Rings and Fields Answers

1. (a) Defining $(f+g)(t) = f(t) + g(t)$ for $f,\, g \in R$, $t \geq 0$ we have $f + g \in R$ for all $f,\, g \in R$ (because the sum of continuous functions is continuous). So this gives us a binary operation $+$ on R. It is associative and commutative because addition on $\mathbb{R}$ is associative and commutative. It has an identity $\mathbf{0}$, the function with constant value 0, because this function is continuous (so belongs to R) and 0 is the identity of $(\mathbb{R}, +)$. Defining $(-f)(t) = -f(t)$ for $f \in R$, $t \geq 0$ we have $-f \in R$ for every $f \in R$ (because a scalar multiple of a continuous function is continuous) and $(-f) + f = \mathbf{0} = f + (-f)$ for every $f \in R$. Thus $(R, +)$ is an abelian group.

(b) The given definition of $f * g$ gives a continuous function (indeed, a differentiable one, by the fundamental theorem of calculus) for all $f,\, g \in R$, so is a binary operation.

To determine $(f * g) * h$, where f, g and $h \in R$, consider

$$\begin{aligned}
((f*g)*h)(t) &= \int_0^t (f*g)(u)h(t-u)du \\
&= \int_0^t \big(\int_0^v f(v)g(u-v)h(t-u)dv\big)du \\
&= \int_0^t \big(\int_v^t f(v)g(u-v)h(t-u)du\big)dv \\
&= \int_0^t \big(\int_0^{t-v} f(v)g(w)h(t-v-w)dw\big)dv \\
&= \int_0^t f(v)(g*h)(t-v)dv \\
&= (f*(g*h))(t).
\end{aligned}$$

(In the formulae above, we use the substitution $w = u - v$.) Thus $*$ is associative.

(c) To determine $f * (g + h)$ we have

$$\begin{aligned}
(f*(g+h))(t) &= \int_0^t f(u)(g+h)(t-u)du \\
&= \int_0^t f(u)g(t-u)du + \int_0^t f(u)h(t-u)du \\
&= (f*g)(t) + (f*h)(t).
\end{aligned}$$

(The point here is that integration is additive.) Thus $f * (g + h) = f * g + f * h$ for all $f,\, g,\, h \in R$. Similarly $(f + g) * h = f * h + g * h$.

(d) Multiplication is commutative because

$$\begin{aligned}
(f*g)(t) &= \int_0^t f(u)g(t-u)du = \int_0^t f(t-w)g(w)dw \\
&= \int_0^t g(w)f(t-w)dw = (g*f)(t).
\end{aligned}$$

(e) Finally, there is a function $f \in R$ such that $f(0) = 1$, but for any $g \in R$ we have $(f * g)(0) = \int_0^0 f(u)g(-u)du = 0$, so that $f * g \neq f$; thus no $g \in R$ can be a multiplicative identity.

2. (a) A *ring* is a set R together with two binary operations $+, \cdot$ such that
(i)(α) $x + y \in R$ for all $x, y \in R$;
(β) $(x + y) + z = x + (y + z)$ for all $x, y, z \in R$;
(γ) there is an additive identity $0 \in R$ such that $x + 0 = 0 + x = x$ for all $x \in R$;
(δ) for every $x \in R$ there is an additive inverse $-x \in R$ such that $(-x) + x = x + (-x) = 0$;
(ϵ) $x + y = y + x$ for all $x, y \in R$;
(ii)(α) $xy \in R$ for all $x, y \in R$;
(β) $(xy)z = x(yz)$ for all $x, y, z \in R$;
(iii)(α) $x(y + z) = xy + xz$ for all $x, y, z \in R$;
(β) $(x + y)z = xz + yz$ for all $x, y, z \in R$.

(b)(i) Taking ordinary matrix addition and multiplication, this is a ring.
(ii) Taking ordinary matrix addition and multiplication, this is not a ring; it fails (a-i-α).
(iii) Taking ordinary addition and multiplication, this is not a ring; it fails (a-i-γ).
(iv) Taking addition and multiplication mod 12, this is a ring.
(v) Not a ring; it fails (a-ii-β).
(vi) Taking ordinary matrix addition and multiplication, this is not a ring; it fails (a-ii-α).
(vii) Taking symmetric difference for addition and intersection for multiplication, this is a ring.
(viii) Not a ring; it fails (a-iii-α).

3. (a) A *ring* is a set R together with two binary operations $+, \cdot$ such that
(i)(α) $x + y \in R$ for all $x, y \in R$;
(β) $(x + y) + z = x + (y + z)$ for all $x, y, z \in R$;
(γ) there is an additive identity $0 \in R$ such that $x + 0 = 0 + x = x$ for all $x \in R$;
(δ) for every $x \in R$ there is an additive inverse $-x \in R$ such that $(-x) + x = x + (-x) = 0$;
(ϵ) $x + y = y + x$ for all $x, y \in R$;
(ii)(α) $xy \in R$ for all $x, y \in R$;
(β) $(xy)z = x(yz)$ for all $x, y, z \in R$;
(iii)(α) $x(y + z) = xy + xz$ for all $x, y, z \in R$;
(β) $(x + y)z = xz + yz$ for all $x, y, z \in R$.

A *subring* of R is a set $S \subseteq R$ such that
$x + y \in S$ for all $x, y \in S$;
$0 \in S$;
$-x \in S$ for all $x \in S$;
$xy \in S$ for all $x, y \in S$.

(b) Let R be the set of group homomorphisms from G to itself.

(i) For ϕ, $\psi \in R$ define $\phi + \psi : G \to G$ by setting $(\phi + \psi)(x) = \phi(x) + \psi(x)$ for all $x \in G$.

(α) If ϕ, $\psi \in R$, $\phi + \psi \in R$. **P** For any x, $y \in G$ we have

$$(\phi + \psi)(x + y) = \phi(x + y) + \psi(x + y) = (\phi(x) + \phi(y)) + (\psi(x) + \psi(y))$$

because ϕ and ψ are homomorphisms

$$= (\phi(x) + \psi(x)) + (\phi(y) + \psi(y))$$

because G is abelian

$$= (\phi + \psi)(x) + (\phi + \psi)(y). \mathbf{Q}$$

(β) If ψ, ϕ and $\chi \in R$, then for any $x \in G$ we have

$$\begin{aligned}((\psi + \phi) + \chi)(x) &= (\phi + \psi)(x) + \chi(x) = (\phi(x) + \psi(x)) + \chi(x)\\ &= \phi(x) + (\psi(x) + \chi(x)) = (\phi + (\psi + \chi))(x),\end{aligned}$$

so $(\phi + \psi) + \chi = \phi + (\psi + \chi)$.

(γ) Set $\mathbf{0}(x) = 0$, the identity of G, for every $x \in G$. Then $\mathbf{0}(x + y) = 0 = \mathbf{0}(x) + \mathbf{0}(y)$ for all x, $y \in G$ so $\mathbf{0} \in R$. If now $\phi \in R$ we have

$$(\phi + \mathbf{0})(x) = \phi(x) + \mathbf{0}(x) = \phi(x) + 0 = \phi(x) = 0 + \phi(x) = \mathbf{0}(x) + \phi(x) = (\mathbf{0} + \phi)(x)$$

for all $x \in G$, so $\phi + \mathbf{0} = \phi = \mathbf{0} + \phi$.

(δ) If $\phi \in R$, define $-\phi : G \to G$ by setting $(-\phi)(x) = -\phi(x)$ for all $x \in G$. Then for any x, $y \in G$

$$\begin{aligned}(-\phi)(x + y) &= -(\phi(x + y)) = -(\phi(x) + \phi(y)) = -\phi(y) + (-\phi(x))\\ &= -\phi(x) + (-\phi(y)) = (-\phi)(x) + (-\phi(y)),\end{aligned}$$

so $-\phi \in R$. Next, for any $x \in G$,

$$\begin{aligned}(\phi + (-\phi))(x) &= \phi(x) + (-\phi)(x) = \phi(x) - \phi(x) = 0 = \mathbf{0}(x)\\ &= -\phi(x) + \phi(x) = (-\phi + \phi)(x),\end{aligned}$$

so $\phi + (-\phi) = \mathbf{0} = -\phi + \phi$.

(ϵ) If ϕ, $\psi \in R$ and $x \in G$, then

$$(\phi + \psi)(x) = \phi(x) + \psi(x) = \psi(x) + \phi(x) = (\psi + \phi)(x),$$

so $\phi + \psi = \psi + \phi$.

(ii) For ϕ, $\psi \in R$ define $\phi\psi : G \to G$ by setting $(\phi\psi)(x) = \phi(\psi(x))$ for all $x \in G$.

(α) $\phi\psi \in R$ for all ϕ, $\psi \in R$ because the composition of two group homomorphisms is a homomorphism.

(β) $(\phi\psi)\chi = \phi(\psi\chi)$ for all ϕ, ψ, $\chi \in R$ because composition of functions is associative.

(iii)(α) If ϕ, ψ, $\chi \in R$ and $x \in G$ then

$$\begin{aligned}(\phi(\psi + \chi))(x) &= \phi((\psi + \chi)(x)) = \phi(\psi(x) + \chi(x)) = \phi(\psi(x)) + \phi(\chi(x))\\ &= (\phi\psi)(x) + (\phi\chi)(x) = (\phi\psi + \phi\chi)(x);\end{aligned}$$

as x is arbitrary, $\phi(\psi + \chi) = \phi\psi + \phi\chi$.

