Chapter 2 solutions

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

Here are solutions to the first few. Try the rest yourself.

(a) **N** is not a ring, since (A3) fails: the additive inverse of 1 is not in **N**. (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 $n > 0$, since it contains x^n and x^n but not their product x^{2n}: that is, (M0) fails. For $n = 0$, we have just the set of constant polynomials, which does form a ring (isomorphic to **R**).

(Note that a question whose statement is open to interpretation may not have a unique answer!)

(c) $\mathbf{Z}[x]$ is a ring.

(d) This set R is a non-empty subset of $\mathbf{Z}[x]$. Moreover, if two polynomials f and g have constant term 0, then so do $f - g$ and fg. (You can show this either by writing out two general polynomials with constant term 0 and checking, or by showing that the constant term of f is just $f(0)$, the result of substituting 0 for x.) So R is a subring of $\mathbf{Z}[x]$, hence a ring.

(e) Not a ring: as in (b), condition (M0) fails. (x^4 and x^4 are in the set but x^8 is not.)

2.2. It is necessary to verify the ring axioms individually. Not all the proofs will be given in detail below. (A0) and (M0) are true by definition: the sum and product of 2×2 matrices are 2×2 matrices. (A1)

$$\begin{aligned}
\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) + \begin{pmatrix} i & j \\ k & l \end{pmatrix} &= \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} + \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
&= \begin{pmatrix} (a+e)+i & (b+f)+j \\ (c+g)+k & (d+h)+l \end{pmatrix}, \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \left(\begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} i & j \\ k & l \end{pmatrix}\right) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e+i & f+j \\ g+k & h+l \end{pmatrix} \\
&= \begin{pmatrix} a+(e+i) & b+(f+j) \\ c+(g+k) & d+(h+l) \end{pmatrix},
\end{aligned}$$

and these matrices are equal, because $(a+e)+i = a+(e+i)$ and three similar equations hold in R (since R satisfies (A0)).

(A4), (M1) and (D) are similar.

(A2): The zero matrix is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where 0 is the zero element of R.

(A3) The inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$, by a similar calculation.

2.3. (a) The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is symmetric if and only if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix},$$

that is, $b = c$. Now the matrices $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ are symmetric, but their product

$$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$$

is not; so (M0) fails.

(b) The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is symmetric if and only if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -c \\ -b & -d \end{pmatrix},$$

that is, $b = -c$ and $a = d = 0$. Now the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is skew-symmetric, but its square $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is not; so (M0) fails.

(c) Apply the Second Subring Test:

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

Both of these are upper triangular, so the test succeeds.

(d) and (e): Both of these are subrings; this is again shown by applying the Second Subring Test.

2.4. We showed that an expression like $a_1 + a_2 + \cdots + a_n$ is meaningful in a ring, because of the associative law. (The question makes no sense without this observation.)

Now, we show by induction that $a(b_1 + \cdots + b_n) = ab_1 + \cdots + ab_n$. This is true for $n = 1$ trivially, and for $n = 2$ by the distributive law. Assuming the result for $n = m$, we have

$$\begin{aligned} a(b_1 + \cdots + b_{m+1}) &= a((b_1 + \cdots + b_m) + b_{m+1}) \\ &= a(b_1 + \cdots + b_m) + ab + m + 1 \text{ by (D)} \\ &= ab_1 + \cdots + ab_m + ab_{m+1} \text{ by the inductive hypothesis.} \end{aligned}$$

So the result is proved for $n = m + 1$. Thus, it holds for all n by induction.

Similarly, $(a_1 + \cdots + a_n)b = a_1b + \cdots + a_nb$ for all n.

Now we prove the result in the problem as follows:

$$(a_1 + \cdots + a_m)(b_1 + \cdots + b_n) = a_1(b_1 + \cdots + b_n) + \cdots + a_m(b_1 + \cdots + b_n),$$

by the second result above (with $b = b_1 + \cdots + b_n$). Then expand each term on the right using the first result.

