 \\ 0 & c+f \end{pmatrix}.
\end{aligned}$$

Similarly

$$\begin{aligned}
\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right)\theta &= \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}\theta = \begin{pmatrix} ad & 0 \\ 0 & cf \end{pmatrix}, \\
\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\theta\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\theta &= \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} d & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & 0 \\ 0 & cf \end{pmatrix}.
\end{aligned}$$

So θ is a homomorphism.

The image of θ clearly is S, the set of all diagonal matrices. Its kernel is

$$\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} = O\right\} = I.$$

Thus, by the three parts of the First Isomorphism Theorem, we conclude that S is a subring of R; that I is an ideal of R; and that $R/I \cong S$.

2.23. Using x to denote the coset $12\mathbb{Z}+x$, the units of $\mathbb{Z}/12\mathbb{Z}$ are $1,5,7,11$ (the cosets whose representatives are coprime to 12), and so the associate classes are

$$\{0\},\{1,5,7,11\},\{2,10\},\{3,9\},\{4,8\},\{6\}.$$

2.25 If R is an integral domain, then $\deg(fg) = \deg(f) + \deg(g)$ for any two non-zero polynomials f and g in $R[x]$. For if f and g have leading terms $a_m x^m$ and $b_n x^n$ respectively, with $a_m, b_n \neq 0$, then fg has leading term $a_m b_n x^{m+n}$, and $a_m b_n \neq 0$ since R is an integral domain.

Thus, a polynomial of degree greater than 0 can never be a unit, since multiplying it by any non-zero polynomial increases the degree.

A polynomial of degree zero is a constant, and is a unit in $R[x]$ if and only if it is a unit in R.

Remark If $R = \mathbb{Z}_8$, we have

$$(1+2x)(1-2x+4x^2) = 1,$$

so that $1+2x$ is a unit. So the condition that R is an integral domain is necessary for the proof.

2.27. We have

$$\begin{aligned}&(1+x)(1-x+x^2-\cdots+(-1)^{n-1}x^{n-1})\\ &\quad = (1+x)-(x+x^2)+\cdots+(-1)^{n-1}(x^{n-1}+x^n)\\ &\quad = 1+(-1)^{n-1}x^n = 1.\end{aligned}$$

2.29. (a) If $a = x+y\mathrm{i}$ and $b = s+t\mathrm{i} \neq 0$, then

$$\frac{a}{b} = \frac{(x+y\mathrm{i})(s-t\mathrm{i})}{s^2+t^2} = \frac{xs+yt}{s^2+t^2} + \frac{ys-xt}{s^2+t^2}\mathrm{i} = u+v\mathrm{i},$$

as claimed. Now let m and n be the integers nearest to u and v respectively. Then $|u-m| \leq \frac{1}{2}$ and $|v-n| \leq \frac{1}{2}$, so

$$|(u+v\mathrm{i})-(m+n\mathrm{i}| \leq \sqrt{\tfrac{1}{2}^2+\tfrac{1}{2}^2} = 1/\sqrt{2},$$

as claimed. This means that $a = bq+r$, where $q = m+n\mathrm{i}$ and $r = b((u-m)+(v-n)\mathrm{i})$; we have

$$|r| \leq |b|/\sqrt{2} < |b|,$$

and the Euclidean property is verified.

(b) The point of this proof is that there is an element of R whose distance from any given complex number is strictly less than 1, in fact at most $1/\sqrt{2}$. This can be seen geometrically by noticing that the points of R are the vertices of the square lattice in the complex plane, and any point is at distance at most $1/\sqrt{2}$ from some corner of the square containing it. Now the Eisenstein integers are the points of the unit triangular lattice in the plane, and any point is at distance less than 1 (in fact, at most $1/\sqrt{3}$) from some corner of the triangle containing it. The rest of the proof proceeds as before.