(β) If ϕ, ψ, $\chi \in R$ and $x \in G$ then

$$((\phi + \psi)\chi)(x) = (\phi + \psi)(\chi(x)) = \phi(\chi(x)) + \psi(\chi(x)) = (\phi\chi)(x) + (\psi\chi)(x) = (\phi\chi + \psi\chi)(x);$$

as x is arbitrary, $(\phi + \psi)\chi = \phi\chi + \psi\chi$.

(c) A function $T : V \to V$ is linear iff it is a homomorphism of the additive group and moreover
$$T(\alpha v) = \alpha T v$$
for all $v \in V$ and all $\alpha \in F$, the field of scalars.

(i) If S, T are linear then
$$(S+T)(\alpha v) = S(\alpha v) + T(\alpha v) = \alpha S v + \alpha T v = \alpha(Sv + Tv) = \alpha(S+T)(v)$$
for all $v \in V$, $\alpha \in F$. So $S + T$ is linear.

(ii) Defining $\mathbf{0}$ as above we have
$$\mathbf{0}(\alpha v) = 0 = \alpha \mathbf{0}(v)$$
for all α, v, so $\mathbf{0}$ is linear.

(iii) If $T : V \to V$ is linear, then defining $-T$ as above we have
$$(-T)(\alpha v) = -T(\alpha v) = -\alpha T v = \alpha(-Tv) = \alpha(-T)v$$
for all α, v, so $-T$ is linear.

(iv) If S and T are linear then
$$(ST)(\alpha v) = S(T(\alpha v)) = S(\alpha T(v)) = \alpha S(T(v))) = \alpha(ST)(v)$$
for all α, v, so ST is linear.

4. If R is a ring, an *ideal* of R is a set $I \subseteq R$ such that
$x+y \in I$ for all $x, y \in I$;
$0 \in I$;
$-x \in I$ for all $x \in I$;
ax, $xa \in I$ for all $x \in I$, $a \in R$.

(a)(i) Consider the relation $\equiv$ on R defined by saying

$$x \equiv y \text{ if } x-y \in I.$$

Then $\equiv$ is an equivalence relation on R. **P** (α) $x-x=0 \in I$ so $x \equiv x$ for every $x \in I$. (β) If $x \equiv y$ then $y-x=-(x-y) \in I$ so $y \equiv x$. (γ) If $x \equiv y$ and $y \equiv z$ then $x-z=(x-y)+(y-z) \in I$ and $x \equiv z$. **Q**

(ii) If $x \equiv x'$ and $y \equiv y'$ then $x+y \equiv x'+y'$ and $xy \equiv x'y'$. **P** (α) $(x+y)-(x'+y') = (x-x')+(y-y') \in I$. (β) $xy-x'y' = (x-x')(y-y')+x'(y-y')+(x-x')y' \in I$. **Q**

(iii) Because $\equiv$ is an equivalence relation it splits R into equivalence classes. Write $a^\bullet$ for the equivalence class of $a \in R$, so that $a^\bullet = b^\bullet$ iff $a \equiv b$. Write R/I for the set $\{a^\bullet : a \in R\}$ of equivalence classes.

Now part (ii) tells us that we can define addition and multiplication on R/I by the formulae

$$a^\bullet + b^\bullet = (a+b)^\bullet, \quad , a^\bullet b^\bullet = (ab)^\bullet.$$

(iv) Thus we have two binary operations on R/I and R/I is closed under both. If a, b, $c \in R$ then
$(a^\bullet + b^\bullet) + c^\bullet = (a+b)^\bullet + c^\bullet = ((a+b)+c)^\bullet = (a+(b+c))^\bullet = a^\bullet + (b+c)^\bullet = a^\bullet + (b^\bullet + c^\bullet)$.
$a^\bullet + 0^\bullet = (a+0)^\bullet = a^\bullet = (0+a)^\bullet = 0^\bullet + a^\bullet$.
$a^\bullet + (-a)^\bullet = (a+(-a))^\bullet = 0^\bullet = (-a+a)^\bullet = (-a)^\bullet + a^\bullet$.
$a^\bullet + b^\bullet = (a+b)^\bullet = (b+a)^\bullet = b^\bullet + a^\bullet$.
$(a^\bullet b^\bullet)c^\bullet = (ab)^\bullet c^\bullet = ((ab)c)^\bullet = (a(bc))^\bullet = a^\bullet (bc)^\bullet = a^\bullet(b^\bullet c^\bullet)$.
$(a^\bullet + b^\bullet)c^\bullet = (a+b)^\bullet c^\bullet = ((a+b)c)^\bullet = (ac+bc))^\bullet = (ac)^\bullet + (bc)^\bullet = (a^\bullet c^\bullet) + (b^\bullet c^\bullet)$.
$a^\bullet(b^\bullet + c^\bullet) = a^\bullet(b+c)^\bullet = (a(b+c))^\bullet = (ab+ac)^\bullet = (ab)^\bullet + (ac)^\bullet = (a^\bullet b^\bullet) + (a^\bullet c^\bullet)$.
Thus R/I is a ring, with zero $0^\bullet$ and negatives $-(a^\bullet) = (-a)^\bullet$.

(b) aR is always a subring of R; it is an ideal iff $bx \in aR$ whenever $x \in aR$, $b \in R$; a sufficient condition for this is that $ab = ba$ for every $b \in R$.

(c)**Apology:** Question should read 'If R is a ring with $\mathbf{1} \ldots$'.

For matrices $\mathbf{A}$ in $M_n(R)$, let their coefficients be a_{ij}. If J is an ideal of $M_n(R)$, set $I = \{a_{11} : \mathbf{A} \in J\} \subseteq R$. If $\mathbf{A}+\mathbf{B} = \mathbf{C}$ then $c_{11} = a_{11} + b_{11}$, so I is closed under addition. Considering the zero matrix $\mathbf{0}$, we see that $0 \in I$. If $\mathbf{A} \in J$ then $-\mathbf{A} \in J$; so if $a \in I$ then $-a \in I$. If $a \in I$ and $b \in R$, take some $\mathbf{A} \in J$ such that $a = a_{11}$, and let $\mathbf{B} \in M_n(R)$ be the matrix with top left coefficient b, all others zero; then $\mathbf{AB}$, $\mathbf{BA}$ have top left coefficients ab, ba respecively, and belong to J, so ab and ba belong to I.

Thus I is an ideal of R. For i, $j \le n$ let $\mathbf{E}_{ij}$ be the matrix with (i,j) coefficient 1, all others 0. Now observe that if $\mathbf{A} \in J$ and i, $j \le n$, then $\mathbf{E}_{1i}\mathbf{A}\mathbf{E}_{j1}$ belongs to J and has top left coefficient a_{ij}. Thus $a_{ij} \in I$. As $\mathbf{A}$, i and j are arbitrary, $J \subseteq M_n(I)$.

Finally, if $\mathbf{A} \in M_n(I)$, then for each (i,j) choose $\mathbf{A}_{ij} \in J$ such that the top left coefficient of $\mathbf{A}_{ij}$ is a_{ij}. Now $\mathbf{E}_{i1}\mathbf{A}_{ij}\mathbf{E}_{1j}$ belongs to J and has (i,j) coefficient a_{ij}, all others 0; so $\mathbf{A} = \sum_{i,j \le n} \mathbf{E}_{i1}\mathbf{A}_{ij}\mathbf{E}_{1j} \in J$. Thus J is precisely $M_n(I)$.

(d) Every member of R can be uniquely expressed as the sum of a member of I and a zero-one matrix. So there are $2^4 = 16$ equivalence classes. Because $\mathbf{E}_{11}\mathbf{E}_{12} = \mathbf{E}_{12} \notin I$, and $\mathbf{E}_{12}\mathbf{E}_{11} = \mathbf{0}$, $\mathbf{E}_{11}^\bullet \mathbf{E}_{12}^\bullet \ne \mathbf{E}_{12}^\bullet \mathbf{E}_{11}^\bullet$, so R/I is not commutative.

5. (a) If R and S are rings, a function $\phi : R \to S$ is a *homomorphism* if $\phi(x+y) = \phi(x) + \phi(y)$, $\phi(xy) = \phi(x)\phi(y)$ for all x, $y \in R$.

If R is a ring, a *subring* of R is a set $S \subseteq R$ such that $0 \in S$ and $x+y$, $-x$, $xy \in S$ for all x, $y \in S$.

An *ideal* of R is a set $I \subseteq R$ which is a subring and moreover is such that ax, $xa \in I$ for all $x \in I$, $a \in R$.

If R and S are rings, a function $\phi : R \to S$ is an *isomorphism* if it is a bijective homomorphism.

(b) If R is a ring and I an ideal of R, we have an equivalence relation $\equiv$ on R given by $x \equiv y$ if $x - y \in I$. If $x \equiv x'$ and $y \equiv y'$ then $x + y \equiv x' + y'$ and $xy \equiv x'y'$. Consequently we may define addition and multiplication on the set R/I of equivalence classes under $\equiv$ by setting $x^\bullet + y^\bullet = (x+y)^\bullet$, $x^\bullet y^\bullet = (xy)^\bullet$ for all x, $y \in R$, writing $x^\bullet \in R/I$ for the equivalence class of $x \in R$. Under this multiplication and addition R/I is a ring.