2.5. (a) $(m+n)\cdot x$ means $x+\cdots+x$ ($m+n$ times). Break this sum up into the sum of m xs and the sum of n xs, which is $m\cdot x+n\cdot x$.

Similarly, $(mn)\cdot x$ is the sum of mn xs. Break this sum into the sum of m groups each consisting of n xs. Then the sum of each group is $y=n\cdot x$, and so the total expression is $m\cdot y=m\cdot(n\cdot x)$.

[These results look like associative and distributive laws, but they are not, since m and n are positive integers, not ring elements.]

(b) Suppose that $n\cdot 1=0$, and let x be any element. Using the result we proved in Question 2, we have

$$\begin{aligned} n\cdot x &= x+\cdots+x \ (n \text{ terms}) \\ &= 1x+\cdots+1x \ (n \text{ terms}) \\ &= (1+\cdots+1)x \ (n \text{ terms in bracket}) \\ &= (n\cdot 1)x=0x=0. \end{aligned}$$

2.6. We prove this result by induction on n. For $n=1$, since $\binom{1}{0}=\binom{1}{1}=1$, the right-hand side is $x+y$, and the result is true.

Suppose that it holds for a given value n. Then

$$(x+y)^{n+1}=(x+y)^n(x+y)=\left(\sum_{i=0}^{n}\binom{n}{i}\cdot x^{n-i}y^i\right)(x+y).$$

Now the term in x^{n+1-i} in this expression is made up of two parts:

$$\left(\binom{n}{i}x^{n-i}y^i\right)x+\left(\binom{n}{i-1}x^{n-(i-1)}y^{i-1}\right)y.$$

Using the fact that x and y commute, we can move x over y^i in the first term and obtain

$$\left(\binom{n}{i}+\binom{n}{i-1}\right)x^{n+1-i}y^i=\binom{n+1}{i}x^{n+1-i}y^i,$$

using a standard identity for binomial coefficients.

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.

2.8. (a) We have $(x+x)^2 = x+x$. But, by Exercise 2.4,

$$(x+x)^2 = (x+x)(x+x) = x^2+x^2+x^2+x^2 = x+x+x+x.$$

Cancelling two of the xs gives $x+x=0$, or $x=-x$.

(b) Similarly,

$$x+y = (x+y)^2 = x^2+xy+yx+y^2 = x+xy+yx+y.$$

Cancelling $x$and y gives $xy+yx=0$, so $xy=-yx$. But $-yx=yx$ by part (a), so $xy=yx$.

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.

2.10. This is given at the end of Chapter 2.

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

The displayed identity is easily checked:

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

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.

2.12. The standard way to show that a subset of a ring is an ideal and to find the factor ring is to find a homomorphism having the given subset as its kernel. In this case, the homomorphism is not far to seek. If we denote by $\overline{a}$ the coset $I+a$ (an element of R/I), then we define a map θ on $M_n(R)$ by the rule: if $A=(a_{ij})\in M_n(R)$, then $A\theta=(\overline{a_{ij}})$. (That is, we replace each entry in the matrix by the coset containing it.) The result is a matrix whose entries belong to R/I, that is, an element of R/I. So θ maps $M_n(R)$ to $M_n(R/I)$, and it is clear that it is onto.

Now θ is a homomorphism. For example, the (i,j) entry in $(AB)\theta$ is

$$\overline{\sum_{k=1}^{n} a_{ik}b_{kj}}=\sum_{k=1}^{n}\overline{a_{ik}}\,\overline{b_{kj}},$$

the equality holding since the map $a\to\overline{a}$ is a homomorphism (in fact, the canonical homomorphism from R to R/I). Addition is similar but easier.

Finally, the kernel of θ consists of all matrices (a_{ij}) for which $\overline{a_{ij}}=0$ (that is, $a_{ij}\in I$) for all i and j: this is just $M_n(I)$.