2.31 Since $9 = 3^2$, we have to start with a field F with 3 elements (which we take to be the integers mod 3, say $\{0,1,2\}$), and an irreducible polynomial of degree 2 over F (which you can find by trial and error: there are three irreducible polynomials, one of which is x^2+1, but any one would do.) [How to check? If a quadratic polynomial is reducible, it must be a product of two factors of degree 1, and hence it must have a root in F. So we can check that x^2+1 is irreducible by noting that

$$0^2+1 = 1 \neq 0, \qquad 1^2+1 = 2 \neq 0, \qquad 2^2+1 = 2 \neq 0.]$$

Now let α be a root of the polynomial $x^2+1 = 0$. Then the elements of $K = F[x]/(x^2+1)$ have the form $c_0+c_1\alpha$, where $c_0, c_1 \in F$: there are $3^2 = 9$ such elements. We add and multiply them in the usual way, using the fact that $\alpha^2 = -1$ to ensure that no power of α higher than the first occurs.

2.33 Each coset has a unique representative of degree less than n, of the form $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, where $\alpha = (f) + x$. Each of the n coefficients $a_0, \ldots, a_{n-1}$ can be chosen to be any of the q elements of F. So there are q^n cosets.

2.35 (a) This is true by definition: R is an integral domain if and only if the product of non-zero elements cannot be zero.

(b) The proof is almost identical to that for the field of fractions of an integral domain. The ring axioms are easily checked; the embedding of R is by the map $a \mapsto [a,1]$; and $[a,b] = ab^{-1}$, since $[b,1][1,b] = [1,1]$.

2.37 (a) If I is an ideal with $a \in I$, then $na \in I$ for any element $n \in \mathbb{Z}$; and any element of the form sa, at, or s_iat_i for $s,t,s_i,t_i \in R$, belongs to I; hence any sum of such elements also belongs to I. So $\langle a \rangle \in I$. To finish the argument we have to show that the set of such elements is an ideal (in which case it is clearly the smallest). Closure under subtraction follows from $(n_1 - n_2)a = n_1a - n_2a$, $(s_1 - s_2)a = s_1a - s_2a$, $a(t_1 - t_2) = at_1 - at_2$. Closure under multiplication on the right by an element $r \in R$ follows from $(na)r = a(nr)$, $(at)r = a(tr)$, and $(s_iat_i)r = s_ia(t_ir)$. Closure under left multiplication is similar.

(b) If R has an identity then we can write na as $(n1)a$, and $sa = sa1$, $at = 1at$. So every term in the sum is of the form s_iat_i.

(c) If a is central then we can replace each term s_iat_i by $a(s_it_i)$, and na by $a(n1)$; and then

$$\sum a(s_it_i) = a\left(\sum s_it_i\right).$$

(d) In this case, $\langle a \rangle$ is the set of elements of the form $na + ar$ for $n \in \mathbb{Z}$, $a \in R$. The proof is over to you.

2.39 (a) $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$, so $1 - e$ is an idempotent.

(b) These elements are clearly idempotents. To show that $(1,0)$ is central, observe that $(1,0)(r,s) = (r,0) = (r,s)(1,0)$.

(c) Note that eR and $(1-e)R$ are ideals of R. Define a bijection θ from R to $eR \times (1-e)R$ by the rule

$$r\theta = (er, (1-e)r).$$

It is straightforward to show that θ is a homomorphism. If $r \in \mathrm{Ker}(\theta)$, then $er = (1-e)r = 0$; adding, we see that $r = 0$. So θ is injective. Now take $es \in eR$ and $(1-e)t \in (1-e)r$. Let $r = es + (1-e)t$. Then

$$\begin{aligned} er &= e^2s + e(1-e)t = es, \\ (1-e)r &= (1-e)es + (1-e)^2t = (1-e)t, \end{aligned}$$

so $r\theta = (es, (1-e)t)$. Thus θ is onto, and is an isomorphism.

2.41 Suppose that $r^n = 1$. Then

$$(1+r)(1 - r + r^2 - \cdots + (-1)^{n-1}r^{n-1}) = 1 + (-1)^{n-1}r^n = 1,$$

so $1 + r$ is a unit (we have found its inverse).