(c)(i) If x, $y \in I$ and $a \in R$ then

$\phi(x+y) = \phi(x) + \phi(y) = 0 + 0 = 0$, so $x + y \in I$;
$\phi(0) = 0$, so $0 \in I$;
$\phi(-x) = -\phi(x) = -0 = 0$, so $-x \in I$;
$\phi(xa) = \phi(x)\phi(a) = 0\phi(a) = 0$, so $xa \in I$;
$\phi(ax) = \phi(a)\phi(x) = \phi(a)0 = 0$, so $ax \in I$.

Thus I is an ideal.

(ii) If a, $b \in \phi[R]$, take x, $y \in R$ such that $\phi(x) = a$ and $\phi(y) = b$; then

$a + b = \phi(x+y) \in \phi[R]$;
$0 = \phi(0) \in \phi[R]$;
$-a = \phi(-x) \in \phi[R]$;
$ab = \phi(xy) \in \phi[R]$.

Thus S is a subring.

(d) If $\phi(r) = s$ then $\theta(s) = \{x : \phi(r) = \phi(x)\} = \{x : \phi(x-r) = \phi(x) + \phi(-r) = 0\} = \{x : x - r \in I\} = \{x : x \equiv r\} = r^\bullet$. Thus $\theta(s) \in R/I$ for all $s \in \phi[R]$. If s_1, $s_2 \in \phi[R]$ take r_1, r_2 such that $\phi(r_1) = s_1$ and $\phi(r_2) = s_2$; then $\phi(r_1 r_2) = s_1 s_2$ so $\theta(s_1 s_2) = (r_1 r_2)^\bullet = r_1^\bullet r_2^\bullet = \theta(s_1)\theta(s_2)$; similarly $\theta(s_1 + s_2) = \theta(s_1) + \theta(s_2)$. Thus θ is a homomorphism. Also, if $\theta(s_1) = \theta(s_2)$, then $r_1^\bullet = r_2^\bullet$ so $r_1 \equiv r_2$ and $r_1 - r_2 \in I$ and $s_1 - s_2 = \phi(r_1 - r_2) = 0$ and $s_1 = s_2$; thus θ is injective. Finally, every member of R/I is of the form $r^\bullet = \theta(\phi(r))$ so θ is surjective. So θ is an isomorphism.

6. No answer written out.

7. Note first that we can define na, for $n \in \mathbb{Z}$ and $a \in R$, as follows. First, take $0a = 0$; next, set $(n+1)a = na+a$ for each integer $n \geq 0$; this defines na for all integers $n \geq 0$. It is easy to prove by induction that $(m+n)a = ma + na$, $m(a+b) = ma + mb$, $(mn)a = m(na)$ and $m(ab) = (ma)b = a(mb)$ for all a, $b \in R$ and all integers m, $n \geq 0$. Next, for integers $m < 0$ and $a \in R$, define ma to be $-((-m)a)$, where $(-m)a$ is defined as just above and $-((-m)a)$ is the additive inverse of $(-m)a$ in R. A straightforward check (considering several cases individually) shows that now $m(a+b) = ma + mb$, $(m+n)a = ma + na$, $(mn)a = m(na)$ and $m(ab) = (ma)b = a(mb)$ for all m, $n \in \mathbb{Z}$ and a, $b \in R$.

Define $+$, $\times$ on R_1 by setting

$$(me + a) + (ne + b) = (m+n)e + (a+b),$$
$$(me + a) \times (ne + b) = mne + (mb + na + ab),$$

using the rules above to define ma, nb. A routine check shows that this makes R_1 a ring; for instance, for the associative law of multiplication, we have

$$\begin{aligned}
((me+a) \times (ne+b)) \times (pe+c) &= (mne + (mb+na+ab)) \times (pe+c) \\
&= mnpe + mnc + p(mb+na+ab) + (mb+na+ab)c \\
&= mnpe + npa + mpb + mnc + mbc + nac + pab + abc \\
&= mnpe + m(nc+pb+bc) + npa + a(nc+pb+bc) \\
&= (me+a) \times (npe + (nc+pb+bc)) \\
&= (me+a) \times ((ne+b) \times (pe+c)).
\end{aligned}$$

To see that R_1 has a $\mathbf{1}$, consider $\mathbf{1} = 1e + 0$; then $\mathbf{1} \times (me+a) = 1me + 1a + m0 + 0a = me + a = m1e + m0 + 1a + a0 = (me+a) \times \mathbf{1}$ for all m, a, so that $\mathbf{1}$ is a multiplicative identity of R_1, and of course it is not the zero of R_1, which is $0e + 0$.

The map $a \mapsto 0e + a : R \to R_1$ is an injective ring homomorphism, so its image is a subring of R_1 which is a copy of R.

Apology: It is not true that if R is an integral domain so is R_1. Consider, for instance, the case $R = \mathbb{Z}$. Then we see that

$$(1e + 0) \times (0e + (-1)) = 0e + 0,$$

so that R_1 has zero divisors.

8. (a) A *ring* is a set R together with two binary operations $+$, $\cdot$ such that
   (i)(α) $x + y \in R$ for all x, $y \in R$;
   (β) $(x + y) + z = x + (y + z)$ for all x, y, $z \in R$;
   (γ) there is an additive identity $0 \in R$ such that $x + 0 = 0 + x = x$ for all $x \in R$;
   (δ) for every $x \in R$ there is an additive inverse $-x \in R$ such that $(-x) + x = x + (-x) = 0$;
   (ϵ) $x + y = y + x$ for all x, $y \in R$;
   (ii)(α) $xy \in R$ for all x, $y \in R$;
   (β) $(xy)z = x(yz)$ for all x, y, $z \in R$;
   (iii)(α) $x(y + z) = xy + xz$ for all x, y, $z \in R$;
   (β) $(x + y)z = xz + yz$ for all x, y, $z \in R$.

An *ideal* of a ring R is a set $I \subseteq R$ such that
   $x + y \in I$ for all x, $y \in I$;
   $0 \in I$;
   $-x \in I$ for all $x \in I$;
   ax, $xa \in I$ for all $x \in I$, $a \in R$.

An *integral domain* is a ring R such that
   multiplication in R is commutative;
   R has a multiplicative identity $1 \neq 0$;
   if $ab = 0$ then at least one of a, b is 0.

(b) For f, $g \in R$ define $f + g : [0, 1] \to \mathbb{R}$ and $f \times g : [0, 1] \to \mathbb{R}$ by setting $(f + g)(t) = f(t) + g(t)$, $(f \times g)(t) = f(t)g(t)$ for all $t \in [0, 1]$. Then $f + g$, $f \times g$ belong to R because the sum and product of continuous functions is always continuous.

Addition in R is associative and commutative because addition on $\mathbb{R}$ is associative and commutative. It has an identity $\mathbf{0}$, the function with constant value 0, because this function is continuous (so belongs to R) and 0 is the identity of $(\mathbb{R}, +)$. Defining $(-f)(t) = -f(t)$ for $f \in R$, $t \geq 0$ we have $-f \in R$ for every $f \in R$ (because a scalar multiple of a continuous function is continuous) and $(-f) + f = \mathbf{0} = f + (-f)$ for every $f \in R$. Thus $(R, +)$ is an abelian group.

Multiplication in R is associative and commutative because mulitplication in $\mathbb{R}$ is associative and commutative. It has an identity $\mathbf{1}$, the function with constant value 1, because this function is continuous (so belongs to R) and 1 is the identity of $(\mathbb{R}, .)$; and of course $\mathbf{1} \neq \mathbf{0}$ because $[0, 1]$ is not empty.

Finally multiplication in R is distributive over addition because multiplication in $\mathbb{R}$ is distributive over addition.

R is not an integral domain because, for instance, $f \times g = \mathbf{0}$ where

$$f(t) = 1 - 2t \text{ for } t \in [0, \tfrac{1}{2}],\ 0 \text{ for } t \in [\tfrac{1}{2}, 1],$$
$$g(t) = 0 \text{ for } t \in [0, \tfrac{1}{2}],\ 2t - 1 \text{ for } t \in [\tfrac{1}{2}, 1].$$

(c) R/I is not an integral domain because if we take $f(t) = \sqrt{t}$ for $t \in [0, 1]$, then $f \notin I$ but $f \times f = e \in I$; consequently, writing $f^\bullet \in R/I$ for the equivalence class of f, we have $f^\bullet \neq 0^\bullet$, the zero of R/I, while $f^\bullet \times f^\bullet = e^\bullet = 0^\bullet$.

(d) If f, $g \in J$ and $h \in R$ then $(f + g)(0) = f(0) + g(0) = 0$, $(-f)(0) = -f(0) = 0$, $(f \times h)(0) = (h \times f)(0) = f(0)h(0) = 0$; thus $f + g$, $-f$, $f \times h$ all belong to J; also $\mathbf{0}(0) = 0$ so $\mathbf{0} \in J$.

Defining $\phi : R \to \mathbb{R}$ by $\phi(f) = f(0)$ we see that ϕ is a homomorphism with kernel J and image $\mathbb{R}$. By the First Isomorphism Theorem, R/J is isomorphic to $\mathbb{R}$.