We conclude from the First Isomorphism Theorem that $M_n(I)$ is an ideal if $M_n(R)$ and that $M_n(R)/M_n(I)\cong M_n(R/I)$.

2.13. As in 2.12, we use the First Isomorphism Theorem. We define a function θ from $R[x]$ to $(R/I)[x]$ by the rule that

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

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 $f=\sum a_nx^n$ and $g=\sum b_nx^n$, then

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

with a similar but easier calculation for addition. The kernel of θ consists of all polynomials $\sum a_nx^n\in R[x]$ 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 $R[x]/I[x]\cong(R/I)[x]$.

2.14. As in the Hint, let E_{ij} be the matrix with entry 1 in the ith row and jth column and entries 0 elsewhere. If $A=(a_{ij})$ is any matrix, then we have $A=\sum_{i=1}^n\sum_{b=1}^n a_{ij}E_{ij}$. Now it is easy to check that

$$E_{ij}E_{kl}=\begin{cases}E_{il} & \text{if } j=k,\\ O & \text{otherwise.}\end{cases}$$

From this it follows that $E_{ki}AE_{jl}$ is as claimed.

Now let J be an ideal of $M_n(R)$, and let I be the set of elements of R which appear in the first row and column of some matrix in J. Now, if $A\in J$, then $E_{11}AE_{11}=a_{11}E_{11}\in J$; so I has an alternative description:

$$I=\{a:aE_{11}\in J\}.$$

From this and the facts that

$$\begin{aligned} aE_{11} + bE_{11} &= (a+b)E_{11}, \\ (aE_{11})(bE_{11}) &= abE_{11}, \end{aligned}$$

we see that I is an ideal. Moreover, for any i and j, and any $a \in I$, we have $E_{i1}(aE_{11})E_{1j} = aE_{ij} \in J$. Taking the sum over i and j of suitable matrices of this form, we see that $M_n(I) \subseteq J$.

Conversely, if $A = (a_{ij}) \in J$, then for any i and j we have

$$E_{1i}AE_{j1} = a_{ij}E_{11} \in J,$$

so that $a_{ij} \in I$. Thus $J \subseteq M_n(I)$, and we have $J = M_n(I)$ as required.

2.15. (a) Recall that (m) is the set of all multiples of m. If (m) contains (n) then, in particular, $n \in (m)$, 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) is in (m), or (m) contains n.

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

(c) By exactly the same argument, the number of ideals of $\mathbf{Z}/(n)$ 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.

2.16. (a) Let $R = \{a + b\mathrm{i} : a, b \in \mathbf{Z}\}$. Then R is non-empty and, for any $a + b\mathrm{i}, c + d\mathrm{i} \in R$, we have

$$\begin{aligned} (a + b\mathrm{i}) - (c + d\mathrm{i}) &= (a - c) + (b - d)\mathrm{i} \in R, \\ (a + b\mathrm{i})(c + d\mathrm{i}) &= (ac - bd) + (ad + bc)\mathrm{i} \in R, \end{aligned}$$

since $a - c, b - d, ac - bd, ad + bc \in \mathbf{Z}$ for all $a, b, c, d \in \mathbf{Z}$. So R is a subring of $\mathbf{C}$.

(b) The easiest way to prove this requires some case-by-case argument. Let R denote the set of Eisenstein integers as in the question. Take two elements $x = a + b\sqrt{-3}$ and $y = c + d\sqrt{-3}$ in R. There are four cases:

(1) $a, b, c, d \in \mathbf{Z}$;

(2) $a, b, c - \frac{1}{2}, d - \frac{1}{2} \in \mathbf{Z}$;

(3) $a - \frac{1}{2}, b - \frac{1}{2}, c, d \in \mathbf{Z}$; and

(4) $a - \frac{1}{2}, b - \frac{1}{2}, c - \frac{1}{2}, d - \frac{1}{2} \in \mathbf{Z}$.