9. (a) A **1** is a multiplicative identity not equal to 0.

If e, e' are both multiplicative identities in a ring R, then $e = ee' = e'$; so that R can have at most one multiplicative identity.

In a ring R with **1**, an *invertible element* is an element $x \in R$ with an *inverse* y such that $xy = yx = \mathbf{1}$. If y, y' are both inverses of x, then

$$y = y1 = y(xy') = (yx)y' = 1y' = y',$$

so $y = y'$.

If x, y are both invertible, with inverses x^{-1} and y^{-1}, then

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1x^{-1} = xx^{-1} = 1,$$
$$(y^{-1}x^{-1})xy) = y^{-1}(x^{-1}x)y = y^{-1}1y = y^{-1}y = 1,$$

so xy is also invertible. Thus the set U of invertible elements is closed under multiplication. $11 = 1$ so $1 \in U$ and is the identity of U. If $x \in U$ then $xx^{-1} = x^{-1}x = 1$ so x is the inverse of x^{-1} and $x^{-1} \in U$; of course x^{-1} is the inverse of x in U, so every element of U has an inverse in U and U is a group.

(b) (i) An *integral domain* is a ring R such that
multiplication in R is commutative;
R has a **1**;
if $ab = 0$ then at least one of a, b is 0.

A *field* is a commutative ring with **1** in which every non-zero element is invertible.

(ii) If R is a finite integral domain, take any non-zero $a \in R$. Consider the map $x \mapsto ax : R \to R$. If $ax = ax'$ then $a(x - x') = ax - ax' = 0$; because R is an integral domain, $x - x' = 0$, i.e., $x = x'$. Thus the map $x \mapsto ax$ is injective. Because R is finite, it must also be surjective. In particular, there is an $x \in R$ such that $ax = 1$, the identity of R. Because R is commutative, $xa = 1$ and x is the inverse of a. As a is arbitrary, R is a field.

(iii) $\mathbb{Z}$ is an integral domain but not a field; 2 has no inverse. If we take $R = \mathbb{Z}$, $a = 2$ in the argument above, the map $x \mapsto ax = 2x$ is still injective, but it is not surjective; this is possible because $\mathbb{Z}$ is infinite.

10. (a) A *ring* is a set R together with two binary operations $+$, $\cdot$ such that
(i)(α) $x + y \in R$ for all x, $y \in R$;
(β) $(x + y) + z = x + (y + z)$ for all x, y, $z \in R$;
(γ) there is an additive identity $0 \in R$ such that $x + 0 = 0 + x = x$ for all $x \in R$;
(δ) for every $x \in R$ there is an additive inverse $-x \in R$ such that $(-x) + x = x + (-x) = 0$;
(ϵ) $x + y = y + x$ for all x, $y \in R$;
(ii)(α) $xy \in R$ for all x, $y \in R$;
(β) $(xy)z = x(yz)$ for all x, y, $z \in R$;
(iii)(α) $x(y + z) = xy + xz$ for all x, y, $z \in R$;
(β) $(x + y)z = xz + yz$ for all x, y, $z \in R$.

An *integral domain* is a ring R such that
multiplication in R is commutative;
R has a **1** (that is, a multiplicative identity not equal to 0);
if $ab = 0$ then at least one of a, b is 0.

A *field* is a commutative ring with **1** in which every non-zero element is invertible.

(b) Let R be an integral domain.

(i) Let us observe first that we have a cancellation law: if $ab = ac$ and $a \neq 0$ then $b = c$. **P** $0 = ab - ac = a(b - c)$; as $a \neq 0$, $b - c$ must be 0, i.e., $b = c$. **Q**

(ii) Let X be the set $R \times (R \setminus \{0\})$. On X define a relation $\sim$ by saying

$$(a, b) \sim (a', b') \text{ if } ab' = ba'.$$

Then $\sim$ is an equivalence relation on X. **P** (α) $ab = ba$ so $(a, b) \sim (a, b)$ for all $(a, b) \in X$. (β) If $(a, b) \sim (a', b')$ then $b'a = ab' = ba' = a'b$ so $(a', b') \sim (a, b)$. (γ) If $(a, b) \sim (a', b')$ and $(a', b') \sim (a'', b'')$ then $b'ab'' = ab'b'' = ba'b'' = bb'a'' = b'ba''$; as $b' \neq 0$, $ab'' = ba''$ and $(a, b) \sim (a'', b'')$. **Q**

(iii) Let F be the set of equivalence classes in X for $\sim$. For $(a, b) \in X$ write $\frac{a}{b} \in F$ for the equivalence class containing (a, b); thus $\frac{a}{b} = \frac{a'}{b'}$ iff $ab' = ba'$.

(iv) If $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$. **P** Note first that as $bd \neq 0$, $b'd' \neq 0$, $\frac{ad+bc}{bd}$ and $\frac{a'd'+b'c'}{b'd'}$ are defined in F. Now examine

$$(ad + bc)b'd' = adb'd' + bcb'd' = ab'dd' + bb'cd' = ba'dd' + bb'dc'$$
$$= bda'd' + bdb'c' = bd(a'd' + b'c').\textbf{Q}$$

Consequently we can define an operation $+$ on F by writing

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

whenever (a, b), $(c, d) \in X$.

(v) If $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then $\frac{ac}{bd} = \frac{a'c'}{b'd'}$. **P** As before, $\frac{ac}{bd}$ and $\frac{a'c'}{b'd'}$ are defined in F because bd and $b'd'$ are non-zero. Now

$$acb'd' = ab'cd' = ba'dc' = bda'c',$$

as required. **Q** Consequently we may define an operation $\times$ on F by writing

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

whenever (a, b) and (c, d) belong to X.

(vi) We have already seen that $+$ is a binary operation on F taking values in F. Now

(α) $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} + \frac{cf+de}{df} = \frac{adf+b(cf+de)}{bdf} = \frac{adf+bcf+bde}{bdf} = \frac{(ad+bc)f+bde}{bdf} = \frac{ad+bc}{bd} + \frac{e}{f} = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$, so addition on F is associative.

(β) Writing $0_F = \frac{0}{1}$, we have

$$\frac{a}{b} + 0_F = \frac{a1+b0}{b1} = \frac{a}{b} = \frac{0b+1a}{1b} = 0_F + \frac{a}{b}$$

for all $(a, b) \in X$, so 0_F is an additive identity for F.

(γ) If $(a, b) \in X$, then

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab+b(-a)}{b^2} = \frac{ab-ba}{b^2} = \frac{0}{b^2} = \frac{-ab+ab}{b^2} = \frac{(-a)b+ab}{b^2} = \frac{-a}{b} + \frac{a}{b},$$

while $\frac{0}{b^2} = \frac{0b^2}{1b^2} = \frac{0}{1} = 0_F$, so $\frac{-a}{b}$ is an additive inverse of $\frac{a}{b}$.

(δ) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$, so addition on F is commutative.

(ϵ) We have already seen that $\times$ is a binary operation on F. Now for any (a, b), (c, d), $(e, f) \in X$, $\frac{a}{b} \times (\frac{c}{d} \times \frac{e}{f}) = \frac{a}{b} \times \frac{ce}{df} = \frac{ace}{bdf} = \frac{ac}{bd} \times \frac{e}{f} = (\frac{a}{b} \times \frac{c}{d}) \times \frac{e}{f}$, so multiplication on F is associative.

(ζ) $\frac{a}{b} \times (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \times \frac{cf+de}{df} = \frac{a(cf+de)}{bdf} = \frac{acf+ade}{bdf} = \frac{bacf+bade}{b^2df} = \frac{acbf+bdae}{bdbf} = \frac{ac}{bd} + \frac{ae}{bf} = (\frac{a}{b} \times \frac{c}{d}) + (\frac{a}{b} \times \frac{e}{f})$, and similarly $(\frac{a}{b} + \frac{c}{d}) \times \frac{e}{f} = (\frac{a}{b} \times \frac{e}{f}) + (\frac{c}{d} \times \frac{e}{f})$, so multiplication in F is distributive over addition.

Thus $(F, +, \times)$ is a ring.

(vii) To see that F is a field, we need to check the following:

(α) $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \times \frac{a}{b}$, so $\times$ is commutative.

(β) Set $1_F = \frac{1}{1}$. Because $1.1 = 1 \neq 0 = 1.0$, $1_F \neq 0_F$. If $\frac{a}{b} \in F$, $\frac{a}{b} \times 1_F = \frac{a1}{b1} = \frac{a}{b} = \frac{1a}{1b} = 1_F \times \frac{a}{b}$, so 1_F is a multiplicative identity for F.

(γ) Suppose that $\frac{a}{b} \in F \setminus \{0_F\}$. Then $a = a1 \neq b0 = 0$ so $(b, a) \in X$. Now $\frac{a}{b} \times \frac{b}{a} = \frac{ab}{ba} = \frac{ab1}{ab1} = \frac{1}{1} = 1_F = \frac{b}{a} \times \frac{a}{b}$, so $\frac{b}{a}$ is a multiplicative inverse for $\frac{a}{b}$. As $\frac{a}{b}$ is arbitrary, F is a field.

(c) If R is the ring of Gaussian integers, then F can be identified with the set of complex numbers of the form $\frac{m+ni}{p+qi}$, where m, n, p, $q \in \mathbb{Z}$ and p, q are not both 0. Now $\frac{m+ni}{p+qi} = \frac{(m+ni)(p-qi)}{p^2+q^2} = \frac{mp+nq}{p^2+q^2} + \frac{np-mq}{p^2+q^2}i$ is of the form $r + si$ where r, $s \in \mathbb{Q}$; and conversely, if r, $s \in \mathbb{Q}$, $r + is$ can be expressed as $\frac{m+ni}{p}$ where m, n and p are integers. Thus F is precisely the set of complex numbers with both real and imaginary parts rational.

11. No answer written out.

12. (a) An *integral domain* is a ring R such that
multiplication in R is commutative;
R has a $\mathbf{1}$, that is, a multiplicative identity $1 \neq 0$;
if $ab = 0$ then at least one of a, b is 0.

A *Euclidean domain* is an integral domain R with a *Euclidean valuation* $\nu : R \setminus \{0\} \to \{0, 1, 2, \ldots\}$ such that
$\nu(a) \leq \nu(ab)$ for all $a, b \in R \setminus \{0\}$;
for all $a \in R$, $b \in R \setminus \{0\}$ there are q, $r \in R$ such that $a = bq + r$ and either $r = 0$ or $\nu(r) < \nu(b)$.

If R is a ring, an *ideal* of R is a set $I \subseteq R$ such that
$x + y \in I$ for all $x, y \in I$;
$0 \in I$;
$-x \in I$ for all $x \in I$;
ax, $xa \in I$ for all $x \in I$, $a \in R$.

(b) If $I = \{0\}$ then $I = 0R$. Otherwise, set $m = \min\{\nu(x) : x \in I \setminus \{0\}\} \geq 0$ and take $a \in I \setminus \{0\}$ such that $\nu(a) = m$. Because I is an ideal, $aR \subseteq I$. Now let b be any member of I. Then there are q, $r \in R$ such that $b = aq + r$ and either $r = 0$ or $\nu(r) < \nu(a) = m$. But $r = b - aq \in I$, so by the definition of m the second alternative is impossible, and $r = 0$; thus $b = aq \in aR$. As b is arbitrary, $I \subseteq aR$ and $I = aR$.

(c)(i) Not an integral domain;

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(ii) A Euclidean domain; take $\nu(n) = |n|$ for $n \neq 0$.

(iii) A Euclidean domain; take $\nu(p)$ to be the degree of p for any non-zero polynomial p.

(iv) $\mathbb{Z}[x]$ is an integral domain ($R[x]$ is an integral domain for any integral domain R) but is not a Euclidean domain, because the ideal $\{p :$ the constant coefficient of p is even$\}$ is not of the form $p\mathbb{Z}[x]$ for any $p \in \mathbb{Z}[x]$.

(v) As in (iv), $\mathbb{R}[x, y]$ is an integral domain, but it is not a Euclidean domain because $\{p : p$ is not constant$\}$ is a non-principal ideal.

(vi) Not an integral domain, as it has no $\mathbf{1}$.

13. No answer written out.

14. (a) Let R be any ring. Write $R[x]$ for the set of all expressions

$$p = p_0 + p_1 x + p_2 x^2 + \dots$$

where $p_0, p_1, \dots$ belong to R and all but finitely many of them are zero. Define addition and multiplication on $R[x]$ by writing

$$(p_0 + p_1 x + p_2 x^2 + \dots) + (q_0 + q_1 x + q_2 x^2 + \dots) \\ = (p_0 + q_0) + (p_1 + q_1)x + (p_2 + q_2)x^2 + \dots ,$$

$$(p_0 + p_1 x + p_2 x^2 + \dots)(q_0 + q_1 x + q_2 x^2 + \dots) \\ = (p_0 q_0) + (p_1 q_0 + p_0 q_1)x + (p_2 q_0 + p_1 q_1 + p_0 q_2)x^2 + \dots ;$$

generally, the coefficient of x^n in $p + q$ is $p_n + q_n$, while the coefficient of x^n in pq is $\sum_{i=0}^{n} p_{n-i} q_i$.

It is easy to check that $R[x]$ is an abelian group under addition, with its zero the polynomial with all coefficients 0, and the additive inverse of $p = p_0 + p_1 x + \dots$ the polynomial $(-p_0) + (-p_1)x + (-p_2)x^2 + \dots$. To check the associativity of multiplication, let $p = p_0 + p_1 x + \dots$, $q = q_0 + q_1 x + \dots$, $r = r_0 + r_1 x + \dots$ be three polynomials, and consider $(pq)r$ and $p(qr)$. The coefficient of x^n in $(pq)r$ is

$$\sum_{i=0}^{n} \Bigl(\sum_{j=0}^{n-i} p_{n-i-j} q_j\Bigr) r_i = \sum_{i=0}^{n} \Bigl(\sum_{k=i}^{n} p_{n-k} q_{k-i}\Bigr) r_i$$

(substituting $k = i + j$ in the internal sum)

$$= \sum_{k=0}^{n} \sum_{i=0}^{k} p_{n-k} q_{k-i} r_i ,$$

which is the coefficient of x^n in $p(qr)$; so $(pq)r = p(qr)$. The distributive law in $R[x]$ is now easy to check.

(b) If R is an integral domain, an element p of R is *irreducible* if it is not 0, not invertible and whenever $p = ab$ then one of a, b is invertible.

If R is an integral domain, an element of R is *prime* if it is not 0, not invertible and whenever p is a factor of a product ab then it is a factor of at least one of a, b.

A *principal ideal domain* is an integral domain R such that every ideal in R is of the form aR for some $a \in R$.

Suppose now that $R[x]$ is a principal ideal domain.

(i) If a, $b \in R$ then consider the polynomials $\hat{a} = a + 0x + 0x^2 + \dots$, $\hat{b} = b + 0x + 0x^2 + \dots$; we have $\hat{a}\hat{b} = ab + 0x + \dots$ and $\hat{b}\hat{a} = ba + 0x + \dots$. But $R[x]$ is commutative, so $ab = ba$; as a and b are arbitrary, R is commutative.

(ii) $R[x]$ has a **1** of the form $e = e_0 + e_1 x + \dots \neq 0 + 0x + \dots$; so $R \neq \{0\}$. If $a \in R$, then $e\hat{a} = \hat{a} = \hat{a}e$, so that, in particular, $e_0 a = a = a e_0$; thus e_0 is a multiplicative identity for R; as $R \neq \{0\}$, $e_0 \neq 0$ and R has a **1**.

(iii) Now take any non-zero $a \in R$ and consider

$$I = \{p : p \in R[x],\ a \text{ divides } p_0\}.$$

Then I is an ideal of $R[x]$ so is of the form $qR[x]$ for some $q \in R[x]$. Now $\hat{a} \in I$, so is expressible as qp, and $0 + e_0 x + 0x^2 + \dots \in I$, so is expressible as qr. We have $q_0 p_0 = a$, $q_0 r_0 = 0$ and $q_0 r_1 + q_1 r_0 = e_0$. Because $q_0 p_0 = a \neq 0$, $q_0 \neq 0$. Next, because $q_0 r_0 = 0$ in R, $\hat{q}_0 \hat{r}_0 = 0_{R[x]}$; but $R[x]$ is an integral domain and $\hat{q}_0 \neq 0_{R[x]}$, so $\hat{r}_0 = 0_{R[x]}$ and $r_0 = 0$. So $q_0 r_1 = e_0$. But also $q = qe \in I$ so q_0 is divisible by a; say $q_0 = ab$; then $abr_1 = e_0$. As R is commutative, br_1 is a multiplicative inverse of a. As a is arbitrary, R is a field.

15. No answer written out.

16. No answer written out.

17. (a) $(m+n\omega)+(m'+n'\omega)=(m+m')+(n+n')\omega$ so R is closed under addition; $0=0+0\omega\in R$; $-(m+n\omega)=(-m)+(-n)\omega$ so $-z\in R$ for every $z\in R$ and R is a subgroup of $(\mathbb{C},+)$. Finally, $\omega^2=-1-\omega$ so $(m+n\omega)(m'+n'\omega)=(mm'-nn')+(mn'+nm'-nn')\omega$ and R is closed under multiplication.

(b) For $m+n\omega\in R\setminus\{0\}$ set $\nu(m+n\omega)=|m+n\omega|^2=(m-\frac{1}{2}n)^2+\frac{3}{4}n^2=m^2-mn+n^2\in\mathbb{N}$. Then of course $\nu(a)\le\nu(a)\nu(b)=\nu(ab)$ for all non-zero a, $b\in R$. If a, $b\in R\setminus\{0\}$, write $z=\frac{a}{b}\in\mathbb{C}$. Then there is a $q\in R$ such that $|z-q|<1$, because the members of R form a triangular lattice with side 1. So setting $r=a-bq\in R$ we have $|r|=|b||z-q|<|b|$ and either $r=0$ or $\nu(r)<\nu(b)$. Thus ν is a Euclidean valuation and R is a Euclidean domain.