The arguments are similar in all cases; I will consider case 3. We have $(a-c) - \frac{1}{2}, (b-d) - \frac{1}{2} \in \mathbf{Z}$, so $x - y \in R$. For the product, let $a = m + \frac{1}{2}, b = n + \frac{1}{2}$, where m and n are integers. Then

$$xy = ((m+\tfrac{1}{2})c - 3(n+\tfrac{1}{2})d) + ((m+\tfrac{1}{2})d + (n+\tfrac{1}{2})d)\sqrt{3}.$$

Let $p = (m+\frac{1}{2})c - 3(n+\frac{1}{2})d$ and $q = (m+\frac{1}{2})d + (n+\frac{1}{2})c$. It is clear that each of p and q is either an integer or an integer plus $\frac{1}{2}$. So it is enough to prove that $p - q$ is an integer. But

$$p - q = (m-n)(c-d) + 4(n+\tfrac{1}{2})d \in \mathbf{Z},$$

as required.

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!)

2.18. This is an algebraist's construction of the complex numbers: we *define* $\mathbf{C} = \mathbf{R}[x]/(x^2+1)\mathbf{R}[x]$. See Sections 2.4 and 6.1 of the book.

The fact that θ is a homomorphism follows, either by the same arguments that were used in Question 2.17, or by the result of that question (taking $\mathbf{R}$ as a subring of $\mathbf{C}$, and taking $u = \mathrm{i}$ in the result of the question).

The image is clearly $\mathbf{C}$, since $(a+bx)\theta = a + b\mathrm{i}$.

The kernel of θ consists of all real polynomials f such that $f(\mathrm{i}) = 0$. Now, if f is a multiple of x^2+1, say $f(x) = (x^2+1)g(x)$, then clearly $f(\mathrm{i}) = 0$. Conversely, suppose that $f(\mathrm{i}) = 0$. Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$. Then

$$f(\mathrm{i}) = a_0 + a_1\mathrm{i} + a_2\mathrm{i}^2 + \ldots = 0.$$

Taking the complex conjugate, and using the fact that all the coefficients $a_0, a_1, a_2, \ldots$ are real, we have

$$f(-\mathrm{i}) = a_0 - a_1\mathrm{i} + a_2\mathrm{i}^2 - \ldots = 0.$$

Thus both i and $-\mathrm{i}$ are roots of f. By the Remainder Theorem, f is divisible by $(x-\mathrm{i})(x+\mathrm{i}) = x^2+1$, as required.

Note: we have used various properties of the complex numbers in the proof. Does this matter if we are intending to use this result as a definition of $\mathbf{C}$?

2.19. The homomorphism is given by

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

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

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

2.20. Remember that $\mathcal{P}(X)$ means the set of all subsets of X; addition is symmetric difference, and multiplication is intersection.

To show that θ is a homomorphism, we have to show that

$$\begin{aligned}(A+B)\theta &= A\theta + B\theta,\\ (AB)\theta &= A\theta B\theta.\end{aligned}$$

If we translate the ring operations, and also put in the fact that $A\theta = A\cap Y$, then what we have to show is

$$\begin{aligned}(A\triangle B)\cap Y &= (A\cap Y)\triangle(B\cap Y),\\ (A\cap B)\cap Y &= (A\cap Y)\cap(B\cap Y).\end{aligned}$$

The second is clear from properties of intersection; the first can be proved by an argument like this. The left-hand side consists of all elements which lie in either A or B but not both, and also lie in Y. These are precisely the elements which lie *either* in A and Y *or* in B and Y *but not in both.* But this is just the description of the right-hand side. (Draw a Venn diagram and mark the two sets in.)

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 $R/I \cong S$.

2.22. Let R be a commutative ring with identity. If x is both a zero-divisor and a unit, then there exist y and z such that $yx = 1$ and $xz = 0$, with $z \neq 0$. But we have

$$z = 1z = (yx)z = y(xz) = y0 = 0,$$

contrary to assumption.

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

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

2.24 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.

Since 1 has degree zero, it follows that any unit u must have degree zero, and so must be a non-zero constant polynomial. And, if $uv = 1$, then u is a unit in R.