(c) Let us begin by examining the invertible elements of R. Note first that if $u\in R$ is invertible in R, its inverse u^{-1} in R is just $\frac{1}{u}$, taken in $\mathbb{C}$; so that $|u^{-1}|=1/|u|$. Now because $|m+n\omega|^2=m^2-mn+n^2$ is an integer for all integral m and n, $|u|$ must be precisely 1. To find the integers m, n with $m^2-mn+n^2=1$, we have $m^2-mn+n^2=(m-\frac{1}{2}n)^2+\frac{3}{4}n^2=1$, so n must be 0, 1 or -1; now it is easy to see that the only members of R of modulus 1 are 1, -1, ω, $-\omega$, $1+\omega$ and $-1-\omega$, and that these are all invertible in R.

(i) If $2=ab$ in R, we have $|a|^2|b|^2=4$, while $|a|^2$ and $|b|^2$ are integers. If $|a|^2=1$ then a is invertible; if $|b|^2=1$ then b is invertible. The only other possibility is that $|a|^2=|b|^2=2$. **?** But if $a=m+n\omega$, with m, $n\in\mathbb{Z}$ and $|a|^2=2$, we have $4|a|^2=(2m-n)^2+3n^2=8$; because neither of 8, $8-3$ is a perfect square, this is not possible. **X** Thus 2 is irreducible.

(ii) If $2+\omega=ab$ we have $|a|^2|b|^2=3$ so one of $|a|^2$, $|b|^2$ is 1 and one of a, b is invertible. So $2+\omega$ is irreducible.

(c) Examining $2R$, we see that its points form a triangular lattice; a central triangle has vertices 0, 2 and $2(1+\omega)$. Every element of R is of the form $2q+r$ where r lies within or on this triangle. So every member of $R/2R$ is of the form $r^\bullet$ where r lies in or on the triangle, that is, is one of

$$0,\ 1,\ 2,\ 1+\omega,\ 2+\omega,\ 2+2\omega.$$

Now of course $0^\bullet=2^\bullet=(2+2\omega)^\bullet$, so we are reduced to at most four equivalence classes, being $0^\bullet$, $1^\bullet$, $(1+\omega)^\bullet=\bar\omega^\bullet$, $(2+\omega)^\bullet=\omega^\bullet$; and these are indeed all distinct because all the representatives 0, 1, $1+\omega$ and $2+\omega$ are distance less than 2 from each other, so their differences cannot belong to $2R$ (recalling that R has no elements of modulus strictly between 0 and 1).

The addition and multiplication tables of $R/2R$ are now defined by the identities $\bar\omega^\bullet+\bar\omega^\bullet=0^\bullet=\omega^\bullet+\omega^\bullet$, $\omega^\bullet\omega^\bullet=\bar\omega^\bullet$, $\bar\omega^\bullet\bar\omega^\bullet=\omega^\bullet$, $\omega^\bullet\bar\omega^\bullet=1$. Written out in full they are

[not available]

18. (a)(i) A *unique factorisation domain* is an integral domain R such that (α) every non-zero, non-invertible element of R is expressible as a product of irreducible elements (β) if $p_1, \ldots, p_m$, $q_1, \ldots, q_n$ are irreducible and $p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$ then $m = n$ and $p_1, \ldots, p_m$ can be re-ordered in such a way as to make each p_i an associate of the corresponding q_i.

(ii) If R is a unique factorisation domain then of course every non-zero, non-invertible element is expressible as a product of irreducibles. To see that irreducibles are prime, let p be irreducible, and suppose that p is a factor of ab; that $pc = ab$. If either a or b is 0, then it is a multiple of p; if either a or b is invertible then the other is a multiple of p. If none of these happen, then $ab \neq 0$ (because R is an integral domain) so $c \neq 0$; also, because p is ireducible, it cannot be a multiple of ab, so c is not invertible.

We may therefore express a, b, c as products of irreducibles,

$$a = q_1 \ldots q_k,\ b = q'_1 \ldots q'_m,\ c = p_1 \ldots p_n$$

and get $pp_1 \ldots p_n = q_1 \ldots q_k q'_1 \ldots q'_m$. Because factorisation in R is unique, we must have $k + m = 1 + n$ and also there must be an invertible e such that pe is one of the q_i or q'_j. But in this case, because every q_i is a factor of a and every q'_j is a factor of b, p is a factor of at least one of a, b. As a and b are arbitrary, p is prime, as required.

(iii) Now suppose that R satisfies the two conditions. To show that R is a unique factorisation domain we need to prove (β) of the definition above. Do this by induction on m. If $m = 1$ we have $p_1 = q_1 \ldots q_n$; but as p_1 is irreducible all but one of the q_i must be invertible, and this means that $n = 1$ and $q_1 = p_1$ is an associate of p_1. For the inductive step to $m + 1$ we have $p_1 \ldots p_m p_{m+1} = q_1 \ldots q_n$. Now this means that p_{m+1} is a factor of $q_1 \ldots q_n$; but p_{m+1} is irreducible and we are supposing that irreducibles are prime, so p_{m+1} is a factor of q_k for some $k \leq n$. Since q_k is also irreducible, there must be an invertible e such that $q_k = ep_{m+1}$. Now we have

$$p_1 \ldots p_m = eq_1 \ldots q_{k-1} q_{k+1} \ldots q_n$$

(because R is an integral domain, so we may cancel p_{m+1} from both sides). But eq_1 (or eq_2, if $k = 1$) is also irreducible, so the inductive hypothesis tells us that $m = n - 1$ and that $eq_1, \ldots, q_{k-1}, q_{k+1}, \ldots, q_n$ can be got by shuffling $p_1, \ldots, p_m$ and multiplying them by appropriate invertible elements. But this means that $m = n + 1$ and (since $q_k = ep_{m+1}$) the whole list $q_1, \ldots, q_n$ can be got by shuffling $p_1, \ldots, p_{m+1}$ and multiplying them by invertible elements. Thus the induction proceeds.

(b)(i) Set $R = \{m + n\gamma : m, n \in \mathbb{Z}\}$ where $\gamma = i\sqrt{5}$. Because $\gamma^2 = -5 \in \mathbb{Z}$, R is a subring of $\mathbb{C}$. If $r \in R$, set $\nu(r) = |r|^2 \in \mathbb{Z}$. Then $\nu(ab) = \nu(a)\nu(b)$ for all $a, b \in R$, and $\nu(a) \leq 1$ iff a is either 0 or ± 1, that is, is either 0 or invertible in R.

It follows that every non-zero non-invertible element a of R is expressible as a product of irreducibles. **P** Induce on $\nu(a)$. The induction starts with the vacuous case $\nu(a) = 1$. For the inductive step to $\nu(a) = n+1$, if a is itself irreducible, we can stop; otherwise it is expressible as bc where neither b nor c is invertible, so $\nu(b) > 1$ and $\nu(c) > 1$ and $\nu(b) < \nu(a)$ and $\nu(c) < \nu(a)$. By the inductive hypothesis both b and c are expressible as the products of irreducibles, so a also is. Thus the induction proceeds. **Q**

To see that R is not a unique factorisation domain, consider

$$(1+\gamma)(1-\gamma) = 6 = 2.3.$$

Because $\nu(1+\gamma) = 6 = \nu(1-\gamma)$, $\nu(2) = 4$, $\nu(3) = 9$ any non-trivial factor p of of any of these must have $\nu(p) = 1$, 2 or 3; in the first case p is invertible and the other two cases are impossible, as neither 2 nor 3 is expressible as $m^2 + 5n^2$. So $1+\gamma$, $1-\gamma$, 2 and 3 are all irreducible and the factorisation of 6 into irreducibles is not unique.

(ii) seems to be hard. If we are allowed Zorn's Lemma we may take a maximal subring R of $\mathbb{R}$ containing 1 but not containing $\frac{1}{2}$. R is a subring of $\mathbb{R}$ contining 1 so is an integral domain. It is not a field because $2 \in R$ is not invertible.

If $b \in R$ then $\frac{1}{1-2b} \in R$. To see this, set $x = \frac{1}{1-2b}$ and consider $R[x] = \{a_0 + a_1x + \ldots + a_nx^n : a_0, \ldots, a_n \in R\}$. **?** If $x \notin R$ then $R[x]$ is a subring of $\mathbb{R}$ strictly bigger than R; but as R is maximal, $R[x]$ must contain $\frac{1}{2}$, so that we have $a_0, \ldots, a_n \in R$ such that $a_0 + \ldots + a_nx^n = \frac{1}{2}$ and $2a_0(1-2b)^n + \ldots + 2a_n = (1-2b)^n$. But multiplying out this means that $1 = 2d$ for some $d \in R$, which is impossible. **X**

Next, if $c \in R$ and $c \geq 0$, we must have $\sqrt{c} \in R$. **P** Consider $R[\sqrt{c}] = \{a_0 + a_1\sqrt{c} : a_0, a_1 \in R\}$. This is a subring of $\mathbb{R}$ including R. **?** If it is not R it must contain $\frac{1}{2}$, so we have $\frac{1}{2} = a + b\sqrt{c}$ where $a, b \in R$. Now $(1-2b)\sqrt{c} = 2a$; but from the last paragraph we know that $\frac{1}{1-2b} \in R$ so $\sqrt{c} \in R$, which is absurd, as in this case $R[\sqrt{c}] = R$. **X** Thus $R[\sqrt{c}] = R$ and $\sqrt{c} \in R$, as claimed. **Q**

So suppose that $a \in R$ is not invertible. Then either $\sqrt{a}$ or $\sqrt{-a}$ belongs to R, and cannot be invertible, because a cannot be a product of invertible elements. So a is a product of non-invertible elements and is not irreducible.

We can do this without the axiom of choice by taking R to be the smallest subring of $\mathbb{R}$ containing 1 and such that $\frac{1}{1-2b} \in R$ for every $b \in R$, $\sqrt{a} \in R$ for every positive $a \in R$.

Now R cannot be a unique factorisation domain because 2 cannot be expressed as a product of irreducible elements.

19. (a) An *integral domain* is a ring R such that
multiplication in R is commutative;
R has a multiplicative identity $1 \neq 0$;
if $ab = 0$ then at least one of a, b is 0.

A *principal ideal domain* is an integral domain R such that every ideal in R is of the form aR for some $a \in R$.

Let R be an integral domain. Set $X = R \times (R \setminus \{0\})$ and define a relation $\sim$ on X by saying that $(a, b) \sim (c, d)$ if $ad = bc$. Because R is an integral domain, this is an equivalence relation on X. It is easy to check that if $(a, b) \sim (a', b')$ and $(c, d) \sim (c'd')$ then $(ad+bc, bd) \sim (a'd' + b'c', b'd')$ and $(ac, bd) \sim (a'c', b'd')$; consequently we may define addition and mutliplication on the set F of equivalence classes in X by setting $(a, b)^\bullet + (c, d)^\bullet = (ad + bc, bd)^\bullet$, $(a, b)^\bullet(c, d)^\bullet = (ac, bd)^\bullet$. It is straightforward to verify that F is a ring under these operations, with zero $0_F = (0_R, 1_R)^\bullet$. F has a multiplicative identity $1_F = (1_R, 1_R)^\bullet$ which is not equal to 0_F because $1_R 1_R = 1_R \neq 0_R = 1_R 0_R$. Finally F is a field, with the multiplicative inverse of $(a, b)^\bullet$ being $(b, a)^\bullet$ whenever a, $b \in R \setminus \{0\}$.

(b) If R is a principal ideal domain then (α) every non-zero, non-invertible element of R is expressible as a product of irreducible elements (β) if $p_1, \dots, p_m$, $q_1, \dots, q_n$ are irreducible and $p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$ then $m = n$ and there are invertible elements $e_1, \dots, e_n$ and a permutation π of $\{1, \dots, n\}$ such that $q_i = e_i p_{\pi(i)}$ for every i.

(c) (**Apology:** for 'distinct' read 'non-associate'.) If $r = 1$ this is trivial. So take $r > 1$. For each $i \leq r$ let $a_i = p_1^{k_1} \dots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \dots p_r^{k_r}$. Because R is a principal ideal domain there are $b_1, \dots, b_r \in R$ such that $d = b_1 a_1 + \dots + b_r a_r$ is a factor of every a_i. Any irreducible factor of d would have to be an associate of some p_i, for $i > 1$, because d is a factor of a_1; but it would also have to be an associate of some p_j, for $j \neq i$, because d is a factor of a_j; and this is impossible because p_i and p_j are not associates. Accordingly d is invertible and we have $q = qd^{-1}d = q'd$ say. Now $x = q' \sum_{i \leq r} b_i a_i / p_1^{k_1} \dots p_r^{k_r} = \sum_{i \leq r} q_i / p_i^{k_i}$ where $q_i = q' b_i$ for each i.

(d) We have $60 = 2^2.3.5$ while $15 = 3.5$, $20 = 2^2.5$ and $12 = 2^2.3$ are coprime; now we have $1 = 3.15 - 1.20 - 2.12$ so that $17 = 51.15 - 17.20 - 34.12$ and $\frac{17}{60} = \frac{51}{4} - \frac{17}{3} - \frac{34}{5}$.

20. No answer written out.

21. A *Euclidean domain* is an integral domain R with a *Euclidean valuation* $\nu : R \setminus \{0\} \to \{0, 1, 2, \dots\}$ such that

$\nu(a) \leq \nu(ab)$ for all a, $b \in R \setminus \{0\}$;

for all $a \in R$, $b \in R \setminus \{0\}$ there are q, $r \in R$ such that $a = bq + r$ and either $r = 0$ or $\nu(r) < \nu(b)$.

A *principal ideal domain* is an integral domain R such that every ideal in R is of the form aR for some $a \in R$.

If R is a principal ideal domain then (α) every non-zero, non-invertible element of R is expressible as a product of irreducible elements (β) if $p_1, \dots, p_m$, $q_1, \dots, q_n$ are irreducible and $p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$ then $m = n$ and there are invertible elements $e_1, \dots, e_n$ and a permutation π of $\{1, \dots, n\}$ such that $q_i = e_i p_{\pi(i)}$ for every i.

Set $\nu(a) = |a|^2$ for $a \in R \setminus \{0\}$. Then $\nu(m + ni) = m^2 + n^2 \in \mathbb{N}$ for $m + ni \in R \setminus \{0\}$. If a, $b \in R \setminus \{0\}$ then $\nu(ab) = \nu(a)\nu(b) \geq \nu(a)$. If $a \in R$, $b \in R \setminus \{0\}$ then $\frac{a}{b} \in \mathbb{C}$ must be within a distance $\frac{1}{\sqrt{2}}$ of some $q \in R$; now $r = a - bq$ has $|r| \leq \frac{1}{\sqrt{2}}|b|$ so either $r = 0$ or $\nu(r) \leq \frac{1}{2}\nu(b) < \nu(b)$, while $a = bq + r$. Thus ν is a Euclidean valuation on R and R is a Euclidean domain.

Suppose $m + ni$ is irreducible and $m^2 + n^2$ is not a prime in $\mathbb{Z}$; say $m^2 + n^2 = rs$ where r, $s \in Z$ and neither is ± 1. Note that if there were a non-trivial factorisation of $m - ni$ as ab, then $m + ni$ would be $\bar{a}\bar{b}$, which is not so; so $m - ni$ is also irreducible. We have $m^2 + n^2 = (m + ni)(m - ni)$, so by the unique factorisation theorem in R, r and s must be associates of $m + ni$ and $m - ni$; that is, multiples of these by 1, -1, i or $-i$. Accordingly $m + ni$ is either real or purely imaginary, that is, one of m, n is 0; and of course the other must be of the form $\pm p$ for some prime $p \in \mathbb{N}$. Finally, in this case, we cannot have $p = r^2 + s^2$, as then it would have a factorisation $(r + is)(r - is)$ in R which would give a factorisation of $m + ni$.

Now for the converse. If $\nu(m+ni) = m^2+n^2$ is a prime then it cannot be expressed as $\nu(a)\nu(b)$ unless one of $\nu(a)$, $\nu(b)$ is 1, so that $m+ni$ cannot be expressed as ab unless one of a, b is invertible in R. If p is a prime in $\mathbb{N}$ which is not the sum of two squares, but $p = (r + is)(r' + is')$ in R, then $\nu(p) = p^2 = \nu(r + is)\nu(r' + is')$, so $\nu(r + is)$ is either 1 or p or p^2. In the first case $r + is$ is invertible and in the third case $r' + is'$ is invertible; and the middle case is impossible because p is not the sum of two squares. So p is irreducible in R. Accordingly its associates $-p$, ip and $-ip$ are also irreducible in R.

22. (a) A *Euclidean domain* is an integral domain R with a *Euclidean valuation* $\nu : R\setminus\{0\} \to \{0,1,2,\dots\}$ such that

$\nu(a) \le \nu(ab)$ for all $a,\, b \in R\setminus\{0\}$;

for all $a \in R,\, b \in R\setminus\{0\}$ there are $q,\, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\nu(r) < \nu(b)$.

If R is an integral domain, an element p of R is *irreducible* if it is not 0, not invertible and whenever $p = ab$ then one of $a,\, b$ is invertible.

If R is an integral domain, an element of R is *prime* if it is not 0, not invertible and whenever p is a factor of a product ab then it is a factor of at least one of $a,\, b$.

A *principal ideal domain* is an integral domain R such that every ideal in R is of the form aR for some $a \in R$.

(b)(i) Let R be an integral domain and $p \in R$ a prime. Then of course p is non-zero and non-invertible. If $p = ab$, then p divides ab, so divides one of $a,\, b$; suppose the former, so that $a = pc$ and $p = ab = pcb$. Because R is an integral domain and $p \ne 0$ we may cancel p and get $1 = cb$, so that b is invertible. As a and b are arbitrary, p is irreducible.

(ii) Now suppose that R is a principal ideal domain and that p is irreducible. Then of course p is non-zero and non-invertible. Let $a,\, b$ be such that p divides ab. Then $pR + aR$ is an ideal of R, so is of the form dR; we have $d = pr + as$ for appropriate r and s, and also d is a common divisor of a and p. Let q be such that $p = dq$; then one of d and q must be invertible.

If d is invertible, we have $b = bd^{-1}d = bd^{-1}(pr + as) = pbd^{-1}r + abd^{-1}s$ which is a multiple of p because ab is.

If q is invertible then $d = pq^{-1}$ is a multiple of p while a is a multiple of d, so a is a multiple of p.

Because $a,\, b$ are arbitrary, p is prime.