2.25. This depends on some facts about determinants; if you do not know these facts, you may wish to defer this question until Chapter 4. A solution is given for (b), since (a) is a special case of (b).

Since $\det(AB) = \det(A)\det(B)$ and $\det(I) = 1$, we see that, if A is a unit, then $\det(A)$ is a unit. Conversely, suppose that $\det(A)$ is a unit. If A^* denotes the transposed matrix of cofactors of A, then

$$AA^* = A^*A = \det(A)I,$$

so the matrix $(\det(A))^{-1}A^*$ is an inverse of A.

2.26. We have

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

2.27. (a) This can be done by the Euclidean algorithm, but there is an easier way. $x^2+3x+2 = (x+1)(x+2)$ is a factorisation into irreducibles. Using the Remainder Theorem, we see that neither $x+1$ nor $x+2$ divides $x^5+2x^4+5x^3+6x+2$. So the greatest common divisor is 1.

2.28. (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.

2.29. (a) Suppose that the Gaussian integer $x + y\mathrm{i}$ is a unit: say $(x+y\mathrm{i})(u+v\mathrm{i}) = 1$. Taking the complex conjugate, $(x-y\mathrm{i})(u-v\mathrm{i}) = 1$. Multiplying, we obtain $(x^2 + y^2)(u^2+v^2) = 1$. Since x and y are integers, this implies that $x^2 + y^2 = 1$, whence either $x = \pm 1$, $y = 0$, or $x = 0$, $y = \pm 1$. So there are four units, namely $1, -1, \mathrm{i}, -\mathrm{i}$.

(b) Suppose that the Gaussian integer $x + y\mathrm{i}$ is irreducible. If $y = 0$, then x must be an integer prime, say $x = p$; and, moreover, p cannot be a sum of two squares, since if $p = a^2 + b^2$ then we would have the factorisation $p = (a+b\mathrm{i})(a-b\mathrm{i})$ in the Gaussian integers, with neither factor a unit (by part (a)).

On the other hand, suppose that $\neq 0$. Then $x - y\mathrm{i}$ is also irreducible, since if we had a factorisation of it then taking the complex conjugate would give a factorisation of $x + \mathrm{i}$. We claim that $p = x^2 + y^2$ is an integer prime. If it had a proper factorisation in the integers, say

$$p = x^2 + y^2 = q_1 q_2 \cdots q_r,$$

then we could factorise each q_i into irreducibles in the Gaussian integers and obtain two different factorisations of p, contrary to the fact that the Gaussian integers form a Euclidean domain (by Problem 2.28(a)).

From the fact that $\mathbf{R}[x]$ is a principal ideal domain, we know that the ideal (f,g) is equal to (d), where d is the greatest common divisor of f and g. Since $d = 1$, we see that (f,g) consists of all multiples of 1; that is, it is the whole ring $\mathbf{R}[x]$.

2.30. 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.

2.31 If either polynomial could be factorised, then it would have a linear factor, and hence a root in $F=\mathbf{Z}/2\mathbf{Z}$. But neither 0 nor 1 is a root of either polynomial.

The corresponding fields are isomorphic. Indeed, we claim that, in the field $F(\alpha)$ where $\alpha^3+\alpha+1=0$, the element $\beta=\alpha^3$ satisfies $\beta^3+\beta^2+1=0$. To see this, we calculate the powers of α to form a 'table of logarithms' for the field:

$$\begin{aligned}\alpha^3&=\alpha+1\\ \alpha^4&=\alpha^2+\alpha\\ \alpha^5&=\alpha^2+\alpha+1\\ \alpha^6&=\alpha^2+1\\ \alpha^7&=1=\alpha^0\end{aligned}$$

Hence

$$\beta^3+\beta^2+1=\alpha^9+\alpha^6+1=\alpha^2+(\alpha^2+1)+1=0.$$

2.32. 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.

2.33. (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 $[b,1][1,b]=[1,1]$.