(c) If R is a principal ideal domain, it is a *unique factorisation domain*, that is, it is an integral domain such that (α) every non-zero, non-invertible element of R is expressible as a product of irreducible elements (β) if $p_1,\dots,p_m,\, q_1,\dots,q_n$ are irreducible and $p_1p_2\dots p_m = q_1q_2\dots q_n$ then $m = n$ and $p_1,\dots,p_m$ can be re-ordered in such a way as to make each p_i an associate of the corresponding q_i.

(d) Because $\omega^2 = -1-\omega$, R is a subring of $\mathbb{C}$. (It is obvious that R is closed under addition and additive inverses and contains 0; to see that it is closed under multiplication, we note that $(m+n\omega)(m'+n'\omega) = (mm'-nn') + (mn'+m'n-nn')\omega \in R$ whenever $m+n\omega,\, m'+n'\omega \in R$.) As it also contains 1 and $\mathbb{C}$ is an integral domain, R is an integral domain. Now define $\nu : R\setminus\{0\} \to \mathbb{N}$ by setting $\nu(m+n\omega) = |m+n\omega|^2 = m^2 - mn + n^2$ for $m + n\omega \in R\setminus\{0\}$. Then we have $\nu(ab) = \nu(a)\nu(b) \ge \nu(a)$ whenever $a,\, b \in R\setminus\{0\}$. Now suppose that $a,\, b \in R$ and that $b \ne 0$. Examining the arrangement of the points of R in $\mathbb{C}$, we see that they are the vertices of a lattice made up of equilateral triangles of side 1. So every complex number is within a distance $\frac{1}{\sqrt{3}}$ of some member of R. In particular there is a $q \in R$ such that $|\frac{a}{b} - q| \le \frac{1}{\sqrt{3}}$. Now $|a - bq| \le \frac{1}{\sqrt{3}}|b|$ so setting $r = a - bq$ we have $a = bq + r$ and either $r = 0$ or $\nu(r) \le \frac{1}{3}\nu(b) < \nu(b)$.

We have $6 = 2.3 = 2(2+\omega)(1-\omega)$.

23. (a) $0 = a^2 - b^2 = (a+b)(a-b)$ (because R is commutative); so one of $a+b$, $a-b$ must be 0, that is, either $a = -b$ or $a = b$.

(b) The only solutions of $x^2 = 1 = 1^2$ are $x = \pm 1$. (It can, of course, happen that $1 = -1$, but it doesn't matter.) For all other non-zero x, $x \neq x^{-1}$. So if we multiply all the non-zero elements of F together, we have a collection of products $x.x^{-1}$, all equal to 1, together with -1 and (if $1 \neq -1$) 1 itself, and the product of the whole lot is either -1 or -1.1; in either case the answer is -1.

(c) In the field $\mathbb{Z}_p$, $1 \times_p 2 \times_p \ldots \times_p p-1 = -1$, by (b); so in $\mathbb{Z}$ we must have $1.2.\ldots.p-1 \equiv -1 \bmod p$, as claimed.

(d) The point is that q is even. Now $(p-1)! = q!(p-q)(p-q+1)\ldots(p-1)$; modulo p, we have $p-k \equiv -k$ for each k, so that $-1 \equiv (p-1)! \equiv q!(-1)^q q! = (q!)^2$.

(e) Yes, because it is a Euclidean domain (a valuation is $\nu(a) = |a|^2$); and every Euclidean domain is a principal ideal domain, every principal ideal domain is a unique factorisation domain.

(f) Setting $q = (p-1)/2$, we have $(q!)^2 \equiv -1 \bmod p$, that is, $(q!)^2 + 1$ is a multiple of p; accordingly, setting $n = q!$, there is a k such that $(n-i)(n+i) = kp$. But of course p cannot divide either $n+i$ or $n-i$ (because $p(m+m'i) = pm + pm'i$ will always have imaginary part divisible by p). So p cannot be a prime.

p is therefore not irreducible (because R is a unique factorisation domain). Suppose that $p = rr'$ where r, $r' \in R$ are non-invertible. Now $p^2 = |r|^2|r'|^2$ so $|r|^2$ is either 1 or p or p^2. The first is impossible because the only elements of R of modulus 1 are ± 1, $\pm i$ and all of these are invertible. Similarly $|r'| \neq 1$ and $|r|^2 \neq p^2$. So $p = |r|^2$. But if $r = a + ib$ then $p = a^2 + b^2$ is a sum of two squares.

24. No answer written out.

25. No answer written out.

26. (a) Let $f \in R[x]$ be non-constant and irreducible in $R[x]$. **?** Suppose, if possible, that f is reducible in $F[x]$; say $f = g \times h$ in $F[x]$, where neither g nor h is invertible in $F[x]$. Then we can express g as γg_1 where $\gamma \in F$ and $g_1 \in R[x]$ is primitive in $R[x]$. Now g_1 is primitive in $R[x]$ and is a factor of f in $F[x]$, so must be a factor of f in $R[x]$; say $f = g_1 \times h_1$ in $R[x]$.

But now observe that because $f \neq 0$, neither g nor h is zero; and as F is a field, it follows that neither is constant, so that the degree of g is strictly between 0 and $\deg(f)$, and the degree of g_1 is the same. So neither g_1 nor h_1 can be constant, and therefore neither can be invertible in $R[x]$; and f is not irreducible. **X**

(The argument above relies on the following two facts: **(i)** If R is a unique factorisation domain and F its field of fractions, then every non-constant polynomial in $F[x]$ can be expressed in the form γg where $\gamma \in F$ and $g \in R[x]$ is primitive; **(ii)** If F is a field and $R \subseteq F$ is a subring which is (in itself) a unique factorisation domain, and if $f \in R[x]$ is primitive, then any $g \in R[x]$ which is a multiple of f in $F[x]$ is a multiple of f in $R[x]$. It is good style to write out such basic facts clearly, even if not explicitly asked. In some moods an examiner might expect you to write out the proof of one or more of these.)

(b)(i) The polynomial $2x^2 + x + 2$ is irreducible in $Z[x]$ (because the only possible non-trivial factors are of the form $mx + n$ where m, n are ± 1 or ± 2, and none of these work, by the Remainder Theorem); by the result of (a), $2x^2 + x + 2$ is irreducible in $\mathbb{Q}[x]$; now its associate $x^2 + \frac{1}{2}x + 1$ must also be irreducible.

(ii) $4x^3 + 3x + 2 = (2x + 1)(2x^2 - x + 2)$ so $x^3 + \frac{3}{4}x + \frac{1}{2} = (x + \frac{1}{2})(x^2 - \frac{1}{2}x + 1)$.

(iii) In $\mathbb{Z}[x]$ the only possible factors of degree 1 are $\pm x \pm 1$ (none of which work) and the only possible quadratic factors are of the form $\pm x^2 + mx \pm 1$. If we try multiplying two of these together to get the required polynomial we have

$$\begin{aligned} x^4 + x^3 + x^2 + x + 1 &= (\pm x^2 + mx \pm 1)(\pm x^2 + nx \pm 1) \\ &= \pm x^4 + (\pm m \pm n)x^3 + (\pm 1 \pm 1 \pm mn)x^2 + (\pm m \pm n)x \pm 1. \end{aligned}$$

Examining the coefficients of x^3, x we see that one of m, n must be even; but examining the coefficient of x^2 we see that mn must be odd. So this won't work either.

Accordingly $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}[x]$ and therefore in $\mathbb{Q}[x]$.

None of these polynomials is irreducible in $\mathbb{C}[x]$, by the fundamental theorem of algebra.

27. No answer written out.

28. No answer written out.

29. No answer written out.

30. No answer written out.

31. (a) If R is an integral domain, an element p of R is *irreducible* if it is non-zero, non-invertible and not expressible as ab for any pair of non-invertible elements a, b of R.

In $\mathbb{Z}_2[x]$ the irreducible quadratic is $x^2 + x + 1$ and the irreducible cubics are $x^3 + x + 1$, $x^3 + x^2 + 1$.

(b) $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ is not irreducible. $x^4 + x + 1$ is irreducible because by the Remainder Theorem it has no linear factors and it is not equal to $(x^2 + x + 1)^2$, which is the only reducible quartic without linear factors.

32. (a) (Not written out)

(b) $x^2 + 0 = x \times x$ and $x^2 + 2 = (x + 1)(x + 2)$ are not irreducible; while $x^2 + 1$ is irreducible because (by the Remainder Theorem) it has no linear factor.

(c) Setting $\xi = x^\bullet$, the equivalence class of x in the quotient $F = R/pR$, and $1 = 1_R^\bullet$, $0 = 0_R^\bullet$, we get

$$F = \{0, 1, 2, \xi, \xi + 1, \xi + 2, 2\xi, 2\xi + 1, 2\xi + 2\}.$$

Computing powers in F, we have $\xi^2 = 2$, $\xi^3 = 2\xi$, $\xi^4 = 1$; now $(\xi+1)^2 = 2\xi$, $(\xi+1)^3 = 2\xi+1$, $(\xi+1)^4 = 2$, $(\xi + 1)^5 = 2\xi + 2$, $(\xi + 1)^6 = \xi$, $(\xi + 1)^7 = \xi + 2$, $(\xi + 1)^8 = 1$. So $\xi + 1$ (or $2\xi + 1$ or $2\xi + 2$ or $\xi + 2$) is a generator of $F \setminus \{0\}$.

33. No answer written out.

34. No answer written out.